Citrix Virtual Apps and Desktops 7 2407

Contents

Citrix Virtual Apps and Desktops 7 2407

August 17, 2024

> 重要:
>
> 最新リリース(CR)および長期サービスリリース(LTSR)の製品ライフサイクル戦略は、Lifecycle Milestonesで説明しています。

Citrix Virtual Apps and Desktops は、データセキュリティを強化し、コストを削減し、生産性を向上させながら、あらゆるデバイスやネットワーク経由でアプリケーションやデスクトップを配信するための仮想化ソリューションを提供します。

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

累積更新プログラム 5（CU5）は、2203 LTSR の最新の更新プログラムです。LTSR は、Citrix Virtual Apps and Desktops 1912 でも利用できます。

- ユースケースについては、https://www.citrix.com/products/citrix-virtual-apps-and-desktops/を参照してください。
- Citrix Virtual Apps and Desktops 環境のコンポーネントおよびテクノロジについては、「製品の技術概要」を参照してください。

以前のリリース

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

これ以前のリリースのドキュメントは、「古いドキュメント」にアーカイブされています。

Citrix Cloud の Citrix Virtual Apps and Desktops

Citrix Cloud Virtual Apps and Desktops オファリングと Citrix DaaS は同じ内容です。詳細については、「Citrix DaaS」を参照してください。

便利なリンク

- Citrix Supportability Pack
- LTSR に関するよくある質問（FAQ）
- Citrix Virtual Apps and Desktops サービスオプション

- 製品のライフサイクル日程
- Citrix Workspace アプリ用の LTSR プログラム

Citrix Virtual Apps and Desktops 7 2407

August 17, 2024

このリリースについて

この Citrix Virtual Apps and Desktops リリースには、新しいバージョンの Windows Virtual Delivery Agent（VDA）といくつかのコアコンポーネントの新しいバージョンが含まれています。次の操作を実行できます:

- サイトのインストールまたはアップグレード：このリリースの ISO を使用して、コアコンポーネントと VDA をインストールまたはアップグレードします。最新のバージョンをインストールまたはアップグレードすることで、最新の機能を使用できます。
- 既存のサイトで **VDA** をインストールまたはアップグレードする：環境でコアコンポーネントをアップグレードする準備が整っていない場合でも、新しい VDA をインストール（またはアップグレード）することで、最新の HDX 機能を使用できます。VDA のみをアップグレードすると、強化された機能を実稼働環境以外の環境でテストするのに役立ちます。

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

インストールとアップグレードの手順については、以下を参照してください:

- 新しいサイトを構築する場合は、「インストールと構成」の手順に従います。
- サイトをアップグレードする場合は、「環境のアップグレード」を参照してください。

Citrix Virtual Apps and Desktops 7 2407

セキュアなデフォルト設定

VDA インストーラーには、よりセキュアな初期構成を実現するために、さまざまな機能のデフォルト設定を有効から無効に変更する新しいオプションがあります。詳しくは、「Install Capture」を参照してください。

使用状況テレメトリレポートの機能強化

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

この機能強化を活用するには、ライセンスサーバーを最新バージョンに更新してください。詳しくは、次のトピックを参照してください:

- Citrix ライセンステレメトリ
- 必要なライセンスサーバーの更新
- Citrix ライセンステレメトリのよくある質問

ライセンステレメトリのデータ要素の一覧については、「Citrix ライセンステレメトリのデータ要素」を参照してください。

仮想ループバックポートの除外

特定のポートを仮想ループバックから除外するオプションが追加され、指定されたポートのループバックアドレスへのアプリケーションによる呼び出しが、セッション固有のループバックアドレスに変更されなくなりました。詳しくは、「仮想ループバック」を参照してください。

シームレスなアプリのために **LogonUI** ウィンドウのスケーリングを向上

認証パススルーが発生しないシナリオで、**LogonUI** ウィンドウのスケーリングが向上しました。LogonUI ウィンドウは、使用されているモニターの解像度と DPI 設定に基づいて拡大縮小され、クリッピングされることなく LogonUI ウィンドウ全体が表示されるようになります。
詳しくは、「公開アプリケーションを開いたときに Windows の免責事項メッセージをフルサイズで表示するように LogonUI を変更する方法」を参照してください。

公開アプリケーションのサインアウトチェッカーの機能強化

この新しい機能により、システムで構成されているスタートアップアプリを自動的に検出し、それらをシステムプロセスの一覧に自動的に追加するオプションが提供されるようになりました。これにより、最後に公開されたアプリケーションウィンドウが閉じられたときに、これらのアプリケーションがサインアウトをブロックすることがなくなります。
詳しくは、「公開アプリケーションでのセッションサインアウトの問題のトラブルシューティング」を参照してください。

Virtual Delivery Agent（VDA）2407

サードパーティの **VDA** 展開方法のドキュメントの再構成

サードパーティの VDA 展開ページが再構成され、追加の詳細な手順が含まれるようになりました。詳しくは、「サードパーティの VDA 展開」を参照してください。

MCS 以外でプロビジョニングされた **VDA** のトークンベースの **VDA** 登録（**Technical Preview**）

この機能では、MCS 以外でプロビジョニングされた VDA の登録トークンを生成および管理できるようになりました。この実装により、MCS を使用して VDA をプロビジョニングせずに、WebSocket 経由で VDA を登録できるようになります。この機能は、Linux Virtual Delivery Agent、Citrix Virtual Delivery Agent for macOS、および Citrix Virtual Apps and Desktops を使用したドメイン非参加の VDA もサポートします。詳しくは、「トークンを使用した MCS 以外でプロビジョニングされた VDA の登録」を参照してください。

Web Studio

コンテキストに基づく **App Protection**

この機能を使用すると、管理者は、コントロールを常に有効または常に無効にするのではなく、状況に応じてデバイスとユーザーに App Protection のスクリーンキャプチャ対策とキーロガー対策の制御を適用できます。この実装により、必要な場合にのみ App Protection のスクリーンキャプチャ対策とキーロガー対策を適用できるようになります。詳しくは、「App Protection の管理」を参照してください。

スマートカード認証のサポート

Web Studio はスマートカード認証をサポートするようになり、管理者は PIV カードと CAC カードを使用して Web Studio にアクセスするようになりました。詳しくは、「Web Studio のスマートカード認証の設定」および「スマートカード認証の有効化」を参照してください。

テナント管理

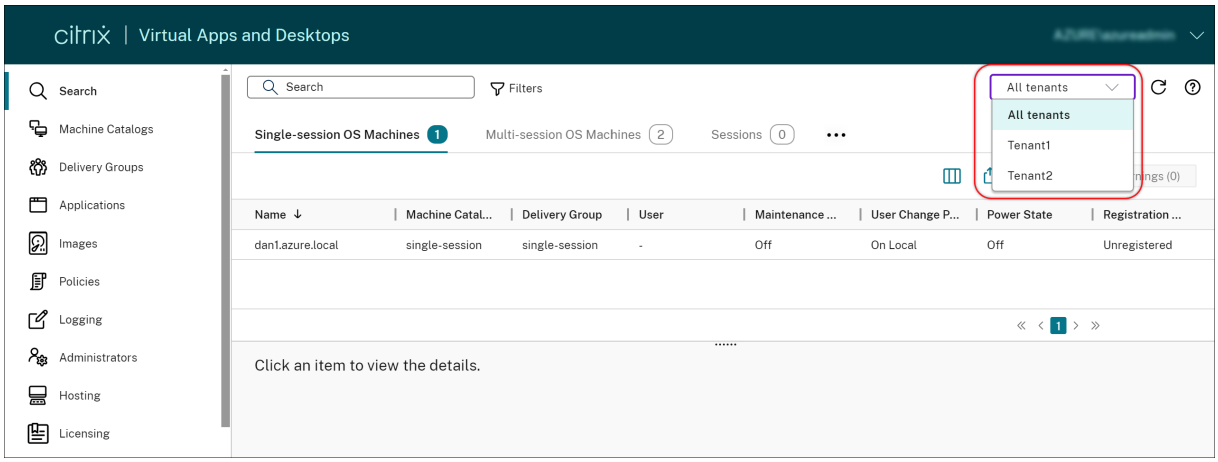
テナント管理によって、単一の Citrix Virtual Apps and Desktops サイト内に管理パーティションを作成できるようになりました。この機能は、次のような組織に最適です：

- さまざまなビジネスサイロ（独立した部門または個別の IT 管理チーム）で業務を行っている。
- Citrix サービスプロバイダーなどの複数の顧客にサービスを提供している。

テナント管理を設定するには、次の手順を実行します：

1. テナントを作成します。［管理者］**>**［スコープ］に移動してテナントスコープを作成し、それらのスコープを関連するリソースや構成（マシンカタログやデリバリーグループなど）と関連付けます。
2. テナントの管理者を追加します。［管理者］**>**［管理者］に移動して、必要に応じてユーザーアカウントに役割やテナントをアサインします。

テナントへの適切なアクセス権を持つ管理者は、Web Studio の右上隅にある ［すべてのテナント］ドロップダウンリストでテナントの名前を表示して選択できます。次に、そのテナントにのみ関連付けられているリソースと構成を管理します。詳しくは、「テナント管理の設定」を参照してください。



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

デフォルトでは、MCS または Citrix Provisioning を使用してプロビジョニングされた、シングルセッションのプールされた VDA は、LHC モードでは使用できません。Web Studio では、デリバリーグループごとにこのデフォルトの動作を上書きできるようになり、LHC 中の新しい接続でそれらの VDA を利用できるようになります。詳しくは、「デリバリーグループの作成」と「デリバリーグループの管理」を参照してください。

VDA 登録トークンの生成と管理

トークンベースの VDA 登録により、Cloud Connector の負荷が軽減され、潜在的な障害ポイントが減少します。Web Studio を使用すると、MCS 以外でプロビジョニングされた VDA の登録トークンを生成および管理できるようになり、登録トークンベースの導入を効率化できます。詳しくは、「登録トークンの生成と管理」を参照してください。

永続的なマルチセッション **VM** の作成

マルチセッションマシンのカタログ作成時に、それらを永続化するかどうかを指定できるようになりました。永続的なマルチセッションマシンの場合、ユーザーがデスクトップに加えた変更は保存され、すべての承認されたユーザー

がアクセスできることに注意してください。詳しくは、「マシンカタログの作成」を参照してください。

ピーク時の **Autoscale** が割り当てた電源オン

永続デスクトップが電源オンになっているのに未使用のままである場合、またはユーザーがログオンしていない場合、管理者は、何もしない、一時停止、またはシャットダウンなどのアクションを実行するまでの待機時間を定義できます。

- 割り当て済みのマシンについて、そのマシンの電源がオンになっていて、ピーク時間の開始後の設定時間内にセッションが接続されていない場合、マシンの電源をオフにするポリシーをデリバリーグループレベルで追加できます。
- 割り当て済みのマシンについて、そのマシンが再開状態にあるのに、ピーク時間の開始後の設定時間内にセッションが接続されていない場合、マシンを一時停止するポリシーをデリバリーグループレベルで追加できます。

この機能は、有給休暇を取っているエンドユーザーやログオンしていないエンドユーザーがいる場合、または会社に長い週末休暇がある場合に役立つものであり、Azure の消費コストを軽減するために待機時間とマシンの切断アクションを設定できます。詳しくは、「シングルセッション OS のランダムデリバリーグループ」および「シングルセッション OS の静的デリバリーグループ」を参照してください。

パッケージアプリケーションをシングルセッションの静的デスクトップおよびオフィス **PC** に配信

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

- デリバリーグループの作成中に、アプリケーションを追加します。
- 次のいずれかのエントリを使用して、既存のデリバリーグループにアプリケーションを追加します:［デリバリーグループ］**>**［アプリケーションの追加］**>**［アプリケーション］、［アプリケーション］**>**［プロパティ］**>**［グループ］、または ［アプリパッケージ］**>**［パッケージ］**>**［デリバリーグループの追加］。

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

デスクトップの表示名の変更

シングルセッション **OS** の静的デリバリーグループの ［マシン割り当て］ページの機能が拡張され、新しい列 ［表示名］が導入されました。この追加により、ユーザーに割り当てられたマシンのデスクトップ表示名を変更できるようになりました。詳しくは、「ユーザー割り当ての管理」を参照してください。

検索ノードの［セッション］タブからのシングルセッションマシンの再起動とシャットダウン

検索ノードの ［セッション］タブで、異常な状態のユーザーセッションを検索し、同じタブ内で関連するシングルセッションマシンをシームレスに再起動またはシャットダウンできるようになりました。この機能により効率が向上し、単一インターフェイス内で特定されたセッションの問題に対して迅速な対応が可能になります。

ライトバックキャッシュディスクへのドライブ文字の割り当て

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

失敗した後にカタログの作成を再試行

カタログの作成が失敗した場合に、カタログの作成を再試行できるようになりました。正常に作成するには、まずトラブルシューティング情報を確認してから、問題を解決します。この情報は、見つかった問題について説明し、それらを解決するための推奨事項を提供します。失敗したカタログにはエラーアイコンが表示されます。詳細を確認するには、各カタログの ［トラブルシューティング］タブに移動します。詳しくは、「マシンカタログの管理」を参照してください。

構成ログでクライアント **IP** を表示

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

コンテキストヘルプの強化

情報の提供に役立つようにヘルプパネルを再設計したため、Web Studio 内の各ノードに対象を絞った情報が提供されます。任意のノードのヘルプアイコンをクリックすると、1 か所で学習エクスペリエンスを提供することを目的とした包括的なリソースのセットにアクセスでき、関連する機能の理解を深めることができます:

- 選択したノードに特に関連する主要なドキュメントにアクセスできます。
- Citrix ロードマップ、既知の問題、制限、システム要件、新機能などのサービス更新に関する最新情報を入手できます。
- Citrix ブログ、Citrix コミュニティ、Citrix 機能の説明、Citrix 製品ドキュメント、Citrix サポート、開発者ドキュメントなどの詳細なリソースにアクセスできます。

強化された検索

次の新機能を導入して、検索ノードを強化しました:

- 精度を高め、使いやすさを向上させるための、ゾーンとプロビジョニングの種類という 2 つの新しいフィルター。
- 2 つの新しい列:
  - ［セッション］タブの ［ユーザー表示名］列。この列を使用すると、特定のユーザーに関連付けられたセッションをすばやく特定できます。
  - ［シングルセッション **OS** マシン］タブと［セッション］タブの両方の ［デスクトップ表示名］列。この列を使用すると、特定のデスクトップに関連付けられているマシンをすばやく特定できます。
- 効率的な検索のための新しいフィルター。これら 2 つの列について詳しくは、「マシンの操作と列」および「セッションの操作と列」を参照してください。
- 検索およびマシンカタログノードの検索パネルにフィルターピンを配置し、頻繁に使用する検索フィルターをページ上でアクセスできるようにしておきます。

アプリケーションノードの機能強化

アプリケーションノードに次の機能強化が実装されました:

- ［表示する列］および［エクスポート］列の機能が、アプリケーションとアプリケーショングループの両方のタブに拡張されました。右上隅に新しく導入されたアイコンを使用すると、アプリケーションとアプリケーショングループのメインビューをカスタマイズし、それらのビューからレコードを CSV ファイルにエクスポートできるようになりました。
- アプリケーションの［詳細］ペインに［ゾーン］フィールドが追加され、アプリケーションが存在するゾーンを表示できるようになりました。この情報は、同じ名前を共有している一方で異なるゾーンから発信されたアプリケーションを区別するときに役立ちます。詳しくは、「ゾーン」を参照してください。

マシンカタログノードとホストノードのデータキャッシュ

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

より柔軟なリソースのアクセス制御のために再設計されたアクセスポリシー **UI**

［デリバリーグループの編集］**>**［アクセスポリシー］の UI を再設計することによって、デリバリーグループのリソースアクセスをより柔軟に管理できるようになりました。新しい設計で利用できる主な機能は次のとおりです:

- ポリシーの追加のサポート。アクセスポリシーを追加して、ユーザー接続の属性に基づいてリソースへのアクセスを制限できるようになりました。ポリシーは、次の 2 種類の基準で構成されます:
  - 包含基準。デリバリーグループへのアクセスを許可するユーザー接続を指定できます。
  - 除外基準。デリバリーグループへのアクセスを禁止するユーザー接続を指定できます。
- 拡張されたフィルターのサポート。さまざまな SmartAccess フィルターを使用して、包含基準と除外基準を定義できるようになりました。これらのフィルターには、`Citrix.Workspace.UsingDomain`や`Citrix-Via-Workspace`などの Workspace フィルターや、ネットワークの場所ベースのアダプティブアクセス用のフィルターが含まれます。
- 含まれる基準に対するすべて一致のロジックのサポート。新しいロジックにより、デリバリーグループに対して許可されるユーザー接続を指定する場合に、高レベルの精度と制御を実現できます。

詳しくは、「デリバリーグループ内のリソースへのアクセスを制限」を参照してください。

AWS カタログ作成のための高度なイメージフィルタリング

AWS カタログの作成中にマシンテンプレートを選択する場合、次の検索基準を使用してターゲットテンプレートの AWS AMI インベントリをフィルタリングできるようになりました:

- イメージ名
- イメージ ID
- イメージタグ

マシンテンプレート一覧は、一覧を下にスクロールすると動的に読み込まれます。最初に 25 個の項目が読み込まれ、スクロールするとさらに多くの項目が読み込まれます。

AWS で休止状態をサポートする **VM** の作成をサポート

AWS 環境で仮想マシン（VM）の休止状態をサポートするマシンカタログを作成できるようになり、展開での全体的な費用対効果が向上します。関連するマシンプロファイルがこの機能をサポートしている場合は、カタログを編集して休止状態対応 VM を含めることもできます。詳しくは、「休止状態」を参照してください。

新しいポリシー検証

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

ポリシーセット

［**Web Studio**］**>**［ポリシー］で、ポリシーセットを使用して役割ベースのアクセスをシンプルにするために、ポリシーをグループ化できるようになりました。ポリシーセットにスコープとデリバリーグループを割り当てて、権限のある管理者のみが関連するユーザーとマシンに適用されるポリシーを管理できるようにします。詳しくは、「ポリシーセット」を参照してください。

ポリシーの複数選択

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

1. ポリシー行をクリックする: ポリシー行をクリックすると、上部の操作バーに 1 つのポリシーのアクションが表示されます。下部の詳細ペインには、ポリシーに関する情報が表示されます。
2. 複数のポリシーのチェックボックスを選択する: ステータスが有効または無効になっている複数のポリシーのチェックボックスを選択すると、上部の操作バーに複数のポリシーのアクションが表示されます。下部の詳細ペインには、選択したポリシーの数が表示されます。

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

依存ポリシーの明確化

一部の設定は他の設定に依存します。以前は、ポリシー設定は相互に依存していても、設定間の関係は明確ではありませんでした。たとえば、子設定が構成されている場合でも、その親設定が有効になっていないと、構成された子設定は有効になりません。以前はその依存関係が明確ではありませんでした。このリリース以降、子ポリシーを構成する前に最初に構成する必要がある親ポリシーが明確に示されるようになりました。詳しくは、「ポリシー設定」を参照してください。

シンプルになったマシンカタログのサブネットの更新

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

新しいポリシー設定 **-** セッションメトリックの収集

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

Citrix は、オペレーティングシステム、稼働時間、コンピューターシステム情報、ビデオコントローラの詳細、VDA のバージョン、展開の種類、ドメイン参加のステータスなどのデータを収集します。さらに、パフォーマンスと信頼性のデータとともにいくつかのセッション構成を収集して、製品の品質向上に役立てることもできます。デフォルトでは、有効になっています。詳しくは、「セッションメトリックの収集」を参照してください。

Secure Private Access と **Web Studio** との統合

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

Citrix Director

ダッシュボード上のアプリケーション使用状況の監視グラフ

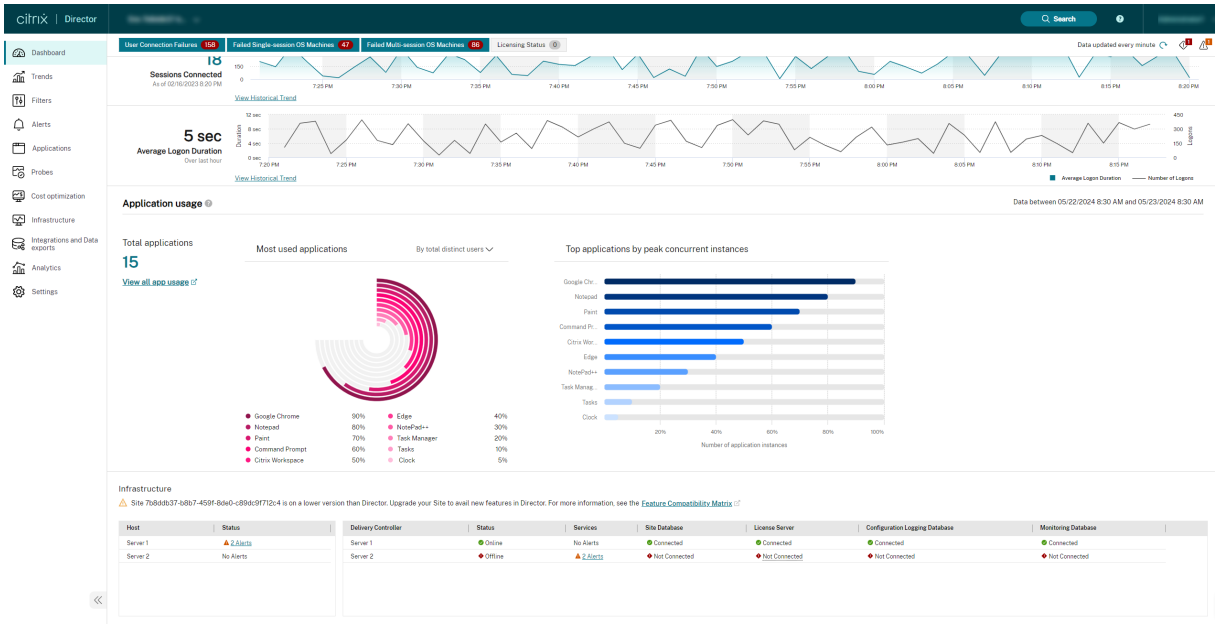
Citrix Director を使用すると、公開アプリケーションの使用状況を監視できるようになります。この機能はダッシュボードに存在し、IT 管理者やアプリケーション管理者が、どのアプリケーションが頻繁に使用されているか、およびその使用範囲を把握するのに役立つ、選択されたグラフが表示されます。

これらのグラフは、過去 24 時間の次のデータポイントで構成されています:

- 使用中のアプリケーション数の合計
- 最も使用されたアプリケーション（最大 10 件）（個別ユーザー数合計ごと）
- 最も使用されたアプリケーション（最大 10 件）（アプリケーション起動数合計ごと）
- 上位のアプリケーションの最大同時インスタンス数

この視覚化により、お客様は人気のある公開アプリケーションを可視化し、消費に対する使用権の効果を分析して、ソフトウェアライセンスの購入にかかるコストを最適化できます。

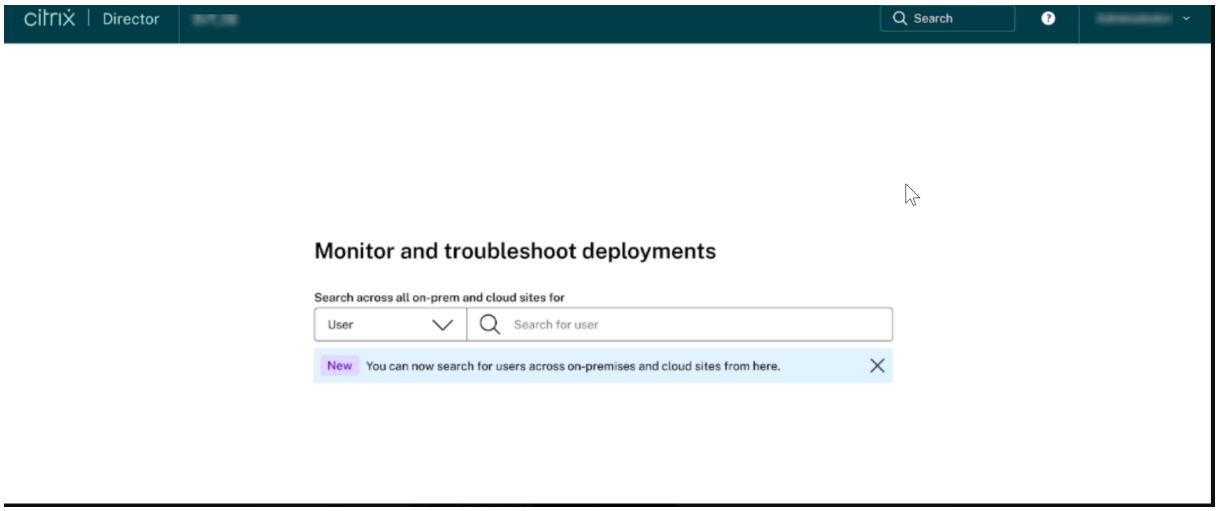
> 注:
>
> この機能は、Platinum ライセンスのサイトでのみ利用できます。

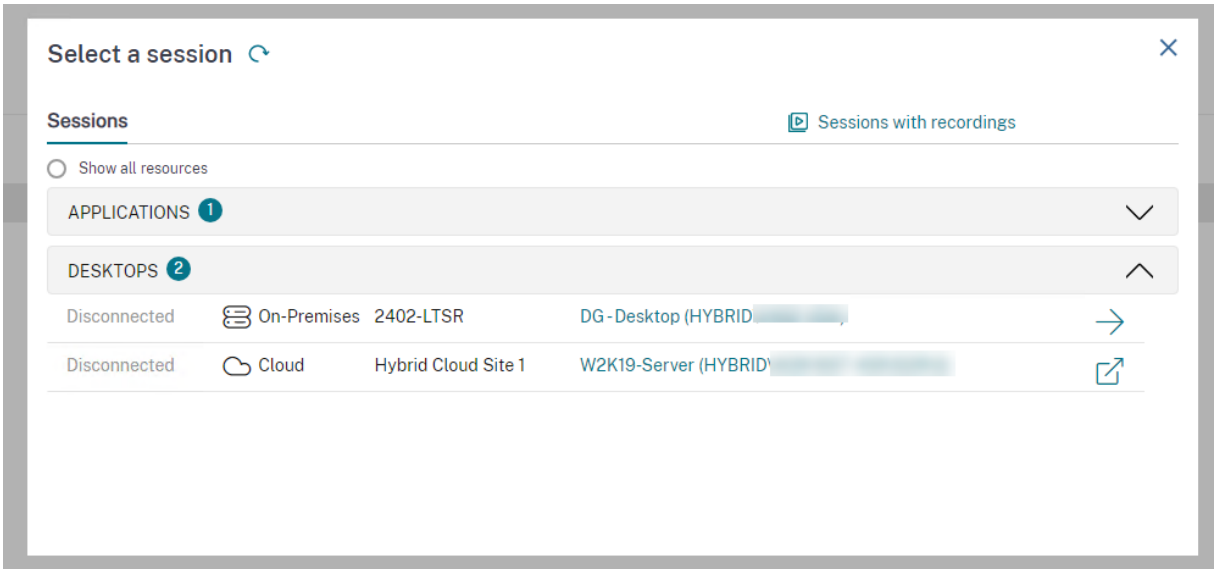


詳しくは、「ダッシュボード上のアプリケーション使用状況の監視グラフ」を参照してください。

クラウドとオンプレミスのユーザー向けの統合検索

以前は、トリアージ中に Director でユーザーを検索すると、ユーザーがオンプレミスサイトのユーザーである場合にのみユーザーの詳細が取得されました。ユーザーがクラウドサイトのユーザーである場合は、Monitor に移動して再度検索する必要がありました。この強化された検索機能により、Director の検索オプションを使用して、クラウドサイトまたはオンプレミスサイトからユーザーを検索できるようになります。この機能により、問題解決までの平均時間が短縮され、データベースのサイズが急激に増大することなく、単一のコンソールによるシームレスなエクスペリエンスが提供されます。





詳しくは、「クラウドとオンプレミスのユーザー向けの統合検索」を参照してください。

セッションログオンビューの機能が向上

［フィルター］>［ユーザーの詳細］ページの ［セッションログオン］タブの、新しい［マシンのスタートアップ］オプションの次のサブセクションでは、さまざまなフェーズで仮想マシンの起動に必要な時間の内訳が表示されます:

- 電源投入 - 仮想マシンの電源オンにかかる時間を表示します
- 起動と登録 - 仮想マシンの起動と登録にかかる時間を表示します

［セッションログオン］ページに新しく導入された折りたたみ可能なボタンを使用すると、［マシンのスタートアップ］と ［対話型セッション］のオプションを折りたたんだり展開したりできます。

デフォルトの ［ログオン期間の段階］テーブルオプション（セッションログオン段階と期間）に加えて、［セッションログオン］ページで次の列を選択することもできます:

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

上記のデータを.CSV ファイルにエクスポートすることもできます。

新しく追加された列 ［電源投入］と ［起動と登録］は、［傾向］>［ログオンパフォーマンス］>［列の選択］の ［ユーザーセッションごとのログオン期間］テーブルに追加できます。［ログオンパフォーマンス］画面でレポートをエクスポートすることもできます。

この機能強化は、ログオン期間に関連する問題を理解し、トラブルシューティングを容易にするのに役立ちます。詳しくは、「ユーザーログオンの問題の診断」を参照してください。

ICA 往復時間またはセッションのログオン期間のデータの入力に失敗した場合のトラブルシューティングのオプション

以前は、EUEM サービスまたは Profile Management サービスの実行に失敗した場合、ICA 往復時間またはセッションのログオン期間に関連するデータの取得に失敗した理由は表示されませんでした。この新機能を使用すると、失敗の理由とそれに対応する解決策を取得できます。

詳しくは、「ICA 往復時間またはセッションのログオン期間のデータの入力に失敗した場合のトラブルシューティングのオプション」を参照してください。

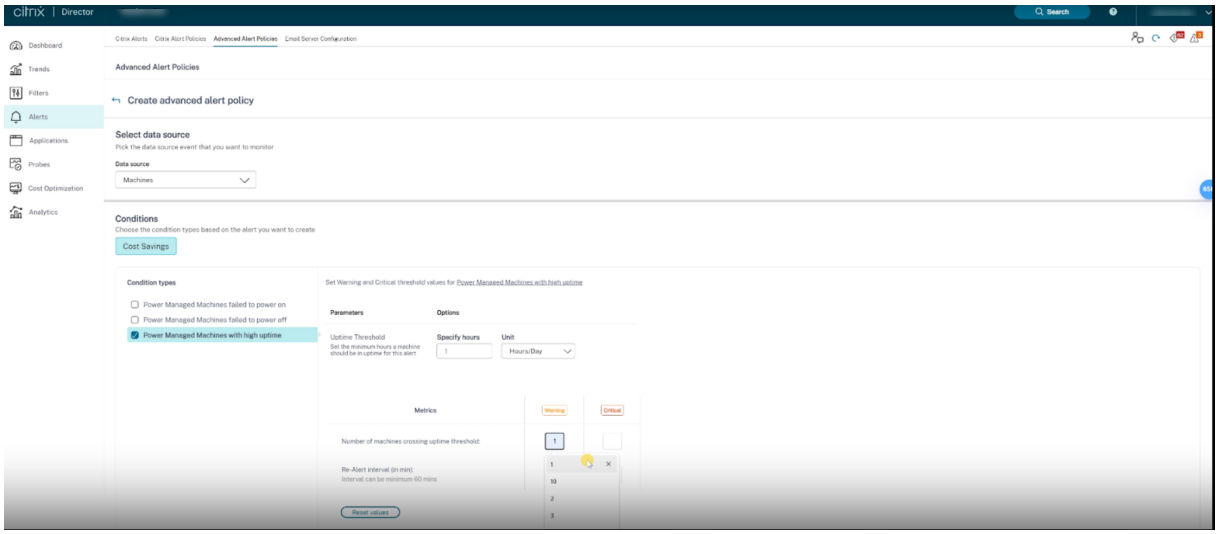
公開デスクトップ名

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

高度なアラートポリシー

Director の積極的な通知およびアラート機能が強化され、高度なアラートポリシーという新しいアラートフレームワークが追加されました。この機能を使用すると、各要素または条件の詳細を含めてアラートを作成できるため、アラートのスコープをより細かく制御できます。現在、これらのポリシーにはコスト削減とインフラストラクチャに関するアラートが含まれています。

この機能を使用すると、重要な問題に対処する際の応答性や有効性の低下につながる可能性のある、過剰なアラートを削減できます。このポリシーは、アラートポリシーの有効性と管理者の関与を測定するのに役立ちます。



詳しくは、「高度なアラートポリシー」を参照してください。

アラートコンテンツの機能強化

Director のアラート機能が強化され、CSV 添付ファイルと JSON ペイロードが含まれるようになりました。この機能強化により、アラートの詳細をメールの CSV 添付ファイルで取得したり、webhook がある場合は JSON ペイロードとして取得したりできるようになります。この CSV 添付ファイルや JSON ペイロードを使用すると、詳細なレベルで充実したコンテンツを受け取ることができ、問題を迅速に特定して解決するのに役立ちます。

現在、この機能強化は次のアラートでのみ利用可能です:

- マシンの稼働時間
- 電源オン操作の失敗
- 電源オフ操作の失敗
- 未登録のマシン（%）

詳しくは、「アラートコンテンツの機能強化」を参照してください。

セッションの種類と最終起動時間を表示およびフィルタリングするオプション

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

同様に、［最終起動時間］を見つける新しいオプションを ［フィルター］>［マシン］セクションに追加できます。［最終起動時間］を ［フィルター］>［セッション］>［列の選択］で、新しい列として追加することもできます。

セッションとアプリケーションインスタンスで期間ごとにデータをフィルタリングするオプション

Citrix Director では、［フィルター］タブの ［セッション］および ［アプリケーションインスタンス］に期間フィルターが追加されました。次のセッションとアプリケーションインスタンスをフィルターできるようになりました:

- 過去 60 分間
- 過去 24 時間
- 過去 7 日間

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

詳しくは、「トラブルシューティングのためのデータのフィルター処理」を参照してください。

強化されたパフォーマンスメトリックパネル

［パフォーマンスメトリック］パネルでは、リアルタイムのメトリックの視覚化が強化されています。［セッションパフォーマンス］タブをクリックすると、ICA 往復時間および ICA 遅延の過去 15 分間のデータとともに、過去 24 時間

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

詳しくは、「パフォーマンスメトリック」セクションを参照してください。

セッションパフォーマンスタブの機能強化

［セッションパフォーマンス］タブの ［セッショントポロジ］セクションが拡張され、次の要素が含まれるようになりました：

- ［セッショントポロジ］ビューの Connector と Citrix Gateway に関する追加の詳細（エンドポイントのホップでのエンドポイント IP、エンドポイント OS、Citrix Workspace アプリのバージョンなど）
- Pop ID、Gateway サービスの場所と国、コネクタ IP、コネクタ名、リソースの場所
- Connector と Citrix Gateway の欠落しているデータ要素の詳細と最新バージョンをダウンロードするためのリンク
- ハイパーバイザーの種類、ホスト接続名、ホスト名などのハイパーバイザーの詳細
- セッション詳細セクションとセッショントポロジビューの HDX プロトコルの名前
- Windows 向け Citrix Workspace アプリに存在する次のエンドポイントメトリック：
  - Wi-Fi 信号の強さ
  - スループットの受信と送信
  - ネットワークインターフェイスタイプ
  - リンク速度

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

ユーザープロファイルのロードの問題のトリアージを強化

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

詳しくは「プロファイルのロード」を参照してください。

コスト最適化

Citrix Director に、コスト最適化と呼ばれる新しい機能が導入されました。この機能は、仮想マシンとセッションの使用状況を効果的に分析するのに役立ちます。この機能は、コストを最適化する方法について詳細情報とともに視覚的に表示します。また、不要なマシンを排除し、コストを削減するのにも役立ちます。

［コスト最適化］ページには次の機能が含まれています：

- コスト削減
- インフラストラクチャの適正化

コスト削減 **[Technical Preview]**

［コスト削減］ページでは、選択した期間に発生したインフラストラクチャのコスト削減額が視覚的に表示され、残りの日数で予想される削減額が予測されます。このページは、マシンの使用状況とセッションを分析することにより、達成された削減額とコスト削減の機会を確認するのに役立ちます。このページでは以下を提供します:

- インフラストラクチャコストの最適化に関する詳細情報
- 削減された金額
- 予測コストを超える可能性があるさまざまなシナリオに関する情報
- インフラストラクチャのコスト削減を実現するための戦略的計画の特定と立案に関する機会

［コストの最適化］>［コスト削減］ページには、［見積もり削減額］と ［**Autoscale** 削減額レポート］が含まれています。

［見積もり削減額］は、インフラストラクチャリソースの効率的な利用を評価するのに役立ちます。［見積もり削減額］は、インフラストラクチャリソースの効率的な利用を評価するのに役立ちます。コスト削減額は、ハイパーバイザーの通貨、または発生したコストの割合で表示されます。以下の過去の期間の結果を表示できます:

- 7 日間
- 30 日間
- 3 か月
- 6 か月
- 12 か月

見積もり削減額グラフには次の内容が表示されます:

- 見積もり削減額 - 選択した期間中にインフラストラクチャで達成された削減額が表示されます。
- 電源管理されているマシン - 電源管理されているマシンの総数が表示されます。
- 予測される削減額 - 残りの期間でインフラストラクチャコストをどれだけ削減できるかが表示されます

［**Autoscale** 削減額レポート］には、Autoscale が構成され有効になっているデリバリーグループに関する情報が表示されます。このレポートは、電源管理されたマシンにのみ適用されます。

詳しくは、「コスト削減」を参照してください。

インフラストラクチャの適正化　［インフラストラクチャの適正化］ページは、リソース使用率に基づいて、デリバリーグループのプロビジョニングとサイズ設定の側面を分析するのに役立ちます。この分析に基づいて、使用パターンに合わせてマシンのプロビジョニングとサイズ設定を最適化できます。未使用のリソースへの支出を削減することで、インフラストラクチャコストを最適化できます。リソース使用率がプロビジョニングされた値よりも一貫して低い場合は、CPU とメモリのスペックが低いマシンを選択することもできます。リソース使用率が一貫して高く、それ

がログオンや *ICA* 往復時間メトリックなどのセッションエクスペリエンスに影響を与えている証拠を確認できる場合は、より高い CPU およびメモリスペックのマシンを選択してパフォーマンスを最適化できます。

以下を使用して、インフラストラクチャの適正化をフィルタリングできます:

- デリバリーグループ - シングルセッション OS またはマルチセッション OS のデリバリーグループをフィルタリングできます
- タグ - タグはマシンに適用されるタグ名です。したがって、同じタグを持つマシンをフィルタリングできます。最大 5 つまで、タグを複数選択できます。複数のタグを選択すると、選択したマシンタグの少なくとも 1 つが適用されているすべてのマシンをフィルターできます。
- 期間 - 過去 24 時間、7 日間、30 日間のデータをフィルタリングできます。

インフラストラクチャの適正化ページでは、次の情報が提供されます:

- 利用状況の詳細に関する分析情報
- リソース使用率の概要
- リソース使用率の傾向

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

［コスト最適化］タブの［コスト削減］の［インフラ ストラクチャの詳細］セクションから **Rightsize this delivery group link** をクリックし、［インフラストラクチャの適正化］ページにアクセスできます。

詳しくは、「インフラストラクチャの適正化」を参照してください。

最近電源操作を行ったマシンを検査する

成功した電源操作と失敗した電源操作のステータスを使用してマシンを検査できるようになりました。この機能は、次の分析に役立ちます:

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

> 注:
>
> データは電源管理されたマシンでのみ使用できます。この機能がサポートされる前に実行された電源操作のデータは利用できません。

次の方法を使用して、マシンの電源操作状態を表示できます:

- ［フィルター］ -> ［マシン］タブ。この場合、デフォルトでは、電源動作時間列と電源操作の結果列が表示されます。表示する列を選択することもできます。
- ［コストの最適化］タブ。この場合、デフォルトのフィルターは、［電源操作のトリガー］が ［**Autoscale**］に設定され、［電源操作の結果］が ［失敗］に設定されます。

この機能を使用すると、電源操作のコントロールの詳細を表示できます。たとえば、誰が操作をトリガーしたか、どの操作が電源状態を変更したか、失敗の理由、操作が完了した時刻を表示できます。これらの詳細をエクスポートすることもできます。

詳しくは、「最近電源操作を行ったマシンを検査する」を参照してください。

電源オフ操作の失敗と電源オン操作の失敗

Director の積極的な通知およびアラート機能が強化され、デリバリーグループ内で電源オンまたはオフに失敗した電源管理マシンの数に基づいて、電源オン操作の失敗と電源オフ操作の失敗という 2 つの新しいアラートが追加されました。新しいアラート条件を使用すると、デリバリー グループ内で電源のオン/オフに失敗した電源管理マシンの数としてアラートしきい値を構成できます。

詳しくは、「電源オフ操作の失敗と電源オン操作の失敗」を参照してください。

マシン稼働時間のアラート

Director の積極的な通知とアラート機能が強化され、デリバリーグループ内の電源管理対象マシンの稼働時間に基づく新しいアラート機能である「マシン稼働時間のアラート」を使用できます。マシンがしきい値を超えたデリバリーグループごとに、そのデリバリーグループのみに関して添付ファイルまたは webhook アラートが送信されます。

新しいアラート条件を使用すると、アラートのしきい値を、デリバリーグループ内でオンになっているマシンの 1 日あたり、1 週間あたり、1 か月あたりの時間数で構成できます。

詳しくは、「マシン稼働時間のアラート」を参照してください。

未登録マシンのアラート

Director の積極的な通知とアラート機能が強化され、デリバリーグループ内の未登録マシンの割合に基づく新しいアラート機能である ［未登録マシン（**%**）］を使用できます。新しいアラート条件を使用すると、警告および重大のしきい値を、デリバリーグループ内の未登録マシンの割合で構成できます。

詳しくは、「未登録マシン」を参照してください。

統合とデータのエクスポート

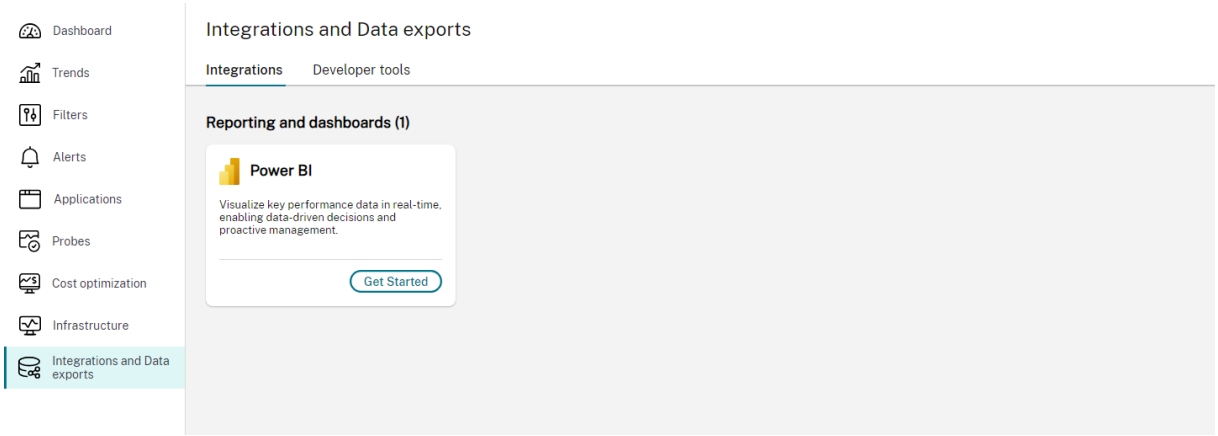
Citrix Director は、統合とデータのエクスポート用の新しい UI を提供するようになりました。この機能は、Citrix Director で利用可能なさまざまなインターフェイスや、サードパーティ統合に関する認識を向上させるのに役立ちます。新しく導入された［統合とデータのエクスポート］ページには、次の内容が表示されています:

- 利用可能な統合
- サポートされている開発者ツール

このページでは、データエクスポートのための REST API のセットアップについて説明しています。また、統合と開発者ツールの使用を開始するためのガイドとドキュメントへの参照リンクも提供します。

現在、Citrix Director は Power BI の監視機能に統合されています。この機能を使用すると、REST API によって Citrix Director から Power BI にパフォーマンスデータとイベントをエクスポートできます。

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



詳しくは、「統合とデータのエクスポート」を参照してください。

過去のユーザーセッションの診断 **[Technical Preview]**

Citrix Director では、アクティブ、切断、または終了状態のセッションの詳細が表示されるようになりました。以前は、アクティブなセッションの詳細のみを表示できました。この機能を使用すると、ヘルプデスク管理者は終了したセッションや終了状態にあるセッションに関する問題をトラブルシューティングできます。セッションの詳細は、過去 24 時間および過去 2 日間で確認できます。終了または中止されたセッションの次の詳細を表示できます:

- マシンの詳細パネル - 選択したセッションが開始されたマシンの利用可能な詳細を表示します。
- セッション詳細パネル - 選択したセッションの利用可能な詳細を表示します。
- セッションのログオン期間 - 選択したセッションへのログオン期間に関する情報を表示します。仲介処理、マシンのスタートアップ、HDX 接続、認証、GPO、ログオンスクリプト、プロファイルのディスクへのロード、対話型セッションにかかる時間に関するグラフを表示できます。

詳しくは、「過去のユーザー セッションの診断」を参照してください。

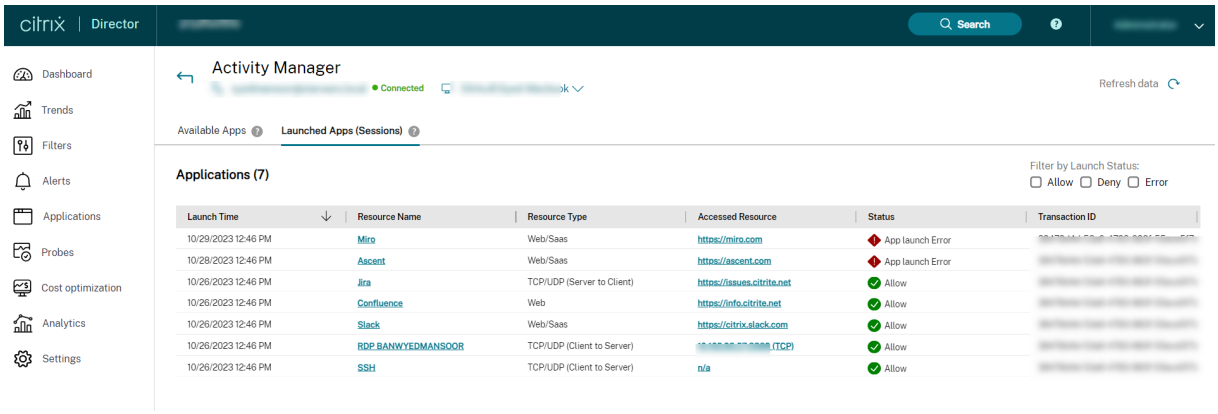
Secure Private Access のアクティビティマネージャーセッションを表示する **[Technical Preview]**

Citrix Director は、Secure Private Access セッションのアクティビティマネージャービューを提供し、セッションアクティビティの全体像を表示します。アクティビティマネージャーでは、正常に開かれたアプリとデスクトップ、開かれなかったアプリとデスクトップ、および Secure Private Access アプリで設定されたポリシーの結果をすべて包括的に確認できます。

アクティビティマネージャーには、利用可能なアプリと起動したアプリの詳細が表示されます。以下はセッションの詳細の内容です:

- 起動時間
- リソース名
- リソースの種類
- アクセスしたリソース
- 状態
- Transaction ID

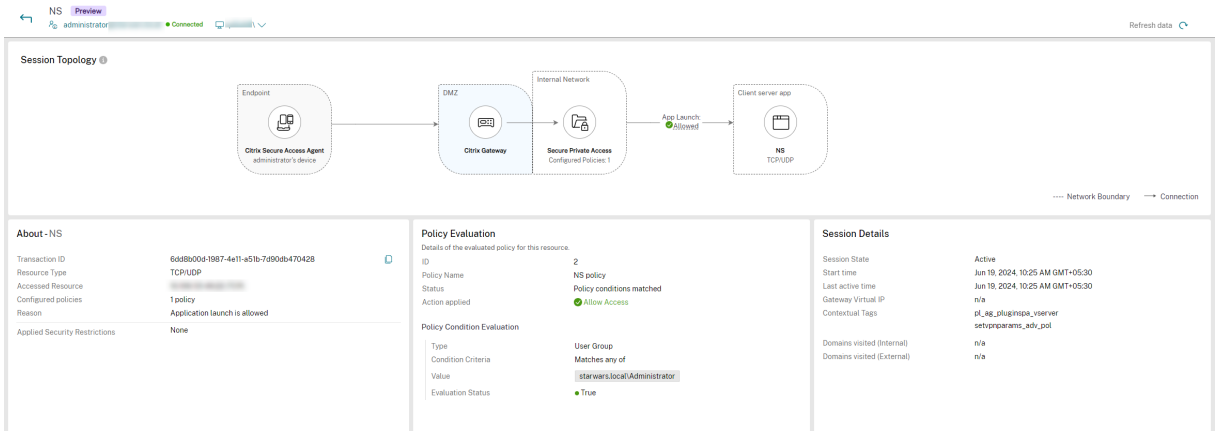
上記の詳細は、許可、拒否、エラーなどのアプリケーションの状態でフィルターすることもできます。上矢印と下矢印を使用して詳細を並べ替えることもできます。



詳しくは、「Secure Private Access のアクティビティマネージャーセッションを表示する」を参照してください。

Secure Private Access アプリのセッショントポロジビュー **[Technical Preview]**

Secure Private Access を使用して開いたアプリのセッショントポロジを表示できます。アクティビティマネージャーで必要なアプリをクリックすると、選択したアプリのセッショントポロジが表示されます。



セッショントポロジビューでは、Secure Private Access を使用して開かれたアプリ、ポリシー評価のステータス、アプリの起動ステータスを表示できます。アプリの詳細、ポリシー評価、セッションの詳細も確認できます。

詳しくは、「Secure Private Access アプリのセッショントポロジビュー」を参照してください。

インフラストラクチャ監視 **[Technical Preview]**

Citrix Director では、Citrix Virtual Apps and Desktops コンポーネントの運用の正常性を可視化できるようになりました。この機能を使用すると、インフラストラクチャに関連する問題を簡単に特定、トラブルシューティング、解決できます。現在、Citrix Provisioning（PVS）および StoreFront コンポーネントの正常性が監視されています。

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

この機能を使用すると、Director の単一のコンソールで、PVS および StoreFront サーバーのシステムのメトリックに関して、重要な監視データセットと積極的なアラートを取得できます。最新の情報を確保するために、監視コンポーネントから 5 分ごとにデータが収集されます。

この機能は、積極的な監視、詳細なメトリック、自動アラートを提供することで運用効率を高め、Citrix インフラストラクチャがスムーズかつ効率的に実行されるようにすることを目的としています。

主な機能　リアルタイム監視:

- Citrix Provisioning（PVS）サーバーや StoreFront などの Citrix インフラストラクチャコンポーネントを継続的に監視します。
- ダッシュボードには、システムの正常性、リソースの使用率、関連するパフォーマンスメトリックが表示されます。

詳細な分析:

- 接続状態、各コンポーネントのサービスまたはプロセスの状態などのシステムの正常性メトリックに関する詳細な分析を提供します。
- CPU、メモリ、ディスク使用率などのリソース使用率メトリックの詳細。

自動アラートと通知:

- 詳細なスコープ付きのさまざまなメトリックと状態に関してカスタマイズ可能なアラートしきい値。
- メールと webhook によるリアルタイム通知。

ユースケース　運用効率:

Citrix 管理チームが Citrix サーバーとサービスの高可用性とパフォーマンスを維持できるようにします。この機能は、多数のユーザーグループに影響が及ぶ前に問題を積極的に特定して管理者に警告することで、ダウンタイムを最小限に抑えるのにも役立ちます。

迅速なチケットの解決:

サーバーの正常性とパフォーマンスに関する主要なメトリックを監視して、ユーザーへの仮想アプリケーションおよびデスクトップの配信が最適かを評価します。これらのメトリックを使用して、関連するコンポーネントを分析し、パフォーマンスに関するユーザーの苦情を診断して解決します。

詳しくは、Infrastructure 監視 [Technical Preview]セクションを参照してください。

インフラストラクチャポリシー **[Technical Preview]**

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

インフラストラクチャ監視のセットアップが完了したら、Director で利用可能な正常性データを使用して、必要なコンポーネントのアラートを構成できます。管理者は、条件、範囲、通知媒体を設定して、重要なアラートを電子メールまたは Webhook 経由の JSON ペイロードで受信できます。発生したアラートは、**Citrix** アラートセクションで分析および管理することもできます。

このポリシーの一環として、次の 4 つの新しいカテゴリが導入されます:

- 到達可能性
- 依存サービス
- 影響
- リソース使用率

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

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

詳しくは、「インフラストラクチャポリシー（Technical Preview）」セクションを参照してください。

Citrix Scout

トレースおよび再現手順の強化

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

2407 リリース以降、この UI オプションは削除されます。別のログ収集を有効にすると、Scout はマシンにインストールされている CDC 関連ツールを自動的に検出し、CDC ツール関連のトレースログを zip パッケージに自動収集します。これらの zip ファイルをカスタマイズして Scout に添付することができます。この自動化により、Citrix Scout をより効果的に使用できるようになり、問題を迅速に診断できるようになります。

詳しくは、「追加のログ収集を有効にする」を参照してください。

Machine Creation Services（MCS）

Azure のイメージバージョンあたりのレプリカの制限が増加

Azure では、Gallery イメージの単一バージョンに対するレプリカの最大数が 100 に引き上げられました。制限が引き上げられたことで、Azure Compute Gallery イメージを使用して MCS マシンカタログを作成するときに、プロパティ`SharedImageGalleryReplicaMaximum`を最大値 100 に設定できるようになりました。詳しくは、「Azure Compute Gallery の構成」を参照してください。

Azure の入れ子構造の仮想化のサポート

この機能では、入れ子構造の仮想化を有効にしてマスター VM を構成すると、そのマスター VM を使用して作成された MCS マシンカタログ内のすべての VM で入れ子構造の仮想化が有効になります。この機能は、永続 VM と非永続 VM の両方に適用できます。イメージの更新を通じて、既存の MCS マシンカタログと既存の VM を更新し、入れ子構造の仮想化を実現できます。

現在、入れ子構造の仮想化をサポートしているのは Dv3 および Ev3 VM サイズのみです。

入れ子構造の仮想化について詳しくは、Microsoft のブログ「Nested Virtualization in Azure」を参照してください。

休止状態の失敗に関する警告メッセージを取得する

MCS でプロビジョニングされた、休止状態対応の既存の仮想マシンで休止状態が失敗した場合は、PowerShell コマンド Get-ProvOperationEvent を使用して警告メッセージを表示できるようになりました。詳しくは、「休止状態の失敗に関する警告メッセージを取得する」を参照してください。

Azure でホスト接続の権限を検証する

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

この機能により、次のことが可能になります:

- ホスト接続の資格情報に割り当てられた権限の一覧を取得する
- 割り当てられた権限で実行できる操作のリストを取得する
- 必要な権限に関する情報
- 必要な権限を追加する方法に関する情報

これにより、事前にトラブルシューティングを行い、必要な権限を取得できるため、ブロックされることなくタスクを実行できるようになります。詳しくは、「ホスト接続の権限を検証する」を参照してください。

Azure でのディスク暗号化を変更

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

- マスターイメージのディスク暗号化セット（DES）とは異なる DES の MCS マシンカタログを作成します。
- 既存の MCS マシンカタログおよび既存の VM のディスク暗号化の種類を、1 つの DES キーから別の DES キーに変更します。
- 以前に CMEK が有効になっていなかった MCS マシンカタログと VM を更新し、顧客管理の暗号キー（CMEK）の暗号化（DES）、ホストでのディスク暗号化、または二重暗号化を有効にします。
- 以前に暗号化されていた既存の MCS マシンカタログと VM を、暗号化されていない状態に更新します。
- プライベートエンドポイント（ProxyHypervisorTrafficThroughConnector が有効になっているホスト接続を使用した MCS マシンカタログ）でディスク暗号化を有効にします。

詳しくは、「ディスク暗号化を変更する」を参照してください。

ページファイル設定の変更をサポート

この機能によって、マスターイメージを更新せずに、既存のカタログに新しく追加された VM のページファイル設定を変更できます。この機能は、現時点では Azure 環境でのみ適用可能です。

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

MCS は **AWS** 環境でボリュームの種類が **GP3** の **ID** ディスクを作成

以前の AWS 環境では、VM の ID ディスク（ID）はボリュームの種類が GP2 でした。この機能により、MCS は、ボリュームの種類 GP3 の ID ディスクを使用して VM をプロビジョニングできるようになりました。ボリュームの種類 GP3 は、AWS が提供する最も安価なオプションであるため、この機能によりコストが最小限に抑えられます。

この機能は、新しいカタログに追加された VM と、既存のカタログに追加された新しい VM にのみ適用されます。この機能の前に作成された既存の VM では、ID ディスクがリセットされない限り、ボリュームの種類 GP2 の ID ディスクが引き続き使用されます。

AWS のマシンプロファイルソースを使用した追加のプロパティのキャプチャをサポート

AWS 環境では、この機能強化により、次の内容を含むマシンプロファイルベースのカタログを作成または更新できるようになりました:

- MCS マシンカタログを作成するときに、マシンプロファイルソースの CPU オプション、テナントの種類、休止状態機能をキャプチャします。
- MCS マシンカタログを編集するときに、マシンプロファイルソースのテナントの種類を変更します。この機能は、カタログに追加された新しい VM に適用されます。
- MCS マシンカタログを編集するときに、マシンプロファイルソースの休止状態機能を変更します。この機能は、カタログに追加された新しい VM に適用されます。

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

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

AWS で **MCS** マシンカタログ **VM** の **ID** ディスクの暗号化をサポート

以前は、AWS 環境では、プロビジョニングされた VM の OS ディスクのみの暗号化が MCS で許可されていました。この機能を使用すると、OS ディスクに加えて ID ディスクも暗号化できるようになりました。この機能により、AWS KMS キー（顧客管理キーと AWS 管理キー）を使用して、VM に接続されたディスクに対して暗号化操作を実行できるようになります。

OS ディスクと ID ディスクの暗号化では、次のいずれかを構成します:

- 暗号化されたマスターイメージを使用する（たとえば、KMS キーで暗号化されたルートボリュームを含むインスタンスまたはスナップショットから作成された AMI）
- 暗号化されたルートボリュームを含むマシンプロファイルのソース（VM または起動テンプレート）を使用する。

詳しくは、「OS ディスクと ID ディスクを暗号化する」を参照してください。

AWS でホスト接続の権限を検証

AWS 環境で、MCS マシンカタログの作成と管理に関連するタスクを実行するために、ホスト接続の権限を検証できるようになりました。この実装により、VM の作成、削除、更新、VM の電源管理、EBS 暗号化などのさまざまなシナリオに必要な不足している権限を事前に見つけることができ、重要なタイミングでブロックされることを回避できます。詳しくは、「ホスト接続の権限を検証する」を参照してください。

マシンプロファイルソースから **GCP** 内の仮想マシンおよびディスクへのラベルの継承をサポート

この機能により、MCS マシンカタログの VM とディスク（ID ディスク、ライトバックキャッシュディスク、OS ディスク）は、マシンプロファイルのソース（GCP VM インスタンスまたはインスタンステンプレート）のラベルを継承できるようになりました。ラベルを使用して、異なるチームが所有するインスタンスを区別することができ（たとえ

ば、team:research と team:analytics)、さらに原価計算や予算編成にも活用できます。ラベルについて詳しくは、GCP ドキュメント「ラベルを使用してリソースを整理する」を参照してください。

この機能は、永続および非永続の MCS マシンカタログに適用できます。

マシンプロファイルのソースを使用して、新しい MCS マシンカタログを作成したり、既存のカタログを更新したり、既存の VM を更新してラベルを継承したりできます。

詳しくは、「継承されたラベルの VM とディスク」を参照してください。

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

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

マシンプロファイルからプロビジョニングされた仮想マシンへのカスタムタグの継承をサポート

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

MCS マシンカタログを作成する前に構成を検証

この機能により、New-ProvScheme コマンドの parameter -validate を使用して、MCS マシンカタログを作成する前に構成設定を検証できるようになりました。パラメーターを指定してこの PowerShell コマンドを実行すると、間違ったパラメーターが使用されている場合、またはパラメーターが別のパラメーターと競合している場合は、適切なエラーメッセージが表示されます。その後、エラーメッセージを使用して問題を解決し、PowerShell を使用して MCS マシンカタログを正常に作成できます。

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

AWS、**GCP**、**XenServer** でアクティブなコンピューターアカウントの **ID** 情報を修復

AWS、GCP、XenServer 環境で、ID 関連の問題があるアクティブなコンピューターアカウントの ID 情報をリセットできるようになりました。マシンのパスワードと信頼キーのみをリセットするか、ID ディスクのすべての構成をリセットするかを選択できます。この実装は、永続および非永続の両方の MCS マシンカタログに適用できます。現

在、この機能は AWS、Azure、GCP、VMware、および XenServer 仮想化環境でサポートされています。詳しくは、「アクティブなコンピューターアカウントの ID 情報を修復する」を参照してください。

MCS I/O ライトバックキャッシュディスクへの特定のドライブ文字の割り当てをサポート

以前は、Windows オペレーティングシステムが MCS I/O ライトバックキャッシュディスクにドライブ文字を自動的に割り当てていました。この機能で、MCS I/O ライトバックキャッシュディスクに特定のドライブ文字を割り当てることができるようになりました。この機能の導入は、使用するアプリケーションのドライブ文字と MCS I/O ライトバックキャッシュディスクのドライブ文字の間の競合を回避するのに役立ちます。この機能は、Windows オペレーティングシステムのみに適用されます詳しくは、「MCS I/O ライトバックキャッシュディスクへの特定のドライブ文字の割り当て」を参照してください。

Profile Management

新機能について詳しくは、該当するドキュメントの「新機能」の記事を参照してください。

Linux VDA

新機能について詳しくは、該当するドキュメントの「新機能」の記事を参照してください。

Session Recording

新機能について詳しくは、該当するドキュメントの「新機能」の記事を参照してください。

Workspace Environment Management

新機能について詳しくは、該当するドキュメントの「新機能」の記事を参照してください。

Citrix Provisioning

新機能について詳しくは、該当するドキュメントの「新機能」の記事を参照してください。

フェデレーション認証サービス

新機能について詳しくは、該当するドキュメントの「新機能」の記事を参照してください。

解決された問題

August 17, 2024

Citrix Virtual Apps and Desktops 7 2407 には、次の解決された問題が含まれています:

グラフィック

- 作業中に、Citrix ソフトウェアグラフィックプロセス（Ctxgfx.exe）がリセットされ、約 10 秒間断続的に画面が消えることがあります。twencodeスレッドでアクセス違反の例外が発生し、ctxExceptionHandlerがミニダンプを記録することでこの問題が発生します。ctxExceptionHandlerは、検査用に完全なダンプを生成するように設定されています。[CVADHELP-24877]

Machine Creation Services

- 複数の Delivery Controller サイトを 2402 より前の LTSR バージョン（バージョン 2302、2305、2308、2311 を含む）から 2402 LTSR にアップグレードするときに、サイトが部分的にしかアップグレードされていない場合、仮想マシンの電源操作が失敗することがあります。詳しくは、CTX666299を参照してください。

シングルセッション **OS** 対応 **VDA**

クリップボード

- VDA 2203 LTSR CU4 を使用し、WebP 形式のコンテンツをコピーして貼り付けると、WfShellが機能しなくなります。[CVADHELP-25356]
- 公開リモートアプリのクリップボードへのコピーオプションは、CU3 および CU4 バージョンでは機能しません。[CVADHELP-24687]
- サーバー VDA インスタンス上の Citrix Smart Card Service で、メモリ消費が最大で 100% に達し、メモリリークの問題が発生する場合があります。[CVADHELP-25389]

セッション/接続

- 次のモジュールのアクセス違反のため、OpenTEXT ETX アプリケーションを開くことができません:

  C:\Program Files\Citrix\HDX\bin\CtxMFPlugin64.dll [CVADHELP-24985]

スマートカード

- サーバー VDA インスタンス上の Citrix Smart Card Service で、メモリ消費が最大で 100% に達し、メモリリークの問題が発生する場合があります。[CVADHELP-25389]

マルチセッション **OS** 対応 **VDA**

クリップボード

- VDA 2203 LTSR CU4 を使用し、WebP 形式のコンテンツをコピーして貼り付けると、`WfShell`が機能しなくなります。[CVADHELP-25356]
- 公開リモートアプリのクリップボードへのコピーオプションは、CU3 および CU4 バージョンでは機能しません。[CVADHELP-24687]
- サーバー VDA インスタンス上の Citrix Smart Card Service で、メモリ消費が最大で 100% に達し、メモリリークの問題が発生する場合があります。[CVADHELP-25389]

セッション/接続

- 次のモジュールのアクセス違反のため、OpenTEXT ETX アプリケーションを開くことができません:

  `C:\Program Files\Citrix\HDX\bin\CtxMFPlugin64.dll` [CVADHELP-24985]

スマートカード

- サーバー VDA インスタンス上の Citrix Smart Card Service で、メモリ消費が最大で 100% に達し、メモリリークの問題が発生する場合があります。[CVADHELP-25389]

既知の問題

August 17, 2024

Citrix Virtual Apps and Desktops 7 2407 には、次の既知の問題が含まれています:

メモ

- 既知の問題に回避策がある場合は、問題の説明の後に回避策が記載されています。
- レジストリエントリの変更を伴う回避策については、次の点に注意してください:

> 警告:
>
> レジストリエディターの使用を誤ると、深刻な問題が発生する可能性があり、オペレーティングシステムの再インストールが必要になる場合もあります。レジストリエディターの誤用による障害に対して、Citrix では一切責任を負いません。レジストリエディターは、お客様の責任と判断の範囲でご使用ください。また、レジストリファイルのバックアップを作成してから、レジストリを編集してください。

一般

- アプリバーを起動してから、Windows 向け Citrix Workspace アプリでコネクションセンターメニューを開くと、アプリバーがホストサーバーの下に表示されません。[HDX-27504]
- Windows 向け Citrix Workspace アプリを使用していて、アプリバーを縦向きで起動すると、バーが［スタート］メニューまたはシステムクロックトレイに重なって表示されます。[HDX-27505]
- ユーザーが既にホストでフォーカスされているコンボボックスを選択すると、コンボボックスが正しく表示されない場合があります。この問題を回避するには、別の UI 要素を選択してからコンボボックスを選択します。[HDX-21671]
- Windows 10 から Windows 11 への OS のインプレースアップグレードを実行した後、Citrix Desktop Service の起動に失敗する場合があります。この問題を解決するには、マシンを再起動します。[HDX-58399]
- マルチセッション VDA のセッションの制限設定は、Windows Server 2022、Windows 10 Enterprise マルチセッション、および Windows 11 Enterprise マルチセッションを実行しているセッションホストでは拒否されます。
  この問題を回避するために、GPO で **RDS** セッション時間制限を構成できます。[HDX-47001]
- 管理者権限でアプリケーションを実行している場合、FIDO2 に関連付けられた Windows セキュリティダイアログボックスが ICA セッションウィンドウの前面に表示されません。Windows セキュリティダイアログボックスが昇格された権限で実行されている場合、オペレーティングシステムの設計上、ICA セッションウィンドウの背後に隠れます。[HDX-26794]
- クライアントから ICA セッションへの 100MB を超えるデータの場合、クリップボードのコピーと貼り付けが失敗する場合があります。大きなバッファのコピーはサポートされていません。[HDX-59028]
- 復元ポイントは作成されますが、Windows 10 または Windows 11 マルチセッションプラットフォームで VDA のインストールが失敗した場合は、VDA を復元できません。VDA のインストールは UI またはコマンドラインを使用して開始されました。[HDX-58915]
- Windows 10 または Windows 11 マルチセッション OS は、Windows システムの復元をサポートしていません。したがって、復元ポイントを作成するオプションは UI で利用できません。コマンドラインオプション/`EnableRestore`または/`EnableRestoreCleanup`は無視され、システムの復元を無効にすることは現在 Windows 10/11 マルチセッション OS ではサポートされていません、というメッセージが記録されます。[HDX-58915]

- Citrix は、Citrix が生成したバイナリとサードパーティのバイナリの両方に署名します。つまり、バイナリは Citrix によって認証されます。サードパーティバイナリのバージョンは、サードパーティから取得されているため、同じままです。バイナリが既にインストールされている場合、バージョンが一致するため、VDA アップグレードではバイナリはインストールされません。この制限を回避するには、以下を実行してください:

  1. バイナリを許可リストに含めます。これにより、バイナリに署名する必要がなくなります。
  2. 古い VDA をアンインストールし、新しい VDA をインストールします。これは新規 VDA インストールに似たプロセスであり、署名されたバージョンが適用されます。

  [HDX-62302]

- 一部のシナリオでは、クライアント IP ポリシーフィルターを使用すると、正しくない IP アドレスがポリシーの評価に使用されます。[HDX-62375]
- シングルサインオンに拡張ドメイン パススルーを使用する場合、クライアントデバイスまたはセッションホストで Windows 11 が実行されていると、セッションへの SSO が失敗する可能性があります。[HDX-62973]
- 無効なポリシー設定でサイトがアップグレードされると、ポリシーデータが失われる可能性があります。この問題が発生した場合は、Citrix サポートポータルでテクニカルサポートケースを開きます。[GP-1671]
- Citrix Rendezvous V2 のインストールで、VDAWorkstationSetup_2402、VDAServerSetup_2402、または VDAWorkstationCoreSetup_2402 パッケージを使用する場合、これらのパッケージには Citrix.Diagnostics.Tracing.dll ファイルがないため、インストールが失敗する可能性があります。この問題を解決するには、次の操作を行います:

  - Citrix Rendezvous V2 を完全な CVAD Citrix Virtual Apps and Desktops 7 2402 LTSR パッケージから、または Citrix_Virtual_Apps_and_Desktops_7_2402_LTSR.iso からインストールします。
  - または、不足している Citrix.Diagnostics.Tracing.dll ファイルを置き換えます。ファイルを置き換えるには、以下を実行します:

    1. Citrix.Diagnostics.Tracing.dll ファイルを CVAD Citrix Virtual Apps and Desktops 7 2402 LTSR パッケージから、または「x64\XenDesktop Setup」フォルダーの ISO からコピーします。
    2. 一時フォルダーを作成します。例:「C:\Workaround」。
    3. 次のコマンドを実行して、最小限のインストーラーパッケージを一時フォルダーから展開します: VDAWorkstationSetup_2402.exe /extract “C:\Workaround”。
    4. Citrix.Diagnostics.Tracing.dll ファイルを「C:\Workaround\Extract\Image-Full\x64\XenDesktop Setup」フォルダーにコピーします。
    5. 次のコマンドを実行して VDA のインストールを開始します:「C:\Workaround\Extract\Image-Full\x64\XenDesktop Setup\XenDesktopVdaSetup.exe」[HDX-65363]

Web Studio

Secure Private Access と **Web Studio** との統合

- ユーザーが［概要］タブ >［ライセンスサーバー URL を追加する］リンクから［設定］>［統合］ページにリダイレクトされると、ナビゲーションバーが一部非表示になります。ページを更新して、ナビゲーションバーを表示してください。[SPAOP-4782]
- 誤ったゲートウェイ URL を入力すると、空白の警告ポップアップが表示されます。警告アイコンの上にマウスを置くと、警告メッセージが表示されます。[SPAOP-4947]
- 計画段階の統合を実行し、データベースを構成しようとすると、手動モードから自動モードに切り替えた後、警告ポップアップ内のテキストが表示されません。警告アイコンの上にマウスを置くとメッセージが表示されます。[SPAOP-4948]
- コンソール内のすべてのタブで垂直スクロールバーが部分的に表示されます。この問題に回避策は必要ありません。また、機能やユーザーエクスペリエンスに影響はありません。[SPAOP-4851]
- ブラウザーのウィンドウが小さい場合、［設定］**>**［統合］タブで、垂直スクロールバーがページの下部に表示されません。ブラウザーウィンドウが最大化されている場合、水平スクロール バーは必要ありません。[SPAOP-4844]
- トラブルシューティングログで、ログの詳細ダイアログボックスが開かれている場合、垂直スクロールバーがページの下部に表示されません。この問題に回避策は必要ありません。また、機能やユーザーエクスペリエンスに影響はありません。[SPAOP-4843]
- Secure Private Access コンソールにログインしたとき、または Web Studio に戻って Secure Private Access コンソールに戻ったときに、［概要］タブは強調表示されません。この問題に回避策は必要ありません。また、機能やユーザーエクスペリエンスに影響はありません。[SPAOP-4691]
- ［設定］**>**［統合］タブで、エラーメッセージがダイアログボックスの前面ではなく背後に表示されます。この問題に回避策はありません。また、機能やユーザーエクスペリエンスに影響はありません。[SPAOP-4856]

注:

上記の問題はすべて、Web Studio から Secure Private Access にアクセスした場合にのみ発生します。スタンドアロンの Secure Private Access にアクセスする場合には、該当しません。

Web Studio

ディスクに CMEK を使用して Google Cloud の Web Studio でカタログを編集する場合、ウィザードの手順をスキップすると、将来マシンを追加するときに失敗する可能性があります。この問題を回避するには、手順をスキップせずにウィザード全体を完了するか、PowerShell SDK を使用して操作を実行します。[STUD-31280]

グラフィック

- Theora 圧縮形式で 64 ビット Web カメラを使用してビデオプレビューを起動すると、セッションがクラッシュすることがあります。[HDX-21443]

- デスクトップアプリ用 Skype のリモートデスクトップに追加の Web カメラが接続されている場合があります。これらの追加の Web カメラのプレビューはブロックされており、セキュリティ上の理由により黒い画面が表示される場合があります。追加の Web カメラを無視して、エンドポイントで Web カメラを使用し続けることができます。[HDX-58807]
- Intel および一部の NVIDIA GPU 上の H265 444 では、セッション内にアーティファクトが表示される可能性があります。Intel GPU に関連する問題については、セッションのサイズを変更するか、全画面モードに切り替えるという一時的な回避策があります。[PMCS-41084]

Machine Creation Services

- AWS でホストされている VMware 環境では、マスターイメージで vTPM が有効になっていると、MCS マシンカタログの作成が失敗します。この問題は、Citrix Virtual Apps and Desktops のすべてのバージョンに影響します。VMware のサポートについては、「Get Support」を参照してください。[PMCS-37603]

印刷

- 仮想デスクトップで選択されたユニバーサルプリントサーバープリンターがコントロールパネルの ［デバイスとプリンター］ウィンドウに表示されません。この問題が発生しても、アプリケーションからこのプリンターを使って正しく印刷できます。この問題は、Windows 10 でのみ発生します。詳しくは、CTX213540を参照してください。[HDX-5043, 335153]
- 印刷ダイアログウィンドウで、通常使うプリンターが正しくマークされていないことがあります。この問題は、通常使うプリンターに送信される印刷ジョブには影響しません。[HDX-12755]
- ユニバーサルプリントサーバーへの SSL 接続が有効になっていると、負荷分散されたネットワークプリンターからの一部の印刷ジョブが失敗することがあります。これは、印刷ジョブが次々と急激に実行される場合に発生します。[HDX-58316]

サードパーティの問題

- Chrome は、Web ページ関連のツールバー、タブ、メニュー、ボタンに対してのみ UI オートメーションをサポートします。Chrome のこの問題によって、タッチデバイスの Chrome ブラウザーでは自動キーボード表示機能が動作しない場合があります。この問題を回避するには、`chrome --force-renderer-accessibility`を実行するか新しいブラウザータブを開いて`chrome://accessibility`を入力し、特定のページまたは全ページでネイティブの **Accessibility API** を有効にします。さらに、シームレスアプリの公開時に、Chrome で`--force-renderer-accessibility`スイッチを公開できます。[HDX-20858]
- セッションホストに FSLogix 2201 HF1 がインストールされている場合、セッションの起動時に黒い画面が表示されることがあります。この問題に対処するには、FSLogix を新しいバージョンにアップグレードする必要があります。[HDX-46159]

Profile Management

- Profile Management 2407 のドキュメントには、このリリースの更新に関する特定の情報が記載されています。

Linux VDA

- Linux VDA 2407 のドキュメントには、このリリースの更新に関する特定の情報が記載されています。

Session Recording

- Session Recording 2407 のドキュメントには、このリリースの更新に関する特定の情報が記載されています。

Workspace Environment Management

- Workspace Environment Management 2407 のドキュメントには、このリリースの更新に関する特定の情報が記載されています。

Citrix Provisioning

- Citrix Provisioning 2407 のドキュメントには、このリリースの更新に関する特定の情報が記載されています。

フェデレーション認証サービス

- フェデレーション認証サービス 2407 のドキュメントには、このリリースの更新に関する特定の情報が記載されています。

廃止

August 17, 2024

この記事は、お客様が適宜ビジネス上の決定を下せるように、段階的に廃止されるプラットフォーム、Citrix 製品、機能について前もってお知らせするためのものです。Citrix ではお客様の使用状況とフィードバックをチェックして、各プラットフォーム、Citrix 製品、機能を撤廃するかどうかを判断しています。お知らせする内容は以降のリリースで変わることがあり、廃止される機能がすべて含まれるわけではありません。製品ライフサイクルサポートについて

詳しくは、「製品ライフサイクルサポートポリシー」の記事を参照してください。長期サービスリリース（LTSR）サービスオプションについては、https://support.citrix.com/article/CTX205549を参照してください。

廃止と削除

廃止または削除されるプラットフォーム、Citrix 製品、機能を以下の表に示します。太字はこのリリースでの変更を示します。

廃止

廃止とは、将来のリリースから機能または性能を削除する予定であることを意味します。機能または性能は、正式に削除されるまで引き続き動作し、完全にサポートされます。この廃止通知は数か月から数年にわたる場合があります。削除すると、機能や性能は動作しなくなります。この通知は、機能または性能が削除される前に、十分な時間をかけてコードを計画および更新できるようにするためのものです。可能な場合、廃止される項目の代替が提案されます。

アイテム	廃止が発表されたバージョン	代替手段
複数のモニターフック	2407	-
Rendezvous V1	2402	Rendezvous V2 を使用します。
SecureICA	2402	-
Windows Server 2016 での VDA サポート	2402	Windows Server の最新バージョンにアップグレードします。
Delivery Controller、Web Studio、Citrix Director、Citrix License Server、Citrix StoreFront、シングルセッション OS 対応サーバー VDI、マルチセッション OS 対応 VDA、Active Directory フォレストとドメイン、Windows Server 2016 上のユニバーサルプリントサーバーのサポート	2402	Windows Server の最新バージョンにアップグレードします。
サイト構成データベース、構成ログデータベースおよび監視データベースでサポートされている Microsoft SQL Server のバージョン 2016 および 2017	2402	Microsoft SQL Server の最新バージョンにアップグレードします。
ディスクキャッシュのみを含め、メモリキャッシュを含めないライトバックキャッシュの構成をサポート	2402	メモリキャッシュサイズ構成オプションを使用して、ゼロ以外のサイズを指定します。

アイテム	廃止が発表されたバージョン	代替手段
オンデマンドプロビジョニング機能（「レガシー」カタログ）が廃止される前に作成された Azure カタログのサポート	2402	Azure レガシーカタログ VM を再作成します。カタログはオンデマンドでプロビジョニングされるため、ストレージコストの節約に役立ちます。
保持する最低フレーム数ポリシー	2311	グラフィック状態インジケーターを使用して、保持する最低フレーム数を変更します。
Citrix Connector 3.1 for System Center Configuration Manager のサポート	2311	イメージまたはアプリケーションの手動更新。
カタログが作成されたリージョンとは異なるリージョンでのマスターイメージ使用のサポート	2311	Azure Compute Gallery を使用して、マスターイメージを目的のリージョンに複製します。
HDX グラフィックの表示メモリの制限設定	2311	クライアントの表示レイアウトに完全に対応できるように、必要な最小限のメモリが割り当てられます。
HDX グラフィックでのプログレッシブモードのサポート	2311	Thinwire を使用します。「プログレッシブモード」を参照してください。
Internet Explorer 11 でブラウザーコンテンツリダイレクトをサポート	2311	Google Chrome ベースのブラウザーコンテンツリダイレクトを使用します。
AWS ボリュームワーカーのサポートが削除されました	2311	ディスクの直接アップロードとダウンロードを使用します。「ディスクの直接アップロードとダウンロード」を参照してください。
Broker での SQL Server 2016 のサポート	2308	最新バージョンの使用。詳しくは、「システム要件」を参照してください。
Director での XenApp 5.x のサポート	2308	—
Director での XenApp 6.x のサポート	2308	—
Director のアラート用の SCOM Pack	2308	—
Director でのプラグインのサポート	2308	—
WebRTC SDP 形式（Plan B）のサポート	2308	Citrix Workspace アプリをサポートされているバージョンにアップグレードしてください。

アイテム	廃止が発表されたバージョン	代替手段
Microsoft Teams 最適化におけるシングルウィンドウモードのサポート	2308	Citrix Workspace アプリをマルチウィンドウモードをサポートするバージョンにアップグレードしてください。詳しくは、「機能マトリックスとバージョンのサポート」を参照してください。
AWS 環境で使用されるAwsCaptureInstanceProperties のサポート	2308	マシンプロファイルを使用する。「マシンプロファイルを使用してカタログを作成する」を参照してください。
Schedule-ProvVMUpdate PowerShell コマンド	2305	Set-ProvVMUpdateTimeWindow を使用します。
Request-ProvVMUpdate PowerShell コマンド	2305	パラメーター-StartsNowおよび-DurationInMinutes -1を指定してSet-ProvVMUpdateTimeWindow を実行します。
Cancel-ProvVMUpdate PowerShell コマンド	2305	Clear-ProvVMUpdateTimeWindow を使用します。
DedicatedTenancyコマンドで使用するNew-ProvSchemeパラメーター	2303	TenancyTypeパラメーターを使用します。
ライセンスサーバー VPX	2206	—
Azure 環境で仮想マシンをプロビジョニングするための非管理ディスク	2206	Managed Disks を使用します。
ホストからクライアントへの（URL）リダイレクト	2203	コンテンツの双方向リダイレクト。

アイテム	廃止が発表されたバージョン	代替手段
クラウドおよびオンプレミス環境で使用される 4 つの AWS 固有のコマンド、`Revoke-HypSecurityGroupIngress`、`Revoke-HypSecurityGroupEgress`、`Grant-HypSecuritygroupegress` および `Grant-HypSecurityGroupIngress` のサポート。	2203	—
VDA Metainstaller からの Citrix Files for Windows および Citrix Files for Outlook。	2203	スタンドアロンインストーラーを使用。
VDA Metainstaller からの WEM エージェントコンポーネント。	2203	—
リモート PC アクセス用の SCCM 統合 Wake on LAN オプション。	2012	スタンドアロンの Wake on LAN 機能を使用します。
Citrix SCOM Management Pack for XenApp and XenDesktop、Provisioning Services、および StoreFront。監視できる製品バージョンについては、Citrix SCOM Management Pack のドキュメントを参照してください。	1912	Director を使用して、展開を監視および管理します。SCOM EOL と代替手段について詳しくは、https://support.citrix.com/article/CTX266943を参照してください。
Mobility SDK/Mobile SDK（旧 Citrix Labs のもの）	7.16	モバイルエクスペリエンスのポリシー設定と、ホストされるデスクトップ/アプリのネイティブエクスペリエンスにより一時停止されます。

削除

削除されたアイテムは、Citrix Virtual Apps and Desktops から削除されるか、サポートされなくなります。

アイテム	廃止が発表されたバージョン	削除されたバージョン	代替手段
Windows 向け Citrix Workspace アプリ 1912	—	2402	最新バージョンの使用。
HDX グラフィックの全画面 + テキストの最適化	2311	2311	
HDX 3D Pro での NVIDIA Frame Buffer Capture（NVFBC）のサポート	2308	2311	デスクトップ複製 API（DDAPI）を使用します。
ポリシー設定「付属のプリンタードライバーの自動インストール」の VDA サポート。	7.16	2311	ありません。以前の OS のみ（Windows 7、Windows Server 2012 R2 以前）で、VDA でサポートされているポリシー設定。
NVIDIA GPU ハードウェアエンコーディング（NVENC）。vGPU 11 以降、およびドライバーバージョン 466.77 以降を使用。	2305	2305	現在サポートされている NVIDIA ドライバーを使用。vGPU 13 以降、バージョン 471.41 以降。
VDA メタインストーラーからダウンロードできる Citrix Supportability Tools（Supportability-Tool_x64 .msi）。	—	2212	—
Citrix ライセンス管理コンソール（最後に Windows ライセンスサーバー 11.16.3 ビルド 30000 に含まれ、Windows ライセンスサーバー v11.16.6 ビルド 31000 で削除されました）。	2003	2006	Citrix Licensing Manager を使用します。
Windows 10 バージョン 1709 以前での Citrix Indirect Display Driver（IDD）グラフィックアダプターのサポート。	2003	2003	Citrix Virtual Apps and Desktops 7 1912 LTSR VDA を使用します。

アイテム	廃止が発表されたバージョン	削除されたバージョン	代替手段
GRID 9 以前のディスプレイドライバーを使用した NVIDIA GPU（NVENC）によるハードウェアエンコーディング。	2003	2003	Citrix Virtual Apps and Desktops 7 2003 以降の VDA で GRID 10 ディスプレイドライバーを使用するか、Citrix Virtual Apps and Desktops 7 1912 LTSR VDA を使用します。
セルフサービスパスワードリセット（SSPR）機能。	2003	2006	—
Microsoft .NET Framework の 4.8 より前のバージョンが VDA およびコアサーバーコンポーネントでサポート。Delivery Controller、Studio、Director、StoreFront を含みます。	1912	2003	.NET Framework バージョン 4.8 にアップグレードします。
Windows Server 2012 R2 の VDA。	1912	2003	サポートされているオペレーティングシステムに VDA をインストールします。
Citrix Virtual Apps and Desktops プレミアムエディションの AppDNA アプリケーション移行コンポーネント。	1909	2003	—
32 ビット（x86）マシンに Studio をインストールします。	1909	2003	サポートされている x64 オペレーティングシステムにインストールします。
シームレスアプリケーションでの Excel フックのサポート。これは、Microsoft Excel 2010 のブックごとに個別のタスクバーアイコンを作成するために使用されました。	1909	1909	—

アイテム	廃止が発表されたバージョン	削除されたバージョン	代替手段
Windows Server 2012 R2（Service Pack を含む）上のコアサーバーコンポーネント。Delivery Controller、Studio、Director を含みます。	1906	2003	サポートされているより新しいオペレーティングシステムにインストールします。
Microsoft SQL Server versions 2008 R2、2012、2014（すべての Service Pack とエディションを含みます）でサイト構成データベース、構成ログデータベースおよび監視データベースをサポート。	1906	2003	サポートされているバージョンの Microsoft SQL Server にデータベースをインストールします。
x86 プラットフォームにおける Windows 10 での VDA のサポート。	1906	1909*	サポートされる x64 オペレーティングシステムに VDA をインストールします。* この機能は、Citrix Virtual Apps and Desktops 7 1912 LTSR で引き続きサポートされています。
Citrix Virtual Apps and Desktops インストールメディアからの Citrix Smart Tools Agent の削除。	1903	1906	—
StoreFront 内で次の販売終了製品から Delivery Controller オプションを削除：VDI-in-a-Box および XenMobile（9.0 以前）。	1903	1903	—
Red Hat Enterprise Linux/CentOS 7.5 での Linux VDA のサポート。	1903	1903	Red Hat Enterprise Linux のそれ以降のバージョンに Linux VDA をインストールします。

アイテム	廃止が発表されたバージョン	削除されたバージョン	代替手段
StoreFront による Citrix Virtual Apps and Desktops（旧 XenApp および XenDesktop）、Citrix Receiver、ワークスペースハブ間の TLS 1.0 および TLS 1.1 プロトコルのサポート。	7.17	2203	Citrix Receiver を、TLS 1.2 プロトコルをサポートする Citrix Workspace アプリにアップグレードします。Citrix Workspace アプリについて詳しくは、https://docs.citrix.com/ja-jp/citrix-workspace-appを参照してください。
ポリシー設定「付属のプリンタードライバーの自動インストール」の VDA サポート。	7.16	2311	ありません。以前の OS のみ（Windows 7、Windows Server 2012 R2 以前）で、VDA でサポートされているポリシー設定。
StoreFront でのデスクトップアプライアンスサイト上のデスクトップへのアクセスのサポート	1811	1912	ドメインに参加しない場合は、Desktop Lockを使用します。
Framehawk ディスプレイリモートテクノロジのサポート	1811	1903	アダプティブトランスポートが有効なThinwireを使用します。
すべての Citrix Virtual Apps and Desktops（および、XenApp および XenDesktop）バージョンでの Citrix Smart Scale 機能のサポート。この機能は、2019 年 5 月 31 日に製品終了となります。	1808	1906	強化された電源管理機能を Citrix Cloud で利用するには、Virtual Apps and Desktops サービスを使用することを検討してください。

アイテム	廃止が発表されたバージョン	削除されたバージョン	代替手段
Citrix StoreFront、Citrix VDA、Citrix Studio、Citrix Director、および Citrix Delivery Controller による Microsoft .NET Framework バージョン 4.5.1、4.5.2、4.6、4.6.1、4.6.2、および 4.7 のサポート。	7.18	1808	.NET Framework バージョン 4.7.1 以降にアップグレードします。(.NET Framework 4.7.1 がインストールされていない場合は、インストーラーによって自動的にインストールされます)。
Red Hat Enterprise Linux 7.3 での Linux VDA のサポート	7.18	1808	Red Hat Enterprise Linux のそれ以降のバージョンに Linux VDA をインストールします。
SUSE Linux Enterprise Server 11 Service Pack 4 での Linux VDA のサポート。	7.16	7.16	サポートされている SUSE バージョンに Linux VDA をインストールします。
VDA での Citrix WDDM ドライバーのサポート	7.16	7.16	Citrix WDDM ドライバーは VDA でインストールされなくなりました。
Windows 10 バージョン 1511（Threshold 2）および Windows 8.x と Windows 7 を含む、以前の Windows シングルセッション OS リリース用 VDA（https://www.citrix.com/blogs/2018/01/08/the-citrix-strategy-for-windows-7-virtual-desktop-users/を参照)。	7.15 LTSR（および 7.12）	7.16	Windows 10 最小バージョン 1607（Redstone 1）以降の半期チャネル用シングルセッション OS VDA をインストールします。1607 LTSB を使用している場合、7.15 VDA をお勧めします。CTX224843を参照してください。
Windows Server 2008 R2 および Windows Server 2012（Service Pack を含む）上の VDA。	7.15 LTSR（および 7.12）	7.16	サポートされているオペレーティングシステムに VDA をインストールします。

アイテム	廃止が発表されたバージョン	削除されたバージョン	代替手段
デスクトップコンポジションのリダイレクト（旧 DirectX コマンドリモート処理）（DCR）	7.15 LTSR	7.16	Thinwireを使用します。
Citrix Receiver for Web クラシックエクスペリエンス（「緑色の泡」ユーザーインターフェイス）	7.15 LTSR（および StoreFront 3.12）	1903	Citrix Receiver for Web 統合エクスペリエンス。
Windows Server 2012 および Windows Server 2008 R2（Service Pack を含む）上のコアコンポーネント。Delivery Controller、Studio、Director、StoreFront、ライセンスサーバー、およびユニバーサルプリントサーバーを含みます。	7.15 LTSR	7.18	サポートされているオペレーティングシステムにコンポーネントをインストールします。
Windows Server 2012 および Windows Server 2008 R2（Service Pack を含む）上のセルフサービスパスワードリセット（SSPR）機能	7.15 LTSR	7.18	サポートされているより新しいオペレーティングシステムにインストールします。
Windows 7、Windows 8、および Windows 8.1（Service Pack を含む）上の Studio。	7.15 LTSR	7.18	サポートされているオペレーティングシステムに Studio をインストールします。

アイテム	廃止が発表されたバージョン	削除されたバージョン	代替手段
Flash リダイレクト	7.15 LTSR	1912	ビデオコンテンツを HTML5 ビデオとして作成します。管理コンテンツには HTML5 ビデオのリダイレクト、公開 Web サイトにはブラウザーコンテンツリダイレクトを使用します。詳しくは、Flash リダイレクトの製品終了（EOL）に関する記述を参照してください。
StoreFront を含む Citrix Online Integration（Goto 製品）	7.14（および StoreFront 3.11）	StoreFront 3.12	—
VDA インストール時に作成され、VDA マシンのローカル管理者グループに追加されるユーザーアカウント CtxAppVCOMAdmin は、作成されなくなります。基になる「COM」メカニズムも削除されます。	7.14	7.14	Windows サービス CtxAppVService が同じ機能を実行します。このサービスは自動的にインストールされ、構成されるため、ユーザー操作は必要ありません。
Windows Server 2008 32 ビットでのユニバーサルプリントサーバーの UpsServer コンポーネントサポート。	7.14	7.14	サポートされているより新しいオペレーティングシステムにインストールします。
Internet Explorer 8 用 StoreFront および Receiver for Web	7.13	7.13	—
Citrix App-V コンポーネントをインストールしない、VDA コマンドラインでのインストールオプション/no_appv	7.13	7.13	コマンドラインインストールオプション/exclude “Citrix Personalization for App-V - VDA” を使用します。

アイテム	廃止が発表されたバージョン	削除されたバージョン	代替手段
全製品インストーラーでの新規インストール時に、Citrix.Common.Commands スナップインはインストールされなくなりました。このスナップインは、既存インストールのアップグレード時に自動で削除されます。	7.13	7.13	Citrix.Common.Commands スナップインによって提供されていた一部の PowerShell コマンドは、XenApp 6.5 SDK で引き続き使用できます。
*-CtxIcon コマンドレットによって提供されていたアイコンデータを操作するための機能の一部。	7.13	7.13	Broker Service の *-BrokerIcon コマンドレットによって提供されるようになりました。
従来の Thinwire モード	7.12	7.16	Thinwireを使用します。Windows Server 2008 R2 で従来の Thinwire モードを使用している場合は、Windows Server 2012 R2 または Windows Server 2016 に移行し、Thinwire を使用します。
StoreFront 2.0、2.1、2.5、および 2.5.2 からのインプレースアップグレード。	7.13	7.16	これらのバージョンは、以降のサポート対象バージョンにアップグレードしてから、XenApp および XenDesktop 7.16 にアップグレードします。

アイテム	廃止が発表されたバージョン	削除されたバージョン	代替手段
XenDesktop 5.6 または 5.6 FP1 からのインプレースアップグレード。	7.12	7.16	XenDesktop 5.6 または 5.6 FP1 展開を、最新の XenDesktop バージョンに移行します。これを行うには、まず XenDesktop 7.6 LTSR（最新の CU を含む）にアップグレードしてから、最新の Citrix Virtual Desktops（旧 XenDesktop）リリースまたは LTSR バージョンにアップグレードします。
32 ビット（x86）マシンに Delivery Controller、Director、StoreFront、またはライセンスサーバーをインストールします。	7.12	7.16	サポートされている x64 オペレーティングシステムにインストールします。
接続リース	7.12	7.16	ローカルホストキャッシュを使用します。
Windows XP 上で使用される XenDesktop 5.6。Windows XP 上の VDA インストールはサポートされません。	7.12	7.16	サポートされているオペレーティングシステムに VDA をインストールします。
CloudPlatform 接続のサポート	7.12	2003	サポートされている各種ハイパーバイザーまたはクラウドサービスを使用します。
Azure Classic（別名 Azure Service Management）接続のサポート	7.12	2003	Citrix Cloud で Virtual Apps and Desktops サービスを使用することを検討してください。
AppDisk の機能（およびそれをサポートする Studio への AppDNA の統合）	7.13	2003	Citrix App Layering を使用します。

アイテム	廃止が発表されたバージョン	削除されたバージョン	代替手段
Personal vDisk の機能	7.15	2006†	Citrix App Layering ユーザーレイヤーテクノロジ、またはユーザー個人設定レイヤーテクノロジを使用します。

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

システム要件

August 17, 2024

はじめに

ここで説明するシステム要件は、この製品バージョンがリリースされた時点で確認済みのものです。定期的に更新が行われます。このトピックで説明されていないシステム要件コンポーネント（ホストシステム、Citrix Workspace アプリ、および Citrix Provisioning）については、各コンポーネントのドキュメントを参照してください。

インストールの前に、「インストールの準備」の内容を確認してください。

特に断りのない限り、前提条件となるソフトウェア（.NET や C++ パッケージなど）の必須バージョンがインストールされていないことが検出された場合、コンポーネントのインストーラーにより自動的にインストールされます。これらの必須ソフトウェアの一部は、Citrix 製品のインストールメディアにも収録されています。

インストールメディアには複数のサードパーティ製コンポーネントが収録されています。Citrix ソフトウェアを使用する前に、サードパーティからのセキュリティに関するアップデートを確認して、必要に応じてインストールしてください。

グローバリゼーションの情報について詳しくは、Knowledge Center の記事CTX119253を参照してください。

Windows Server にインストール可能なコンポーネントと機能に関しては、Nano Server のインストールは記載がない限りサポートされていません。Server Core は、Delivery Controller および Director に対してのみサポートされています。

ハードウェア要件

RAM およびディスクスペースの値は、マシン上の製品イメージ、オペレーティングシステム、およびそのほかのソフトウェアの要件に追加されます。パフォーマンスは構成に応じて異なります。構成には、使用する機能やユーザーの数なども含まれます。最低限のみを使うとパフォーマンスが低下する可能性があります。

次の表は、コアコンポーネントでの最小要件を示しています。

コンポーネント	最小
1 つのサーバー上のすべてのコアコンポーネントおよび StoreFront（実稼働環境ではなく評価用のみ）	5GB の RAM
1 つのサーバー上のすべてのコアコンポーネントおよび StoreFront（テスト展開または小規模実稼働展開用）	12GB の RAM
Delivery Controller（ローカルホストキャッシュを使用するには、さらに多くのディスクスペースが必要）	5GB の RAM、800MB のハードディスク、データベース：「サイジングガイダンス」参照
Studio	1GB の RAM、100MB のハードディスク
Director	2GB の RAM、200MB のハードディスク
StoreFront	2GB の RAM。ディスクの推奨事項については、StoreFront のドキュメント参照
ライセンスサーバー	8GB の RAM。ディスクの推奨事項については、ライセンス管理のドキュメント参照

デスクトップやアプリケーションを配信する仮想マシンのサイジング

ハードウェアの提供は複雑かつ動的であり、展開にはそれぞれ一意のニーズがあるため、特定の推奨事項を示すことはできません。通常、Citrix Virtual Apps 仮想マシンのサイズ変更は、ユーザーのワークロードではなくハードウェアに基づきます。例外は RAM です。より多くを消費するアプリケーションには、より多くの RAM が必要です。

さらに、以下の情報を参照してください：

- Citrix Tech Zoneには、サイズ変更に関するガイダンスが含まれています。
- 「Citrix Virtual Apps and Desktops の単一サーバーのスケーラビリティ」では、単一の物理ホストでサポートされるユーザーまたは仮想マシンの数について説明します。

Microsoft Visual C++

Delivery Controller、Virtual Delivery Agent（VDA）、またはユニバーサルプリントサーバーをインストールする場合、Citrix インストーラーは Microsoft Visual C++ 2015–2022 再頒布可能パッケージを自動的にインストールします。

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

Delivery Controller

以下のオペレーティングシステムがサポートされています：

- Windows Server Core 2022
- Windows Server 2022
- Windows Server 2019 の Standard Edition、Datacenter Edition、および Server Core オプション付き

要件：

- Microsoft .NET Framework 4.8 以降がインストールされていない場合は、自動的にインストールされます。
- Windows PowerShell 3.0、4.0、または 5.0。
- Microsoft Visual C++ 2015～2022 再頒布可能パッケージ。

データベース

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

- SQL Server 2022 の Express、Standard、および Enterprise Edition。
- SQL Server 2019 の Express、Standard、および Enterprise Edition。
- SQL Server 2017 の Express、Standard、および Enterprise Edition。
  - 新規インストール：デフォルトでは、Controller のインストール時に適切なバージョンの SQL Server が検出されない場合、SQL Server Express 2017 と累積更新プログラム（CU）16 がインストールされます。
  - アップグレードの場合、既存の SQL Server Express バージョンはアップグレードされません。
- SQL Server 2016 SP2 の Express、Standard、および Enterprise Edition。

以下のデータベース高可用性ソリューションがサポートされます（スタンドアロンモードのみをサポートする SQL Server Express を除く）。

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

Controller と SQL Server サイトデータベース間の接続には Windows 認証が必要です。

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

- Controller をインストールするとき、ローカルホストキャッシュ機能と連携して使用するために、デフォルトで Microsoft SQL Server Express LocalDB 2019 と累積更新プログラム（CU）15 がインストールされます。これは、サイトデータベースのデフォルトの SQL Server Express インストールとは異なるインストールです。
- Controller をアップグレードする場合、既存の Microsoft SQL Server Express LocalDB バージョンは自動的にアップグレードされません。置き換えの要件と手順については、「SQL Server Express LocalDB の置き換え」を参照してください。

データベースの詳細情報：

- データベース
- CTX114501はサポートされている最新の主なデータベース一覧を表示
- データベースのサイジングガイダンス
- ローカルホストキャッシュ

Web Studio

> 注：
>
> - Web Studio（Web ベース）と Citrix Studio（Windows ベース）の 2 つの管理コンソールを使用して、Citrix Virtual Apps and Desktops の展開を管理できます。この記事では Web Studio のみを扱います。Citrix Studio について詳しくは、Citrix Virtual Apps and Desktops 7 2212 以前の同様の記事を参照してください。
> - Web Studio は、オンプレミスの Citrix Virtual Apps and Desktops 環境を構成および管理する Web ベースの管理コンソールです。これは、ユーザーエクスペリエンスを向上させるように設計されており、通常、Windows ベースの管理コンソールである Citrix Studio よりも高速に応答します。「Web Studio のインストール」を参照してください。

以下のオペレーティングシステムがサポートされています：

- Windows Server Core 2022
- Windows Server 2022
- Windows Server 2019 の Standard Edition、Datacenter Edition、および Server Core オプション付き

Citrix Director

以下のオペレーティングシステムがサポートされています:

- Windows Server Core 2022
- Windows Server 2022
- Windows Server 2019 の Standard Edition、Datacenter Edition、および Server Core オプション付き

要件:

- Microsoft .NET Framework 4.8 以降がインストールされていない場合は、自動的にインストールされます。
- Microsoft インターネットインフォメーションサービス（IIS）7.0 および ASP.NET 2.0。IIS と一緒に［静的コンテンツ］の役割サービスがインストールされていることを確認してください。このソフトウェアがまだインストールされていない場合は、Windows Server のインストールメディアを指定するためのメッセージが表示されます。次に、そのソフトウェアがインストールされます。
- Citrix Director がインストールされているマシンのイベントログを表示するには、Microsoft .NET Framework 2.0 をインストールする必要があります。

Citrix Profile Management:

- Citrix Profile Management と Citrix Profile Management WMI プラグインが VDA にインストールされていて（インストールウィザードの ［追加コンポーネント］ページ)、Citrix Profile Management サービスが実行され Director でユーザープロファイルの詳細を表示できることを確認します。

System Center Operations Manager（SCOM）の統合要件は以下のとおりです。

- System Center 2012 R2 Operations Manager

Director を表示するための以下の Web ブラウザー。

- Internet Explorer 11 以降。Internet Explorer の互換モードはサポートされていません。Director へのアクセスには、Web ブラウザーの推奨設定を使用してください。Internet Explorer をインストールするときに、セキュリティおよび互換性に関するデフォルトの推奨設定を適用してください。インストール済みの Internet Explorer で推奨設定を使用していない場合は、［ツール］**>**［インターネットオプション］**>**［詳細設定］**>**［リセット］の順に選択し、表示される指示に従います。
- Microsoft Edge
- Firefox ESR（Extended Support Release)。
- Chrome。

Director の表示に推奨される最適な画面解像度は 1440 x 1024 です。

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

以下のオペレーティングシステムがサポートされています：

- Windows 11
- Windows 10（x64 のみ）、現在メインストリームサポートが提供されているすべてのバージョン。
  - エディションのサポートについては、Knowledge Center の記事CTX224843を参照してください。

要件：

- Microsoft .NET Framework 4.8 以降がインストールされていない場合は、自動的にインストールされます。
- Microsoft Visual C++ 2015～2022 再頒布可能パッケージ。

リモート PC アクセスでは、この VDA を社内の物理 PC 上にインストールします。この VDA では、Windows 11 および Windows 10 での Citrix Virtual Desktops リモート PC アクセス向けのセキュアブートがサポートされています。

いくつかのマルチメディアアクセラレーション機能（HDX MediaStream Windows Media リダイレクトなど）では、VDA のインストール先マシンに Microsoft メディアファンデーションをインストールする必要があります。マシンにメディアファンデーションがインストールされていない場合は、マルチメディアアクセラレーション機能がインストールされません。Citrix ソフトウェアのインストール後にマシンからメディアファンデーションを削除しないでください。これを削除すると、ユーザーがマシンにログオンできなくなります。サポートされている Windows シングルセッション OS のほとんどのエディションには、メディアファンデーションがあらかじめインストールされており、削除することはできません。ただし、N エディションには一部のメディア関連機能が付属しません。これらのソフトウェアは、Microsoft 社またはサードパーティから入手できます。詳しくは、「インストールの準備」を参照してください。

Linux VDA については、「Linux Virtual Delivery Agent」を参照してください。

サポートされる Windows Server マシンでは、コマンドラインインターフェイスを使用して Windows シングルセッション OS 対応 VDA をインストールし、サーバー VDI 機能を使用できます。詳しくは、「サーバー VDI」を参照してください。

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

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

以下のオペレーティングシステムがサポートされています：

- Windows 11（Citrix DaaS でのみサポート）
- Windows 10（x64 のみ、Citrix DaaS でのみサポート）、現在メインストリームサポートが提供されているすべてのバージョン。
- Windows Server 2022

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

インストーラーにより、以下が自動的に展開されます。これらのソフトウェアは、Citrix が提供するインストールメディアの **Support** フォルダーに収録されています:

- Microsoft .NET Framework 4.8 以降がインストールされていない場合は、自動的にインストールされます。
- Microsoft Visual C++ 2015～2022 再頒布可能パッケージ。

リモートデスクトップサービスの役割サービスが自動的にインストールされて有効になります。

いくつかのマルチメディアアクセラレーション機能（HDX MediaStream Windows Media リダイレクトなど）では、VDA のインストール先マシンに Microsoft メディアファンデーションをインストールする必要があります。マシンにメディアファンデーションがインストールされていない場合は、マルチメディアアクセラレーション機能がインストールされません。Citrix ソフトウェアのインストール後にマシンから Media Foundation を削除しないでください。これを削除すると、ユーザーがマシンにログオンできなくなります。ほとんどの Windows Server バージョンでは、メディアファンデーション機能はサーバーマネージャーを介してインストールされます。詳しくは、「インストールの準備」を参照してください。

VDA にメディアファンデーションがない場合、これらのマルチメディア機能は機能しません:

- Windows Media リダイレクト
- HTML5 ビデオリダイレクト
- HDX RealTime Web カメラリダイレクト

Linux VDA については、「Linux Virtual Delivery Agent」を参照してください。

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

ホスト/仮想化リソース

サポートされているホスト/仮想化リソースは以下のとおりです（アルファベット順）。該当する場合は、*major.minor* バージョン（およびこれらのバージョンの更新プログラム）がサポートされます。最新のバージョン情報と既知の問題へのリンクは、Knowledge Center の記事CTX131239に記載されています。

一部のホストプラットフォームまたは一部のプラットフォームバージョンでのみサポートされている機能もあります。詳しくは、各機能のドキュメントを参照してください。

リモート PC アクセスの Wake on LAN 機能を使用するには、Microsoft System Center Configuration Manager 2012 以上が必要です。

サポートされるハイパーバイザー:

- **XenServer**（旧称 **Citrix Hypervisor**）

  最新のバージョン情報と既知の問題へのリンクは、CTX131239に記載されています。

  詳しくは、「XenServer 仮想化環境」を参照してください。

- **Microsoft System Center Virtual Machine Manager**

  サポートされる System Center Virtual Machine Manager のバージョンに登録できるあらゆる Hyper-V のバージョンが含まれます。

  最新のバージョン情報と既知の問題へのリンクは、CTX131239に記載されています。

  詳しくは、「Microsoft System Center Virtual Machine Manager 仮想化環境」を参照してください。

- **Nutanix Acropolis**

  最新のバージョン情報と既知の問題へのリンクは、CTX131239に記載されています。

  詳しくは、「Nutanix 仮想化環境」を参照してください。

- **VMware vSphere（vCenter + ESXi）**

  vSphere vCenter のリンクモードはサポートされません。

  最新のバージョン情報と既知の問題へのリンクは、CTX131239に記載されています。

  詳しくは、「VMware 仮想化環境」を参照してください。

サポートされているパブリッククラウドホスト：

- **Amazon Web Services（AWS）**

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

- **Google Cloud Platform**
  詳しくは、「Google Cloud Platform 仮想化環境」と「Google Cloud で Citrix DaaS の使用を開始する」をご覧ください。

- **Microsoft Azure Resource Manager**

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

- **Nutanix** クラウドおよびパートナーソリューション

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

- **VMware** クラウドおよびパートナーソリューション

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

パブリッククラウドホスト接続を展開環境に追加するときは、次のことを考慮してください：

- ハイブリッド権利ライセンスが必要です。ハイブリッド権利ライセンスについては、「移行とトレードアップ（TTU）とハイブリッド権利」を参照してください。ライセンスの追加については、「サイトの作成」を参照してください。

- 情報ソースから、Citrix DaaS のドキュメントに移動できます。Citrix DaaS 製品のパブリッククラウドホストに精通している場合、オンプレミスバージョンにはいくつかの違いがあります。
  - Citrix DaaS では、管理インターフェイスは完全な構成と呼ばれます。オンプレミスの Citrix Virtual Apps and Desktops では、管理インターフェイスは Web Studio と呼ばれます。
  - 更新は、約 4 週間ごとに Citrix DaaS にロールアウトされます。そのため、Citrix DaaS で使用できる特定の機能がオンプレミスバージョンでは使用できない場合があります。

Active Directory の機能レベル

Active Directory フォレストとドメインの以下の機能レベルがサポートされています:

- Windows Server 2012
- Windows Server 2008 R2
- Windows Server 2008

HDX

オーディオ

Windows 向け Citrix Workspace アプリおよび Linux 向け Citrix Workspace アプリ 13 では、マルチストリーム ICA での UDP オーディオがサポートされています。

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

該当する HDX 機能のサポートおよび要件を参照してください。HDX 機能と Citrix Workspace アプリについて詳しくは、Feature matrixを参照してください。

HDX - Windows Media 配信

Windows Media のクライアント側でのコンテンツ取得、Windows Media リダイレクト、およびリアルタイム Windows Media マルチメディアトランスコードでは、次のクライアントがサポートされています: Windows 向け Citrix Workspace アプリ、iOS 向け Citrix Workspace アプリ、Linux 向け Citrix Workspace アプリ。

Windows Media コンテンツを Windows 8 デバイス側で取得するには、デフォルトプログラムとして Citrix Multimedia Redirector を設定します: これを行うには、[コントロールパネル] **>** [プログラム] **>** [既定のプログラム] **>** [既定のプログラムの設定] の順に選択し、[**Citrix Multimedia Redirector**] を選択して [すべての項目に対し、既定のプログラムとして設定する] または [既定でこのプログラムで開く項目を選択する] のいずれかをクリックします。GPU トランスコードでは、NVIDIA CUDA が有効な GPU（Compute Capability 1.1 以上）が必要です。詳しくは、https://developer.nvidia.com/cuda/cuda-gpusを参照してください。

HDX 3D Pro

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

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

- GPU パススルーは、以下で利用可能です:
  - XenServer
  - Nutanix AHV
  - VMware vSphere および VMware ESX では、仮想 Direct Graphics Acceleration（vDGA）と呼ばれます
- vGPU は以下で利用可能です:
  - XenServer
  - Nutanix AHV
  - VMware vSphere

https://docs.citrix.com/en-us/citrix-virtual-apps-desktops/graphics/hdx-3d-proを参照してください。

ホストコンピューターとして、4GB 以上の RAM と 2.3GHz 以上の 4 つの仮想 CPU を Citrix では推奨します。

GPU（Graphical Processing Unit）:

- NVIDIA GRID API を使用する仮想化グラフィックアクセラレーションでは、NVIDIA Virtual GPU（vGPU）ソフトウェアバージョン 13 以降でサポートされるすべての NVIDIA GRID GPU を HDX 3D Pro と併用できます。「https://docs.nvidia.com/grid/index.html」を参照してください。
  サポートされているハイパーバイザーとサポートされているハードウェアの詳細な一覧については、NVIDIA vGPU ソフトウェアのドキュメントを参照してください。
- 仮想化グラフィックアクセラレーションは、データセンターグラフィックプラットフォームの Intel Xeon Processor E3 ファミリと Intel データセンター GPU フレックスシリーズでサポートされます。詳しくは、「GPU フレックスシリーズ」を参照してください。
- AMD GPU は、AMD の MxGPU 仮想化でサポートされています。サポートされるハードウェアについて詳しくは、AMD のドキュメントを参照してください。

ユーザーデバイス:

- Citrix は、ハードウェアリソースに応じて、最大 8 台の 4K モニターをサポートします。使用する GPU によっては、この最大値に関して他のハードウェア制限が存在する場合があります。
- Citrix では、ユーザーデバイスでは、4GB 以上の RAM と 1.6GHz 以上の CPU を推奨します。パフォーマンスを最適化するには、ユーザーデバイスに 8GB 以上の RAM および 3GHz 以上のデュアルコア CPU を Citrix ではお勧めします。

- マルチモニター環境の場合は、Citrix ではクアッドコア CPU をお勧めします。
- Citrix Workspace アプリのインストールが必要です。

詳しくは、「HDX 3D Pro」およびwww.citrix.com/xenapp/3dを参照してください。

ユニバーサルプリントサーバー

ユニバーサルプリントサーバーは、クライアント側およびサーバー側のコンポーネントで構成されています。UpsClient コンポーネントは、VDA と一緒にインストールされます。UpsServer コンポーネントは、ユーザーセッションで Citrix ユニバーサルプリンタードライバーをプロビジョニングする共有プリンターがある各印刷サーバー上にインストールします。

UpsServer は以下でサポートされています。

- Windows Server 2022
- Windows Server 2019

要件:

- Microsoft Visual C++ 2015〜2022 再頒布可能パッケージ
- Microsoft .NET Framework 4.8（最小）

マルチセッション OS 対応 VDA で、印刷操作間にユーザー認証を実行するには、ユニバーサルプリントサーバーは、VDA と同じドメインに参加する必要があります。

スタンドアロンクライアントとサーバーコンポーネントのパッケージはダウンロードして入手することもできます。

詳しくは、「プリンターのプロビジョニング」を参照してください。

その他

Citrix ライセンスサーバー 11.17.2 以降のみがサポートされています。詳しくは、「ライセンス」を参照してください。

バージョンの互換性について詳しくは、製品マトリクスを参照してください。

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

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

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

複数の NIC がサポートされています。

最新の VDA をインストールした場合、デフォルトで Windows 向け Citrix Workspace アプリはインストールされません。詳しくは、Windows 向け Citrix Workspace アプリのドキュメントを参照してください。

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

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

この製品は、PowerShell のバージョン 3 から 5 までをサポートします。

製品の技術概要

August 17, 2024

Citrix Virtual Apps and Desktops の仮想化ソリューションで、IT 担当者は仮想マシン、アプリケーション、ライセンス、セキュリティを完全に制御でき、あらゆるデバイスからのアクセスを提供できます。

Citrix Virtual Apps and Desktops では次のことが可能です:

- エンドユーザーは、デバイスで動作するオペレーティングシステムやインターフェイスに依存せずにアプリケーションやデスクトップを実行できます。
- 管理者はネットワークを管理して、特定のデバイスまたはすべてのデバイスにアクセスを制御できます。
- 管理者は、単一のデータセンターからネットワーク全体を管理できます。

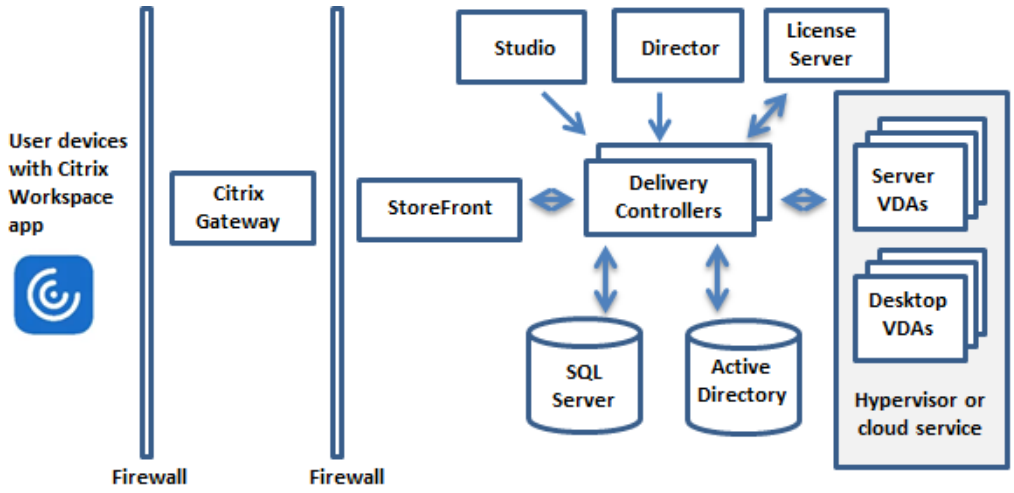
Citrix Virtual Apps and Desktops では「FlexCast Management Architecture（FMA）」と呼ばれる共通の統合アーキテクチャが使用されます。FMA により、単一サイトで複数のバージョンの Citrix Virtual Apps または Citrix Virtual Desktops を実行でき、プロビジョニング機能が統合されます。

製品名の変更についてはこちらを参照してください。

主要コンポーネント

この記事は、Citrix Virtual Apps and Desktops を初めてご使用の方に役立ちます。

次の図は、サイトと呼ばれる典型的な展開での主要なコンポーネントを示しています。



Delivery Controller

Delivery Controller は、サイトでの中心的な管理コンポーネントです。各サイトには、1 つ以上の Delivery Controller が必要です。データセンター内で動作する 1 つ以上のサーバー上にインストールします。サイトの信頼性および可用性を向上させるには、複数のサーバー上に Controller をインストールします。展開にハイパーバイザーまたはその他のサービスが含まれている場合、Controller サービスはハイパーバイザーまたはその他のサービスと通信して、以下を行います:

- アプリケーションとデスクトップの配信
- ユーザーアクセスの認証と管理
- ユーザーとユーザーのデスクトップおよびアプリケーションとの間の接続の仲介
- ユーザー接続の最適化
- 接続の負荷分散

Controller の Broker Service は、ログオンしているユーザー、ログオン先、ユーザーのセッションリソース、既存のアプリケーションへの再接続が必要かどうかを追跡します。Broker Service は、PowerShell コマンドレットを実行し、VDA 上の TCP ポート 80 で Broker Agent と通信します。TCP ポート 443 を使用するオプションはありません。

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

Controller サービスからのデータはサイトデータベースに格納されます。

Controller は、仮想デスクトップの状態を管理してユーザーからの要求や管理構成に基づいてそれらを起動および停止します。

データベース

各サイトには、構成情報やセッション情報を格納するための Microsoft SQL Server データベースが少なくとも 1 つ必要です。このデータベースには、Controller を構成する各サービスによって収集および管理されたデータが格納されます。データセンター内にデータベースをインストールして、Controller と永続的に接続されるようにしてください。

サイトは、構成ログデータベースおよび監視データベースも使用します。これらはデフォルトではサイトデータベースと同じ場所にインストールされますが、その場所は変更できます。

Virtual Delivery Agent（VDA）

サイトでユーザーが利用可能な各物理マシンおよび仮想マシン上に VDA をインストールします。これらのマシンでは、アプリケーションやデスクトップが配信されます。VDA により、これらのマシンが Controller に登録され、ユーザーがこれらのマシンおよびマシン上でホストされるリソースを使用できるようになります。VDA は、マシンとユーザーデバイスとの間の接続を確立して管理します。また、VDA は Citrix ライセンスがユーザーまたはセッションで使用可能であることを確認し、セッションに対して構成されているポリシーを適用します。

VDA は、VDA 内の Broker Agent を介して Controller 上の Broker Service とセッションに関する情報を送受信します。Broker Agent は複数のプラグインをホストし、リアルタイムデータを収集します。Studio は、TCP ポート 80 で Controller と通信します。

「VDA」という語は、VDA がインストールされているエージェントやマシンを指すためにも使用されることがあります。

VDA はシングルセッションおよびマルチセッションの Windows オペレーティングシステムで利用できます。マルチセッション Windows OS 対応 VDA では、同時に複数のユーザーがそのサーバーに接続できます。シングルセッション Windows OS 対応 VDA では、一度に許可されるのはデスクトップへの単一ユーザー接続のみです。Linux VDAも利用可能です。

Citrix StoreFront

StoreFront はユーザーを認証して、ユーザーのデスクトップやアプリケーションのストアを管理します。StoreFront により、デスクトップやアプリケーションへのセルフサービスアクセスをユーザーに提供する「エンタープライズアプリケーションストア」がホストされます。また、ユーザーのアプリケーションのサブスクリプション、ショートカット名、およびその他のデータを追跡します。これにより、ユーザーが複数のデバイス間で一貫性のある操作を行えるようになります。

Citrix Workspace アプリ

Citrix Workspace アプリは、ユーザーデバイスや他のエンドポイント（仮想デスクトップなど）にインストールされ、ドキュメント、アプリケーション、およびデスクトップへの迅速かつ安全なセルフサービスアクセスをユーザー

に提供します。また、Citrix Workspace アプリにより、Windows、Web、および SaaS（Software as a Service）アプリケーションへのオンデマンドアクセスも可能になります。デバイス固有の Citrix Workspace アプリソフトウェアをインストールできないデバイスでは、HTML5 互換の Web ブラウザーから HTML5 向け Citrix Workspace アプリを使用してアクセスすることもできます。

Studio

Web Studio（Web ベース）と Citrix Studio（Windows ベース）の 2 つの管理コンソールを使用して、Citrix Virtual Apps and Desktops の展開を管理できます。この製品ドキュメントは、Web Studio のみを対象としています。Citrix Studio について詳しくは、Citrix Virtual Apps and Desktops 7 2212 以前の記事を参照してください。

Web Studio　Web Studio は、オンプレミスの Citrix Virtual Apps and Desktops 環境を構成および管理する Web ベースの管理コンソールです。これは、ユーザーエクスペリエンスを向上させるように設計されており、通常、Windows ベースの管理コンソールである Citrix Studio よりも高速に応答します。「Web Studio のインストール」を参照してください。

Citrix Studio　Citrix Studio は、Citrix Virtual Apps and Desktops の展開を設定および管理する管理コンソールです。Citrix Studio により、アプリケーションやデスクトップの配信を管理するための個別の管理コンソールが不要になります。Citrix Studio では、環境のセットアップ、アプリケーションやデスクトップをホストするためのワークロードの作成、およびアプリケーションやデスクトップのユーザーへの割り当てを案内するさまざまなウィザードが提供されます。Studio を使用して、サイトの Citrix ライセンスの割り当てや追跡を行うこともできます。

Citrix Studio は、Controller 上の Broker Service と TCP ポート 80 経由で通信して、そこからの情報を表示します。

Secure Private Access

Citrix Secure Private Access オンプレミスソリューションは、Web および SaaS アプリへの統合アクセスポータルとして StoreFront を使用し、Citrix Workspace の統合部分として仮想アプリとデスクトップを使用することで、ブラウザーベースのアプリ（社内 Web アプリおよび SaaS アプリ）へのゼロトラストネットワークアクセスを簡単に提供できるため、組織の全体的なセキュリティとコンプライアンスの体制を強化します。このソリューションは、バージョンを変更することなく、NetScaler および StoreFront の既存のリリースと互換性があります。詳しくは、「オンプレミスストアの Secure Private Access」を参照してください。

Citrix Director

Director は、IT サポート担当者やヘルプデスクのスタッフが環境の状態を監視して、重大な障害が生じる前にトラブルシューティングを講じたりエンドユーザーをサポートしたりするための Web ベースのツールです。Director で

は、複数の Citrix Virtual Apps または Citrix Virtual Desktops サイトに接続して監視することができます。

Director には次のものが表示されます:

- Controller 上の Broker Service からのリアルタイムセッションデータ。これには、VDA 内の Broker Agent から Broker Service が収集したデータも含まれます。
- Controller 上の Monitor Service からのサイト履歴データ。

Director では、Citrix Gateway デバイスでキャプチャされた ICA パフォーマンスおよびヒューリスティックデータを使用してデータから分析を作成し、管理者に提示します。

また、Windows リモートアシスタンスを使用すると、Director を介してユーザーのセッションを表示したり制御したりすることもできます。

Citrix ライセンスサーバー

ライセンスサーバーは Citrix 製品のライセンスを管理します。Controller と通信して各ユーザーセッションのライセンスを管理し、Studio と通信してライセンスファイルを割り当てます。各サイトには、ライセンスファイルを格納および管理するためのライセンスサーバーが 1 つ以上必要です。

ハイパーバイザーまたはその他のサービス

ハイパーバイザーまたはその他のサービスは、サイトの仮想マシンをホストします。これらのサービスには、アプリケーションやデスクトップをホストするために使用する仮想マシンと、Citrix Virtual Apps and Desktops のコンポーネントをホストするために使用する仮想マシンも含まれます。ハイパーバイザーは、仮想マシンをホストする専用のコンピューター上にインストールします。

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

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

追加のコンポーネント

以下のコンポーネントが Citrix Virtual Apps and Desktops 展開に含まれていることもあります。詳しくは、それぞれのドキュメントを参照してください。

Citrix Provisioning

Citrix Provisioning（旧 Provisioning Services）は、一部のエディションで使用できるオプションコンポーネントです。仮想マシンをプロビジョニングする MCS の代替として使用できます。MCS がマスターイメージのコピーを

作成するのに対し、PVS はマスターイメージをユーザーデバイスにストリーム配信します。PVS ではハイパーバイザーが不要なため、物理マシンをホストすることができます。PVS は Controller と通信して、ユーザーにリソースを提供します。

Citrix Gateway

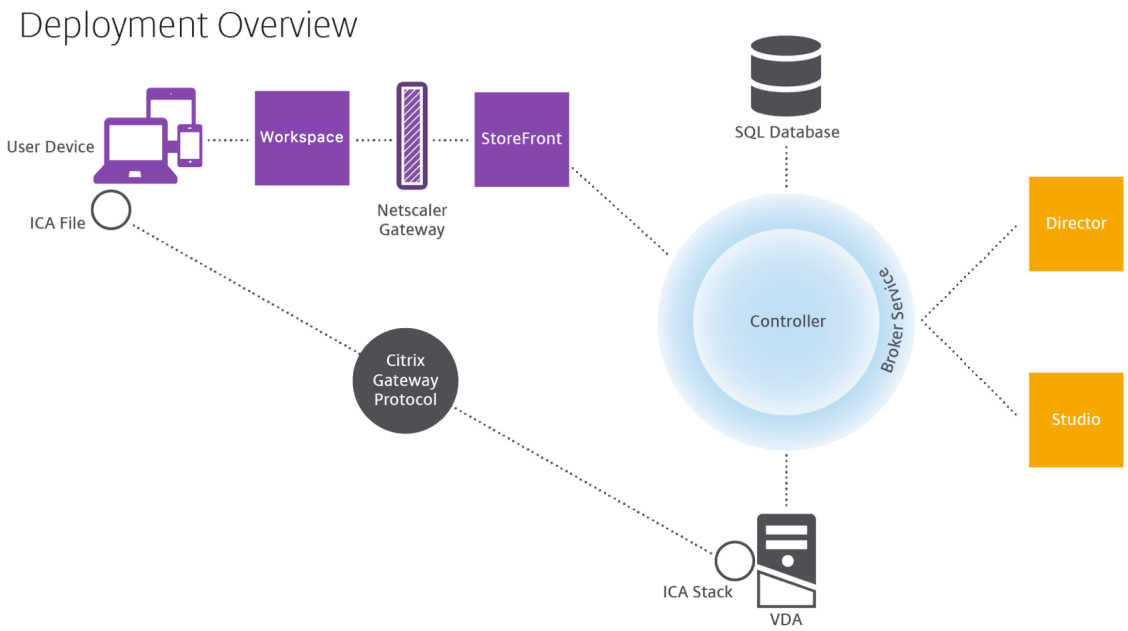
ユーザーが社内ファイアウォールの外側から接続する場合、Citrix Virtual Apps and Desktops で Citrix Gateway（旧 Access Gateway および NetScaler Gateway）テクノロジを使用して接続を TLS で保護できます。Citrix Gateway や VPX 仮想アプライアンスは非武装地帯（DMZ）に配置する SSL VPN アプライアンスであり、企業ファイアウォールを介した安全な単一アクセスポイントを提供します。

Citrix SD-WAN

支店など遠隔地のユーザーが WAN を介して仮想デスクトップに接続する環境では、Citrix SD-WAN 技術により WAN 接続のパフォーマンスを最適化できますリピーターは、WAN 全体のパフォーマンスを向上させます。ネットワーク内のリピーターによって、WAN 接続でも LAN 接続のようなユーザーエクスペリエンスが支店のユーザーに提供されます。Citrix SD-WAN では、さまざまなユーザー操作に優先順位を割り当てることができます。たとえば、ネットワーク上で大きなファイルや印刷ジョブを送信する操作に高い優先度を割り当てて、遠隔地のユーザーがストレスなく作業できるようにします。HDX WAN の最適化によりトークン化された圧縮およびデータ重複排除が提供され、帯域幅消費が減少してパフォーマンスが向上します。

典型的な展開方法

サイトは、スケーラビリティ、高可用性、およびフェールオーバーを実現する特定の役割を持ついくつかのマシンで構成され、計画的にセキュアなソリューションを提供します。サイトは、VDA がインストールされているサーバーマシンとデスクトップマシン、およびアクセスを管理する Delivery Controller で構成されます。



VDA は、ユーザーがデスクトップやアプリケーションにアクセスすることを可能にするエージェントソフトウェアです。VDA はデータセンター内の仮想マシン上にインストールされますが、リモート PC アクセス展開では物理 PC 上にインストールされることもあります。

Controller は、リソース、アプリケーション、およびデスクトップを管理したりユーザー接続を最適化および負荷分散したりする、独立したいくつかの Windows サービスで構成されます。各サイトには 1 つまたは複数の Delivery Controller があります。セッションは遅延、帯域幅、ネットワークの信頼性の影響を受けるため、可能であればすべての Controller を同じ LAN 上に配置します。

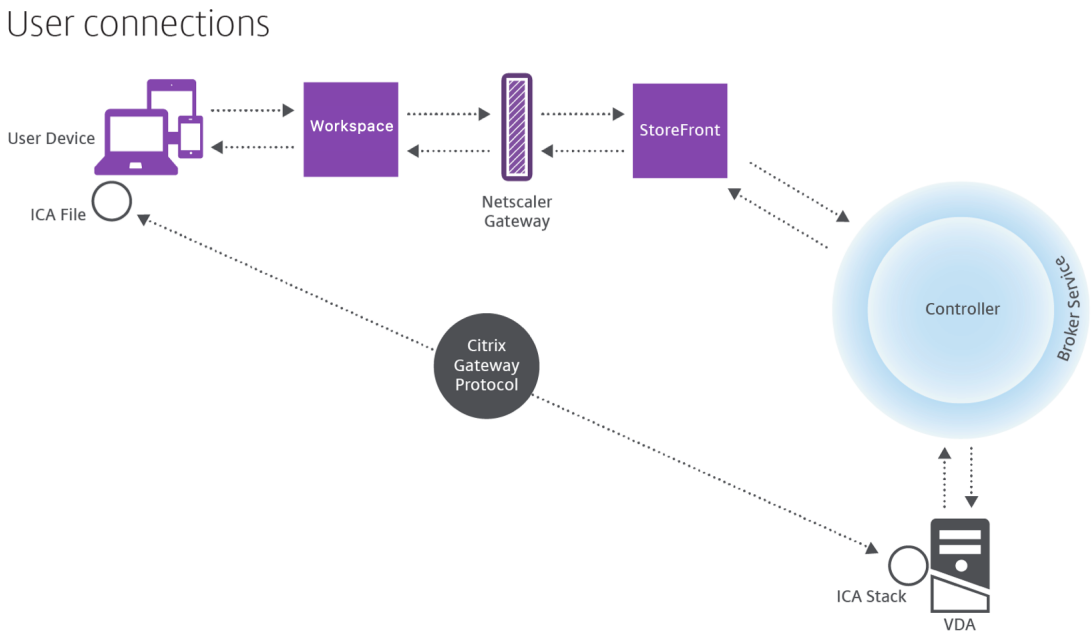
ユーザーが Controller に直接アクセスすることはありません。ユーザーと Controller 間の通信の中継点として VDA が機能します。ユーザーが StoreFront を使用してログオンすると、その資格情報は Controller 上の Broker Service にパススルーされます。Broker Service は、設定されているポリシーに基づいてプロファイルと利用可能なリソースを取得します。

ユーザー接続を処理するしくみ

セッションを開始するには、ユーザーデバイス上にインストールされている Citrix Workspace アプリ、または StoreFront Web サイトを使用して接続します。

ユーザーは、使用する物理デスクトップまたは仮想デスクトップ、または仮想アプリケーションを選択します。

下図の経路で、Controller にアクセスするためのユーザーの資格情報が転送されます。Controller は、Broker Service と通信して必要なリソースを決定します。Citrix Workspace アプリから送信される資格情報を暗号化で保護するために、StoreFront 上に SSL 証明書をインストールすることをお勧めします。



Broker Service により、ユーザーがアクセスできるデスクトップやアプリケーションが決定されます。

資格情報の検証後、アクセス可能なデスクトップやアプリケーションの情報が StoreFront と Citrix Workspace アプリ経由でユーザー側に返送されます。ユーザーがこのリストからアプリケーションまたはデスクトップを選択すると、その情報が同じ経路で Controller に送信されます。Controller は、特定のアプリケーションまたはデスクトップをホストするための適切な VDA を決定します。

Controller はユーザーの資格情報をメッセージとして VDA に送信し、さらにユーザーと接続に関するすべてのデータを VDA に送信します。VDA は接続を受け入れ、同じ経路で Citrix Workspace アプリに情報を返送します。必要なパラメーターのセットが StoreFront 上で収集されます。収集されたパラメーターは、Citrix Workspace アプリ StoreFront 間でのプロトコル変換の一部として、または Independent Computing Architecture（ICA）ファイルに変換されダウンロードされて、Citrix Workspace アプリに送信されます。サイトが正しく構成されている場合、ユーザーの資格情報はこれらの処理をとおして暗号化されたまま転送されます。

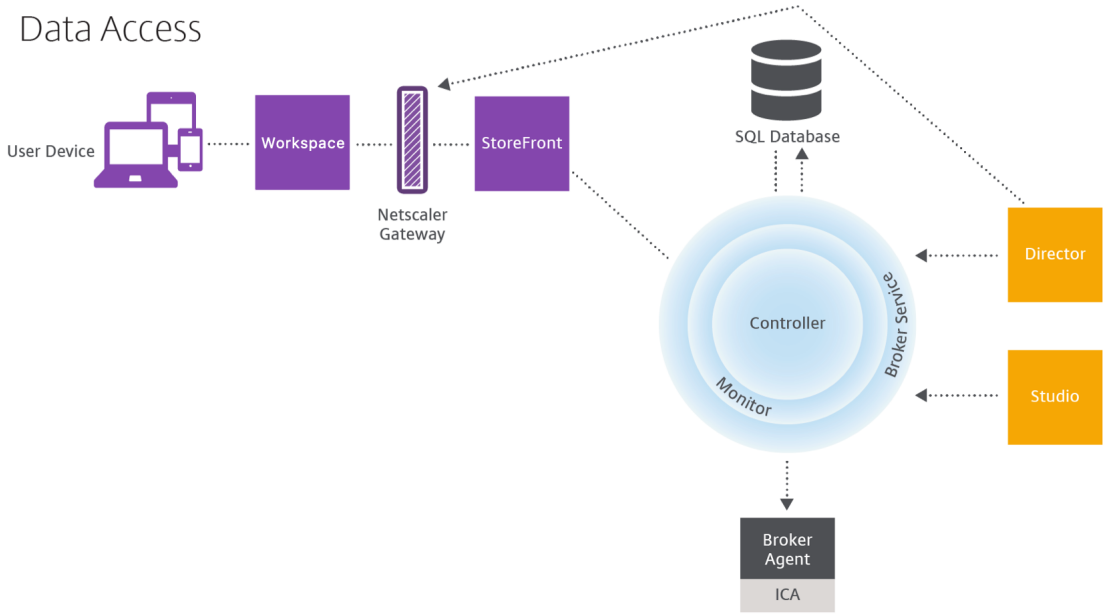
ICA ファイルがユーザーデバイスにコピーされ、VDA 上で実行される ICA スタックとの直接接続が確立されます。この接続により、管理インフラストラクチャ（Citrix Workspace アプリ、StoreFront、および Controller）がバイパスされます。

Citrix Workspace アプリと VDA 間の接続では Citrix Gateway Protocol（CGP）が使用されます。接続が中断されても、セッション画面の保持機能により同じ VDA に再接続されます。管理インフラストラクチャ経由でセッションを再起動する必要はありません。セッション画面の保持機能の有効または無効の設定は Citrix ポリシーで行います。

クライアントが VDA に接続すると、VDA はユーザーがログオンしていることを Controller に通知します。Controller はその情報をサイトデータベースに送信し、監視データベースにデータを記録し始めます。

データアクセスのしくみ

IT 担当者は、Citrix Virtual Apps and Desktops の各セッションにより提供されるデータに Studio や Director でアクセスできます。Studio を使用すると、管理者は Broker Agent からのリアルタイムデータにアクセスしてサイトを管理できます。Director は、同じデータに加えて、監視データベースに格納されている履歴データにアクセスします。また、ヘルプデスクによるサポートとトラブルシューティングのために NetScaler Gateway からの HDX データにアクセスします。



Controller 内では、Broker Service がリアルタイムデータを提供するマシン上の各セッションについてのセッションデータをレポートします。Monitor Service もこのリアルタイムデータを追跡して、履歴データとして監視データベース内に格納します。

Studio は Broker Service のみと通信します。Studio はリアルタイムデータのみにアクセスします。Director は、Broker Service と（Broker Agent 内のプラグイン経由で）通信してサイトデータベースにアクセスします。

また、Director は Citrix Gateway にもアクセスして、HDX データの情報を取得します。

デスクトップおよびアプリケーションの配信

アプリケーションおよびデスクトップを配信するマシンをマシンカタログにセットアップします。次に、（カタログにあるマシンを使用して）利用可能なアプリケーションやデスクトップ、およびどのユーザーがそれらにアクセスできるかを指定するデリバリーグループを作成します。また、アプリケーショングループを作成して、アプリケーションのコレクションを管理できます。

マシンカタログ

マシンカタログとは、単一のエンティティとして管理される物理マシンまたは仮想マシンのグループを指します。これらのマシンおよびそのアプリケーションや仮想デスクトップは、ユーザーに提供する「リソース」です。カタログ内のすべてのマシンには、同じオペレーティングシステムおよび VDA がインストールされている必要があります。また、同じアプリケーションまたは仮想デスクトップがある必要があります。

通常、管理者はマスターイメージを作成して、それを基にカタログ内に同一構成の仮想マシンを作成します。仮想マシンの場合、そのカタログにあるマシンのプロビジョニング方法を以下から指定できます：Citrix ツール（Citrix Provisioning または MCS）または他のツール。または、独自の既存イメージを使用することもできます。その場合、管理者は、サードパーティ製の ESD（Electronic Software Delivery：電子ソフトウェア配信）ツールを使用してターゲットデバイスを個別または集合的に管理します。

有効なマシンの種類は以下のとおりです。

- マルチセッション **OS**：マルチセッションオペレーティングシステムを搭載した仮想マシンまたは物理マシン。Citrix Virtual Apps 公開アプリケーション（「サーバーベースでホストされるアプリケーション」とも呼ばれます）および Citrix Virtual Apps 公開デスクトップ（「サーバーでホストされるデスクトップ」とも呼ばれます）の配信に使用されます。これらのマシンには同時に複数のユーザーが接続できます。
- シングルセッション **OS**：シングルセッションオペレーティングシステム使用の仮想マシンまたは物理マシン。VDI デスクトップ（オプションでパーソナライズできるシングルセッション OS を実行しているデスクトップ）、VM でホストされるアプリケーション（シングルセッション OS からのアプリケーション）、およびホストされる物理デスクトップの配信に使用されます。これらの各デスクトップに一度にアクセスできるのは 1 人のユーザーのみです。
- リモート **PC** アクセス：リモートユーザーが Citrix Workspace アプリを実行している任意のデバイスから社内の物理 PC にアクセスできるようにします。オフィス PC は、Citrix Virtual Desktops の展開によって管理され、ユーザーデバイスを許可リストで指定する必要があります。

詳しくは、「Citrix Virtual Apps and Desktops のイメージ管理」および「マシンカタログの作成」を参照してください。

デリバリーグループ

デリバリーグループは、どのユーザーがどのマシンのどのアプリケーションまたはデスクトップ（またはその両方）を使用できるかを指定します。デリバリーグループには、マシンカタログに記載されているマシンと、サイトへのアクセス権を持つ Active Directory ユーザーが含まれています。Active Directory グループとデリバリーグループは同様の要件に基づいてユーザーをグループ化する方法であるため、Active Directory グループを使用してデリバリーグループにユーザーを割り当てることができます。

1 つのデリバリーグループに複数のカタログからのマシンを含めることができ、1 つのカタログからのマシンを複数のデリバリーグループで使用できます。ただし、1 つのマシンが複数のデリバリーグループに属することはできません。

管理者は、デリバリーグループ内のユーザーがどのリソースにアクセスできるのかを定義します。たとえば、異なるアプリケーションを異なるユーザーに配信する場合、1 つのマシンカタログのマスターイメージにそれらのすべてのアプリケーションをインストールしておき、複数のデリバリーグループに分配するための十分な数のマシンをそのカタログに作成します。次に、マシンにインストールされているアプリケーションの異なるサブセットが配信されるように各デリバリーグループを構成します。

詳しくは、「デリバリーグループの作成」を参照してください。

アプリケーショングループ

アプリケーショングループは、さらに多くのデリバリーグループを使用するのに比べて、アプリケーション管理とリソース制御に利点をもたらします。タグによる制限機能を使用すると、複数の公開タスクに既存のマシンを使用できるので、追加のマシンを展開および管理するコストを削減できます。タグ制限は、デリバリーグループのマシンをさらに分割（またはパーティション化）するものと考えることができます。また、アプリケーショングループを使用すると、デリバリーグループ内のマシンのサブセットを分離してトラブルシューティングするときに便利です。

詳しくは、「アプリケーショングループの作成」を参照してください。

追加情報

- Citrix Virtual Apps and Desktops の図
- ネットワークポート
- データベース
- サポートされるハイパーバイザーとその他のサービス

データベース

August 17, 2024

> 注:
>
> Web Studio（Web ベース）と Citrix Studio（Windows ベース）の 2 つの管理コンソールを使用して、Citrix Virtual Apps and Desktops の展開を管理できます。この記事では Web Studio のみを扱います。Citrix Studio について詳しくは、Citrix Virtual Apps and Desktops 7 2212 以前の同様の記事を参照してください。

Citrix Virtual Apps サイトおよび Citrix Virtual Desktops サイトでは、次の 3 つの SQL Server データベースを使用します:

- サイト:（別名：サイト構成）実行中のサイト構成に加えて、その時点でのセッションの状態と接続情報を格納します。

- ログ：（別名：構成ログ）サイト構成の変更や管理タスクに関する情報を格納します。このデータベースは、構成ログ機能が有効化（デフォルトは有効）されているときに使用されます。
- モニター：セッションや接続情報などのデータを格納するために、Director により使用されます。

各 Delivery Controller は、サイトデータベースと通信します。Controller とデータベース間の接続には Windows 認証が必要です。任意の Controller をシャットダウンしても、そのサイトのほかの Controller には影響しません。しかしながら、これはサイトデータベースが単一障害点になりうることを意味します。このデータベースサーバーで障害が発生しても、既存の接続は、ユーザーがログオフまたは切断するまでは機能し続けます。サイトデータベースが利用不可能な場合の接続動作について詳しくは、「ローカルホストキャッシュ」を参照してください。

データベースに関しては、Citrix では以下をお勧めします：

- 定期的にバックアップを取ります。データベースのバックアップを定期的に作成して、データベースサーバーに障害が発生してもバックアップから復元できるようにします。各データベースを異なる方法でバックアップしなければならない場合があります。詳しくは、CTX135207を参照してください。ただし、ここで説明されている CitrixXenDesktopDB は、サポートされなくなった、または既にお客様が利用できなくなった CitrixXenDesktopDB を指しています。
- サイト、監視、および **SQL Server** データベースを定期的にバックアップおよび復元します。SQL Server データベースに関する特定の情報については、「SQL Server データベースの完全バックアップおよび差分バックアップの作成」を参照してください。

サイトに複数のゾーンが含まれている場合は、プライマリゾーンには必ずサイトデータベースを格納してください。すべてのゾーンのコントローラーは、このデータベースと通信します。

高可用性

自動フェールオーバーを確実にするために、数種類の高可用性ソリューションがあります。

- **AlwaysOn** 可用性グループ機能（基本的な可用性グループを含む）： SQL Server 2012 で導入されたエンタープライズレベルの高可用性および障害回復ソリューション。これにより、1 つまたは複数のデータベースの可用性を最大化できます。AlwaysOn 可用性グループ機能では、Windows Server Failover Clustering（WSFC）ノード上に SQL Server インスタンスが存在する必要があります。詳しくは、「SQL Server での Windows Server フェールオーバークラスタリング」を参照してください。
- **SQL Server** データベースのミラーリング：データベースをミラーリングすると、アクティブなデータベースサーバーが停止しても自動フェールオーバー処理が実行され、ユーザーは通常、停止の影響を受けません。各データベースサーバー上に完全な SQL Server ライセンスが必要になるため、ほかのソリューションよりも費用が高くつきます。SQL Server Express エディションを使用してデータベースをミラーリングすることはできません。
- **SQL** クラスタリング： Microsoft の SQL クラスタリングテクノロジを使用して、任意のサーバーに障害が起きた場合に別のサーバーが自動的にタスクや実行内容を引き継ぐようにできます。ただし、このソリューションのセットアップは複雑で、SQL ミラーリングなどほかのソリューションよりも自動フェールオーバー処理には一般的に時間がかかります。

- ハイパーバイザーの高可用性機能の使用：この方法では、仮想マシンとしてデータベースを展開し、ハイパーバイザーの高可用性機能を使用します。このソリューションでは既存のハイパーバイザーソフトウェアを使用でき、また SQL Server Express エディションも使用できるため、ミラーリングよりも費用が安いというメリットがあります。ただし、データベースの新しい仮想マシンの起動に時間がかかるため、自動フェールオーバー処理が遅くなり、ユーザーへのサービスが中断する可能性があります。

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

サイト内のすべての Controller で障害が起きた場合、VDA が高可用性モードで動作するように構成できます。これにより、ユーザーは障害発生後もデスクトップやアプリケーションにアクセスして使用することができます。高可用性モードでは、Controller を経由しない、VDA への直接 ICA 接続が可能になります。Controller とのすべての通信に失敗した場合にのみ、この機能を使用してください。この機能を他の高可用性ソリューションの代わりに使用しないでください。詳しくは、CTX 127564を参照してください。

SQL クラスター化または SQL ミラー化インストールにおける、ノード上への Controller のインストールはサポートされていません。

データベースソフトウェアのインストール

デフォルトでは、初めて Delivery Controller をインストールしたときに、そのサーバーで他の SQL Server インスタンスが検知されなかった場合に、SQL Server Express エディションがインストールされます。通常、概念実証またはパイロット展開では、このデフォルトの動作で十分です。ただし、SQL Server Express は Microsoft の高可用性機能をサポートしていません。

デフォルトのインストールでは、デフォルトの Windows サービスアカウントおよび権限を使用します。Windows サービスアカウントを sysadmin ロールに追加する方法など、デフォルトの設定について詳しくは、Microsoft 社のドキュメントを参照してください。Controller は、この構成で Network Service アカウントを使用します。SQL Server に追加のロールまたは権限は必要ありません。

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

ほとんどの実稼働環境、および Microsoft の高可用性機能を利用しているすべての環境では、Express 以外のサポート対象エディションの SQL Server のみを使用することをお勧めします。最初の Controller がインストールされているサーバー以外のマシンに、SQL Server をインストールします。サポートされる SQL Server のバージョンについては、「システム要件」を参照してください。データベースは 1 つまたは複数のマシンに常駐できます。

サイトを作成する前に、SQL Server ソフトウェアをインストールしておく必要があります。データベースを作成する必要はありませんが、作成する場合は、必ず空にしておいてください。Microsoft 高可用性テクノロジの構成も推奨されます。

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

サイトの作成ウィザードを使ったデータベースのセットアップ

［サイトの作成］ウィザードの ［データベース］ページで、データベースの名前とアドレス（場所）を指定します。(「データベースのアドレス形式」を参照してください)。Director が Monitor Service をクエリするときのエラーを防ぐため、監視データベースの名前にはスペースを使用しないでください。

［データベース］ページには、自動とスクリプト使用の 2 つのデータベース設定オプションがあります。Web Studio ユーザーや Citrix 管理者が、必要なデータベースアクセス権を持っている場合は、通常、自動オプションを使用します（「データベースのセットアップに必要な権限」を参照してください)。

構成ログや監視データベースの場所は、サイトの作成後に変更できます。「データベースの場所の変更」を参照してください。

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

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

サイトの作成後にミラーリング設定を検証するには、PowerShell コマンドレット`get-configdbconnection`を実行して、ミラーに対する接続文字列でフェールオーバーパートナーが設定されていることを確認します。

ミラー化されたデータベース環境で Delivery Controller を後から追加、移動、または削除する場合は、「Delivery Controller」を参照してください。

自動セットアップ

必要なデータベース権限を持っている場合は、サイトの作成ウィザードの ［データベース］ページにある ［**Studio** でデータベースを作成および設定する］を選択します。次に、プリンシパルデータベースの名前とアドレスを入力します。

指定したアドレスにデータベースが存在する場合、そのデータベースは空でなければなりません。指定されたアドレスにデータベースが存在しない場合、データベースが見つからないというメッセージが表示され、データベースを作成するかどうかの確認を求められます。作成に同意すると、Web Studio により自動的にデータベースが作成され、プリンシパルデータベースとレプリカデータベースに初期化スクリプトが適用されます。

スクリプトを使ったセットアップ

必要なデータベース権限がない場合は、データベース管理者など、必要なデータベース権限を持っている人に支援を依頼してください。手順は以下のとおりです:

1. サイトの作成ウィザードの ［データベース］ページで、［スクリプトを生成して手動でセットアップ］を選択します。この操作により、次のプリンシパルデータベースとレプリカデータベースのそれぞれに対して、サイト、監視、およびログのデータベースの 3 種類のスクリプトが生成されます。

   - 名前に「*SysAdmin*」を含むスクリプト。データベースと Delivery Controller のログインを作成するスクリプト。これらのタスクには、securityadmin 権限が必要です。
   - 名前に「*DbOwner*」を含むスクリプト。データベースでユーザー役割を作成し、ログインを追加してから、データベーススキーマを作成するスクリプト。これらのタスクには`db_owner`の権限が必要です。
   - 名前に「*Mixed*」を含むスクリプト。必要な権限にかかわらず、1 つのスクリプトにすべてのタスクを含めます。

   スクリプトの格納先を指定します。

   > 注:
   >
   > エンタープライズ環境では、データベースのセットアップに、役割（権限）が異なる（`securityadmin`または`db_owner`）チームが処理する可能性があるスクリプトが含まれます。該当する場合は、最初に役割`securityadmin`の管理者が「SysAdmin」スクリプトを実行し、次に`db_owner`権限を持つ管理者が「DbOwner」スクリプトを実行します。これらのスクリプトの生成には、PowerShell を使用することもできます。詳しくは、「優先データベース権限スクリプト」を参照してください。

2. これらのスクリプトをデータベース管理者に渡します。この時点で、サイトの作成ウィザードは自動的に停止します。後で戻ってきたときに、サイトの作成を続行するように求められます。

その後、データベース管理者がデータベースを作成します。個々のデータベースには、次の特性が必要です:

- 「`_CI_AS_KS`」で終わる照合順序を使用します。`_100_CI_AS_KS`で終わる照合順序を使用することをお勧めします。
- 最適なパフォーマンスを実現するには、SQL Server Read-Committed Snapshot を有効化します。詳しくは、CTX137161を参照してください。
- 構成済みの高可用性機能（該当する場合）。
- ミラーリングを構成するには、まず、完全復旧モデルを使用するようにデータベースを設定します（デフォルトは簡易モデル）。プリンシパルデータベースをファイルにバックアップして、それをミラーサーバーにコピーします。次に、ミラーサーバーにバックアップファイルを復元します。最後に、プリンシパルサーバーでミラーリングを開始します。

データベース管理者は、SQLCMD コマンドラインユーティリティ、または SQL Server Management Studio を SQLCMD モードで使用して、以下のことができます:

- 高可用性 SQL Server データベースインスタンスで、各xxx_Replica.sqlスクリプトを実行する（高可用性が構成されている場合）
- プリンシパル SQL Server データベースインスタンスで、各xxx_Principal.sqlスクリプトを実行する。

SQLCMD について詳しくは、Microsoft のドキュメントを参照してください。

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

サイト作成の続行を求めるメッセージが表示されます。［データベース］ページに戻ります。渡されたアドレスを入力します。データベースをホストしているサーバーのいずれかに接続できない場合、エラーメッセージが表示されます。

データベースのセットアップに必要な権限

データベースを作成し、初期化（または、データベースの場所を変更）するには、ローカル管理者およびドメインユーザーでなければなりません。また、特定の SQL Server 権限も必要です。以下の権限は、Active Directory のグループメンバーシップで明示的に構成または取得できます。Web Studio を使用する管理者にこれらの権限がない場合、SQL Server ユーザーの資格情報を入力する必要があります。

操作	目的	サーバーロール	データベースロール
データベースの作成	空のデータベースを作成します	dbcreator	
スキーマの作成	サービス固有のすべてのスキーマを作成して、サイトに最初の Controller を追加します	securityadmin*	db_owner
Controller の追加	サイトに Controller（2 つ目以降）を追加します	securityadmin*	db_owner
Controller（ミラーサーバー）の追加	ミラー化されたデータベースのミラーロールのデータベースサーバーに Controller ログインを追加します	securityadmin*	
Controller の削除	サイトから Controller を削除します	**	db_owner
スキーマの更新	スキーマの更新および Hotfix を適用します		db_owner

* securityadminは、技術的にはより限定的なサーバーの役割ですが、実際にはsysadminのサーバーの役割と同等のものとして扱われます。

** サイトから Controller を削除しても、データベースサーバーへの Controller ログオンは削除されません。これは、同じマシン上のほかの Citrix 製品のサービスで使用されるログオンが削除されるのを防ぐためです。ログオンが不要になった場合は、手動で削除する必要があります。この操作には、securityadminのサーバーの役割メンバーシップが必要です。

Web Studio を使用してこれらの操作を実行する場合、Web Studio ユーザーは、適切なサーバーロールのメンバーとして明示的にデータベースサーバーアカウントを持っているか、またはアカウントの資格情報を提供できることが必要です。

優先データベース権限スクリプト

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

PowerShell を使用して、優先データベース権限を指定することができます。デフォルト以外の値を指定すると、個別のスクリプトが作成されます。1 つのスクリプトには、securityadminの役割が必要なタスクが含まれています。もう 1 つのスクリプトは、db_ownerの権限のみが必要で、データベース管理者に連絡することなく Citrix 管理者が実行できます。

get-*DBSchemaコマンドレットの-DatabaseRightsオプションで有効な値は以下のとおりです:

- SA : データベースと Delivery Controller のログインを作成するスクリプトを生成します。これらのタスクにはsecurityadminの権限が必要です。
- DBO : データベースでユーザー役割を作成し、ログインを追加してから、データベーススキーマを作成するスクリプトを生成します。これらのタスクにはdb_ownerの権限が必要です。
- Mixed : （デフォルト）必要な権限にかかわらず、1 つのスクリプトにすべてのタスクを含めます。

詳しくは、コマンドレットのヘルプを参照してください。

データベースのアドレス形式

データベースのアドレスは、以下の形式のいずれかで指定できます。

- ServerName
- ServerName\InstanceName
- ServerName,PortNumber

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

データベースの場所の変更

構成ログや監視データベースの場所は、サイトの作成後に変更できます。（サイトデータベースの場所を変更することはできません。）データベースの場所を変更する場合は、以下の点に注意してください：

- 変更前のデータベース内のデータは変更後のデータベースにインポートされません。
- 構成ログデータベースの場所を変更する場合、変更前のデータベースの内容は集約されなくなります。
- 変更後のデータベースの最初にデータベースの変更を示すログが記録されますが、変更前のデータベースの場所は記録されません。

データベースが切断されているときの構成変更が禁止された環境（必須ログ機能）では、構成ログの場所を変更することはできません。

データベースの場所を変更する場合は、次の手順に従います。

1. データベースを常駐させるサーバーに、サポートされているバージョンの Microsoft SQL Server がインストールされていることを確認します。必要に応じて、高可用性機能をセットアップします。
2. Web Studio にサインインし、左側のペインで ［設定］を選択します。
3. ［データベース］タイルを見つけて、［編集］を選択します。
4. ［データベースの管理］ページで、新しい場所を指定するデータベースを選択して、操作バーの ［データベースの変更］を選択します。
5. 変更後の場所とデータベース名を指定します。
6. 必要な権限を持ち、データベースを Web Studio で作成する場合は、［完了］をクリックします。確認のメッセージが表示され、［完了］をクリックすると Web Studio によりデータベースが自動的に作成されます。Web Studio ユーザーの資格情報を使ってデータベースへのアクセスが試行されます。それが失敗すると、データベースユーザーの資格情報の入力を求められます。アクセスに成功すると、Web Studio によりデータベーススキーマがデータベースにアップロードされます（資格情報はデータベース作成時のみ保持されます）。
7. Web Studio にデータベースを作成させない場合、または必要な権限がない場合は、［データベーススクリプトの作成］をクリックします。作成されるスクリプトには、データベースおよびミラーデータベース（構成する場合）を手動で作成するためのコマンドが記述されます。スキーマをアップロードする前に、データベースが空であること、および 1 人以上のユーザーがそのデータベースにアクセスでき、変更できることを確認してください。

追加情報

- データベースのサイズ評価ツール
- 「サイト構成データベースのサイズ変更」および「接続文字列の構成」（SQL Server の高可用性のためのソリューションを使用する場合）

配信方法

August 17, 2024

Citrix Virtual Apps and Desktops では、さまざまな配信方法が提供されます。1 つの配信方法で、すべてのニーズを満たせることはまずありません。

はじめに

適切なアプリケーション配信方法を選択することで、スケーラビリティ、管理性、ユーザーエクスペリエンスを高めることができます。

- アプリのインストール：アプリケーションが、ベースのデスクトップイメージに含まれます。インストールプロセスでは、レジストリが変更されるとともに、dll ファイルや exe ファイルなどすべてのファイルがイメージドライブにコピーされます。詳しくは、「マシンカタログの作成」を参照してください。
- アプリのストリーム配信（**Microsoft App-V**）：アプリケーションはプロファイル化され、オンデマンドでネットワーク上のデスクトップへ配信されます。アプリケーションファイルとレジストリの設定は仮想デスクトップのコンテナ内に配置され、ベースオペレーティングシステムや別の設定から隔離されます。これによって、互換性の問題を解決しやすくなります。詳しくは、「App-V アプリケーションの展開および配信」を参照してください。
- アプリのレイヤー化（**Citrix App Layering**）：レイヤーごとに、アプリケーション、エージェント、またはオペレーティングシステムを 1 つ配置します。管理者は、OS レイヤーを 1 つ、プラットフォームレイヤー（VDA、Citrix Provisioning エージェント）を 1 つ、アプリケーションレイヤー複数を統合することで、展開可能な新しいイメージを簡単に作成できます。レイヤー化では 1 つのレイヤーに存在する OS、エージェント、アプリケーションが 1 つになるため、定期的なメンテナンスを簡単に行えます。レイヤーを更新すると、そのレイヤーを含む展開済みイメージがすべて更新されます。詳しくは、「Citrix App Layering」を参照してください。
- **Windows** アプリのホスト：アプリケーションをマルチユーザー Citrix Virtual Apps ホストにインストールし、デスクトップではなくアプリケーションとして展開します。ユーザーは、アプリがリモートで実行されていることを意識することなく、VDI デスクトップまたはエンドポイントデバイスからホストされている Windows アプリへシームレスにアクセスできます。詳しくは、「デリバリーグループの作成」を参照してください。
- ローカルアプリ：アプリケーションをエンドポイントデバイスに展開します。アプリケーションがエンドポイント上で実行される場合でも、そのインターフェイスはユーザーのホストされた VDI セッション内に表示されます。詳しくは、「ローカルアプリケーションアクセスと URL のリダイレクト」を参照してください。

デスクトップについては、公開デスクトップまたは VDI デスクトップを選択します。

Citrix Virtual Apps の公開アプリケーションと公開デスクトップ

Citrix Virtual Apps and Desktops の公開アプリケーションと公開デスクトップは、マルチセッション OS マシンを使用してユーザーに配信します。

ユースケース:

- サーバーベースで安価に配信を行うことで、最小限のコストでアプリケーションを多くのユーザーに配信しながら、高度なセキュリティと良好なユーザーエクスペリエンスを提供する。
- 明確に定義されたタスクだけを実行し、個人用設定やオフラインアクセスが不要なユーザー。たとえば、コールセンターのオペレーター、販売員、ワークステーションを共有する作業者など。
- アプリケーションの種類:任意のアプリケーション。

特長と注意事項:

- データセンター内で簡単に管理できるスケーラブルなソリューション。
- 最もコスト効率に優れたアプリケーション配信ソリューション。
- ホスト上のアプリケーションを一元管理でき、ユーザーはアプリケーションを変更できませんこれにより、安全で信頼性が高く一貫したユーザーエクスペリエンスが提供されます。
- アプリケーションにアクセスするユーザーは常にオンライン状態である必要があります。

ユーザーエクスペリエンス:

- ユーザーは、StoreFront、[スタート] メニュー、または特定の URL からアプリケーションにアクセスします。
- アプリケーションはユーザーデバイス上に仮想的に配信され、シームレスかつ高品位に表示されます。
- プロファイル設定によっては、ユーザーによる変更内容がアプリケーションセッションの終了時に保存されます。それ以外の場合、変更は削除されます。

プロセス、ホスト、および配信:

- アプリケーションのプロセスはユーザーデバイスではなくホストマシン上で実行されます。物理マシンまたは仮想マシンでアプリケーションをホストできます。
- アプリケーションおよびデスクトップはマルチセッション OS マシン上にインストールされます。
- マシンは、マシンカタログを作成することで使用可能になります。
- マシンカタログのマシンはデリバリーグループにまとめられ、同じアプリケーションセットがユーザーグループに配信されます。
- マルチセッション OS マシンは、デスクトップまたはアプリケーション、もしくはその両方をホストするデリバリーグループをサポートします。

セッション管理と割り当て:

- マルチセッション OS マシンは、単一マシン上で複数のセッションを実行して、同時に接続する複数のユーザーに複数のアプリケーションとデスクトップを配信します。各ユーザーは、単一のセッション内ですべてのアプリケーションを実行します。

たとえば、ユーザーがログオンしてアプリケーションを要求すると、そのマシン上で 1 つのセッションがホストされ、ほかのユーザーはそのセッションを使用できません。2 人目のユーザーが同じマシンにログオンしてアプリケーションを要求すると、2 つ目のセッションがホストされ、ほかのユーザーが使用できないセッションが 2 つになります。これら 2 人のユーザーがさらにアプリケーションを要求しても、同一のセッションでアプリケーションを複数実行できるため追加のセッションはホストされません。さらに別の 2 人のユーザーがログオンしてデスクトップを要求すると、このマシンでは 4 つのセッションが 4 人のユーザー用にホストされます。

- ユーザーが割り当てられるデリバリーグループ内で、最も負荷が軽いサーバー上のマシンが選択されます。ユーザーのログオン時に、アプリケーション配信用のマシンがランダムに割り当てられます。

VM Hosted Apps

VM Hosted App は、シングルセッションOS マシンを使用してユーザーに配信します。

ユースケース:

- 安全で一元管理可能であり、ホストサーバーごとに複数のユーザーをサポートできるクライアントベースのアプリケーション配信ソリューションを実現する。対象ユーザーには、アプリケーションを高画質でシームレスに表示する。
- ユーザーは、内部または外部契約社員、サードパーティの協力者、臨時社員などである。ホスト上のアプリケーションへのオフラインアクセスは不要。
- アプリケーションの種類:ほかのアプリケーションと共存できないアプリケーションや、オペレーティングシステムと一緒に動作する Microsoft .NET Framework などのアプリケーション。これらのアプリケーションは、仮想マシン上でのホストに適しています。

特長と注意事項:

- マスターイメージ上のアプリケーションおよびデスクトップは、データセンター内のマシン上でセキュアに管理、ホスト、および実行されます。また、最もコスト効率に優れたアプリケーション配信ソリューションでもあります。
- ユーザーがログオンすると、同じアプリケーションをホストするデリバリーグループ内のマシンにランダムに割り当てられます。管理者は、ユーザーがログオンするたびに同じマシンが割り当てられるように構成することもできます。このようにマシンをユーザーに静的に割り当てると、ユーザーが仮想マシンにアプリケーションをインストールしたり独自に管理したりできるようになります。
- シングルセッションOS マシンでは、複数のセッションを実行できません。このため、ユーザーがログオンするとデリバリーグループ内の 1 つのマシンが消費され、オフライン状態ではアプリケーションにアクセスできなくなります。
- この方法では、アプリケーションの処理に必要なサーバーリソースと、ユーザーのデータ用のストレージ容量が増大します。

ユーザーエクスペリエンス:

- マルチセッション OS マシン上でホストされる共有アプリケーションと同様のシームレスなユーザーエクスペリエンスが提供されます。

プロセス、ホスト、および配信:

- これらは仮想シングルセッションOS マシンであるという以外はマルチセッション OS マシンと同様です。

セッション管理と割り当て:

- シングルセッションOS マシンで実行できるデスクトップセッションは 1 つのみです。アプリケーションにのみアクセスする場合は、各アプリケーションが個別のセッションと見なされるため、1 人のユーザーが複数のアプリケーションを使用できます。
- デリバリーグループ内では、ログオンしたユーザーは、静的に割り当てられたマシン（毎回、必ず同じマシンにログオンする）、またはセッションの可用性に基づいてランダムに割り当てられたマシンにアクセスします。

VDI デスクトップ

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

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

VDI デスクトップでは、公開デスクトップよりも多くのリソースが必要になります。ただし、サーバーオペレーティングシステムをサポートしないアプリケーションをインストールできる点が公開デスクトップと異なります。また、使用する VDI デスクトップの種類にもよりますが、特定のユーザーにデスクトップを割り当てることができます。このようにすることで、ユーザーは詳細な個人設定を行うことができます。

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

- ランダムな非永続デスクトップ（プール **VDI** デスクトップ）: ユーザーはいずれかのデスクトップにログオンするたびに、デスクトッププールのうち指定されたデスクトップに接続されます。このプールは、単一のマスターイメージに基づきます。デスクトップに対するユーザーの変更内容は、マシンの再起動時に破棄されます。
- 静的な非永続デスクトップ: ユーザーは初回ログオン時に、デスクトッププールのデスクトップに割り当てられます（プールの各マシンは単一のマスターイメージに基づきます）。以降のログオンでは、初回ログオン時に割り当てられたデスクトップに接続されます。デスクトップに対するユーザーの変更内容は、マシンの再起動時に破棄されます。
- 静的な永続デスクトップ: 他の VDI デスクトップとは異なり、ユーザーは完全な個人設定が可能です。初回ログオン時に、デスクトッププールのデスクトップに割り当てられますそのユーザーによる以降のログオンでは、最初の使用時に割り当てられたデスクトップに接続します。デスクトップに対するユーザーの変更内容は、マシンを再起動しても保持されます。

リモート **PC** アクセス

リモート PC アクセスは Citrix Virtual Apps and Desktops の機能であり、組織で従業員が安全な方法でリモートから企業リソースに簡単にアクセスできるようにします。Citrix プラットフォームでは、ユーザーが社内の物理的な PC にアクセスできるようにすることで、この安全なアクセスを可能にします。ユーザーが社内 PC にアクセスできる場合、作業に必要なすべてのアプリケーション、データ、リソースにアクセスできます。リモート PC アクセスにより、テレワークに対応するために他のツールを導入したり提供したりする必要がなくなります。たとえば、仮想デスクトップまたはアプリケーション、および関連するインフラストラクチャなどです。

リモート PC アクセスでは、仮想デスクトップとアプリケーションを配信するのと同じ Citrix Virtual Apps and Desktops コンポーネントが使用されます。その結果、リモート PC アクセスの展開と構成の要件およびプロセスは、仮想リソースの配信のために Citrix Virtual Apps and Desktops の展開に必要なものと同じです。この統一性により、一貫性のある統一された管理エクスペリエンスが実現されます。ユーザーは、Citrix HDX を使用して社内 PC セッションを提供することで、最高のユーザーエクスペリエンスを実現できます。

詳しくは、「リモート PC アクセス」を参照してください。

ネットワークポート

August 17, 2024

ネットワークポート情報について詳しくは、「Citrix テクノロジで使用される通信ポート」に記載されています。

Citrix コンポーネントをインストールすると、デフォルトのネットワークポートと一致するように、オペレーティングシステムのホストのファイアウォールもデフォルトで更新されます。

以下のように、ポートの情報が必要な場合があります:

- 法令順守のため。
- Citrix Virtual Apps and Desktops のコンポーネントと他の Citrix 製品またはコンポーネントとの間にネットワークファイアウォールがある場合、ファイアウォールを適切に構成できる。
- オペレーティングシステムのホストファイアウォールではなく、アンチマルウェアパッケージなどが付属したサードパーティ製のホストファイアウォールを使用する。
- これらのコンポーネントでホストファイアウォールの構成を変更する（通常 Windows ファイアウォールサービス）。
- コンポーネントの機能を再構成して、別のポートやポート範囲を使用し、構成で使用されていないポートを無効にする、またはブロックする必要がある。

ポートの一部は、Internet Assigned Numbers Authority（IANA）に登録されています。こうした割り当てについて詳しくは、http://www.iana.org/assignments/port-numbersを参照してください。ただし、IANA の保有する情報には、最新の使用状況が反映されていない場合があります。

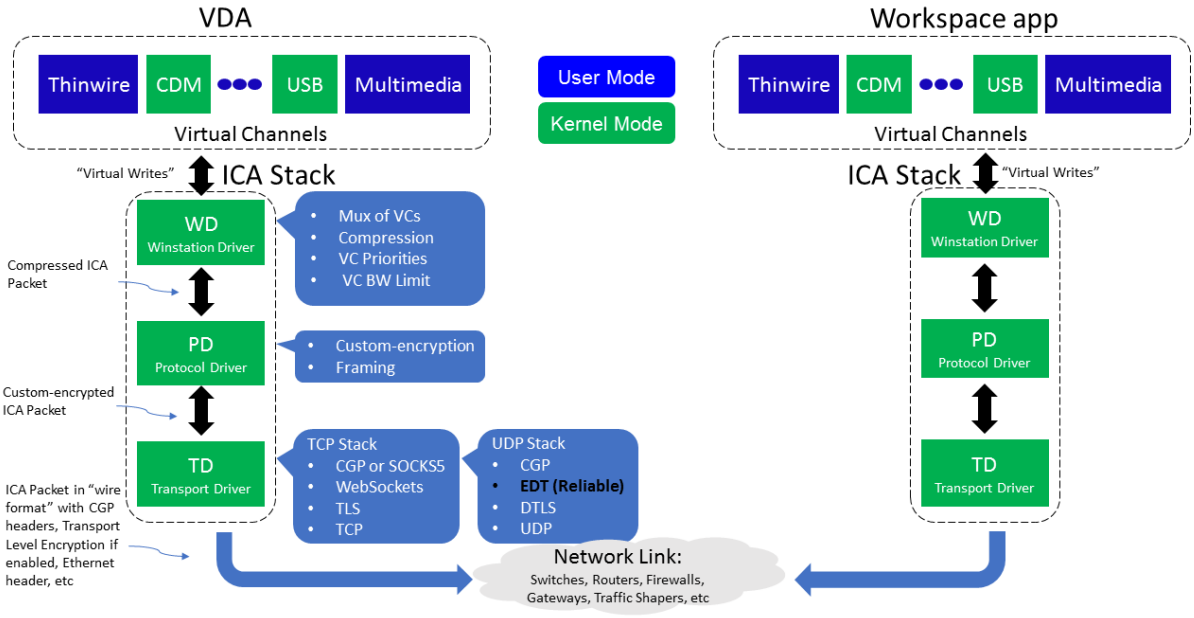
また、VDA および Delivery Controller のオペレーティングシステムには、専用の受信ポートが必要です。詳しくは、Microsoft Windows のドキュメントを参照してください。

HDX

August 17, 2024

> 警告:
>
> レジストリエディターの使用を誤ると、深刻な問題が発生する可能性があり、オペレーティングシステムの再インストールが必要になる場合もあります。レジストリエディターの誤用による障害に対して、Citrix では一切責任を負いません。レジストリエディターは、お客様の責任と判断の範囲でご使用ください。また、レジストリファイルのバックアップを作成してから、レジストリを編集してください。

Citrix HDX には、デバイス上とネットワーク上で一元化されたアプリケーションとデスクトップの高品位なユーザーエクスペリエンスを実現する幅広いテクノロジが搭載されています。

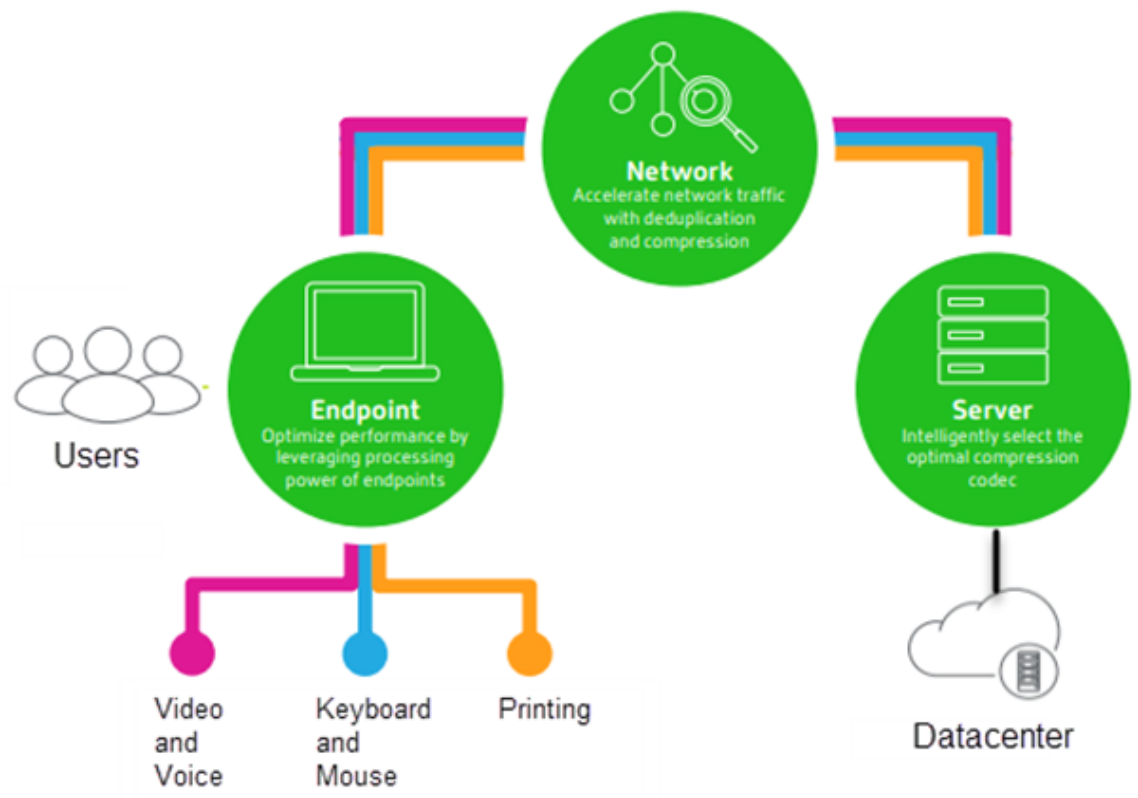


HDX は、次の 3 つの技術原則に基づいて設計されています:

- インテリジェントリダイレクト
- 連続文字圧縮
- データ重複排除

これらの原則をさまざまに組み合わせて適用することで、IT 部門およびユーザーの操作を最適化し、帯域幅の消費量を抑えてホストサーバーあたりのユーザー密度を増やすことができます。

- インテリジェントリダイレクト - 画面のアクティビティ、アプリケーションのコマンド、エンドポイントデバイス、ネットワークとサーバーの容量を調べることで、アプリケーションやデスクトップのアクティビティのレンダリング方法と表示場所を即座に決定します。レンダリングは、エンドポイントデバイスまたはホストサーバーのどちらかで行われます。
- アダプティブ圧縮 - 細いネットワーク接続でも、マルチメディアを高鮮明に表示して配信できます。HDX はまず、入力のタイプ、デバイスのタイプ、ディスプレイのタイプ（テキスト、動画、音声、マルチメディア）などのいくつかの変動要素を評価します。次に、最適な圧縮コーデックと、CPU および GPU の最適な使用率を選択します。さらに、ユニークユーザーごとにこの設定をインテリジェントにカスタマイズします。このインテリジェントな適応は、ユーザーごと、またはセッションごとでも行われます。



- データ重複排除 - 重複したネットワークトラフィックを排除することで、クライアントとサーバー間で送信される総データ量を削減します。これは、ビットマップ画像、ドキュメント、印刷ジョブ、ストリーム配信メディアなどのアクセス頻度の高いデータで繰り返されるパターンを活用して行っています。これらのパターンをキャッシュ化することで、重複したトラフィックを排除し、ネットワークで変更内容のみを送信できます。HDX では、マルチメディアストリームのマルチキャストもサポートされます。このマルチキャストでは、ソースからの単一の送信データを、ユーザーごとの 1 対 1 接続ではなく、1 つの場所にいる複数のサブスクライバーが視聴します。

詳しくは、『ユーザーワークスペースの高品位化による生産性の向上』を参照してください。

デバイスで

ユーザーデバイスのコンピューティング容量を利用して、ユーザーエクスペリエンスを拡張および最適化します。HDX テクノロジにより、スムーズでシームレスなマルチメディアコンテンツが仮想デスクトップやアプリケーションに提供されます。ワークスペースコントロール機能により、仮想デスクトップやアプリケーションのセッションを一時停止して、ほかのデバイスでそのセッションでの作業を再開できます。

ネットワークで

HDX による高度な最適化およびアクセラレーションにより、待機時間が長く低帯域幅の WAN 接続を含むあらゆるネットワークにおいて最高のパフォーマンスが提供されます。

HDX 機能は環境のさまざまな条件に応じて最適化されます。パフォーマンスと消費帯域幅を調和させる機能。社内ネットワークからデスクトップやアプリケーションにローカルにアクセスする場合やファイアウォールの外側からリモートにアクセスする場合など、各ユーザーシナリオに応じて最適な機能が適用されます。

データセンターでは

HDX では、サーバー側の処理能力およびスケーラビリティを利用して、クライアントデバイス側の能力に制限されずに高度なグラフィックパフォーマンスを提供できます。

Citrix Director では、ユーザーデバイスに接続している HDX チャネルの状態を監視できます。

HDX Insight

HDX Insight により、NetScaler Network Inspector および Performance Manager が Director に統合されます。ICA トラフィックに関するデータを収集して、リアルタイムおよび履歴の詳細をダッシュボードに表示します。このデータには、クライアント側およびサーバー側の ICA セッション遅延、ICA チャネルの帯域幅使用量、および各セッションの ICA 往復時間値が含まれます。

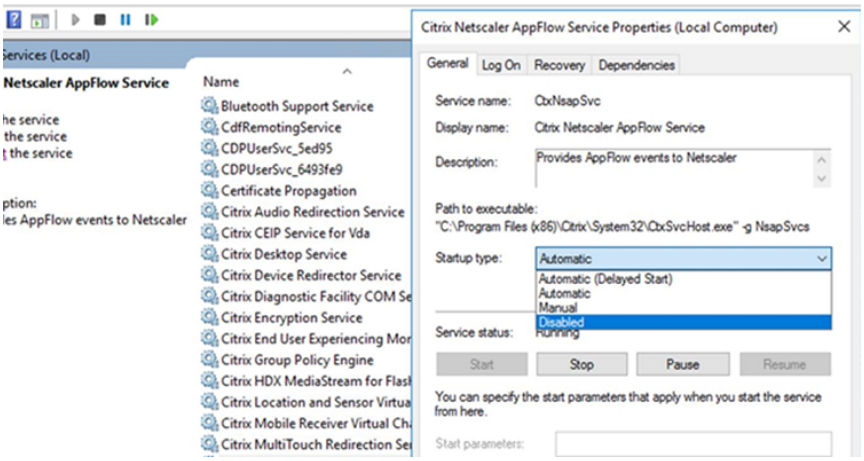
NetScaler で HDX Insight 仮想チャネルを使用して必要なすべてのデータポイントを非圧縮形式で移動できるようにすることができます。この機能を無効にした場合、NetScaler デバイスは、さまざまな仮想チャネルに分散した ICA トラフィックを暗号化解除して解凍します。単一の仮想チャネルを使用すると、複雑さが軽減され、スケーラビリティが向上し、コスト効率が向上します。

最小要件:

- NetScaler バージョン 12.0 ビルド 57.x
- Windows 向け Citrix Workspace アプリ 1808
- Citrix Receiver for Windows 4.10
- Mac 向け Citrix Workspace アプリ 1808
- Citrix Receiver for Mac 12.8

HDX Insight 仮想チャネルを有効または無効にする

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



仮想デスクトップからの **HDX** 機能の体験

- Web ブラウザーコンテンツリダイレクト（4 つある HDX マルチメディアリダイレクト技術のうちの 1 つ）により、HTML5 と WebRTC マルチメディアコンテンツの配信がどのように高速化されるかを体験するには、次の手順に従います：

  1. Chrome ブラウザーの拡張機能をダウンロードして、仮想デスクトップにインストールします。
  2. 仮想デスクトップへのマルチメディアコンテンツ配信に関する Web ブラウザーコンテンツリダイレクトのパフォーマンスを体験するには、仮想デスクトップで HTML5 動画を含むウェブサイト（YouTube など）にアクセスして、動画を再生します。ユーザーには、Web ブラウザーコンテンツリダイレクトがいつ実行されているかはわかりません。Web ブラウザーコンテンツリダイレクトが使用されているかどうかを確認するには、Web ブラウザーのウィンドウをすばやくドラッグします。ビューポートやユーザーインターフェイスの表示が遅れるか、これらの間のフレームが消失します。また、ウェブページ上で右クリックすると、メニューに ［**HDX Web** ブラウザーリダイレクトについて］が表示されます。

- HDX により高品位オーディオがどのように配信されるかを体験するには、次の手順に従います：

  1. Citrix Workspace アプリで、最高の音質を選択します。詳しくは、Citrix Workspace アプリのドキュメントを参照してください。
  2. デスクトップ上のデジタルオーディオプレーヤー（iTunes など）で音楽ファイルを再生します。

HDX では、特別な構成を行わなくてもデフォルトで、一般的なユーザーに適したグラフィックおよびビデオ配信が提供されます。Citrix ポリシー設定は、一般的な使用環境で最適なユーザーエクスペリエンスが提供されるようにデフォルトで有効になっています。

- HDX は、クライアントプラットフォーム、アプリケーション、およびネットワーク帯域幅に基づいて最適な配信方法を自動的に選択し、状況の変化に応じて自動調整します。
- HDX は、2D および 3D のグラフィックおよびビデオのパフォーマンスを最適化します。
- HDX は、インターネットやイントラネット上のマルチメディアコンテンツなどをホストサーバーを介さず直接ユーザーデバイス上にストリーム配信します。このクライアント側でのコンテンツ取得に必要な条件が満たされない場合、メディア配信はサーバー側でのコンテンツ取得とマルチメディアリダイレクトにフォールバックします。通常、マルチメディアリダイレクト機能に関するポリシーを変更する必要はありません。
- マルチメディアリダイレクトが利用できない場合、HDX は仮想デスクトップにサーバー側でレンダリングしたビデオコンテンツを提供します。http://www.microsoft.com/silverlight/iis-smooth-streaming/demo/などのサイトにアクセスして、高品位ビデオを含む Web サイト上のビデオをご覧ください。

ヒント:

- HDX 機能に関するサポートおよび要件については、「システム要件」を参照してください。特に注記のあるものを除き、Windows マルチセッション OS マシン、Windows シングルセッションOS マシン、およびリモート PC アクセスのデスクトップで HDX 機能を使用できます。
- このセクションのトピックでは、ユーザーエクスペリエンスを最適化したり、サーバーのスケーラビリティを改善したり、消費帯域幅を抑えたりする方法について説明します。Citrix ポリシーおよびそのポリシー設定について詳しくは、このリリースの「Citrix ポリシー」を参照してください。
- レジストリを編集する場合は細心の注意が必要です: レジストリエディターの使用を誤ると、深刻な問題が発生する可能性があり、Windows の再インストールが必要になる場合もあります。レジストリエディターの誤用による障害に対して、Citrix では一切責任を負いません。レジストリエディターは、お客様の責任と判断の範囲でご使用ください。また、レジストリファイルのバックアップを作成してから、レジストリを編集してください。

クライアントの自動再接続とセッション画面の保持

ホストされるアプリケーションまたはデスクトップにアクセスすると、ネットワークが中断される場合があります。再接続をスムーズに行うために、クライアントの自動再接続とセッション画面の保持が利用できます。デフォルト構成では、セッション画面の保持が起動した後、クライアントの自動再接続が起動します。

クライアントの自動再接続:

クライアントの自動再接続によってクライアントのエンジンが再起動され、切断されたセッションに再接続します。クライアントの自動再接続によって設定で指定した時間が経過すると、ユーザーセッションがクローズ（または切断）されます。クライアントの自動再接続の実行中に、システムからユーザーに次のようなアプリケーションとデスクトップに関するネットワーク中断通知が送信されます:

- デスクトップ。セッションウィンドウが灰色表示になり、カウントダウンタイマーが再接続されるまでの時間を表示します。

- アプリケーション。セッションウィンドウがクローズし、ダイアログが開いて再接続が試行されるまでの時間を示すカウントダウンタイマーが表示されます。

クライアントの自動再接続中に、セッションはネットワーク接続を見越して再起動されます。クライアントの自動再接続の実行中は、セッションを操作できません。

再接続では、切断されたセッションは、保存された接続情報を使って再接続されます。ユーザーは、正常にアプリケーションおよびデスクトップを操作できます。

クライアントの自動再接続のデフォルト設定:

- クライアントの自動再接続のタイムアウト：120 秒
- クライアントの自動再接続：有効
- クライアントの自動再接続時の認証：無効
- クライアントの自動再接続のログ：無効

詳しくは、「クライアントの自動再接続のポリシー設定」を参照してください。

セッション画面の保持:

セッション画面の保持によって ICA セッションは、ネットワークの中断を挟んでもシームレスに再接続されます。セッション画面の保持によって設定で指定した時間が経過すると、ユーザーセッションがクローズ（または切断）されます。セッション画面の保持がタイムアウトした後で、クライアントの自動再接続設定が有効になり、切断されたセッションへの再接続が行われます。セッション画面の保持の実行中に、ユーザーに次のようなアプリケーションとデスクトップに関するネットワーク中断通知が送信されます。

- デスクトップ。セッションウィンドウが半透明表示になり、カウントダウンタイマーが再接続されるまでの時間を表示します。
- アプリケーション。ウィンドウが半透明表示になると同時に、通知領域に中断された接続のポップアップが表示されます。

セッション画面の保持がアクティブの間は、ユーザーは ICA セッションを操作できません。ただし、キー入力のようなユーザー操作は、ネットワーク中断直後の数秒間バッファーされ、ネットワークが再接続されたら再送信されます。

再接続されると、クライアントとサーバーは、プロトコルを交換したポイントからセッションを再開します。セッションウィンドウの半透明表示が解除され、アプリケーションに対する適切なポップアップが通知領域に表示されます。

セッション画面の保持のデフォルト設定

- セッション画面の保持のタイムアウト 180 秒
- 再接続 UI の透過レベル：80%
- セッション画面の保持の接続：有効
- セッション画面の保持のポート番号：2598

詳しくは、「セッション画面の保持のポリシー設定」を参照してください。

NetScaler とクライアントの自動再接続およびセッション画面の保持:

マルチストリームポリシーとマルチポートポリシーがサーバー上で有効化され、次の条件のいずれかまたはすべてに合致する場合、クライアントの自動再接続は機能しません。

- セッション画面の保持機能が NetScaler Gateway で無効化されている。
- NetScaler アプライアンスでフェールオーバーが発生している。
- NetScaler Gateway で NetScaler SD-WAN を使用している。

HDX アダプティブスループット

HDX アダプティブスループットは、出力バッファーを調整することで、ICA セッションのピークスループットをインテリジェントに微調整します。出力バッファーの数は、最初は大きい値に設定されます。値を大きくすることで、特に高遅延のネットワークで、データをより迅速かつ効率的にクライアントに送信できます。高い双方向性、高速なファイル転送、スムーズなビデオ再生、および高いフレームレートと解像度により、優れたユーザーエクスペリエンスを実現します。

セッションの双方向性を常に測定して、ICA セッション内のデータストリームが双方向性に悪影響を及ぼしているかどうかを判別します。悪影響を及ぼしている場合、スループットを低下させて、大規模データストリームがセッションに与える影響を減らし、双方向性を回復できるようにします。

> 重要:
>
> HDX アダプティブスループットでは、このメカニズムをクライアントから VDA に移行することにより、出力バッファーの設定方法を変更しています。手動での構成は必要ありません。

この機能には以下の要件があります:

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

ユーザーデバイスに送信されるイメージ品質の改善

視覚表示ポリシー設定は、仮想デスクトップからユーザーデバイスに送信されるイメージの品質を制御します。

- 表示品質。ユーザーデバイス上に表示されるイメージの表示品質として、[低]、[中]、[高]、[常に無損失]、または［操作時は低品質］を指定します。デフォルトは［中］です。メディアのデフォルト設定による実際のビデオ品質は、利用可能な帯域幅によって異なります。
- ターゲットフレーム数仮想デスクトップからユーザーデバイスに送信されるイメージの 1 秒あたりの最大フレーム数（fps）を指定します。デフォルトは 30fps です。CPU が低速なデバイスでは、小さい値を指定した方がユーザーエクスペリエンスが向上する場合があります。サポートされている 1 秒あたりの最大フレームレートは 60 です。

- 表示メモリの制限。セッションのビデオバッファーの最大サイズをキロバイト単位で指定します。デフォルトは 65536KB です。高い色数および解像度を使用するセッションでは、大きい値を指定します。必要なメモリの量は算出できます。

> 注:
>
> [表示メモリの制限] 設定は廃止されました。この変更により、Citrix は表示メモリを制限しなくなりました。代わりに、クライアントの表示レイアウトに完全に対応できるように、必要な最小限のメモリが割り当てられます。

ビデオ会議パフォーマンスの改善

いくつかの一般的なビデオ会議アプリケーションは、マルチメディアリダイレクトを介する Citrix Virtual Apps and Desktops からの配信に最適化されています（「HDX RealTime Optimization Pack」などを参照）。最適化されていないアプリケーションでは、HDX Web カメラビデオ圧縮を使用すると、セッションでのビデオ会議で Web カメラの帯域幅使用効率および遅延に対する耐性が向上します。この機能では、Web カメラのトラフィックが専用のマルチメディア仮想チャネルでストリーム配信されます。この機能では、HDX Plug-n-Play USB リダイレクトサポートのアイソクロナス転送に比べて帯域幅消費が少なく、WAN 接続に適しています。

このデフォルト設定は、Citrix Workspace アプリユーザーが Desktop Viewer の［マイクと Web カメラ］設定で、［マイクおよび **Web** カメラを使用しない］を選択すると無効になります。ユーザーが［HDX Web カメラビデオ圧縮］から切り替えられないようにするには、［ICA ポリシーの設定］>［USB デバイスのポリシー］のポリシー設定を使用して、USB デバイスのリダイレクトを無効にします。

HDX Web カメラビデオ圧縮を使用するには、以下のポリシー設定を有効にする必要があります（これらの設定項目はデフォルトで有効になっています）。

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

Web カメラでハードウェアエンコード機能がサポートされる場合、HDX Web カメラビデオ圧縮ではデフォルトでそのハードウェアエンコードが使用されます。ハードウェアエンコード機能は、ソフトウェアエンコードより多くの帯域幅を消費する場合があります。ソフトウェアエンコードが使用されるようにするには、レジストリキー HKEY_CURRENT_USER\Software\Citrix\HdxRealTime に DWORD 値 DeepCompress_ForceSWEncode=1 を設定します。

ネットワークトラフィックの優先度

QoS（サービス品質）機能をサポートするルーターを使ってセッションに複数の接続を使用する場合、ネットワークトラフィックの優先度を割り当てることができます。ユーザーデバイスとサーバー間の ICA トラフィックでは、4 つの TCP ストリームと 2 つのユーザーデータグラムプロトコル（UDP）ストリームを使用できます。

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

各仮想チャネルには特定の優先度が割り当てられており、対応する接続を使って転送が行われます。これらの仮想チャネルには、使用される TCP ポート番号に基づいて個別に優先度を設定できます。

Windows 10、Windows 8 および Windows 7 マシンにインストールした Virtual Delivery Agent（VDA）では、複数チャネルのストリーム接続がサポートされます。ネットワーク管理者に問い合わせて、［マルチポートポリシー］設定で指定した CGP（Common Gateway Protocol）ポートが、ネットワークルーター上で正しく割り当てられていることを確認してください。

QoS（サービス品質）は、セッション画面の保持機能のポートまたは CGP ポートが複数構成されている環境でのみサポートされます。

> 警告：
>
> この機能を使用する場合は、トランスポートセキュリティを使用してください。IPsec（Internet Protocol Security）または TLS（Transport Layer Security）を使用することを Citrix ではお勧めします。TLS 接続がサポートされるのは、マルチストリーム ICA をサポートする NetScaler Gateway を通過するトラフィックのみです。企業内ネットワークでは、TLS を使用したマルチストリーム接続はサポートされません。

マルチストリーム接続のサービス品質を設定するには、ポリシーに以下の Citrix ポリシー設定を追加します（詳しくは、「マルチストリーム接続のポリシー設定」を参照してください）。

- マルチポートポリシー - 複数接続を介した ICA トラフィックで使用されるポートおよびそのネットワーク優先度を指定します。
  - ［CGP デフォルトポートの優先度］ボックスの一覧で、優先度を選択します。デフォルトでは、プライマリポート（2598）に優先度［高］が設定されています。
  - ［CGP ポート 1］、［CGP ポート 2］、および［CGP ポート 3］ボックスに追加の CGP ポートを入力して、それぞれ優先度を選択します。各ポートには異なる優先度を設定する必要があります。

  VDA 側のファイアウォールで、追加した TCP トラフィックを明示的に許可する必要があります。
- マルチストリームコンピューター設定 - この設定は、デフォルトでは無効になっています。Citrix NetScaler SD-WAN でマルチストリーム機能をサポートする場合は、この設定項目を使用する必要はありません。このポリシー設定は、サードパーティ製のルーターや従来の NetScaler SD-WAN を使用する環境で QoS（サービス品質）優先度を指定するときに使用できます。
- マルチストリームユーザー設定—この設定は、デフォルトでは無効になっています。

ポリシーの設定を反映させるには、ユーザーがネットワークに再ログオンする必要があります。

リモート言語バーを表示または非表示にする

言語バーには、アプリケーションセッションでの優先される入力言語が表示されます。この機能が有効（デフォルト）になっている場合、Windows 向け Citrix Workspace アプリの ［詳細設定］ > ［言語バー］から言語バーを表示ま

たは非表示にできます。VDA 側でレジストリ設定を使用すると、言語バー機能のクライアント制御を無効にできます。この機能を無効にした場合、クライアントの UI 設定が有効にならず、ユーザーごとの現在の設定によって言語バーの状態が決まります。詳しくは、「ユーザーエクスペリエンスの向上」を参照してください。

VDA から言語バー機能のクライアント制御を無効にするには:

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

Unicode キーボードマッピング

Windows 以外の Citrix Receiver は、ローカルのキーボードレイアウト（Unicode）を使用します。ユーザーがローカルのキーボードレイアウトとサーバーのキーボードレイアウト（スキャンコード）を変更すると、それらが同期しない可能性があり、出力が不正になります。たとえば、User1 が、ローカルのキーボードレイアウトを英語からドイツ語に変更しました。その後、User1 は、サーバー側のキーボードをドイツ語に変更しました。両方のキーボードレイアウトがドイツ語であっても、これらが同期しない可能性があり、不正な文字出力の原因となります。

Unicode キーボードレイアウトマッピングを有効または無効にする

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

KEY_LOCAL_MACHINE/SOFTWARE/Citrix/CtxKlMap

値の名前：EnableKlMap

種類：DWORD

値：1

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

Unicode キーボードレイアウトマッピング互換モードを有効にする

デフォルトでは、Unicode キーボードレイアウトマッピングは、サーバー側のキーボードレイアウトを変更すると、新しい Unicode キーボードレイアウトマップをリロードするためになんらかの Windows API に自動的にフックします。いくつかのアプリケーションはフックされないことがあります。互換性を維持するために、機能を互換モードに変更して、これらのフックされないアプリケーションをサポートすることができます。次のレジストリキーを追加します:

HKEY_LOCAL_MACHINE/SOFTWARE/Citrix/CtxKlMap

値の名前：DisableWindowHook

種類：DWORD

値：1

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

Citrix ICA 仮想チャネル

August 17, 2024

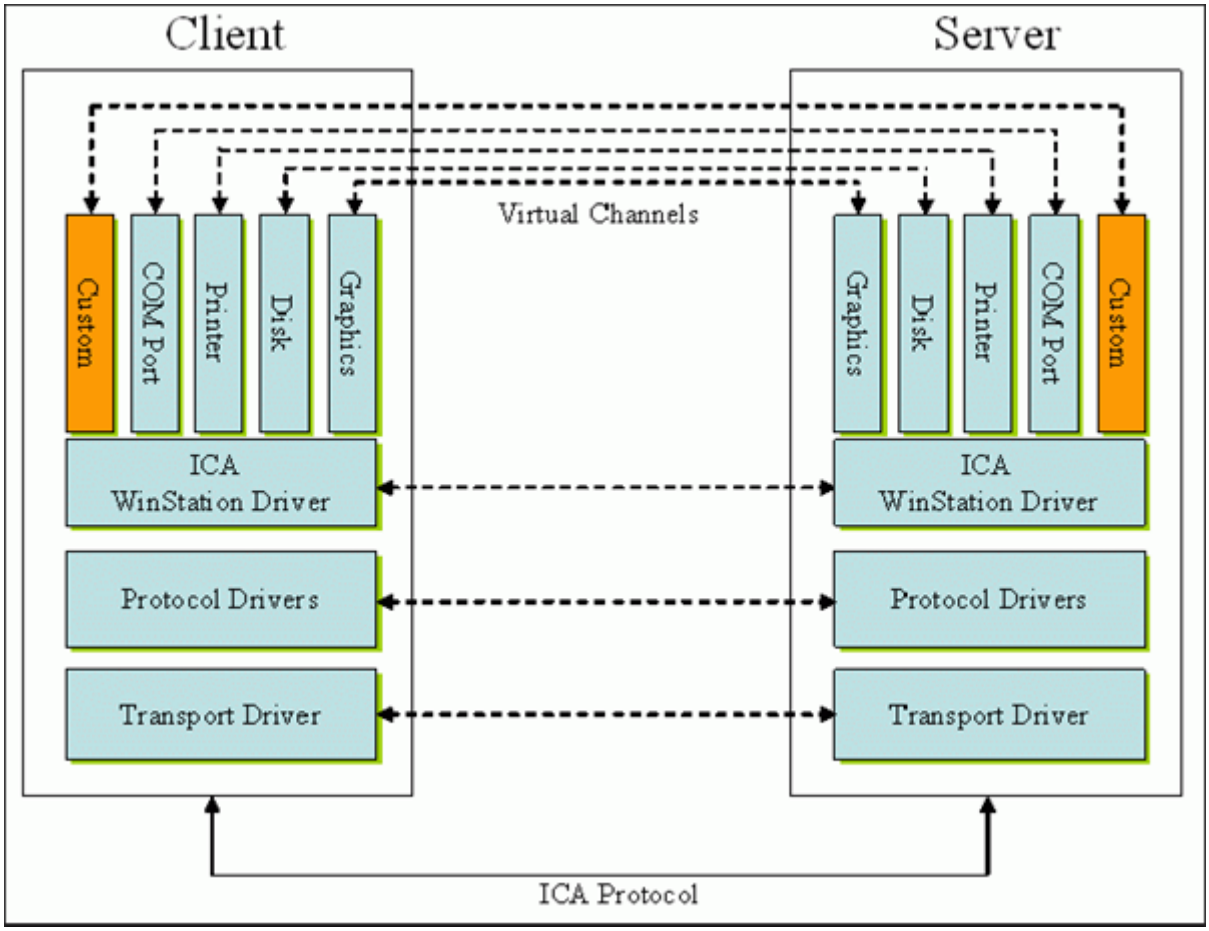
> 警告：
>
> レジストリエディターの使用を誤ると、深刻な問題が発生する可能性があり、オペレーティングシステムの再インストールが必要になる場合もあります。レジストリエディターの誤用による障害に対して、Citrix では一切責任を負いません。レジストリエディターは、お客様の責任と判断の範囲でご使用ください。また、レジストリファイルのバックアップを作成してから、レジストリを編集してください。

ICA 仮想チャネルとは何か

Citrix Workspace アプリと Citrix Virtual Apps and Desktops サーバー間の機能および通信の大部分は、仮想チャネル経由で実行されます。仮想チャネルは Citrix Virtual Apps and Desktops サーバーを使用したリモートコンピューティング環境に不可欠な要素です。仮想チャネルは次の用途に使用されます：

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

Citrix Virtual Apps and Desktops サーバーおよび Citrix Workspace アプリの新しいバージョンとともに、追加機能を提供する新しい仮想チャネルが随時リリースされます。



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

仮想チャネルによって、さまざまなタスクを安全な方法で実行できます。たとえば、Citrix Virtual Apps サーバー上で動作するアプリケーションとクライアント側デバイス間の通信や、アプリケーションとクライアント側環境間の通信などです。

クライアント側では、仮想チャネルは仮想ドライバーに対応します。各仮想ドライバーは、特定の機能を提供します。通常の動作に必要な仮想ドライバーやオプションの仮想ドライバーもあります。仮想ドライバーは、プレゼンテーション層のプロトコルレベルで動作します。Windows Station（WinStation）プロトコル層で提供されたチャネルを多重化することにより、いつでも複数のプロトコルをアクティブにできます。

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

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

または

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

- Thinwire3.0（必須）
- ClientDrive
- ClentPrinterQueue
- ClentPrinterPort
- クリップボード
- ClientComm
- ClientAudio
- LicenseHandler（必須）
- TWI（必須）
- SmartCard
- ICACTL（必須）
- SSPI
- TwainRdr
- UserEXperience
- Vd3d

> 注:
>
> レジストリキーからこれらの 1 つまたは複数の値を削除することによって、特定のクライアント機能を無効にできます。たとえば、クライアントクリップボードを削除する場合は、**Clipboard** という単語を削除します。

この一覧には、クライアント仮想ドライバーファイルと対応する機能が含まれています。Citrix Virtual Apps および Windows 向け Citrix Workspace アプリはこれらのファイルを使用します。これらは Windows ドライバー（カーネルモード）形式ではなく、ダイナミックリンクライブラリ（ユーザーモード）形式のファイルです。ただし、「汎用 USB 仮想チャネル」で説明する汎用 USB は例外です。

- vd3dn.dll –デスクトップコンポジションリダイレクトに使用される Direct3D 仮想チャネル
- vdcamN.dll –双方向オーディオ
- vdcdm30n.dll –クライアントドライブマッピング
- vdcom30N.dll - クライアント側 COM ポートのマッピング
- vdcpm30N.dll –クライアント側プリンターのマッピング
- vdctln.dll –ICA コントロールチャネル
- vddvc0n.dll –動的仮想チャネル
- vdeuemn.dll - EUEM（End User Experience Monitoring：エンドユーザー状況監視）
- vdgusbn.dll –汎用 USB 仮想チャネル
- vdkbhook.dll –透過的なキーのパススルー
- vdlfpn.dll –UDP 経由の Framehawk ディスプレイチャネル（転送など）
- vdmmn.dll –マルチメディアのサポート
- vdmrvc.dll –Mobile Receiver 仮想チャネル

- vdmtchn.dll - マルチタッチのサポート
- vdscardn.dll –スマートカードのサポート
- vdsens.dll –センサー仮想チャネル
- vdspl30n.dll –クライアントの UPD
- vdsspin.dll –Kerberos
- vdtuin.dll –透過的な UI
- vdtw30n.dll –クライアントの Thinwire
- vdtwin.dll –シームレス
- vdtwn.dll –Twain

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

64 ビット環境との互換性

Windows 向け Citrix Workspace アプリは 64 ビット環境との互換性があります。32 ビット用にコンパイルされた大半のバイナリのように、これらのクライアントファイルには、64 ビットでコンパイル版があります:

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

汎用 **USB** 仮想チャネル

汎用 USB 仮想チャネルの実装では、仮想チャネルドライバー vdgusbn.dll とともに 2 つのカーネルモードドライバーが使用されます:

- ctxusbm.sys
- ctxusbr.sys

ICA 仮想チャネルの動作

仮想チャネルはさまざまな方法で読み込まれます。シェル（サーバーの場合 WfShell、ワークステーションの場合 PicaShell）によって読み込まれる仮想チャネルがあります。一部の仮想チャネルは Windows サービスとしてホストされています。

以下は、シェルによって読み込まれる仮想チャネルモジュールの例です：

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

以下の例のように、カーネルモードで読み込まれる場合もあります：

- ctxDvcs.sys –動的仮想チャネル
- icausbb.sys –汎用 USB リダイレクト
- picadm.sys –クライアントドライブマッピング
- picaser.sys –COM ポートリダイレクト
- picapar.sys –LPT ポートリダイレクト

サーバー側のグラフィック仮想チャネル

`ctxgfx.exe`はワークステーションとターミナルサーバーの両方でセッションごとにグラフィック仮想チャネルをホストします。`Ctxgfx`は、対応するドライバー（RDSH の場合は`Icardd.dll`、ワークステーションの場合は`vdod.dll`と`vidd.dll`）と通信するプラットフォーム固有のモジュールをホストします。

XenDesktop 3D Pro 展開では、OEM グラフィックドライバーは VDA の対応する GPU にインストールされています。`Ctxgfx`は、OEM グラフィックドライバーと通信するための専用のアダプターモジュールを読み込みます。

Windows サービスでの専用チャネルのホスト

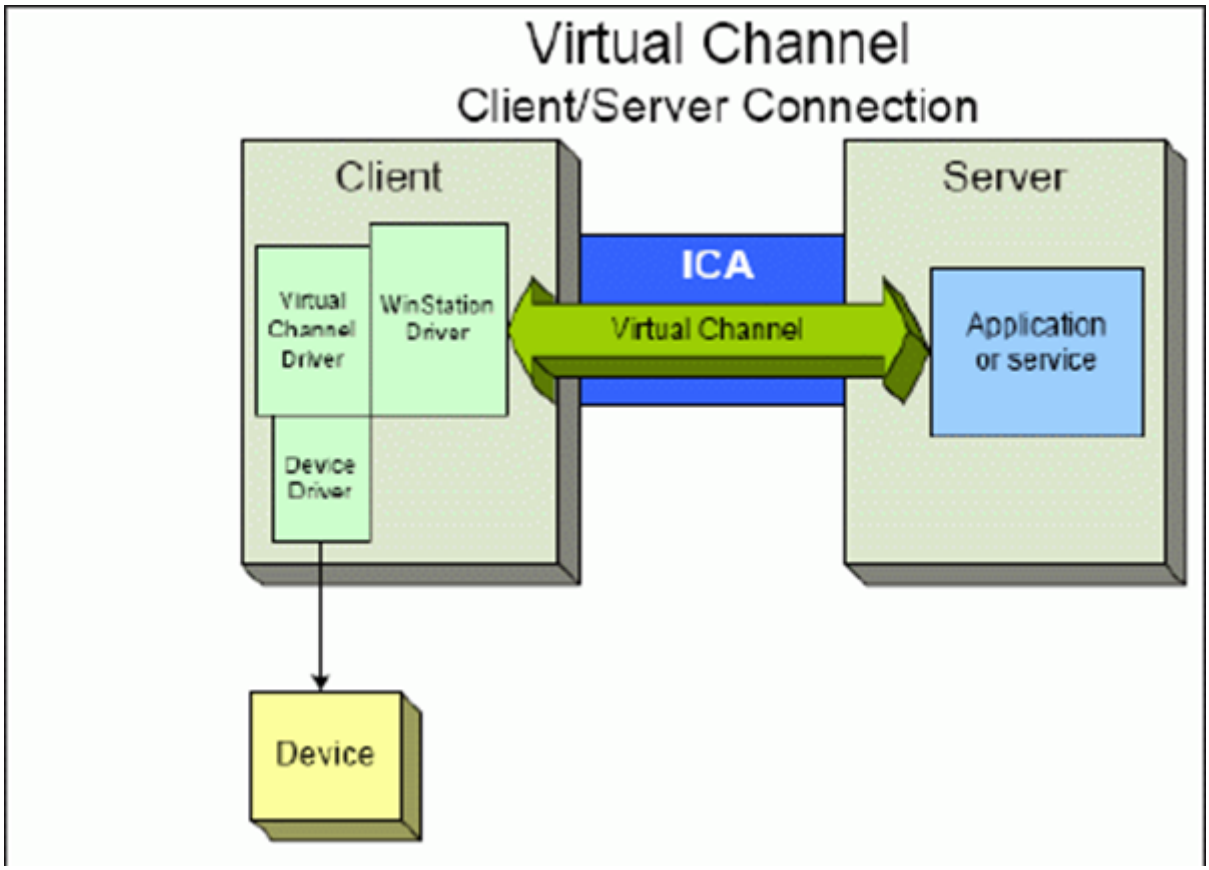
Citrix Virtual Apps and Desktops サーバーでは、さまざまなチャネルが Windows サービスとしてホストされています。これによって、サーバー上のシングルセッションおよびマルチセッションで複数のアプリケーションの 1 対多の運用が可能になります。以下はこうしたサービスの例です：

- Citrix Device Redirector Service
- Citrix Dynamic Virtual Channel Service
- Citrix EUEM （End User Experience Monitoring：エンドユーザー状況監視）
- Citrix Location and Sensor Virtual Channel Service

- Citrix MultiTouch Redirection Service
- Citrix Print Manager Service
- Citrix Smartcard Service
- Citrix Audio Redirection Service（Citrix Virtual Desktops のみ）
- Citrix ICA Status Channel Service

Windows オーディオサービスを使用して Citrix Virtual Apps でオーディオ仮想チャネルがホストされます。

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



これは、仮想チャネルを使用したクライアント-サーバー間のデータ交換処理の概要を示します。

1. クライアントが Citrix Virtual Apps and Desktops サーバーに接続します。クライアントは、サポートする仮想チャネルに関する情報をサーバーに渡します。
2. サーバー側アプリケーションが起動し、仮想チャネルのハンドルを取得して、必要に応じて仮想チャネルに関する情報を問い合わせます。
3. クライアント仮想ドライバーとサーバー側アプリケーションは、次の 2 つの方法でデータを渡します：
    - サーバー側アプリケーションにクライアントへの送信データがある場合は、そのデータが直ちにクライ

アントに送信されます。クライアントがこのデータを受け取ると、WinStation ドライバーが ICA ストリームから仮想チャネルデータを逆多重化し、それを直ちにクライアント仮想ドライバーに渡します。

- クライアント仮想ドライバーにサーバーへの送信データがある場合は、WinStation ドライバーが次回ポーリングを行ったときにそのデータが送信されます。サーバーがこのデータを受信すると、そのデータは仮想チャネルアプリケーションが読み込むまでキューに保持されます。サーバーがデータを受け取ったことは、サーバーの仮想チャネルアプリケーションに通知されません。

4. サーバーの仮想チャネルアプリケーションが読み取りを完了すると、アプリケーションは仮想チャネルを終了し、割り当てられているすべてのリソースが解放されます。

仮想チャネル **SDK** を使って独自の仮想チャネルを作成する

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

仮想チャネル SDK を使って仮想チャネルを作成するには、プログラミング知識が必要です。この方法で、クライアントとサーバー間の主要な通信パスを提供します。例として、クライアント側であるデバイス（スキャナーなど）をセッション内のプロセスとともに使用する機能を実装する場合などがあります。

> 注:
>
> - 仮想チャネル SDK では、WFAPI SDK で仮想チャネルのサーバー側を作成する必要があります。
> - Citrix Virtual Apps and Desktops のセキュリティが強化されているため、ICA セッションで開くことができる仮想チャネルを指定する必要があります。詳しくは、「仮想チャネルの許可リストポリシー設定」を参照してください。

ICA クライアントオブジェクト **SDK** を使って独自の仮想チャネルを作成する

ICA クライアントオブジェクト（ICO）を使用した仮想チャネルの作成は、仮想チャネル SDK を使用する場合より簡単です。プログラム内で **CreateChannels** メソッドを使って名前付きオブジェクトを作成し、ICO を使用します。

> 重要:
>
> Citrix Receiver for Windows バージョン 10.00 以降（および Windows 向け Citrix Workspace アプリ）ではセキュリティが強化されているため、ICO 仮想チャネルの作成時に追加手順が必要になります。

仮想チャネルのパススルー機能

Citrix から提供される仮想チャネルの大部分は、ICA セッション内またはより一般にパススルーセッションと呼ばれるセッション内で Windows 向け Citrix Workspace アプリを使用する場合でも変更なしで動作しますが、マルチホップ構成でクライアントを使用する場合はいくつか注意すべき点があります。

以下の機能は、シングルホップ構成でもマルチホップ構成でも同様に動作します：

- クライアント側 COM ポートのマッピング
- クライアントドライブマッピング
- クライアント側プリンターのマッピング
- クライアントの UPD
- EUEM（End User Experience Monitoring：エンドユーザー状況監視）
- 汎用 USB
- kerberos
- マルチメディアのサポート
- スマートカードのサポート
- 透過的なキーのパススルー
- Twain

各ホップで実行される圧縮、展開、レンダリングなどの処理に本質的に伴う遅延やその他の要因により、一部の機能ではクライアントが経由するホップが増えるとパフォーマンスが影響を受ける可能性があります。以下は影響を受ける機能です：

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

> 重要：
>
> デフォルトでは、パススルーセッション内で動作するクライアントのインスタンスによってマップされるクライアントドライブは、接続元クライアントドライブに制限されます。

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

多くの Citrix 製品は、Windows 向け Citrix Workspace アプリが Citrix Virtual Desktops サーバー上の ICA セッション内（一般的にはパススルーセッションとして知られている）で使用されている場合、操作が変更されることなく動作する仮想チャネルを提供しています。

具体的には、Citrix Virtual Desktops サーバー上で **picaPassthruHook** を実行する VDA Hook があります。これによって、クライアントを CPS サーバー上で動作していると信じさせ、一般的なパススルーモードへと設定します。

以下の標準的な仮想チャネルおよびその機能がサポートされています：

- クライアント
- クライアント側 COM ポートのマッピング

- クライアントドライブマッピング
- クライアント側プリンターのマッピング
- 汎用 USB（パフォーマンスにより制限あり）
- マルチメディアのサポート
- スマートカードのサポート
- SSON
- 透過的なキーのパススルー

セキュリティと **ICA** 仮想チャネル

使用環境でのセキュリティ確保は、仮想チャネルのプランニング、開発、実装における重要な要素です。この文書には、特定分野のセキュリティに関する参照情報が記載しています。

ベストプラクティス

仮想チャネルは接続時および再接続時に開き、ログオフ時および切断時に閉じます。

仮想チャネル機能を使用するスクリプトを作成する場合は、以下の指針に従います。

仮想チャネルの名前付け：

仮想チャネルは最大で 32 個作成できます。そのうち 17 個は、特定の用途に予約されています。

- 仮想チャネルには、7 文字以下の名前を付ける必要があります。
- 最初の 3 文字はベンダー名、それ以降の 4 文字はチャネルの種類を表します。たとえば、**CTXAUD** は Citrix のオーディオ仮想チャネルを表します。

仮想チャネルは、ASCII 文字からなる 7 文字以下の名前で参照されます。ICA プロトコルの以前のバージョンでは仮想チャネルに番号が付けられていましたが、現在のバージョンでは ASCII 名に基づいて動的に番号が付けられるため、実装が簡単になっています。社内でのみ使用する独自の仮想チャネルを開発する場合、仮想チャネルには既存の仮想チャネル名と異なる任意の 7 文字の名前を付けることができます。仮想チャネル名では、ASCII 文字の大文字、小文字、数字だけを使用できます。独自の仮想チャネルを追加する場合は、既存の命名規則に従います。あらかじめ定義されているいくつかの仮想チャネルがあります。これらの仮想チャネルはすべて、OEM 識別子 CTX から始まる名前を持ち、Citrix によってのみ使用されます。

ダブルホップのサポート：

仮想チャネル	ダブルホップがサポートされているか
オーディオ	いいえ
ブラウザーコンテンツリダイレクト	いいえ
CDM	はい

仮想チャネル	ダブルホップがサポートされているか
CEIP	いいえ
クリップボード	はい
Continuum（MRVC）	いいえ
コントロール VC	はい
HTML5 ビデオリダイレクト（v1）	はい
キーボード、マウス	はい
マルチタッチ	いいえ
NSAPVC	いいえ
印刷	はい
SensVC	いいえ
Smartcard	はい
Twain	はい
USB VC	はい
WAYCOM デバイス（USB VC 使用の K2M）	はい
Web カメラビデオ圧縮	はい
Windows Media リダイレクト	はい

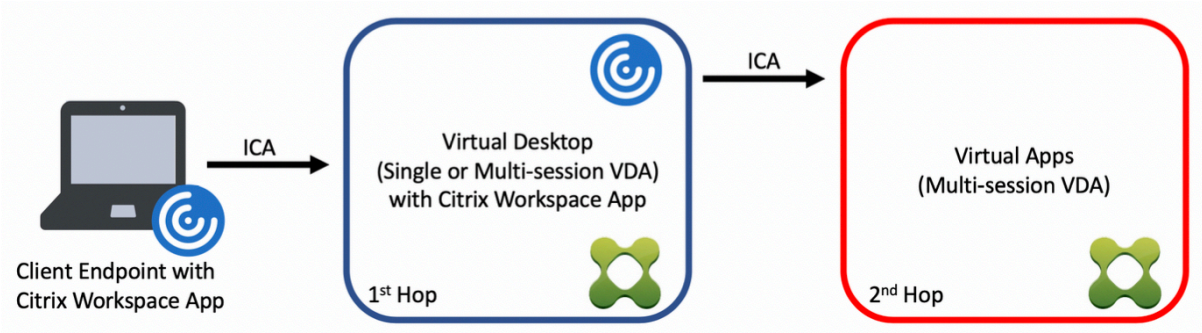
関連項目

- ICA 仮想チャネル SDK
- Citrix Developer Networkには、Citrix SDK に関するあらゆる技術的なリソースおよび解説が集約されています。このネットワークでは、SDK、サンプルコード、スクリプト、拡張機能、プラグインや、SDK ドキュメントにアクセスできます。また、Citrix Developer Network フォーラムでは、各 Citrix SDK に関する技術的な議論を参照できます。

Citrix Virtual Apps and Desktops でのダブルホップ

August 17, 2024

Citrix クライアントセッションでは、「ダブルホップ」という用語は、Citrix Virtual Desktops セッション内で実行されている Citrix Virtual Apps セッションを指します。次の図は、ダブルホップを示しています。



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

ダブルホップ展開モデルを使用して、さまざまなユースケースをサポートできます。Citrix Virtual Desktops 環境と Citrix Virtual Apps 環境が異なるエンティティによって管理されるケースはよくある一例です。この方法は、アプリケーションの互換性の問題を解決するのにも有効です。

システム要件

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

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

最高のパフォーマンスと互換性を実現するために、使用中の VDA バージョンと同じバージョンまたは新しいバージョンの Citrix クライアントを使用することをお勧めします。

最初のホップに、Citrix Virtual Apps セッションと組み合わされたサードパーティ製（Citrix 以外）の仮想デスクトップソリューションが含まれる環境では、サポートは Citrix Virtual Apps 環境に制限されます。Citrix Workspace アプリの互換性、ハードウェアデバイスのリダイレクト、セッションのパフォーマンスなど、サードパーティ製の仮想デスクトップに関連する問題が発生した場合、Citrix は限られた範囲でテクニカルサポートを提供できます。トラブルシューティングの一環として、最初のホップの Citrix Virtual Desktops が必要になる場合があります。

ダブルホップでの **HDX** の展開に関する考慮事項

一般に、ダブルホップの各セッションは一意であり、クライアントサーバー機能は特定のホップに分離されます。このセクションには、Citrix 管理者による特別な配慮が必要な領域が含まれています。お客様が必要な HDX 機能を徹底的にテストし、特定の環境構成のユーザーエクスペリエンスとパフォーマンスが適切であることを確認することを Citrix ではお勧めします。

グラフィック

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

遅延

エンドツーエンドの遅延は、全体的なユーザーエクスペリエンスに影響を与える可能性があります。最初のホップと 2 番目のホップの間に付加される遅延を考慮します。これは、ハードウェアデバイスのリダイレクトで特に重要です。

マルチメディア

オーディオおよびビデオコンテンツのサーバー側（セッション内）レンダリングは、最初のホップで最も効果を発揮します。2 番目のホップでのビデオ再生には、最初のホップでのデコードと再エンコードが必要なため、結果として帯域幅とハードウェアリソースの使用率が高まります。オーディオおよびビデオのコンテンツは、可能な限り最初のホップに限定する必要があります。

USB デバイスリダイレクト

HDX には、汎用リダイレクトモードと最適化されたリダイレクトモードがあり、さまざまな種類の USB デバイスをサポートしています。各ホップで使用するモードには特に注意し、次の表を参考にして最良の結果が得られるようにしてください。汎用リダイレクトモードと最適化されたリダイレクトモードについて詳しくは、「一般的 USB デバイス」を参照してください。

最初のホップ（VDI または公開されたデスクトップ）	2 番目のホップ（Virtual Apps）	サポートノート
最適化	最適化	推奨（デバイスサポートに基づく）。たとえば、USB 大容量記憶装置、TWAIN スキャナー、Web カメラ、オーディオなどです。
汎用	汎用	最適化されたオプションが使用できないデバイスの場合。
汎用	最適化	技術的には可能ですが、デバイスサポートが使用可能な場合には、両方のホップで最適化されたモードを使用することをお勧めします。
最適化	汎用	未サポート

最初のホップ（VDI または公開されたデスクトップ）	2 番目のホップ（Virtual Apps）	サポートノート

> 注:
>
> USB プロトコル固有のチャット性のために、ホップ全体でパフォーマンスが低下することがあります。機能と結果は、特定のデバイスおよびアプリケーションの要件によって異なります。検証テストは、デバイスリダイレクトのすべてのケースで強く推奨され、ダブルホップのシナリオでは特に重要です。

サポートの例外

ダブルホップセッションでは、以下を除くほとんどの HDX 機能をサポートしています:

- ブラウザーコンテンツリダイレクト
- ローカルアプリアクセス
- RealTime Optimization Pack for Skype for Business
- Microsoft Teams の最適化

インストールと構成

August 17, 2024

個々の展開手順を開始する前に、参考記事を確認して、展開中に何が起こるか、何を指定する必要があるのかを前もって確認してください。

Citrix Virtual Apps and Desktops を展開するには、次の手順を実行します。

準備

「インストールの準備」を確認し、必要なタスクをすべて完了します。

- コンセプト、機能、これまでのリリースとの差異、システム要件、およびデータベースに関する情報の参照先。
- コアコンポーネントのインストール先を決定する際の考慮事項。
- Active Directory の権限と要件。
- 利用できるインストーラー、ツール、およびインターフェイスに関する情報。

コアコンポーネントのインストール

Delivery Controller、Web Studio、Citrix Director、Citrix ライセンスサーバーをインストールします。Citrix StoreFront をインストールすることもできます。詳しくは、「コアコンポーネントのインストール」または「コマンドラインを使ったインストール」を参照してください。

サイトの作成

コアコンポーネントをインストールして Studio を起動後、サイトを作成するよう求められます。

1 つまたは複数の **Virtual Delivery Agent**（**VDA**）のインストール

Windows オペレーティングシステムが実行されているマシンに VDA をインストールします。このとき、マスターイメージにインストールすることも、各マシン上に直接インストールすることもできます。「VDA のインストール」または「コマンドラインを使ったインストール」を参照してください。Active Directory 経由で VDA をインストールする場合のスクリプト例が用意されています。

Linux オペレーティングシステムを使用しているマシンでは、「Linux Virtual Delivery Agent」のガイダンスに従ってください。

リモート PC アクセス機能を使用する場合は、オフィスにある各ユーザーの PC 上にシングルセッション OS 対応 VDA をインストールします。コア VDA サービスのみが必要な場合は、スタンドアロンの`VDAWorkstationCoreSetup.exe`インストーラーと、既存の電子ソフトウェア配信（ESD）の方法を使用します。（利用できる VDA のインストーラーについては、「インストールの準備」を参照してください。）

オプションコンポーネントのインストール

ユニバーサルプリントサーバーの使用を計画している場合は、そのサーバーコンポーネントをプリントサーバーにインストールします。「コアコンポーネントのインストール」または「コマンドラインを使ったインストール」を参照してください。

StoreFront での認証オプション（SAML アサーションなど）の使用を許可するには、Citrix Federated 認証サービスをインストールします。

エンドユーザーが自身のユーザーアカウントをより詳細に制御できるようにするには、セルフサービスパスワードリセットをインストールします。

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

- Citrix Provisioningはオプションコンポーネントで、マスターイメージをターゲットデバイスにストリーム配信してマシンをプロビジョニングします。

- Citrix Gatewayはアプリケーションアクセスのセキュリティを保護するソリューションで、詳細なアプリケーションレベルのポリシーと操作の制御機能を管理者に提供し、アプリケーションとデータへのアクセスのセキュリティを保護します。
- Citrix SD-WANは、WAN 接続のパフォーマンスを最適化するための一連のアプライアンスです。

マシンカタログの作成

Studio でサイトの作成が完了すると、マシンカタログの作成へ誘導されます。

カタログには、物理マシンまたは仮想マシン（VM）のどちらでも使用できます。仮想マシンはマスターイメージから作成できます。VM の提供にハイパーバイザーやその他のサービスを使用している場合は、まず、そのホストにマスターイメージを作成します。その後、カタログ作成時に、このイメージを指定します。これは VM を作成するときに使用されます。

デリバリーグループの作成

Web Studio で 1 つ目のマシンカタログの作成が完了すると、デリバリーグループの作成に誘導されます。

デリバリーグループは、選択されたカタログにあるマシンにアクセスできるユーザーと、そのユーザーが利用可能なアプリケーションを指定します。

アプリケーショングループの作成（オプション）

デリバリーグループの作成後、オプションでアプリケーショングループを作成できます。さまざまなデリバリーグループで共有されているアプリケーションや、デリバリーグループ内のユーザーのサブセットで使用されるアプリケーションについて、アプリケーショングループを作成できます。

既知の制限事項

Windows 向け Citrix Workspace アプリバージョン 1912 以前を使用すると、しばらくするとセッションが切断されます。この問題は、Citrix Workspace アプリの新しい LTSR および CR バージョンで修正されています。
サポートされているリリースバージョンについて詳しくは、Windows 向け Citrix Workspace アプリ/Citrix Receiver for Windows 長期サービスリリースを参照してください。

マシン **ID**

August 17, 2024

各マシンには、一意のマシン ID（コンピューターアカウント）が必要です。マシン ID は、ローカルのマシンやディレクトリ（オンプレミスの Active Directory（AD）または Azure AD）で作成および管理できます。Citrix では、Active Directory 参加済み、Azure Active Directory 参加済み、Hybrid Azure Active Directory 参加済み、またはドメイン非参加のマシンで、仮想アプリケーションおよび仮想デスクトップをホストできます。

マシン **ID** の種類

次のマシン ID の種類がサポートされています。

マシン **ID** の種類	説明
AD に参加済み	ID がオンプレミスの Active Directory で作成および管理されます。プロビジョニングされたマシンは、割り当てられたマシン ID を使用してオンプレミスの Active Directory に参加します。
Hybrid Azure AD 参加済み	ID がオンプレミスの Active Directory で作成され、Azure AD Connect で Azure AD と同期されます。プロビジョニングされたマシンは、オンプレミスの Active Directory に参加します。その後、マシンは Hybrid Azure AD 参加済みになります。Hybrid Azure AD 参加済み仮想マシンをインポートする場合、その仮想マシンは Citrix Virtual Apps and Desktops によって Active Directory 参加済み仮想マシンとして扱われます。

サポートされる構成

以下は、各シナリオでサポートされている構成の詳細です。

サポートされるインフラストラクチャ

マシン **ID**	**Citrix Virtual Apps and Desktops**	**Citrix Workspace**	**Citrix StoreFront**	**Citrix Gateway** サービス	**Citrix Gateway**
AD に参加済み	はい	はい	はい	はい	はい
Azure AD に参加済み	いいえ	はい	いいえ	はい	いいえ
Hybrid Azure AD 参加済み	はい	はい	はい	はい	はい

マシン **ID**	**Citrix Virtual Apps and Desktops**	**Citrix Workspace**	**Citrix StoreFront**	**Citrix Gateway** サービス	**Citrix Gateway**
ドメイン非参加	いいえ	はい	いいえ	はい	いいえ

サポートされるワークスペース認証 **ID** プロバイダー

マシン **ID**	**Azure Active Directory**	**Active Directory**	**Active Directory** とトークン	**Okta**	**SAML**	**Citrix Gateway**	アダプティブ認証
AD に参加済み	はい	はい	はい	はい	はい	はい	はい
Azure AD に参加済み	はい	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
Hybrid Azure AD 参加済み	はい	はい	はい	はい	はい	はい	はい
ドメイン非参加	はい	はい	はい	はい	はい	はい	はい

Active Directory 参加済み

August 17, 2024

認証および承認には Active Directory が使用されます。Active Directory の Kerberos インフラストラクチャにより、Delivery Controller との通信の機密性および整合性が保護されます。Kerberos について詳しくは、Microsoft 社のドキュメントを参照してください。

「システム要件」で、フォレストとドメインでサポートされる機能レベルについて確認してください。ポリシーのモデル作成を使用するには、サポートされているすべてのサーバー OS 上でドメインコントローラーが実行されている必要があります。これは、ドメインの機能レベルには影響しません。

以下の環境がサポートされています。

- ユーザーアカウントおよびコンピューターアカウントが単一 **Active Directory** フォレスト内のドメインに属している。同一フォレスト内であれば、ユーザーアカウントとコンピューターアカウントが異なるドメイン

に属していても構いません。このような環境では、すべてのドメイン機能レベルおよびフォレスト機能レベルがサポートされます。

- ユーザーアカウントが、**Controller** および仮想デスクトップのコンピューターアカウントと異なる **Active Directory** フォレストに属している。このような環境では、Controller および仮想デスクトップのコンピューターアカウントのドメインが、ユーザーアカウントのドメインを信頼している必要があります。フォレストの信頼または外部の信頼を使用できます。このような環境では、すべてのドメイン機能レベルおよびフォレスト機能レベルがサポートされます。
- **Controller** のコンピューターアカウントが、仮想デスクトップのコンピューターアカウントが属している追加の **Active Directory** フォレストと異なるフォレストに属している。このような環境では、Controller のコンピューターアカウントのドメインと、仮想デスクトップのコンピューターアカウントのすべてのドメインとの間に相互信頼関係が必要です。このような環境では、Controller または仮想デスクトップのコンピューターアカウントが属しているすべてのドメインが［Windows 2000 ネイティブ］機能レベルまたはそれ以上である必要があります。すべてのフォレスト機能レベルがサポートされます。
- 書き込み可能なドメインコントローラー。読み取り専用のドメインコントローラーはサポートされません。

必要に応じて、Virtual Delivery Agent（VDA）で登録可能な Controller を検出するときに、Active Directory の情報を使用することもできます。この機能は主に後方互換性を保持するためのもので、VDA と Controller が同じ Active Directory フォレストに属している場合のみ使用できます。この検出方法について詳しくは、「Active Directory OU ベースの検出」およびCTX118976を参照してください。

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

複数の **Active Directory** フォレスト環境での展開

複数のフォレストがある Active Directory 環境では、一方向または双方向の信頼関係が構成済みの場合に、DNS フォワーダーまたは条件付きフォワーダーによる名前参照や登録を使用できます。適切な Active Directory ユーザーがコンピューターアカウントを作成できるようにするには、オブジェクト制御の委任ウィザードを使用します。このウィザードについて詳しくは、Microsoft 社のドキュメントを参照してください。

適切な DNS フォワーダーがフォレスト間に存在する場合、DNS インフラストラクチャに DNS 逆引きゾーンは必要ありません。

VDA と Controller が別のフォレストにある場合、Active Directory と NetBIOS の名前が異なっているかどうかに関係なく、レジストリキー`SupportMultipleForest`が必要です。以下の情報を使用して、レジストリキーを VDA および Delivery Controller に追加します。

> 注意:
>
> レジストリエディターの使用を誤ると、深刻な問題が発生する可能性があり、オペレーティングシステムの再インストールが必要になる場合もあります。レジストリエディターの誤用による障害に対して、Citrix では一

> 切責任を負いません。レジストリエディターは、お客様の責任と判断の範囲でご使用ください。また、レジストリファイルのバックアップを作成してから、レジストリを編集してください。

VDA で次を構成します: `HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent\SupportMultipleForest`。

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

すべての Delivery Controller で次を構成します: `HKEY_LOCAL_MACHINE\Software\Citrix\DesktopServer\SupportMultipleForest`。

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

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

Kerberos よりも安全性が低い NTLM 認証を VDA で不要に有効化しないように、レジストリエントリが追加されました。このエントリは、`SupportMultipleForest`エントリ（後方互換性があるため引き続き使用可能）の代わりに使用できます。

VDA で次を構成します:`HKEY_LOCAL_MACHINE\Software\Policies\Citrix\VirtualDesktopAgent`。

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

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

セットアップ時に外部信頼が構成済みの場合は、レジストリキー`ListOfSIDs`が必要になります。また、Active Directory の FQDN が DNS FQDN と異なる場合、またはドメインコントローラーのドメインが Active Directory FQDN とは異なる NetBIOS 名を持っている場合も、レジストリキー`ListOfSIDs`が必要です。以下のレジストリキーを追加します。

VDA の場合、レジストリキー`HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent\ListOfSIDs`を検索します。

- 値の名前: `ListOfSIDs`
- 種類: `REG_SZ`
- データ: Controller のセキュリティ識別子（SID）。（SID は、`Get-BrokerController`コマンドレットの結果に含まれています。）

適切な外部の信頼が構成済みの場合、VDA 上で以下の変更を行います:

1. ファイルProgram Files\Citrix\Virtual Desktop Agent\brokeragent.exe.configを検索します。
2. ファイルのバックアップコピーを作成します。
3. メモ帳などのテキストエディターを使ってファイルを開きます。
4. テキストallowNtlm="false"を検索して、テキストをallowNtlm="true"に変更します。
5. ファイルを保存します。

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

次の表は、サポートされる信頼の種類を示しています。

信頼の種類	推移性	方向	このリリースでのサポート
親および子	推移的	双方向	はい
ツリールート	推移的	双方向	はい
外部	非推移的	一方向または双方向	はい
フォレスト	推移的	一方向または双方向	はい
ショートカット	推移的	一方向または双方向	はい
領域	推移的または非推移的	一方向または双方向	いいえ

複雑な Active Directory 環境での展開について詳しくは、CTX134971を参照してください。

Hybrid Azure Active Directory 参加済み

August 17, 2024

> 注:
>
> 2023 年 7 月より、Microsoft は Azure Active Directory（Azure AD）の名前を Microsoft Entra ID に変更しました。このドキュメントでは、Azure Active Directory、Azure AD、または AAD への言及はすべて、Microsoft Entra ID を意味することになります。

この記事では、「Citrix DaaS のシステム要件」セクションで概説されている要件に加えて、Citrix DaaS を使用して Hybrid Azure Active Directory（HAAD）参加済みカタログを作成するための要件について説明します。

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

> 注:
>
> Hybrid Azure AD 参加済み仮想マシンは、フェデレーション ID インフラストラクチャと管理対象 ID インフラストラクチャの両方でサポートされています。

要件

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

制限事項

- Citrix Federated Authentication Service（FAS）が使用されている場合、シングルサインオンは Azure AD ではなくオンプレミス AD に送信されます。この場合は、ユーザーのログオン時にプライマリ更新トークン（Primary Refresh Token：PRT）が生成されるように、Azure AD 証明書ベースの認証を構成することをお勧めします。これにより、セッション内の Azure AD リソースへのシングルサインオンが容易になります。この構成にしないと、PRT が生成されず、Azure AD リソースへの SSO が機能しません。フェデレーション認証サービス（FAS）を使用して、ハイブリッド参加済み VDA への Azure AD のシングルサインオン（SSO）を実現する方法については、「ハイブリッド参加済み VDA」を参照してください。
- マシンカタログの作成中または更新中にイメージの準備をスキップしないでください。イメージの準備をスキップする場合は、マスター VM が Azure AD または Hybrid Azure AD に参加していないことを確認してください。

注意事項

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

  1. `gpedit.msc`を実行します。
  2. ［コンピューターの構成］**>** ［管理用テンプレート］**>** ［**Windows** コンポーネント］**>** ［デバイスの登録］に移動します。
  3. ［ドメインに参加しているコンピューターをデバイスとして登録する］を ［無効］に設定します。

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

```
$VirtualDesktopKeyPath = 'HKLM:\Software\AzureAD\VirtualDesktop'
$WorkplaceJoinKeyPath = 'HKLM:\SOFTWARE\Policies\Microsoft\
   Windows\WorkplaceJoin'
$MaxCount = 60

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

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

    $provider = (Get-Item -Path $VirtualDesktopKeyPath).GetValue(
       "Provider", $null)
    if ($provider -eq 'Citrix')
    {

        break;
     }


    if ($provider -eq 1)
    {

        Set-ItemProperty -Path $VirtualDesktopKeyPath -Name "
           Provider" -Value "Citrix" -Force
        Set-ItemProperty -Path $WorkplaceJoinKeyPath -Name "
           autoWorkplaceJoin" -Value 1 -Force
        Start-Sleep 5
        dsregcmd /join
        break
     }

   }


  Start-Sleep 1
 }
```

次の手順

Hybrid Azure Active Directory 参加済みマシンカタログの作成について詳しくは、「Hybrid Azure Active Directory 参加済みカタログの作成」を参照してください。

インストールの準備

August 17, 2024

Citrix Virtual Apps and Desktops の展開では、まず次のコンポーネントをインストールします。このプロセスでは、アプリケーションとデスクトップをファイアウォール内のユーザーに配信する準備をします。

- 1 つまたは複数の Delivery Controller
- Citrix Director
- Citrix StoreFront
- Citrix ライセンスサーバー
- 1 つまたは複数の Citrix Virtual Delivery Agent（VDA）
- オプションのコンポーネントやテクノロジ（たとえば、ユニバーサルプリントサーバー、フェデレーション認証サービス、およびセルフサービスパスワードリセット）

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

> 注:
>
> サーバー OS とワークステーション OS で次の Microsoft の前提条件が満たされていることを確認してください:
>
> - Microsoft ボリュームシャドウコピーサービスおよび **Microsoft** ソフトウェアのシャドウコピープロバイダーサービスが実行されています。詳しくは、「ボリュームシャドウコピーサービス」を参照してください。
> - **MS-Defender** のバージョンは、4.18.2105.5 以降である必要があります。詳しくは、「Microsoft Defender ウイルス対策セキュリティインテリジェンスと製品更新プログラム」を参照してください。

展開に Windows Server ワークロードが含まれている場合は、Microsoft RDS ライセンスサーバーを構成します。

製品 ISO に含まれる全製品インストーラーを使用すると、多くのコンポーネントとテクノロジを展開できます。VDA は、スタンドアロン VDA インストーラーを使用してインストールできます。スタンドアロン VDA インストーラーは Citrix のダウンロードサイトから入手できます。すべてのインストーラーで、グラフィカルおよびコマンドラインインターフェイスが提供されます。「インストーラー」を参照してください。

製品 ISO には、Active Directory のマシンの VDA をインストール、アップグレード、または削除するサンプルスクリプトも収録されています。また、これらのスクリプトを使って、Machine Creation Services（MCS）および Citrix Provisioning（旧称 Provisioning Services）のイメージを管理することもできます。詳しくは、「スクリプトを使用した VDA のインストール」を参照してください。

インストール前に確認する情報

- Technical overview：製品およびコンポーネントについて理解を深める場合。
- セキュリティ：展開環境について計画する場合。
- 既知の問題：このバージョンで起きる可能性がある問題。
- データベース：システムデータベースおよびこれらの設定方法について理解を深めてください。Controller のインストール時に、サイトデータベース用に SQL Server Express をインストールできます。コアコンポーネントをインストールした後のサイト作成時に、データベース情報のほとんどを設定します。
- リモート PC アクセス：ユーザーがオフィスの物理マシンにリモートでアクセスできる環境を展開している場合。
- 接続とリソース：ハイパーバイザーまたはその他のサービスを使用してアプリケーションやデスクトップの VM マシンをホストまたはプロビジョニングしている場合。（コアコンポーネントをインストールした後の）サイト作成時に、最初の接続を構成することができます。仮想化環境はそれより前に設定できます。
- Microsoft System Center Configuration Manager：ConfigMgr を使用してアプリケーションおよびデスクトップへのアクセスを管理しているか、リモート PC アクセスとともに Wake on LAN 機能を使用している場合。
- パブリッククラウドホスト接続：ハイブリッド権利ライセンスがあれば、パブリッククラウドへのホスト接続を作成できます。ハイブリッド権利ライセンスに関連する情報については、「ハイブリッド権利の更新」を参照してください。パブリッククラウドの資格情報に関する情報と今回の変更が行われた理由については、CTX270373を参照してください。

コンポーネントのインストール先

サポートされるプラットフォーム、オペレーティングシステム、バージョンについては、「システム要件」を参照してください。記載されているものを除いて、コンポーネントの必須条件は自動的にインストールされます。サポートされるプラットフォームと前提条件については、Citrix StoreFront および Citrix ライセンスサーバーのドキュメントを参照してください。

コアコンポーネントは、同じサーバー上にインストールしたり別のサーバー上にインストールしたりできます。

- 1 つのサーバー上にすべてのコアコンポーネントをインストールすれば、評価展開、テスト展開、または小規模実稼働展開に使用できます。
- 将来の拡張に対応するには、異なるサーバーにコンポーネントをインストールすることを検討してください。たとえば、Controller をインストールしたサーバーとは別のマシンに Studio をインストールすると、サイトをリモートで管理できます。
- 大部分の実稼働展開では、コアコンポーネントを別々のサーバーにインストールすることをお勧めします。

  他のサーバーに他のコンポーネントをインストールする前に、Citrix ライセンスサーバーとライセンスをインストールしてください。
- サポートされているコンポーネントをサーバーコア OS（Delivery Controller など）にインストールするにはコマンドラインを使用する必要があります。このタイプの OS ではグラフィカルユーザーインターフェイス

を利用できないため、まず Studio などのツールを別の場所にインストールし、それらにコントローラーサーバーを参照させます。

Delivery Controller とマルチセッション OS 対応 VDA を同一サーバー上にインストールできます。インストーラーを起動して目的の Delivery Controller（およびマシンにインストールするその他のコンポーネント）を選択します。次に、もう一度インストーラーを起動してマルチセッション OS の **Virtual Delivery Agent** を選択します。

各オペレーティングシステムに最新の更新を適用しておく必要があります。

すべてのマシンのシステムクロックを同期しておく必要があります。この同期は、Kerberos でマシン間の通信を保護するために必要です。

XenServer では、仮想マシンの電源状態が登録されているように見える場合でも、不明として表示されることがあります。この問題を解決するには、レジストリキーの`HostTime`値を編集して、ホストとの時間同期を無効にします:

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

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

> ヒント:
>
> デフォルトの値は`HostTime="UTC"`です。この値を、`Local`など、UTC 以外の値に変更します。この変更により、ホストとの時間同期が効果的に無効になります。

シングルセッション Windows 10 マシンでの最適化ガイダンスは、CTX216252を参照してください。

コンポーネントのインストールが不適切な場所:

- Active Directory ドメインコントローラーには一切コンポーネントをインストールしないでください。
- SQL Server クラスター化インストール、SQL Server ミラー化インストール、または Hyper-V を実行しているサーバーにおけるノード上への Controller のインストールはサポートされていません。

この製品バージョンでサポートされていない Windows OS に VDA をインストールまたはアップグレードしようとすると、メッセージが表示され、オプションについて記述された記事が示されます。

Active Directory の権限と要件

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

スタンドアロン VDA インストーラーを使用するには、管理者権限を持っているか、［管理者として実行］を使用する必要があります。

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

- サポートされる Active Directory の機能レベルの一覧は「システム要件」に記載されています。「Active Directory 参加済み」には詳細情報が記載されています。

- Active Directory ドメインサービスを実行するドメインコントローラーが少なくとも 1 つ必要です。
- ドメインコントローラーには Citrix Virtual Apps and Desktops をインストールしないでください。
- Studio で組織単位名を指定するときは、スラッシュ（/）を使用しないでください。

Citrix ライセンスサーバーのインストールに使用した Windows ユーザーアカウントは、自動的に、すべての管理タスクの実行権限を持つ委任管理者として設定されます。

さらに、以下の情報を参照してください:

- セキュリティに関する推奨事項
- 委任管理
- Active Directory の構成に関する Microsoft 社のドキュメント

インストールのガイダンス、考慮事項、およびベストプラクティス

任意のコンポーネントのインストール時

- Delivery Controller、Studio、ライセンスサーバー、または Director を全製品メディアからインストールまたはアップグレードする場合、マシンの過去の Windows インストールから再起動が保留されていることが Citrix インストーラーで検知されると、インストーラーは終了/リターンのコード 9 で停止します。マシンを再起動するように求められます。

  これは、Citrix による強制再起動ではありません。この状況は、以前マシンにインストールされた他のコンポーネントが原因で発生します。この状況が発生した場合、マシンを再起動してから、Citrix インストーラーを再起動します。

  コマンドラインインターフェイスを使用する場合、コマンドに`/no_pending_reboot_check`オプションを含めて保留中の再起動のチェックを阻止できます。

- 通常、コンポーネントの前提条件が存在していない場合は、インストーラーによってインストールされます。前提条件によっては、マシンの再起動が必要なものがあります。
- インストールの前、最中、および後に作成するオブジェクトには、重複しない名前を指定してください。こうしたオブジェクトには、ネットワーク、グループ、カタログ、リソースなどがあります。
- 正しくインストールできないコンポーネントがあった場合は、インストールが停止してエラーメッセージが表示されます。この時点でインストール済みのコンポーネントは保持されるため、再インストールする必要はありません。
- コンポーネントをインストール（またはアップグレード）すると、Citrix Analytics が自動的に収集されます。デフォルトでは、インストールの完了時に、そのデータが Citrix へ自動的にアップロードされます。また、コンポーネントをインストールすると、自動的に Citrix カスタマーエクスペリエンス向上プログラム（CEIP）に登録され、匿名データがアップロードされます。

インストール中に、メンテナンスやトラブルシューティングのために診断情報を収集する別の Citrix プログラムに参加することもできます。これらのプログラムについて詳しくは、「Citrix Insight Services」を参照してください。

- Studio をインストール（またはアップグレード）すると、Google Analytics が自動的に収集され（後でアップロードされ）ます。Studio をインストールした後、レジストリキー`HKLM\Software\Citrix\DesktopStudio\GAEnabled`でこの設定を変更できます。値 **1** で収集とアップロードを有効にし、**0** で収集とアップロードを無効にします。
- VDA のインストールが失敗すると、MSI アナライザーはエラーのある MSI ログを解析し、正確なエラーコードを表示します。このアナライザーは、既知の問題であった場合は、CTX 記事を示します。アナライザーはまた、故障エラーコードに関する匿名化データも収集します。このデータは、CEIP によって収集された他のデータに含まれます。CEIP への登録を終了すると、収集された MSI アナライザーのデータは Citrix に送信されなくなります。

VDA インストール時

- Windows 向け Citrix Workspace アプリを使用可能ですが、デフォルトでは VDA をインストールしてもこのアプリはインストールされません。Windows 向け Citrix Workspace アプリおよび他の Citrix Workspace アプリは、管理者またはユーザーが Citrix Web サイトからダウンロードし、インストールできます。また、StoreFront サーバーでこれらの Citrix Workspace アプリを公開することもできます。詳しくは、StoreFront のドキュメントを参照してください。
- Microsoft の印刷スプーラーサービスを有効にする必要があります。そのサービスが無効になっている場合、VDA を正常にインストールすることはできません。
- サポートされているほとんどの Windows のエディションには、Microsoft Media Foundation が既にインストールされています。マシンにメディアファンデーションがインストールされていない場合（N エディションなど）は、複数のマルチメディア機能がインストールされておらず、動作しません。
  - Windows Media リダイレクト
  - HTML5 ビデオリダイレクト
  - HDX RealTime Web カメラリダイレクト

  その制限を認識するか、VDA のインストールを中止して、Media Foundation をインストールした後に再開してください。グラフィカルユーザーインターフェイス上に、この選択がメッセージとして表示されます。制限を認識するには、コマンドラインで`/no_mediafoundation_ack`オプションを使用してください。
- VDA をインストールすると、**Direct Access Users**（直接アクセスユーザー）という名前の新しいローカルユーザーグループが自動的に作成されます。シングルセッション OS 対応 VDA では、このグループは RDP 接続のみに適用されます。マルチセッション OS 対応 VDA では、このグループは ICA 接続と RDP 接続に適用されます。
- VDA には、通信を行う Controller の有効なアドレスが保持されている必要があります。保持されていない場合は、セッションを確立することができません。Controller のアドレスは、VDA のインストール時に指定す

ることも、後で指定することもできます。ただし、必ず指定しなければならないことを覚えておいてください。詳しくは、「VDA 登録」を参照してください。

VDA サポートツール

各 VDA インストーラーには、VDA のパフォーマンス（全体的な正常性や接続品質など）をチェックするための Citrix ツールを含む、サポート MSI が含まれています。こうした MSI のインストールを行うかどうかは、VDA インストーラーのグラフィカルユーザーインターフェイスの ［追加コンポーネント］ページで指定します。インストールを無効にするには、コマンドラインから、`/exclude "Citrix Supportability Tools"`オプションを実行します。

デフォルトでは、サポート MSI は`c:\Program Files (x86)\Citrix\Supportability Tools\`にインストールされています。この場所は、VDA インストーラーのグラフィカルユーザーインターフェイスの ［コンポーネント］ページ、または`/installdir`コマンドラインオプションで変更できます。この場所を変更すると、サポートツールのみでなく、インストールされているすべての VDA コンポーネントの場所が変更されることに注意してください。

サポート MSI 内の現在のツール：

- Citrix Health Assistant：詳しくは、CTX207624を参照してください。
- VDA Cleanup Utility：詳しくは、CTX209255を参照してください。

VDA のインストール時にこのツールをインストールしない場合は、CTX の記事に、現在のダウンロードパッケージへのリンクが含まれています。

VDA インストール時およびその後の再起動

VDA のインストールプロセスの最後にマシンを再起動する必要があります。デフォルトでは、再起動は自動で行われます。

VDA をバージョン 7.17（またはそれ以降のサポートされているバージョン）にアップグレードするときは、アップグレード中に再起動が行われます。これを防ぐことはできません。

VDA インストール中の再起動の回数を最小限に抑えるには：

- VDA のインストールが開始される前に.NET Framework バージョンがインストールされていることを確認してください。
- Windows マルチセッション OS マシンでは、RDS の役割サービスをインストールして有効にしてから VDA をインストールしてください。

VDA インストール前にこれらの前提条件をインストールしない場合：

- グラフィカルインターフェイスを使用した場合、またはコマンドラインインターフェイスを`/noreboot`オプションなしで使用した場合、前提条件のインストール後にマシンが自動で再起動します。

- コマンドラインインターフェイスで/`noreboot`オプションを使用した場合、手動で再起動を開始する必要があります。

VDA バージョンをアップグレードする場合、アップグレード中に再起動が行われます。これを防ぐことはできません。

インストールまたはアップグレードの失敗時の復元

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

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

マルチセッション VDA のインストールまたはアップグレードが失敗し、「失敗時の復元」機能が有効になっている場合、マシンはインストールまたはアップグレードの開始前に実行されたバックアップに戻ります。

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

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

デフォルトでは、この機能は無効になっています。

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

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

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

- VDA インストーラーのグラフィカルインターフェイスを使用する場合（自動開始または`XenDesktopVDASetup.exe`コマンドを restore オプションや quiet オプションなしで使用する場合など）は、［概要］ページの ［更新に失敗した場合に自動復元を有効にする］チェックボックスをオンにします。

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

- コマンドラインで、/enablerestoreまたは/enablerestorecleanupオプションのどちらかを指定して VDA インストーラーを実行します。
  - /enablerestorecleanupオプションを指定した場合、インストールまたはアップグレードが正常に完了すると、復元ポイントまたはサーバーバックアップは自動的に削除されます。
  - /enablerestoreオプションを指定した場合、インストールまたはアップグレードが正常に完了すると、復元ポイントは使用されませんが、保持されます。

インストーラー

全製品インストーラー

ISO で提供される全製品インストーラーを使用すると、以下のことができます:

- コアコンポーネント（Delivery Controller、Studio、Director、ライセンスサーバー）のインストール、アップグレード、削除
- StoreFront のインストールまたはアップグレード
- シングルセッション OS またはマルチセッション OS 対応 Windows VDA のインストールまたはアップグレード
- プリントサーバーへのユニバーサルプリントサーバーUpsServerコンポーネントのインストール
- フェデレーション認証サービスのインストール
- Session Recordingのインストール
- Workspace Environment Managementをインストールします。

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

（Web サイト開発などで）1 人のユーザー用にマルチセッション OS からデスクトップを配信するには、全製品インストーラーのコマンドラインインターフェイスを使用します。詳しくは、「サーバー VDI」を参照してください。

スタンドアロン **VDA** インストーラー

スタンドアロン VDA インストーラーは Citrix のダウンロードページから入手できます。（製品のインストールメディアでは入手できません。）スタンドアロン VDA インストーラーは、全製品 ISO よりはるかにサイズが小さいです。これらのインストーラーを使用すると、以下のような展開環境に簡単に対応することができます:

- ステージングするかまたはローカルにコピーした電子ソフトウェア配信（ESD）パッケージを使用する環境
- 物理マシンのある環境
- リモートオフィスのある環境

デフォルトでは、自己抽出型のスタンドアロン VDA 内のファイルは **Temp** フォルダーに抽出されます。**Temp** フォルダーに抽出される場合は、全製品インストーラーを使用する場合よりも、マシンに多くのディスクスペースが必要です。ただし、インストールの完了後、**Temp** フォルダーに抽出されたファイルは自動的に削除されます。または、絶対パスとともに/`extract`コマンドを使用できます。

3 つのスタンドアロン VDA インストーラーを、ダウンロードで入手できます。

VDAServerSetup.exe:

マルチセッション OS 対応 VDA をインストールします。全製品インストーラーで利用できるマルチセッション OS 対応 VDA オプションをすべてサポートしています。

VDAWorkstationSetup.exe:

シングルセッション OS 対応 VDA をインストールします。全製品インストーラーで利用できるシングルセッション OS 対応 VDA オプションをすべてサポートしています。

VDAWorkstationCoreSetup.exe:

リモート PC アクセス展開またはコア VDI インストールに最適化されたシングルセッション OS 対応 VDA をインストールします。リモート PC アクセスマシンでは物理マシンを使用します。コア VDI インストールとは、イメージとして使用されない仮想マシンのことを指します。コア VDI インストールでは、こうした展開環境への VDA 接続に必要なコアサービスのみがインストールされます。このため、全製品インストーラーまたは`VDAWorkstationSetup.exe`インストーラーで有効であるオプションのサブセットだけがサポートされます。

このインストーラーは、次のものに使用されるコンポーネントをインストールしないか、含みません:

- App-V。
- Profile Management。インストールから Citrix Profile Management を除外すると、Citrix Director の表示に影響が生じます。詳しくは、「VDA のインストール」を参照してください。
- Machine Identity Service。
- Citrix Supportability Tools
- Citrix Files for Windows
- Citrix Files for Outlook

`VDAWorkstationCoreSetup.exe`インストーラーには Windows 向け Citrix Workspace アプリは含まれておらず、インストールされません。

`VDAWorkstationCoreSetup.exe`を使用することは、全製品または`VDAWorkstationSetup`インストーラーを使用することと同等であり、シングルセッション OS VDA をインストールして、次のいずれかを実行します:

- グラフィカルインターフェイス:［環境］ページで［リモート PC アクセス］オプションを選択します。

- コマンドラインインターフェイス：/remotepcオプションを指定します。
- コマンドラインインターフェイス：/components vdaと/excludeオプションを指定して、有効な追加コンポーネントの名前をすべて一覧表示します。

全製品インストーラーを実行すれば、省略したコンポーネントおよび機能を後からインストールできます。この操作では、不足しているコンポーネントをすべてインストールできます。

VDAWorkstationCoreSetup.exeインストーラーは自動的に Web ブラウザーコンテンツリダイレクト MSI をインストールします。この自動インストールは、VDA リリース 2003 以降でサポートされるリリースで使用できます。

Citrix インストールリターンコード

インストールログには、Microsoft の値ではなく、Citrix のリターンコードとしてコンポーネントをインストールした結果が含まれています。

- 0 = Success（成功）
- 1 = Failed（失敗）
- 2 = PartialSuccess（一部成功）
- 3 = PartialSuccessAndRebootNeeded（一部成功、再起動が必要）
- 4 = FailureAndRebootNeeded（失敗、再起動が必要）
- 5 = UserCanceled（ユーザーキャンセル）
- 6 = BadCommandLineArgument（不正なコマンドライン引数）
- 7 = NewerVersionFound（新バージョン検出）
- 8 = SuccessRebootNeeded（成功、再起動が必要）
- 9 = FileLockReboot（ファイルロック、再起動）
- 10 = Aborted（中止）
- 11 = FailedMedia（失敗したメディア）
- 12 = FailedLicense（失敗したライセンス）
- 13 = FailedPrecheck（事前チェックに失敗しました）
- 14 = AbortedPendingRebootCheck（中止、再起動チェックの保留）
- -1 = Exit（終了）

たとえば、Microsoft System Center Configuration Manager などのツールを使用する場合、インストールログにリターンコード 3 が含まれていると、スクリプトによる VDA インストールが失敗したように見えることがあります。これは、VDA インストーラーが人を介して開始する必要がある再起動を待っているとき（たとえば、サーバーに RDS の役割の前提条件をインストールした後）に発生することがあります。VDA のインストールは、すべての前提条件と選択したコンポーネントがインストールされ、インストール後にマシンが再起動された後でのみ、完了したとみなされます。

代わりの方法として、インストールコマンドを CMD スクリプト（Microsoft の終了コードを返します）内に記述するか、Configuration Manager パッケージの成功コードを変更してください。

Windows Server ワークロード用の **Microsoft RDS** ライセンスサーバーの構成

この製品は、Windows 2016 などの Windows Server ワークロードを配信するとき、Windows Server リモートセッション機能にアクセスします。これには通常、リモートデスクトップサービスクライアントアクセスライセンス（RDS CAL）が必要です。VDA は、RDS CAL の要求のために RDS ライセンスサーバーに接続できる必要があります。ライセンスサーバーをインストールしてアクティブ化してください。詳しくは、Microsoft 社のドキュメント「リモートデスクトップサービスライセンスサーバーをアクティブ化する」を参照してください。概念実証環境では、Microsoft から提供される猶予期間を利用できます。

この方法により、このサービスでライセンスサーバーの設定を適用できます。イメージの RDS コンソールでは、ライセンスサーバーおよび接続ユーザー数モードを構成できます。また、Microsoft のグループポリシー設定を使用して、ライセンスサーバーを構成することもできます。詳しくは、Microsoft 社のドキュメント「クライアントアクセスライセンス（CAL）を使用して RDS 展開をライセンスする」を参照してください。

グループポリシー設定を使用して RDS ライセンスサーバーを構成するには:

1. 使用可能なマシンに、リモートデスクトップサービスのライセンスサーバーをインストールします。マシンは常に使用可能である必要があります。また、Citrix 製品のワークロードが常にこのライセンスサーバーに接続できる必要があります。
2. Microsoft のグループポリシーを使用して、ライセンスサーバーアドレスと単一ユーザーライセンスモードを指定します。　詳細については、Microsoft 社のドキュメント「リモートデスクトップサービスライセンスサーバーをアクティブ化する」を参照してください。

Windows 10 ワークロードには、適切な Windows 10 ライセンスのアクティブ化が必要です。Microsoft のドキュメントに従って、Windows 10 ワークロードをアクティブ化することをお勧めします。

追加情報

特定のホストタイプのリソースの場所を設定する場合:

- AWS クラウド環境
- XenServer 仮想化環境
- Google Cloud 環境
- Microsoft Azure Resource Manager クラウド環境
- Microsoft System Center Configuration Manager 環境
- Microsoft System Center Virtual Machine Manager 仮想化環境
- Nutanix 仮想化環境
- Nutanix クラウドおよびパートナーソリューション
- VMware 仮想化環境
- VMware クラウドおよびパートナーソリューション

AWS クラウド環境

August 17, 2024

この記事では、Citrix Virtual Apps and Desktops で使用できるリソースの場所としての Amazon Web Services アカウントを設定する方法について説明します。このリソースの場所には基本的なコンポーネントセットのみが含まれており、概念実証など、リソースを複数のアベイラビリティゾーンに展開する必要のない展開に最適です。本記事のタスクの完了後、VDA のインストール、マシンのプロビジョニング、マシンカタログの作成、デリバリーグループの作成を行えます。

この記事のタスクを完了すると、リソースの場所に次のコンポーネントが追加されます:

- 単一アベイラビリティゾーン内にパブリックサブネットとプライベートサブネットを持つ仮想プライベートクラウド（VPC）。
- VPC のプライベートサブネットに配置され、Active Directory ドメインコントローラーと DNS サーバーの両方として実行されるインスタンス。
- VPC のパブリックサブネットで踏み台ホストとして機能するインスタンス。このインスタンスは、管理目的でプライベートサブネット内のインスタンスへの RDP 接続を開始するために使用されます。リソースの場所の設定が完了したら、このインスタンスをシャットダウンし、アクセスできないようにしてもかまいません。プライベートサブネット内の他のインスタンス（VDA インスタンスなど）を管理する必要性が生じた場合に、このインスタンスを再起動できます。

タスクの概要

パブリックサブネットとプライベートサブネットを持つ仮想プライベートクラウド（**VPC**）の設定。このタスクを完了すると、パブリックサブネット内のエラスティック IP アドレスを持つ NAT ゲートウェイが AWS によって展開されます。この結果、プライベートサブネット内のインスタンスからインターネットにアクセスできるようになります。パブリックサブネット内のインスタンスが受信パブリックトラフィックにアクセスできるようになりますが、プライベートサブネット内のインスタンスはアクセスできません。

セキュリティグループの構成。セキュリティグループは、VPC 内のインスタンスのトラフィックを制御する仮想ファイアウォールとして機能します。セキュリティグループにルールを追加することで、パブリックサブネット内のインスタンスがプライベートサブネット内のインスタンスと通信できるようになります。また、これらのセキュリティグループを仮想プライベートクラウド内の各インスタンスに関連付けることもできます。

DHCP オプションセットの作成。Amazon VPC ではデフォルトで DHCP サービスと DNS サービスが提供されるため、Active Directory ドメインコントローラーの DNS の構成方法が変わります。Amazon の DHCP を無効にすることはできません。また Amazon の DNS は、Active Directory の名前解決には使用できず、パブリック DNS 解決にのみ使用できます。DHCP 経由でインスタンスに渡すドメインサーバーとネームサーバーを指定するため、DHCP オプションセットを作成します。このセットにより Active Directory ドメインサフィックスを割り当てて、VPC 内のすべてのインスタンスに DNS サーバーを指定します。ドメインへのインスタンスの参加時にホスト（A）レコード

と逆引き参照（PTR）レコードが自動的に登録されるようにするため、プライベートサブネットに追加するインスタンスごとに、ネットワークアダプタープロパティを構成します。

VPC に踏み台ホストとドメインコントローラーを追加。踏み台ホストにより、プライベートサブネット内のインスタンスにログオンし、ドメインの設定、ドメインへのインスタンスの追加を行うことができます。

タスク **1**：**VPC** を設定する

1. AWS マネジメントコンソールで ［**VPC**］を選択します。
2. VPC ダッシュボードで、［**Create VPC**］を選択します。
3. ［**VPC and more**］を選択します。
4. ［NAT gateways ($)］で ［**In 1 AZ**］または ［**1 per AZ**］を選択します。
5. ［DNS］オプションで ［**Enable DNS hostnames**］が選択されたままにします。
6. ［**Create VPC**］を選択します。AWS により、パブリックサブネット、プライベートサブネット、インターネットゲートウェイ、ルートテーブル、デフォルトのセキュリティグループが作成されます。

タスク **2**：セキュリティグループを構成する

このタスクでは、VPC 用に次のセキュリティグループを作成して構成します：

- パブリックサブネット内のインスタンスを関連付けるパブリックセキュリティグループ。
- プライベートサブネット内のインスタンスを関連付けるプライベートセキュリティグループ。

セキュリティグループを作成するには：

1. VPC ダッシュボードで、［**Security Groups**］を選択します。
2. パブリックセキュリティグループのセキュリティグループを作成します。［**Create Security Group**］を選択し、グループの名前タグと説明を入力します。［VPC］では、先ほど作成した VPC を選択します。［**Yes, Create**］を選択します。

パブリックセキュリティグループを構成する

1. セキュリティグループの一覧で、先ほど作成したパブリックセキュリティグループを選択します。
2. ［**Inbound Rules**］タブを選択し、［**Edit**］を選択して次の規則を作成します：

種類	接続元
すべてのトラフィック	プライベートセキュリティグループを選択します。
すべてのトラフィック	パブリックセキュリティグループを選択します。
ICMP	0.0.0.0/0

種類	接続元
22（SSH）	0.0.0.0/0
80（HTTP）	0.0.0.0/0
443（HTTPS）	0.0.0.0/0
1494（ICA/HDX）	0.0.0.0/0
2598（セッション画面の保持）	0.0.0.0/0
3389（RDP）	0.0.0.0/0

3. 完了したら、[**Save**]を選択します。
4. [**Outbound Rules**]タブを選択し、[**Edit**]を選択して次のルールを作成します:

種類	接続先
すべてのトラフィック	プライベートセキュリティグループを選択します。
すべてのトラフィック	0.0.0.0/0
ICMP	0.0.0.0/0

5. 完了したら、[**Save**]を選択します。

プライベートセキュリティグループを構成する

1. セキュリティグループの一覧で、先ほど作成したプライベートセキュリティグループを選択します。
2. パブリックセキュリティグループからのトラフィックを設定していない場合は、TCP ポートを設定する必要があります。[**Inbound Rules**]タブを選択し、[**Edit**]を選択して次のルールを作成します:

種類	接続元
すべてのトラフィック	プライベートセキュリティグループを選択します。
すべてのトラフィック	パブリックセキュリティグループを選択します。
ICMP	パブリックセキュリティグループを選択します。
TCP 53（DNS）	パブリックセキュリティグループを選択します。
UDP 53（DNS）	パブリックセキュリティグループを選択します。
80（HTTP）	パブリックセキュリティグループを選択します。

種類	接続元
TCP 135	パブリックセキュリティグループを選択します。
TCP 389	パブリックセキュリティグループを選択します。
UDP 389	パブリックセキュリティグループを選択します。
443（HTTPS）	パブリックセキュリティグループを選択します。
TCP 1494（ICA/HDX）	パブリックセキュリティグループを選択します。
TCP 2598（セッション画面の保持）	パブリックセキュリティグループを選択します。
3389（RDP）	パブリックセキュリティグループを選択します。
TCP 49152～65535	パブリックセキュリティグループを選択します。

3. 完了したら、［**Save**］を選択します。
4. ［**Outbound Rules**］タブを選択し、［**Edit**］を選択して次のルールを作成します：

種類	接続先
すべてのトラフィック	プライベートセキュリティグループを選択します。
すべてのトラフィック	0.0.0.0/0
ICMP	0.0.0.0/0
UDP 53（DNS）	0.0.0.0/0

5. 完了したら、［**Save**］を選択します。

タスク **3**：インスタンスを起動する

次の手順に従い、EC2 インスタンスを 2 つ作成し、Amazon で生成されたデフォルトの管理者パスワードの暗号化を解除します：

1. AWS マネジメントコンソールで ［**EC2**］を選択します。
2. EC2 ダッシュボードで ［**Launch Instance**］を選択します。
3. Windows Server マシンのイメージとインスタンスの種類を選択します。
4. ［**Configure Instance Details**］ページで、インスタンスの名前を入力し、先ほど設定した VPC を選択します。
5. ［**Subnet**］で、各インスタンスに対して次の選択を行います：

- Bastion host：パブリックサブネットを選択します
- Domain Controller:：プライベートサブネットを選択します

6. [**Auto-assign Public IP address**］で、各インスタンスに対して次の選択を行います：

   - Bastion host：[**Enable**］を選択します。
   - Domain Controller：[**Use default setting**］または ［**Disable**］を選択します。

7. [**Network Interfaces**］で、ドメインコントローラーのプライベートサブネットの IP 範囲に含まれるプライマリ IP アドレスを入力します。
8. 必要に応じて、[**Add Storage**］ページでディスクサイズを変更します。
9. [**Tag Instance**］ページで、各インスタンスにわかりやすい名前を付けます。
10. [**Configure Security Groups**］ページで、[**Select an existing security group**］を選択し、インスタンスごとに次の選択を行います：

    - Bastion host：パブリックセキュリティグループを選択します。
    - ドメインコントローラー：プライベートセキュリティグループを選択します。

11. 選択した内容を確認し、[**Launch**］を選択します。
12. 新しいキーペアを作成するか、既存のキーペアを選択します。新しいキーペアを作成する場合は、秘密キー（.pem）ファイルをダウンロードして安全な場所に保管します。インスタンスのデフォルトの管理者パスワードを取得するときに、この秘密キーを提供する必要があります。
13. [**Launch Instances**］を選択してから ［**View Instances**］を選択し、インスタンスの一覧を表示します。新しく起動したインスタンスがすべての状態チェックに合格するまで待ってから、インスタンスにアクセスします。
14. 各インスタンスのデフォルトの管理者パスワードを取得します：

    a) インスタンスの一覧で目的のインスタンスを選択し、[**Connect**］を選択します。
    b) [**RDP client**］タブに移動し、［**Get Password**］を選択し、プロンプトが表示されたら秘密キー（`.pem`）ファイルをアップロードします。
    c) 人間が判読できるパスワードを取得するには、[**Decrypt Password**］を選択します。AWS にデフォルトのパスワードが表示されます。

15. 2 つのインスタンスを作成し終わるまで、手順 2 以降のすべてのステップを繰り返します：

    - パブリックサブネットに含まれる 1 つの踏み台ホストインスタンス
    - ドメインコントローラーとして使用する、プライベートサブネット内の 1 つのインスタンス。

タスク **4**：**DHCP** オプションセットを作成する

1. VPC ダッシュボードで ［**DHCP Options Sets**］を選択します。

2. 次の情報を入力します:

   - Name tag: オプションセットのフレンドリ名を入力します。
   - Domain name: ドメインコントローラーインスタンスの構成に使用する完全修飾ドメイン名を入力します。
   - Domain name servers: ドメインコントローラーインスタンスに割り当てたプライベート IP アドレスと、「**AmazonProvidedDNS**」という文字列をカンマで区切って入力します。
   - NTP servers: このフィールドは空白のままにします。
   - NetBIOS name servers: ドメインコントローラーインスタンスのプライベート IP アドレスを入力します。
   - NetBIOS node type:「**2**」と入力します。

3. [**Yes, Create**] を選択します。

4. 新しく作成したセットを VPC に関連付けます:

   a) VPC ダッシュボードで [**Your VPCs**] を選択し、先ほど設定した VPC を選択します。
   b) [**Actions**] **>** [**Edit DHCP Options Set**] の順に選択します。
   c) プロンプトが表示されたら、新しく作成したセットを選択して [**Save**] を選択します。

タスク **5**: インスタンスを構成する

1. RDP クライアントを使用して、要塞ホストインスタンスのパブリック IP アドレスに接続します。プロンプトが表示されたら、管理者アカウントの資格情報を入力します。

2. 踏み台ホストインスタンスでリモートデスクトップ接続を起動し、構成するインスタンスのプライベート IP アドレスに接続します。プロンプトが表示されたら、インスタンスの管理者アカウントの資格情報を入力します。

3. プライベートサブネット内のすべてのインスタンスに対して、DNS 設定を構成します:

   a) [スタート] **>** [コントロールパネル] **>** [ネットワークとインターネット] **>** [ネットワークと共有センター] **>** [アダプターの設定の変更] の順に選択します。表示されたネットワーク接続をダブルクリックします。

   b) [プロパティ] **>** [インターネットプロトコルバージョン **4** (**TCP/IPv4**)] **>** [プロパティ] を選択します。

   c) [詳細設定] **>** [**DNS**] を選択します。次の設定を有効にして [**OK**] を選択します:

      - この接続のアドレスを DNS に登録する
      - この接続の DNS サフィックスを DNS 登録に使う

4. ドメインコントローラーを構成する:

   a) サーバーマネージャーを使用して、すべてのデフォルト機能を持つ Active Directory ドメインサービスの役割を追加します。

b) インスタンスをドメインコントローラーに昇格させます。昇格時には、DNS を有効にして、DHCP オプションセットの作成時に指定したドメイン名を使用します。メッセージに従ってインスタンスを再起動します。

次の手順

- コアコンポーネントのインストール
- VDA のインストール
- サイトの作成
- AWS での接続の作成と管理については、「AWS への接続」を参照してください。

追加情報

- 接続とリソースの作成と管理
- マシンカタログの作成

XenServer 仮想化環境

August 17, 2024

XenServer は運用管理を簡素化し、集中的なワークロードに対して高品位なユーザーエクスペリエンスを保証します。

XenServer をセットアップするには、「インストールの準備」を参照してください。

次の手順

- コアコンポーネントのインストール
- VDA のインストール
- サイトの作成
- XenServer での接続の作成と管理については、「XenServer への接続」を参照してください

追加情報

- 接続とリソースの作成と管理
- マシンカタログの作成

Google Cloud 環境

August 17, 2024

Citrix Virtual Apps and Desktops を使用すると、Google Cloud でマシンをプロビジョニングおよび管理できます。

要件

- Citrix Cloud アカウント。この記事で説明する機能は、Citrix Cloud でのみ使用できます。
- Google Cloud プロジェクト。このプロジェクトには、マシンカタログに関連付けられたすべてのコンピューティングリソースが格納されます。既存のプロジェクトでも新しいプロジェクトでもかまいません。
- Google Cloud プロジェクトで 4 つの API を有効にします。詳しくは、「Google Cloud API の有効化」を参照してください。
- Google Cloud サービスアカウント。サービスアカウントは、プロジェクトへのアクセスを可能にするために、Google Cloud に対して認証されます。詳しくは、「サービスアカウントの構成と更新」を参照してください。
- Google プライベートアクセスの有効化。詳しくは、「プライベート Google アクセスの有効化」を参照してください。

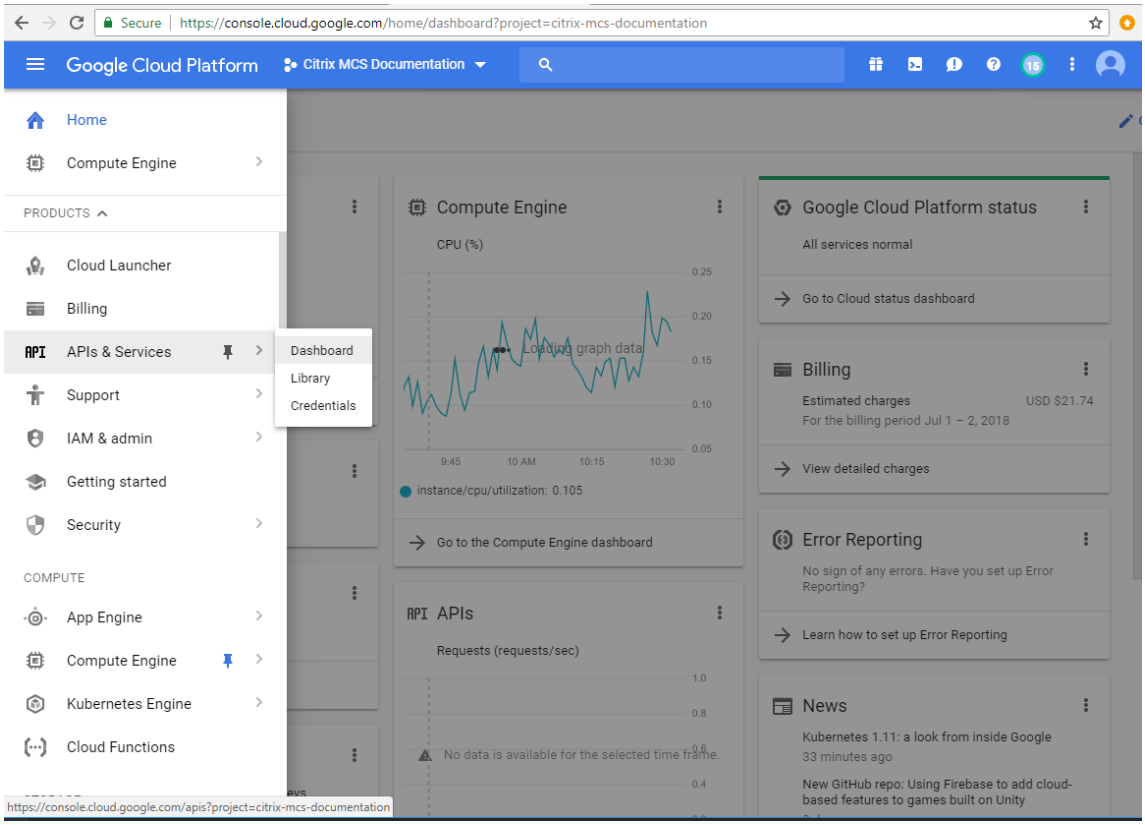
Google Cloud API の有効化

Web Studio で Google Cloud 機能を使用するには、Google Cloud プロジェクトで次の API を有効にします:

- Compute Engine API
- Cloud Resource Manager API
- Identity and Access Management（IAM）API
- Cloud Build API
- Cloud Key Management Service（KMS）

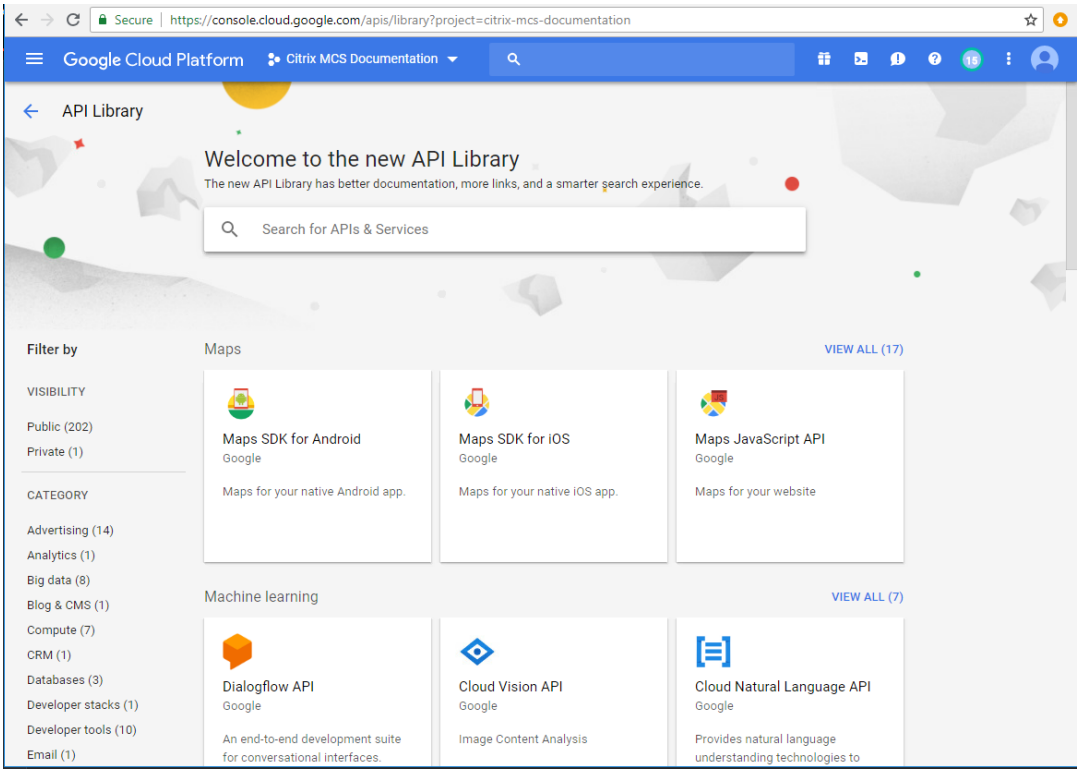
Google Cloud コンソールから、次の手順を実行します:

1. 左上隅のメニューで ［**API** とサービス］**>**［ダッシュボード］を選択します。



2. ［ダッシュボード］画面で、Compute Engine API が有効になっていることを確認します。有効になっていない
   場合、次の手順を実行します：

   a) ［**API** とサービス］**>** ［ライブラリ］の順に選択します。



b) 検索ボックスに「*Compute Engine*」と入力します。

c) 検索結果から、[**Compute Engine API**] を選択します。

d) [**Compute Engine API**] ページで、[**Enable**] を選択します。

3. Cloud Resource Manager API を有効にします。

a) [**API** とサービス] **>** [ライブラリ] の順に選択します。

b) 検索ボックスに「*Cloud Resource Manager*」と入力します。

c) 検索結果から、[**Cloud Resource Manager API**] を選択します。

d) [**Cloud Resource Manager API**] ページで、[**Enable**] を選択します。API のステータスが表示されます。

4. 同様に、[**Identity and Access Management**（**IAM**）**API**] および [**Cloud Build API**] を有効にします。

Google Cloud Shell を使用して API を有効にすることもできます。これを行うには、以下の手順に従います:

1. Google コンソールを開き、Cloud Shell を読み込みます。
2. Cloud Shell で次の 4 つのコマンドを実行します:

- gcloud services enable compute.googleapis.com
- gcloud services enable cloudresourcemanager.googleapis.com
- gcloud services enable iam.googleapis.com

- gcloud services enable cloudbuild.googleapis.com

3. Cloud Shell でプロンプトが表示されたら、［**Authorize**］をクリックします。

サービスアカウントの構成と更新

> 注:
>
> 2024 年 4 月 29 日、GCP は Cloud Build サービスのデフォルトの動作とサービスアカウントの使用に関する変更を導入します。詳しくは、「Cloud Build サービスアカウントの変更」を参照してください。2024 年 4 月 29 日より前に Cloud Build API が有効になっていた既存の Google プロジェクトは、この変更の影響を受けません。ただし、4 月 29 日以降も既存の Cloud Build サービスの動作を継続する場合は、Cloud Build API を有効にする前に、制約の適用を無効にする組織ポリシーを作成または適用できます。これにより、以下のコンテンツは「2024 年 4 月 29 日より前」と「2024 年 4 月 29 日以降」の 2 つに分割されます。新しい組織ポリシーを設定する場合は、「2024 年 4 月 29 日より前」のセクションに従ってください。

2024 年 **4** 月 **29** 日より前

Citrix Cloud は、Google Cloud プロジェクト内で次の 3 つの個別のサービスアカウントを使用します:

- *Citrix Cloud* サービスアカウント: このサービスアカウントにより、Citrix Cloud は Google プロジェクトにアクセスし、マシンをプロビジョニングおよび管理できます。このサービス アカウントは、Google Cloud によって生成された キー を使用して Google Cloud に対して認証されます。

  ここで説明するように、このサービスアカウントを手動で作成する必要があります。詳しくは、「Citrix Cloud サービスアカウントの作成」を参照してください。

  このサービスアカウントは、メールアドレスで識別できます。例: `<my-service-account>@<project-id>.iam.gserviceaccount.com`。

- *Cloud Build* サービスアカウント: このサービスアカウントは、「Google Cloud API の有効化」に記載されているすべての API を有効にすると自動的にプロビジョニングされます。自動的に作成されたサービスアカウントをすべて表示するには、**Google Cloud** コンソールで ［**IAM & admin**］**>** ［**IAM**］の順に移動し、［**Google** 提供のロール付与を含める］チェックボックスをオンにします。

  このサービスアカウントは、**Project ID** と、**cloudbuild** で始まるメールアドレスで識別できます。例: `<project-id>@cloudbuild.gserviceaccount.com`

  サービスアカウントに次の役割が付与されているかどうかを確認します。役割を追加する必要がある場合は、「Cloud Build サービスアカウントへの役割の追加」で説明されている手順に従います。

  - Cloud Build サービスアカウント
  - コンピューティングインスタンス管理者
  - サービスアカウントユーザー

- *Cloud Compute* サービスアカウント：このサービスアカウントは、Compute API がアクティブ化されると、Google Cloud で作成されたインスタンスに Google Cloud によって追加されます。このアカウントには、操作を行うための IAM の基本編集者の役割があります。ただし、より詳細な制御を行うためにデフォルトのアクセス権限を削除する場合は、次のアクセス権限を必要とする ストレージ管理者の役割を追加する必要があります：

  - resourcemanager.projects.get
  - storage.objects.create
  - storage.objects.get
  - storage.objects.list

このサービスアカウントは、**Project ID** と、**compute** で始まるメールアドレスで識別できます。例：<project-id>-compute@developer.gserviceaccount.com。

Citrix Cloud サービスアカウントの作成　Citrix Cloud サービスアカウントを作成するには、次の手順に従います：

1. Google Cloud コンソールで、［**IAM** と管理］**>**［サービスアカウント］の順に選択します。
2. ［**Service accounts**］ページで、［**CREATE SERVICE ACCOUNT**］を選択します。
3. ［**Create service account**］ページで必要な情報を入力してから、［**CREATE AND CONTINUE**］を選択します。
4. ［**Grant this service account access to project**］ページで、［**Select a role**］ドロップダウンメニューをクリックし、必要な役割を選択します。役割を追加する場合は、［**+ADD ANOTHER ROLE**］をクリックします。

   各アカウント（個人またはサービス）には、プロジェクトの管理を定義するさまざまな役割があります。このサービスアカウントに次の役割を付与します：

   - コンピューティング管理者
   - ストレージ管理者
   - Cloud Build エディター
   - サービスアカウントユーザー
   - クラウドデータストアユーザー
   - Cloud KMS Crypto Operator

   Cloud KMS Crypto Operator には次の権限が必要です：

   - cloudkms.cryptoKeys.get
   - cloudkms.cryptoKeys.list
   - cloudkms.keyRings.get
   - cloudkms.keyRings.list

> 注:
>
> すべての API を有効にして、新しいサービスアカウントの作成中に、使用できる役割の完全な一覧を取得してください。

5. [**CONTINUE**] をクリックします
6. [**Grant users access to this service account**] ページでユーザーまたはグループを追加し、このサービスアカウントで操作を実行できるアクセス権をユーザーに付与します。
7. [**DONE**] をクリックします。
8. IAM メインコンソールに移動します。
9. 作成されたサービスアカウントを識別します。
10. 役割が正常に割り当てられていることを確認します。

注意事項:

サービスアカウントを作成するときは、次の点を考慮してください:

- [**Grant this service account access to project**] と **Grant users access to this service account**] の手順は任意です。これらのオプションの構成手順をスキップする場合、新しく作成されたサービスアカウントは [**IAM** と管理] **>** [**IAM**] ページには表示されません。
- サービスアカウントに関連付けられている役割を表示するには、オプションの手順をスキップせずに役割を追加します。このプロセスにより、構成されたサービスアカウントの役割が確実に表示されます。

Citrix Cloud サービスアカウントキー　Citrix DaaS で接続を作成するには、Citrix Cloud サービスアカウントキーが必要です。キーは資格情報ファイル（.json）に含まれています。キーを作成すると、ファイルが自動的にダウンロードされ、「**Downloads**」フォルダーに保存されます。キーを作成するときは、必ずキータイプを JSON に設定してください。それ以外の場合、Citrix の完全な構成インターフェイスでは解析できません。

サービスアカウントキーを作成するには、[**IAM & Admin**] **>** [**Service accounts**] に移動して Citrix Cloud サービスアカウントのメールアドレスをクリックします。[**Keys**] タブを選択してから、[**Add Key**] **>** [**Create new key**] を選択します。キーの種類として必ず **JSON** を選択してください。

> ヒント:
>
> Google Cloud コンソールの [**Service accounts**] ページを使用してキーを作成します。セキュリティのために、キーを定期的に変更することをお勧めします。既存の Google Cloud 接続を編集することで、Citrix Virtual Apps and Desktops アプリケーションに新しいキーを提供できます。

Citrix Cloud サービスアカウントへの役割の追加　Citrix Cloud サービスアカウントに役割を追加するには:

1. Google Cloud コンソールで、[**IAM** と管理] **>** [**IAM**] の順に選択します。

2. [**IAM**] > [**PERMISSIONS**] ページで、作成したサービスアカウントを見つけ、メールアドレスで識別します。

   例：<my-service-account>@<project-id>.iam.gserviceaccount.com

3. 鉛筆アイコンを選択して、サービスアカウントのプリンシパルへのアクセス権を編集します。
4. 選択したプリンシパルオプションの［**Edit access to "project-id"**］ページで、[**ADD ANOTHER ROLE**] を選択してサービスアカウントに必要な役割を 1 つずつ追加し、［**SAVE**］を選択します。

Cloud Build サービスアカウントへの役割の追加　Cloud Build サービスアカウントに役割を追加するには：

1. Google Cloud コンソールで、[**IAM** と管理] > [**IAM**] の順に選択します。
2. [**IAM**] ページで、**Project ID** と、**cloudbuild** で始まるメールアドレスで識別できる Cloud Build サービスアカウントを見つけます。

   例：<project-id>@cloudbuild.gserviceaccount.com

3. 鉛筆アイコンを選択して、Cloud Build アカウントの役割を編集します。
4. 選択したプリンシパルオプションの［**Edit access to "project-id"**］ページで、[**ADD ANOTHER ROLE**] を選択して Cloud Build サービスアカウントに必要な役割を 1 つずつ追加し、［**SAVE**］を選択します。

   > 注：
   >
   > すべての API を有効にして、役割の完全な一覧を取得します。

2024 年 **4** 月 **29** 日以降

Citrix Cloud は、Google Cloud プロジェクト内で次の 2 つの個別のサービスアカウントを使用します：

- *Citrix Cloud* サービスアカウント：このサービスアカウントにより、Citrix Cloud は Google プロジェクトにアクセスし、マシンをプロビジョニングおよび管理できます。このサービス アカウントは、Google Cloud によって生成された キー を使用して Google Cloud に対して認証されます。

  このサービスアカウントは手動で作成する必要があります。

  このサービスアカウントは、メールアドレスで識別できます。例：<my-service-account>@<project-id>.iam.gserviceaccount.com。

- *Cloud Compute* サービスアカウント：このサービスアカウントは、「Google Cloud API の有効化」に記載されているすべての API を有効にすると自動的にプロビジョニングされます。自動的に作成されたサービスアカウントをすべて表示するには、**Google Cloud** コンソールで ［**IAM & admin**］> ［**IAM**］の順に移動し、[**Google** 提供のロール付与を含める］チェックボックスをオンにします。このアカウントには、操作を行うための IAM の基本編集者の役割があります。ただし、より詳細な制御を行うためにデフォルトのアクセス権限を削除する場合は、次のアクセス権限を必要とする ストレージ管理者の役割を追加する必要があります：

  - resourcemanager.projects.get

- storage.objects.create
- storage.objects.get
- storage.objects.list

このサービスアカウントは、**Project ID** と、**compute** で始まるメールアドレスで識別できます。例: `<project-id>-compute@developer.gserviceaccount.com`.

サービスアカウントに次の役割が付与されているかどうかを確認します。

- Cloud Build サービスアカウント
- コンピューティングインスタンス管理者
- サービスアカウントユーザー

Citrix Cloud サービスアカウントの作成　Citrix Cloud サービスアカウントを作成するには、次の手順に従います:

1. Google Cloud コンソールで、[**IAM** と管理] **>** [サービスアカウント] の順に選択します。
2. [**Service accounts**] ページで、[**CREATE SERVICE ACCOUNT**] を選択します。
3. [**Create service account**] ページで必要な情報を入力してから、[**CREATE AND CONTINUE**] を選択します。
4. [**Grant this service account access to project**] ページで、[**Select a role**] ドロップダウンメニューをクリックし、必要な役割を選択します。役割を追加する場合は、[**+ADD ANOTHER ROLE**] をクリックします。

   各アカウント（個人またはサービス）には、プロジェクトの管理を定義するさまざまな役割があります。このサービスアカウントに次の役割を付与します:

   - コンピューティング管理者
   - ストレージ管理者
   - Cloud Build エディター
   - サービスアカウントユーザー
   - クラウドデータストアユーザー
   - Cloud KMS Crypto Operator

   Cloud KMS Crypto Operator には次の権限が必要です:

   - cloudkms.cryptoKeys.get
   - cloudkms.cryptoKeys.list
   - cloudkms.keyRings.get
   - cloudkms.keyRings.list

> 注:
>
> すべての API を有効にして、新しいサービスアカウントの作成中に、使用できる役割の完全な一覧を取得してください。

5. [**CONTINUE**] をクリックします
6. [**Grant users access to this service account**] ページでユーザーまたはグループを追加し、このサービスアカウントで操作を実行できるアクセス権をユーザーに付与します。
7. [**DONE**] をクリックします。
8. IAM メインコンソールに移動します。
9. 作成されたサービスアカウントを識別します。
10. 役割が正常に割り当てられていることを確認します。

注意事項:

サービスアカウントを作成するときは、次の点を考慮してください:

- [**Grant this service account access to project**] と **Grant users access to this service account**] の手順は任意です。これらのオプションの構成手順をスキップする場合、新しく作成されたサービスアカウントは [**IAM** と管理] **>** [**IAM**] ページには表示されません。
- サービスアカウントに関連付けられている役割を表示するには、オプションの手順をスキップせずに役割を追加します。このプロセスにより、構成されたサービスアカウントの役割が確実に表示されます。

Citrix Cloud サービスアカウントキー　Citrix DaaS で接続を作成するには、Citrix Cloud サービスアカウントキーが必要です。キーは資格情報ファイル（.json）に含まれています。キーを作成すると、ファイルが自動的にダウンロードされ、「**Downloads**」フォルダーに保存されます。キーを作成するときは、必ずキータイプを JSON に設定してください。それ以外の場合、Citrix の完全な構成インターフェイスでは解析できません。

サービスアカウントキーを作成するには、[**IAM & Admin**] **>** [**Service accounts**] に移動して Citrix Cloud サービスアカウントのメールアドレスをクリックします。[**Keys**] タブを選択してから、[**Add Key**] **>** [**Create new key**] を選択します。キーの種類として必ず **JSON** を選択してください。

> ヒント:
>
> Google Cloud コンソールの [**Service accounts**] ページを使用してキーを作成します。セキュリティのために、キーを定期的に変更することをお勧めします。既存の Google Cloud 接続を編集することで、Citrix Virtual Apps and Desktops アプリケーションに新しいキーを提供できます。

Citrix Cloud サービスアカウントへの役割の追加　Citrix Cloud サービスアカウントに役割を追加するには:

1. Google Cloud コンソールで、[**IAM** と管理] **>** [**IAM**] の順に選択します。

2. [**IAM**] > [**PERMISSIONS**] ページで、作成したサービスアカウントを見つけ、メールアドレスで識別します。

   例：<my-service-account>@<project-id>.iam.gserviceaccount.com

3. 鉛筆アイコンを選択して、サービスアカウントのプリンシパルへのアクセス権を編集します。
4. 選択したプリンシパルオプションの［**Edit access to "project-id"**］ページで、[**ADD ANOTHER ROLE**] を選択してサービスアカウントに必要な役割を 1 つずつ追加し、［**SAVE**］を選択します。

Cloud Compute サービスアカウントに役割を追加する　Cloud Compute サービスアカウントに役割を追加するには：

1. Google Cloud コンソールで、［**IAM** と管理］>［**IAM**］の順に選択します。
2. [**IAM**] ページで、**Project ID** と、**compute** で始まるメールアドレスで識別できる Cloud Build サービスアカウントを見つけます。

   例：<project-id>-compute@developer.gserviceaccount.com

3. 鉛筆アイコンを選択して、Cloud Build アカウントの役割を編集します。
4. 選択したプリンシパルオプションの［**Edit access to "project-id"**］ページで、[**ADD ANOTHER ROLE**] を選択して Cloud Build サービスアカウントに必要な役割を 1 つずつ追加し、［**SAVE**］を選択します。

   > 注：
   >
   > すべての API を有効にして、役割の完全な一覧を取得します。

ストレージ権限とバケットの管理

Citrix Virtual Apps and Desktops は、Google Cloud サービスのクラウドビルドエラーのレポートプロセスを改善します。このサービスは、Google Cloud でビルドを実行します。Citrix Virtual Apps and Desktops は、Google Cloud サービスがビルドログ情報をキャプチャするcitrix-mcs-cloud-build-logs-{ region } -{ 5 random characters }という名前のストレージバケットを作成します。このバケットには、30 日後にコンテンツを削除するオプションが設定されています。このプロセスでは、接続に使用するサービスアカウントで、Google Cloud の権限がstorage.buckets.updateに設定されている必要があります。サービスアカウントにこの権限が設定されていない場合、Citrix Virtual Apps and Desktops はエラーを無視し、カタログの作成プロセスを続行します。この権限がないと、ビルドログのサイズが大きくなり、手動によるクリーンアップが必要になります。

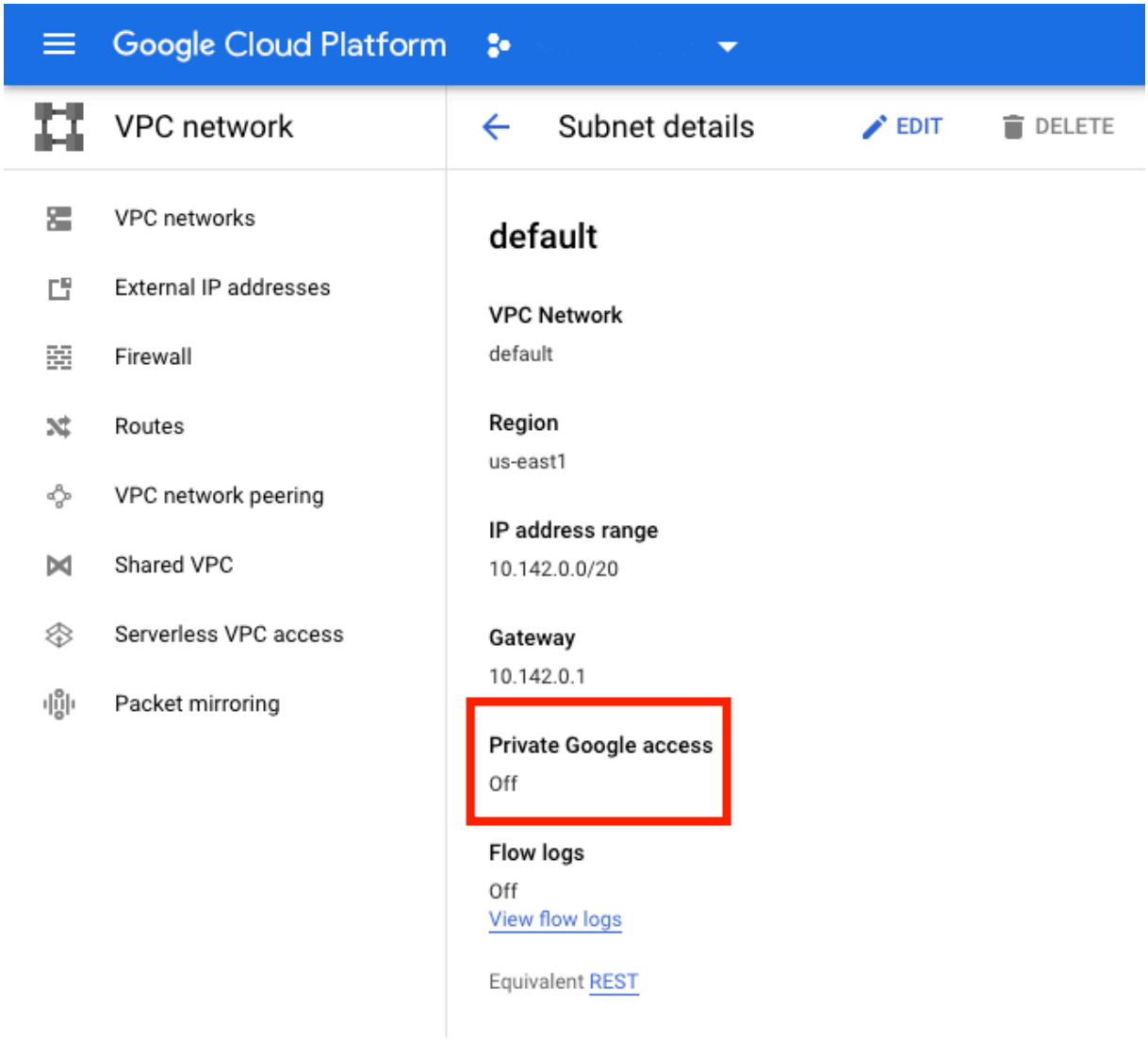
プライベート **Google** アクセスの有効化

ネットワークインターフェイスに割り当てられた外部 IP アドレスが VM にない場合、パケットは他の内部 IP アドレスの宛先にのみ送信されます。プライベートアクセスを有効にすると、VM は Google API および関連サービスで使用される外部 IP アドレスのセットに接続します。

> 注:
>
> プライベート Google アクセスが有効になっているかどうかに関係なく、パブリック IP アドレスを持つ VM もパブリック IP アドレスを持たない VM もすべて、特にサードパーティのネットワークアプライアンスが環境にインストールされている場合、Google パブリック API にアクセスできる必要があります。

サブネット内の VM が、MCS プロビジョニング用のパブリック IP アドレスなしで Google API にアクセスできるようにするには:

1. Google Cloud で、[**VPC network configuration**] にアクセスします。
2. [サブネットの詳細] 画面で、[プライベート **Google** アクセス] をオンにします。



詳しくは、「プライベート Google アクセスの構成」を参照してください。

> 重要:
>
> インターネットへの VM アクセスを防止するようにネットワークが構成されている場合は、VM が接続されているサブネットに対してプライベート Google アクセスを有効にすることに関連するリスクを、組織が想定していることを確認してください。

次の手順

- コアコンポーネントのインストール
- VDA のインストール
- サイトの作成
- Google Cloud 環境での接続の作成と管理については、「Google Cloud 環境への接続」を参照してください。

追加情報

- 接続とリソースの作成と管理
- マシンカタログの作成

HPE Moonshot 仮想化環境

August 17, 2024

Citrix Virtual Apps and Desktops は、Citrix が管理する HPE Moonshot プラグインを通じて HPE Moonshot ワークロードを管理します。このプラグインを使用すると、HPE Moonshot シャーシへの接続の作成、カタログの作成、カタログ内のマシンの電源管理が可能になります。

条件

Citrix 管理の HPE Moonshot プラグインを Delivery Controller にインストールします。

> 注:
>
> - Citrix 管理の HPE Moonshot プラグインと HPE 管理の HPE Moonshot プラグインの両方がインストールされている場合、Delivery Controller は Citrix 管理の HPE Moonshot プラグインを使用します。
> - Citrix 管理の HPE Moonshot プラグインと HPE 管理の HPE Moonshot プラグインの両方がインストールされており、HPE 管理の Moonshot プラグインを使用する場合は、Citrix 管理の HPE Moonshot プラグインをアンインストールし、`RegisterPlugin`キャッシュを更新します。

Citrix 管理の **HPE Moonshot** プラグインをインストールする

Citrix 管理の HPE Moonshot プラグインをインストールするには、以下を実行します:

1. E:\x64\Citrix Desktop Delivery Controller\MoonshotPlugin.msi をインストールします。E:\は ISO です。
2. 管理者として PowerShell を開き、次のコマンドを実行します。

```
C:\Program Files\Common Files\Citrix\HCLPlugins> .\RegisterPlugins
    .exe -pluginsroot .\CitrixMachineCreation\v1.0.0.0\
```

3. プラグインの登録が成功したら、タスクマネージャーから以下のサービスを再起動します:
   a) CitrixBrokerService
   b) CitrixHostService
   c) CitrixMachineCreationService
4. Get-HypHypervisorPluginsを実行して、プラグインが Delivery Controller にインストールされているかどうかを確認します。出力の **DisplayName** フィールドには **HPE Moonshot** が表示される必要があります。

Citrix 管理の **HPE Moonshot** プラグインをアンインストールし **RegisterPlugin** キャッシュを更新する

Citrix 管理の HPE Moonshot プラグインと HPE 管理の HPE Moonshot プラグインの両方がインストールされており、HPE 管理の Moonshot プラグインを使用する場合は、Citrix 管理の HPE Moonshot プラグインをアンインストールし、RegisterPluginキャッシュを更新する必要があります。必要な操作:

1. Citrix 管理の HPE Moonshot プラグインをインストールします。
2. 管理者として PowerShell を開き、次のコマンドを実行します:

```
cd `C:\Program Files\Common Files\Citrix\HCLPlugins`
C:\Program Files\Common Files\Citrix\HCLPlugins> .\RegisterPlugins
    .exe -PluginsRoot ` C:\Program Files\Common Files\Citrix\
    HCLPlugins\ManagedMachine\v2.5.0.0`
```

3. プラグインの登録が成功したら、タスクマネージャーから以下のサービスを再起動します:
   a) CitrixBrokerService
   b) CitrixHostService
   c) CitrixMachineCreationService
4. Get-HypHypervisorPluginsを実行して、プラグインが Delivery Controller にインストールされているかどうかを確認します。出力の **DisplayName** フィールドには **HPE Moonshot Machine Manager** が表示される必要があります。

主な手順

1. HPE 環境をセットアップします。
2. HPE Moonshot シャーシへの接続を作成します。
3. マシンカタログを作成します。

   > 注:
   >
   > カタログを作成する前に、1 つ以上の HPE Moonshot カートリッジノードが存在し、それらのノードに VDA がインストールされていることを確認してください。HPE Moonshot シャーシをハイパーバイザーとして、カートリッジノードを VM として考えることができます。

4. デリバリーグループを作成します。
5. 残りの非管理対象 HPE Moonshot ノードを管理対象カタログまたはデリバリーグループに移行します。

次の手順

- コアコンポーネントのインストール
- VDA のインストール
- サイトの作成
- HPE Moonshot での接続の作成と管理については、「HPE Moonshot への接続」を参照してください

追加情報

- 接続とリソースの作成と管理
- マシンカタログの作成

Microsoft Azure Resource Manager クラウド環境

August 17, 2024

Microsoft Azure Resource Manager を使用して、Citrix Virtual Apps and Desktops 環境で仮想マシンをプロビジョニングする場合は、次のことをよく理解しておいてください:

- Azure Active Directory: https://docs.microsoft.com/en-in/azure/active-directory/fundamentals/active-directory-whatis/
- 同意フレームワーク: https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/plan-an-application-integration

- サービスプリンシパル：https://docs.microsoft.com/en-us/azure/active-directory/develop/app-objects-and-service-principals/

Microsoft Azure Resource Manager をセットアップするには、「インストールの準備」を参照してください。

次の手順

- コアコンポーネントのインストール
- VDA のインストール
- サイトの作成
- Azure 環境での接続の作成と管理については、「Microsoft Azure への接続」を参照してください。

追加情報

- 接続とリソースの作成と管理
- マシンカタログの作成
- CTX219211：Microsoft Azure Active Directory アカウントの設定
- CTX219243：Azure サブスクリプションへの XenApp および XenDesktop アクセス権の付与
- CTX219271：サイト間 VPN を使用したハイブリッドクラウドの展開

Microsoft System Center Configuration Manager 環境

August 17, 2024

Microsoft System Center Configuration Manager（Configuration Manager）でアプリケーションやデスクトップへのアクセスを管理しているサイトでは、Configuration Manager の管理機能を Citrix Virtual Apps and Desktops 環境まで拡張できます。以下のオプションを使用できます：

- SCCM を使用した VDA のインストール。
- **Configuration Manager** のウェイクアッププロキシ機能：リモート PC アクセスの Wake on LAN 機能は、Configuration Manager でサポートされます。詳しくは、「Wake on LAN - SCCM 統合」を参照してください。
- **Citrix Virtual Apps and Desktops** のプロパティ：プロパティ設定により、Configuration Manager で管理する Citrix Virtual Desktops を識別できるようになります。（Configuration Manager の一部のバージョンでは、Citrix Virtual Apps and Desktops の旧称：XenApp および XenDesktop が使用されます。）

プロパティ

Microsoft System Center Configuration Manager では仮想デスクトップを管理するためのプロパティを利用できます。

Configuration Manager に表示されるプロパティのブール値は、true と false ではなく1と0で表示されます。

プロパティは、名前空間Root\Citrix\DesktopInformationのCitrix_virtualDesktopInfoクラスで使用できます。これらのプロパティの名前は、Windows Management Instrumentation（WMI）プロバイダーでのものです。

プロパティ	説明
AssignmentType	IsAssigned の値を設定します。有効な値: ClientIP、ClientName、None、User（IsAssignedをTrueに設定）
BrokerSiteName	HostIdentifierと同じ値を返します
DesktopCatalogName	デスクトップに関連付けられたマシンカタログの名前です。
DesktopGroupName	デスクトップに関連付けられたデリバリーグループの名前です。
HostIdentifier	BrokerSiteNameと同じ値を返します。
IsAssigned	デスクトップを各ユーザーに割り当てる場合はTrue、ランダムデスクトップの場合はFalseを設定します
IsMasterImage	マスターイメージかどうかを指定します。たとえば、プロビジョニングされたマシンではなく、イメージにアプリケーションをインストールします。有効な値：イメージとして使用される仮想マシンではTrue。この値は、選択オプションに基づいてインストール時に設定されます。マスターイメージからプロビジョニングされる仮想マシンでは Cleared になります。
IsVirtualMachine	仮想マシンではTrue、物理マシンでは**false**になります。
OSChangesPersist	再起動時にデスクトップのオペレーティングシステムイメージをクリーンな状態にリセットする場合はFalse、リセットしない場合は**true**になります。
PersistentDataLocation	Configuration Manager が永続データを格納する場所です。ユーザーはアクセスできません。
BrokerSiteName、DesktopCatalogName、DesktopGroupName、HostIdentifier	デスクトップが Controller に登録されるときに設定されます。完全には登録されていないデスクトップの場合は null になります。

これらのプロパティを収集するには、Configuration Manager でハードウェアインベントリを実行します。プロパティを表示するには、Configuration Manager のリソースエクスプローラーを使用します。これらのインスタンスでは、名前にスペースが含まれたり、プロパティ名とわずかに違ったものになったりします。たとえば、`BrokerSiteName`は`Broker Site Name`と表示されます。

- Configuration Manager を構成して Citrix VDA から Citrix WMI プロパティを収集する。
- Citrix WMI プロパティを使用してクエリベースのデバイスコレクションを作成する。
- Citrix WMI プロパティに基づいてグローバル条件を作成する。
- グローバル条件を使用してアプリケーションの展開の種類の要件を定義する。

また、Microsoft クラスの`CCM_DesktopMachine`の Microsoft プロパティを名前空間`Root\ccm_vdi`で使用することもできます。詳しくは、Microsoft のドキュメントを参照してください。

Microsoft System Center Virtual Machine Manager 仮想化環境

August 17, 2024

Hyper-V と Microsoft System Center Virtual Machine Manager（VMM）を使用して仮想マシンを提供する場合は、このトピックのガイダンスに従ってください。

このリリースは、「システム要件」に記載された VMM バージョンをサポートします。

> 注:
>
> 混合 Hyper-V クラスター（異なる Hyper-V バージョンを実行しているサーバーを含む）はサポートされていません。

Citrix Provisioning（旧称 Provisioning Services）および Machine Creation Services を使用して、次のものをプロビジョニングできます:

- サポートされる第 1 世代デスクトップまたはサーバー OS の VM
- サポートされる第 2 世代デスクトップまたはサーバー OS の VM（セキュアブートのサポートを含む）。

ハイパーバイザーのインストールおよび構成

> 重要:
>
> すべての Delivery Controller が VMM サーバーと同じフォレストに含まれている必要があります。

1. サーバー上に Microsoft Hyper-V Server および VMM をインストールします。
2. すべての Controller に System Center Virtual Machine Manager コンソールをインストールします。コンソールのバージョンは管理サーバーと同じバージョンにする必要があります。古いコンソールを管理サーバーに接続することはできますが、バージョンが異なる場合、VDA のプロビジョニングは失敗します。

3. 次のアカウント情報を確認します：

   Studio でホストを指定するために使用するアカウントは、VMM 管理者またはその Hyper-V マシンの VMM 委任管理者である必要があります。このアカウントに VMM の委任管理者の役割のみがある場合は、ホストの作成時にストレージデータが Studio の一覧に表示されません。

   Studio 統合に使用されるユーザーアカウントは、各 Hyper-V サーバー上の管理者ローカルセキュリティグループのメンバーでもある必要があります。この構成は、仮想マシンの作成、更新、削除などの仮想マシンライフサイクル管理をサポートします。

   Hyper-V が動作するサーバー上に Controller をインストールすることはサポートされていません。

単一の SCVMM が異なるデータセンターの複数のクラスターを管理する大規模な環境では、委任された管理者のホストグループのスコープを制限できます。

ホストグループのスコープを制限するには、Microsoft System Center Virtual Machine Manager（VMM）コンソールで Delegated Admin の役割を使用します：

1. [**Create User Roles Wizard**]で、ユーザー役割として Fabric Administrator（Delegated Administrator）を選択します。
2. [**Members**] で、委任された管理者として使用するユーザーアカウントを Active Directory に追加します。
3. [**Scope**] で、委任された管理者にアクセス権を与えるホストグループを選択します。
4. 委任された管理者のユーザー資格情報で、新しい実行アカウントを作成します。これらの資格情報を使用して、後でハイパーバイザー接続を作成します。メインの管理者の役割アカウントは使用しないでください。

SCVMM を介した **Azure Stack HCI** のプロビジョニング

Azure Stack HCI は、ハイパーコンバージドインフラストラクチャ（HCI）クラスターソリューションであり、ハイブリッドのオンプレミス環境で、仮想化された Windows および Linux ワークロードとそれらのストレージをホストします。

Azure ハイブリッドサービスは、クラウドベースの監視、サイト回復、VM バックアップなどの機能でクラスターを強化します。Azure Portal ですべての Azure Stack HCI 展開を表示することもできます。

注意事項

以下に注意してください：

- Windows 10 Enterprise マルチセッションおよび Windows 11 Enterprise マルチセッションのワークロードはサポートされていません。
- Azure Stack HCI 23H2 クラスターの管理のサポートは、SCVMM 2025 に付属しています。

Azure Stack HCI の **SCVMM** との統合

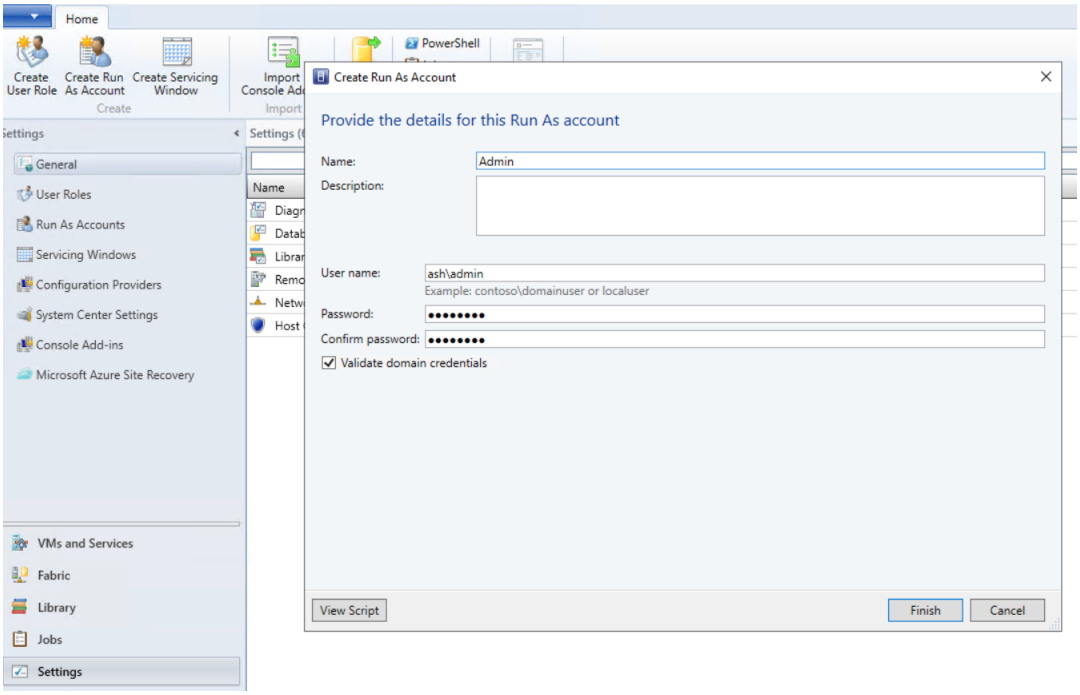
Azure Stack HCI を SCVMM と統合するには、最初に Azure Stack HCI クラスターを作成してから、そのクラスターを SCVMM と統合する必要があります。

1. Azure Stack HCI クラスターを作成するには、Microsoft 社のドキュメント「Azure Stack HCI を Azure に接続する」を参照してください。
2. Azure Stack HCI クラスターを SCVMM と統合するには、次の手順を実行します:

   a) SCVMM サーバーをホストする準備ができているマシンにログインし、SCVMM 2019 UR3 以降をインストールします。

   > 注:
   >
   > すべてのコントローラーに SCVMM 2019 UR3 以降の管理者コンソールをインストールします。

   b) VMM コンソールの ［設定］ページで、実行アカウントを作成します。



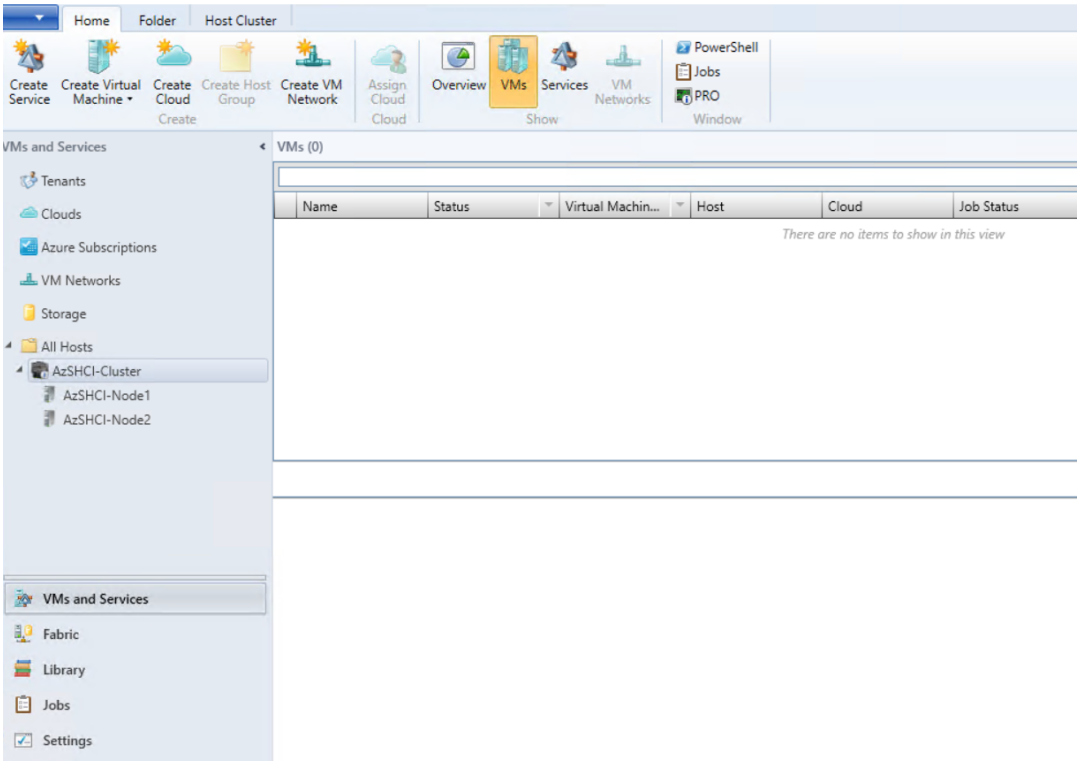
   c) SCVMM サーバーで管理者権限を使用して次の PowerShell コマンドを実行し、ホストとして Azure Stack HCI クラスターを追加します:

```
$runAsAccountName = 'Admin'
$runAsAccount = Get-SCRunAsAccount -Name $runAsAccountName
$hostGroupName = 'All Hosts'
$hostGroup = Get-SCVMHostGroup -Name $hostGroupName
$hostCluster = 'FQDN of Azure Stack HCI cluster'
Add-SCVMHostCluster -Name $hostCluster -RunAsynchronously -
    VMHostGroup
```



```
7  $hostGroup -Credential $runAsAccount -RemoteConnectEnabled
       $true
```

d) これで、VMM コンソールのノードと合わせて Azure Stack HCI クラスターを確認できるようになりました。



e) Web Studio で、SCVMM ホスト接続を作成してから、MCS マシンカタログを作成します。

次の手順

- コアコンポーネントのインストール
- VDA のインストール
- サイトの作成
- SCVMM での接続の作成と管理については、「Microsoft System Center Virtual Machine Manager への接続」を参照してください。

追加情報

- 接続とリソースの作成と管理
- マシンカタログの作成

Nutanix 仮想化環境

August 17, 2024

Citrix Virtual Apps and Desktops 環境で Nutanix Acropolis を使用して仮想マシンを提供する場合は、以下のガイダンスに従ってください。セットアップ処理には、次のタスクが含まれます。

- Citrix Virtual Apps and Desktops 環境に Nutanix プラグインをインストールして登録する。
- Nutanix Acropolis ハイパーバイザーとの接続を作成する。
- Nutanix ハイパーバイザーで作成したマスターイメージのスナップショットを使用するマシンカタログを作成する。

詳しくは、Nutanix サポートポータルにある『Nutanix Acropolis MCS plug-in Installation Guide』を参照してください。

Nutanix プラグインのインストールと登録

次の手順に従って、すべての Delivery Controller に Nutanix プラグインをインストールして登録します。Citrix Studio を使用して、Nutanix への接続を作成します。次に、Nutanix 環境で作成したマスターイメージのスナップショットを使用するマシンカタログを作成します。

> ヒント:
>
> Nutanix プラグインをインストールまたは更新するときは、Citrix Host Service、Citrix Broker Service、および Machine Creation Services を停止してから再起動することをお勧めします。

Nutanix プラグインのインストールについて詳しくは、Nutanix のドキュメントサイトを参照してください。

次の手順

- コアコンポーネントのインストール
- VDA のインストール
- サイトの作成
- Nutanix 環境での接続の作成と管理については、「Nutanix への接続」を参照してください。

追加情報

- 接続とリソースの作成と管理
- マシンカタログの作成

Nutanix クラウドおよびパートナーソリューション

August 17, 2024

Citrix Virtual Apps and Desktops は、次の Nutanix クラウドおよびパートナーソリューションをサポートしています:

- Nutanix Cloud Clusters on AWS

Nutanix Cloud Clusters on AWS

Citrix Virtual Apps and Desktops は、Nutanix Cloud Clusters on AWS をサポートしています。Nutanix Clusters は、プライベートクラウドまたは複数のパブリッククラウドでのアプリケーションの実行をシンプルにします。Nutanix Cloud Clusters on AWS について詳しくは、「Nutanix Cloud Clusters on AWS Deployment and User Guide」を参照してください。

> ヒント:
>
> このサポートは、Nutanix オンプレミスクラスターと同じ機能を提供します。単一のクラスターのみサポートされます（*Prism Element*）。詳しくは、こちらを参照してください。

要件

Nutanix Clusters on AWS を使用するには、以下のものが必要です:

- Nutanix アカウント。
- 次の権限を持つ AWS アカウント:
  - IAMFullAccess
  - AWSConfigRole
  - AWSCloudFormationFullAccess

Nutanix Cluster の作成

Nutanix Cluster を作成するには:

1. Nutanix アカウントにログインします。
2. [**Nutanix cluster**] オプションを見つけ、[**Launch**] をクリックします。[**Nutanix Console**] が開きます。詳しくは、「Get Started with Nutanix Cluster on AWS」を参照してください。
3. [**new VPC**] の作成を選択します。

クラスター作成プロセスは、次のエラーで失敗することがあります:

- Cluster failed to create within a given time. Deleting cluster.（指定された時間内にクラスターを作成できませんでした。クラスターを削除しています）
- Host Nutanix Cluster - Node XXXXXXXXXX: Instance i-xxxxxxxxxxxxx: disable network interface source/dest check error.
- Host Nutanix Cluster - Node XXXXXXXXXX: Unable to obtain instance i-xxxxxxxxxxxxxx network interface info.

クラスターの作成に失敗した場合は:

- もう一度、別のリージョンで 1 つ作成してみてください。
- もう一度試す前に、必ず Nutanix CloudFormation スタック（CFS）を削除してください。

他のリソースに加えて、Nutanix CFS は以下を作成します:

- 「*Nutanix Cluster xxxxxxxxxxxx* 10.0.0.0/16」という名前の 1 つの VPC
- 「10.0.128.0/24」と「10.0.129.0/24」という 2 つのサブネット
- 1 つのインターネットゲートウェイ
- 1 つの NAT ゲートウェイ

クラスターが作成されたら、**Nutanix Prism** のアドレスを取得します:

1. [**Nutanix Console**] に移動します。
2. コンソールの右上にある [**Launch Prism Element**] リンクにマウスを合わせて、URL をコピーします。

次の手順

- コアコンポーネントのインストール
- VDA のインストール
- サイトの作成
- Nutanix クラウドおよびパートナーソリューションの接続の作成と管理については、「Nutanix クラウドおよびパートナーソリューションへの接続」を参照してください。

追加情報

- 接続とリソースの作成と管理
- マシンカタログの作成

VMware 仮想化環境

August 17, 2024

VMware を使用して仮想マシンを提供する場合は、このトピックのガイダンスに従ってください。

vCenter Server および必要な管理ツールをインストールします（vSphere vCenter のリンクモードはサポートされません。）

MCS を使用する場合は、vCenter Server のデータストアブラウザー機能は無効にしないでください（https://kb.vmware.com/s/article/2101567を参照）。この機能を無効にすると、MCS が正しく動作しなくなります。

次の手順

- コアコンポーネントのインストール
- VDA のインストール
- サイトの作成
- VMware 環境での接続の作成と管理については、「VMware への接続」を参照してください。

追加情報

- 接続とリソースの作成と管理
- マシンカタログの作成

VMware クラウドおよびパートナーソリューション

August 17, 2024

Citrix Virtual Apps and Desktops は、次の VMware Cloud およびパートナーソリューションをサポートしています:

- Azure VMware Solution（AVS）
- Google Cloud VMware Engine
- VMware Cloud on AWS（Amazon Web Services）

Azure VMware Solution（AVS）の統合

Citrix Virtual Apps and Desktop サービスではAVSがサポートされています。AVS では、Azure インフラストラクチャによって作成された vSphere クラスターを含むクラウドインフラストラクチャが提供されます。オンプレミス環境で vSphere を使用するのと同じ方法で、Citrix Virtual Apps and Desktops サービスで AVS を使用して VDA ワークロードをプロビジョニングします。

AVS クラスターのセットアップ

Citrix Virtual Apps and Desktops サービスで AVS を使用できるようにするには、Azure で次の手順を実行します:

- ホストクォータの要求
- Microsoft.AVS リソースプロバイダーの登録
- ネットワークチェックリスト
- Azure VMware Solution プライベートクラウドの作成
- Azure VMware Solution プライベートクラウドへのアクセス
- Azure での VMware プライベートクラウドのネットワークの構成
- Azure VMware Solution の DHCP の構成
- Azure VMware Solution へのネットワークセグメントの追加
- Azure VMware Solution 環境の確認

Azure Enterprise Agreement の顧客のホストクォータの要求　Azure Portal の［**Help + Support**］ページで［**New support request**］を選択し、次の情報を含めます:

- Issue type:［Technical］
- Subscription:自分のサブスクリプションを選択する
- Service:［All services］>［Azure VMware Solution］
- Resource:［General question］
- Summary:［Need capacity］
- Problem type:［Capacity Management Issues］
- Problem subtype:［Customer Request for Additional Host Quota/Capacity］

サポートチケットの［**Description**］で［**Details**］タブに次の情報を含めます:

- 概念実証または実稼働
- リージョン名
- ホストの数
- その他の詳細

> 注:
>
> AVS には少なくとも 3 つのホストが必要です。冗長性のため 1 つ多くホストを使用することをお勧めします。

サポートチケットの詳細を指定した後、［**Review + Create**］を選択して Azure に要求を送信します。

Microsoft.AVS リソースプロバイダーの登録　ホストクォータを要求した後、リソースプロバイダーを登録します:

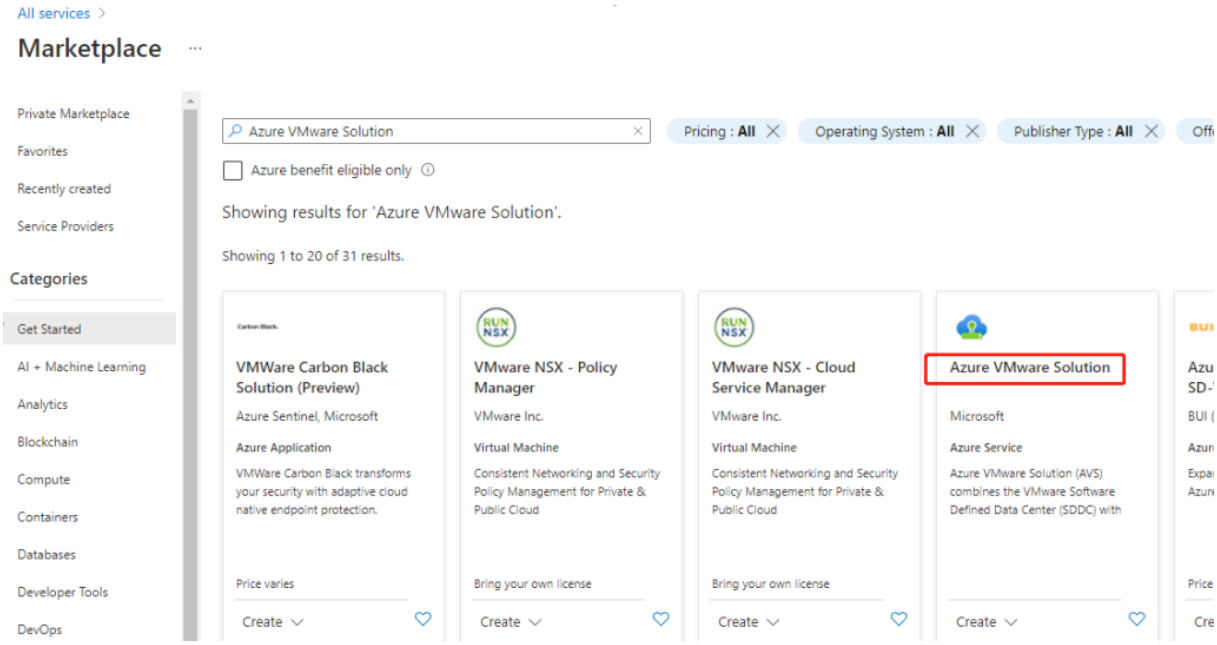
1. Azure Portal にサインインします。

2. Azure Portal のメニューで、[**All services**] を選択します。
3. [**All services**] メニューで、サブスクリプションを入力し、[**Subscriptions**] を選択します。
4. サブスクリプション一覧からサブスクリプションを選択します。
5. [**Resource providers**] を選択し、検索バーに 「**Microsoft.AVS**」と入力します。
6. リソースプロバイダーが登録されていない場合は、[**Register**] を選択します。

ネットワークに関する考慮事項　AVS では、特定のネットワークアドレス範囲とファイアウォールポートを必要とするネットワークサービスが提供されます。詳しくは、「Azure VMware Solution のネットワーク計画のチェックリスト」を参照してください。

Azure VMware Solution プライベートクラウドの作成　ご使用の環境のネットワーク要件を検討した後、ASV プライベートクラウドを作成します:

1. Azure Portal にサインインします。
2. [**Create a new resource**] を選択します。
3. [**Search the Marketplace**] ボックスで、「*Azure VMware Solution*」と入力し、一覧から [**Azure VMware Solution**] を選択します。



の画像

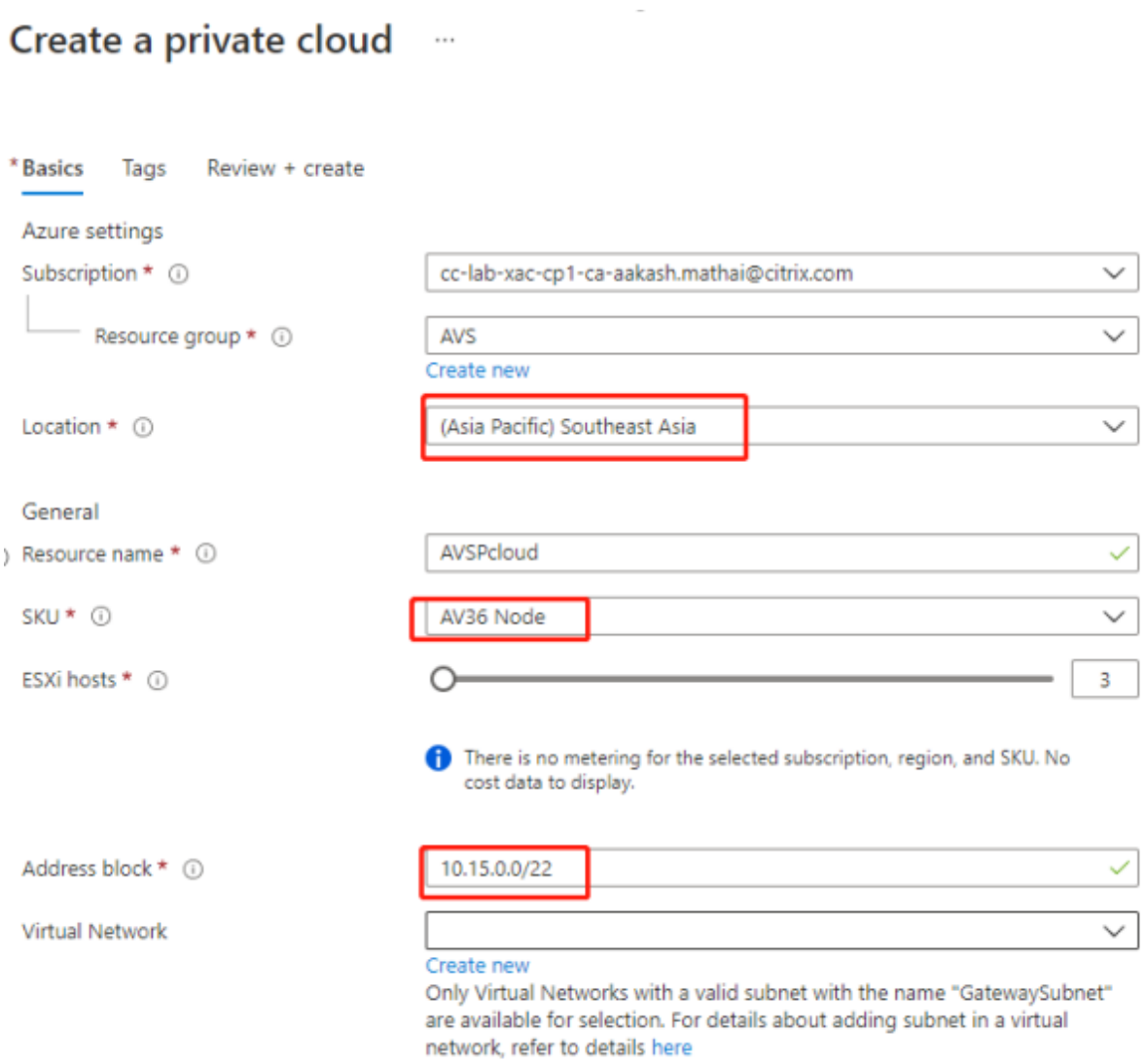
[**Azure VMware Solution**] ウィンドウで、次のことを行います:

1. [作成] を選択します。
2. [**Basics**] タブをクリックします。
3. 以下の表内の情報を使用してフィールドの値を入力します:

フィールド	値
Subscription	環境で使用する予定のサブスクリプションを選択します。Azure サブスクリプション内のすべてのリソースが一緒に請求されます。
リソースグループ	プライベートクラウドのリソースグループを選択します。Azure リソースグループは、Azure リソースが展開され管理される論理コンテナです。または、自分のプライベートクラウド用の新しいリソースグループを作成することもできます。
場所	米国東部など、場所を選択します。これは、計画フェーズで定義したリージョンです。
リソース名	Azure VMware Solution プライベートクラウドの名前を入力します。
SKU	AV36 を選択します。
ホスト	プライベートクラウドのクラスターに割り当てられているホストの数を示します。デフォルト値は 3 であり、展開後に増減できます。
Address block	プライベートクラウド用に IP アドレスブロックを提供します。CIDR（クラスレスドメイン間ルーティング）は、プライベートクラウド管理ネットワークを表し、vCenter Server や NSX-T Manager などのクラスター管理サービスに使用されます。/22 アドレススペースを使用します。たとえば、10.175.0.0/22 です。アドレスは一意である必要があり、他の Azure 仮想ネットワークやオンプレミスネットワークと重複しないようにする必要があります。
仮想ネットワーク	Azure VMware Solution ExpressRoute 回線は展開後の手順として確立されるので、これは空白のままにします。

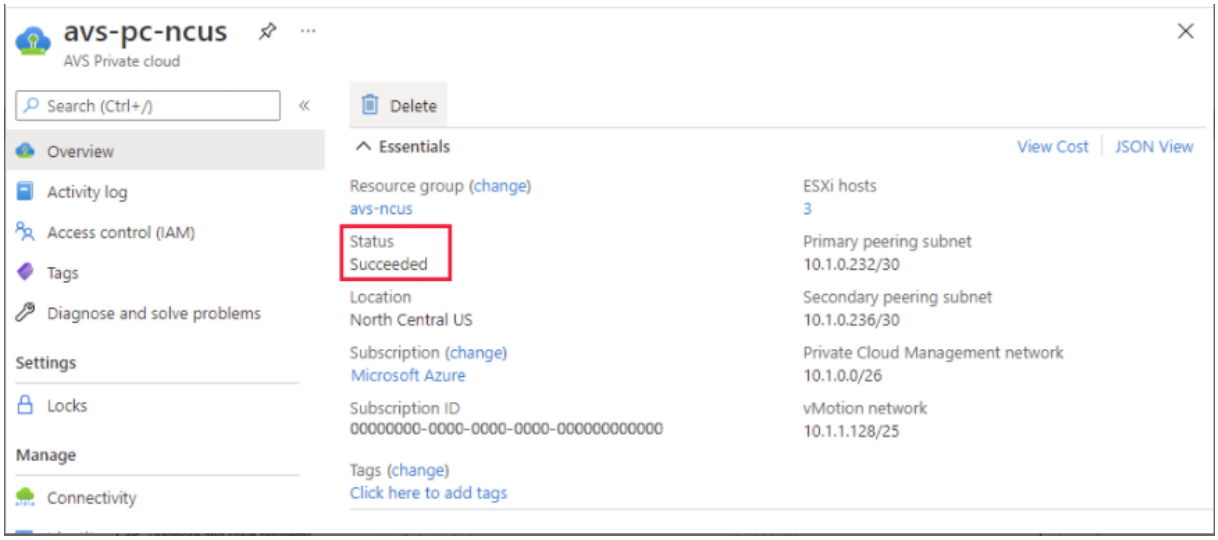
［**Create a private cloud**］画面で、次のことを行います：

1. ［**Location**］フィールドで、AVS があるリージョンを選択します。リソースグループのリージョンは AVS リージョンと同じです。
2. ［**SKU**］フィールドで、［**AV36 Node**］を選択します。
3. ［**Address Block**］フィールドで IP アドレスを指定します。たとえば、10.15.0.0/22 です。
4. ［**Review + Create**］を選択します。
5. 情報を確認したら、［**Create**］をクリックします。



> ヒント:
>
> プライベートクラウドの作成には 3～4 時間かかる場合があります。単一のホストをクラスターに追加するには、30～45 分かかる場合があります。

展開が成功したことを確認します。作成したリソースグループに移動し、プライベートクラウドを選択します。［**Status**］が ［**Succeeded**］になると、展開は完了です。



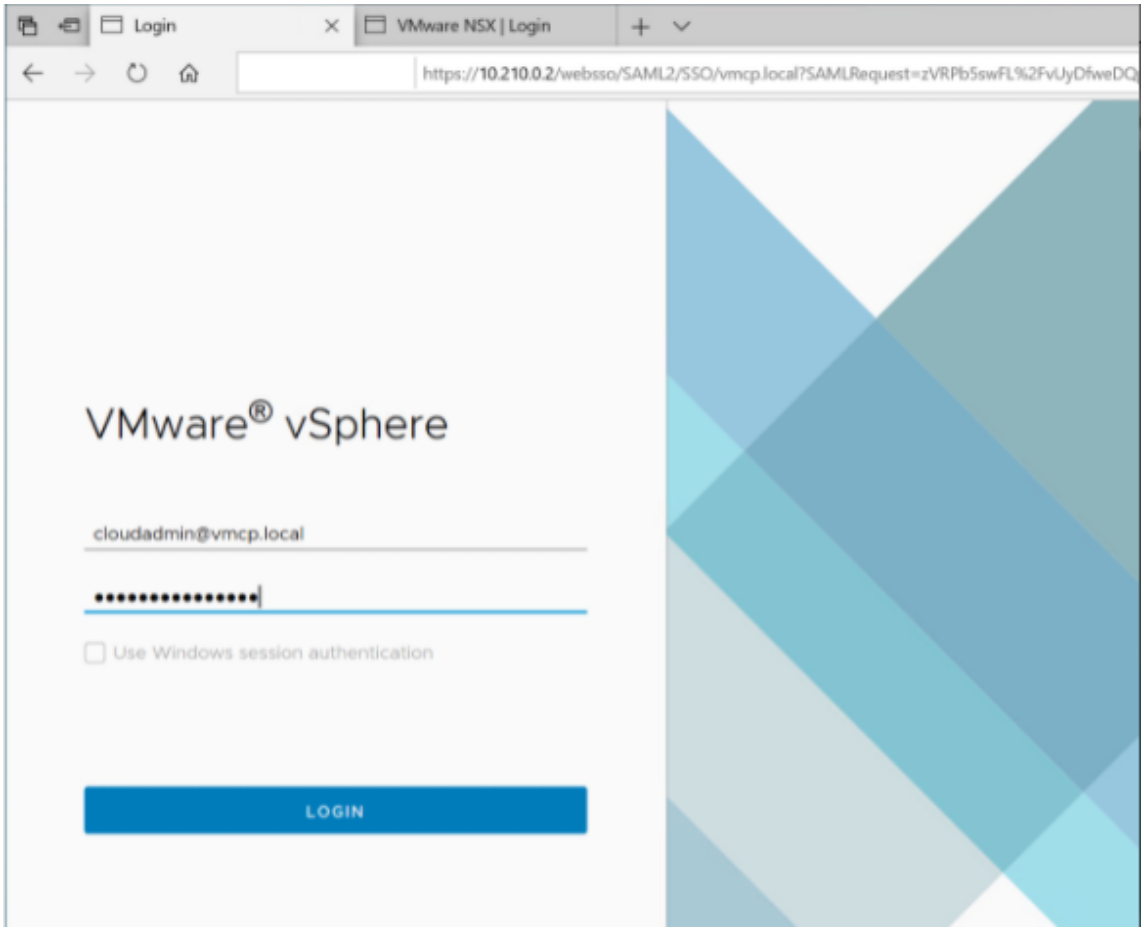
Azure VMware Solution プライベートクラウドへのアクセス　プライベートクラウドを作成したら、Windows VM を作成し、プライベートクラウドのローカル vCenter に接続します。

新しい **Windows** 仮想マシンの作成

1. リソースグループで、[**+ Add**] を選択してから、「**Microsoft Windows 10/2016/2019**」を検索して選択します。
2. [作成] をクリックします。
3. 必要な情報を入力してから、[**Review + Create**] を選択します。
4. 検証に合格したら、[**Create**] を選択して仮想マシン作成プロセスを開始します。

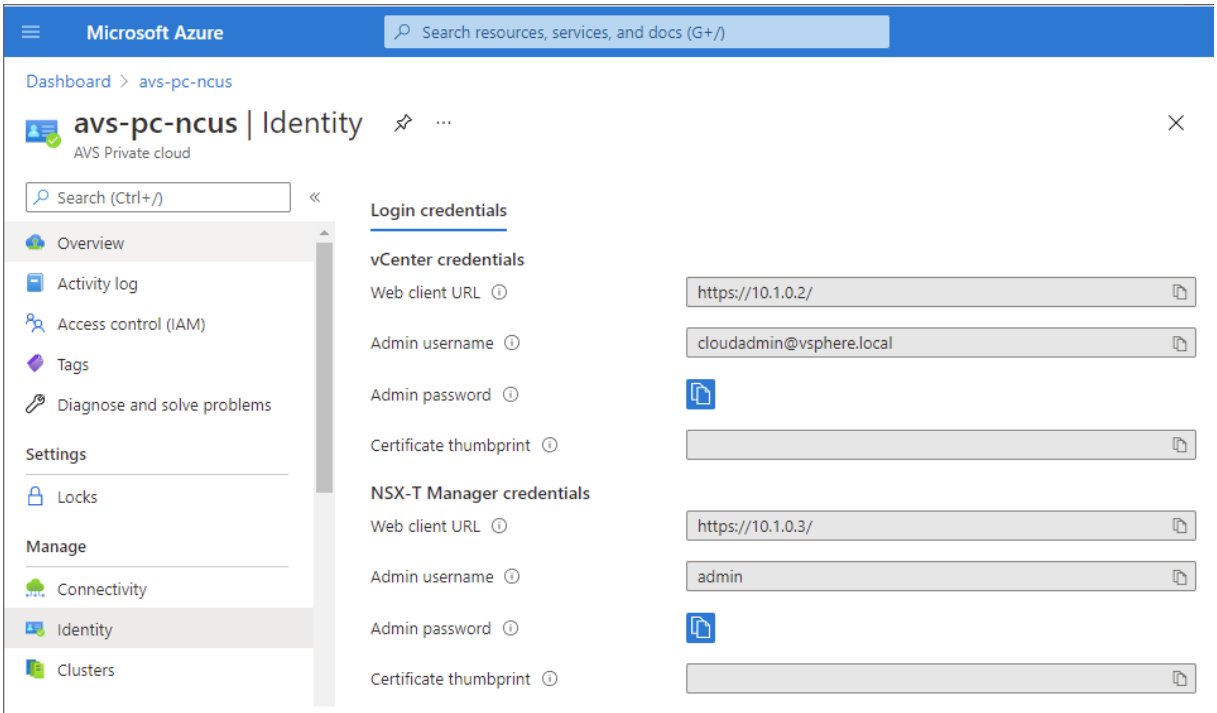
プライベートクラウドのローカル **vCenter** への接続

1. クラウド管理者として **vSphere Client with VMware vCenter SSO** にサインインします。



2. Azure Portal で、プライベートクラウドを選択してから、［**Manage**］**>**［**Identity**］を選択します。

プライベートクラウドの vCenter と NSX-T Manager について、URL、およびユーザーの資格情報が表示されます:



Display private cloud vCenter and NSX Manager URLs and credentials.

URL およびユーザーの資格情報を確認した後、次のことを行います:

1. 前の手順で作成した VM に移動し、その仮想マシンに接続します。
2. Windows VM で、ブラウザーを開き、2 つのブラウザータブで vCenter および NSX-T Manager の URL に移動します。[vCenter] タブで、前の手順のユーザー資格情報「*cloudadmin@vmcp.local*」を入力します。

Azure での **VMware** プライベートクラウドのネットワークの構成　ASV プライベートクラウドにアクセスした後、仮想ネットワークとゲートウェイを作成することでネットワークを構成します。

仮想ネットワークの作成

1. Azure Portal にサインインします。
2. 以前に作成したリソースグループに移動します。
3. [**+ Add**] を選択して新しいリソースを定義します。
4. [**Search the Marketplace**] ボックスに「*virtual network*」と入力します。仮想ネットワークリソースを見つけて選択します。
5. [**Virtual Network**] ページで、[**Create**] を選択してプライベートクラウドの仮想ネットワークをセットアップします。
6. [**Create Virtual Network**] ページで、仮想ネットワークの詳細を入力します。
7. [**Basics**] タブで、仮想ネットワークの名前を入力し、適切なリージョンを選択して、[**Next : IP Addresses**] をクリックします。
8. [**IP Addresses**] タブで、IPv4 アドレススペースの下に、以前に作成したアドレスを入力します。

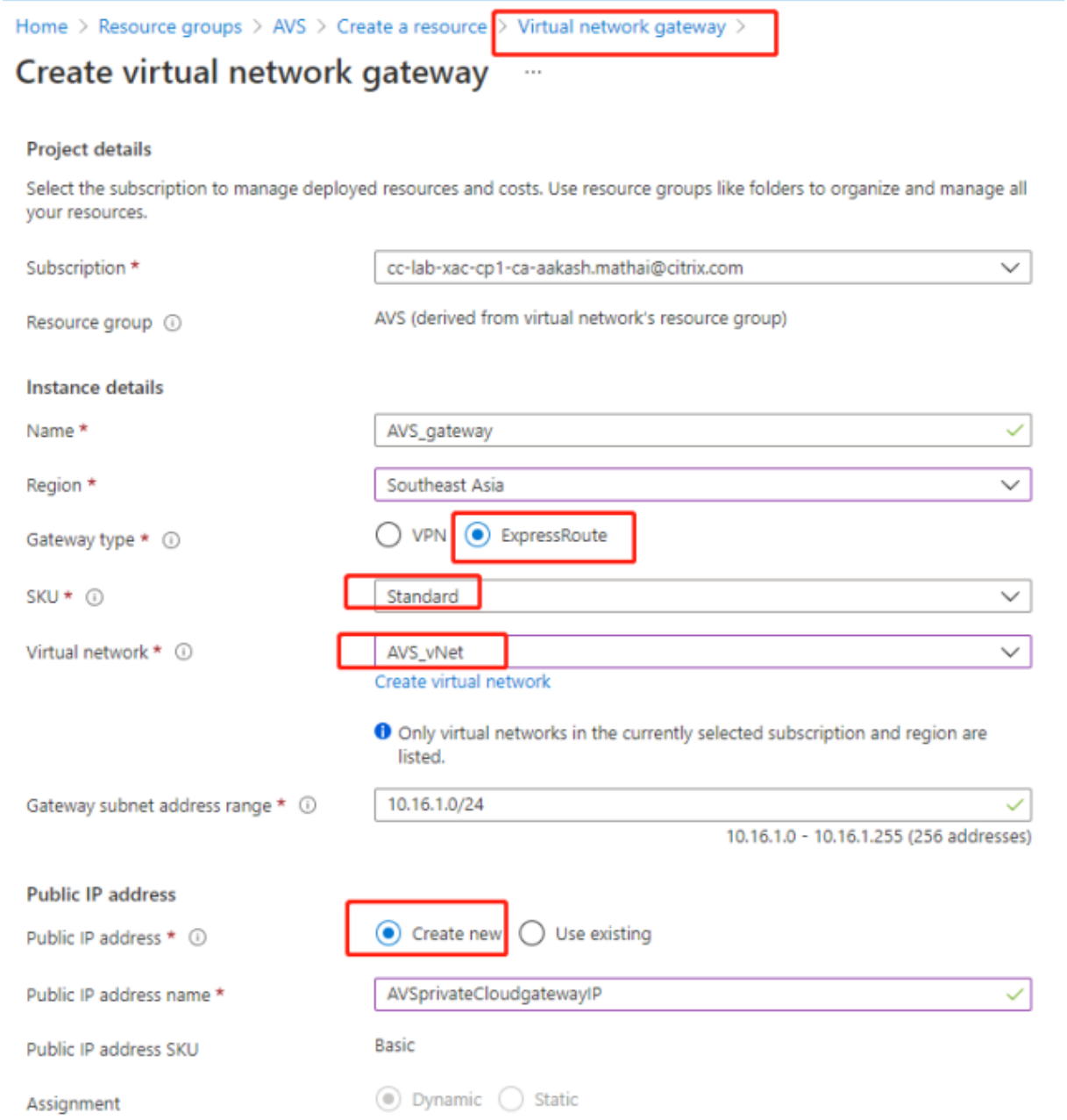
> 重要:
>
> プライベートクラウドの作成時に使用したアドレススペースと重複しないアドレスを使用してください。

アドレススペースに入った後、次のことを行います:

1. [**+ Add subnet**] を選択します。
2. [**Add subnet**] ページで、サブネットに名前と適切なアドレス範囲を指定します。
3. [追加] をクリックします。
4. [**Review + create**] を選択します。
5. 情報を確認し、[**Create**] をクリックします。展開が完了すると、仮想ネットワークがリソースグループに表示されます。

仮想ネットワークゲートウェイの作成　仮想ネットワークを作成したら、仮想ネットワークゲートウェイを作成します。

1. リソースグループで、[**+ Add**] を選択して新しいリソースを追加します。
2. [**Search the Marketplace**] ボックスに 「*virtual network gateway*」と入力します。仮想ネットワークリソースを見つけて選択します。
3. [**Virtual Network gateway**] ページで、[**Create**] をクリックします。
4. [**Create virtual network gateway**] ページの [**Basics**] タブで、フィールドに値を入力します。
5. [**Review + create**] をクリックします。

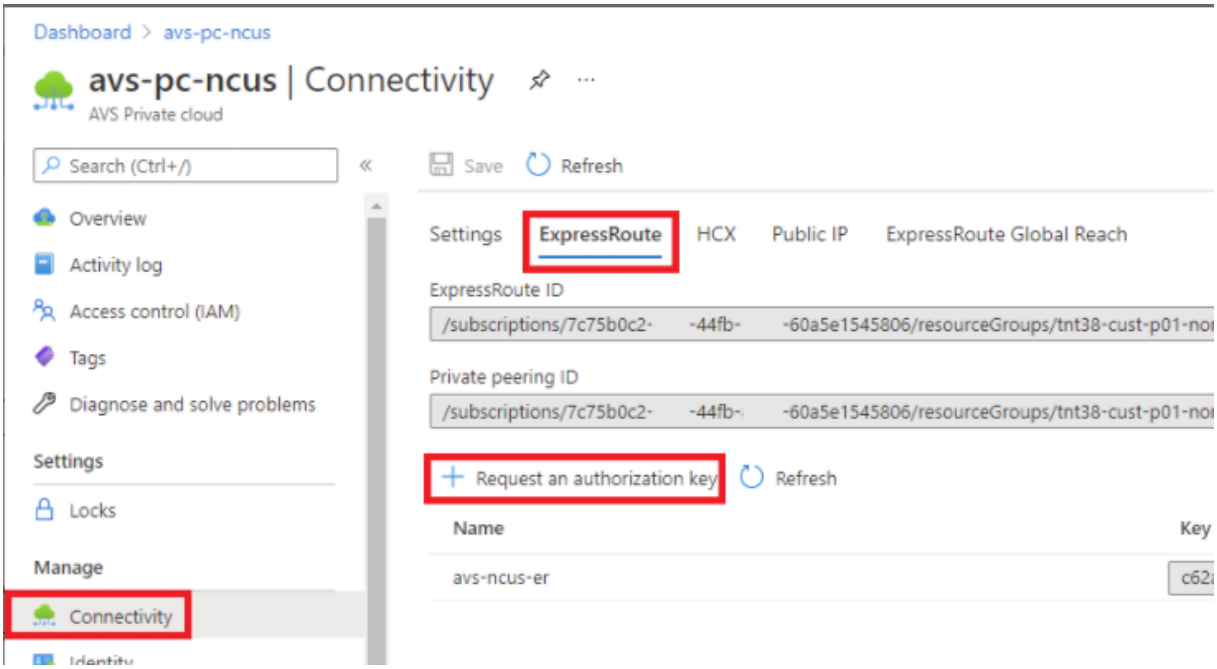


仮想ネットワークゲートウェイの構成を確認したら、[**Create**]をクリックして仮想ネットワークゲートウェイを展開します。
展開が完了したら、**ExpressRoute** を、Azure AVS プライベートクラウドを含む仮想ネットワークゲートウェイに接続します。

仮想ネットワークゲートウェイへの **ExpressRoute** の接続　仮想ネットワークゲートウェイを展開した後、仮想ネットワークゲートウェイと Azure AVS プライベートクラウドの間の接続を追加します:

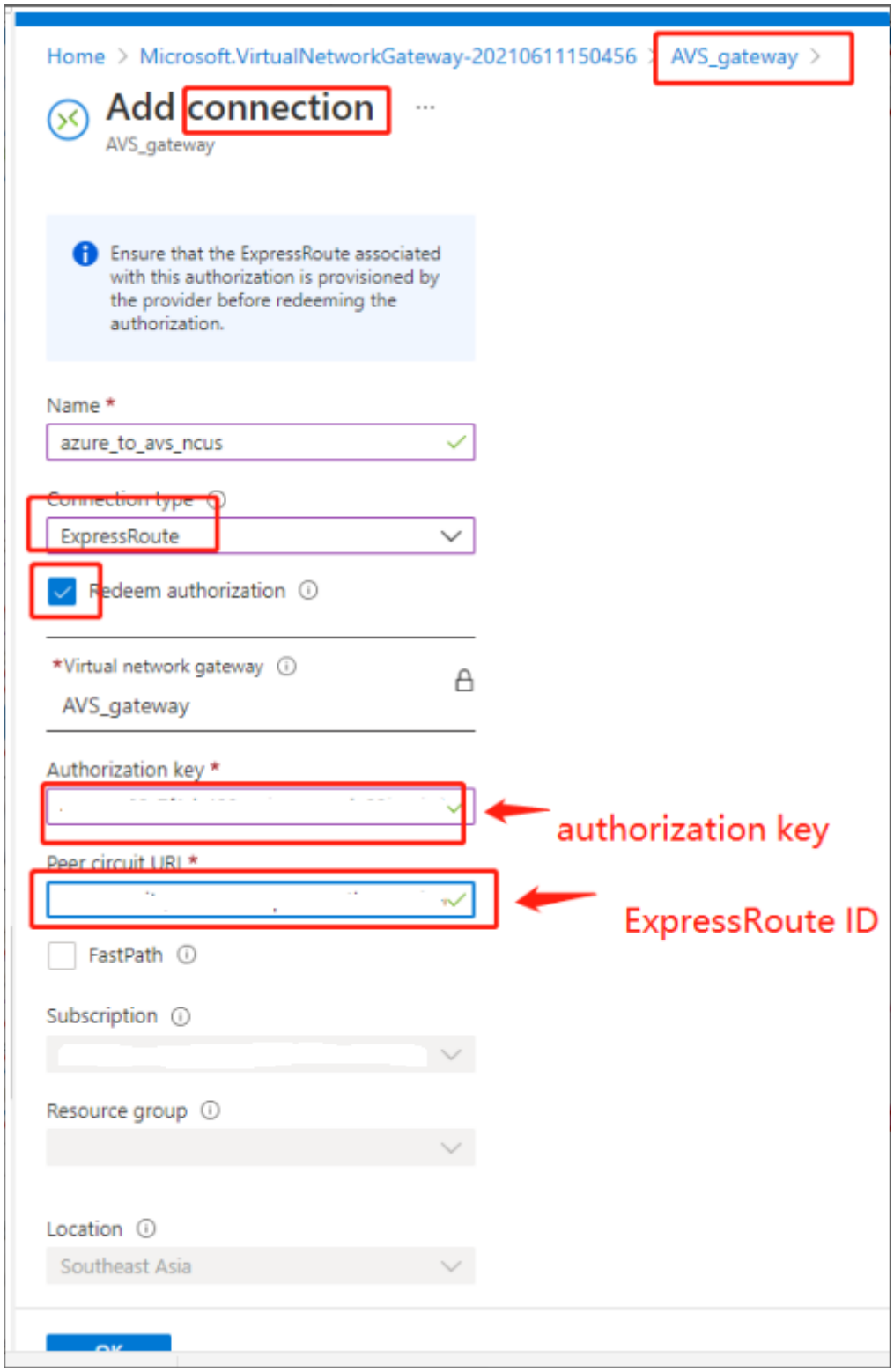
1. ExpressRoute 承認キーを要求します。

2. Azure Portal で、**Azure VMware Solution** プライベートクラウドに移動します。[**Manage**] > [**Connectivity**] > [**ExpressRoute**] を選択してから、[**+ Request an authorization key**] を選択します。

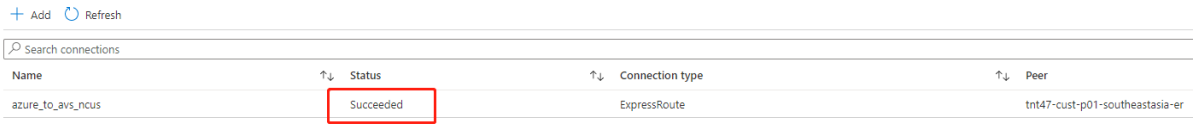


承認キーを要求した後、次のことを行います:

1. キーの名前を入力し、[**Create**] をクリックします。キーの作成には約 30 秒かかる場合があります。作成されると、新しいキーがプライベートクラウドの承認キーの一覧に表示されます。
2. その承認キーと **ExpressRoute ID** をコピーします。ピアリングプロセスを完了するためにそれらが必要になります。表示された承認キーはしばらくすると消えるので、表示されたらすぐにコピーします。
3. 使用する予定の仮想ネットワークゲートウェイに移動し、[**Connections> + Add**] を選択します。
4. [**Add connection**] ページで、フィールドに値を入力し、[**OK**] を選択します。



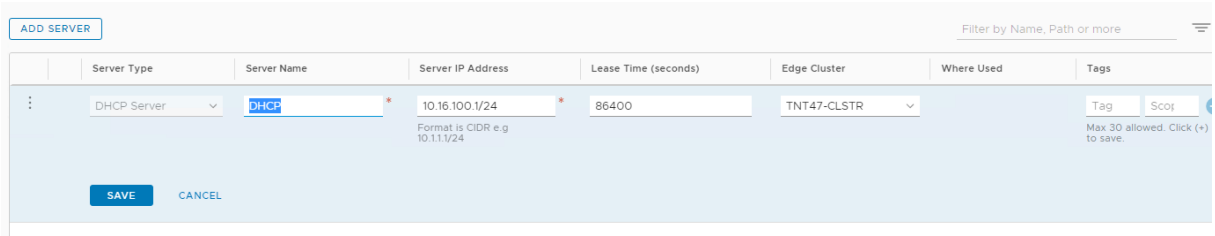
ExpressRoute 回線と仮想ネットワークの間に接続が確立されます:



Azure VMware Solution の **DHCP** の構成　ExpressRoute を仮想ゲートウェイに接続した後、DHCP を構成します。

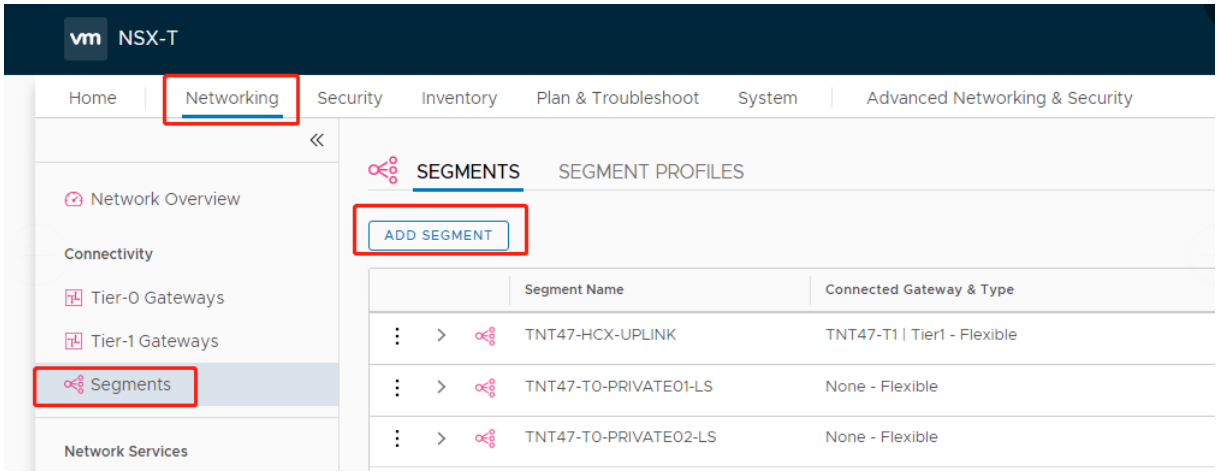
NSX-T の使用による **DHCP** サーバーのホスト　NSX-T Manager で、次のことを行います:

1. [**Networking**] > [**DHCP**] を選択してから、[**Add Server**] を選択します。
2. [**Server Type**] として [**DHCP**] を選択し、サーバー名と IP アドレスを入力します。
3. [保存] をクリックします。
4. [**Tier 1 Gateways**] を選択し、Tier-1 ゲートウェイの縦の省略記号を選択してから、[**Edit**] を選択します。
5. [**No IP Allocation Set**] を選択してサブネットを追加します。
6. [**Type**] として [**DHCP Local Server**] を選択します。
7. [**DHCP Server**] で、[**Default DHCP**] を選択してから、[**Save**] をクリックします。
8. もう一度 [**Save**] をクリックしてから、[**Close Editing**] を選択します。



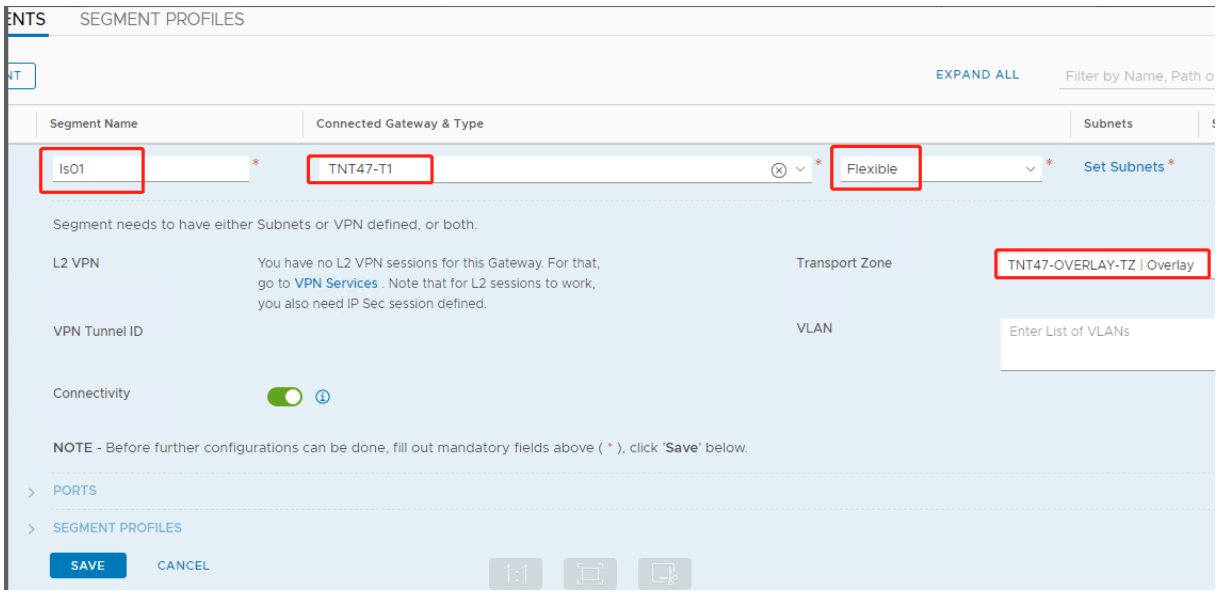
Azure VMware Solution へのネットワークセグメントの追加　DHCP をセットアップした後、ネットワークセグメントを追加します。

ネットワークセグメントを追加するには、NSX-T Manager で、[**Networking**] > [**Segments**] を選択してから [**Add Segment**] をクリックします。



[**Segments profile**] 画面で、次のことを行います:

1. セグメントの名前を入力します。
2. [**Connected Gateway**] として [**Tier-1 Gateway (TNTxx-T1)**] を選択し、[**Type**] を [**Flexible**] のままにします。
3. 事前設定されたオーバーレイ [**Transport Zone(TNTxx-OVERLAY-TZ)**] を選択します。
4. [**Set Subnets**] をクリックします。



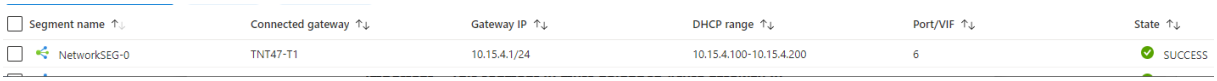
[**Azure ASV**] セクションで、次のことを行います:

1. ゲートウェイの IP アドレスを入力します。
2. [**Add**] を選択します。

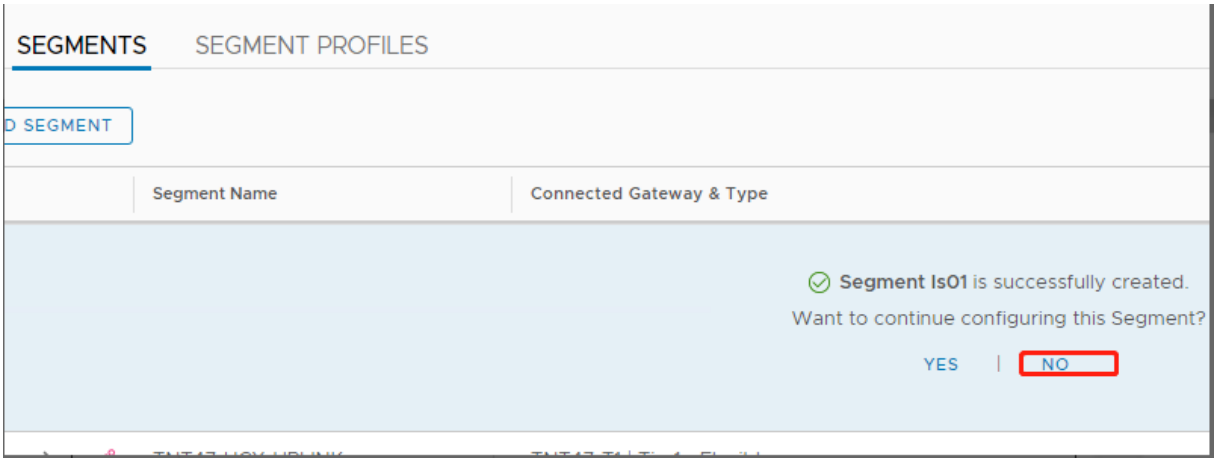
> 重要:
>
> このセグメント IP アドレスは、Azure ゲートウェイの IP アドレス（10.15.0.0/22）に属している必要があり

> ます。

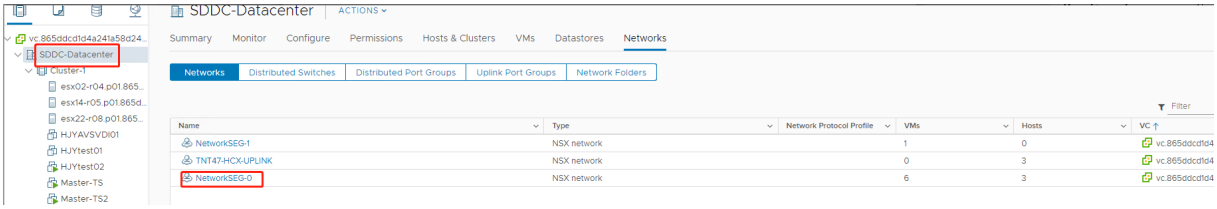
DHCP 範囲は、セグメント IP アドレスに属している必要があります:



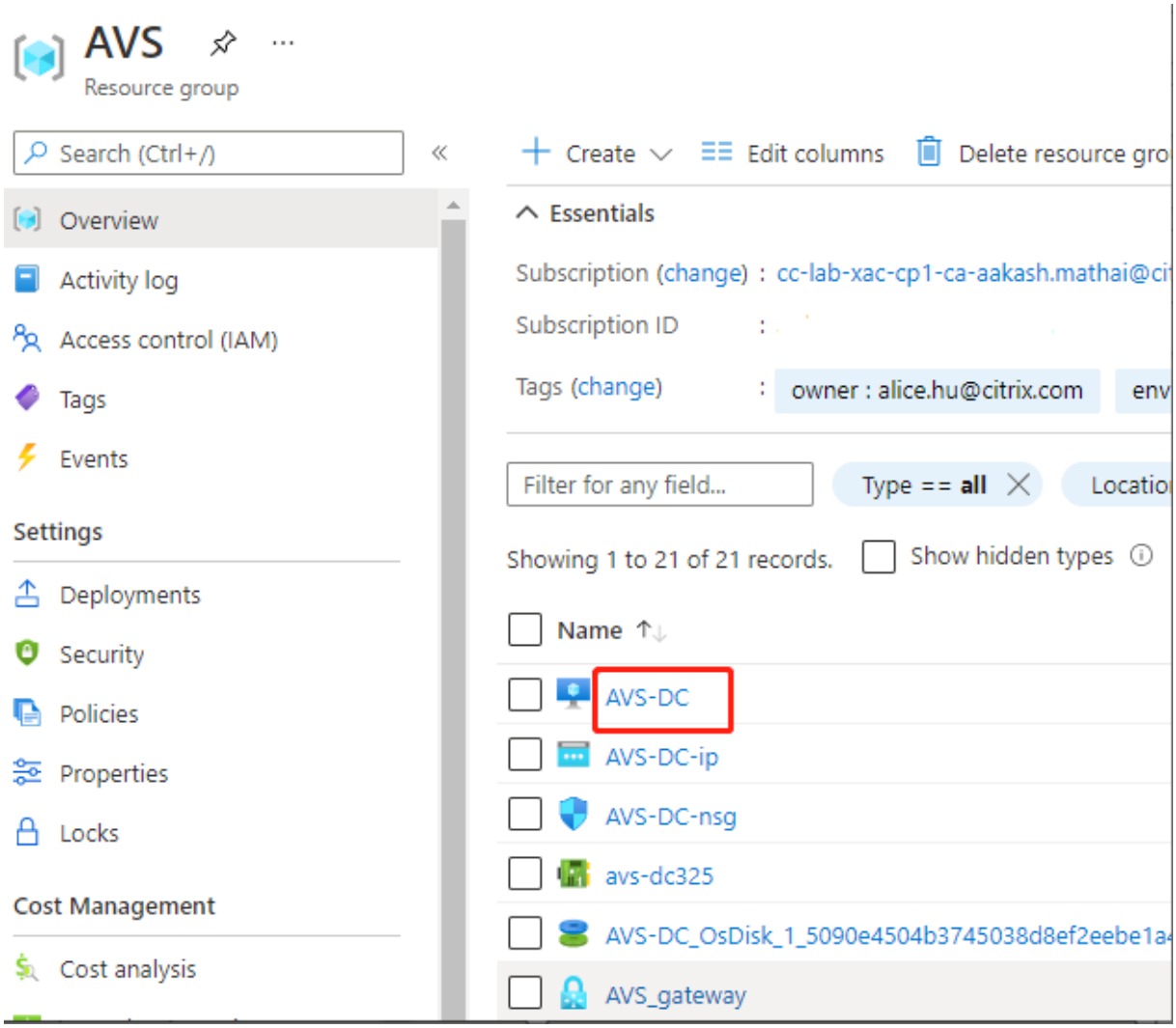
[**No**] を選択して、セグメントの構成を続行するオプションを拒否します:



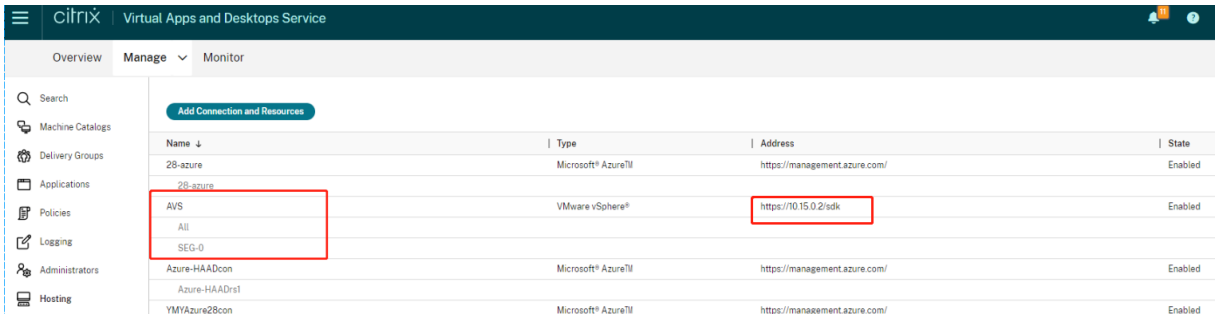
vCenter で、[**Networking**] > [**SDDC-Datacenter**] を選択します:



Azure AVS 環境の確認　Azure リソースグループで直接接続とコネクタをセットアップします:



vCenter の資格情報を使用して接続を確認します:



Google Cloud VMware Engine

Citrix Virtual Apps and Desktops を使用して、VMware ベースのオンプレミスの Citrix ワークロードを Google Cloud VMware Engine に移行できます。

Google Cloud VMware Engine の構成

次の手順では、Google Cloud VMware Engine でクラスターを取得して設定する方法について説明します。

VMware Engine ポータルへのアクセス

1. **Google Cloud** コンソールで、ナビゲーションメニューをクリックします。
2. [**Compute**] セクションで、[**VMware Engine**] をクリックして、新しいブラウザータブで VMware Engine を開きます。

最初のプライベートクラウドを作成するための要件　Google Cloud VMware Engine、使用可能な VMware Engine ノードクォータ、および適切な IAM 役割にアクセスできる必要があります。プライベートクラウドの作成を続行する前に、次の要件を準備してください:

1. API アクセス権とノードクォータを要求します。詳しくは、「API のアクセス権と割り当てのリクエスト」を参照してください。
2. VMware 管理アプライアンスと HCX 展開ネットワークに使用するアドレス範囲に注意してください。詳しくは、「ネットワーキングの要件」を参照してください。
3. VMware Engine Service Admin IAM 役割を取得します。

最初のプライベートクラウドの作成

1. VMware Engine ポータルにアクセスします。
2. VMware Engine のホームページで、[**Create a private cloud**] をクリックします。ホスティングの場所とハードウェアノードの種類が一覧表示されます。
3. プライベートクラウドのノード数を選択します。少なくとも 3 つのノードが必要です。
4. VMware 管理ネットワークのクラスレスドメイン間ルーティング（CIDR）範囲を入力します。
5. HCX 展開ネットワークの CIDR 範囲を入力します。

   > 重要:
   >
   > CIDR 範囲は、オンプレミスのサブネットまたはクラウドのサブネットと重複してはいけません。CIDR 範囲は、「/27」以上である必要があります。

6. [**Review and create**] を選択します。
7. 設定を確認します。設定を変更するには、[**Back**] をクリックします。
8. [**Create**] をクリックして、プライベートクラウドの作成を開始します。

VMware Engine は、新しいプライベートクラウドを作成するときに、いくつかの VMware コンポーネントを展開し、プライベートクラウド内のクラスターの初期の Autoscale ポリシーを設定します。プライベートクラウドの作成には、30 分～2 時間かかることがあります。プロビジョニングが完了すると、メールが届きます。

Google Cloud VMware Engine VPN Gateway のセットアップ　Google Cloud VMware Engine への初期接続を確立するために、VPN ゲートウェイを使用できます。これは OpenVPN ベースのクライアント VPN であり、これを使用して VMware Software Defined Data Center（SDDC）vCenter に接続し、必要な初期の構成を行うことができます。

VPN ゲートウェイを展開する前に、SDDC が展開されているリージョンの［**Edge Services**］範囲を構成します。これを行うには、以下の手順に従います：

1. **Google Cloud VMware Engine** ポータルにログオンし、［**Network**］**>**［**Regional Settings**］に移動します。［**Add Region**］をクリックします。
2. SDDC が展開されているリージョンを選択し、［**Internet Access**］と［**Public IP Service**］を有効にします。
3. 計画時にメモした［Edge Services］範囲を指定し、［**Submit**］をクリックします。これらのサービスを有効にするには、10〜15 分かかります。

   完了すると、［Regional Settings］ページの［Edge Services］が［**Enabled**］として表示されます。これらの設定を有効にすると、パブリック IP アドレスを SDDC に割り当てることができます。これは、VPN ゲートウェイを展開するための要件です。

VPN ゲートウェイを展開するには：

1. **Google Cloud VMware Engine** ポータルで、［**Network**］**>**［**VPN Gateways**］に移動します。［**Create New VPN Gateway**］をクリックします。
2. 計画時に用意した VPN ゲートウェイとクライアントサブネットの名前を指定します。［次へ］をクリックします。
3. VPN アクセスを許可するユーザーを選択します。［次へ］をクリックします。
4. VPN 経由でアクセスが必要なネットワークを指定します。［次へ］をクリックします。
5. 概要画面が表示されます。選択内容を確認し、［**Submit**］をクリックして VPN ゲートウェイを作成します。［VPN Gateways］ページが表示され、新しい VPN ゲートウェイのステータスが［**Creating**］として表示されます。
6. ステータスが［**Operational**］に変わったら、その新しい VPN ゲートウェイをクリックします。
7. ［**Download my VPN configuration**］をクリックして、VPN ゲートウェイ用に事前構成した OpenVPN プロファイルを含む ZIP ファイルをダウンロードします。UDP/1194 と TCP/443 を使用した接続のプロファイルを使用できます。基本設定を選択して、その設定を Open VPN にインポートし、接続します。
8. ［**Resources**］に移動し、SDDC を選択します。

VPN の接続

1. VPN ゲートウェイのセットアップを通じて、オンプレミスネットワークとプライベートクラウドの間にポイント対サイト接続を確立します。詳しくは、Google Cloud VMware Engine VPN Gateway のセットアップを参照してください。

2. 「Google Cloud VMware Engine VPN Gateway のセットアップ」でダウンロードした VPN 構成をアップロードします。
3. その VPN 構成を OpenVPN Connect などの VPN クライアントにインポートします。

詳しくは、VPN を使用した接続を参照してください。

最初のサブネットの作成

VMware Engine ポータルからの **NSX-T Manager** へのアクセス　サブネットを作成するプロセスは、VMware Engine を介してアクセスする NSX-T で行います。NSX-T Manager にアクセスするには、次の手順を実行します。

1. [**Google Cloud VMware Engine**] ポータルにログオンします。
2. メインナビゲーションから、[**Resources**] に移動します。
3. サブネットを作成するプライベートクラウドに対応するプライベートクラウド名をクリックします。
4. プライベートクラウドの詳細ページで、[**vSphere Management Network**] タブをクリックします。
5. NSX-T Manager に対応する **FQDN** をクリックします。
6. プロンプトが表示されたら、サインイン資格情報を入力します。vIDM を設定し、それを Active Directory などの ID ソースに接続している場合は、代わりに ID ソースの資格情報を使用してください。

> 注意：
>
> 生成された資格情報は、プライベートクラウドの詳細ページから取得できます。

サブネットの **DHCP** サービスのセットアップ　サブネットを作成する前に、DHCP サービスをセットアップします：

NSX-T Manager で、次のことを行います：

1. [**Networking**] **>** [**DHCP**] に移動します。ネットワークダッシュボードでは、1 つの Tier-0 ゲートウェイと、1 つの Tier-1 ゲートウェイが DHCP サービスによって作成されることが示されます。
2. DHCP サーバーのプロビジョニングを開始するには、[**Add Server**] をクリックします。
3. [**Server Type**] として [**DHCP**] を選択し、サーバー名と IP アドレスを入力します。
4. [**Save**] をクリックして、DHCP サービスを作成します。

この DHCP サービスを、関連する Tier-1 ゲートウェイに接続するには、次のことを行います：デフォルトの Tier-1 ゲートウェイは、DHCP サービスによって既にプロビジョニングされています：

1. [**Tier 1 Gateways**] を選択し、Tier-1 ゲートウェイの縦の省略記号を選択してから、[**Edit**] を選択します。
2. [**IP Address Management**] フィールドで、[**No IP Allocation Set**] を選択します。
3. [**Type**] として [**DHCP Local Server**] を選択します。

4. ［**DHCP Server**］用に作成した DHCP サーバーを選択します。
5. ［保存］をクリックします。
6. ［**Close Editing**］をクリックします。

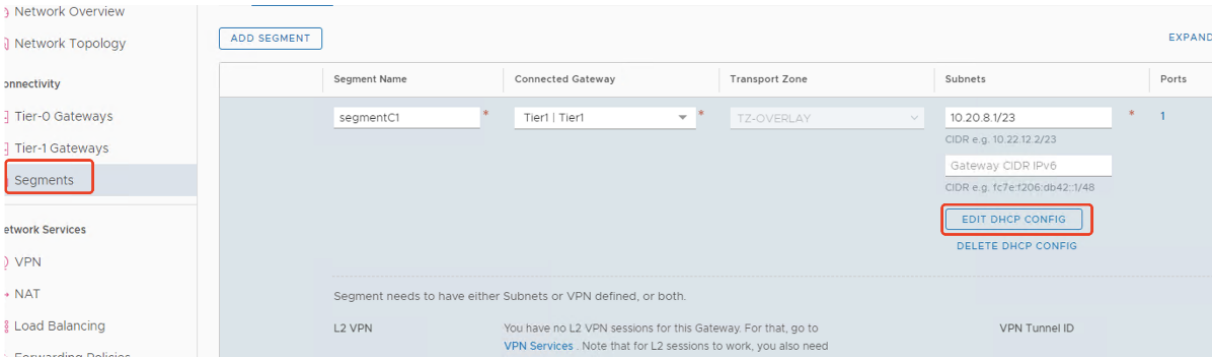
これで、NSX-T でネットワークセグメントを作成できます。NSX-T の DHCP について詳しくは、DHCP に関する VMware のドキュメントを参照してください。

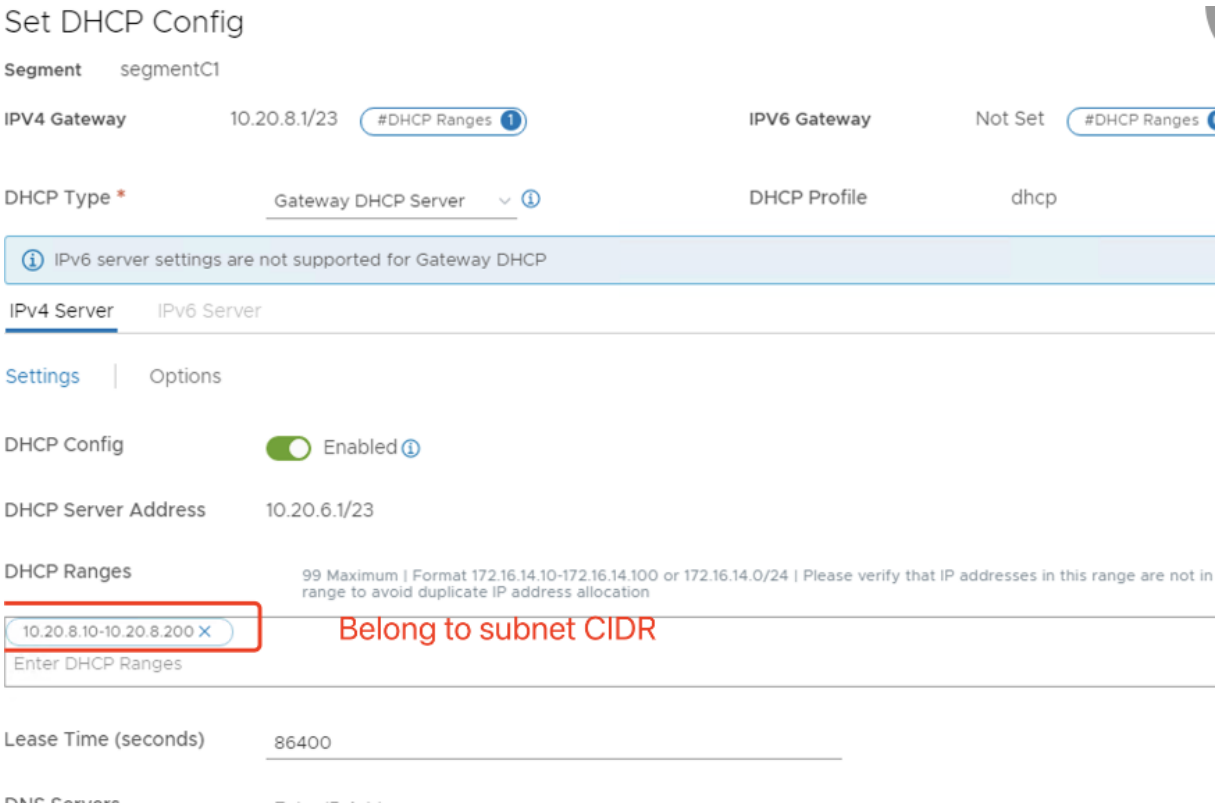
NSX-T でのネットワークセグメントの作成　ワークロード VM の場合、プライベートクラウドの NSX-T ネットワークセグメントとしてサブネットを作成します:

1. NSX-T Manager で、［**Networking**］**>**［**Segments**］に移動します。
2. ［**Add Segment**］をクリックします。
3. セグメントの名前を入力します。
4. ［**Connected Gateway**］として ［**Tier-1**］を選択し、［Type］を ［**Flexible**］のままにします。
5. ［**Set Subnets**］をクリックします。
6. ［**Add Subnets**］をクリックします。
7. ［**Gateway IP/Prefix Length**］にサブネット範囲を入力します。最後のオクテットとして「**.1**」を付けて、サブネット範囲を指定します。例：**10.12.2.1/24**。
8. DHCP 範囲を指定し、［**ADD**］をクリックします。
9. ［**Transport Zone**］のドロップダウンリストで ［**TZ-OVERLAY**］を選択します。
10. ［保存］をクリックします。VM を作成する際、vCenter でこのネットワークセグメントを選択できるようになりました。

特定のリージョンでは、プライベートサービスアクセス権を使用して、VMware Engine から VPC ネットワークに一意のルートを最大 100 個設定できます。これには、たとえば、プライベートクラウド管理の IP アドレス範囲、NSX-T ワークロードネットワークセグメント、および HCX ネットワーク IP アドレス範囲が含まれます。この制限には、リージョン内のすべてのプライベートクラウドが含まれます。

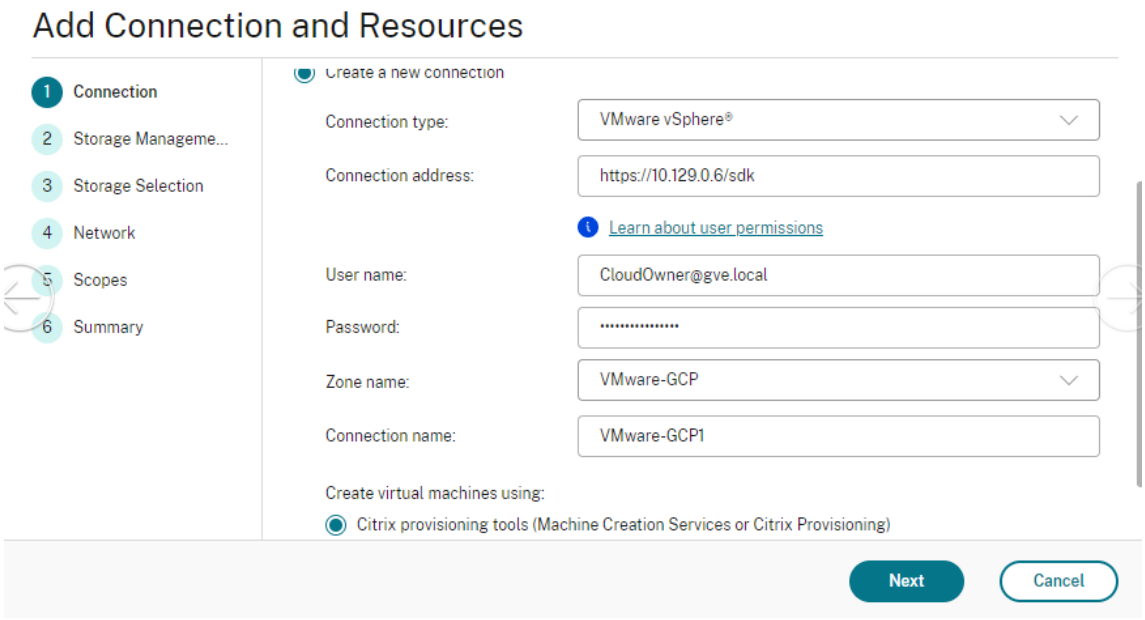
> 注:
>
> DHCP 範囲設定を数回構成する必要があることによる、Google Cloud の構成の問題があります。そのため、必ず Google Cloud を構成した後に DHCP 範囲を構成してください。［**EDIT DHCP CONFIG**］をクリックして、DHCP 範囲を構成します。





Citrix Studio での **Google Cloud VMware** 接続の作成

1. vCenter にマシンを作成します。
2. Citrix Studio を起動します。
3. ホスティングノードを選択し、［接続およびリソースの追加］をクリックします。
4. ［接続］画面で ［新しい接続を作成する］を選択し、次のことを行います:



a) ［接続の種類］で ［**VMware vSphere**］を選択します。
b) ［接続アドレス］に、vCenter プライベート IP アドレスを入力します。
c) vCenter の資格情報を入力します。
d) 接続名を入力します。
e) 仮想マシンを作成するツールを選択します。

5. ［ネットワーク］画面で、NSX-T サーバーで作成したサブネットを選択します。
6. ウィザードを完了します。

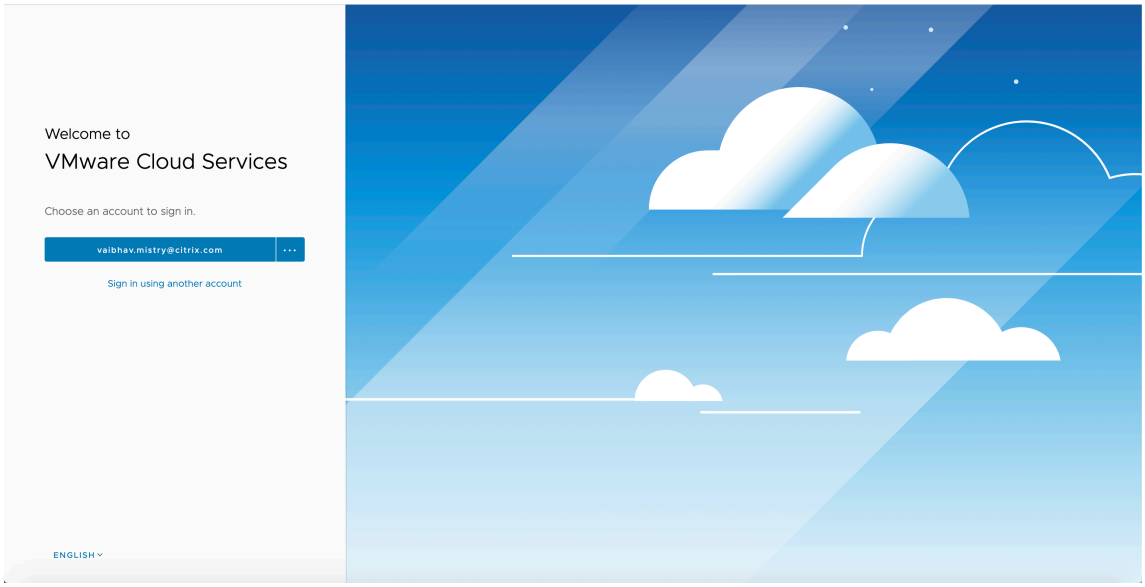
VMware Cloud on AWS（Amazon Web Services）

VMware Cloud on AWS（Amazon Web Services）を使用すると、VMware ベースのオンプレミスの Citrix ワークロードを AWS Cloud に移行できます。

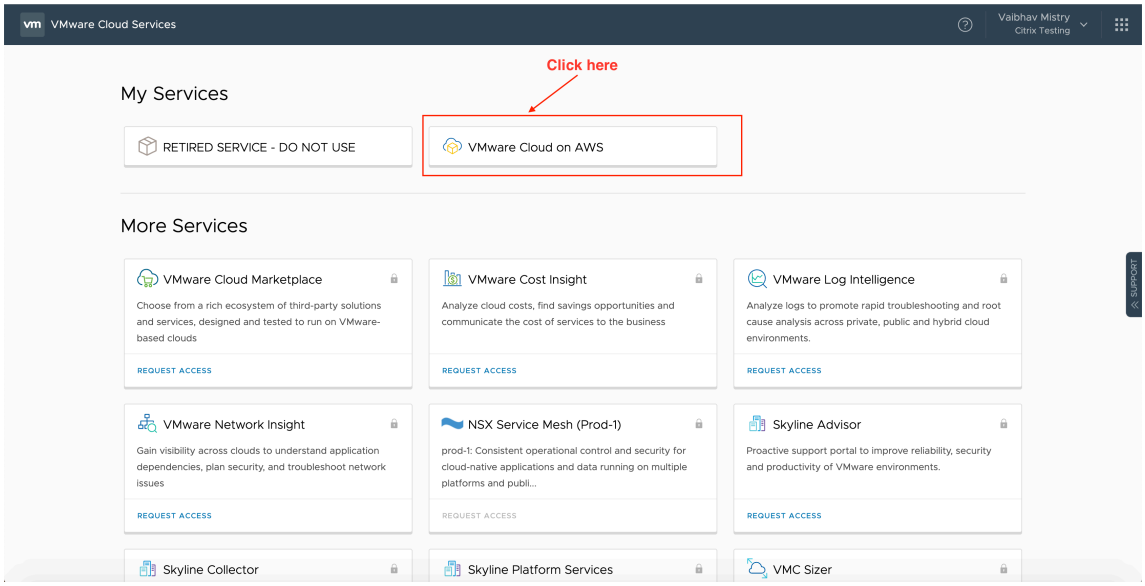
この記事では、VMware Cloud on AWS をセットアップする手順について説明します。

VMware クラウド環境へのアクセス

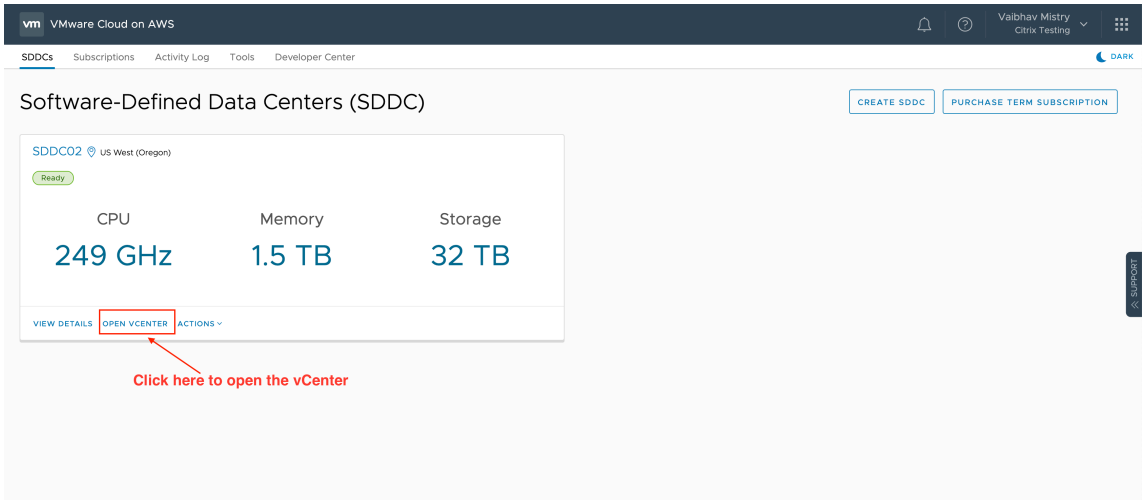
1. URL「https://console.cloud.vmware.com/」を使用して、VMware Cloud サービスにログインします。

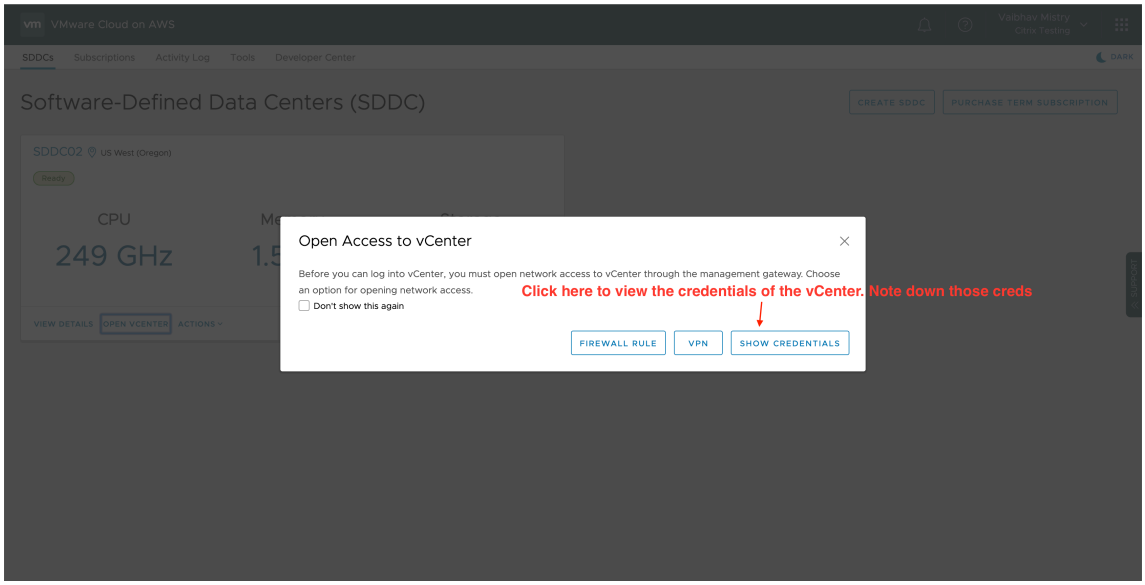


2. [**VMware Cloud on AWS**] をクリックします。ソフトウェア定義データセンター（SDDC：Software-Defined Data Centers）ページが表示されます。

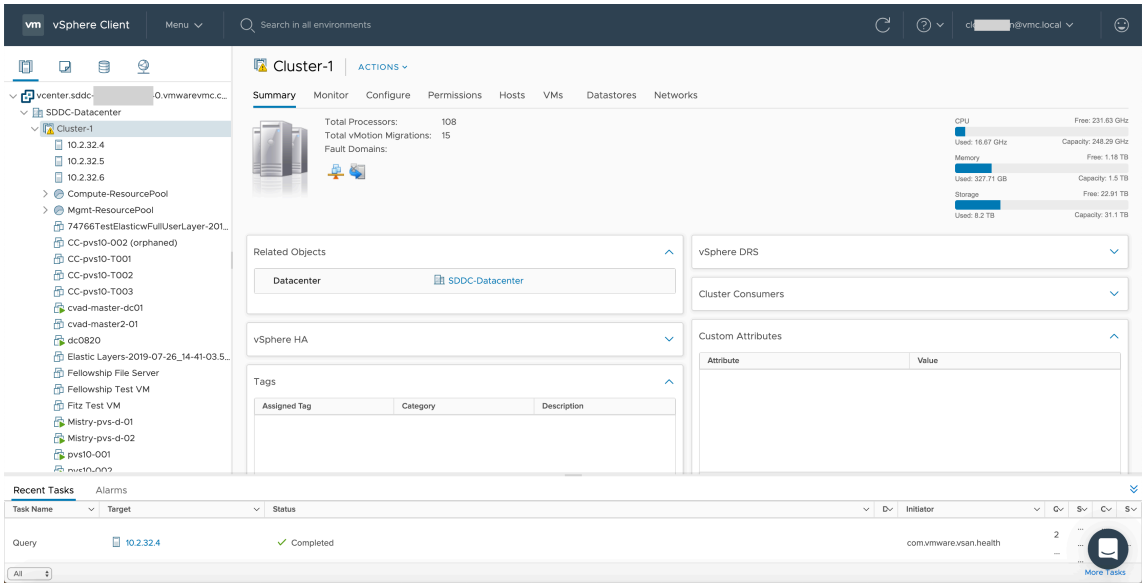


3. [**OPEN VCENTER**] をクリックしてから、[**SHOW CREDENTIALS**] をクリックします。後で使用するために資格情報をメモしておきます。





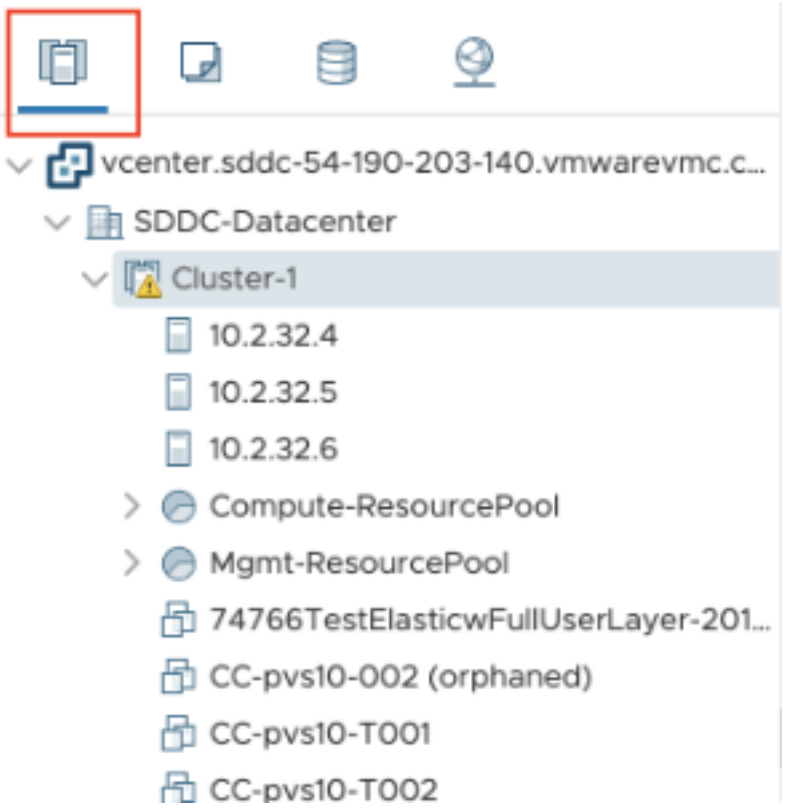
4. Web ブラウザーを開き、vSphere Web Client の URL を入力します。
5. メモした資格情報を入力し、［**Login**］をクリックします。vSphere クライアントの Web ページは、オンプレミス環境に似ています。



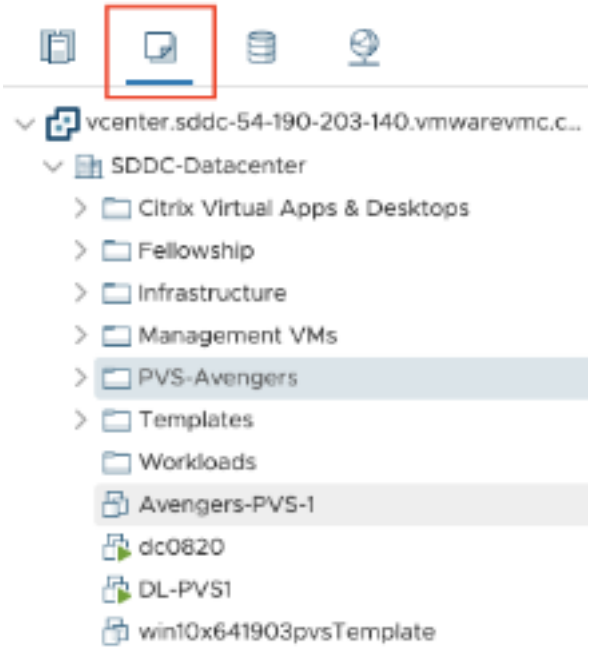
VMware クラウド環境について

vSphere クライアントの Web ページには 4 つのビューがあります。

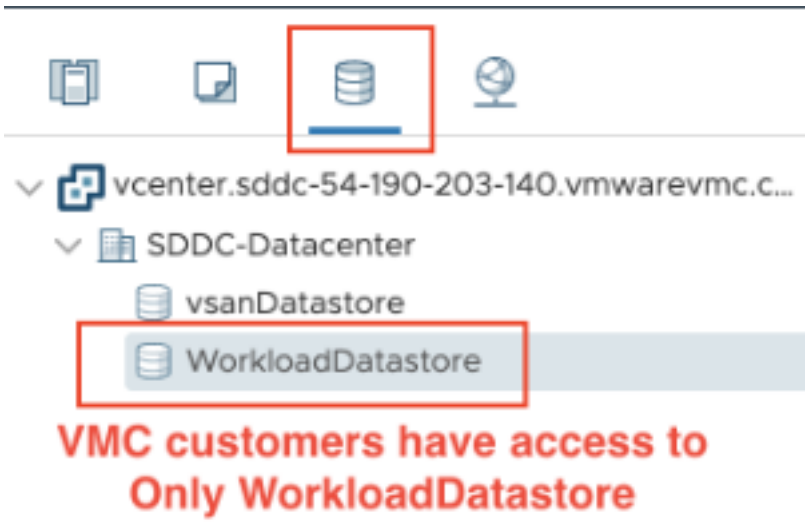
- Host and Cluster ビュー：新しい Cluster を作成することはできませんが、クラウド管理者は複数のリソースプールを作成できます。



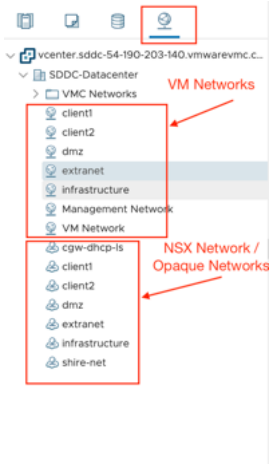
- VM and Template ビュー：クラウド管理者は多くのフォルダーを作成できます。



- Storage ビュー：Citrix Studio にホスティングユニットを追加する場合は、Workload Datastore にしかアクセスできないため、**WorkloadDatastore** ストレージを選択します。



- Network ビュー：VMware Cloud ネットワークと不透明ネットワークでアイコンが異なります。



クラスターをセットアップした後、接続とリソースの追加については、「VMware 仮想化環境」を参照してください。

次の手順

- コアコンポーネントのインストール
- VDA のインストール
- サイトの作成

- 接続の作成と管理については、「VMware クラウドおよびパートナーソリューションへの接続」を参照してください。

追加情報

- 接続とリソースの作成と管理
- マシンカタログの作成

コアコンポーネントのインストール

August 17, 2024

> 重要:
>
> Citrix は、ライセンスコンプライアンスを含む正当な利益のために、必要に応じて基本的なライセンスデータを収集します。詳しくは、「Citrix ライセンスデータ」を参照してください。

コアコンポーネントとは、Citrix Delivery Controller、Citrix Studio、Web Studio、Citrix Director、Citrix ライセンスサーバーのことを指します。

> 注:
>
> Citrix Studio は、オンプレミスの Citrix Virtual Apps and Desktops 環境を構成および管理する Windows ベースの管理コンソールです。Web Studio は次世代の Citrix Studio であり、Citrix Studio と完全に同等の機能を提供する Web ベースの管理コンソールです。Web Studio について詳しくは、「Web Studio のインストール」を参照してください。

(2003 より前のバージョンでは、Citrix StoreFront もコアコンポーネントに含まれていました。引き続き、[**Citrix StoreFront**] タイルをクリックするか、インストールメディアでコマンドを実行して StoreFront をインストールすることができます。)

インストールを始める前に、本記事と「インストールの準備」を確認してください。

この記事では、コアコンポーネントをインストールする場合のインストールウィザードの手順を説明します。同等の機能を持つコマンドラインが用意されています。詳しくは、「コマンドラインを使ったインストール」を参照してください。

手順 **1**: 製品ソフトウェアをダウンロードしてウィザードを起動する

Citrix アカウント資格情報を使用して、Citrix Virtual Apps and Desktops のダウンロードページにアクセスします。製品の ISO ファイルをダウンロードします。

ファイルを解凍します。必要な場合は、ISO ファイルから DVD を作成します。

ローカルの管理者アカウントを使って、コアコンポーネントのインストール先マシンにログオンします。

DVD をドライブに挿入するか、ISO ファイルをマウントします。インストーラーが自動的に起動しない場合は、**AutoSelect** アプリケーションまたはマウントされたドライブをダブルクリックします。

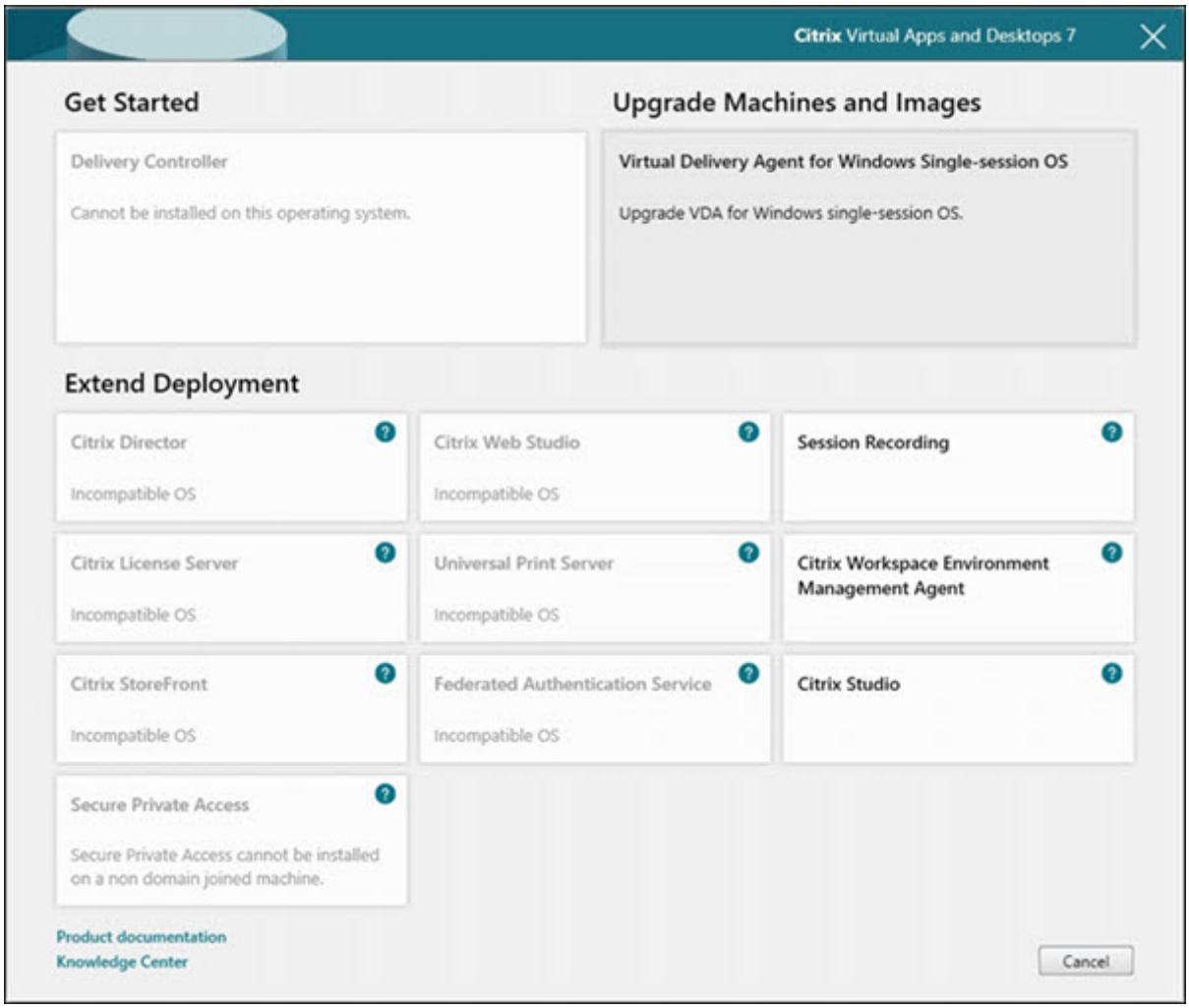
手順 **2**：インストールする製品を選択する

インストールする製品（Virtual Apps または Virtual Apps and Desktops）の隣にある ［開始］をクリックします。

（マシンに Citrix Virtual Apps and Desktops コンポーネントが既にインストールされている場合、このページは表示されません。）

コマンドラインオプション：/xenappを使用して Citrix Virtual Apps をインストールします。オプションを指定しない場合、Citrix Virtual Apps and Desktops がインストールされます。

手順 **3**：インストールするものを選択する

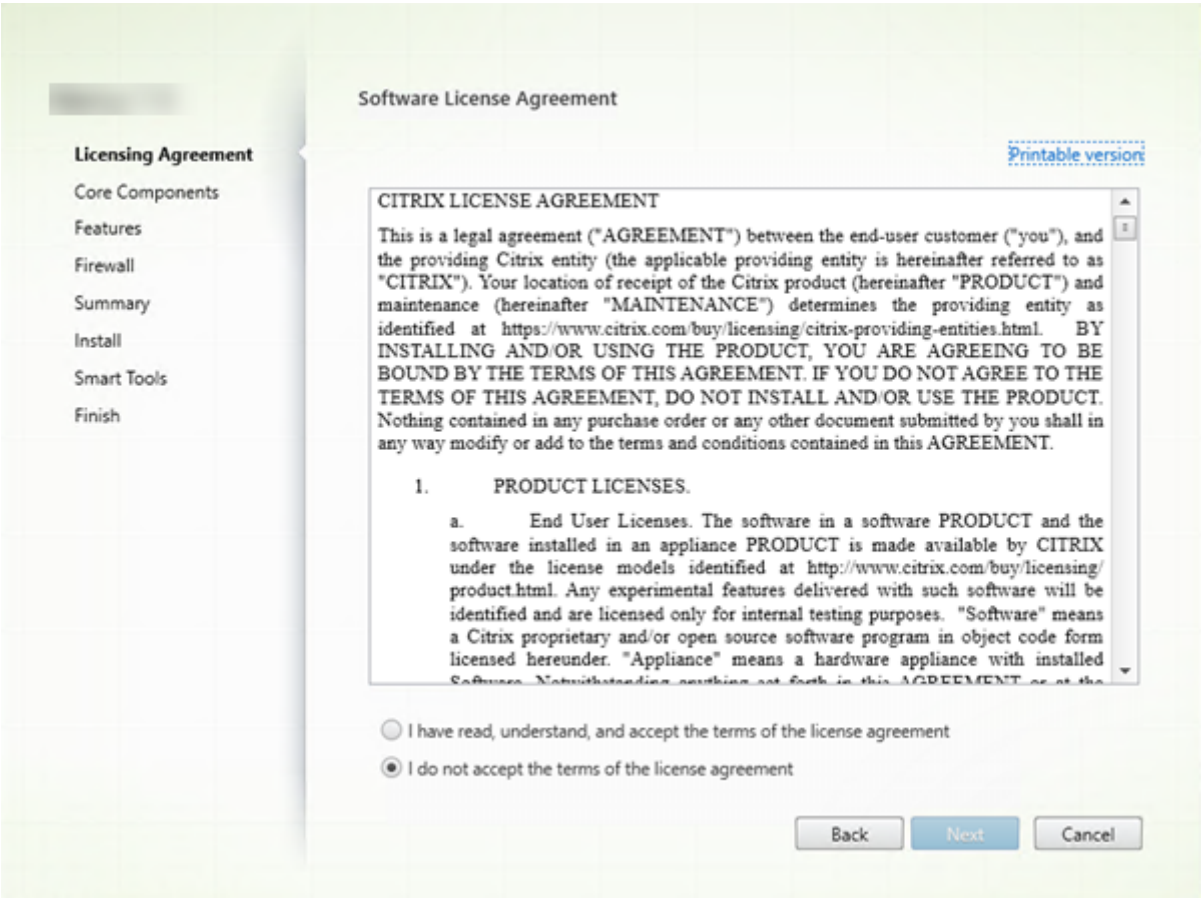


製品を初めてインストールする場合は、[**Delivery Controller**] をクリックします（後のページで、このマシンにインストールする特定のコンポーネントを選択します）。

Controller が（このマシンまたは別のマシンに）既にインストールされていて、別のコンポーネントをインストールする場合は、[拡張展開] セクションからコンポーネントを選択します。

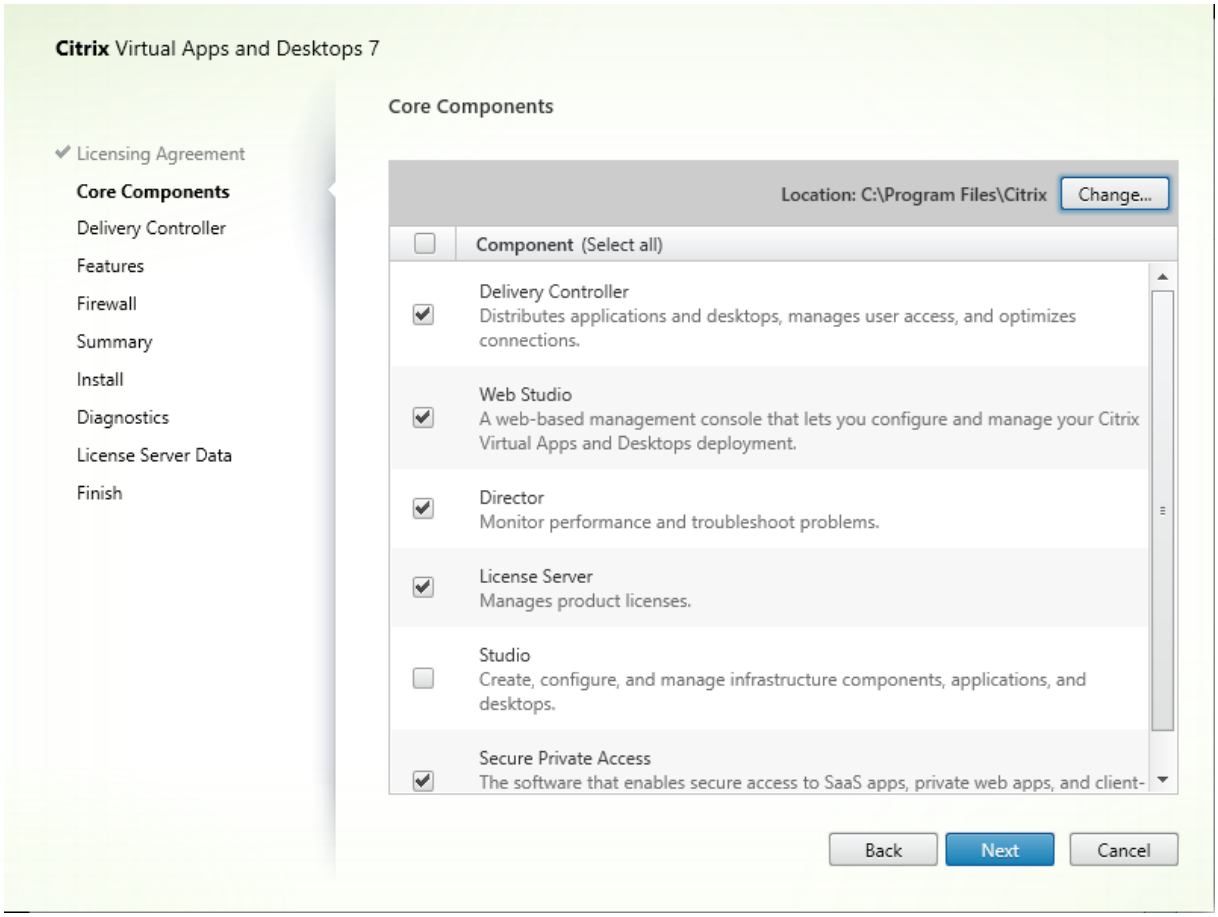
コマンドラインオプション：`/components`

手順 **4**：ライセンス契約書を読み、同意する



［ライセンス契約］ページで、ライセンス契約を読み、読んで同意したことを明示します。［次へ］をクリックします。

手順 **5**：インストールするコンポーネントおよびインストール場所を選択する



［コアコンポーネント］ページで次の作業を行います：

- 場所：デフォルトでは、`C:\Program Files\Citrix`に各コンポーネントがインストールされます。ほとんどの展開ではデフォルトで十分です。別の場所を指定する場合は、Network Service アカウントでの実行権限が必要です。
- コンポーネント：デフォルトでは、すべてのコアコンポーネントのチェックボックスがオンになっています。1 つのサーバー上にすべてのコアコンポーネントをインストールすることは、概念実証展開、テスト展開、または小規模実稼働展開には十分です。より大きな稼働環境では、Director、StoreFront、Secure Private Access、および License Server を別々のサーバーにインストールすることをお勧めします。

  > 注：
  >
  > コンポーネントを複数のサーバーにインストールする場合は、他のサーバーに他のコンポーネントをインストールする前に、まず Citrix ライセンスサーバーとライセンスをインストールしてください。ガイダンスについては、「Citrix Virtual Apps and Desktops ライセンスガイド」の「自動インストール」セクションを参照してください。

  このマシン上で必要なコアコンポーネントをインストールしないように選択すると、アイコンの警告が表示さ

れます。この警告では、このマシンでは不要であるにもかかわらず、このコンポーネントをインストールするように通知されます。

［次へ］をクリックします。

コマンドラインオプション：/installdir、/components、/exclude

ハードウェアチェック

Delivery Controller をインストールまたはアップグレードすると、ハードウェアがチェックされます。マシンの RAM が推奨容量（5GB）未満である場合、インストーラーで通知されます。推奨容量に達していないと、サイトの安定性に影響を与える可能性があります。詳しくは、「ハードウェア要件」を参照してください。

グラフィカルインターフェイス：ダイアログボックスが表示されます。

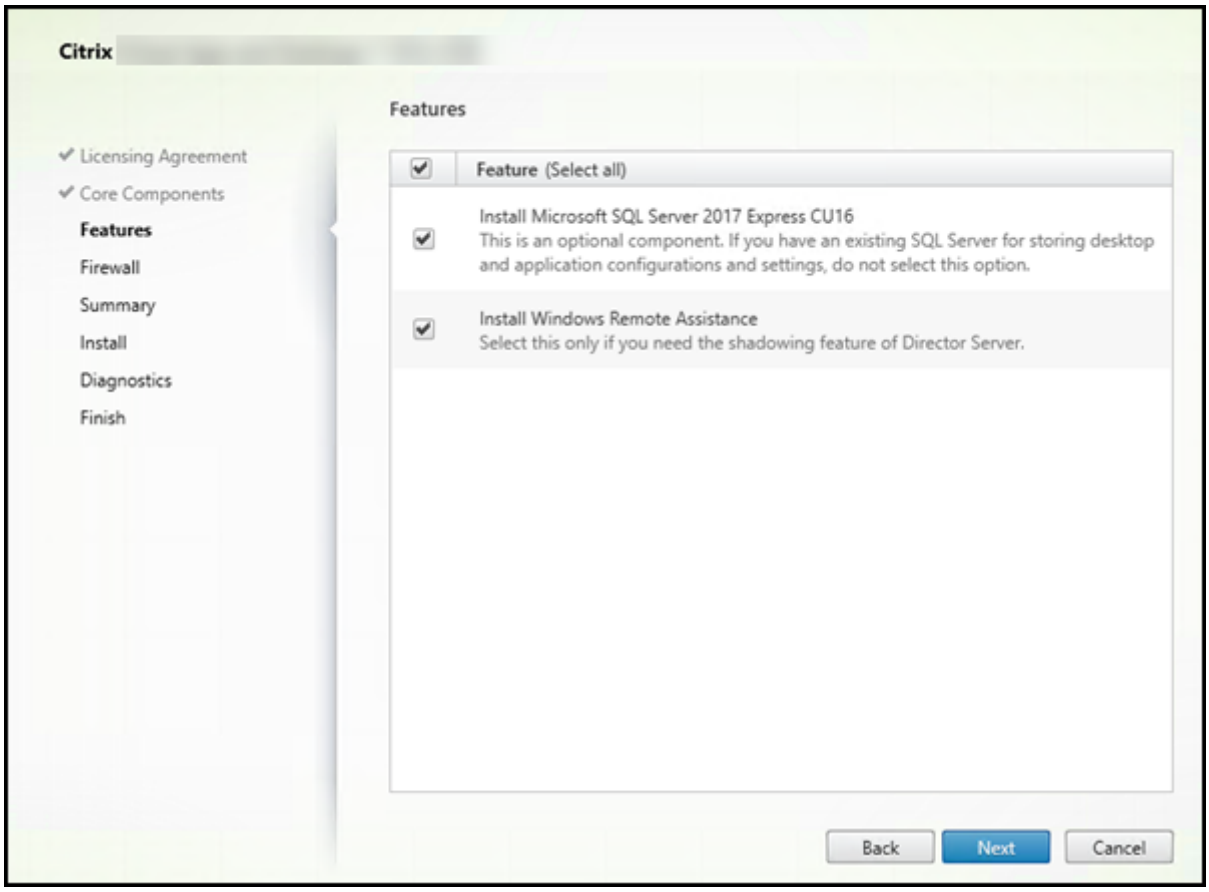
- 推奨：［キャンセル］をクリックしてインストールを停止します。マシンに RAM を追加してから、インストールを再開します。
- または、［次へ］をクリックしてインストールを続行します。サイトの安定性に問題がある可能性があります。

コマンドラインインターフェイス：インストールまたはアップグレードが終了します。インストールログに、検出された内容と使用可能なオプションを説明するメッセージが出力されます。

- 推奨：マシンに RAM を追加してから、コマンドを再実行します。
- または、/ignore_hw_check_failureオプションを使用してコマンドを再実行して、警告を無視します。サイトに安定性の問題がある可能性があります。

アップグレード時に、OS または SQL Server のバージョンがサポートされなくなった場合にも通知が表示されます。「環境のアップグレード」を参照してください。

手順 **6**：機能を有効または無効にする



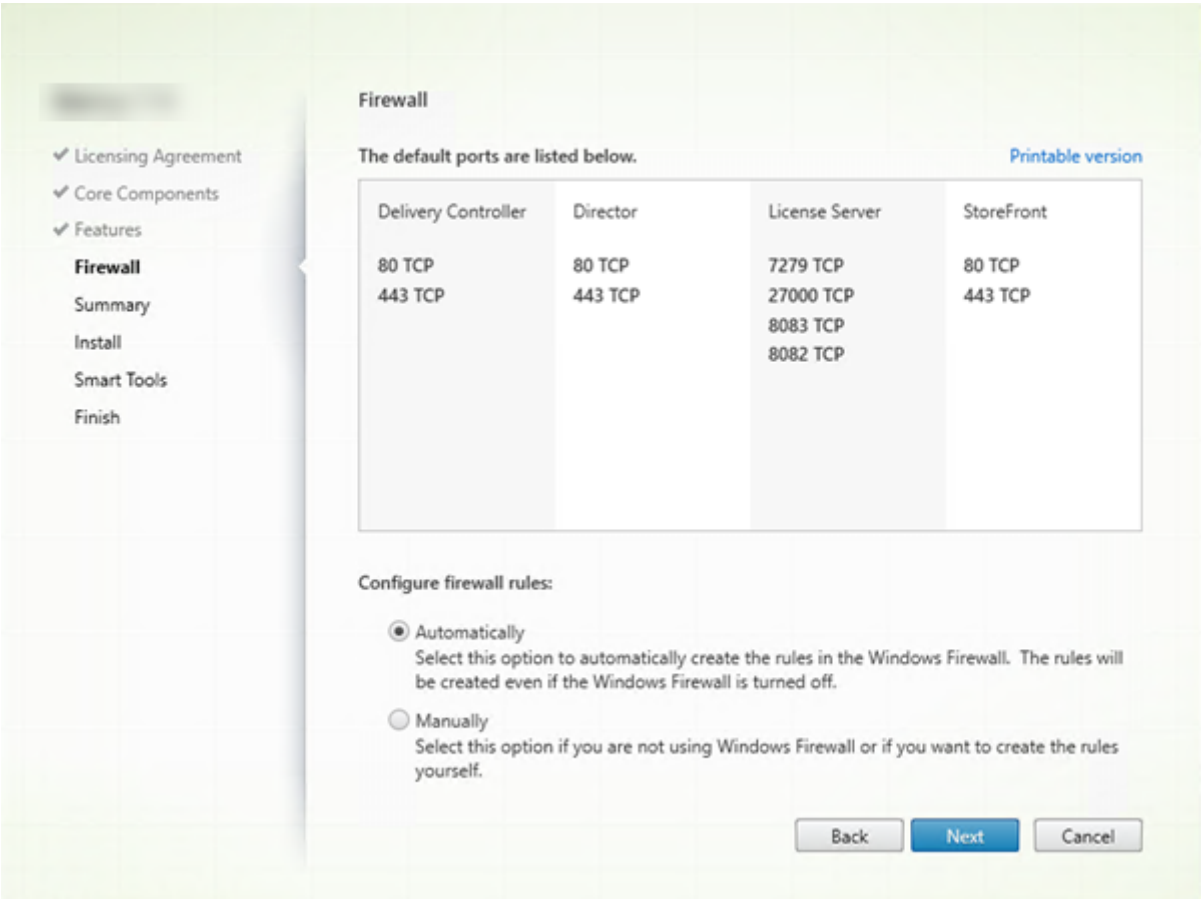
［機能］ページで次の作業を行います：

- Microsoft SQL Server Express をサイトデータベースとして使用するためにインストールするかどうかを選択します。デフォルトでは、これはオンになっています。Citrix Virtual Apps and Desktops のデータベースについて詳しくは、「データベース」を参照してください。
- Director をインストールすると、Windows リモートアシスタンスも自動的にインストールされます。Director ユーザーのシャドウで使用するために Windows リモートアシスタンスのシャドウ機能を有効にするかどうかを選択します。シャドウ機能を有効にすると、TCP ポート 3389 が開きます。この機能は、デフォルトで有効になります。ほとんどの展開ではデフォルト設定で十分です。この機能は Director のインストール時のみ表示されます。

［次へ］をクリックします。

コマンドラインオプション：`/nosql`（インストールを阻止するため）、`/no_remote_assistance`（有効化を阻止するため）

手順 **7**：**Windows** ファイアウォールポートを開放する



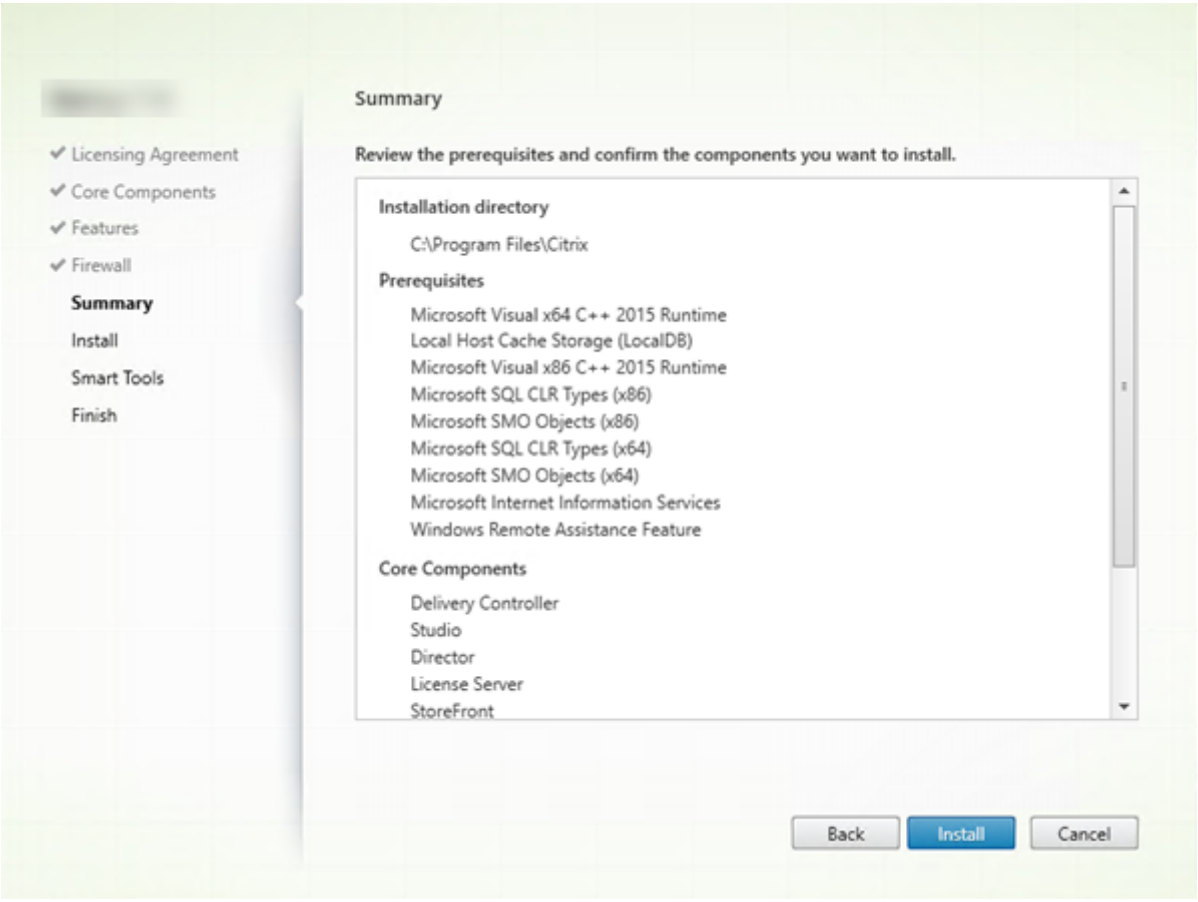
Windows ファイアウォールサービスが実行されている場合、ファイアウォールが無効になっていても、デフォルトで ［ファイアウォール］ページに示されているポートが自動的に開放されます。ほとんどの展開ではデフォルト設定で十分です。ポートについて詳しくは、「ネットワークポート」を参照してください。

［次へ］をクリックします。

（この図は、すべてのコアコンポーネントをこのマシンにインストールした場合のポート一覧を示します。このようなタイプのインストールは、通常テスト展開でのみ行われます）。

コマンドラインオプション：`/configure_firewall`

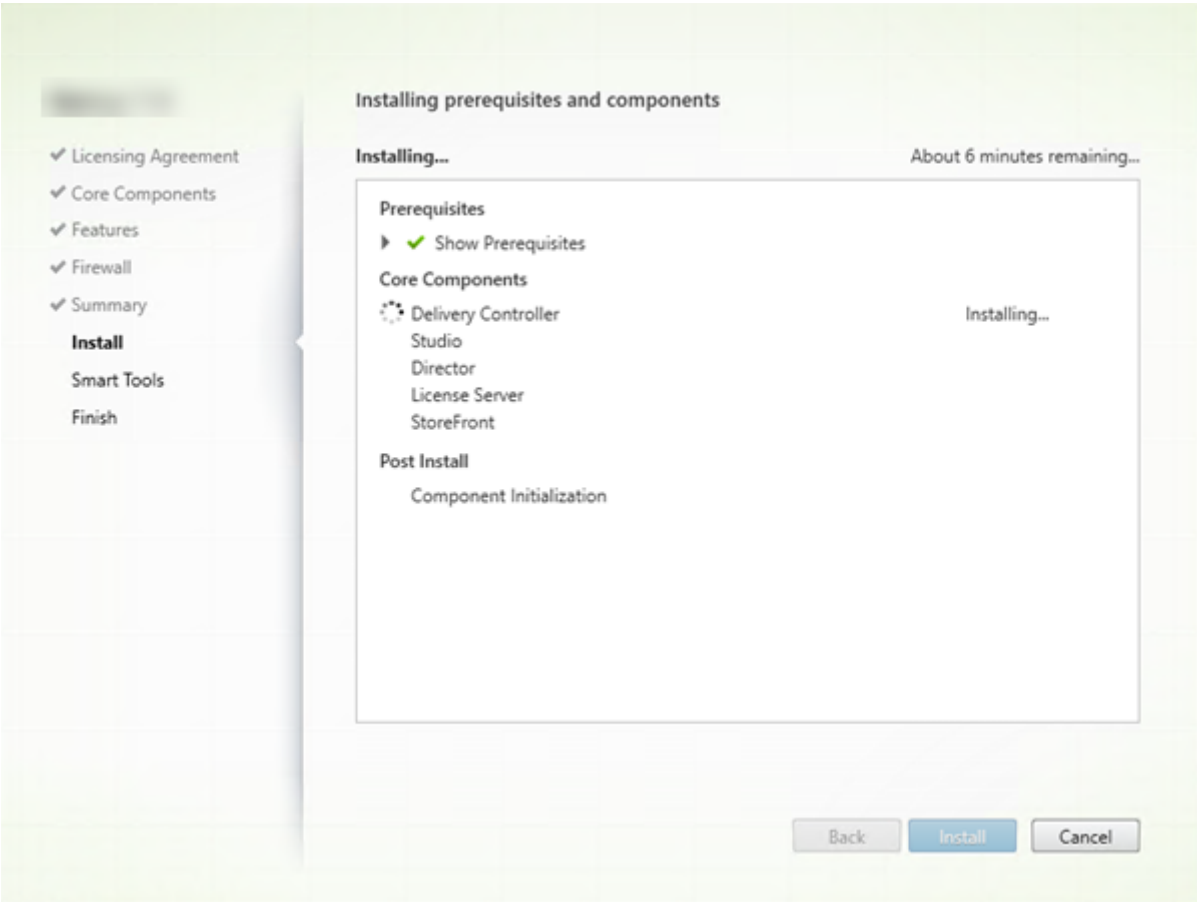
手順 **8**：インストール前に前提条件を確認する



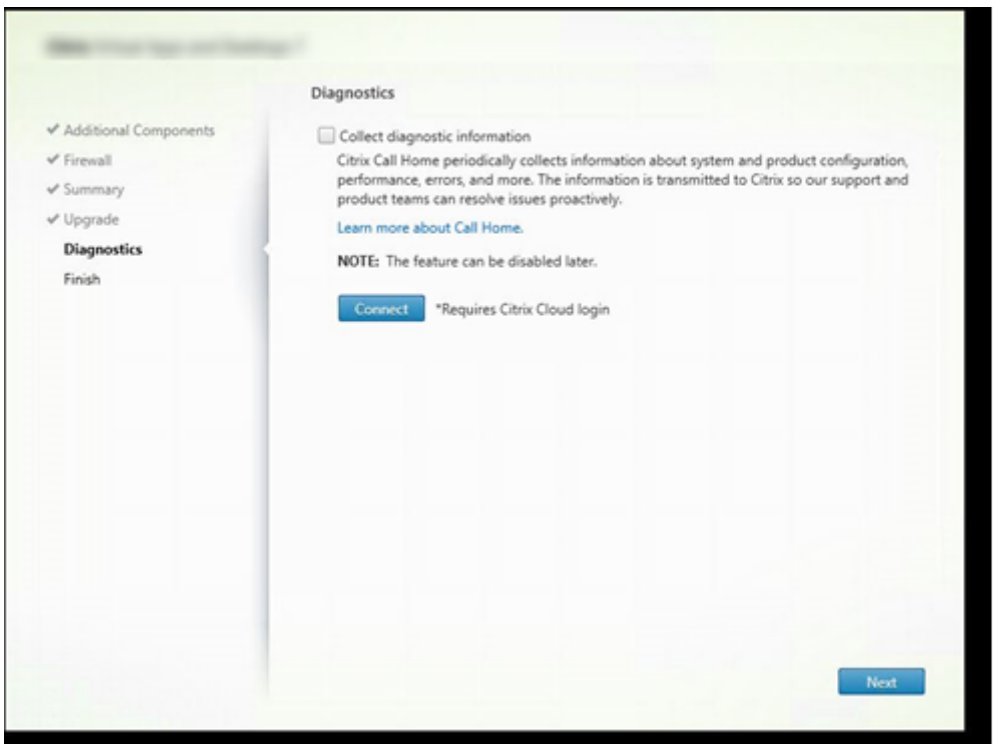
［概要］ページに、インストールされるものが表示されます。必要に応じて、［戻る］ボタンをクリックして前のウィザードページに戻り、選択を変更できます。

準備ができたら、［インストール］をクリックします。

画面にインストールの進捗が表示されます：



手順 **9**：**Cloud Software Group** と診断情報を共有する



［診断］ページで、Citrix Call Home に参加するかどうかを選択します。

このページは、グラフィカルユーザーインターフェイスで Delivery Controller をインストールするときに表示されます。StoreFront（Controller ではない）をインストールすると、このページがウィザードに表示されます。（Controller または StoreFront ではなく）その他のコアコンポーネントをインストールする場合、ウィザードにこのページは表示されません。

Call Home が既に有効な場合、またはインストーラーで Citrix Telemetry Service に関連するエラーが発生した場合には、アップグレード時にこのページは表示されません。

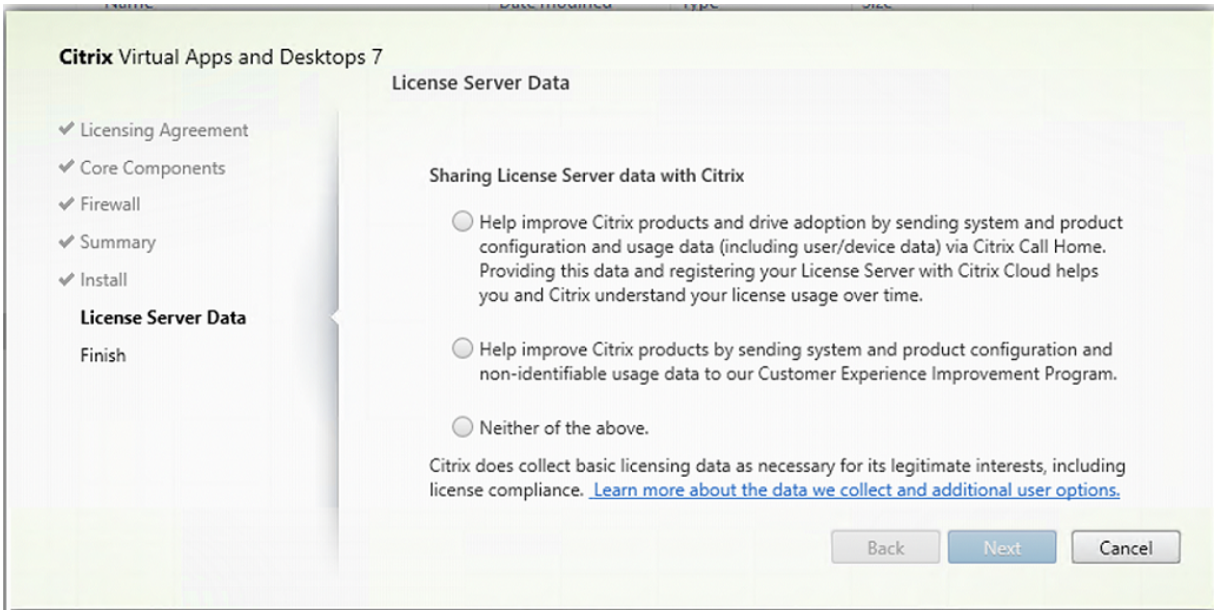
参加することを選択する場合（デフォルト）、［接続］をクリックします。求められたら、Citrix アカウント資格情報を入力します。登録時の選択内容はインストール後に変更できます。

資格情報が確認されたら（または参加しないことを選択した場合）、［次へ］をクリックします。

［診断情報を収集する］を選択せずに ［診断］ページで ［接続］をクリックすると、［**Citrix Insight Services** に接続します］ダイアログを閉じたあとに ［次へ］ボタンが無効になります。次のページに移動できません。［次へ］ボタンを再度有効にするには、［診断情報を収集する］を選択してすぐに選択解除します。

詳しくは、「Call Home」を参照してください。

手順 **10**：ライセンスサーバーのデータを **Cloud Software Group** と共有する



［ライセンスサーバーのデータ］ページで、Call Home データまたはカスタマー エクスペリエンス向上プログラム（CEIP）データのいずれかを共有してください。さらに、Cloud Software Group も、正当な利益のために必要に応じて、ライセンスコンプライアンスなどの基本的なライセンスデータの収集を要求しています。

ライセンスサーバーをインストールすると、［ライセンスサーバーのデータ］ページが表示されます：

- スタンドアロンとして。
- Delivery Controller のインストール時のコアコンポーネントとして。

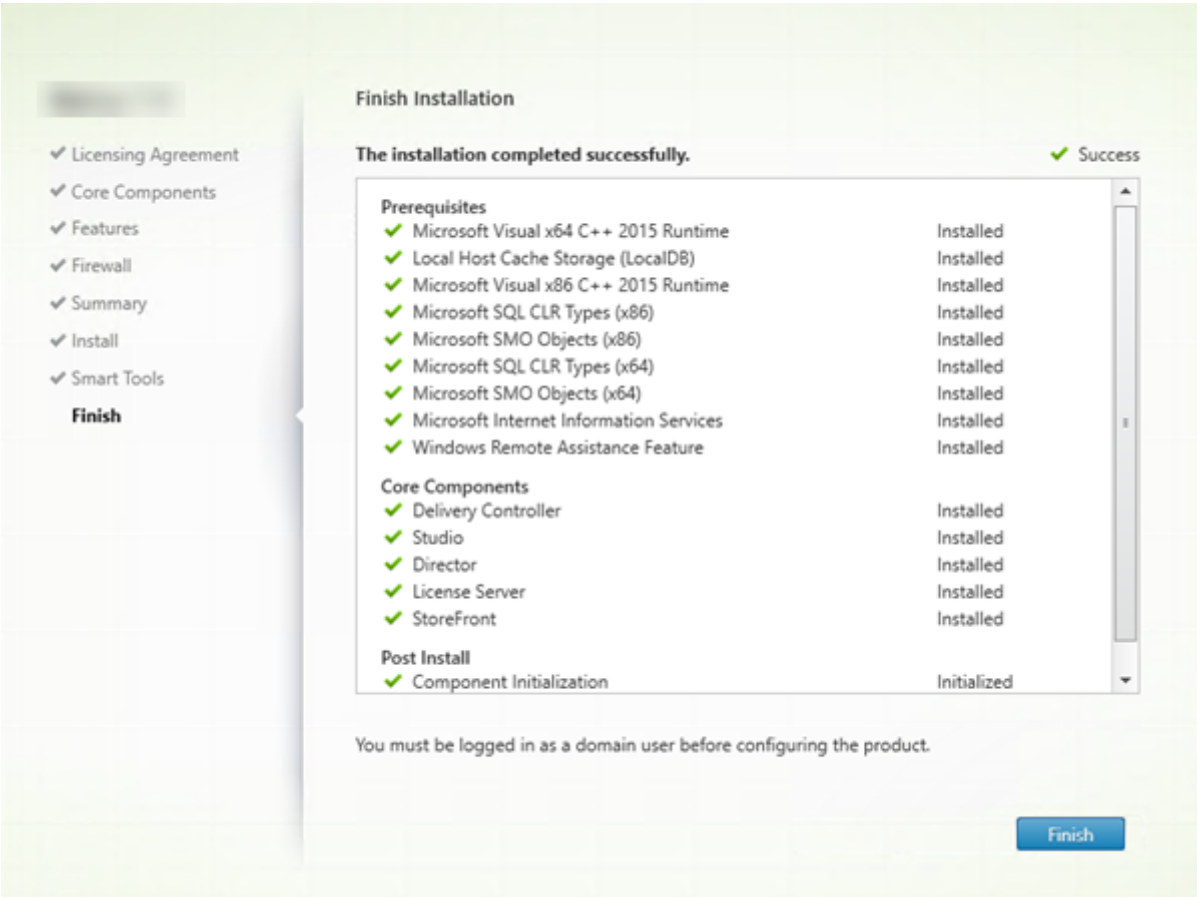
`/CITRIX.opt`：ファイルで既に構成が設定されている場合、アップグレード中にこのページは表示されません。

ライセンスサーバーは、ライセンスデータ、Call Home データ、CEIP データなど、いくつかの種類のユーザーデータを監視します。Call Home データと CEIP データ収集を有効にするには、参加する（オプトインする）ことを選択する必要があります。

コマンドラインを使用してインストールするときに Call Home データと CEIP データの収集を有効にする方法について詳しくは、「コアコンポーネントのインストールに使用されるコマンドラインオプション」を参照してください。

Cloud Software Group のライセンスデータの収集について詳しくは、「Citrix ライセンスデータ収集プログラム」を参照してください。

手順 **11**：インストールを完了する



[完了] ページに、すべての前提条件と正常にインストールおよび初期化されたコンポーネントが緑色のチェックマークで示されます。

[完了] をクリックします。

手順 **12**：残りのコアコンポーネントを他のマシンにインストールする

1 台のマシンにすべてのコアコンポーネントをインストールした場合、次の手順に進みます。それ以外の場合は、その他のマシンでインストーラーを実行し、残りのコンポーネントをインストールします。追加の Controller を他のサーバーにインストールすることもできます。

次の手順

必要なコンポーネントをすべてインストールしたら、Studio を使用してサイトを作成します。

サイトを作成したら、VDA をインストールします。

いつでも全製品インストーラーを使用して展開を拡張し、次のコンポーネントを含めることができます。

- ユニバーサルプリントサーバーコンポーネント：プリントサーバー上でインストーラーを起動します。

  1. ［拡張展開］セクションで ［ユニバーサルプリントサーバー］を選択します。
  2. ライセンス契約に同意します。
  3. Windows ファイアウォールサービスが実行されている場合、デフォルトの動作では ［ファイアウォール］ページに示される TCP ポート 7229 および 8080 が開放されます。これはファイアウォールが無効になっていても同じです。手動でポートを開放する場合は、そのデフォルト動作を無効にできます。

  コマンドラインからこのコンポーネントをインストールするには、「ユニバーサルプリントサーバーをインストールするためのコマンドラインオプション」を参照してください。

- フェデレーション認証サービス。
- Session Recording。
- Workspace Environment Management。

コマンドラインを使用したインストール

August 17, 2024

> 重要：
>
> - アップグレードをする予定で、現在のバージョンで Personal vDisk または AppDisk ソフトウェアを使用またはインストールしている場合は、「PvD、AppDisk、およびサポートされていないホストの削除 」を参照してください。
> - Citrix は、ライセンスコンプライアンスを含む正当な利益のために、必要に応じて基本的なライセンスデータを収集します。詳しくは、「Citrix ライセンスデータ」を参照してください。

はじめに

この記事は、Windows オペレーティングシステムがインストールされたマシンへのコンポーネントのインストールに適用されます。Linux オペレーティングシステムの VDA については、「Linux Virtual Delivery Agent」を参照してください。

このアーティクルでは、製品のインストールコマンドの実行方法を説明します。インストールを始める前に、「インストールの準備」を読んでください。そのアーティクルには、利用できるインストーラーの説明があります。

コマンドの実行状態を確認して値を返すには、マシンの管理者であるか ［管理者として実行］を使用する必要があります。詳しくは、Microsoft 社のコマンドに関するドキュメントを参照してください。

インストールコマンドを直接使用するだけでなく、製品 ISO イメージにあるサンプルスクリプトを使用して Active Directory でマシンの VDA をインストール、アップグレード、または削除できます。詳しくは、「スクリプトを使用した VDA のインストール」を参照してください。

このバージョンの Citrix Virtual Apps and Desktops でサポートしていないバージョンの Windows OS に VDA をインストールまたはアップグレードしようとすると、メッセージが表示され、オプションに関する情報が示されます。「以前のオペレーティングシステム」を参照してください。

Citrix がコンポーネントのインストールの結果を報告する方法については、「Citrix インストールリターンコード」を参照してください。

全製品インストーラーの使用

全製品インストーラーのコマンドラインインターフェイスへのアクセス:

1. Citrix から製品パッケージをダウンロードします。ダウンロードサイトにアクセスするには、Citrix アカウントの資格情報が必要です。
2. ファイルを解凍します。必要な場合は、ISO ファイルから DVD を作成します。
3. ローカルの管理者アカウントを使って、インストール先のサーバーにログオンします。
4. DVD をドライブに挿入するか、ISO ファイルをマウントします。
5. 製品メディアの`\x64\XenDesktop Setup`ディレクトリから適切なコマンドを実行します。

   コンポーネントをインストールするには:「コアコンポーネントのインストールに使用されるコマンドラインオプション」セクションに記載されているオプションを指定して、`XenDesktopServerSetup.exe`を実行します。

   VDA をインストールするには: `XenDesktopVDASetup.exe`を実行します。これには、「VDA のインストールに使用されるコマンドラインオプション」に記載されているオプションを使用します。

   StoreFront をインストールするには: インストールメディアの`x64 > StoreFront`フォルダーで`CitrixStoreFront-x64.exe`を実行します。

   ユニバーサルプリントサーバーをインストールするには:「ユニバーサルプリントサーバーをインストールするためのコマンドラインオプション」のガイダンスに従ってください。

   Federated Authentication Service をインストールするには: Citrix ではグラフィカルインターフェイスを使用することをお勧めします

   Sesssion Recording をインストールするには: Session Recordingのガイダンスに従ってください。

   Workspace Environment Management をインストールするには: Workspace Environment Managementのガイダンスに従ってください。

   StoreFront をインストールするには: インストールメディアの`x64 > XenDesktop`セットアップフォルダーで`XenDesktopSPASetup.exe`を実行します。「Secure Private Access をインストールするためのコマンドラインオプション」のガイダンスに従ってください。

コアコンポーネントのインストールに使用されるコマンドラインオプション

次のパラメーターオプションは、`XenDesktopServerSetup.exe`コマンドを使用してコアコンポーネントをインストールするときに有効です。オプションについて詳しくは、「コアコンポーネントのインストール」を参照してください。

- **/ceipoptin** *ceipoptin* [,*ceipoptin*] …

  Call Home データとカスタマーエクスペリエンス向上プログラム（CEIP）データの収集を有効にします。以下の値を指定します：

  - `DIAGNOSTIC`：Citrix ライセンスサーバーが Call Home データを収集できるようにするには、この値を選択します。
  - `ANONYMOUS`：Citrix ライセンスサーバーが未識別の CEIP データ（ユーザーを識別しない）を収集できるようにするには、この値を選択します。
  - `NONE`：Citrix ライセンスサーバーが CEIP データを収集できないようにするには、この値を選択します。

  Call Home データの収集について詳しくは、「Citrix ライセンス Call Home」を参照してください。

  CEIP データの収集について詳しくは、「Citrix ライセンスカスタマーエクスペリエンス向上プログラム」を参照してください。

  CEIP データについて詳しくは、「Citrix ライセンス CEIP データ要素」を参照してください。

  ライセンスサーバーのライセンスデータについて詳しくは、「Citrix ライセンスデータ」を参照してください。

- **/components** *component* [,*component*] …

  インストールまたは削除するコンポーネントをコンマ区切りのリストで指定します。以下の値を指定します：

  - `CONTROLLER`：Controller
  - `DESKTOPSTUDIO`：Studio
  - `WEBSTUDIO`：Web Studio
  - `DESKTOPDIRECTOR`：Director
  - `LICENSESERVER`：Citrix ライセンスサーバー
  - `SECUREPRIVATEACCESS`：Secure Private Access

  このオプションを指定しない場合、すべてのコンポーネントがインストール（または、`/remove`オプションも指定されている場合は削除）されます。

  （2003 より前のリリースでは、有効な値に`STOREFRONT`が含まれています。バージョン 2003 以降では、「全製品インストーラーの使用」に記載されている StoreFront 専用インストールコマンドを使用します）。

- **/onlyprereqs**

  選択したコンポーネントの前提条件のみがインストールされます。Citrix 製品コンポーネントはインストールされません。

- **/configure_firewall**

  Windows ファイアウォールサービスが実行されている場合に（ファイアウォールが無効になっていても）、インストールされるコンポーネントで使用されるポートが開放されます。サードパーティ製のファイアウォールを使用している場合は、適切なポートを手動で開く必要があります。

- **/disableexperiencemetrics**

  インストール、アップグレード、または削除中に収集される分析の Citrix への自動アップロードが阻止されます。

- **/exclude** “*feature*” [,” *feature*”]

  二重引用符で囲まれた機能、サービス、またはテクノロジをインストールしません。複数の機能、サービス、またはテクノロジを指定する場合は、コンマで区切って、それぞれを直線の二重引用符で囲みます。以下の値を指定します：

  - `"Local Host Cache Storage (LocalDB)"`：ローカルホストキャッシュに使用されるデータベースのインストールが阻止されますこのオプションは、サイトデータベースとして使うために SQL Server Express がインストールされているかには影響しません。

- **/help** または **/h**

  コマンドのヘルプを表示します。

- **/ignore_hw_check_failure**

  ハードウェアチェックが失敗した場合でも（RAM の不足などが原因で）、Delivery Controller のインストールやアップグレードは続行できます。詳しくは、「ハードウェアチェック」を参照してください。

- **/ignore_site_test_failure**

  Controller のアップグレード中にのみ有効です。通常、サイトテストの失敗は無視され、アップグレードが進行します。省略された場合（または false に設定されている場合）、サイトテストに失敗するとアップグレードを実行せずにインストーラーが失敗します。デフォルト値：false

  アップグレード中、サポートされていない SQL Server バージョンが検出されると、このオプションは無視されます。詳しくは、「SQL Server のバージョンチェック」を参照してください。

- **/installdir *directory***

  コンポーネントのインストール先として既存の空ディレクトリを指定します。デフォルト値：c:\Program Files\Citrix

- **/logpath *path***

  ログファイルのパスを指定します。既存のフォルダーを指定する必要があります。インストーラーによって作成されません。デフォルト値：`TEMP%\Citrix\XenDesktop Installer`

- **/no_remote_assistance**

Director をインストールする場合にのみ有効です。Windows リモートアシスタンス機能を使用するシャドウ機能を無効化します。

- **/noreboot**

  インストール後の再起動を無効にします。（ほとんどのコアコンポーネントでは、デフォルトで再起動が無効になっています）。

- **/noresume**

  デフォルトでは、インストール中にマシンの再起動が必要になった場合、再起動が完了すると自動的にインストーラーが再開します。デフォルトを上書きするには、/noresumeを指定します。これは、メディアを再マウントする必要がある場合、または自動インストール中に情報をキャプチャする必要がある場合に役立ちます。

- **/nosql**

  Controller のインストール先サーバーに Microsoft SQL Server Express をインストールしない場合に指定します。このオプションを指定しない場合、SQL Server Express がサイトデータベースとして使用するためにインストールされます。

  このオプションは、ローカルホストキャッシュに使用される SQL Server Express LocalDB のインストールには影響しません。

- **/quiet** または**/passive**

  ユーザーインターフェイスを表示せずにインストールを実行します。インストールプロセスは、Windows タスクマネージャーにのみ表示されます。このオプションを指定しない場合、インストールウィザードが表示されます。

- **/remove**

  /componentsオプションで指定したコアコンポーネントを削除します。

- **/removeall**

  インストール済みのすべてのコアコンポーネントを削除します。

- **/SKIPHDXDRIVERCHECK**

  VDA メタインストーラーへの HDX ドライバーのチェックをスキップします。

- **/sendexperiencemetrics**

  Citrix Insight Services へのインストール、アップグレード、または削除中に収集される分析が自動的に送信されます。これが省略される場合（または/disableexperiencemetricsが指定される場合）、分析はローカルで収集されますが、自動的には送信されません。

- **/tempdir** *directory*

  インストール時に一時ファイルを作成するディレクトリを指定します。デフォルト値：c:\Windows\Temp

- **/xenapp**

Citrix Virtual Apps をインストールします。このオプションを指定しない場合、Citrix Virtual Apps and Desktops がインストールされます。

コアコンポーネントのインストールの例

次のコマンドを実行すると、Delivery Controller、Studio、Citrix ライセンスサーバー、および SQL Server Express がサーバー上にインストールされます。コンポーネントの通信で使用されるファイアウォールポートは自動的に開放されます。

```
\x64\XenDesktop Setup\XenDesktopServerSetup.exe /components controller
,desktopstudio,licenseserver /configure_firewall
```

次のコマンドを実行すると、Citrix Virtual Apps、Controller、Studio、および SQL Server Express がサーバー上にインストールされます。コンポーネントの通信で使用されるファイアウォールポートは自動的に開放されます。

```
\x64\XenDesktop Setup\\XenDesktopServerSetup.exe /xenapp /components
controller,desktopstudio /configure_firewall
```

次のコマンドを実行すると、Delivery Controller、Secure Private Access、および SQL Server Express がサーバー上にインストールされます。コンポーネントの通信で使用されるファイアウォールポートは自動的に開放されます。

```
\x64\XenDesktop Setup XenDesktopServerSetup.exe /xenapp /components
controller,secureprivateaccess /configure_firewall
```

スタンドアロン **VDA** インストーラーの使用

ダウンロードサイトにアクセスするには、Citrix アカウントの資格情報が必要です。インストールは、管理者権限（または ［管理者として実行］）で実行する必要があります。

1. Citrix から適切なパッケージをダウンロードします:
   - マルチセッション OS Virtual Delivery Agent: `VDAServerSetup_xxxx.exe`
   - シングルセッション OS Virtual Delivery Agent: `VDAWorkstationSetup_xxxx.exe`
   - シングルセッション OS Core Services Virtual Delivery Agent:`VDAWorkstationCoreSetup_xxxx.exe`
2. まず、パッケージから既存のディレクトリにファイルを抽出して、インストールコマンドを実行するか、または通常どおりにパッケージを実行します。

   インストール前にファイルを展開するには、絶対パスを指定して`/extract`を実行します（例: `C:\YourExtractFolder\VDAWorkstationCoreSetup.exe /extract %temp%\CitrixVDAInstallMedia`）。ディレクトリはあらかじめ存在する必要があります。存在しない場合、抽出に失敗します。次に、別のコマンドで、この記事に記載されている有効なオプションを使用して、適切なコマンドを実行します。

- VDAServerSetup_XXXX.exeについては、<extract folder>\Extract\Image-Full\x64\XenDesktop Setup\XenDesktopVDASetup.exeを実行します。
- VDAWorkstationCoreSetup_XXXX.exeについては、<extract folder>\Extract\Image-Full\x64\XenDesktop Setup\XenDesktopRemotePCSetup.exeを実行します。
- VDAWorkstationSetup_XXXX.exeについては、<extract folder>\Extract\Image-Full\x64\XenDesktop Setup\XenDesktopVDASetup.exeを実行します。

ダウンロードした対象名のパッケージを実行します:VDAServerSetup.exe、VDAWorkstationSetup.exe、またはVDAWorkstationCoreSetup.exe。この記事で説明する有効なオプションを使用してください。

全製品インストーラーに慣れている場合:

- スタンドアロンのVDAServerSetup.exeまたはVDAWorkstationSetup.exeは名前以外、XenDesktopVdaSetup.exeコマンドと同じですので、同様に実行してください。
- VDAWorkstationCoreSetup.exeインストーラーは、他のインストーラーで利用できるオプションのサブセットをサポートしているので異なります。

VDA のインストールに使用されるコマンドラインオプション

次のオプションは、次の各コマンド（インストーラー）の 1 つ以上で使用できます: VDAServerSetup_xxxx.exe、VDAWorkstationSetup_xxxx.exe、VDAWorkstationCoreSetup_xxxx.exe。

オプションについて詳しくは、「VDA のインストール」を参照してください。

- **/components** *component*[,*component*]

  インストールまたは削除するコンポーネントをコンマ区切りのリストで指定します。以下の値を指定します:

  - VDA: Virtual Delivery Agent
  - PLUGINS: Windows 向け Citrix Workspace アプリ

  VDA および Windows 向け Citrix Workspace アプリをインストールするには、「/components vda,plugins」と指定するか、いずれのコンポーネントも指定しません。コンポーネントが指定されていない場合は、デフォルトで VDA のみがインストールされます。

  VDA のみをインストールして、Citrix Workspace アプリのインストールを除外するには、「/components vda」と指定します。

  このオプションは、VDAWorkstationCoreSetup_xxxx.exeインストーラーを使用している場合無効です。このインストーラーでは、Citrix Workspace アプリをインストールできません。

- **/onlyprereqs**

  選択したコンポーネントの前提条件のみがインストールされます。Citrix 製品コンポーネントはインストールされません。

- **/controllers** *"controller [controller]"*

  VDA が通信する Controller の FQDN を、直線の二重引用符で囲んだスペース区切りのリストで指定します。/site_guidと/controllersの両方を指定しないでください。

- **/disableexperiencemetrics**

  インストール、アップグレード、または削除中に収集される分析の Citrix への自動アップロードが阻止されます。

- **/enable_hdx_ports**

  Windows ファイアウォールサービスが実行されている場合に（ファイアウォールが無効になっていても）、VDA および有効な機能 (Windows リモートアシスタンスは除く) で必要なポートが開放されます。Windows 以外のファイアウォールを使用している場合は、手作業でファイアウォールを構成する必要があります。ポートについて詳しくは、「ネットワークポート」を参照してください。

  HDX アダプティブトランスポートが使用する UDP ポートを解放するには、この/enable_hdx_portsに加えて、/enable_hdx_udp_portsを指定します。

- **/enable_hdx_udp_ports**

  Windows ファイアウォールサービスが検出された場合に（ファイアウォールが無効になっていても）、HDX アダプティブトランスポートに使用するポートが Windows ファイアウォールで開放されます。Windows 以外のファイアウォールを使用している場合は、手作業でファイアウォールを構成する必要があります。ポートについて詳しくは、「ネットワークポート」を参照してください。

  VDA が使用する追加のポートを解放するには、この/enable_hdx_udp_portsに加えて、/enable_hdx_portsを指定します。

- **/enable_hdx_tls_dtls**

  HDX Direct V1 用に TCP および UDP ポート 443 を開きます。

- **/enable_real_time_transport**

  オーディオパケットで UDP を使用してパフォーマンスを向上させる機能（RealTime Audio Transport）を有効または無効にします。この機能を有効にすると、オーディオパフォーマンスを向上させることができます。Windows ファイアウォールサービスが検出されたときに UDP ポートが開放されるようにするには、/enable_hdx_portsを指定してください。

- **/enable_remote_assistance**

  Director で使用する Windows リモートアシスタンスのシャドウ機能を有効にします。このオプションを指定すると、Windows リモートアシスタンスによってファイアウォールで動的ポートが解放されます。

- **/enablerestore** または**/enablerestorecleanup**

  （シングルセッション VDA にのみ有効）これにより、VDA のインストールまたはアップグレードが失敗した場合に、復元ポイントへの自動復帰が有効になります。

  インストールまたはアップグレードが正常に完了した場合：

  - /enablerestorecleanupは、復元ポイントを削除するようインストーラーに指示します。
  - /enablerestoreは、復元ポイントが使用されなかった場合でも、その復元ポイントを保持するようインストーラーに指示します。

  詳しくは、「インストールまたはアップグレードの失敗時の復元」を参照してください。

- **/ENABLE_SECURE_DEFAULTS**

  より安全な初期構成を実現するために、さまざまな機能のデフォルト設定を有効から無効に変更します。関連する機能は、クライアントドライブのリダイレクト、ユーザーフォルダーのリダイレクト、ドラッグアンドドロップ、TWAIN デバイスのリダイレクト、クライアント USB プラグアンドプレイデバイスリダイレクト、クライアントプリンターのリダイレクト、クライアントクリップボードリダイレクト、およびクライアントマイクのリダイレクトです。

- **/enable_ss_ports**

  Windows ファイアウォールサービスが検出された場合に（ファイアウォールが無効になっていても）、画面共有に必要なポートが Windows ウォールで開放されます。Windows 以外のファイアウォールを使用している場合は、手作業でファイアウォールを構成する必要があります。

- **/exclude** “*component*”[,”*component*”]

  二重引用符で囲まれた、オプションコンポーネントをインストールしません。複数のコンポーネントを指定する場合は、コンマで区切って、それぞれ直線の二重引用符で囲みます。たとえば、MCS が管理していないイメージ上で VDA をインストールまたはアップグレードする場合、Machine Identity Service コンポーネントは必要ありません。有効な値は次のとおりです：

マルチセッション OS	シングルセッション OS	シングルセッション OS Core Services
Citrix Authentication Identity Assertion VDA Plug-in	Citrix Authentication Identity Assertion VDA Plug-in	Citrix Authentication Identity Assertion VDA Plug-in
Citrix Backup and Restore	Citrix Backup and Restore	Citrix Browser Content Redirection
Citrix Browser Content Redirection	Citrix Browser Content Redirection	Citrix Personalization **for** App-V - VDA

マルチセッション OS	シングルセッション OS	シングルセッション OS Core Services
Citrix MCS IODriver	Citrix MCS IODriver	Citrix Telemetry Service
Citrix Personalization **for** App-V - VDA	Citrix Personalization **for** App-V - VDA	Citrix Universal Print Client
Citrix Profile Management	Citrix Profile Management	Citrix Vda Log Capture Service
Citrix Profile Management WMI Plug-in	Citrix Profile Management WMI Plug-in	CSE Component
Citrix Rendezvous V2	Citrix Rendezvous V2	Director VDA Plug-in
Citrix Telemetry Service	Citrix Telemetry Service	Machine Management Provider
Citrix Universal Print Client	Citrix Universal Print Client	VDA Monitor Plug-in
Citrix Vda Log Capture Service	Citrix Vda Log Capture Service	VDA WMI Proxy Plug-in
Citrix VDA Upgrade Agent	Citrix VDA Upgrade Agent	
CSE Component	CSE Component	
Director VDA Plug-in	Director VDA Plug-in	
Machine Identity Service	Machine Identity Service	
Machine Management Provider	Machine Management Provider	
VDA Monitor Plug-in	User Personalization Layer	
VDA WMI Proxy Plug-in	VDA Monitor Plug-in	
	VDA WMI Proxy Plug-in	
Citrix App Protection Component	Citrix App Protection Component	Citrix App Protection Component

マルチセッション OS	シングルセッション OS	シングルセッション OS Core Services
Citrix HyperV Filter Driver	Citrix HyperV Filter Driver	
Citrix Personalization for App-V - VDA	Citrix Personalization for App-V - VDA	Citrix Personalization for App-V - VDA

インストール（/exclude "Citrix Profile Management"）から Citrix Profile Management を除くと、Citrix Director を使った VDA の監視やトラブルシューティングに影響があります。［ユーザーの詳細］ページの［個人設定］パネル、および ［エンドポイント］ページの［ログオン処理時間］パネルに不具合が発生します。［ダッシュボード］ページと ［傾向］ページでは、Profile Management がインストールされているマシンについてのデータしか［平均ログオン処理時間］パネルに表示されません。

サードパーティのユーザープロファイル管理ソリューションを使用している場合でも、Citrix Profile Management Service をインストールして実行することを Citrix ではお勧めします。Citrix Profile Management Service の有効化は、必須ではありません。

/excludeおよび/includeadditionalの両方に同じコンポーネント名を指定した場合、そのコンポーネントはインストールされません。

このオプションは、VDAWorkstationCoreSetup.exeインストーラーを使用している場合無効です。そのインストーラーは、これらの項目の多くを自動的に除外します。

- **/h** または **/help**

  コマンドのヘルプを表示します。

- **/includeadditional** “*component*”［,” *component*” ］

  インストールするオプションコンポーネントを 1 つ以上、それぞれ直線の二重引用符で囲みコンマ区切りで指定します。このオプションを使用すると、リモート PC アクセス展開を作成する場合に、デフォルトでは含まれない他のコンポーネントをインストールできます。有効な値は次のとおりです:

マルチセッション OS	シングルセッション OS
Citrix Backup and Restore	Citrix Backup and Restore
Citrix MCS IODriver	Citrix MCS IODriver
Citrix Personalization for App-V - VDA	Citrix Personalization for App-V - VDA
Citrix Profile Management	Citrix Profile Management

マルチセッション OS	シングルセッション OS
Citrix Profile Management WMI Plug-in	Citrix Profile Management WMI Plug-in
Citrix Rendezvous V2	Citrix Rendezvous V2
Citrix VDA Upgrade Agent	Citrix VDA Upgrade Agent
Citrix Web Socket Vda Registration Tool	Citrix Web Socket Vda Registration Tool
Machine Identity Service	Machine Identity Service
	User Personalization Layer

/excludeおよび/includeadditionalの両方に同じコンポーネント名を指定した場合、そのコンポーネントはインストールされません。

- **/installdir** *directory*

  コンポーネントのインストール先として既存の空ディレクトリを指定します。デフォルト値: c:\Program Files\Citrix

- **/install_mcsio_driver**

  使用しないでください。代わりに、/includeadditional "Citrix MCS IODriver"または/exclude "Citrix MCS IODriver"を使用してください。

- **/logpath** *path*

  ログファイルのパスを指定します。既存のフォルダーを指定する必要があります。インストーラーによって作成されません。Default = 「%TEMP%\Citrix\XenDesktop Installer」

  このオプションはグラフィカルインターフェイスでは使用できません。

- **/masterimage**

  仮想マシン上に VDA をインストールする場合にのみ有効です。他のマシンの作成に使用するイメージとして VDA を設定します。このオプションは/mastermcsimageと同等です。

  このオプションは、VDAWorkstationCoreSetup_xxxx.exeインストーラーを使用している場合無効です。

- **/mastermcsimage**

  インストールするマシンを、Machine Creation Services で使用するイメージに指定します。このオプションは/masterimageと同等です。

- **/masterpvsimage**

インストールするマシンを、Citrix Provisioning またはサードパーティのプロビジョニングツール（Microsoft System Center Configuration Manager など）で VM のプロビジョニングに使用するイメージに指定します。

- **/websockettoken** *WebSocketToken*

  Web Socket VDA を作成します。WebSocketToken は、必要なトークン用です。

- **/websockettokenfile** *FileContainingWebSockToken*

  Web Socket VDA を作成します。*FileContainingWebSockToken* は、必要なトークンを含むファイル用です。

- **/websockettokenstdin** <*WebSocketToken*

  Web Socket VDA を作成します。<*WebSocketToken* は、STDIN でトークンが渡されるために必要です。

- **/no_mediafoundation_ack**

  Microsoft の Media Foundation がインストールされていなければ、複数の HDX マルチメディア機能はインストールされず、動作しないものがあることを認識します。このオプションが省略されていて、Media Foundation がインストールされていない場合、前提条件が満たされないため VDA インストールは終了します。サポートされているほとんどの Windows のエディションには、N エディションの例外を除けば、Media Foundation が既にインストールされています。Windows の機能、メディアの機能の順に手動で有効にすると、Citrix のメタインストーラーによって検索されたレジストリキーに設定値が存在しない可能性があります。インストールプロセスを開始する前に`SOFTWARE\Microsoft\Windows\CurrentVersion\Setup\Windows-Features\WindowsMediaVersion`レジストリキーをチェックして、値が存在し空でないことを確認してください。

- **/nodesktopexperience**

  拡張デスクトップエクスペリエンス機能は使用できなくなりました。このオプション（およびポリシー設定）は、指定しても無視されます。

  マルチセッション OS 対応 VDA をインストールする場合にのみ有効です。デスクトップエクスペリエンス拡張機能を無効にします。この機能の有効/無効は、Citrix ポリシー設定の［拡張デスクトップエクスペリエンス］でも制御できます。

- **/noreboot**

  インストール後の再起動を無効にします。VDA は、再起動後にのみ使用できます。

- **/noresume**

  デフォルトでは、インストール中にマシンの再起動が必要になった場合、再起動が完了すると自動的にインストーラーが再開します。デフォルトを上書きするには、`/noresume`を指定します。これは、メディアを再マウントする必要がある場合、または自動インストール中に情報をキャプチャする必要がある場合に役立ちます。

- **/physicalmachine**

リモート PC のインストールには、この引数を/remotepcとともに使用します。そうしないと、特定のユーザーシナリオで VDA が正常に動作しない場合があります。

- **/portnumber** *port*

  /reconfigオプションを指定する場合にのみ有効です。Virtual Delivery Agent と Controller 間の通信で使用されるポート番号を変更します。変更前のポートは無効になります（ポート 80 を除く）。

- **/proxyconfig** “アドレスまたは *PAC* ファイルパス”

  環境内の Gateway サービス、VDA アップグレードサービスなどで Rendezvous プロトコルを使用し、ネットワークに送信接続用の非透過プロキシがある場合は、ここでプロキシを指定します。HTTP プロキシのみがサポートされています。Rendezvous プロトコルで使用するためのプロキシのアドレス、または PAC ファイルパス。このコマンドラインは、/includeadditional “Citrix Rendezvous V2”が使用されたかのように Citrix Rendezvous V2 を自動的にインストールします。機能について詳しくは、「Rendezvous プロトコル」を参照してください。

  - プロキシアドレスの形式：`http://<url-or-ip>:<port>`
  - PAC ファイルの形式：`http://<url-or-ip>:<port>/<path>/<filename>.pac`

- **/quiet** または**/passive**

  ユーザーインターフェイスを表示せずにインストールを実行します。インストールおよび構成プロセスは、Windows タスクマネージャーにのみ表示されます。このオプションを指定しない場合、インストールウィザードが表示されます。

- **/reconfigure**

  インストール済みの Virtual Delivery Agent 設定をカスタマイズします。/portnumber、/controllers、または/enable_hdx_portsオプションと一緒に使用します。/quietオプションを指定しない場合は、VDA をカスタマイズするためのグラフィカルインターフェイスが開きます。

- **/remotepc**

  リモート PC アクセス展開（シングルセッション OS）または仲介接続（マルチセッション OS）でのみ有効です。追加コンポーネントのインストールを除外します（/excludeおよび/includeadditionalオプションのあるコンポーネントの一覧を参照してください）。

  このオプションは、VDAWorkstationCoreSetup.exeインストーラーを使用している場合無効です。このインストーラーは、上記のコンポーネントのインストールを自動的に除外します。

  /remotepcは、この/servervdiオプションに対応していません。

- **/remove**

  /componentsオプションで指定したコンポーネントを削除します。

- **/remove_appdisk_ack**

  AppDisks VDA プラグインがインストールされている場合、それをアンインストールする権限を VDA インストーラーに与えます。

- **/remove_pvd_ack**

  Personal vDisk がインストールされている場合、それをアンインストールする権限を VDA インストーラーに与えます。

- **/removeall**

  VDA を削除します。Citrix Workspace アプリは削除されません（インストールされている場合）。

- **/REMOVEALLWITHCWA**

  VDA とともに Citrix Workspace アプリも削除します。

- **/sendexperiencemetrics**

  Citrix Insight Services へのインストール、アップグレード、または削除中に収集される分析が自動的に送信されます。これが省略される場合（または/disableexperiencemetricsが指定される場合）、分析はローカルで収集されますが、自動的には送信されません。

- **/servervdi**

  サポートされる Windows マルチセッションマシンにシングルセッション OS 対応 VDA をインストールします。Windows マルチセッションマシンにマルチセッション OS 対応 VDA をインストールするときにこのオプションを省略します。

  このオプションを使用する前に、「サーバー VDI」を参照してください。

  このオプションは、全製品 VDA インストーラーでのみ使用します。

- **/site_guid** *guid*

  サイトの Active Directory 組織単位（OU）のグローバル一意識別子（GUID）を指定します。Active Directory OU ベースの Controller 検出を使用する場合、GUID により仮想デスクトップとサイトが関連付けられます（デフォルトの検出方法である自動更新を使用することをお勧めします）。サイト GUID は、Studio に表示されるサイトプロパティです。/site_guidと/controllersの両方を指定しないでください。

- **/tempdir** *directory*

  インストール時に一時ファイルを作成するディレクトリを指定しますデフォルト値：c:\Windows\Temp

  このオプションはグラフィカルインターフェイスでは使用できません。

- **/virtualmachine**

  仮想マシン上に VDA をインストールする場合にのみ有効です。インストーラーによる物理マシンの検出を上書きして、BIOS 情報を仮想マシンに渡して物理マシンとして振る舞うようにします。

  このオプションはグラフィカルインターフェイスでは使用できません。

- **/xendesktopcloud**

  VDA が Citrix DaaS（Citrix Cloud）展開にインストールされていることを示します。

VDA のインストールの例

フル製品インストーラーを使用して **VDA** をインストールします:

次のコマンドを実行すると、仮想マシン上のデフォルトの場所にシングルセッション OS 対応 VDA および Citrix Workspace アプリがインストールされます。この VDA はイメージとなり、MCS を使用して VM をプロビジョニングします。VDA はmydomainドメインの「Contr-Main」という名前の Controller に登録されます。VDA は、ユーザー個人設定レイヤーおよび Windows リモートアシスタンスを使用します。

```
\x64\XenDesktop Setup\XenDesktopVdaSetup.exe /quiet /components vda
,plugins /controllers "Contr-Main.mydomain.local"/enable_hdx_ports
 /includeadditional "user personalization layer"/mastermcsimage /
enable_remote_assistance
```

VDAWorkstationCoreSetup スタンドアロンインストーラーでシングルセッション **OS VDA** をインストールする:

次のコマンドは、リモート PC アクセスまたは VDI 展開で使用するためにシングルセッション OS に Core Services VDA をインストールします。Citrix Workspace アプリとその他の非コアサービスはインストールされません。Controller のアドレスが指定され、Windows ファイアウォールサービスのポートが自動的に開放されます。管理者が再起動を処理します。

```
VDAWorkstationCoreSetup .exe /quiet /controllers "Contr-East.domain.
com"/enable_hdx_ports /noreboot
```

VDA のカスタマイズ

VDA をインストールした後で、いくつかの設定をカスタマイズできます。製品メディアの\x64\XenDesktop Setupフォルダーから、以下のオプションを指定してXenDesktopVdaSetup.exeを実行します（各オプションについては「VDA のインストールに使用されるコマンドラインオプション」を参照してください）。

- /reconfigure（VDA をカスタマイズする場合は必須のオプションです）
- /h または /help
- /quiet
- /noreboot
- /controllers
- /portnumber port
- /enable_hdx_ports

VDA のトラブルシューティング

- デリバリーグループの Studio 表示では、［詳細］ペインの ［インストール済み **VDA** のバージョン］エントリがマシンにインストールされているバージョンではないことがあります。マシンの Windows の［プログラム

と機能］には、VDA の実際のバージョンが表示されます。

- インストール後、VDA は Delivery Controller に登録されるまでユーザーにアプリやデスクトップを配信することはできません。

  VDA の登録方法および登録の問題のトラブルシューティングについては、「VDA 登録」を参照してください。

ユニバーサルプリントサーバーをインストールするためのコマンドラインオプション

次のオプションは`XenDesktopPrintServerSetup.exe`コマンドで有効です。

- **/enable_upsserver_port**

このオプションが指定されていない場合、インストーラーはグラフィカルインターフェイスからファイアウォールページを表示します。**Automatically** を選択すると、インストーラーは自動的に Windows ファイアウォール規則を追加し、**Manually** を選択すると管理者が手動でファイアウォールを構成できるようにします。

プリントサーバーにこのソフトウェアをインストールした後で、「プリンターのプロビジョニング」の説明に従って構成します。

Secure Private Access をインストールするためのコマンドラインオプション

次のオプションはどちらでも有効です：

1. CVAD インストーラー：`XenDesktopSPASetup.exe`
2. SPA オンプレミスインストーラー：`SecurePrivateAccessSetup_XXXX.exe`

- **/enable_spa_ports**

  Windows ファイアウォールサービスが検出された場合に（ファイアウォールが無効になっていても）、Secure Private Access に必要なポートが Windows ファイアウォールで開放されます。Windows 以外のファイアウォールを使用している場合は、手作業でファイアウォールを構成する必要があります。ポートについて詳しくは、「ネットワークポート」を参照してください。

- **/nosql**

  Secure Private Access のインストール先サーバーに Microsoft SQL Server Express をインストールしない場合に指定します。このオプションを指定しない場合、SQL Server Express がサイトデータベースとして使用するためにインストールされます。

- **/help** または**/h** または**/?**

  コマンドのヘルプを表示します

- **/noreboot**

  インストール後の再起動を無効にします。Secure Private Access は再起動するまで使用できません。

- **/quiet** または**/passive**

  ユーザーインターフェイスを表示せずにインストールを実行します。インストールおよび構成プロセスは、Windows タスクマネージャーにのみ表示されます。このオプションを指定しない場合、インストールウィザードが表示されます。

- **/remove**

  Secure Private Access を削除します。

オプションについて詳しくは、「Secure Private Access インストーラー」を参照してください。

追加情報

Citrix がコンポーネントのインストールの結果を報告する方法については、「Citrix インストールリターンコード」を参照してください。

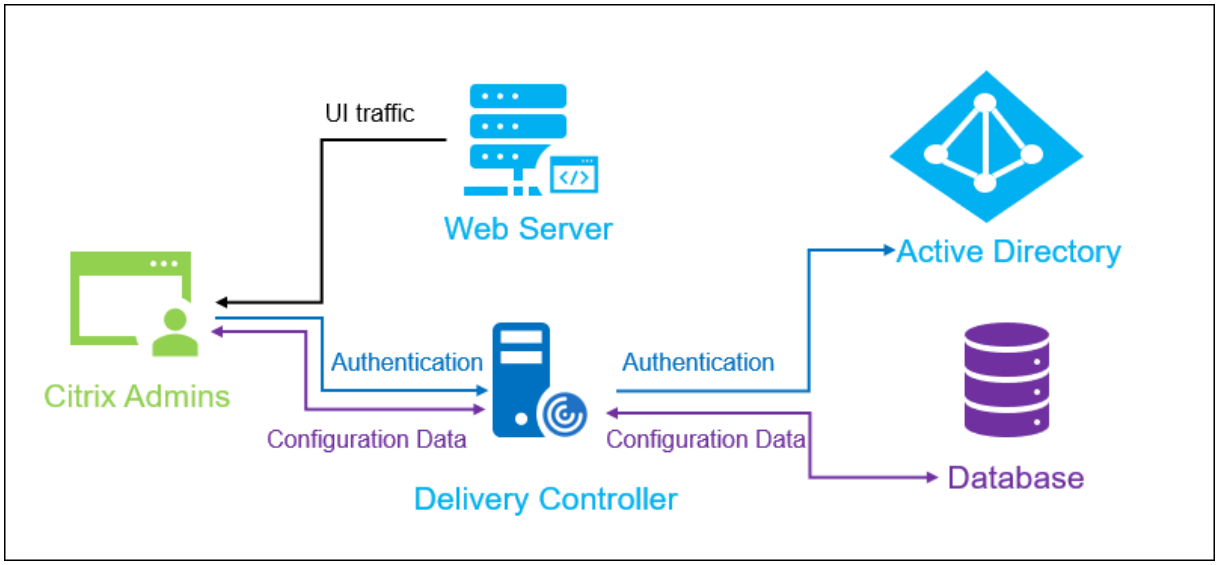
Web Studio をインストールする

August 20, 2024

はじめに

Citrix Studio は、Citrix Virtual Apps and Desktops 環境を構成および管理する Windows ベースの管理コンソールです。Web Studio は次世代の Citrix Studio であり、Citrix Studio と完全に同等の機能を提供する Web ベースの管理コンソールです。Web Studio は、Citrix DaaS の［完全な構成］インターフェイス と同じ外観で、ネイティブの Web エクスペリエンスを提供することで、管理エクスペリエンスを刷新しています。

Web Studio は、インターネットインフォメーションサービス（IIS）がインストールされている任意の Windows サーバーに展開できます。迅速な展開のために、Delivery Controller とともに Web Studio をインストールすることをお勧めします。その場合、Web Studio は Web サイトとして Delivery Controller にインストールされます。アーキテクチャをシンプルにし、管理オーバーヘッドを減らすために、この設定に従うことをお勧めします。次の図は、Web Studio のアーキテクチャを示しています：



Web Studio を起動して実行するための一般的なワークフローは次のとおりです:

1. Web Studio をインストールする。
2. サイトを設定する。
3. 管理用に Delivery Controller を Web Studio に追加する。
4. Web Studio にログインする。

負荷分散された Web Studio 展開を設定するには、この記事を参照してください。

Web Studio で利用可能な新機能

「新機能」の記事を参照してください。

システム要件

以下のオペレーティングシステムがサポートされています:

- Windows Server 2022
- Windows Server 2019 の Standard Edition、Datacenter Edition、および Server Core オプション付き
- Windows Server 2016 の Standard Edition、Datacenter Edition、および Server Core オプション付き

サポートされているブラウザー:

- Microsoft Edge 92

- Firefox ESR（Extended Support Release）90
- Google Chrome 92
- Safari 14

Web Studio の表示に推奨される最適な画面解像度は 1440 x 1024 です。

前提条件

Web Studio のこのリリースは、Citrix Virtual Apps and Desktops 2212 以降と互換性があります。

2212 より前の環境の場合は、まず 2212 にアップグレードしてから、Web Studio をインストールします。

既知の制限事項

Web Studio と Citrix Studio を無差別に使用する場合は、Web Studio で作成したテンプレートが Citrix Studio に表示されず、その逆も同様であるという制限がありますので、注意してください。これは、Web Studio が Citrix Studio と異なるデータベースを使用してテンプレートを保存するためです。回避策として、Web Studio でテンプレートからポリシーを作成し、Citrix Studio でこのポリシーからテンプレートを作成します。その逆も同様です。

- Web Studio を正常にインストールできるようにするため、インターネットインフォメーションサービス（IIS）マネージャーでデフォルトのサイト名（[既定の **Web** サイトのホーム］の値）を変更しないでください。デフォルトのサイト名を変更すると、インストールが失敗するからです。

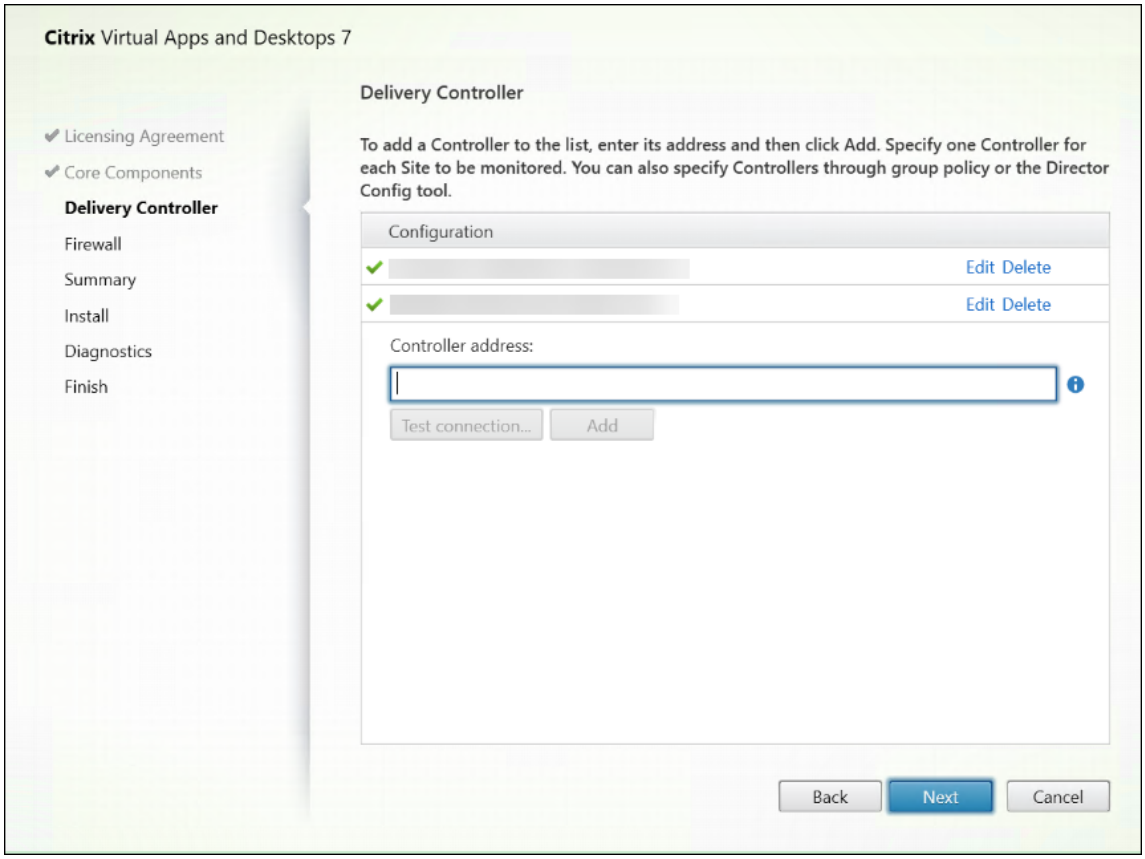
Web Studio をインストールする

以下の情報は、「コアコンポーネントのインストール」のガイダンスを補足するものです。Web Studio をインストールするには:

- Citrix Virtual Apps and Desktops の完全な製品 ISO インストーラーを使用して Web Studio をインストールします。ISO インストーラーは前提条件を確認し、不足しているコンポーネントをインストールし、Web Studio Web サイトを（Delivery Controller のインストール時に含まれていた場合は Delivery Controller 上で）セットアップし、基本的な構成を実行します。
- インストール時に Web Studio が含まれていなかった場合は、インストーラーを使用して Web Studio を追加します。
- Web Studio のインストール時に、Delivery Controller のアドレスを入力するよう求められます。

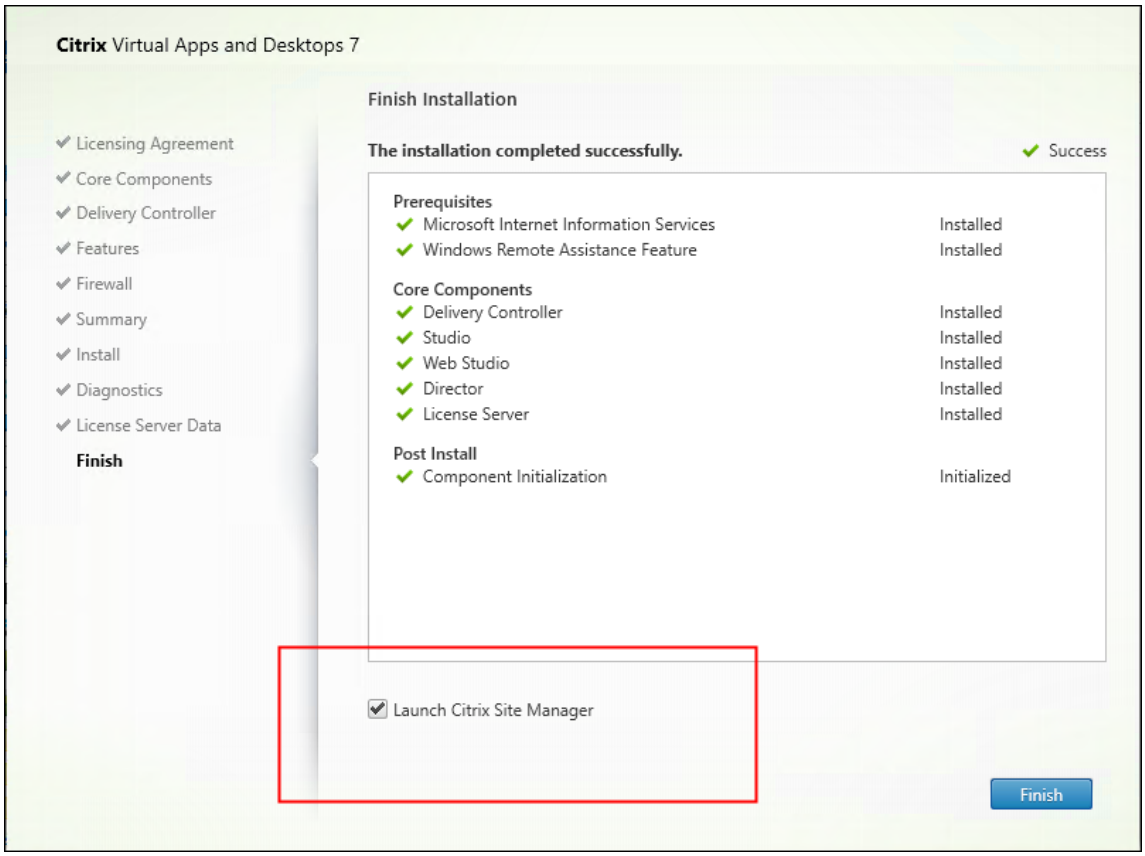
  > 注:
  >
  > – 複数の Delivery Controller を追加できます。Web Studio はランダムな順序で接続を試みます。Web Studio が接続しようとしている Delivery Controller に到達できない場合、Web Studio は自動的に他の Delivery Controller にフォールバックします。

- ［コアコンポーネント］で Director を選択してインストールした場合、ここで追加する Delivery Controller は Web Studio と Director の両方で使用されます。
- 外部パブリック証明機関の証明書を構成せず、エンタープライズ CA の証明書を要求しない場合、Delivery Controller の FQDN を構成するだけで済みます。
- 外部パブリック証明機関の証明書があり、Delivery Controller のパブリック DNS を構成できる場合は、Delivery Controller アドレスとして DNS 名を入力できます。
- エンタープライズ証明機関の証明書を要求して個人の DNS を指定できる場合は、Delivery Controller アドレスとして個人の DNS を追加できます。



- ブラウザーと Web サーバー間、およびブラウザーと Delivery Controller 間の通信を保護するには、Web Studio をホストする IIS Web サイトと Delivery Controller で TLS 暗号化を有効にする必要があります。Delivery Controller に TLS 証明書が構成されていない場合、インストーラーは自己署名証明書を作成し、Delivery Controller の FQDN と localhost を DNS 名の証明書として使用します。TLS 証明書が構成されている場合、インストーラーは何も変更しません。TLS 暗号化について詳しくは、「Web Studio 環境の保護（オプション）」を参照してください。
- Citrix Site Manager が自動で開くように、［完了］ページの ［**Site Manager** を起動する］チェックボックスがデフォルトでオンになっています。後で起動するには、デスクトップの［スタート］メニューを開き、［**Citrix**］**>** ［**Citrix Site Manager**］を選択します。Web Studio を起動する前に、Citrix Site Manager を使用してサイトを作成するか、既存のサイトに参加する必要があります。詳しくは、「サイトのセットアッ

プ」を参照してください。



> 注:
>
> コマンドラインを使用して Web Studio をインストールすることもできます。例: `.\XenDesktopServerSetup.exe /components webstudio /controllers "ddc1.studio.local"/configure_firewall /quiet`。詳しくは、「コマンドラインを使ったインストール」を参照してください。

サイトを設定する

Citrix Virtual Apps and Desktops 環境（サイト）をセットアップするには、ツールの Citrix Site Manager を使用します。ツールは Delivery Controller に自動的にインストールされます

サイトを設定するには、次の手順に従います:

1. Delivery Controller で、デスクトップの［スタート］メニューを開き、［**Citrix**］**>** ［**Citrix Site Manager**］を選択します。
2. Citrix Site Manager で、［サイトの作成］を選択します。サイトのインストールウィザードが表示されます。
3. サイトを作成し、次のように設定を構成します:
    - ［はじめに］ページで、サイトの名前を入力します。

- ［データベース］ページには、サイト、監視、および構成ログの各データベースを設定するための選択肢が含まれています。詳しくは、「手順 3：データベース。
- ［ライセンス］ページでライセンスサーバーのアドレスを指定して、使用（インストール）するライセンスを決定します。詳しくは、「手順 4：ライセンス」を参照してください。

4. ［概要］ページですべての設定を確認し、［送信］をクリックします。

   この Controller の IP アドレスは、サイトに自動的に追加されます。

   > 注:
   >
   > サイトを作成する管理者には、そのサイトのすべての管理タスクの実行権限が設定されます。詳しくは、「管理者権限の委任」を参照してください。

サイトの作成後に新しい Controller をインストールする場合は、Controller をサイトに追加する必要があります。詳細な手順は次のとおりです:

1. この新しい Controller で Citrix Site Manager を実行します。
2. ［**Join an existing site**］を選択します。
3. サイトに既に追加されている Controller のアドレスを入力します。
4. ［**Submit**］をクリックします。

管理用に **Delivery Controller** を **Web Studio** に追加する

Studio 構成ツールを使用して、管理用の Delivery Controller を Web Studio に追加します。このツールは、Web Studio インストールフォルダーにあります。

デフォルトでは、ツールは次のデフォルトフォルダーにインストールされます。

- `C:\Program Files\Citrix\Web Studio\Tool\StudioConfig.exe`

Web Studio で管理するサイトに次の 2 つの Delivery Controller を設定するとします: `ddc1.studio.local`および`ddc2.studio.local`。次の PowerShell コマンドを実行します:

- `.\StudioConfig.exe --server "ddc1.studio.local,ddc2.studio.local"`

> 注:
>
> - このツールには、コンピューター管理者権限が必要です。
> - IIS サーバーのキャッシュ設定が原因で、Delivery Controller 構成の変更がすぐに有効にならない場合があります。すぐに有効にするには、Web Studio サーバーに移動し、インターネットインフォメーションサービス（IIS）マネージャーを開き、［スタートページ］>［サイト］>［Default Web Site］に移動し、［Web サイトの管理］ペインで ［再起動］を選択します。
> - サポートされているすべてのパラメーターを表示するには、`StudioConfig.exe --help`を実

> 行します。

Web Studio を Delivery Controller のプロキシとして構成する（オプション）

デフォルトでは、Web Studio コンソールを使用して環境を管理する場合、Web ブラウザーを介して Web Studio サーバーと Delivery Controller の両方に接続します。Web Studio サーバーを Delivery Controller のプロキシとして構成するオプションが提供されます。その結果、環境を管理するときは、Web Studio サーバーにのみ接続します。

このセクションでは、Web Studio サーバーを Delivery Controller のプロキシとして構成する方法について説明します。Web Studio と Delivery Controller が別々のサーバーにインストールされていることを前提としています。

開始する前に、環境内に必要なコアコンポーネントがすべてインストールされていることを確認します。詳しくは、「コアコンポーネントのインストール」を参照してください。

Web Studio のプロキシモードを有効にするには、次の手順に従います:

1. Web Studio サーバーで、Windows PowerShell を管理者として実行します。
2. `fqdn_of_webstudio_machine`を Web Studio サーバーの FQDN に置き換えて、次のコマンドを実行します。

   ```
   & "c:\Program Files\Citrix\Web Studio\Tool\StudioConfig.exe"--enableproxy --proxyserver "fqdn_of_webstudio_machine"
   ```

   > 注:
   >
   > 負荷分散された Web Studio 展開の場合は、`fqdn_of_webstudio_machine`をロードバランサーサーバー（仮想サーバーとも呼ばれます）の FQDN に置き換えます。詳しくは、「負荷分散された Web Studio 展開のセットアップ」を参照してください。

Web Studio のプロキシモードを無効にするには、次の PowerShell コマンドを実行します:

```
`& "c:\Program Files\Citrix\Web Studio\Tool\StudioConfig.exe" --disableproxy`
```

> 注:
>
> ベストプラクティスとして、外部パブリック証明機関の証明書またはエンタープライズ証明機関（CA）の証明書を使用して、Web Studio 環境を保護することをお勧めします。詳しくは、「Web Studio 環境の保護」を参照してください。

Web Studio へのログイン

Web Studio の Web サイトは`https://<address of the server hosting Web Studio>/Citrix/Studio`にあります。

Web Studio にログオンするには、デスクトップの［スタート］メニューを開き、［**Citrix**］**>** ［**Citrix Web Studio**］を選択します。Web Studio の権限を持つ管理者は、Active Directory ドメインユーザーである必要があります。Web Studio にログオンするときは、次のシナリオを考慮してください:

- サイトの Delivery Controller をまだ指定していない場合。Web Studio に一時的にアクセスできるように、Delivery Controller を指定するよう求められます。
- 現在、指定された Delivery Controller に到達できない場合、Web Studio にログオンできません。接続をテストして、それらの Delivery Controller に到達できることを確認します。または、代わりの Delivery Controller を指定して、Web Studio に一時的にアクセスできるようにします。

次の手順

1. VDA のインストール
2. Web Studio を使用して、次の方法で仮想アプリと仮想デスクトップをユーザーに配信します:
   a) マシンカタログの作成
   b) デリバリーグループの作成
   c) アプリケーショングループの作成（オプション）

VDA のインストール

August 17, 2024

> 重要:
>
> - アップグレードをする予定で、現在のバージョンで Personal vDisk または AppDisk ソフトウェアをインストールしてある場合は、「PvD、AppDisk、およびサポートされていないホストの削除」を参照してください。
> - Citrix 配布のバイナリは、署名されるようになりました。署名されたバイナリは、Citrix が生成した証明書または正規のサードパーティ証明書のいずれかによって検証されていることを示します。

Windows マシン用には 2 種類の VDA があります: マルチセッション OS 対応 VDA とシングルセッション OS 対応 VDA です。(Linux マシン用の VDA については、「Linux Virtual Delivery Agent」を参照してください)。

インストールを開始する前に、「インストールの準備」を確認して準備作業をすべて完了させます。

VDA をインストールする前に、コアコンポーネントをインストールします。VDA をインストールする前にサイトを作成することもできます。

この記事では、VDA をインストールする場合のインストールウィザードの手順を説明します。同等の機能を持つコマンドラインが用意されています。詳しくは、「コマンドラインを使ったインストール」を参照してください。

手順 **1**：製品ソフトウェアをダウンロードしてウィザードを起動する

全製品インストーラーを使用する場合：

1. まだ製品 ISO をダウンロードしていない場合：
   - Citrix アカウント資格情報を使用して、Citrix Virtual Apps and Desktops のダウンロードページにアクセスします。製品の ISO ファイルをダウンロードします。
   - ファイルを解凍します。必要な場合は、ISO ファイルから DVD を作成します。
2. VDA をインストールするイメージまたはマシン上で、ローカル管理者アカウントを使用します。DVD をドライブに挿入するか、ISO ファイルをマウントします。インストーラーが自動的に起動しない場合は、マウントしたドライブにある **AutoSelect** アプリケーションをダブルクリックします。

   インストールウィザードが起動します。

スタンドアロンパッケージを使用する場合：

1. Citrix アカウント資格情報を使用して、Citrix Virtual Apps and Desktops のダウンロードページにアクセスします。適切なパッケージをダウンロードします：
   - `VDAServerSetup_2308.exe`：マルチセッション OS VDA バージョン
   - `VDAWorkstationSetup_2308.exe`：シングルセッション OS VDA バージョン
   - `VDAWorkstationCoreSetup_2308.exe`：シングルセッション OS Core Services VDA バージョン
2. このパッケージを右クリックして、［管理者として実行］を選択します。

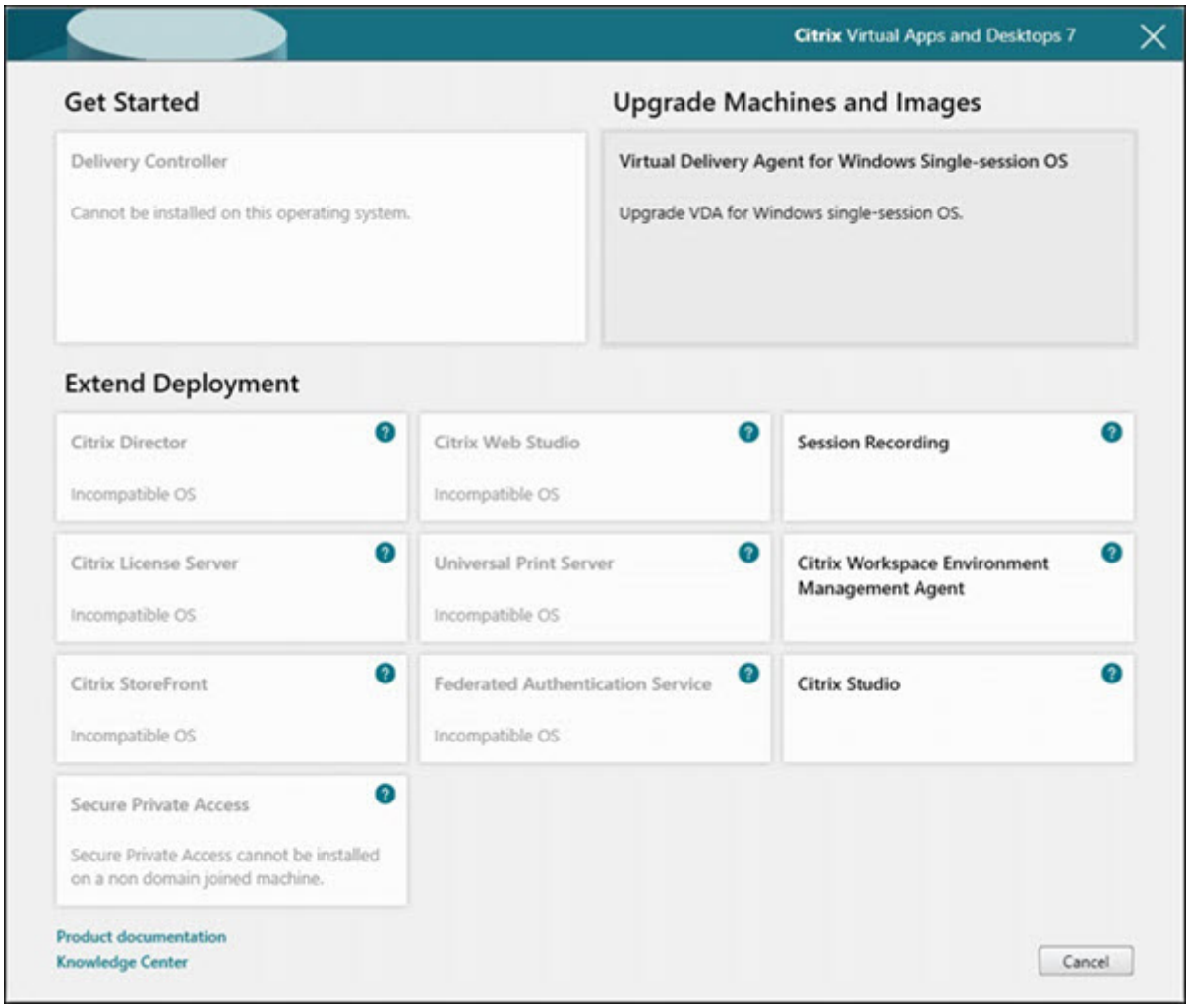
   インストールウィザードが起動します。

手順 **2**：インストールする製品を選択する

インストールする製品（Citrix Virtual Apps または Citrix Virtual Desktops）の横にある ［開始］をクリックします。（マシンに Citrix Virtual Apps コンポーネントまたは Citrix Virtual Desktops コンポーネントが既にインストールされている場合、このページは表示されません。）

コマンドラインオプション：/xenappを使用して Citrix Virtual Apps をインストールします。このオプションを指定しない場合、Citrix Virtual Desktops がインストールされます。

手順 **3**：**VDA** を選択する

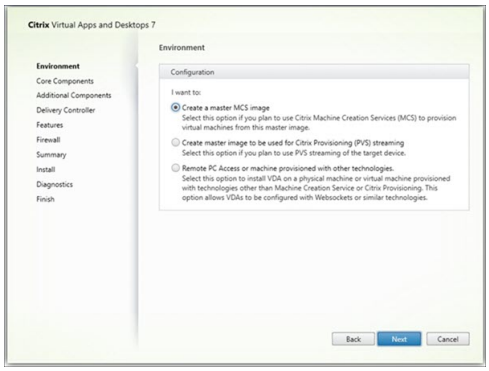


Virtual Delivery Agent エントリを選択します。インストーラーはシングルセッション OS とマルチセッション OS のどちらで実行されているかを認識しているので、適切な種類の VDA のみが提示されます。

たとえば、Windows 2019 マシンでインストーラーを実行すると、マルチセッション OS 対応 VDA のオプションが利用可能になります。シングルセッション OS 対応 VDA のオプションは提示されません。

このバージョンの Citrix Virtual Apps and Desktops でサポートされていない OS で Windows VDA をインストール（またはアップグレード）しようとすると、メッセージが表示され、選択肢についての説明が示されます。

手順 **4**：**VDA** の使用方法を指定する



[環境] ページで、他のマシンをプロビジョニングするためにこのマシンをイメージとして使用するかどうかなど、VDA の使用方法を選択します。

選択したオプションにより、どの Citrix Provisioning ツール（存在する場合）が自動でインストールされるか、および VDA インストーラーの［追加コンポーネント］ページのデフォルト値が決定されます。

VDA をインストールすると、複数の MSI（プロビジョニング用など）が自動的にインストールされます。これらがインストールされないようにするには、コマンドラインで `/exclude` オプションを付けてインストールを行ってください。

次のいずれかのオプションを選択します：

- マスター **MCS** イメージを作成する：仮想マシンのプロビジョニングに Machine Creation Services を使用する場合は、このオプションを選択して仮想マシンイメージに VDA をインストールします。このオプションは、Machine Identity Service をインストールします。これはデフォルトのオプションです。

  コマンドラインオプション：`/mastermcsimage` または `/masterimage`

> 重要：
>
> インストールメディアまたは ISO イメージはローカルにマウントする必要があります。ソフトウェアをインストールする目的で、ネットワークドライブから ISO イメージをマウントすることはサポートされていません。

- **Citrix Provisioning** またはサードパーティのプロビジョニングツールを使用してマスターイメージを作成する：仮想マシンのプロビジョニングに Citrix Provisioning またはサードパーティのプロビジョニングツール（Microsoft System Center Configuration Manager など）を使用する場合は、このオプションを選択して仮想マシンイメージに VDA をインストールします。

  コマンドラインオプション：`/masterpvsimage`

- （マルチセッション OS マシンでのみ表示）サーバーへの仲介接続を有効にする：別のマシンのプロビジョニングにイメージとして使用しない物理マシンまたは仮想マシンに VDA をインストールするには、このオプションを選択します。

  コマンドラインオプション：`/remotepc`

- （シングルセッションOS マシンでのみ表示）リモート **PC** アクセスを有効にする：リモート PC アクセスで使用する物理マシンに VDA をインストールするには、このオプションを選択します。

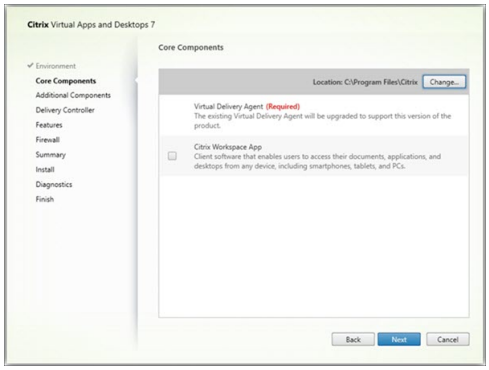
  コマンドラインオプション：`/remotepc`

［次へ］をクリックします。

次の場合、このページは表示されません：

- VDA のアップグレード時
- `VDAWorkstationCoreSetup_2308.exe` 、`VDAServerSetup_2308.exe` 、 または `VDAWorkstationSetup_2308.exe`インストーラーを使用する場合

手順 **5**：インストールするコンポーネントおよびインストール場所を選択する



［コアコンポーネント］ページで次の作業を行います：

- 場所：デフォルトでは、`C:\Program Files\Citrix`に各コンポーネントがインストールされます。ほとんどの展開ではデフォルトで十分です。別の場所を指定する場合は、Network Service アカウントでの`execute`権限が必要です。
- コンポーネント：デフォルトでは、Windows 向け Citrix Workspace アプリは VDA とともにインストールされません。`VDAWorkstationCoreSetup.exe`インストーラーを使用する場合、Windows 向け Citrix Workspace アプリはインストールされないため、このチェックボックスは表示されません。

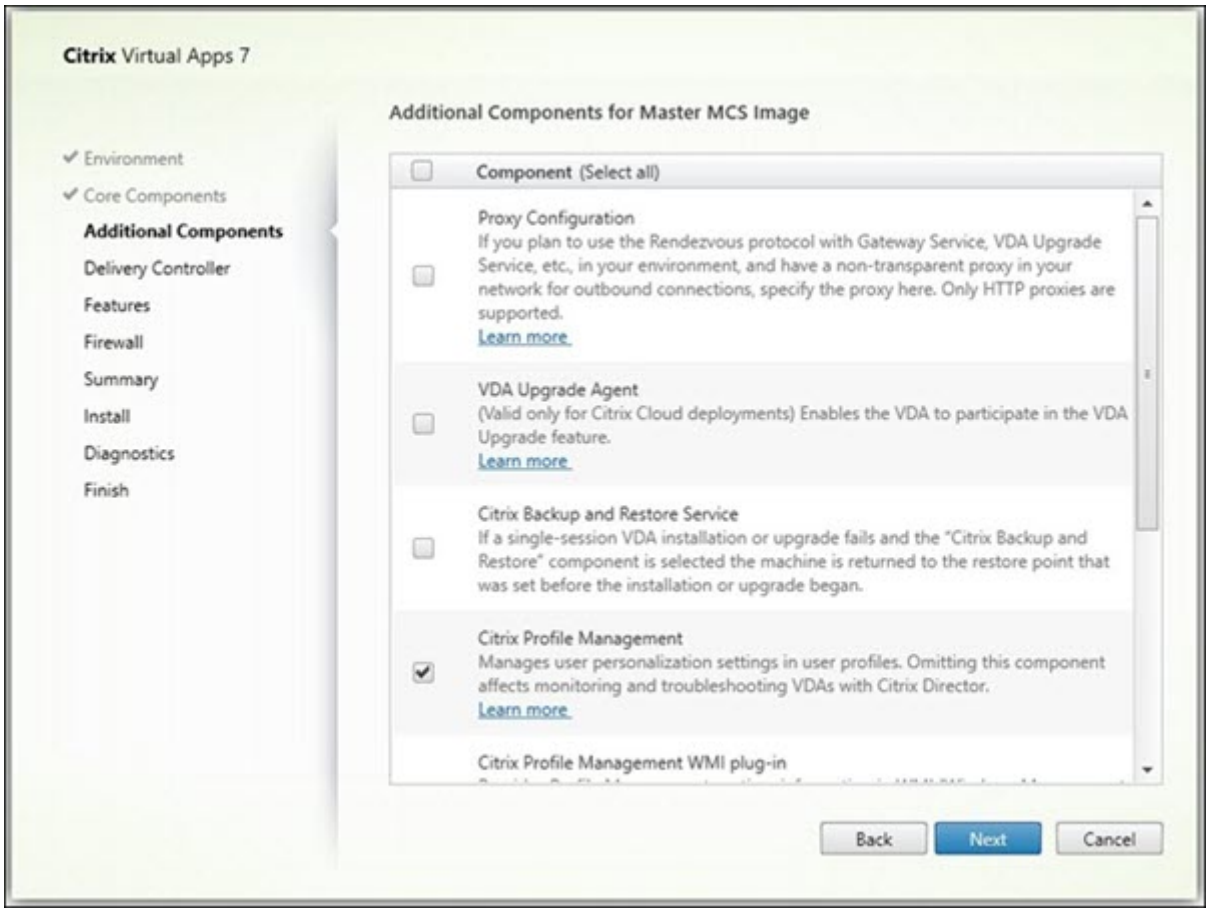
［次へ］をクリックします。

コマンドラインオプション：`/installdir`。VDA および Windows 向け Citrix Workspace アプリをインストールする場合は`/components vda,plugin`

> 注：
>
> 次のシナリオでは、VDA のインストール、アップグレード、またはアンインストール中に Citrix Workspace アプリをインストール、アップグレード、またはアンインストールすることを選択できます：
>
> - VDA のインストール中に、Citrix Workspace アプリをインストールすることを選択できます。デフォルトでは、Citrix Workspace アプリは VDA のインストール中にインストールされません。

- VDA のアップグレード中に、Citrix Workspace アプリが VDA にまだインストールされていない場合は、Citrix Workspace アプリをインストールすることを選択できます。
- VDA のアップグレード中に、Citrix Workspace アプリのバージョンをアップグレードできる場合は、Citrix Workspace アプリをアップグレードするオプションが表示されます。
- VDA のアンインストール中に、Citrix Workspace アプリをアンインストールしないことを選択できます。デフォルトでは、Citrix Workspace アプリは VDA のアンインストール中にアンインストールされます。

手順 **6**: 追加コンポーネントのインストール



[追加コンポーネント] ページには、VDA とともにほかの機能やテクノロジをインストールするかどうかを指定するチェックボックスがあります。コマンドラインインストールでは、`/exclude`オプションまたは`/includeadditional`オプションを指定して、使用可能なコンポーネントを 1 つまたは複数明示的に除外またはインストールすることができます。

次の表に、このページの項目のデフォルト設定を示します。デフォルトの設定は、[環境] ページで選択したオプションによって異なります。

［追加コンポーネント］ページ	［環境］ページ：［マスター MCS イメージを作成する］または［Citrix Provisioning またはサードパーティの…］を選択	［環境］ページ：［サーバーへの仲介接続を有効にする］（マルチセッション OS 対応）または［リモート PC アクセスを有効にする］（シングルセッション OS 対応）を選択
Citrix Personalization for App-V - VDA	未選択	未選択
ユーザー個人設定レイヤー	未選択	このユースケースでは無効なため表示されません。
Citrix Profile Management	選択済み	未選択
Citrix Profile Management WMI プラグイン	選択済み	未選択
Citrix VDA Upgrade Agent	未選択	未選択
Citrix Backup and Restore	未選択	未選択
Citrix MCS IODriver	未選択	未選択
Citrix Rendezvous V2	未選択	未選択

次の場合、このページは表示されません：

- `VDAWorkstationCoreSetup.exe`インストーラーを使用している。また、追加コンポーネント用のコマンドラインオプションはこのインストーラーでは無効です。
- VDA をアップグレードしており、追加コンポーネントが既にすべてインストールされている。追加コンポーネントのいくつかが既にインストールされている場合、このページにはインストールされていないものだけが表示されます。

次のチェックボックスをオンまたはオフにします（コンポーネントは、インストーラーにおいて異なる順序で表示されることがあります）。

- **Citrix Personalization for App-V**： Microsoft App-V パッケージのアプリケーションを使用する場合、このコンポーネントをインストールします。詳しくは、「App-V アプリケーションの展開および配信」を参照してください。

  コマンドラインオプション：インストールする場合は`/includeadditional "Citrix Personalization for App-V - VDA"`、インストールしない場合は`/exclude "Citrix Personalization for App-V - VDA"`。

- **Citrix** ユーザー個人設定レイヤー：ユーザー個人設定レイヤーの MSI をインストールします。詳しくは、「ユーザー個人設定レイヤー」を参照してください。

  このコンポーネントは、シングルセッション Windows 10 マシンに VDA をインストールするときにのみ表示されます。

コマンドラインオプション: インストールする場合は/includeadditional "User Personalization Layer"、インストールしない場合は/exclude "User Personalization Layer"。

- **Citrix Profile Management**: このコンポーネントは、ユーザープロファイル内のユーザーの個人設定を管理します。詳しくは、「Profile Management」を参照してください。

  インストールから Citrix Profile Management を除くと、Citrix Director を使った VDA の監視やトラブルシューティングに影響があります。［ユーザーの詳細］ページの ［個人設定］パネル、および ［エンドポイント］ページの ［ログオン処理時間］パネルに不具合が発生します。［ダッシュボード］ページと ［傾向］ページでは、Profile Management がインストールされているマシンについてのデータしか ［平均ログオン処理時間］パネルに表示されません。

  サードパーティのユーザープロファイル管理ソリューションを使用している場合でも、Citrix Profile Management Service をインストールして実行することを Citrix ではお勧めします。Citrix Profile Management Service の有効化は、必須ではありません。

  コマンドラインオプション:インストールする場合は/includeadditional "Citrix Profile Management"、インストールしない場合は/exclude "Citrix Profile Management"。

- **Citrix Profile Management WMI** プラグイン: このプラグインは、プロファイルプロバイダー、プロファイルの種類、サイズ、ディスク使用率などの Profile Management ランタイム情報を、WMI（Windows Management Instrumentation）オブジェクトに格納して提供します。WMI オブジェクトは、Director にセッション情報を提供します。

  コマンドラインオプション:インストールする場合は/includeadditional "Citrix Profile Management WMI Plug-in"、インストールしない場合は/exclude "Citrix Profile Management WMI Plug-in"。

- **VDA Upgrade Agent**: Citrix DaaS（旧称 Citrix Virtual Apps and Desktops サービス）展開でのみ利用可能。VDA がVDA のアップグレード機能に参加できるようにします。この機能を使用すると、管理コンソールから、直ちに、またはスケジュールされた時間に、カタログの VDA をアップグレードできます。このエージェントがインストールされていない場合は、マシン上で VDA インストーラーを実行することで VDA をアップグレードできます。

  コマンドラインオプション: インストールする場合は/includeadditional "Citrix VDA Upgrade Agent"、インストールしない場合は/exclude "Citrix VDA Upgrade Agent"。

- ストレージ最適化用 **MCSIO** 書き込みキャッシュ: **Citrix MCS I/O** ドライバーをインストールします。詳しくは、「ハイパーバイザー間で共有されるストレージ」および「一時データ用キャッシュの構成」を参照してください。

  コマンドラインオプション: インストールする場合は/includeadditional "Citrix MCS IODriver"、インストールしない場合は/exclude "Citrix MCS IODriver"。

- プロキシ構成：環境内の Gateway サービス、VDA アップグレードサービスなどで Rendezvous プロトコルを使用する場合はこのコンポーネントをインストールし、ネットワークに送信接続用の非透過プロキシがある場合は、ここでプロキシを指定します。HTTP プロキシのみがサポートされています。

  このコンポーネントをインストールする場合は、[**Rendezvous** プロキシの構成] ページでプロキシのアドレス、または PAC ファイルパスを指定します。機能について詳しくは、「Rendezvous プロトコル」を参照してください。

  コマンドラインオプション：インストールする場合は/`includeadditional "Citrix Rendezvous V2"`、インストールしない場合は/`exclude "Citrix Rendezvous V2"`。

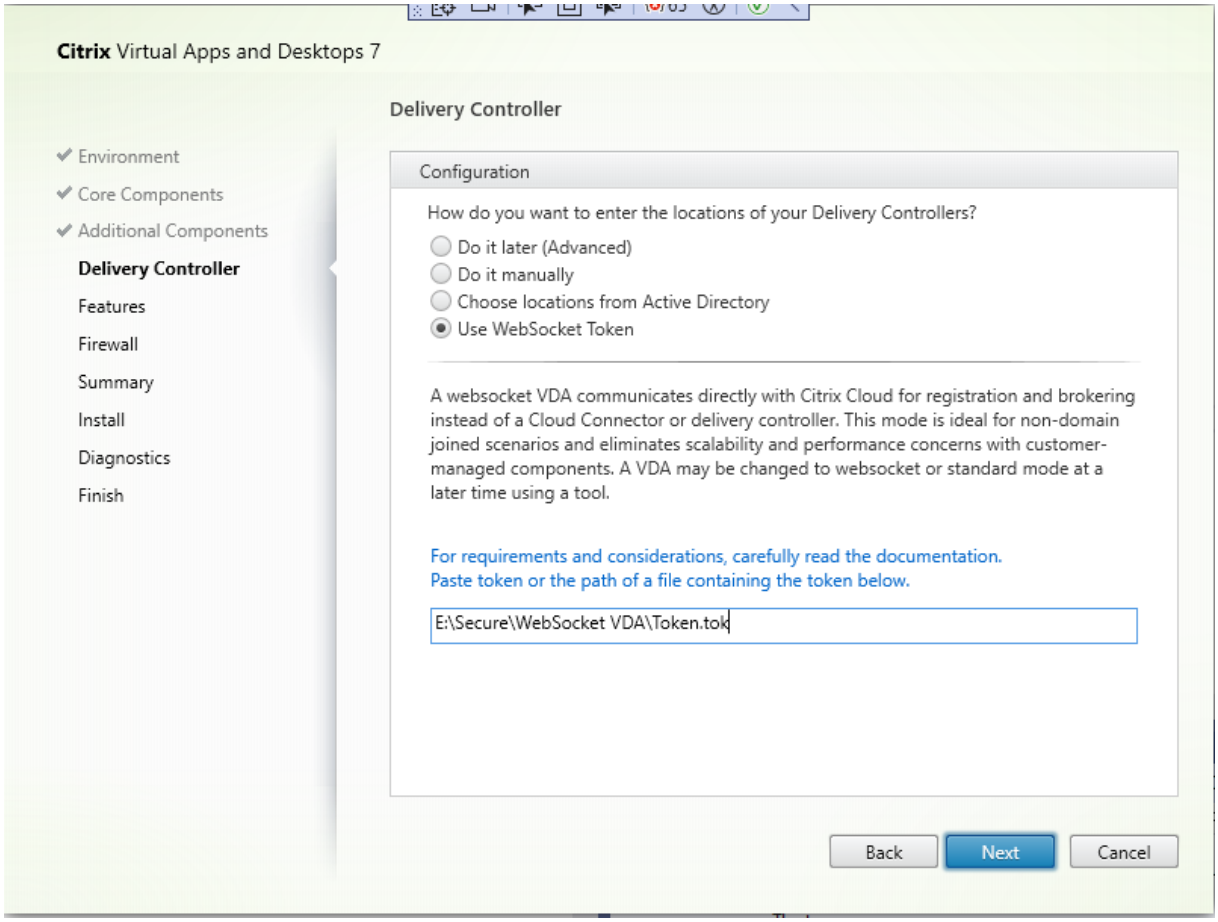
- **Citrix Backup and Restore**： VDA のインストールまたはアップグレードが失敗した場合、このコンポーネントはマシンをインストールまたはアップグレードする前に実行されたバックアップに戻すことができます。

「インストールの準備」で説明されている、Microsoft の前提条件が満たされていることを確認してください。

コマンドラインオプション:インストールする場合は/`includeadditional "Citrix Backup and Restore"`、インストールしない場合は/`exclude "Citrix Backup and Restore"`。

> 注:
>
> MCS ストレージの最適化が有効になっている場合、Windows サーバーまたはデスクトップオペレーティングシステムのバックアップまたは復元が失敗する可能性があります。これを解決するには、メタインストーラーで MCS ストレージ最適化オプションを無効にします。

手順 **7**：**Delivery Controller** アドレス



[**Delivery Controller**] ページで、インストール済みの Controller のアドレスを入力する方法を選択します Citrix では、VDA のインストール時にアドレスを指定することをお勧めします（[手動で指定する]）。VDA は、この情報がないと Controller に登録できません。VDA が登録されない場合、ユーザーはその VDA 上のアプリケーションやデスクトップにアクセスできません。

- 手動で指定する：（デフォルト）：インストールされている Controller の FQDN を入力し、[追加] をクリックします。追加の Controller をインストールした場合は、アドレスも追加します。
- 後で実行（上級）：このオプションを選択すると、ウィザードは続行する前に、選択を確認するよう求めてきます。後でアドレスを指定する場合は、インストーラーを再実行するか、Citrix グループポリシーを使用することができます。ウィザードは、[概要] ページでも確認を求めます。
- **Active Directory** から場所を選択する：マシンがドメインに参加していて、ユーザーがドメインユーザーである場合にのみ有効です。
- **WebSocket** トークンの使用（**Technical Preview**）WebSocket VDA を作成します。WebSocketToken は、必要なトークン用です。
- **Machine Creation Services** で自動的に指定する： MCS を使用してマシンをプロビジョニングする場合のみ有効です。

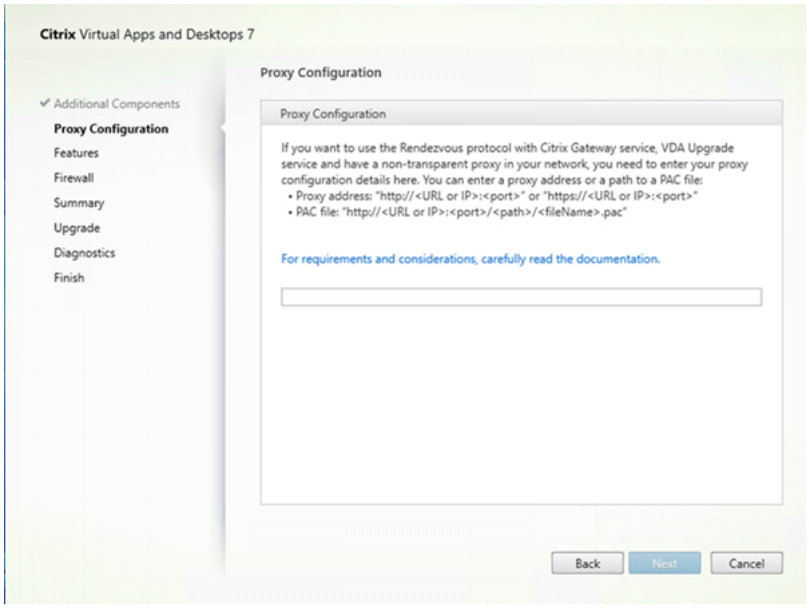
［次へ］をクリックします。［後で実行（上級）］を選択した場合、後でコントローラーのアドレスを指定することを確認するメッセージが表示されます。

そのほかの考慮事項:

- アドレスに使用できるのは、英数字のみです。
- VDA のインストールおよびグループポリシーでアドレスを指定すると、インストール中に行われた設定がポリシーの設定によって上書きされます。
- VDA 登録を行うには、Controller を使用した通信に使用されるファイアウォールポートが開いている必要があります。デフォルトでは、ウィザードの ［ファイアウォール］ページでこのポートの開放が有効化されています。
- （VDA のインストール時またはその後に）Controller のロケーションを指定すると、Controller が追加または削除された場合に、自動更新機能を使用して VDA を更新できます。VDA による Controller の検出方法、および VDA を Controller とともに登録する方法について詳しくは、「VDA 登録」を参照してください。

コマンドラインオプション: `/controllers`

手順 **8**: プロキシ構成



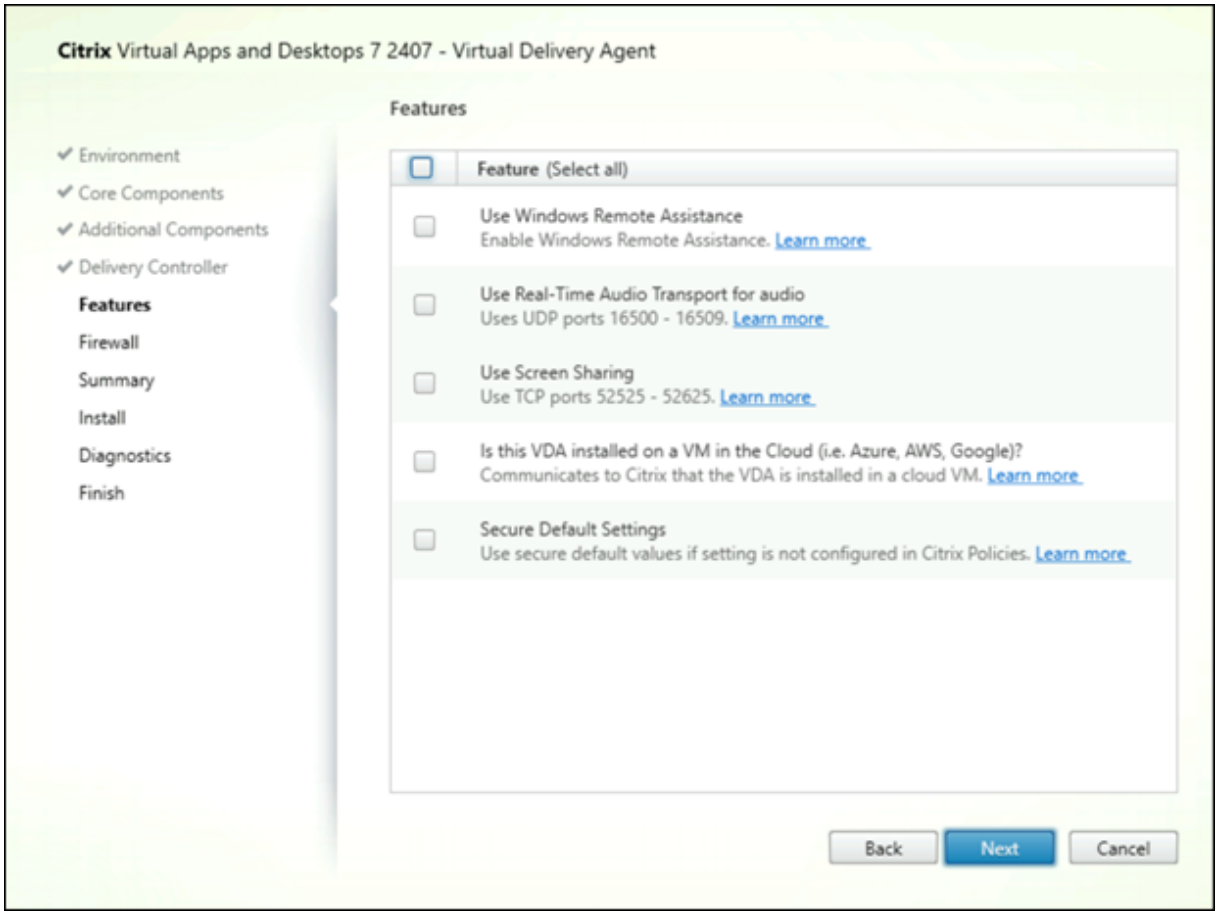
［プロキシの構成］ページは、［追加コンポーネント］ページの ［プロキシの構成］チェックボックスをオンにした場合にのみ表示されます。

1. プロキシアドレスまたは PAC ファイルパスのどちらでプロキシソースを指定するかを選択します。
2. プロキシアドレスまたは PAC ファイルパスを指定します。
   - プロキシアドレスの形式: `http://<url-or-ip>:<port>`
   - PAC ファイルの形式: `http://<url-or-ip>:<port>/<path>/<filename>.pac`

接続テストを成功させるには、プロキシポートのファイアウォールが開いている必要があります。プロキシに接続できない場合は、VDA のインストールを続行するかどうかを選択できます。

コマンドラインオプション：/proxyconfig

手順 **9**：機能を有効または無効にする



［機能］ページで、チェックボックスを使用して、使用する機能を有効または無効にします。

- **Windows** リモートアシスタンスの使用：この機能を有効にすると、Director のユーザーシャドウ機能で、Windows リモートアシスタンスが使用されます。Windows リモートアシスタンスによってファイアウォールで動的ポートが解放されます。（デフォルト = 無効）

  コマンドラインオプション：/enable_remote_assistance

- オーディオにリアルタイムオーディオ転送を使用：ネットワークで Voice over IP が広く使われている場合、この機能を有効化します。この機能を使用すると、遅延が短縮され、損失の多いネットワーク経由の音声復元性が改善されます。オーディオデータを UDP トランスポート経由の RTP を使用して伝送することが可能になります。（デフォルト = 無効）

  コマンドラインオプション：/enable_real_time_transport

- 画面共有の使用：有効にすると、画面共有で使用されるポートが Windows ファイアウォールで開きます。（デフォルト = 無効）

  コマンドラインオプション：/enable_ss_ports

- この **VDA** はクラウドの仮想マシンにインストールされていますか：この設定は、Citrix が、オンプレミスおよびサービス（Citrix Cloud）の VDA 展開でテレメトリのために適切なリソースの場所を特定するのに役立ちます。この機能が、お客様のサービスのご利用に影響を与えることはありません。利用環境で Citrix DaaS を使用する場合は、この設定を有効にします（デフォルト = 無効）。

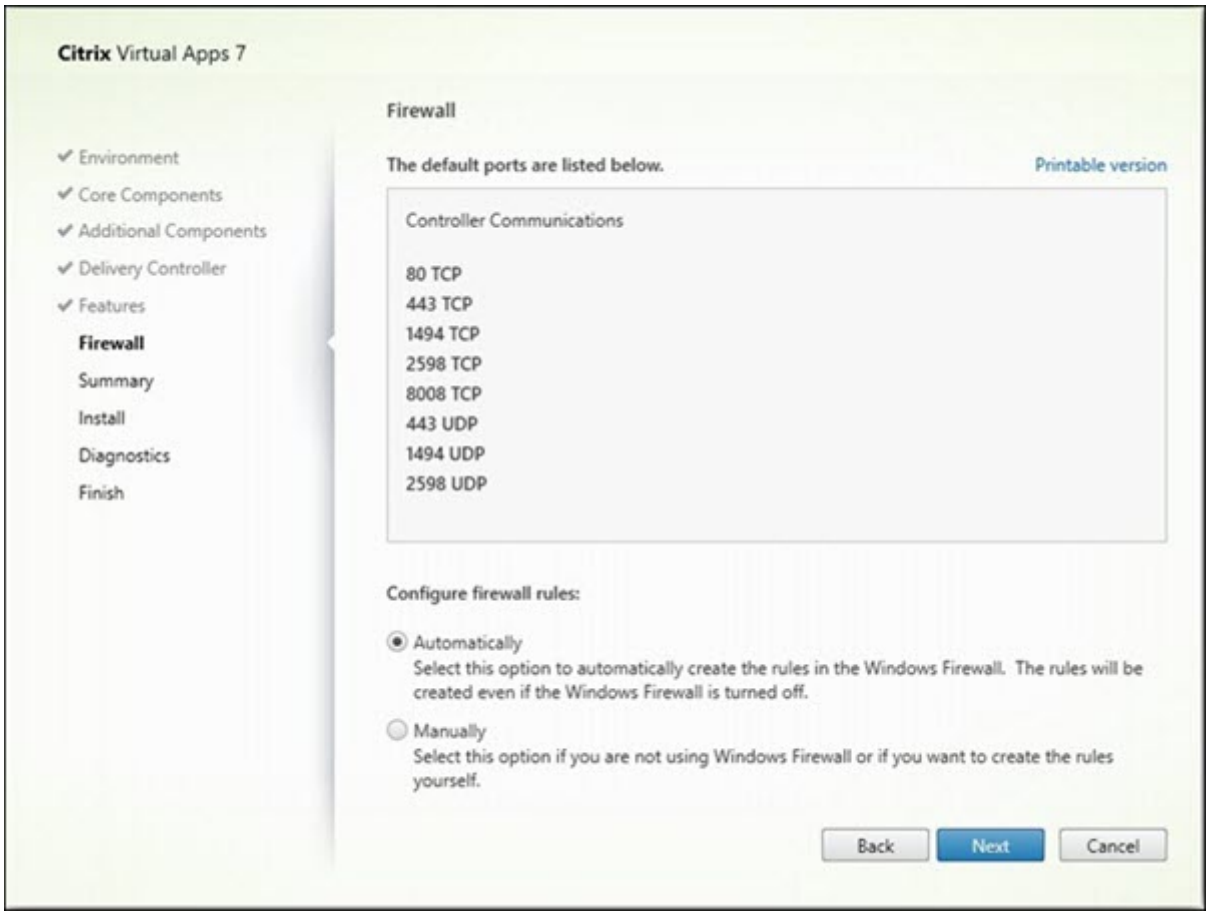
  コマンドラインオプション：/xendesktopcloud

- 安全なデフォルト設定：このオプションは、より安全な初期構成を実現するために、さまざまな機能のデフォルト設定を有効から無効に変更します。関連する機能は、クライアントドライブのリダイレクト、ユーザーフォルダーのリダイレクト、ドラッグアンドドロップ、TWAIN デバイスのリダイレクト、クライアント USB プラグアンドプレイデバイスリダイレクト、クライアントプリンターのリダイレクト、クライアントクリップボードリダイレクト、およびクライアントマイクのリダイレクトです。

コマンドラインオプション：/ENABLE_SECURE_DEFAULTS

［次へ］をクリックします。

手順 **10**：ファイアウォールポート

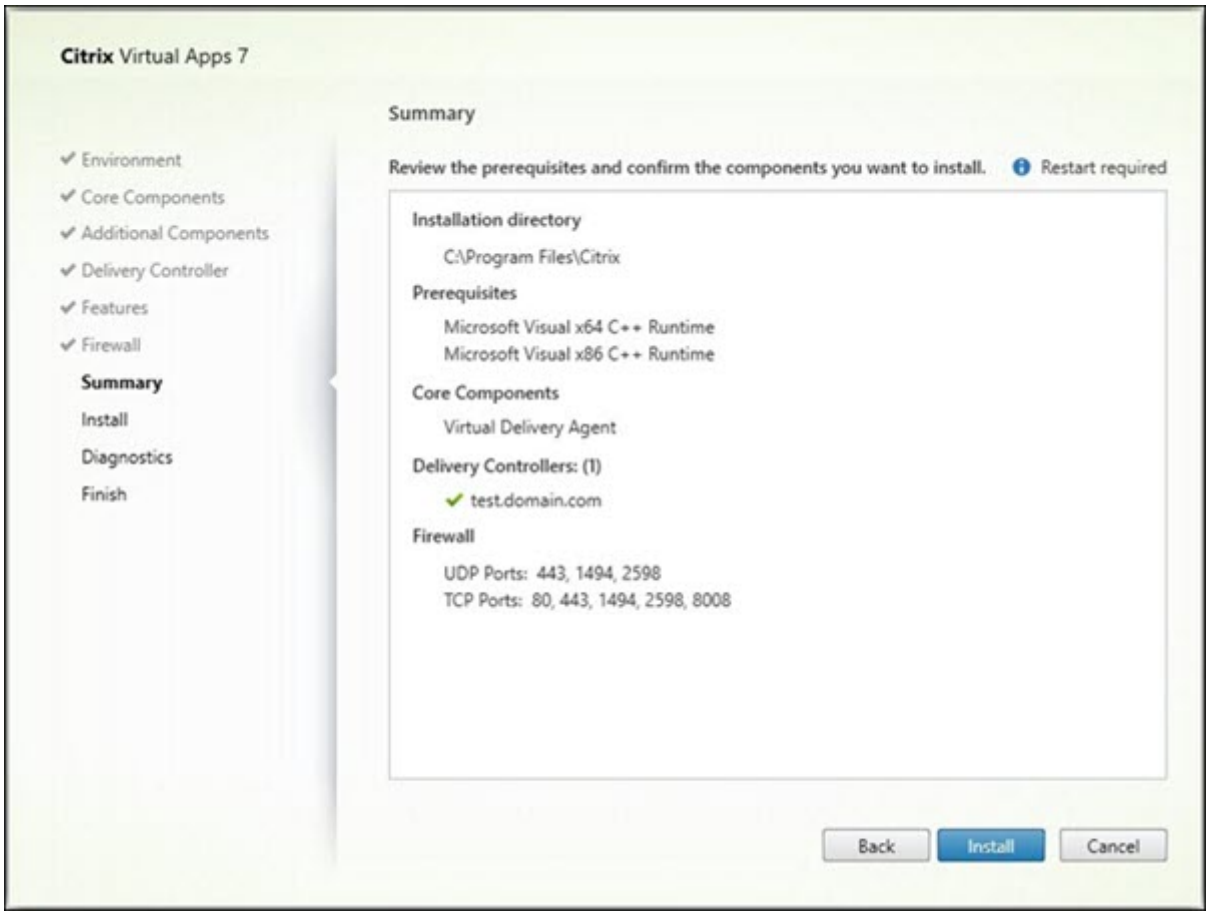


Windows ファイアウォールサービスが実行されている場合、ファイアウォールが無効になっていても、［ファイアウォール］ページに示されているポートがデフォルトで開放されます。ほとんどの展開ではデフォルト設定で十分です。ポートについて詳しくは、「ネットワークポート」を参照してください。

［次へ］をクリックします。

コマンドラインオプション：`/enable_hdx_ports`

手順 **11**：インストール前に前提条件を確認する

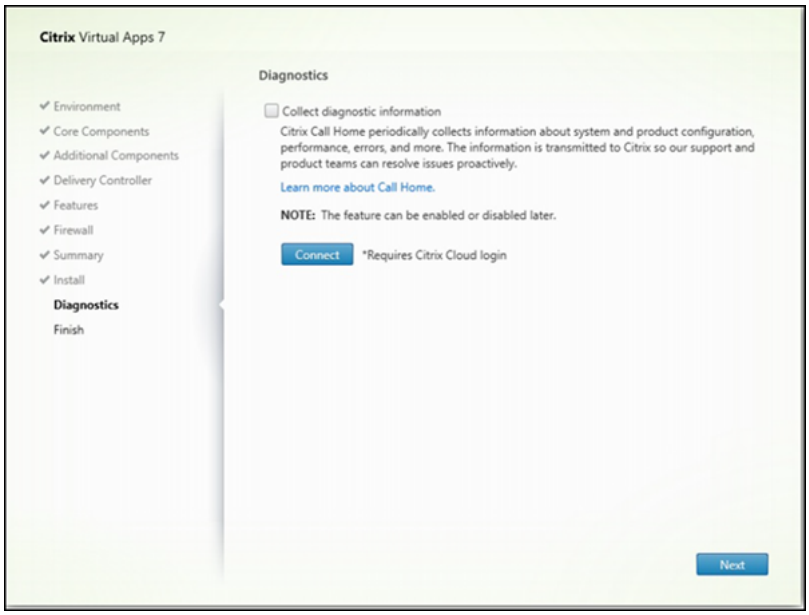


［概要］ページに、インストールされるものが表示されます。［戻る］ボタンをクリックして前のウィザードページに戻り、選択を変更できます。

準備ができたら、［インストール］をクリックします。

前提条件がまだインストールまたは有効化されていない場合、マシンが 1 回以上再起動する場合があります。「インストールの準備」を参照してください。

手順 **12**：診断



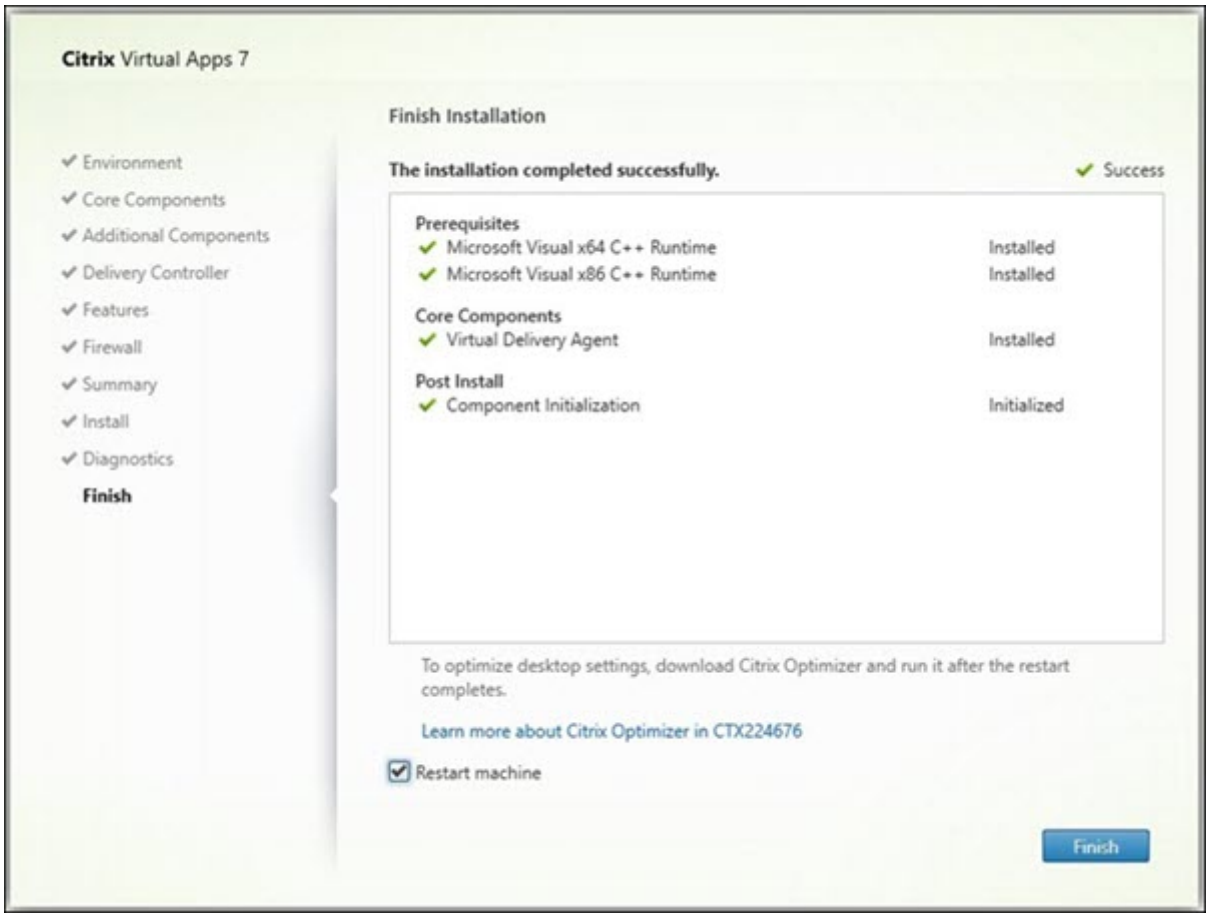
［診断］ページで、Citrix Call Home に参加するかどうかを選択します。参加することを選択する場合（デフォルト）、［接続］をクリックします。求められたら、Citrix アカウント資格情報を入力します。

資格情報が確認されたら（または参加しないことを選択した場合）、［次へ］をクリックします。

全製品インストーラーを使用する場合、［診断情報を収集する］を選択せずに ［診断］ページで ［接続］をクリックすると、［**Citrix Insight Services** に接続します］ダイアログを閉じたあとに ［次へ］ボタンが無効になります。次のページに移動できません。［次へ］ボタンを再度有効にするには、［診断情報を収集する］を選択してすぐに選択解除します。

詳しくは、「Call Home」を参照してください。

手順 **13**：このインストールを完了する



［完了］ページに、すべての前提条件と正常にインストールおよび初期化されたコンポーネントが緑色のチェックマークで示されます。

［完了］をクリックします。デフォルトでは、マシンは自動的に再起動します自動再起動を無効にすることもできますが、マシンを再起動するまで VDA は使用できません。

次の手順

必要に応じて上の手順を繰り返し、他のマシンまたはイメージ上に VDA をインストールします。

すべての VDA をインストールしたら、Studio を起動します。サイトをまだ作成していない場合は、そのタスクのガイドが Studio により自動的に表示されます。それが済んだら、ガイドに従ってマシンカタログ、デリバリーグループを作成します。次を参照してください：

- サイトの作成
- マシンカタログの作成
- デリバリーグループの作成

Citrix Optimizer

Citrix Optimizer は、さまざまなコンポーネントを削除して最適化することで、Citrix の管理者が VDA を最適化できるよう支援する Windows OS 用のツールです。

VDA をインストールして最後の再起動を完了したら、Citrix Optimizer をダウンロードしてインストールします。CTX224676を参照してください。CTX の記事には、ダウンロードパッケージに加えて、Citrix Optimizer のインストールと使用に関する手順が含まれています。

VDA のカスタマイズ

VDA をカスタマイズする場合:

1. プログラムの削除と変更を行う Windows のコントロールパネルで、[**Citrix Virtual Delivery Agent**] または [**Citrix Remote PC Access/VDI Core Services VDA**] を選択します。次に右クリックして [変更] を選択します。
2. [**Virtual Delivery Agent** 設定のカスタマイズ] を選択します。インストーラーが起動したら、次を変更できます。
    - Controller のアドレス
    - Controller への登録に使用される TCP/IP ポート（デフォルトは 80）
    - Windows ファイアウォールポートを自動的に開放するかどうか

トラブルシューティング

- Citrix がコンポーネントのインストールの結果を報告する方法については、「Citrix インストールリターンコード」を参照してください。
- デリバリーグループの Studio 表示では、[詳細] ペインの [インストール済み **VDA** のバージョン] エントリがマシンにインストールされているバージョンではないことがあります。マシンの Windows の [プログラムと機能] には、VDA の実際のバージョンが表示されます。
- インストール後、VDA は Delivery Controller に登録されるまでユーザーにアプリやデスクトップを配信することはできません。

  VDA の登録方法および登録の問題のトラブルシューティングについては、「VDA 登録」を参照してください。

既知の制限事項

Windows 向け Citrix Workspace アプリバージョン 1912 以前を使用すると、しばらくするとセッションが切断されます。この問題は、Citrix Workspace アプリの新しい LTSR および CR バージョンで修正されています。
サポートされているリリースバージョンについて詳しくは、Windows 向け Citrix Workspace アプリ/Citrix Receiver for Windows 長期サービスリリースを参照してください。

VDA インストールに関連した Windows Defender アクセス制御の構成

August 17, 2024

お客様は、署名されていないバイナリの読み込みを禁止するように Windows Defender アクセス制御（WDAC）設定を構成します。したがって、VDA インストーラー経由で配布される署名されていないバイナリは禁止され、これによって VDA のインストールが制限されます。

Citrix は現在、Citrix が生成したすべてのバイナリに Citrix コード署名証明書を使用して署名しています。さらに、当社製品とともに配布されるサードパーティのバイナリに、それらのサードパーティのバイナリが信頼できるバイナリであることを証明する証明書で署名します。

> 重要:
>
> 署名されていないサードパーティのバイナリを含む古い VDA から、署名されたバイナリを含む新しい VDA バージョンにアップグレードすると、アップグレードされたマシンに署名されたバイナリが配置されない場合があります。
> これは、システムをアップグレードしてもバイナリが同じバージョンに置き換えられない OS 内のメカニズムによるものです。
> サードパーティのバイナリは署名されていますが、サードパーティによって管理されているバージョンは Citrix によって更新できないため、これらのバイナリは更新されません。この制限を回避するには、以下を実行してください:
>
> 1. バイナリを許可リストに含めます。これにより、バイナリに署名する必要がなくなります。
> 2. 古い VDA をアンインストールし、新しい VDA をインストールします。これは新規 VDA インストールに似たプロセスであり、署名されたバージョンがインストールされます。

ウィザードを使用して新しい基本ポリシーを作成する

WDAC を使用すると、システム上で実行する信頼できるバイナリを追加できます。WDAC のインストール後、**Windows Defender Application Control Policy Wizard** が自動的に開きます。

バイナリを追加するには、新しい基本 WDAC ポリシーを作成する必要があります。このセクションでは、基本ポリシーを作成するための Citrix 推奨ガイドラインについて説明します。

- **Signed and Reputable Mode** を 基本テンプレートとして選択します。これは、Windows オペレーティング コンポーネント、Microsoft ストアからインストールされたアプリ、すべての Microsoft 署名済みソフトウェア、およびサードパーティの Windows ハードウェア互換ドライバーを承認するためです。
- **Audit Mode** を有効にすると、新しい Windows Defender Application Control ポリシーを適用する前にテストできるようになります。
- ファイル規則のカスタム規則を追加することで、アプリケーションが識別され信頼されるレベルを指定し、参照ファイルを提供します。規則の種類として「Publisher」（発行元）を選択すると、Citrix 証明書のいずれかによって署名された参照ファイルを選択できます。

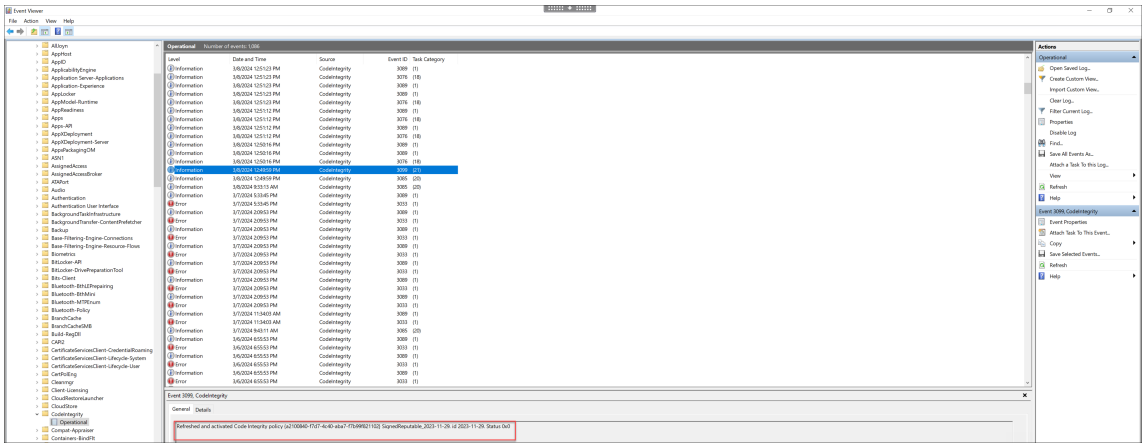
- 規則を追加したら、.XMLおよび.CIPファイルが保存されているフォルダーに移動します。.XMLファイルには、ポリシーで定義されているすべての規則が含まれています。規則を変更、追加、または削除するようにこれを構成できます。
- WDAC ポリシーを展開する前に、.XMLファイルをバイナリ形式に変換する必要があります。WDAC ファイルは、.XMLファイルを.CIPファイルに変換します。
- .CIPファイルをコピーして「C:\WINDOWS\System32\CodeIntegrity\CiPolicies\Active」に貼り付け、マシンを再起動します。生成されたポリシーは監査モードで適用されます。
- 基本ポリシーを作成する手順については、「ウィザードを使用した新しい基本ポリシーの作成」を参照してください。

このポリシーを適用すると、WDAC は指定された発行元/CA によって署名された Citrix ファイルについて警告しません。

同様に、サードパーティによって署名されたファイルに対して発行元レベルの規則を作成することもできます。

適用されたポリシーを確認する

1. マシンを再起動した後、イベントビューアーを開き、[**Aplications and Services Logs**] > [**Microsoft**] > [**Windows**] > [**CodeIntegrity**] > [**Operational**] に移動します。
2. 適用されたポリシーがアクティブになっていることを確認します。



3. ポリシーに違反したログを探し、そのファイルのプロパティを確認します。まず、署名されていることを確認します。署名されておらず、このマシンが VDA アップグレードを実行後の場合は、上記の制限で説明したケースである可能性が高くなります。署名されている場合、このファイルは、前述のように代わりの証明書で署名されている可能性があります。

Citrix 証明書で署名された Citrix 生成ファイルの例は C:\Windows\System32\drivers\picadm.sysです。
Citrix サードパーティ証明書で署名されたサードパーティバイナリの例はC:\Program Files\Citrix\IcaConfigTool\Microsoft.Practices.Unity.dllです。

スクリプトを使用した **VDA** のインストール

August 17, 2024

> 注:
>
> Citrix は、顧客の実稼働環境に合わせて調整されたスクリプトによって引き起こされる問題について責任を負いません。インストールに関連する Citrix の問題については、Citrix サポートポータルを使用してテクニカルサポートケースを開き、関連するインストールログを添付します。

この記事は、Windows オペレーティングシステムがインストールされたマシンへの VDA のインストールに適用されます。Linux オペレーティングシステムの VDA については、「Linux Virtual Delivery Agent」を参照してください。

インストールメディアには、Active Directory 環境のマシンで Virtual Delivery Agent（VDA）をインストール、アップグレード、または削除するサンプルスクリプトが収録されています。また、このスクリプトを使って、Machine Creation Services および Citrix Provisioning（旧称 Provisioning Services）のマスターイメージを管理することもできます。

以下のアクセス権限が必要です。

- スクリプトを実行するには、VDA インストールコマンドがあるネットワーク共有に対するすべてのユーザーの読み取りアクセスが必要です。インストールコマンドは、完全な製品 ISO では`XenDesktopVdaSetup.exe`、スタンドアロンインストーラーでは`VDAWorkstationSetup.exe`または`VDAServerSetup.exe`です。
- ログの詳細は各ローカルマシンに保存されます。また、レビューおよび分析のために結果ログをネットワーク上に保存する場合は、そのネットワーク共有に対するすべてのユーザーの読み取りおよび書き込みアクセスが必要です。

スクリプトの実行結果をチェックするには、ネットワーク共有のログを調べます。このログには、スクリプトログ、インストーラーログ、および MSI インストールログが含まれます。各インストールまたは削除に関するログは、日時を示すフォルダー内に保存されます。フォルダー名には、操作の結果として PASS または FAIL のプレフィックスが付きます。失敗したインストールまたは削除処理を検索できるように、ネットワーク共有を使用します。これにより、ターゲットマシンのローカルドライブに代わるツールが提供されます。

インストールを始める前に、「インストールの準備」を読んで、必要なタスクを完了しておいてください。

スクリプトを使って **VDA** をインストールまたはアップグレードする

1. インストールメディアの\Support\AdDeploy\にある **InstallVDA.bat** サンプルスクリプトを開きます。スクリプトをカスタマイズする前に、元のスクリプトをバックアップしておくことをお勧めします。
2. スクリプトを編集します：

- インストールする VDA のバージョンを指定します：SET DESIREDVERSION。完全な値は、インストールメディアの ProductVersion.txt ファイルに記載されています。ただし、完全に一致させる必要はありません。
- 実行するインストーラーのネットワーク共有を指定します。レイアウトのルート（ツリーの最上位）を指定します。スクリプトにより、適切なバージョンのインストーラー（32 ビットまたは 64 ビット）が自動的に実行されます。例：SET DEPLOYSHARE=\\fileserver1\share1。
- オプションとして、ログを保存するためのネットワーク共有を指定します。例：SET LOGSHARE =\\fileserver1\log1)。
- 「コマンドラインを使ったインストール」の説明に従って、VDA の構成オプションを指定します。/quietおよび/norebootオプションはスクリプトにデフォルトで含まれており、必須です：SET COMMANDLINEOPTIONS=/QUIET /NOREBOOT。

3. グループポリシースタートアップスクリプトを使って、マシンが存在する組織単位にスクリプトを割り当てます。VDA をインストールするマシン以外のものがこの組織単位に属していないことを確認してください。組織単位内のマシンの再起動時にスクリプトが実行され、サポートされるオペレーティングシステムの各マシン上に VDA がインストールされます。

スクリプトを使って **VDA** を削除する

1. インストールメディアの\Support\AdDeploy\からサンプルスクリプトの UninstallVDA.bat を開きます。スクリプトをカスタマイズする前に、元のスクリプトをバックアップしておくことをお勧めします。
2. スクリプトを編集します。
   - 削除する VDA のバージョンを指定します：SET CHECK_VDA_VERSION。完全な値はインストールメディアの ProductVersion.txt ファイルに記述されています（7.0.0.3018 など）。ただし、完全に一致させる必要はありません。
   - オプションとして、ログを保存するためのネットワーク共有を指定します。
3. グループポリシースタートアップスクリプトを使って、マシンが存在する組織単位にスクリプトを割り当てます。VDA を削除するマシン以外のものがこの組織単位に属していないことを確認してください。組織単位内のマシンの再起動時にスクリプトが実行され、各マシンから VDA が削除されます。

トラブルシューティング

- スクリプトにより、スクリプトの進捗を示す内部ログファイルが生成されます。スクリプトは、展開の起動後すぐにKickoff_VDA_Startup_Scriptログをネットワーク共有にコピーします。これにより、処理全体が実行中であることを確認できます。このログがネットワーク共有にコピーされない場合は、ローカルマシンを調べることでトラブルシューティングを実行します。スクリプトにより、各マシンの%temp%フォルダーに以下の 2 つのデバッグログファイルが生成されます。
  - Kickoff_VDA_Startup_Script_<DateTimeStamp>.log

  - VDA_Install_ProcessLog_<DateTimeStamp>.log

  これらのログから、次の点を確認します。

  - スクリプトが正しく実行されたかどうか。
  - ターゲットのオペレーティングシステムが正しく検出されているかどうか。
  - DEPLOYSHARE共有でROOT（AutoSelect.exeファイルを含んでいるフォルダー）が正しく構成されているかどうか。
  - DEPLOYSHAREおよびLOGで指定した両方のネットワーク共有にアクセスできるかどうか。

- Citrix がコンポーネントのインストールの結果を報告する方法については、「Citrix インストールリターンコード」を参照してください。
- デリバリーグループの Studio 表示では、［詳細］ペインの ［インストール済み **VDA** のバージョン］エントリがマシンにインストールされているバージョンではないことがあります。マシンの［プログラムと機能］には、VDA の実際のバージョンが表示されます。
- インストール後、VDA は Delivery Controller に登録されるまでユーザーにアプリやデスクトップを配信することはできません。

  VDA の登録方法および登録の問題のトラブルシューティングについては、「VDA 登録」を参照してください。

サードパーティの **VDA** 展開方法

August 17, 2024

Microsoft System Center Configuration Manager（SCCM）または同様のソフトウェア配信ツール（Ansible や Microsoft Intunes など）を使用して Virtual Delivery Agent（VDA）を正常に展開するには、VDA インストーラーを一連の手順で使用することを Citrix ではお勧めします。

> 注:
>
> この記事では、Citrix が環境をテストした方法に基づいた推奨事項のみについて説明します。これらの手順は、必要に応じてカスタマイズできます。Citrix は、お客様がニーズに合わせて追加された更新や調整については責任を負いません。

- SCCM を使用した VDA のインストール
- Ansible を使用した VDA のインストール
- Microsoft Intune を使用した VDA のインストール

SCCM を使用した VDA のインストール

August 17, 2024

概要

Microsoft Endpoint Configuration Manager（旧称 System Center Configuration Manager（SCCM））は、企業全体のデバイスとアプリケーションの管理、展開、セキュリティを可能にする Windows 製品です。

> 注:
>
> 以下の記事では、Citrix が環境をテストした方法に基づいた推奨事項のみについて説明します。これらの手順は、必要に応じてカスタマイズできます。Citrix は、お客様がニーズに合わせて追加された更新や調整については責任を負いません。

推奨事項

- SCCM または同様のソフトウェア配信ツールを使用して Virtual Delivery Agent（VDA）を正常に展開するには、VDA インストーラーを手順どおりに使用することを Citrix ではお勧めします。
- VDA のインストールまたはアップグレードの一部として VDA Cleanup Utility を使用することはお勧めしません。VDA Cleanup Utility は、以前に VDA インストーラーで失敗した場合にのみ使用してください。

はじめに

VDA のインストール中に必要な再起動回数は、環境によって異なります。例:

- 以前のソフトウェアインストールからの更新や再起動が保留になっている場合は、再起動が必要になることがあります。
- 以前に別のプロセスによってロックされていたファイルは、更新が必要になり追加で再起動が必要になる場合があります。
- VDA インストーラーの一部のオプションコンポーネント（Citrix Profile Management、Citrix Files など）は、再起動が必要な場合があります。
- VDA をアップグレードする場合、VDA がインストールされているマシンは、セッションがなく、メンテナンスモードである必要があります。
- マシン上で VDA インストールを初めて実行すると、使用されている VDA インストーラーがそのマシン上にコピーされます。
  VDA のインストールについて詳しくは、「インストーラー」を参照してください。

SCCM のタスクシーケンサーにより、必要なすべての再起動が管理されます。

SCCM を使用して VDA を展開するための主な手順

次の手順では、仮想マシン上で SCCM を使用して VDA を展開する方法について説明します。

1. VDA をインストールします。
2. 組織単位（OU）を作成します。
3. マシンを検証します。
4. VDA を使用してコンテンツを配布します。

手順 1：VDA のインストール

すべての前提条件を確認したら、**SCCM** のタスクシーケンサーを使用して次のタスクを完了します：

1. インストールメディアのアクセス可能なコピーから、または VDA スタンドアロンインストーラーの 1 つからインストールします：

   - VDAWorkstationSetup_XXXX.exe
   - VDAServerSetup_XXXX.exe
   - VDAWorkstationCoreSetup_XXXX.exe

   VDA インストーラーについて詳しくは、「インストーラー」を参照してください。

   > 注：
   >
   > VDA をアップグレードする場合、VDA がインストールされているマシンは、セッションがなく、メンテナンスモードである必要があります。

2. マシン上で VDA インストールを初めて実行すると、使用されている VDA インストーラーがそのマシン上にコピーされます。

   - VDAWorkstationCoreSetup_XXXX.exe以外の VDA インストーラーを使用している場合、VDA インストーラーは%ProgramData%\Citrix\XenDesktopSetup\XenDesktopVdaSetup.exeにコピーされます。
   - VDAWorkstationCoreSetup_XXXX.exeを使用すると、VDA インストーラーは%ProgramData%\Citrix\XenDesktopSetup\XenDesktopRemotePCSetup.exe.にコピーされます

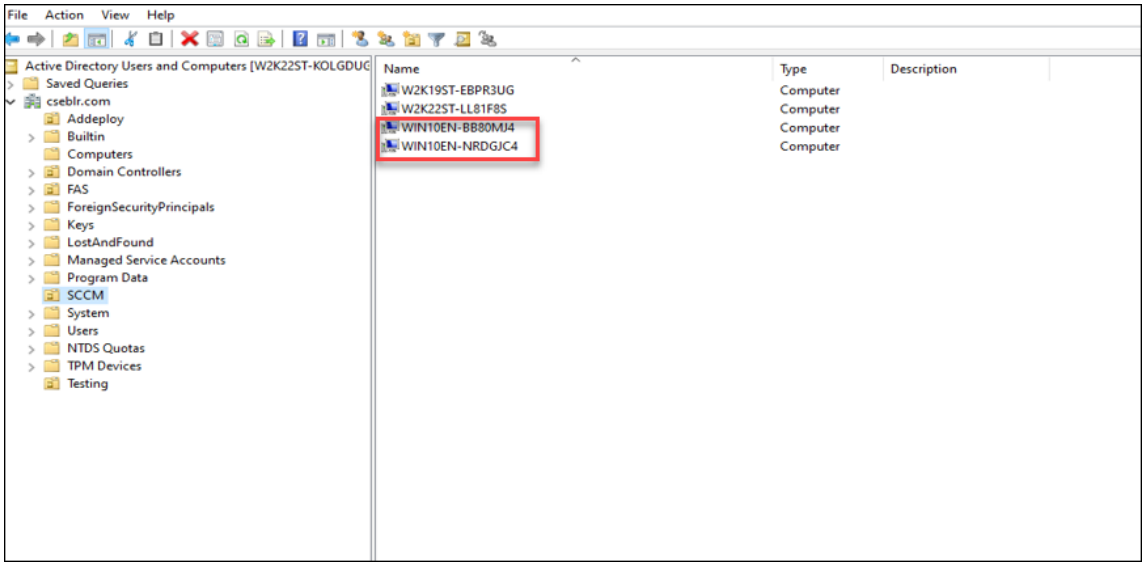
3. VDA インストーラーのディレクトリの場所もレジストリHKEY_LOCAL_MACHINE\SOFTWARE\Citrix\MetaInstall” “MetaInstallerInstallLocation”に保存されます。
4. 既存のコマンドラインオプションに、コマンドラインオプション /NOREBOOT、/NORESUME、/QUIETを追加します。

   - /QUIET：SCCM がインストールプロセスを制御できるように、インストール中にユーザーインターフェイスを表示しないでください。

- /NOREBOOT：VDA インストーラーが自動的に再起動されないようにします。SCCM は、必要に応じて再起動をトリガーします。
- /NORESUME：通常、インストール中に再起動が必要な場合、VDA インストーラーは Runonce レジストリキー（\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce）を設定します。マシンが再起動されると、Windows はこのキーを使用して VDA インストーラーを起動します。これは、SCCM がインストールをモニターして終了コードをキャプチャすることができないため、SCCM の問題です。

手順 **2**：組織単位（**OU**）を作成

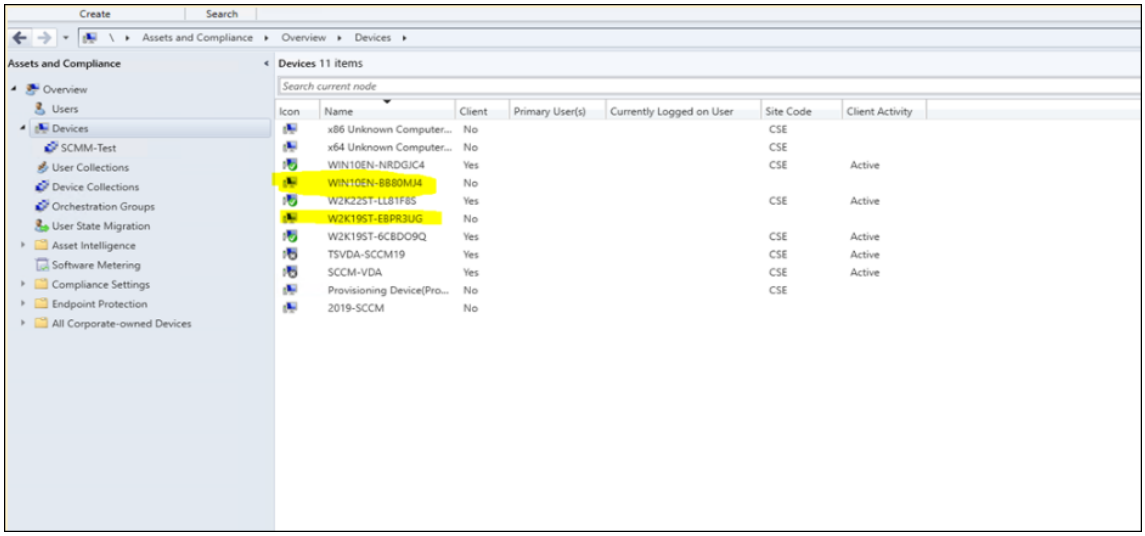
1. OU に追加するドメインに参加している仮想マシンを 2 台作成します。仮想マシンが最初に作成されると、それらは **Computers** フォルダーに格納されます。仮想マシンを **SCCM** フォルダーに移動します。
   例：WIN10EN-BB80MJ4.cseblr.com
   W2K19ST-EBPR3UG.cseblr.com

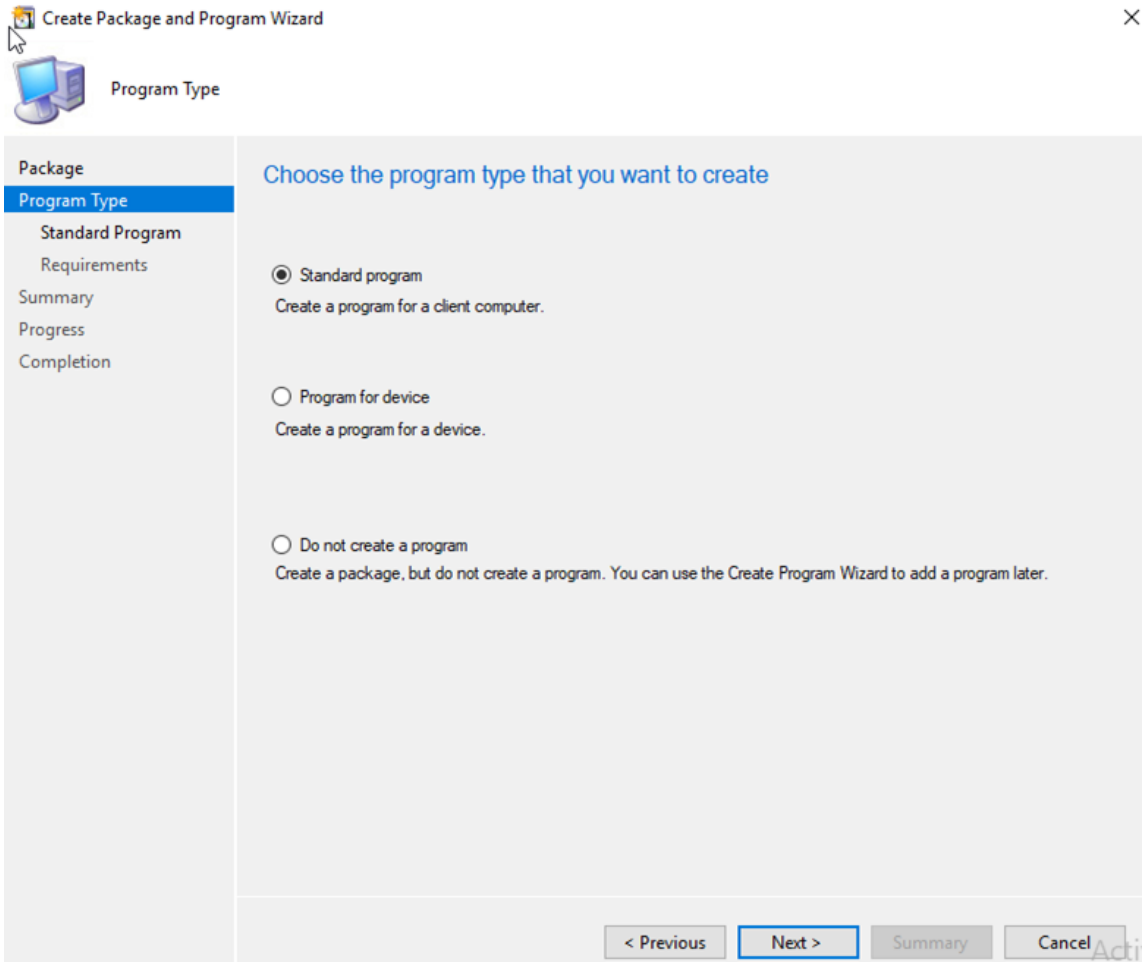


2. Microsoft Configuration Manager で\Administration\Overview\Hierarchy Configuration\Discovery Methods\に移動します。
3. [**Active Directory System Discovery**]をクリックし、[**Enable Active Directory System Discovery**]チェックボックスを選択して、新しく作成された仮想マシンの自動検出を有効にします。
4. 新しいコンテナを選択するには、  アイコンをクリックします。
5. [**Location**]セクションで、SCCM 仮想マシンが格納されている場所へのパスを追加します。
6. \Administration\Overview\Site Configuration\Sitesに移動し、SCCM VDA を右クリックします。

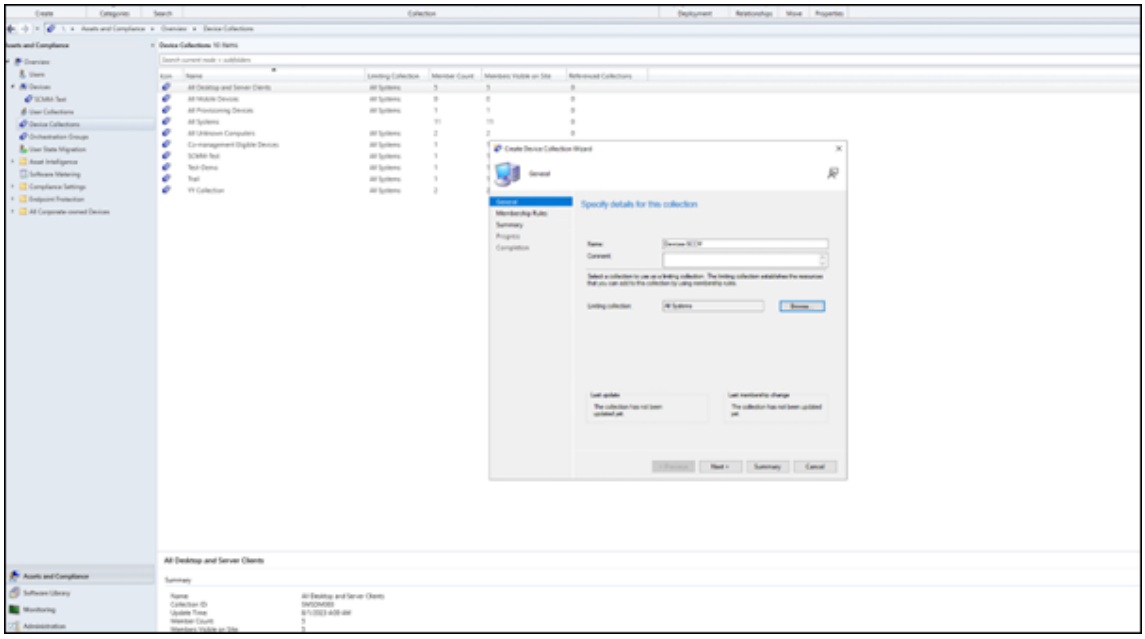
7. ［クライアントインストール設定］>［クライアントプッシュインストール］を選択します。［クライアントプッシュインストールのプロパティ］ウィンドウが開きます。

8. 仮想マシンを`Enabled`に設定すると、次の画像に示すように仮想マシンの一覧が表示されます。

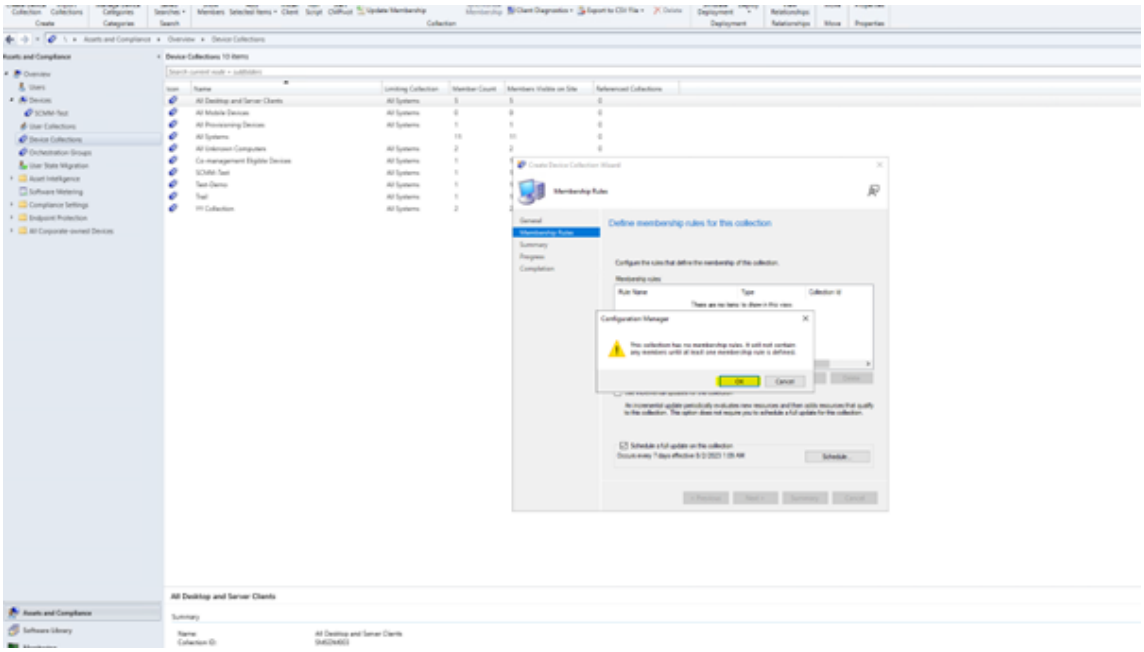




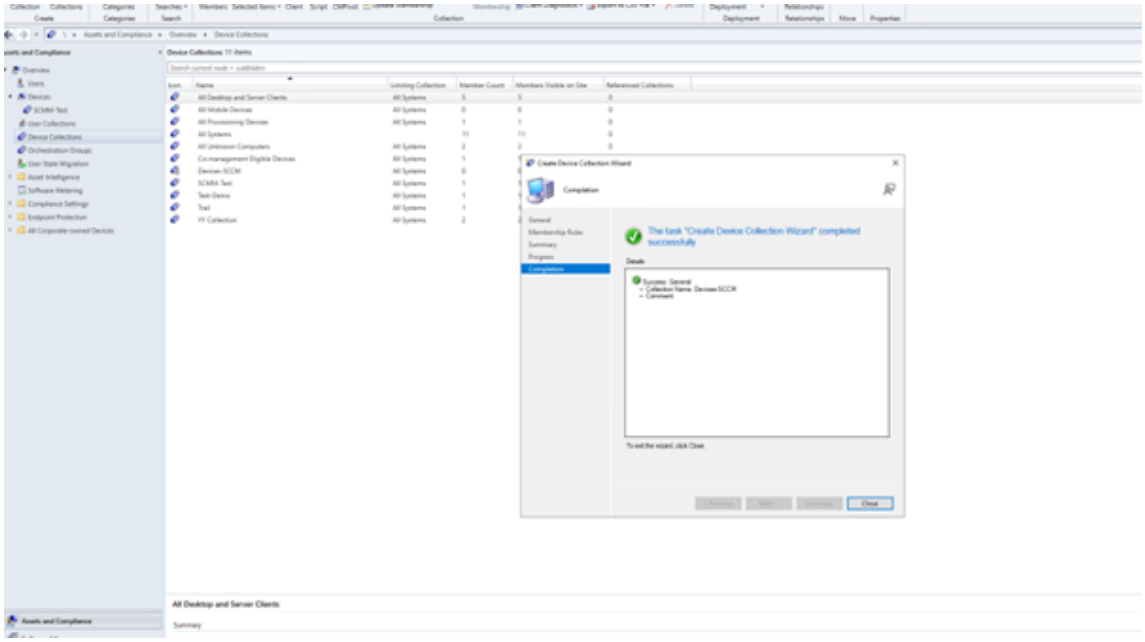
9. OU を作成するには、デバイスコレクションを作成します。コレクション名の名前を入力します。



10. ウィザードの手順に従います。

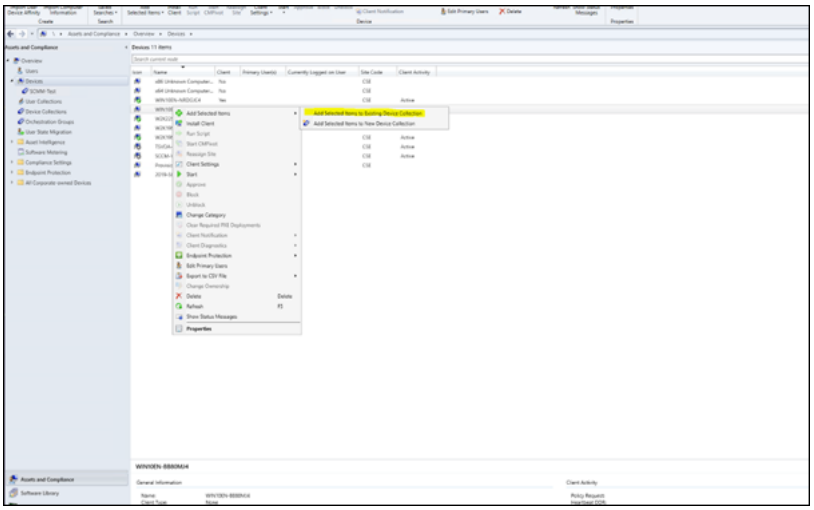


OU が作成されます。

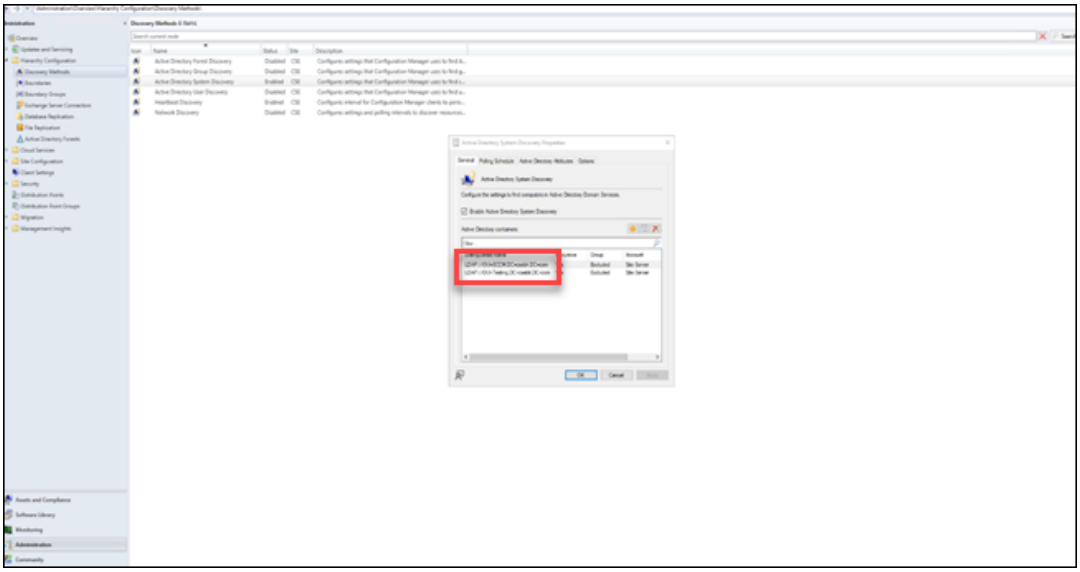


11. 作成した仮想マシンを新しく作成したデバイスコレクションに追加します。

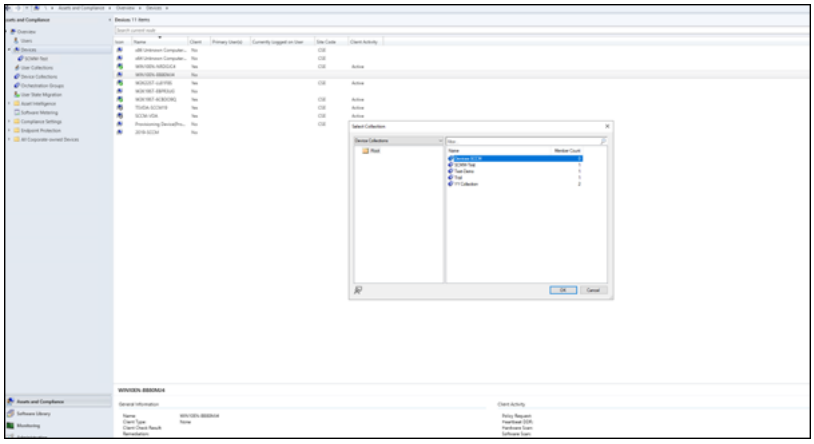
    a) 仮想マシンを右クリックします。［選択した項目を追加する］**>**［選択した項目を既存のデバイス コレクションに追加する］の順に選択します。



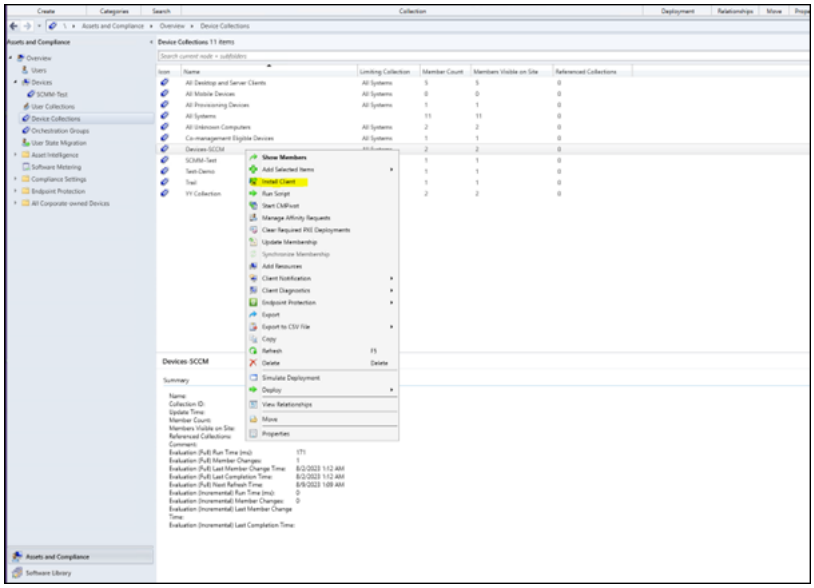
    b) ［コレクションの選択］ウィンドウで、必要なデバイス名を選択します。この例では、Devices-SCCMです。



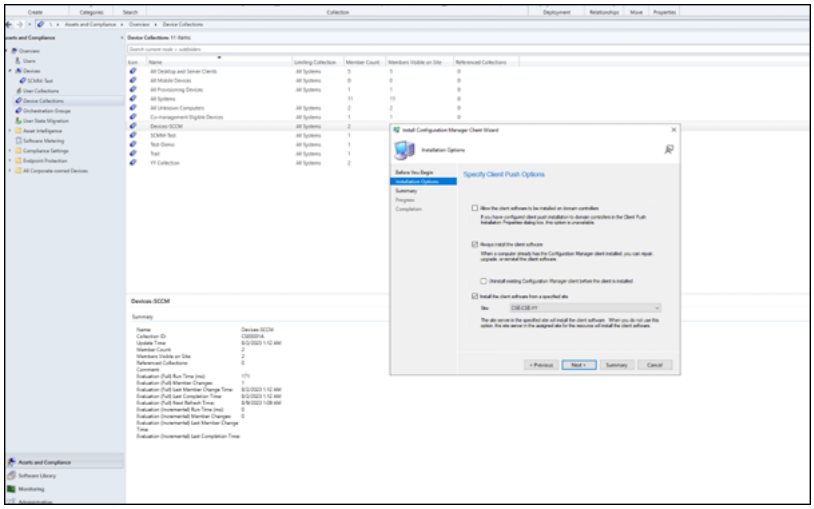
Devices-SCCMは、[資産とコンプライアンス] > [概要] > [デバイスコレクション] に表示されています。



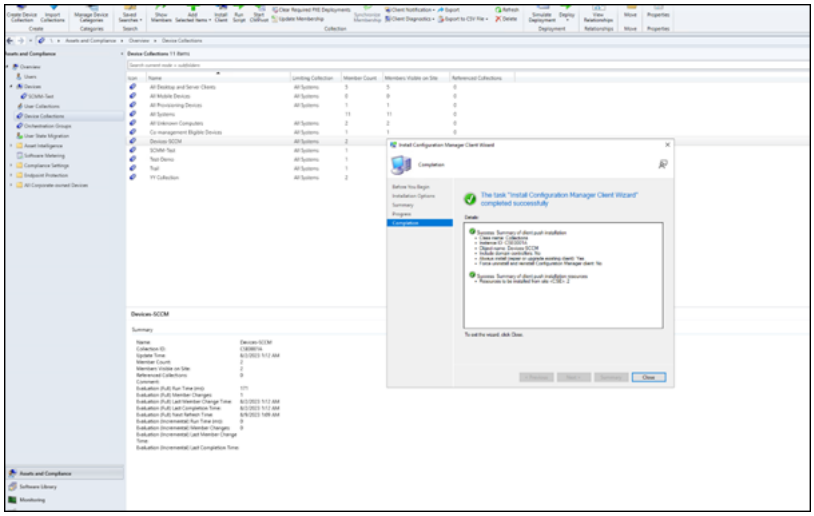
12. デバイスコレクションで [クライアントのインストール] を選択します。



13. 必要なインストール サイトを選択します。



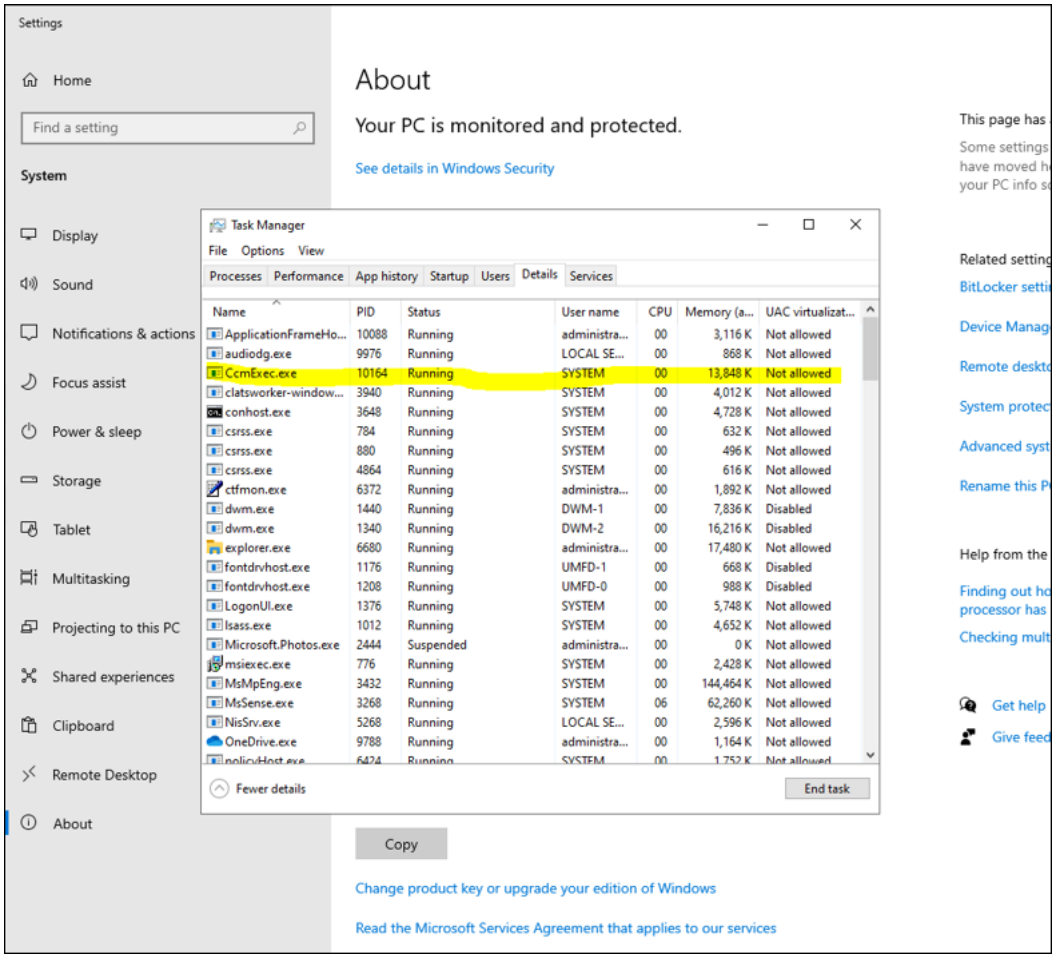
14. ウィザードの手順に従います。**Configuration Manager** クライアントのインストール ウィザードが正常に完了しました。



詳細については、Microsoft ドキュメントの「Configuration Manager でコレクションを管理する方法」を参照してください。

手順 **3**：マシンの検証

1. クライアントマシンで、CCMExecプロセスが実行されているかどうかを確認して、クライアントがインストールされていることを確認します。



2. SCCM 上の仮想マシンに対してクライアントが実行されているかどうかを確認します。

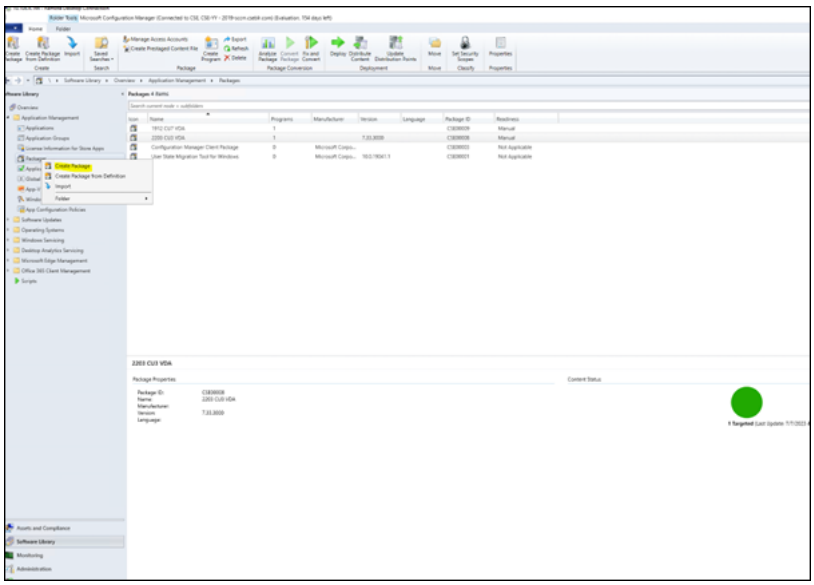
手順 **4**：**VDA** を使用したコンテンツの配布

次の手順では、展開された VDA を使用して、関連付けられた仮想マシンにコンテンツを配布する方法について説明します。

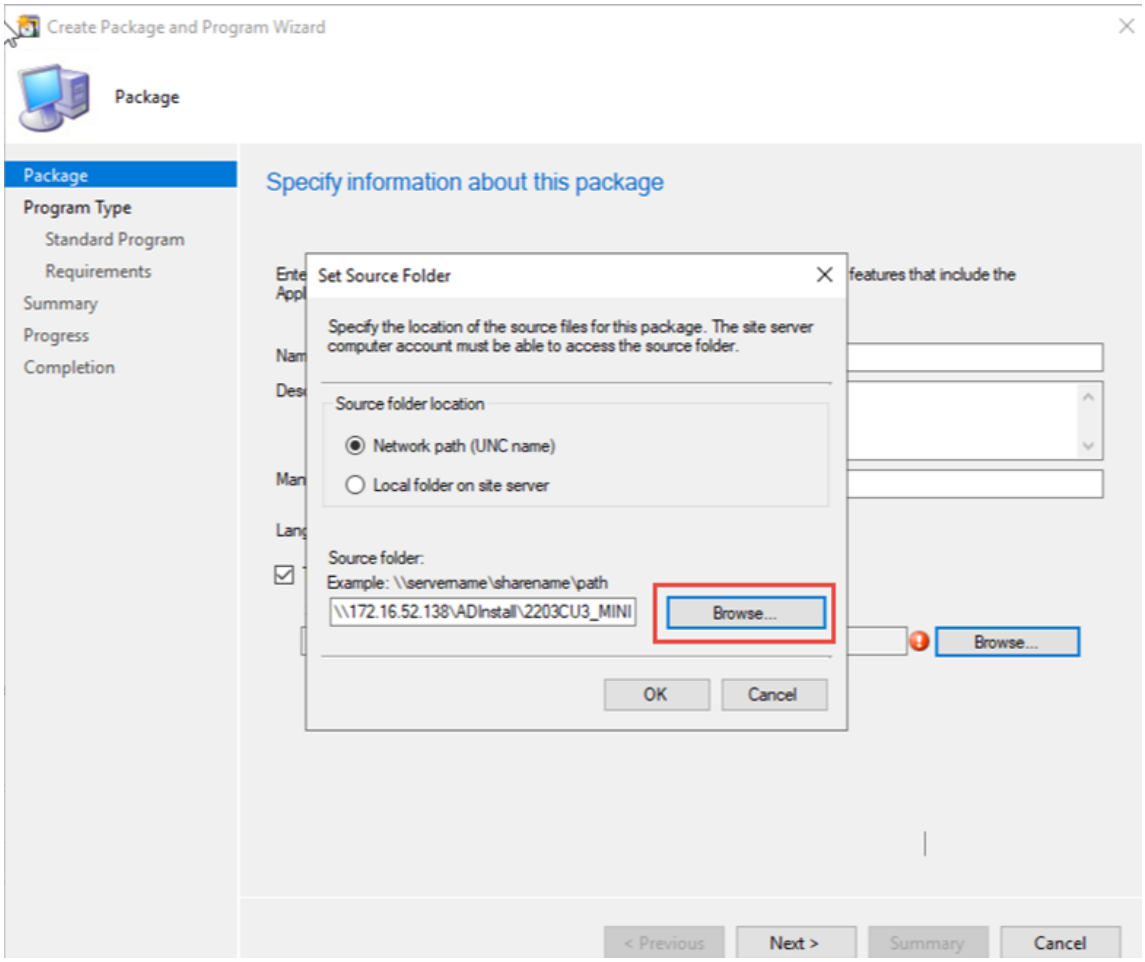
1. パッケージを作成する
2. コンテンツを配布する

パッケージを作成する

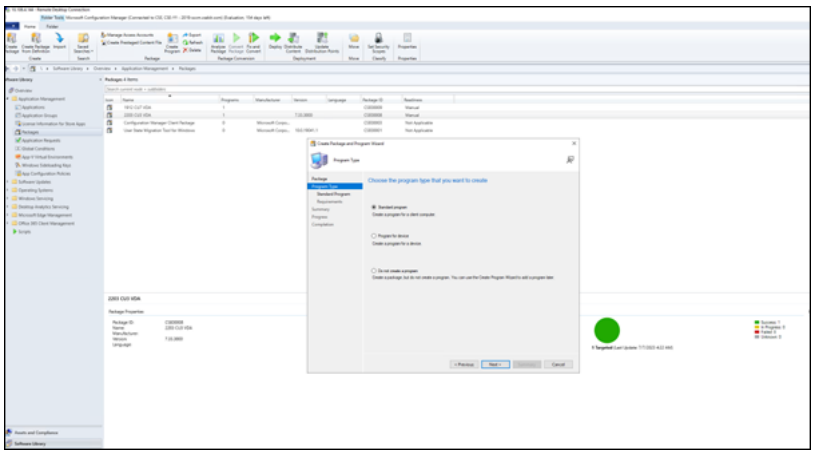
1. パッケージを作成するには、必要な VDA を右クリックし、［パッケージの作成］をクリックします。



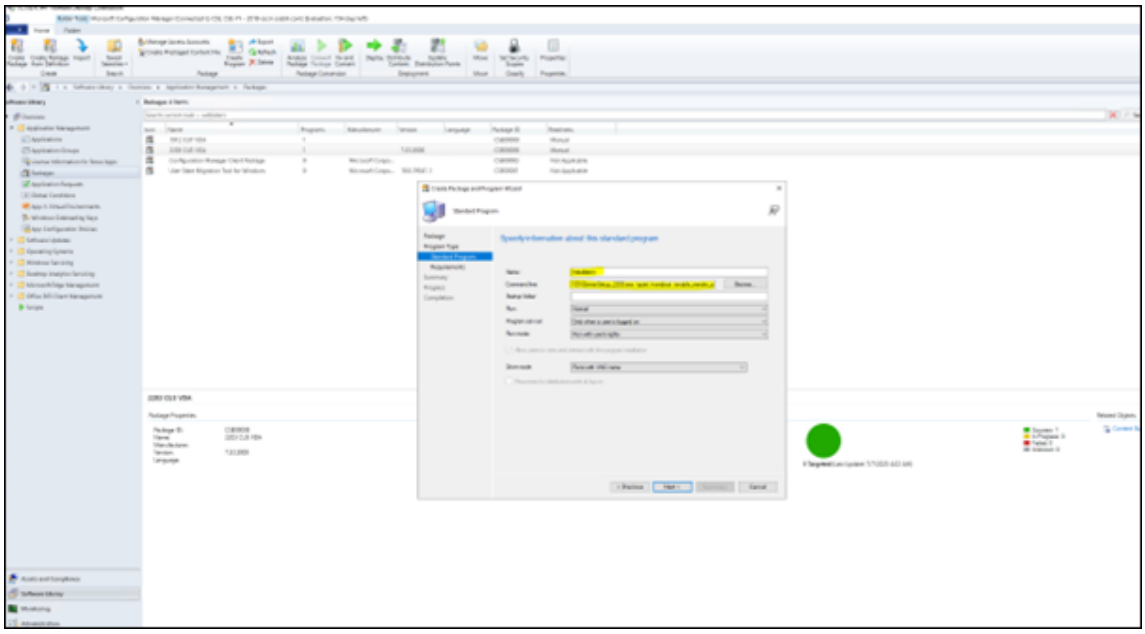
2. ［参照］をクリックして、このパッケージのソースファイルの場所を指定します。



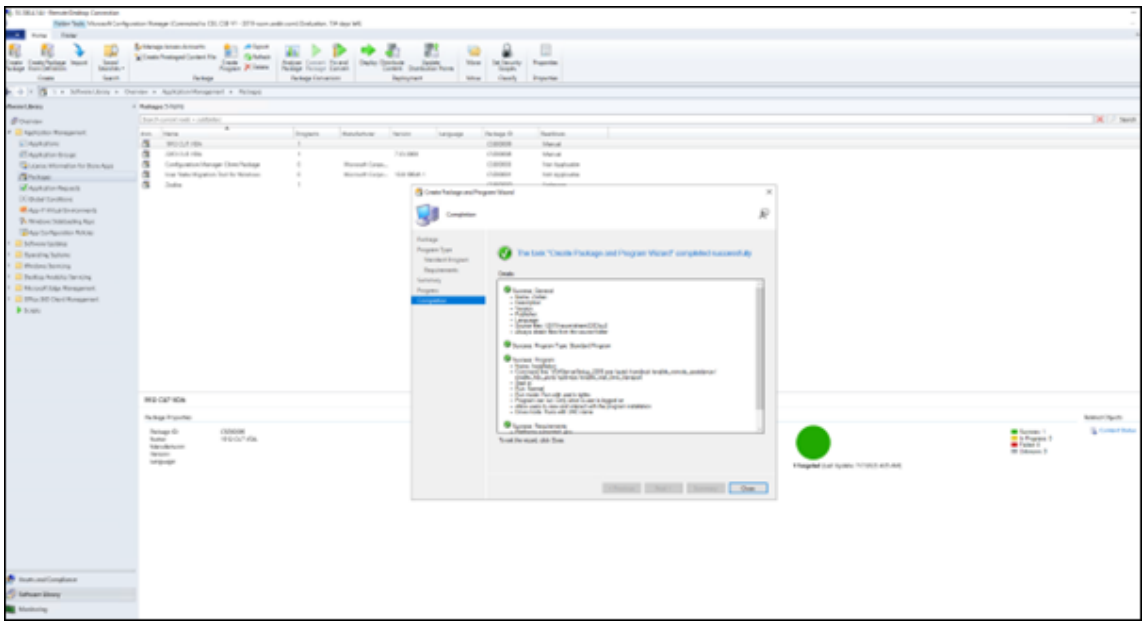
3. 必要なパッケージタイプを選択します。



4. パッケージの名前とコマンドラインを入力します。



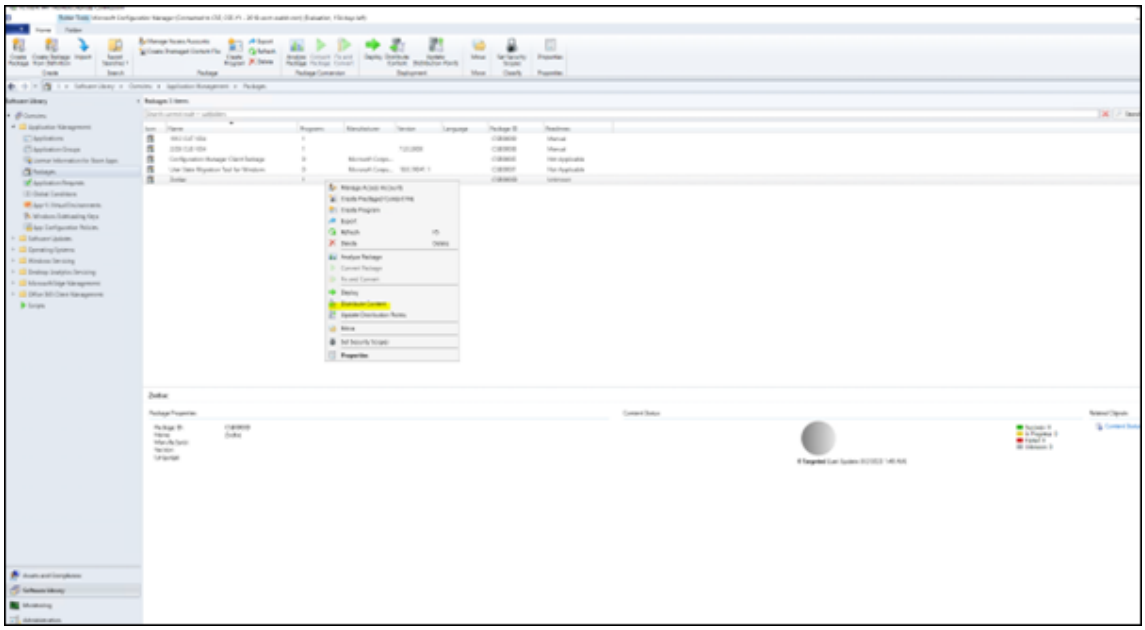
5. ［次へ］をクリックします。



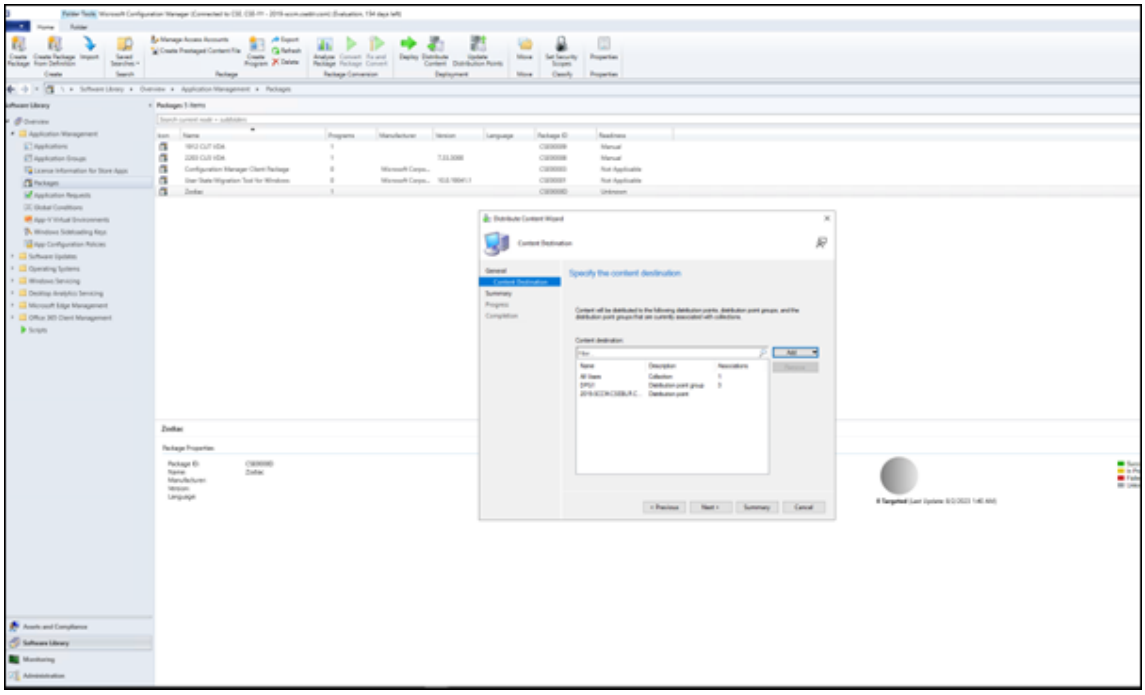
詳細については、Microsoft ドキュメントの「Configuration Manager のパッケージとプログラム」を参照してください。

コンテンツを配布する

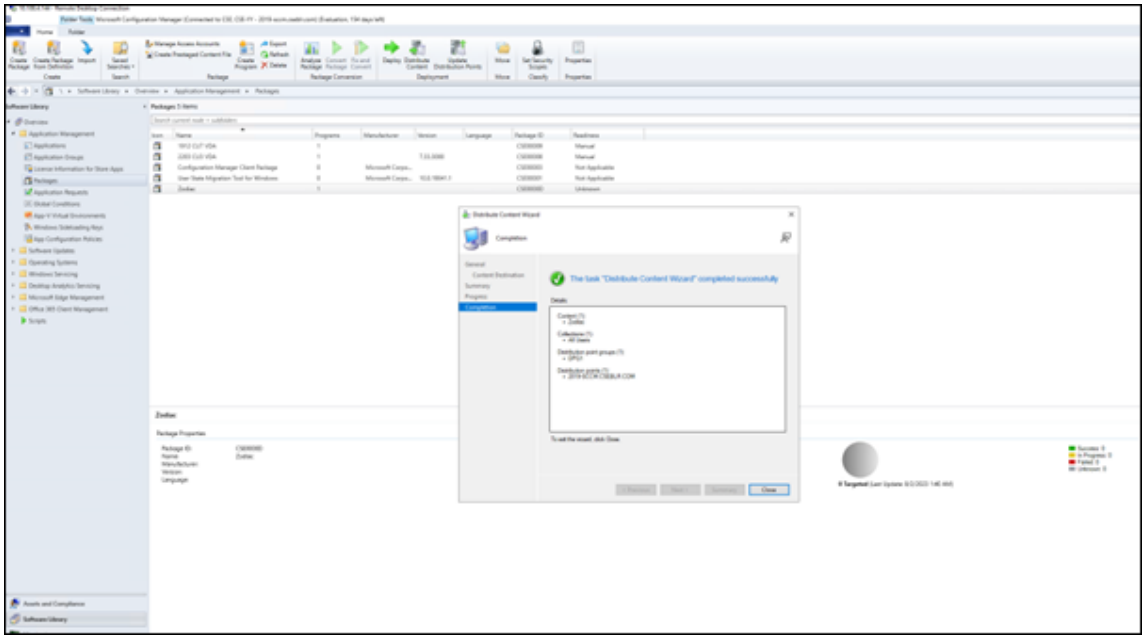
1. 作成したパッケージ名を右クリックします。
2. ［コンテンツを配布］を選択します。



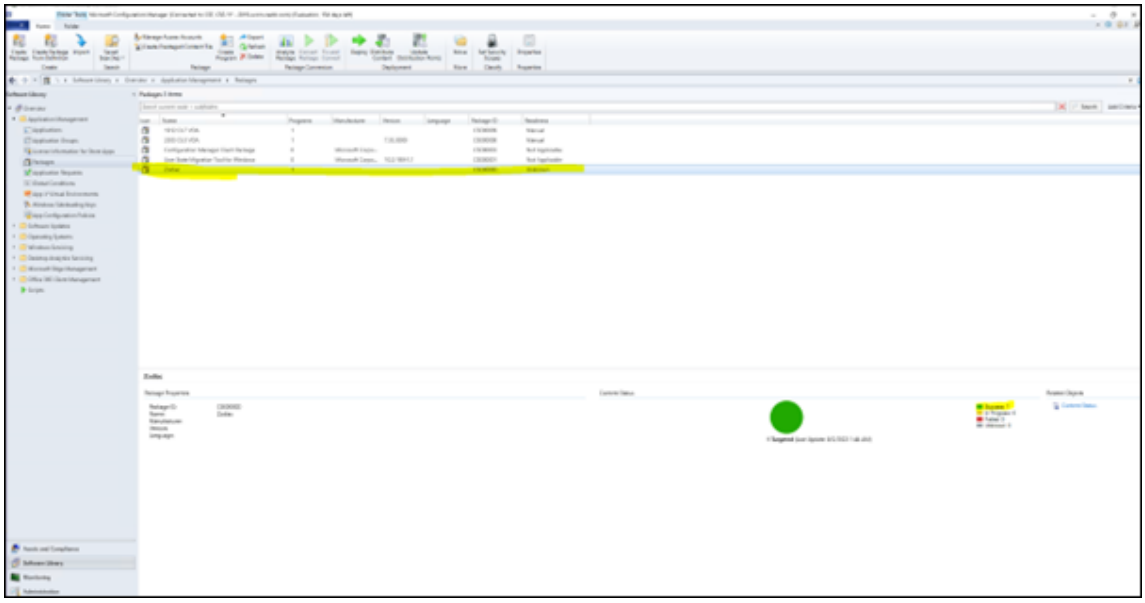
3. コンテンツの配布ウィザードウィンドウで、作成したパッケージのソースファイルの場所を選択します。この例では、2019-SCCMです。［次へ］をクリックします。



4. パッケージ（この例ではZodiac）が利用可能であることを確認します。



次の画像は、パッケージを展開できることを示しています。

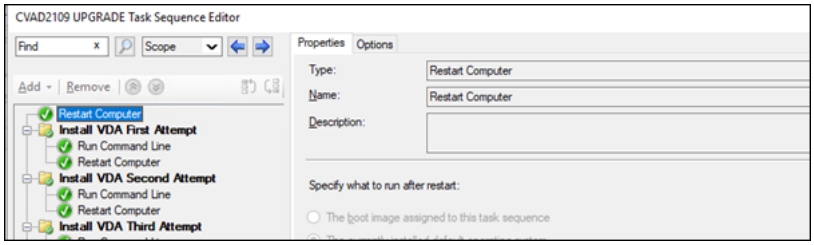


詳細については、Microsoft ドキュメントの「Configuration Manager のコンテンツを展開および管理する」を参照してください。

SCCM を使用したインストールシーケンスの例

以下は、インストールシーケンスの例です。

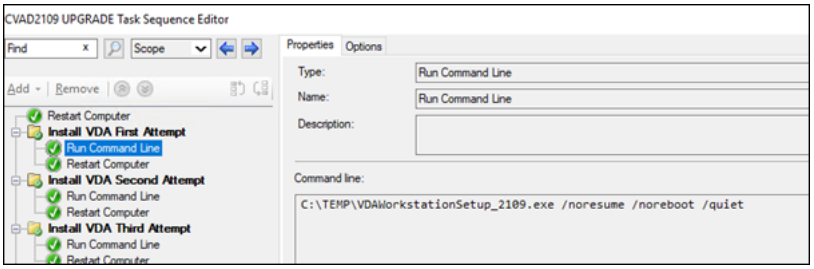
1. **Restart Computer**：マシンを再起動することでマシンを準備します。



2. **Install VDA First Attempt**： VDA のインストールを開始します。

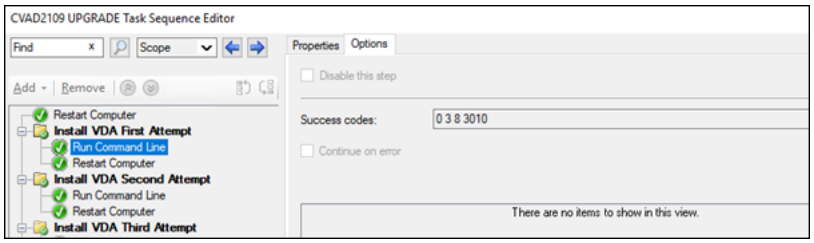
   a) 既存のコマンドラインオプションに/quiet、/noreboot、/noresumeオプションを追加します。

   b) 任意の VDA インストーラー（ローカルイメージ、または最小限のインストーラーの 1 つ）を実行します。

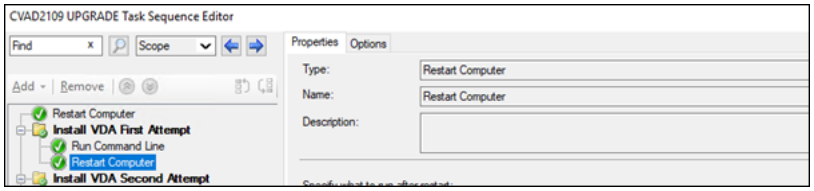


c) SCCM がリターンコードをキャプチャする必要があります。

- リターンコードが 0 または 8 の場合、インストールは完了しており、再起動が必要です。

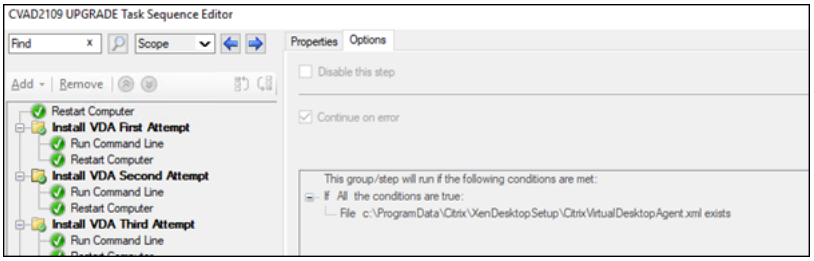


- リターンコードが 3 の場合は、マシンを再起動してから、[**Install VDA Second Attempt**] に制御を渡します。



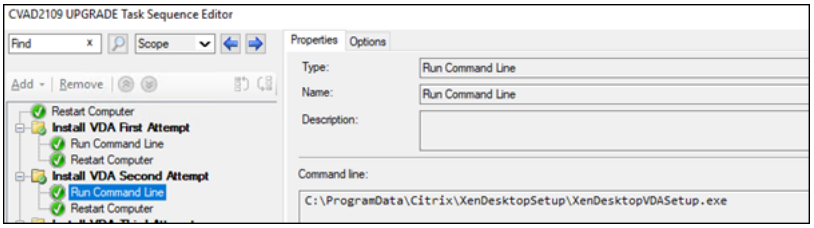
3. **Install VDA Second Attempt**: VDA のインストールを続行します。

a) [**Install VDA First Attempt**] 後、%programdata%\Citrix\XenDesktopSetup\CitrixVirtualDesktopAgent.xmlファイルが存在する場合、インストールは完了していないため、再起動の完了後に続行される必要があります。



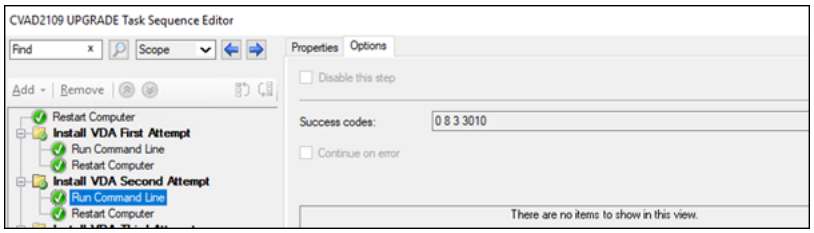
b) %programdata%\Citrix\XenDesktopSetup\CitrixVirtualDesktopAgent.xmlファイルが 存在しなくなるか、0 または 8 以外のリターンコードが返されるまで、[**Install VDA Second Attempt**] が繰り返されます。その他のリターンコードはエラーとして扱われ、INSTALL VDA SECOND ATTEMPT は、エラーを報告して停止します。

c) 適切な VDA インストーラー（ほとんどの場合は、XenDesktopVdaSetup.exeまたはVDAWorkstationCoreSetup_XXXX.exeが使用されている場合はXenDesktopRemotePCSetup.exe）を、ファイル%programdata%\ Citrix\XenDesktopSetup\ ディレクトリから、コマンドラインパラメーターなしで実行することで VDA のインストールを再開します。（VDA インストーラーは、その初回実行時に保存されたパラメーターを使用します。）



d) VDA インストーラーからのリターンコードを確認します。

- 0 または 8：成功し、インストールが完了し、再起動が必要です。



- 3：インストールが完了していません。ファイル%programdata%\Citrix\XenDesktopSetup\CitrixVirtualDesktopAgent.xmlが存在しなくなるか、0 または 8 のリターンコードが返されるまで、マシンを再起動して INSTALL VDA SECOND ATTEMPT が繰り返されます。その他のリターンコードはエラーとして扱われ、INSTALL VDA SECOND ATTEMPT は、エラーを報告して終了します。

リターンコードについて詳しくは、「Citrix インストールリターンコード」を参照してください。

VDA インストールコマンドの例

使用可能なインストールオプションは、使用するインストーラーによって異なります。コマンドラインオプションの詳細については、次の記事を参照してください。

- VDA のインストール
- コマンドラインを使用したインストール

リモート PC アクセス用のインストールコマンド

- 次のコマンドでは、シングルセッションのコア VDA インストーラー（VDAWorkstationCoreSetup.exe）を使用します：

  ```
  VDAWorkstationCoreSetup.exe /quiet /controllers “control.domain.com” /enable_hdx_ports /noresume /noreboot
  ```

- 次のコマンドでは、シングルセッションの完全版 VDA インストーラー（VDAWorkstationSetup.exe）を使用します：


```
VDAWorkstationSetup.exe /quiet /remotepc /physicalmachine /
controllers “control.domain.com” /enable_hdx_ports /noresume
/noreboot
```

専用 **VDI** のインストールコマンド

- 次のコマンドでは、シングルセッションの完全版 VDA インストーラー（VDAWorkstationSetup.exe）を使用します：

```
VDAWorkstationSetup.exe /quiet /components vda /controllers “
control.domain.com” /enable_hdx_ports /enable_remote_assistance
/noresume /noreboot
```

Microsoft Intune を使用した **VDA** のインストール

August 20, 2024

概要

この記事では、Microsoft Intune を使用して VDA を展開する方法について説明します。詳しくは、Microsoftのドキュメントを参照してください。

> 注：
>
> 以下の記事では、Citrix が環境をテストした方法に基づいた推奨事項のみについて説明します。これらの手順は、必要に応じてカスタマイズできます。Citrix は、お客様がニーズに合わせて追加された更新や調整については責任を負いません。

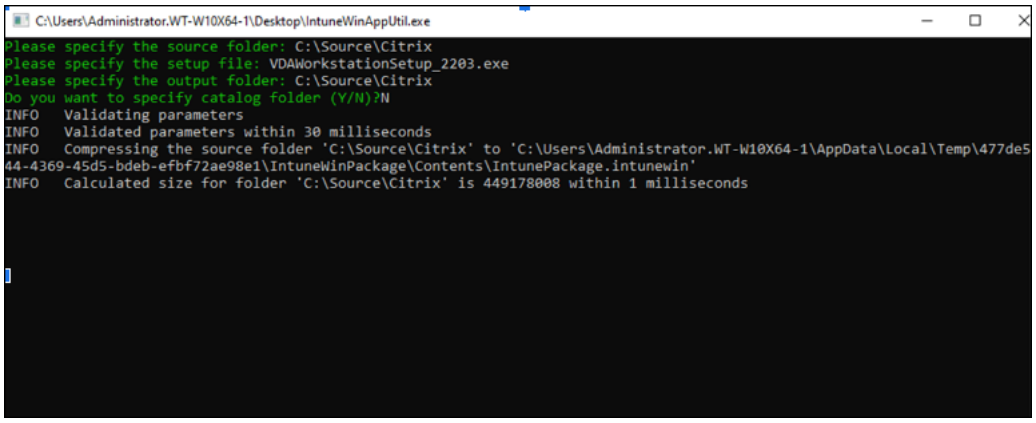
Microsoft Intune を使用して **VDA** を展開するための主な手順

1. Citrix VDA のインストールを準備します。
2. Microsoft 365 開発者プログラムのサブスクライバーを設定します。
3. アプリを追加して割り当てます。
4. 登録したデバイスにアプリをインストールします。

手順 **1**：**Citrix VDA** のインストールを準備する

1. 更新されたIntuneWinAppUtil.exeを GitHub からダウンロードします。

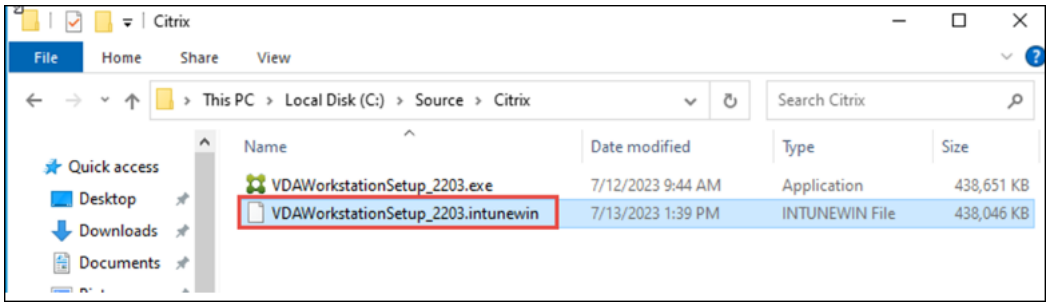
2. ［管理者として実行］を使用して、`IntuneWinAppUtil.exe`ファイルを実行します。
3. 次のデータを入力します：



   a) **Please specify the source folder**：アプリケーションのセットアップファイルが含まれているフォルダーを入力します。例：C:\source\Citrix。
   b) **Please specify the setup file**：セットアップファイル名（setup.exe や setup.msi など）を入力します。例：VDAWorkstationSetup_2203.exe。
   c) **Please specify the output folder**：.intunewin ファイルを生成する出力フォルダーのパスを入力します。例：C:\source\Citrix。
   d) **Do you want to specify catalog folder**（**Y/N**）：N を入力します。

> 注：
>
> **Win32** コンテンツ準備ツールの実行中、数分間お待ちください。`.intunewin`ファイルが生成されると、コマンドプロンプトの下部にステータスが 100% と表示されます。

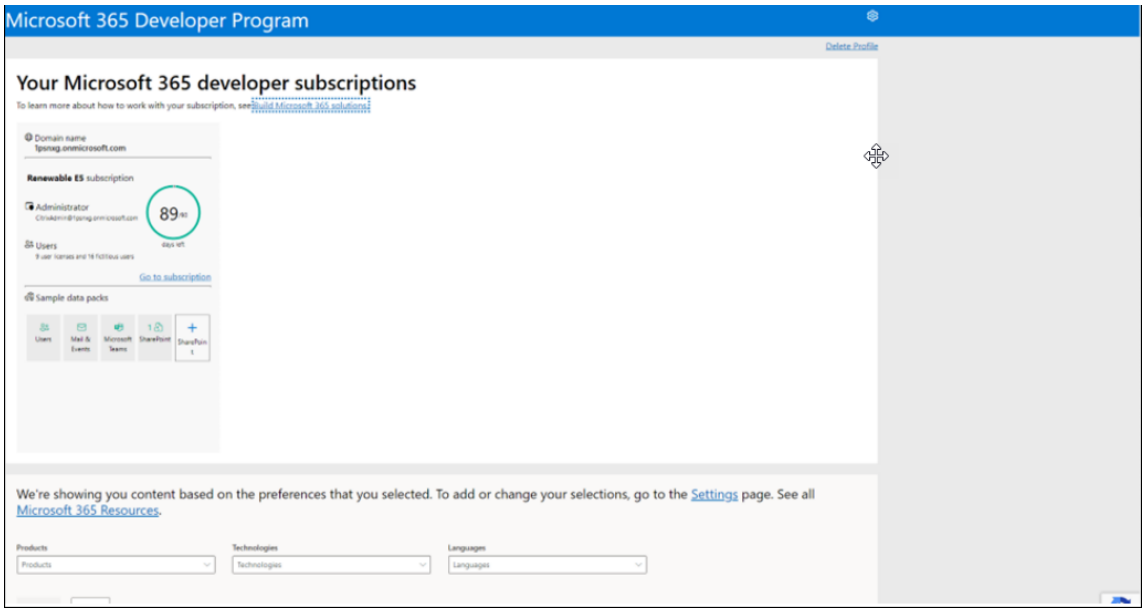
4. プロセスが完了したら、出力フォルダー（この例では`C:\source\Citrix`）に移動して、Microsoft Intune 展開ファイルを取得します。
5. Microsoft Intune の無料のお試し版にサインアップしてください。



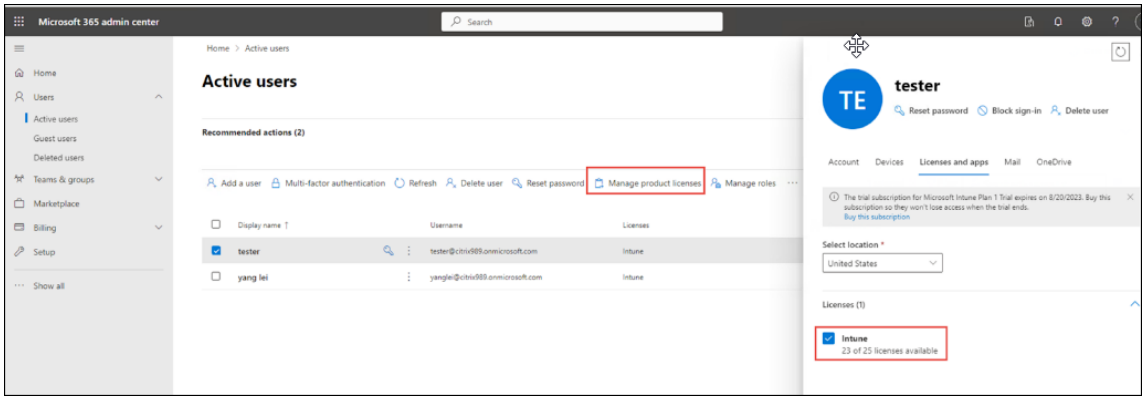
手順 **2**：**Microsoft 365** 開発者プログラムのサブスクライバーを設定

1. サブスクリプションを有効にするには、インスタントサンドボックスを作成します。
   開発者サンドボックスを取得するには、Microsoft 365 開発者プログラムダッシュボードに移動し、［**Add a**

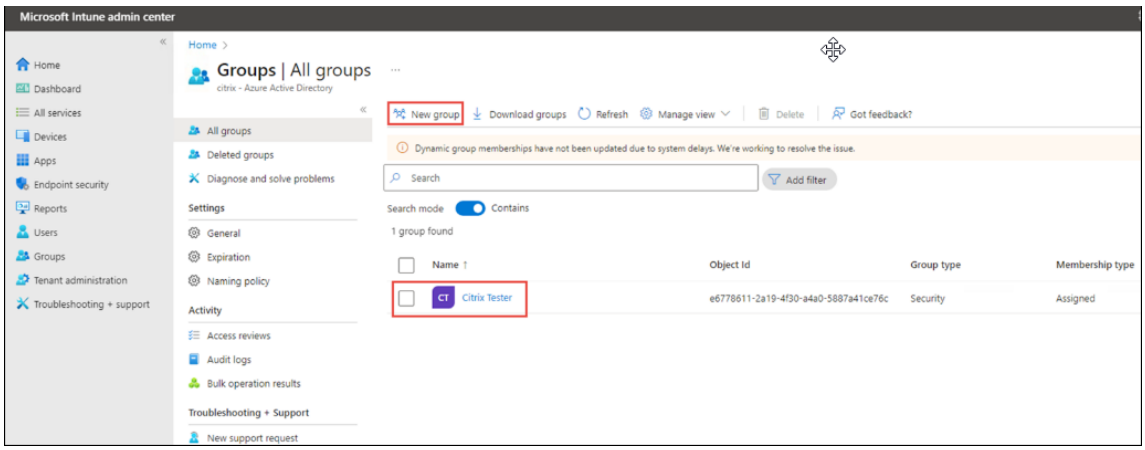
new subscription］を選択します。



2. Microsoft 365 管理センターでユーザーを作成し、ユーザーにライセンスを割り当てます。



3. グループを作成します。

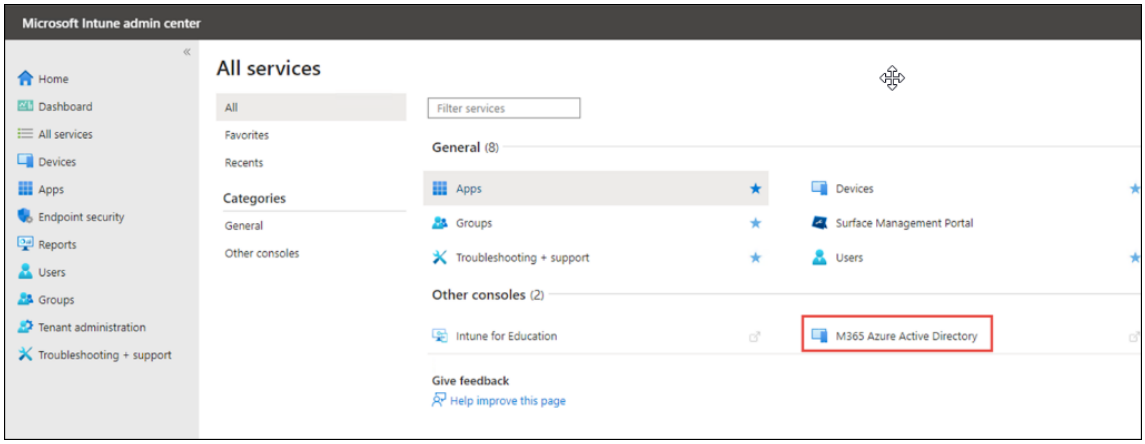


4. グループを作成したら、グループに MDM 権限を付与する必要があります。自動登録を設定します。アクティ

ブ化まで 1 分ほどかかる場合があります。
または、次の手順を実行して、MDM 権限をグループに手動で追加することもできます:

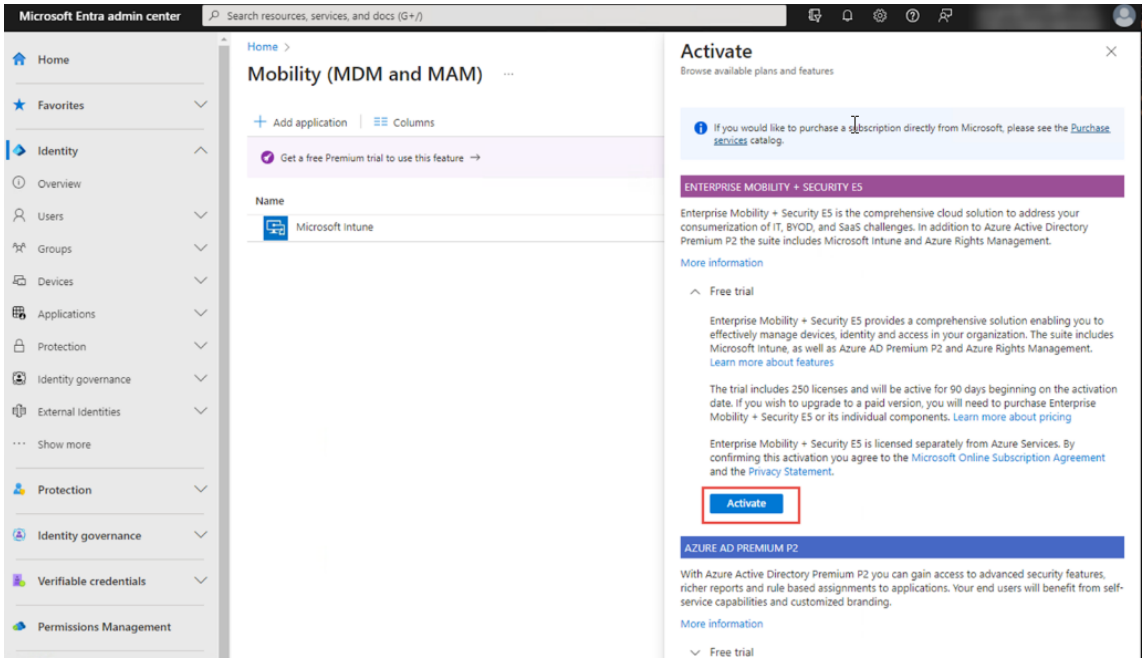
a) **All services > Microsoft Entra** に移動します。
b) **settings > Mobility** に移動して、**Microsoft Intune** を選択します。
c) 作成したグループを選択します。これにより、MDM ユーザースコープのページが開きます。
d) [保存] をクリックします。

5. [**All Services**] タブで、[**M365 Azure Active Directory**] をクリックします。

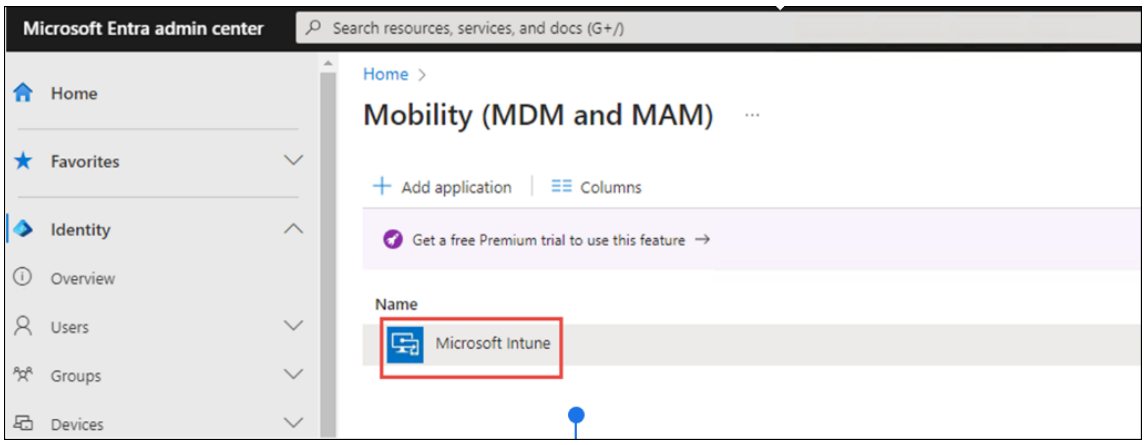


6. [**Get a free Premium trial to use this feature**] をクリックします。

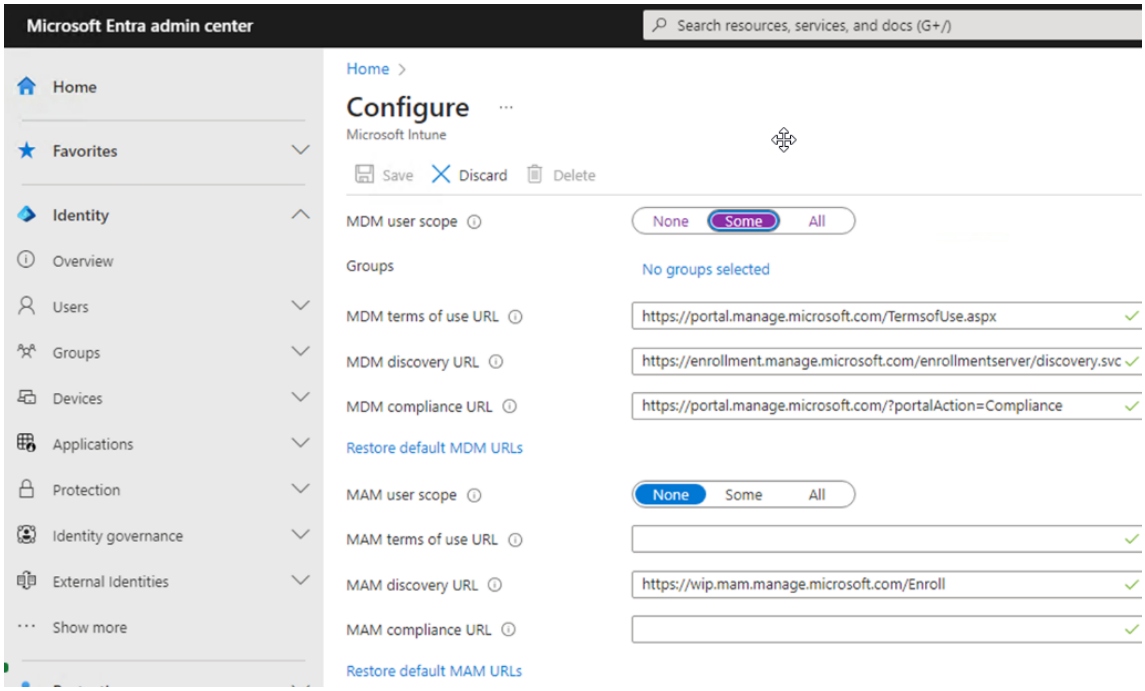
7. [**Activate**] をクリックします。



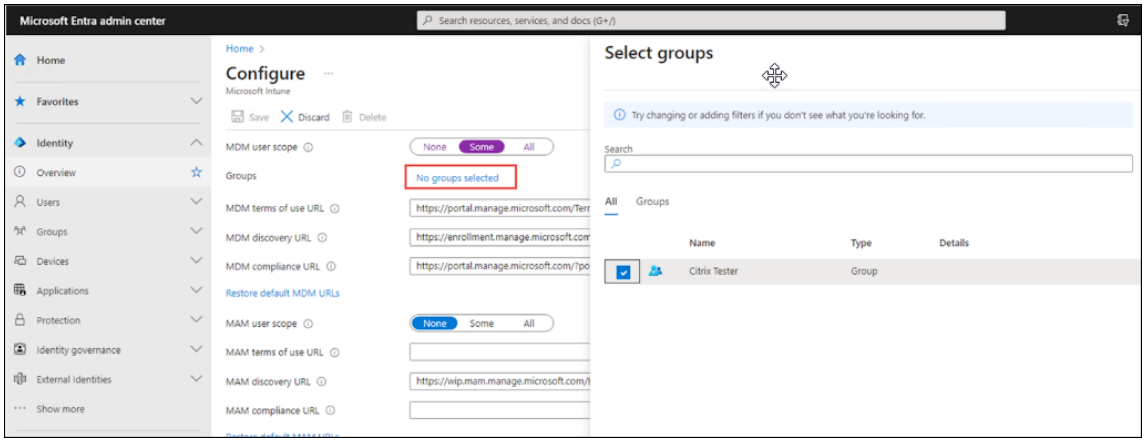
8. [**Microsoft Intune**] をクリックします。



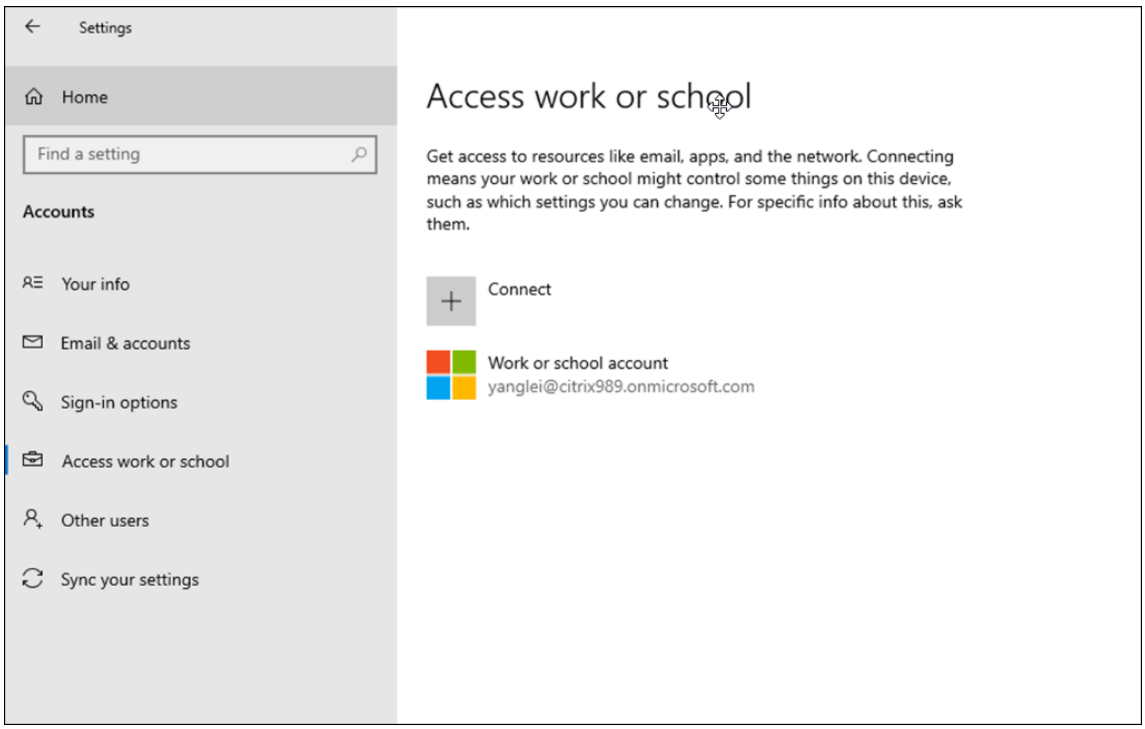
9. [**Configure**] タブで、必要な構成を入力します。



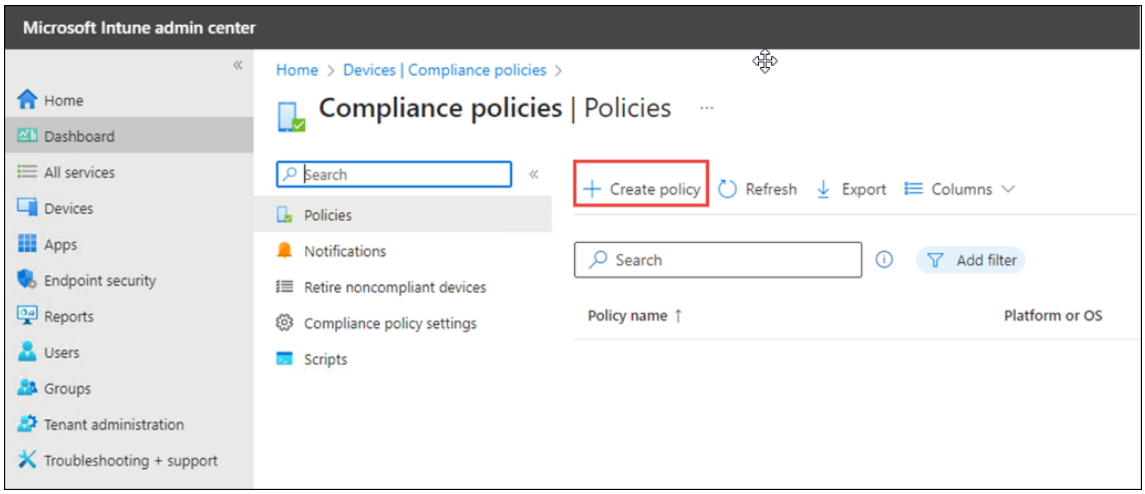
10. グループを追加するには、［**No groups selected**］をクリックします。



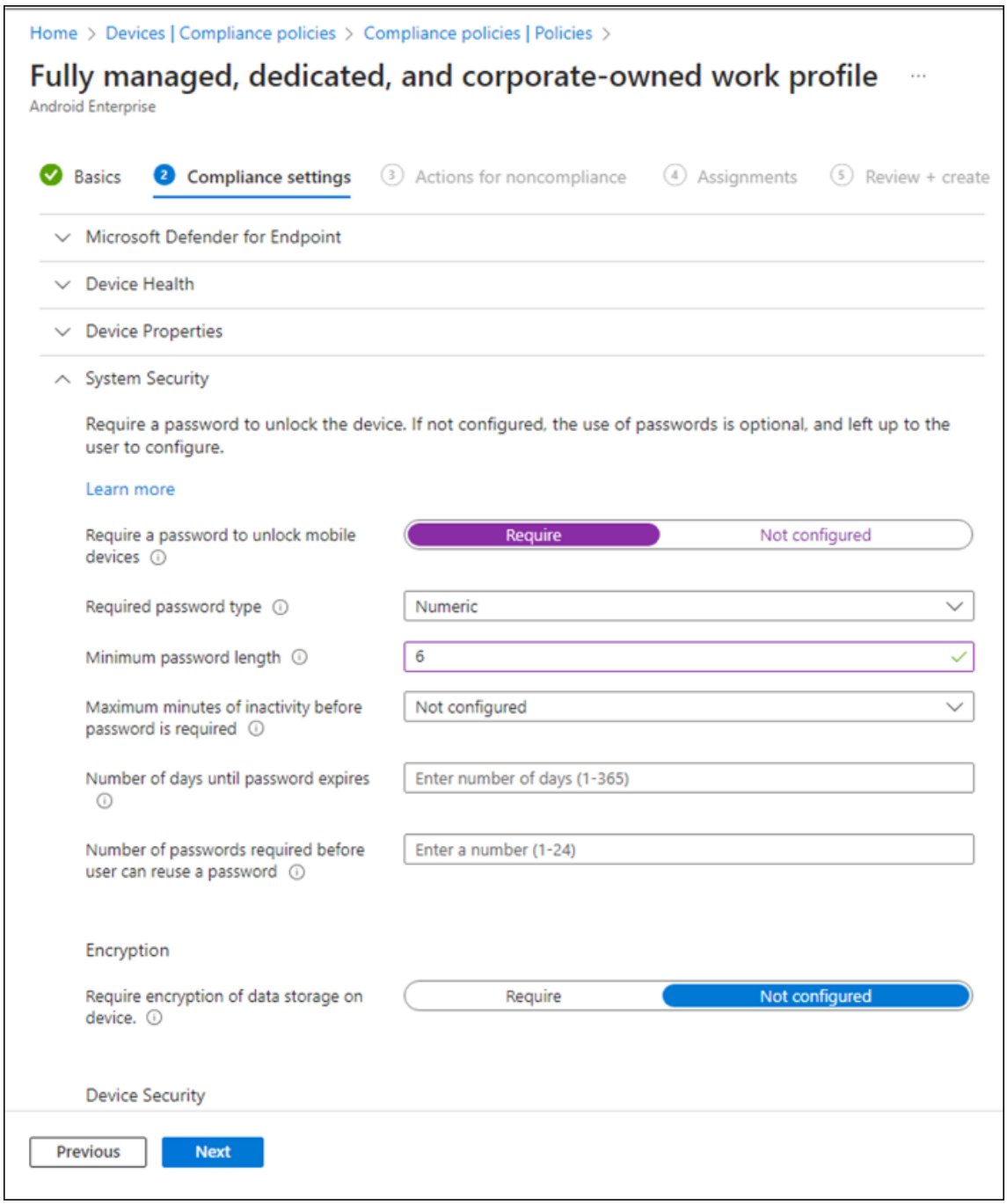
11. デバイスを登録します。



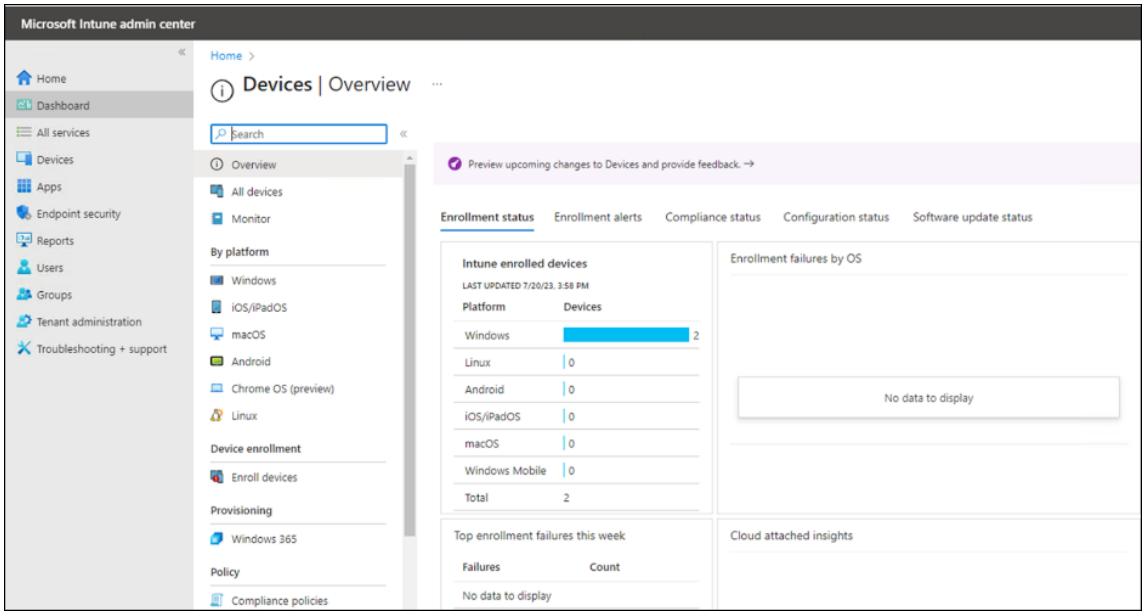
12. 新しく作成したデバイスのコンプライアンスを`Compliant`に変更するための、デバイスコンプライアンスポリシーを作成します。



13. 新しく作成したグループを追加するには、［**Assignments**］タブに移動します。



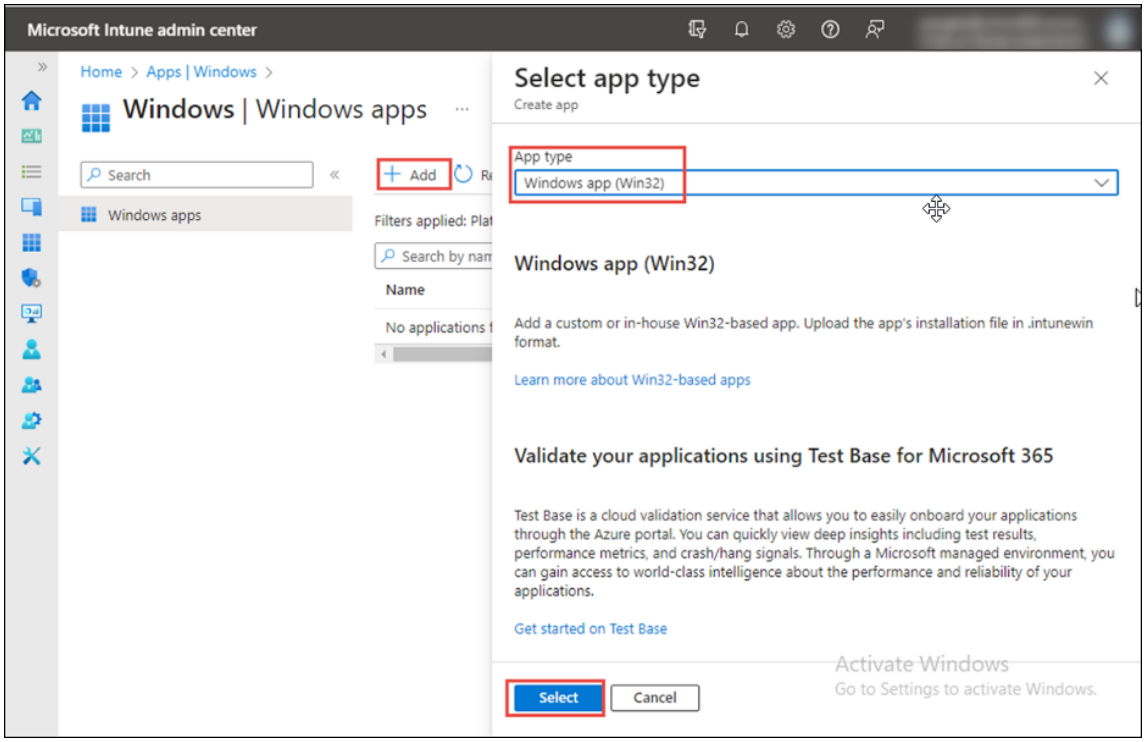
14. デバイスの登録を確認します。



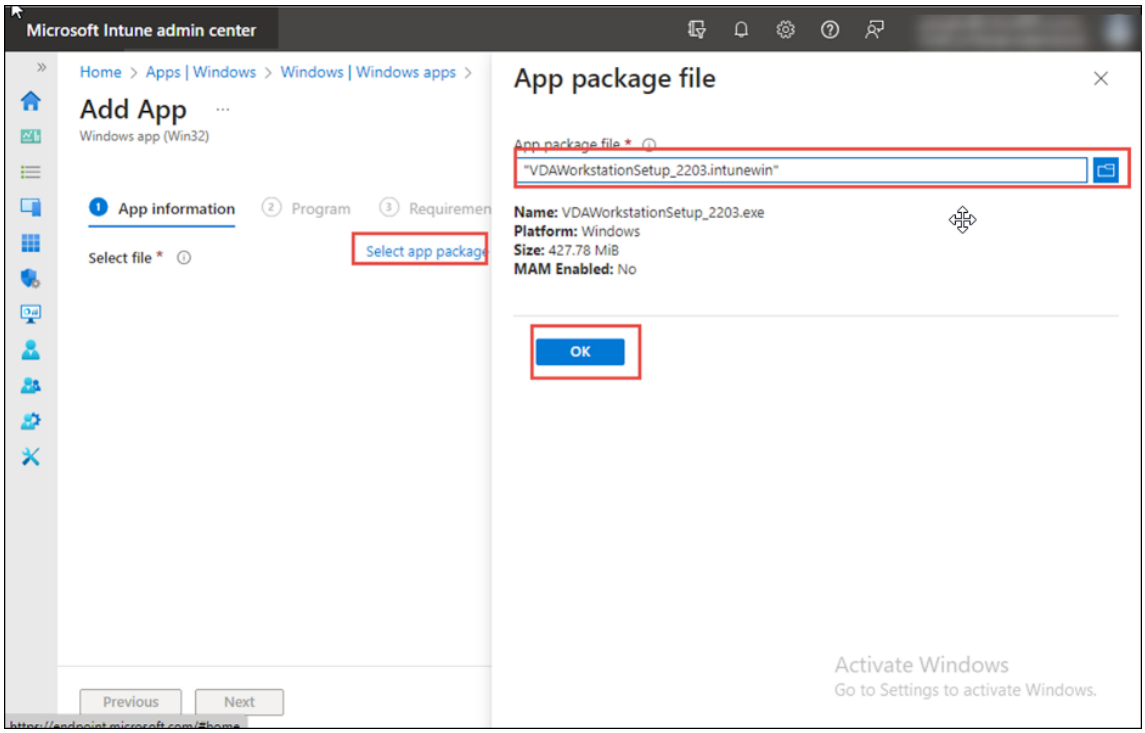
詳しくは、「Microsoft 365 開発者プログラム」を参照してください。

手順 **3**：アプリの追加と割り当て

1. Microsoft Intune 管理センターにサインインします。
2. [**Apps**] > [**All apps**] > [**Add**] の順に選択するか、[**Apps**] > [**Windows**] > [**Windows Apps**] に移動します。

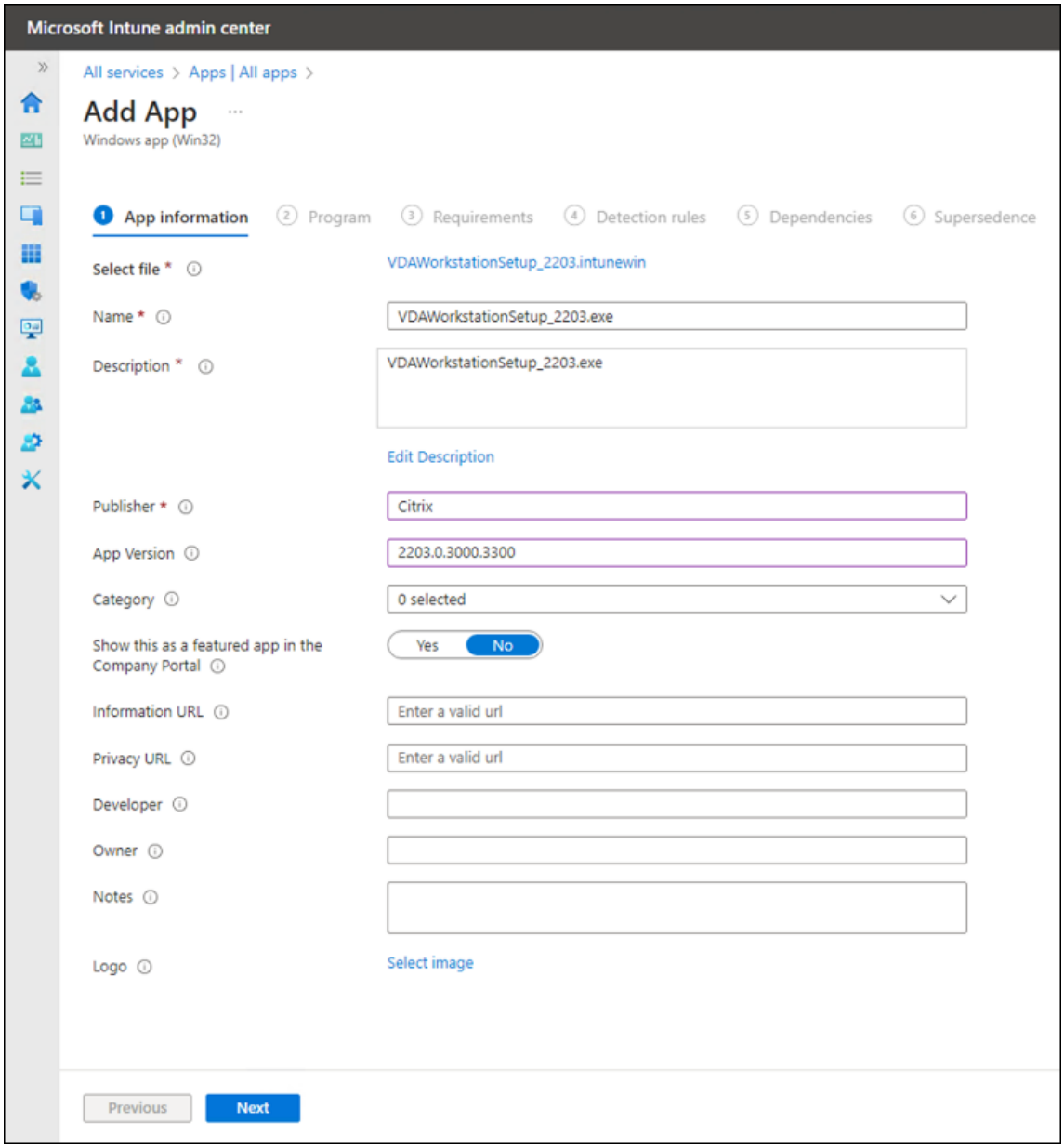


3. [**Select app type**] ペインで [**Other app types**] > [**Windows app (Win32)**] を選択し、[**Select**] をクリックします。
4. [**Add app**] ペインで [**Select app package file**] をクリックします。[**browse**] をクリックします。
5. 拡張子 `.intunewin` の準備されたファイルを選択します。準備されたファイルは、「Citrix VDA のインストールを準備する」の手順で作成されます。アプリの詳細情報を含むページが表示されます。



> 注:
>
> - サーバーコアマシンを使用している場合は、VDA ワークステーションコアを使用する必要があります。
> - Windows 10 デスクトップ OS を使用している場合は、VDA ワークステーションを使用する必要があります。
> - サーバー OS（Windows 2022 など）を使用している場合は、VDA サーバーのセットアップを使用する必要があります。
> - この例では 2203 バージョンを使用していますが、これはすべてのバージョンに適用できます。

6. [**App package file**] ペインで [**OK**] をクリックします。
7. 次の画面の [**App Information**] タブで、アプリの [**Name**] に入力し、Windows アプリの [**Description**] を入力します。[**Publisher**] の名前を `Citrix` と入力して、追加のアプリ情報をここで指定できます。[次へ] をクリックします。



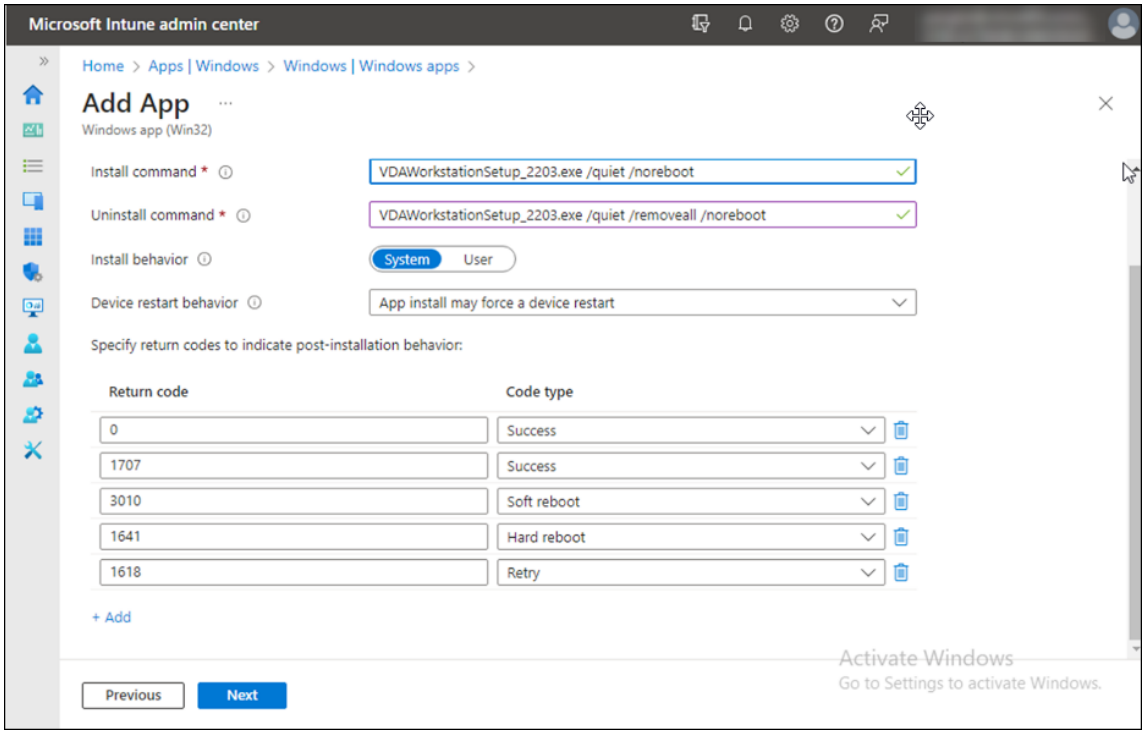
8. 次の画面で、以下の値を入力します:

   - **Install command**: `VDAWorkstationSetup_2203.exe /quiet /noreboot`
   - **Uninstall command**: `VDAWorkstationSetup_2203.exe /quiet /removeall /noreboot`
   - **Install behavior**:
     - **System**: グループ内のすべてのデバイスにアプリをインストールするには、このオプションを選択します。
     - **User**: グループ内の特定のユーザーデバイスにのみアプリをインストールするには、このオプションを選択します。

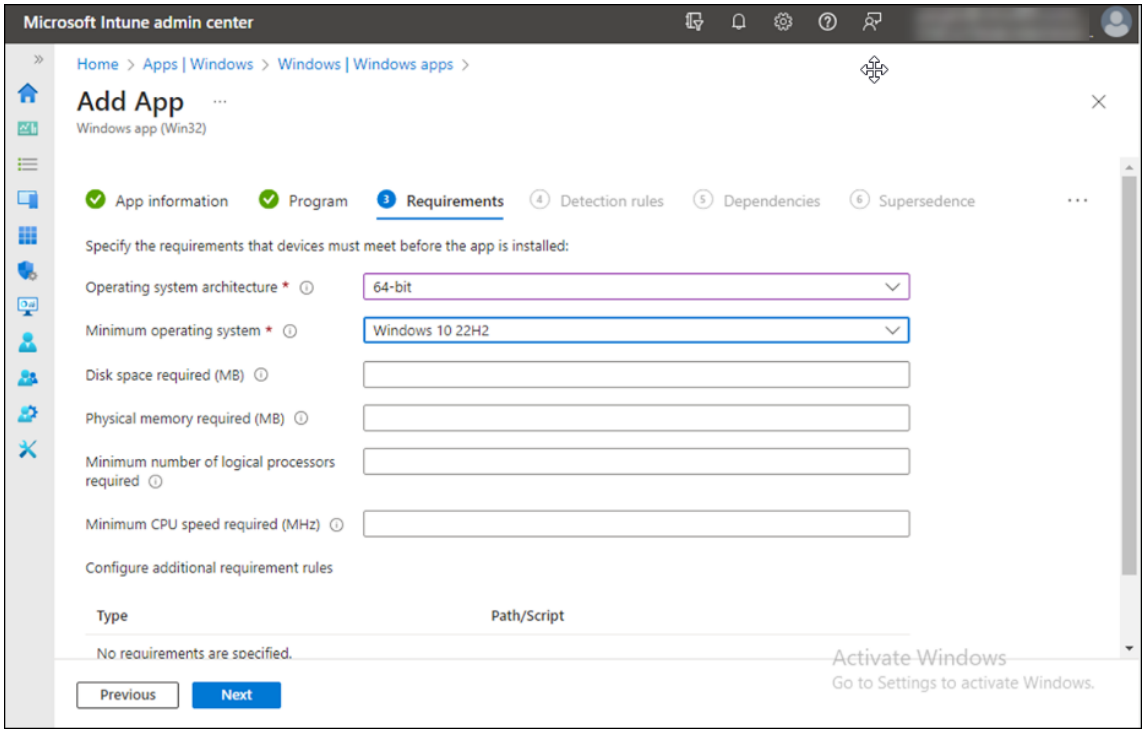
9. [次へ] をクリックします。

注:

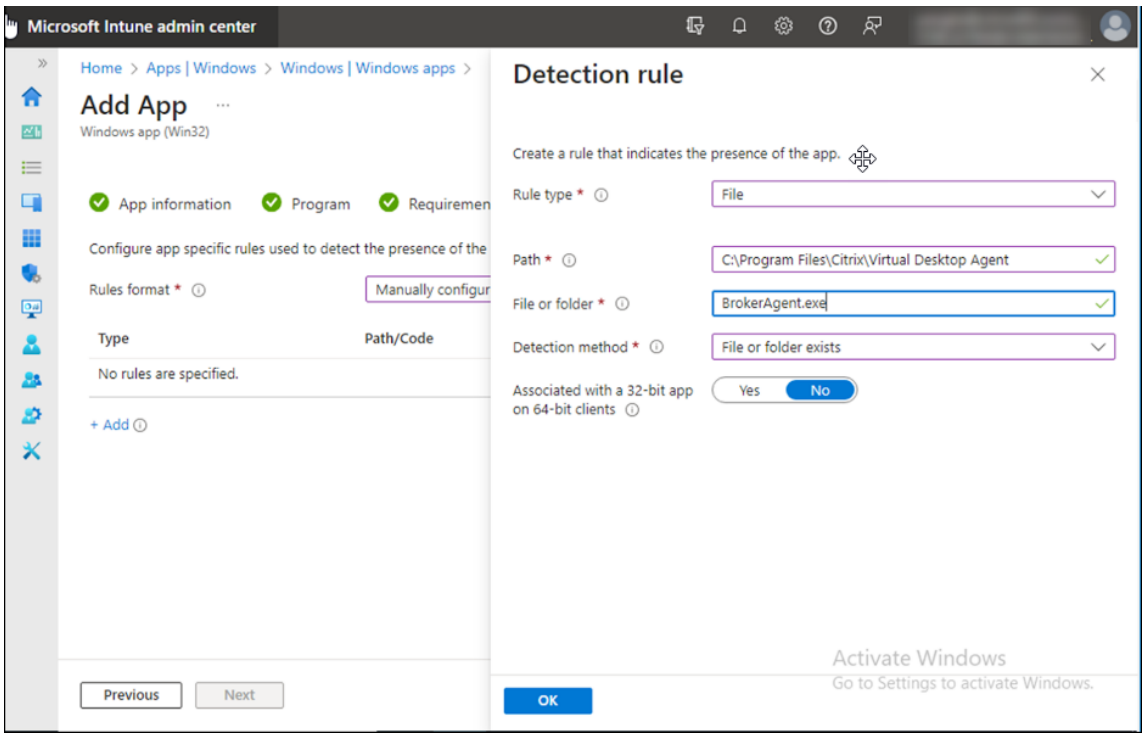
- この例では 2203 バージョンを使用していますが、どのバージョンでも使用できます。
- コマンドに`/noreboot`を追加しても、インストールまたは展開中に再起動が行われないわけではなく、強制的な再起動が強制されるだけです。
  スクリプトについて詳しくは、「VDA のインストールに使用されるコマンドラインオプション」を参照してください。
- [**Device restart behavior**] で [**Intune will force a mandatory device restart**] を選択します。
- [**Return code**] テキストボックスで、インストールの成功後の`0`、`3`、`8`を入力します。
  その他のリターンコードについて詳しくは、「Citrix インストールリターンコード」を参照してください。



10. 次の画面の [**Requirements**] タブで、必要な値を入力します。[次へ] をクリックします。



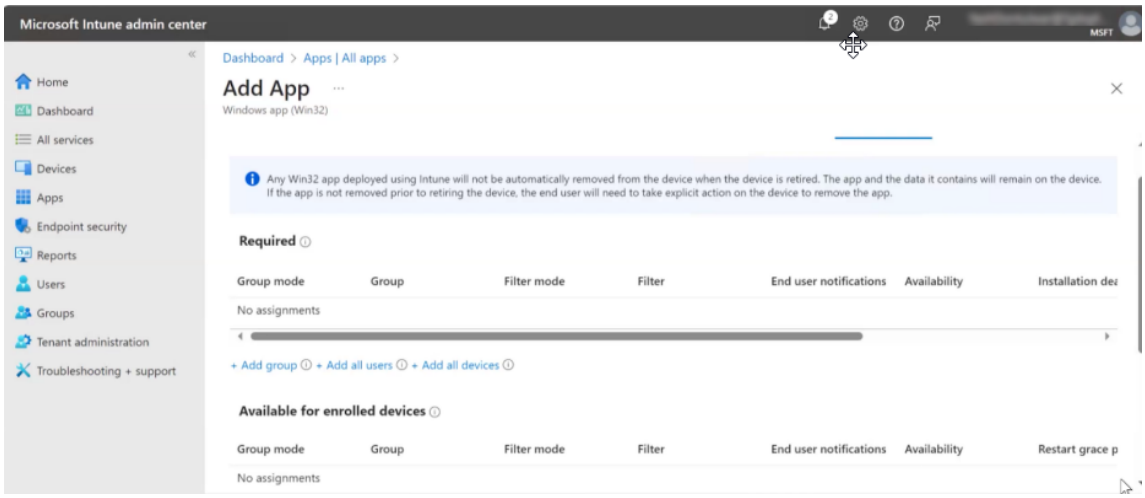
11. 次の画面の［**Detection rule**］タブで［**Detection rule**］を追加して、Broker Agent を追加します。［**OK**］をクリックします。



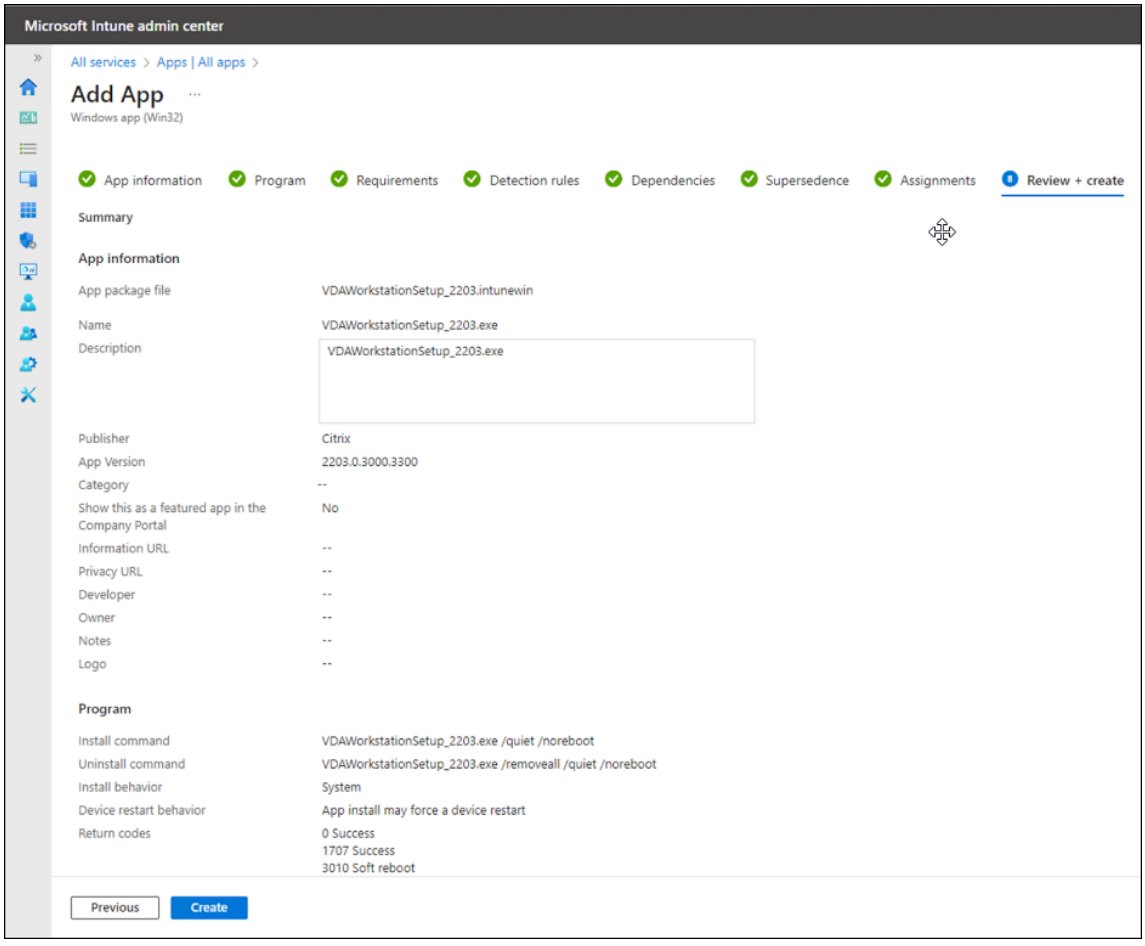
12. ［**Assignments**］タブの以下の値にデバイスを追加できます：

    - **Required**：自動的に更新が行われるデバイス。

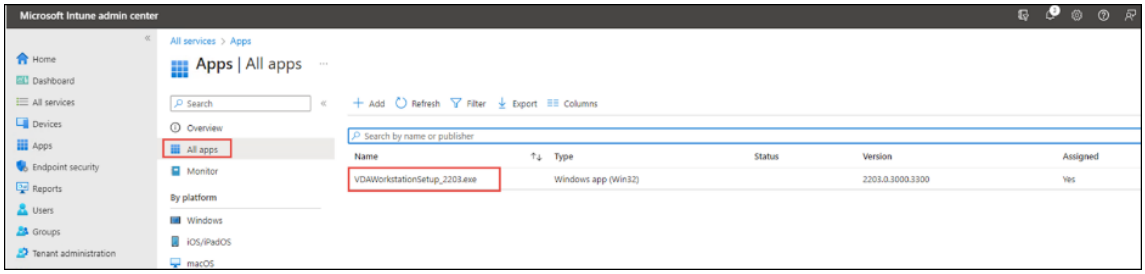
- **Available for enrolled devices**：手動で更新が行われるデバイス。



13. 詳細を確認して、［**Create**］をクリックします。



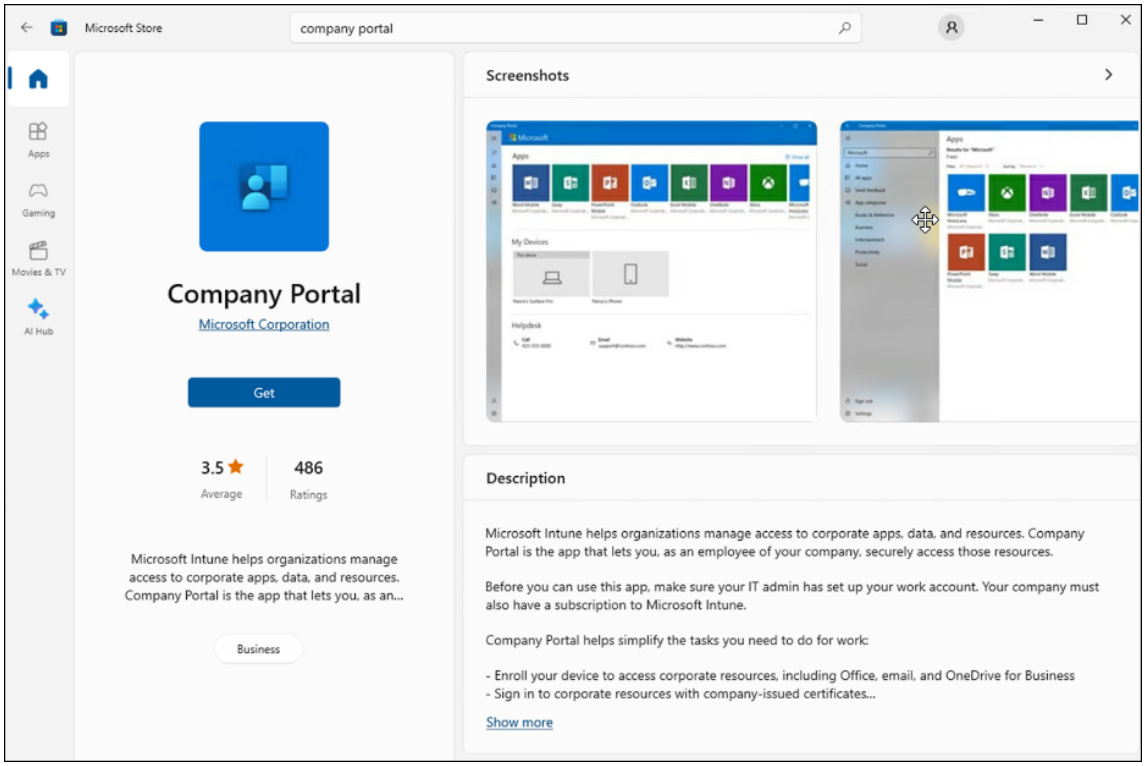
アプリは正常に割り当てられました。



詳細については、「アプリを追加して割り当てる」を参照してください。

手順 **4**: 登録したデバイスにアプリをインストール

1. 登録済みの Windows 10 デスクトップデバイスにサインインします。
   デバイスは Microsoft Intune に登録されている必要があります。また、アプリに割り当てたグループに含まれるアカウントを使用してデバイスにサインインする必要があります。詳しくは、Microsoftのドキュメントを参照してください。
2. ［スタート］メニューから、**Microsoft Store** を開きます。
3. ポータルサイトアプリを見つけてインストールします。



4. ポータルサイトアプリを実行します。
5. Microsoft Intune を使用して追加したアプリをクリックします。
   Intune ユーザーにアプリが正常に割り当てられなかった場合は、次のメッセージが表示されます:


```
Your IT administrator did not make any apps available to you.
```

6. [**Install**] をクリックします。

サイトの作成

August 17, 2024

> 注:
>
> サイトの作成中に、ハイブリッド権利ライセンスを有効にするライセンスを追加した後、サイトの作成が完了するまで、パブリッククラウドホスト（Microsoft Azure、Google Cloud Platform、Amazon Web Services など）は接続の種類のリストに表示されません。

サイトとは、Citrix Virtual Apps and Desktops 展開に指定する名前のことです。サイトは、Delivery Controller などのコアコンポーネント、VDA（Virtual Delivery Agent）、ホストへの接続、およびマシンカタログやデリバリーグループで構成されます。コアコンポーネントをインストールしたら、最初のマシンカタログやデリバリーグループを作成する前に、サイトを作成します。

Controller が Server Core にインストールされている場合は、Citrix Virtual Apps and Desktops SDKの PowerShell コマンドレットを使用してサイトを作成します。

サイトを作成すると、Citrix のカスタマーエクスペリエンス向上プログラム（CEIP）に自動的に登録されます。CEIP では、統計情報や使用状況が匿名で収集され、Citrix に送信されます。最初のデータパッケージは、サイトを作成してから約 7 日後に Citrix に送信されます。登録内容は、サイトの作成後いつでも変更できます。Web Studio の左側のペインで ［設定］を選択し、**Citrix** カスタマーエクスペリエンス向上プログラムの設定を見つけます。詳しくは、http://more.citrix.com/XD-CEIPを参照してください。

サイトを作成する管理者には、そのサイトのすべての管理タスクの実行権限が設定されます。詳しくは、「管理者権限の委任」を参照してください。

成り行きを予想できるように、この記事を確認してからサイトを作成してください。

手順 **1**：サイト作成ウィザードを開く **- Citrix Site Manager**

Citrix Site Manager というツールを使用して、Citrix Virtual Apps and Desktops 環境（サイト）をセットアップします。ツールは、Delivery Controller のインストール時に自動的にインストールされます。

このツールを実行するには、Delivery Controller でデスクトップの［スタート］メニューを開き、［**Citrix**］**>** [**Citrix Site Manager**］を選択します。「Web Studio のインストール」を参照してください。

手順 **2**：サイト名

［はじめに］ページで、サイトの名前を入力します。

手順 **3**：データベース

［データベース］ページには、サイト、監視、および構成ログの各データベースを設定するための選択肢が含まれています。データベースセットアップでの選択肢および要件について詳しくは、「データベース」を参照してください。

> 注：
>
> SQL Server Always On リスナーが TLS 暗号化用に構成されている場合、データベース作成権限がある資格情報を入力するように求められる場合があります。有効な管理者資格情報を入力した場合でも、データベースを作成しようとすると失敗します。SQL Server 証明書のサブジェクト別名（SAN）にリスナーの DNS 名が含まれていることを確認します。詳しくは、https://docs.microsoft.com/en-us/sql/database-engine/availability-groups/windows/listeners-client-connectivity-application-failover#SSLcertificatesを参照してください。

サイトデータベースとして使用する目的で SQL Server Express をインストールするように選択した場合（これはデフォルト設定です）、このソフトウェアのインストール後に再起動が行われます。SQL Server Express ソフトウェアをサイトデータベースとしてインストールしない場合、再起動は行われません。

デフォルトの SQL Server Express を使用しない場合は、サイトを作成する前に、マシンに SQL Server ソフトウェアがインストールされていることを確認してください。サポートされるバージョンについては、「システム要件」を参照してください。

サイトに Delivery Controller を追加する必要があり、Controller ソフトウェアが別のサーバーに既にインストールされている場合、このページからこれらの Controller を追加できます。また、データベースをセットアップするスクリプトを生成する予定の場合には、スクリプトを生成する前に Controller を追加します。

手順 **4**：ライセンス

［ライセンス］ページでライセンスサーバーのアドレスを指定して、使用（インストール）するライセンスを決定します。

- ライセンスサーバーのアドレスを、`name:[port]`という形式で指定します。名前は、FQDN（完全修飾ドメイン名）、NetBIOS、または IP アドレスである必要があります。推奨は FQDN です。ポート番号（<port>）を入力しない場合は、デフォルトの 27000 が使用されます。［接続］をクリックします。ライセンスサーバーに接続されるまでは、次のページに進めません。
- 接続が確立されると、［既存のライセンスを使用する］がデフォルトで選択されます。ディスプレイには、現在インストールされているライセンスに基づいて、この製品を構成できる互換性のある製品が一覧表示されます。

- 一覧にある製品（Citrix Virtual Apps Premium または Citrix Virtual Desktops Premium など）の 1 つとしていずれかのライセンスを使用してこの製品を構成する場合は、そのエントリを選択します。
- この製品で使用するライセンスを（Citrix Manage Licenses Tool を使用して）割り当ててダウンロードしたが、ライセンスをまだインストールしていない場合：
  * ［ライセンス ファイルの参照…］をクリックします。
  * ファイルエクスプローラーで、ダウンロードしたライセンスを見つけて選択します。関連付けられた製品が、サイト作成ウィザードの ［ライセンス］ページに表示されます。使用するエントリを選択します。
- 必要な製品が表示されない場合、または割り当て済みライセンスやダウンロード済みのライセンスがない場合は、ライセンスの割り当て、ダウンロード、インストールを実行できます。これを行うには、ライセンスサーバーがインターネットにアクセスできる必要があります。また、必要な製品のライセンスアクセスコードが必要です。コードは Citrix からメールで届きます。
  * ［割り当ておよびダウンロード］をクリックします。
  * ［ライセンスの割り当て］ダイアログボックスで Citrix から届いたライセンスアクセスコードを入力します。［ライセンスの割り当て］をクリックします。
  * 新しいライセンスに関連付けられた製品が、サイト作成ウィザードの ［ライセンス］ページに表示されます。使用するエントリを選択します。

  または、［**30** 日間無料のトライアルを使用する］を選択し、ライセンスを後でインストールします。詳しくは、「ライセンス」を参照してください。

手順 **5**：まとめ

［概要］ページに、指定した情報が一覧表示されます。内容を変更する場合は、［戻る］をクリックします。完了したら、［完了］をクリックします。

追加情報

ホスト接続、ネットワーク、およびストレージ

ハイパーバイザーやその他のサービスで仮想マシンを使用してアプリケーションとデスクトップを提供する場合、必要に応じて、そのホストへの最初の接続を作成できます。その接続のストレージリソースとネットワークリソースも指定できます。サイトの作成後、この接続やリソースを変更したり、追加の接続を作成したりできます。詳しくは、「接続とリソース」を参照してください。

- ［接続］ページで指定する情報については、「接続とリソース」を参照してください。
  - ハイパーバイザーやその他のサービスで仮想マシンを使用している場合（または Web Studio を使用して専用ブレード PC 上でデスクトップを管理する場合）には、接続の種類として ［なし］を選択します。

  - リモート PC アクセスサイトを構成しており、Wake on LAN 機能を使用する予定の場合、[**Microsoft System Center Configuration Manager**] または [リモート **PC Wake on LAN**] を選択します。詳しくは、「Wake on LAN」を参照してください。

接続の種類に加え、仮想マシンの作成で Citrix のツール（Machine Creation Services など）を使用するか、その他のツールを使用するかも指定します。

- [ストレージ] および [ネットワーク] ページで指定された情報については、「ホストストレージ」、「ストレージ管理」、「ストレージの選択」を参照してください。
- ハイブリッド権利ライセンスがあり、パブリッククラウドホスト接続（AWS など）を追加した場合、その接続はここに一覧表示されます。これらのパブリッククラウドホスト接続を表示するには、それらを追加してから数分後に Web Studio を更新します。

リモート **PC** アクセス

リモート PC アクセス展開について詳しくは、「リモート PC アクセス」を参照してください。

Wake on LAN 機能を使用している場合、サイトを作成する前に Microsoft System Center Configuration Manager の構成手順を実行します。詳しくは、「Configuration Manager とリモート PC アクセスの Wake on LAN」を参照してください。

接続とリソースの作成と管理

August 17, 2024

> 重要:
>
> Citrix Virtual Apps and Desktops 7 2006 では、現在の展開で次のテクノロジのいずれかを使用している場合、これらのテクノロジを使用する製品終了（EOL）アイテムを削除した後でのみ、展開を現在のリリースにアップグレードできます。
>
> - Personal vDisk（PvD）
> - AppDisk
> - パブリッククラウドのホストタイプ：Citrix CloudPlatform、Microsoft Azure Classic
>
> 詳しくは、「PvD、AppDisk、およびサポートされていないホストの削除」を参照してください。
>
> 注:
>
> Web Studio（Web ベース）と Citrix Studio（Windows ベース）の 2 つの管理コンソールを使用して、Citrix Virtual Apps and Desktops の展開を管理できます。この記事では Web Studio のみを扱います。Citrix Studio について詳しくは、Citrix Virtual Apps and Desktops 7 2212 以前の同様の記事を参照してくださ

> い。

展開環境に対してパブリッククラウドホスト接続を使用する場合、新規インストールを完了する、または最新リリースにアップグレードするのに、ハイブリッド権利ライセンスが必要です。

1 つまたは複数のサポートされていないテクノロジ、またはハイブリッド権利ライセンスなしのホスト接続をインストーラーが検出すると、アップグレードが一時停止または停止し、説明メッセージが表示されます。インストーラーログに詳細が記載されています。詳しくは、「環境のアップグレード」を参照してください。

ホスト接続でのハイブリッド権利ライセンスの影響

ハイブリッド権利ライセンスの使用権に基づいて、パブリッククラウドホストへのホスト接続が影響を受けるシナリオは 3 つあります:

- パブリッククラウドホストへの新しいホスト接続を作成するには、ハイブリッド権利ライセンスが必要です。
- ハイブリッド権利ライセンスはあるがライセンスの有効期限が切れている場合、パブリッククラウドホストへの既存の接続は権限なしとマークされ、メンテナンスモードになります。既存のホスト接続がメンテナンスモードの場合、次を実行することはできません:
  - ホスト接続の追加または変更
  - カタログの作成とイメージの更新
  - 電源操作の実行
- 権限のないホスト接続が権限のあるものに変更されると、既存のホスト接続が再度有効になります。

はじめに

管理者は、サイトを作成するときに、オプションでホストリソースへの最初の接続を作成できます。後でその接続を変更したり、別の接続を作成したりできます。接続の構成には、サポートされているハイパーバイザーから接続タイプを選択すること、およびその接続について、リソースから選択したストレージとネットワークを選択することが含まれます。

読み取り専用管理者は、接続とリソースの詳細を表示できます。接続とリソースの管理を行うには、すべての管理権限を実行できる管理者である必要があります。詳しくは、「委任管理」を参照してください。

接続の種類に関する情報の参照先

管理者は、サポートされている仮想化プラットフォームを使用して、Citrix Virtual Apps や Citrix Virtual Desktops の環境をホストおよび管理できます。サポートされる種類については、「システム要件」を参照してください。

詳しくは、以下の情報ソースを参照してください:

- **XenServer**（旧称 **Citrix Hypervisor**）:

  - XenServer 仮想化環境。
  - XenServer のドキュメント。

- **Nutanix Acropolis**:

  - Nutanix 仮想化環境
  - Nutanix のドキュメント

- **VMware**:

  - VMware 仮想化環境
  - VMware 製品ドキュメント:

- **Microsoft Hyper-V**:

  - 「Microsoft System Center Virtual Machine Manager 仮想化環境」
  - Microsoft 社のドキュメント

- パブリッククラウドホスト接続（**AWS**、**Google Cloud**、**Microsoft Azure**、**Nutanix** クラウドおよびパートナーソリューション、**VMware** クラウドおよびパートナーソリューション）**:** パブリッククラウドホストについては、「リソースの種類の設定」を参照してください。

  > 注:
  >
  > 情報ソースから、Citrix DaaS のドキュメントに移動できます。Citrix DaaS 製品のパブリッククラウドホストに精通している場合、オンプレミスバージョンにはいくつかの違いがあります。オンプレミスの Virtual Apps and Desktops では、管理インターフェイスは Web Studio と呼ばれます。更新は、約 4 週間ごとにサービスにロールアウトされます。そのため、サービスで使用できる特定の機能がオンプレミスバージョンでは使用できない場合があります。

ホストストレージ

ストレージ製品は、サポートされているハイパーバイザーで管理される場合にサポートされます。Citrix サポートでは、これらのストレージ製品ベンダーによる問題のトラブルシューティングと解決をサポートし、必要に応じて Knowledge Center でそれらの問題をドキュメント化します。

マシンのプロビジョニング時、データは種類別に分類されます:

- マスターイメージを含むオペレーティングシステム（OS）データ。
- 一時データ。このデータには、MCS でプロビジョニングされたマシンに書き込まれるすべての非永続データ、Windows ページファイル、ユーザープロファイルデータ、および ShareFile と同期されるすべてのデータなどが含まれます。このデータは、マシンの再起動のたびに破棄されます。

データの種類ごとに個別のストレージを用意することにより、各ストレージデバイスの負荷が軽減されてパフォーマンスが向上し、ホストで使用可能なリソースを最大限に活用できます。さらに、他のデータに比べて永続性と復元性がより重要なデータなど、データの種類に応じて適切なストレージを使用できるようになります。

ストレージは共有（中央に配置し、すべてのホストから分離して、すべてのホストで使用）することも、ハイパーバイザーのローカルに配置することもできます。中央共有ストレージの例として、1 つまたは複数の Windows Server 2012 クラスターストレージボリューム（接続されたストレージありまたはなし）や、ストレージベンダーからのアプライアンスなどがあります。中央ストレージには、ハイパーバイザーのストレージ制御パスやパートナープラグインからの直接アクセスなど、独自の最適化が備わっていることもあります。

一時データをローカルに保存することにより、共有ストレージへのアクセスでネットワークを経由する必要がなくなります。さらに、共有ストレージデバイスの負荷も軽減されます。共有ストレージは費用が高いため、ローカルにデータを保存することによってコストを抑えられます。こうした利点は、ハイパーバイザーサーバー上で十分なストレージを使用できることよりも重要になるでしょう。

接続の作成時、ストレージをハイパーバイザー間で共有するか、またはストレージをハイパーバイザーのローカルに配置する 2 つのストレージ管理方法からいずれかを選択してください。

1 つまたは複数の XenServer ホスト上のローカルストレージを一時データストレージとして使用する場合は、プール内の各ストレージの場所に一意の名前が付いていることを確認してください。（XenCenter で名前を変更するには、ストレージを右クリックして名前のプロパティを編集します。）

ハイパーバイザー間で共有されるストレージ

ハイパーバイザー間でストレージを共有する方法では、長期間保持する必要のあるデータが保存され、バックアップおよび管理を一元的に行うことができます。このストレージは OS ディスクを保持します。

この方法を選択する場合、一時マシンデータに（同じハイパーバイザープール内のサーバー上の）ローカルストレージを使用するかどうかを選択できます。この方法では、永続性や、一時データキャッシュと呼ばれる共有ストレージ内のデータと同等の復元性は、必要ありません。ローカルディスクを使用することにより、メイン OS ストレージへのトラフィックが軽減されます。このディスクは、マシンの再起動のたびにクリアされます。ディスクは、ライトスルーメモリキャッシュを介してアクセスされます。一時データにローカルストレージを使用すると、プロビジョニングされた VDA は特定のハイパーバイザーホストに関連付けられます。このホストで障害が生じると、VM を起動できなくなります。

例外：クラスターストレージボリューム（CSV）を使用する場合、Microsoft System Center Virtual Machine Manager は、ローカルストレージでの一時データキャッシュディスクを許可しません。

接続を作成して一時データをローカルに保存してから、各 VM のキャッシュディスクサイズおよびメモリサイズにデフォルトではない値を有効にして構成します。デフォルト値は接続の種類に適切な値に設定されており、ほとんどの場合はデフォルト値で十分です。詳しくは、「マシンカタログの作成」を参照してください。

また、ハイパーバイザーはディスクイメージのローカルな読み込みキャッシュによる最適化テクノロジを提供します。たとえば、XenServer は IntelliCache を提供しており、これにより中央ストレージへのネットワークトラフィックを削減します。

ハイパーバイザーのローカルに配置するストレージ

ストレージをハイパーバイザーのローカルに配置する方法では、データはハイパーバイザー上にローカルで保存されます。この方法では、マスターイメージとその他の OS データがサイトのハイパーバイザーに転送されます。このプロセスは、最初のマシンの作成と将来のイメージの更新のために行われます。このプロセスにより、管理ネットワークでかなりのトラフィックが生じます。イメージ転送も時間がかかる処理であり、各ホストでイメージを利用できるようになるタイミングも異なります。

接続とリソースの作成

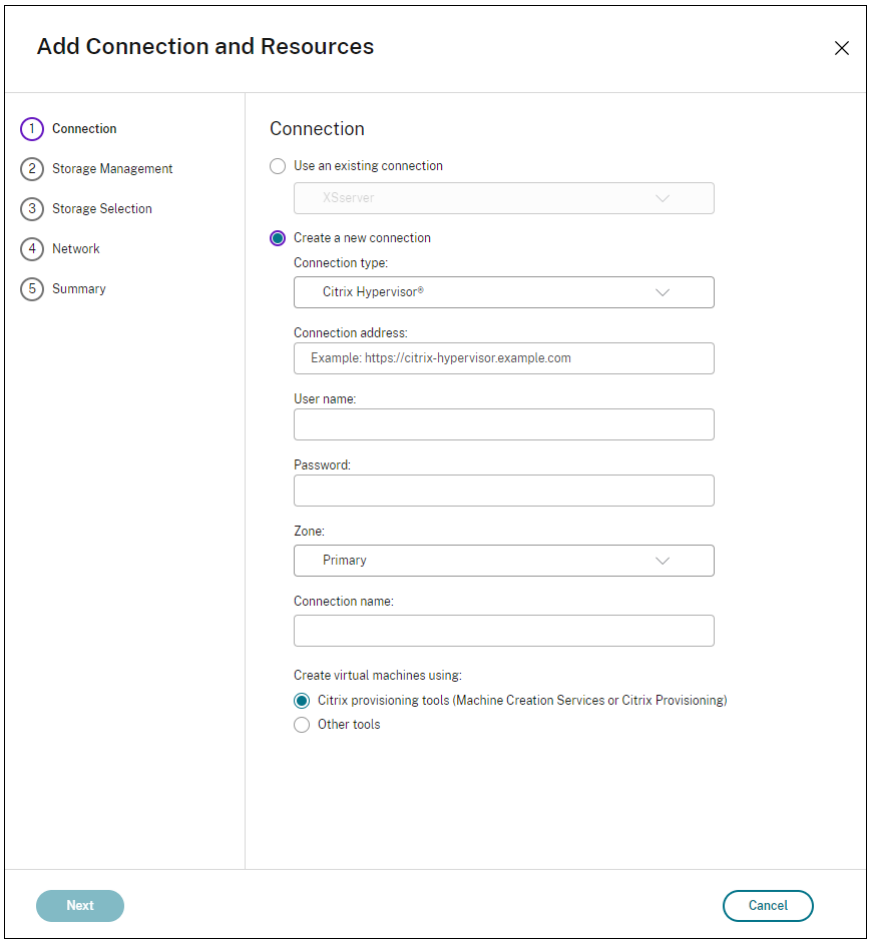
管理者は、サイトを作成するときに、オプションで最初の接続を作成できます。サイト作成ウィザードには、以下のセクションで説明する接続関連のページが含まれています。

サイト作成後に接続を作成する場合は、手順 1 から開始してください。

> 重要:
>
> 接続を作成する前に、ホストリソース（ストレージとネットワーク）が使用可能になっている必要があります。

1. Web Studio にサインインします。
2. 左側のペインで ［ホスト］を選択します。
3. 操作バーの ［接続およびリソースの追加］を選択します。
4. ウィザードの指示に従って、以下のページの操作を行います（具体的なページ内容は、選択した接続の種類に応じて異なります）。各ページの操作を終えたら、［概要］ページに到達するまで ［次へ］をクリックします。

接続

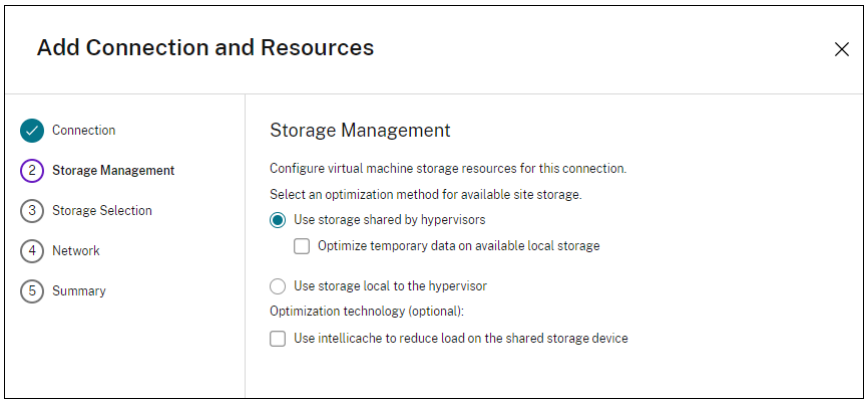


［接続］ページで以下を実行します：

- 接続を作成するには、［新しい接続を作成する］をクリックします。既存の接続と同じホスト構成に基づいて接続を作成する場合は、［既存の接続を使用する］を選択してから該当の接続を選択します。
- ［接続の種類］フィールドで、使用しているハイパーバイザーを選択します。パブリッククラウドホスト接続は、ハイブリッド権利ライセンスを使用している場合にのみドロップダウンリストに表示されます。または、PowerShell コマンド`Get-HypHypervisorPlugin [-ZoneUid] $rluid [-IncludeUnavailable]`の false または true を使用して、次の情報を取得することができます：
  - Citrix がサポートするすべてのハイパーバイザープラグインの一覧（サードパーティのプラグインを含む）。
  - ハイパーバイザープラグインの可用性。可用性のステータスが **false** の場合、ハイパーバイザーのプラグインが正しくインストールされていないか、ハイブリッド権利ライセンスが付与されていないことが考えられます。
- 接続のアドレスおよび資格情報は、選択した接続の種類に応じて異なります。要求された情報を入力します。

- 接続名を入力します。この接続名は Web Studio で表示されます。
- 仮想マシンの作成に使用するツールを、Web Studio ツール（Machine Creation Services や Citrix Provisioning など）またはその他のツールから選択します。

ストレージの管理



ストレージ管理の種類と方法について詳しくは、「ホストストレージ」を参照してください。

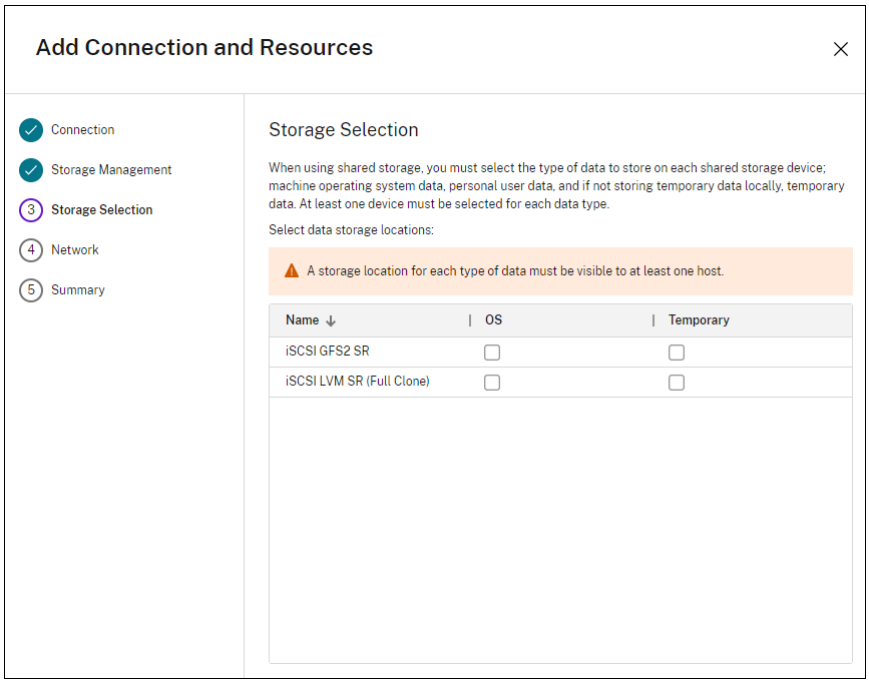
Hyper-V または VMware ホストに対する接続を構成している場合は、クラスター名を参照してから選択します。他の接続の種類では、クラスター名は要求されません。

ストレージ管理方法（ハイパーバイザー間で共有されるストレージまたはハイパーバイザーのローカルに配置するストレージ）を選択します。

- ハイパーバイザー間で共有されるストレージを選択する場合、一時データを使用可能なローカルストレージで保持するかどうかを指定します（この接続を使用するマシンカタログで、デフォルトではない一時ストレージのサイズを指定できます）。例外：クラスターストレージボリューム（CSV）を使用する場合、Microsoft System Center Virtual Machine Manager は、ローカルストレージでの一時データキャッシュディスクを許可しません。Web Studio でそのストレージ管理設定を構成すると失敗します。

XenServer プール上で共有ストレージを使用する場合は、IntelliCache を使用して共有ストレージデバイスにかかる負荷を減らすかどうかを指定します。「XenServer 接続での IntelliCache の使用」を参照してください。

ストレージの選択



ストレージの選択について詳しくは、「ホストストレージ」を参照してください。

使用可能なデータの種類ごとに 1 つ以上のストレージデバイスを選択します。前のページで選択したストレージ管理方法によって、このページで選択できるデータの種類は変化します。サポートされる各データの種類に対して 1 つ以上のストレージデバイスを選択すると、ウィザードの次のページに進むことができます。

ハイパーバイザーによって共有されるストレージを選択し、前のページで ［利用可能なローカルストレージ上で一時データを最適化します］を有効にした場合、［ストレージの選択］ページの下部に表示される構成オプションが増えます。一時データに使用するローカルストレージデバイスを選択できます。

現在選択中のストレージデバイスの数が表示されます（前述の図では「1 個のストレージデバイスが選択されました」）。このエントリの上にカーソルを合わせると、選択したデバイスの名前が表示されます。

1. 使用するストレージデバイスを変更するには［選択］をクリックします。
2. ［ストレージの選択］ダイアログボックスで、ストレージデバイスのチェックボックスをオンまたはオフにして［**OK**］をクリックします。

ネットワーク

［ネットワーク］ページで、リソースの名前を入力します。この名前は、接続に関連付けられたストレージとネットワークの組み合わせを識別できるように、Web Studio に表示されます。

仮想マシンで使用するネットワークを 1 つまたは複数選択します。

まとめ

［概要］ページで、選択した内容を確認します。確認が完了したら、［完了］をクリックします。

重要事項：一時データをローカルに保存すると、この接続を使用するマシンを含んだマシンカタログを作成するときに、一時データストレージにデフォルトではない値を設定できます。「マシンカタログの作成」を参照してください。

接続の設定の編集

接続の名前の変更または接続の作成のために、この手順を使用しないでください。これらの接続は異なる操作です。現在のホストマシンに新しいアドレスがある場合にのみ、アドレスを変更します。別のマシンへのアドレスを入力すると、接続のマシンカタログが壊れます。

接続の **GPU** 設定を変更することはできません。これは、そのリソースにアクセスするマシンカタログで、GPU 固有のマスターイメージを使用する必要があるためです。接続の作成

1. Web Studio にサインインします。
2. 左側のペインで ［ホスト］を選択します。
3. 接続を選択し、操作バーの ［接続の編集］を選択します。
4. 接続の編集時に可能な設定については、ガイダンスに従います。
5. 完了したら ［適用］をクリックして行った変更を適用しウィンドウを開いたままにするか、［保存］をクリックして変更を適用しウィンドウを閉じます。

［接続のプロパティ］ページ：

- 接続アドレスおよび資格情報を変更するには、［設定の編集…］をクリックし、新しい情報を入力します。
- XenServer 接続に対して高可用性サーバーを指定する場合は、［設定の編集…］でサーバーを選択します。プールマスターに障害が生じても XenServer との通信が中断されないように、プール内のすべてのサーバーを選択することをお勧めします。

  > 注：
  >
  > HTTPS を使用していて、高可用性サーバーを構成する場合は、ワイルドカード証明書をプール内のすべてのサーバーにインストールしないようにしてください。サーバーごとに個別の証明書が必要です。

［詳細設定］ページ：

- 接続の種類が、リモート PC アクセスで使用される Microsoft System Center Configuration Manager（ConfMgr）の Wake On LAN 接続の場合は、**ConfMgr** のウェイクアッププロキシ、マジックパケット、およびパケットの転送情報を入力します。
- 制限しきい値設定を使用して、接続に対して許可される電源操作の最大数を指定することができます。電源管理設定で同時に起動するマシンの数が多すぎたり少なすぎたりする場合に、この設定を行います。接続の種類

のそれぞれには固有のデフォルト値が設定されています。これらの値は、ほとんどのケースに適切であり変更する必要はありません。

- ［同時操作（すべての種類）］設定では次の 2 つの値を指定します：この接続で同時に実行できる操作の最大数（絶対数）、すべてのマシンのうちこの接続を使用できるマシンの割合（パーセンテージ）で指定します。絶対値とパーセンテージ値の両方が必要です。実際に適用される制限は、いずれか値の小さい方になります。

  たとえば、［同時操作（すべての種類）］の絶対値が 10、パーセンテージ値が 10、この接続の総仮想マシン数が 34 の場合、実際に適用される上限値は、絶対値の 10 よりも小さい、34 の 10% を四捨五入した 3 になります。

- ［**1** 分あたりの最大新規操作］は、絶対値です。パーセンテージ値はありません。
- ［接続オプション］ボックスへの情報の入力は、Citrix サポート担当者からの指示があった場合か、ドキュメントで明示的に指示を受けた場合のみ行ってください。

［共有テナント］ページ：

この接続のサブスクリプションと Azure Compute Gallery を共有しているテナントとサブスクリプションを追加します。その結果、カタログを作成または更新するときに、それらのテナントおよびサブスクリプションから共有イメージを選択できます。

- この接続に関連付けられているアプリケーションのアプリケーション **ID** とアプリケーションシークレットを入力します。この情報を使用して、Azure に認証できます。セキュリティを確保にするために、キーを定期的に変更することをお勧めします。
- 共有テナントとサブスクリプションを指定します。最大 8 つの共有テナントを追加できます。テナントごとに最大 8 つのサブスクリプションを追加できます。
- 変更が完了したら ［保存］、［適用］の順にクリックします。

［接続オプション］ボックスへの情報の入力は、Citrix サポート担当者からの指示があった場合だけ行ってください。

ネットワークの編集

接続するネットワークを変更できます。以下を実行します：

1. ［ホスト］に移動します。
2. 接続のターゲットリソースを選択し、操作バーの ［**Edit Network**］を選択します。
3. 仮想マシンで使用するネットワークを選択してください。
4. ［保存］をクリックして変更を保存し、終了します。

接続のメンテナンスモードのオン/オフの切り替え

接続のメンテナンスモードをオンにすると、その接続（ホスト）上に格納されているマシンに新規の電源操作が適用されるのを防ぐことができます。ユーザーは、メンテナンスモードになっているマシンには接続できません。ユーザーが既に接続している場合は、そのユーザーがログオフした時点でメンテナンスモードが有効になります。

1. Web Studio にサインインします。
2. 左側のペインで ［ホスト］を選択します。
3. 接続を選択します。メンテナンスモードをオンにする場合は、操作バーの ［メンテナンスモードをオンにする］を選択します。メンテナンスモードをオフにするには、［メンテナンスモードをオフにする］を選択します。

個々のマシンのメンテナンスモードをオンまたはオフにすることもできます。マシンカタログ内またはデリバリーグループ内のマシンに対し、メンテナンスモードをオンまたはオフにすることもできます。

接続の削除

接続の削除は、多くのマシンおよびそのデータの損失が発生する可能性のある操作です。削除されるマシン上に重要なユーザーデータがないかどうかを確認し、重要なデータがある場合はバックアップを作成しておいてください。

接続を削除する前に、以下の点について確認してください:

- 接続上に格納されているマシンからすべてのユーザーがログオフしていること。
- 実行したまま切断されたユーザーセッションがないこと。
- プールおよび専用のマシンの場合は、メンテナンスモードになっていること。
- 接続で使用されている、マシンカタログ内のすべてのマシンの電源がオフになっていること。

マシンカタログで指定されている接続を削除すると、そのカタログを使用できなくなります。削除する接続がマシンカタログにより参照されている場合は、同時にそのカタログを削除することもできます。ただし、そのマシンカタログがほかの接続で使用されていないことを確認してから削除してください。

1. Web Studio にサインインします。
2. 左側のペインで ［ホスト］を選択します。
3. 接続を選択し、操作バーの ［接続の削除］を選択します。
4. この接続上にマシンが格納されている場合、マシンを削除するかどうかを確認するメッセージが表示されます。削除する場合は、それらのマシンの Active Directory コンピューターアカウントに対する操作を指定します。

接続の名前変更またはテスト

1. Web Studio にサインインします。
2. 左側のペインで ［ホスト］を選択します。
3. 接続を選択し、操作バーで ［接続名の変更］または ［テスト接続］を選択します。

接続上のマシンの詳細の表示

1. Web Studio にサインインします。
2. 左側のペインで ［ホスト］を選択します。
3. 接続を選択し、操作バーで ［マシンの表示］を選択します。

上ペインにその接続でアクセスするマシンの一覧が表示されます。マシンを選択すると、その詳細が下ペインに表示されます。実行中のセッションがある場合は、そのセッションの詳細も表示されます。

検索機能を使うと、マシンをすばやく見つけることができます。ウィンドウ上部の一覧から保存済みの検索を選択するか、または検索を作成します。マシン名の一部または全体を入力して検索したり、詳細な検索式を作成したりできます。検索式を作成するには、［展開］をクリックして、一覧からプロパティや演算子を選択します。

接続上のマシンの管理

1. Web Studio にサインインします。
2. 左側のペインで ［ホスト］を選択します。
3. 接続を選択し、［操作］ペインの ［マシンの表示］を選択します。
4. 操作バーで次のいずれかを選択します。マシンの状態や接続ホストの種類によっては、一部の操作を選択できません。

アクション	説明
開始	電源がオフまたは一時停止状態のマシンを起動します。
一時停止	マシンをシャットダウンすることなく一時的に停止して、マシン一覧を更新します。
シャットダウン	オペレーティングシステムにシャットダウンを要求します。
強制シャットダウン	マシンの電源を強制的に切って、マシン一覧を更新します。
再起動	オペレーティングシステムに再起動を要求します。オペレーティングシステムで再起動を実行できない場合、デスクトップの状態は変更されません。
メンテナンスモードの有効化	マシンへの接続を一時的に停止します。この状態のマシンにユーザーが接続することはできません。ユーザーが既に接続している場合は、そのユーザーがログオフした時点でメンテナンスモードが有効になります（前述のとおり、接続上のすべてのマシンのメンテナンスモードをオンまたはオフにすることもできます。）
デリバリー グループから削除	マシンをデリバリーグループから削除しても、そのデリバリーグループで使用するマシンカタログからは削除されません。ユーザーが接続しているマシンは削除できません。削除するマシンにユーザーが接続しないようにするには、メンテナンスモードを一時的にオンにしてください。

アクション	説明
削除	マシンを削除すると、ユーザーはそのマシンにアクセスできなくなります。また、そのマシンはマシンカタログから削除されます。マシンを削除する前に、必要なユーザーデータをすべてバックアップしておいてください。ユーザーが接続しているマシンは削除できません。削除するマシンにユーザーが接続しないようにするには、メンテナンスモードを一時的にオンにしてください。

マシンのシャットダウンを伴う操作でマシンが 10 分以内にシャットダウンしない場合、電源が切れ、強制的にシャットダウンされます。シャットダウン中に Windows が更新のインストールを開始すると、更新が完了する前にマシンの電源が切れる危険性があります。

ストレージの編集

接続を使用する仮想マシンのオペレーティングシステムおよび一時データの保存に使用されているサーバーの状態を表示できます。データの種類それぞれの保存に使用するサーバーを指定することもできます。

1. Web Studio にサインインします。
2. 左側のペインで ［ホスト］を選択します。
3. 接続を選択し、操作バーの ［ストレージの編集］を選択します。
4. 左側のペインでデータの種類（オペレーティングシステムデータ、または一時データ）を選択します。
5. 選択したデータの種類に対し、1 つ以上のストレージデバイスのチェックボックスをオンまたはオフにします。
6. ［**OK**］をクリックします。

一覧の各ストレージデバイスには、デバイス名とストレージの状態が表示されます。有効なストレージの状態の値は次のとおりです:

- 使用中: ストレージはマシンの作成に使用されています。
- 置き換え済み: ストレージは既存のマシン用にのみ使用されています。このストレージに新しいマシンは追加されません。
- 使用中でない: ストレージはマシンの作成に使用されていません。

現在使用中のデバイスのチェックボックスをオフにすると、ステータスが一時停止に変更されます。既存のマシンは引き続きそのストレージデバイスを使用し、そのデバイスにデータを書き込むことができます。そのため、マシンの作成に使用されなくなっても、ストレージの空き領域が足りなくなる場合があります。

リソースの削除、名前変更、またはテスト

1. Web Studio にサインインします。

2. 左側のペインで ［ホスト］を選択します。
3. リソースを選択してから、操作バーで次の適切なエントリを選択します：［リソースの削除］、［リソース名の変更］、または ［リソースのテスト］。

孤立した **Azure** リソースを検出する

孤立したリソースはシステム内に存在する未使用のリソースであり、不要な出費につながる可能性があります。

この機能を使用すると、Citrix Virtual Apps and Desktops サイト上のホスト内で孤立した Azure リソースを検出できます。

Web Studio で次の手順を実行します：

1. ［管理］から、左側のペインで ［ホスト］を選択します。
2. 接続を選択し、操作バーで ［孤立したリソースを検出する］を選択します。［孤立したリソースを検出する］ダイアログボックスに孤立したリソースのレポートが表示されます。
3. 孤立したリソースのレポートを表示するには、［レポートの表示］を選択します。

または、PowerShell を使用して孤立した Azure リソースを検出することもできます。詳しくは、「孤立したリソースの一覧の取得」を参照してください。

孤立したリソースの背後にある理由を理解し、それらへの対処をさらに進める方法について詳しくは、「Citrix を使用して孤立した Azure リソースを効率的に管理する」を参照してください。

接続タイマー

ポリシー設定を使用すると、以下の 3 つの接続タイマーを構成できます。

- 最長接続タイマー：ユーザーデバイスと仮想デスクトップ間の連続セッションを自動的にログオフするまでの時間を制御します。これを構成するには、ポリシーの［セッション接続タイマー］設定および［セッション接続タイマー間隔］設定を使用します。
- 接続アイドルタイマー：ユーザーからの入力がないユーザーデバイスとデスクトップ間の連続セッションを自動的にログオフするまでの時間を制御します。これを構成するには、ポリシーの ［セッションアイドルタイマー］設定および ［セッションアイドルタイマーの間隔］設定を使用します。
- 切断タイマー：切断状態でロックされた仮想デスクトップセッションを自動的にログオフするまでの時間を制御します。これを構成するには、ポリシーの ［切断セッションタイマー］設定および ［切断セッションタイマーの間隔］設定を使用します。

これらの設定項目を変更する場合は、環境全体で設定が一貫していることを確認してください。

詳しくは、ポリシー設定のドキュメントを参照してください。

孤立したリソースの一覧の取得

MCS で作成されたのに、MCS で追跡されなくなった孤立したリソースの一覧を取得できます。これは現時点では Azure 環境で適用可能です。リストを取得するには、PowerShell コマンドを使用できます。接続を使用してフィルタリングできます。

> 注:
>
> - プロビジョニングまたはイメージの更新が処理中の場合、PowerShell コマンドは拒否されます。
> - すべての Citrix タグでタグ付けされた顧客が管理するリソースは、孤立したリソースとして検出されます。ただし、値が true の別のタグ CitrixDetectIgnore をそのリソースに追加すると、孤立したリソースの検出中にリソースは無視されます。

制限事項

- 組み込みのすべての管理権限を実行できる管理者、または Cloud Admin の役割を持つ管理ユーザーのみが PowerShell コマンドを実行して、孤立したリソースの一覧を取得できます。
- 孤立したリソースをフィルタリングしている間は VM の電源を入れないでください。孤立したリソースが誤って認識されるのを避けるためです。
- 孤立したリソースとしては、ワークロードが高くなる可能性がある場合、約 2,000 レコードのみが表示されます。

孤立したリソースのリストを表示するには:

1. **PowerShell** ウィンドウを開きます。
2. 次のコマンドを実行します:

   a) 接続 UID を取得します。接続 UID は、HypervisorConnectionUid 属性の値です。

   ```
   Get-ChildItem xdhyp:\connections | where {
     $_.PluginId -like 'Azure*'  }
    "
   ```

   b) 孤立したリソースの一覧を取得します。

   ```
   get-provorphanedresource -HypervisorConnectionUid <connection
       uid>
   ```

サブスクリプション ID から、孤立したリソースの一覧を表示するには:

1. **PowerShell** ウィンドウを開きます。
2. 次のコマンドを実行します:

   a) サブスクリプション ID を使用して接続 UID を見つけます。接続 UID は、HypervisorConnectionUid 属性の値です。


```
Get-ChildItem xdhyp:\connections | where {
  $_.CustomProperties -match '<subscriptionId>'  }
```

b) 孤立したリソースの一覧を取得します:

```
get-provorphanedresource -HypervisorConnectionUid <connection
    uid>
```

> 注:
>
> 削除する前にリソースを慎重に確認してください。

次の手順

特定のホストの種類への接続については、次を参照してください:

- AWS への接続
- XenServer への接続
- Google クラウド環境への接続
- Microsoft Azure への接続
- Microsoft System Center Virtual Machine Manager への接続
- Nutanix への接続
- Nutanix クラウドおよびパートナーソリューションへの接続
- VMware への接続
- VMware クラウドおよびパートナーソリューションへの接続

初期展開プロセスを行っている場合は、マシンカタログを作成します。

AWS への接続

August 17, 2024

「接続とリソースの作成と管理」では接続を作成するためのウィザードについて説明しています。以下の情報は、AWS クラウド環境に固有の詳細について説明しています。

> 注:
>
> AWS への接続を作成する前に、まず AWS アカウントをリソースの場所として設定する必要があります。「AWS クラウド環境」を参照してください。

接続の作成

Studio から接続を作成する場合：

- API キーと秘密キーの値を指定する必要があります。AWS でこれらの値を含んでいるキーファイルをエクスポートしてから、値をインポートすることができます。また、リージョン、アベイラビリティゾーン、仮想プライベートクラウド名、サブネットアドレス、ドメイン名、セキュリティグループ名、および資格情報も必要になります。
- AWS コンソールから取得するルート AWS アカウント用の資格情報ファイルでは、標準的な AWS ユーザーのものとは異なる形式が使用されています。このため、このファイルを Citrix Virtual Apps and Desktops 管理コンソールで、API キーと秘密キーの情報を入力するために使用することはできません。AWS Identity Access Management（IAM）形式の資格情報ファイルを使用してください。

> 注：
>
> 接続を作成した後、API キーと秘密キーを更新しようとすると失敗することがあります。この問題を解決するには、プロキシサーバーまたはファイアウォールの制限を確認し、次のアドレスに接続できることを確認してください：`https://*.amazonaws.com`。

ホスト接続のデフォルト値

AWS クラウド環境のホスト接続を作成すると、次のデフォルト値が表示されます：

オプション	絶対	パーセンテージ
同時操作（すべての種類）	125	100
1 分あたりの最大新規操作	125	

MCS は、デフォルトで最大 100 の同時プロビジョニング操作をサポートします。

サービスエンドポイント **URL**

標準ゾーンのサービスエンドポイント **URL**

MCS を使用すると、API キーと API シークレットで新しい AWS 接続が追加されます。この情報と認証済みアカウントで、MCS は AWS DescribeRegions EC2 API 呼び出しを使用して、サポートされているゾーンのクエリを AWS に対して実行します。このクエリは、一般的な EC2 サービスエンドポイント URL の`https://ec2.amazonaws.com/`を使用して行われます。MCS を使用して、サポートされているゾーンの一覧から、接続するゾーンを選択します。そのゾーンで優先される AWS サービスエンドポイント URL が自動的に選択されます。ただし、サービスエンドポイント URL を作成した後は、URL を設定または変更することはできなくなります。

IAM 権限の定義

このセクションの情報を使用して、AWS 上の Citrix Virtual Apps and Desktops の IAM アクセス許可を定義します。Amazon の IAM サービスでは、複数のユーザーを持つアカウントが許可されており、さらにグループに編成することができます。これらのユーザーは、アカウントに関連付けられた操作の実行を制御できるさまざまな権限を持つことができます。IAM アクセス許可について詳しくは、「IAM JSON ポリシーのリファレンス」を参照してください。

IAM アクセス権限ポリシーを新しいユーザーグループに適用するには、次を実行します:

1. AWS 管理コンソールにログインし、ドロップダウンリストから ［**IAM service**］を選択します。
2. ［**Create a New Group of Users**］を選択します。
3. 新しいユーザーグループの名前を入力し、［**Continue**］を選択します。
4. ［**Permissions**］ページで ［**Custom Policy**］を選択します。［**Select**］を選択します。
5. ［**Permissions policy**］の名前を入力します。
6. ［**Policy Document**］セクションで、関連する権限の情報を入力します。

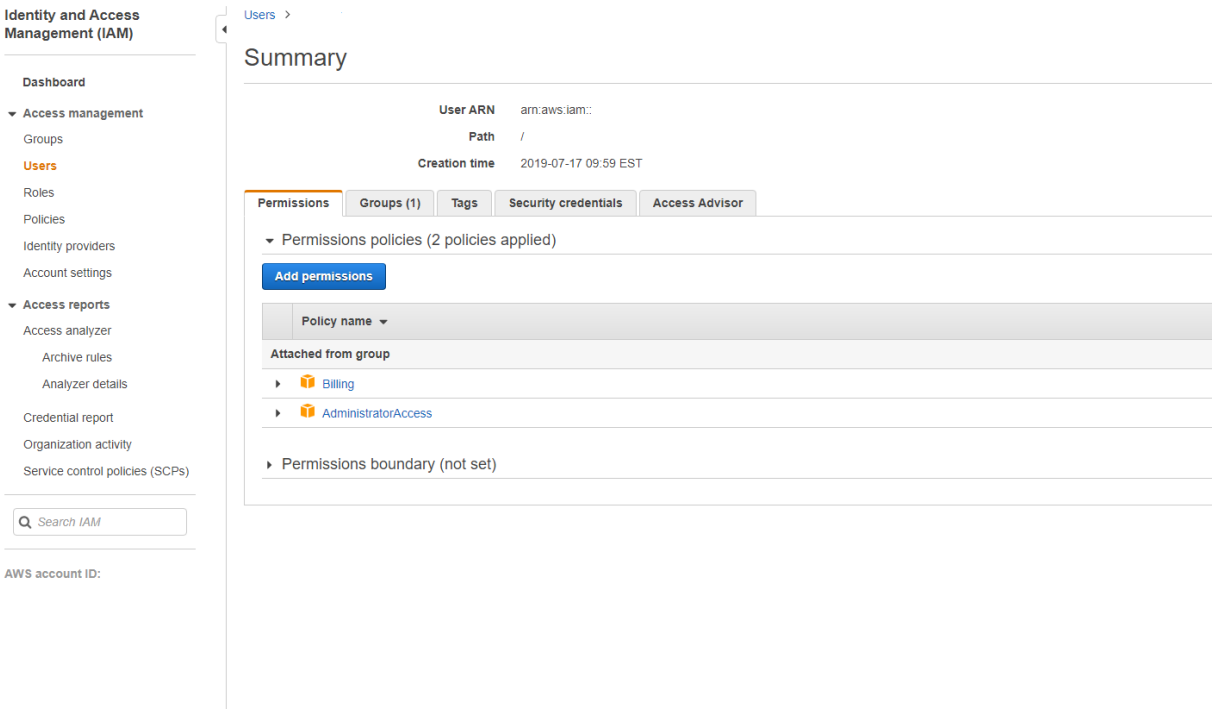
ポリシー情報の入力後、［**Continue**］を選択してユーザーのグループを完了します。グループ内のユーザーには、Citrix Virtual Apps and Desktops に必要なアクションのみを実行するためのアクセス許可が付与されます。

> 重要:
>
> 前述の例で提供されているポリシーテキストを使用して、Citrix Virtual Apps and Desktops が特定のリソースに限定せずに AWS アカウント内でアクションを実行するために使用するアクションを一覧表示します。Citrix では、この例はテスト目的で使用することをお勧めします。実稼働環境では、リソースにさらに制限を加えることを選択できます。

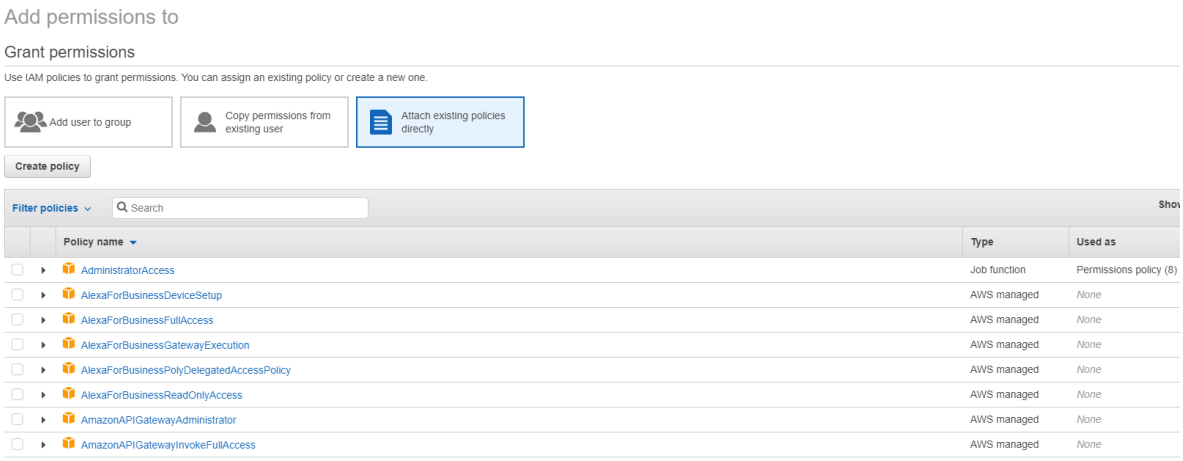
IAM アクセス許可の設定

AWS マネジメントコンソールの ［**IAM**］セクションで、アクセス許可を設定します:

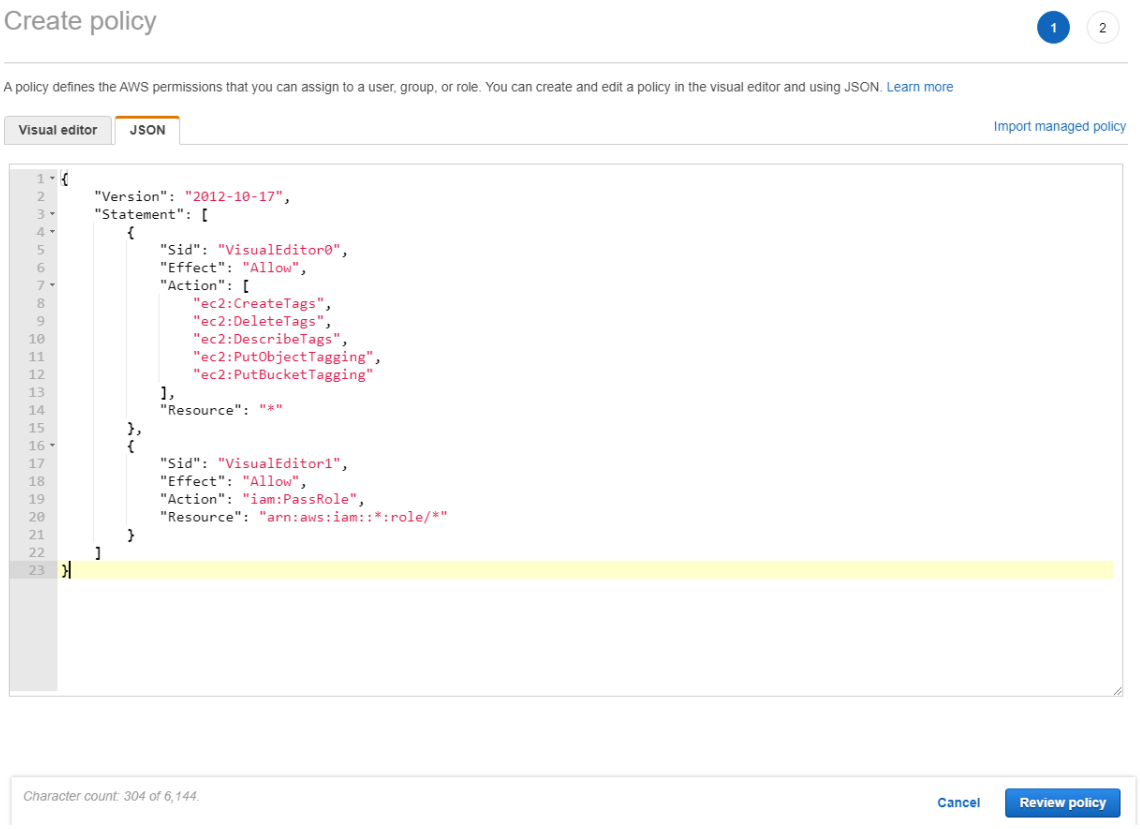
1. ［**Summary**］パネルで ［**Permissions**］タブを選択します。
2. ［**Add permissions**］を選択します。



[**Add Permissions to**]画面でアクセス許可を付与します:



以下は［**JSON**］タブの例です:



> ヒント：
>
> JSON の例には、環境に対するすべての権限が含まれているとは限らないことに注意してください。詳しくは、「AWS で Citrix Virtual Apps and Desktops を実行する ID アクセス管理の権限を定義する方法」を参照してください。

必要な **AWS** 権限

このセクションでは、AWS 権限の完全なリストが示されています。

> 注：
>
> *iam:PassRole* 権限は、**role_based_auth** でのみ必要です。

ホスト接続の作成

AWS からの情報を使用して、新しいホスト接続が追加されます。

```
{

    "Version": "2012-10-17",
    "Statement": [
        {
```



```
6
7               "Action": [
8                   "ec2:DescribeAvailabilityZones",
9                   "ec2:DescribeImages",
10                  "ec2:DescribeInstances",
11                  "ec2:DescribeInstanceTypes",
12                  "ec2:DescribeSecurityGroups",
13                  "ec2:DescribeSubnets",
14                  "ec2:DescribeVpcs"
15              ],
16              "Effect": "Allow",
17              "Resource": "*"
18          }
19
20      ]
21  }
```

VM の電源管理

マシンインスタンスの電源がオンまたはオフです。

```
1  {
2
3      "Version": "2012-10-17",
4      "Statement": [
5          {
6
7              "Action": [
8                  "ec2:AttachVolume",
9                  "ec2:CreateVolume",
10                 "ec2:DeleteVolume",
11                 "ec2:DescribeInstances",
12                 "ec2:DescribeVolumes",
13                 "ec2:DetachVolume",
14                 "ec2:StartInstances",
15                 "ec2:StopInstances"
16             ],
17             "Effect": "Allow",
18             "Resource": "*"
19         }
20
21     ]
22 }
```

VM の作成、更新、または削除

マシンカタログは、AWS インスタンスとしてプロビジョニングされた VM で、作成、更新、または削除されます。

```
1  {
```



```
2
3       "Version": "2012-10-17",
4       "Statement": [
5           {
6
7               "Action": [
8                   "ec2:AttachVolume",
9                   "ec2:AssociateIamInstanceProfile",
10                  "ec2:AuthorizeSecurityGroupEgress",
11                  "ec2:AuthorizeSecurityGroupIngress",
12                  "ec2:CreateImage",
13                  "ec2:CreateLaunchTemplate",
14                  "ec2:CreateSecurityGroup",
15                  "ec2:CreateTags",
16                  "ec2:CreateVolume",
17                  "ec2:DeleteVolume",
18                  "ec2:DescribeAccountAttributes",
19                  "ec2:DescribeAvailabilityZones",
20                  "ec2:DescribeIamInstanceProfileAssociations",
21                  "ec2:DescribeImages",
22                  "ec2:DescribeInstances",
23                  "ec2:DescribeInstanceTypes",
24                  "ec2:DescribeLaunchTemplates",
25                  "ec2:DescribeLaunchTemplateVersions",
26                  "ec2:DescribeNetworkInterfaces",
27                  "ec2:DescribeRegions",
28                  "ec2:DescribeSecurityGroups",
29                  "ec2:DescribeSnapshots",
30                  "ec2:DescribeSubnets",
31                  "ec2:DescribeTags",
32                  "ec2:DescribeVolumes",
33                  "ec2:DescribeVpcs",
34                  "ec2:DetachVolume",
35                  "ec2:DisassociateIamInstanceProfile",
36                  "ec2:RunInstances",
37                  "ec2:StartInstances",
38                  "ec2:StopInstances",
39                  "ec2:TerminateInstances"
40              ],
41              "Effect": "Allow",
42              "Resource": "*"
43          }
44  ,
45          {
46
47              "Action": [
48                  "ec2:AuthorizeSecurityGroupEgress",
49                  "ec2:AuthorizeSecurityGroupIngress",
50                  "ec2:CreateSecurityGroup",
51                  "ec2:DeleteSecurityGroup",
52                  "ec2:RevokeSecurityGroupEgress",
53                  "ec2:RevokeSecurityGroupIngress"
54              ],
```



```
            "Effect": "Allow",
            "Resource": "*"
        }
,
        {

            "Action": [
                "s3:CreateBucket",
                "s3:DeleteBucket",
                "s3:PutBucketAcl",
                "s3:PutBucketTagging",
                "s3:PutObject",
                "s3:GetObject",
                "s3:DeleteObject",
                "s3:PutObjectTagging"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:s3:::citrix*"
        }
,
        {

            "Action": [
                "ebs:StartSnapshot",
                "ebs:GetSnapshotBlock",
                "ebs:PutSnapshotBlock",
                "ebs:CompleteSnapshot",
                "ebs:ListSnapshotBlocks",
                "ebs:ListChangedBlocks",
                "ec2:CreateSnapshot"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }

    ]
}
```

> 注:
>
> セキュリティグループに関連する EC2 セクションは、カタログの作成中に準備 VM 用に分離セキュリティグループを作成する必要がある場合にのみ必要です。これが行われると、これらの権限は必要ありません。

ディスクの直接アップロードとダウンロード　ディスクの直接アップロードは、マシンカタログプロビジョニングのボリュームワーカー要件をなくし、代わりに AWS が提供するパブリック API を使用します。この機能により、追加のストレージアカウントに関連するコストと、ボリュームワーカーの操作を維持する複雑さが軽減されます。

> 注:
>
> ボリュームワーカーのサポートは廃止されました。

次の権限をポリシーに追加する必要があります:

- ebs:StartSnapshot
- ebs:GetSnapshotBlock
- ebs:PutSnapshotBlock
- ebs:CompleteSnapshot
- ebs:ListSnapshotBlocks
- ebs:ListChangedBlocks
- ec2:CreateSnapshot
- ec2:DeleteSnapshot
- ec2:DescribeLaunchTemplates

> 重要:
>
> - ボリュームワーカー AMI やボリュームワーカー VM などのボリュームワーカー操作を行わなくても、既存のマシンカタログに VM を追加できます。
> - 以前にボリュームワーカーを使用していた既存のカタログを削除すると、ボリュームワーカーに関連するアーティファクトを含むすべてのアーティファクトが削除されます。

作成されたボリュームの **EBS** 暗号化

AMI が暗号化されている場合、または EBS がすべての新しいボリュームを暗号化するように構成されている場合、EBS は新しく作成されたボリュームを自動で暗号化できます。ただし、この機能を実装するには、次の権限が IAM ポリシーに含まれている必要があります。

```
{

     "Version": "2012-10-17",
     "Statement": [
        {

            "Effect": "Allow",
            "Action": [
                 "kms:CreateGrant",
                 "kms:Decrypt",
                 "kms:DescribeKey",
                 "kms:GenerateDataKeyWithoutPlainText",
                 "kms:ReEncryptTo",
                 "kms:ReEncryptFrom"
            ],
            "Resource": "*"
         }

    ]
 }
```


> 注:
>
> Resource と Condition のブロックを含めることにより、ユーザーの裁量で権限を特定のキーに制限できます。たとえば、**Condition** を使用した **KMS** 権限:

```
{

     "Version": "2012-10-17",
     "Statement": [
        {

            "Effect": "Allow",
            "Action": [
                 "kms:CreateGrant",
                 "kms:Decrypt",
                 "kms:DescribeKey",
                 "kms:GenerateDataKeyWithoutPlainText",
                 "kms:ReEncryptTo",
                 "kms:ReEncryptFrom"
            ],
            "Resource": [
                "arn:aws:kms:us-east-2:123456789012:key/abcd1234-a123
                   -456d-a12b-a123b4cd56ef"
            ],
            "Condition": {

                "Bool": {

                    "kms:GrantIsForAWSResource": true
                 }

             }

          }

    ]
 }
```

以下のキーポリシーステートメントは、アカウントが IAM ポリシーを使用して KMS キーの全操作（kms:*）の権限を委任できるようにするために必要な KMS キーのデフォルトのキーポリシー全体です。

```
{

"Sid": "Enable IAM policies",
"Effect": "Allow",
"Principal": {

"AWS": "arn:aws:iam::111122223333:root"
 }
 ,
"Action": "kms:",
"Resource": ""
```



```
12    }
```

詳しくは、AWS Key Management Service 公式ドキュメントを参照してください。

IAM 役割ベースの認証

以下の権限が、役割ベースの認証をサポートするために追加されています。

```
1  {
2
3       "Version": "2012-10-17",
4       "Statement": [
5          {
6
7              "Effect": "Allow",
8              "Action": "iam:PassRole",
9              "Resource": "arn:aws:iam::*:role/*"
10          }
11
12      ]
13   }
```

最低限の IAM 権限ポリシー

以下の JSON は、現在サポートされているすべての機能に使用できます。このポリシーを使用して、ホスト接続の作成、VM の作成、更新、削除、および電源管理を行うことができます。
「IAM 権限の定義」セクションで説明されているように、ポリシーをユーザーに適用できます。または、**role_based_auth** セキュリティキーと秘密キーを使用して、役割ベースの認証を使用することもできます。

> 重要:
>
> **role_based_auth** を使用するには、まずサイトのすべての Delivery Controller で必要な IAM 役割を構成します。Web Studio を使用して、ホスティング接続を追加し、認証キーとシークレットの role_based_auth を指定します。これらの設定のホスティング接続は、役割ベースの認証を使用します。

```
1  {
2
3      "Version": "2012-10-17",
4      "Statement": [
5          {
6
7              "Action": [
8                  "ec2:AttachVolume",
9                  "ec2:AssociateIamInstanceProfile",
10                 "ec2:AuthorizeSecurityGroupEgress",
11                 "ec2:AuthorizeSecurityGroupIngress",
```



```
                "ec2:CreateImage",
                "ec2:CreateLaunchTemplate",
                "ec2:CreateNetworkInterface",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:DeleteLaunchTemplate",
                "ec2:DeleteNetworkInterface",
                "ec2:DeleteSecurityGroup",
                "ec2:DeleteSnapshot",
                "ec2:DeleteTags",
                "ec2:DeleteVolume",
                "ec2:DeregisterImage",
                "ec2:DescribeAccountAttributes",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeIamInstanceProfileAssociations",
                "ec2:DescribeImages",
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceTypes",
                "ec2:DescribeLaunchTemplates",
                "ec2:DescribeLaunchTemplateVersions",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeRegions",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSnapshots",
                "ec2:DescribeSubnets",
                "ec2:DescribeTags",
                "ec2:DescribeVolumes",
                "ec2:DescribeVpcs",
                "ec2:DetachVolume",
                "ec2:DisassociateIamInstanceProfile",
                "ec2:RebootInstances",
                "ec2:RunInstances",
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
,
        {

            "Action": [
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateSecurityGroup",
                "ec2:DeleteSecurityGroup",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupIngress"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
```



```
,
        {

            "Action": [
                "s3:CreateBucket",
                "s3:DeleteBucket",
                "s3:DeleteObject",
                "s3:GetObject",
                "s3:PutBucketAcl",
                "s3:PutObject",
                "s3:PutBucketTagging",
                "s3:PutObjectTagging"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:s3:::citrix*"
         }
,
        {

            "Action": [
                "ebs:StartSnapshot",
                "ebs:GetSnapshotBlock",
                "ebs:PutSnapshotBlock",
                "ebs:CompleteSnapshot",
                "ebs:ListSnapshotBlocks",
                "ebs:ListChangedBlocks",
                "ec2:CreateSnapshot"
            ],
            "Effect": "Allow",
            "Resource": "*"
         }
,
        {

            "Effect": "Allow",
            "Action": [
                 "kms:CreateGrant",
                 "kms:Decrypt",
                 "kms:DescribeKey",
                 "kms:GenerateDataKeyWithoutPlainText",
                 "kms:GenerateDataKey",
                 "kms:ReEncryptTo",
                 "kms:ReEncryptFrom"
            ],
            "Resource": "*"
         }
,
        {

            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "arn:aws:iam::*:role/*"
         }
```



```
118
119         ]
120     }
```

> 注:
>
> - SecurityGroups に関連する EC2 セクションは、カタログの作成中に準備 VM 用に分離セキュリティグループを作成する必要がある場合にのみ必要です。これが行われると、これらの権限は必要ありません。
> - EBS ボリューム暗号化を使用している場合は、KMS セクションのみが必要です。
> - iam:PassRole 権限セクションは、**role_based_auth** でのみ必要です。
> - 要件と環境に基づいて、フルアクセス権限の代わりに、特定のリソースレベルのアクセス権限を追加できます。詳しくは、AWS ドキュメントの「Demystifying EC2 Resource-Level Permissions」と「AWS リソースのアクセス管理」を参照してください。

ホスト接続の権限を検証する

MCS マシンカタログの作成と管理に関連するタスクを実行するために、ホスト接続の権限を検証できます。この実装により、VM の作成、削除、更新、VM の電源管理、EBS 暗号化などのさまざまなシナリオに必要な不足している権限を事前に見つけることができ、重要なタイミングでブロックされることを回避できます。

PowerShell コマンド`Test-HypHypervisorConnection`を使用して、ホスト接続の権限を検証できます。コマンドの結果は一覧としてキャプチャされ、一覧内の各項目は 3 つのセクションに分割されます。

- カテゴリ：ユーザーが MCS マシンカタログを作成および管理するために実行できるアクションまたはタスク。
- 修正アクション：ユーザーの不足している権限による不一致を解決するために管理者が実行する必要がある手順。
- 不足している権限：カテゴリに不足している権限の一覧。

権限を検証するには、次の手順を実行します：

1. AWS へのホスト接続を作成します。
2. Delivery Controller ホストから PowerShell ウィンドウを開きます。
3. `asnp citrix*`を実行し、Citrix 固有の PowerShell モジュールをロードします。
4. 必要な権限があるかどうか確認するために権限を検索するには、次のコマンドを実行します。

   ```
   1 Test-HypHypervisorConnection -LiteralPath "XDHyp:\Connections\
       AWSCon"
   ```

5. 権限を検索するために必要な不足している権限を追加した後、次のコマンドを実行して、次のカテゴリの権限があるかどうかを確認します：

   - 作成 更新 削除
   - 電源管理

- EBS 暗号化

```
Test-HypHypervisorConnection -LiteralPath "XDHyp:\Connections\
    AWSCon" [-SecurePassword -Password] "password" -UserName "" -
    CustomProperties ""
```

権限の追加について詳しくは、「IAM アクセス許可の設定」を参照してください。

次の手順

- 初期展開プロセスを行っている場合は、「マシンカタログの作成」を参照してください
- AWS 固有の情報については、「AWS カタログの作成」を参照してください。

追加情報

- 接続とリソース
- マシンカタログの作成

XenServer への接続

August 17, 2024

「接続とリソースの作成と管理」では接続を作成するためのウィザードについて説明しています。以下の情報は、XenServer 仮想化環境に固有の詳細について説明しています。

> 注:
>
> XenServer への接続を作成する前に、まず XenServer アカウントをリソースの場所として設定する必要があります。「XenServer 仮想化環境」を参照してください。

XenServer への接続を作成する

XenServer（旧称：Citrix Hypervisor）への接続の作成時には、VM パワー管理者以上の権限を持つアカウントの資格情報を指定する必要があります。

XenServer との通信を HTTPS で保護することをお勧めします。HTTPS を使用するには、XenServer にインストールされているデフォルトの SSL 証明書を置き換える必要があります（CTX128656を参照）。

高可用性機能で使用されるハイパーバイザーを選択することもできます（XenServer サーバーの高可用性が有効な場合）。プールマスターに障害が生じても XenServer サーバーとの通信が中断されないように、（[Edit High Availability] から）プール内のすべてのサーバーを選択することをお勧めします。

XenServer で vGPU がサポートされる場合は、GPU の種類およびグループ、または GPU パススルーを選択することができます。選択した項目で専用の GPU リソースが使用可能かどうか画面に表示されます。

1 つまたは複数の XenServer ホスト上のローカルストレージを一時データストレージとして使用する場合は、プール内の各ストレージの場所に一意の名前が付いていることを確認してください。（XenCenter で名前を変更するには、ストレージを右クリックして名前のプロパティを編集します。）

Citrix Provisioning（旧称 Provisioning Services）および Machine Creation Services（MCS）を使用して、次のものをプロビジョニングできます:

- サポートされるデスクトップまたはサーバー OS の VM のレガシー BIOS。
- サポートされるデスクトップまたはサーバー OS の VM の UEFI（セキュアブートを含む）。

> 注:
>
> MCS を構成する場合は、プールオペレーター以上の権限が必要です。

XenServer 接続での **IntelliCache** の使用

IntelliCache を使用すると、共有ストレージとローカルストレージを組み合わせて使用できるようになり、VDI 展開のコスト効率が向上します。これによってパフォーマンスが向上し、ネットワークトラフィックが減少します。この機能では、共有ストレージ上のマスターイメージがローカルストレージにキャッシュされ、共有ストレージでのデータ読み取り回数が減少します。共有デスクトップの場合、差分ディスクへの書き込みはホスト上のローカルストレージに書き込まれ、共有ストレージには書き込まれません。

- IntelliCache を使用する場合、共有ストレージは NFS である必要があります。
- パフォーマンスを向上させるため、高パフォーマンスのローカルストレージデバイスを使用することをお勧めします。

IntelliCache を使用するには、XenServer と Studio の両方でこの機能を有効にする必要があります。

- XenServer のインストール時に、［シンプロビジョニングの有効化（**Virtual Desktops** に最適化されたストレージ）］を選択します。IntelliCache が有効なサーバーと無効なサーバーを同一プールで混在させることはサポートされません。詳しくは、XenServer のドキュメントを参照してください。
- Citrix Virtual Apps and Desktops では、IntelliCache はデフォルトで無効になっています。この機能は XenServer 接続の作成時にのみ有効にでき、これを後で無効にすることはできません。XenServer 接続を追加する場合は、以下の手順に従います:
  - ストレージの種類として、［共有］を選択します。
  - ［**IntelliCache** を使用して共有ストレージデバイス上の負荷を軽減させる］チェックボックスをオンにします。

必要な **XenServer** の権限

XenServer の権限は役割ベース（RBAC）です。XenServer の役割ベースのアクセス制御（RBAC：Role Based Access Control）機能では、特定のユーザー（つまり XenServer 管理者）に役割を割り当てて、XenServer へのアクセスや実行可能な管理タスクを制御できます。この機能では、ユーザー（またはグループ）が XenServer の管理タスクの定義済みセットである「役割」にマップされ、この役割に基づいて、特定の管理タスクを実行するために必要な XenServer ホストへのアクセス許可が決定されます。

詳しくは、「役割ベースのアクセス制御」を参照してください。

役割の階層は、権限が増加する順に、読み取り専用 → VM オペレーター → VM 管理者 → VM パワー管理者 → プールオペレーター → プール管理者です。

次のセクションでは、各プロビジョニングタスクに必要な最小限の役割についてまとめます。

ホスト接続の作成

タスク	最低限必要な役割
XenServer から取得した情報を使用して、ホスト接続を追加する	読み取り専用
ユーザーと割り当てられた役割を表示する	読み取り専用

VM の電源管理

タスク	最低限必要な役割
VM の電源オン/オフ	VM オペレータ

VM の作成、更新、または削除

タスク	最低限必要な役割
既存のスナップショットスケジュールに VM を追加または削除する	VM パワー管理者
スナップショットスケジュールを追加、変更、削除する	プールオペレータ
マスターイメージを公開する	プールオペレーター（スイッチポートロックが必要）
マシンカタログの作成	プールオペレーター：スイッチポートロックが必要

タスク	最低限必要な役割
VM を追加または削除する（GPU 対応 VM は除く）	VM 管理者
VM を追加または削除する（GPU 対応 VM）	プールオペレータ
仮想ディスクまたは CD デバイスを追加、削除、または構成する	VM 管理者
タグの管理	VM オペレータ

RBAC の役割と権限について詳しくは、「RBAC 役割と権限」を参照してください。

スイッチポートロックについて詳しくは、「スイッチポートロックの使用」を参照してください。

次の手順

- 初期展開プロセスを行っている場合は、「マシンカタログの作成」を参照してください
- XenServer 固有の情報については、「XenServer カタログの作成」を参照してください

追加情報

- 接続とリソース
- マシンカタログの作成

Google クラウド環境への接続

August 17, 2024

「接続とリソースの作成と管理」では接続を作成するためのウィザードについて説明しています。以下の情報は、Google クラウド環境に固有の詳細について説明しています。

> 注:
>
> Google クラウド環境への接続を作成する前に、まず Google クラウドアカウントをリソースの場所として設定する必要があります。「Google Cloud 環境」を参照してください。

接続の追加

「接続とリソースの作成」の手順に従います。次の説明は、ホスト接続を設定する手順を示しています:

1. ［管理］**>**［構成］の左側のペインで ［ホスト］を選択します。
2. 操作バーの ［接続およびリソースの追加］を選択します。
3. ［接続］ページで、［新しい接続を作成する］と ［**Citrix** プロビジョニングツール］を選択してから ［次へ］を選択します。
   - 接続の種類。メニューから ［**Google Cloud**］を選択します。
   - 接続名。接続名を入力します。
4. ［リージョン］ページで、メニューからプロジェクト名を選択し、使用するリソースを含むリージョンを選択して、［次へ］を選択します。
5. ［ネットワーク］ページで、リソースの名前を入力し、メニューから仮想ネットワークを選択し、サブセットを選択してから ［次へ］を選択します。このリージョンとネットワークの組み合わせを識別するためのわかりやすいリソース名を指定してください。名前に *(Shared)* サフィックスが付加された仮想ネットワークは、共有 VPC を表しています。共有 VPC にサブネットレベルの IAM 役割を設定する場合、共有 VPC の特定のサブネットのみがサブネットリストに表示されます。

   > 注:
   >
   > - リソース名は 1～64 文字にし、空白スペースのみにしたり記号（`\ / ; : # . * ? = < > | [ ] { } "' ( )' )`）を含めたりすることはできません。

6. ［概要］ページで情報を確認してから、［完了］を選択し、［接続およびリソースの追加］ウィンドウを終了します。

接続とリソースを作成すると、作成した接続とリソースが一覧表示されます。接続を構成するには、接続を選択してから、操作バーで該当するオプションを選択します。

同様に、接続の下で作成されたリソースを削除、名前変更、またはテストすることができます。これを行うには、接続の下のリソースを選択してから、操作バーで該当するオプションを選択します。

サービスエンドポイント **URL**

次の URL にアクセスできる必要があります:

- https://oauth2.googleapis.com
- https://cloudresourcemanager.googleapis.com
- https://compute.googleapis.com
- https://storage.googleapis.com
- https://cloudbuild.googleapis.com

Google Cloud プロジェクト

基本的に、Google Cloud プロジェクトには次の 2 種類があります:

- プロビジョニングプロジェクト: この場合、現在の管理者アカウントは、プロジェクトでプロビジョニングされたマシンを所有しています。このプロジェクトは、ローカルプロジェクトとも呼ばれます。
- 共有 VPC プロジェクト: プロビジョニングプロジェクトで作成されたマシンが、共有 VPC プロジェクトの VPC を使用するプロジェクト。プロジェクトのプロビジョニングに使用される管理者アカウントには、このプロジェクトでの権限が制限されています。具体的には、VPC を使用する権限のみです。

GCP 管理トラフィックのための安全な環境の作成

自身の Google Cloud プロジェクトには、プライベート Google アクセスを許可できます。この実装により、機密データを処理するためのセキュリティが強化されます。これを実現するために、次のいずれかを実行できます:

- Cloud Build サービスアカウントに VPC サービスコントロールの次の Ingress ルールを含めます。この手順を実行する場合は、GCP 管理トラフィック用の安全な環境を作成するための以下の手順には従わないでください。

```
Ingress Rule 1
From:
Identities:
<ProjectID>@cloudbuild.gserviceaccount.com
Source > All sources allowed
To:
Projects =
All projects
Services =
Service name: All services
```

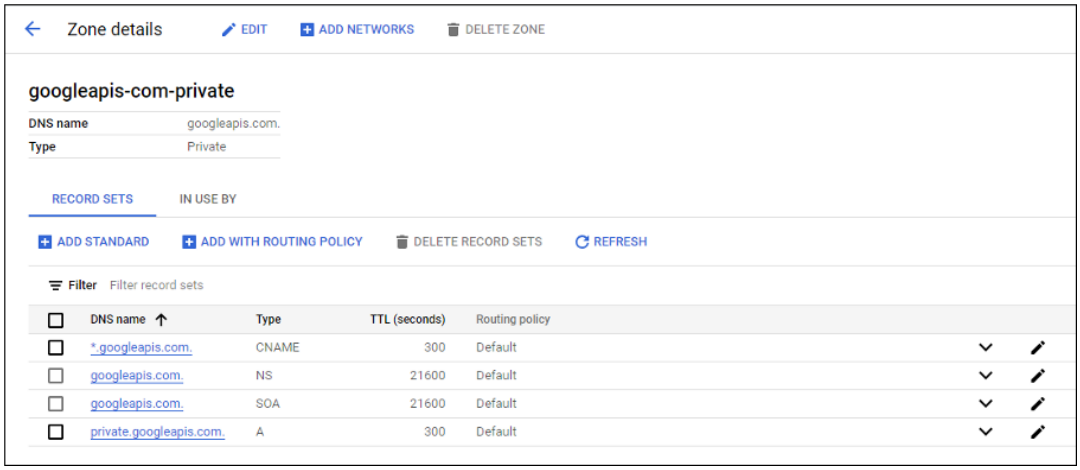
- プライベートワーカープールを使用する場合は、`CustomProperties`に`UsePrivateWorkerPool`を追加します。プライベートワーカープールについて詳しくは、「プライベートプールの概要」を参照してください。

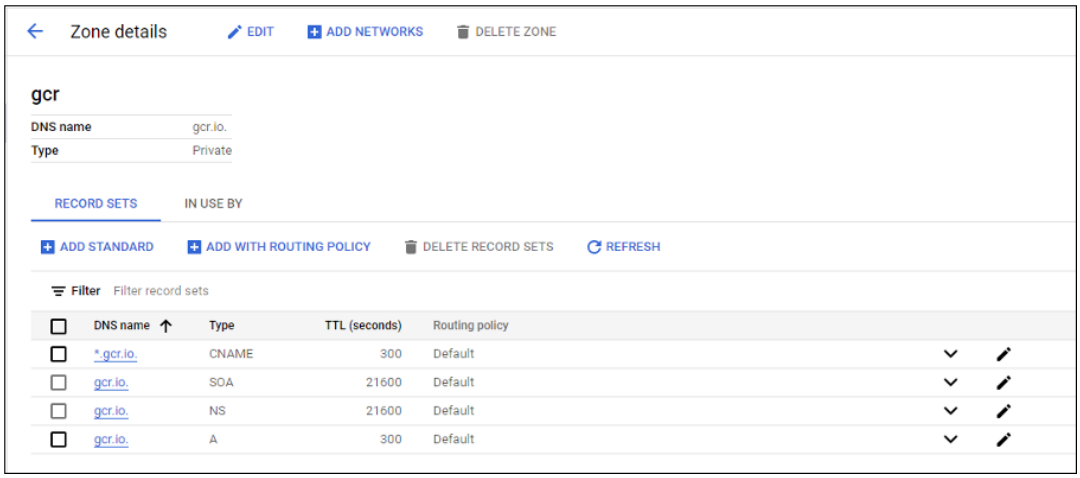
GCP 管理トラフィックのための安全な環境の作成要件

GCP 管理トラフィックのための安全な環境の作成要件は以下のとおりです。

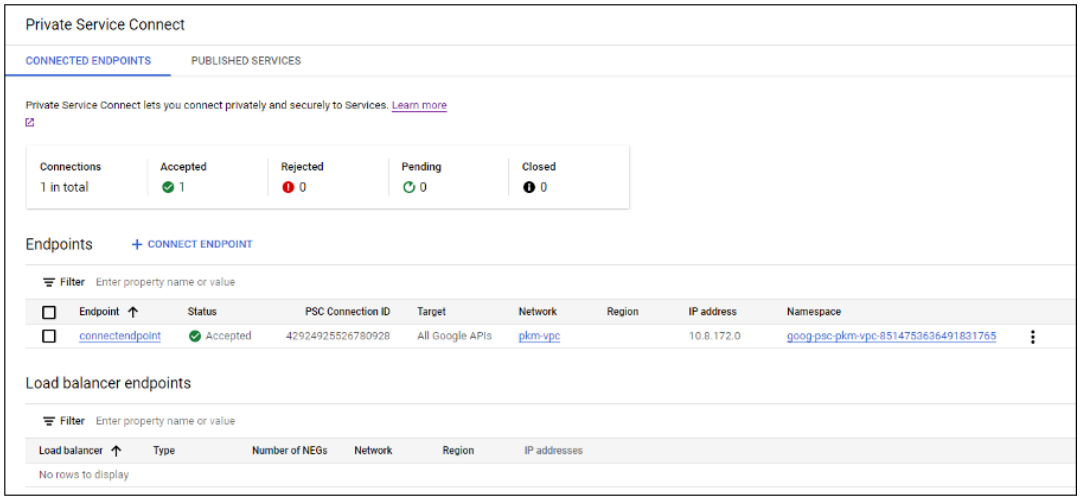
- カスタムプロパティを更新するときは、ホスト接続がメンテナンスモードであることを確認する。
- プライベートワーカープールを使用するには、以下の変更が必要です。
  - Citrix Cloud Services アカウントの場合、以下の IAM ロールを追加します。
    - Cloud Build サービスアカウント
    - コンピューティングインスタンス管理者

  - サービスアカウントユーザー
  - サービスアカウントトークン作成者
  - Cloud Build ワーカープールの所有者
- ホスト接続の作成に使用するのと同じプロジェクトに、Citrix Cloud Services のアカウントを作成します。
- 「DNS 構成」の説明に従って、**private**.googleapis.comおよびgcr.io用の DNS ゾーンを設定します。

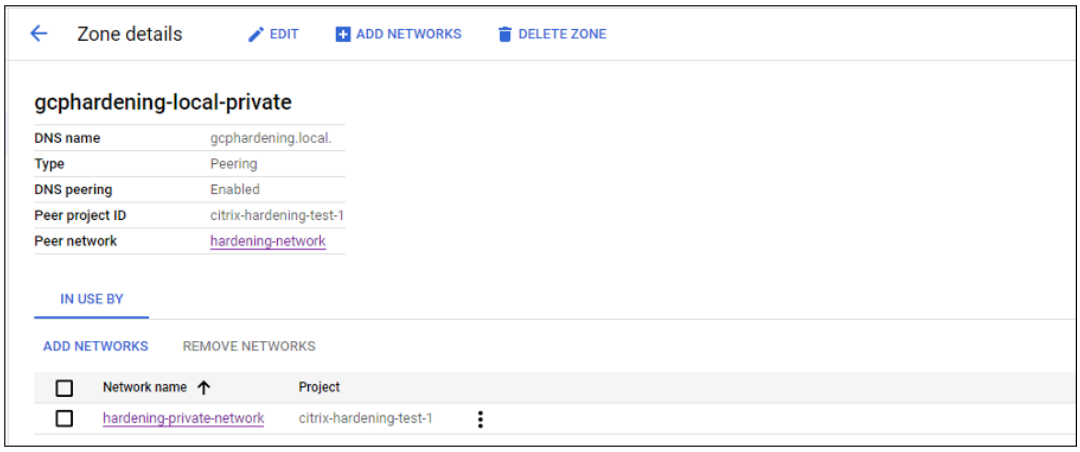




- プライベートネットワークアドレス変換 (NAT) を設定するか、プライベートサービス接続を使用します。詳しくは、「エンドポイントから Google API にアクセスする」を参照してください。



- ピアリングされた VPC を使用する場合は、ピアリングされた VPC にピアリングする Cloud DNS ゾーンを作成します。詳しくては、「ピアリングゾーンを作成する」を参照してください。



- VPC サービスの制御で、API と VM がインターネットと通信できるように送信用の規則を設定します。送信用の規則はオプションです。例:

```
Egress Rule 1
From:
Identities:ANY_IDENTITY
To:
Projects =
All projects
Service =
Service name: All services
```

プライベートワーカープールを有効にする

プライベートワーカープールを有効にするには、ホスト接続でカスタムプロパティを次のように設定します:

1. Delivery Controller ホストから PowerShell ウィンドウを開くか、Remote PowerShell SDK を使用します。Remote PowerShell SDK について詳しくは、「SDK および API」を参照してください。

2. 次のコマンドを実行します:

   a) `Add-PSSnapin citrix*`
   b) `cd XDHyp:\Connections\`
   c) `dir`

3. 接続の`CustomProperties`をメモ帳にコピーします。
4. プロパティ設定 `<Property xsi:type="StringProperty"Name="UsePrivateWorkerPool "Value="True"/>`を追加します。例:

```
```
<CustomProperties xmlns:xsi="http://www.w3.org/2001/XMLSchema-
    instance" xmlns="http://schemas.citrix.com/2014/xd/
    machinecreation">
<Property xsi:type="StringProperty" Name="UsePrivateWorkerPool"
    Value="True"/>
</CustomProperties>
```
```

5. PowerShell ウィンドウで、変更したカスタムプロパティに変数を割り当てます。例: `$customProperty = '<CustomProperties…</CustomProperties>'`。
6. `$gcpServiceAccount = "<ENTER YOUR SERVICE ACCOUNT EMAIL HERE>"`を 実行します。
7. `$gcpPrivateKey = "<ENTER YOUR SERVICE ACCOUNT PRIVATE KEY HERE AFTER REMOVING ALL INSTANCES OF \n >"`を実行します。
8. `$securePassword = ConvertTo-SecureString $gcpPrivateKey -AsPlainText -Force`を実行します。
9. 以下を実行して、既存のホスト接続を更新します:

```
Set-Item -PassThru -Path @('XDHyp:\Connections\<ENTER YOUR
    CONNECTION NAME HERE>') -SecurePassword $securePassword -
    UserName $gcpServiceAccount -CustomProperties $customProperty
```

必要な **GCP** の権限

このセクションでは、GCP の権限の完全な一覧が示されています。機能を正しく動作させるには、このセクションで示した権限の完全なセットを使用します。

> 注:
>
> 2024 年 4 月 29 日、GCP は Cloud Build サービスのデフォルトの動作とサービスアカウントの使用に関する変更を導入します。詳しくは、「Cloud Build サービスアカウントの変更」を参照してください。2024 年 4 月 29 日より前に Cloud Build API が有効になっていた既存の Google プロジェクトは、この変更の影響を受け

> ません。ただし、4 月 29 日以降も既存の Cloud Build サービスの動作を維持する場合は、API を有効にする前に、制約の適用を無効にする組織ポリシーを作成または適用できます。新しい組織ポリシーを設定する場合でも、このセクションの既存の権限と、「**Cloud Build** サービスアカウントの変更前」と記載されている項目に従うことができます。そうでない場合は、「**Cloud Build** サービスアカウントの変更後」と記載されている既存の権限と項目に従います。

ホスト接続の作成

- プロビジョニングプロジェクトにおいて Citrix Cloud サービスアカウントに必要な最低限の権限:

```
compute.instanceTemplates.list
compute.instances.list
compute.networks.list
compute.projects.get
compute.regions.list
compute.subnetworks.list
compute.zones.list
resourcemanager.projects.get
```

  次の Google 定義の役割には、上に一覧表示された権限があります:

  - コンピューティング管理者
  - クラウドデータストアユーザー

- 共有 VPC プロジェクトにおいて Citrix Cloud サービスアカウントの共有 VPC に必要な追加の権限:

```
compute.networks.list
compute.subnetworks.list
resourcemanager.projects.get
```

  次の Google 定義の役割には、上に一覧表示された権限があります:

  - コンピューティングネットワークユーザー

VM の電源管理

プロビジョニングプロジェクトにおいて Citrix Cloud サービスアカウントに必要な最低限の権限（電源管理のみのカタログの場合）:

```
compute.instanceTemplates.list
compute.instances.list
compute.instances.get
compute.instances.reset
compute.instances.resume
compute.instances.start
compute.instances.stop
compute.instances.suspend
compute.networks.list
```



```
compute.projects.get
compute.regions.list
compute.subnetworks.list
compute.zones.list
resourcemanager.projects.get
compute.zoneOperations.get
```

次の Google 定義の役割には、上に一覧表示された権限があります:

- コンピューティング管理者
- クラウドデータストアユーザー

VM の作成、更新、または削除

- プロビジョニングプロジェクトにおいて Citrix Cloud サービスアカウントに必要な最低限の権限:

```
cloudbuild.builds.create
cloudbuild.builds.get
cloudbuild.builds.list
compute.acceleratorTypes.list
compute.diskTypes.get
compute.diskTypes.list
compute.disks.create
compute.disks.createSnapshot
compute.disks.delete
compute.disks.get
compute.disks.list
compute.disks.setLabels
compute.disks.use
compute.disks.useReadOnly
compute.firewalls.create
compute.firewalls.delete
compute.firewalls.list
compute.globalOperations.get
compute.images.create
compute.images.delete
compute.images.get
compute.images.list
compute.images.setLabels
compute.images.useReadOnly
compute.instanceTemplates.create
compute.instanceTemplates.delete
compute.instanceTemplates.get
compute.instanceTemplates.list
compute.instanceTemplates.useReadOnly
compute.instances.attachDisk
compute.instances.create
compute.instances.delete
compute.instances.detachDisk
compute.instances.get
compute.instances.list
```



```
compute.instances.reset
compute.instances.resume
compute.instances.setDeletionProtection
compute.instances.setLabels
compute.instances.setMetadata
compute.instances.setServiceAccount
compute.instances.setTags
compute.instances.start
compute.instances.stop
compute.instances.suspend
compute.machineTypes.get
compute.machineTypes.list
compute.networks.list
compute.networks.updatePolicy
compute.nodeGroups.list
compute.nodeTemplates.get
compute.projects.get
compute.regions.list
compute.snapshots.create
compute.snapshots.delete
compute.snapshots.list
compute.snapshots.get
compute.snapshots.setLabels
compute.snapshots.useReadOnly
compute.subnetworks.get
compute.subnetworks.list
compute.subnetworks.use
compute.zoneOperations.get
compute.zoneOperations.list
compute.zones.get
compute.zones.list
iam.serviceAccounts.actAs
resourcemanager.projects.get
storage.buckets.create
storage.buckets.delete
storage.buckets.get
storage.buckets.list
storage.buckets.update
storage.objects.create
storage.objects.delete
storage.objects.get
storage.objects.list
compute.networks.get
compute.resourcePolicies.use
```

次の Google 定義の役割には、上に一覧表示された権限があります:

- コンピューティング管理者
- ストレージ管理者
- Cloud Build エディター
- サービスアカウントユーザー
- クラウドデータストアユーザー

- 共有 VPC プロジェクトから VPC およびサブネットワークを使用してホスティングユニットを作成するために、共有 VPC プロジェクトにおいて Citrix Cloud サービスアカウントの共有 VPC で必要な追加の権限:

```
compute.firewalls.list
compute.networks.list
compute.projects.get
compute.regions.list
compute.subnetworks.get
compute.subnetworks.list
compute.subnetworks.use
compute.zones.list
resourcemanager.projects.get
```

  次の Google 定義の役割には、上に一覧表示された権限があります:

  - コンピューティングネットワークユーザー
  - クラウドデータストアユーザー

- (Cloud Build サービスアカウントの変更前): 準備の指示ディスクを MCS にダウンロードするときに、プロビジョニングプロジェクトにおいて Cloud Build サービスアカウントで Google Cloud Build サービスが必要とする最低限の権限:

- (Cloud Build サービスアカウントの変更後): 準備の指示ディスクを MCS にダウンロードするときに、プロビジョニングプロジェクトにおいて Cloud Compute サービスアカウントで Google Cloud Compute サービスが必要とする最低限の権限:

```
compute.disks.create
compute.disks.delete
compute.disks.get
compute.disks.list
compute.disks.setLabels
compute.disks.use
compute.disks.useReadOnly
compute.images.get
compute.images.list
compute.images.useReadOnly
compute.instances.create
compute.instances.delete
compute.instances.get
compute.instances.getSerialPortOutput
compute.instances.list
compute.instances.setLabels
compute.instances.setMetadata
compute.instances.setServiceAccount
compute.machineTypes.list
compute.networks.get
compute.networks.list
compute.projects.get
compute.subnetworks.list
compute.subnetworks.use
compute.subnetworks.useExternalIp
compute.zoneOperations.get
```



```
compute.zones.list
iam.serviceAccounts.actAs
logging.logEntries.create
pubsub.topics.publish
resourcemanager.projects.get
source.repos.get
source.repos.list
storage.buckets.create
storage.buckets.get
storage.buckets.list
storage.objects.create
storage.objects.delete
storage.objects.get
storage.objects.list
```

次の Google 定義の役割には、上に一覧表示された権限があります:

- Cloud Build サービスアカウント（Cloud Build サービスアカウントの変更後は、Cloud Compute サービスアカウントになります）
- コンピューティングインスタンス管理者
- サービスアカウントユーザー

- 準備の指示ディスクを MCS にダウンロードするときに、プロビジョニングプロジェクトにおいて Cloud Compute サービスアカウントで Google Cloud Build サービスが必要とする最低限の権限:

```
resourcemanager.projects.get
storage.objects.create
storage.objects.get
storage.objects.list
```

次の Google 定義の役割には、上に一覧表示された権限があります:

- コンピューティングネットワークユーザー
- ストレージアカウントユーザー
- クラウドデータストアユーザー

- (Cloud Build サービスアカウントの変更前): 準備の指示ディスクを MCS にダウンロードするときに、プロビジョニングプロジェクトにおいて Cloud Build サービスアカウントの共有 VPC で Google Cloud Build サービスが必要とする追加の権限:

- (Cloud Build サービスアカウントの変更後): 準備の指示ディスクを MCS にダウンロードするときに、プロビジョニングプロジェクトにおいて Cloud Compute サービスアカウントの共有 VPC で Google Cloud Compute サービスが必要とする追加の権限:

```
compute.firewalls.list
compute.networks.list
compute.subnetworks.list
compute.subnetworks.use
resourcemanager.projects.get
```


次の Google 定義の役割には、上に一覧表示された権限があります：

- コンピューティングネットワークユーザー
- ストレージアカウントユーザー
- クラウドデータストアユーザー

- プロビジョニングプロジェクトにおいて Citrix Cloud サービスアカウントのクラウドキー管理サービス（KMS）に必要な追加の権限：

```
cloudkms.cryptoKeys.get
cloudkms.cryptoKeys.list
cloudkms.keyRings.get
cloudkms.keyRings.list
```

次の Google 定義の役割には、上に一覧表示された権限があります：

- コンピューティング KMS 閲覧者

一般的な権限

以下はプロビジョニングプロジェクトで MCS がサポートするすべての機能に対する Citrix Cloud サービスアカウントの権限です。これらの権限では、今後も必要な互換性を提供する予定です。

```
resourcemanager.projects.get
cloudbuild.builds.create
cloudbuild.builds.get
cloudbuild.builds.list
compute.acceleratorTypes.list
compute.diskTypes.get
compute.diskTypes.list
compute.disks.create
compute.disks.createSnapshot
compute.disks.delete
compute.disks.get
compute.disks.setLabels
compute.disks.use
compute.disks.useReadOnly
compute.firewalls.create
compute.firewalls.delete
compute.firewalls.list
compute.globalOperations.get
compute.images.create
compute.images.delete
compute.images.get
compute.images.list
compute.images.setLabels
compute.images.useReadOnly
compute.instanceTemplates.create
compute.instanceTemplates.delete
compute.instanceTemplates.get
```



```
compute.instanceTemplates.list
compute.instanceTemplates.useReadOnly
compute.instances.attachDisk
compute.instances.create
compute.instances.delete
compute.instances.detachDisk
compute.instances.get
compute.instances.list
compute.instances.reset
compute.instances.resume
compute.instances.setDeletionProtection
compute.instances.setLabels
compute.instances.setMetadata
compute.instances.setTags
compute.instances.start
compute.instances.stop
compute.instances.suspend
compute.instances.update
compute.instances.updateAccessConfig
compute.instances.updateDisplayDevice
compute.instances.updateSecurity
compute.instances.updateShieldedInstanceConfig
compute.instances.updateShieldedVmConfig
compute.machineTypes.get
compute.machineTypes.list
compute.networks.list
compute.networks.updatePolicy
compute.nodeGroups.list
compute.nodeTemplates.get
compute.projects.get
compute.regions.list
compute.snapshots.create
compute.snapshots.delete
compute.snapshots.list
compute.snapshots.get
compute.snapshots.setLabels
compute.snapshots.useReadOnly
compute.subnetworks.get
compute.subnetworks.list
compute.subnetworks.use
compute.subnetworks.useExternalIp
compute.zoneOperations.get
compute.zoneOperations.list
compute.zones.get
compute.zones.list
resourcemanager.projects.get
storage.buckets.create
storage.buckets.delete
storage.buckets.get
storage.buckets.list
storage.buckets.update
storage.objects.create
storage.objects.delete
```



```
storage.objects.get
storage.objects.list
cloudkms.cryptoKeys.get
cloudkms.cryptoKeys.list
cloudkms.keyRings.get
cloudkms.keyRings.list
compute.disks.list
compute.instances.setServiceAccount
compute.networks.get
compute.networks.use
compute.networks.useExternalIp
iam.serviceAccounts.actAs
compute.resourcePolicies.use
```

次の手順

- 初期展開プロセスを行っている場合は、「マシンカタログの作成」を参照してください
- Google Cloud Platform（GCP）固有の情報については、「Google Cloud Platform カタログの作成」を参照してください。

追加情報

- 接続とリソース
- マシンカタログの作成

HPE Moonshot への接続

August 17, 2024

「接続とリソースの作成と管理」では接続を作成するためのウィザードについて説明しています。以下の情報は、HPE Moonshot に固有の詳細について説明しています。

> 注:
>
> HPE Moonshot への接続を作成する前に、まず HPE アカウントの設定を完了する必要があります。「HPE Moonshot 仮想化環境」を参照してください。

接続の作成

以下を使用して、HPE Moonshot への接続を作成できます:

- Web Studio
- PowerShell コマンド

Web Studio で接続を作成する

1. ［接続およびリソースの追加］ページで、接続の種類として ［**HPE Moonshot**］を選択します。
2. Moonshot iLO Chassis Manager の接続アドレスを入力します。アドレスには、IP アドレス、ホスト名、または FQDN を使用できます。
3. シャーシの管理資格情報とわかりやすい接続名を入力します。

次のいずれかの状況が発生すると、接続のセットアップは停止します:

- Citrix Virtual Apps and Desktops がエラーのあるパブリック CA 署名証明書を受信した場合: エラーメッセージが表示されます。画面上の指示に従って問題を解決してください。解決しない限り、接続の作成を続行できません。
- Citrix Virtual Apps and Desktops は、プライベート CA 署名証明書を受け取ります。警告ページが表示されます。受信した拇印をサーバーの拇印と比較して、証明書の有効性を確認します。有効な場合は、［証明書を信頼する］を選択し、［**OK**］をクリックして接続の作成を続行します。その後、Citrix Virtual Apps and Desktops は証明書を信頼し、今後の検証のために拇印を保存します。

PowerShell コマンドを使用して接続を作成する

PowerShell コマンドを使用して接続を作成する場合は、次の情報を指定します:

- IP: HPE サーバーの IP アドレス
- ユーザー名: HPE ユーザー名
- パスワード: HPE パスワード

例:

```
New-Item -ConnectionType "Custom" -HypervisorAddress $IP -Metadata @{
 "Citrix_Orchestration_Hypervisor_Secret_Allow_Edit"="false" }
  -Path @("XDHyp:\Connections$connectionName") -Persist -PluginId "
     HPMoonshotFactory" -Scope @() -SecurePassword $Password -UserName
     $UserName -sslthumbprint $SslThumbprint New-
     BrokerHypervisorConnection -HypHypervisorConnectionUid
     $HypervisorConnectionID
```

> 注:
>
> `sslthumbprint`パラメーターは、プライベート CA 署名証明書の場合にのみ必須です。

証明書と拇印の検証

HPE Moonshot への接続を正常に作成するには、証明書にエラーがなく、拇印に正しい値が含まれている必要があります。証明書と拇印の検証に関連するユースケースは次のとおりです:

- パブリック CA 署名証明書にエラーがあります。接続が正常に作成されません。エラーの詳細を確認して問題を解決してください。
- パブリック CA 署名証明書にエラーがありません。接続は正常に作成され、SslThumbprintsの値は **Null** です。
- プライベート CA 署名証明書にエラーがなく、sslthumbprintの値がありません。接続は正しいSslThumbprintsの値で正常に作成されます。
- プライベート CA 署名証明書の拇印の値が正しくありません。接続が正常に作成されません。
- プライベート CA 署名証明書にエラーがありません。接続は正常に作成されます。接続を作成するとき、SSlThumbprintsは **Null** です。SSlThumbprintsの値は、サイトサービスによる値に更新されます。

接続の管理

このセクションでは、接続を管理する方法について詳しく説明します:

- Web Studio を使用して証明書の問題を解決する
- PowerShell コマンドを使用して拇印の値を更新する

証明書の問題を修正する

Citrix Virtual Apps and Desktops は、証明書の問題が発生すると HPE Moonshot 接続をブロックし、ユーザーは関連する HPE Moonshot ノードでワークロードを配信および管理できなくなります。［ホスト接続］リストの接続の横にエラーアイコンが表示されます。特定の問題と解決策については、次の表を参照してください。

問題	解決策
パブリック CA 署名証明書で証明書エラーが発生する 受信した証明書はプライベート CA 署名証明書であるものの、有効期限が切れている。	接続をクリックし、［トラブルシューティング］タブを選択します。エラーの詳細を表示し、問題を解決します。ホスト接続を編集して証明書の拇印を更新します。詳細な手順: 1. 接続を選択し、［接続の編集］をクリックします。 1. ［接続のプロパティ］ページで、［設定の編集］をクリックします。 1. HPE Moonshot シャーシに接続するためのパスワードを入力し、［保存］をクリックします。 1. 表示される ［警告］ページで、受信した拇印とサーバーの拇印を比較して証明書の有効性を確認します。

問題	解決策
	1. それらが同じ場合は、[証明書を信頼する] を選択し、[**OK**] をクリックします。

拇印の値を更新する

接続を作成した後、`Set-Item` PowerShell コマンドを使用して接続の拇印の値を更新できます。たとえば、次のコマンドを実行します:

1. 接続の詳細を取得します。例:

```
Get-Item -LiteralPath xdhyp:\connections\SinMoonshot-101
```

2. 拇印の値を更新します。例:

```
Set-Item -LiteralPath xdhyp:\connections\SinMoonshot-101 -Username
    Administrator -SslThumbprint
   xxxxxxxxxxx12AD048480631BB7AB10D69xxxxx
```

3. 更新された拇印の値を確認します。例:

```
Get-Item -LiteralPath xdhyp:\connections\SinMoonshot-101
```

> 注:
>
> 正しくない拇印の値を`Set-Item`コマンドで指定すると、更新は失敗します。

次の手順

- 初期展開プロセスを行っている場合は、「マシンカタログの作成」を参照してください
- AWS 固有の情報については、「HPE Moonshot マシンカタログの作成」を参照してください

追加情報

- 接続とリソース
- マシンカタログの作成

Microsoft Azure への接続

August 17, 2024

> 注:
>
> 2023 年 7 月より、Microsoft は Azure Active Directory（Azure AD）の名前を Microsoft Entra ID に変更しました。このドキュメントでは、Azure Active Directory、Azure AD、または AAD への言及はすべて、Microsoft Entra ID を意味することになります。

「接続とリソースの作成と管理」では接続を作成するためのウィザードについて説明しています。以下の情報は、Azure Resource Manager クラウド環境に固有の詳細について説明しています。

> 注:
>
> Microsoft Azure への接続を作成する前に、Azure アカウントをリソースの場所として設定する必要があります。「Microsoft Azure Resource Manager クラウド環境」を参照してください。

サービスプリンシパルと接続の作成

接続を作成する前に、接続で Azure リソースへのアクセスに使用されるサービスプリンシパルを設定する必要があります。接続は次の 2 つの方法で作成できます。

- Web Studio を使用したサービスプリンシパルと接続の作成
- 以前に作成したサービスプリンシパルを使用した接続の作成

このセクションでは、次のタスクを完了する方法を説明します。

- Web Studio を使用したサービス プリンシパルと接続の作成
- PowerShell を使用したサービスプリンシパルの作成
- Azure でのアプリケーションシークレットの取得
- 既存のサービスプリンシパルを使用した接続の作成

注意事項

- Contributor（投稿者）の役割でサービスプリンシパルを使用することを Citrix ではお勧めします。ただし、最低限の権限の一覧を取得する方法については、「最低限の権限」セクションを参照してください。
- 最初の接続を作成するときに、必要な権限付与を求めるプロンプトが Azure で表示されます。その後の接続でも認証は必要ですが、Azure では以前の同意が記憶され、このプロンプトは再表示されません。
- 認証に使用されるアカウントは、サブスクリプションの共同管理者である必要があります。
- 認証に使用されるアカウントは、サブスクリプションのディレクトリのメンバーである必要があります。注意すべき 2 つのタイプのアカウントがあります。「職場または学校」と「個人用 Microsoft アカウント」です。詳しくは、CTX219211を参照してください。
- 既存の Microsoft アカウントは、サブスクリプションのディレクトリのメンバーとして追加することで使用できますが、ユーザーが以前にそのディレクトリのリソースのいずれかへのゲストアクセスを許可されていた

場合は、複雑になる可能性があります。この場合、必要な権限を与えないディレクトリにプレースホルダーエントリが存在し、エラーが返されることがあります。

ディレクトリからリソースを削除してこれを修正し、明示的に追加し直します。ただし、そのアカウントがアクセスできる他のリソースに対して意図せず影響を与えるため、このオプションは注意深く実行してください。

- 特定のアカウントが実際にメンバーであるときにディレクトリゲストとして検出されるという既知の問題があります。これは、通常、古い確立済みのディレクトリアカウントで発生します。回避策：アカウントをディレクトリに追加します。これにより適切なメンバーシップ値が取得されます。
- リソースグループはリソースのコンテナにすぎず、そのリージョン以外のリージョンのリソースを含む場合があります。これが原因で、リソースグループのリージョンに表示されているリソースを利用できると期待した場合に、混乱を招く可能性があります。
- ネットワークとサブネットが、必要な数のマシンをホストするのに十分な大きさであることを確認してください。これには多少先見の明が必要ですが、Microsoft が、アドレススペースの容量に関するガイダンスを示して、適切な値を指定できるようサポートします。

Web Studio を使用したサービス プリンシパルと接続の作成

> 重要：
>
> この機能は、Azure China のサブスクリプションではまだ利用できません。

Web Studio を使用すると、サービスプリンシパルと接続の両方を 1 つのワークフローで作成できます。サービスプリンシパルにより、接続で Azure リソースにアクセスできるようになります。Azure に認証してサービスプリンシパルを作成すると、Azure にアプリケーションが登録されます。登録されたアプリケーションの秘密キー（クライアントシークレットまたはアプリケーションシークレットと呼ばれる）が作成されます。登録されたアプリケーション（この場合は接続）は、クライアントシークレットを使用して Azure AD に認証します。

手順を開始する前に、次の前提条件を満たしていることを確認してください。

- サブスクリプションの Azure Active Directory テナントにユーザーアカウントがあること。
- Azure AD のユーザーアカウントが、リソースのプロビジョニングに使用する Azure サブスクリプションの共同管理者でもあること。
- 認証のグローバル管理者、アプリケーション管理者、またはアプリケーション開発者の権限があること。これらの権限は、ホスト接続の作成後に失効する可能性があります。役割について詳しくは、「Azure AD の組み込みロール」を参照してください。

接続およびリソースの追加ウィザードを使用して、サービスプリンシパルと接続を同時に作成します。

1. ［接続］ページで ［新しい接続を作成する］を選択します。次に、接続の種類として ［**Microsoft Azure**］を選択し、Azure 環境を選択します。
2. 仮想マシンの作成にどのツールを使用するかを選択し、［次へ］を選択します。

3. ［接続の詳細］ページで、Azure サブスクリプション ID と接続の名前を入力します。サブスクリプション ID を入力すると、［新規作成］ボタンが有効になります。

   > 注:
   >
   > 接続名は 1〜64 文字にし、空白スペースのみにしたり記号（`\/;:#.*?=<>|[]{ } "'()'`）を含めたりすることはできません。

4. ［新規作成］を選択してから、Azure Active Directory アカウントのユーザー名とパスワードを入力します。
5. ［サインイン］を選択します。
6. ［承認］を選択して、表示された権限を Citrix Virtual Apps and Desktops に付与します。Citrix Virtual Apps and Desktops によって、指定されたユーザーの代わりに Azure リソースを管理することを許可するサービスプリンシパルが作成されます。
7. ［承認］を選択すると、ウィザードの ［接続］ページに戻ります。

   > 注:
   >
   > Azure への認証に成功すると、［新規作成］ボタンと ［既存を使用］ボタンが表示されなくなります。緑色のチェックマークが付いた「接続に成功しました」というテキストが表示され、これは Azure サブスクリプションへの接続に成功したことを示します。

8. ［接続の詳細］ページで、［次へ］を選択します。

   > 注:
   >
   > Azure への認証が完了し、必要な権限の付与に同意しない限り、次のページに進むことはできません。

9. 接続用のリソースを構成します。リソースには領域とネットワークが含まれます。

   - ［リージョン］ページで領域を選択します。
   - ［ネットワーク］ページで、次の手順を実行します:
     - 1〜64 文字のリソース名を入力して、リージョンとネットワークの組み合わせを特定できるようにします。リソース名は、空白のみにしたり記号（`\/;:#.*?=<>|[]{ } "'()'`）を含めたりすることはできません。
     - 仮想ネットワークとリソースグループのペアを選択します。（複数の仮想ネットワークを同じ名前にする場合、ネットワーク名とリソースグループをペアリングすると一意の組み合わせになります。）前のページで選択したリージョンに仮想ネットワークがない場合は、前のページに戻って仮想ネットワークのあるリージョンを選択します。

10. ［概要］ページで、設定の概要を表示し、［完了］を選択してセットアップを完了します。

アプリケーション **ID** の表示　接続を作成した後、その接続で Azure リソースへのアクセスに使用されるアプリケーション ID を表示できます。

［接続およびリソースの追加］一覧で、接続を選択して詳細を表示します。［詳細］タブで、アプリケーション ID が表示されます。

PowerShell を使用したサービスプリンシパルの作成

PowerShell を使用してサービスプリンシパルを作成するには、Azure Resource Manager サブスクリプションに接続して、後述の PowerShell コマンドレットを使用します。

以下のアイテムを必ず準備してください。

- **SubscriptionId**: VDA をプロビジョニングするサブスクリプションの Azure Resource Manager SubscriptionID。
- **ActiveDirectoryID**: Azure AD に登録したアプリケーションのテナント ID。
- **ApplicationName**: Azure AD 内で作成されるアプリケーションの名前。

詳細な手順は次のとおりです:

Azure Resource Manager サブスクリプションに接続します。

```
`Connect-AzAccount`
```

1. サービスプリンシパルを作成する Azure Resource Manager サブスクリプションを選択します。

   ```
   Get-AzSubscription -SubscriptionId $subscriptionId | Select-
   AzSubscription
   ```

2. AD テナントでアプリケーションを作成します。

   ```
   $AzureADApplication = New-AzADApplication -DisplayName $ApplicationName
   ```

3. サービスプリンシパルを作成します。

   ```
   New-AzADServicePrincipal -ApplicationId $AzureADApplication.AppId
   ```

4. サービスプリンシパルに役割を割り当てます。

   ```
   New-AzRoleAssignment -RoleDefinitionName Contributor -ServicePrincipalName
    $AzureADApplication.AppId -scope /subscriptions/$SubscriptionId
   ```

5. PowerShell コンソールの出力ウィンドウから、ApplicationId をメモします。この ID は、ホスト接続を作成するときに使用します。

Azure でのアプリケーションシークレットの取得

既存のサービスプリンシパルを使用して接続を作成するには、まず Azure Portal でサービスプリンシパルのアプリケーション ID とシークレットを取得する必要があります。

詳細な手順は次のとおりです:

1. Web Studio から、または PowerShell を使用してアプリケーション **ID** を取得します。
2. Azure Portal にサインインします。
3. Azure で ［**Azure Active Directory**］を選択します。
4. Azure AD の ［**App registrations**］でアプリケーションを選択します。
5. ［**Certificates & secrets**］に移動します。
6. ［**Client secrets**］をクリックします。

既存のサービスプリンシパルを使用した接続の作成

サービスプリンシパルが既にある場合は、そのサービスプリンシパルと Web Studio を使用して接続を作成できます。

以下のアイテムを必ず準備してください。

- サブスクリプション ID
- Active Directory ID（テナント ID）
- アプリケーション ID
- アプリケーションシークレット

  詳しくは、「アプリケーションシークレットの取得」を参照してください。
- シークレットの有効期限

詳細な手順は次のとおりです:

接続およびリソースの追加ウィザードで以下を行います:

1. ［接続］ページで ［新しい接続を作成する］を選択します。次に、接続の種類として ［**Microsoft Azure**］を選択し、Azure 環境を選択します。
2. 仮想マシンの作成にどのツールを使用するかを選択し、［次へ］を選択します。
3. ［接続の詳細］ページで、Azure サブスクリプション ID と接続の名前を入力します。

   > 注:
   >
   > 接続名は 1〜64 文字にし、空白スペースのみにしたり記号（`\/;:#.*?=<>|[]{ } "'()'`）を含めたりすることはできません。

4. ［既存を使用］を選択します。［既存のサービスプリンシパルの詳細］ウィンドウで、既存のサービスプリンシパルに次の設定を入力します。詳細を入力すると、［保存］ボタンが有効になります。［**Save**］を選択します。有効な詳細を入力しない限り、このページの先には進めません。

   - サブスクリプション **ID**。Azure サブスクリプション ID を入力します。サブスクリプション ID を取得するには、Azure Portal にサインインし、［**Subscriptions**］**>** ［**Overview**］に移動します。

- **Active Directory ID**（テナント ID）。Azure AD に登録したアプリケーションのディレクトリ（テナント）ID を入力します。
- アプリケーション **ID**。Azure AD に登録したアプリケーションのアプリケーション（クライアント）ID を入力します。
- アプリケーションシークレット。秘密キー（クライアントシークレット）を作成します。登録されたアプリケーションは、キーを使用して Azure AD への認証を行います。セキュリティのために、キーを定期的に変更することをお勧めします。後でキーを取得することはできないため、必ずキーを保存してください。
- シークレットの有効期限。アプリケーションシークレットの有効期限が切れる日付を入力します。シークレットキーの有効期限が切れる前に、コンソールに通知が表示されます。ただし、秘密キーの有効期限が切れると、エラーが発生します。

  > 注:
  >
  > セキュリティ上の理由から、有効期限は現在から 2 年を超えることはできません。

- 認証 **URL**。このフィールドは自動的に入力され、編集できません。
- 管理 **URL**。このフィールドは自動的に入力され、編集できません。
- ストレージのサフィックス。このフィールドは自動的に入力され、編集できません。

  Azure で MCS カタログを作成するには、次のエンドポイントへのアクセスが必要です。これらのエンドポイントにアクセスすると、ネットワークと Azure Portal およびそのサービスとの間の接続が最適化されます。

  - 認証 URL: https://login.microsoftonline.com/
  - 管理 URL: https://management.azure.com/。これは、Azure Resource Manager プロバイダー API の要求 URL です。管理用のエンドポイントは環境によって異なります。たとえば、Azure Global の場合はhttps://management.azure.com/、Azure US Government の場合はhttps://management.usgovcloudapi.net/です。
  - ストレージのサフィックス: https://*.core.windows.net./。ここで「*」は、ストレージ サフィックスのワイルドカード文字です。例: `https://demo.table.core.windows.net/`。

5. ［保存］を選択すると、［接続の詳細］ページに戻ります。［次へ］を選択して次のページに移動します。
6. 接続用のリソースを構成します。リソースには領域とネットワークが含まれます。

   - ［リージョン］ページで領域を選択します。
   - ［ネットワーク］ページで、次の手順を実行します:
     - 1～64 文字のリソース名を入力して、リージョンとネットワークの組み合わせを特定できるようにします。リソース名は、空白のみにしたり記号（`\/;:#.*?=<>|[]{ } "'()'`）を含めたりすることはできません。

- 仮想ネットワークとリソースグループのペアを選択します。（複数の仮想ネットワークを同じ名前にする場合、ネットワーク名とリソースグループをペアリングすると一意の組み合わせになります。）前のページで選択したリージョンに仮想ネットワークがない場合は、前のページに戻って仮想ネットワークのあるリージョンを選択します。

7. ［概要］ページで、設定の概要を表示し、［完了］を選択してセットアップを完了します。

サービスプリンシパルと接続の管理

このセクションでは、サービスプリンシパルと接続を管理する方法について説明します。

- Azure の調整設定の構成
- Azure でイメージの共有を有効にする
- ［完全な構成］を使用して共有テナントを接続に追加する
- PowerShell を使用した画像共有の実装
- アプリケーションシークレットとその有効期限の管理

Azure の調整設定の構成

Azure Resource Manager はサブスクリプションおよびテナントの要求を調整し、プロバイダーの特定のニーズに対応して定義された制限を基にルーティングします。詳しくは、Microsoft 社のサイトの「Resource Manager の要求のスロットル」を参照してください。制限は、サブスクリプションやテナントで多数のマシンの管理が問題となりうる場合に存在します。たとえば、多数のマシンを含むサブスクリプションは、電源操作に関連してパフォーマンスの問題が発生することがあります。

> ヒント：
>
> 詳しくは「Machine Creation Services による Azure のパフォーマンスの向上」を参照してください。

これらの問題の影響を軽減するために MCS 内部の調整を削除して、より高い値の Azure の要求クォータを利用することができます。

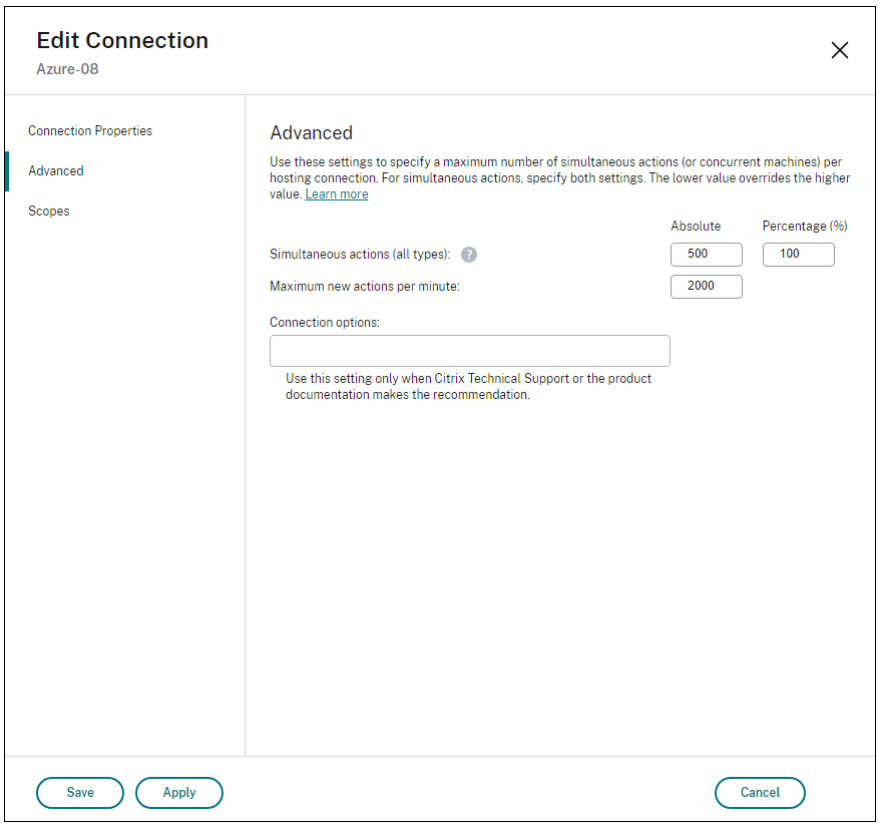
大量のサブスクリプション（1,000 台の仮想マシンを含む場合など）で仮想マシンをオンまたはオフにする場合、次の最適設定をお勧めします：

- 絶対同時操作：500
- 1 分あたりの最大新規操作：2000
- 最大同時操作：500

Web Studio を使用して指定の Azure 接続で Azure 操作を構成します：

1. Web Studio の左側ペインで ［ホスト］を選択します。
2. 接続を選択します。
3. 接続の編集ウィザードで ［詳細設定］を選択します。

4. ［詳細設定］画面で構成オプションを使用し、同時操作の数、1 分あたりの最大新規操作、その他追加の接続オプションを指定します。



MCS は、デフォルトで最大 500 の同時操作をサポートします。または、Remote PowerShell SDK を使用して、同時操作の最大数を設定することもできます。

PowerShell プロパティ`MaximumConcurrentProvisioningOperations`を使用して、同時 Azure プロビジョニング操作の最大数を指定します。このプロパティを使用するときは、次のことを考慮してください:

- `MaximumConcurrentProvisioningOperations`のデフォルト値は 500 です。
- PowerShell コマンド`Set-item`を使用して`MaximumConcurrentProvisioningOperations`パラメーターを構成します。

Azure でイメージの共有を有効にする

マシンカタログを作成または更新するときに、(Azure Compute Gallery を介して共有する) さまざまな Azure テナントおよびサブスクリプションからイメージを選択できます。テナント内またはテナント間での画像の共有を有効にするには、Azure で必要な設定を行う必要があります。

- 単一のテナント内（サブスクリプション間）でのイメージの共有
- テナント間でのイメージの共有

単一のテナント内（サブスクリプション間）でのイメージの共有　別のサブスクリプションに属する Azure Compute Gallery のイメージを選択するには、そのイメージをそのサブスクリプションのサービスプリンシパル（SPN）と共有する必要があります。

たとえば、Studio で次のように構成されているサービスプリンシパル（SPN 1）があるとします:

サービスプリンシパル: SPN 1

サブスクリプション: サブスクリプション 1

テナント: テナント 1

イメージは別のサブスクリプションにあり、Studio で次のように構成されています:

サブスクリプション: サブスクリプション 2

テナント: テナント 1

サブスクリプション 2 のイメージをサブスクリプション 1（SPN 1）と共有する場合は、サブスクリプション 2 に移動し、リソースグループを SPN 1 と共有します。

イメージは、Azure の役割ベースのアクセス制御（RBAC）を使用して別の SPN と共有する必要があります。Azure RBAC は、Azure リソースへのアクセスを管理するために使用される承認システムです。Azure RBAC について詳しくは、Microsoft 社のドキュメント「Azure ロールベースのアクセス制御（Azure RBAC）とは」を参照してください。アクセス権を付与するには、Contributor の役割を使用して、リソースグループのスコープでサービスプリンシパルに役割を割り当てます。Azure の役割を割り当てるには、ユーザーアクセス管理者や所有者などの`Microsoft.Authorization/roleAssignments/write`権限が必要です。別の SPN と画像を共有する方法について詳しくは、Microsoft 社のドキュメント「Azure portal を使用して Azure ロールを割り当てる」を参照してください。

別のサブスクリプションからイメージを選択する PowerShell コマンドについて詳しくは、「別のサブスクリプションでのイメージの選択」を参照してください。

テナント間でのイメージの共有　Azure Compute Gallery を使用してテナント間でイメージを共有するには、アプリケーション登録を作成します。

たとえば、2 つのテナント（テナント 1 とテナント 2）があり、イメージギャラリーをテナント 1 と共有する場合は、次のようにします:

1. テナント 1 のアプリケーション登録を作成します。詳しくは、「アプリの登録を作成する」を参照してください。
2. ブラウザーでサインインを要求し、テナント 2 にアプリケーションへのアクセスを許可します。`Tenant2 ID`をテナント 1 のテナント ID に置き換えます。`Application (client)ID` を、作成したアプリケーション登録のアプリケーション ID に置き換えます。置換が完了したら、この URL をブラウザーに貼り付け、サインインプロンプトに従ってテナント 2 にサインインします。例:

```
https://login.microsoftonline.com/<Tenant 2 ID>/oauth2/authorize?
    client_id=<Application (client) ID>&response_type=code&
    redirect_uri=https%3A%2F%2Fwww.microsoft.com%2F
```


詳しくは、「テナント 2 にアクセス権を付与する」を参照してください。

3. テナント 2 リソースグループへのアプリケーションアクセスを許可します。テナント 2 としてサインインし、アプリケーション登録に、ギャラリーイメージを含むリソースグループへのアクセスを許可します。詳しくは、「テナントをまたいだ認証要求」を参照してください。

PowerShell コマンドを使用して、別のテナントのイメージでカタログを作成するには、次の手順を実行します:

1. ホスト接続のカスタムプロパティの共有テナント ID の更新。
2. 別のテナントでの画像の選択。

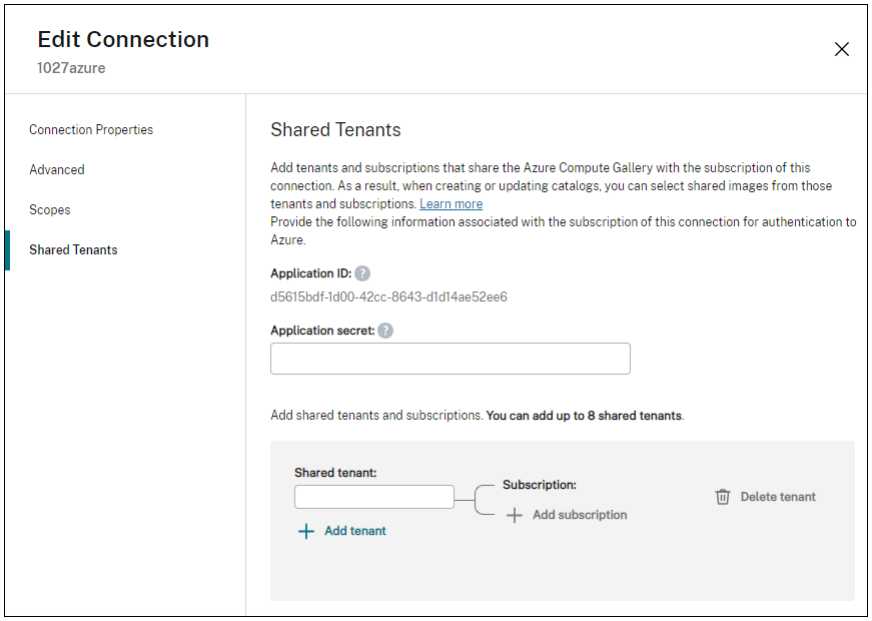
[完全な構成] を使用して共有テナントを接続に追加する

Web Studio でマシンカタログを作成または更新するときに、(Azure Compute Gallery を介して共有する) さまざまな Azure テナントおよびサブスクリプションから共有イメージを選択できます。この機能では、関連付けられたホスト接続の共有テナントおよびサブスクリプション情報を提供する必要があります。

> 注:
>
> テナント間での画像の共有を有効にするための必要な設定を Azure で構成したことを確認してください。詳しくは、「テナント間でのイメージの共有」を参照してください。

接続ごとに次の手順を実行します:

1. Web Studio の左側ペインで [ホスト] を選択します。
2. 接続を選択し、操作バーの [接続の編集] を選択します。



3. [共有テナント] で、次の操作を行います:

- 接続のサブスクリプションに関連付けられているアプリケーション ID とアプリケーションシークレットを提供します。Citrix Virtual Apps and Desktops は、この情報を使用して Azure AD に認証します。
- 接続のサブスクリプションと Azure Compute Gallery を共有しているテナントとサブスクリプションを追加します。テナントごとに最大 8 つの共有テナントと 8 つのサブスクリプションを追加できます。

4. 完了したら、[適用] を選択して行った変更を適用しウィンドウを開いたままにするか、[**OK**] を選択して変更を適用しウィンドウを閉じます。

PowerShell を使用した画像共有の実装

このセクションでは、PowerShell を使用して画像を共有するプロセスについて説明します。

- 別のサブスクリプションでの画像の選択
- ホスト接続のカスタムプロパティの共有テナント ID の更新
- 別のテナントでの画像の選択

別のサブスクリプションでの画像の選択　同じ Azure テナント内の別の共有サブスクリプションに属する Azure Compute Gallery のイメージを選択し、PowerShell コマンドを使用して MCS カタログを作成および更新できます。

1. ホスティングユニットのルートフォルダーに、sharedsubscriptionという名前の新しい共有サブスクリプションフォルダーが作成されます。
2. テナント内のすべての共有サブスクリプションを表示します。

```
Get-ChildItem -Path "XDhyp:\HostingUnits\azres\sharedsubscription.folder"
```

3. 1 つの共有サブスクリプションを選択し、その共有サブスクリプションのすべての共有リソースグループを表示します。

```
Get-ChildItem -Path "XDhyp:\HostingUnits\azres\image.folder\abc123.sharedsubscription"
```

4. リソースグループを選択し、そのリソースグループのすべてのギャラリーを表示します。

```
Get-ChildItem -Path "XDhyp:\HostingUnits\azres\image.folder\abc123.sharedsubscription\ xyz.resourcegroup"
```

5. ギャラリーを選択し、そのギャラリーのすべてのイメージ定義を表示します。

```
Get-ChildItem -Path "XDhyp:\HostingUnits\azres\image.folder\abc123.sharedsubscription\xyz.resourcegroup\testgallery.gallery"
```

6. 1 つのイメージ定義を選択し、そのイメージ定義のすべてのイメージバージョンを表示します。


```
Get-ChildItem -Path "XDhyp:\HostingUnits\azres\image.folder\abc123
    .sharedsubscription\xyz.resourcegroup\sigtestdef.
    imagedefinition"
```

7. 次の要素を使用して、MCS カタログを作成および更新します:

   - リソースグループ
   - ギャラリー
   - ギャラリーイメージの定義
   - ギャラリーイメージのバージョン

   Remote PowerShell SDK を使用してカタログを作成する方法については、https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/を参照してください。

ホスト接続のカスタムプロパティの共有テナント **ID** の更新　`Set-Item`を使用して、ホスト接続のカスタムプロパティを共有テナント ID とサブスクリプション ID で更新します。`CustomProperties`にプロパティ`SharedTenants`を追加します。`Shared Tenants`の形式は次のとおりです:

```
[{
 "Tenant":"94367291-119e-457c-bc10-25337231f7bd","Subscriptions":["7
    bb42f40-8d7f-4230-a920-be2781f6d5d9"] }
 ,{
 "Tenant":"50e83564-c4e5-4209-b43d-815c45659564","Subscriptions":["06
    ab8944-6a88-47ee-a975-43dd491a37d0"] }
 ]
```

例:

```
Set-Item -CustomProperties "<CustomProperties xmlns=`"http://schemas.
    citrix.com/2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org
    /2001/XMLSchema-instance`">
<Property xsi:type=`"StringProperty`" Name=`"SubscriptionId`" Value=`"
    123`" />
<Property xsi:type=`"StringProperty`" Name=`"ManagementEndpoint`" Value
    =`"https://management.azure.com/`" />
<Property xsi:type=`"StringProperty`" Name=`"AuthenticationAuthority`"
    Value=`"https://login.microsoftonline.com/`" />
<Property xsi:type=`"StringProperty`" Name=`"StorageSuffix`" Value=`"
    core.windows.net`" />
<Property xsi:type=`"StringProperty`" Name=`"TenantId`" Value=`"123abc`
    " />
<Property xsi:type=`"StringProperty`" Name=`"SharedTenants`" Value=`"`[
     {
  'Tenant':'123abc', 'Subscriptions':['345', '567']  }
  ]`"` />
</CustomProperties>"
-LiteralPath @("XDHyp:\Connections\aazure") -PassThru -UserName "
    advc345" -SecurePassword
```



```
12 $psd
```

> 注:
>
> 複数のテナントを追加できます。各テナントは複数のサブスクリプションを持つことができます。

別のテナントでの画像の選択　別の Azure テナントに属する Azure Compute Gallery のイメージを選択し、PowerShell コマンドを使用して MCS カタログを作成および更新できます。

1. ホスティングユニットのルートフォルダーに、sharedsubscriptionという名前の新しい共有サブスクリプションフォルダーが作成されます。
2. すべての共有サブスクリプションを表示します。

```
1 Get-ChildItem XDHyp:\HostingUnits\azres\sharedsubscription.folder
```

3. 1 つの共有サブスクリプションを選択し、その共有サブスクリプションのすべての共有リソースグループを表示します。

```
1 Get-ChildItem XDHyp:\HostingUnits\azres\image.folder\abc123.
      sharedsubscription
```

4. リソースグループを選択し、そのリソースグループのすべてのギャラリーを表示します。

```
1 Get-ChildItem XDHyp:\HostingUnits\azres\image.folder\abc123.
      sharedsubscription\ xyz.resourcegroup
```

5. ギャラリーを選択し、そのギャラリーのすべてのイメージ定義を表示します。

```
1 Get-ChildItem XDHyp:\HostingUnits\azres\image.folder\abc123.
      sharedsubscription\xyz.resourcegroup\efg.gallery
```

6. 1 つのイメージ定義を選択し、そのイメージ定義のすべてのイメージバージョンを表示します。

```
1 Get-ChildItem XDHyp:\HostingUnits\azres\image.folder\abc123.
      sharedsubscription\xyz.resourcegroup\efg.gallery\hij.
      imagedefinition
```

7. 次の要素を使用して、MCS カタログを作成および更新します:

   - リソースグループ
   - ギャラリー
   - ギャラリーイメージの定義
   - ギャラリーイメージのバージョン

   Remote PowerShell SDK を使用してカタログを作成する方法については、https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/を参照してください。

アプリケーションシークレットとその有効期限の管理

接続のアプリケーションシークレットは、その有効期限が切れる前に必ず変更してください。秘密キーの有効期限が切れる前に、Web Studio にアラートが表示されます。

Azure でのアプリケーションシークレットの作成　Azure Portal で、接続のアプリケーションシークレットを作成できます。

1. ［**Azure Active Directory**］を選択します。
2. Azure AD の ［**App registrations**］でアプリケーションを選択します。
3. ［**Certificates & secrets**］に移動します。
4. ［**Client secrets**］**>** ［**New client secret**］をクリックします。
5. シークレットの説明を入力し、期間を指定します。完了したら、［追加］を選択します。

   > 注:
   >
   > クライアントシークレットは後で取得できないため、必ず保存してください。

6. クライアントシークレット値と有効期限をコピーします。
7. Web Studio で、対応する接続を編集し、［アプリケーションシークレット］および ［シークレットの有効期限］フィールドの値を、コピーした値に置き換えます。

シークレットの有効期限の変更　Web Studio で、使用中のアプリケーションシークレットの有効期限を追加または変更できます。

1. ［接続とリソースの追加］ウィザードで接続を右クリックし、［接続の編集］をクリックします。
2. ［接続のプロパティ］ページで ［シークレットの有効期限］をクリックして、使用中のアプリケーションシークレットの有効期限を追加または変更します。

必要な **Azure** 権限

このセクションでは、Azure の一般的な必要最低限の権限について説明します。

最低限の権限

最低限の権限により、セキュリティ制御が向上します。ただし、最低限の権限しか使用していないため、追加の権限を必要とする新機能は失敗します。

ホスト接続の作成　Azure から取得した情報を使用して、新しいホスト接続を追加します。

```
"Microsoft.Network/virtualNetworks/read",
"Microsoft.Compute/virtualMachines/read",
"Microsoft.Compute/disks/read",
"Microsoft.Resources/providers/read",
"Microsoft.Resources/subscriptions/locations/read",
"Microsoft.Resources/tenants/read"
```

VM の電源管理　マシンインスタンスの電源をオンまたはオフにします。

```
"Microsoft.Compute/virtualMachines/read",
"Microsoft.Resources/subscriptions/resourceGroups/read",
"Microsoft.Compute/virtualMachines/deallocate/action",
"Microsoft.Compute/virtualMachines/start/action",
"Microsoft.Compute/virtualMachines/restart/action",
"Microsoft.Insights/diagnosticsettings/delete",
"Microsoft.Insights/diagnosticsettings/read",
"Microsoft.Insights/diagnosticsettings/write",
```

VM の作成、更新、または削除　マシンカタログを作成してから、マシンを追加、削除、更新し、マシンカタログを削除します。

以下は、マスターイメージが管理対象ディスクである場合、またはスナップショットがホスト接続と同じリージョンにある場合に必要となる最低限の権限の一覧です。

```
"Microsoft.Resources/subscriptions/resourceGroups/read",
"Microsoft.Resources/deployments/validate/action",
"Microsoft.Resources/tags/read",
"Microsoft.Resources/tags/write",
"Microsoft.Compute/virtualMachines/read",
"Microsoft.Compute/virtualMachines/write",
"Microsoft.Compute/virtualMachines/delete",
"Microsoft.Compute/virtualMachines/deallocate/action",
"Microsoft.Compute/snapshots/read",
"Microsoft.Compute/snapshots/write",
"Microsoft.Compute/snapshots/delete",
"Microsoft.Compute/snapshots/beginGetAccess/action",
"Microsoft.Compute/snapshots/endGetAccess/action",
"Microsoft.Compute/disks/read",
"Microsoft.Compute/disks/write",
"Microsoft.Compute/disks/delete",
"Microsoft.Compute/disks/beginGetAccess/action",
"Microsoft.Compute/disks/endGetAccess/action",
"Microsoft.Compute/locations/publishers/artifacttypes/types/versions/
   read",
"Microsoft.Compute/skus/read",
"Microsoft.Compute/virtualMachines/extensions/read",
"Microsoft.Compute/virtualMachines/extensions/write",
"Microsoft.Features/providers/features/read",
```



```
"Microsoft.Network/virtualNetworks/read",
"Microsoft.Network/virtualNetworks/subnets/join/action",
"Microsoft.Network/virtualNetworks/subnets/read",
"Microsoft.Network/networkSecurityGroups/read",
"Microsoft.Network/networkSecurityGroups/write",
"Microsoft.Network/networkSecurityGroups/delete",
"Microsoft.Network/networkSecurityGroups/join/action",
"Microsoft.Network/networkInterfaces/read",
"Microsoft.Network/networkInterfaces/write",
"Microsoft.Network/networkInterfaces/delete",
"Microsoft.Network/networkInterfaces/join/action",
"Microsoft.Network/locations/usages/read",
```

以下の機能の最低限の権限に基づき、以下の追加の権限が必要です:

- マスターイメージが、ホスト接続と同じリージョンにあるストレージアカウント内の VHD である場合:

```
"Microsoft.Storage/storageAccounts/read",
"Microsoft.Storage/storageAccounts/listKeys/action",
```

- マスターイメージが、Shared Image Gallery の ImageVersion である場合:

```
"Microsoft.Compute/galleries/read",
"Microsoft.Compute/galleries/images/read",
"Microsoft.Compute/galleries/images/versions/read",
```

- マスターイメージが管理対象ディスクであり、スナップショットまたは VHD がホスト接続のリージョンとは異なるリージョンにある場合:

```
"Microsoft.Storage/storageAccounts/read",
"Microsoft.Storage/storageAccounts/listKeys/action",
"Microsoft.Storage/storageAccounts/write",
"Microsoft.Storage/storageAccounts/delete",
"Microsoft.Storage/checknameavailability/read",
"Microsoft.Storage/locations/usages/read",
"Microsoft.Storage/skus/read",
```

- Citrix 管理対象リソースグループを使用する場合:

```
"Microsoft.Resources/subscriptions/resourceGroups/write",
"Microsoft.Resources/subscriptions/resourceGroups/delete",
```

- 共有テナントまたはサブスクリプションでマスターイメージを、Azure Compute Gallery（旧称：Shared Image Gallery）に配置した場合:

```
"Microsoft.Compute/galleries/write",
"Microsoft.Compute/galleries/images/write",
"Microsoft.Compute/galleries/images/versions/write",
"Microsoft.Compute/galleries/read",
"Microsoft.Compute/galleries/images/read",
"Microsoft.Compute/galleries/images/versions/read",
"Microsoft.Compute/galleries/delete",
```



```
"Microsoft.Compute/galleries/images/delete",
"Microsoft.Compute/galleries/images/versions/delete",
"Microsoft.Resources/subscriptions/read",
```

- Azure 専用ホストサポートを使用する場合:

```
"Microsoft.Compute/hostGroups/read",
"Microsoft.Compute/hostGroups/write",
"Microsoft.Compute/hostGroups/hosts/read",
```

- 顧客管理キー（CMK）でサーバー側暗号化（SSE）を使用する場合:

```
"Microsoft.Compute/diskEncryptionSets/read",
```

- ARM テンプレート（マシンプロファイル）を使用して VM を展開する場合:

```
"Microsoft.Resources/deployments/write",
"Microsoft.Resources/deployments/operationstatuses/read",
"Microsoft.Resources/deployments/read",
"Microsoft.Resources/deployments/delete",
"Microsoft.Insights/DataCollectionRuleAssociations/Read",
"Microsoft.Insights/dataCollectionRules/read",
```

- Azure テンプレートスペックをマシンプロファイルとして使用する場合:

```
"Microsoft.Resources/templateSpecs/read",
"Microsoft.Resources/templateSpecs/versions/read",
```

非管理対象ディスクを使用するマシンの作成、更新、および削除　以下は、マスターイメージが VHD であり、管理者から提供されたリソースグループを使用する場合に必要となる最低限の権限の一覧です:

```
"Microsoft.Resources/subscriptions/resourceGroups/read",
"Microsoft.Resources/tags/read",
"Microsoft.Resources/tags/write",
"Microsoft.Storage/storageAccounts/delete",
"Microsoft.Storage/storageAccounts/listKeys/action",
"Microsoft.Storage/storageAccounts/read",
"Microsoft.Storage/storageAccounts/write",
"Microsoft.Storage/checknameavailability/read",
"Microsoft.Storage/locations/usages/read",
"Microsoft.Storage/skus/read",
"Microsoft.Compute/virtualMachines/deallocate/action",
"Microsoft.Compute/virtualMachines/delete",
"Microsoft.Compute/virtualMachines/read",
"Microsoft.Compute/virtualMachines/write",
"Microsoft.Resources/deployments/validate/action",
"Microsoft.Network/networkInterfaces/delete",
"Microsoft.Network/networkInterfaces/join/action",
"Microsoft.Network/networkInterfaces/read",
"Microsoft.Network/networkInterfaces/write",
"Microsoft.Network/networkSecurityGroups/delete",
```



```
"Microsoft.Network/networkSecurityGroups/join/action",
"Microsoft.Network/networkSecurityGroups/read",
"Microsoft.Network/networkSecurityGroups/write",
"Microsoft.Network/virtualNetworks/subnets/read",
"Microsoft.Network/virtualNetworks/read",
"Microsoft.Network/virtualNetworks/subnets/join/action",
"Microsoft.Network/locations/usages/read",
```

一般的な権限

Contributor（投稿者）の役割には、すべてのリソースを管理するための完全なアクセス権があります。この一連の権限は、新しい機能の取得を妨げるものではありません。

以下の一連の権限は、現在の機能セットで必要とされるよりも多くの権限が含まれていますが、今後の互換性の面でベストなものを提供します：

```
"Microsoft.Compute/diskEncryptionSets/read",
"Microsoft.Compute/disks/beginGetAccess/action",
"Microsoft.Compute/disks/delete",
"Microsoft.Compute/disks/endGetAccess/action",
"Microsoft.Compute/disks/read",
"Microsoft.Compute/disks/write",
"Microsoft.Compute/galleries/delete",
"Microsoft.Compute/galleries/images/delete",
"Microsoft.Compute/galleries/images/read",
"Microsoft.Compute/galleries/images/versions/delete",
"Microsoft.Compute/galleries/images/versions/read",
"Microsoft.Compute/galleries/images/versions/write",
"Microsoft.Compute/galleries/images/write",
"Microsoft.Compute/galleries/read",
"Microsoft.Compute/galleries/write",
"Microsoft.Compute/hostGroups/hosts/read",
"Microsoft.Compute/hostGroups/read",
"Microsoft.Compute/hostGroups/write",
"Microsoft.Compute/snapshots/beginGetAccess/action",
"Microsoft.Compute/snapshots/delete",
"Microsoft.Compute/snapshots/endGetAccess/action",
"Microsoft.Compute/snapshots/read",
"Microsoft.Compute/snapshots/write",
"Microsoft.Compute/virtualMachines/deallocate/action",
"Microsoft.Compute/virtualMachines/delete",
"Microsoft.Compute/virtualMachines/read",
"Microsoft.Compute/virtualMachines/restart/action",
"Microsoft.Compute/virtualMachines/start/action",
"Microsoft.Compute/virtualMachines/write",
"Microsoft.Compute/locations/publishers/artifacttypes/types/versions/
   read",
"Microsoft.Compute/skus/read",
"Microsoft.Compute/virtualMachines/extensions/read",
"Microsoft.Compute/virtualMachines/extensions/write",
"Microsoft.Network/networkInterfaces/delete",
```



```
"Microsoft.Network/networkInterfaces/join/action",
"Microsoft.Network/networkInterfaces/read",
"Microsoft.Network/networkInterfaces/write",
"Microsoft.Network/networkSecurityGroups/delete",
"Microsoft.Network/networkSecurityGroups/join/action",
"Microsoft.Network/networkSecurityGroups/read",
"Microsoft.Network/networkSecurityGroups/write",
"Microsoft.Network/virtualNetworks/subnets/read",
"Microsoft.Network/virtualNetworks/read",
"Microsoft.Network/virtualNetworks/subnets/join/action",
"Microsoft.Network/locations/usages/read",
"Microsoft.Resources/deployments/operationstatuses/read",
"Microsoft.Resources/deployments/read",
"Microsoft.Resources/deployments/validate/action",
"Microsoft.Resources/deployments/write",
"Microsoft.Resources/deployments/delete",
"Microsoft.Resources/subscriptions/resourceGroups/read",
"Microsoft.Resources/subscriptions/resourceGroups/write",
"Microsoft.Resources/subscriptions/resourceGroups/delete",
"Microsoft.Resources/providers/read",
"Microsoft.Resources/subscriptions/locations/read",
"Microsoft.Resources/subscriptions/read",
"Microsoft.Resources/tags/read",
"Microsoft.Resources/tags/write",
"Microsoft.Resources/tenants/read",
"Microsoft.Resources/templateSpecs/read",
"Microsoft.Resources/templateSpecs/versions/read",
"Microsoft.Storage/storageAccounts/delete",
"Microsoft.Storage/storageAccounts/listKeys/action",
"Microsoft.Storage/storageAccounts/read",
"Microsoft.Storage/storageAccounts/write",
"Microsoft.Storage/checknameavailability/read",
"Microsoft.Storage/locations/usages/read",
"Microsoft.Storage/skus/read",
"Microsoft.Features/providers/features/read",
"Microsoft.Insights/DataCollectionRuleAssociations/Read",
"Microsoft.Insights/dataCollectionRules/read",
"Microsoft.Insights/diagnosticsettings/delete",
"Microsoft.Insights/diagnosticsettings/read",
"Microsoft.Insights/diagnosticsettings/write",
```

ホスト接続の権限を検証する

MCS マシンカタログの作成と管理に関連するタスクを実行するために、ホスト接続の権限を検証できます。この実装により、VM の作成、削除、更新、VM の電源管理などのさまざまなシナリオに必要な不足している権限を事前に見つけることができ、重要なタイミングでブロックされることを回避できます。

PowerShell コマンド`Test-HypHypervisorConnection`を使用して、ホスト接続の権限を検証できます。コマンドの結果は一覧としてキャプチャされ、一覧内の各項目は 3 つのセクションに分割されます。

- カテゴリ：ユーザーが MCS マシンカタログを作成および管理するために実行できるアクションまたはタスク。

- 修正アクション：ユーザーの不足している権限による不一致を解決するために管理者が実行する必要がある手順。
- 不足している権限：カテゴリに不足している権限の一覧。

権限を検証するには、次の手順を実行します：

1. Azure へのホスト接続を作成します。
2. Delivery Controller ホストから PowerShell ウィンドウを開きます。
3. `asnp citrix*`を実行し、Citrix 固有の PowerShell モジュールをロードします。
4. 接続をテストするために必要な権限があるかどうか確認するには、次のコマンドを実行します。

   ```
   Test-HypHypervisorConnection -LiteralPath "XDHyp:\Connections\
       AzureCon"
   ```

   SPN に必要な役割レベルの権限：

   - Microsoft.Authorization/roleDefinitions/read（サブスクリプションレベル、またはリソースグループが提供されている場合はリソースグループレベル）
   - Microsoft.Authorization/roleAssignments/read（サブスクリプションレベル、またはリソースグループが提供されている場合はリソースグループレベル）

   SPN に必要な **API** レベルの権限：

   Microsoft.Graph：

   - Application.Read.All
   - Directory.Read.All
   - ServicePrincipalEndpoint.Read.All

5. 権限を検索するために必要な不足している権限を追加した後、次のコマンドを実行して、さまざまなカテゴリの権限があるかどうかを確認します。

   例：

   必要なより高いレベルの承認とともに、サブスクリプションレベルで接続をテストするには：

   ```
   Test-HypHypervisorConnection -LiteralPath XDHyp:\Connections\
       AzureCon -SecurePassword $password -UserName 922e65d5-38ae-4cf5
       -xxxx-xxxxxxxxx
   ```

   例：

   高いレベルの承認なしで、リソースグループレベルで接続をテストするには：

   ```
   Test-HypHypervisorConnection -LiteralPath XDHyp:\Connections\
       testles -CustomProperties $customProperties | Format-List
   ```


> 注:
>
> リソースグループは接続固有の情報であるため、CustomProperties パラメーターはリソースグループレベルを提供するために使用されます。

例:

より高いレベルの承認とともに、リソースグループレベルで接続をテストするには:

```
Test-HypHypervisorConnection -LiteralPath XDHyp:\Connections\
    testles -SecurePassword $password -UserName 922e65d5-38ae-4cf5
    -832b-54122196b7dd -CustomProperties $customProperties
```

権限について詳しくは、「必要な Azure 権限」を参照してください。

次の手順

- 初期展開プロセスを行っている場合は、「マシンカタログの作成」を参照してください
- Azure 固有の情報については、「Microsoft Azure カタログの作成」を参照してください。

追加情報

- 接続とリソース
- マシンカタログの作成

Microsoft System Center Virtual Machine Manager への接続

August 17, 2024

「接続とリソースの作成と管理」では接続を作成するためのウィザードについて説明しています。次の情報は、Microsoft System Center Virtual Machine Manager（VMM）に固有の詳細について説明しています。

> 注:
>
> VMM への接続を作成する前に、まず VMM アカウントをリソースの場所として設定する必要があります。「Microsoft System Center Virtual Machine Manager 仮想化環境」を参照してください。

接続の作成

MCS を使用して仮想マシンをプロビジョニングした場合は、接続作成ウィザードで次の操作を行います:

- アドレスにホストサーバーの完全修飾ドメイン名を入力します。

- 先ほど設定した管理者アカウントの資格情報を入力します。このアカウントには、仮想マシンを新規作成できる権限が必要です。
- ［ホスト詳細］ダイアログボックスで、仮想マシンの作成時に使用するクラスターまたはスタンドアロンホストを選択します。

  > 重要
  >
  > 単一 Hyper-V ホストによる展開でも、クラスターまたはスタンドアロンホストを参照します。

次の手順

- 初期展開プロセスを行っている場合は、「マシンカタログの作成」を参照してください
- SMB 3 ファイル共有で MCS を使用してマシンカタログを作成する方法については、「Microsoft System Center Virtual Machine Manager カタログの作成」を参照してください。

追加情報

- 接続とリソース
- マシンカタログの作成

Nutanix への接続

August 17, 2024

「接続とリソースの作成と管理」では接続を作成するためのウィザードについて説明しています。以下の情報は、Nutanix に固有の詳細について説明しています。

> 注:
>
> Nutanix への接続を作成する前に、まず Nutanix アカウントをリソースの場所として設定する必要があります。「Nutanix 仮想化環境」を参照してください。

Nutanix との接続の作成

以下の情報は、「接続とリソース」のガイダンスを補足するものです。Nutanix 接続を作成するときは、Nutanix に固有の詳細に注意しながら、その記事の一般的なガイダンスに従ってください。

接続とリソースの追加ウィザードの ［接続］ページで、接続の種類として［Nutanix］を選択し、アドレスと資格情報、接続の名前を指定します。［ネットワーク］ページで、ホスティングユニットのネットワークを選択します。

選択できる接続の種類は次のとおりです：**Nutanix AHV**、**Nutanix AHV DRaaS**、**Nutanix AHV PC**。

- **Nutanix AHV** の場合は、Prism Element（PE）クラスターのアドレスと資格情報を指定します。
- **Nutanix AHV PC** の場合は、Prism Central（PC）のアドレスと資格情報を指定します。

  > 注:
  >
  > 現在、接続の種類として Nutanix AHV PC を使用するのは、Nutanix Cloud Cluster（NC2）on Azure への接続を作成する場合に限られます。また、マシンカタログは、NC2 on Azure 接続内の単一のクラスターでのみホストできます。

- **Nutanix AHV DRaaS** の場合は、DRaaS テナントのアドレスとユーザー名を指定します。プライベートおよびパブリックの Nutanix DRaaS 資格情報ファイル（`.pem`）をインポートします。

> ヒント:
>
> Nutanix AHV（Prism Element）をリソースとして使用してマシンを展開する場合は、VM のディスクが存在するコンテナを選択します。

次の手順

- 初期展開プロセスを行っている場合は、「マシンカタログの作成」を参照してください
- Nutanix 固有の情報については、「Nutanix カタログの作成」を参照してください。

追加情報

- 接続とリソース
- マシンカタログの作成

Nutanix クラウドおよびパートナーソリューションへの接続

August 17, 2024

「接続とリソースの作成と管理」では接続を作成するためのウィザードについて説明しています。以下の情報は、Nutanix クラウドおよびパートナーソリューションに固有の詳細について説明しています。

Citrix Virtual Apps and Desktops は、次の Nutanix クラウドおよびパートナーソリューションをサポートしています:

- Nutanix Cloud Clusters on AWS

> 注:
>
> Nutanix クラウドおよびパートナーソリューションへの接続を作成する前に、まずそれぞれのアカウントをリソースの場所として設定する必要があります。「Nutanix クラウドおよびパートナーソリューション」を参照してください。

Nutanix Prism への接続

Nutanix クラスターを作成したら、Nutanix Prism に接続します。

Nutanix Prism に接続するには、次の手順を実行します:

1. 「10.0.129.0/24」サブネットに踏み台 VM を作成します。
2. 踏み台 VM に RDP（リモートデスクトッププロトコル）で接続し、前のセクションでコピーした **Prism Element** の URL に移動します。
3. デフォルトの資格情報を使用してログインします: `admin:nutanix/4u`。忘れずにパスワードを変更してください。

Nutanix Cluster での VM の作成

Nutanix Prism に接続した後、Nutanix クラスター上に VMを作成します。

VM がインターネットアクセスを必要とする場合

1. AWS コンソールに移動します。
2. Nutanix CFS によって作成されたものと同じ VPC で、新しく「10.0.130.0/24」サブネットを作成します。
3. このサブネットのルートテーブルにルートを追加して、すべての非ローカルトラフィックを上記の NAT ゲートウェイに転送します。
4. 踏み台 VM に RDP（リモートデスクトッププロトコル）で接続し、前のセクションでコピーした **Prism Element** の URL に移動して、ログインします。
5. 新しいネットワークの追加［**Settings**］**>**［**Network Configuration**］**>**［**Create Subnet**］に移動します。AWS で使用しているものと同じ「10.0.130.0/24」サブネットを使用します。
6. その新しいサブネットにすべての VM（AD、CC、VDA など）を作成します。

VM がインターネットアクセスを必要としない場合

1. 踏み台 VM に RDP（リモートデスクトッププロトコル）で接続し、前のセクションでコピーした **Prism Element** の URL に移動して、ログインします。
2. 新しいネットワークの追加［**Settings**］**>**［**Network Configuration**］**>**［**Create Subnet**］に移動します。「10.0.129.0/24」サブネットを使用します。

3. そのサブネットにすべての VM（AD、CC、VDA など）を作成します。

> ヒント:
>
> VM の時間とタイムゾーン情報が正しく設定されていることを確認してください。これは特に AD（Active Directory）に当てはまります。

ホスト接続の作成

1. Web Studio を起動します。
2. ホスティングノードを選択し、［接続およびリソースの追加］をクリックします。
3. ［接続］画面で、［新しい接続を作成する］を選択し、［接続アドレス］に「`https://xxx.xxx.xxx.xxx:9440`」を入力します。
4. UI に従ってウィザードを完了します。

> 注:
>
> Web Studio で Nutanix のオプションを表示するには、nutanix プラグインが（nutanix ゾーンで使用されていなくても）すべてのコネクタ VM にインストールされている必要があります。

次の手順

- 初期展開プロセスを行っている場合は、「マシンカタログの作成」を参照してください
- Nutanix 固有の情報については、「Nutanix カタログの作成」を参照してください。

追加情報

- 接続とリソース
- マシンカタログの作成

VMware への接続

August 17, 2024

「接続とリソースの作成と管理」では接続を作成するためのウィザードについて説明しています。以下の情報は、VMware 仮想化環境に固有の詳細について説明しています。

> 注:

> VMware への接続を作成する前に、まず VMware アカウントをリソースの場所として設定する必要があります。「VMware 仮想化環境」を参照してください。

接続の作成

接続の作成ウィザードで、以下を実行します。

1. 接続の種類として［VMware］を選択します。
2. vCenter SDK のアクセスポイントのアドレスを指定します。
3. 仮想マシンを作成する権限を持つ、既存の VMware ユーザーアカウントの資格情報を指定します。ユーザー名を「domain/username」形式で指定します。

VMware SSL の拇印機能

VMware SSL 拇印機能により、VMware vSphere ハイパーバイザーへのホスト接続を手動で作成する必要がなくなります。接続を作成する前に、サイトの Delivery Controller とハイパーバイザーの証明書との信頼関係を手動で作成する必要がなくなりました。

VMware SSL 拇印機能は、信頼されていない証明書の拇印をサイトデータベースに保存します。この構成により、Controller ではなくても、Citrix Virtual Apps and Desktops でハイパーバイザーを信頼できるものとして継続的に識別できます。

Studio で vSphere のホスト接続を確立する場合、接続しようとしているマシンの証明書をダイアログボックスで見ることができます。その証明書を見て、信頼するかどうかを選択できます。

必要な権限

この記事にリストされている権限の組み合わせまたはそのすべてを使用して、VMware ユーザーアカウントおよび 1 つまたは複数の VMware の役割を作成します。役割の作成は、さまざまな Citrix DaaS 処理をいつでも要求可能にする上で、ユーザーの権限に必要となるレベルまで細分化して行ってください。いつでもユーザー固有の権限を付与できるようにするために、データセンター以上のレベルで ［**Propagate to children**］オプションを選択して、ユーザーを各役割に関連付けます。

以下の表に、Citrix Virtual Apps and Desktops の処理と最低限必要な VMware 権限の間の対応関係を示します。

> 注:
>
> 権限リストの表示名、特にユーザーインターフェイスは、vSphere のバージョンによって異なります。たとえば、vSphere 6.7 のユーザーインターフェイス上の権限は、［メモリの変更］および ［設定の変更］であり、このページの「必要な権限」で記載されている ［設定］および ［メモリ］とは異なっています。

接続およびリソースの追加

SDK	ユーザーインターフェイス
System. Anonymous、System. Read、および System.View	自動的に追加されます。組み込みの読み取り専用の役割を使用できます。

電源管理

SDK	ユーザーインターフェイス
VirtualMachine.Interact.PowerOff	[Virtual machine] > [Interaction] > [Power Off]
VirtualMachine.Interact.PowerOn	[Virtual machine] > [Interaction] > [Power On]
VirtualMachine.Interact.Reset	[Virtual machine] > [Interaction] > [Reset]
VirtualMachine.Interact.Suspend	[Virtual machine] > [Interaction] > [Suspend]
Datastore.Browse	[Datastore] > [Browse datastore]

マシンのプロビジョニング（**Machine Creation Services**）

MCS を使用してマシンをプロビジョニングするには、次の権限が必須です：

SDK	ユーザーインターフェイス
Datastore.AllocateSpace	[Datastore] > [Allocate space]
Datastore.Browse	[Datastore] > [Browse datastore]
Datastore.FileManagement	[Datastore] > [Low level file operations]
Network.Assign	[Network] > [Assign network]
Resource.AssignVMToPool	[Resource] > [Assign virtual machine to resource pool]
VirtualMachine.Config.AddExistingDisk	[Virtual machine] > [Configuration] > [Add existing disk]
VirtualMachine.Config.AddNewDisk	[Virtual machine] > [Configuration] > [Add new disk]
Virtual machine.Config.Add or remove device	[Virtual machine] > [Configuration] > [Add or remove device]

SDK	ユーザーインターフェイス
VirtualMachine.Config.AdvancedConfig	[Virtual machine] > [Configuration] > [Advanced]
VirtualMachine.Config.RemoveDisk	[Virtual machine] > [Configuration] > [Remove disk]
VirtualMachine.Config.CPUCount	[Virtual machine] > [Configuration] > [Change CPU count]
VirtualMachine.Config.Memory	[Virtual machine] > [Configuration] > [Change memory]
VirtualMachine.Config.Settings	[Virtual machine] > [Configuration] > [Change settings]
VirtualMachine.Interact.PowerOff	[Virtual machine] > [Interaction] > [Power Off]
VirtualMachine.Interact.PowerOn	[Virtual machine] > [Interaction] > [Power On]
VirtualMachine.Interact.Reset	[Virtual machine] > [Interaction] > [Reset]
VirtualMachine.Interact.Suspend	[Virtual machine] > [Interaction] > [Suspend]
VirtualMachine.Inventory.CreateFromExisting	[Virtual machine] > [Inventory] > [Create from existing]
VirtualMachine.Inventory.Create	[Virtual machine] > [Inventory] > [Create new]
VirtualMachine.Inventory.Delete	[Virtual machine] > [Inventory] > [Remove]
VirtualMachine.Provisioning.Clone	[Virtual machine] > [Provisioning] > [Clone virtual machine]
VirtualMachine.State.CreateSnapshot	vSphere 5.0, Update 2、vSphere 5.1, Update 1、および vSphere 6.x, Update 1：[Virtual machine] > [State] > [Create snapshot]。vSphere 5.5：[Virtual machine] > [Snapshot management] > [Create snapshot]

イメージの更新とロールバック

SDK	ユーザーインターフェイス
Datastore.AllocateSpace	[Datastore] > [Allocate space]
Datastore.Browse	[Datastore] > [Browse datastore]
Datastore.FileManagement	[Datastore] > [Low level file operations]
Network.Assign	[Network] > [Assign network]

SDK	ユーザーインターフェイス
Resource.AssignVMToPool	[Resource] > [Assign virtual machine to resource pool]
VirtualMachine.Config.AddExistingDisk	[Virtual machine] > [Configuration] > [Add existing disk]
VirtualMachine.Config.AddNewDisk	[Virtual machine] > [Configuration] > [Add new disk]
VirtualMachine.Config.AdvancedConfig	[Virtual machine] > [Configuration] > [Advanced]
VirtualMachine.Config.RemoveDisk	[Virtual machine] > [Configuration] > [Remove disk]
VirtualMachine.Interact.PowerOff	[Virtual machine] > [Interaction] > [Power Off]
VirtualMachine.Interact.PowerOn	[Virtual machine] > [Interaction] > [Power On]
VirtualMachine.Interact.Reset	[Virtual machine] > [Interaction] > [Reset]
VirtualMachine.Inventory.CreateFromExisting	[Virtual machine] > [Inventory] > [Create from existing]
VirtualMachine.Inventory.Create	[Virtual machine] > [Inventory] > [Create new]
VirtualMachine.Inventory.Delete	[Virtual machine] > [Inventory] > [Remove]
VirtualMachine.Provisioning.Clone	[Virtual machine] > [Provisioning] > [Clone virtual machine]

プロビジョニングされたマシンの削除

SDK	ユーザーインターフェイス
Datastore.Browse	[Datastore] > [Browse datastore]
Datastore.FileManagement	[Datastore] > [Low level file operations]
VirtualMachine.Config.RemoveDisk	[Virtual machine] > [Configuration] > [Remove disk]
VirtualMachine.Interact.PowerOff	[Virtual machine] > [Interaction] > [Power Off]
VirtualMachine.Inventory.Delete	[Virtual machine] > [Inventory] > [Remove]

ストレージプロファイル（**vSAN**）

vSAN データストアでのカタログ作成中にストレージポリシーを表示、作成、または削除するには、次の権限が必須です：

SDK	ユーザーインターフェイス
StorageProfile.Update	PROFILE 駆動のストレージ > Profile 駆動のストレージ更新。vSphere 8 の場合：VM ストレージポリシー > Update VM storage policies
StorageProfile.View	PROFILE 駆動のストレージ > Profile 駆動のストレージ表示。vSphere 8 の場合：VM ストレージポリシー > View VM storage policies

タグとカスタム属性

タグとカスタム属性を使用すると、vSphere インベントリで作成された VM にメタデータをつなげて、これらのオブジェクトを検索およびフィルタリングしやすくすることができます。タグまたはカテゴリを作成、編集、割り当て、および削除するには、次の権限が必須です：

SDK	ユーザーインターフェイス
InventoryService.Tagging.CreateTag	vSphere のタグ付け > vSphere タグの作成
InventoryService.Tagging.CreateCategory	vSphere のタグ付け > vSphere タグカテゴリの作成
InventoryService.Tagging.EditTag	vSphere のタグ付け > vSphere タグの編集
InventoryService.Tagging.EditCategory	vSphere のタグ付け > vSphere タグカテゴリの編集
InventoryService.Tagging.DeleteTag	vSphere のタグ付け > vSphere タグの削除
InventoryService.Tagging.DeleteCategory	vSphere のタグ付け > vSphere タグカテゴリの削除
InventoryService.Tagging.AttachTag	vSphere のタグ付け > vSphere タグの割り当てまたは割り当て解除
InventoryService.Tagging.ObjectAttachable	vSphere のタグ付け > オブジェクトへの vSphere タグの割り当てまたは割り当て解除
Global.ManageCustomFields	[Global] > [Manage custom attributes]
Global.SetCustomField	[Global] > [Set custom attribute]

> 注:
>
> MCS は、マシンカタログを作成するときに、ターゲット VM に特別な名前タグを付けます。これらのタグは、マスターイメージを MCS 作成 VM と区別し、イメージの準備に MCS 作成 VM を使用できないようにします。vCenter の`XdProvisioned`属性の値で違いを識別できます。MCS で VM を作成する場合、この属性は **True** に設定されます。

暗号化操作

暗号化操作権限は、誰がどのタイプのオブジェクトに対してどの種類の暗号化操作を実行できるかを制御します。vSphere Native Key Provider は`Cryptographer.*`権限を使用します。暗号化操作には、次の最低限の権限が必要です:

> 注:
>
> これらの権限は、vTPM が組み込まれた VM で MCS マシンカタログを作成するために必要です。

SDK	ユーザーインターフェイス
Cryptographer.Access	[Privileges] > [All Privileges] > [Cryptographic operations] > [Direct Access]
Cryptographer.AddDisk	[Privileges] > [All Privileges] > [Cryptographic operations] > [Add disk]
Cryptographer.Clone	[Privileges] > [All Privileges] > [Cryptographic operations] > [Clone]
Cryptographer.Encrypt	[Privileges] > [All Privileges] > [Cryptographic operations] > [Encrypt]
Cryptographer.EncryptNew	[Privileges] > [All Privileges] > [Cryptographic operations] > [Encrypt new]
Cryptographer.Decrypt	[Privileges] > [All Privileges] > [Cryptographic operations] > [Decrypt]
Cryptographer.Migrate	[Privileges] > [All Privileges] > [Cryptographic operations] > [Clone]
Cryptographer.ReadKeyServersInfo	[Privileges] > [All Privileges] > [Cryptographic operations] > [Read KMS information]

マシンのプロビジョニング（**Citrix Provisioning**）

Citrix Provisioning コンソールで、Citrix Virtual Apps and Desktops インストールウィザード、およびデバイスのエクスポートウィザードを使用して仮想マシンをプロビジョニングするには、テンプレートを複製および展開する

権限が必要です。ホスト接続を作成するときに権限を設定します。マシンのプロビジョニング（Machine Creation Services）のすべての権限と、以下が必要です。

SDK	ユーザーインターフェイス
VirtualMachine.Config.AddRemoveDevice	[Virtual machine] > [Configuration] > [Add or remove device]
VirtualMachine.Config.CPUCount	[Virtual machine] > [Configuration] > [Change CPU Count]
VirtualMachine.Config.Memory	[Virtual machine] > [Configuration] > [Memory]
VirtualMachine.Config.Settings	[Virtual machine] > [Configuration] > [Settings]
VirtualMachine.Provisioning.CloneTemplate	[Virtual machine] > [Provisioning] > [Clone template]
VirtualMachine.Provisioning.DeployTemplate	[Virtual machine] > [Provisioning] > [Deploy template]
VApp.Export	[vApp] > [Export]

> 注:
>
> `VApp.Export`は、マシンプロファイルを使用して MCS マシンカタログを作成するために必要です。

証明書の取得とインポート

vSphere 通信を保護するため、Citrix では HTTP ではなく HTTPS を使用することをお勧めします。

HTTPS を使用するにはデジタル証明書が必要です。組織のセキュリティポリシーの要件を満たす証明書機関から発行されたデジタル証明書を使用してください。

証明機関のデジタル証明書を使用できない場合は、VMware によりインストールされる自己署名証明書を使用することもできます。この方法は、組織のセキュリティポリシーで許可されている場合にのみ使用してください。VMware vCenter の証明書を各 Delivery Controller に追加します。

1. vCenter Server を実行しているコンピューターの完全修飾ドメイン名（FQDN）を、そのサーバーのホストファイル（`%SystemRoot%/WINDOWS/system32/Drivers/etc/`）に追加します。この手順は、vCenter Server を実行しているコンピューターの FQDN がドメイン名システムに登録されていない場合にのみ必要です。
2. 以下の 3 つの内いずれかの方法で、vCenter の証明書を入手します:

   vCenter サーバーからコピーする。

   a) vCenter サーバー上の rui.crt ファイルを、Delivery Controller からアクセス可能な場所にコピーします。

b) Controller で、エクスポートした証明書の保存先に移動し、rui.crt ファイルを開きます。

Web ブラウザーでダウンロードする。Internet Explorer を使用している場合は、Internet Explorer を右クリックして ［管理者として実行］を選択します。

a) Web ブラウザーを開き、vCenter サーバー（https://server1.domain1.com)など）への保護された接続を確立します。
b) セキュリティに関する警告を受け入れます。
c) 証明書のエラーが表示されるアドレスバーをクリックします。
d) 証明書を表示して、［詳細］タブをクリックします。
e) ［ファイルへコピー］を選択して、任意のファイル名を指定して CER 形式でエクスポートします。
f) エクスポートした証明書を保存します。
g) エクスポートした証明書の CER ファイルを開きます。

管理者として実行する **Internet Explorer** から直接インポートします。

- Web ブラウザーを開き、vCenter サーバー（https://server1.domain1.com)など）への保護された接続を確立します。
- セキュリティに関する警告を受け入れます。
- 証明書のエラーが表示されるアドレスバーをクリックします。
- 証明書を表示します。

3. 各 Controller 上の証明書ストアに証明書をインポートします。

a) ［証明書のインストール］オプションをクリックして ［ローカルマシン］を選択し、［次へ］をクリックします。
b) ［証明書をすべて次のストアに配置する］を選択して、［参照］をクリックします。［信頼されたユーザー］を選択し、［**OK**］をクリックします。［次へ］、［完了］の順にクリックします。

インストール後に vSphere サーバーの名前を変更する場合は、サーバー上で新しい自己署名証明書を作成してから、新しい証明書をインポートする必要があります。

次の手順

- 初期展開プロセスを行っている場合は、「マシンカタログの作成」を参照してください
- VMware 固有の情報については、「VMware カタログの作成」を参照してください。

追加情報

- 接続とリソース
- マシンカタログの作成

VMware クラウドおよびパートナーソリューションへの接続

August 17, 2024

Azure VMware Solution（AVS）クラスター、Google Cloud VMware Engine、VMware cloud on AWSをセットアップしたら、接続を作成します。接続の作成については、「VMware への接続」を参照してください。

次の手順

- 初期展開プロセスを行っている場合は、「マシンカタログの作成」を参照してください
- VMware 固有の情報については、「VMware カタログの作成」を参照してください。

追加情報

- 接続とリソース
- マシンカタログの作成

イメージ管理（Technical Preview）

August 17, 2024

はじめに

MCS カタログの作成または更新プロセスには、次の 2 つのフェーズがあります：

- マスタリング：ソースイメージを公開イメージに変換する
- クローン作成：公開されたイメージから新しい VM が作成される

イメージ管理機能により、MCS はマスタリングフェーズを全体的なプロビジョニングワークフローから分離します。

単一のソースイメージからさまざまな MCS イメージバージョン（準備済みイメージ）を準備し、複数の異なる MCS マシンカタログで使用できます。この実装により、ストレージと時間のコストが大幅に削減され、VM の展開とイメージ更新のプロセスが簡素化されます。

このイメージ管理機能を使用するメリットは次のとおりです：

- カタログを作成せずに、事前に準備済みイメージを生成します。
- カタログの作成や更新など、複数のシナリオで準備済みイメージを再利用します。

- カタログの作成または更新時間を大幅に短縮します。

> 注:
>
> - この機能は現在、Azure および VMware 仮想化環境に適用できます。
> - 準備済みイメージを使用せずに MCS マシンカタログを作成できます。その場合、この機能のメリットを活用することはできません。

使用例

イメージ管理機能のユースケースは次のとおりです:

- バージョン管理:イメージバージョンを使用すると、次のことが可能になります:
  - 特定のイメージに対するさまざまな反復または更新を管理する。
  - さまざまな目的に合わせてイメージの複数のバージョンを維持する。
- 論理的なグループ化:複数のイメージ定義を作成して、次のことが可能になります:
  - プロジェクト、部門、アプリケーション、デスクトップの種類などのさまざまな基準に基づいて、イメージバージョンを論理的にグループ化する。
  - 組織内でイメージをより効率的に管理する。

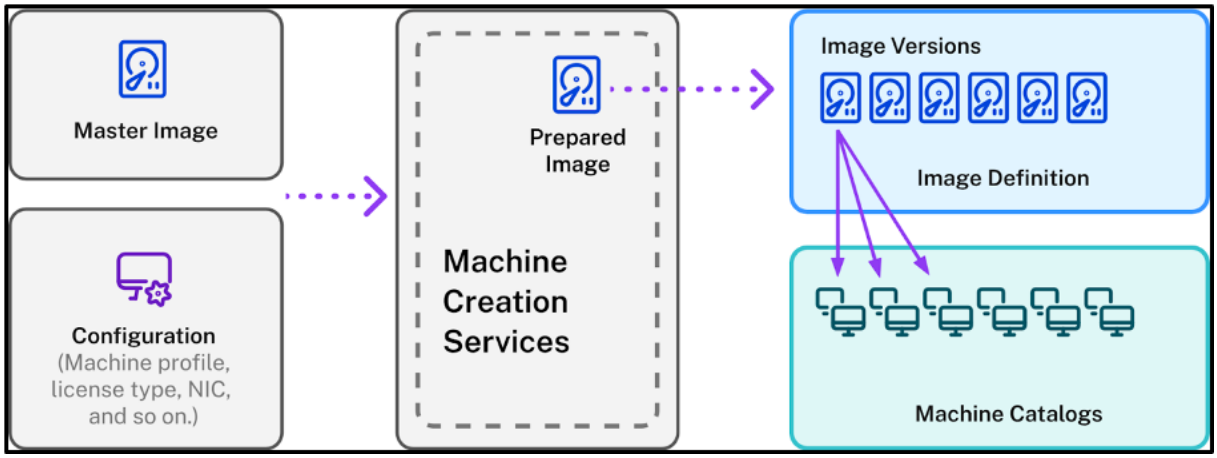
準備済みイメージとは何ですか❓

MCS はイメージ管理機能を使用して、マスタリングフェーズをカタログ作成または更新ワークフロー全体から切り離し、プロセスを 2 つの段階に分割します:

1. 単一のソースイメージから準備済みイメージを作成します。
2. 準備済みイメージを使用して、MCS マシンカタログを作成または更新します。

準備済みイメージを事前に作成しておくことができます。1 つの準備済みイメージを使用して、複数の MCS でプロビジョニングされたマシンカタログを作成または更新できます。

イメージから Web Studio を使用する場合に、準備済みイメージが複数の MCS マシン カタログにわたってどのように使用されるかを理解します:



イメージ定義：イメージ定義は、イメージのバージョンを論理的にグループ化したものです。イメージ定義には次の情報が保持されます：

- なぜこのイメージが作られたのか
- どの OS 向けか
- イメージの使用に関するその他の情報。

カタログはイメージ定義から作成されるのではなく、イメージ定義に基づいて作成されたイメージバージョンから作成されます。

イメージバージョン：イメージバージョンは、イメージ定義のバージョン管理を行います。イメージ定義には複数のイメージバージョンを含めることができます。イメージバージョンを準備済みイメージとして使用して、カタログを作成または更新します。

または、PowerShell コマンドを使用してカタログの作成または更新のためにプロビジョニングスキームを作成する場合は、環境に応じて、マスターイメージバージョン仕様に基づいた準備済みイメージバージョン仕様を作成する必要があります。

Technical Preview への参加

Technical Preview への参加に関心がある場合は、こちらに連絡先情報を入力していただくようお願いします。

テスト環境の設定をお手伝いし、必要に応じて技術サポートも提供いたします。

条件

- Windows マスターイメージの場合、バージョン 2311 以降の VDA イメージで、MCS/IO が有効になっているもののみがサポートされています。

制限事項

現在、この機能は以下をサポートしていません:

- Azure の複数の NIC
- 永続データディスク機能
- マルチセッションの休止状態
- イメージの種類の変更

Web Studio を使用したイメージライフサイクル管理

Web Studio を使用する場合のイメージのライフサイクルは次のとおりです:

1. 準備済みイメージを作成する: イメージ定義とその初期イメージバージョンを作成します。
2. 初期イメージバージョンからイメージバージョンを作成します。
3. イメージバージョンを準備済みイメージとして使用してカタログを作成します。
4. 別の準備済みイメージでマシンカタログを更新します。
5. イメージ定義とバージョンの管理: イメージバージョンの名前と説明、およびイメージ定義の説明を編集します。
6. イメージバージョンを削除します。
7. イメージ定義を削除します。

または、PowerShell を使用してイメージを管理することもできます。「PowerShell を使用したイメージライフサイクル管理」を参照してください。

準備済みイメージを使用してカタログを作成または更新する

準備済みイメージを作成し、その準備済みイメージを使用して、次の方法で MCS マシンカタログを作成または更新します:

- Web Studio
- PowerShell コマンド

Web Studio の使用

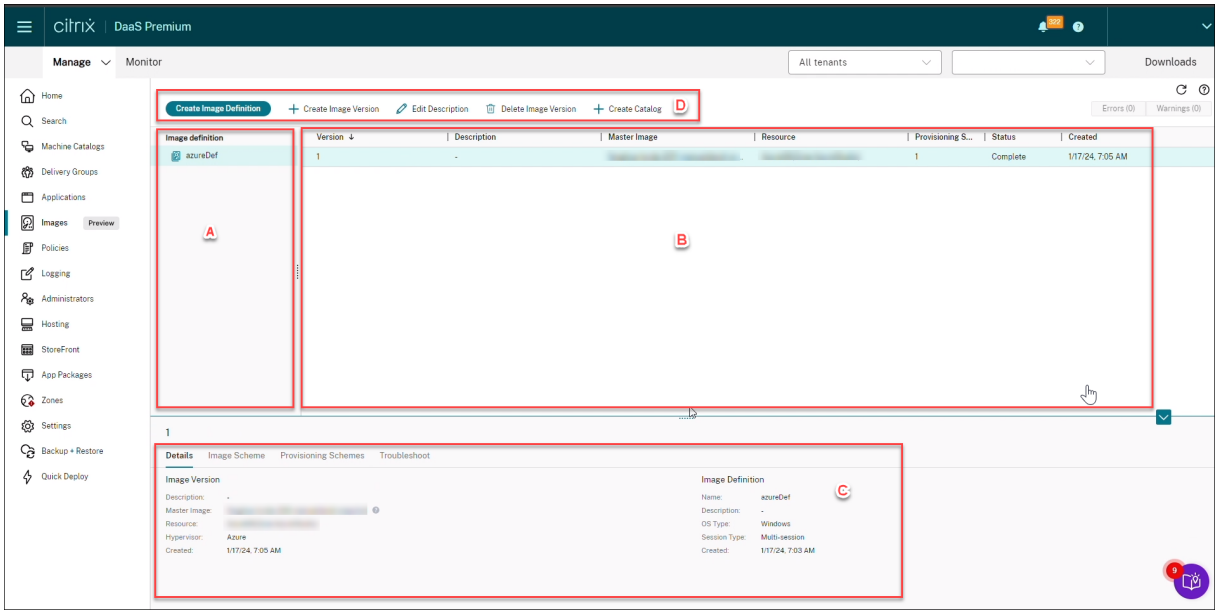
次のトピックを参照してください:

- イメージノードについて
- イメージ定義と初期イメージバージョンを作成する
- イメージバージョンを作成する
- イメージノードからマシンカタログを作成する

- マシンカタログノードからマシンカタログを作成する
- 別の準備済みイメージでマシンカタログを更新する
- イメージ定義とバージョンを管理する

イメージノードについて

イメージノードを使用して、MCS で準備済みのイメージを作成および管理します。メインビューは 4 つの部分に分かれています:



ラベル	部分	説明
A	イメージ定義	以前に作成されたイメージ定義を一覧表示します。
B	イメージバージョン	選択したイメージ定義のイメージ バージョンを表示します。
C	詳細	• [詳細] タブには、マスターイメージ、リソース、ハイパーバイザー、イメージ定義の名前、OS の種類、セッションの種類など、選択したイメージ定義またはバージョンに関する詳細情報が表示されます。 • [イメージスキーム] タブには、ハード ディスク、マシン サイズ、ライセンスの種類、ディスク暗号化セット、マシンプロファイルなど、イメージの準備に使用されるテンプレートに関する情報が表示されます。 • [プロビジョニングスキーム] タブには、カタログの作成に
D	操作バー	[イメージバージョンの作成]、[説明の編集]、[イメージバージョンの削除]、[カタログの作成] など、イメージ定義とバージョンに対して実行できる操作を一覧表示します。

準備済みイメージを使用してマシンカタログを作成する

準備済みイメージを使用して MCS マシンカタログを作成するための主な手順は次のとおりです:

1. イメージ定義と初期イメージバージョンを作成します。
2. イメージバージョンを準備済みイメージとして使用してカタログを作成します。

イメージ定義と初期イメージバージョンを作成する

イメージ定義と初期イメージバージョンを作成するには、次の手順を実行します:

1. Web Studio にサインインし、イメージノードを選択します。[はじめに] ページで [次へ] をクリックします。
2. [イメージ定義] ページで、イメージ定義の [**OS** の種類] と [セッションの種類] を指定します。
3. [イメージ] ページで、[リソース] と、イメージバージョンを作成するためのテンプレートとして使用するマスターイメージを選択します。[マシンプロファイルを使用する] チェックボックスをオンにして、マシンプロファイルを選択できます。

   > 注:
   >
   > イメージを選択する前に、マスターイメージに VDA 2311 以降がインストールされており、VDA に MCSIO ドライバーがインストールされていることを確認します。

4. (Azure のみ) [ストレージとライセンスの種類] ページで、イメージ準備プロセスの一部として使用するストレージとライセンスの種類を選択します。

   > 注:
   >
   > [イメージ] ページでマシンプロファイルを選択すると、プロファイル設定に基づいてマシンプロファイルのライセンスの種類が事前に選択されます。

5. [マシン仕様] ページ:

   - Azure の場合は、マシンのサイズを選択します。[イメージ] ページでマシンプロファイルを選択した場合、マシンプロファイルのマシンサイズがデフォルトで選択されます。
   - VMware の場合、マシンプロファイルを選択すると、マシンプロファイルから取得された仮想 CPU 数が表示されますが、これは変更できません。マシンプロファイルを選択しない場合は、マスターイメージから取得されたメモリサイズのみが表示されます。

6. [**NIC**] ページで、準備イメージの NIC を選択または追加します。各 NIC に対して、関連付けられている仮想ネットワークを選択します。

   VMware の場合、マシンプロファイルを選択しないと、マスターイメージに関連付けられた NIC がデフォルトで選択されます。マシンプロファイルを選択した場合、NIC はマシンプロファイルから派生し、その数は変更できません。

> 注:
>
> Azure では複数の NIC はサポートされていません。

7. (Azure のみ) [ディスク設定] ページで、顧客が管理する暗号化キー (CMEK) を選択します。マシンプロファイルに CMEK が存在せず、マスターイメージに存在する場合は、マスターイメージから CMEK が事前に選択されます。
8. [バージョンの説明] ページで、作成された初期イメージバージョンの説明を入力します。
9. [概要] ページで、イメージ定義の詳細と作成された初期イメージバージョンを確認します。イメージ定義の名前と説明を入力します。[完了] をクリックします。

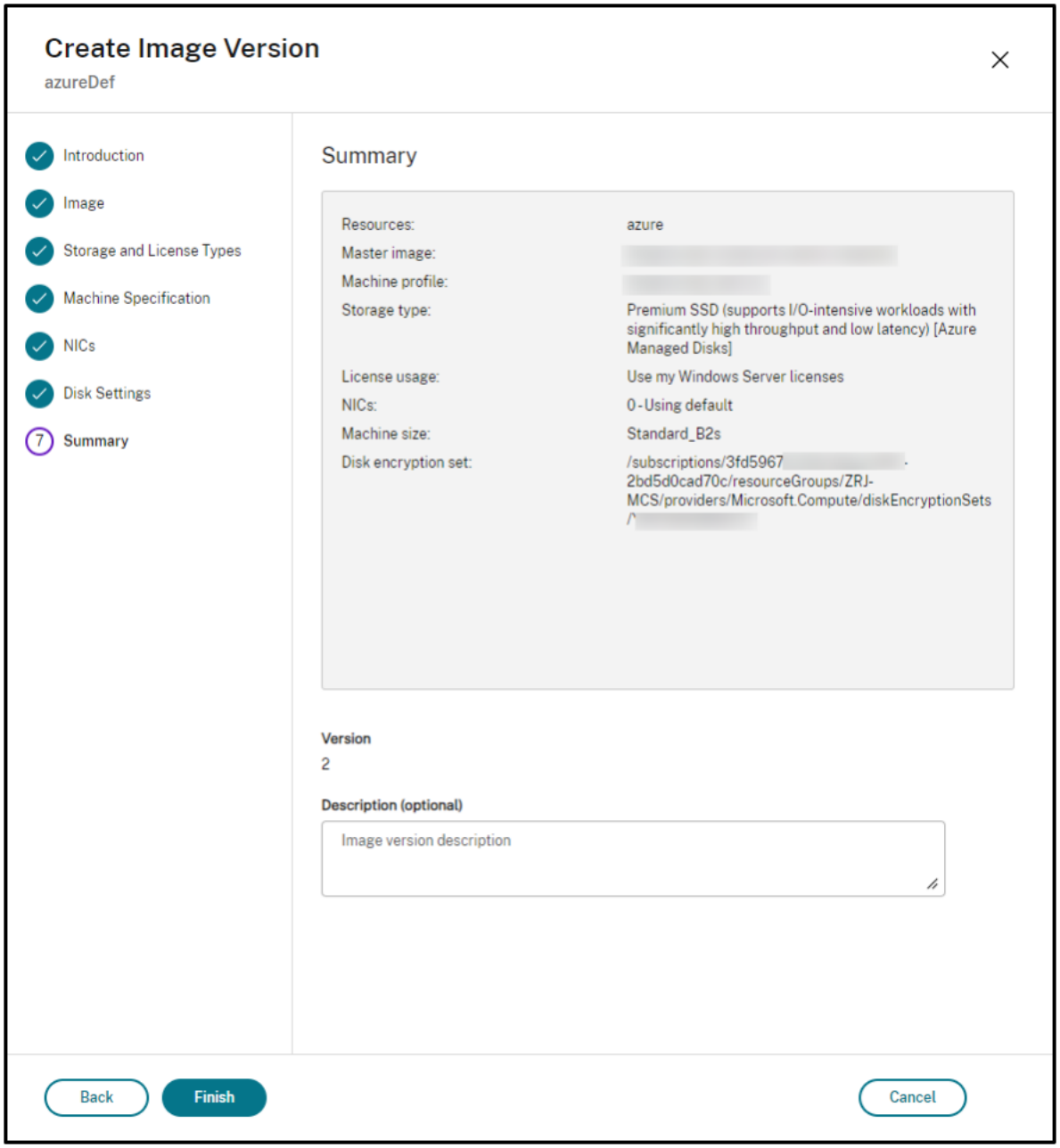
イメージバージョンを作成する

イメージバージョンを使用すると、特定のイメージに対するさまざまな反復または更新を管理できます。この機能を使用すると、さまざまな目的に合わせてイメージの複数のバージョンを維持できます。

初期イメージバージョンからイメージバージョンを作成するには、次の手順を実行します:

> 注:
>
> すべてのイメージバージョンのホスティング ユニットは同じである必要があります。

1. [イメージ] ノードに移動し、イメージバージョンを選択して、[イメージバージョンの作成] を選択します。
2. イメージバージョンの構成を初期構成のイメージバージョンと異なるものにする場合は、[イメージバージョンの作成] ダイアログの [イメージ]、[ストレージとライセンスの種類]、[マシン仕様]、[**NIC**]、および [ディスク設定] ページで設定を構成します。
3. イメージバージョンの説明を追加します。[完了] をクリックします。



イメージノードからマシンカタログを作成する

イメージバージョンを使用してカタログを作成するには、［イメージ］ノードの ［カタログの作成］オプションを使用します。

または、［マシンカタログ］ノードでカタログを作成するときにバージョンを選択し、カタログ作成ワークフローの準備済みイメージオプションにリンクすることもできます。「マシンカタログノードからマシンカタログを作成する」を参照してください

［イメージ］ノードから MCS マシンカタログを作成するには、次の手順を実行します：

1. イメージバージョンを選択し、［カタログの作成］をクリックします。［はじめに］ページで ［次へ］をクリックします。
2. ［デスクトップエクスペリエンス］ページで、必要なデスクトップエクスペリエンスを選択します。
3. ［イメージ］ページから ［ディスク設定］ページまで、選択したイメージバージョンに基づいて設定が事前に選択されます。
4. （Azure の場合）［リソースグループ］ページで、新しいリソースグループを作成するか、既存のリソースグループを使用してこのカタログのリソースを配置するかを選択できます。
5. 次のページで設定を完了します。
6. ［概要］ページで、マシンカタログの詳細を確認します。マシンカタログの名前と説明を入力します。［完了］をクリックします。
7. 作成されたマシンカタログを表示するには、［マシンカタログ］ノードに移動します。

マシンカタログノードからマシンカタログを作成する

［マシンカタログ］ノードから MCS マシンカタログを作成するには、次の手順を実行します：

1. 左側のナビゲーションペインで ［マシンカタログ］をクリックします。
2. ［マシンカタログの作成］をクリックします。［マシンカタログのセットアップ］ページが表示されます。［はじめに］、［マシンの種類］、［マシン管理］の各ページで ［次へ］をクリックします。
3. イメージ ページ：

   a) 提供されたイメージを選択します。
   b) ［準備済みイメージ］の下で、イメージ定義のイメージバージョンを選択します。
   c) イメージバージョン名をクリックします。選択したイメージバージョンの詳細を表示するには、下線が引かれたバージョン番号をクリックします。
   d) 選択したイメージバージョンがマシンプロファイルで構成されている場合は、マシンプロファイルを選択します。選択したイメージバージョンがマシンプロファイルで構成されていない場合は、マシンプロファイルの使用を選択することはできません。

4. 次のページで設定を構成します。
5. ［ディスク設定］ページで、選択した準備済みイメージがディスク暗号化セットを使用している場合、暗号化セットを削除することはできませんが、キーを別の暗号化キーに変更することはできます。
6. （Azure の場合）［リソースグループ］ページで、新しいリソースグループを作成するか、既存のリソースグループを使用してこのカタログのリソースを配置するかを選択できます。
7. 次のページで設定を完了します。
8. ［概要］ページで、マシンカタログの詳細を確認します。マシンカタログの名前と説明を入力します。［完了］をクリックします。

別の準備済みイメージでマシンカタログを更新する

既存の MCS マシンカタログを別の準備済みイメージで更新するには、次の手順を実行します：

1. 左側のナビゲーションペインで ［マシンカタログ］をクリックし、更新するマシンカタログを選択します。右クリックして ［準備済みイメージの変更］を選択します。
2. ［イメージ］ページで、準備済みイメージを選択します。
3. ［ロールアウト方法］ページで、選択した準備済みイメージを使用してこのカタログを更新するタイミングを選択します。
4. ［概要］ページで詳細を確認します。［完了］をクリックします。

カタログで行われたイメージの変更履歴を確認できます。履歴を表示するには、次の手順を実行します:

1. マシンカタログを選択してください。
2. ［テンプレートのプロパティ］タブの ［準備済みイメージ］フィールドで、［イメージの履歴を表示］をクリックします。

イメージ定義とバージョンを管理する

イメージ定義とバージョンを編集および削除して、作成されたさまざまなイメージ バージョンと定義の使用を管理できます。

イメージ定義を編集する　イメージ定義の名前と説明を編集できます。

イメージ定義を編集するには、次の手順を実行します:

1. ［イメージ］ノードに移動し、イメージ定義を選択して、［イメージ定義の編集］を選択します。

イメージバージョンの編集　イメージバージョンの説明を編集して、そのイメージバージョンの目的を指定できます。

イメージバージョンを編集するには、次の手順を実行します:

1. ［イメージ］ノードに移動し、イメージバージョンを選択して、［イメージバージョンの削除］を選択します。

イメージバージョンを削除する　イメージバージョンを削除するには、次の手順を実行します:

1. ［イメージ］ノードに移動し、イメージバージョンを選択して、［イメージバージョンの削除］を選択します。

> 注:
>
> マシンカタログで使用されているイメージバージョンは削除できません。

イメージ定義を削除する　イメージ定義を削除するには、次の手順を実行します:

1. ［イメージ］ノードに移動し、イメージ定義を選択して、［イメージ定義の削除］を選択します。

> 注:
>
> イメージ定義にイメージバージョンが含まれている場合は、そのイメージ定義を削除することはできません。

PowerShell を使用したイメージライフサイクル管理　PowerShell コマンドを使用してプロビジョニングスキームを作成する場合は、環境に応じて、マスターイメージバージョン仕様に基づいて準備済みイメージバージョン仕様を作成する必要があります。

マスターイメージバージョン仕様：マスターイメージバージョン仕様は、イメージバージョンの下に追加または作成された特定のイメージです。ハイパーバイザー内の既存のイメージをマスターイメージバージョン仕様として追加したり、環境の必要に応じてマスターイメージバージョン仕様に基づいて準備済みイメージバージョン仕様を作成したりできます。準備済みイメージバージョン仕様は、複数のプロビジョニングスキームに使用できます。

PowerShell コマンドを使用する場合のイメージのライフサイクルは次のとおりです：

1. イメージを作成します：
    a) イメージ定義を作成します。
    b) イメージバージョンを作成します。
    c) マスターイメージバージョン仕様を追加します。
    d) 準備済みイメージバージョン仕様を作成します。
2. 準備済みイメージバージョン仕様を使用して MCS マシンカタログを作成します：
    a) ブローカーカタログを作成します。
    b) ID プールを作成します。
    c) `New-ProvScheme`コマンドを使用して、準備済みイメージバージョン仕様の UID のパラメーターを指定してプロビジョニングスキームを作成します。
    d) ブローカーカタログをプロビジョニングスキームにリンクします。
3. MCS マシンカタログで VM を作成します。
4. `Set-ProvScheme`コマンドを使用して、プロビジョニングスキームの準備済みイメージバージョン仕様を変更します。
5. イメージ定義とバージョンの管理：イメージバージョンとイメージ定義を編集します。
6. MCS マシンカタログの削除：削除の順序は次のとおりです。準備済みイメージバージョン仕様 > マスターイメージバージョン仕様 > イメージバージョン > イメージ定義。イメージバージョン使用の削除前に、準備済みイメージバージョン仕様がどの MCS マシンカタログにも関連付けられていないことを確認してください。

PowerShell の使用

PowerShell コマンドを使用して次の操作を実行できます：

- 準備済みイメージを作成する
- 準備済みイメージバージョン仕様を使用してカタログを作成する
- 準備済みイメージバージョン仕様を使用してカタログを更新する
- イメージ定義、イメージバージョン、準備済みイメージバージョン仕様を削除する
- イメージ定義とイメージバージョンを管理する
- イメージ定義、イメージバージョン、準備済みイメージバージョン仕様、プロビジョニングスキームの詳細を取得する

準備済みイメージを作成する

準備済みイメージ バージョン仕様を作成するための詳細な PowerShell コマンドは次のとおりです:

1. `Test-ProvImageDefinitionNameAvailable command`を使用して使用可能なイメージ定義名を確認します。たとえば、

```
Test-ProvImageDefinitionNameAvailable -ImageDefinitionName <string
    []>
```

2. `New-ProvImageDefinition`コマンドを使用してイメージ定義を作成します。たとえば、

```
New-ProvImageDefinition -ImageDefinitionName image1 -OsType
    Windows -VdaSessionSupport MultiSession
```

3. `New-ProvImageVersion`コマンドを使用してイメージバージョンを作成します。たとえば、

```
New-ProvImageVersion -ImageDefinitionName image1 -Description "
    version 1"
```

4. `Add-ProvImageVersionSpec`コマンドを使用して、イメージバージョンにマスターイメージバージョン仕様を追加します。たとえば、

```
Add-ProvImageVersionSpec -ImageDefinitionName  image1  -
    ImageVersionNumber  1 -HostingUnitName azure -MasterImagePath "
    XDHyp:\HostingUnits\azure\image.folder\azureresourcegroup.
    resourcegroup\win2022-snapshot.snapshot"
```

> 注:
>
> ホスティングユニットの 1 つのイメージバージョンに追加できるマスターイメージバージョン仕様は、1 つだけです。

5. `New-ProvImageVersionSpec`コマンドを使用して、マスターイメージバージョン仕様から準備済みイメージ バージョン仕様を作成します。たとえば、


```
New-ProvImageVersionSpec
-SourceImageVersionSpecUid  c6e7384c-b2f8-46d6-9519-29a2c57ed3cb
-NetworkMapping @{
 "0"="XDHyp:\HostingUnits\azure\virtualprivatecloud.folder\
    azureresourcegroup.resourcegroup\azure-vnet-eastus.
    virtualprivatecloud\dev.network"
-ServiceOffering "XDHyp:\HostingUnits\azure\serviceoffering.folder
    \Standard_B2ms.serviceoffering" -CustomProperties "<
    CustomProperties xmlns=`"http://schemas.citrix.com/2014/xd/
    machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
    instance`"></CustomProperties>" -RunAsynchronously
```

> 注:
>
> 1 つのホスティングユニットと準備タイプには、準備済みインスタンスを 1 つだけ含めることができます。

Azure でイメージ定義、イメージバージョン、準備済みイメージバージョン仕様を作成するための **Powershell** コマンドの完全なセットの例:

```
$ImageDefintion = New-ProvImageDefinition
-ImageDefinitionName image1 -OsType Windows -VdaSessionSupport
    MultiSession
 $ImageVersion = New-ProvImageVersion -ImageDefinitionName
    $ImageDefintion.ImageDefinitionName -Description "version 1"
$MasterImagePath = "XDHyp:\HostingUnits\azure\image.folder\
    azureresourcegroup.resourcegroup\win2022-snapshot.snapshot"
$SourceImageVersionSpec = Add-ProvImageVersionSpec -ImageDefinitionName
    $ImageVersion.ImageDefinitionName -ImageVersionNumber $ImageVersion
    .ImageVersionNumber -HostingUnitName azure -MasterImagePath
    $MasterImagePath
$Task = New-ProvImageVersionSpec -SourceImageVersionSpecUid
    $SourceImageVersionSpec.ImageVersionSpecUid -NetworkMapping @{
 "0"="XDHyp:\HostingUnits\azure\virtualprivatecloud.folder\
    azureresourcegroup.resourcegroup\azure-vnet-eastus.
    virtualprivatecloud\dev.network" }
  -ServiceOffering "XDHyp:\HostingUnits\azure\serviceoffering.folder\
    Standard_B2ms.serviceoffering" -CustomProperties "<
    CustomProperties xmlns=`"http://schemas.citrix.com/2014/xd/
    machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
    instance`"></CustomProperties>" -RunAsynchronously
Get-ProvTask -TaskId $Task.TaskId
```

VMware でイメージ定義、イメージバージョン、準備済みイメージバージョン仕様を作成するための **Powershell** コマンドの完全なセットの例:

```
$ImageDefintion = New-ProvImageDefinition -ImageDefinitionName image2 -
    OsType Windows -VdaSessionSupport SingleSession
$ImageVersion = New-ProvImageVersion -ImageDefinitionName
    $ImageDefintion.ImageDefinitionName -Description "version 1"
$MasterImagePath = "XDHyp:\HostingUnits\vmware\win10-master.vm\win10-
    master-snap.snapshot"
```



```
$SourceImageVersionSpec = Add-ProvImageVersionSpec -ImageDefinitionName
    $ImageVersion.ImageDefinitionName -ImageVersionNumber $ImageVersion
    .ImageVersionNumber -HostingUnitName vmware -MasterImagePath
    $MasterImagePath
$Task = New-ProvImageVersionSpec -SourceImageVersionSpecUid
    $SourceImageVersionSpec.ImageVersionSpecUid -NetworkMapping @{
 "0"="XDHyp:\HostingUnits\vmware\DSwitch-VM Network.network" }
  -VMCpuCount 2 -VMMemoryMB 4096 -RunAsynchronously
Get-ProvTask -TaskId $Task.TaskId
```

注:

- イメージ定義内のすべてのイメージバージョン仕様は、同じホスティングユニットに属している必要があります。
- イメージバージョンには、マスターイメージバージョン仕様を 1 つと準備済みイメージバージョン仕様を 1 つだけ含めることができます。
- すべてのイメージバージョン仕様にマシンプロファイルが存在するか、またはどのイメージバージョン仕様にもマシンプロファイルが存在しないようにする必要があります。
- イメージバージョン仕様を作成するときにリソースグループを指定することはできません。

準備済みイメージバージョン仕様を使用してカタログを作成する

New-ProvSchemeコマンドを使用して、準備済みイメージバージョン仕様から MCS マシンカタログを作成します。たとえば、

```
New-ProvScheme -ProvisioningSchemeName <string> -ImageVersionSpecUid <
    Guid> -HostingUnitUid <Guid> -IdentityPoolUid <Guid> [-VMCpuCount <
    int>] [-VMMemoryMB <int>] [-UseWriteBackCache] [-NetworkMapping <
    Hashtable>] [-CleanOnBoot] [-Scope <string[]>] [-Metadata <Hashtable
    >] [-ServiceOffering <string>] [-SecurityGroup <string[]>] [-
    TenancyType <string>] [-MachineProfile <string>] [-CustomProperties
    <string>] [-ResetAdministratorPasswords] [-
    UseFullDiskCloneProvisioning] [-RunAsynchronously] [-
    PurgeJobOnSuccess] [-ProvisioningSchemeType <ProvisioningSchemeType
    >]
```

または、

```
New-ProvScheme -ProvisioningSchemeName <string> -ImageVersionSpecUid <
    Guid> -HostingUnitName <string> -IdentityPoolName <string> [-
    VMCpuCount <int>] [-VMMemoryMB <int>] [-UseWriteBackCache] [-
    NetworkMapping <Hashtable>] [-CleanOnBoot] [-Scope <string[]>] [-
    Metadata <Hashtable>] [-ServiceOffering <string>] [-SecurityGroup <
    string[]>] [-TenancyType <string>] [-MachineProfile <string>] [-
    CustomProperties <string>] [-ResetAdministratorPasswords] [-
    UseFullDiskCloneProvisioning] [-RunAsynchronously] [-
    PurgeJobOnSuccess] [-ProvisioningSchemeType <ProvisioningSchemeType
    >]
```


Azure でカタログを作成するための **Powershell** コマンドの完全なセットの例:

```
$Catalog = New-BrokerCatalog  -AllocationType "Random"  -IsRemotePC $False  -MinimumFunctionalLevel "L7_20" -Name "azurecatalog" -PersistUserChanges "Discard" -ProvisioningType "MCS" -Scope @() -SessionSupport "MultiSession"
$IdentityPool = New-AcctIdentityPool  -AllowUnicode  -Domain "azure.local" -IdentityPoolName "azurecatalog" -IdentityType "ActiveDirectory"  -NamingScheme "azure##" -NamingSchemeType "Numeric" -Scope @()
$PreparedImageVersionSpec = Get-ProvImageVersionSpec -ImageDefinitionName image1 -ImageVersionNumber 1 -Filter "PreparationType -eq 'Mcs'"
$Task = New-ProvScheme -ProvisioningSchemeName azurecatalog -ImageVersionSpecUid $PreparedImageVersionSpec.ImageVersionSpecUid -HostingUnitName azure -IdentityPoolName azurecatalog -CleanOnBoot -Scope @() -SecurityGroup @() -ServiceOffering "XDHyp:\HostingUnits\azure\serviceoffering.folder\Standard_B2s.serviceoffering" -NetworkMapping @{
 "0"="XDHyp:\HostingUnits\azure\virtualprivatecloud.folder\azureresourcegroup.resourcegroup\azure-vnet-eastus.virtualprivatecloud\dev.network" }
  -CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com/2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-instance`"><Property xsi:type=`"StringProperty`" Name=`"StorageAccountType`" Value=`"StandardSSD_LRS`" /></CustomProperties>" -RunAsynchronously
Get-ProvTask -TaskId $Task.TaskId
$ProvScheme = Get-ProvScheme -ProvisioningSchemeName azurecatalog
Set-BrokerCatalog -Name $Catalog.Name -ProvisioningSchemeId $ProvScheme.ProvisioningSchemeUid
```

VMware でカタログを作成するための **Powershell** コマンドの完全なセットの例:

```
$Catalog = New-BrokerCatalog  -AllocationType "Random"  -IsRemotePC $False  -MinimumFunctionalLevel "L7_20" -Name "vmwarecatalog" -PersistUserChanges "Discard" -ProvisioningType "MCS" -Scope @() -SessionSupport "MultiSession"
$IdentityPool = New-AcctIdentityPool  -AllowUnicode  -Domain "vmware.local" -IdentityPoolName "vmwarecatalog" -IdentityType "ActiveDirectory"  -NamingScheme "vmware##" -NamingSchemeType "Numeric" -Scope @()
$PreparedImageVersionSpec = Get-ProvImageVersionSpec -ImageDefinitionName image2 -ImageVersionNumber 1 -Filter "PreparationType -eq 'Mcs'"
$Task = New-ProvScheme -ProvisioningSchemeName vmwarecatalog -ImageVersionSpecUid $PreparedImageVersionSpec.ImageVersionSpecUid -HostingUnitName vmware -IdentityPoolName vmwarecatalog -CleanOnBoot -Scope @() -SecurityGroup @() -NetworkMapping @{
 "0"="XDHyp:\HostingUnits\vmware\DSwitch-VM Network.network" }
  -VMCpuCount 2 -VMMemoryMB 4096 -RunAsynchronously
Get-ProvTask -TaskId $Task.TaskId
$ProvScheme = Get-ProvScheme -ProvisioningSchemeName vmwarecatalog
Set-BrokerCatalog -Name $Catalog.Name -ProvisioningSchemeId $ProvScheme
```



```
        .ProvisioningSchemeUid
```

準備済みイメージバージョン仕様を使用してカタログを更新する

Set-ProvSchemeImageコマンドを使用してカタログを更新できます。たとえば、

```
1 Set-ProvSchemeImage -ProvisioningSchemeUid <Guid> -ImageVersionSpecUid
      <Guid> [-DoNotStoreOldImage] [-RunAsynchronously] [-
      PurgeJobOnSuccess]
```

または、

```
1 Set-ProvSchemeImage -ProvisioningSchemeName <string> -
      ImageVersionSpecUid <Guid> [-DoNotStoreOldImage] [-RunAsynchronously
      ] [-PurgeJobOnSuccess]
```

カタログを更新するための **Powershell** コマンドの完全なセットの例:

```
1 $PreparedImageVersionSpec = Get-ProvImageVersionSpec -
      ImageDefinitionName image1 -ImageVersionNumber 2 -Filter "
      PreparationType -eq 'Mcs'"
2 Set-ProvSchemeImage -ProvisioningSchemeName azurecatalog -
      ImageVersionSpecUid $PreparedImageVersionSpec.ImageVersionSpecUid -
      RunAsynchronously
```

イメージ定義、イメージバージョン、準備済みイメージバージョン仕様を削除する

イメージ定義、イメージバージョン、準備済みイメージバージョン仕様を削除する前に、次の点を考慮してください:

- イメージ定義にイメージバージョンが含まれている場合、そのイメージ定義は削除できません。
- イメージバージョン仕様が含まれている場合、イメージバージョンを削除することはできません。
- マスターイメージバージョン仕様は、他の準備済みイメージバージョン仕様によって使用されている場合は削除できません。
- 準備済みイメージバージョン仕様は、プロビジョニングスキームによって使用されている場合は削除できません。

詳細な手順は次のとおりです:

1. 準備済みイメージ バージョン仕様を削除します。たとえば、

   ```
   1 $PreparedImageVersionSpec = Get-ProvImageVersionSpec -
         ImageDefinitionName image1 -ImageVersionNumber 1 -Filter "
         PreparationType -eq 'Mcs'"
   2 Remove-ProvImageVersionSpec -ImageVersionSpecUid
         $PreparedImageVersionSpec.ImageVersionSpecUid -
         RunAsynchronously
   ```


> 注:
>
> マスターイメージバージョン仕様は、関連付けられている準備済みイメージバージョン仕様がない場合にのみ削除できます。

2. マスターイメージバージョン仕様を削除します。たとえば、

```
$MasterImageVersionSpec = Get-ProvImageVersionSpec -
    ImageDefinitionName image1 -ImageVersionNumber 1 -Filter "
    PreparationType -eq 'None'"
Remove-ProvImageVersionSpec -ImageVersionSpecUid
    $PreparedImageVersionSpec.ImageVersionSpecUid -
    RunAsynchronously
```

3. イメージバージョンを削除します。たとえば、

```
Remove-ProvImageVersion -ImageDefinitionName image1 -
    ImageVersionNumber 1
```

4. イメージ定義を削除します。たとえば、

```
Remove-ProvImageDefinition -ImageDefinitionName image1
```

PowerShell コマンドの完全なセットの例:

```
$PreparedImageVersionSpec = Get-ProvImageVersionSpec -
    ImageDefinitionName image1 -ImageVersionNumber 1 -Filter "
    PreparationType -eq 'Mcs'"
$Task = Remove-ProvImageVersionSpec -ImageVersionSpecUid
    $PreparedImageVersionSpec.ImageVersionSpecUid -RunAsynchronously
$MasterImageVersionSpec = Get-ProvImageVersionSpec -ImageDefinitionName
    image1 -ImageVersionNumber 1 -Filter "PreparationType -eq 'None'"
$Task = Remove-ProvImageVersionSpec -ImageVersionSpecUid
    $PreparedImageVersionSpec.ImageVersionSpecUid -RunAsynchronously
Remove-ProvImageVersion -ImageDefinitionName image1 -ImageVersionNumber
    1
Remove-ProvImageDefinition -ImageDefinitionName image1
```

イメージ定義とイメージバージョンを管理する

イメージ定義の名前変更や編集、イメージバージョンの編集を実行できます。

- `Rename-ProvImageDefinition`コマンドを使用してイメージ定義の名前を変更します。例:

```
Rename-ProvImageDefinition -ImageDefinitionUid <Guid> -
    NewImageDefinitionName <string>
```

または、


```
Rename-ProvImageDefinition -ImageDefinitionName <string> -
    NewImageDefinitionName <string>
```

- Set-ProvImageDefinitionコマンドを使用してイメージ定義を編集します。例:

```
Set-ProvImageDefinition -ImageDefinitionUid <Guid> [-Description
    <string>]
```

または、

```
Set-ProvImageDefinition -ImageDefinitionName <string> [-
    Description <string>]
```

- Set-ProvImageVersionコマンドを使用してイメージバージョンを編集します。例:

```
Set-ProvImageVersion -ImageVersionUid <Guid> [-Description <
    string>]
```

または、

```
Set-ProvImageVersion -ImageDefinitionName <string> -
    ImageVersionNumber <int> [-Description <string>]
```

イメージ定義、イメージバージョン、準備済みイメージバージョン仕様、プロビジョニングスキームの詳細を取得する

- Get-ProvImageDefinitionコマンドを使用してイメージ定義の詳細を取得します。例:

```
Get-ProvImageDefinition [-ImageDefinitionName <string>] [-
    ImageDefinitionUid <Guid>] [-ReturnTotalRecordCount] [-
    MaxRecordCount <int>] [-Skip <int>] [-SortBy <string>] [-
    Filter <string>]
```

- Get-ProvImageVersionコマンドを使用してイメージバージョンの詳細を取得します。例:
  - イメージ定義でイメージバージョンを一覧表示する場合、

    ```
    Get-ProvImageVersion -ImageDefinitionUid <Guid>
    ```

    または、

    ```
    Get-ProvImageVersion -ImageDefinitionName <string>
    ```

  - イメージバージョンの詳細を取得する場合、

    ```
    Get-ProvImageVersion -ImageVersionUid <Guid>
    ```

    または、

    ```
    Get-ProvImageVersion -ImageDefinitionName <string> -
        ImageVersionNumber <int>
    ```


- Get-ProvImageVersionSpecコマンドを使用して、準備済みイメージバージョン仕様を取得します。例:
  - イメージバージョンで準備されたすべてのイメージバージョン仕様を一覧表示する場合、

```
Get-ProvImageVersionSpec -ImageVersionUid <Guid>
```

  - 準備済みイメージバージョン仕様でマスターイメージバージョン仕様を一覧表示する場合、

```
Get-ProvImageVersionSpec -ImageVersionUid <Guid> -Filter '
    PreparationType -eq "None"'
```

  - マスターイメージに関連付けられたイメージバージョンに準備済みイメージバージョン仕様を一覧表示する場合、

```
Get-ProvImageVersionSpec -ImageVersionUid <Guid> -Filter '
    PreparationType -eq "MCS" -and SourceImageVersionSpecUid -
    eq "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"'
```

  - イメージバージョンで準備済みイメージバージョン仕様を正常に取得する場合、

```
Get-ProvImageVersionSpec -ImageVersionUid <Guid> -Filter '
    PreparationType -eq "MCS" -and SourceImageVersionSpecUid -
    eq "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" -and
    ImageVersionSpecStatus -eq "Complete"'
```

  - 準備済みイメージバージョン仕様の詳細を取得する場合、

```
Get-ProvImageVersionSpec -ImageVersionSpecUid <Guid>
```

- Get-ProvSchemeコマンドを使用してプロビジョニング スキームの詳細を取得します。例:

```
Get-ProvScheme [[-ProvisioningSchemeName] <String>] [-
    ProvisioningSchemeUid <Guid>] [-ScopeId <Guid>] [-ScopeName <
    String>] [-ReturnTotalRecordCount] [-MaxRecordCount <Int32>]
    [-Skip <Int32>] [-SortBy <String>] [-Filter <String>] [-
    FilterScope <Guid>]
```

- Get-ProvSchemeImageVersionSpecHistoryコマンドを使用して、プロビジョニングスキームの準備済みイメージバージョン仕様の履歴を取得します。例:

```
Get-ProvSchemeImageVersionSpecHistory [-ProvisioningSchemeName <
    String>] [-ProvisioningSchemeUid <Guid>] [-ImageVersionSpecUid
     <Guid>] [-ImageVersionSpecHistoryUid <Guid>] [-
    ReturnTotalRecordCount] [-MaxRecordCount <Int32>] [-Skip <
    Int32>] [-SortBy <String>] [-Filter <String>] [-FilterScope <
    Guid>]
```


マシンカタログの作成

August 20, 2024

> 重要:
>
> Citrix Virtual Apps and Desktops 7 2006 では、現在の展開で次のテクノロジのいずれかを使用している場合、これらのテクノロジを使用する製品終了（EOL）アイテムを削除した後でのみ、展開を現在のリリースにアップグレードできます。
>
> - Personal vDisk（PvD）
> - AppDisk
> - パブリッククラウドのホストタイプ：Citrix CloudPlatform、Microsoft Azure Classic
>
> 詳しくは、「PvD、AppDisk、およびサポートされていないホストの削除」を参照してください。
>
> 注:
>
> Web Studio（Web ベース）と Citrix Studio（Windows ベース）の 2 つの管理コンソールを使用して、Citrix Virtual Apps and Desktops の展開を管理できます。この記事では Web Studio のみを扱います。Citrix Studio について詳しくは、Citrix Virtual Apps and Desktops 7 2212 以前の同様の記事を参照してください。

展開環境に対してパブリッククラウドホスト接続を使用する場合、新規インストールを完了する、または最新リリースにアップグレードするのに、ハイブリッド権利ライセンスが必要です。

1 つまたは複数のサポートされていないテクノロジ、またはハイブリッド権利ライセンスがないホスト接続をインストーラーが検出すると、アップグレードが一時停止または停止します。説明メッセージが表示されます。インストーラーログに詳細が記載されています。詳しくは、「環境のアップグレード」を参照してください。

はじめに

物理マシンまたは仮想マシンのグループは、「マシンカタログ」と呼ばれる単一のエンティティとして管理されます。カタログ内のすべてのマシンには、同じ種類のオペレーティングシステム（マルチセッション OS またはシングルセッション OS、Windows マシンまたは Linux マシン）がインストールされています。

サイトを作成した後、Web Studio では最初のマシンカタログを作成する手順が表示されます。最初のカタログを作成した後、Web Studio では最初のデリバリーグループを作成する手順が表示されます。作成したカタログを後で変更したり、追加のカタログを作成したりすることができます。

> ヒント:
>
> Machine Creation Services（MCS）のストレージ最適化（MCS I/O）機能を有効にする既存の展開をアップグレードする場合、追加の構成は必要ありません。Virtual Delivery Agent（VDA）および Delivery

> Controller アップグレードにより、MCS I/O アップグレードが処理されます。

概要

仮想マシンのカタログの作成時には、それらの仮想マシンのプロビジョニング方法を指定します。Machine Creation Services（MCS）を使用できます。または、独自のツールを使用してマシンをプロビジョニングすることもできます。

次の点を考慮してください：

- MCS は、仮想マシンイメージから 1 つのシステムディスクをサポートします。このイメージに接続されている残りのデータディスクは無視されます。
- MCS を使用して仮想マシンをプロビジョニングする場合、カタログ内に同じ仮想マシンを作成するためのマスターイメージ（またはイメージのスナップショット）を提供します。カタログを作成する前に、ツールを使用してマスターイメージを作成し、構成します。この処理には、イメージへの Virtual Delivery Agent（VDA）のインストールが含まれます。その後、Web Studio でマシンカタログを作成します。そのイメージ（またはスナップショット）を選択し、カタログで作成する仮想マシンの数を指定して、追加情報を構成します。
- マシンが既に提供されている場合でも、マシンに対して 1 つまたは複数のマシンカタログを作成する必要があります。
- PowerShell SDK を使用してカタログを直接作成する場合、イメージまたはそのスナップショットの代わりに、ハイパーバイザーテンプレート（**VMTemplates**）を指定できます。
- テンプレートを使用したカタログのプロビジョニングは、試験段階の機能と見なされています。この方法を使用すると、仮想マシンの準備に失敗する場合があります。そのため、テンプレートを使用してカタログを公開することができなくなります。

MCS または Citrix Provisioning を使用して最初のカタログを作成する場合、サイトの作成時に構成したホスト接続を使用します。後で（最初のマシンカタログおよびデリバリーグループを作成した後に）、その接続に関する情報を変更したり、追加接続を作成したりすることができます。

カタログの作成ウィザードを完了すると、テストが自動的に実行され、正しく構成されているかどうかが検証されます。テストが完了したら、テストレポートを表示できます。Web Studio からテストをいつでも実行できます。

> 注：
>
> MCS では、Windows 10 IoT Core および Windows 10 IoT Enterprise はサポートされていません。詳しくは、Microsoft 社のサイトを参照してください。

Citrix Provisioning ツールの技術的な詳細については、「Citrix Virtual Apps and Desktops のイメージ管理」を参照してください。

RDS ライセンスチェック

Citrix Studio は現在、Windows マルチセッション OS マシンが含まれるマシンカタログの作成時に Microsoft RDS ライセンスの有効性をチェックしません。Windows マルチセッション **OS** マシン用の Microsoft RDS ライセ

ンスの状態を確認するには、Citrix Director にアクセスしてください。［マシンの詳細］パネルで、Microsoft RDS（Remote Desktop Services）ライセンスの状態を表示します。このパネルは、［マシンの詳細とユーザーの詳細］ページにあります。詳しくは、「Microsoft RDS ライセンスの正常性」を参照してください。

VDA 登録

仲介セッションを起動する場合、Delivery Controller に VDA が登録されている必要があります。VDA が登録されていないと、登録されていれば使用されるはずの資源が使用されない場合があります。VDA が登録されない理由はさまざまですが、その多くは管理者がトラブルシューティングできます。Web Studio では、カタログ作成ウィザードで、マシンをカタログからデリバリーグループに登録した後に、トラブルシューティング情報が提供されます。

ウィザードを使用して既存のマシンを追加すると、コンピューターアカウント名の一覧に、各マシンがカタログに追加するのに適しているかどうかが示されます。各マシンの横にあるアイコンにマウスを合わせると、そのマシンに関する情報メッセージが表示されます。

メッセージで問題のあるマシンが示された場合は、該当のマシンを削除するか、マシンを追加します。たとえば、マシンに関する情報を取得できない可能性があることを示すメッセージが表示された場合でも、そのマシンを追加します。

詳しくは、次のトピックを参照してください:

- CTX136668: VDA 登録のトラブルシューティングガイダンス
- VDA バージョンと機能レベル
- VDA の登録方法

MCS カタログ作成の概要

以下は、カタログの作成ウィザードに情報を入力した後のデフォルトの MCS 操作の簡単な概要です。

- （スナップショットではなく）マスターイメージを選択した場合、MCS でスナップショットが作成されます。
- MCS でスナップショットの完全コピーが作成され、ホスト接続で定義されたストレージの各場所に格納されます。
- MCS によってマシンが Active Directory に追加され、そこで一意の識別子が作成されます。
- ウィザードで指定した数の仮想マシンが MCS によって作成され、各仮想マシンに対して 2 つのディスクが定義されます。1 つの仮想マシンにつき 2 つのディスクに加えて、同じストレージの場所にマスターも保存されます。ストレージの場所が複数定義されている場合、それぞれの場所に以下の種類のディスクが割り当てられます。
  - スナップショットの完全コピー。読み取り専用であり、作成した仮想マシン間で共有されます。
  - 各仮想マシンに一意の識別子を与える、一意の ID ディスク（16MB）。各仮想マシンに対し、1 つの ID ディスクが割り当てられます。

  - 仮想マシンへの書き込みを保存する、一意の差分ディスク。このディスクは（ホストストレージでサポートされている場合）シンプロビジョニングされ、必要に応じてマスターイメージの最大サイズまで拡大します。各仮想マシンに対し、1 つの差分ディスクが割り当てられます。差分ディスクには、セッション中に加えられた変更が保存されます。専用デスクトップの場合、この変更は無期限に保存されます。プールデスクトップの場合、Delivery Controller によって再起動のたびにこの変更は削除され、新しい変更が作成されます。

または、仮想マシンを作成して静的デスクトップを配信する場合、（カタログの作成ウィザードの ［マシン］ページで）シックな（完全なコピーの）仮想マシンのクローンを指定できます。完全なクローンでは、すべてのデータストアにマスターイメージを保持する必要はありません。各仮想マシンに独自のファイルが存在します。

Machine Creation Services のストレージの考慮事項

Machine Creation Services（MCS）のストレージソリューション、構成、容量を決定する際には、多くの要因があります。以下に、適切なストレージ容量を決定するための考慮事項を示します:

容量に関する考慮事項:

- ディスク

  ほとんどの MCS 環境において、デルタ（差分）ディスクが各 VM の容量を一番多く占めます。MCS により作成される仮想マシンには、作成時にディスクが 2 つ以上割り当てられます。

  - ディスク 0 = 差分ディスク：マスター基本イメージからコピーした OS が含まれます。
  - ディスク 1 = ID ディスク：16MB - 各仮想マシンの Active Directory データが含まれます。

  製品の進化にともない、特定のユースケースや機能の消費容量に合わせたディスクの追加が必要になることがあります。例:

  - MCS ストレージ最適化では、仮想マシンごとに書き込みキャッシュ形式のディスクが作成されます。
  - 前述のデルタディスクの使用例とは対照的に、MCS には、完全なクローンを使用する機能が追加されています。

  Hypervisor の機能も、こうした要因になることがあります。例:

  - XenServer IntelliCacheは、各 XenServer のローカルストレージ上に読み取りディスクを作成します。このオプションはマスターイメージに対する IOPS を保存します。このマスターイメージは、共有ストレージの場所に保存することもできます。

- ハイパーバイザーのオーバーヘッド

  ハイパーバイザーごとに固有のファイルを使用するため、このファイルが仮想マシンのオーバーヘッドとなります。ハイパーバイザーは、管理操作および一般的なログ記録でストレージを使用します。容量は、以下のオーバーヘッドを考慮して計算してください:

  - ログファイル

  - ハイパーバイザー固有のファイル。例:
    * VMware により、**VM storage** フォルダーにファイルが追加されます。VMware のベストプラクティスを参照してください。
    * 仮想マシン全体で必要なサイズを計算してください。たとえば、仮想ディスクに 20GB、スワップファイルに 16GB、ログファイルに 100MB を使用している仮想マシンでは、合計で 36.1GB を消費することを考慮に入れます。
  - XenServer のスナップショットおよびVMware のスナップショット。

- プロセスのオーバーヘッド

  カタログの作成と更新、およびマシンの追加を行なうと、それぞれ以下のようにストレージに影響が及びます。例:

  - カタログを初めて作成する場合、各ストレージの場所に基本ディスクをコピーする必要があります。
    * また、一時的に準備用の仮想マシンを作成する必要もあります。
  - カタログにマシンを追加する場合は、各ストレージの場所に基本ディスクをコピーする必要はありません。ただし、カタログの作成方法は、選択した機能によって異なります。
  - カタログを更新して、ストレージの場所ごとに基本ディスクを追加で作成します。また、カタログに含まれる仮想マシンに一定期間にわたって 2 つの差分ディスクが割り当てられるため、一時的にストレージ占有量が急増することになります。

そのほかの考慮事項:

- **RAM** のサイズ設定: I/O 最適化ディスク、書き込みキャッシュ、スナップショットファイルなど、特定のハイパーバイザーファイルとディスクのサイズに影響します。
- シン/シックプロビジョニング: シンプロビジョニング機能を備えているため、NFS ストレージが推奨されます。

Machine Creation Services（**MCS**）ストレージ最適化

MCS I/O と呼ばれる Machine Creation Services（MCS）ストレージの最適化機能の特徴:

- 書き込みキャッシュコンテナは、Citrix Provisioning と同様にファイルベースです。たとえば、Citrix Provisioning の書き込みキャッシュのファイル名は「`D:\vdiskdif.vhdx`」、MCS I/O 書き込みキャッシュのファイル名は「`D:\mcsdif.vhdx`」です。
- 書き込みキャッシュディスクへの Windows クラッシュダンプファイルの書き込みをサポートするなどの方法によって、診断機能が向上します。
- MCS I/O は、引き続きハードディスクへのオーバーフローありで *RAM* にキャッシュするテクノロジを利用して、複数層の書き込みキャッシュに関して最適なソリューションを提供します。この機能により、管理者は各層のコスト、RAM とディスク、パフォーマンスのバランスを取りながら、必要なワークロードに対応できます。

書き込みキャッシュの方法をディスクベースからファイルベースに更新するには、以下の変更が必要です:

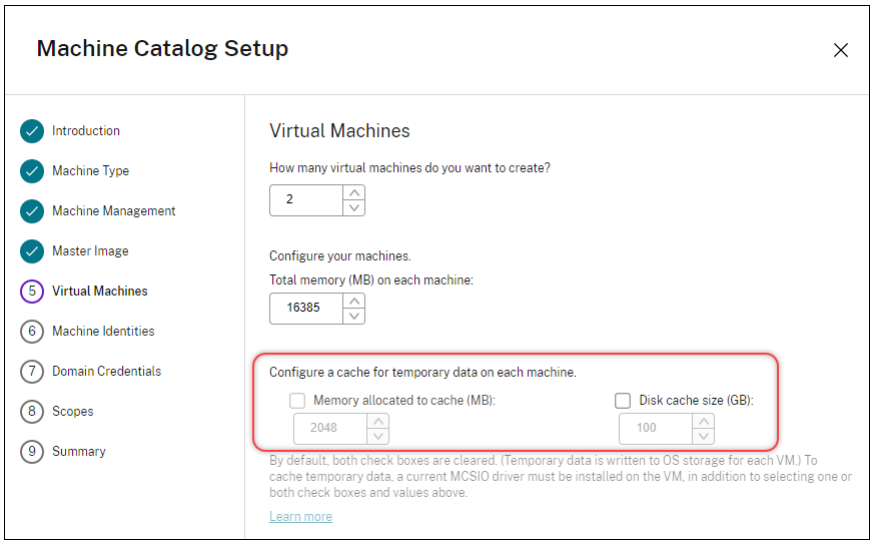
1. MCS I/O では、RAM のみのキャッシュはサポートされなくなります。マシンカタログの作成中に Web Studio でディスクサイズを指定します。
2. 仮想マシンの初回起動時に、書き込みキャッシュディスクが自動的に作成およびフォーマットされます。仮想マシンが起動すると、書き込みキャッシュファイル`mcsdif.vhdx`はフォーマット済みボリューム`MCSWCDisk`に書き込まれます。
3. ページファイルは、このフォーマットされたボリュームの`MCSWCDisk`にリダイレクトされます。その結果、このディスクサイズはディスクスペースの合計を考慮します。これには、ディスクサイズと生成されたワークロードの差分、およびページファイルサイズが含まれます。これは通常、VM RAM サイズに関連しています。

MCS ストレージ最適化の更新を有効にする　MCS I/O ストレージ最適化機能を有効にするには、Delivery Controller と VDA を最新バージョンの Citrix Virtual Apps and Desktops にアップグレードします。

> 注:
>
> MCS I/O が有効化された既存の環境をアップグレードする場合、追加の構成は必要ありません。VDA および Delivery Controller アップグレードにより、MCS I/O アップグレードが処理されます。

MCS ストレージ最適化の更新を有効にするときは、次の点を考慮してください:

- マシンカタログを作成するとき、管理者は RAM とディスクサイズを構成できます。



- 既存のマシンカタログを、バージョン 1903 の VDA を含む新しい仮想マシンスナップショットに更新すると、その新しいスナップショットは、RAM とディスクサイズに関する既存のカタログの MCS I/O 設定を引き続き使用します。既存の未フォーマットディスクはフォーマットされます。

> 重要:
>
> MCS ストレージ最適化は、Citrix Virtual Apps and Desktops バージョン 1903 で変更されました。このリ

> リースでは、ファイルベースの書き込みキャッシュテクノロジがサポートされ、パフォーマンスと安定性が向上しています。MCS I/O で提供される新機能は、Citrix Virtual Apps and Desktops の過去のリリースと比較して、より高い書き込みキャッシュストレージ要件が必要になることがあります。割り当てられたワークフローと追加のページファイル用の十分なディスク領域があることを確認するために、ディスクサイズを再評価することをお勧めします。ページファイルのサイズは通常、システム RAM の容量に関連しています。既存のカタログのディスクサイズが不十分な場合は、マシンカタログを作成し、より大きな書き込みキャッシュディスクを割り当ててください。

MCS I/O ライトバックキャッシュディスクへの特定のドライブ文字の割り当て

MCS I/O ライトバックキャッシュディスクに特定のドライブ文字を割り当てることができます。この機能の導入は、使用するアプリケーションのドライブ文字と MCS I/O ライトバックキャッシュディスクのドライブ文字の間の競合を回避するのに役立ちます。MCS の I/O ライトバックキャッシュディスクにドライブ文字を割り当てる場合は、PowerShell コマンドを使用できます。サポートされているハイパーバイザーは、Azure、GCP、VMware、SCVMM、および XenServer です。

> 注:
>
> この機能では、VDA バージョン 2305 以降が必要です。

制限事項

- Windows オペレーティングシステムのみに適用されます
- ライトバックキャッシュディスクに適用できるドライブ文字：E～Z
- Azure 一時ディスクがライトバックキャッシュディスクとして使用されている場合は適用されません
- 新しいマシンカタログを作成する場合にのみ適用されます

ライトバックキャッシュディスクにドライブ文字を割り当てる

ライトバックキャッシュディスクにドライブ文字を割り当てるには、次の手順を実行します:

1. **PowerShell** ウィンドウを開きます。
2. `asnp citrix*`を実行します。
3. ID プールをまだ作成していない場合は作成します。
4. `New-ProvScheme`コマンドをプロパティ`WriteBackCacheDriveLetter`で使用してプロビジョニングスキームを作成します。例:

```
New-ProvScheme -CleanOnBoot `
-HostingUnitName "<name>" `
-IdentityPoolName $schemeName `
-ProvisioningSchemeName $schemeName `
```



```
-InitialBatchSizeHint 1 `
-UseWriteBackCache -WriteBackCacheDiskSize 127 -
   WriteBackCacheMemorySize 256 -WriteBackCacheDriveLetter E `
-MasterImageVM "XDHyp:\HostingUnits<name>\image.folder\abcd-
   resources.resourcegroup\
   MCSIOMasterVm_OsDisk_1_d3e2d6352xxxxxxxx2130aa145ec77.
   manageddisk" `
-NetworkMapping @{
 "0"="XDHyp:\HostingUnits\name\virtualprivatecloud.folder\East US.
    region\virtualprivatecloud.folder\abcd-resources.resourcegroup
    \abcd-resources-vnet.virtualprivatecloud\default.network" }
  `
-ServiceOffering "XDHyp:\HostingUnits\<name>\serviceoffering.
   folder\Standard_D2s_v5.serviceoffering" `
-CustomProperties '<CustomProperties xmlns="http://schemas.citrix.
   com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/
   XMLSchema-instance">
<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="
   true" />
<Property xsi:type="StringProperty" Name="OsType" Value="Windows"
   />
<Property xsi:type="StringProperty" Name="StorageType" Value="
   Premium_LRS"/>
<Property xsi:type="StringProperty" Name="PersistWBC" Value="false
   " />
<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="
   false" />
<Property xsi:type="StringProperty" Name="PersistVm" Value="false"
    />
<Property xsi:type="StringProperty" Name="WBCDiskStorageType"
   Value="Premium_LRS" />
<Property xsi:type="StringProperty" Name="UseTempDiskForWBC" Value
   ="false" />
<Property xsi:type="StringProperty" Name="ResourceGroups" Value="
   abcd-group1" />
<Property xsi:type="StringProperty" Name="LicenseType" Value="
   Windows_Client" />
<Property xsi:type="StringProperty" Name="SchemaVersion" Value="2"
    />
</CustomProperties>'
```

5. カタログの作成を完了します。詳しくは、「https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/」を参照してください。

マスターイメージの準備

接続ホストの作成について詳しくは、「接続とリソース」を参照してください。

マスターイメージには、オペレーティングシステム、仮想化しないアプリケーション、VDA、およびそのほかのソフトウェアをインストールしておきます。

ヒント:

- マスターイメージは、「クローンイメージ」、「ゴールデンイメージ」、「ベース仮想マシン」、または「基本イメージ」と呼ばれることがあります。ホストベンダーによって、異なる用語を使用します。
- ホストに、作成されたマシン数に対応する十分なプロセッサ、メモリ、ストレージがあることを確認してください。
- デスクトップとアプリケーションで必要な適切な量のハードディスク領域を構成します。この値は、後で、またはマシンカタログ内で変更することはできません。
- リモート PC アクセスのマシンカタログでは、マスターイメージを使用しません。

マスターイメージに以下のソフトウェアをインストールして構成します:

- ハイパーバイザー用の統合ツール（Citrix VM Tools、Hyper-V 統合サービス、VMware Tools など）。この手順を省略すると、アプリケーションやデスクトップが正しく動作しなくなる場合があります。
- VDA。最新の機能を利用できるように、最新バージョンをインストールすることを Citrix ではお勧めします。マスターイメージに VDA をインストールできないと、カタログ作成が失敗します。
- アンチウイルスプログラムや電子ソフトウェア配信エージェントなどのサードパーティツール（必要に応じて）。ユーザーやマシンの種類に適した設定で、サービス（更新機能など）を構成します。
- 仮想化せずにユーザーに提供するサードパーティのアプリケーション。ただし、可能な場合はアプリケーションを仮想化することを Citrix ではお勧めします。仮想化することで、アプリケーションを追加したり再構成したりするたびにマスターイメージを更新する必要がなくなり、コストが削減されます。また、各デスクトップにインストールするアプリケーションが少なくなるため、マスターイメージのハードディスクのサイズを減らしてストレージコストを節約できます。
- App-V アプリケーションを公開する場合は、推奨設定の App-V クライアント。App-V Client は、Microsoft 社から提供されます。
- MCS で作成したマシンカタログで、ローカライズされた Microsoft Windows を配信する場合は、マスターイメージに言語パックをインストールして言語オプション（システムロケールや表示言語など）を設定しておく必要があります。これにより、プロビジョニング時にスナップショットが作成されると、その言語パックおよび言語オプションが仮想マシンで使用されます。

> 重要:
>
> MCS を使用する場合は、マスターイメージ上で Microsoft System Preparation Utility（Sysprep）を実行しないでください。

マスターイメージを準備するには

1. ハイパーバイザーの管理ツールを使用して、マスターイメージを作成してから、オペレーティングシステムと、すべてのサービスパックおよび更新プログラムをインストールします。仮想 CPU の数を指定します。また、PowerShell を使用してマシンカタログを作成する場合、仮想 CPU の値を指定することもできます。Web Studio を使用してカタログを作成する場合には、仮想 CPU の数は指定できません。デスクトップとアプリケーションで必要な量のハードディスク領域を構成します。この値は、後で、またはカタログ内で変更することはできません。

2. ハードディスクはデバイスの場所「0」で接続されている必要があります。多くの標準マスターイメージテンプレートでは、デフォルトでこの場所にハードディスクが構成されますが、カスタムテンプレートを使用する場合は注意してください。
3. マスターイメージに前述のソフトウェアをインストールして構成します。
4. MCS を使用していない場合、マスターイメージはアプリケーションとデスクトップがメンバーとなっているドメインに統合します。マスターイメージが、仮想マシンを作成するホスト上で使用できることを確認してください。MCS を使用している場合、ドメインへのマスターイメージの統合は必要ありません。プロビジョニングされたマシンは、カタログの作成ウィザードで指定されたドメインに統合されます。
5. マスターイメージのスナップショットを作成して、名前を付けることをお勧めします。カタログの作成時にスナップショットの代わりにマスターイメージを指定すると、Web Studio によりスナップショットが作成されます。これに名前を付けることはできません。

ボリュームライセンス認証

MCS は、Windows オペレーティングシステムと Microsoft Office のライセンス認証を自動化および管理するためのボリュームライセンス認証をサポートしています。MCS でサポートされるボリュームライセンス認証モデルは、次の 3 種類です:

- キー管理サービス（KMS）
- Active Directory によるライセンス認証（ADBA）
- マルチライセンス認証キー（MAK）

マシンカタログを作成した後にライセンス認証の設定を変更できます。

キー管理サービス（**KMS**）

KMS は、専用システムを必要としない軽量のサービスであり、他のサービスを提供するシステムで簡単に共同ホストできます。この機能は、Citrix がサポートするすべての Windows バージョンでサポートされています。イメージの準備中に、MCS は Microsoft Windows と Microsoft Office の KMS リセットを行います。コマンド`Set-Provserviceconfigurationdata`を実行すると、リセットをスキップできます。イメージ準備中の Microsoft Windows KMS リセットおよび Microsoft Office KMS リセットについて詳しくは、「Machine Creation Services: Image Preparation Overview and Fault-Finding」を参照してください。KMS のアクティブ化について詳しくは、「Activate using Key Management Service」を参照してください。

> 注:
>
> コマンド`Set-Provserviceconfigurationdata`の実行後に作成されたすべてのマシンカタログは、コマンドで指定されたものと同じ設定になります。

Active Directory によるライセンス認証（**ADBA**）

ADBA を使用すると、ドメイン接続を介してマシンをアクティブ化できます。マシンは、ドメインに参加するとすぐにアクティブになります。これらのマシンは、ドメインに参加し、ドメインに接続している限り、アクティブのままです。この機能は、Citrix がサポートするすべての Windows バージョンでサポートされています（Windows Server 2022 を除く）。Active Directory によるライセンス認証について詳しくは、「Active Directory によるライセンス認証」を参照してください。

マルチライセンス認証キー（**MAK**）

MAK はボリュームをアクティブ化する方法の 1 つで、Microsoft サーバーの助けを借りて Windows システムを認証します。一定数のアクティベーションカウントが割り当てられている MAK キーを Microsoft から購入する必要があります。Windows システムがアクティブ化されるたびに、アクティベーションカウントが減少します。システムをアクティブ化するには、次の 2 つの方法があります：

- オンラインアクティベーション：アクティブ化する Windows システムがインターネットにアクセスできる場合、システムはプロダクトキーのインストール時に Windows を自動的にアクティブ化します。このプロセスにより、対応する MAK のアクティベーションカウントが 1 減ります。
- オフラインアクティベーション：Windows システムがインターネットに接続してオンラインアクティベーションを実行できない場合、MCS は Microsoft サーバーから確認 ID とインストール ID を取得して、Windows システムをアクティブ化します。このアクティベーション方法は、非永続的なマシンカタログに役立ちます。

> 注：
>
> - MCS は MAK を使用した Microsoft Office のアクティベーションをサポートしていません。
> - 必要な VDA の最小バージョンは 2303 です。

主な要件

- Delivery Controller にはインターネットアクセスが必要です。
- 更新される新しいイメージの MAK キーが元のイメージと異なる場合は、新しいカタログを作成します。
- マスターイメージ上に MAK キーをインストールします。Windows システムに MAK キーをインストールする手順については、「Deploy MAK Activation」を参照してください。
- イメージの準備を使用しない場合：
  1. `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform\Activation`の下に DWORD レジストリ値`Manual`を追加します。
  2. 値を`1`に設定します。

ライセンス認証数　MAK キーの残りのライセンス認証の数を表示したり、VM が 2 つ以上のライセンス認証を使用しているかどうかを確認するには、Volume Activation Management Tool（VAMT）を使用します。「VAMT のインストール」を参照してください。

MAK を使用して **Windows** システムをアクティブ化する　MAK を使用して Windows システムをアクティブ化するには:

1. マスターイメージにプロダクトキーをインストールします。この手順では、1 つのアクティベーションカウントが消費されます。
2. MCS マシンカタログを作成します。
3. イメージの準備を使用していない場合:

   a) `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform\Activation`の下に DWORD レジストリ値`Manual`を追加します。
   b) 値を`1`に設定します。

   この方法では、オンラインアクティベーションのオプションが無効になります。
4. VM をマシンカタログに追加します。
5. VM の電源をオンにします。
6. オンラインアクティベーションかオフラインアクティベーションかに応じて、Windows システムがアクティブ化されます。

   - アクティベーションがオンラインの場合、プロダクトキーのインストール後に Windows システムがアクティブ化されます。
   - アクティベーションがオフラインの場合、MCS はプロビジョニングされた VM と通信して、Windows システムのアクティベーションステータスを取得します。次に、MCS は確認 ID とインストール ID を Microsoft サーバーから取得します。これらの ID は、Windows システムをアクティブ化するために使用されます。

トラブルシューティング　プロビジョニングした VM がインストールした MAK キーでライセンス認証されない場合は、PowerShell ウィンドウで`Get-ProvVM`または`Get-ProvScheme`コマンドを実行します。

- コマンド`Get-ProvScheme`: 最新のマスターイメージから MCS マシンカタログに関連付けられたパラメータ`WindowsActivationType`を参照します。
- コマンド`Get-ProvVM`:パラメータ`WindowsActivationType`、`WindowsActivationStatus`、`WindowsActivationStatusErrorCode`、および`WindowsActivationStatusError`を参照してください。

エラーを確認し、問題解決の手順を確認できます。

Web Studio でのマシンカタログの作成

カタログを作成する前に:

- 以下のセクションを確認して、選択する項目および指定する情報について理解しておいてください。
- マシンをホストするハイパーバイザーやクラウドサービスなどのリソースに対して、接続を作成していることを確認してください。
- マシンのプロビジョニングに使用するマスターイメージを作成している場合は、そのイメージに VDA がインストールされていることを確認してください。

カタログ作成ウィザードを開始するには、次の操作を行います:

1. 初めてカタログを作成する場合には、適切な選択を行うためのガイドが表示されます（「マシンをセットアップし、マシンカタログを作成して、アプリとデスクトップを実行します」など）。カタログ作成ウィザードが開きます。
2. すでにカタログを作成済みで、別のカタログを作成したい場合は、次の手順に従います:
   a) Web Studio にサインインし、左側のペインで ［マシンカタログ］を選択してから操作バーで ［マシンカタログの作成］を選択します。
   b) フォルダーを使用してカタログを整理するには、デフォルトのマシンカタログフォルダーの下にフォルダーを作成します。詳しくは、「カタログフォルダーの作成」を参照してください。
   c) カタログを作成するフォルダーを選択し、［マシンカタログの作成］をクリックします。カタログ作成ウィザードが開きます。

ウィザードの指示に従って、以下の項目の操作を行います。選択内容によって、異なるウィザードページが表示されます。

オペレーティングシステム

各カタログでは、以下のいずれかの種類のマシンを追加します。いずれかを選択します。

- マルチセッション **OS**: マルチセッション OS カタログは、ホストされた共有デスクトップを提供します。マシンでは、サポートされているバージョンの Windows または Linux オペレーティングシステムを実行できますが、両方をカタログに含めることはできません。（この OS について詳しくは、Linux VDA のドキュメントを参照してください）。
- シングルセッション **OS**: シングルセッション OS カタログでは、さまざまなユーザーに割り当てることができる VDI デスクトップが提供されます。
- リモート **PC** アクセス: リモート PC アクセスのカタログでは、オフィスにあるユーザーの物理デスクトップマシンへのリモートアクセスが提供されます。リモート PC アクセスでは、セキュリティを保護するための VPN が不要です。

マシン管理

このページは、リモート PC アクセスカタログを作成するときには表示されません。

［マシン管理］ページでは、マシンの管理方法と、マシンの展開に使用するツールが示されます。

Web Studio を使用してカタログ内のマシンの電源を管理するかを選択します。

- Web Studio で電源管理されるマシン（仮想マシンやブレード PC など）。このオプションは、ホストへの接続を構成済みの場合にのみ使用可能です。
- Web Studio で電源管理しないマシン（物理マシンなど）。

マシンが Web Studio で電源管理されるように指定した場合、仮想マシンの作成に使用するツールを選択します。

- Citrix Provisioning テクノロジ
  - **Citrix Machine Creation Services**（**MCS**） MCS を使用して、プロビジョニングされイメージが作成された仮想マシンのカタログを作成します。MCS は、マスターイメージから複製されたイメージをそれらの仮想マシンにコピーします。
  - **Citrix Provisioning Services**（**PVS**） MCS を使用してプロビジョニングされ、PVS を使用してイメージが作成された仮想マシンのカタログを作成します。これらの仮想マシンは PVS ターゲットデバイスとして機能し、PVS サーバーは単一の共有ディスクイメージをそれらにストリーミングできます。

    > 注:
    >
    > * このオプションは、Citrix Cloud に登録された PVS サイトでのみ使用でき、現在は Azure リソースに限定されています。
    > * Citrix Provisioning カタログを作成するときに、［ターゲットデバイス］ページで、プロビジョニングするマシンのファームとサイトを選択するためのドロップダウンメニューに、存在しなくなったファームとサイトが表示されることがあります。回避策として、PowerShell コマンド`Unregister-HypPvsSite`を実行して、データベースから該当するファームとサイトを削除できます。PowerShell コマンドについて詳しくは、「Unregister-HypPvsSite」を参照してください。

- ほかのサービスまたはテクノロジ データセンター内の既存のマシンを管理するための、上記以外のツール。この場合、Microsoft System Center Configuration Manager またはほかのサードパーティアプリケーションを使用してカタログ内のマシン構成の一貫性を保つことを Citrix ではお勧めします。

デスクトップの種類（デスクトップエクスペリエンス）

> 注:
>
> ［デスクトップエクスペリエンス］ページに表示されるオプションは、［マシンの種類］ページで選択したマシンの種類に応じて異なります。

- マルチセッション **OS** マシンの場合、ユーザーには、ログインするたびにランダムデスクトップが割り当てられます。次のいずれかのオプションを選択します:
  - はい。仮想デスクトップをホストしているマシンのローカルディスクに変更を保存します。(永続)
  - いいえ、ユーザーのログオフ時にすべての変更を破棄して仮想デスクトップをクリアする。(非永続)

  > 注:
  >
  > 永続的なマルチセッションマシンの場合、ユーザーがデスクトップに加えた変更は保存され、すべての承認されたユーザーがアクセスできます。

- シングルセッション **OS** マシンの場合、[デスクトップエクスペリエンス] ページには次のオプションが表示されます:
  - ユーザーがログオンするたびに新しいデスクトップに接続する (ランダム)。
  - ユーザーがログオンするたびに同じデスクトップに接続する (静的)。

    静的デスクトップの場合、ユーザーが行った変更をログオフ後に保存するか破棄するかを決定できます。

イメージ

このページは、MCS を使用して仮想マシンを作成するときにのみ表示されます。

1. マシンカタログのイメージの種類を選択し、イメージを選択します。次の 2 種類のイメージを使用できます:
   - マスターイメージ。イメージ準備プロセスで処理されていないイメージ。カタログの作成が開始されると、イメージ準備プロセスが自動的に開始されます。

     > 注:
     >
     > - MCS を使用する場合は、マスターイメージ上で Microsoft System Preparation Utility (Sysprep) を実行しないでください。
     > - スナップショットの代わりにマスターイメージを指定すると、Web Studio でスナップショットが作成されますが、そのスナップショットにわかりやすい名前を付けることはできません。

   - 準備済みイメージ。イメージ準備プロセスを経た、VM の作成に直接使用できるイメージ。カタログ作成にマスターイメージではなく準備されたイメージを選択すると、イメージのライフサイクル管理が合理化されるとともに、マシンカタログの作成がより迅速になり、信頼性が高くなります。

     > 注:
     >
     > - 準備済みイメージを使用して作成された VM は休止状態をサポートしません。
     > - 現在、準備済みイメージを使用したカタログの作成は、Azure および VMware 環境でのみ可能です。

準備済みイメージの作成方法について詳しくは、「イメージ管理（Technical Preview）」を参照してください。

イメージを選択するときに、必要に応じて選択したイメージにメモを追加できます。

最新の製品機能を使用できるようにするため、マスターイメージに最新の VDA バージョンがインストールされていることを確認してください。デフォルトで選択されている最小 VDA は変更しないでください。ただし、以前のバージョンの VDA を使用する必要がある場合には、「VDA バージョンと機能レベル」を参照してください。

ウィザードで過去に選択したマシン管理テクノロジとの互換性がないスナップショットまたは仮想マシンを選択すると、エラーメッセージが表示されます。

2. 既存の VM をマシンプロファイルとして使用するには、［マシンプロファイルを使用する］を選択し、VM を選択します。

   > 注:
   >
   > 現在、マシンプロファイルの使用は、Azure、AWS、GCP、および VMware VM に制限されています。

   VMware 展開の場合、マシンプロファイルを使用してマシンカタログを作成するときに、仮想マシンを保存するフォルダーを指定する必要があります。

   仮想マシンフォルダーの場所を指定するには、カタログ作成ウィザードで［**Virtual Machines**］ページに移動し、［**Select a folder to place the machines**］セクションに移動して、仮想マシンフォルダーの場所を選択します。指定されていない場合、システムは選択したマシンプロファイルのフォルダーをデフォルトの場所と見なします。

3. カタログの最小機能レベルを選択します。最新の製品機能を使用できるようにするため、マスターイメージに最新の VDA バージョンがインストールされていることを確認してください。

マシン

このページは、リモート PC アクセスカタログを作成するときには表示されません。

このページのタイトルは、［マシン管理］ページで選択した項目：［マシン］、［仮想マシン］、［仮想マシンとユーザー］によって変わります。

MCS を使用する場合：

- 作成する仮想マシンの数を指定します。何も作成しない場合は、**0**（ゼロ）を入力します。後で、［マシンの追加］を実行して空のカタログに対して仮想マシンを作成できます。
- 各仮想マシンのメモリ量（MB 単位）を選択します。
- 作成された各仮想マシンにハードディスクがあります。そのサイズはマスターイメージに設定されます。カタログでハードディスクのサイズを変更することはできません。
- 環境に複数のゾーンがある場合は、カタログのゾーンを選択できます。

- 静的なデスクトップ仮想マシンを作成する場合は、仮想マシンコピーモードを選択します。「仮想マシンコピーモード」を参照してください。
- vDisk を使用しないランダムなデスクトップ仮想マシンを作成する場合は、各マシンの一時データに対して使用するキャッシュを構成できます。「一時データ用キャッシュの構成」を参照してください。

他のツールを使用する場合:

Active Directory マシンアカウント名の追加（またはアカウント名一覧のインポート）仮想マシンの Active Directory アカウント名は、追加またはインポートした後に変更できます。［デスクトップエクスペリエンス］ページで静的なマシンを指定すると、追加する各仮想マシンにオプションで Active Directory ユーザー名を指定できます。

名前を追加またはインポートした後で、［削除］ボタンを使用して、ユーザーはページ上のままで一覧から名前を削除できます。

他のツール（**MCS** 以外）を使う場合:

追加（またはインポート）する各マシンのアイコンとヒントにより、カタログに追加できない可能性のあるマシン、または Delivery Controller に登録できない可能性のあるマシンを特定できます。詳しくは、「VDA バージョンと機能レベル」を参照してください。

仮想マシン作成時の **SID** の追加

`ADAccountSid`パラメーターを追加して、新しい仮想マシンの作成時にマシンを一意に識別できるようになりました。

これを行うには、以下の手順に従います:

1. サポートされている ID タイプでカタログを作成します。
2. `NewProvVM`を使用してマシンをカタログに追加します。例:

```
1 New-ProvVM  -ProvisioningSchemeName "name"  -ADAccountSid @("SID "
      )  -RunAsynchronously
```

ただし、次のものを使用してマシンをプロビジョニングすることはできません:

- カタログ ID プールにない AD アカウント
- 使用可能な状態にない AD アカウント

仮想マシンコピーモード

［マシン］ページで指定するコピーモードによって、MCS がマスターイメージからシン（簡易コピー）クローンまたはシック（完全なコピー）クローンのどちらを作成するかが決まります。（デフォルトはシンクローン）

- 簡易コピークローンは、効率的にストレージを使用し、すばやくマシンを作成したい場合に使います。

- 完全コピークローンは、マシン作成後に IOPS が潜在的に低下した場合に、質の高いデータの復元と移行サポートが必要な場合に使います。

VDA バージョンと機能レベル

カタログの機能レベルにより、どの製品機能がカタログにあるマシンで利用可能かが制御されます。新しい製品バージョンで導入された機能を使用するには、新しい VDA が必要です。機能レベルを設定すると、そのバージョン（機能レベルが変更されない場合はそのバージョン以降）で導入されたすべての機能がカタログで利用できるようになります。ただし、以前の VDA バージョンのカタログにあるマシンは登録できません。

［マシン］（または ［デバイス］）ページの下部近くにあるメニューを使って、最小 VDA レベルを選択できます。これにより、カタログの最小機能レベルが設定されます。デフォルトで、オンプレミスの展開には最新の機能レベルが選択されます。Citrix の推奨事項に従って VDA とコアコンポーネントを常に最新のバージョンでインストールおよびアップグレードする場合は、この選択を変更する必要がありません。以前の VDA バージョンを使用し続ける必要がある場合は、正しい値を選択してください

Citrix Virtual Apps and Desktops のリリースには、新しい VDA バージョンが含まれないことがあります。または、新しい VDA は、機能レベルに影響を与えません。このような場合、機能レベルは、インストールまたはアップグレードされたコンポーネントより以前の VDA バージョンであることを示します。デフォルトの機能レベルの変更については、各リリースの新機能の記事に記載されています。

選択した機能レベルは、このレベルのマシンの一覧に影響します。一覧で、各エントリの横にあるツールチップは、マシンの VDA がその機能レベルでカタログと互換性があるかどうかを示します。

各マシンの VDA が選択した最小機能レベルを満たさない、または超過している場合、ページにメッセージが表示されます。ウィザードは続行できますが、これらのマシンは後で Controller によって登録できない可能性があります。代わりに、以下を行うことができます。

- 古い VDA が含まれるマシンを一覧から削除し、VDA をアップグレードしてからマシンをカタログに追加し直します。
- 低い機能レベルを選択します。これによって最新の製品機能にアクセスできなくなります。

マシンの種類が正しくないためにマシンがカタログに追加されなかった場合には、メッセージも表示されます。たとえば、シングルセッション OS カタログにサーバーを追加しようとした場合や、ランダム割り当て用に作成されたシングルセッション OS マシンを静的マシンのカタログに追加した場合などです。

> 重要：
>
> リリース 1811 では、次の機能レベルが追加されました：**1811**（またはそれ以降）。このレベルは、今後の Citrix Virtual Apps and Desktops 機能での使用を想定しています。**7.9**（またはそれ以降）の選択はデフォルトのままです。このデフォルトは、すべての環境で有効になりました。
>
> **1811**（またはそれ以降）を選択した場合、そのカタログの以前の VDA バージョンは Controller には登録できません。ただし、バージョン 1811 以降のサポート対象バージョンでカタログに VDA のみが含まれている場

> 合は、それらはすべて登録対象です。これには、新しい Citrix Virtual Apps and Desktops リリース（バージョン 1903 および現在のリリースより前の 19XX リリースを含む）用に構成された VDA を含むカタログが含まれます。

一時データ用キャッシュの構成

MCS を使用してカタログ内のランダムな非永続マシンを管理する場合、マシンのライトバックキャッシュを有効にして、I/O パフォーマンスを向上させることができます。

ライトバックキャッシュは MCSIO と呼ばれます。詳しくは、このブログ記事を参照してください。

前提条件　ライトバックキャッシュを有効にするには、カタログが次の要件を満たしている必要があります:

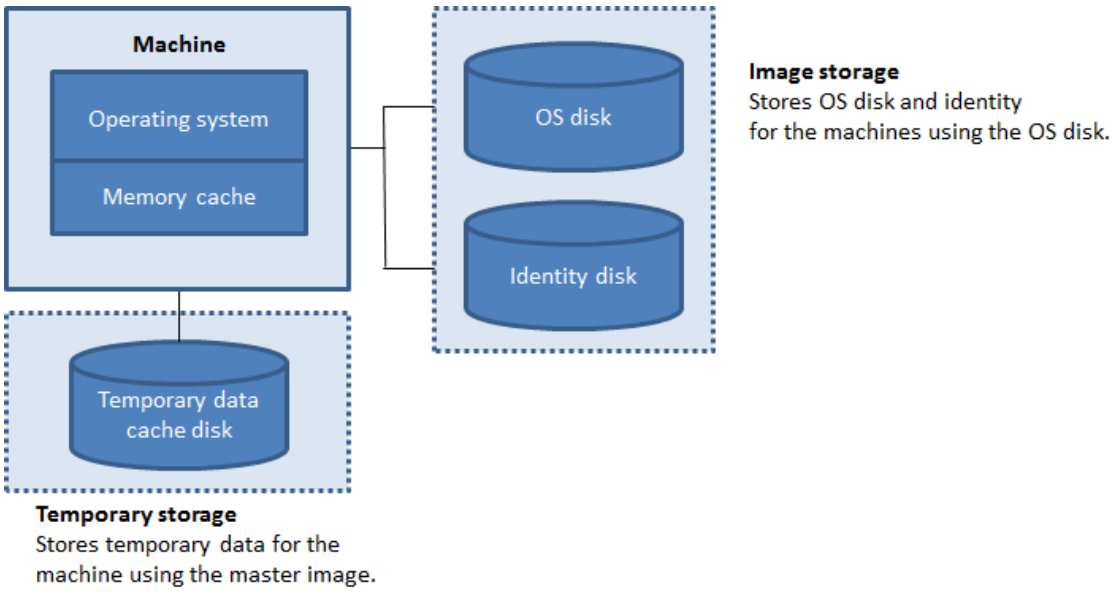
- 一時データのストレージを指定する接続を使用します。詳しくは、「接続およびリソース」を参照してください。
- VDA はバージョン 7.9 以降であり、最新の MCSIO ドライバーがインストールされている必要があります。

  > 注:
  >
  > このドライバーは、VDA のインストール時またはアップグレード時にオプションとしてインストールできます。デフォルトでは、このドライバーはインストールされません。

- ディスクキャッシュのドライブ文字の割り当てを有効にするには、仮想マシンが次の追加の要件を満たしている必要があります:
  - オペレーティングシステム: Windows
  - VDA バージョン: 2305 以降

注意事項

- ライトバックキャッシュには、メモリキャッシュとディスクキャッシュがあります。デフォルトでは、接続の種類によってデフォルト値が異なります。通常は、デフォルト値で十分なことが多いですが、次のデータに必要な容量を検討してください:
  - Windows ページファイルなどの、Windows 自体が作成する一時データファイル
  - ユーザープロファイルデータ
  - ユーザーのセッションに同期される ShareFile データ。
  - セッションユーザーによって作成またはコピーされるデータや、ユーザーがセッション内にインストールするアプリケーション。



- ディスクキャッシュのみを使用し、メモリキャッシュを使用しないライトバックキャッシュの構成は廃止されました。一時データのキャッシュを有効にするには、［ディスクキャッシュサイズ（**GB**）］と ［キャッシュに割り当てられたメモリ（**MB**）］の両方を選択し、メモリキャッシュに 0 より大きいサイズを指定することをお勧めします。一時データは最初にメモリキャッシュに書き込まれます。メモリキャッシュが、構成された制限に達すると、古いデータから先に一時データキャッシュディスクに移動されます。
- メモリキャッシュは、各マシンの合計メモリ容量の一部です。そのため、［メモリキャッシュサイズ（**MB**）（推奨）］チェックボックスをオンにする場合は、各マシンの合計メモリ容量を増やすことを検討してください。
- ［メモリキャッシュサイズ（**MB**）（推奨）］チェックボックスをオフのままにすると、最小限のメモリを使用して、一時データがディスクキャッシュに直接書き込まれます。
- ［ディスクキャッシュサイズ（**GB**）］をデフォルト値から変更すると、パフォーマンスに影響することがあります。サイズはユーザー要件とマシンの負荷に合わせる必要があります。

  > 重要：
  >
  > ディスクキャッシュの容量が不足すると、ユーザーセッションは利用できなくなります。

- ［ディスクキャッシュサイズ］チェックボックスをオフにすると、キャッシュディスクは作成されません。この場合、［キャッシュに割り当てられたメモリ］にすべての一時的なデータを保持するのに十分な値を指定します。これは、各仮想マシンへの割り当てに大量の RAM が使用できる場合にのみ可能です。
- 両方のチェックボックスをオフにすると、一時データはキャッシュされず、各仮想マシンの差分ディスク（OS ストレージにあります）に書き込まれます。（これは、7.9 より前のリリースでは、プロビジョニングアクションです。）
- このカタログを使用して AppDisk を作成しようとしている場合は、キャッシュを有効にしないでください。
- マシンカタログの作成後は、キャッシュ値を変更できません。

NIC

このページは、リモート PC アクセスカタログを作成するときには表示されません。

［ネットワークインターフェイスカード］ページで、複数の NIC を使用する場合は、各 NIC に仮想ネットワークを関連付けます。たとえば、特定のセキュアネットワークへのアクセスに 1 つの NIC を割り当てて、より一般的なネットワークへのアクセスに別の NIC を割り当てることができます。また、このページで NIC を追加または削除することもできます。

マシンアカウント

このページは、リモート PC アクセスカタログを作成するときにのみ表示されます。

［マシンアカウント］ページで、ユーザーまたはユーザーグループに対応する Active Directory マシンアカウントまたは組織単位（OU）を指定して追加します。組織単位名にはスラッシュ（/）を使用しないでください。

組織単位を追加するとき、ドメインがリストに表示されていない場合は、次の操作を実行できます：

- 完全一致を使用して検索します。
- すべてのドメインを参照して見つけます。

構成済みの電源管理接続を選択するか、電源管理を使用しないことを選択します。電源管理に必要な接続が構成済みでない場合は、マシンカタログの作成後に新しい接続を作成してから、そのマシンカタログを編集して電源管理設定を更新できます。

マシン **ID**

このページは、MCS を使用して仮想マシンを作成するときにのみ表示されます。

カタログ内の各マシンは、一意の ID を持っている必要があります。このページでは、カタログ内のマシンの ID を構成できます。マシンは、プロビジョニングされた後、ID に結合されます。カタログの作成後に ID の種類を変更することはできません。

このページで設定を構成するための一般的なワークフローは次のとおりです：

1. 一覧から ID を選択します。
2. アカウントを作成するか既存のアカウントを選択して、アカウントの場所（ドメイン）を指定します。

次のいずれかのオプションを選択できます：

- オンプレミス **Active Directory**。組織が所有しているマシンで、その組織に属した Active Directory アカウントでサインインしたマシン。これらのマシンはオンプレミスに存在します。
- **Hybrid Azure Active Directory** 参加済み。組織が所有しているマシンであり、その組織に属した Active Directory Domain Services アカウントでサインインしたマシン。これらのマシンはクラウドとオンプレミ

スに存在します。要件、制限、および考慮事項については、「Hybrid Azure Active Directory 参加済み」を参照してください。

> 注:
>
> - Hybrid Azure Active Directory 参加を使用する前に、Azure 環境が前提条件を満たしていることを確認してください。https://docs.microsoft.com/en-us/azure/active-directory/devices/hybrid-azuread-join-managed-domainsを参照してください。
> - このオプションを使用するには、マスターイメージがオペレーティングシステムの前提条件を満たしている必要があります。詳しくは、Microsoft 社のドキュメントを参照してください: https://learn.microsoft.com/en-us/azure/active-directory/devices/concept-azure-ad-join-hybrid。

> 重要:
>
> - ID の種類に［オンプレミス **Active Directory**］または［**Hybrid Azure Active Directory joined**］を選択した場合、カタログ内の各マシンには、対応する Active Directory コンピューターアカウントが必要です。

アカウントを作成する場合は、マシンが存在する OU にコンピューターアカウントを作成する権限が必要です。カタログ内の各マシンは、一意の名前である必要があります。作成するマシンのアカウント名前付けスキームを指定します。詳しくは、「マシンのアカウント名前付けスキーム」を参照してください。

> 注:
>
> OU 名にスラッシュ（/ ）が使用されていないことを確認してください。

既存のアカウントを使用する場合、アカウントを参照するか、［インポート］をクリックしてアカウント名が含まれる CSV ファイルを指定します。インポートするファイルでは、次の形式を使用する必要があります:

- [ADComputerAccount] AD コンピューターアカウント名. ドメイン

追加するすべてのマシンに十分な数のアカウントをインポートする必要があります。Web Studio インターフェイスはこれらのアカウントを管理します。そのため、すべてのアカウントのパスワードのリセットを［完全な構成］インターフェイスに許可するか、アカウントのパスワードを指定します（すべてのアカウントで同じパスワードを使用する必要があります）。

物理マシンまたは既存のマシン用のカタログでは、既存のアカウントを選択またはインポートして、各マシンを Active Directory コンピューターアカウントおよびユーザーアカウントに割り当てます。

マシンのアカウント名前付けスキーム

カタログ内の各マシンは、一意の名前である必要があります。カタログを作成するときに、マシンのアカウント名前付けスキームを指定する必要があります。名前で、連続した数字または文字を表示するには、プレースホルダーとしてワイルドカード（ハッシュ記号）を使用します。

名前付けスキームを指定するときは、次の規則に注意してください:

- 名前付けスキームには、少なくとも 1 個のワイルドカードを含める必要があります。すべてのワイルドカードは同時に指定する必要があります。
- 名前全体には、ワイルドカードを含め、2 文字以上 15 文字以下が含まれている必要があります。少なくとも 1 つの数字ではない値と、1 つの #（ワイルドカード）文字を含める必要があります。
- 名前にスペースや次の文字を含めることはできません: `,~!@'$%^&.()} { \/*?"<>|=+[];:_".`。
- 名前をハイフン「-」で終了することはできません。

また、名前付けスキームを指定するときは、後で文字が増える余地を十分に残してください。次の例を考慮に入れてください:「veryverylong#」という名前付けスキームで 1,000 台分のマシンのアカウントを作成した場合、最後に作成されるアカウント名（veryverylong1000）には 16 文字が含まれます。そのため、この名前付けスキームでは、1 つまたは複数のマシン名が上限の 15 文字を超えることになります。

連続する値を数字（0〜9）にするか、文字（A〜Z）にするかを指定できます:

- **0〜9**。選択した場合、指定したワイルドカードは連番になります。

  > 注:
  >
  > ワイルドカードが 1 つ（#）しかない場合、アカウント名は 1 で始まります。2 つある場合、アカウント名は 01 で始まります。3 つある場合、アカウント名は 001 で始まります。

- **A-Z**。選択した場合、指定したワイルドカードは連続した文字になります。

たとえば、名前付けスキームとして「PC-Sales-##」を指定して［**0-9**］を選択すると、PC-Sales-01、PC-Sales-02、PC-Sales-03 などのアカウント名が作成されます。

オプションで、アカウント名の先頭を指定できます。

- ［**0-9**］を選択すると、アカウントには指定した数字から順番に名前が付けられます。前のフィールドで使用するワイルドカードの数に応じて、1 つまたは複数の数字を入力します。たとえば、2 つのワイルドカードを使用する場合は、2 桁以上を入力します。
- ［**A-Z**］を選択すると、アカウントには指定した文字から順番に名前が付けられます。前のフィールドで使用するワイルドカードの数に応じて、1 つまたは複数の文字を入力します。たとえば、2 つのワイルドカードを使用する場合は、2 文字以上を入力します。

ドメイン資格情報

［資格情報の入力］を選択して、ターゲットの Active Directory ドメインでアカウント操作を実行する権限を持つ管理者の資格情報を入力します。

［名前の確認］オプションを使用して、ユーザー名が有効か一意かを確認します。このオプションは、次のような場合に役立ちます:

- 同じユーザー名が複数のドメインに存在する。目的のユーザーを選択するように求められます。
- ドメイン名を忘れた。ドメイン名を指定せずにユーザー名を入力できます。この確認が完了すると、ドメイン名が自動的に入力されます。

> 注:
>
> ［マシン **ID**］で選択した ID の種類が ［**Hybrid Azure Active Directory joined**］である場合、入力する資格情報に`Write userCertificate`権限が付与されている必要があります。

概要、名前、および説明

［概要］ページで、指定した設定を確認します。カタログの名前と説明を入力します。これらの情報は Web Studio に表示されます。

完了したら、［完了］をクリックしてカタログの作成を開始します。
完了したら、［完了］をクリックしてカタログの作成を開始します。

［マシンカタログ］では、新しいカタログがインラインプログレスバーとともに表示されます。

作成の進行状況の詳細を表示するには:

1. マシンカタログの上にマウスポインターを置きます。
2. 表示されるツールチップで、［詳細の表示］をクリックします。

   手順ごとの進行状況グラフが表示され、次のことがわかります:

   - 手順の履歴
   - 現在の手順の進行状況と実行時間
   - 残りの手順

MCS 時間同期

時間同期は、マスターイメージと、カタログにあるマシン ID の種類によって決定されます。マスターイメージとカタログに従って、時間同期の方法が以下のようになります:

マスターイメージ	カタログ	時間同期の方法（結果）
NDJ	AD または Hybrid Azure AD	デフォルトでは、NT5DS です。マスターイメージのレジストリ設定を使用して、MCS による時間同期設定の変更を無効化できます。
NDJ	NDJ または Azure AD	元の時間同期設定と同じ
AD または Hybrid Azure AD	AD または Hybrid Azure AD	元の時間同期設定と同じ

マスターイメージ	カタログ	時間同期の方法（結果）
Azure AD	Azure AD	元の時間同期設定と同じ

> 注:
>
> 元の時間同期は、以下のレジストリ設定によって制御され、変更できません:
>
> - Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Config
>
> 値: MaxAllowedPhaseOffset, MaxNegPhaseCorrection and MaxPosPhaseCorrection
>
> - Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Parameters
>
> 値: Type

MCS による時間同期設定の変更を無効にするには、マスターイメージで以下のレジストリ設定の値を設定します:

- `Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix`
- 名前: TimeSyncMethodKeep
- 種類: DWORD
- 0（または値 TimeSyncMethodKeep が構成されていない）: 元の時間同期設定を保持しません。
- 1: 元の時間同期設定とデフォルトのパラメーター値を保持します。

カスタムプロパティの設定に関する重要な考慮事項

カスタムプロパティは、GCP および Azure 環境の`New-ProvScheme`と`Set-ProvScheme`で正しく設定する必要があります。存在しないカスタムプロパティを指定すると、次のエラーメッセージが表示され、コマンドの実行に失敗します。

- Azure の場合: `Invalid property found: <invalid property>. Ensure that the CustomProperties parameter supports the property.`
- GCP の場合: `Invalid property found: <invalid property>. Ensure that the value supplied for the property is supported in the Hypervisor.`

トラブルシューティング

> 重要:
>
> Web Studio を使用してマシンカタログを作成すると、それ以降は`Get-ProvTask` PowerShell コマンドを使用してマシンカタログの作成に関連するタスクを取得することができなくなります。これはマシンカタロ

> グが正常に作成されたかどうかにかかわらず、取得対象のタスクが Web Studio によって削除されることから生じる制限です。

サポートチームが解決策を提供するのに役立つログを Citrix で収集することをお勧めします。Citrix Provisioning を使用する場合、以下の手順でログファイルを生成します:

1. マスターイメージで次のレジストリキーを作成し、値（DWORD（32 ビット）の値）を 1 に設定します: `HKLM\Software\Citrix\MachineIdentityServiceAgent\LOGGING`。
2. マスターイメージを閉じて、スナップショットを作成します。
3. Delivery Controller で、次の PowerShell コマンドを実行します: `Set-ProvServiceConfigurationData -Name ImageManagementPrep_NoAutoShutdown -Value $True`。
4. このスナップショットに基づいてカタログを作成します。
5. ハイパーバイザーで準備用仮想マシンが作成されたら、ログインして C:\:Image-prep.log and PvsVmAgentLog.txt のルートから次のファイルを抽出します。
6. マシンをシャットダウンすると、その時点でエラーが報告されます。
7. 次の PowerShell コマンドを実行して、イメージ準備用マシンの自動シャットダウンを再度有効にします: `Remove-ProvServiceConfigurationData -Name ImageManagementPrep_NoAutoShutdo`。

イメージ準備の問題

MCS は単一のイメージから多くのマシンを作成するため、すべてのマシンが一意であり、ライセンスが正しく割り当てられていることを確認するために、いくつかの手順を実行します。イメージの準備は、カタログ作成プロセスの一部です。この準備により、プロビジョニングされたすべてのマシンが一意の IP アドレスを持ち、一意のインスタンスとして KMS サーバーに正しくアナウンスされます。MCS 内で、マスターイメージのスナップショットを選択した後にイメージの準備が行われます。選択されたマシンからカタログを分離できるように、コピーが作成されます。元の仮想マシンをベースにして準備用の仮想マシンが作成されますが、ネットワーク接続は切断されています。ネットワーク接続を切断すると、他のマシンとの競合が回避でき、準備用の仮想マシンは新しくコピーされたディスクにのみ接続されるようになります。

イメージの準備を実行するために必要な手順を含む小さな 指示 ディスクが、準備用の仮想マシンに接続されます。この準備用の仮想マシンが起動し、イメージの準備プロセスが開始されます。イメージの準備には、次のプロセスが含まれます:

- DHCP を有効にします。DHCP を有効にすると、プロビジョニングされたマシンによる IP アドレスの競合が発生しなくなります。DHCP はすべてのネットワークカードで有効になっています。
- Microsoft Windows KMS をリセットします。KMS をリセットすると、Microsoft Windows に正しく確実にライセンスが割り当てられます。リセットされた OS が呼び出されるため、新しいインスタンスとして KMS ライセンスサーバーに正しく報告されます。

- Microsoft Office KMS をリセットします（Microsoft Office がインストールされている場合）。Microsoft Office をリセットすると、Microsoft Office（2010 以降）のすべてのバージョンが正しく確実に KMS サーバーに登録されます。Microsoft Office のリセットが呼び出されると、新しいインスタンスとして KMS ライセンスサーバーに報告されます。

> ヒント：
>
> イメージ準備プロセスが終了すると、ハイパーバイザーから指示ディスクが取得されます。ハイパーバイザーには、イメージ準備プロセスで収集された情報が含まれています。

イメージの準備段階が失敗する理由はさまざまです。次のようなエラーメッセージが表示されます：イメージ準備 Office のリセットに失敗しました。

これらのエラーについては、次のセクションで説明します。

DHCP の有効化　これらのエラーの場合は、静的 IP アドレスをサポートしていないネットワークカードが原因で発生します。たとえば、以前のバージョンの Dell SonicWall ネットワークカードです。SonicWall カードはファイアウォールネットワークカードであるため、操作に失敗しました。DHCP のみをサポートしているため、カードを DHCP に設定しても意味がありません。これは、Citrix Virtual Apps and Desktops の新しいバージョンで修正されました。ただし、この現象が他の種類のネットワークカードで見られる場合は、フォーラムまたはサポート担当者を通じて Citrix に報告する必要があります。

> 注：
>
> 次の例のこの PowerShell 設定は、Citrix Virtual Apps and Desktops サイトに適用されるため、すべての新しいカタログと既存のカタログに対して実行されるイメージの更新に影響を与えます。

他のネットワークカードでこの問題が発生した場合は、Delivery Controller で PowerShell コマンドを実行することで解決できます。

```
Set-ProvServiceConfigurationData -Name ImageManagementPrep_Excluded_Steps
 -Value EnableDHCP
```

Microsoft Office のリセット　Microsoft Office のリセット段階でさまざまな KMS リセットエラーが発生する可能性があります。主なエラーは次のとおりです：

- **Access Runtime** などの一部の Microsoft Office Runtime は、Office のリセットを呼び出して失敗する可能性があります。
- KMS バージョンの Microsoft Office がインストールされていません。
- リセット回数を超えました。

エラーが誤検知である場合は、Delivery Controller で次の PowerShell コマンドを実行することで解決できます。

```
Set-ProvServiceConfigurationData -Name ImageManagementPrep_Excluded_Steps
 -Value OfficeRearm
```


Microsoft Windows のリセット　Microsoft Windows のリセット段階では、さまざまな KMS エラーが発生する可能性があります。主なエラーは次のとおりです：

- インストールされている Windows のバージョンは、KMS を使用してアクティブ化されていません。たとえば、マルチライセンス認証キー（MAK）を使用しています。
- リセット回数を超えました。

Microsoft Windows のバージョンに正しくライセンスが割り当てられている場合は、Delivery Controller で次の PowerShell コマンドを実行して、OS リセットをクリアできます：

```
Set-ProvServiceConfigurationData -Name ImageManagementPrep_Excluded_Steps
 -Value OsRearm
```

完全なエラーのインスタンス　イメージ準備マシンは設計上ネットワークに接続されていません。つまり、イメージ準備段階では完全なエラーしか報告できない可能性があります。このエラーの種類の例は次のようになります：マスター仮想マシンイメージの準備に失敗しました。サポートされている OS（Windows 7 など）および適切なバージョンの VDA（7.0 以降）がイメージにインストールされていることを確認してください。

完全なエラーの主な理由は次のとおりです：

Virtual Delivery Agent（**VDA**）がインストールされていないか、**VDA** バージョン **5.x** がインストールされている　VDA 7.x がマスターイメージにインストールされていない場合、イメージの準備は 20 分後にタイムアウトになり、上記のエラーを報告します。これは、イメージ準備段階を実行して成功または失敗を報告するソフトウェアがマスターイメージにインストールされていないためです。これを解決するには、マスターイメージとして選択したスナップショットに VDA（最小バージョン 7）がインストールされていることを確認してください。

DISKPART SAN ポリシー　マスターイメージに設定されている`DISKPART SAN`ポリシーが原因で、イメージ準備段階全体が失敗する可能性があります。イメージ準備の指示ディスクがオンラインになるように設定されていない場合、マシンはシャットダウンされ、イメージ準備は 20 分後にエラーを報告します。マスターイメージでこれを確認するには、次のコマンドを実行します：

```
1 C:>; Diskpart.exe
2 DISKPART>; San
```

このコマンドは、現在のポリシーを返します。*Online All* でない場合は、次のコマンドを実行して変更します：

```
DISKPART>; San policy=OnlineAll
```

マスターイメージをシャットダウンし、そのマシンのスナップショットを作成して、基本 MCS イメージとして使用します。

別の理由でイメージ準備が失敗した場合　イメージの準備が失敗し、エラーの明確な理由がない場合は、MCS カタログを作成するときにイメージの準備プロセスを省略できます。ただし、このプロセスを省略すると、サイトの KMS ライセンス設定とネットワーク設定（DHCP）で問題が発生する可能性があります。次の PowerShell コマンドを使用します:

```
Set-ProvServiceConfigurationData -Name
    ImageManagementPrep_DoImagePreparation -Value $false
```

可能な場合は Citrix サポートチームのログを収集し、フォーラムまたはサポート担当者を介して Citrix に問題を報告してください。ログを収集するには、次を実行します:

1. マスターイメージで次のレジストリキーを作成し、値（「DWORD（32 ビット）の値」）を 1 に設定します: `HKLM\Software\Citrix\MachineIdentityServiceAgent\LOGGING`。
2. マスターイメージを閉じて、スナップショットを作成します。Delivery Controller で、Citrix PowerShell スナップインを読み込んで PowerShell を起動し、`Set-ProvServiceConfigurationData -Name ImageManagementPrep_NoAutoShutdown -Value $True`を実行します。
3. このスナップショットに基づいてカタログを作成します。
4. ハイパーバイザーで準備用仮想マシンが作成されたら、ログインして C ドライブのルートから抽出します:

```
Image-prep.log
PvsVmAgentLog.txt
```

マシンをシャットダウンします。この時点で、エラーが報告されます。

次の PowerShell コマンドを実行して、イメージ準備マシンの自動シャットダウンを再度有効にします:

```
Remove-ProvServiceConfigurationData -Name
ImageManagementPrep_NoAutoShutdown
```

MCS I/O ライトバックキャッシュディスクへの特定のドライブ文字の割り当て

MCS I/O ライトバックキャッシュディスクに特定のドライブ文字を割り当てることができます。この機能の導入は、使用するアプリケーションのドライブ文字と MCS I/O ライトバックキャッシュディスクのドライブ文字の間の競合を回避するのに役立ちます。これを行うには、PowerShell コマンドを使用できます。サポートされているハイパーバイザーは、Azure、GCP、VMware、SCVMM、および XenServer です。

> 注:
>
> この機能では、VDA バージョン 2305 以降が必要です。

制限事項

- Windows オペレーティングシステムのみに適用されます
- ライトバックキャッシュディスクに適用できるドライブ文字：E～Z

- Azure 一時ディスクがライトバックキャッシュディスクとして使用されている場合は適用されません
- 新しいマシンカタログを作成する場合にのみ適用されます

ライトバックキャッシュディスクにドライブ文字を割り当てる

ライトバックキャッシュディスクにドライブ文字を割り当てるには、次の手順を実行します:

1. **PowerShell** ウィンドウを開きます。
2. `asnp citrix*`を実行します。
3. ID プールをまだ作成していない場合は作成します。詳しくは、「Creating a Catalog」を参照してください。
4. `New-ProvScheme`コマンドをプロパティ`WriteBackCacheDriveLetter`で使用してプロビジョニングスキームを作成します。例:

```
New-ProvScheme -CleanOnBoot `
-HostingUnitName "<name>" `
-IdentityPoolName $schemeName `
-ProvisioningSchemeName $schemeName `
-InitialBatchSizeHint 1 `
-UseWriteBackCache -WriteBackCacheDiskSize 127 -
   WriteBackCacheMemorySize 256 -WriteBackCacheDriveLetter E `
-MasterImageVM "XDHyp:\HostingUnits<name>\image.folder\abcd-
   resources.resourcegroup\
   MCSIOMasterVm_OsDisk_1_d3e2d6352xxxxxxxxx2130aa145ec77.
   manageddisk" `
-NetworkMapping @{
 "0"="XDHyp:\HostingUnits\name\virtualprivatecloud.folder\East US.
    region\virtualprivatecloud.folder\abcd-resources.resourcegroup
    \abcd-resources-vnet.virtualprivatecloud\default.network" }
  `
-ServiceOffering "XDHyp:\HostingUnits\<name>\serviceoffering.
   folder\Standard_D2s_v5.serviceoffering" `
-CustomProperties '<CustomProperties xmlns="http://schemas.citrix.
   com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/
   XMLSchema-instance">
<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="
   true" />
<Property xsi:type="StringProperty" Name="OsType" Value="Windows"
   />
<Property xsi:type="StringProperty" Name="StorageType" Value="
   Premium_LRS"/>
<Property xsi:type="StringProperty" Name="PersistWBC" Value="false
   " />
<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="
   false" />
<Property xsi:type="StringProperty" Name="PersistVm" Value="false"
    />
<Property xsi:type="StringProperty" Name="WBCDiskStorageType"
   Value="Premium_LRS" />
```



```
<Property xsi:type="StringProperty" Name="UseTempDiskForWBC" Value
    ="false" />
<Property xsi:type="StringProperty" Name="ResourceGroups" Value="
    abcd-group1" />
<Property xsi:type="StringProperty" Name="LicenseType" Value="
    Windows_Client" />
<Property xsi:type="StringProperty" Name="SchemaVersion" Value="2"
     />
</CustomProperties>'
```

5. カタログの作成を完了します。

MCS マシンカタログを作成する前に構成を検証

New-ProvSchemeコマンドで-validateパラメーターを使用して、MCS マシンカタログを作成する前に構成設定を検証できます。パラメーターを指定してこの PowerShell コマンドを実行すると、間違ったパラメーターが使用されている場合、またはパラメーターが別のパラメーターと競合している場合は、適切なエラーメッセージが表示されます。その後、エラーメッセージを使用して問題を解決し、PowerShell を使用して MCS マシンカタログを正常に作成できます。現在、この機能は Azure、GCP、および VMware 仮想化環境に適用できます。

> 注:
>
> 検証中は、実際の MCS マシンカタログを作成しないでください。コマンドの結果を使用してエラーを修正し、正常なカタログを作成する必要があります。したがって、New-ProvSchemeコマンドの実行中は、偽の ID プール名を使用します。

構成を検証するには、次の手順を実行します:

1. Delivery Controller ホストから PowerShell ウィンドウを開きます。
2. asnp citrix*を実行し、Citrix 固有の PowerShell モジュールをロードします。
3. New-ProvSchemeコマンドを実行し、パラメーター-validateを使用します。コマンドが機能するように偽の ID プール名を指定します。たとえば、

```
$result =New-ProvScheme  -CleanOnBoot -HostingUnitName "vSanRg" -
    IdentityPoolName "mptmpcatalogdemo" -InitialBatchSizeHint 1  -
    MasterImageVM "XDHyp:\HostingUnits\vSanRg\Windows19MasterImage.
    vm\Citrix_XD_NonMachineProfileWin19Machines.snapshot" -
    NetworkMapping @{
 "0"="XDHyp:\HostingUnits\vSanRg\VM Network.network" }
  -ProvisioningSchemeName "MachineProfileW10Machines"  -Scope @()
-VMCpuCount 2  -VM
MemoryMB 6143 -MachineProfile "XDHyp:\HostingUnits\vSanRg\TRW-
    Win11-tpm-BL-TEMPLATE.template" -TenancyType Shared  -
    FunctionalLevel "L7_20" -Validate
$result.TerminatingError | Format-List -Property *
```

エラーメッセージ:


```
ErrorData    : {
 [[ValidationFailureCount, xxx], [InvalidMemoryValue, The memory
    size provided 6143 must be a multiple of 4 MB and must be
    greater than or equal to 4 MB.], [InconsistentGuestOsSetting,
    The GuestOs setting - windows9_64Guest of the selected machine
     profile does not match with the setting -
    windows2019srv_64Guest of master image. Please select a
    machine profile that matches the GuestOs setting of the master
     image.], [InconsistentVtpmSetting, The vTPM setting of the
    selected machine profile does not match with the selected
    master image. Please select a machine profile that matches the
     vTPM setting of the master image.], [
    InconsistentFirmwareSetting, The firmware setting - efi of the
     selected machine profile does not match with the setting -
    bios of master image. Please select a machine profile that
    matches the firmware setting of the master image ErrorId
    : ValidationFailure
ErrorMessage : ValidationFailure
Operation    : ValidatingInputs
```

4. 構成設定を検証した後、実際の ID プール名と正しいパラメーターを使用して MCS マシンカタログを作成できます。

次の手順

特定のクラウドサービスカタログの作成については、次を参照してください:

- AWS カタログの作成
- XenServer カタログの作成
- Google Cloud Platform カタログの作成
- Microsoft Azure カタログの作成
- Microsoft System Center Virtual Machine Manager カタログの作成
- Nutanix カタログの作成
- VMware カタログの作成

最初のカタログを作成すると、Web Studio ではデリバリーグループを作成する手順が表示されます。

構成プロセス全体を確認するには、「インストールと構成」を参照してください。

完全な構成ユーザーインターフェイスと PowerShell を使用して、Citrix Provisioning カタログを作成できるようになりました。
この機能の導入には、次のような利点があります:

- MCS と Citrix Provisioning カタログの両方を管理できる単一の統合コンソール。
- ID 管理ソリューション、オンデマンドプロビジョニングなどの Citrix Provisioning カタログの新機能を利用できる。

現在、この機能は Azure および VMware のワークロードでのみ使用できます。ただし、VMware 環境では、現在 PowerShell コマンドのみを使用してカタログを作成できます。詳しくは、「Citrix Studio での Citrix Provisioning カタログの作成」を参照してください。

追加情報

- 接続とリソースの作成と管理
- さまざまな参加の種類を収めたカタログの作成
- マシンカタログの管理

AWS カタログの作成

August 17, 2024

「マシンカタログの作成」では、マシンカタログを作成するウィザードについて説明します。以下の情報は、AWS 仮想化環境に固有の詳細について説明しています。

> 注:
>
> AWS カタログを作成する前に、AWS への接続の作成を完了する必要があります。「AWS への接続」を参照してください。

イメージの準備中のネットワーク設定

イメージの準備中に、元の仮想マシンに基づいて準備用の仮想マシン（VM）が作成されます。この準備 VM はネットワークから切断されています。ネットワークを準備 VM から切断するために、すべての受信および送信トラフィックを拒否するネットワークセキュリティグループが作成されます。このネットワークセキュリティグループは保持され、再利用されます。ネットワークセキュリティグループの名前は`Citrix.XenDesktop.IsolationGroup-GUID`で、GUID がランダムに生成されます。

AWS テナントの構成

AWS には、次のテナントオプションが用意されています。

- 共有テナント（デフォルトのテナントの種類）：さまざまな顧客の複数の Amazon EC2 インスタンスが同じ物理ハードウェア上に存在することができます。
- 専用テナント：EC2 インスタンスは、ユーザーが展開したほかのインスタンスを含むハードウェア上のみで実行されます。ほかの顧客は同じハードウェアを使用しません。

PowerShell を使用して、MCS で AWS 専用のホストをプロビジョニングすることができます。

PowerShell を使用した **AWS** 専用ホストテナントの構成

PowerShell で定義されたホストテナントを持つマシンのカタログを作成できます。

Amazon [EC2] 専用ホストは、完全に専用の [EC2] インスタンス容量を搭載した物理サーバーです。既存のソケット単位または VM 単位のソフトウェアライセンスを使用することができます。

専用ホストには、インスタンスの種類に基づいて使用率が事前に設定されています。たとえば、C4 ラージインスタンスの種類の 1 つの割り当てられた専用ホストは、16 個のインスタンスの実行に限定されます。詳しくは、AWS のサイトを参照してください。

AWS ホストへのプロビジョニングの要件は次のとおりです:

- インポートされた BYOL（ライセンス持ち込み）のイメージ（AMI）。専用ホストでは、既存のライセンスを使用および管理します。
- プロビジョニング要求を満たすのに十分な使用率を持つ専用ホストの割り当て。
- 自動配置を有効にします。

PowerShell を使用して AWS の専用ホストにプロビジョニングするには、**New-ProvScheme** コマンドレットを、パラメーターTenancyTypeに *Host* を設定して使用します。

詳しくは、Citrix Developer のドキュメントを参照してください。

AMI からマシンのプロパティをキャプチャ

AWS で Machine Creation Services（MCS）を使用してマシンをプロビジョニングするカタログを作成する場合、このカタログのマスター/ゴールデンイメージに相当する AMI を選択します。MCS は、この AMI からディスクのスナップショットを使用します。以前のリリースでは、マシンに役割やタグが必要な場合 AWS コンソールを使用して個別に設定していました。この機能はデフォルトで有効になっています。

> ヒント:
>
> AWS インスタンスプロパティキャプチャを使用するには、AMI に関連付けられた VM が必要です。

このプロセスを改善するために、**MCS** は AMI が作成されたインスタンスからプロパティを読み取り、マシンの ID アクセス管理（IAM）の役割およびタグを提供されたカタログにプロビジョニングされたマシンに適用します。このオプション機能を使用する場合、カタログ作成プロセスでは、選択した AMI ソースインスタンスが検索され、限定されたプロパティセットが読み取られます。これらのプロパティは、そのカタログのマシンをプロビジョニングするために使用される AWS 起動テンプレートに保存されます。カタログ内のすべてのマシンがキャプチャされたインスタンスのプロパティを継承します。

キャプチャされたプロパティには、以下が含まれます:

- IAM 役割–プロビジョニングされたインスタンスに適用

- タグ - プロビジョニングされたインスタンスやそのディスク、NIC に適用。これらのタグは次のような一時的な Citrix リソースに適用されます：S3 バケットおよびオブジェクト、AMI、スナップショット、起動テンプレート。

> ヒント：
>
> 一時的な Citrix リソースのタグ付けはオプションで、カスタムプロパティ `AwsOperationalResourcesTagging` を使用して構成できます。

AWS インスタンスプロパティのキャプチャ

この機能は、AWS ホスト接続でプロビジョニングスキーム作成時にカスタムプロパティ `AwsCaptureInstancePropertie` を指定することで使用できます：

```
New-ProvScheme -CustomProperties "AwsCaptureInstanceProperties,true"
…<standard provscheme parameters
```

詳しくは、Citrix Developer のドキュメントを参照してください。

> 注：
>
> `AwsCaptureInstanceProperties` は廃止済みです。代わりに、マシンプロファイルを使用して VM のマシンプロパティを指定することをお勧めします。

マシンプロファイルからマシンプロパティをキャプチャ

MCS を使用して AWS マシンをプロビジョニングするためのカタログを作成する場合、マシンプロファイルを使用して特定のマシンプロパティ設定を事前設定できます。

そのためには、次の手順を実行します：

1. このカタログを作成しているリソースと同じアベイラビリティゾーンにマシンプロファイルを保存します。
2. カタログ作成ウィザードの ［マシンテンプレート］ ページで、［マシンプロファイルを使用する］ を選択します。選択したリソースと同じ利用可能なゾーンにあるマシンプロファイルが表示されます。
3. 必要に応じてマシンプロファイルを選択します。

> 注：
>
> マシンプロファイルまたは AMI のいずれかを使用して、マシンプロパティをキャプチャできます。Web Studio で、［マシンプロファイルを使用する］ を選択すると、［マシンテンプレートのプロパティを仮想マシンに適用する］ オプションが自動的に非表示になります。

AWS 運用リソースのタグ付け

MCS を使用して AWS でマシンをプロビジョニングするカタログを作成する場合、IAM の役割とタグのプロパティをそれらのマシンに適用するかを制御できます。マシンタグを運用リソースに適用するかを制御することもできます。

Amazon Machine Image（AMI）は、Amazon クラウド環境内で仮想マシンを作成するために使用される、一般に EC2 と呼ばれる仮想アプライアンスの種類を表します。AMI を使用して、EC2 環境を使用するサービスを展開します。AWS で MCS を使用してマシンをプロビジョニングするカタログを作成する場合、このカタログのゴールデンイメージとして機能する **AMI** を選択します。

> 重要:
>
> インスタンスプロパティと起動テンプレートをキャプチャしてカタログを作成することは、運用リソースのタグ付けに必要です。

AWS カタログを作成するには、最初にゴールデンイメージとして使用するインスタンスの AMI を作成する必要があります。MCS は、そのインスタンスからタグを読み取り、起動テンプレートに組み込みます。起動テンプレートタグは、AWS 環境で作成されたすべての Citrix リソースに適用されます。これには以下が含まれます:

- 仮想マシン
- VM ディスク
- VM ネットワークインターフェイス
- S3 バケット
- S3 オブジェクト
- 起動テンプレート
- AMI

運用リソースのタグ付け

PowerShell を使用してリソースにタグを付けるには、次の手順を実行します:

1. DDC ホストから PowerShell ウィンドウを開きます。
2. コマンド`asnp citrix`を実行し、Citrix 固有の PowerShell モジュールをロードします。

プロビジョニングされた仮想マシンのリソースにタグを付けるには、新しいカスタムプロパティ`AwsOperationalResourcesTagging`を使用します。以下はこのプロパティの構文です:

```
New-ProvScheme -CustomProperties "AwsCaptureInstanceProperties,true;
AwsOperationalResourcesTagging,true"…<standard provscheme parameters
>
```


VM 上のタグをコピーする

マシンプロファイルで指定されている NIC およびディスク（ID ディスク、ライトバックキャッシュディスク、OS ディスク）上のタグを、MCS マシンカタログ内に新しく作成された VM にコピーできます。これらのタグは、任意のマシンプロファイルソース（AWS VM インスタンスまたは AWS 起動テンプレートバージョン）で指定できます。この機能は、永続および非永続のマシンカタログと VM に適用できます。

> 注:
>
> - AWS EC2 コンソールでは、**Launch Template Version Resource Tags** の下に **Tag Network Interfaces** の値が表示されません。ただし、PowerShell コマンド`aws ec2 describe-launch-template-versions --launch-template-id lt-0bb652503d45dcbcd --versions 12`を実行してタグの仕様を確認することができます。
> - マシンプロファイルソース（仮想マシンまたは起動テンプレートバージョン）に 2 つのネットワークインターフェイス（eni-1 と eni-2）があり、eni-1 にタグ t1 があり、eni-2 にタグ t2 がある場合、仮想マシンは 2 つのネットワークインターフェイスのタグ両方を取得します。

マシンプロファイルを使用してカタログを作成する

マシンプロファイルを使用して、EC2 インスタンス（VM）からハードウェアプロパティをキャプチャしたり、テンプレートバージョンを起動してプロビジョニングされたマシンに適用したりできます。キャプチャされるプロパティには、たとえば、EBS ボリュームプロパティ、インスタンスの種類、EBS の最適化、CPU オプション、テナントの種類、休止状態機能、およびその他のサポートされている AWS 構成が含まれます。

AWS EC2 インスタンス（VM）または AWS 起動テンプレートのバージョンをマシンプロファイルの入力として使用できます。

> 注:
>
> - EBS ボリュームのプロパティは、マシンプロファイルからの値のみを使用します。
> - MCS は、ボリュームの種類 GP3 の ID ディスクを使用して VM をプロビジョニングします。ボリュームの種類 GP3 は、AWS が提供する最も安価なオプションであるため、この機能によりコストが最小限に抑えられます。この実装は、新しいカタログに追加された VM と、既存のカタログに追加された新しい VM にのみ適用されます。この機能の前に作成された既存の VM では、ID ディスクがリセットされない限り、ボリュームの種類 GP2 の ID ディスクが引き続き使用されます。

重要な注意事項

MCS マシンカタログを作成する際の重要注意事項は以下のとおりです:

- `New-ProvScheme`および`Set-ProvScheme`コマンドにパラメーターを追加すると、パラメーターで指定された値がマシンプロファイルの値を上書きします。

- AwsCaptureInstancePropertiesを**true**として設定し、MachineProfileプロパティを設定しない場合は、IAM の役割とタグのみがキャプチャされます。
- AwsCaptureInstancePropertiesとMachineProfileを同時に設定することはできません。

> ** 注:
>
> AwsCaptureInstancePropertiesは廃止済みです。

- マシンプロファイルが指定されていない場合は、以下のプロパティの値を明示的に指定する必要があります:
  - セキュリティグループ
  - ENI または仮想ネットワーク
- AwsCaptureInstancePropertiesを有効にするか、マシンプロファイルを指定する場合にのみ、AwsOperationalResourcesTaggingを有効にすることができます。

MCS マシンカタログを作成した後の重要な注意事項は以下のとおりです:

- マシンプロファイルベースのカタログのカタログを非マシンプロファイルベースのカタログに変更することはできません。

マシンプロファイルを使用してマシンカタログを作成する

マシンプロファイルを使用してマシンカタログを作成するには、以下の手順を実行します:

1. **PowerShell** ウィンドウを開きます。
2. asnp citrix*を実行し、Citrix 固有の PowerShell モジュールをロードします。
3. ID プールをまだ作成していない場合は作成します。たとえば、

```
1 New-AcctIdentityPool -IdentityPoolName idPool -NamingScheme ms## -
    Domain abcdf -NamingSchemeType Numeric
```

4. New-ProvScheme コマンドを実行します。例:

```
1 New-ProvScheme -ProvisioningSchemeName demet-test-1
2 -HostingUnitUid aa633238-9xxd-4cf6-80e8-232a758a1xx1
3 -IdentityPoolUid 34d5b088-e312-416f-907d-16573xxxxxc4
4 -CleanOnBoot
5 -MasterImageVM 'XDHyp:\HostingUnits\cvad-test-scalestress\citrix-
    demet-ami.0 (ami-0ca813xxxxxx061ef).template'
6 -MachineProfile 'XdHyp:\HostingUnits\cvad-test-scalestress\us-east
    -1a.availabilityzone\machine-profile-instance i (i-0xxxxxxxx).
    vm'
```

5. カタログの作成を完了します。詳しくは、「Citrix PowerShell SDK」を参照してください。

マシンプロファイルの更新

マシンプロファイルを使用して最初にプロビジョニングされたカタログのマシンプロファイルを更新するには、次の手順を実行します。MCS マシンカタログを編集するときに、マシンプロファイルソースのテナントの種類と休止状態機能を変更することもできます。

1. Set-ProvSchemeコマンドを実行します。たとえば、

```
Set-ProvScheme `
-ProvisioningSchemeUid "<ID" `
-MachineProfile "XDHyp:\HostingUnits\abc\us-east-1a.
   availabilityzone\citrix-cvad-machineprofile-instance (i-0
   xxxxxxxx).vm"
```

起動テンプレートのバージョンを使用してカタログを作成する

起動テンプレートのバージョンをマシンプロファイルの入力に使用して、MCS マシンカタログを作成できます。マシンプロファイルカタログの入力に関しては、仮想マシンから起動テンプレートのバージョンに更新したり、起動テンプレートのバージョンから仮想マシンに更新したりすることもできます。

AWS EC2 コンソールでは、起動テンプレートのインスタンス構成情報をバージョン番号とともに指定できます。マシンカタログの作成または更新時に起動テンプレートのバージョンをマシンプロファイルの入力に指定すると、そのバージョンの起動テンプレートのプロパティが、プロビジョニングされた VDA VM にコピーされます。

次のプロパティは、マシンプロファイル入力を使用するか、New-ProvSchemeまたはSet-ProvSchemeコマンドのパラメーターとして明示的に指定して提供できます。これらがNew-ProvSchemeまたはSet-ProvSchemeコマンドで指定された場合、これらのプロパティのマシンプロファイル値よりも優先されます。

- サービスオファリング
- ネットワーク
- セキュリティグループ
- テナントの種類

> 注:
>
> サービスオファリングがマシンプロファイル起動テンプレートで、またはNew-ProvSchemeコマンドのパラメーターとして提供されていない場合は、関連のエラーが発生します。

起動テンプレートのバージョンをマシンプロファイルの入力として使用してカタログを作成するには、次の手順を実行します:

1. **PowerShell** ウィンドウを開きます。
2. asnp citrix*を実行し、Citrix 固有の PowerShell モジュールをロードします。

3. 起動テンプレートに関して、起動テンプレートのバージョン一覧を取得します。例:

```
XDHyp:\HostingUnits\test\test-mp-sard (lt-01xxxxx).launchtemplate>
    ls | Select FullPath
```

4. ID プールを作成していない場合は作成します。例:

```
New-AcctIdentityPool `
-IdentityPoolName "abc11" `
-NamingScheme "abc1-##" `
-NamingSchemeType Numeric `
-Domain "citrix-xxxxxx.local" `
-ZoneUid "xxxxxxxx" `
```

5. マシンプロファイルの入力として起動テンプレートのバージョンを使用してプロビジョニングスキームを作成します。例:

```
New-ProvScheme `
-ProvisioningSchemeName "MPLT1" `
-HostingUnitUid "c7f71f6a-3f45-4xxx-xxxx-xxxxxxxxxx" `
-IdentityPoolUid "bf3a6ba2-1f80-4xxx-xxxx-xxxxxxxxx" `
-MasterImageVM "XDHyp:\HostingUnits\xxxd-ue1a\apollo-non-
   persistent-vda-win2022 (ami-0axxxxxxxxxxx).template" `
-CleanOnBoot `
-MachineProfile "XDHyp:\HostingUnits\xxxx-ue1a\machineprofiletest
   (lt-01xxxxx).launchtemplate\lt-01xxxxx (1).
   launchtemplateversion"
```

6. プロビジョニングスキームをブローカーカタログとして登録します。例:

```
New-BrokerCatalog -Name "MPLT1" `
-AllocationType Random `
-Description "Machine profile catalog" `
-ProvisioningSchemeId fe7df345-244e-4xxxx-xxxxxxxxx `
-ProvisioningType Mcs `
-SessionSupport MultiSession `
-PersistUserChanges Discard
```

7. カタログの作成を完了します。詳しくは、「Citrix PowerShell SDK」を参照してください。

マシンプロファイルカタログの入力に関しては、仮想マシンから起動テンプレートのバージョンに更新したり、起動テンプレートのバージョンから仮想マシンに更新したりすることもできます。例:

- マシンプロファイルカタログの入力を仮想マシンから起動テンプレートのバージョンに更新するには、以下を実行します:

```
Set-ProvScheme -ProvisioningSchemeName "CloudServiceOfferingTest"
    `
-MachineProfile "XDHyp:\HostingUnits\xxxx-ue1a\machineprofiletest
    (lt-0bxxxxxxxxxxxx).launchtemplate\lt-0bxxxxxxxxxxx (1).
   launchtemplateversion"
```


- マシンプロファイルカタログの入力を起動テンプレートのバージョンから仮想マシンに更新するには、以下を実行します:

```
Set-ProvScheme -ProvisioningSchemeName "CloudServiceOfferingTest"
`
-MachineProfile "XDHyp:\HostingUnits\sard-ue1a\us-east-1a.
   availabilityzone\apollo-non-persistent-vda-win2022-2 (i-08
   xxxxxxxxx).vm"
```

OS ディスクと ID ディスクを暗号化する

OS ディスクと ID ディスクの暗号化に使用できる AWS KMS キー（顧客管理キーと AWS 管理キー）を使用して、VM の永続カタログおよび非永続カタログを作成できます。

- AWS 管理キーは毎年自動的にローテーションされます。
- 顧客管理キーは自動ローテーションのオプションであり、手動で管理できます。

KMS キーの詳細については、次の AWS ドキュメントを参照してください:

- AWS KMS について
- 自動キーローテーションの仕組み。

OS ディスクと ID ディスクの暗号化では、次のいずれかを構成します:

- 暗号化されたマスターイメージを使用する（たとえば、KMS キーで暗号化された EBS ルートボリュームを含むインスタンスまたはスナップショットから作成された AMI）
- 暗号化された EBS ルートボリュームを含むマシンプロファイルのソース（VM または起動テンプレート）を使用する。

制限事項

次の制限事項に注意してください:

- MCS は現在、マスターイメージ AMI 上で 1 つのディスクのみをサポートしています。
- 既存の暗号化されていない EBS ボリュームまたはスナップショットを直接暗号化したり、既存の暗号化されたボリュームの KMS キーを変更したりすることはできません。このためには、以下を実行する必要があります:

  1. そのボリュームの新しいスナップショットを作成します。
  2. そのスナップショットから新しいボリュームを作成します。
  3. この新しいボリュームを暗号化します。

次の AWS ドキュメントを参照してください:

- 暗号化されていないリソースの暗号化
- EBS ボリュームの自動暗号化またはデフォルトの暗号化の制限：既存および新しい Amazon EBS ボリュームを自動的に暗号化します。

ディスク暗号化でカタログを作成する

ディスク暗号化で MCS マシンカタログを作成するには、以下を使用します：

- マスターイメージ
- マシンプロファイル

ディスク暗号化にマシンプロファイルの入力を使用する場合の考慮事項：

- マシンプロファイルの入力の KMS キーは、マスターイメージの KMS キーよりも優先されます。
- マシンプロファイルの入力が指定されていない場合は、マスターイメージ AMI の KMS キーを使用してカタログ VM のディスクが暗号化されます。
- マシンプロファイルにブロックデバイスマッピングが存在する場合、マスターイメージテンプレート（AMI）とマシンプロファイルに存在するブロックデバイスが一致する必要があります。たとえば、AMI に`/dev/sda1`定義されたデバイスがある場合、マシンプロファイルにも`/dev/sda1`で定義されたデバイスが必要です。
- マシンプロファイルのソースにキーがなく、マスターイメージが暗号化されていない場合、カタログ VM のディスクは暗号化されません。
- マスターイメージが暗号化されている場合、有効な入力と見なされるためには、マシンプロファイルのソース VM または起動テンプレートに暗号化されたルートボリュームが必要です。

既存のカタログを変更する

既存のカタログを、次が含まれるように、`Set-ProvScheme`を使用して変更できます：

- 新しい KMS キーを含むボリュームがあるマシンプロファイルの入力。
- 新しい KMS キーで暗号化されたマスターイメージテンプレート AMI。

重要な注意事項

- カタログに追加された新しい VM のボリュームは、新しい KMS キーで暗号化されます。
- 既存のマシンプロファイルがある場合に暗号化設定を更新するには、新しいマシンプロファイルで`Set-ProvScheme`を実行します。
- 既存のカタログを、暗号化されたボリュームから暗号化されていないボリュームに変更することはできません。暗号化されたマスター AMI から暗号化されていないマスター AMI へのイメージ更新を実行することはできません。

VM インスタンスのフィルタリング

マシンプロファイル VM として使用する AWS EC2 インスタンスは、マシンカタログを作成して正しく機能させるために互換性が必要です。マシンプロファイルの入力 VM として使用できる AWS EC2 インスタンスを一覧表示するには、Get-HypInventoryItemコマンドを使用できます。このコマンドは、ホスティングユニットで使用可能な VM のインベントリに対して、ページネーションとフィルタリングを実行できます。

ページネーション:

Get-HypInventoryItem は、次の 2 つのページネーションモードをサポートしています:

- ページングモードでは、-MaxRecordsおよび-Skipパラメーターを使用して項目のセットを返します:
  - -MaxRecords: デフォルトは **1** です。これにより、返される項目の数が制御されます。
  - -Skip: デフォルトは **0** です。これは、ハイパーバイザー内の一覧の絶対的な先頭（または絶対的な末尾）からスキップする項目の数を制御します。
- スクロールモードでは、-MaxRecords、-ForwardDirection、および-ContinuationTokenパラメーターを使用してレコードをスクロールできます:
  - -ForwardDirection: デフォルトは **True** です。これは-MaxRecordsとともに使用され、次の一致するレコードのセットまたは前の一致するレコードのセットを返します。
  - -ContinuationToken: 直後（または-ForwardDirectionが **false** の場合は直前）の項目を返しますが、-ContinuationTokenで指定された項目は含まれません。

ページネーションの例:

- 一番下にある名前を持つマシンテンプレートの単一レコードを返します。AdditionalDataフィールドには、TotalItemsCountとTotalFilteredItemsCountが含まれます:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
    -ResourceType template
```

- 一番下にある名前のマシンテンプレート 10 個のレコードを返すには、以下を実行します:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
    -ResourceType template -MaxRecords 10 | select Name
```

- 一番上にある名前で終わるレコードの配列を返すには、以下を実行します:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
    -ResourceType template -ForwardDirection $False -MaxRecords 10
     | select Name
```

- 指定されたContinuationTokenに関連付けられたマシンテンプレートで始まるレコードの配列を返すには、以下を実行します:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
    -ResourceType template -ContinuationToken "ami-07xxxxxxxxx" -
    MaxRecords 10
```


フィルタリング:

フィルタリングでは、次の追加のオプションパラメーターがサポートされています。これらのパラメーターをページネーションオプションと組み合わせることができます。

- -ContainsName "my_name":指定された文字列がAMI名の一部と一致する場合、そのAMIはGet結果に含まれます。例:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
    -ResourceType template -MaxRecords 100 -ContainName  'apollo'
     | select Name
```

- -Tags '{ "Key0": "Value0", "Key1": "Value1", "Key2": "Value2" } ': AMIにこれらのタグの少なくとも1つがある場合、そのAMIはGet結果に含まれます。例:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
    -ResourceType template -MaxRecords 100 -Tags '{
"opex owner": "Not tagged" }
' | select Name
```

> 注:
>
> 2つのタグ値がサポートされています。**Not Tagged**タグ値は、タグの一覧に指定されたタグが含まれていない項目と一致します。**All values**タグ値は、タグの値に関係なくタグを持つ項目と一致します。それ以外の場合、項目にタグがあり、その値がフィルターで指定されたものと等しい場合にのみ一致が発生します。

- -Id "ami-0a2d913927e0352f3": AMIが指定されたIDと一致する場合、そのAMIはGet結果に含まれます。例:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
    -ResourceType template -Id ami-xxxxxxxxxxxx
```

AdditionalDataパラメーターのフィルタリング:

AdditionalDataフィルターパラメーターは、機能、サービスオファリング、またはAdditionalData内のプロパティに基づいてテンプレートまたはVMを一覧表示します。例:

```
(Get-HypInventoryItem -ResourceType "launchtemplateversion" -
    LiteralPath "XDHyp:\HostingUnits\aws" -MaxRecords 200).
    AdditionalData
```

-Warnパラメーターを追加して、互換性のないVMを示すこともできます。このVMは、**Warning**という名前のAdditionalDataフィールドに含まれます。例:

```
(Get-HypInventoryItem -ResourceType "launchtemplateversion" -
    LiteralPath "XDHyp:\HostingUnits\aws" -MaxRecords 200 -Template "ami
    -015xxxxxxxxx" -Warn $true).AdditionalData
```


次の手順

- 最初のカタログを作成すると、Web Studio ではデリバリーグループを作成する手順が表示されます。
- 構成プロセス全体を確認するには、「インストールと構成」を参照してください
- カタログを管理するには、「マシンカタログの管理」と「AWS カタログの管理」を参照してください

追加情報

- 接続とリソースの作成と管理
- AWS への接続
- マシンカタログの作成

XenServer カタログの作成

August 17, 2024

「マシンカタログの作成」では、マシンカタログを作成するウィザードについて説明します。以下の情報は、XenServer 仮想化環境に固有の詳細について説明しています。

> 注:
>
> XenServer カタログを作成する前に、XenServer への接続の作成を完了する必要があります。「XenServer への接続」を参照してください。

XenServer 接続を使用してマシンカタログを作成する

GPU 対応のマシンでは、専用のマスターイメージが必要です。これらの仮想マシンには、GPU をサポートするビデオカードドライバーが必要です。仮想マシンが GPU を使用して稼働するソフトウェアによって動作できるように、GPU 対応のマシンを構成します。

1. XenCenter を使用して、標準的な VGA、ネットワーク、および vCPU を指定して仮想マシンを作成します。
2. 作成した仮想マシンの構成を変更して、GPU 機能（パススルーまたは仮想 GPU）を有効にします。
3. 仮想マシンに適切なオペレーティングシステムをインストールして、RDP を有効にします。
4. Citrix VM Tools と NVIDIA ドライバーをインストールします。
5. パフォーマンスを最適化するため、Virtual Network Computing（VNC）Admin Console をオフにして、仮想マシンを再起動します。
6. RDP の使用を確認するメッセージが表示されます。RDP を使用して VDA をインストールし、仮想マシンを再起動します。
7. 必要に応じて、仮想マシンのスナップショットを作成します。このスナップショットは、ほかの GPU マスターイメージのテンプレートとして使用できます。

8. RDP を使用して、XenCenter で構成され、GPU を使用する顧客固有のアプリケーションをインストールします。

制限事項

- Citrix Hypervisor 8.2 累積更新プログラム 1 でホストされている VM を使用した Citrix Virtual Apps and Desktops の展開で、単一の MCS カタログで複数の GFS2 SR を使用する場合、カタログ内の VM は展開中に VDI にアクセスできません。「VDI は現在使用中です」というエラーが報告されます。
- Citrix Hypervisor 8.2 累積更新プログラム 1 は、MCS 完全クローン仮想マシンでの GFS2 ストレージリポジトリの使用をサポートしていません。

詳しくは、「制約」を参照してください。

これらの制約は XenServer 8 以降には適用されません。

マシンプロファイルを使用してマシンカタログを作成する

MCS を使用してマシンをプロビジョニングするためのカタログを作成する場合、マシンプロファイルを使用して、仮想マシンからハードウェアプロパティをキャプチャし、カタログで新しくプロビジョニングされた VM に適用できます。`MachineProfile`パラメーターが使用されていない場合、ハードウェアプロパティはマスターイメージ VM またはスナップショットからキャプチャされます。

> 注:
>
> 現在、マシンプロファイル入力として使用できるのは VM のみです。

次のパラメーターを明示的に構成して、マシンプロファイル入力のパラメーターの値を上書きできます:

- `VMCpuCount`
- `VMMemory`
- `NetworkMapping`

マシンプロファイルを含むカタログを作成するには、以下の手順を実行します:

1. PowerShell ウィンドウを開きます。
2. `asnp citrix*`を実行します。
3. ID プールを作成します。ID プールは、作成される VM の Active Directory（AD）アカウントのコンテナです。例:

```
1 New-AcctIdentityPool -Domain "citrix-xxxxxx.local" -
      IdentityPoolName "ExampleIdentityPool" -NamingScheme "abc1-##"
      -NamingSchemeType "Numeric" -Scope @() -ZoneUid "xxxxxxxx"
```

4. Active Directory に必要な AD コンピューターアカウントを作成します。


```
$password = "password123" | ConvertTo-SecureString -AsPlainText -
    Force
New-AcctADAccount -IdentityPoolName "ExampleIdentityPool" -Count
    10 -ADUserName "citrix-xxxxxx\admin1" -ADPassword $password
Set-AcctAdAccountUserCert -IdentityPoolName "ExampleIdentityPool"
    -ADUserName "citrix-xxxxxx\admin1" -ADPassword $password
```

5. New-ProvSchemeコマンドを実行してカタログを作成します。例:

```
New-ProvScheme -CleanOnBoot -HostingUnitName "ExampleHostingUnit"
    -IdentityPoolName "ExampleIdentityPool" -InitialBatchSizeHint 2
     -CustomProperties '<CustomProperties xmlns="http://schemas.
    citrix.com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.
    org/2001/XMLSchema-instance">
<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="
    true" />
</CustomProperties>'
-MasterImageVM "XDHyp:\HostingUnits\ExampleHostingUnit\ExampleVDA.
    vm\ExampleVDA.snapshot" -ProvisioningSchemeName "ExampleCatalog
    " -Scope @() -SecurityGroup @()
-MachineProfile "XDHyp:\HostingUnits\ExampleHostingUnit\
    ExampleMachineProfile.vm"
```

6. プロビジョニングスキームをブローカーカタログとして登録します。例:

```
$ConfigZone = Get-ConfigZone | Where-Object {
  $_.Name -eq "xxxxxx"  }

New-BrokerCatalog -Name "MPLT1" -AllocationType Random -
    Description "Machine profile catalog" -ProvisioningSchemeId
    fe7df345-244e-4xxxx-xxxxxxxxx -ProvisioningType Mcs -
    SessionSupport MultiSession -PersistUserChanges Discard -
    ZoneUid ($ConfigZone.Uid)
```

7. VM をマシンカタログに追加します。

新しいマシンプロファイルでマシンカタログを更新するには、次の手順を実行します:

1. Set-ProvSchemeコマンドを実行します。例:

```
Set-ProvScheme -ProvisioningSchemeName "ExampleCatalog" -
    MachineProfile "XDHyp:\HostingUnits\ExampleHostingUnit\
    ExampleMachineProfileVm.vm\ExampleMachineProfileSnapshot.
    snapshot"
```

   Set-ProvScheme コマンドについて詳しくは、「Set-ProvScheme」を参照してください。

> 注:
>
> - この場合、Set-ProvSchemeコマンドは、カタログ内の既存 VM のマシンプロファイルを変更しません。新しいマシンプロファイルは、カタログに追加された新しく作成された VM のみにあります。

> - マシンプロファイルベースのマシンカタログを非マシンプロファイルベースのマシンカタログに変換することはできません。

次の手順

- 最初のカタログを作成すると、Web Studio ではデリバリーグループを作成する手順が表示されます。
- 構成プロセス全体を確認するには、「インストールと構成」を参照してください
- カタログを管理するには、「マシンカタログの管理」と「XenServer カタログの管理」を参照してください

追加情報

- 接続とリソースの作成と管理
- XenServer への接続
- マシンカタログの作成

Google Cloud Platform カタログの作成

August 20, 2024

「マシンカタログの作成」では、マシンカタログを作成するウィザードについて説明します。以下の情報は、Google クラウド環境に固有の詳細について説明しています。

> 注:
>
> Google Cloud Platform（GCP）カタログを作成する前に、GCP への接続の作成を完了する必要があります。「Google クラウド環境への接続」を参照してください。

マスター仮想マシンインスタンスと永続ディスクを準備する

> ヒント:
>
> 永続ディスクは、仮想ディスクを表す Google Cloud の用語です。

マスター仮想マシンインスタンスを準備するには、計画されたマシンカタログの複製された VDA インスタンスに必要な構成と一致するプロパティで仮想マシンインスタンスを作成して構成します。構成は、インスタンスのサイズとタイプのみに適用されるわけではありません。また、メタデータ、タグ、GPU 割り当て、ネットワークタグ、サービスアカウントプロパティなどのインスタンス属性も含まれます。

マスタリングプロセスの一部として、MCS はマスター VM インスタンスを使用して Google Cloud インスタンステンプレートを作成します。次に、インスタンステンプレートを使用して、マシンカタログを構成する複製された VDA

インスタンスを作成します。複製されたインスタンスは、インスタンステンプレートが作成されたマスター仮想マシンインスタンスのプロパティ（VPC、サブネット、および永続ディスクのプロパティを除く）を継承します。

マスター仮想マシンインスタンスのプロパティを仕様に合わせて構成した後、インスタンスを起動し、インスタンスの永続ディスクを準備します。

ディスクのスナップショットを手動で作成することをお勧めします。これにより、意味のある命名規則を使用してバージョンを追跡でき、マスターイメージの以前のバージョンを管理するためのオプションが増え、マシンカタログの作成時間を節約できます。独自のスナップショットを作成しない場合、MCS が一時的なスナップショットを作成します（これはプロビジョニングプロセスの最後に削除されます）。

マシンカタログの作成

マシンカタログは次の 2 つの方法で作成できます。

- Web Studio でのマシンカタログの作成
- PowerShell を使用してマシンカタログを作成する

Web Studio でのマシンカタログの作成

> 注:
>
> マシンカタログを作成する前にリソースを作成してください。マシンカタログを構成するときは、Google Cloud で定められた命名規則を使用します。詳しくは、「バケットとオブジェクトの命名ガイドライン」を参照してください。

「マシンカタログの作成」のガイダンスに従ってください。次の説明は、Google Cloud のカタログに固有の説明です。

1. Web Studio にサインインし、左側のペインで ［マシンカタログ］をクリックします。
2. 操作バーで ［マシンカタログの作成］を選択します。
3. ［オペレーティングシステム］ページで、［マルチセッション **OS**］を選択してから ［次へ］を選択します。
    - Citrix Virtual Apps and Desktops ではシングルセッション OS もサポートしています。
4. ［マシン管理］ページで、［電源管理されているマシン］および ［**Citrix Machine Creation Services**］オプションを選択してから ［次へ］を選択します。複数のリソースがある場合は、メニューから 1 つ選択してください。
5. ［イメージ］ページで、必要に応じて次の手順を実行し、［次へ］をクリックします。
    a) スナップショットまたは VM をマスターイメージとして選択します。単一テナント機能を使用する場合は、必ずノードグループプロパティが正しく構成されているイメージを選択してください。「ゾーン選択の有効化」を参照してください。

b) 既存の VM をマシンプロファイルとして使用するには、［マシンプロファイルを使用する］を選択し、VM を選択します。

> 注:
>
> 現在、このカタログ内の VM は、ディスク暗号化セット ID、マシンサイズ、ストレージの種類、およびゾーン設定をマシンプロファイルから継承します。

c) カタログの最小機能レベルを選択します。単一テナント機能を使用する場合は、必ずノードグループプロパティが正しく構成されているイメージを選択してください。

6. ［ストレージの種類］ページで、このマシンカタログのオペレーティングシステムを格納するために使用するストレージの種類を選択します。次のストレージオプションにはそれぞれ、固有の価格とパフォーマンスの特性があります（ID ディスクは、常にゾーン標準永続ディスクを使用して作成されます）。

   - 標準永続ディスク
   - バランス永続ディスク
   - SSD 永続ディスク

   Google Cloud ストレージオプションについて詳しくは、https://cloud.google.com/compute/docs/disks/を参照してください。

7. ［仮想マシン］ページで、作成する VM の数を指定し、VM の詳細な仕様を表示してから、［次へ］を選択します。マシンカタログに単一テナントノードグループを使用する場合は、予約済み単一テナントノードが使用可能なゾーンのみを選択するようにしてください。「ゾーン選択の有効化」を参照してください。

8. ［コンピューターアカウント］ページで、Active Directory アカウントを選択してから ［次へ］を選択します。

   - ［新しい **Active Directory** アカウントを作成する］を選択する場合、ドメインを選択してから Active Directory で作成されたプロビジョニング済みの VM コンピューターアカウントで名前付けスキームに対応した文字列を入力します。アカウント名前付けスキームに指定できる文字数は 1～64 文字であり、空白スペース、非 ASCII 文字、および特殊文字を含めることはできません。
   - ［既存の **Active Directory** アカウントを使用する］を選択した場合、［参照］を選択し、選択したマシンの既存の Active Directory コンピューターアカウントに移動します。

9. ［ドメイン資格情報］ページで、［資格情報の入力］を選択し、ユーザー名とパスワードを入力し、［保存］を選択してから ［次へ］を選択します。

   - 入力する資格情報には、Active Directory アカウント操作を実行する権限が必要です。

10. ［概要］ページで、情報を確認し、カタログの名前を指定してから、［完了］を選択します。

> 注:
>
> バージョン 2402 以降、GCP カタログ名は次の規則に準拠する必要があります:
>
> - 小文字で始めます。
> - 小文字（a～z）、数字、ハイフンのみを含めます。

> - 小文字または数字で終わります。
>
> これらの規則に準拠していない既存の GCP カタログの名前を変更しようとすると、エラーメッセージが表示され、更新された規則に従って名前を変更するように指示されます。

マシンカタログの作成が完了するまでに時間がかかる場合があります。ターゲットノードグループにマシンが作成されていることを確認するには、Google Cloud コンソールに移動します。

手動で作成した **Google Cloud** マシンのインポート

Google Cloud への接続を作成してから、*Google Cloud* マシンを含むカタログを作成できます。次に、Citrix Virtual Apps and Desktops を使用して、Google Cloud マシンの電源を手動で再投入できます。この機能により、次のことが可能になります:

- 手動で作成した Google Cloud マルチセッション OS マシンを Citrix Virtual Apps and Desktops マシンカタログにインポートします。
- 手動で作成した Google Cloud マルチセッション OS マシンを Citrix Virtual Apps and Desktops カタログから削除します。
- 既存の Citrix Virtual Apps and Desktops の電源管理機能を使用して、Google Cloud Windows マルチセッション OS マシンの電源管理を行います。たとえば、これらのマシンの再起動スケジュールを設定します。

この機能には、Citrix Virtual Apps and Desktops の既存のプロビジョニングワークフローの変更や、既存機能の削除は必要はありません。手動で作成された Google Cloud マシンをインポートする代わりに、MCS を使用して Web Studio でマシンをプロビジョニングすることをお勧めします。

共有仮想プライベートクラウド

共有仮想プライベートクラウド（VPC）は、共有サブネットが使用可能なホストプロジェクトと、リソースを使用する 1 つ以上のサービスプロジェクトで構成されます。共有 VPC は、企業の共有 Google Cloud リソースの制御、使用、管理を一元的に行うため、大規模なインストールでは望ましいオプションです。詳しくは、Google のドキュメントのサイトを参照してください。

この機能により、Machine Creation Services（MCS）は、共有 VPC に展開されたマシンカタログのプロビジョニングと管理をサポートします。このサポートは、現在ローカル VPC で提供されているサポートと同等の機能ですが、次の 2 つの点が異なります:

1. ホスト接続の作成に使用するサービスアカウントに追加の権限を付与する必要があります。このプロセスにより、MCS は共有 VPC リソースにアクセスして使用できるようになります。
2. 受信用と送信用の 2 つのファイアウォール規則を作成する必要があります。これらのファイアウォール規則は、イメージのマスタリングプロセスで使用されます。

新しい権限が必要

ホスト接続を作成するときは、特定の権限を持つ Google Cloud サービスアカウントが必要です。これらの追加の権限は、VPC ベースのホスト接続を作成するために使用されるすべてのサービスアカウントに付与する必要があります。

> ヒント:
>
> これらの追加権限は、Citrix Virtual Apps and Desktops では新しい権限ではありません。これらは、ローカル VPC の実装を容易にするために使用されます。共有 VPC の場合、これらの追加権限により、共有 VPC リソースへのアクセスが許可されます。

共有 VPC をサポートするには、ホスト接続に関連付けられたサービスアカウントに追加の権限を最大 4 つ付与する必要があります:

1. **compute.firewalls.list** - この権限は必須です。これにより、MCS は共有 VPC に存在するファイアウォール規則のリストを取得できます。
2. **compute.networks.list** - この権限は必須です。これにより、MCS がサービスアカウントで使用可能な共有 VPC ネットワークを識別できます。
3. **compute.subnetworks.list** –この権限は、VPC の使用方法に応じてオプションとなります。これにより、MCS は可視の共有 VPC 内のサブネットを識別できます。この権限は、ローカル VPC を使用する場合は既に必須ですが、共有 VPC ホストプロジェクトでも割り当てる必要があります。
4. **compute.subnetworks.use** - この権限は、VPC の使用方法に応じてオプションとなります。プロビジョニングされたマシンカタログでは、サブネットリソースを使用する必要があります。この権限は、ローカル VPC を使用する場合は既に必須ですが、共有 VPC ホストプロジェクトでも割り当てる必要があります。

これらの権限を使用する場合は、マシンカタログの作成に使用する権限の種類によって方法が異なることを考慮してください:

- プロジェクトレベルの権限:
  - ホストプロジェクト内のすべての共有 VPC へのアクセスを許可します。
  - 権限 #3 と #4 をサービスアカウントに割り当てる必要があります。
- サブネットレベルの権限:
  - 共有 VPC 内の特定のサブネットへのアクセスを許可します。
  - 権限 #3 と #4 は、サブネットレベルの割り当てに組み込まれているため、サービスアカウントに直接割り当てる必要はありません。

組織のニーズとセキュリティ基準に合ったアプローチを選択します。

> ヒント:

> プロジェクトレベルとサブネットレベルの権限の違いについて詳しくは、Google Cloud のドキュメントを参照してください。

ファイアウォール規則

マシンカタログの準備中に、カタログのマスターイメージシステムディスクとして機能するマシンイメージが準備されます。このプロセスが発生すると、ディスクは一時的に仮想マシンに接続されます。この VM は、すべての受信および送信ネットワークトラフィックが禁止された、分離された環境で実行する必要があります。これは、2 つの deny-all ファイアウォール規則によって実現されます：1 つは受信トラフィック用で、もう 1 つは送信トラフィック用です。Google Cloud ローカル VCP を使用する場合、MCS はこのファイアウォールをローカルネットワーク上に作成し、マスタリングのためにマシンに適用します。マスタリングが完了すると、ファイアウォール規則がイメージから削除されます。

Shared VPC を使用するために必要な新しい権限の数は最小限に抑えることを推奨します。共有 VPC は、より高レベルの企業リソースであり、通常はより厳格なセキュリティプロトコルを採用しています。このため、共有 VPC リソース上のホストプロジェクトに 2 つのファイアウォール規則を作成します。1 つは受信用、もう 1 つは送信用です。それらに最も高い優先度を割り当てます。次の値を使用して、これらの各規則に新しいターゲットタグを適用します：

```
citrix-provisioning-quarantine-firewall
```

MCS は、マシンカタログを作成または更新するときに、このターゲットタグを含むファイアウォール規則を検索します。次に、規則が正しいかを調べ、カタログのマスターイメージの準備で使用されたマシンにそれを適用します。ファイアウォール規則が見つからない場合、または規則は見つかったが規則やその優先度が正しくない場合には、次のようなメッセージが表示されます：

```
"Unable to find valid INGRESS and EGRESS quarantine firewall rules
for VPC <name> in project <project>. "Please ensure you have created
 'deny all'firewall rules with the network tag 'citrix-provisioning-
quarantine-firewall'and proper priority.""Refer to Citrix Documentation
 for details."
```

共有 **VPC** の構成

Web Studio で共有 VPC をホスト接続として追加する前に、次の手順を実行して、プロビジョニングするプロジェクトのサービスアカウントを追加します：

1. IAM 役割を作成します。
2. CVAD ホスト接続の作成に使用するサービスアカウントを、共有 VPC ホストプロジェクト IAM 役割に追加します。
3. プロビジョニングするプロジェクトの Cloud Build サービスアカウントを、共有 VPC ホストプロジェクト IAM 役割に追加します。
4. ファイアウォール規則を作成します。

IAM 役割を作成する　役割のアクセスレベル（プロジェクトレベルのアクセスか、またはサブネットレベルのアクセスを使用する、より制限されたモデル）を決定します。

IAM 役割のプロジェクトレベルのアクセス。プロジェクトレベルの IAM 役割には、次の権限を含めます：

- compute.firewalls.list
- compute.networks.list
- compute.subnetworks.list
- compute.subnetworks.use

プロジェクトレベルの IAM 役割を作成するには、次の手順を実行します：

1. Google Cloud コンソールで、[**IAM & admin**] **>** [**Roles**] の順に選択します。
2. [**Roles**] ページで、[**CREATE ROLE**] を選択します。
3. [**Create Role**] ページで、役割名を指定します。[**ADD PERMISSIONS**] を選択します。

    a) [**Add permissions**] ページで、役割に権限を個別に追加します。権限を追加するには、[**Filter table**] フィールドで権限の名前を入力します。権限を選択し、[**ADD**] を選択します。
    b) [**CREATE**] を選択します。

サブネットレベルの **IAM** 役割。この役割では、[**CREATE ROLE**] を選択した後、権限`compute.subnetworks.list`と`compute.subnetworks.use`の追加が省略されます。この IAM アクセスレベルでは、新しい役割に権限`compute.firewalls.list`と`compute.networks.list`を適用する必要があります。

サブネットレベルの IAM 役割を作成するには、次の手順を実行します：

1. Google Cloud コンソールで、[**VPC network**] > [**Shared VPC**] に移動します。[**Shared VPC**] ページが開き、ホストプロジェクトに含まれる共有 VPC ネットワークのサブネットが表示されます。
2. [**Shared VPC**] ページで、アクセスするサブネットを選択します。
3. 右上隅にある [**ADD MEMBER**] を選択して、サービスアカウントを追加します。
4. [**Add members**] ページで、次の手順を実行します：

    a) [**New members**] フィールドにサービスアカウントの名前を入力し、メニューでサービスアカウントを選択します。
    b) [**Select a role**] フィールドを選択し、[**Compute Network User**] を選択します。
    c) [**SAVE**] を選択します。

5. Google Cloud コンソールで、[**IAM & admin**] > [**Roles**] の順に選択します。
6. [**Roles**] ページで、[**CREATE ROLE**] を選択します。
7. [**Create Role**] ページで、役割名を指定します。[**ADD PERMISSIONS**] を選択します。

    a) [**Add permissions**] ページで、役割に権限を個別に追加します。権限を追加するには、[**Filter table**] フィールドで権限の名前を入力します。権限を選択し、[**ADD**] を選択します。
    b) [**CREATE**] を選択します。

ホストプロジェクトの **IAM** 役割にサービスアカウントを追加する　IAM 役割を作成した後、次の手順を実行して、ホストプロジェクトのサービスアカウントを追加します:

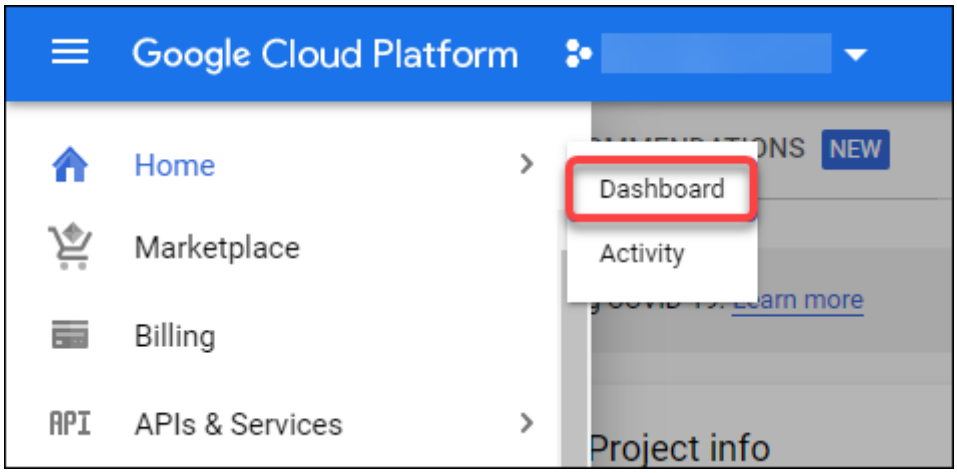
1. Google Cloud コンソールでホストプロジェクトに移動し、[**IAM & admin**] > [**IAM**] の順に選択します。
2. [**IAM**] ページで、[**ADD**] を選択してサービスアカウントを追加します。
3. [**Add members**] ページで、次の操作を行います:

    a) [**New members**] フィールドにサービスアカウントの名前を入力し、メニューでサービスアカウントを選択します。
    b) 役割のフィールドを選択し、作成した IAM 役割を入力して、メニューでその役割を選択します。
    c) [**SAVE**] を選択します。

これで、ホストプロジェクト用のサービスアカウントが構成されました。

Cloud Build サービスアカウントを共有 **VPC** に追加する　すべての Google Cloud サブスクリプションは、プロジェクト ID 番号の後にサービスアカウントが指定され、その後に`cloudbuild.gserviceaccount`が続きます。例: `705794712345@cloudbuild.gserviceaccount`。

プロジェクトのプロジェクト ID 番号を確認するには、Google Cloud コンソールで [**Home**] と [**Dashboard**] を選択します:



画面の [**Project Info**] 領域でプロジェクト番号を探します。

Cloud Build サービスアカウントを共有 VPC に追加するには、次の手順を実行します:

1. Google Cloud コンソールでホストプロジェクトに移動し、[**IAM & admin**] > [**IAM**] の順に選択します。
2. [**Permissions**] ページで、[**ADD**] を選択してアカウントを追加します。
3. [**Add members**] ページで、次の手順を実行します:

    a) [**New members**] フィールドに Cloud Build サービスアカウントの名前を入力し、メニューでサービスアカウントを選択します。
    b) [**Select a role**] フィールドを選択し、`Computer Network User`を入力して、メニューで役割を選択します。

c)［**SAVE**］を選択します。

ファイアウォール規則の作成　マスタリングプロセスの一部として、MCS は選択されたマシンイメージをコピーし、それを使用してカタログ用のマスターイメージシステムディスクを準備します。マスタリングでは、MCS がディスクを一次仮想マシンに接続し、そこで準備スクリプトが実行されます。この VM は、すべての受信および送信ネットワークトラフィックが禁止された、分離された環境で実行する必要があります。分離された環境を作成するには、MCS に 2 つの *deny all* ファイアウォール規則（受信規則と送信規則）が必要です。したがって、ホストプロジェクトに次のように 2 つのファイアウォール規則を作成します：

1. Google Cloud コンソールでホストプロジェクトに移動し、［**VPC network**］**>**［**Firewall**］の順に選択します。
2. ［**Firewall**］ページで、［**CREATE FIREWALL RULE**］を選択します。
3. ［**Create a firewall rule**］ページで、次の操作を行います：
   - 名前。規則名を入力します。
   - **Network**：受信ファイアウォール規則を適用する共有 VPC ネットワークを選択します。
   - **Priority**：値が小さいほど、規則の優先度は高くなります。小さい値（10 など）を指定することをお勧めします。
   - **Direction of traffic**：［**Ingress**］を選択します。
   - **Action on match**：［**Deny**］を選択します。
   - **Targets**：デフォルトの ［**Specified target tags**］を使用します。
   - **Target tags**：「`citrix-provisioning-quarantine-firewall`」と入力します。
   - **Source filter**：デフォルトの ［**IP ranges**］を使用します。
   - **Source IP ranges**：すべてのトラフィックに一致する範囲を入力します。「`0.0.0.0/0`」と入力します。
   - **Protocols and ports**：［**Deny all**］を選択します。
4. ［**CREATE**］を選択して規則を作成します。
5. さらに規則を作成するには、手順 1～4 を繰り返します。［**Direction of traffic**］で、［**Egress**］を選択します。

接続の追加　Google クラウド環境への接続を追加します。「接続の追加」を参照してください。

ゾーン選択の有効化

Citrix Virtual Apps and Desktops では、ゾーン選択をサポートしています。ゾーン選択では、VM を作成するゾーンを指定します。ゾーン選択により、管理者は選択したゾーン間に単一のテナントノードを配置できます。単一テナントを構成するには、Google Cloud で次の手順を実行する必要があります：

- Google Cloud の単一テナントノードを予約する
- VDA マスターイメージを作成する

Google Cloud の単一テナントノードを予約する

単一テナントノードを予約するには、Google Cloud のドキュメントを参照してください。

> 重要:
>
> ノードテンプレートは、ノードグループで予約されているシステムのパフォーマンス特性を示すために使用されます。これらの特性には、vGPU の数、ノードに割り当てられたメモリの量、ノード上に作成されたマシンに使用されるマシンの種類が含まれます。詳しくは、Google Cloud のドキュメントを参照してください。

VDA マスターイメージを作成する

単一テナントノードにマシンを正常に展開するには、マスター VM イメージの作成時に追加の手順を実行する必要があります。Google Cloud 上のマシンインスタンスには、ノードアフィニティラベルと呼ばれるプロパティがあります。単一テナントノードに展開されたカタログのマスターイメージとして使用されるインスタンスには、ターゲットノードグループの名前と一致するノードアフィニティラベルが必要です。これを実現するには、次の点に注意してください:

- 新しいインスタンスの場合は、インスタンスの作成時に Google Cloud コンソールでラベルを設定します。詳しくは、「インスタンスの作成時にノードアフィニティラベルを設定する」を参照してください。
- 既存のインスタンスの場合は、**gcloud** コマンドラインを使用してラベルを設定します。詳しくは、「既存のインスタンスのノードアフィニティラベルを設定する」を参照してください。

> 注:
>
> 共有 VPC で単一テナントを使用する場合は、「共有仮想プライベートクラウド」を参照してください。

インスタンスの作成時にノードアフィニティラベルを設定する　ノードアフィニティラベルを設定するには、次の手順に従います:

1. Google Cloud コンソールで、[**Compute Engine**] > [**VM instances**] に移動します。
2. [**VM instances**] ページで、[**Create instance**] を選択します。
3. [**Instance creation**] ページで、必要な情報を入力または設定し、[**management**]、[**security**]、[**disks**]、[**networking**]、[**sole tenancy**] の順に選択して設定パネルを開きます。
4. [**Sole tenancy**] タブで、[**Browse**] を選択して、現在のプロジェクトで使用可能なノードグループを表示します。[**Sole-tenant node**] ページが開き、使用可能なノードグループのリストが表示されます。
5. [**Sole-tenant node**] ページで、リストから該当するノードグループを選択し、[**Select**] を選択して [**Sole tenancy**] タブに戻ります。[node affinity labels] フィールドに、選択した情報が入力されます。この設定により、インスタンスから作成されたマシンカタログが、選択したノードグループに展開されます。
6. [**Create**] を選択してインスタンスを作成します。

既存のインスタンスのノードアフィニティラベルを設定する　ノードアフィニティラベルを設定するには、次の手順に従います:

1. Google Cloud Shell 端末ウィンドウで、*gcloud compute instances* コマンドを使用してノードアフィニティラベルを設定します。**gcloud** コマンドに次の情報を含めます:

   - 仮想マシンの名前。たとえば、「s*2019-vda-base」という名前の既存の VM を使用します。*
   - ノードグループの名前。以前に作成したノードグループ名を使用します。例: mh-sole-tenant-node-group-1。
   - インスタンスが存在するゾーン。たとえば、仮想マシンは*us-east-1b* zoneにあります。

   たとえば、端末ウィンドウで次のコマンドを入力します:

   - `gcloud compute instances set-scheduling "s2019-vda-base"--node-group="mh-sole-tenant-node-group-1"--zone="us-east1-b"`

   gcloud compute instances コマンドについて詳しくは、Google デベロッパーツールのドキュメント（https://cloud.google.com/sdk/gcloud/reference/beta/compute/instances/set-scheduling）を参照してください。

2. インスタンスの［**VM instance details**］ページに移動し、［**Node Affinities**］フィールドにラベルが入力されていることを確認します。

マシンカタログの作成　ノードアフィニティラベルを設定した後、マシンカタログを構成します。

顧客管理暗号キー（**CMEK**）

MCS カタログでは、顧客管理暗号キー（CMEK: Customer Managed Encryption Keys）を使用できます。この機能を使用する場合は、Google Cloud キー管理サービスのCryptoKey Encrypter/Decrypter役割を Compute Engine サービスエージェントに割り当てます。Citrix Virtual Apps and Desktops のアカウントには、キーが保存されているプロジェクトでの適切な権限が必要です。詳しくは、「Cloud KMS 鍵を使用してリソースを保護する」を参照してください。

Compute Engine サービスエージェントの形式は次のとおりです: service-<Project _Number>@compute-system.iam.gserviceaccount.com。この形式は、デフォルトの Compute Engine サービスアカウントとは異なります。

> 注:
>
> この Compute Engine サービスアカウントは、Google コンソールの［**IAM Permissions**］画面に表示されないことがあります。このような場合は、「Cloud KMS 鍵を使用してリソースを保護する」で説明されているgcloudコマンドを使用します。

Citrix Virtual Apps and Desktops アカウントへの権限の割り当て

Google Cloud KMS の権限はさまざまな方法で設定できます。プロジェクトレベルの KMS 権限、またはリソースレベルの KMS 権限のいずれかを指定できます。詳しくは、「権限と役割」を参照してください。

プロジェクトレベルの権限　1 つのオプションは、Citrix Virtual Apps and Desktops アカウントに Cloud KMS リソースを参照するためのプロジェクトレベルの権限を提供することです。これを行うには、カスタム役割を作成し、次の権限を追加します:

- `cloudkms.keyRings.list`
- `cloudkms.keyRings.get`
- `cloudkms.cryptokeys.list`
- `cloudkms.cryptokeys.get`

Citrix Virtual Apps and Desktops にこのカスタム役割を割り当てます。これにより、インベントリ内の関連プロジェクトの地域キーを参照できます。

リソースレベルの権限　もう 1 つのオプションであるリソースレベルの権限の場合、Google Cloud コンソールで、MCS プロビジョニングに使用する`cryptoKey`を参照します。Citrix Virtual Apps and Desktops アカウントを、カタログプロビジョニングに使用するキーリングまたはキーに追加します。

> ヒント:
>
> このオプションを使用すると、Citrix Virtual Apps and Desktops アカウントに Cloud KMS リソースに対するプロジェクトレベルのリスト権限がないため、インベントリ内のプロジェクトの地域キーを参照できません。ただし、以下で説明する`ProvScheme`カスタムプロパティで正しい`cryptoKeyId`を指定することにより、CMEK を使用してカタログをプロビジョニングできます。

カスタムプロパティを使用した **CMEK** によるプロビジョニング

PowerShell でプロビジョニングスキームを作成するとき は、`ProvScheme CustomProperties`で`CryptoKeyId`プロパティを指定します。例:

```
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
   machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
   instance">
    <Property xsi:type="StringProperty" Name="CryptoKeyId" Value="<
       yourCryptoKeyId>" />
</CustomProperties>'
```

`cryptoKeyId`は次の形式で指定する必要があります:

`projectId:location:keyRingName:cryptoKeyName`

たとえば、リージョンus-east1にあるキーリングmy-example-key-ringのキーmy-example-keyと、ID がmy-example-project-1のプロジェクトを使用する場合、ProvSchemeカスタム設定は次のようになります:

```
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
    machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
    instance">
     <Property xsi:type="StringProperty" Name="CryptoKeyId" Value="my-
        example-project-1:us-east1:my-example-key-ring:my-example-key"
        />
</CustomProperties>'
```

このプロビジョニングスキームに関連するすべての MCS プロビジョニングされたディスクとイメージは、このCMEK（顧客管理暗号キー）を使用します。

> ヒント:
>
> グローバルキーを使用する場合、顧客プロパティの場所はリージョン名ではなくglobalである必要があります。上記の例では、**us-east1** です。例: <Property xsi:type="StringProperty"Name="CryptoKeyId"Value="my-example-project-1:global:my-example-key-ring:my-example-key"/>。

顧客管理キーの交換

Google Cloud では、既存の永続ディスクまたはイメージでのキーの交換をサポートしていません。マシンがプロビジョニングされると、作成時に使用されていたバージョンのキーに関連付けられます。ただし、新しいバージョンのキーを作成することはでき、その新しいキーは、カタログが新しいマスターイメージで更新されたときに作成される、新しくプロビジョニングされたマシンまたはリソースに使用されます。

キーリングに関する重要な注意事項　キーリングの名前を変更したり、削除したりすることはできません。また、構成時に予期しない料金が発生する場合があります。キーリングを削除すると、Google Cloud は次のエラーメッセージを表示します:

```
Sorry, you can't delete or rename keys or key rings. We were concerned
    about the security implications of allowing multiple keys or key
    versions over time to have the same resource name, so we decided to
    make names immutable. (And you can't delete them, because we wouldn'
    t be able to do a true deletion--there would still have to be a
    tombstone tracking that this name had been used and couldn't be
    reused).
We're aware that this can make things untidy, but we have no immediate
    plans to change this.
If you want to avoid getting billed for a key or otherwise make it
    unavailable, you can do so by deleting all the key versions; neither
     keys nor key rings are billed for, just the active key versions
    within the keys.
```


> ヒント：
>
> 詳しくは、「Editing or deleting a key ring from the console」を参照してください。

均一なバケットレベルのアクセスの互換性

Citrix Virtual Apps and Desktops は、Google Cloud の均一なバケットレベルのアクセス制御ポリシーと互換性があります。この機能は、サービスアカウントにアクセス許可を付与して、ストレージバケットなどのリソースの操作を許可する IAM ポリシーの使用を強化します。均一なバケットレベルのアクセス制御により、Citrix Virtual Apps and Desktops では、アクセス制御リスト（ACL）を使用して、ストレージバケットまたはそれらに格納されているオブジェクトへのアクセスを制御できます。Google Cloud の均一なバケットレベルのアクセスに関する概要情報については、「均一なバケットレベルのアクセス」を参照してください。構成情報については、「均一なバケットレベルのアクセス」を参照してください。

PowerShell を使用してマシンカタログを作成する

このセクションでは、PowerShell を使用してカタログを作成する方法について説明します。

- 永続的なライトバックキャッシュディスクのカタログを作成する
- MCSIO による起動パフォーマンスの向上
- マシンプロファイルを使用してマシンカタログを作成する
- インスタンステンプレートとしてマシンプロファイルを使用してマシンカタログを作成する
- PowerShell を使用してシールドされた仮想マシンでカタログを作成する
- 単一テナントノードに Windows 11 VM を作成する

永続的なライトバックキャッシュディスクのカタログを作成する

永続的なライトバックキャッシュディスクのカタログを構成するには、PowerShell パラメーター`New-ProvScheme CustomProperties`を使用します。

> ヒント：
>
> ここで、PowerShell パラメーターはクラウドベースのホスティング接続にのみ使用してください。オンプレミスソリューション（XenServer など）で永続的なライトバックキャッシュディスクを使用してマシンをプロビジョニングする場合、ディスクは自動的に永続化されるため、PowerShell は必要ありません。

このパラメーターでは追加プロパティ`PersistWBC`をサポートしており、これを使用することで、MCS でプロビジョニングされたマシンのライトバックキャッシュディスクを永続化させる方法を指定できます。`PersistWBC`プロパティは、`UseWriteBackCache`パラメーターが指定され、`WriteBackCacheDiskSize`パラメーターがディスクが作成されたことを示すよう設定された場合のみ使用されます。

> 注:
>
> この動作は、電源を入れ直したときにデフォルトの MCSIO ライトバックキャッシュディスクが削除されて再作成される Azure および GCP の両方に適用されます。ディスクを永続化すると、MCSIO ライトバックキャッシュディスクの削除と再作成を回避できます。

プロパティ［PersistWBC］を「**true**」に設定すると、Citrix Virtual Apps and Desktops 管理者が管理インターフェイスでマシンをシャットダウンしたときに、ライトバックキャッシュディスクが消去されません。

プロパティ［PersistWBC］を「**false**」に設定すると、Citrix Virtual Apps and Desktops 管理者が管理インターフェイスでマシンをシャットダウンしたときに、ライトバックキャッシュディスクが消去されます。

> 注:
>
> プロパティ［PersistWBC］を省略すると、デフォルトが「**false**」になるので、管理インターフェイスでマシンをシャットダウンしたときにライトバックキャッシュが消去されます。

たとえば、CustomProperties パラメーターを使用して［PersistWBC］を「**true**」に設定する場合を考えましょう:

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
   machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
   instance">
<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true"
    />
<Property xsi:type="StringProperty" Name="StorageAccountType" Value="
   Premium_LRS" />
<Property xsi:type="StringProperty" Name="ResourceGroups" Value="
   benvaldev5RG3" />
<Property xsi:type="StringProperty" Name="PersistWBC" Value="true" />
</CustomProperties>
```

> 注:
>
> PersistWBCプロパティは、New-ProvScheme PowerShell コマンドレットを使用してのみ設定できます。作成後にプロビジョニングスキームのCustomPropertiesを変更しようとしても、マシンがシャットダウンしたときにマシンカタログやライトバックキャッシュディスクの永続性は影響を受けません。

例: プロパティ［PersistWBC］を「**true**」に設定してライトバックキャッシュを使用するようにNew-ProvSchemeを設定すると、次のようになります:

```
New-ProvScheme
-CleanOnBoot
-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com
   /2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/
   XMLSchema-instance`"><Property xsi:type=`"StringProperty`" Name=`"
   UseManagedDisks`" Value=`"true`" /><Property xsi:type=`"
   StringProperty`" Name=`"StorageAccountType`" Value=`"Premium_LRS`"
   /><Property xsi:type=`"StringProperty`" Name=`"ResourceGroups`"
   Value=`"benvaldev5RG3`" /><Property xsi:type=`"StringProperty`" Name
   =`"PersistWBC`" Value=`"true`" /></CustomProperties>"
```



```
-HostingUnitName "adSubnetScale1"
-IdentityPoolName "BV-WBC1-CAT1"
-MasterImageVM "XDHyp:\HostingUnits\adSubnetScale1\image.folder\
   GoldImages.resourcegroup\W10MCSIO-01
   _OsDisk_1_a940e6f5bab349019d57ccef65d2c7e3.manageddisk"
-NetworkMapping @{
 "0"="XDHyp:\HostingUnits\adSubnetScale1\virtualprivatecloud.folder\
    CloudScale02.resourcegroup\adVNET.virtualprivatecloud\
    adSubnetScale1.network" }

-ProvisioningSchemeName "BV-WBC1-CAT1"
-ServiceOffering "XDHyp:\HostingUnits\adSubnetScale1\serviceoffering.
   folder\Standard_D2s_v3.serviceoffering"
-UseWriteBackCache
-WriteBackCacheDiskSize 127
-WriteBackCacheMemorySize 256
```

MCSIO による起動パフォーマンスの向上

MCSIO が有効な場合、Azure や GCP の管理対象ディスクの起動パフォーマンスを向上させることができます。New-ProvSchemeコマンドで PowerShell カスタムプロパティPersistOSDiskを使用してこの機能を構成します。New-ProvSchemeに関連するオプションは次のとおりです:

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
   machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
   instance">
<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true"
    />
<Property xsi:type="StringProperty" Name="StorageAccountType" Value="
   Premium_LRS" />
<Property xsi:type="StringProperty" Name="Resource ``````<!--NeedCopy
   -->
````````Groups" Value="benvaldev5RG3" />
<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="true"
   />
</CustomProperties>
```

この機能を有効にするには、カスタムプロパティ［PersistOSDisk］を「**true**」に設定します。例:

```
New-ProvScheme
-CleanOnBoot
-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com
   /2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/
   XMLSchema-instance`"><Property xsi:type=`"StringProperty`" Name=`"
   UseManagedDisks`" Value=`"true`" /><Property xsi:type=`"
   StringProperty`" Name=`"StorageAccountType`" Value=`"Premium_LRS`"
   /><Property xsi:type=`"StringProperty`" Name=`"ResourceGroups`"
   Value=`"benvaldev5RG3`" /><Property xsi:type=`"StringProperty`" Name
   =`"PersistOsDisk`" Value=`"true`" /></CustomProperties>"
-HostingUnitName "adSubnetScale1"
-IdentityPoolName "BV-WBC1-CAT1"
```


```

```
-MasterImageVM "XDHyp:\HostingUnits\adSubnetScale1\image.folder\
   GoldImages.resourcegroup\W10MCSIO-01
   _OsDisk_1_a940e6f5bab349019d57ccef65d2c7e3.manageddisk"
-NetworkMapping @{
 "0"="XDHyp:\HostingUnits\adSubnetScale1\virtualprivatecloud.folder\
    CloudScale02.resourcegroup\adVNET.virtualprivatecloud\
    adSubnetScale1.network" }

-ProvisioningSchemeName "BV-WBC1-CAT1"
-ServiceOffering "XDHyp:\HostingUnits\adSubnetScale1\serviceoffering.
   folder\Standard_D2s_v3.serviceoffering"
-UseWriteBackCache
-WriteBackCacheDiskSize 127
-WriteBackCacheMemorySize 256
```

マシンプロファイルを使用してマシンカタログを作成する

Machine Creation Services（MCS）を使用してマシンをプロビジョニングするためのカタログを作成する場合、マシンプロファイルを使用して、仮想マシンからハードウェアプロパティをキャプチャし、カタログで新しくプロビジョニングされた VM に適用できます。`MachineProfile`パラメーターが使用されていない場合、ハードウェアプロパティはマスターイメージ VM またはスナップショットからキャプチャされます。
明示的に定義する一部のプロパティ（`StorageType`、`CatalogZones`、`CryptoKeyIs`など）は、マシンプロファイルから無視されます。

- マシンプロファイルを含むカタログを作成するには、`New-ProvScheme`コマンドを使用します。例: `New-ProvScheme -MachineProfile "path to VM"`。`MachineProfile`パラメーターを指定しない場合、ハードウェアプロパティはマスターイメージ VM からキャプチャされます。
- 新しいマシンプロファイルでカタログを更新するには、`Set-ProvScheme`コマンドを使用します。例: `Set-ProvScheme -MachineProfile "path to new VM"`。このコマンドは、カタログ内の既存 VM のマシンプロファイルを変更しません。新しいマシンプロファイルは、カタログに追加された新しく作成された VM のみにあります。
- マスターイメージを更新することもできますが、マスターイメージを更新しても、ハードウェアプロパティは更新されません。ハードウェアプロパティを更新する場合は、`Set-ProvScheme`コマンドを使用してマシンプロファイルを更新する必要があります。これらの変更は、カタログ内の新しいマシンにのみ適用されます。既存マシンのハードウェアプロパティを更新する場合、`-StartsNow`および`-DurationInMinutes -1`パラメーターを指定した`Set-ProvVMUpdateTimeWindow`コマンドを使用できます。

  > 注:
  >
  > - `StartsNow`は、スケジュールの開始時刻が現在時刻であることを指定します。
  > - 負の数（-1 など）の`DurationInMinutes`は、スケジュールの期間に上限がないことを示します。

インスタンステンプレートとしてマシンプロファイルを使用してマシンカタログを作成する

マシンプロファイルの入力として GCP インスタンステンプレートを選択できます。インスタンステンプレートは GCP のライトウェイトリソースであるため、費用対効果が非常に高くなります。

インスタンステンプレートとしてマシンプロファイルを使用して新しいマシンカタログを作成する

1. PowerShell ウィンドウを開きます。
2. `asnp citrix*`を実行し、Citrix 固有の PowerShell モジュールをロードします。
3. 次のコマンドを使用して、GCP プロジェクトでインスタンステンプレートを見つけます:

```
cd XDHyp:\HostingUnits<HostingUnitName>\instanceTemplates.folder
```

4. NewProvScheme コマンドを使用して、インスタンステンプレートとしてマシンプロファイルを使用して新しいマシンカタログを作成します:

```
New-ProvScheme -ProvisioningSchemeName <CatalogName>  -
    HostingUnitName <HostingUnitName> -IdentityPoolName <identity
    pool name> -MasterImageVM
XDHyp:\HostingUnits<HostingUnitName> \Base.vm\Base.snapshot -
    MachineProfile XDHyp:\HostingUnits<HostingUnitName>\
    instanceTemplates.folder\mytemplate.template
```

   New-ProvScheme コマンドについて詳しくは、「https://developer-docs.citrix.com/projects/citrix-daas-sdk/en/latest/MachineCreation/New-ProvScheme/」を参照してください。

5. PowerShell コマンドを使用して、マシンカタログの作成を完了します。Remote PowerShell SDK を使用してカタログを作成する方法については、https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/を参照してください。

インスタンステンプレートを既存のマシンカタログのマシンプロファイルに変更する

インスタンステンプレートを既存のマシンカタログのマシンプロファイルに変更する詳細な手順は、次のとおりです:

1. PowerShell ウィンドウを開きます。
2. `asnp citrix*`を実行し、Citrix 固有の PowerShell モジュールをロードします。
3. 次のコマンドを実行します:

```
Set-ProvScheme -ProvisioningSchemeName  <CatalogName> -
    MachineProfile XDHyp:\HostingUnits<HostingUnitName>\
    instanceTemplates.folder<TemplateName>.template
```


Set-ProvScheme コマンドについて詳しくは、「https://developer-docs.citrix.com/projects/citrix-daas-sdk/en/latest/MachineCreation/Set-ProvScheme/」を参照してください。

PowerShell を使用してシールドされた仮想マシンでカタログを作成する

シールドされた仮想マシンプロパティを使用して MCS マシンカタログを作成できます。シールドされた仮想マシンは、セキュアブート、仮想トラステッドプラットフォームモジュール、UEFI ファームウェア、整合性監視などの高度なプラットフォームセキュリティ機能を使用して、Compute Engine インスタンスの検証可能な整合性を提供する一連のセキュリティ制御によって強化されます。

MCS は、マシンプロファイルワークフローを使用したカタログの作成をサポートしています。マシンプロファイルワークフローを使用する場合は、仮想マシンインスタンスのシールドされた仮想マシンプロパティを有効にする必要があります。その後、この仮想マシンインスタンスをマシンプロファイルの入力で使用できます。

マシンプロファイルワークフローを使用して、シールドされた仮想マシンで MCS マシンカタログを作成するには、次の手順に従います。

1. Google Cloud コンソールで仮想マシンインスタンスのシールドされた仮想マシンオプションを有効にします。「クイックスタート: Shielded VM オプションを有効にする」を参照してください。
2. 仮想マシンインスタンスを使用して、マシンプロファイルワークフローで MCS マシンカタログを作成します。
   a) PowerShell ウィンドウを開きます。
   b) `asnp citrix*`を実行し、Citrix 固有の PowerShell モジュールをロードします。
   c) ID プールをまだ作成していない場合は作成します。
   d) `New-ProvScheme`コマンドを実行します。例:

```
New-ProvScheme -ProvisioningSchemeName <catalog-name>
-HostingUnitName gcp-hostint-unit
-MasterImageVM XDHyp:\HostingUnits\gcp-hostint-unit\catalog-vda.vm
-MachineProfile XDHyp:\HostingUnits\gcp-hostint-unit\catalog-machine.vm
```

3. マシンカタログの作成を完了します。

新しいマシンプロファイルでマシンカタログを更新するには、次の手順を実行します:

1. `Set-ProvScheme`コマンドを実行します。例:

```
Set-ProvScheme -ProvisioningSchemeName <catalog-name>
-MasterImageVM XDHyp:\HostingUnits<hostin-unit>\catalog-vda.vm
-MachineProfile "DHyp:\HostingUnits<hostin-unit>\catalog-machine.vm
```


Set-ProvSchemeで行った変更を既存の仮想マシンに適用するには、Set-ProvVMUpdateTimeWindowコマンドを実行します。

1. Set-ProvVMUpdateTimeWindowコマンドを実行します。例:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog -
    VMName <List-Of-Vm-Names> -StartsNow -DurationInMinutes -1
```

2. VM を再起動します。

単一テナントノードに **Windows 11 VM** を作成する

GCP で Windows 11 VM を作成できます。ただし、マスターイメージに Windows 11 をインストールする場合は、マスターイメージの作成プロセス中に vTPM を有効にする必要があります。また、マシンプロファイルソース（VM またはインスタンステンプレート）で vTPM を有効にする必要があります。

単一テナントノードに Windows 11 VM を作成するための主な手順は次のとおりです:

1. Google Cloud 仮想化環境をセットアップします。詳しくは、「Google Cloud 環境」を参照してください。
2. VDA のインストール。「VDA のインストール」を参照してください。
3. Google クラウド環境への接続を作成します。詳しくは、「Google クラウド環境への接続」を参照してください。
4. Windows 11 のライセンス持ち込み（BYOL）マスターイメージを作成し、そのイメージを Google Cloud にインポートします。「Windows 11 BYOL マスターイメージを作成する」を参照してください。
5. マシンプロファイルソースを作成します。単一テナントノードで VM をプロビジョニングし、ソースマシンプロファイルの vTPM を有効にします。「単一テナントノードに VM をプロビジョニングする」を参照してください。
6. vTPM が有効になっている Windows 11 マシンプロファイルソースを使用して、MCS マシンカタログを作成します。マシンプロファイルソースは、単一テナントノードで説明されているものと同じインスタンスの種類である必要があります。「Windows 11 マシンプロファイルソースを使用して MCS マシンカタログを作成する」を参照してください。

Windows 11 BYOL マスターイメージを作成する

Windows 11 BYOL マスターイメージを作成し、そのマスターイメージを Google Cloud にインポートするには、次の 2 つのオプションがあります:

- Google Cloud Cloud Build ツールを使用する
- 他のハイパーバイザー上にマスターイメージを作成する

Google Cloud Cloud Build ツールを使用する

1. Windows 11 ISO、GCP SDK、.NET フレームワーク、PowerShell インストーラーファイルを GCP ストレージバケットにアップロードします。
2. Cloud Build `.yaml`ファイル内のファイルの場所をパラメーターとして指定します。
3. 最終的な Windows 11 イメージを構築するには、コマンドラインから次の Cloud Build を実行します。GCP は、GCP の Daisy ワークフローを使用して、選択したプロジェクトでマスターイメージをブートストラップして作成し、マスターイメージを GCP にインポートします。

```
gcloud compute instances import INSTANCE-NAME--source-uri=gs://
    BUCKET/IMAGE-OVF-FILE.ovf --guest-os-features=UEFI_COMPATIBLE
    --byol --machine-type=MACHINE-TYPE --zone=ZONE
```

> 注:
>
> すべての大文字のテキストを実際のリソースの詳細に置き換えます。

詳しくは、「カスタム Windows BYOL イメージを作成する」を参照してください。

他のハイパーバイザー上にマスターイメージを作成する

1. 他のハイパーバイザーを使用して Windows 11 マスターイメージを作成します。
2. マスターイメージを OVF 形式でローカルマシンにエクスポートします。
3. ローカル gcloud CLI を使用して、OVF ファイルを GCP ストレージバケットにアップロードします。

```
gsutil cp LOCAL_IMAGE_PATH_OVF_FILES gs://BUCKET_NAME/
```

4. 最終的な Windows 11 イメージを構築するには、コマンドラインから次の Cloud Build を実行します。GCP は、GCP の Daisy ワークフローを使用して、選択したプロジェクトでマスターイメージをブートストラップして作成し、マスターイメージを GCP にインポートします。

```
gcloud compute instances import INSTANCE-NAME --source-uri=gs://
    BUCKET/IMAGE-OVF-FILE.ovf --guest-os-features=UEFI_COMPATIBLE
    --byol --machine-type=MACHINE-TYPE --zone=ZONE
```

> 注:
>
> すべての大文字のテキストを実際のリソースの詳細に置き換えます。

単一テナントノードに **VM** をプロビジョニングする

単一テナントノードを使用すると、VM を他のプロジェクトの VM から物理的に分離したり、同じホストハードウェア上で VM をグループ化したりできます。単一テナントノードについて詳しくは、GCP ドキュメントの「単一手ナンシーの概要」を参照してください。

単一テナントノードで VM（マシンプロファイルソース）をプロビジョニングする方法については、GCP ドキュメントの「単一テナントノードに VM をプロビジョニングする」を参照してください。

> 注:
>
> - ノードグループと同じインスタンスの種類とリージョンを選択します。
> - Shielded VM セクションで vTPM を有効にします。詳しくは、「クイックスタート: Shielded VM オプションを有効にする」を参照してください。
> - ソース VM 上の Bitlocker を無効にします。

Windows 11 マシンプロファイルソースを使用して **MCS** マシンカタログを作成する

Web Studio または PowerShell コマンドを使用して、MCS マシンカタログを作成し、Windows 11 VM を作成できます。

> 注:
>
> - マスターイメージには、Windows 11 スナップショットまたは VM を選択します。
> - マシンプロファイルソースには、マシンプロファイルとして Windows 11 VM を選択します。マシンプロファイルソースは、単一テナントノードで説明されているものと同じインスタンスの種類である必要があります。

Web Studio の使用について詳しくは、「Web Studio でのマシンカタログの作成」を参照してください。

PowerShell コマンドについて詳しくは、「マシンプロファイルを使用してマシンカタログを作成する」を参照してください

カタログを作成して VM の電源をオンにすると、Google Cloud コンソールの単一テナントノードで実行されている Windows 11 VM を確認できます。

継承されたラベルを持つ **VM** とディスク

MCS マシンカタログの VM とディスク（ID ディスク、ライトバックキャッシュディスク、OS ディスク）は、マシンプロファイルのソース（GCP VM インスタンスまたはインスタンステンプレート）のラベルを継承できます。ラベルを使用して、異なるチームが所有するインスタンスを区別することができ（たとえば、team:research と team:analytics)、さらに原価計算や予算編成にも活用できます。ラベルについて詳しくは、GCP ドキュメント「ラベルを使用してリソースを整理する」を参照してください。

マシンプロファイルのソースを使用して、新しいカタログを作成したり、既存のカタログを更新したり、既存の VM を更新してラベルを継承したりできます。

この機能は、永続および非永続の MCS マシンカタログに適用できます。

以下の操作を実行できます:

- 継承されたラベルのあるカタログを作成する
- 継承されたラベルを使用して既存のカタログを更新する

- 継承されたラベルで既存の VM を更新する
- VM と起動ディスクのラベルの情報を取得する
- VM を削除する

継承されたラベルのあるカタログを作成する

VM とディスクがマシンプロファイルのソースからラベルを継承する MCS マシンカタログを作成するには、次の手順を実行します:

1. ラベル付きのマシンプロファイルのソース（VM インスタンスまたはインスタンステンプレート）を作成します。ラベル付きの VM の作成について詳しくは、GCP ドキュメント「ラベルを適用したリソースを作成する」を参照してください。インスタンステンプレートは VM から作成され、VM で定義されたラベルを取得します。
2. 完全な構成または PowerShell コマンドを使用して、MCS マシンカタログを作成します。
3. 完全な構成インターフェイスを使用する場合は、［イメージ］ページで ［マシンプロファイルを使用する］を選択し、VM またはテンプレートを選択します。
4. PowerShell コマンドを使用する場合は、次を実行します:

   a) PowerShell ウィンドウを開きます。

   b) asnp citrix* を実行します。

   c) ID プールを作成します。ID プールは、作成される VM の Active Directory（AD）アカウントのコンテナです。

   d) Active Directory に必要な AD コンピューターアカウントを作成します。

   e) `New-ProvScheme`コマンドを実行してカタログを作成します。例:

   New-ProvScheme と、テンプレートをマシンプロファイルの入力として使用する（永続カタログ）:

```
New-ProvScheme `
-ProvisioningSchemeName "catalog-name" `
-HostingUnitUid "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" `
-IdentityPoolUid "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" `
-MasterImageVM "XDHyp:\HostingUnits\hosting-unit-name\vm-name.
   vm" `
-MachineProfile "XDHyp:\HostingUnits\hosting-unit-name\
   instanceTemplates.folder\instance-template-name.template" `
```

   New-ProvScheme と、インスタンステンプレートをマシンプロファイルの入力として使用する（非永続カタログ）:

```
New-ProvScheme `
-ProvisioningSchemeName "catalog-name" `
-HostingUnitUid "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" `
-IdentityPoolUid "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" `
```



```
-MasterImageVM "XDHyp:\HostingUnits\hosting-unit-name\vm-name.vm" `
-MachineProfile "XDHyp:\HostingUnits\hosting-unit-name\instanceTemplates.folder\instance-template-name.template" `
-CleanOnBoot
```

New-ProvScheme と、VM インスタンスをマシンプロファイルの入力として使用する（永続カタログ）：

```
New-ProvScheme `
-ProvisioningSchemeName "catalog-name" `
-HostingUnitUid "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" `
-IdentityPoolUid "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" `
-MasterImageVM "XDHyp:\HostingUnits\hosting-unit-name\vm-name.vm" `
-MachineProfile "XDHyp:\HostingUnits\hosting-unit-name\vm-name.vm" `
```

New-ProvScheme と、VM インスタンスをマシンプロファイルの入力として使用する（非永続カタログ）：

```
New-ProvScheme `
-ProvisioningSchemeName "catalog-name" `
-HostingUnitUid "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" `
-IdentityPoolUid "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" `
-MasterImageVM "XDHyp:\HostingUnits\hosting-unit-name\vm-name.vm" `
-MachineProfile "XDHyp:\HostingUnits\hosting-unit-name\vm-name.vm" `
-CleanOnBoot
```

f) プロビジョニングスキームをブローカーカタログとして登録します。

g) VM をマシンカタログに追加します。

継承されたラベルを使用して既存のカタログを更新する

新しいマシンプロファイルのために既存のカタログを更新するには、Set-ProvScheme コマンドを使用します。コマンドを実行すると、カタログに追加されたすべての新しい VM に、新しいマシンプロファイルのソースのラベルが付けられます。非永続カタログは、次回の電源投入時に更新されます。

例：

Set-ProvScheme と、インスタンステンプレートをマシンプロファイルの入力として使用する：

```
Set-ProvScheme `
-ProvisioningSchemeName "catalog-name" `
-MachineProfile "XDHyp:\HostingUnits\hosting-unit-name\instanceTemplates.folder\instance-template-name.template" `
```

Set-ProvScheme と、VM インスタンスをマシンプロファイルの入力として使用する：


```
Set-ProvScheme `
-ProvisioningSchemeName "catalog-name" `
-MachineProfile "XDHyp:\HostingUnits\hosting-unit-name\vm-name.vm" `
```

継承されたラベルで既存の **VM** を更新する

更新されたマシンプロファイルのソースを使用して既存の VM を更新するには、次のコマンドを実行します:

1. `Set-ProvScheme`
2. `Set-ProvVMUpdateTimeWindow`。例:

   ```
   Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog -
       VMName <List-Of-Vm-Names> -StartsNow -DurationInMinutes -1
   ```

3. VM を再起動します。

VM と起動ディスクのラベルの情報を取得する

VM を作成した後、`AdditionalData`パラメーターを指定した`Get-Item`コマンドを使用して、VM と起動ディスクラベルの情報を取得できます。

VM ラベルの情報を取得するには、次のコマンドを実行します:

```
(Get-Item XDHyp:\HostingUnits\hosting-unit-name\vm_name.vm).
   AdditionalData.Tags
```

起動ディスクラベルの情報を取得するには、次のコマンドを実行します:

```
(Get-Item XDHyp:\HostingUnits\hosting-unit-name\vm_name.vm\bootdisk-
   name.attacheddisk).AdditionalData.Tags
```

> 注:
>
> 当社は、さまざまなハイパーバイザー間で一貫性を保つために、「タグ」という用語を使用して GCP ラベルを表示します。

VM を削除する

カタログから VM を削除することはできますが、GCP から VM を削除することはできません。この場合、Citrix ラベルは VM からのみ削除されます。追加された他のすべてのラベルは VM から削除されません。[完全な構成] インターフェイスまたは PowerShell コマンドを使用して、VM を削除できます。

完全な構成インターフェイスの使用

1. VM を選択して右クリックします。
2. [削除] をクリックします。
3. [カタログから仮想マシンを削除するが、仮想マシンは消去しない] を選択します。

PowerShell コマンドの使用　`Remove-ProvVM`を`ForgetVM`パラメーターで実行します。詳しくは、SDK ドキュメントRemove-ProvVMを参照してください。

Google Cloud Marketplace

Google Cloud Marketplace で Citrix 提供イメージを参照して選択することで、マシンカタログを作成できます。現在、MCS はこの機能でマシンプロファイルワークフローのみをサポートします。

Google Cloud Marketplace で Citrix VDA VM 製品を検索するには、https://console.cloud.google.com/marketplaceにアクセスしてください。

カスタムイメージ、または **Google Cloud Marketplace** の Citrix Ready イメージを使用して、マシンカタログのイメージを更新できます。

> 注:
>
> マシンプロファイルにストレージの種類の情報が含まれていない場合、値はカスタムプロパティから取得されます。

サポートされている Google Cloud Marketplace イメージは次のとおりです:

- Windows 2019 シングルセッション
- Windows 2019 マルチセッション
- Ubuntu

マシンカタログを作成するためのソースとして Citrix Ready イメージを使用する例:

```
New-ProvScheme -ProvisioningSchemeName GCPCatalog \
-HostingUnitName GcpHu -IdentityPoolName gcpPool -CleanOnBoot \
-MasterImageVM XDHyp:\HostingUnits\GcpHu\images.folder\citrix-daas-
   win2019-single-vda-v20220819.publicimage \
-MachineProfile XDHyp:\HostingUnits\GcpHu\Base.vm
```

次の手順

- 最初のカタログを作成すると、Web Studio ではデリバリーグループを作成する手順が表示されます。
- 構成プロセス全体を確認するには、「インストールと構成」を参照してください
- カタログを管理するには、「マシンカタログの管理」と「Google Cloud Platform カタログの管理」を参照してください。

追加情報

- 接続とリソースの作成と管理
- Google クラウド環境への接続
- マシンカタログの作成

HPE Moonshot マシンカタログの作成

August 17, 2024

「マシンカタログの作成」では、マシンカタログを作成するウィザードについて説明します。以下の情報は、HPE Moonshot 環境に固有の詳細について説明しています。

> 注:
>
> - HPE Moonshot への接続を作成する
> - 必ず 1 つ以上の HPE Moonshot ノードを利用可能にして、それらのノードに VDA をインストールしてください。
> - 初期の HPE Moonshot カートリッジイメージの作成については、Moonshot での OS 展開ユーザーガイドを参照してください。

以下を使用して、HPE Moonshot マシンカタログを作成できます:

- Web Studio
- PowerShell コマンド

Web Studio でのマシンカタログの作成

マシンカタログセットアップウィザードで、以下を実行します:

1. ［オペレーティングシステム］ページで、［マルチセッション **OS**］または ［シングルセッション **OS**］を選択します。
2. ［マシン管理］ページで、［電源管理されているマシン］と ［ほかのサービスまたはテクノロジ］を選択します。
3. ［仮想マシン］ページで、マシンとその Active Directory マシンアカウントを追加します。次のいずれかを実行できます:
    - ［マシンの追加］をクリックしてマシンを手動で追加します。［**VM** の選択］ウィンドウが表示されます。既に作成した HPE Moonshot シャーシ接続を展開し、追加するノード（VM）を選択します。次に、関連するマシンアカウント名を追加します。

- ［**CSV** ファイルの追加］をクリックしてマシンを一括追加します。CSV ファイルを使用してマシンを追加する方法については、「CSV ファイルを使用してマシンをカタログに一括追加する」を参照してください。

［スコープ］ページおよび ［概要］ページには、HPE Moonshot 固有の情報は表示されません。

PowerShell コマンドを使用してマシンカタログを作成する

New-BrokerCatalogおよびNew-BrokerMachine PowerShell コマンドを実行してブローカーカタログを作成し、マシンをブローカーカタログにインポートします。

例:

```
1 New-BrokerCatalog  -AdminAddress "MyDDC.MyDomain.local" -AdminClientIP
     "103.14.252.249" -AllocationType "Random" -IsRemotePC $False -
     MachinesArePhysical $False -MinimumFunctionalLevel "L7_20" -Name "
     BurMC" -PersistUserChanges "OnLocal" -ProvisioningType "Manual" -
     Scope @() -SessionSupport "MultiSession" -ZoneUid "e166e2cb-25dc
     -4578-bc07-bcf2a82d1463"
2 New-BrokerMachine  -AdminAddress "MyDDC.MyDomain.local" -AdminClientIP
     "103.14.252.249" -CatalogUid 3 -HostedMachineId "c10n1" -
     HypervisorConnectionUid 4 -IsReserved $False -MachineName "S
     -1-5-21-2589939477-3963209805-1860259709-1121"
```

次の手順

- 最初のカタログを作成すると、Web Studio ではデリバリーグループを作成する手順が表示されます。
- 構成プロセス全体を確認するには、「インストールと構成」を参照してください
- カタログを管理するには、「マシンカタログの管理」と「HPE Moonshot カタログの管理」を参照してください

追加情報

- 接続とリソースの作成と管理
- HPE Moonshot への接続
- マシンカタログの作成

Microsoft Azure カタログの作成

August 20, 2024

> 注:
>
> 2023 年 7 月より、Microsoft は Azure Active Directory（Azure AD）の名前を Microsoft Entra ID に変更しました。このドキュメントでは、Azure Active Directory、Azure AD、または AAD への言及はすべて、Microsoft Entra ID を意味することになります。

「マシンカタログの作成」では、マシンカタログを作成するウィザードについて説明します。以下の情報は、Microsoft Azure Resource Manager クラウド環境に固有の詳細について説明しています。

> 注:
>
> Microsoft Azure カタログを作成する前に、Microsoft Azure への接続の作成を完了する必要があります。「Microsoft Azure への接続」を参照してください。

マシンカタログの作成

マシンカタログは次の 2 つの方法で作成できます。

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

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

イメージは、マシンカタログ内に VM を作成するために使用される Azure Compute Gallery 内のイメージ定義のイメージバージョンの場合もあれば、ディスクまたはスナップショットの場合もあります。マシンカタログを作成する前に、Azure Resource Manager でイメージを作成します。イメージについて詳しくは、「マシンカタログの作成」を参照してください。

> 注:
>
> ホスト接続で構成されたリージョンとは異なるリージョンからマスターイメージを使用することに対するサポートは、廃止されました。Azure Compute Gallery を使用して、マスターイメージを目的のリージョンに複製します。

イメージの準備中に、元の VM に基づいて準備用の VM が作成されます。この準備 VM はネットワークから切断されています。ネットワークを準備 VM から切断するために、すべての受信および送信トラフィックを拒否するネットワークセキュリティグループが作成されます。ネットワークセキュリティグループは、自動的にカタログごとに 1 回作成されます。ネットワークセキュリティグループの名前は`Citrix-Deny-All-a3pgu-GUID`で、GUID がランダムに生成されます。例: `Citrix-Deny-All-a3pgu-3f161981-28e2-4223-b797-88b04d336dd1`。

マシンカタログ作成ウィザードで次の操作を行います:

- ［マシンの種類］ページと ［マシン管理］ページには、Azure 固有の情報は含まれていません。「マシンカタログの作成」のガイダンスに従ってください。
- ［イメージ］ページで、このカタログでマシンの作成に使用するテンプレートのイメージを選択します。

  使用するイメージの種類としてマスターイメージを選択した場合は、［イメージを選択］をクリックし、必要に応じて次の手順でマスターイメージを選択します：

  1. (テナント内またはテナント間で共有イメージを使用して構成された接続にのみ適用可能) イメージが存在するサブスクリプションを選択します。
  2. リソースグループの選択
  3. Azure VHD、Azure Compute Gallery、または Azure イメージバージョンに移動します。必要に応じて、選択したイメージにメモを追加します。

  イメージを選択するときは、次の点を考慮してください：

  - Citrix VDA がイメージにインストールされていることを確認します。
  - VM に接続されている VHD を選択した場合は、次の手順に進む前に VM をシャットダウンする必要があります。

  > 注：
  >
  > - カタログにマシンを作成した接続（ホスト）のサブスクリプションは、緑色の点で示されます。他のサブスクリプションは、Azure Compute Gallery をそのサブスクリプションと共有します。これらのサブスクリプションでは、共有ギャラリーのみが表示されます。共有サブスクリプションの構成方法については、「単一のテナント内（サブスクリプション間）での画像の共有」および「テナント間での画像の共有」を参照してください。
> - トラステッド起動が有効になっているイメージまたはスナップショットを選択する場合は、［セキュリティの種類］としてトラステッド起動が選択されているマシンプロファイルを使用する必要があります。次に、マシンプロファイルの値を指定することにより、SecureBoot と vTPM を有効または無効にできます。トラステッド起動は、Shared Image Gallery ではサポートされていません。Azure のトラステッド起動については、「https://docs.microsoft.com/en-us/azure/virtual-machines/trusted-launch」を参照してください。
> - トラステッド起動で、Windows でエフェメラル OS ディスクを使用して、プロビジョニングスキームを作成できます。トラステッド起動でイメージを選択する場合は、vTPM が有効になっているトラステッド起動でマシンプロファイルを選択する必要があります。エフェメラル OS ディスクを使用してマシンカタログを作成する方法については、「エフェメラル OS ディスクを使用してマシンを作成する方法」を参照してください。
> - イメージのレプリケーション中に、先に進んでそのイメージをマスターイメージとして選択し、セットアップを完了することができます。ただし、イメージのレプリケーション中は、カタログ作成完了までの時間が長くなることがあります。MCS では、カタログの作成開始から 1 時間以内にレプリケーションを完了する必要があります。レプリケーションがタイムアウトすると、カタログの作成は失敗します。レプリケーションステータスは Azure で確認できます。レプリケーションがま

> だ保留中の場合、またはレプリケーションが完了した後で再試行してください。
> - Azure でマシンカタログのマスターイメージを選択すると、MCS は、選択されたマスターイメージとマシンプロファイルに基づいて OS の種類を識別します。MCS で識別できない場合は、マスターイメージに一致する OS の種類を選択してください。
> - Gen2 イメージを使用して Gen 2 VM カタログをプロビジョニングし、起動時のパフォーマンスを向上させることができます。ただし、Gen1 イメージを使用した Gen2 マシンカタログの作成はサポートされていません。同様に、Gen2 イメージを使用した Gen1 マシンカタログの作成もサポートされていません。また、世代情報を持たない古いイメージはすべて Gen1 イメージです。

使用するイメージの種類として準備済みイメージを選択した場合は、[イメージを選択] をクリックし、必要に応じて準備済みイメージを選択します。

VM の作成を成功させるには、イメージに Citrix VDA 2311 以降がインストールされており、VDA に MCSIO が存在することを確認します。

イメージを選択すると、[マシンプロファイルを使用する（**Azure Active Directory** では必須）] チェックボックスが自動的に選択されます。[マシンプロファイルを選択] を クリックして、リソースグループの一覧から VM または ARM テンプレートスペックを参照します。カタログ内の VM は、指定したマシンプロファイルから構成を継承できます。

ARM テンプレートスペックを検証して、マシンカタログを作成するためにマシンプロファイルとして使用できるかどうかを確認します。ARM テンプレートスペックを検証する方法は 2 つあります:

- リソースグループの一覧から ARM テンプレートスペックを選択したら、[次へ] をクリックします。ARM テンプレートスペックにエラーがある場合、エラーメッセージが表示されます。
- 次の PowerShell コマンドのいずれかを実行します:
  * `Test-ProvInventoryItem -HostingUnitName <string> -InventoryPath <string>`
  * `Test-ProvInventoryItem -HostingUnitUid <Guid> -InventoryPath <string>`

VM がマシンプロファイルから継承できる構成の例として、次のようなものがあります:

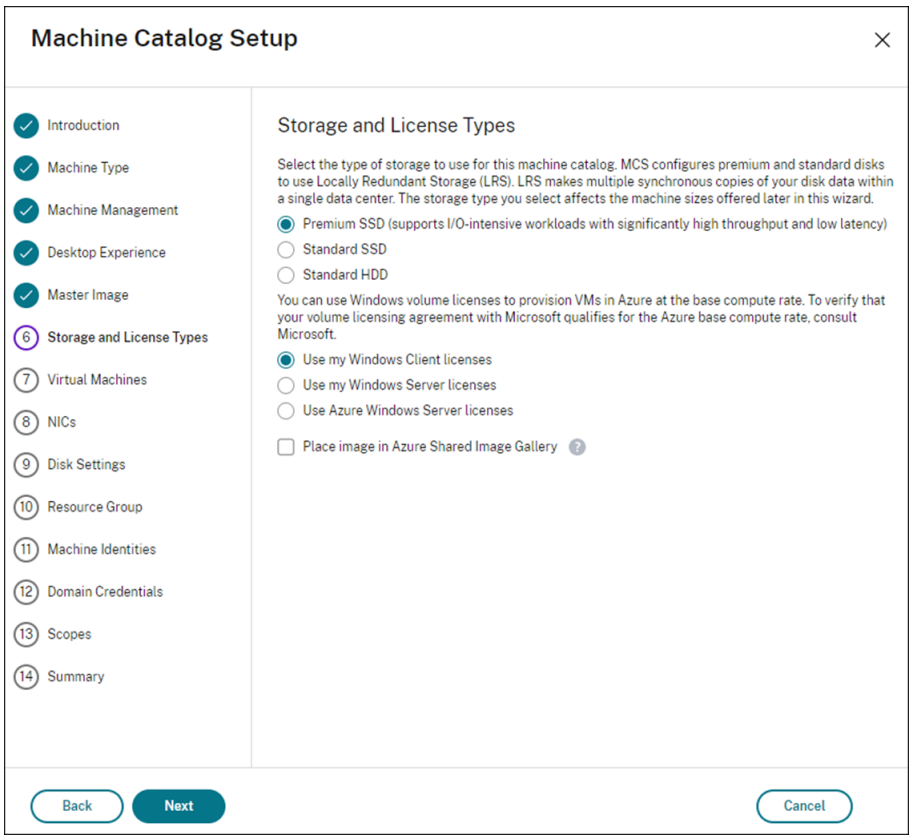
- 高速ネットワーク
- ブート診断
- ホストのディスクキャッシュ（OS および MCSIO ディスク関連）
- マシンサイズ（別途指定されていない場合）
- VM に適用されたタグ

カタログを作成した後、イメージがマシンプロファイルから継承している構成を表示できます。[マシンカタログ] ノードで、カタログを選択して下部ペインに詳細を表示します。次に、[テンプレートのプロパティ] タブをクリックしてマシンプロファイルのプロパティを表示します。[タグ] セクションには、最大 3 つのタグが表示されます。その VM に配置されているすべてのタグを表示するには、[すべて表示] をクリックします。

MCS で Azure 専用ホストに VM をプロビジョニングする場合は、［専用のホストグループを使用する］チェックボックスをオンにし、一覧からホストグループを選択します。ホストグループは、専用ホストのコレクションを表すリソースです。専用ホストは、1 つまたは複数の VM をホストする物理サーバーを提供するサービスです。サーバーは Azure サブスクリプション専用であり、他のサブスクライバーとは共有されません。専用ホストを使用する場合、Azure は、VM がそのホストで実行されている唯一のマシンであることを保証します。この機能は、規制または内部のセキュリティ要件を満たす必要があるシナリオに適しています。ホストグループとそれらを使用する際の考慮事項について詳しくは、「Azure 専用ホスト」を参照してください。

> 重要：
>
> - Azure の自動配置が有効になっているホストグループのみが表示されます。
> - ホストグループを使用すると、ウィザードの後半で表示される［**Virtual Machines**］ページが変更されます。選択したホストグループに含まれるマシンサイズのみが、このページに表示されます。また、アベイラビリティゾーンは自動的に選択され、選択できません。

- ［ストレージとライセンスの種類］ページは、Azure Resource Manager イメージを使用するときのみ表示されます。



マシンカタログに使用するストレージの種類は次のとおりです：

- プレミアム **SSD**：I/O を多用するワークロードを持つ VM に適した、高性能かつ低遅延のディスクストレージオプションを提供します。

- 標準 **SSD**：低 IOPS レベルで安定したパフォーマンスを必要とするワークロードに適した、コスト効率の高いストレージオプションを提供します。
- 標準 **HDD**：遅延の影響を受けないワークロードを実行している VM に対して、信頼性の高い低コストのディスクストレージオプションを提供します。
- **Azure** エフェメラル **OS** ディスク VM のローカルディスクを再利用してオペレーティングシステムディスクをホストする、コスト効率の高いストレージオプションを提供します。または、PowerShell を使用して、エフェメラル OS ディスクを使用するマシンを作成することもできます。詳しくは、「Azure エフェメラルディスク」を参照してください。エフェメラル OS ディスクを使用する場合は、次の考慮事項に注意してください：
  * Azure エフェメラル OS ディスクと MCS I/O を同時に有効にすることはできません。
  * エフェメラル OS ディスクを使用するマシンを更新するには、サイズが仮想マシンのキャッシュディスクまたは一時的ディスクのサイズを超えないイメージを選択する必要があります。
  * ウィザードの後半で表示される ［電源サイクル中に仮想マシンとシステムディスクを保持する］オプションを使用することはできません。

> 注：
>
> ID ディスクは、選択したストレージの種類に関係なく、常に標準 SSD を使用して作成されます。

ストレージの種類によって、ウィザードの ［仮想マシン］ページに表示されるマシンのサイズが変わります。MCS は、ローカル冗長ストレージ（LRS）を使用するようにプレミアムディスクと標準ディスクを構成します。LRS は、単一のデータ センター内でデータの複数の同期コピーを作成します。Azure エフェメラル OS ディスクは、VM のローカルディスクを使用してオペレーティングシステムを格納します。Azure のストレージの種類およびストレージの複製について詳しくは、以下のドキュメントを参照してください：

- https://docs.microsoft.com/en-us/azure/storage/common/storage-introduction/
- https://docs.microsoft.com/en-us/azure/virtual-machines/premium-storage-performance/
- https://docs.microsoft.com/en-us/azure/storage/common/storage-redundancy/

既存の Windows ライセンスを使用するか Linux ライセンスを使用するかを選択します。

- Windows ライセンス：Windows ライセンスと Windows イメージ（Azure プラットフォームのサポートイメージまたはカスタムイメージ）を使用すると、Azure で Windows VM を低コストで実行できます。ライセンスには次の 2 種類があります：
  * **Windows Server** ライセンス。Windows Server ライセンスまたは Azure Windows Server ライセンスを使用できます。これにより、Azure Hybrid 特典を使用できます。詳しくは、https://azure.microsoft.com/en-us/pricing/hybrid-benefit/を参照してください。Azure Hybrid 特典を使用すると、Azure ギャラリーからの Windows Server 追加ライセンス料金が不要になるため、Azure での仮想マシン実行コストを基本計算料金のみに抑えられます。
  * **Windows** クライアントライセンス。Windows 10 ライセンスおよび Windows 11 ライセンスを Azure に移行できるため、追加のライセンスなしで Windows 10 VM および Windows 11 VM

を Azure で実行できます。詳しくは、「クライアントアクセスライセンスと管理ライセンス」を参照してください。

プロビジョニングされた仮想マシンがライセンス特典を使用していることを確認するには、次の PowerShell コマンドを実行します：`Get-AzVM -ResourceGroup MyResourceGroup -Name MyVM`。

- [Windows Server のライセンスの種類] で、ライセンスの種類が [**Windows_Server**] であることを確認します。詳しくは、https://docs.microsoft.com/en-us/azure/virtual-machines/windows/hybrid-use-benefit-licensing/を参照してください。
- [Windows クライアントのライセンスの種類] で、ライセンスの種類が [**Windows_Client**] であることを確認します。詳しくは、https://docs.microsoft.com/en-us/azure/virtual-machines/windows/windows-desktop-multitenant-hosting-deployment/を参照してください。

または、`Get-Provscheme` PowerShell SDK を使用して確認することもできます。例：`Get-Provscheme -ProvisioningSchemeName "My Azure Catalog"`。このコマンドレットについて詳しくは、https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/MachineCreation/Get-ProvScheme/を参照してください。

- Linux ライセンス：bring-your-own-subscription（BYOS）Linux ライセンスを使用すると、ソフトウェアの料金を支払う必要がありません。BYOS の料金には、コンピューティングハードウェアの料金のみが含まれます。ライセンスには次の 2 種類があります：
  - **RHEL_BYOS**：RHEL_BYOS の種類を正しく使用するには、Azure サブスクリプションで Red Hat Cloud Access を有効にします。
  - **SLES_BYOS**：SLES の BYOS バージョンには、SUSE からのサポートが含まれています。

  LicenseType 値を`New-ProvScheme`および`Set-ProvScheme`で Linux オプションに設定できます。

  LicenseType を`New-ProvScheme`で RHEL_BYOS に設定した例：

```
New-ProvScheme -CleanOnBoot -ProvisioningSchemeName "
    azureCatalog" -RunAsynchronously -Scope @() -SecurityGroup
    @() -CustomProperties '<CustomProperties xmlns="http://
    schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http
    ://www.w3.org/2001/XMLSchema-instance"><Property xsi:type="
    StringProperty" Name="UseManagedDisks" Value="true" /><
    Property xsi:type="StringProperty" Name="StorageAccountType
    " Value="StandardSSD_LRS" /><Property xsi:type="
    StringProperty" Name="ResourceGroups" Value="hu-dev-mcs"
    /><Property xsi:type="StringProperty" Name="OsType" Value="
    Linux" /><Property xsi:type="StringProperty" Name="
    LicenseType" Value="RHEL_BYOS" /></CustomProperties>'
```

  LicenseType を`Set-ProvScheme`で SLES_BYOS に設定した例：


```
Set-ProvScheme -ProvisioningSchemeName "azureCatalog" -
    CustomProperties '<CustomProperties xmlns="http://schemas.
    citrix.com/2014/xd/machinecreation" xmlns:xsi="http://www.
    w3.org/2001/XMLSchema-instance"><Property xsi:type="
    StringProperty" Name="UseManagedDisks" Value="true" /><
    Property xsi:type="StringProperty" Name="StorageAccountType
    " Value="StandardSSD_LRS" /><Property xsi:type="
    StringProperty" Name="ResourceGroups" Value="hu-dev-mcs"
    /><Property xsi:type="StringProperty" Name="OsType" Value="
    Linux" /><Property xsi:type="StringProperty" Name="
    LicenseType" Value="SLES_BYOS" /></CustomProperties>'
```

> 注:
>
> `LicenseType`値が空の場合、デフォルト値は、OsType 値に応じて、Azure Windows Server ライセンスまたは Azure Linux ライセンスになります。

LicenseType を空にした例:

```
Set-ProvScheme -ProvisioningSchemeName "azureCatalog" -
    CustomProperties '<CustomProperties xmlns="http://schemas.
    citrix.com/2014/xd/machinecreation" xmlns:xsi="http://www.
    w3.org/2001/XMLSchema-instance"><Property xsi:type="
    StringProperty" Name="UseManagedDisks" Value="true" /><
    Property xsi:type="StringProperty" Name="StorageAccountType
    " Value="StandardSSD_LRS" /><Property xsi:type="
    StringProperty" Name="ResourceGroups" Value="hu-dev-mcs"
    /><Property xsi:type="StringProperty" Name="OsType" Value="
    Linux" /></CustomProperties>'
```

ライセンスの種類と利点を理解するには、次のドキュメントを参照してください:

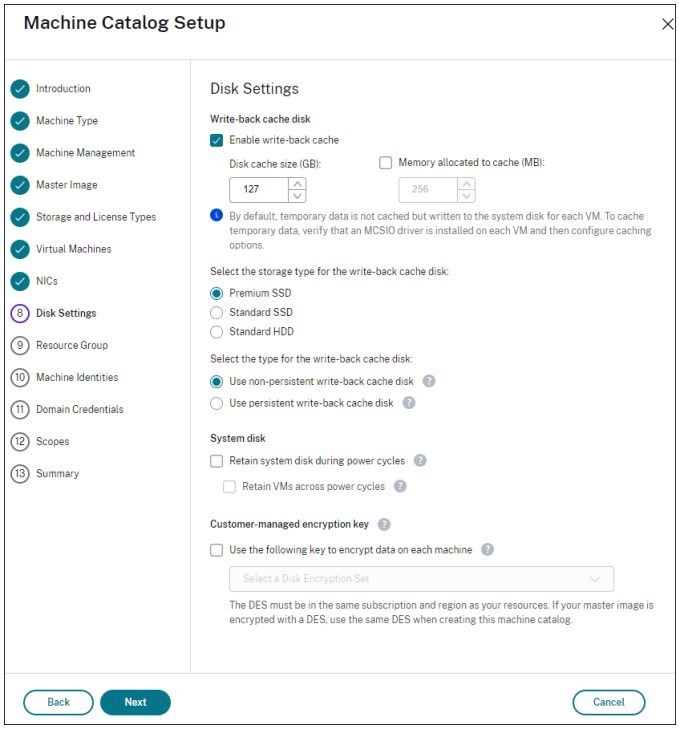
- https://docs.microsoft.com/en-us/dotnet/api/microsoft.azure.management.compute.models.virtualmachine.licensetype?view=azure-dotnet
- https://docs.microsoft.com/en-us/azure/virtual-machines/linux/azure-hybrid-benefit-linux

Azure Compute Gallery（旧称 Azure Shared Image Gallery）は、イメージを管理および共有するためのリポジトリです。これにより、組織全体でイメージを利用できるようになります。大規模な永続的でないマシンカタログを作成する場合は、よりすばやく VDA OS ディスクをリセットできるため、イメージを SIG に保存することをお勧めします。［準備されたイメージを **Azure Compute Gallery** に配置します］を選択すると、［**Azure Computer Gallary** の設定］セクションが表示され、追加の Azure Compute Gallery 設定を指定できます:

- イメージレプリカに対する仮想マシンの比率。Azure で保持するイメージレプリカに対する仮想マシンの比率を指定できます。デフォルトでは、Azure は 40 台の非永続的なマシンごとに 1 つのイメージレプリカを保持します。永続マシンの場合、その数はデフォルトで 1,000 になります。

  - 最大レプリカ数。Azure で保持するイメージレプリカの最大数を指定できます。デフォルトは 100 です。

- ［仮想マシン］ページで、作成する仮想マシンの数を指定します。少なくとも 1 つを指定し、マシンサイズを選択する必要があります。カタログ作成後、カタログを編集してマシンサイズを変更できます。
- ［**NIC**］ページには、Azure 固有の情報は表示されません。「マシンカタログの作成」のガイダンスに従ってください。
- ［ディスク設定］ページで、ライトバックキャッシュを有効にするかどうかを選択します。MCS ストレージ最適化機能を有効にすると、カタログを作成するときに以下の設定を構成できます。これらの設定は、Azure 環境と GCP 環境の両方に適用されます。



ライトバックキャッシュを有効にした後、次の操作を実行できます：

  - 一時データのキャッシュに使用するディスクと RAM のサイズを構成する。詳しくは、「一時データ用キャッシュの構成」を参照してください。
  - ライトバックキャッシュディスク用のストレージの種類を選択します。ライトバックキャッシュディスクには、次のストレージのオプションを使用できます：
    * プレミアム SSD
    * 標準 SSD
    * 標準 HDD
  - プロビジョニングされた VM に対してライトバックキャッシュディスクを保持するかどうかを選択します。このオプションを使用可能にするには、［ライトバックキャッシュを有効にする］を選択します。デフォルトでは、［非永続的なライトバックキャッシュディスクを使用する］が選択されています。

- ライトバックキャッシュディスクの種類を選択します。
  - 非永続的なライトバックキャッシュディスクを使用する。選択した場合、ライトバックキャッシュディスクは電源サイクル中に削除されます。リダイレクトされたデータはすべて失われます。VM の一時ディスクに十分なスペースがある場合、それはライトバックキャッシュディスクのホストに使用され、コストを削減します。カタログの作成後、プロビジョニングされたマシンが一時ディスクを使用しているかどうかを確認できます。これを行うには、カタログをクリックして、［テンプレートのプロパティ］タブの情報を確認します。一時ディスクが使用されている場合は、［非永続的なライトバックキャッシュディスク］が表示され、その値は ［はい（**VM** の一時ディスクを使用)］になっていますそうでない場合は、［非永続的なライトバックキャッシュディスク］が表示され、その値は ［いいえ］（**VM** の一時ディスクを使用しない）になっています。
  - 永続的なライトバックキャッシュディスクを使用する。選択した場合、ライトバックキャッシュディスクは、プロビジョニングされた VM で保持されます。このオプションを有効にすると、ストレージコストが増加します。
- 電源サイクル中に VDA 用の仮想マシンとシステムディスクを保持するかどうかを選択します。

  電源サイクル中に仮想マシンおよびシステムディスクを保持します。［ライトバックキャッシュを有効にする］を選択した場合に使用できます。デフォルトでは、仮想マシンとシステムディスクはシャットダウン時に削除され、スタートアップ時に再作成されます。仮想マシンの再起動時間を短縮したい場合は、このオプションを選択します。このオプションを有効にすると、ストレージコストも増加することに注意してください。
- ストレージコストの削減を有効にするかどうかを選択します。有効にすると、VM のシャットダウン時にストレージディスクを標準 HDD にダウングレードすることで、ストレージコストを削減できます。VM は、再起動時に元の設定に切り替わります。このオプションは、ストレージディスクとライトバックキャッシュディスクの両方に適用されます。または、PowerShell を使用することもできます。「仮想マシンのシャットダウン時にストレージの種類をダウングレードする」を参照してください。

  > 注:
  >
  > Microsoft は、VM のシャットダウン中のストレージの種類の変更に制限を課しています。Microsoft が将来的にストレージの種類の変更を禁止する可能性もあります。詳しくは、Microsoft 社の記事を参照してください。
- カタログでプロビジョニングされるマシンのデータを暗号化するかどうかを選択します。顧客が管理する暗号化キーを使用したサーバー側暗号化により、管理対象ディスクレベルで暗号化を管理し、カタログ内のマシン上のデータを保護できます。詳しくは、「Azure サーバー側暗号化」を参照してください。

- ［リソースグループ］ページで、リソースグループを作成するか、既存のグループを使用するかを選択します。
  - リソースグループを作成する場合は、［次へ］を選択します。
  - 既存のリソースグループを使用する場合は、［使用可能なプロビジョニングリソースグループ］ボックスの一覧からグループを選択します。注意事項：カタログで作成しているマシンを収容するのに十分なグループを選択してください。選択が少なすぎると、メッセージが表示されます。後でカタログにさらに

VM を追加する予定がある場合は、必要最小限よりも多く選択しておくことをお勧めします。カタログが作成された後、カタログにリソースグループをさらに追加することはできません。

詳しくは、「Azure リソースグループ」を参照してください。

- ［マシン **ID**］ページで ID の種類を選択し、このカタログ内のマシンの ID を設定します。［**Azure Active Directory** 参加］として仮想マシンを選択すると、それらを Azure AD セキュリティグループに追加できます。詳細な手順は次のとおりです：

  1. ［**ID** の種類］フィールドから、［**Azure Active Directory** 参加］を選択します。［**Azure AD** セキュリティグループ（オプション）］オプションが表示されます。
  2. ［**Azure AD** セキュリティグループ：新規作成］をクリックします。
  3. グループ名を入力して、［作成］をクリックします。
  4. 画面の指示に従って、Azure にサインインします。
     グループ名が Azure に存在しない場合は、緑色のアイコンが表示されます。それ以外の場合は、新しい名前の入力を求めるエラーメッセージが表示されます。
  5. 仮想マシンのマシンアカウント名前付けスキームを入力します。

  カタログの作成後、Citrix Virtual Apps and Desktops はユーザーに代わって Azure にアクセスし、セキュリティグループとグループの動的メンバーシップ規則を作成します。この規則に基づいて、このカタログで指定された名前付けスキームの仮想マシンがセキュリティグループに自動的に追加されます。

  このカタログに別の名前付けスキームの仮想マシンを追加するには、Azure にサインインする必要があります。これにより、Citrix Virtual Apps and Desktops は Azure にアクセスし、新しい名前付けスキームに基づいて動的メンバーシップ規則を作成できます。

  このカタログを削除する場合、Azure からセキュリティグループを削除するには、Azure へのサインインも必要です。

- ［ドメイン資格情報］ページおよび ［概要］ページには、Azure 固有の情報は表示されません。「マシンカタログの作成」のガイダンスに従ってください。

ウィザードを完了します。

Azure 一時ディスクをライトバックキャッシュディスクとして使用するための条件

次のすべての条件が満たされている場合にのみ、Azure 一時ディスクをライトバックキャッシュディスクとして使用できます：

- Azure 一時ディスクは永続データには適していないため、ライトバックキャッシュディスクは非永続である必要があります。
- 選択した Azure VM のサイズには、一時ディスクが含まれている必要があります。
- エフェメラル OS ディスクを有効にする必要はありません。

- ライトバックキャッシュファイルを Azure 一時ディスクに保存することを受け入れます。
- Azure 一時ディスクのサイズは、「ライトバックキャッシュディスクサイズ + ページングファイル用に予約されたスペース + 1GB のバッファスペース」の合計サイズよりも大きい必要があります。

非永続的なライトバックキャッシュディスクのシナリオ

次の表は、マシンカタログの作成中に一時ディスクがライトバックキャッシュに使用される場合の 3 つの異なるシナリオを示しています。

シナリオ	結果
ライトバックキャッシュに一時ディスクを使用するためのすべての条件が満たされている。	WBC ファイル`mcsdif.vhdx`は一時ディスクに保存されます。
一時ディスクに、ライトバックキャッシュを使用するための十分なスペースがない。	VHD ディスク`MCSWCDisk`が作成され、このディスクに WBC ファイル`mcsdif.vhdx`が保存されます。
一時ディスクに、ライトバックキャッシュを使用するための十分なスペースがあるが、`UseTempDiskForWBC`は **false** に設定されている。	VHD ディスク`MCSWCDisk`が作成され、このディスクに WBC ファイル`mcsdif.vhdx`が保存されます。

Azure テンプレートスペックを作成する

Azure Portal で Azure テンプレートスペックを作成し、それを Web Studio と PowerShell コマンドで使用して、MCS マシンカタログを作成または更新できます。

既存の仮想マシンの Azure テンプレートスペックを作成するには、以下の手順に従います:

1. Azure Portal に移動します。リソースグループを選択してから、仮想マシンとネットワークインターフェイスを選択します。上の［…］メニューで、［**Export template**］をクリックします。
2. カタログプロビジョニング用のテンプレートスペックを作成する場合は、［**Include parameters**］チェックボックスをオフにします。
3. テンプレートスペックを後で変更するには、［**Add to library**］をクリックします。
4. ［**Importing template**］ページで、**Name**、**Subscription**、**Resource Group**、**Location**、**Version** などの必要な情報を入力します。［**Next: Edit Template**］をクリックします。
5. カタログをプロビジョニングする場合は、独立したリソースとしてネットワークインターフェイスも必要です。したがって、テンプレートスペックで指定されている`dependsOn`を削除する必要があります。例:

```
"dependsOn": [
"[resourceId('Microsoft.Network/networkInterfaces', 'tnic937')]"
],
```


6. [**Review+Create**] を作成してテンプレートスペックを作成します。
7. [**Template Specs**] ページで、作成したテンプレートスペックを確認します。テンプレートスペックをクリックします。左側のパネルで、[**Versions**] をクリックします。
8. [**Create new version**] をクリックして、新しいバージョンを作成できます。新しいバージョン番号を指定し、現在のテンプレートスペックを変更して、[**Review + Create**] をクリックし、新しいバージョンのテンプレートスペックを作成します。

次の PowerShell コマンドを使用して、テンプレートスペックとテンプレートのバージョンに関する情報を取得できます:

- テンプレートスペックに関する情報を取得するには、次を実行します:

```
get-item XDHyp:\HostingUnits\East\machineprofile.folder\abc.
    resourcegroup\bggTemplateSpec.templatespec
```

- テンプレートスペックのバージョンに関する情報を取得するには、次を実行します:

```
get-item XDHyp:\HostingUnits\East\machineprofile.folder\abc.
    resourcegroup\bggTemplateSpec.templatespec\bgg1.0.
    templatespecversion
```

カタログの作成または更新でテンプレートスペックを使用する

テンプレートスペックをマシンプロファイルの入力に使用して、MCS マシンカタログを作成または更新できます。これを行うには、Web Studio または PowerShell コマンドを使用できます。

- Web Studio については、「Web Studio で Azure Resource Manager イメージを使用してマシンカタログを作成する」を参照してください。
- PowerShell については、「PowerShell を使用したカタログの作成または更新でテンプレートスペックを使用する」を参照してください。

Azure サーバー側暗号化

Citrix Virtual Apps and Desktops は、Azure Key Vault を使用して Azure Managed Disks の顧客が管理する暗号化キーをサポートします。このサポートにより、独自の暗号キーを使用してマシンカタログの管理対象ディスクを暗号化して、組織およびコンプライアンスの要件を管理できます。詳しくは、「Azure Disk Storage のサーバー側暗号化」を参照してください。

管理対象ディスクにこの機能を使用する場合:

- ディスクが暗号化されているキーを変更するには、`DiskEncryptionSet`の現在のキーを変更します。`DiskEncryptionSet`に関連付けられているすべてのリソースは、新しいキーで暗号化されるように変更されます。

- キーを無効にするか削除すると、そのキーを使用するディスクのある VM はすべて自動的にシャットダウンします。シャットダウン後、キーを再度有効にするか、新しいキーを割り当てない限り、VM は使用できません。このキーを使用するカタログの電源をオンにすることはできません。また、VM をカタログに追加することもできません。

顧客が管理する暗号化キーを使用する場合の重要な考慮事項

この機能を使用するときは、次のことに注意してください:

- 顧客が管理するキーに関連するすべてのリソース（Azure Key Vault、ディスク暗号化セット、VM、ディスク、スナップショット）は、同じサブスクリプションとリージョンに配置される必要があります。
- 顧客が管理するキーで暗号化されたディスク、スナップショット、イメージは、別のリソースグループおよびサブスクリプションに移動できません。
- リージョンごとのディスク暗号化セットの制限については、Microsoft 社のサイトを参照してください。

> 注:
>
> Azure サーバー側暗号化の構成については、「クイックスタート: Azure Portal を使用してキーコンテナを作成する」を参照してください。

Azure の顧客が管理する暗号キー

マシンカタログを作成するときに、カタログでプロビジョニングされるマシンのデータを暗号化するかどうかを選択できます。顧客が管理する暗号化キーを使用したサーバー側暗号化により、管理対象ディスクレベルで暗号化を管理し、カタログ内のマシン上のデータを保護できます。ディスク暗号化セット（DES）は、顧客が管理するキーを表します。この機能を使用するには、最初に Azure で DES を作成する必要があります。DES の形式は次のとおりです:

- `/subscriptions/12345678-1234-1234-1234-123456789012/resourceGroups/Sample-RG/providers/Microsoft.Compute/diskEncryptionSets/SampleEncryption`

一覧から DES を選択します。選択した DES は、リソースと同じサブスクリプションおよびリージョンに存在する必要があります。

「顧客管理暗号キーを使用したマシンカタログの作成」を参照してください。

ホストでの Azure ディスク暗号化

ホスト機能での暗号化を使用して、MCS マシンカタログを作成できます。現在、MCS はこの機能でマシンプロファイルワークフローのみをサポートします。VM またはテンプレートスペックをマシンプロファイルの入力として使用できます。

この暗号化方法は、Azure Storage でデータを暗号化しません。VM をホストするサーバーがデータを暗号化し、暗号化されたデータが Azure Storage サーバーを通過します。つまり、この暗号化方法はデータをエンドツーエンドで暗号化します。

制限:

ホストでの Azure ディスク暗号化は:

- すべての Azure マシンサイズでサポートされているわけではありません
- Azure Disk Encryption と互換性がありません

ホスト機能での暗号化を使用してマシンカタログを作成するには、次の手順を実行します:

1. ホスト機能での暗号化がサブスクリプションで有効になっているかどうかを確認します。確認する方法については、「https://learn.microsoft.com/en-us/rest/api/resources/features/get?tabs=HTTP/」を参照してください。有効になっていない場合は、サブスクリプションの機能を有効にする必要があります。サブスクリプションでこの機能を有効にする方法については、「https://learn.microsoft.com/en-us/azure/virtual-machines/disks-enable-host-based-encryption-portal?tabs=azure-powershell#prerequisites/」を参照してください。
2. 使用する Azure VM のサイズがホストでの暗号化をサポートしているかどうかを確認します。確認するには、PowerShell ウィンドウで次のいずれかを実行します:

   ```
   PS XDHyp:\Connections<your connection>\east us.region\
      serviceoffering.folder>
   ```

   ```
   PS XDHyp:\HostingUnits<your hosting unit>\serviceoffering.folder>
   ```

3. Azure Portal でホストでの暗号化を有効にして、マシンプロファイルの入力として、VM またはテンプレートスペックを作成します。

   - VM を作成する場合は、ホストでの暗号化をサポートしている VM サイズを選択します。VM を作成すると、VM プロパティの ［**Encryption at host**］が有効になります。
   - テンプレートスペックを使用する場合は、`Encryption at Host`パラメーターを`securityProfile`内で **true** にします。

4. VM またはテンプレートスペックを選択して、マシンプロファイルワークフローで MCS マシンカタログを作成します。

   - OS ディスクまたはデータディスク: 顧客管理キーとプラットフォーム管理キーによって暗号化されます
   - エフェメラル OS ディスク: プラットフォーム管理キーだけで暗号化されます
   - キャッシュディスク: 顧客管理キーとプラットフォーム管理キーによって暗号化されます

   Web Studio を使用するか、PowerShell コマンドを実行して、マシンカタログを作成できます。

マシンプロファイルからホストでの暗号化情報を取得する

`AdditionalData`パラメーターを指定して PowerShell コマンドを実行すると、マシンプロファイルからホストでの暗号化情報を取得できます。`EncryptionAtHost`パラメーターが **True** の場合、ホストでの暗号化がマシンプロファイルに対して有効であることを示します。

例：マシンプロファイル入力が VM の場合、次のコマンドを実行します：

```
(get-item XDHyp:\HostingUnits\myAzureNetwork\machineprofile.folder\abc.
    resourcegroup\def.vm).AdditionalData
```

例：マシンプロファイル入力がテンプレートスペックの場合、次のコマンドを実行します：

```
(get-item XDHyp:\HostingUnits\myAzureNetwork\machineprofile.folder\abc.
    resourcegroup\def_templatespec.templatespec\EncryptionAtHost.
    templatespecversion).AdditionalData
```

管理対象ディスクの二重暗号化

二重暗号化を使用してマシンカタログを作成できます。この機能を使用して作成されたカタログでは、すべてのディスクがプラットフォームキーと顧客管理キーの両方によってサーバー側で暗号化されています。Azure Key Vault、暗号キー、およびディスク暗号化セット（DES）は、顧客が所有し、維持します。

二重暗号化とは、プラットフォーム側の暗号化（デフォルト）と顧客管理の暗号化（CMEK）です。したがって、暗号化アルゴリズム、実装、またはキーの侵害に関するリスクを懸念している、セキュリティに非常に敏感なお客様は、この二重暗号化を選択できます。永続的 OS ディスクとデータディスク、スナップショット、イメージはすべて二重暗号化により保存時に暗号化されます。

> 注：
>
> - Web Studio を使用するか、PowerShell コマンドを実行することで、二重暗号化を使用してマシンカタログを作成し、更新できます。PowerShell コマンドについては、「二重暗号化を使用したマシンカタログの作成」を参照してください。
> - 二重暗号化を使用してマシンカタログを作成または更新するには、非マシンプロファイルベースのワークフローまたはマシンプロファイルベースのワークフローを使用できます。
> - 非マシンプロファイルベースのワークフローを使用してマシンカタログを作成する場合は、保存されている`DiskEncryptionSetId`を再利用できます。
> - マシンプロファイルを使用する場合は、VM またはテンプレートスペックをマシンプロファイルの入力に使用できます。

制限事項：

- 二重暗号化は、Ultra Disk または Premium SSD v2 ディスクではサポートされていません。
- 二重暗号化は、非管理ディスクではサポートされません。

- カタログに関連付けられている DiskEncryptionSet キーを無効にすると、カタログの VM が無効になります。
- 顧客が管理するキーに関連するすべてのリソース（Azure Key Vault、ディスク暗号化セット、VM、ディスク、スナップショット）は、同じサブスクリプションとリージョンに存在する必要があります。
- サブスクリプションごとに、リージョンあたり最大 50 のディスク暗号化セットのみを作成できます。

Azure リソースグループ

Azure プロビジョニングのリソースグループは、アプリケーションとデスクトップをユーザーに提供する VM をプロビジョニングする方法を提供します。MCS マシンカタログを作成するときに既存の空の Azure リソースグループを追加するか、新しいリソースグループを作成することができます。Azure リソースグループについて詳しくは、Microsoft 社のドキュメントを参照してください。

Azure リソースグループの使用

Azure リソースグループごとの仮想マシン、管理対象ディスク、スナップショット、およびイメージの数に制限はありません（Azure リソースグループごとに仮想マシンは 240、管理対象ディスクは 800 という数の制限はなくなりました）。

- フルスコープのサービスプリンシパルを使用してマシンカタログを作成する場合、MCS は 1 つの Azure リソースグループのみを作成し、カタログのこのグループを使用します。
- スコープの狭いサービスプリンシパルを使用してマシンカタログを作成する場合、事前に作成された空の Azure リソースグループを指定する必要があります。

Azure エフェメラルディスク

Azure エフェメラルディスクを使用すると、キャッシュディスクまたは一時ディスクを再利用して、Azure 対応の仮想マシンの OS ディスクを保存できます。この機能は、標準の HDD ディスクよりも高性能の SSD ディスクを必要とする Azure 環境で役立ちます。Azure エフェメラルディスクを使用したカタログの作成については、「Azure エフェメラルディスクを使用したカタログの作成」を参照してください。

> 注:
>
> 永続カタログでは、エフェメラル OS ディスクはサポートされていません。

エフェメラル OS ディスクでは、プロビジョニングスキームで管理対象ディスクと Shared Image Gallery を使用する必要があります。

エフェメラル **OS** 一時ディスクの保存

エフェメラル OS ディスクを VM 一時ディスクまたはリソースディスクに保存するオプションがあります。この機能により、キャッシュがないか、キャッシュが不十分な VM で、エフェメラル OS ディスクを使用できます。このような VM には、Ddv4などのエフェメラル OS ディスクを保存するための一時ディスクまたはリソースディスクがあります。

以下に注意してください:

- エフェメラルディスクは、VM キャッシュディスクまたは VM の一時（リソース）ディスクのいずれかに保存されます。キャッシュディスクが OS ディスクの内容を保持するのに十分な大きさでない場合を除き、キャッシュディスクは一時ディスクよりも優先されます。
- 更新の際は、キャッシュディスクよりも大きいが一時ディスクよりも小さい新しいイメージにより、エフェメラル OS ディスクが VM の一時ディスクに置き換えられます。

Azure エフェメラルディスクと **Machine Creation Services**（**MCS**）ストレージ最適化（**MCS I/O**）

Azure エフェメラル OS ディスクと MCS I/O を同時に有効にすることはできません。

重要な考慮事項は次のとおりです:

- エフェメラル OS ディスクと MCS I/O の両方を同時に有効にしてマシンカタログを作成することはできません。
- New-ProvSchemeまたはSet-ProvSchemeで **true** に設定された PowerShell パラメーター（UseWriteBackCacheおよびUseEphemeralOsDisk）を使用すると、対応するエラーメッセージが表示されて失敗します。
- 両方の機能を有効にして作成した既存のマシンカタログについては、次のことができます:
  - マシンカタログの更新。
  - VM の追加または削除。
  - マシンカタログの削除。

Azure Compute Gallery

Azure において、MCS でプロビジョニングされたマシンの公開イメージリポジトリとして Azure Shared Image Gallery（旧称: Azure Shared Image Gallery）を使用します。公開イメージをギャラリーに保存して、OS ディスクの作成とハイドレーションを高速化し、非永続仮想マシンの起動時間とアプリケーションの起動時間を改善できます。Shared Image Gallery には、次の 3 つの要素が含まれています:

- ギャラリー: イメージはここに保存されます。MCS は、マシンカタログごとに 1 つのギャラリーを作成します。

- ギャラリーイメージの定義：この定義には、公開イメージに関する情報（オペレーティングシステムの種類と状態、Azure リージョン）が含まれます。MCS は、カタログ用に作成されたイメージごとに 1 つのイメージ定義を作成します。
- ギャラリーイメージバージョン：Shared Image Gallery の各イメージには複数のバージョンを含めることができ、各バージョンには異なるリージョンに複数のレプリカを含めることができます。各レプリカは、公開イメージの完全なコピーです。

> 注：
>
> Shared Image Gallery の機能は、管理対象ディスクとのみ互換性があります。従来のマシンカタログでは使用できません。

詳しくは、「Azure Compute Gallery の概要」を参照してください。

PowerShell と Azure Compute Gallery イメージを使用したマシンカタログの作成または更新については、「Azure Compute Gallery イメージを使用してマシンカタログを作成または更新する」を参照してください。

Azure Confidential VM

Azure Confidential Computing VM によって、仮想デスクトップは確実にメモリ内で暗号化され、使用中に保護されます。

MCS を使用して、Azure Confidential VM を含むカタログを作成できます。このようなカタログを作成するには、マシンプロファイルワークフローを使用する必要があります。VM と ARM テンプレートスペックの両方をマシンプロファイル入力として使用できます。

Confidential VM に関する重要な考慮事項

サポートされる VM サイズと、Confidential VM を含むマシンカタログの作成に関する重要な考慮事項は次のとおりです：

- サポートされる VM サイズ：Confidential VM は次の VM サイズをサポートします：
  - DCasv5 シリーズ
  - DCadsv5 シリーズ
  - ECasv5 シリーズ
  - ECadsv5 シリーズ
- Confidential VM を含むマシンカタログを作成します。
  - Web Studio と PowerShell コマンドを使用することで、Azure Confidential VM を使用してマシンカタログを作成できます。

- Azure Confidential VM でマシンカタログを作成するには、マシンプロファイルベースのワークフローを使用する必要があります。VM またはテンプレートスペックをマシンプロファイルの入力として使用できます。
- マスターイメージとマシンプロファイル入力は両方とも同じ機密のセキュリティの種類で有効にする必要があります。セキュリティの種類は次のとおりです:
  - **VMGuestStateOnly**: VM ゲスト状態のみが暗号化された Confidential VM
  - **DiskWithVMGuestState**: OS ディスクと VM ゲスト状態の両方がプラットフォーム管理キーまたは顧客管理キーで暗号化された Confidential VM。通常の OS ディスクとエフェメラル OS ディスクの両方を暗号化できます。
- AdditionalData パラメーターを使用すると、管理対象ディスク、スナップショット、Azure Compute Gallery イメージ、VM、ARM テンプレートスペックなど、さまざまなリソースの種類の Confidential VM 情報を取得できます。例:

```
PS C:\Users\username> (get-item XDHyp:\HostingUnits\mynetwork
    \image.folder\username-dev-testing-rg.resourcegroup\
    username-dev-tsvda.vm).AdditionalData
```

  追加のデータフィールドは次のとおりです:

  - DiskSecurityType
  - ConfidentialVMDiskEncryptionSetId
  - DiskSecurityProfiles

  マシンサイズの Confidential Computing プロパティを取得するには、次のコマンドを実行します:`(Get-Item -path "XDHyp:\Connections\my-connection-name\East US.region\serviceoffering.folder\abc.serviceoffering").AdditionalData`

  追加のデータフィールドは`ConfidentialComputingType`です。
- マスターイメージまたはマシンプロファイルを機密のセキュリティの種類から機密以外のセキュリティ種類に、または機密以外のセキュリティに酒類から機密のセキュリティの種類に変更することはできません。
- 構成が正しくない場合は、適切なエラーメッセージが表示されます。

マスターイメージとマシンプロファイルを準備する

Confidential VM のセットを作成する前に、次の手順に従ってそれらのマスターイメージとマシンプロファイルを準備します:

1. Azure ポータルで、次のような特定の設定で Confidential VM を作成します:
   - セキュリティの種類: Confidential VM

- **OS** ディスクの機密暗号化：有効になっています。
- キー管理：プラットフォーム管理キーを使用した機密ディスクの暗号化

Confidential VM の作成について詳しくは、こちらの Microsoft の記事を参照してください。

2. 作成した VM 上でマスターイメージを準備します。作成した VM 上で必要なアプリケーションと VDA をインストールします。

   > 注：
   >
   > VHD を使用した Confidential VM の作成はサポートされていません。代わりに、Azure Compute Gallery、Managed Disks、またはスナップショットを使用します。

3. 次のいずれかの方法でマシンプロファイルを作成します：

   - 手順 1 で作成した既存の VM に必要なマシンプロパティがある場合は、それを使用します。
   - マシンプロファイルとして ARM テンプレートスペックを選択する場合は、必要に応じてテンプレートスペックを作成します。具体的には、*SecurityEncryptionType* や *diskEncryptionSet*（顧客管理キーの場合）など、Confidential VM の要件を満たすパラメーターを構成します。詳しくは、「Azure テンプレートスペックの作成」を参照してください。

     > 注：
     >
     > - マスターイメージとマシンプロファイルのセキュリティキーの種類が同じであることを確認します。
     > - 顧客管理キーを使用して OS ディスクの機密暗号化を必要とする Confidential VM を作成するには、マスターイメージとマシンプロファイルの両方のディスク暗号化セット ID が同一であることを確認します。

Web Studio または **PowerShell** コマンドを使用して **Confidential VM** を作成する

Confidential VM のセットを作成するには、マスターイメージと、目的の Confidential VM に基づくマシンプロファイルを使用してマシンカタログを作成します。

Web Studio を使用してカタログを作成するには、「マシンカタログの作成」で説明されている手順に従います。次の考慮事項に留意してください：

- ［イメージ］ページで、Confidential VM の作成用に準備したマスターイメージとマシンプロファイルを選択します。マシンプロファイルの選択は必須であり、選択したマスターイメージと同じセキュリティ暗号化の種類に一致するプロファイルのみが選択可能です。
- ［仮想マシン］ページでは、Confidential VM をサポートするマシンサイズのみが選択肢に表示されます。
- ［ディスク設定］ページでは、選択したマシンプロファイルから継承されるため、ディスク暗号化セットを指定することはできません。

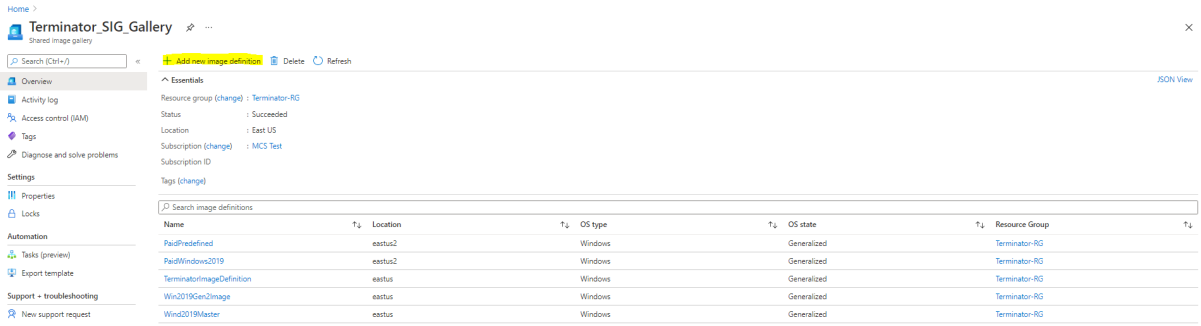
Azure Marketplace

Citrix Virtual Apps and Desktops では、プラン情報を含んだ Azure 内マスターイメージを使用してマシンカタログを作成できます。詳しくは、Microsoft Azure Marketplaceを参照してください。

> ヒント：
>
> 標準の Windows Server イメージなど、Azure Marketplace にある一部のイメージには、プラン情報が追加されていません。Citrix Virtual Apps and Desktops 機能は、有料イメージ用です。

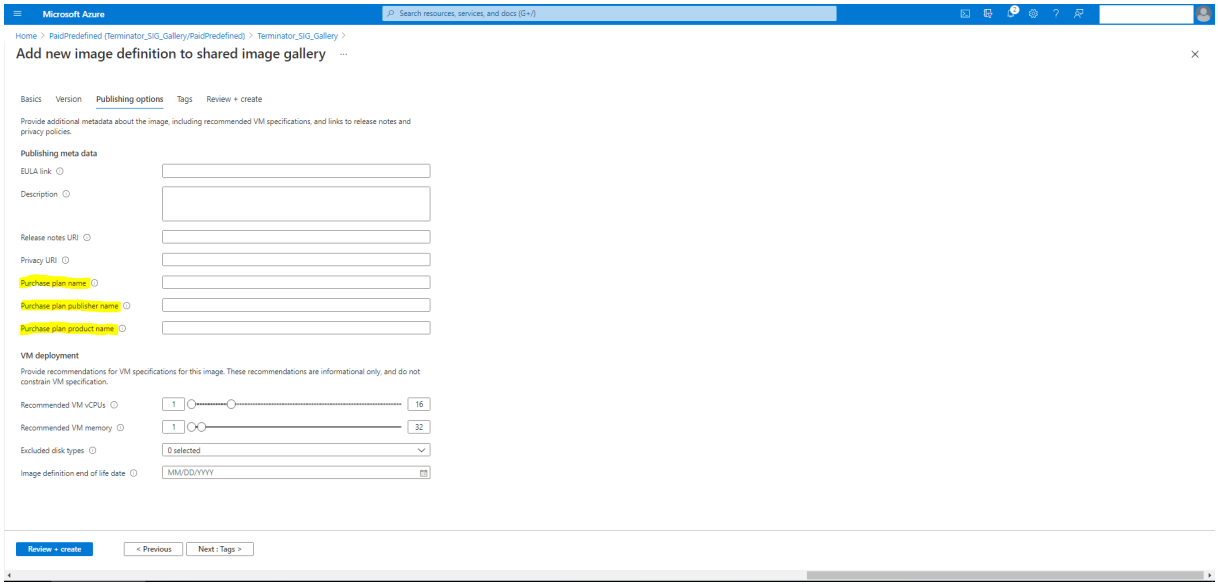
Shared Image Gallery で作成されたイメージに **Azure** プラン情報が含まれていることの確認

このセクションの手順を使用して、Web Studio で Shared Image Gallery のイメージを表示します。これらのイメージは、マスターイメージに使用することもできます。イメージを Shared Image Gallery に配置するには、ギャラリーでイメージ定義を作成します。

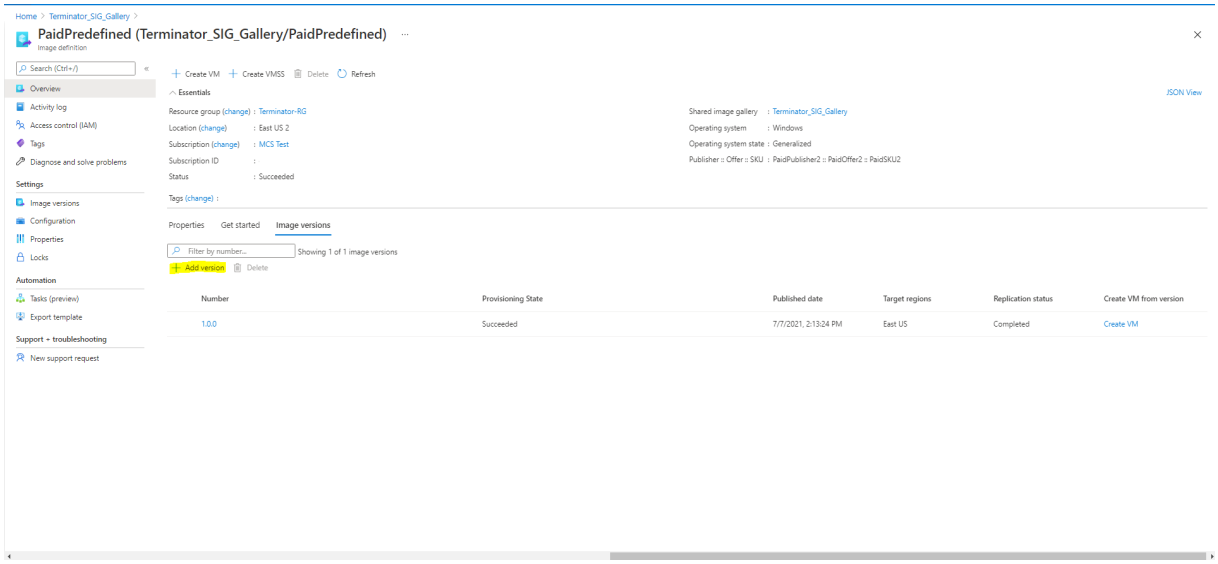


［公開オプション］ページで、購入プラン情報を確認します。

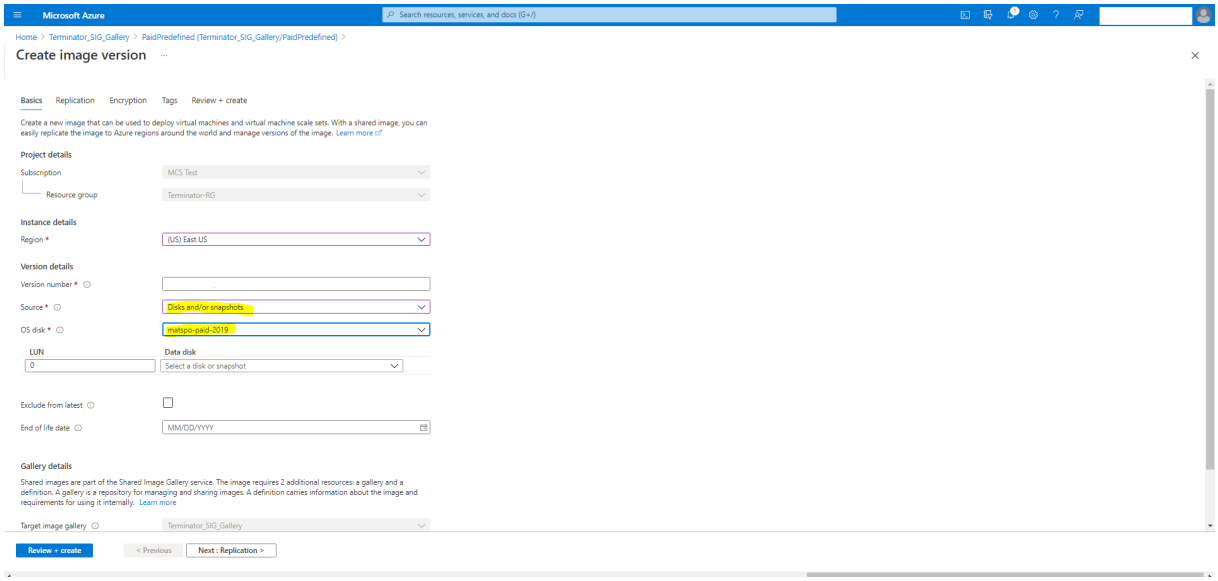
購入プラン情報フィールドは最初は空欄です。これらのフィールドに、イメージに使用されている購入プラン情報を入力します。購入プラン情報を入力しないと、マシンカタログプロセスが失敗する可能性があります。



購入プラン情報を確認した後、定義内にイメージバージョンを作成します。これはマスターイメージとして使用されます。[バージョンの追加] をクリックします:



[バージョンの詳細] セクションで、ソースとしてイメージスナップショットか管理対象ディスクを選択します:



入れ子構造の仮想化

入れ子構造の仮想化を有効にしてマスター VM を構成すると、そのマスター VM を使用して作成された MCS マシンカタログ内のすべての VM で入れ子構造の仮想化が有効になります。この機能は、永続 VM と非永続 VM の両方に適用できます。イメージの更新を通じて、既存の MCS マシンカタログと既存の VM を更新し、入れ子構造の仮想化を実現できます。

現在、入れ子構造の仮想化をサポートしているのは Dv3 および Ev3 VM サイズのみです。

入れ子構造の仮想化について詳しくは、Microsoft のブログ「Nested Virtualization in Azure」を参照してください。

PowerShell を使用してマシンカタログを作成する

このセクションでは、PowerShell を使用してカタログを作成する方法について説明します。

- 非永続的なライトバックキャッシュディスクのカタログを作成する
- 永続的なライトバックキャッシュディスクのカタログを作成する
- MCSIO による起動パフォーマンスの向上
- PowerShell を使用したカタログの作成または更新でテンプレートスペックを使用する
- トラステッド起動を使用したマシンカタログ
- マシンプロファイルのプロパティ値を使用する
- 顧客管理暗号キーを使用したマシンカタログの作成
- 二重暗号化を使用したマシンカタログの作成
- Azure エフェメラルディスクを使用したカタログの作成
- Azure 専用ホスト

- Azure Compute Gallery イメージを使用してマシンカタログを作成または更新する
- Shared Image Gallery を構成する
- 指定されたアベイラビリティゾーンへのマシンのプロビジョニング
- ストレージの種類
- ページファイル設定の更新
- Azure Spot VM を使用したカタログの作成
- バックアップ VM サイズの構成
- すべてのリソースのタグをコピーする
- [Azure Monitor エージェントがインストールされたカタログ VM をプロビジョニングする]

非永続的なライトバックキャッシュディスクのカタログを作成する

非永続的なライトバックキャッシュディスクのカタログを構成するには、PowerShell パラメーター`New-ProvScheme CustomProperties`を使用します。このカスタムプロパティ`UseTempDiskForWBC`は、ライトバックキャッシュファイルを保存するのに、Azure 一時ストレージの使用を受け入れるかどうかを示します。一時ディスクをライトバックキャッシュディスクとして使用する場合は、`New-ProvScheme`実行時に「true」に設定する必要があります。このパラメーターが指定されていない場合、デフォルトは **False** に設定されます。

例：`CustomProperties`パラメーターを使用して`UseTempDiskForWBC`を **true** に設定した場合：

```
-CustomProperties '<CustomProperties xmlns=" http://schemas.citrix.com
    /2014/xd/machinecreation" xmlns:xsi=" http://www.w3.org/2001/
    XMLSchema-instance"> `
<Property xsi:type="StringProperty" Name="PersistWBC" Value="false"/> `
<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="false
    "/> `
<Property xsi:type="StringProperty" Name="PersistVm" Value="false"/> `
<Property xsi:type="StringProperty" Name="StorageAccountType" Value="
    Premium_LRS"/> `
<Property xsi:type="StringProperty" Name="WBCDiskStorageType" Value="
    Premium_LRS"/> `
<Property xsi:type="StringProperty" Name="LicenseType" Value="
    Windows_Client"/> `
<Property xsi:type="StringProperty" Name="UseTempDiskForWBC" Value="
    true"/> `
</CustomProperties>'
```

> 注：
>
> マシンカタログをコミットして、ライトバックキャッシュファイル用として Azure ローカル一時ストレージを使用すると、後から VHD を使用するように変更することはできません。

永続的なライトバックキャッシュディスクのカタログを作成する

永続的なライトバックキャッシュディスクのカタログを構成するには、PowerShell パラメーター`New-ProvScheme CustomProperties`を使用します。このパラメーターでは追加プロパティ`PersistWBC`をサポートしており、これを使用することで、MCS でプロビジョニングされたマシンのライトバックキャッシュディスクを永続化させる方法を指定できます。`PersistWBC`プロパティは、`UseWriteBackCache`パラメーターが指定され、`WriteBackCacheDiskSize`パラメーターがディスクが作成されたことを示すよう設定された場合のみ使用されます。

以下は、`PersistWBC`をサポートする前に`CustomProperties`パラメーターで使用されるプロパティの例です:

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />
<Property xsi:type="StringProperty" Name="StorageAccountType" Value="Premium_LRS" />
<Property xsi:type="StringProperty" Name="ResourceGroups" Value="benvaldev5RG3" />
</CustomProperties>
```

これらのプロパティを使用するときは、プロパティが`CustomProperties`パラメーターから省略されている場合にデフォルトの値が含まれるようにしてください。`PersistWBC`プロパティには、次の 2 つの値が設定可能です: **true** または **false**。

`PersistWBC`プロパティを **true** に設定すると、Citrix Virtual Apps and Desktops 管理者が Web Studio を使用してマシンをシャットダウンしたときにライトバックキャッシュディスクが消去されません。

`PersistWBC`プロパティを **false** に設定すると、Citrix Virtual Apps and Desktops 管理者が Web Studio を使用してマシンをシャットダウンしたときにライトバックキャッシュディスクが消去されます。

> 注:
>
> `PersistWBC`プロパティを省略する場合、デフォルトは **false** になり、Web Studio を使用してマシンをシャットダウンするとライトバックキャッシュは消去されます。

例: `CustomProperties`パラメーターを使用して`PersistWBC`を true に設定した場合:

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />
<Property xsi:type="StringProperty" Name="StorageAccountType" Value="Premium_LRS" />
<Property xsi:type="StringProperty" Name="ResourceGroups" Value="benvaldev5RG3" />
<Property xsi:type="StringProperty" Name="PersistWBC" Value="true" />
```



```
</CustomProperties>
```

> 重要:
>
> PersistWBCプロパティは、New-ProvScheme PowerShell コマンドレットを使用してのみ設定できます。作成後にプロビジョニングスキームのCustomPropertiesを変更しようとしても、マシンがシャットダウンしたときにマシンカタログやライトバックキャッシュディスクの永続性は影響を受けません。

例: PersistWBCプロパティを true に設定するときにNew-ProvSchemeを設定してライトバックキャッシュを使用した場合:

```
New-ProvScheme
-CleanOnBoot
-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com
   /2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/
   XMLSchema-instance`"><Property xsi:type=`"StringProperty`" Name=`"
   UseManagedDisks`" Value=`"true`" /><Property xsi:type=`"
   StringProperty`" Name=`"StorageAccountType`" Value=`"Premium_LRS`"
   /><Property xsi:type=`"StringProperty`" Name=`"ResourceGroups`"
   Value=`"benvaldev5RG3`" /><Property xsi:type=`"StringProperty`" Name
   =`"PersistWBC`" Value=`"true`" /></CustomProperties>"
-HostingUnitName "adSubnetScale1"
-IdentityPoolName "BV-WBC1-CAT1"
-MasterImageVM "XDHyp:\HostingUnits\adSubnetScale1\image.folder\
   GoldImages.resourcegroup\W10MCSIO-01
   _OsDisk_1_a940e6f5bab349019d57ccef65d2c7e3.manageddisk"
-NetworkMapping @{
 "0"="XDHyp:\HostingUnits\adSubnetScale1\virtualprivatecloud.folder\
    CloudScale02.resourcegroup\adVNET.virtualprivatecloud\
    adSubnetScale1.network" }

-ProvisioningSchemeName "BV-WBC1-CAT1"
-ServiceOffering "XDHyp:\HostingUnits\adSubnetScale1\serviceoffering.
   folder\Standard_D2s_v3.serviceoffering"
-UseWriteBackCache
-WriteBackCacheDiskSize 127
-WriteBackCacheMemorySize 256
```

MCSIO による起動パフォーマンスの向上

MCSIO が有効な場合、Azure や GCP の管理対象ディスクの起動パフォーマンスを向上させることができます。New-ProvSchemeコマンドで PowerShell カスタムプロパティPersistOSDiskを使用してこの機能を構成します。New-ProvSchemeに関連するオプションは次のとおりです:

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
   machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
   instance">
<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true"
    />
```



```
<Property xsi:type="StringProperty" Name="StorageAccountType" Value="
    Premium_LRS" />
<Property xsi:type="StringProperty" Name="Resource ``````<!--NeedCopy
    -->
````````Groups" Value="benvaldev5RG3" />
<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="true"
    />
</CustomProperties>
```

この機能を有効にするには、カスタムプロパティ［PersistOSDisk］を「**true**」に設定します。例:

```
New-ProvScheme
-CleanOnBoot
-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com
    /2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/
    XMLSchema-instance`"><Property xsi:type=`"StringProperty`" Name=`"
    UseManagedDisks`" Value=`"true`" /><Property xsi:type=`"
    StringProperty`" Name=`"StorageAccountType`" Value=`"Premium_LRS`"
    /><Property xsi:type=`"StringProperty`" Name=`"ResourceGroups`"
    Value=`"benvaldev5RG3`" /><Property xsi:type=`"StringProperty`" Name
    =`"PersistOsDisk`" Value=`"true`" /></CustomProperties>"
-HostingUnitName "adSubnetScale1"
-IdentityPoolName "BV-WBC1-CAT1"
-MasterImageVM "XDHyp:\HostingUnits\adSubnetScale1\image.folder\
    GoldImages.resourcegroup\W10MCSIO-01
    _OsDisk_1_a940e6f5bab349019d57ccef65d2c7e3.manageddisk"
-NetworkMapping @{
 "0"="XDHyp:\HostingUnits\adSubnetScale1\virtualprivatecloud.folder\
     CloudScale02.resourcegroup\adVNET.virtualprivatecloud\
     adSubnetScale1.network" }

-ProvisioningSchemeName "BV-WBC1-CAT1"
-ServiceOffering "XDHyp:\HostingUnits\adSubnetScale1\serviceoffering.
    folder\Standard_D2s_v3.serviceoffering"
-UseWriteBackCache
-WriteBackCacheDiskSize 127
-WriteBackCacheMemorySize 256
```

PowerShell を使用したカタログの作成または更新でテンプレートスペックを使用する

テンプレートスペックをマシンプロファイルの入力に使用して、MCS マシンカタログを作成または更新できます。これを行うには、Web Studio または PowerShell コマンドを使用できます。

Web Studio については、「Web Studio で Azure Resource Manager イメージを使用してマシンカタログを作成する」を参照してください。

PowerShell コマンドを使用する:

1. **PowerShell** ウィンドウを開きます。
2. `asnp citrix*`を実行します。


```

3. カタログを作成または更新します。

   - カタログを作成するには:

     a) マシンプロファイルの入力で、テンプレートスペックをNew-ProvSchemeコマンドとともに使用します。例:

     ```
     New-ProvScheme -MasterImageVM "XDHyp:/HostingUnits/azure/
         image.folder/fgthj.resourcegroup/nab-ws-
         vda_OsDisk_1_xxxxxxxxxxa.manageddisk"
     MachineProfile "XDHyp:/HostingUnits/azure/machineprofile.
         folder/fgthj.resourcegroup/test.templatespec/V1.
         templatespecversion"
     -ProvisioningSchemeName <String>
     -HostingUnitName <String>
     -IdentityPoolName <String>
     [-ServiceOffering <String>][-CustomProperties <String>
     [-LoggingId <Guid>]
     [-BearerToken <String>][-AdminAddress <String>]
     [<CommonParameters>]
     ```

     b) カタログの作成を完了します。

   - カタログを更新するには、マシンプロファイルの入力で、テンプレートスペックをSet-ProvSchemeコマンドとともに使用します。例:

     ```
     Set-ProvScheme -MasterImageVm 'XDHyp://Connections/Azure/East
         Us.region/vm.folder/MasterDisk.vm'
     MachineProfile 'XDHyp:/HostingUnits/azure/machineprofile.
         folder/fgthj.resourcegroup/testing.templatespec/V1.
         templatespecversion'
     [-ProvisioningSchemeName] <String>
     [-CustomProperties <String>][-ServiceOffering <String>] [-
         PassThru]
     [-LoggingId <Guid>] [-BearerToken <String>][-AdminAddress <
         String>] [<CommonParameters>]
     ```

トラステッド起動を使用したマシンカタログ

トラステッド起動でマシンカタログを正常に作成するには、次を使用します:

- トラステッド起動を使用したマシンプロファイル
- トラステッド起動をサポートする VM サイズ
- トラステッド起動をサポートする Windows VM バージョン。現在、Windows 10、Windows 11、Windows Server 2016、2019、および 2022 はトラステッド起動をサポートしています。

> 重要:
>
> MCS は、トラステッド起動が有効な VM を使用した新しいカタログの作成をサポートしています。ただし、既存の永続カタログと既存の VM を更新するには、Azure Portal を使用する必要があります。非永続カタログの

> トラステッド起動を更新することはできません。詳しくは、Microsoft ドキュメント「既存の Azure VM でトラステッド起動を有効にする」を参照してください。

Citrix Virtual Apps and Desktops オファリングのインベントリアイテムを表示し、VM サイズがトラステッド起動をサポートしているかどうかを判断するには、次のコマンドを実行します:

1. PowerShell ウィンドウを開きます。
2. **asnp citrix*** を実行し、Citrix 固有の PowerShell モジュールをロードします。
3. 次のコマンドを実行します:

```
$s = (ls XDHyp:\HostingUnits<name of hosting unit>\serviceoffering
    .folder"<VM size>.serviceoffering)
```

4. `$s | select -ExpandProperty Additionaldata`を実行します
5. `SupportsTrustedLaunch`属性の値を確認してください。
   - `SupportsTrustedLaunch`が **True** の場合、VM サイズはトラステッド起動をサポートします。
   - `SupportsTrustedLaunch`が **False** の場合、VM サイズはトラステッド起動をサポートしません。

Azure の PowerShell に従って、次のコマンドを使用してトラステッド起動をサポートする VM サイズを決定できます:

```
(Get-AzComputeResourceSku | where {
 $_.Locations.Contains($region) -and ($_.Name -eq "<VM size>")  }
 )[0].Capabilities
```

Azure PowerShell コマンドを実行した後、VM サイズがトラステッド起動をサポートするかどうかを説明する例を次に示します。

- 例 *1*: Azure VM が第 1 世代のみをサポートしている場合、その VM はトラステッド起動をサポートしていません。したがって、Azure PowerShell コマンドを実行した後、`TrustedLaunchDisabled`機能は表示されません。
- 例 *2*: Azure VM が第 2 世代のみをサポートし、`TrustedLaunchDisabled`機能が **True** の場合、第 2 世代の VM サイズはトラステッド起動ではサポートされません。
- 例 *3*:Azure VM が第 2 世代のみをサポートし、PowerShell コマンドの実行後に`TrustedLaunchDisabled`機能が表示されない場合、第 2 世代の VM サイズはトラステッド起動でサポートされます。

Azure 仮想マシンのトラステッド起動ついて詳しくは、Microsoft のドキュメント「Azure Virtual Machines のトラステッド起動」を参照してください。

トラステッド起動を使用したマシンカタログの作成

1. トラステッド起動が有効になっているマスターイメージを作成します。Microsoft のドキュメント「トラステッド起動 VM イメージ」を参照してください。

2. セキュリティの種類をトラステッド起動 **VM** として VM またはテンプレートスペックを作成します。VM またはテンプレートスペックの作成について詳しくは、Microsoft ドキュメント「トラステッド起動の VM をデプロイする」を参照してください。
3. Web Studio または PowerShell コマンドを使用してマシンカタログを作成します。
   - Web Studio を使用する場合は、「Web Studio で Azure Resource Manager イメージを使用してマシンカタログを作成する」を参照してください。
   - PowerShell コマンドを使用する場合は、New-ProvSchemeコマンドを使用し、マシンプロファイルの入力に VM またはテンプレートスペックを指定します。カタログ作成コマンドの完全な一覧については、「Creating a catalog」を参照してください。

     マシンプロファイルの入力に VM を使用したNew-ProvSchemeの例:

     ```
     New-ProvScheme -CleanOnBoot -HostingUnitName "name" -
        IdentityPoolName "name" -InitialBatchSizeHint 1
     -MasterImageVM "XDHyp:/HostingUnits/azure/image.folder/fgthj.
        resourcegroup/nab-ws-vda_OsDisk_1_xxxxxxxxxxa.manageddisk"
     -MachineProfile "XDHyp:\HostingUnits<adnet>\machineprofile.
        folder<def.resourcegroup><machine profile vm.vm>"
     -ProvisioningSchemeName <String>
     -HostingUnitName <String>
     -IdentityPoolName <String>
     [-ServiceOffering <String>][-CustomProperties <String>]
     [<CommonParameters>]
     ```

     マシンプロファイルの入力にテンプレートスペックを使用したNew-ProvSchemeの場合:

     ```
     New-ProvScheme -CleanOnBoot -HostingUnitName "name" -
        IdentityPoolName "name" -InitialBatchSizeHint 1
     -MasterImageVM "XDHyp:/HostingUnits/azure/image.folder/fgthj.
        resourcegroup/nab-ws-vda_OsDisk_1_xxxxxxxxxxa.manageddisk"
     MachineProfile "XDHyp:/HostingUnits/azure/machineprofile.
        folder/fgthj.resourcegroup/test.templatespec/V1.
        templatespecversion"
     -ProvisioningSchemeName <String>
     -HostingUnitName <String>
     -IdentityPoolName <String>
     [-ServiceOffering <String>][-CustomProperties <String>]
     [<CommonParameters>]
     ```

トラステッド起動でマシンカタログを作成する際のエラー

トラステッド起動を使用してマシンカタログを作成しているときに、次のシナリオに応じたエラーが発生します:

シナリオ	エラー
非管理対象カタログの作成中にマシンプロファイルを選択した場合	MachineProfileNotSupportedForUnmanagedCata
非管理対象ディスクをマスターイメージとしてカタログを作成するときに、トラステッド起動をサポートするマシンプロファイルを選択した場合	SecurityTypeNotSupportedForUnmanagedDisk
セキュリティの種類でトラステッド起動を使用し、マスターイメージソースを使用して管理カタログを作成するときに、マシンプロファイルを選択しない場合	MachineProfileNotFoundForTrustedLaunchMaste
マスターイメージとは異なるセキュリティの種類のマシンプロファイルを選択した場合	SecurityTypeConflictBetweenMasterImageAndMa
トラステッド起動をサポートしない VM サイズを選択しながら、カタログの作成時にトラステッド起動をサポートするマスターイメージを使用する場合	MachineSizeNotSupportTrustedLaunch

マシンプロファイルのプロパティ値を使用する

マシンカタログは、カスタムプロパティで定義されている次のプロパティを使用します:

- アベイラビリティゾーン
- 専用ホストグループ ID
- ディスク暗号化セット ID
- OS の種類
- ライセンスの種類
- ストレージの種類

これらのカスタムプロパティが明示的に定義されていない場合、プロパティ値はマシンプロファイルとして使用されている ARM テンプレートスペックの指定または仮想マシンのいずれかから設定されます。また、`ServiceOffering`が指定されていない場合は、マシンプロファイルから設定されます。

> 注:
>
> 一部のプロパティがマシンプロファイルで指定されておらず、カスタムプロパティで定義されていないとき、プロパティのデフォルト値が常に適用されます（該当する場合）。

次のセクションでは、`CustomProperties`ですべてのプロパティが定義されている場合、または値が MachineProfile から由来している場合、`New-ProvScheme`および`Set-ProvScheme`でのシナリオについて説明します。

- New-ProvScheme シナリオ

- MachineProfile ですべてのプロパティが定義され、CustomProperties は定義されていません。例:

  ```
  New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit
  \machineprofile.folder\azure.resourcegroup\mpA.vm"
  ```

  カタログのカスタムプロパティとして、次の値が設定されています:

  ```
  1  Get-ProvScheme | select CustomProperties
  2  <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
        machinecreation" xmlns:xsi="http://www.w3.org/2001/
        XMLSchema-instance">
  3  <Property xsi:type="StringProperty" Name="StorageAccountType"
         Value="<mpA-value>"/>
  4  <Property xsi:type="StringProperty" Name="OSType" Value="<mpA
        -value>"/>
  5  <Property xsi:type="StringProperty" Name="LicenseType" Value=
        "<mpA-value>"/>
  6  <Property xsi:type="StringProperty" Name="DiskEncryptionSetId
        " Value="<mpA-value>"/>
  7  <Property xsi:type="StringProperty" Name="
        DedicatedHostGroupId" Value="<mpA-value>"/>
  8  <Property xsi:type="StringProperty" Name="Zones" Value="<mpA-
        value>"/>
  9  </CustomProperties>
  ```

- MachineProfile で一部のプロパティが定義され、CustomProperties は定義されていません。例: MachineProfile には LicenseType と OsType のみが含まれます。

  ```
  New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit
  \machineprofile.folder\azure.resourcegroup\mpA.vm"
  ```

  カタログのカスタムプロパティとして、次の値が設定されています:

  ```
  1  Get-ProvScheme | select CustomProperties
  2  <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
        machinecreation" xmlns:xsi="http://www.w3.org/2001/
        XMLSchema-instance">
  3  <Property xsi:type="StringProperty" Name="OSType" Value="<mpA
        -value>"/>
  4  <Property xsi:type="StringProperty" Name="LicenseType" Value=
        "<mpA-value>"/>
  5  </CustomProperties>
  ```

- MachineProfile と CustomProperties の両方がすべてのプロパティを定義します。例:

  ```
  New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit
  \machineprofile.folder\azure.resourcegroup\mpA.vm"-CustomProperties
   $CustomPropertiesA
  ```

  カスタムプロパティが優先されます。カタログのカスタムプロパティとして、次の値が設定されています:


```
Get-ProvScheme | select CustomProperties
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
   machinecreation" xmlns:xsi="http://www.w3.org/2001/
   XMLSchema-instance">
<Property xsi:type="StringProperty" Name="StorageAccountType"
    Value="<CustomPropertiesA-value>"/>
<Property xsi:type="StringProperty" Name="OSType" Value="<
   CustomPropertiesA-value>"/>
<Property xsi:type="StringProperty" Name="LicenseType" Value=
   "<CustomPropertiesA-value>"/>
<Property xsi:type="StringProperty" Name="DiskEncryptionSetId
   " Value="<CustomPropertiesA-value>"/>
<Property xsi:type="StringProperty" Name="
   DedicatedHostGroupId" Value="<CustomPropertiesA-value>"/>
<Property xsi:type="StringProperty" Name="Zones" Value="<
   CustomPropertiesA-value>"/>
</CustomProperties>
```

- 一部のプロパティは MachineProfile で定義され、一部のプロパティは CustomProperties で定義されます。例:
  - CustomProperties は、LicenseType と StorageAccountType を定義します
  - MachineProfile は、LicenseType、OsType、Zones を定義します

  ```
  New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit
  \machineprofile.folder\azure.resourcegroup\mpA.vm"-CustomProperties
   $CustomPropertiesA
  ```

  カタログのカスタムプロパティとして、次の値が設定されています:

  ```
  Get-ProvScheme | select CustomProperties
  <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
     machinecreation" xmlns:xsi="http://www.w3.org/2001/
     XMLSchema-instance">
  <Property xsi:type="StringProperty" Name="StorageAccountType"
      Value="<CustomPropertiesA-value>"/>
  <Property xsi:type="StringProperty" Name="OSType" Value="<mpA
     -value>"/>
  <Property xsi:type="StringProperty" Name="LicenseType" Value=
     "<CustomPropertiesA-value>"/>
  <Property xsi:type="StringProperty" Name="Zones" Value="<mpA-
     value>"/>
  </CustomProperties>
  ```

- 一部のプロパティは MachineProfile で定義され、一部のプロパティは CustomProperties で定義されます。また、ServiceOffering は定義されていません。例:
  - CustomProperties は StorageType を定義します
  - MachineProfile は LicenseType を定義します

  ```
  New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit
     \machineprofile.folder\azure.resourcegroup\mp.vm"
  ```



```
2   -ServiceOffering "XDHyp:\HostingUnits\azureunit\
       serviceoffering.folder<explicit-machine-size>.
       serviceoffering"
```

カタログのカスタムプロパティとして、次の値が設定されています:

```
1   Get-ProvScheme | select ServiceOffering
2   serviceoffering.folder<explicit-machine-size>.serviceoffering
3
4   Get-ProvScheme | select CustomProperties
5   <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
       machinecreation" xmlns:xsi="http://www.w3.org/2001/
       XMLSchema-instance">
6   <Property xsi:type="StringProperty" Name="StorageAccountType"
        Value="explicit-storage-type"/>
7   <Property xsi:type="StringProperty" Name="LicenseType" Value=
       "value-from-machineprofile"/>
8   </CustomProperties>
```

- OsType が CustomProperties にも MachineProfile にもない場合、次のようになります:
  - 値はマスターイメージから読み取られます。
  - マスターイメージが非管理対象ディスクの場合、OsType は Windows に設定されます。例:

```
New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit
\machineprofile.folder\azure.resourcegroup\mpA.vm"-MasterImageVM
 "XDHyp:\HostingUnits\azureunit\image.folder\linux-master-
image.manageddisk"
```

マスターイメージの値は、カスタムプロパティに書き込まれます（この場合は Linux）。

```
1   Get-ProvScheme | select CustomProperties
2   <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
       machinecreation" xmlns:xsi="http://www.w3.org/2001/
       XMLSchema-instance">
3   <Property xsi:type="StringProperty" Name="OSType" Value="
       Linux"/>
4   </CustomProperties>
```

- Set-ProvScheme シナリオ
  - 既存のカタログ:
    - StorageAccountTypeおよび OsType の CustomProperties
    - Zones を定義する MachineProfile mpA.vm
  - 更新:
    - StorageAccountType を定義する MachineProfile mpB.vm
    - LicenseType と OsType を定義するカスタムプロパティの新しいセット $CustomPropertiesB


```
Set-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit
\machineprofile.folder\azure.resourcegroup\mpB.vm"-CustomProperties
 $CustomPropertiesB
```

カタログのカスタムプロパティとして、次の値が設定されています:

```
1  Get-ProvScheme | select CustomProperties
2  <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
      machinecreation" xmlns:xsi="http://www.w3.org/2001/
      XMLSchema-instance">
3  <Property xsi:type="StringProperty" Name="StorageAccountType"
       Value="<mpB-value>"/>
4  <Property xsi:type="StringProperty" Name="OSType" Value="<
      CustomPropertiesB-value>"/>
5  <Property xsi:type="StringProperty" Name="LicenseType" Value=
      "<CustomPropertiesB-value>"/>
6      </CustomProperties>
```

- 既存のカタログ:
  - StorageAccountTypeおよび OsType の CustomProperties
  - StorageAccountType と LicenseType を定義する MachineProfile mpA.vm
- 更新:
  - StorageAccountType と OsType を定義するカスタムプロパティの新しいセット $Custom-PropertiesB

```
Set-ProvScheme -CustomProperties $CustomPropertiesB
```

カタログのカスタムプロパティとして、次の値が設定されています:

```
1  Get-ProvScheme | select CustomProperties
2  <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
      machinecreation" xmlns:xsi="http://www.w3.org/2001/
      XMLSchema-instance">
3  <Property xsi:type="StringProperty" Name="StorageAccountType"
       Value="<CustomPropertiesB-value>"/>
4  <Property xsi:type="StringProperty" Name="OSType" Value="<
      CustomPropertiesB-value>"/>
5  <Property xsi:type="StringProperty" Name="LicenseType" Value=
      "<mp-A-value>"/>
6  </CustomProperties>
```

- 既存のカタログ:
  - StorageAccountTypeおよび OsType の CustomProperties
  - Zones を定義する MachineProfile mpA.vm
- 更新:
  - StorageAccountType と LicenseType を定義する MachineProfile mpB.vm

* ServiceOfferingは指定されていません

```
Set-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit
\machineprofile.folder\azure.resourcegroup\mpB.vm"
```

カタログのカスタムプロパティとして、次の値が設定されています:

```
Get-ProvScheme | select ServiceOffering
serviceoffering.folder<value-from-machineprofile>.
    serviceoffering

Get-ProvScheme | select CustomProperties
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
    machinecreation" xmlns:xsi="http://www.w3.org/2001/
    XMLSchema-instance">
<Property xsi:type="StringProperty" Name="StorageAccountType"
     Value="<mpB-value>"/>
<Property xsi:type="StringProperty" Name="OSType" Value="<
    prior-CustomProperties-value>"/>
<Property xsi:type="StringProperty" Name="LicenseType" Value=
    "<mpB-value>"/>
</CustomProperties>
```

[**Azure Monitor** エージェントがインストールされたカタログ **VM** をプロビジョニングする]

Azure の監視は、Azure 環境および社内のオンプレミス環境からテレメトリデータを収集、分析し、それに基づいて操作するために使用できるサービスです。

Azure Monitor エージェント（AMA）は、仮想マシンなどのコンピューティングリソースから監視データを収集し、そのデータを Azure Monitor に配信します。現在、イベントログ、Syslog、パフォーマンスメトリックの収集がサポートされており、収集した結果を Azure Monitor メトリックと Azure Monitor の Log Analytics エージェントのデータソースとして送信します。

監視データ内の VM を一意に識別して監視を有効にするには、AMA を拡張機能としてインストールして MCS マシンカタログの VM をプロビジョニングします。

要件

- 権限:「必要な Azure 権限」で規定されている最小限の Azure の権限と、Azure Monitor を使用するための次の権限を持っていることを確認します:
  - Microsoft.Compute/virtualMachines/extensions/read
  - Microsoft.Compute/virtualMachines/extensions/write
  - Microsoft.Insights/DataCollectionRuleAssociations/Read
  - Microsoft.Insights/dataCollectionRuleAssociations/write
  - Microsoft.Insights/DataCollectionRules/Read

- データ収集規則（DCR）: Azure Portal でデータ収集規則を設定します。DCR の設定について詳しくは、「データ収集規則の作成」を参照してください。DCR はプラットフォーム（Windows または Linux）に固有です。必要なプラットフォームに応じた DCR を必ず作成してください。
  AMA はデータ収集規則（DCR）を使用して、VM などのリソースと、Azure Monitor メトリックや Azure Monitor の Log Analytics エージェントなどのデータ ソースとのマッピングを管理します。
- デフォルトのワークスペース: Azure Portal でワークスペースを作成します。ワークスペースの作成については、「Log Analytics ワークスペースの作成」を参照してください。収集したログとデータの情報は、ワークスペースに保存されます。ワークスペースは、一意のワークスペース ID とリソース ID を持っています。ワークスペース名は、特定のリソースグループに対して固有のものにする必要があります。ワークスペースを作成した後、データがワークスペースに保存されるようにデータソースとソリューションを構成します。
- モニター拡張機能を許可リストに登録しました: 拡張機能`AzureMonitorWindowsAgent`および`AzureMonitorLinuxAgent`が、Citrix が定義している許可リストに登録されました。許可リストに登録されている拡張機能の一覧を表示するには、PoSH コマンド`Get-ProvMetadataConfiguration`を使用します。
- マスターイメージ: Microsoft では、既存のマシンから新しいマシンを作成する前に、既存のマシンから拡張機能を削除することを推奨しています。拡張子を削除しないと、ファイルが残ったり、予期しない動作が行われたりする可能性があるからです。詳しくは、「既存の VM を再作成する場合」を参照してください。

AMA を有効にしてカタログ VM をプロビジョニングするには:

1. マシンプロファイルテンプレートを設定します。
   - VM をマシンプロファイルテンプレートとして使用する場合は、次の手順を実行します:
     a) Azure Portal で VM を作成します。
     b) VM の電源を入れます。
     c) [リソース] で、VM をデータ収集規則に追加します。これにより、テンプレート VM へのエージェントのインストールが起動されます。

     > 注:
     >
     > Linux カタログを作成する場合は、Linux マシンをセットアップします。

   - テンプレートスペックをマシンプロファイルテンプレートとして使用する場合は、次の手順を実行します:
     a) テンプレートスペックを設定します。
     b) 生成されたテンプレートスペックに次の拡張機能とデータ収集規則の関連付けを追加します:

```
{

"type": "Microsoft.Compute/virtualMachines/extensions",
"apiVersion": "2022-03-01",
"name": "<vm-name>/AzureMonitorWindowsAgent",
```



```
"dependsOn": [
    "Microsoft.Compute/virtualMachines/<vm-name>"
],
"location": "<azure-region>",
"properties": {

    "publisher": "Microsoft.Azure.Monitor",
    "type": "AzureMonitorWindowsAgent",
    "typeHandlerVersion": "1.0",
    "autoUpgradeMinorVersion": true,
    "enableAutomaticUpgrade": true
 }

 }
 ,
 {

    "type": "Microsoft.Insights/
       dataCollectionRuleAssociations",
    "apiVersion": "2021-11-01",
    "name": "<associatio-name>",
    "scope": "Microsoft.Compute/virtualMachines/<vm-name>",
    "dependsOn": [
     "Microsoft.Compute/virtualMachines/<vm-name>",
    "Microsoft.Compute/virtualMachines/<vm-name>/extensions
       /AzureMonitorWindowsAgent"
    ],
    "properties": {

       "description": "Association of data collection rule.
           Deleting this association will break the data
          collection for this Arc server.",
     "dataCollectionRuleId": "/subscriptions/<azure-
        subscription>/resourcegroups/<azure-resource-group
        >/providers/microsoft.insights/datacollectionrules
        /<azure-data-collection-rule>"
      }

     }
```

2. MCS マシンカタログを作成または更新します。

   - 新しい MCS カタログを作成するには:

     a) Web Studio で、前述の VM またはテンプレートスペックをマシンプロファイルとして選択します。

     b) 次の手順に進んでカタログを作成します。

   - 既存の MCS カタログを更新する場合は、次の PoSH コマンドを使用します:

     – 更新したマシンプロファイルテンプレートを新しい VM に取り込むには、次のコマンドを実行します:


```
Set-ProvScheme -ProvisioningSchemeName "name"
-MachineProfile "XDHyp:\HostingUnits\Unit1\machineprofile.
    folder\abc.resourcegroup\ab-machine-profile.vm"
```

- 更新したマシンプロファイルテンプレートを使用して既存の VM を更新するには:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-
    catalog -StartsNow -DurationInMinutes -1
```

3. カタログ VM の電源を入れます。
4. Azure Portal に移動し、モニター拡張機能が VM にインストールされているかどうか、および VM が DCR の［リソース］の下に表示されているかどうかを確認します。数分後、監視データが Azure Monitor に表示されます。

トラブルシューティング

Azure Monitor エージェントのトラブルシューティングガイダンスについて詳しくは、以下を参照してください:

- https://learn.microsoft.com/en-us/azure/azure-monitor/agents/azure-monitor-agent-troubleshoot-windows-vm/
- https://learn.microsoft.com/en-us/azure/azure-resource-manager/troubleshooting/create-troubleshooting-template/

顧客管理暗号キーを使用したマシンカタログの作成

顧客管理暗号キーを使用してマシンカタログを作成する方法の詳細な手順は次のとおりです。

1. PowerShell ウィンドウを開きます。
2. `asnp citrix*`を実行し、Citrix 固有の PowerShell モジュールをロードします。
3.「`cd xdhyp:/`」を入力します。
4.「`cd .\HostingUnits\(your hosting unit)`」を入力します。
5.「`cd diskencryptionset.folder`」を入力します。
6.「`dir`」と入力して、ディスク暗号化セットの一覧を取得します。
7. ディスク暗号化セットの ID をコピーします。
8. ディスク暗号化セットの ID を含むカスタムプロパティ文字列を作成します。例:

```
$customProperties = "<CustomProperties xmlns=`"http://schemas.
    citrix.com/2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.
    org/2001/XMLSchema-instance`">
```



```
<Property xsi:type=`"StringProperty`" Name=`"StorageAccountType`" Value=`"Standard_LRS`" />
<Property xsi:type=`"StringProperty`" Name=`"persistWBC`" Value=`"False`" />
<Property xsi:type=`"StringProperty`" Name=`"PersistOsDisk`" Value=`"false`" />
<Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`" Value=`"true`" />
<Property xsi:type=`"StringProperty`" Name=`"DiskEncryptionSetId`" Value=`"/subscriptions/0xxx4xxx-xxb-4bxx-xxxx-xxxxxxxx/resourceGroups/abc/providers/Microsoft.Compute/diskEncryptionSets/abc-des`"/>
</CustomProperties>
```

9. ID プールをまだ作成していない場合は作成します。例:

```
New-AcctIdentityPool -IdentityPoolName idPool -NamingScheme ms## -Domain def.local -NamingSchemeType Numeric
```

10. New-ProvScheme コマンドを実行します。例:

```
New-ProvScheme -CleanOnBoot -HostingUnitName "name" -IdentityPoolName "name" -InitialBatchSizeHint 1
-MasterImageVM "XDHyp:\HostingUnits\azure-res2\image.folder\def.resourcegroup\def.snapshot"
-NetworkMapping @{
 "0"="XDHyp:\HostingUnits\azure-res2\virtualprivatecloud.folder\def.resourcegroup\def-vnet.virtualprivatecloud\subnet1.network" }

-ProvisioningSchemeName "name"
-ServiceOffering "XDHyp:\HostingUnits\azure-res2\serviceoffering.folder\Standard_DS2_v2.serviceoffering"
-MachineProfile "XDHyp:\HostingUnits<adnet>\machineprofile.folder<def.resourcegroup><machine profile vm.vm>"
-CustomProperties $customProperties
```

11. マシンカタログの作成を完了します。

二重暗号化を使用したマシンカタログの作成

Web Studio を使用するか、PowerShell コマンドを実行することで、二重暗号化を使用してマシンカタログを作成し、更新できます。

二重暗号化を使用してマシンカタログを作成する方法の詳細な手順は次のとおりです。

1. プラットフォーム管理キーと顧客が管理するキーを使用して Azure Key Vault と DES を作成します。Azure Key Vault と DES を作成する方法については、「Azure portal を使用して、マネージドディスクの保存時の二重暗号化を有効にします」を参照してください。
2. ホスト接続で利用可能な DiskEncryptionSets を参照するには、次の手順を実行します:

a) **PowerShell** ウィンドウを開きます。
b) 次の PowerShell コマンドを実行します:
   i. `asnp citrix*`
   ii. `cd xdhyp:`
   iii. `cd HostingUnits`
   iv. `cd YourHostingUnitName`（例: azure-east）
   v. `cd diskencryptionset.folder`
   vi. `dir`

`DiskEncryptionSet`の ID を使用したカスタムプロパティで、カタログを作成または更新できます。

3. マシンプロファイルワークフローを使用する場合は、マシンプロファイルの入力用に VM またはテンプレートスペックを作成します。

   - VM をマシンプロファイルの入力に使用する場合は、次の手順を実行します:
     a) Azure Portal で VM を作成します。
     b) **Disks > Key management** に移動して、VM を`DiskEncryptionSetID`で直接暗号化します。
   - テンプレートスペックをマシンプロファイルの入力に使用する場合は、次の手順を実行します:
     a) テンプレートの`properties`>`storageProfile`>`osDisk`>`managedDisk`の下に`diskEncryptionSet`パラメーターを追加し、二重暗号化の DES の ID を追加します。

4. マシンカタログを作成します。

   - Web Studio を使用している場合は、「マシンカタログの作成」の手順に加えて、次のいずれかを実行します。
     - マシンプロファイルベースのワークフローを使用しない場合は、[ディスク設定] ページで、[次のキーを使用して各マシンのデータを暗号化] を選択します。次に、ドロップダウンから二重暗号化の DES を選択します。カタログの作成を続けます。
     - マシンプロファイルワークフローを使用している場合は、[イメージ] ページでマスターイメージとマシンプロファイルを選択します。マシンプロファイルのプロパティにディスク暗号化セット ID があることを確認してください。

     カタログ内に作成されたすべてのマシンは、選択した DES に関連付けられたキーによって二重暗号化されます。
   - PowerShell コマンドを使用する場合は、次のいずれかを実行します:
     - マシンプロファイルベースのワークフローを使用しない場合は、`New-ProvScheme`コマンドにカスタムプロパティ`DiskEncryptionSetId`を追加します。例:

```
1  New-ProvScheme -CleanOnBoot -CustomProperties '<
       CustomProperties xmlns="http://schemas.citrix.com/2014/
       xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/
       XMLSchema-instance">
```



```
<Property xsi:type="StringProperty" Name="UseManagedDisks"
    Value="true" />
<Property xsi:type="StringProperty" Name="
   StorageAccountType" Value="Premium_LRS" />
<Property xsi:type="StringProperty" Name="
   DiskEncryptionSetId" Value="/subscriptions/12345678-
   xxxx-1234-1234-123456789012/resourceGroups/Sample-RG/
   providers/Microsoft.Compute/diskEncryptionSets/
   SampleEncryptionSet" />
</CustomProperties>'
-HostingUnitName "Redacted"
-IdentityPoolName "Redacted"
-InitialBatchSizeHint 1
-MasterImageVM "Redacted"
-NetworkMapping @{
"0"="Redacted" }

-ProvisioningSchemeName "Redacted"
-ServiceOffering "Redacted"
```

- マシンプロファイルベースのワークフローを使用する場合は、New-ProvSchemeコマンドで入力したマシンプロファイルを使用します。例:

```
New-ProvScheme -CleanOnBoot
-HostingUnitName azure-east
-IdentityPoolName aio-ip
-InitialBatchSizeHint 1
-MasterImageVM XDHyp:\HostingUnits\azure-east\image.folder
   \abc.resourcegroup\fgb-vda-snapshot.snapshot
-NetworkMapping @{
"0"="XDHyp:\HostingUnits\azure-east\virtualprivatecloud.
   folder\apa-resourceGroup.resourcegroup\apa-
   resourceGroup-vnet.virtualprivatecloud\default.network"
    }

-ProvisioningSchemeName aio-test
-MachineProfile XDHyp:\HostingUnits\azure-east\
   machineprofile.folder\abc.resourcegroup\abx-mp.
   templatespec\1.0.0.templatespecversion
```

5. Remote PowerShell SDK を使用してカタログの作成を完了します。Remote PowerShell SDK を使用してカタログを作成する方法については、https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/を参照してください。カタログ内に作成されたすべてのマシンは、選択した DES に関連付けられたキーによって二重暗号化されます。

暗号化されていないカタログを二重暗号化を使用するように変換

マシンカタログの暗号化の種類を（カスタムプロパティまたはマシンプロファイルを使用して）更新できます。

- マシンプロファイルベースのワークフローを使用しない場合は、Set-ProvSchemeコマンドにカスタム

プロパティ DiskEncryptionSetId を追加します。例:

```
Set-ProvScheme -ProvisioningSchemeName "SampleProvSchemeName"
-CustomProperties '<CustomProperties xmlns="http://schemas.citrix
    .com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.org
    /2001/XMLSchema-instance">
<Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
    Value="/subscriptions/12345678-xxxx-1234-1234-123456789012/
    resourceGroups/Sample-RG/providers/Microsoft.Compute/
    diskEncryptionSets/SampleEncryptionSet" />
</CustomProperties>'
```

- マシンプロファイルベースのワークフローを使用する場合は、Set-ProvSchemeコマンドで入力したマシンプロファイルを使用します。例:

```
Set-ProvScheme -ProvisioningSchemeName mxiao-test -MachineProfile
     XDHyp:\HostingUnits\azure-east\machineprofile.folder\aelx.
    resourcegroup\elx-mp.templatespec\1.0.0.templatespecversion
```

成功すると、カタログ内に追加されたすべてのマシンは、選択した DES に関連付けられたキーによって二重暗号化されます。

カタログが二重暗号化されていることの確認

- Web Studio の場合:
  1. [マシンカタログ] に移動します。
  2. 確認するカタログを選択します。画面の下部近くにある [テンプレートのプロパティ] タブをクリックします。
  3. [**Azure** の詳細] の [ディスク暗号化セット] でディスク暗号化セット ID を確認します。カタログの DES ID が空白の場合、カタログは暗号化されていません。
  4. Azure Portal で、DES ID に関連付けられた DES の暗号化の種類が、プラットフォーム管理キーと顧客が管理するキーであることを確認します。
- PowerShell コマンドを使用する場合:
  1. **PowerShell** ウィンドウを開きます。
  2. asnp citrix*を実行し、Citrix 固有の PowerShell モジュールをロードします。
  3. Get-ProvSchemeを使用して、マシンカタログの情報を取得します。例:

     ```
     Get-ProvScheme -ProvisioningSchemeName "SampleProvSchemeName"
     ```

  4. マシンカタログの DES ID カスタムプロパティを取得します。例:


```
<Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
     Value="/subscriptions
    /12345678-1234-1234-1234-123456789012/resourceGroups/Sample
    -RG/providers/Microsoft.Compute/diskEncryptionSets/
    SampleEncryptionSet" />
```

5. Azure Portal で、DES ID に関連付けられた DES の暗号化の種類が、プラットフォーム管理キーと顧客が管理するキーであることを確認します。

Azure エフェメラルディスクを使用したカタログの作成

エフェメラルディスクを使用するには、New-ProvSchemeを実行するとき、カスタムプロパティUseEphemeralOsDiskを **true** に設定する必要があります。

> 注:
>
> カスタムプロパティUseEphemeralOsDiskが **false** に設定されているか、値が指定されていない場合、プロビジョニングされたすべての VDA は引き続きプロビジョニングされた OS ディスクを使用します。

以下は、プロビジョニングスキームで使用するカスタムプロパティのセットの例です:

```
"CustomProperties": [
            {

                "Name": "UseManagedDisks",
                "Value": "true"
             }
 ,
            {

                "Name": "StorageType",
                "Value": "Standard_LRS"
             }
 ,
            {

                "Name": "UseSharedImageGallery",
                "Value": "true"
             }
 ,
            {

                "Name": "SharedImageGalleryReplicaRatio",
                "Value": "40"
             }
 ,
            {

                "Name": "SharedImageGalleryReplicaMaximum",
                "Value": "10"
```



```
30                }
31   ,
32               {
33
34                   "Name": "LicenseType",
35                   "Value": "Windows_Server"
36                }
37   ,
38               {
39
40                   "Name": "UseEphemeralOsDisk",
41                   "Value": "true"
42                }
43
44           ],
```

カタログのエフェメラルディスクを構成する

カタログの Azure エフェメラル OS ディスクを構成するには、Set-ProvSchemeのUseEphemeralOsDiskパラメーターを使用します。UseEphemeralOsDiskパラメーターの値を「**true**」に設定します。

> 注:
>
> この機能を使用するには、パラメーターのUseManagedDisksとUseSharedImageGalleryも有効にする必要があります。

例:

```
1  Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties <
       CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
       machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
       instance">
2  <Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true"
        />
3  <Property xsi:type="StringProperty" Name="UseSharedImageGallery" Value=
       "true" />
4  <Property xsi:type="StringProperty" Name="UseEphemeralOsDisk" Value="
       true" />
5  </CustomProperties>'
```

エフェメラルディスクに関する重要な考慮事項

New-ProvSchemeを使用してエフェメラル OS ディスクのプロビジョニングをするには、次の制約を考慮してください:

- カタログに使用される VM サイズは、エフェメラル OS ディスクをサポートする必要があります。
- VM サイズに関連付けられているキャッシュまたは一時ディスクのサイズは、OS ディスクのサイズ以上である必要があります。

- 一時ディスクのサイズは、キャッシュディスクのサイズよりも大きい必要があります。

次の場合にも、これらの問題を考慮してください:

- プロビジョニングスキームを作成する場合。
- プロビジョニングスキームを変更する場合。
- イメージを更新する場合。

Azure 専用ホスト

MCS を使用して、Azure 専用ホストで VM をプロビジョニングできます。Azure 専用ホストで VM をプロビジョニングする前に、以下を実行します:

- ホストグループを作成します。
- そのホストグループにホストを作成します。
- カタログと仮想マシンを作成するために十分なホスト容量が確保されていることを確認してください。

管理者は、次の PowerShell スクリプトで定義されたホストテナントを持つマシンのカタログを作成できます:

```
1 New-ProvScheme <otherParameters> -CustomProperties '<CustomProperties
     xmlns="http://schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi
     ="http://www.w3.org/2001/XMLSchema-instance">
2  <Property xsi:type="StringProperty" Name="HostGroupId" Value="
      myResourceGroup/myHostGroup" />
3  ...other Custom Properties...
4  </CustomProperties>
```

MCS を使用して、Azure 専用ホストで仮想マシンをプロビジョニングする場合、次の点を考慮してください:

- 専用ホストはカタログプロパティであり、カタログの作成後に変更することはできません。専用テナントは現在、Azure ではサポートされていません。
- `HostGroupId`パラメーターを使用する場合は、ホスティングユニットの領域に事前構成された Azure ホストグループが必要です。
- Azure の自動配置が必要です。この機能は、ホストグループに関連付けられたサブスクリプションをオンボードするように要求します。詳しくは、「Azure 専用ホストの VM スケールセット - パブリックプレビュー」を参照してください。自動配置が有効になっていない場合、MCS はカタログの作成中にエラーをスローします。

Azure Compute Gallery イメージを使用してマシンカタログを作成または更新する

マシンカタログの作成に使用するイメージを選択するときに、Azure Compute Gallery で作成したイメージを選択できます。

これらのイメージを表示するには、次のことを行う必要があります:

1. Citrix Virtual Apps and Desktops サイトを構成します。

2. Azure Resource Manager に接続します。
3. Azure ポータルで、リソースグループを作成します。詳しくは、「ポータルを使用して Azure Compute Gallery を作成する」を参照してください。
4. リソースグループで、Azure Compute Gallery を作成します。
5. Azure Compute Gallery で、イメージ定義を作成します。
6. イメージ定義で、イメージバージョンを作成します。

次の PowerShell コマンドを使用して、Azure Compute Gallery からのイメージでマシンカタログを作成または更新します:

1. PowerShell ウィンドウを開きます。
2. `asnp citrix*`を実行し、Citrix 固有の PowerShell モジュールをロードします。
3. リソースグループを選択し、そのリソースグループのすべてのギャラリーを表示します。

```
Get-ChildItem -LiteralPath @("XDHyp:\HostingUnits\testresource\
    image.folder\sharedImageGalleryTest.resourcegroup")
```

4. ギャラリーを選択し、そのギャラリーのすべてのイメージ定義を表示します。

```
Get-ChildItem -LiteralPath @("XDHyp:\HostingUnits\testresource\
    image.folder\sharedImageGalleryTest.resourcegroup\
    sharedImageGallery.sharedimagegallery")
```

5. 1 つのイメージ定義を選択し、そのイメージ定義のすべてのイメージバージョンを表示します。

```
Get-ChildItem -LiteralPath @("XDHyp:\HostingUnits\testresource\
    image.folder\sharedImageGalleryTest.resourcegroup\
    sharedImageGallery.sharedimagegallery\sigtestimage.
    imagedefinition")
```

6. 次の要素を使用して、MCS カタログを作成および更新します:

    - リソースグループ
    - ギャラリー
    - ギャラリーイメージの定義
    - ギャラリーイメージのバージョン

    Remote PowerShell SDK を使用してカタログを作成する方法については、https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/を参照してください。

Shared Image Gallery を構成する

`New-ProvScheme`コマンドを使用することで、Shared Image Gallery をサポートする新しいプロビジョニングスキームを作成できます。`Set-ProvScheme`コマンドでは、プロビジョニングスキームでのこの機能の有効化または無効化と、レプリカの比率およびレプリカの最大値の変更が可能です。

Shared Image Gallery 機能をサポートするために、プロビジョニングスキームに 3 つのカスタムプロパティが追加されました:

UseSharedImageGallery

- Shared Image Gallery を使用して公開イメージを保存するかどうかを定義します。**True** に設定すると、イメージは Shared Image Gallery イメージとして保存されます。True に設定しない場合、イメージはスナップショットとして保存されます。
- 有効な値は、**True** および **False** です。
- プロパティが定義されていない場合、デフォルト値は **False** です。

SharedImageGalleryReplicaRatio

- ギャラリーイメージバージョンのレプリカに対するマシンの比率を定義します。
- 有効な値は、0 より大きい整数です。
- プロパティが定義されていない場合は、デフォルト値が使用されます。永続 OS ディスクのデフォルト値は 1000 であり、非永続 OS ディスクのデフォルト値は 40 です。

SharedImageGalleryReplicaMaximum

- 各ギャラリーイメージバージョンのレプリカの最大数を定義します。
- プロパティが定義されていない場合、デフォルト値は 100 です。
- プロパティが定義されていない場合、デフォルト値は 100 です。

> ヒント:
>
> Shared Image Gallery を使用して MCS プロビジョニングされたカタログの公開イメージを保存する場合、MCS は、カタログ内のマシンの数、レプリカの比率、およびレプリカの最大数に基づいて、ギャラリーイメージバージョンのレプリカ数を設定します。レプリカ数は、カタログ内のマシンの数をレプリカ比率（最も近い整数値に切り上げ）で除算し、最大レプリカ数で値を制限することによって計算されます。たとえば、レプリカの比率が 20 で最大 5 の場合、0〜20 台のマシンで 1 つのレプリカが作成され、21〜40 台で 2 つ、41〜60 台で 3 つ、61〜80 台で 4 つ、81 台以上で 5 つのレプリカが作成されます。

ユースケース：**Shared Image Gallery** のレプリカ比率とレプリカの最大値を更新する

既存のマシンカタログは Shared Image Gallery を使用します。Set-ProvSchemeコマンドを使用して、カタログ内の既存のすべてのマシンおよび将来のマシンのカスタムプロパティを更新します:

```
1 Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties '
    <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
    machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
    instance"> <Property xsi:type="StringProperty" Name="StorageType"
    Value="Standard_LRS"/> <Property xsi:type="StringProperty" Name="
    UseManagedDisks" Value="True"/> <Property xsi:type="StringProperty"
    Name="UseSharedImageGallery" Value="True"/> <Property xsi:type="
    IntProperty" Name="SharedImageGalleryReplicaRatio" Value="30"/> <
```



```
        Property xsi:type="IntProperty" Name="
        SharedImageGalleryReplicaMaximum" Value="20"/></CustomProperties>'
```

ユースケース：スナップショットカタログを **Shared Image Gallery** カタログに変換する

このユースケースの場合：

1. UseSharedImageGalleryフラグを **True** に設定してSet-ProvSchemeを実行します。オプションで、SharedImageGalleryReplicaRatioおよびSharedImageGalleryReplicaMaximumプロパティを含めます。
2. カタログを更新します。
3. マシンの電源を入れ直して、強制的に更新します。

例：

```
1 Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties '
    <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
    machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
    instance"> <Property xsi:type="StringProperty" Name="StorageType"
    Value="Standard_LRS"/> <Property xsi:type="StringProperty" Name="
    UseManagedDisks" Value="True"/> <Property xsi:type="StringProperty"
    Name="UseSharedImageGallery" Value="True"/> <Property xsi:type="
    IntProperty" Name="SharedImageGalleryReplicaRatio" Value="30"/> <
    Property xsi:type="IntProperty" Name="
    SharedImageGalleryReplicaMaximum" Value="20"/></CustomProperties>'
```

> ヒント：
>
> パラメーターSharedImageGalleryReplicaRatioおよびSharedImageGalleryReplicaMaximumは必須ではありません。Set-ProvSchemeコマンドが完了した後、Shared Image Gallery イメージはまだ作成されていません。ギャラリーを使用するようにカタログを構成すると、次回のカタログ更新操作で公開イメージがギャラリーに保存されます。カタログ更新コマンドは、ギャラリー、ギャラリーイメージ、およびイメージバージョンを作成します。マシンの電源を入れ直すとマシンが更新されます。そのとき、必要に応じてレプリカ数が更新されます。それ以降、既存のすべての非永続マシンは Shared Image Gallery イメージを使用してリセットされ、新しくプロビジョニングされたすべてのマシンはイメージを使用して作成されます。古いスナップショットは、数時間以内に自動的にクリーンアップされます。

ユースケース：**Shared Image Gallery** カタログをスナップショットカタログに変換する

このユースケースの場合：

1. UseSharedImageGalleryフラグを **False** に設定するか、定義せずにSet-ProvSchemeを実行します。
2. カタログを更新します。

3. マシンの電源を入れ直して、強制的に更新します。

例:

```
Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties '
    <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
    machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
    instance"> <Property xsi:type="StringProperty" Name="StorageType"
    Value="Standard_LRS"/> <Property xsi:type="StringProperty" Name="
    UseManagedDisks" Value="True"/> <Property xsi:type="StringProperty"
    Name="UseSharedImageGallery" Value="False"/></CustomProperties>'
```

> ヒント:
>
> スナップショットから Shared Image Gallery カタログへの更新とは異なり、各マシンのカスタムデータは、新しいカスタムプロパティを反映するようにまだ更新されていません。次のコマンドを実行して、元の Shared Image Gallery のカスタムプロパティを表示します: `Get-ProvVm -ProvisioningSchemeName catalog-name`。`Set-ProvScheme`コマンドが完了した後、イメージスナップショットはまだ作成されていません。ギャラリーを使用しないようにカタログを構成すると、次回のカタログ更新操作で公開イメージがスナップショットとして保存されます。その時点から、既存のすべての非永続マシンはスナップショットを使用してリセットされ、新しくプロビジョニングされたすべてのマシンはスナップショットから作成されます。マシンの電源を入れ直すと更新され、そのときカスタムマシンデータが更新されて、`UseSharedImageGallery`が **False** に設定されていることが反映されます。古い Shared Image Gallery アセット（ギャラリー、イメージ、バージョン）は、数時間以内に自動的にクリーンアップされます。

指定されたアベイラビリティゾーンへのマシンのプロビジョニング

Azure 環境の特定のアベイラビリティゾーンにマシンをプロビジョニングできます。これは、PowerShell を使用して実行できます。

> 注:
>
> ゾーンが指定されていない場合、MCS は Azure にマシンをリージョン内に配置させます。複数のゾーンが指定されている場合、MCS はマシンをそれらにランダムに分散します。

PowerShell を使用したアベイラビリティゾーンの構成

PowerShell を使用する場合、`Get-Item`でオファリングのインベントリアイテムを表示できます。たとえば、米国東部リージョン `Standard_B1ls`のサービスオファリングを表示するには、以下を実行します:

```
$serviceOffering = Get-Item -path "XDHyp:\Connections\my-connection-
    name\East US.region\serviceoffering.folder\Standard_B1ls.
    serviceoffering"
```

ゾーンを表示するには、アイテムの`AdditionalData`パラメーターを使用します:

`$serviceOffering.AdditionalData`

アベイラビリティゾーンが指定されていない場合、マシンのプロビジョニング方法に変更はありません。

PowerShell を使用してアベイラビリティゾーンを構成するには、`New-ProvScheme`操作で、使用可能な **Zones** カスタムプロパティを使用します。**Zones** プロパティは、マシンをプロビジョニングするアベイラビリティゾーンの一覧を定義します。これらのゾーンには、1 つまたは複数のアベイラビリティゾーンを含めることができます。たとえば、Zones 1 と 3 の場合は、`<Property xsi:type="StringProperty"Name="Zones"Value="1, 3"/>` のようになります。

`Set-ProvScheme`コマンドを使用して、プロビジョニングスキームのゾーンを更新します。

無効なゾーンが指定された場合、プロビジョニングスキームは更新されず、無効なコマンドを修正する方法を示すエラーメッセージが表示されます。

> ヒント:
>
> 無効なカスタムプロパティを指定すると、プロビジョニングスキームは更新されず、関連するエラーメッセージが表示されます。

ストレージの種類

MCS を使用する Azure 環境の仮想マシン用に異なるストレージの種類を選択します。ターゲット VM の場合、MCS は以下をサポートします:

- OS ディスク: プレミアム SSD、SSD または HDD
- ライトバックキャッシュディスク: プレミアム SSD、SSD、または HDD

これらのストレージの種類を使用するときは、次の点を考慮してください:

- VM が選択したストレージの種類をサポートしていることを確認してください。
- 構成で Azure エフェメラルディスクを使用している場合、ライトバックキャッシュディスク設定のオプションは使用できません。

> ヒント:
>
> `StorageType`は、OS タイプとストレージアカウント用に構成されています。`WBCDiskStorageType`は、ライトバックキャッシュのストレージの種類用に構成されています。通常のカタログの場合、`StorageType`が必要です。`WBCDiskStorageType`が構成されていない場合は、`WBCDiskStorageType`のデフォルトとして`StorageType`が使用されます。

WBCDiskStorageType が構成されていない場合、WBCDiskStorageType のデフォルトとして StorageType が使用されます

ストレージの種類の構成

VM 用のストレージの種類を構成するには、New-ProvSchemeのStorageTypeパラメーターを使用します。StorageTypeパラメーターの値を、いずれかのサポートされているストレージの種類に設定します。

以下は、プロビジョニングスキームで使用するCustomPropertiesパラメーターのセットの例です:

```
1 Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties '
     <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
     machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
     instance">
2 <Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true"
      />
3 <Property xsi:type="StringProperty" Name="StorageType" Value="
     Premium_LRS" />
4 <Property xsi:type="StringProperty" Name="LicenseType" Value="
     Windows_Client" />
5 </CustomProperties>'
```

ゾーン冗長ストレージの有効化

カタログの作成中にゾーン冗長ストレージを選択できます。ゾーン冗長ストレージは複数のアベイラビリティゾーンにわたって Azure Managed Disks を同期的に複製するため、別のゾーンの冗長を利用して、ゾーンでの障害から回復できます。

ストレージの種類のカスタムプロパティで **Premium_ZRS** および **StandardSSD_ZRS** を指定できます。ZRS ストレージは、既存のカスタムプロパティを使用するか、**MachineProfile** テンプレートを使用して設定できます。ZRS ストレージも-StartsNowおよび-DurationInMinutes -1パラメーターを指定したSet-ProvVMUpdateTimeWindowコマンドによりサポートされており、既存のマシンを LRS から ZRS ストレージに変更できます。

制限事項:

- 管理対象ディスクでのみサポートされます
- プレミアムおよびスタンダードのソリッドステートドライブ（SSD）でのみサポートされます
- StorageTypeAtShutdownではサポートされません
- 特定のリージョンでのみ利用できます。
- ZRS ディスクを大量に作成すると、Azure のパフォーマンスが低下します。したがって、最初の電源投入時には、小規模なバッチ（一度に 300 台未満のマシン）ごとにマシンの電源をオンにします。

ゾーン冗長ストレージをディスクストレージの種類として設定する　最初のカタログ作成時にゾーン冗長ストレージを選択するか、既存のカタログでストレージの種類を更新できます。

PowerShell コマンドを使用してゾーン冗長ストレージを選択する　`New-ProvScheme` PowerShell コマンドを使用して Azure で新しいカタログを作成するときは、`StorageAccountType`の値として`Standard_ZRS`を使用します。
例:

```
<Property xsi:type="StringProperty" Name="StorageAccountType" Value="
    StandardSSD_ZRS" />
```

この値を設定すると、適切に使用できるかどうかを判断する動的 API によって検証されます。ZRS の使用がカタログで有効でない場合、次の例外が発生する可能性があります:

- **StorageTypeAtShutdownNotSupportedForZrsDisks**: StorageTypeAtShutdown カスタムプロパティは、ZRS ストレージでは使用できません。
- **StorageAccountTypeNotSupportedInRegion**: この例外は、ZRS をサポートしていない Azure リージョンで ZRS ストレージを使用しようとすると発生します。
- **ZrsRequiresManagedDisks**: ゾーン冗長ストレージは、管理対象ディスクでのみ使用できます。

次のカスタムプロパティを使用して、ディスクストレージの種類を設定できます:

- `StorageType`
- `WBCDiskStorageType`
- `IdentityDiskStorageType`

> 注:
>
> カスタムプロパティが設定されていない場合、カタログの作成中にマシンプロファイルの OS ディスク（`StorageType`）が使用されます。

マシンプロファイルから **VM** および **NIC** の診断設定をキャプチャする

マシンカタログの作成中、既存のマシンカタログの更新中、および既存の VM の更新中に、マシンプロファイルから VM および NIC の診断設定をキャプチャできます。

VM またはテンプレートスペックをマシンプロファイルのソースとして使用できます。

主な手順

1. Azure で必要な ID を設定します。これらの ID をテンプレートスペックで指定する必要があります。
    - ストレージアカウント
    - Log Analytics ワークスペース
    - 標準レベルの料金設定のイベントハブ名前空間
2. マシンプロファイルのソースを作成します。
3. 新しいマシンカタログを作成するか、既存のカタログを更新するか、既存の VM を更新します。

Azure で必要な **ID** を設定する

Azure で次のいずれかを設定します:

- ストレージアカウント
- Log Analytics ワークスペース
- 標準レベルの料金設定のイベントハブ名前空間

ストレージアカウントをセットアップする　Azure で標準ストレージアカウントを作成します。テンプレートスペックでは、ストレージアカウントの完全な resourceId を`storageAccountId`として指定します。

データをストレージアカウントに記録するように VM を設定すると、データは`insights-metrics-pt1m`コンテナの下に表示されます。

Log Analytics ワークスペースをセットアップする　Log Analytics ワークスペースを作成します。テンプレートスペックでは、Log Analytics ワークスペースの完全な resourceId を workspaceId として指定します。

ワークスペースにデータを記録するように VM を設定すると、Azure のログでデータを照会できるようになります。ログで Azure の次のコマンドを実行すると、リソースによって記録されたすべてのメトリックの数を表示できます:

‘AzureMetrics
| summarize Count=count() by ResourceId# Microsoft Azure カタログの作成

> 注:
>
> 2023 年 7 月より、Microsoft は Azure Active Directory（Azure AD）の名前を Microsoft Entra ID に変更しました。このドキュメントでは、Azure Active Directory、Azure AD、または AAD への言及はすべて、Microsoft Entra ID を意味することになります。

「マシンカタログの作成」では、マシンカタログを作成するウィザードについて説明します。以下の情報は、Microsoft Azure Resource Manager クラウド環境に固有の詳細について説明しています。

> 注:
>
> Microsoft Azure カタログを作成する前に、Microsoft Azure への接続の作成を完了する必要があります。「Microsoft Azure への接続」を参照してください。

マシンカタログの作成

マシンカタログは次の 2 つの方法で作成できます。

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

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

イメージは、マシンカタログ内に VM を作成するために使用される Azure Compute Gallery 内のイメージ定義のイメージバージョンの場合もあれば、ディスクまたはスナップショットの場合もあります。マシンカタログを作成する前に、Azure Resource Manager でイメージを作成します。イメージについて詳しくは、「マシンカタログの作成」を参照してください。

> 注:
>
> ホスト接続で構成されたリージョンとは異なるリージョンからマスターイメージを使用することに対するサポートは、廃止されました。Azure Compute Gallery を使用して、マスターイメージを目的のリージョンに複製します。

イメージの準備中に、元の VM に基づいて準備用の VM が作成されます。この準備 VM はネットワークから切断されています。ネットワークを準備 VM から切断するために、すべての受信および送信トラフィックを拒否するネットワークセキュリティグループが作成されます。ネットワークセキュリティグループは、自動的にカタログごとに 1 回作成されます。ネットワークセキュリティグループの名前は <!JEKYLL@5300@0> で、GUID がランダムに生成されます。例：<!JEKYLL@5300@1>。

マシンカタログ作成ウィザードで次の操作を行います：

- ［マシンの種類］ページと ［マシン管理］ページには、Azure 固有の情報は含まれていません。「マシンカタログの作成」のガイダンスに従ってください。
- ［イメージ］ページで、このカタログでマシンの作成に使用するテンプレートのイメージを選択します。

  使用するイメージの種類としてマスターイメージを選択した場合は、［イメージを選択］をクリックし、必要に応じて次の手順でマスターイメージを選択します：

  1. (テナント内またはテナント間で共有イメージを使用して構成された接続にのみ適用可能) イメージが存在するサブスクリプションを選択します。
  2. リソースグループの選択
  3. Azure VHD、Azure Compute Gallery、または Azure イメージバージョンに移動します。必要に応じて、選択したイメージにメモを追加します。

  イメージを選択するときは、次の点を考慮してください：

  - Citrix VDA がイメージにインストールされていることを確認します。
  - VM に接続されている VHD を選択した場合は、次の手順に進む前に VM をシャットダウンする必要があります。

  > 注:
  >
  > - カタログにマシンを作成した接続（ホスト）のサブスクリプションは、緑色の点で示されます。他のサブスクリプションは、Azure Compute Gallery をそのサブスクリプションと共有します。これらのサブスクリプションでは、共有ギャラリーのみが表示されます。共有サブスクリプションの

構成方法については、「単一のテナント内（サブスクリプション間）での画像の共有」および「テナント間での画像の共有」を参照してください。

- トラステッド起動が有効になっているイメージまたはスナップショットを選択する場合は、［セキュリティの種類］としてトラステッド起動が選択されているマシンプロファイルを使用する必要があります。次に、マシンプロファイルの値を指定することにより、SecureBoot と vTPM を有効または無効にできます。トラステッド起動は、Shared Image Gallery ではサポートされていません。Azure のトラステッド起動については、「https://docs.microsoft.com/en-us/azure/virtual-machines/trusted-launch」を参照してください。
- トラステッド起動で、Windows でエフェメラル OS ディスクを使用して、プロビジョニングスキームを作成できます。トラステッド起動でイメージを選択する場合は、vTPM が有効になっているトラステッド起動でマシンプロファイルを選択する必要があります。エフェメラル OS ディスクを使用してマシンカタログを作成する方法については、「エフェメラル OS ディスクを使用してマシンを作成する方法」を参照してください。
- イメージのレプリケーション中に、先に進んでそのイメージをマスターイメージとして選択し、セットアップを完了することができます。ただし、イメージのレプリケーション中は、カタログ作成完了までの時間が長くなることがあります。MCS では、カタログの作成開始から 1 時間以内にレプリケーションを完了する必要があります。レプリケーションがタイムアウトすると、カタログの作成は失敗します。レプリケーションステータスは Azure で確認できます。レプリケーションがまだ保留中の場合、またはレプリケーションが完了した後で再試行してください。
- Azure でマシンカタログのマスターイメージを選択すると、MCS は、選択されたマスターイメージとマシンプロファイルに基づいて OS の種類を識別します。MCS で識別できない場合は、マスターイメージに一致する OS の種類を選択してください。
- Gen2 イメージを使用して Gen 2 VM カタログをプロビジョニングし、起動時のパフォーマンスを向上させることができます。ただし、Gen1 イメージを使用した Gen2 マシンカタログの作成はサポートされていません。同様に、Gen2 イメージを使用した Gen1 マシンカタログの作成もサポートされていません。また、世代情報を持たない古いイメージはすべて Gen1 イメージです。

使用するイメージの種類として準備済みイメージを選択した場合は、［イメージを選択］をクリックし、必要に応じて準備済みイメージを選択します。

VM の作成を成功させるには、イメージに Citrix VDA 2311 以降がインストールされており、VDA に MCSIO が存在することを確認します。

イメージを選択すると、［マシンプロファイルを使用する（**Azure Active Directory** では必須）］チェックボックスが自動的に選択されます。［マシンプロファイルを選択］を クリックして、リソースグループの一覧から VM または ARM テンプレートスペックを参照します。カタログ内の VM は、指定したマシンプロファイルから構成を継承できます。

ARM テンプレートスペックを検証して、マシンカタログを作成するためにマシンプロファイルとして使用できるかどうかを確認します。ARM テンプレートスペックを検証する方法は 2 つあります：

- リソースグループの一覧から ARM テンプレートスペックを選択したら、［次へ］をクリックします。ARM テンプレートスペックにエラーがある場合、エラーメッセージが表示されます。

  - 次の PowerShell コマンドのいずれかを実行します:
    * <!JEKYLL@5300@2>
    * <!JEKYLL@5300@3>

  VM がマシンプロファイルから継承できる構成の例として、次のようなものがあります:

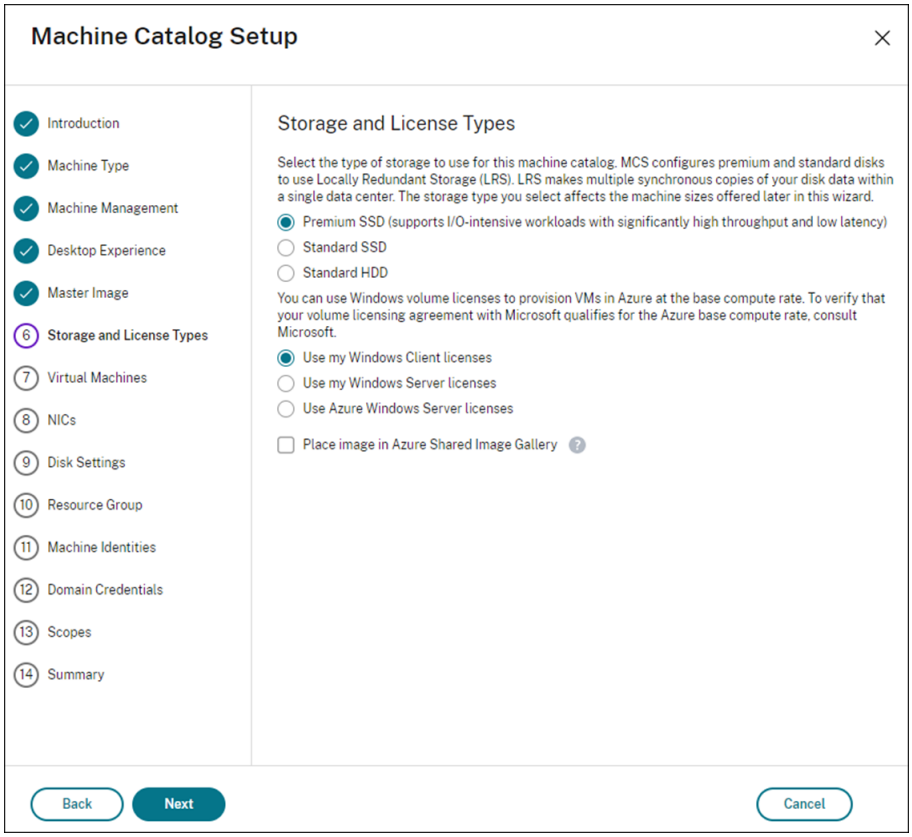
  - 高速ネットワーク
  - ブート診断
  - ホストのディスクキャッシュ（OS および MCSIO ディスク関連）
  - マシンサイズ（別途指定されていない場合）
  - VM に適用されたタグ

  カタログを作成した後、イメージがマシンプロファイルから継承している構成を表示できます。［マシンカタログ］ノードで、カタログを選択して下部ペインに詳細を表示します。次に、［テンプレートのプロパティ］タブをクリックしてマシンプロファイルのプロパティを表示します。［タグ］セクションには、最大 3 つのタグが表示されます。その VM に配置されているすべてのタグを表示するには、［すべて表示］をクリックします。

  MCS で Azure 専用ホストに VM をプロビジョニングする場合は、［専用のホストグループを使用する］チェックボックスをオンにし、一覧からホストグループを選択します。ホストグループは、専用ホストのコレクションを表すリソースです。専用ホストは、1 つまたは複数の VM をホストする物理サーバーを提供するサービスです。サーバーは Azure サブスクリプション専用であり、他のサブスクライバーとは共有されません。専用ホストを使用する場合、Azure は、VM がそのホストで実行されている唯一のマシンであることを保証します。この機能は、規制または内部のセキュリティ要件を満たす必要があるシナリオに適しています。ホストグループとそれらを使用する際の考慮事項について詳しくは、「Azure 専用ホスト」を参照してください。

  > 重要:
  >
  > - Azure の自動配置が有効になっているホストグループのみが表示されます。
  > - ホストグループを使用すると、ウィザードの後半で表示される［**Virtual Machines**］ページが変更されます。選択したホストグループに含まれるマシンサイズのみが、このページに表示されます。また、アベイラビリティゾーンは自動的に選択され、選択できません。

- ［ストレージとライセンスの種類］ページは、Azure Resource Manager イメージを使用するときのみ表示されます。



マシンカタログに使用するストレージの種類は次のとおりです：

- プレミアム **SSD**：I/O を多用するワークロードを持つ VM に適した、高性能かつ低遅延のディスクストレージオプションを提供します。
- 標準 **SSD**：低 IOPS レベルで安定したパフォーマンスを必要とするワークロードに適した、コスト効率の高いストレージオプションを提供します。
- 標準 **HDD**：遅延の影響を受けないワークロードを実行している VM に対して、信頼性の高い低コストのディスクストレージオプションを提供します。
- **Azure** エフェメラル **OS** ディスク VM のローカルディスクを再利用してオペレーティングシステムディスクをホストする、コスト効率の高いストレージオプションを提供します。または、PowerShell を使用して、エフェメラル OS ディスクを使用するマシンを作成することもできます。詳しくは、「Azure エフェメラルディスク」を参照してください。エフェメラル OS ディスクを使用する場合は、次の考慮事項に注意してください：
  - Azure エフェメラル OS ディスクと MCS I/O を同時に有効にすることはできません。
  - エフェメラル OS ディスクを使用するマシンを更新するには、サイズが仮想マシンのキャッシュディスクまたは一時的ディスクのサイズを超えないイメージを選択する必要があります。
  - ウィザードの後半で表示される ［電源サイクル中に仮想マシンとシステムディスクを保持する］オプションを使用することはできません。

> 注:
>
> ID ディスクは、選択したストレージの種類に関係なく、常に標準 SSD を使用して作成されます。

ストレージの種類によって、ウィザードの ［仮想マシン］ページに表示されるマシンのサイズが変わります。MCS は、ローカル冗長ストレージ（LRS）を使用するようにプレミアムディスクと標準ディスクを構成します。LRS は、単一のデータ センター内でデータの複数の同期コピーを作成します。Azure エフェメラル OS ディスクは、VM のローカルディスクを使用してオペレーティングシステムを格納します。Azure のストレージの種類およびストレージの複製について詳しくは、以下のドキュメントを参照してください:

- https://docs.microsoft.com/en-us/azure/storage/common/storage-introduction/
- https://docs.microsoft.com/en-us/azure/virtual-machines/premium-storage-performance/
- https://docs.microsoft.com/en-us/azure/storage/common/storage-redundancy/

既存の Windows ライセンスを使用するか Linux ライセンスを使用するかを選択します。

- Windows ライセンス: Windows ライセンスと Windows イメージ（Azure プラットフォームのサポートイメージまたはカスタムイメージ）を使用すると、Azure で Windows VM を低コストで実行できます。ライセンスには次の 2 種類があります:
  - **Windows Server** ライセンス。Windows Server ライセンスまたは Azure Windows Server ライセンスを使用できます。これにより、Azure Hybrid 特典を使用できます。詳しくは、https://azure.microsoft.com/en-us/pricing/hybrid-benefit/を参照してください。Azure Hybrid 特典を使用すると、Azure ギャラリーからの Windows Server 追加ライセンス料金が不要になるため、Azure での仮想マシン実行コストを基本計算料金のみに抑えられます。
  - **Windows** クライアントライセンス。Windows 10 ライセンスおよび Windows 11 ライセンスを Azure に移行できるため、追加のライセンスなしで Windows 10 VM および Windows 11 VM を Azure で実行できます。詳しくは、「クライアントアクセスライセンスと管理ライセンス」を参照してください。

プロビジョニングされた仮想マシンがライセンス特典を使用していることを確認するには、次の PowerShell コマンドを実行します: <!JEKYLL@5300@4>。

- ［Windows Server のライセンスの種類］で、ライセンスの種類が ［**Windows_Server**］であることを確認します。詳しくは、https://docs.microsoft.com/en-us/azure/virtual-machines/windows/hybrid-use-benefit-licensing/を参照してください。
- ［Windows クライアントのライセンスの種類］ で、ライセンスの種類が ［**Windows_Client**］であることを確認します。詳しくは、https://docs.microsoft.com/en-us/azure/virtual-machines/windows/windows-desktop-multitenant-hosting-deployment/を参照してください。

または、<!JEKYLL@5300@5> PowerShell SDK を使用して確認することもできます。例: <!JEKYLL@5300@6>。このコマンドレットについて詳しくは、https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/MachineCreation/Get-ProvScheme/を参照してください。

- Linux ライセンス: bring-your-own-subscription（BYOS）Linux ライセンスを使用すると、ソフトウェアの料金を支払う必要がありません。BYOS の料金には、コンピューティングハードウェアの料金のみが含まれます。ライセンスには次の 2 種類があります:

  * **RHEL_BYOS**: RHEL_BYOS の種類を正しく使用するには、Azure サブスクリプションで Red Hat Cloud Access を有効にします。
  * **SLES_BYOS**: SLES の BYOS バージョンには、SUSE からのサポートが含まれています。

  LicenseType 値を <!JEKYLL@5300@7> および <!JEKYLL@5300@8> で Linux オプションに設定できます。

  LicenseType を <!JEKYLL@5300@9> で RHEL_BYOS に設定した例:

  <!JEKYLL@5300@10>

  LicenseType を <!JEKYLL@5300@11> で SLES_BYOS に設定した例:

  <!JEKYLL@5300@12>

  > 注:
  >
  > <!JEKYLL@5300@13> 値が空の場合、デフォルト値は、OsType 値に応じて、Azure Windows Server ライセンスまたは Azure Linux ライセンスになります。

  LicenseType を空にした例:

  <!JEKYLL@5300@14>

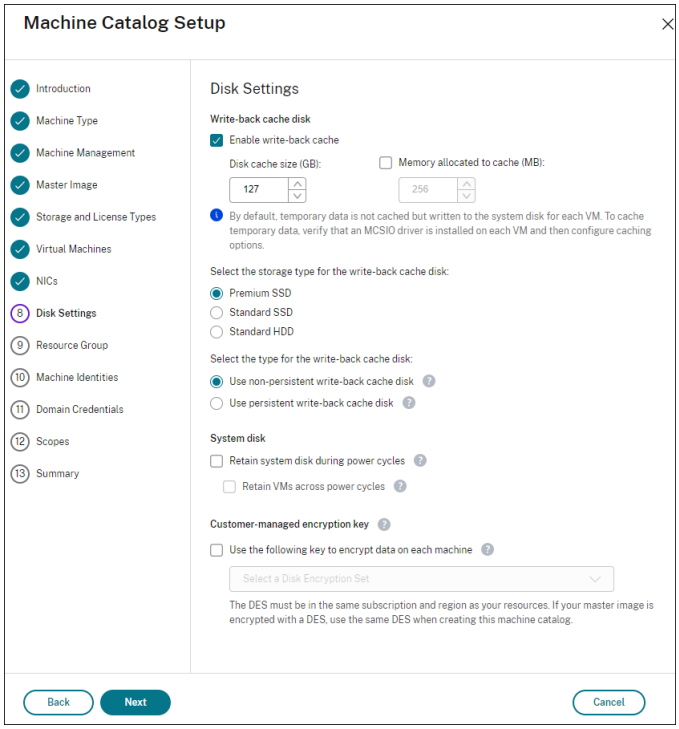
ライセンスの種類と利点を理解するには、次のドキュメントを参照してください:

- https://docs.microsoft.com/en-us/dotnet/api/microsoft.azure.management.compute.models.virtualmachine.licensetype?view=azure-dotnet
- https://docs.microsoft.com/en-us/azure/virtual-machines/linux/azure-hybrid-benefit-linux

Azure Compute Gallery（旧称 Azure Shared Image Gallery）は、イメージを管理および共有するためのリポジトリです。これにより、組織全体でイメージを利用できるようになります。大規模な永続的でないマシンカタログを作成する場合は、よりすばやく VDA OS ディスクをリセットできるため、イメージを SIG に保存することをお勧めします。[準備されたイメージを **Azure Compute Gallery** に配置します] を選択すると、[**Azure Computer Gallary** の設定] セクションが表示され、追加の Azure Compute Gallery 設定を指定できます:

  - イメージレプリカに対する仮想マシンの比率。Azure で保持するイメージレプリカに対する仮想マシンの比率を指定できます。デフォルトでは、Azure は 40 台の非永続的なマシンごとに 1 つのイメージレプリカを保持します。永続マシンの場合、その数はデフォルトで 1,000 になります。
  - 最大レプリカ数。Azure で保持するイメージレプリカの最大数を指定できます。デフォルトは 100 です。

- [仮想マシン] ページで、作成する仮想マシンの数を指定します。少なくとも 1 つを指定し、マシンサイズを選択する必要があります。カタログ作成後、カタログを編集してマシンサイズを変更できます。
- [**NIC**] ページには、Azure 固有の情報は表示されません。「マシンカタログの作成」のガイダンスに従ってください。
- [ディスク設定] ページで、ライトバックキャッシュを有効にするかどうかを選択します。MCS ストレージ最適化機能を有効にすると、カタログを作成するときに以下の設定を構成できます。これらの設定は、Azure 環境と GCP 環境の両方に適用されます。



ライトバックキャッシュを有効にした後、次の操作を実行できます:

  - 一時データのキャッシュに使用するディスクと RAM のサイズを構成する。詳しくは、「一時データ用キャッシュの構成」を参照してください。
  - ライトバックキャッシュディスク用のストレージの種類を選択します。ライトバックキャッシュディスクには、次のストレージのオプションを使用できます:
    * プレミアム SSD
    * 標準 SSD
    * 標準 HDD

- プロビジョニングされた VM に対してライトバックキャッシュディスクを保持するかどうかを選択します。このオプションを使用可能にするには、［ライトバックキャッシュを有効にする］を選択します。デフォルトでは、［非永続的なライトバックキャッシュディスクを使用する］が選択されています。
- ライトバックキャッシュディスクの種類を選択します。
  - 非永続的なライトバックキャッシュディスクを使用する。選択した場合、ライトバックキャッシュディスクは電源サイクル中に削除されます。リダイレクトされたデータはすべて失われます。VM の一時ディスクに十分なスペースがある場合、それはライトバックキャッシュディスクのホストに使用され、コストを削減します。カタログの作成後、プロビジョニングされたマシンが一時ディスクを使用しているかどうかを確認できます。これを行うには、カタログをクリックして、［テンプレートのプロパティ］タブの情報を確認します。一時ディスクが使用されている場合は、［非永続的なライトバックキャッシュディスク］が表示され、その値は ［はい（**VM** の一時ディスクを使用)］になっていますそうでない場合は、［非永続的なライトバックキャッシュディスク］が表示され、その値は ［いいえ］（**VM** の一時ディスクを使用しない）になっています。
  - 永続的なライトバックキャッシュディスクを使用する。選択した場合、ライトバックキャッシュディスクは、プロビジョニングされた VM で保持されます。このオプションを有効にすると、ストレージコストが増加します。
- 電源サイクル中に VDA 用の仮想マシンとシステムディスクを保持するかどうかを選択します。

  電源サイクル中に仮想マシンおよびシステムディスクを保持します。［ライトバックキャッシュを有効にする］を選択した場合に使用できます。デフォルトでは、仮想マシンとシステムディスクはシャットダウン時に削除され、スタートアップ時に再作成されます。仮想マシンの再起動時間を短縮したい場合は、このオプションを選択します。このオプションを有効にすると、ストレージコストも増加することに注意してください。
- ストレージコストの削減を有効にするかどうかを選択します。有効にすると、VM のシャットダウン時にストレージディスクを標準 HDD にダウングレードすることで、ストレージコストを削減できます。VM は、再起動時に元の設定に切り替わります。このオプションは、ストレージディスクとライトバックキャッシュディスクの両方に適用されます。または、PowerShell を使用することもできます。「仮想マシンのシャットダウン時にストレージの種類をダウングレードする」を参照してください。

  > 注:
  >
  > Microsoft は、VM のシャットダウン中のストレージの種類の変更に制限を課しています。Microsoft が将来的にストレージの種類の変更を禁止する可能性もあります。詳しくは、Microsoft 社の記事を参照してください。
- カタログでプロビジョニングされるマシンのデータを暗号化するかどうかを選択します。顧客が管理する暗号化キーを使用したサーバー側暗号化により、管理対象ディスクレベルで暗号化を管理し、カタログ内のマシン上のデータを保護できます。詳しくは、「Azure サーバー側暗号化」を参照してください。

- ［リソースグループ］ページで、リソースグループを作成するか、既存のグループを使用するかを選択します。
  - リソースグループを作成する場合は、［次へ］を選択します。

  - 既存のリソースグループを使用する場合は、［使用可能なプロビジョニングリソースグループ］ボックスの一覧からグループを選択します。注意事項：カタログで作成しているマシンを収容するのに十分なグループを選択してください。選択が少なすぎると、メッセージが表示されます。後でカタログにさらに VM を追加する予定がある場合は、必要最小限よりも多く選択しておくことをお勧めします。カタログが作成された後、カタログにリソースグループをさらに追加することはできません。

  詳しくは、「Azure リソースグループ」を参照してください。

- ［マシン **ID**］ページで ID の種類を選択し、このカタログ内のマシンの ID を設定します。［**Azure Active Directory** 参加］として仮想マシンを選択すると、それらを Azure AD セキュリティグループに追加できます。詳細な手順は次のとおりです：

  1. ［**ID** の種類］フィールドから、［**Azure Active Directory** 参加］を選択します。［**Azure AD** セキュリティグループ（オプション）］オプションが表示されます。
  2. ［**Azure AD** セキュリティグループ：新規作成］をクリックします。
  3. グループ名を入力して、［作成］をクリックします。
  4. 画面の指示に従って、Azure にサインインします。
     グループ名が Azure に存在しない場合は、緑色のアイコンが表示されます。それ以外の場合は、新しい名前の入力を求めるエラーメッセージが表示されます。
  5. 仮想マシンのマシンアカウント名前付けスキームを入力します。

  カタログの作成後、Citrix Virtual Apps and Desktops はユーザーに代わって Azure にアクセスし、セキュリティグループとグループの動的メンバーシップ規則を作成します。この規則に基づいて、このカタログで指定された名前付けスキームの仮想マシンがセキュリティグループに自動的に追加されます。

  このカタログに別の名前付けスキームの仮想マシンを追加するには、Azure にサインインする必要があります。これにより、Citrix Virtual Apps and Desktops は Azure にアクセスし、新しい名前付けスキームに基づいて動的メンバーシップ規則を作成できます。

  このカタログを削除する場合、Azure からセキュリティグループを削除するには、Azure へのサインインも必要です。

- ［ドメイン資格情報］ページおよび ［概要］ページには、Azure 固有の情報は表示されません。「マシンカタログの作成」のガイダンスに従ってください。

ウィザードを完了します。

Azure 一時ディスクをライトバックキャッシュディスクとして使用するための条件

次のすべての条件が満たされている場合にのみ、Azure 一時ディスクをライトバックキャッシュディスクとして使用できます：

- Azure 一時ディスクは永続データには適していないため、ライトバックキャッシュディスクは非永続である必要があります。

- 選択した Azure VM のサイズには、一時ディスクが含まれている必要があります。
- エフェメラル OS ディスクを有効にする必要はありません。
- ライトバックキャッシュファイルを Azure 一時ディスクに保存することを受け入れます。
- Azure 一時ディスクのサイズは、「ライトバックキャッシュディスクサイズ + ページングファイル用に予約されたスペース + 1GB のバッファスペース」の合計サイズよりも大きい必要があります。

非永続的なライトバックキャッシュディスクのシナリオ

次の表は、マシンカタログの作成中に一時ディスクがライトバックキャッシュに使用される場合の 3 つの異なるシナリオを示しています。

シナリオ	結果
ライトバックキャッシュに一時ディスクを使用するためのすべての条件が満たされている。	WBC ファイル <!JEKYLL@5300@15> は一時ディスクに保存されます。
一時ディスクに、ライトバックキャッシュを使用するための十分なスペースがない。	VHD ディスク <!JEKYLL@5300@16> が作成され、このディスクに WBC ファイル <!JEKYLL@5300@17> が保存されます。
一時ディスクに、ライトバックキャッシュを使用するための十分なスペースがあるが、<!JEKYLL@5300@18> は **false** に設定されている。	VHD ディスク <!JEKYLL@5300@19> が作成され、このディスクに WBC ファイル <!JEKYLL@5300@20> が保存されます。

Azure テンプレートスペックを作成する

Azure Portal で Azure テンプレートスペックを作成し、それを Web Studio と PowerShell コマンドで使用して、MCS マシンカタログを作成または更新できます。

既存の仮想マシンの Azure テンプレートスペックを作成するには、以下の手順に従います:

1. Azure Portal に移動します。リソースグループを選択してから、仮想マシンとネットワークインターフェイスを選択します。上の［…］メニューで、［**Export template**］をクリックします。
2. カタログプロビジョニング用のテンプレートスペックを作成する場合は、［**Include parameters**］チェックボックスをオフにします。
3. テンプレートスペックを後で変更するには、［**Add to library**］をクリックします。
4. ［**Importing template**］ページで、**Name**、**Subscription**、**Resource Group**、**Location**、**Version** などの必要な情報を入力します。［**Next: Edit Template**］をクリックします。

5. カタログをプロビジョニングする場合は、独立したリソースとしてネットワークインターフェイスも必要です。したがって、テンプレートスペックで指定されている <!JEKYLL@5300@21> を削除する必要があります。例:

   <!JEKYLL@5300@22>

6. [**Review+Create**] を作成してテンプレートスペックを作成します。
7. [**Template Specs**] ページで、作成したテンプレートスペックを確認します。テンプレートスペックをクリックします。左側のパネルで、[**Versions**] をクリックします。
8. [**Create new version**] をクリックして、新しいバージョンを作成できます。新しいバージョン番号を指定し、現在のテンプレートスペックを変更して、[**Review + Create**] をクリックし、新しいバージョンのテンプレートスペックを作成します。

次の PowerShell コマンドを使用して、テンプレートスペックとテンプレートのバージョンに関する情報を取得できます:

- テンプレートスペックに関する情報を取得するには、次を実行します:

  <!JEKYLL@5300@23>

- テンプレートスペックのバージョンに関する情報を取得するには、次を実行します:

  <!JEKYLL@5300@24>

カタログの作成または更新でテンプレートスペックを使用する

テンプレートスペックをマシンプロファイルの入力に使用して、MCS マシンカタログを作成または更新できます。これを行うには、Web Studio または PowerShell コマンドを使用できます。

- Web Studio については、「Web Studio で Azure Resource Manager イメージを使用してマシンカタログを作成する」を参照してください。
- PowerShell については、「PowerShell を使用したカタログの作成または更新でテンプレートスペックを使用する」を参照してください。

Azure サーバー側暗号化

Citrix Virtual Apps and Desktops は、Azure Key Vault を使用して Azure Managed Disks の顧客が管理する暗号化キーをサポートします。このサポートにより、独自の暗号キーを使用してマシンカタログの管理対象ディスクを暗号化して、組織およびコンプライアンスの要件を管理できます。詳しくは、「Azure Disk Storage のサーバー側暗号化」を参照してください。

管理対象ディスクにこの機能を使用する場合:

- ディスクが暗号化されているキーを変更するには、<!JEKYLL@5300@25> の現在のキーを変更します。<!JEKYLL@5300@26> に関連付けられているすべてのリソースは、新しいキーで暗号化されるように変更されます。
- キーを無効にするか削除すると、そのキーを使用するディスクのある VM はすべて自動的にシャットダウンします。シャットダウン後、キーを再度有効にするか、新しいキーを割り当てない限り、VM は使用できません。このキーを使用するカタログの電源をオンにすることはできません。また、VM をカタログに追加することもできません。

顧客が管理する暗号化キーを使用する場合の重要な考慮事項

この機能を使用するときは、次のことに注意してください:

- 顧客が管理するキーに関連するすべてのリソース（Azure Key Vault、ディスク暗号化セット、VM、ディスク、スナップショット）は、同じサブスクリプションとリージョンに配置される必要があります。
- 顧客が管理するキーで暗号化されたディスク、スナップショット、イメージは、別のリソースグループおよびサブスクリプションに移動できません。
- リージョンごとのディスク暗号化セットの制限については、Microsoft 社のサイトを参照してください。

> 注:
>
> Azure サーバー側暗号化の構成については、「クイックスタート: Azure Portal を使用してキーコンテナを作成する」を参照してください。

Azure の顧客が管理する暗号キー

マシンカタログを作成するときに、カタログでプロビジョニングされるマシンのデータを暗号化するかどうかを選択できます。顧客が管理する暗号化キーを使用したサーバー側暗号化により、管理対象ディスクレベルで暗号化を管理し、カタログ内のマシン上のデータを保護できます。ディスク暗号化セット（DES）は、顧客が管理するキーを表します。この機能を使用するには、最初に Azure で DES を作成する必要があります。DES の形式は次のとおりです:

- <!JEKYLL@5300@27>

一覧から DES を選択します。選択した DES は、リソースと同じサブスクリプションおよびリージョンに存在する必要があります。

「顧客管理暗号キーを使用したマシンカタログの作成」を参照してください。

ホストでの **Azure** ディスク暗号化

ホスト機能での暗号化を使用して、MCS マシンカタログを作成できます。現在、MCS はこの機能でマシンプロファイルワークフローのみをサポートします。VM またはテンプレートスペックをマシンプロファイルの入力として使用できます。

この暗号化方法は、Azure Storage でデータを暗号化しません。VM をホストするサーバーがデータを暗号化し、暗号化されたデータが Azure Storage サーバーを通過します。つまり、この暗号化方法はデータをエンドツーエンドで暗号化します。

制限:

ホストでの Azure ディスク暗号化は:

- すべての Azure マシンサイズでサポートされているわけではありません
- Azure Disk Encryption と互換性がありません

ホスト機能での暗号化を使用してマシンカタログを作成するには、次の手順を実行します:

1. ホスト機能での暗号化がサブスクリプションで有効になっているかどうかを確認します。確認する方法については、「https://learn.microsoft.com/en-us/rest/api/resources/features/get?tabs=HTTP/」を参照してください。有効になっていない場合は、サブスクリプションの機能を有効にする必要があります。サブスクリプションでこの機能を有効にする方法については、「https://learn.microsoft.com/en-us/azure/virtual-machines/disks-enable-host-based-encryption-portal?tabs=azure-powershell#prerequisites/」を参照してください。
2. 使用する Azure VM のサイズがホストでの暗号化をサポートしているかどうかを確認します。確認するには、PowerShell ウィンドウで次のいずれかを実行します:

   <!JEKYLL@5300@28>

   <!JEKYLL@5300@29>
3. Azure Portal でホストでの暗号化を有効にして、マシンプロファイルの入力として、VM またはテンプレートスペックを作成します。

   - VM を作成する場合は、ホストでの暗号化をサポートしている VM サイズを選択します。VM を作成すると、VM プロパティの ［**Encryption at host**］が有効になります。
   - テンプレートスペックを使用する場合は、<!JEKYLL@5300@30> パラメーターを <!JEKYLL@5300@31> 内で **true** にします。
4. VM またはテンプレートスペックを選択して、マシンプロファイルワークフローで MCS マシンカタログを作成します。

   - OS ディスクまたはデータディスク: 顧客管理キーとプラットフォーム管理キーによって暗号化されます
   - エフェメラル OS ディスク: プラットフォーム管理キーだけで暗号化されます
   - キャッシュディスク: 顧客管理キーとプラットフォーム管理キーによって暗号化されます

   Web Studio を使用するか、PowerShell コマンドを実行して、マシンカタログを作成できます。

マシンプロファイルからホストでの暗号化情報を取得する

<!JEKYLL@5300@32> パラメーターを指定して PowerShell コマンドを実行すると、マシンプロファイルからホストでの暗号化情報を取得できます。<!JEKYLL@5300@33> パラメーターが **True** の場合、ホストでの暗号化がマシンプロファイルに対して有効であることを示します。

例：マシンプロファイル入力が VM の場合、次のコマンドを実行します：

<!JEKYLL@5300@34>

例：マシンプロファイル入力がテンプレートスペックの場合、次のコマンドを実行します：

<!JEKYLL@5300@35>

管理対象ディスクの二重暗号化

二重暗号化を使用してマシンカタログを作成できます。この機能を使用して作成されたカタログでは、すべてのディスクがプラットフォームキーと顧客管理キーの両方によってサーバー側で暗号化されています。Azure Key Vault、暗号キー、およびディスク暗号化セット（DES）は、顧客が所有し、維持します。

二重暗号化とは、プラットフォーム側の暗号化（デフォルト）と顧客管理の暗号化（CMEK）です。したがって、暗号化アルゴリズム、実装、またはキーの侵害に関するリスクを懸念している、セキュリティに非常に敏感なお客様は、この二重暗号化を選択できます。永続的 OS ディスクとデータディスク、スナップショット、イメージはすべて二重暗号化により保存時に暗号化されます。

> 注：
>
> - Web Studio を使用するか、PowerShell コマンドを実行することで、二重暗号化を使用してマシンカタログを作成し、更新できます。PowerShell コマンドについては、「二重暗号化を使用したマシンカタログの作成」を参照してください。
> - 二重暗号化を使用してマシンカタログを作成または更新するには、非マシンプロファイルベースのワークフローまたはマシンプロファイルベースのワークフローを使用できます。
> - 非マシンプロファイルベースのワークフローを使用してマシンカタログを作成する場合は、保存されている <!JEKYLL@5300@36> を再利用できます。
> - マシンプロファイルを使用する場合は、VM またはテンプレートスペックをマシンプロファイルの入力に使用できます。

制限事項：

- 二重暗号化は、Ultra Disk または Premium SSD v2 ディスクではサポートされていません。
- 二重暗号化は、非管理ディスクではサポートされません。
- カタログに関連付けられている DiskEncryptionSet キーを無効にすると、カタログの VM が無効になります。
- 顧客が管理するキーに関連するすべてのリソース（Azure Key Vault、ディスク暗号化セット、VM、ディスク、スナップショット）は、同じサブスクリプションとリージョンに存在する必要があります。

- サブスクリプションごとに、リージョンあたり最大 50 のディスク暗号化セットのみを作成できます。

Azure リソースグループ

Azure プロビジョニングのリソースグループは、アプリケーションとデスクトップをユーザーに提供する VM をプロビジョニングする方法を提供します。MCS マシンカタログを作成するときに既存の空の Azure リソースグループを追加するか、新しいリソースグループを作成することができます。Azure リソースグループについて詳しくは、Microsoft 社のドキュメントを参照してください。

Azure リソースグループの使用

Azure リソースグループごとの仮想マシン、管理対象ディスク、スナップショット、およびイメージの数に制限はありません（Azure リソースグループごとに仮想マシンは 240、管理対象ディスクは 800 という数の制限はなくなりました）。

- フルスコープのサービスプリンシパルを使用してマシンカタログを作成する場合、MCS は 1 つの Azure リソースグループのみを作成し、カタログのこのグループを使用します。
- スコープの狭いサービスプリンシパルを使用してマシンカタログを作成する場合、事前に作成された空の Azure リソースグループを指定する必要があります。

Azure エフェメラルディスク

Azure エフェメラルディスクを使用すると、キャッシュディスクまたは一時ディスクを再利用して、Azure 対応の仮想マシンの OS ディスクを保存できます。この機能は、標準の HDD ディスクよりも高性能の SSD ディスクを必要とする Azure 環境で役立ちます。Azure エフェメラルディスクを使用したカタログの作成については、「Azure エフェメラルディスクを使用したカタログの作成」を参照してください。

> 注:
>
> 永続カタログでは、エフェメラル OS ディスクはサポートされていません。

エフェメラル OS ディスクでは、プロビジョニングスキームで管理対象ディスクと Shared Image Gallery を使用する必要があります。

エフェメラル OS 一時ディスクの保存

エフェメラル OS ディスクを VM 一時ディスクまたはリソースディスクに保存するオプションがあります。この機能により、キャッシュがないか、キャッシュが不十分な VM で、エフェメラル OS ディスクを使用できます。このような VM には、<!JEKYLL@5300@37> などのエフェメラル OS ディスクを保存するための一時ディスクまたはリソースディスクがあります。

以下に注意してください:

- エフェメラルディスクは、VM キャッシュディスクまたは VM の一時（リソース）ディスクのいずれかに保存されます。キャッシュディスクが OS ディスクの内容を保持するのに十分な大きさでない場合を除き、キャッシュディスクは一時ディスクよりも優先されます。
- 更新の際は、キャッシュディスクよりも大きいが一時ディスクよりも小さい新しいイメージにより、エフェメラル OS ディスクが VM の一時ディスクに置き換えられます。

Azure エフェメラルディスクと **Machine Creation Services**（**MCS**）ストレージ最適化（**MCS I/O**）

Azure エフェメラル OS ディスクと MCS I/O を同時に有効にすることはできません。

重要な考慮事項は次のとおりです：

- エフェメラル OS ディスクと MCS I/O の両方を同時に有効にしてマシンカタログを作成することはできません。
- <!JEKYLL@5300@38> または <!JEKYLL@5300@39> で **true** に設定された PowerShell パラメーター（<!JEKYLL@5300@40> および <!JEKYLL@5300@41>）を使用すると、対応するエラーメッセージが表示されて失敗します。
- 両方の機能を有効にして作成した既存のマシンカタログについては、次のことができます：
  - マシンカタログの更新。
  - VM の追加または削除。
  - マシンカタログの削除。

Azure Compute Gallery

Azure において、MCS でプロビジョニングされたマシンの公開イメージリポジトリとして Azure Shared Image Gallery（旧称：Azure Shared Image Gallery）を使用します。公開イメージをギャラリーに保存して、OS ディスクの作成とハイドレーションを高速化し、非永続仮想マシンの起動時間とアプリケーションの起動時間を改善できます。Shared Image Gallery には、次の 3 つの要素が含まれています：

- ギャラリー：イメージはここに保存されます。MCS は、マシンカタログごとに 1 つのギャラリーを作成します。
- ギャラリーイメージの定義：この定義には、公開イメージに関する情報（オペレーティングシステムの種類と状態、Azure リージョン）が含まれます。MCS は、カタログ用に作成されたイメージごとに 1 つのイメージ定義を作成します。
- ギャラリーイメージバージョン：Shared Image Gallery の各イメージには複数のバージョンを含めることができ、各バージョンには異なるリージョンに複数のレプリカを含めることができます。各レプリカは、公開イメージの完全なコピーです。

> 注:
>
> Shared Image Gallery の機能は、管理対象ディスクとのみ互換性があります。従来のマシンカタログでは使用できません。

詳しくは、「Azure Compute Gallery の概要」を参照してください。

PowerShell と Azure Compute Gallery イメージを使用したマシンカタログの作成または更新については、「Azure Compute Gallery イメージを使用してマシンカタログを作成または更新する」を参照してください。

Azure Confidential VM

Azure Confidential Computing VM によって、仮想デスクトップは確実にメモリ内で暗号化され、使用中に保護されます。

MCS を使用して、Azure Confidential VM を含むカタログを作成できます。このようなカタログを作成するには、マシンプロファイルワークフローを使用する必要があります。VM と ARM テンプレートスペックの両方をマシンプロファイル入力として使用できます。

Confidential VM に関する重要な考慮事項

サポートされる VM サイズと、Confidential VM を含むマシンカタログの作成に関する重要な考慮事項は次のとおりです:

- サポートされる VM サイズ: Confidential VM は次の VM サイズをサポートします:
  - DCasv5 シリーズ
  - DCadsv5 シリーズ
  - ECasv5 シリーズ
  - ECadsv5 シリーズ
- Confidential VM を含むマシンカタログを作成します。
  - Web Studio と PowerShell コマンドを使用することで、Azure Confidential VM を使用してマシンカタログを作成できます。
  - Azure Confidential VM でマシンカタログを作成するには、マシンプロファイルベースのワークフローを使用する必要があります。VM またはテンプレートスペックをマシンプロファイルの入力として使用できます。
  - マスターイメージとマシンプロファイル入力は両方とも同じ機密のセキュリティの種類で有効にする必要があります。セキュリティの種類は次のとおりです:
    - **VMGuestStateOnly**: VM ゲスト状態のみが暗号化された Confidential VM

    - **DiskWithVMGuestState**：OS ディスクと VM ゲスト状態の両方がプラットフォーム管理キーまたは顧客管理キーで暗号化された Confidential VM。通常の OS ディスクとエフェメラル OS ディスクの両方を暗号化できます。

- AdditionalData パラメーターを使用すると、管理対象ディスク、スナップショット、Azure Compute Gallery イメージ、VM、ARM テンプレートスペックなど、さまざまなリソースの種類の Confidential VM 情報を取得できます。例：

  <!JEKYLL@5300@42>

  追加のデータフィールドは次のとおりです：

  - DiskSecurityType
  - ConfidentialVMDiskEncryptionSetId
  - DiskSecurityProfiles

  マシンサイズの Confidential Computing プロパティを取得するには、次のコマンドを実行します：<!JEKYLL@5300@43>

  追加のデータフィールドは <!JEKYLL@5300@44> です。

- マスターイメージまたはマシンプロファイルを機密のセキュリティの種類から機密以外のセキュリティ種類に、または機密以外のセキュリティに酒類から機密のセキュリティの種類に変更することはできません。
- 構成が正しくない場合は、適切なエラーメッセージが表示されます。

マスターイメージとマシンプロファイルを準備する

Confidential VM のセットを作成する前に、次の手順に従ってそれらのマスターイメージとマシンプロファイルを準備します：

1. Azure ポータルで、次のような特定の設定で Confidential VM を作成します：

   - セキュリティの種類：Confidential VM
   - **OS** ディスクの機密暗号化：有効になっています。
   - キー管理：プラットフォーム管理キーを使用した機密ディスクの暗号化
     Confidential VM の作成について詳しくは、こちらの Microsoft の記事を参照してください。

2. 作成した VM 上でマスターイメージを準備します。作成した VM 上で必要なアプリケーションと VDA をインストールします。

   > 注：
   >
   > VHD を使用した Confidential VM の作成はサポートされていません。代わりに、Azure Compute Gallery、Managed Disks、またはスナップショットを使用します。

3. 次のいずれかの方法でマシンプロファイルを作成します：

   - 手順 1 で作成した既存の VM に必要なマシンプロパティがある場合は、それを使用します。
   - マシンプロファイルとして ARM テンプレートスペックを選択する場合は、必要に応じてテンプレートスペックを作成します。具体的には、*SecurityEncryptionType* や *diskEncryptionSet*（顧客管理キーの場合）など、Confidential VM の要件を満たすパラメーターを構成します。詳しくは、「Azure テンプレートスペックの作成」を参照してください。

     > 注：
     >
     > – マスターイメージとマシンプロファイルのセキュリティキーの種類が同じであることを確認します。
     > – 顧客管理キーを使用して OS ディスクの機密暗号化を必要とする Confidential VM を作成するには、マスターイメージとマシンプロファイルの両方のディスク暗号化セット ID が同一であることを確認します。

Web Studio または **PowerShell** コマンドを使用して **Confidential VM** を作成する

Confidential VM のセットを作成するには、マスターイメージと、目的の Confidential VM に基づくマシンプロファイルを使用してマシンカタログを作成します。

Web Studio を使用してカタログを作成するには、「マシンカタログの作成」で説明されている手順に従います。次の考慮事項に留意してください：

- ［イメージ］ページで、Confidential VM の作成用に準備したマスターイメージとマシンプロファイルを選択します。マシンプロファイルの選択は必須であり、選択したマスターイメージと同じセキュリティ暗号化の種類に一致するプロファイルのみが選択可能です。
- ［仮想マシン］ページでは、Confidential VM をサポートするマシンサイズのみが選択肢に表示されます。
- ［ディスク設定］ページでは、選択したマシンプロファイルから継承されるため、ディスク暗号化セットを指定することはできません。

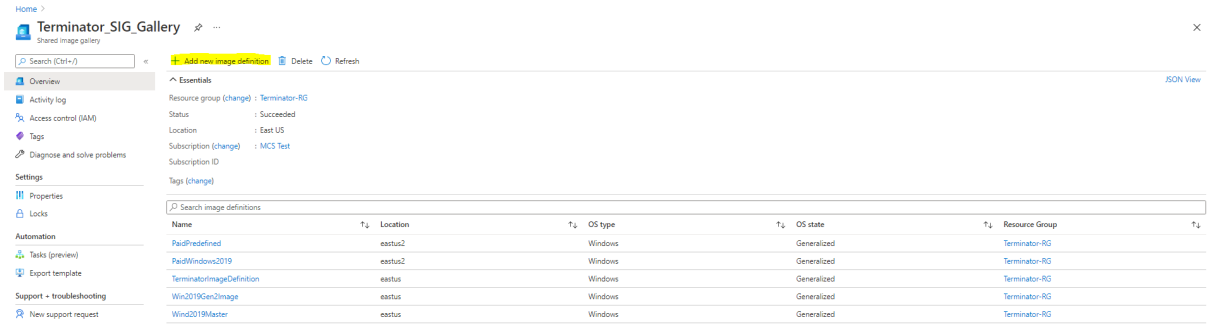
Azure Marketplace

Citrix Virtual Apps and Desktops では、プラン情報を含んだ Azure 内マスターイメージを使用してマシンカタログを作成できます。詳しくは、Microsoft Azure Marketplaceを参照してください。

> ヒント：
>
> 標準の Windows Server イメージなど、Azure Marketplace にある一部のイメージには、プラン情報が追加されていません。Citrix Virtual Apps and Desktops 機能は、有料イメージ用です。

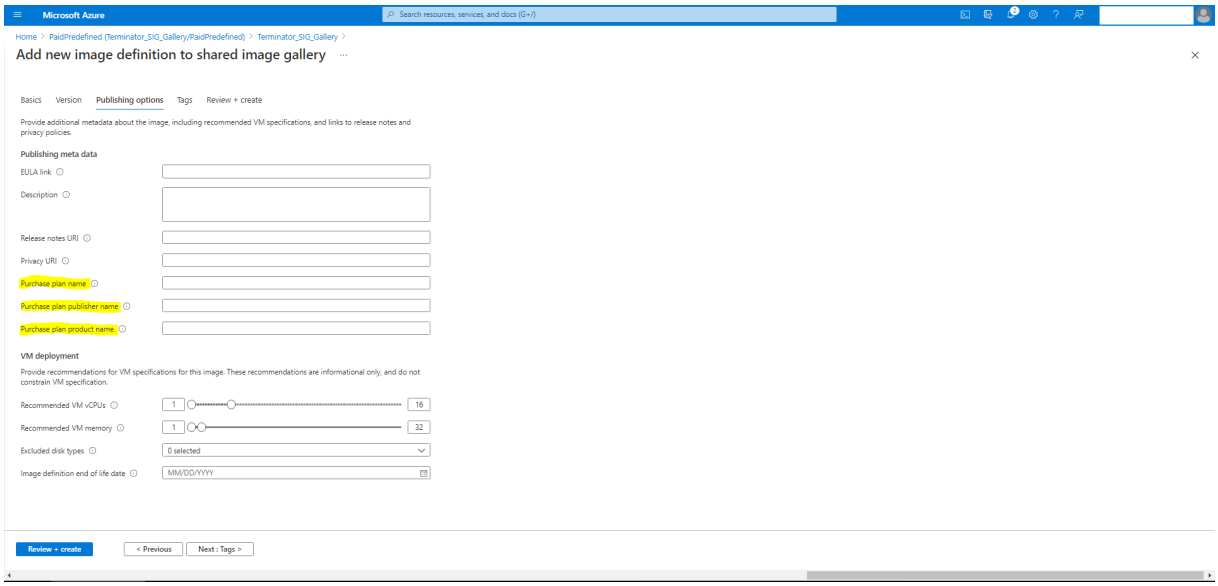
Shared Image Gallery で作成されたイメージに **Azure** プラン情報が含まれていることの確認

このセクションの手順を使用して、Web Studio で Shared Image Gallery のイメージを表示します。これらのイメージは、マスターイメージに使用することもできます。イメージを Shared Image Gallery に配置するには、ギャラリーでイメージ定義を作成します。

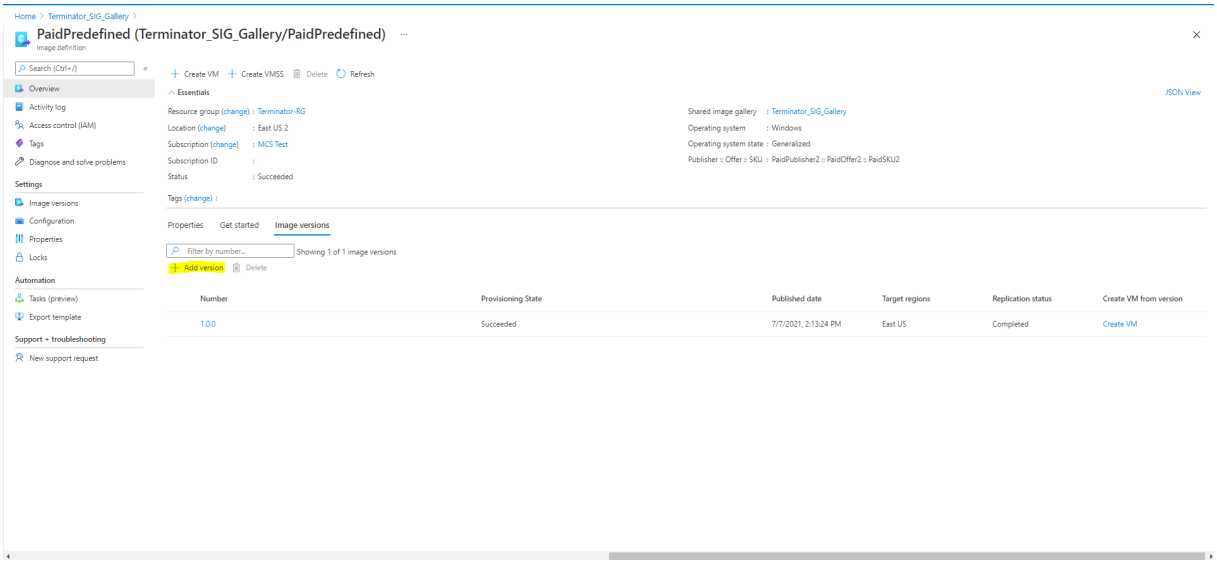


［公開オプション］ページで、購入プラン情報を確認します。

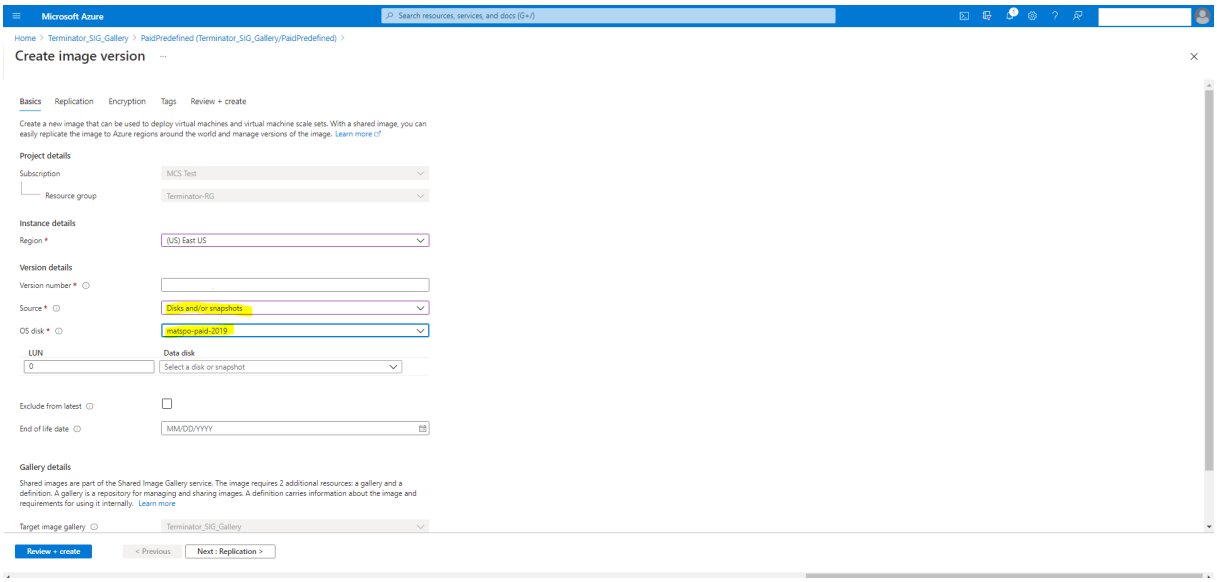
購入プラン情報フィールドは最初は空欄です。これらのフィールドに、イメージに使用されている購入プラン情報を入力します。購入プラン情報を入力しないと、マシンカタログプロセスが失敗する可能性があります。



購入プラン情報を確認した後、定義内にイメージバージョンを作成します。これはマスターイメージとして使用されます。［バージョンの追加］をクリックします:



［バージョンの詳細］セクションで、ソースとしてイメージスナップショットか管理対象ディスクを選択します：



入れ子構造の仮想化

入れ子構造の仮想化を有効にしてマスター VM を構成すると、そのマスター VM を使用して作成された MCS マシンカタログ内のすべての VM で入れ子構造の仮想化が有効になります。この機能は、永続 VM と非永続 VM の両方に適用できます。イメージの更新を通じて、既存の MCS マシンカタログと既存の VM を更新し、入れ子構造の仮想化を実現できます。

現在、入れ子構造の仮想化をサポートしているのは Dv3 および Ev3 VM サイズのみです。

入れ子構造の仮想化について詳しくは、Microsoft のブログ「Nested Virtualization in Azure」を参照してください。

PowerShell を使用してマシンカタログを作成する

このセクションでは、PowerShell を使用してカタログを作成する方法について説明します。

- 非永続的なライトバックキャッシュディスクのカタログを作成する
- 永続的なライトバックキャッシュディスクのカタログを作成する
- MCSIO による起動パフォーマンスの向上
- PowerShell を使用したカタログの作成または更新でテンプレートスペックを使用する
- トラステッド起動を使用したマシンカタログ
- マシンプロファイルのプロパティ値を使用する
- 顧客管理暗号キーを使用したマシンカタログの作成
- 二重暗号化を使用したマシンカタログの作成
- Azure エフェメラルディスクを使用したカタログの作成
- Azure 専用ホスト
- Azure Compute Gallery イメージを使用してマシンカタログを作成または更新する
- Shared Image Gallery を構成する
- 指定されたアベイラビリティゾーンへのマシンのプロビジョニング
- ストレージの種類
- ページファイル設定の更新
- Azure Spot VM を使用したカタログの作成
- バックアップ VM サイズの構成
- すべてのリソースのタグをコピーする
- [Azure Monitor エージェントがインストールされたカタログ VM をプロビジョニングする]

非永続的なライトバックキャッシュディスクのカタログを作成する

非永続的なライトバックキャッシュディスクのカタログを構成するには、PowerShell パラメーター <!JEKYLL@5300@45> を使用します。このカスタムプロパティ <!JEKYLL@5300@46> は、ライトバックキャッシュファイルを保存するのに、Azure 一時ストレージの使用を受け入れるかどうかを示します。一時ディスクをライトバックキャッシュディスクとして使用する場合は、<!JEKYLL@5300@47> 実行時に「true」に設定する必要があります。このパラメーターが指定されていない場合、デフォルトは **False** に設定されます。

例：<!JEKYLL@5300@48> パラメーターを使用して <!JEKYLL@5300@49> を **true** に設定した場合：

<!JEKYLL@5300@50>

> 注：
>
> マシンカタログをコミットして、ライトバックキャッシュファイル用として Azure ローカル一時ストレージを使用すると、後から VHD を使用するように変更することはできません。

永続的なライトバックキャッシュディスクのカタログを作成する

永続的なライトバックキャッシュディスクのカタログを構成するには、PowerShell パラメーター <!JEKYLL@5300@51> を使用します。このパラメーターでは追加プロパティ <!JEKYLL@5300@52> をサポートしており、これを使用することで、MCS でプロビジョニングされたマシンのライトバックキャッシュディスクを永続化させる方法を指定できます。<!JEKYLL@5300@53> プロパティは、<!JEKYLL@5300@54> パラメーターが指定され、<!JEKYLL@5300@55> パラメーターがディスクが作成されたことを示すよう設定された場合のみ使用されます。

以下は、<!JEKYLL@5300@56> をサポートする前に <!JEKYLL@5300@57> パラメーターで使用されるプロパティの例です:

<!JEKYLL@5300@58>

これらのプロパティを使用するときは、プロパティが <!JEKYLL@5300@59> パラメーターから省略されている場合にデフォルトの値が含まれるようにしてください。<!JEKYLL@5300@60> プロパティには、次の 2 つの値が設定可能です: **true** または **false**。

<!JEKYLL@5300@61> プロパティを **true** に設定すると、Citrix Virtual Apps and Desktops 管理者が Web Studio を使用してマシンをシャットダウンしたときにライトバックキャッシュディスクが消去されません。

<!JEKYLL@5300@62> プロパティを **false** に設定すると、Citrix Virtual Apps and Desktops 管理者が Web Studio を使用してマシンをシャットダウンしたときにライトバックキャッシュディスクが消去されます。

> 注:
>
> <!JEKYLL@5300@63> プロパティを省略する場合、デフォルトは **false** になり、Web Studio を使用してマシンをシャットダウンするとライトバックキャッシュは消去されます。

例: <!JEKYLL@5300@64> パラメーターを使用して <!JEKYLL@5300@65> を true に設定した場合:

<!JEKYLL@5300@66>

> 重要:
>
> <!JEKYLL@5300@67> プロパティは、<!JEKYLL@5300@68> PowerShell コマンドレットを使用してのみ設定できます。作成後にプロビジョニングスキームの <!JEKYLL@5300@69> を変更しようとしても、マシンがシャットダウンしたときにマシンカタログやライトバックキャッシュディスクの永続性は影響を受けません。

例: <!JEKYLL@5300@70> プロパティを true に設定するときに <!JEKYLL@5300@71> を設定してライトバックキャッシュを使用した場合:

<!JEKYLL@5300@72>

MCSIO による起動パフォーマンスの向上

MCSIO が有効な場合、Azure や GCP の管理対象ディスクの起動パフォーマンスを向上させることができます。<!JEKYLL@5300@73> コマンドで PowerShell カスタムプロパティ <!JEKYLL@5300@74> を使用してこの機能を構成します。<!JEKYLL@5300@75> に関連するオプションは次のとおりです:

<!JEKYLL@5300@76><!JEKYLL@5300@77><!JEKYLL@5300@78>

この機能を有効にするには、カスタムプロパティ［<!JEKYLL@5300@79>］を「<!JEKYLL@5300@80>」に設定します。例:

<!JEKYLL@5300@81>

PowerShell を使用したカタログの作成または更新でテンプレートスペックを使用する

テンプレートスペックをマシンプロファイルの入力に使用して、MCS マシンカタログを作成または更新できます。これを行うには、Web Studio または PowerShell コマンドを使用できます。

Web Studio については、「Web Studio で Azure Resource Manager イメージを使用してマシンカタログを作成する」を参照してください。

PowerShell コマンドを使用する:

1. **PowerShell** ウィンドウを開きます。
2. <!JEKYLL@5300@82> を実行します。
3. カタログを作成または更新します。

    - カタログを作成するには:
        a) マシンプロファイルの入力で、テンプレートスペックを <!JEKYLL@5300@83> コマンドとともに使用します。例:
        <!JEKYLL@5300@84>
        b) カタログの作成を完了します。
    - カタログを更新するには、マシンプロファイルの入力で、テンプレートスペックを <!JEKYLL@5300@85> コマンドとともに使用します。例:
    <!JEKYLL@5300@86>

トラステッド起動を使用したマシンカタログ

トラステッド起動でマシンカタログを正常に作成するには、次を使用します:

- トラステッド起動を使用したマシンプロファイル
- トラステッド起動をサポートする VM サイズ
- トラステッド起動をサポートする Windows VM バージョン。現在、Windows 10、Windows 11、Windows Server 2016、2019、および 2022 はトラステッド起動をサポートしています。

> 重要:
>
> MCS は、トラステッド起動が有効な VM を使用した新しいカタログの作成をサポートしています。ただし、既存の永続カタログと既存の VM を更新するには、Azure Portal を使用する必要があります。非永続カタログのトラステッド起動を更新することはできません。詳しくは、Microsoft ドキュメント「既存の Azure VM でトラステッド起動を有効にする」を参照してください。

Citrix Virtual Apps and Desktops オファリングのインベントリアイテムを表示し、VM サイズがトラステッド起動をサポートしているかどうかを判断するには、次のコマンドを実行します:

1. PowerShell ウィンドウを開きます。
2. **asnp citrix*** を実行し、Citrix 固有の PowerShell モジュールをロードします。
3. 次のコマンドを実行します:

   <!JEKYLL@5300@87>
4. <!JEKYLL@5300@88> を実行します
5. <!JEKYLL@5300@89> 属性の値を確認してください。
   - <!JEKYLL@5300@90> が **True** の場合、VM サイズはトラステッド起動をサポートします。
   - <!JEKYLL@5300@91> が **False** の場合、VM サイズはトラステッド起動をサポートしません。

Azure の PowerShell に従って、次のコマンドを使用してトラステッド起動をサポートする VM サイズを決定できます:

<!JEKYLL@5300@92>

Azure PowerShell コマンドを実行した後、VM サイズがトラステッド起動をサポートするかどうかを説明する例を次に示します。

- 例 *1*: Azure VM が第 1 世代のみをサポートしている場合、その VM はトラステッド起動をサポートしていません。したがって、Azure PowerShell コマンドを実行した後、<!JEKYLL@5300@93> 機能は表示されません。
- 例 *2*: Azure VM が第 2 世代のみをサポートし、<!JEKYLL@5300@94> 機能が **True** の場合、第 2 世代の VM サイズはトラステッド起動ではサポートされません。
- 例 *3*: Azure VM が第 2 世代のみをサポートし、PowerShell コマンドの実行後に <!JEKYLL@5300@95> 機能が表示されない場合、第 2 世代の VM サイズはトラステッド起動でサポートされます。

Azure 仮想マシンのトラステッド起動ついて詳しくは、Microsoft のドキュメント「Azure Virtual Machines のトラステッド起動」を参照してください。

トラステッド起動を使用したマシンカタログの作成

1. トラステッド起動が有効になっているマスターイメージを作成します。Microsoft のドキュメント「トラステッド起動 VM イメージ」を参照してください。

2. セキュリティの種類をトラステッド起動 **VM** として VM またはテンプレートスペックを作成します。VM またはテンプレートスペックの作成について詳しくは、Microsoft ドキュメント「トラステッド起動の VM をデプロイする」を参照してください。
3. Web Studio または PowerShell コマンドを使用してマシンカタログを作成します。
   - Web Studio を使用する場合は、「Web Studio で Azure Resource Manager イメージを使用してマシンカタログを作成する」を参照してください。
   - PowerShell コマンドを使用する場合は、<!JEKYLL@5300@96> コマンドを使用し、マシンプロファイルの入力に VM またはテンプレートスペックを指定します。カタログ作成コマンドの完全な一覧については、「Creating a catalog」を参照してください。

     マシンプロファイルの入力に VM を使用した <!JEKYLL@5300@97> の例:

     <!JEKYLL@5300@98>

     マシンプロファイルの入力にテンプレートスペックを使用した <!JEKYLL@5300@99> の場合:

     <!JEKYLL@5300@100>

トラステッド起動でマシンカタログを作成する際のエラー

トラステッド起動を使用してマシンカタログを作成しているときに、次のシナリオに応じたエラーが発生します:

シナリオ	エラー
非管理対象カタログの作成中にマシンプロファイルを選択した場合	<!JEKYLL@5300@101>
非管理対象ディスクをマスターイメージとしてカタログを作成するときに、トラステッド起動をサポートするマシンプロファイルを選択した場合	<!JEKYLL@5300@102>
セキュリティの種類でトラステッド起動を使用し、マスターイメージソースを使用して管理カタログを作成するときに、マシンプロファイルを選択しない場合	<!JEKYLL@5300@103>
マスターイメージとは異なるセキュリティの種類のマシンプロファイルを選択した場合	<!JEKYLL@5300@104>
トラステッド起動をサポートしない VM サイズを選択しながら、カタログの作成時にトラステッド起動をサポートするマスターイメージを使用する場合	<!JEKYLL@5300@105>

マシンプロファイルのプロパティ値を使用する

マシンカタログは、カスタムプロパティで定義されている次のプロパティを使用します:

- アベイラビリティゾーン
- 専用ホストグループ ID
- ディスク暗号化セット ID
- OS の種類
- ライセンスの種類
- ストレージの種類

これらのカスタムプロパティが明示的に定義されていない場合、プロパティ値はマシンプロファイルとして使用されている ARM テンプレートスペックの指定または仮想マシンのいずれかから設定されます。また、<!JEKYLL@5300@106> が指定されていない場合は、マシンプロファイルから設定されます。

> 注:
>
> 一部のプロパティがマシンプロファイルで指定されておらず、カスタムプロパティで定義されていないとき、プロパティのデフォルト値が常に適用されます（該当する場合）。

次のセクションでは、<!JEKYLL@5300@107> ですべてのプロパティが定義されている場合、または値が MachineProfile から由来している場合、<!JEKYLL@5300@108> および <!JEKYLL@5300@109> でのシナリオについて説明します。

- New-ProvScheme シナリオ
  - MachineProfile ですべてのプロパティが定義され、CustomProperties は定義されていません。例:

    <!JEKYLL@5300@110>

    カタログのカスタムプロパティとして、次の値が設定されています:

    <!JEKYLL@5300@111>
  - MachineProfile で一部のプロパティが定義され、CustomProperties は定義されていません。例: MachineProfile には LicenseType と OsType のみが含まれます。

    <!JEKYLL@5300@112>

    カタログのカスタムプロパティとして、次の値が設定されています:

    <!JEKYLL@5300@113>
  - MachineProfile と CustomProperties の両方がすべてのプロパティを定義します。例:

    <!JEKYLL@5300@114>

    カスタムプロパティが優先されます。カタログのカスタムプロパティとして、次の値が設定されています:

    <!JEKYLL@5300@115>
  - 一部のプロパティは MachineProfile で定義され、一部のプロパティは CustomProperties で定義されます。例:

    * CustomProperties は、LicenseType と StorageAccountType を定義します
    * MachineProfile は、LicenseType、OsType、Zones を定義します

  <!JEKYLL@5300@116>

  カタログのカスタムプロパティとして、次の値が設定されています:

  <!JEKYLL@5300@117>

- 一部のプロパティは MachineProfile で定義され、一部のプロパティは CustomProperties で定義されます。また、ServiceOffering は定義されていません。例:

    * CustomProperties は StorageType を定義します
    * MachineProfile は LicenseType を定義します

  <!JEKYLL@5300@118>

  カタログのカスタムプロパティとして、次の値が設定されています:

  <!JEKYLL@5300@119>

- OsType が CustomProperties にも MachineProfile にもない場合、次のようになります:

    * 値はマスターイメージから読み取られます。
    * マスターイメージが非管理対象ディスクの場合、OsType は Windows に設定されます。例:

  <!JEKYLL@5300@120>

  マスターイメージの値は、カスタムプロパティに書き込まれます（この場合は Linux）。

  <!JEKYLL@5300@121>

- Set-ProvScheme シナリオ

  - 既存のカタログ:

    * <!JEKYLL@5300@122> および OsType の CustomProperties
    * Zones を定義する MachineProfile <!JEKYLL@5300@123>

  - 更新:

    * StorageAccountType を定義する MachineProfile mpB.vm
    * LicenseType と OsType を定義するカスタムプロパティの新しいセット $CustomPropertiesB

  <!JEKYLL@5300@124>

  カタログのカスタムプロパティとして、次の値が設定されています:

  <!JEKYLL@5300@125>

  - 既存のカタログ:

    * S<!JEKYLL@5300@126> および OsType の CustomProperties

    - StorageAccountType と LicenseType を定義する MachineProfile <!JEKYLL@5300@127>

  - 更新:

    - StorageAccountType と OsType を定義するカスタムプロパティの新しいセット $CustomPropertiesB

  <!JEKYLL@5300@128>

  カタログのカスタムプロパティとして、次の値が設定されています:

  <!JEKYLL@5300@129>

  - 既存のカタログ:

    - <!JEKYLL@5300@130> および OsType の CustomProperties
    - Zones を定義する MachineProfile <!JEKYLL@5300@131>

  - 更新:

    - StorageAccountType と LicenseType を定義する MachineProfile mpB.vm
    - <!JEKYLL@5300@132> は指定されていません

  <!JEKYLL@5300@133>

  カタログのカスタムプロパティとして、次の値が設定されています:

  <!JEKYLL@5300@134>

[**Azure Monitor** エージェントがインストールされたカタログ **VM** をプロビジョニングする]

Azure の監視は、Azure 環境および社内のオンプレミス環境からテレメトリデータを収集、分析し、それに基づいて操作するために使用できるサービスです。

Azure Monitor エージェント（AMA）は、仮想マシンなどのコンピューティングリソースから監視データを収集し、そのデータを Azure Monitor に配信します。現在、イベントログ、Syslog、パフォーマンスメトリックの収集がサポートされており、収集した結果を Azure Monitor メトリックと Azure Monitor の Log Analytics エージェントのデータソースとして送信します。

監視データ内の VM を一意に識別して監視を有効にするには、AMA を拡張機能としてインストールして MCS マシンカタログの VM をプロビジョニングします。

要件

- 権限:「必要な Azure 権限」で規定されている最小限の Azure の権限と、Azure Monitor を使用するための次の権限を持っていることを確認します:

  - <!JEKYLL@5300@135>

  - <!JEKYLL@5300@136>
  - <!JEKYLL@5300@137>
  - <!JEKYLL@5300@138>
  - <!JEKYLL@5300@139>

- データ収集規則（DCR）: Azure Portal でデータ収集規則を設定します。DCR の設定について詳しくは、「データ収集規則の作成」を参照してください。DCR はプラットフォーム（Windows または Linux）に固有です。必要なプラットフォームに応じた DCR を必ず作成してください。
  AMA はデータ収集規則（DCR）を使用して、VM などのリソースと、Azure Monitor メトリックや Azure Monitor の Log Analytics エージェントなどのデータ ソースとのマッピングを管理します。
- デフォルトのワークスペース: Azure Portal でワークスペースを作成します。ワークスペースの作成については、「Log Analytics ワークスペースの作成」を参照してください。収集したログとデータの情報は、ワークスペースに保存されます。ワークスペースは、一意のワークスペース ID とリソース ID を持っています。ワークスペース名は、特定のリソースグループに対して固有のものにする必要があります。ワークスペースを作成した後、データがワークスペースに保存されるようにデータソースとソリューションを構成します。
- モニター拡張機能を許可リストに登録しました: 拡張機能 <!JEKYLL@5300@140> および <!JEKYLL@5300@141> が、Citrix が定義している許可リストに登録されました。許可リストに登録されている拡張機能の一覧を表示するには、PoSH コマンド <!JEKYLL@5300@142> を使用します。
- マスターイメージ: Microsoft では、既存のマシンから新しいマシンを作成する前に、既存のマシンから拡張機能を削除することを推奨しています。拡張子を削除しないと、ファイルが残ったり、予期しない動作が行われたりする可能性があるからです。詳しくは、「既存の VM を再作成する場合」を参照してください。

AMA を有効にしてカタログ VM をプロビジョニングするには:

1. マシンプロファイルテンプレートを設定します。
   - VM をマシンプロファイルテンプレートとして使用する場合は、次の手順を実行します:
     a) Azure Portal で VM を作成します。
     b) VM の電源を入れます。
     c) [リソース] で、VM をデータ収集規則に追加します。これにより、テンプレート VM へのエージェントのインストールが起動されます。

     > 注:
     >
     > Linux カタログを作成する場合は、Linux マシンをセットアップします。

   - テンプレートスペックをマシンプロファイルテンプレートとして使用する場合は、次の手順を実行します:
     a) テンプレートスペックを設定します。
     b) 生成されたテンプレートスペックに次の拡張機能とデータ収集規則の関連付けを追加します:
        <!JEKYLL@5300@143>

2. MCS マシンカタログを作成または更新します。

    - 新しい MCS カタログを作成するには:

        a) Web Studio で、前述の VM またはテンプレートスペックをマシンプロファイルとして選択します。
        b) 次の手順に進んでカタログを作成します。

    - 既存の MCS カタログを更新する場合は、次の PoSH コマンドを使用します:

        – 更新したマシンプロファイルテンプレートを新しい VM に取り込むには、次のコマンドを実行します:

          <!JEKYLL@5300@144>

        – 更新したマシンプロファイルテンプレートを使用して既存の VM を更新するには:

          <!JEKYLL@5300@145>

3. カタログ VM の電源を入れます。
4. Azure Portal に移動し、モニター拡張機能が VM にインストールされているかどうか、および VM が DCR の［リソース］の下に表示されているかどうかを確認します。数分後、監視データが Azure Monitor に表示されます。

トラブルシューティング

Azure Monitor エージェントのトラブルシューティングガイダンスについて詳しくは、以下を参照してください:

- https://learn.microsoft.com/en-us/azure/azure-monitor/agents/azure-monitor-agent-troubleshoot-windows-vm/
- https://learn.microsoft.com/en-us/azure/azure-resource-manager/troubleshooting/create-troubleshooting-template/

顧客管理暗号キーを使用したマシンカタログの作成

顧客管理暗号キーを使用してマシンカタログを作成する方法の詳細な手順は次のとおりです。

1. PowerShell ウィンドウを開きます。
2. <!JEKYLL@5300@146> を実行し、Citrix 固有の PowerShell モジュールをロードします。
3.「<!JEKYLL@5300@147>」を入力します。
4.「<!JEKYLL@5300@148>」を入力します。
5.「<!JEKYLL@5300@149>」を入力します。
6.「<!JEKYLL@5300@150>」と入力して、ディスク暗号化セットの一覧を取得します。

7. ディスク暗号化セットの ID をコピーします。
8. ディスク暗号化セットの ID を含むカスタムプロパティ文字列を作成します。例:

   <!JEKYLL@5300@151>

9. ID プールをまだ作成していない場合は作成します。例:

   <!JEKYLL@5300@152>

10. New-ProvScheme コマンドを実行します。例:

    <!JEKYLL@5300@153>

11. マシンカタログの作成を完了します。

二重暗号化を使用したマシンカタログの作成

Web Studio を使用するか、PowerShell コマンドを実行することで、二重暗号化を使用してマシンカタログを作成し、更新できます。

二重暗号化を使用してマシンカタログを作成する方法の詳細な手順は次のとおりです。

1. プラットフォーム管理キーと顧客が管理するキーを使用して Azure Key Vault と DES を作成します。Azure Key Vault と DES を作成する方法については、「Azure portal を使用して、マネージドディスクの保存時の二重暗号化を有効にします」を参照してください。
2. ホスト接続で利用可能な DiskEncryptionSets を参照するには、次の手順を実行します:

   a) **PowerShell** ウィンドウを開きます。
   b) 次の PowerShell コマンドを実行します:

      i. <!JEKYLL@5300@154>
      ii. <!JEKYLL@5300@155>
      iii. <!JEKYLL@5300@156>
      iv. <!JEKYLL@5300@157>（例：azure-east）
      v. <!JEKYLL@5300@158>
      vi. <!JEKYLL@5300@159>

   <!JEKYLL@5300@160> の ID を使用したカスタムプロパティで、カタログを作成または更新できます。

3. マシンプロファイルワークフローを使用する場合は、マシンプロファイルの入力用に VM またはテンプレートスペックを作成します。

   - VM をマシンプロファイルの入力に使用する場合は、次の手順を実行します:

     a) Azure Portal で VM を作成します。
     b) **Disks > Key management** に移動して、VM を <!JEKYLL@5300@161> で直接暗号化します。

- テンプレートスペックをマシンプロファイルの入力に使用する場合は、次の手順を実行します:
  a) テンプレートの <!JEKYLL@5300@162> の下に <!JEKYLL@5300@163> パラメーターを追加し、二重暗号化の DES の ID を追加します。

4. マシンカタログを作成します。

   - Web Studio を使用している場合は、「マシンカタログの作成」の手順に加えて、次のいずれかを実行します。

     - マシンプロファイルベースのワークフローを使用しない場合は、［ディスク設定］ページで、［次のキーを使用して各マシンのデータを暗号化］を選択します。次に、ドロップダウンから二重暗号化の DES を選択します。カタログの作成を続けます。
     - マシンプロファイルワークフローを使用している場合は、［イメージ］ページでマスターイメージとマシンプロファイルを選択します。マシンプロファイルのプロパティにディスク暗号化セット ID があることを確認してください。

     カタログ内に作成されたすべてのマシンは、選択した DES に関連付けられたキーによって二重暗号化されます。

   - PowerShell コマンドを使用する場合は、次のいずれかを実行します:

     - マシンプロファイルベースのワークフローを使用しない場合は、<!JEKYLL@5300@164> コマンドにカスタムプロパティ <!JEKYLL@5300@165> を追加します。例:

       <!JEKYLL@5300@166>

     - マシンプロファイルベースのワークフローを使用する場合は、<!JEKYLL@5300@167> コマンドで入力したマシンプロファイルを使用します。例:

       <!JEKYLL@5300@168>

5. Remote PowerShell SDK を使用してカタログの作成を完了します。Remote PowerShell SDK を使用してカタログを作成する方法については、https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/を参照してください。カタログ内に作成されたすべてのマシンは、選択した DES に関連付けられたキーによって二重暗号化されます。

暗号化されていないカタログを二重暗号化を使用するように変換

マシンカタログの暗号化の種類を（カスタムプロパティまたはマシンプロファイルを使用して）更新できます。

- マシンプロファイルベースのワークフローを使用しない場合は、<!JEKYLL@5300@169> コマンドにカスタムプロパティ DiskEncryptionSetId を追加します。例:

  <!JEKYLL@5300@170>

- マシンプロファイルベースのワークフローを使用する場合は、<!JEKYLL@5300@171> コマンドで入力したマシンプロファイルを使用します。例:

<!JEKYLL@5300@172>

成功すると、カタログ内に追加されたすべてのマシンは、選択した DES に関連付けられたキーによって二重暗号化されます。

カタログが二重暗号化されていることの確認

- Web Studio の場合:
  1. ［マシンカタログ］に移動します。
  2. 確認するカタログを選択します。画面の下部近くにある ［テンプレートのプロパティ］タブをクリックします。
  3. ［**Azure** の詳細］の ［ディスク暗号化セット］でディスク暗号化セット ID を確認します。カタログの DES ID が空白の場合、カタログは暗号化されていません。
  4. Azure Portal で、DES ID に関連付けられた DES の暗号化の種類が、プラットフォーム管理キーと顧客が管理するキーであることを確認します。
- PowerShell コマンドを使用する場合:
  1. **PowerShell** ウィンドウを開きます。
  2. <!JEKYLL@5300@173> を実行し、Citrix 固有の PowerShell モジュールをロードします。
  3. <!JEKYLL@5300@174> を使用して、マシンカタログの情報を取得します。例:

     <!JEKYLL@5300@175>
  4. マシンカタログの DES ID カスタムプロパティを取得します。例:

     <!JEKYLL@5300@176>
  5. Azure Portal で、DES ID に関連付けられた DES の暗号化の種類が、プラットフォーム管理キーと顧客が管理するキーであることを確認します。

Azure エフェメラルディスクを使用したカタログの作成

エフェメラルディスクを使用するには、<!JEKYLL@5300@177> を実行するとき、カスタムプロパティ <!JEKYLL@5300@178> を **true** に設定する必要があります。

> 注:
>
> カスタムプロパティ <!JEKYLL@5300@179> が **false** に設定されているか、値が指定されていない場合、プロビジョニングされたすべての VDA は引き続きプロビジョニングされた OS ディスクを使用します。

以下は、プロビジョニングスキームで使用するカスタムプロパティのセットの例です:

<!JEKYLL@5300@180>

カタログのエフェメラルディスクを構成する

カタログの Azure エフェメラル OS ディスクを構成するには、<!JEKYLL@5300@181> の <!JEKYLL@5300@182> パラメーターを使用します。<!JEKYLL@5300@183> パラメーターの値を「**true**」に設定します。

> 注:
>
> この機能を使用するには、パラメーターの <!JEKYLL@5300@184> と <!JEKYLL@5300@185> も有効にする必要があります。

例:

<!JEKYLL@5300@186>

エフェメラルディスクに関する重要な考慮事項

<!JEKYLL@5300@187> を使用してエフェメラル OS ディスクのプロビジョニングをするには、次の制約を考慮してください:

- カタログに使用される VM サイズは、エフェメラル OS ディスクをサポートする必要があります。
- VM サイズに関連付けられているキャッシュまたは一時ディスクのサイズは、OS ディスクのサイズ以上である必要があります。
- 一時ディスクのサイズは、キャッシュディスクのサイズよりも大きい必要があります。

次の場合にも、これらの問題を考慮してください:

- プロビジョニングスキームを作成する場合。
- プロビジョニングスキームを変更する場合。
- イメージを更新する場合。

Azure 専用ホスト

MCS を使用して、Azure 専用ホストで VM をプロビジョニングできます。Azure 専用ホストで VM をプロビジョニングする前に、以下を実行します:

- ホストグループを作成します。
- そのホストグループにホストを作成します。
- カタログと仮想マシンを作成するために十分なホスト容量が確保されていることを確認してください。

管理者は、次の PowerShell スクリプトで定義されたホストテナントを持つマシンのカタログを作成できます:

<!JEKYLL@5300@188>

MCS を使用して、Azure 専用ホストで仮想マシンをプロビジョニングする場合、次の点を考慮してください:

- 専用ホストはカタログプロパティであり、カタログの作成後に変更することはできません。専用テナントは現在、Azure ではサポートされていません。
- <!JEKYLL@5300@189> パラメーターを使用する場合は、ホスティングユニットの領域に事前構成された Azure ホストグループが必要です。
- Azure の自動配置が必要です。この機能は、ホストグループに関連付けられたサブスクリプションをオンボードするように要求します。詳しくは、「Azure 専用ホストの VM スケールセット - パブリックプレビュー」を参照してください。自動配置が有効になっていない場合、MCS はカタログの作成中にエラーをスローします。

Azure Compute Gallery イメージを使用してマシンカタログを作成または更新する

マシンカタログの作成に使用するイメージを選択するときに、Azure Compute Gallery で作成したイメージを選択できます。

これらのイメージを表示するには、次のことを行う必要があります:

1. Citrix Virtual Apps and Desktops サイトを構成します。
2. Azure Resource Manager に接続します。
3. Azure ポータルで、リソースグループを作成します。詳しくは、「ポータルを使用して Azure Compute Gallery を作成する」を参照してください。
4. リソースグループで、Azure Compute Gallery を作成します。
5. Azure Compute Gallery で、イメージ定義を作成します。
6. イメージ定義で、イメージバージョンを作成します。

次の PowerShell コマンドを使用して、Azure Compute Gallery からのイメージでマシンカタログを作成または更新します:

1. PowerShell ウィンドウを開きます。
2. <!JEKYLL@5300@190> を実行し、Citrix 固有の PowerShell モジュールをロードします。
3. リソースグループを選択し、そのリソースグループのすべてのギャラリーを表示します。

   <!JEKYLL@5300@191>

4. ギャラリーを選択し、そのギャラリーのすべてのイメージ定義を表示します。

   <!JEKYLL@5300@192>

5. 1 つのイメージ定義を選択し、そのイメージ定義のすべてのイメージバージョンを表示します。

   <!JEKYLL@5300@193>

6. 次の要素を使用して、MCS カタログを作成および更新します:

   - リソースグループ
   - ギャラリー
   - ギャラリーイメージの定義

- ギャラリーイメージのバージョン

Remote PowerShell SDK を使用してカタログを作成する方法については、https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/を参照してください。

Shared Image Gallery を構成する

<!JEKYLL@5300@194> コマンドを使用することで、Shared Image Gallery をサポートする新しいプロビジョニングスキームを作成できます。<!JEKYLL@5300@195> コマンドでは、プロビジョニングスキームでのこの機能の有効化または無効化と、レプリカの比率およびレプリカの最大値の変更が可能です。

Shared Image Gallery 機能をサポートするために、プロビジョニングスキームに 3 つのカスタムプロパティが追加されました:

<!JEKYLL@5300@196>

- Shared Image Gallery を使用して公開イメージを保存するかどうかを定義します。**True** に設定すると、イメージは Shared Image Gallery イメージとして保存されます。True に設定しない場合、イメージはスナップショットとして保存されます。
- 有効な値は、**True** および **False** です。
- プロパティが定義されていない場合、デフォルト値は **False** です。

<!JEKYLL@5300@197>

- ギャラリーイメージバージョンのレプリカに対するマシンの比率を定義します。
- 有効な値は、0 より大きい整数です。
- プロパティが定義されていない場合は、デフォルト値が使用されます。永続 OS ディスクのデフォルト値は 1000 であり、非永続 OS ディスクのデフォルト値は 40 です。

<!JEKYLL@5300@198>

- 各ギャラリーイメージバージョンのレプリカの最大数を定義します。
- プロパティが定義されていない場合、デフォルト値は 100 です。
- プロパティが定義されていない場合、デフォルト値は 100 です。

> ヒント:
>
> Shared Image Gallery を使用して MCS プロビジョニングされたカタログの公開イメージを保存する場合、MCS は、カタログ内のマシンの数、レプリカの比率、およびレプリカの最大数に基づいて、ギャラリーイメージバージョンのレプリカ数を設定します。レプリカ数は、カタログ内のマシンの数をレプリカ比率（最も近い整数値に切り上げ）で除算し、最大レプリカ数で値を制限することによって計算されます。たとえば、レプリカの比率が 20 で最大 5 の場合、0〜20 台のマシンで 1 つのレプリカが作成され、21〜40 台で 2 つ、41〜60 台で 3 つ、61〜80 台で 4 つ、81 台以上で 5 つのレプリカが作成されます。

ユースケース：**Shared Image Gallery** のレプリカ比率とレプリカの最大値を更新する

既存のマシンカタログは Shared Image Gallery を使用します。<!JEKYLL@5300@199> コマンドを使用して、カタログ内の既存のすべてのマシンおよび将来のマシンのカスタムプロパティを更新します：

<!JEKYLL@5300@200>

ユースケース：スナップショットカタログを **Shared Image Gallery** カタログに変換する

このユースケースの場合：

1. <!JEKYLL@5300@201> フラグを **True** に設定して <!JEKYLL@5300@202> を実行します。オプションで、<!JEKYLL@5300@203> および <!JEKYLL@5300@204> プロパティを含めます。
2. カタログを更新します。
3. マシンの電源を入れ直して、強制的に更新します。

例：

<!JEKYLL@5300@205>

> ヒント：
>
> パラメーター <!JEKYLL@5300@206> および <!JEKYLL@5300@207> は必須ではありません。<!JEKYLL@5300@208> コマンドが完了した後、Shared Image Gallery イメージはまだ作成されていません。ギャラリーを使用するようにカタログを構成すると、次回のカタログ更新操作で公開イメージがギャラリーに保存されます。カタログ更新コマンドは、ギャラリー、ギャラリーイメージ、およびイメージバージョンを作成します。マシンの電源を入れ直すとマシンが更新されます。そのとき、必要に応じてレプリカ数が更新されます。それ以降、既存のすべての非永続マシンは Shared Image Gallery イメージを使用してリセットされ、新しくプロビジョニングされたすべてのマシンはイメージを使用して作成されます。古いスナップショットは、数時間以内に自動的にクリーンアップされます。

ユースケース：**Shared Image Gallery** カタログをスナップショットカタログに変換する

このユースケースの場合：

1. <!JEKYLL@5300@209> フラグを **False** に設定するか、定義せずに <!JEKYLL@5300@210> を実行します。
2. カタログを更新します。
3. マシンの電源を入れ直して、強制的に更新します。

例：

<!JEKYLL@5300@211>

> ヒント：
>
> スナップショットから Shared Image Gallery カタログへの更新とは異なり、各マシンのカスタムデータは、新しいカスタムプロパティを反映するようにまだ更新されていません。次のコマンドを実行して、元の Shared Image Gallery のカスタムプロパティを表示します：<!JEKYLL@5300@212>。<!JEKYLL@5300@213> コマンドが完了した後、イメージスナップショットはまだ作成されていません。ギャラリーを使用しないようにカタログを構成すると、次回のカタログ更新操作で公開イメージがスナップショットとして保存されます。その時点から、既存のすべての非永続マシンはスナップショットを使用してリセットされ、新しくプロビジョニングされたすべてのマシンはスナップショットから作成されます。マシンの電源を入れ直すと更新され、そのときカスタムマシンデータが更新されて、<!JEKYLL@5300@214> が **False** に設定されていることが反映されます。古い Shared Image Gallery アセット（ギャラリー、イメージ、バージョン）は、数時間以内に自動的にクリーンアップされます。

指定されたアベイラビリティゾーンへのマシンのプロビジョニング

Azure 環境の特定のアベイラビリティゾーンにマシンをプロビジョニングできます。これは、PowerShell を使用して実行できます。

> 注：
>
> ゾーンが指定されていない場合、MCS は Azure にマシンをリージョン内に配置させます。複数のゾーンが指定されている場合、MCS はマシンをそれらにランダムに分散します。

PowerShell を使用したアベイラビリティゾーンの構成

PowerShell を使用する場合、<!JEKYLL@5300@215> でオファリングのインベントリアイテムを表示できます。たとえば、米国東部リージョン <!JEKYLL@5300@216> のサービスオファリングを表示するには、以下を実行します：

<!JEKYLL@5300@217>

ゾーンを表示するには、アイテムの <!JEKYLL@5300@218> パラメーターを使用します：

<!JEKYLL@5300@219>

アベイラビリティゾーンが指定されていない場合、マシンのプロビジョニング方法に変更はありません。

PowerShell を使用してアベイラビリティゾーンを構成するには、<!JEKYLL@5300@220> 操作で、使用可能な **Zones** カスタムプロパティを使用します。**Zones** プロパティは、マシンをプロビジョニングするアベイラビリティゾーンの一覧を定義します。これらのゾーンには、1 つまたは複数のアベイラビリティゾーンを含めることができます。たとえば、Zones 1 と 3 の場合は、<!JEKYLL@5300@221> のようになります。

<!JEKYLL@5300@222> コマンドを使用して、プロビジョニングスキームのゾーンを更新します。

無効なゾーンが指定された場合、プロビジョニングスキームは更新されず、無効なコマンドを修正する方法を示すエラーメッセージが表示されます。

> ヒント：
>
> 無効なカスタムプロパティを指定すると、プロビジョニングスキームは更新されず、関連するエラーメッセージが表示されます。

ストレージの種類

MCS を使用する Azure 環境の仮想マシン用に異なるストレージの種類を選択します。ターゲット VM の場合、MCS は以下をサポートします：

- OS ディスク：プレミアム SSD、SSD または HDD
- ライトバックキャッシュディスク：プレミアム SSD、SSD、または HDD

これらのストレージの種類を使用するときは、次の点を考慮してください：

- VM が選択したストレージの種類をサポートしていることを確認してください。
- 構成で Azure エフェメラルディスクを使用している場合、ライトバックキャッシュディスク設定のオプションは使用できません。

> ヒント：
>
> <!JEKYLL@5300@223> は、OS タイプとストレージアカウント用に構成されています。<!JEKYLL@5300@224> は、ライトバックキャッシュのストレージの種類用に構成されています。通常のカタログの場合、<!JEKYLL@5300@225> が必要です。<!JEKYLL@5300@226> が構成されていない場合は、<!JEKYLL@5300@227> のデフォルトとして <!JEKYLL@5300@228> が使用されます。

WBCDiskStorageType が構成されていない場合、WBCDiskStorageType のデフォルトとして StorageType が使用されます

ストレージの種類の構成

VM 用のストレージの種類を構成するには、<!JEKYLL@5300@229> の <!JEKYLL@5300@230> パラメーターを使用します。<!JEKYLL@5300@231> パラメーターの値を、いずれかのサポートされているストレージの種類に設定します。

以下は、プロビジョニングスキームで使用する <!JEKYLL@5300@232> パラメーターのセットの例です：

<!JEKYLL@5300@233>

ゾーン冗長ストレージの有効化

カタログの作成中にゾーン冗長ストレージを選択できます。ゾーン冗長ストレージは複数のアベイラビリティゾーンにわたって Azure Managed Disks を同期的に複製するため、別のゾーンの冗長を利用して、ゾーンでの障害から回復できます。

ストレージの種類のカスタムプロパティで **Premium_ZRS** および **StandardSSD_ZRS** を指定できます。ZRS ストレージは、既存のカスタムプロパティを使用するか、**MachineProfile** テンプレートを使用して設定できます。ZRS ストレージも <!JEKYLL@5300@234> および <!JEKYLL@5300@235> パラメーターを指定した <!JEKYLL@5300@236> コマンドによりサポートされており、既存のマシンを LRS から ZRS ストレージに変更できます。

制限事項:

- 管理対象ディスクでのみサポートされます
- プレミアムおよびスタンダードのソリッドステートドライブ（SSD）でのみサポートされます
- <!JEKYLL@5300@237> ではサポートされません
- 特定のリージョンでのみ利用できます。
- ZRS ディスクを大量に作成すると、Azure のパフォーマンスが低下します。したがって、最初の電源投入時には、小規模なバッチ（一度に 300 台未満のマシン）ごとにマシンの電源をオンにします。

ゾーン冗長ストレージをディスクストレージの種類として設定する　最初のカタログ作成時にゾーン冗長ストレージを選択するか、既存のカタログでストレージの種類を更新できます。

PowerShell コマンドを使用してゾーン冗長ストレージを選択する　<!JEKYLL@5300@238> PowerShell コマンドを使用して Azure で新しいカタログを作成するときは、<!JEKYLL@5300@239> の値として <!JEKYLL@5300@240> を使用します。
例:

<!JEKYLL@5300@241>

この値を設定すると、適切に使用できるかどうかを判断する動的 API によって検証されます。ZRS の使用がカタログで有効でない場合、次の例外が発生する可能性があります:

- **StorageTypeAtShutdownNotSupportedForZrsDisks**: StorageTypeAtShutdown カスタムプロパティは、ZRS ストレージでは使用できません。
- **StorageAccountTypeNotSupportedInRegion**: この例外は、ZRS をサポートしていない Azure リージョンで ZRS ストレージを使用しようとすると発生します。
- **ZrsRequiresManagedDisks**: ゾーン冗長ストレージは、管理対象ディスクでのみ使用できます。

次のカスタムプロパティを使用して、ディスクストレージの種類を設定できます:

- <!JEKYLL@5300@242>
- <!JEKYLL@5300@243>
- <!JEKYLL@5300@244>

> 注:

> カスタムプロパティが設定されていない場合、カタログの作成中にマシンプロファイルの OS ディスク（<!JEKYLL@5300@245>）が使用されます。

マシンプロファイルから **VM** および **NIC** の診断設定をキャプチャする

マシンカタログの作成中、既存のマシンカタログの更新中、および既存の VM の更新中に、マシンプロファイルから VM および NIC の診断設定をキャプチャできます。

VM またはテンプレートスペックをマシンプロファイルのソースとして使用できます。

主な手順

1. Azure で必要な ID を設定します。これらの ID をテンプレートスペックで指定する必要があります。
    - ストレージアカウント
    - Log Analytics ワークスペース
    - 標準レベルの料金設定のイベントハブ名前空間
2. マシンプロファイルのソースを作成します。
3. 新しいマシンカタログを作成するか、既存のカタログを更新するか、既存の VM を更新します。

Azure で必要な **ID** を設定する

Azure で次のいずれかを設定します：

- ストレージアカウント
- Log Analytics ワークスペース
- 標準レベルの料金設定のイベントハブ名前空間

ストレージアカウントをセットアップする　Azure で標準ストレージアカウントを作成します。テンプレートスペックでは、ストレージアカウントの完全な resourceId を <!JEKYLL@5300@246> として指定します。

データをストレージアカウントに記録するように VM を設定すると、データは <!JEKYLL@5300@247> コンテナの下に表示されます。

Log Analytics ワークスペースをセットアップする　Log Analytics ワークスペースを作成します。テンプレートスペックでは、Log Analytics ワークスペースの完全な resourceId を workspaceId として指定します。

ワークスペースにデータを記録するように VM を設定すると、Azure のログでデータを照会できるようになります。ログで Azure の次のコマンドを実行すると、リソースによって記録されたすべてのメトリックの数を表示できます：

‘AzureMetrics

イベントハブをセットアップする　Azure Portal でイベントハブをセットアップするには、次の手順を実行します:

1. 標準レベルの料金設定でイベントハブ名前空間を作成します。
2. 名前空間の下にイベントハブを作成します。
3. イベントハブの下の **Capture** に移動します。Avro 出力タイプでキャプチャするにはトグルをオンにします。
4. 既存のストレージアカウントに新しいコンテナを作成して、ログをキャプチャします。
5. テンプレートスペックでは、`eventHubAuthorizationRuleId`を次の形式で指定します: `/subscriptions/093f4c12-704b-4b1d-8339-f339e7557f60/resourcegroups/matspo/providers/Microsoft.EventHub/namespaces/matspoeventhub/authorizationrules/RootManageSharedAccessKey`
6. イベントハブの名前を指定します。

イベントハブにデータを記録するように VM が設定されると、データは構成されたストレージコンテナにキャプチャされます。

マシンプロファイルのソースを作成する

VM またはテンプレートスペックをマシンプロファイルのソースとして使用できます。

診断設定を使用した **VM** ベースのマシンプロファイルの作成　VM をマシンプロファイルとして作成する場合は、まずテンプレート VM 自体で診断設定をセットアップします。Microsoft ドキュメント「Azure Monitor の診断設定」に記載されている詳細な手順を参照してください。

次のコマンドを実行して、VM または NIC に関連付けられた診断設定があることを確認できます:

```
az monitor diagnostic-settings list --resource-group matspo --resource matspo-tog-cc2659 --resource-type microsoft.network/networkInterfaces
```

```
az monitor diagnostic-settings list --resource-group matspo --resource matspo-tog-cc2 --resource-type microsoft.compute/virtualMachines
```

診断設定を使用したテンプレートスペックベースのマシンプロファイルの作成　既に診断設定が有効になっている VM を使用し、それを ARM テンプレートスペックにエクスポートする場合、これらの設定はテンプレート内に自動的に含まれません。ARM テンプレート内の診断設定を手動で追加または変更する必要があります。

ただし、マシンプロファイルとして VM が必要な場合、MCS は重要な診断設定が正確にキャプチャされ、MCS カタログ内のリソースに適用されることを保証します。

1. VM と NIC を定義する標準テンプレートスペックを作成します。

2. スペックに従って診断設定を展開するためのリソースを追加します：Microsoft.Insights diagnosticSettings。スコープについては、テンプレート内の VM または NIC を、部分的な ID を含めた名前で参照します。たとえば、テンプレートスペックで「test-VM」という名前の VM にアタッチされた診断設定を作成するには、スコープを次のように指定します：

```
"scope": "microsoft.compute/virtualMachines/test-VM",
```

3. テンプレートスペックをマシンプロファイルのソースとして使用します。

診断設定を使用したカタログの作成または更新

マシンプロファイルのソースを作成した後、New-ProvSchemeコマンドを使用してマシンカタログを作成し、Set-ProvSchemeコマンドを使用して既存のマシンカタログを更新し、Request-ProvVMUpdateコマンドを使用して既存の VM を更新できるようになりました。

ページファイルの場所の決定

ページファイルの場所は、次のシナリオに従って決定されます：

> 注：
>
> デフォルトのページファイルの場所は OS ディスク上です。

シナリオ	場所
ページファイル設定はカスタムプロパティで指定される	カスタムプロパティで指定された場所
エフェメラル OS ディスクまたは休止状態が有効になっている	OS ディスク
VM に一時ディスクがある	一時ディスク
MCS IO が有効になっている	WBC ディスク

ページファイル設定シナリオ

次の表は、イメージの準備およびプロビジョニングスキーム更新中のページファイル設定について、いくつかの可能なシナリオを示しています：

タイミング	シナリオ	結果
イメージの準備時	ソースイメージページファイルを一時ディスクに設定しており、プロビジョニングスキームで指定した VM サイズに一時ディスクがない	ページファイルは OS に保存されます
イメージの準備時	ソースイメージページファイルを OS ディスクに設定しており、プロビジョニングスキームで指定した VM サイズに一時ディスクがない	ページファイルは一時ディスクに保存されます
イメージの準備時	ソースイメージページファイルを一時ディスクに設定しており、エフェメラル OS ディスクがプロビジョニングスキームで有効になっている	ページファイルは OS ディスクに保存されます
プロビジョニングスキームの更新時	VDA バージョンが 2311 より前の場合にプロビジョニングスキームを更新しようとした	警告でページファイル設定を変更します
プロビジョニングスキームの更新時	VDA バージョンが 2311 以降の場合にプロビジョニングスキームを更新しようとした	ページファイルの場所の決定に従ってページファイルの場所を決定します

ページファイル設定を指定する

PowerShell コマンドを使用して、場所やサイズなどのページファイル設定を指定できます。その場合、ページファイルの場所の決定に従って、MCS によって決定されたページファイル設定は上書きされます。これを行うには、マシンカタログの作成中に次の`New-ProvScheme`コマンドを実行します。

重要な注意事項

カタログの作成を進める前に、以下の点を考慮してください:

- `New-ProvScheme`コマンドですべてのカスタムプロパティ(「PageFileDiskDriveLetterOverride」、「InitialPageFileSizeInMB」、および「MaxPageFileSizeInMB」)を指定するか、いずれも指定しないでください。
- この機能は Citrix Studio ではサポートされていません。
- 初期ページファイルサイズは、16MB～16,777,216MB である必要があります。
- 最大ページファイルサイズは、初期ページファイルサイズ以上で、16,777,216MB 未満である必要があります。
- 初期ページファイルサイズと最大ページファイルサイズの両方を同時に 0 に設定できます。

> 注:
>
> マスターイメージを更新せずに、既存のカタログに新しく追加された VM のページファイル設定を変更できます。ページファイル設定を変更するには、VDA バージョン 2311 以降が必要です。PowerShell コマンドを使用してページファイルの設定を変更できます。詳しくは、「ページファイル設定を変更する」を参照してください。

```
New-ProvScheme -CleanOnBoot `
-HostingUnitName "zijinnet" `
-IdentityPoolName "PageFileSettingExample" `
-ProvisioningSchemeName "PageFileSettingExample" `
-InitialBatchSizeHint 1 `
-MasterImageVM "XDHyp:\HostingUnits\zijinnet\image.folder\neal-
    zijincloud-resources.resourcegroup\
    CustomWin10VDA_OsDisk_1_9473d7c8a6174b2c8284c7d3efeea88f.manageddisk
    " `
-NetworkMapping @{
 "0"="XDHyp:\HostingUnits\zijinnet\virtualprivatecloud.folder\East US.
     region\virtualprivatecloud.folder\neal-zijincloud-resources.
     resourcegroup\neal-zijincloud-resources-vnet.virtualprivatecloud\
     default.network" }
  `
-ServiceOffering "XDHyp:\HostingUnits\zijinnet\serviceoffering.folder\
    Standard_B2ms.serviceoffering" `
-CustomProperties '<CustomProperties xmlns=" http://schemas.citrix.com
    /2014/xd/machinecreation" xmlns:xsi=" http://www.w3.org/2001/
    XMLSchema-instance"> `
<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="false
    "/> `
<Property xsi:type="StringProperty" Name="PersistVm" Value="false"/> `
<Property xsi:type="StringProperty" Name="
    PageFileDiskDriveLetterOverride" Value="d"/> `
<Property xsi:type="StringProperty" Name="InitialPageFileSizeInMB"
    Value="2048"/> `
<Property xsi:type="StringProperty" Name="MaxPageFileSizeInMB" Value
    ="8196"/> `
<Property xsi:type="StringProperty" Name="StorageAccountType" Value="
    Premium_LRS"/> `
<Property xsi:type="StringProperty" Name="LicenseType" Value="
    Windows_Client"/> `
</CustomProperties>'
```

ページファイル設定を変更する

マスターイメージを更新せずに、既存のカタログに新しく追加された VM のページファイル設定を変更できます。この機能は、現時点では Azure 環境でのみ適用可能です。

ページファイル設定を変更するには、VDA バージョン 2311 以降が必要です。PowerShell コマンドを使用してページファイルの設定を変更できます。

Azure 環境で変更できるさまざまなページファイル設定を次に示します:

- PageFileDiskDriveLetterOverride
- InitialPageFileSizeInMB
- MaxPageFileSizeInMB

既存のカタログのページファイル設定を変更する

既存のマシンカタログのページファイル設定を変更するには、Set-ProvSchemeコマンドを実行します。この場合、更新はカタログに追加された新しい VM にのみ適用されます。例:

```
Set-ProvScheme -ProvisioningSchemeName $schemeName -CustomProperties '<
    CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
    machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
    instance">
<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true"
     />
<Property xsi:type="StringProperty" Name="OsType" Value="Windows" />
<Property xsi:type="StringProperty" Name="StorageType" Value="
    StandardSSD_LRS" />
<Property xsi:type="StringProperty" Name="
    PageFileDiskDriveLetterOverride" Value="D" />
<Property xsi:type="StringProperty" Name="InitialPageFileSizeInMB"
    Value="2048" />
<Property xsi:type="StringProperty" Name="MaxPageFileSizeInMB" Value
    ="8196" />
<Property xsi:type="StringProperty" Name="LicenseType" Value="
    Windows_Client" />
<Property  xsi:type="StringProperty" Name="Zones" Value="1" />
<Property xsi:type="StringProperty" Name="ResourceGroups" Value="neal-
    test-group1" />
<Property xsi:type="StringProperty" Name="SchemaVersion" Value="2" />
</CustomProperties>'
```

> 注:
>
> ライトバックキャッシュを有効にし、PowerShell コマンドを使用してPageFileDiskDriveLetterOverrideをC:に設定しようとすると、MCS IO ドライバーはページファイルをC:ではなく正しいディスクドライブに自動的にリダイレクトします。

Azure Spot VM を使用したカタログの作成

Azure Spot VM を使用すると、Azure の未使用のコンピューティング容量を活用することで、大幅なコスト削減になります。ただし、Azure Spot VM を割り当てることができるかどうかは、現在の容量と料金によって異なります。したがって、Azure は削除ポリシーに従って、実行中の VM を削除したり、VM の作成に失敗したり、VM の電源投入に失敗したりする可能性があります。そのため、Azure Spot VM は、一部の重要ではないアプリケーションやデスクトップに適しています。詳しくは、「Azure Spot Virtual Machines を使用する」を参照してください。

制限事項

- Azure Spot VM では、すべての VM サイズがサポートされているわけではありません。詳しくは、「制限」を参照してください。

  次の PowerShell コマンドを実行して、VM サイズが Spot VM をサポートしているかどうかを確認できます。VM サイズが Spot VM をサポートしている場合、`SupportsSpotVM`は **True** です。

```
(Get-Item "XDHyp:\HostingUnits\azure-res-conn2\serviceoffering.
   folder\Standard_D2ds_v4.serviceoffering"). AdditionalData
```

- 現在、Azure Spot VM は休止状態をサポートしていません。

条件

Azure Spot VM カタログのマシンプロファイルのソース（VM またはテンプレートスペック）を作成するときに、Azure Spot インスタンスを選択するか（VM を使用する場合）、`priority`を`Spot`に設定するか（テンプレートスペックを使用する場合）を選択する必要があります。

Azure Spot VM を使用してカタログを作成する手順

1. マシンプロファイルのソース（VM または起動テンプレート）を作成します。
   - Azure Portal を使用して VM を作成する場合は、「Azure portal を使用して Azure Spot Virtual Machines をデプロイする」を参照してください。
   - テンプレートスペックを作成する場合は、テンプレートスペックの **resources > type: Microsoft.Compute/virtualMachines > properties** の下に次のプロパティを追加します。例:

```
"priority": "Spot",
"evictionPolicy": "Deallocate",
"billingProfile": {

"maxPrice": 0.01
 }
```

> 注:
>
> - 削除ポリシーは、**Deallocate** または **Delete** にできます。
>   - 非永続的な VM の場合、MCS は常に削除ポリシーを **Delete** として設定します。VM が削除されると、非永続ディスク（OS ディスクなど）とともに削除されます。永続ディスク（ID ディスクなど）は削除されません。ただし、カタログの種類が永続的であるか、`PersistOsDisk`カスタムプロパティが True に設定されている場合、OS ディスクは永続的です。同様に、`PersistWbc`カスタムプロパティが **True** に設定されている場合、WBC ディスクは永続的です。

> – 永続的な VM の場合、MCS は常に削除ポリシーを Deallocate として設定します。VM が削除されると、割り当てが解除されます。ディスクには変更は加えられません。
> • 最大価格は、1 時間あたり支払い可能な金額です。**Capacity Only** を使用している場合、これは **-1** です。最大価格は、null、-1、または 0 より大きい小数値のみにすることができます。詳しくは、「価格」を参照してください。

2. 次の PowerShell コマンドを実行すると、マシンプロファイルで Azure Spot VM が有効になっているかどうかを確認できます。SpotEnabledパラメーターが **True** で、SpotEvictionPolicyが **Deallocate** または **Delete** に設定されている場合、マシンプロファイルは Azure Spot VM が有効になっています。たとえば、

   • マシンプロファイルのソースが VM の場合、次のコマンドを実行します:

   ```
   (Get-Item "XDHyp:\HostingUnits\azure-res-conn2\machineprofile
       .folder\fifthcolumn.resourcegroup\kb-spot-delete.vm").
       AdditionalData
   ```

   • マシンプロファイルのソースがテンプレートスペックの場合、次のコマンドを実行します:

   ```
   (Get-Item "XDHyp:\HostingUnits\azure-res-conn2\machineprofile
       .folder\fifthcolumn.resourcegroup\fc-aeh-templatespec.
       templatespec\14.0.0-spot-delete.templatespecversion").
       AdditionalData
   ```

3. New-ProvScheme PowerShell コマンドを使用し、マシンプロファイルを使用してマシンカタログを作成します。

Set-ProvSchemeコマンドを使用してカタログを更新できます。PowerShell コマンドSet-ProvVmUpdateTimeWindowを使用して既存の VM を更新することもできます。マシンプロファイルは、次回の電源投入時に更新されます。

実行中の **Azure Spot VM** での削除

コンピューティング容量が利用できない場合、または 1 時間あたりの料金が構成された最大価格より高い場合、Azure は実行中の Spot VM を削除します。デフォルトでは、削除は通知されません。VM は単にフリーズしてから削除されます。Microsoft は、スケジュールされたイベントを使用して削除を監視することを推奨しています。「削除の発生を継続的に監視する」を参照してください。VM 内からスクリプトを実行して、削除前に通知を受け取ることもできます。たとえば、Microsoft には Python ScheduledEvents.csのポーリング スクリプトがあります。

トラブルシューティング

- Get-ProvVMコマンドを使用すると、プロビジョニングされた VM の customMachineData 内の Spot VM プロパティを確認できます。priority フィールドが **Spot** に設定されている場合、Spot は使用中です。

- VM が Azure Portal で Spot を使用しているかどうかを確認できます:

  1. Azure Portal で VM を見つけます。
  2. **Overview** ページに移動します。
  3. 一番下までスクロールして、**Azure Spot** セクションを見つけます。

     - Spot が使用中ではない場合、このフィールドは空です。
     - Spot が使用中の場合、**Azure Spot** と **Azure Spot eviction policy** フィールドが設定されます。

1. [Configuration] ページで、VM の請求プロファイルまたは時間あたりの最大価格を確認できます。

バックアップ **VM** サイズの構成

パブリッククラウドでは、特定の VM サイズで容量が不足する場合があります。また、Azure Spot VM を使用している場合、VM は Azure の容量ニーズによってはいつでも削除されてしまいます。Azure の容量が不十分な場合、または Spot VM の電源投入に失敗した場合、MCS はバックアップ VM サイズにフォールバックします。MCS マシンカタログの作成または更新中に、カスタムプロパティ`BackupVmConfiguration`を使用してバックアップ VM サイズの一覧を提供できます。MCS は、一覧で指定された順序でバックアップ VM サイズにフォールバックしようとします。

MCS が VM に特定のバックアップ構成を使用する場合、次のシャットダウンまでその構成を使用し続けます。次回の電源投入時に、MCS はプライマリ VM 構成の起動を試みます。失敗した場合、MCS は一覧に従ってバックアップ VM サイズの構成を再起動しようとします。

この機能は以下でサポートされています:

- マシンプロファイルを使用するカタログ
- 永続的および非永続的 MCS マシンカタログ
- 現在の Azure 環境

重要な注意事項

- 一覧には複数のバックアップ VM サイズを指定できます。
- この一覧は一意である必要があります。
- 一覧内の各 VM にインスタンスの種類プロパティを追加できます。種類は **Spot** または **Regular** のいずれかです。種類が指定されていない場合、MCS は VM を **Regular** であるとみなします。
- `Set-ProvScheme` PowerShell コマンドを使用して、既存のカタログのバックアップ VM サイズの一覧を変更できます。
- `Set-ProvVMUpdateTimeWindow`コマンドを使用して、カタログに関連付けられたプロビジョニングスキームから作成された既存の VM を更新できます。

- `Set-ProvVM`コマンドを使用して、選択した数の既存の MCS VM に対するバックアップ VM サイズの一覧を構成できます。ただし、更新を適用するには、`Set-ProvVMUpdateTimeWindow`を使用して VM の更新時間枠を設定し、その枠内で VM を起動します。VM で`Set-ProvVm`コマンドが使用される場合、プロビジョニングスキームの一覧が後で更新されたとしても、VM はその特定の VM に設定されたバックアップ VM サイズの一覧を引き続き使用します。`Set-ProvVM`と`-RevertToProvSchemeConfiguration`を使用すると、VM にプロビジョニングスキームのバックアップ一覧を使用させることができます。

バックアップ **VM** サイズを含むカタログを作成する

1. **PowerShell** ウィンドウを開きます。
2. `asnp citrix*`を実行し、Citrix 固有の PowerShell モジュールをロードします。
3. ブローカーカタログを作成します。このカタログには、これから作成されるマシンが含まれています。
4. ID プールを作成します。これは、作成予定のマシン用に作成される AD アカウントのコンテナになります。
5. マシンプロファイルを使用してプロビジョニングスキームを作成します。例:

   - Regular の VM サイズのみの一覧を提供する場合は、次のコマンドを実行します:

```
1  New-ProvScheme -ProvisioningSchemeName "azure-catalog" -
       MasterImageVM "XDHyp:\HostingUnits\azure-zones\image.
       folder\helenli.resourcegroup\helenli-master1-mcsio-
       snapshot.snapshot"
2  -CustomProperties
3  "<CustomProperties xmlns=`"http://schemas.citrix.com/2014/xd/
       machinecreation`"xmlns:xsi=`"http://www.w3.org/2001/
       XMLSchema-instance`">
4  <Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`
       " Value=`"true`" />
5  <Property xsi:type=`"StringProperty`" Name=`"
       StorageAccountType`" Value=`"Premium_LRS`" />
6  <Property xsi:type=`"StringProperty`" Name=`"LicenseType`"
       Value=`"Windows_Server`"/>
7  <Property xsi:type=`"StringProperty`" Name=`"PersistWBC`"
       Value=`"true`"/>  <Property xsi:type=`"StringProperty`"
       Name=`"BackupVmConfiguration`" Value=`"['ServiceOffering':
        'Standard_D2as_v4', 'ServiceOffering': 'Standard_D2s_v3',
        'ServiceOffering': 'C']`"/>
8  </CustomProperties>"
```

   - 混在する VM サイズ（Regular および Spot VM）の一覧を提供する場合は、次のコマンドを実行します:

```
1  New-ProvScheme -ProvisioningSchemeName "azure-catalog" -
       MasterImageVM "XDHyp:\HostingUnits\azure-zones\image.
       folder\helenli.resourcegroup\helenli-master1-mcsio-
       snapshot.snapshot"
2  -CustomProperties
```



```
"<CustomProperties xmlns=`"http://schemas.citrix.com/2014/xd/machinecreation`"xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-instance`">
<Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`" Value=`"true`" />
<Property xsi:type=`"StringProperty`" Name=`"StorageAccountType`" Value=`"Premium_LRS`" />
<Property xsi:type=`"StringProperty`" Name=`"LicenseType`" Value=`"Windows_Server`"/>
<Property xsi:type=`"StringProperty`" Name=`"PersistWBC`" Value=`"true`"/>  <Property xsi:type=`"StringProperty`" Name=`"BackupVmConfiguration`" Value=`"[{
'ServiceOffering': 'Standard_D2as_v4', 'Type': 'Spot' }
, {
'ServiceOffering': 'Standard_D2s_v3', 'Type': 'Regular' }
, {
'ServiceOffering': 'Standard_D2s_v3', 'Type': 'Spot' }
]`"/>
</CustomProperties>"
```

6. プロビジョニングスキームの一意の ID で BrokerCatalog を更新します。
7. VM を作成してカタログに追加します。

既存のカタログの更新

Set-ProvSchemeコマンドを使用してプロビジョニングスキームを更新できます。例:

```
Set-ProvScheme -ProvisioningSchemeName "azure-catalog"
-CustomProperties
"<CustomProperties xmlns=`"http://schemas.citrix.com/2014/xd/machinecreation`"xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-instance`">
<Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`" Value=`"true`" />
<Property xsi:type=`"StringProperty`" Name=`"StorageAccountType`" Value=`"Premium_LRS`" />
<Property xsi:type=`"StringProperty`" Name=`"LicenseType`" Value=`"Windows_Server`"/>
<Property xsi:type=`"StringProperty`" Name=`"PersistWBC`" Value=`"true`"/>
<Property xsi:type=`"StringProperty`" Name=`"BackupVmConfiguration`" Value=`"[{
 'ServiceOffering': 'Standard_D2as_v4', 'Type': 'Spot' }
 , {
 'ServiceOffering': 'Standard_D2s_v3', 'Type': 'Regular' }
 , {
 'ServiceOffering': 'Standard_D2s_v3', 'Type': 'Spot' }
 ]`"/>
</CustomProperties>"
```


既存の **VM** の更新

`Set-ProvVMUpdateTimeWindow` PowerShell コマンドを使用してカタログの既存の VM を更新できます。このコマンドは、指定された時間枠内の次回の電源投入時に、カタログに関連付けられたプロビジョニングスキームから作成された VM を更新します。例:

- `Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName azure-catalog -StartTimeInUTC "3/12/2022 3am"-DurationInMinutes 60`
- `Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName azure-catalog -StartsNow -DurationInMinutes 60`

> 注:
>
> `StartsNow`はスケジュールの開始時刻を示します。`DurationInMinutes`はスケジュールの時間枠です。

`Set-ProvVM`コマンドを使用して、選択した数の既存の MCS VM に対するバックアップ VM サイズの一覧を構成できます。ただし、更新を適用するには、`Set-ProvVMUpdateTimeWindow`を使用して VM の更新時間枠を設定し、その枠内で VM を起動します。例:

1. `Set-ProvVM`コマンドを実行して、選択した数の既存の MCS VM に対するバックアップ VM サイズの一覧を構成します。例:

```
Set-ProvVM -VMName "Vm-001"
-CustomProperties
"<CustomProperties xmlns=`"http://schemas.citrix.com/2014/xd/machinecreation`"xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-instance`">
<Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`" Value=`"true`" />
<Property xsi:type=`"StringProperty`" Name=`"StorageAccountType`" Value=`"Premium_LRS`" />
<Property xsi:type=`"StringProperty`" Name=`"LicenseType`" Value=`"Windows_Server`"/>
<Property xsi:type=`"StringProperty`" Name=`"PersistWBC`" Value=`"true`"/>
<Property xsi:type=`"StringProperty`" Name=`"BackupVmConfiguration`" Value=`"[{
 'ServiceOffering': 'Standard_D2as_v4', 'Type': 'Spot' }
 , {
 'ServiceOffering': 'Standard_D2s_v3', 'Type': 'Regular' }
 , {
 'ServiceOffering': 'Standard_D2s_v3', 'Type': 'Spot' }
 ]`"/>
</CustomProperties>"
```

2. `Set-ProvVMUpdateTimeWindow`コマンドを実行して変更を適用します。例:


```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName azure-catalog -
    StartsNow -DurationInMinutes 60
```

すべてのリソースのタグをコピーする

マシンプロファイルで指定されたタグを、マシンカタログ内の新しい VM または既存の VM の複数の NIC やディスク（OS ディスク、ID ディスク、ライトバックキャッシュディスク）などのすべてのリソースにコピーできます。マシンプロファイルのソースは、VM または ARM テンプレートスペックにすることができます。

> 注:
>
> タグにポリシーを追加するか（「タグの準拠のためのポリシー定義を割り当てる」を参照）、マシンプロファイルのソースにタグを追加してリソース上のタグを保持する必要があります。

前提条件

マシンプロファイルのソース（VM または ARM テンプレートスペック）を作成して、VM、ディスク、およびその VM の NIC にタグを付けます。

- VM をマシンプロファイルの入力で使用する場合は、Azure Portal 内の VM とすべてのリソースにタグを適用します。「Azure Portal を使用してタグを適用する」を参照してください。
- ARM テンプレートスペックをマシンプロファイルの入力として使用する場合は、各リソースの下に次のタグブロックを追加します。

```
 "tags": {

"TagC": "Value3"
 }
,
```

> 注:
>
> テンプレートスペックには、最大 1 つのディスクと少なくとも 1 つの NIC を含めることができます。

新しいマシンカタログ内の **VM** のリソースにタグをコピーする

1. VM または ARM テンプレートスペックをマシンプロファイル入力として使用して、非永続カタログまたは永続カタログを作成します。
2. VM をカタログに追加し、電源をオンにします。マシンプロファイルで指定されたタグがその VM の対応するリソースにコピーされている必要があります。

> 注:
>
> マシンプロファイルで指定された NIC の数と VM で使用する NIC の数が一致しない場合、エラーが発生します。

既存の **VM** のリソースのタグを変更する

1. すべてのリソースのタグを使用してマシンプロファイルを作成します。
2. 更新されたマシンプロファイルで既存のマシンカタログを更新します。例:

```
Set-ProvScheme -ProvisioningSchemeName <YourCatalogName> -
    MachineProfile <PathToYourMachineProfile>
```

3. 更新を適用する VM をオフにします。
4. VM のスケジュールされた更新を要求します。例:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName <
    YourCatalogName>  -VMName machine1 -StartsNow -
    DurationInMinutes -1
```

5. 仮想マシンの電源を入れます。
6. マシンプロファイルで指定されたタグが対応するリソースにコピーされている必要があります。

> 注:
>
> マシンプロファイルで指定された NIC の数と`Set-ProvScheme`で指定された NIC の数が一致しない場合、エラーが発生します。

次の手順

- 最初のカタログを作成すると、Web Studio ではデリバリーグループを作成する手順が表示されます。
- 構成プロセス全体を確認するには、「インストールと構成」を参照してください
- カタログを管理するには、「マシンカタログの管理」と「Microsoft Azure カタログの管理」を参照してください。

追加情報

- 接続とリソースの作成と管理
- Microsoft Azure Resource Manager への接続
- マシンカタログの作成

Microsoft System Center Virtual Machine Manager カタログの作成

August 17, 2024

「マシンカタログの作成」では、マシンカタログを作成するウィザードについて説明します。次の情報は、Microsoft System Center Virtual Machine Manager（VMM）仮想化環境に固有の詳細について説明しています。

> 注:
>
> VMM カタログを作成する前に、VMM への接続の作成を完了する必要があります。「Microsoft System Center Virtual Machine Manager への接続」を参照してください。

マスター仮想マシンの作成

1. マスター VM に VDA をインストールします。このとき、デスクトップを最適化するオプションを選択してパフォーマンスを改善します。
2. バックアップのため、マスター仮想マシンのスナップショットを作成します。
3. 仮想デスクトップを作成します。

SMB 3 ファイル共有の MCS

仮想マシンストレージ用のサーバーメッセージブロック（SMB）3 ファイル共有で Machine Creation Services（MCS）を使用して作成したマシンカタログの場合、資格情報が次の要件を満たしていることを確認してください。これらの要件により、Controller のハイパーバイザー通信ライブラリ（HCL）からの呼び出しが SMB ストレージに正常に接続されることが保証されます:

- VMM のユーザー資格情報には、SMB ストレージに対する完全な読み取りおよび書き込みアクセス権限が必要です。
- 仮想マシンのライフサイクルイベント中のストレージ仮想ディスク操作では、Hyper-V サーバーを介して VMM のユーザー資格情報が使用されます。

SMB をストレージとして使用する場合は、Controller から各 Hyper-V マシンへの CredSSP（Authentication Credential Security Support Provider）を有効にしてください。このプロセスは、Windows Server 2012 上の Hyper-V を備えた VMM 2012 SP1 に使用します。詳しくは、CTX137465 を参照してください。

HCL は`CredSSP`を使用して、Hyper-V マシンへの接続を開きます。この機能は、Kerberos で暗号化されたユーザー資格情報を Hyper-V マシンに渡します。リモート Hyper-V マシン上のセッションの **PowerShell** コマンドは、指定した資格情報で実行されます。この場合は、VMM ユーザーの資格情報です（ストレージへの通信コマンドが正しく機能するように）。

以下のタスクでは、HCL から Hyper-V マシンに送信されて SMB 3.0 ストレージ上で動作する PowerShell スクリプトを使用します。

- マスターイメージの統合：マスターイメージにより、MCS プロビジョニングスキーム（マシンカタログ）が作成されます。作成された新しいディスクから仮想マシンを作成できるようにマスター VM を複製およびフラット化（および元のマスター VM の依存関係を削除）します。

  root\virtualization\v2 名前空間で ConvertVirtualHardDisk を実行します。

  例：

```
$ims = Get-WmiObject -class $class -namespace "root\virtualization\v2";
$result = $ims.ConvertVirtualHardDisk($diskName, $vhdastext)
$result
```

- 差分ディスクの作成：マスターイメージを統合して作成されたマスターイメージから、差分ディスクを作成します。この差分ディスクは、新しい仮想マシンに接続されます。

  root\virtualization\v2 名前空間で CreateVirtualHardDisk を実行します。

  例：

```
$ims = Get-WmiObject -class $class -namespace "root\virtualization\v2";
$result = $ims.CreateVirtualHardDisk($vhdastext);
$result
```

- **ID** ディスクのアップロード： HCL では、ID ディスクを SMB ストレージに直接アップロードすることはできません。そのため、Hyper-V マシンが ID ディスクをストレージにアップロードしてコピーする必要があります。Hyper-V マシンは Controller からディスクを読み取れないため、HCL は Hyper-V マシンを介して ID ディスクをコピーしておく必要があります。

  1. HCL は管理者共有を介して ID ディスクを Hyper-V マシンにアップロードします。
  2. PowerShell リモートセッションで実行される PowerShell スクリプトにより、Hyper-V マシンが ID ディスクを SMB ストレージにコピーします。Hyper-V マシン上にフォルダーが作成され、（リモート PowerShell 接続を介して）そのフォルダーに対する権限が VMM ユーザーのみにロックされます。
  3. HCL が管理者共有からファイルを削除します。
  4. HCL が Hyper-V マシンへの ID ディスクのアップロードを完了すると、リモート PowerShell セッションによって ID ディスクは SMB ストレージにコピーされます。その後、Hyper-V マシンから削除します。

  ID ディスクフォルダーが削除された場合は再作成され、再使用できるようになります。

- **ID** ディスクのダウンロード：アップロードの場合と同様に、ID ディスクが Hyper-V マシンから HCL に渡されます。次の処理により、Hyper-V サーバー上に VMM ユーザー権限のみを持つフォルダーが作成されます（存在しない場合）。

  1. PowerShell スクリプトにより、Hyper-V マシンが SMB ストレージからローカルの Hyper-V ストレージに ID ディスクをコピーします。このスクリプトは、PowerShell V3 リモートセッションで実行されます。
  2. HCL が Hyper-V マシンの管理者共有から ID ディスクをメモリ内に読み取ります。

3. HCL が管理者共有からファイルを削除します。

マシンプロファイルを使用してカタログを作成する

マシンプロファイルを使用して、System Center Virtual Machine Manager（SCVMM）環境で MCS マシンカタログを作成および更新できます。vTPM を有効にできます。プロビジョニングされた VM にマシンプロファイル VM のカスタムタグを追加することもできます。

重要な注意事項

- マスターイメージはスナップショットのみにすることができます。VM にすることはできません。
- VM はマシンプロファイルのソースとしてのみ使用できます。
- VTPM は、SCVMM コンソールからではなく、Hyper-V コンソールから構成できます。
- マスターイメージで vTPM が有効になっている場合は、マシンプロファイルのソースで vTPM を有効にする必要があります。
- vTPM は、第 2 世代マシンでのみサポートされます。
- 次のパラメーターは、個別に指定されている場合、マシンプロファイルでキャプチャされた値を上書きします:
  - VMCpuCount
  - VMMemoryMB
  - Disk storage
- カスタムタグは、マスターイメージからは継承されず、マシンプロファイルからのみ継承されます。`CitrixProvisioningSchemeId`タグはデフォルトで VM に追加されます。`CitrixProvisioningSchemeId`タグを含めたくない場合は、ホスティングユニットの作成時に`-NoVmTagging`パラメーターを追加します。例:

  ```
  New-Item -HypervisorConnectionName $ConnectionName ` -NetworkPath
   @($NetworkPath)` -Path @($HostingUnitPath)` -PersonalvDiskStoragePath
   @()` -RootPath $RootPath ` -StoragePath @($StoragePath)` -
  NoVmTagging
  ```

- `Set-ProvScheme`コマンドを使用して既存のカタログを更新できます。

マシンプロファイルを使用してマシンカタログを作成する

1. マシンプロファイルのソースになる VM を作成します。詳しくは、「VMM ファブリックで仮想マシンをプロビジョニングする」を参照してください。一度選択した世代は変更できません。SCVMM では次の操作を実行できます:

- vTPM を有効にするには、以下を実行します:

  a) VM の作成後、Hyper-V ホストにログインし、**Hyper-V** マネージャーで VM を見つけます。
  b) VM を右クリックし、[**Settings**] に移動します。
  c) [**Security**] で [**Enable Trusted Platform Module**] チェックボックスをオンにします。

2. **PowerShell** ウィンドウを開きます。
3. `asnp citrix*`を実行し、Citrix 固有の PowerShell モジュールをロードします。
4. ブローカーカタログを作成します。このカタログには、これから作成されるマシンが含まれています。
5. ID プールを作成します。これは、作成予定のマシン用に作成される AD アカウントのコンテナになります。
6. マシンプロファイルを使用してプロビジョニングスキームを作成します。例:

```
New-ProvScheme -HostingUnitName "<hostingunit name>"
-IdentityPoolName "ID1" -MasterImageVM "XDHyp:\HostingUnits\HU1<
   path to the checkpoint/snapshot>"
-ProvisioningSchemeName "<catalogname>"  -MachineProfile "XDHyp:<
   path to the machine profile VM>"
```

7. プロビジョニングスキームの一意の ID でブローカーカタログを更新します。
8. VM を作成してカタログに追加します。

既存のカタログの更新

Set-ProvScheme コマンドを使用して、既存のカタログを更新できます。例:

```
Set-ProvScheme -ProvisioningSchemeName "<catalogname>" -MachineProfile
   "XDHyp:<path to the machine profile VM>"
```

VM を削除する

カタログから VM を削除することはできますが、SCVMM から VM を削除することはできません。この場合、`CitrixProvisioningSchemeId`タグは VM からのみ削除されます。カスタムタグは VM から削除されません。[完全な構成] インターフェイスまたは PowerShell コマンドを使用して、VM を削除できます。

完全な構成インターフェイスを使用して **VM** を削除する

1. VM を選択して右クリックします。
2. [削除] をクリックします。
3. [カタログから仮想マシンを削除するが、仮想マシンは消去しない] を選択します。

PowerShell コマンドの使用　`ForgetVM`パラメーターを使用した`Remove-ProvVM`。詳しくは、次のトピックを参照してください:

- タグの削除
- ハイパーバイザーにアクセスできないマシンの削除

次の手順

- 最初のカタログを作成すると、Web Studio ではデリバリーグループを作成する手順が表示されます。
- 構成プロセス全体を確認するには、「インストールと構成」を参照してください
- カタログを管理するには、「マシンカタログの管理」と「Microsoft System Center Virtual Machine Manager カタログの管理」を参照してください。

追加情報

- 接続とリソースの作成と管理
- Microsoft System Center Virtual Machine Manager への接続
- マシンカタログの作成

Nutanix カタログの作成

August 17, 2024

「マシンカタログの作成」では、マシンカタログを作成するウィザードについて説明します。以下の情報は、Nutanix 仮想化環境に固有の詳細について説明しています。

> 注:
>
> Nutanix カタログを作成する前に、Nutanix への接続の作成を完了する必要があります。「Nutanix への接続」を参照してください。

Nutanix スナップショットを使用するマシンカタログの作成

選択したスナップショットは、カタログの仮想マシンの作成に使用されるテンプレートです。カタログを作成する前に、Nutanix でイメージとスナップショットを作成してください。詳しくは、Nutanix ドキュメントを参照してください。

カタログ作成ウィザードで次の操作を行います:

- ［オペレーティングシステム］ページと ［マシン管理］ページには、Nutanix 固有の情報は含まれていません。

- ［コンテナ］または ［クラスターとコンテナ］ページは、Nutanix に固有のものです。

  Nutanix AHV XI をリソースとして使用してマシンを展開すると、［コンテナ］ページが表示されます。VM の ID ディスクを格納するコンテナを選択します。

  Nutanix AHV Prism Central（PC）をリソースとして使用してマシンを展開すると、［クラスターとコンテナ］ページが表示されます。VM の展開に使用するクラスターを選択してから、コンテナを選択します。

- ［イメージ］ページで、イメージのスナップショットを選択します。Citrix Virtual Apps and Desktops で使用する Acropolis のスナップショット名は、”XD_“で始める必要があります。必要に応じて、Acropolis コンソールを使用してスナップショットの名前を変更します。スナップショットの名前を変更した場合は、カタログ作成ウィザードを再起動して、最新の一覧を表示します。
- ［仮想マシン］ページで、仮想 CPU の数と仮想 CPU あたりのコア数を指定します。
- ［ネットワークカード］ページで、NIC（ネットワークインターフェイスカード）の種類を選択して、関連するネットワークをフィルタリングします。NIC には、［**VLAN**］と ［**OVERLAY**］の 2 種類があります。マスターイメージに含まれる 1 つまたは複数の NIC を選択してから、NIC ごとに関連付けられた仮想ネットワークを選択します。
- ［マシン **ID**］ページ、［ドメイン資格情報］ページ、［スコープ］ページ、および ［概要］ページには、Nutanix に固有の情報は含まれていません。

制限事項

Nutanix ホスト接続（具体的には、Nutanix AHV プラグイン 2.7.1）を使用して MCS カタログを作成すると、プロビジョニングされた VM のハードディスクサイズが Web Studio に誤って表示されます。表示されるサイズは、実際のストレージサイズ（50GB）よりもはるかに小さいサイズ（1GB）です。ハードディスクのサイズは、Nutanix コンソールに正しく表示されます。

次の手順

- 最初のカタログを作成すると、Web Studio ではデリバリーグループを作成する手順が表示されます。
- 構成プロセス全体を確認するには、「インストールと構成」を参照してください
- カタログを管理するには、「マシンカタログの管理」を参照してください。

追加情報

- 接続とリソースの作成と管理
- Nutanix への接続
- Nutanix クラウドおよびパートナーソリューションへの接続
- マシンカタログの作成

VMware カタログの作成

August 17, 2024

「マシンカタログの作成」では、マシンカタログを作成するウィザードについて説明します。以下の情報は、VMware 仮想化環境に固有の詳細について説明しています。

> 注:
>
> VMware カタログを作成する前に、VMware への接続の作成を完了する必要があります。「VMware への接続」を参照してください。

マスター仮想マシンの作成

管理者は、マシンカタログのユーザーデスクトップおよびアプリケーションを提供するためのマスター仮想マシンを作成します。ハイパーバイザーで、次の作業を行います。

1. マスター仮想マシンに VDA をインストールします。このとき、デスクトップを最適化するオプションを選択すると、パフォーマンスが向上します。
2. バックアップのため、マスター仮想マシンのスナップショットを作成します。

> 注:
>
> MCS を使用して、vSAN 8.0 環境で VM をプロビジョニングできます。

マシンプロファイルを使用してマシンカタログを作成する

マシンプロファイルを使用して MCS マシンカタログを作成できます。マシンプロファイルの入力のソースは VMware テンプレートです。マシンプロファイルは、VMware テンプレートからハードウェアプロパティを取得し、カタログ内の新しくプロビジョニングされた VM に適用します。

> 注:
>
> - マスターイメージの入力（スナップショット）とマシンプロファイルの入力（VMware テンプレート）は、vTPM が両方とも有効になっているか無効になっている必要があります。この規則は`New-ProvScheme`と`Set-ProvScheme`の両方に適用されます。
> - マスターイメージで vTPM が有効になっている場合、VMware テンプレートはマスターイメージと同じ VM ソースからのみ取得できます。
> - 暗号化ストレージポリシーは完全クローンのみをサポートします。

カタログへの VM のプロビジョニングを可能にするには、マシンプロファイル内の VMware テンプレートがカタログのライフサイクル中に存在する必要があります。VMware テンプレートがないと、新しい VM をプロビジョニング

できません。VMware テンプレートが削除された場合は、`Set-ProvScheme`コマンドを使用して新しいテンプレートを提供する必要があります。

- MCS は、VMware テンプレートのプロパティをキャプチャします。Get-Provscheme コマンドを使用して、VMware テンプレートの保存されたプロパティを参照することで、新しい VMware テンプレートを作成できます。
- また、マシンカタログとプロビジョニングされた VM が存在する場合は、MCS でプロビジョニングされたマシンを使用して新しい VMware テンプレートを作成することもできます。

さまざまな OS に基づいて、さまざまな構成のマシンカタログを作成できます:

- Windows 11 がマスターイメージにインストールされている場合は、マスターイメージで vTPM を有効にすることが要件です。したがって、マシンプロファイルのソースである VMware テンプレートには、vTPM が組み込まれている必要があります。
- Windows 10 が、vTPM が組み込まれていないマスターイメージにインストールされている場合は、マシンプロファイルのソースとして vTPM が含まれない VMware テンプレートを使用してマシンカタログを作成できます。

暗号化されたストレージポリシーが適用されたマシンプロファイルテンプレートを使用して、完全なコピーディスクモードでマシンカタログを作成できる別の構成もあります。

PowerShell コマンドを使用し、マシンプロファイルを入力に使用して新しいマシンカタログを作成するには、次の手順を実行します:

1. **PowerShell** ウィンドウを開きます。
2. `asnp citrix*`を実行します。
3. 次のコマンドを実行します:

    - vTPM が組み込まれた VMware テンプレートをマシンプロファイルの入力のソースとして使用し、Windows 11 がインストールされたマスターイメージを使用してマシンカタログを作成するには、以下を実行します:

```
$identityPool = New-AcctIdentityPool  -IdentityPoolName "<
    string>"
-NamingScheme "<string>-###"
-NamingSchemeType Numeric
-Domain "<domain name"
-ZoneUid "<Uid>"  -Scope @()
```

```
$provScheme =New-ProvScheme  -CleanOnBoot
-HostingUnitName "vSanRg"
-IdentityPoolName "<string>"
-InitialBatchSizeHint 1
-MasterImageVM "XDHyp:\HostingUnits<hosting unit name><
    snapshot name>.snapshot"
-NetworkMapping @{
```



```
"0"="XDHyp:\HostingUnits<hosting unit name>\<network name>.
   network" }

-ProvisioningSchemeName "<string>"
-Scope @() -VMCpuCount 4
-VMMemoryMB 6144
-MachineProfile "XDHyp:\HostingUnits<hosting unit name><
   template name>.template" -TenancyType Shared
-FunctionalLevel "L7_20"
```

```
$catalog = New-BrokerCatalog
-AllocationType "Static"
-PersistUserChanges  "OnLocal"
-Description "<string>"
-IsRemotePC $False
-MinimumFunctionalLevel 'L7_9'
-Name "<catalog name>"
-ProvisioningType 'MCS'
-Scope @()
-SessionSupport "SingleSession" -ZoneUid "<Uid>"
```

```
Set-BrokerCatalog -Name "<string>"
-ProvisioningSchemeId $provScheme.ProvisioningSchemeUid.Guid
```

- vTPM が組み込まれていない VMware テンプレートをマシンプロファイル入力のソースとして使用し、Windows 10 がインストールされたマスターイメージを使用してマシンカタログを作成するには、以下を実行します:

```
$identityPool = New-AcctIdentityPool
-IdentityPoolName "<string>"
-NamingScheme "<string>-###" -NamingSchemeType Numeric
-Domain "<domain name>"
-ZoneUid "<Uid>"  -Scope @()
```

```
$provScheme =New-ProvScheme
-CleanOnBoot -HostingUnitName "<string>"
-IdentityPoolName "<string>"
-InitialBatchSizeHint 1
-MasterImageVM "XDHyp:\HostingUnits<hosting unit name><
   snapshot name>.snapshot
-NetworkMapping @{
"0"="XDHyp:\HostingUnits<hosting unit name>\<string>.network"
    }

-ProvisioningSchemeName "<string>"  -Scope @() -VMCpuCount 4
    -VMMemoryMB 8192
-MachineProfile "XDHyp:\HostingUnits<hosting unit name><
   template name>.template"
-TenancyType Shared  -FunctionalLevel "L7_20"
```

```
$catalog = New-BrokerCatalog
-AllocationType "Static"
```



```
-PersistUserChanges  "OnLocal"
-Description "<string>"
-IsRemotePC $False
-MinimumFunctionalLevel 'L7_9' -Name "<string>" -
    ProvisioningType 'MCS' -Scope @()
-SessionSupport "SingleSession" -ZoneUid "<Uid"
```

```
Set-BrokerCatalog -Name "<string>"
-ProvisioningSchemeId $provScheme.ProvisioningSchemeUid.Guid
```

- 暗号化されたストレージポリシーが適用されたマシンプロファイルテンプレートを使用して、完全なコピーディスクモードでマシンカタログを作成するには、以下を実行します:

```
$identityPool = New-AcctIdentityPool
-IdentityPoolName "<string>"
-NamingScheme "<string>-###"
-NamingSchemeType Numeric
-Domain "<domain name>"
-ZoneUid "<Uid>"  -Scope @()
```

```
$provScheme =New-ProvScheme
-HostingUnitName "<string>"
-IdentityPoolName "<string>"
-InitialBatchSizeHint 1
-MasterImageVM "XDHyp:\HostingUnits<hosting unit name><
    snapshot name>.snapshot"
-NetworkMapping @{
"0"="XDHyp:\HostingUnits<hosting unit name>\<string>.network"
     }

-ProvisioningSchemeName "<string>"
-Scope @() -VMCpuCount 4  -VMMemoryMB 8192 -MachineProfile "
    XDHyp:\HostingUnits<hosting unit name><template name>.
    template"
-TenancyType Shared
-FunctionalLevel "L7_20" -UseFullDiskCloneProvisioning
```

```
$catalog = New-BrokerCatalog
-AllocationType "Static"
-PersistUserChanges  "OnLocal"
-Description "<string>"  -IsRemotePC $False
-MinimumFunctionalLevel 'L7_9'
-Name "<string>" -ProvisioningType 'MCS' -Scope @()
-SessionSupport "SingleSession" -ZoneUid "<Uid>"
```

```
Set-BrokerCatalog -Name "<string>"
-ProvisioningSchemeId $provScheme.ProvisioningSchemeUid.Guid
```

マシンプロファイルを更新するには、Set-ProvScheme コマンドを使用します。例:

```
Set-ProvScheme -ProvisioningSchemeName 'name' -IdentityPoolName 'name'
    -MachineProfile 'XDHyp:\HostingUnits<hosting unit name><template
```



```
        name>.template'
```

複数の **NIC** を確認する

マシンプロファイルとNew-ProvSchemeおよびSet-ProvSchemeコマンドのNetworkMappingパラメーターを使用すると、複数の NIC の事前チェック中にさまざまなエラーメッセージが表示されます。

複数の NIC の事前チェックリストは次のとおりです:

- マシンプロファイルテンプレートからの NIC 数のみが使用され、検証されます。これらの NIC が参照するネットワークは、ホスティングユニットのネットワークに対して使用または検証されません。
- マシンプロファイルテンプレートの NIC 数がホスティングユニット内のネットワーク数より大きい場合は、エラーメッセージが表示されます。
- マシンプロファイルテンプレートの NIC 数がゼロの場合、エラーメッセージが表示されます。
  マシンプロファイルテンプレートの NIC 数が 1 の場合:
  - If no network mapping is specified in the New-ProvScheme or Set-ProvScheme command, and the hosting unit network is one, then the hosting unit network is used.
  - If network mapping is specified, then the specified network mapping is used if it is valid.
- マシンプロファイルテンプレートの NIC 数が 1 より大きい場合、またはホスティングユニットのネットワーク数が 1 より大きい場合:
  - コマンドには有効なネットワークマッピングが必要であり、各 NIC のマッピングを提供する必要があります（つまり、NetworkMapping の数はマシンプロファイルの NIC の数と同じである必要があります）。
  - ホスティングユニット内の同じネットワークに複数の NIC をマッピングすることはできません。
  - NetworkMapping数とマシンプロファイルの NIC 数は、ホスティングユニットのネットワーク数以下である必要があります。
  - NetworkMappingは、各 ID に対して 0 から n-1 までで指定される必要があります。ここで、n はマシンプロファイルテンプレート内のネットワークアダプターの数です。

トラブルシューティング

カタログの作成に失敗した場合は、CTX294978を参照してください。

次の手順

- 最初のカタログを作成すると、Web Studio ではデリバリーグループを作成する手順が表示されます。
- 構成プロセス全体を確認するには、「インストールと構成」を参照してください
- カタログを管理するには、「マシンカタログの管理」と「VMware カタログの管理」を参照してください。

追加情報

- 接続とリソースの作成と管理
- VMware への接続
- マシンカタログの作成

さまざまな参加の種類を収めたカタログの作成

August 17, 2024

MCS を使用すると、オンプレミス AD 参加済み、または Hybrid Azure AD 参加済みのマシンをプロビジョニングできます。

Web Studio でマシン ID を構成する方法については、「マシンカタログの作成」を参照してください。

マシン ID 参加済みカタログの作成方法については、以下を参照してください:

- Hybrid Azure Active Directory 参加済みカタログの作成

Hybrid Azure Active Directory 参加済みカタログの作成

August 17, 2024

> 注:
>
> 2023 年 7 月より、Microsoft は Azure Active Directory（Azure AD）の名前を Microsoft Entra ID に変更しました。このドキュメントでは、Azure Active Directory、Azure AD、または AAD への言及はすべて、Microsoft Entra ID を意味することになります。

この記事では、Hybrid Azure Active Directory（AD）参加済みカタログを作成する方法について説明します。

Web Studio または PowerShell を使用して、Azure AD 参加済みカタログを作成できます。

要件、制限、および考慮事項については、「Hybrid Azure Active Directory 参加済み」を参照してください。

Web Studio の使用

以下の情報は、「マシンカタログの作成」のガイダンスを補完する情報です。Hybrid Azure AD 参加済みカタログを作成するには、Hybrid Azure AD 参加済みカタログに固有の詳細に注意しながら、その記事の一般的なガイダンスに従ってください。

カタログ作成ウィザードで次の操作を行います:

- ［マシン **ID**］ページで、［**Hybrid Azure Active Directory joined**］を選択します。作成済みマシンは組織によって所有され、その組織に属した Active Directory Domain Services アカウントでサインインします。これらのマシンはクラウドとオンプレミスに存在します。

> 注:
>
> ID の種類に ［**Hybrid Azure Active Directory joined**］を選択した場合、カタログ内の各マシンには、対応する AD コンピューターアカウントが必要です。

PowerShell の使用

以下は、Web Studio の操作に相当する PowerShell の手順です。Remote PowerShell SDK を使用してカタログを作成する方法については、https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/を参照してください。

オンプレミス AD 参加済みカタログと Hybrid Azure AD 参加済みカタログの違いは、ID プールとマシンアカウントの作成にあります。

Hybrid Azure AD 参加済みカタログのアカウントとともに ID プールを作成するには、次のようにします:

```
1 New-AcctIdentityPool -AllowUnicode -IdentityType "HybridAzureAD" -
    Domain "corp.local" -IdentityPoolName "HybridAADJoinedCatalog" -
    NamingScheme "HybridAAD-VM-##" -NamingSchemeType "Numeric" -OU "CN=
    AADComputers,DC=corp,DC=local" -Scope @() -ZoneUid "81291221-d2f2-49
    d2-ab12-bae5bbd0df05"
2 New-AcctADAccount -IdentityPoolName "HybridAADJoinedCatalog" -Count 10
    -ADUserName "corp\admin1" -ADPassword $password
3 Set-AcctAdAccountUserCert -IdentityPoolName "HybridAADJoinedCatalog" -
    All -ADUserName "corp\admin1" -ADPassword $password
```

> 注:
>
> `$password`は、書き込み権限を持つ AD ユーザーアカウントに一致するパスワードです。

Hybrid Azure AD 参加済みカタログを作成するために使用される他のすべてのコマンドは、従来のオンプレミス AD 参加済みカタログの場合と同じです。

Hybrid Azure AD 参加プロセスのステータスの表示

Web Studio では、デリバリーグループ内の Hybrid Azure AD 参加マシンが電源オンの状態にあるときに、Hybrid Azure AD 参加プロセスのステータスが表示されます。ステータスを表示するには、［検索］を使用してそれらのマシンを識別し、下ペインの ［詳細］タブで ［マシン **ID**］を 1 つずつチェックします。次の情報が ［マシン **ID**］に表示されることがあります:

- Hybrid Azure AD 参加済み
- Azure AD 未参加

> 注:
>
> - マシンの電源を最初にオンにしたとき、Hybrid Azure AD の参加が遅れることがあります。これは、デフォルトのマシン ID 同期間隔（Azure AD Connect の 30 分）が原因です。マシンは、マシン ID が Azure AD Connect を介して Azure AD に同期された後でのみ、Hybrid Azure AD 参加済み状態になります。
> - マシンが Hybrid Azure AD 参加済み状態にならない場合、それらのマシンは Delivery Controller に登録されません。このような登録ステータスは ［初期化］状態として表示されます。

また、Web Studio で、マシンが使用できない理由を知ることができます。これを行うには、［検索］ノードでマシンをクリックし、下ペインの ［詳細］タブで ［登録］をオンにしてから、ツールチップを読んで追加情報を確認します。

トラブルシューティング

マシンが Hybrid Azure AD 参加済みにならない場合は、次の手順を実行します:

- Microsoft Azure AD ポータルでそのマシンアカウントが Azure AD に同期されているかどうかを確認します。同期されている場合、［**Azure AD** 未参加］と表示され、登録ステータスが保留中であることを示します。

  マシンアカウントを Azure AD に同期するには、次のことを確認してください:

  - そのマシンアカウントが、Azure AD と同期するように構成されている OU（組織単位）内にあること。**userCertificate** 属性のないマシンアカウントは、同期するように構成された OU 内にあっても、Azure AD に同期されません。
  - **userCertificate** 属性が、そのマシンアカウントに事前設定されていること。属性は Active Directory Explorer を使用して表示できます。
  - Azure AD Connect が、マシンアカウントの作成後に少なくとも 1 回同期されていること。一度も同期されていない場合は、Azure AD Connect マシンの PowerShell コンソールで、手動で`Start-ADSyncSyncCycle -PolicyType Delta`コマンドを実行し、即時の同期をトリガーします。

- **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix** の **DeviceKeyPair-Restored** の値をクエリすることにより、Hybrid Azure AD 参加用の Citrix 管理対象デバイスのキーペアが正しくマシンにプッシュされているかどうかを確認します。

  値が「1」であることを確認します。1 でない場合、考えられる理由は次のとおりです:

  - プロビジョニングスキームに関連付けられている ID プールの`IdentityType`が、`HybridAzureAD`に設定されていない。これを確認するには、`Get-AcctIdentityPool`を実行します。
  - マシンが、マシンカタログと同じプロビジョニングスキームを使用してプロビジョニングされていない。
  - マシンが、ローカルドメインに参加していない。ローカルドメイン参加済みであることは、Hybrid Azure AD 参加の前提条件です。

- MCS プロビジョニングマシンで`dsregcmd /status /debug`コマンドを実行して診断メッセージを確認します。
  - Hybrid Azure AD 参加に成功した場合、コマンドラインの出力で「**AzureAdJoined**」と「**DomainJoined**」が「**YES**」と表示されます。
  - YES と表示されない場合は、Microsoft 社のドキュメントを参照し、問題のトラブルシューティングを行ってください：https://docs.microsoft.com/en-us/azure/active-directory/devices/troubleshoot-hybrid-join-windows-current
  - 「サーバーメッセージ：**ID** が **xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx** のデバイスにユーザー証明書が見つかりません」というエラーメッセージが表示された場合は、次の PowerShell コマンドを実行してユーザー証明書を修復します：

    ```
    1  Repair-AcctIdentity -IdentityAccountName TEST\VM1 -Target
       UserCertificate
    ```

    ユーザー証明書の問題について詳しくは、CTX566696を参照してください。

マシンカタログの管理

August 20, 2024

> 注：
>
> Web Studio（Web ベース）と Citrix Studio（Windows ベース）の 2 つの管理コンソールを使用して、Citrix Virtual Apps and Desktops の展開を管理できます。この記事では Web Studio のみを扱います。Citrix Studio について詳しくは、Citrix Virtual Apps and Desktops 7 2212 以前の同様の記事を参照してください。

はじめに

マシンカタログにマシンを追加したり、カタログからマシンを削除したり、マシンカタログの名前や説明を変更したりすることができます。また、カタログの Active Directory コンピューターアカウントを管理できます。

カタログの保守には、各マシンの OS が最新状態に更新されていることを確認することも含まれます。ウイルス対策の更新、オペレーティングシステムのアップグレード、または構成の変更も含まれます。

- Machine Creation Services（MCS）を使用して作成されたプール（ランダム）マシンが含まれるカタログは、カタログで使用されるマスターイメージを更新してからマシンを更新することにより、マシンを管理できます。この方法により、多数のユーザーマシンを効率的に更新することができます。

- 静的で恒久的に割り当てられたマシンが含まれるカタログと、リモート PC アクセスマシンカタログの場合は、ユーザーのマシンに対する更新を Web Studio の外で管理します。サードパーティ製のソフトウェア配信ツールを使用して、個々のデスクトップまたはデスクトップのグループを管理します。

ホストハイパーバイザーへの接続の作成と管理については、「接続とリソース」を参照してください。

> 注:
>
> MCS では、Windows 10 IoT Core および Windows 10 IoT Enterprise はサポートされていません。詳しくは、Microsoft 社のサイトを参照してください。

永続インスタンスについて

永続インスタンスまたは専用インスタンスを使用して作成された MCS カタログを更新する場合、カタログで作成された新しいマシンは更新されたイメージを使用します。既存のインスタンスは引き続き元のインスタンスを使用します。他の種類のカタログでも、イメージの更新プロセスは同様です。以下に注意してください:

- 永続ディスクカタログでは、既存のマシンは新しいイメージに更新されませんが、追加されたマシンは新しいイメージを使用します。
- 永続ディスクカタログではない場合、次回のマシンのリセット後にマシンイメージが更新されます。
- 永続マシンカタログでは、イメージを更新するとそのイメージを使用するカタログインスタンスも更新されます。
- 永続的ではないカタログの場合、マシンごとに異なるイメージを使用するには、個別のカタログ内にイメージが存在する必要があります。

マシンカタログの管理

マシンカタログは次の 2 つの方法で管理できます。

- Web Studio の使用
- PowerShell の使用

Web Studio を使用する

このセクションでは、Web Studio を使用してカタログを管理する方法について説明します:

- マシンカタログの管理
  - はじめに
  - 永続インスタンスについて
- マシンカタログの管理
- Web Studio を使用する

- カタログの詳細の表示
  - カタログへのマシンの追加
  - カタログからのマシンの削除
- カタログの編集
- カタログ名の変更
- 別のゾーンへのカタログの移動
- カタログの削除
- カタログにおける Active Directory コンピューターアカウントの管理
- カタログの更新
  - マスターイメージの更新またはマスターイメージの作成
  - マスターイメージの変更
  - マスターイメージのロールバック
- 機能レベルを変更するか変更を元に戻す
- カタログの複製
- フォルダーを使用したカタログの整理
  - カタログフォルダーの作成
  - カタログの移動
  - カタログフォルダーの管理
- カタログの作成の再試行
- トークンを使用した MCS 以外でプロビジョニングされた VDA の登録（Technical Preview）
- PowerShell の使用
- カタログに関連した警告とエラーの取得
- 1 回限りの再起動スケジュールを有効にする
- イメージへの説明の追加
- OS ディスクのリセット
- 既存のプロビジョニングスキームのネットワーク設定を変更
- マシンカタログのバージョンの管理
- 非マシンプロファイルベースのマシンカタログをマシンプロファイルベースのマシンカタログに変換する
- アクティブなコンピューターアカウントの ID 情報を修復する
  - 条件
  - ID ディスクをリセットする
- 既存のマシンカタログのキャッシュ構成を変更する
  - 要件
  - キャッシュ構成を変更する
- ローカルファイル共有アクセスによる VDA の更新をサポート

  - PowerShell コマンドレット
  - 前提条件
  - ファイル共有権限を設定する方法
  - ローカルファイル共有から VDA を更新する

- トラブルシューティング
- 次の手順

カタログの詳細の表示

1. 検索機能を使用して、特定のマシンカタログを見つけます。手順については、「インスタンスの検索」を参照してください。
2. 検索結果から必要に応じてカタログを選択します。
3. カタログ列の説明については、次の表を参照してください。
4. このカタログの詳細については、下部の詳細ペインのタブをクリックしてください。

列	説明
マシンカタログ	カタログ名と割り当ての種類。以下は割り当ての種類です: ランダム：カタログ内のマシンはユーザーにランダムに割り当てられます。 静的：カタログ内のマシンは、ユーザーに無期限で割り当てられます。
マシンの種類	カタログ内のマシンのサーバーまたはデスクトップの種類。設定可能な値は次のとおりです: OS の種類：マルチセッション OS（仮想）。ユーザーデータ：破棄。 OS の種類：マルチセッション OS（仮想）。ユーザーデータ：ローカルディスク上 OS の種類：シングルセッション OS（リモート PC アクセス）
マシンの数	カタログ内のマシン数とプロビジョニング方法。使用可能なプロビジョニング方法には、Machine Creation Services（MCS）、手動、および Citrix Provisioning Services が含まれます。 OS の種類：マルチセッション OS（仮想）。ユーザーデータ：破棄。
割り当て済み（個）	デリバリーグループに割り当てられたカタログ内のマシンの数。
フォルダー	マシンカタログツリー内のカタログの場所。カタログが含まれているフォルダーの名前（末尾のバックスラッシュを含む）、またはカタログがルートレベルにある場合は–が表示されます。

列	説明
VDA のアップグレード	VDA のアップグレードの状態。設定可能な値には、未構成、スケジュール設定済み、使用可能、および、最新です、が含まれます。
イメージの状態	カタログのイメージの更新状態。非永続マシンカタログにのみ適用されます。設定可能な値は次のとおりです：完全に更新されました、一部更新されました、更新保留中、準備中

カタログへのマシンの追加

以下の点に注意してください：

- 追加するマシンの数に応じて十分なプロセッサ、メモリ、ストレージが仮想化ホスト上にあることを確認してください。
- 十分な数の Active Directory コンピューターアカウントが使用可能であることを確認してください。既存のアカウントを使用している場合、使用可能なアカウントの数により、追加できるマシンの数が制限されることに注意してください。
- 追加するマシン用に Web Studio で Active Directory コンピューターアカウントを作成する場合は、適切なドメイン管理者権限も必要です。

マシンカタログにマシンを追加するには、以下の手順に従います：

1. Web Studio にサインインします。
2. 左側のペインで ［マシンカタログ］を選択します。
3. マシンカタログを選択し、操作バーの ［マシンの追加］を選択します。
4. 追加する仮想マシンの数を選択します。
5. 追加する仮想マシンの数に対し、既存の Active Directory アカウントの数が不足している場合は、作成するアカウントのドメインと場所を選択します。アカウント名前付けスキームを指定します。番号記号（#）により、名前に追加される連番または文字とその位置が定義されます。組織単位名にはスラッシュ（/）を使用しないでください。名前の先頭に番号記号を配置することはできません。たとえば、名前付けスキームとして「PC-Sales-##」を指定して［0〜9］を選択すると、PC-Sales-01、PC-Sales-02、PC-Sales-03 などのコンピューターアカウント名が作成されます。
6. 既存の Active Directory アカウントを使用する場合、アカウントを参照するか、［インポート］をクリックしてアカウント名の一覧の CSV ファイルを指定します。追加するマシンに十分な数のアカウントをインポートする必要があります。Web Studio はこれらのアカウントを管理します。すべてのアカウントのパスワードのリセットを Web Studio に許可するか、アカウントのパスワードを指定します（すべてのアカウントで同じパスワードを使用する必要があります）。

マシンの作成はバックグラウンドプロセスとして実行され、多くのマシンを追加する場合には時間がかかることがあります。Web Studio を終了してもマシンの作成処理は続行されます。

カタログからのマシンの削除

マシンをマシンカタログから削除すると、ユーザーはそのマシンにアクセスできなくなります。そのため、マシンを削除する前に以下の点について確認してください:

- マシン上に重要なユーザーデータがなく、データがある場合はバックアップ済みであること。
- すべてのユーザーがログオフしていること。メンテナンスモードをオンにすると、マシンに新たに接続できなくなります。
- マシンの電源がオフになっていること。

カタログからマシンを削除するには、以下の手順に従います:

1. Web Studio にサインインします。
2. 左側のペインで ［マシンカタログ］を選択します。
3. マシンカタログを選択し、操作バーの ［マシンの表示］を選択します。
4. 1 台または複数のマシンを選択し、操作バーの ［削除］を選択します。

マシンを削除するかどうかを選択します。マシンを削除する場合は、マシンの Active Directory アカウントを残すか、無効にするか、削除するかを指定します。

カタログの編集

1. ［説明］ページでは、カタログの説明を変更します。
2. 左側のペインで ［マシンカタログ］を選択します。
3. マシンカタログを選択し、操作バーの ［マシンカタログの編集］を選択します。
4. ［スコープ］ページで、スコープを変更します。
5. ［**NIC**］ページで、次の操作を実行します:

    - NIC のサブネットマッピングを変更するには、［割り当て済みネットワーク］フィールドからネットワークを選択します。
    - サブネットマッピングを追加するには、［**NIC** を追加］を選択し、［割り当て済みネットワーク］フィールドからネットワークを選択し、［保存］をクリックします。

    カタログに関連付けられたホストに存在するサブネットのみが、［割り当て済みネットワーク］フィールドに表示されます。

    マシンプロファイルがない場合のみ、Azure マシンカタログに NIC を追加できます。

> 注:
>
> - AWS マシンカタログの場合、同じサブネットを複数の NIC にマッピングすることはできません。
> - マシンプロファイルを含むマシンカタログの場合、カタログ上の NIC の数は、マシンプロファイル上の NIC の数と同じである必要があります。
> - この機能は、IBM Cloud ハイパーバイザーではサポートされていません。
> - この機能は、Nutanix ハイパーバイザーの場合、Nutanix Prism Element でのみサポートされます。

6. カタログの種類によっては、他のページが表示される場合があります。

   Azure Resource Manager イメージを使用して作成されたカタログの場合、以下のページが表示されます。変更は、後でカタログに追加したマシンにのみ適用されることに注意してください。既存のマシンは変更されません。

   - [仮想マシン] ページで、マシンサイズと、マシンを作成するアベイラビリティゾーンを変更します。

     > 注:
     >
     > - カタログがサポートするマシンサイズのみが表示されます。
     > - 必要に応じて、[ほかのマシンカタログで使用されるマシンサイズのみを表示する] を選択して、マシンサイズ一覧をフィルタリングします。

   - [マシンプロファイル] ページで、マシンプロファイルを使用するか変更するかを選択します。
   - (カタログが専用グループホストで構成されている場合のみ表示される) [専用ホストグループ] ページで、ホストグループを変更するかどうかを選択します。
   - [ストレージとライセンスの種類] ページで、ストレージの種類、ライセンスの種類、および Azure Compute Gallery 設定 ([準備されたイメージを **Azure Compute Gallery** に配置します] が使用中の場合のみ利用可能) を変更するかどうかを選択します。

     > 注:
     >
     > 新しく選択した設定が現在のマシンサイズをサポートしていない場合、設定を変更するとマシンサイズ設定がリセットされることを通知する警告ダイアログボックスが表示されます。続行を選択すると、仮想マシンメニューの横に赤い点が表示され、新しいマシンサイズを選択するよう求められます。

   - [ライセンスの種類] ページで、Windows ライセンスまたは Linux ライセンス設定を変更するかどうかを選択します。

   リモート PC アクセスカタログの場合、次のページが表示されます:

   - [電源管理] ページでは、電源管理設定の変更、および電源管理接続の選択を行います。
   - [組織単位] ページでは、Active Directory 組織単位を追加または削除します。

7. [適用] をクリックして変更を適用し、[保存] をクリックして終了します。

カタログ名の変更

1. Web Studio にサインインします。
2. 左側のペインで ［マシンカタログ］を選択します。
3. マシンカタログを選択し、操作バーの ［マシンカタログの名前を変更］を選択します。
4. 新しい名前を入力します。

別のゾーンへのカタログの移動

展開に複数のゾーンがある場合、カタログをゾーン間で移動させることができます。

カタログをそのカタログ内の仮想マシンが含まれるハイパーバイザー以外のゾーンに移動すると、パフォーマンスが低下する可能性があります。

1. Web Studio にサインインします。
2. 左側のペインで ［マシンカタログ］を選択します。
3. カタログを選択し、操作バーの ［移動］を選択します。
4. カタログの移動先ゾーンを選択します。

カタログの削除

カタログを削除する前に、以下の点について確認してください:

- すべてのユーザーがログオフしており、切断されたセッションは実行されません。
- カタログ内のすべてのマシンのメンテナンスモードがオンで、新たに接続できないこと。
- カタログ内のすべてのマシンの電源がオフになっていること。
- そのカタログがデリバリーグループに関連付けられていないこと。すなわち、そのカタログのマシンがデリバリーグループに含まれていないこと。

カタログを削除するには、以下の手順に従います:

1. Web Studio にサインインします。
2. 左側のペインで ［マシンカタログ］を選択します。
3. マシンカタログを選択し、操作バーの ［マシンカタログの削除］を選択します。
4. カタログ内のマシンを削除するかを指定します。マシンを削除する場合は、マシンの Active Directory コンピューターアカウントを残すか、無効にするか、削除するかを指定します。

カタログにおける **Active Directory** コンピューターアカウントの管理

マシンカタログの Active Directory アカウントについて、次の操作を行えます:

- シングルセッション OS カタログおよびマルチセッション OS カタログから Active Directory コンピューターアカウントを削除して未使用のマシンアカウントを解放する。解放したアカウントは、ほかのマシンで使用可能になります。
- カタログに追加するマシン用のコンピューターアカウントを追加しておく。組織単位名にはスラッシュ（/）を使用しないでください。

Active Directory アカウントを管理するには、以下の手順に従います:

1. Web Studio にサインインします。
2. 左側のペインで ［マシンカタログ］を選択します。
3. カタログを選択し、操作バーの ［**Active Directory** アカウント管理］を選択します。
4. 必要に応じてコンピューターアカウントを追加または削除します。アカウントを追加する場合は、すべてのアカウントのパスワードをリセットするか、すべてのアカウントに適用されるパスワードを入力するかを選択します。

   アカウントの現在のパスワードがわからない場合は、すべてのアカウントのパスワードをリセットするオプションを選択します。パスワードをリセットするための権限が必要です。パスワードを指定する場合は、アカウントのインポート時にパスワードが変更されます。アカウントを削除する場合は、そのアカウントを Active Directory 内で保持するか、無効にするか、または削除するかを選択します。

マシンをカタログから削除するか、カタログを削除する場合にも、Active Directory アカウントを保持するか、無効にするか、または削除するかを指定することができます。

カタログの更新

カタログ内のマシンを更新する前に、マスターイメージのコピーまたはスナップショットを保存しておくことをお勧めします。データベースには、各マシンカタログで使用されたマスターイメージの履歴記録が保持されます。カタログ内のマシンをロールバックして（元に戻して）、以前のバージョンのマスターイメージを使用します。デスクトップに展開した更新で問題が発生した場合は、この作業を実行します。これにより、ユーザーのダウンタイムが最小限に抑えられます。マスターイメージの削除、移動、または名前変更は行わないでください。カタログを元に戻して使用することはできません。

マシンは、更新後に自動的に再起動されます。

マスターイメージの更新またはマスターイメージの作成

マシンカタログを更新する前に、既存のマスターイメージを更新するか、またはホストハイパーバイザー上で作成します。

1. ハイパーバイザー上で、現在の仮想マシンのスナップショットを作成してわかりやすい名前を付けます。このスナップショットを使用して、カタログ内のマシンを元に戻す（ロールバックする）ことができます。

2. 必要に応じて、マスターイメージをオンにしてログオンします。
3. 更新をインストールするか、マスターイメージに対して必要な変更を加えます。
4. 仮想マシンの電源を切ります。
5. 仮想マシンのスナップショットを作成します。仮想マシンにわかりやすい名前を付けます。この名前は、Web Studio でのカタログの更新時に使用されます。Web Studio でスナップショットを作成することもできますが、ハイパーバイザー側の管理コンソールでスナップショットを作成します。このスナップショットを Web Studio で選択します。これにより、スナップショットに自動生成される名前を付けるのではなく、わかりやすい名前と説明を指定できます。GPU マスターイメージの場合は、XenServer コンソールを使用してマスターイメージのみを変更できます。

マスターイメージの変更

更新を準備し、カタログ内のすべてのマシンにロールアウトするには、以下の手順に従います:

1. Web Studio にサインインします。
2. 左側のペインで ［マシンカタログ］を選択します。
3. カタログを選択し、操作バーの ［マスターイメージの変更］を選択します。
4. ［イメージ］ページで、ホストおよびロールアウトするイメージを選択します。

   > ヒント:
   >
   > MCS で作成したカタログの場合、イメージにメモを追加することで、そのイメージに注釈を付けることができます。メモには最大 500 文字を含めることができます。マスターイメージを変更するたびに、メモを追加するかどうかに関係なく、メモ関連のエントリが作成されます。メモを追加せずにカタログを更新すると、エントリは null（-）として表示されます。イメージのメモ履歴を表示するには、カタログを選択し、下のペインで ［テンプレートのプロパティ］をクリックしてから、［メモ履歴の表示］をクリックします。

5. ［ロールアウト方法］ページで、マシンカタログ内のマシンを新しいマスターイメージによって更新するタイミング：次回シャットダウン時または即時を選択します。

   > 注:
   >
   > ロールアウトは非永続的な VM にのみ適用されるため、永続的な VM では ［ロールアウト戦略］ページを使用できません。

6. ［概要］ページの情報を確認し、［完了］をクリックします。各マシンは、更新後に自動的に再起動されます。

更新の進行状況を追跡するには、［マシンカタログ］でカタログを見つけて、インラインの進行状況バーと手順ごとの進行状況グラフを表示します。

Web Studio ではなく PowerShell SDK を使用してカタログを直接更新する場合、ハイパーバイザーテンプレート（**VMTemplates**）を指定します。これをイメージまたはイメージのスナップショットの代わりに使用します。

ロールアウト方法:

次回のシャットダウン時にイメージを更新すると、現在使用されていないマシン、つまりアクティブなユーザーセッションのないマシンにも即座に反映されます。現在アクティブなセッションが終了すると、使用中のシステムも更新を受け取ります。以下に注意してください:

- 新しいセッションは、該当するマシンで更新が完了するまで起動できません。
- シングルセッション OS マシンでは、マシンが使用されていないとき、またはユーザーがログインしていないときに、即座にマシンが更新されます。
- 子マシンがあるマルチセッション OS の場合、再起動は自動的に行われません。手動でシャットダウンし、再起動する必要があります。

> ヒント:
>
> ホスト接続の詳細設定を使用して、再起動するマシンの数を制限します。これらの設定を使用して、特定のカタログに対して実行されるアクションを変更します。詳細設定は Hypervisor によって異なります。

PowerShell を使用して 1 回限りの再起動スケジュールを有効にするには、「1 回限りの再起動スケジュールを有効にする」を参照してください。

マスターイメージのロールバック

更新後または新規のマスターイメージは、ロールアウトした後にロールバックすることができます。このプロセスは、新たに更新されたマシンで問題が発生した場合に必要になることがあります。ロールバックした場合、カタログ内のマシンは前回の動作イメージまでロールバックされます。より新しいイメージを必要とする新機能は、利用できなくなりました。ロールアウトと同様に、ロールバックでもマシンは再起動されます。

1. Web Studio にサインインします。
2. 左側のペインで ［マシンカタログ］を選択します。
3. カタログを選択し、操作バーの ［マスターイメージのロールバック］を選択します。
4. ロールアウト処理について前述したとおり、古いマスターイメージをマシンに適用するタイミングを指定します。

ロールバックは、復元が必要なマシンにのみ適用されます。新規のまたは更新したマスターイメージが適用されていないマシンのユーザーは、通知メッセージを受信したり強制的にログオフされたりすることはありません。

ロールバックの進行状況を追跡するには、［マシンカタログ］でカタログを見つけて、インラインの進行状況バーと手順ごとの進行状況グラフを表示します。

機能レベルを変更するか変更を元に戻す

マシン上の VDA を新しいバージョンにアップグレードした場合は、マシンカタログの機能レベルを変更する必要があります。すべての VDA を最新バージョンにアップグレードして、最新の機能をすべて使用できるようにすることを Citrix ではお勧めします。

マシンカタログの機能レベルを変更する前に:

- アップグレードしたマシンを起動します。これにより、マシンが Controller に登録されます。このときに、そのマシンカタログ内のマシンについてアップグレードが必要かどうかが Web Studio によりチェックされます。

カタログの機能レベルを変更するには:

1. Web Studio にサインインします。
2. 左側のペインで ［マシンカタログ］を選択します。
3. カタログを選択します。下ペインの ［詳細］タブにバージョン情報が表示されます。
4. ［機能レベルの変更］を選択します。Web Studio によりアップグレードが必要なことが検出されると、メッセージが表示されます。画面の指示に従って操作します。アップグレードできないマシンがある場合は、その理由を説明するメッセージが示されます。すべてのマシンを適切に動作させるため、［変更］をクリックする前にマシンの問題を解決しておくことを Citrix ではお勧めします。

カタログを変更した後でマシンを以前の VDA バージョンに戻すには、カタログを選択し、操作バーで ［機能レベルの変更を元に戻す］を選択します。

カタログの複製

カタログを複製する前に、次の考慮事項に注意してください:

- オペレーティングシステムとマシンの管理に関連する設定は変更できません。複製されたカタログは、元のカタログからこれらの設定を継承します。
- カタログの複製は、完了するまでに時間がかかることがあります。必要に応じて ［進行状況を隠す］を選択して、バックグラウンドで複製を実行します。
- 複製されたカタログは元のカタログの名前を継承し、サフィックスとして「Copy」が付きます。この名前は変更できます。「カタログ名の変更」を参照してください。
- 複製が完了したら、複製したカタログを必ずデリバリーグループに割り当ててください。

1. Web Studio にサインインし、左側のペインで ［マシンカタログ］をクリックします。
2. カタログを選択し、操作バーの ［複製］を選択します。
3. ［選択したマシンカタログの複製］ウィンドウで、複製されたカタログの設定を表示し、必要に応じて設定を構成します。［次へ］を選択して、次のページに進みます。
4. ［概要］ページで、設定の概要を表示し、［完了］を選択して複製を開始します。
5. 必要に応じて ［進行状況を隠す］を選択して、バックグラウンドで複製を実行します。

フォルダーを使用したカタログの整理

カタログを整理するためのフォルダーを作成して、アクセスを簡単にすることができます。たとえば、イメージの種類や組織構造ごとにカタログを整理できます。

カタログフォルダーの作成

始める前に、まずカタログを整理する方法を計画します。以下に注意してください:

- 最大で 5 レベルまでの階層構造でフォルダーをネストできます（デフォルトのルートフォルダーを除く）。
- カタログフォルダーには、カタログとサブフォルダーを含めることができます。
- バックエンドのフォルダーツリーは、Web Studio のすべてのノード（［マシンカタログ］や ［アプリケーション］ノードなど）で共有されます。フォルダーの名前変更や移動時に他のノードと名前が競合しないように、異なるノードの第 1 レベルのフォルダーには異なる名前を付けることをお勧めします。

カタログフォルダーを作成するには、次の手順に従います:

1. 左側のペインで ［マシンカタログ］を選択します。
2. フォルダー階層でフォルダーを選択し、［アクション］バーで ［フォルダーの作成］を選択します。
3. 新しいフォルダーの名前を入力し、［完了］をクリックします。

> ヒント:
>
> 意図しない場所にフォルダーを作成した場合は、それを正しい場所にドラッグできます。

カタログの移動

フォルダー間でカタログを移動できます。詳細な手順は次のとおりです:

1. 左側のペインで ［マシンカタログ］を選択します。
2. フォルダーごとにカタログを表示します。フォルダー階層の上にある ［すべて表示］をオンにして、一度にすべてのカタログを表示することもできます。
3. カタログを右クリックし、［マシンカタログの移動］を選択します。
4. カタログの移動先のフォルダーを選択し、［完了］をクリックします。

> ヒント:
>
> カタログをフォルダーにドラッグできます。

カタログフォルダーの管理

カタログフォルダーの削除、名前変更、および移動を行うことができます。

フォルダーの削除は、フォルダーとそのサブフォルダーにカタログが含まれていない場合にのみ可能となります。

フォルダーを管理するには、以下の手順に従います:

1. 左側のペインで ［マシンカタログ］を選択します。
2. フォルダー階層でフォルダーを選択し、必要に応じて ［アクション］バーでアクションを選択します:

- フォルダーの名前を変更するには、［フォルダーの名前変更］を選択します。
- フォルダーを削除するには、［フォルダーの削除］を選択します。
- フォルダーを移動するには、［フォルダーの移動］を選択します。

3. 画面の指示に従って、残りの手順を完了します。

カタログの作成の再試行

> 注:
>
> この機能は MCS カタログにのみ適用されます。

失敗したカタログにはエラーアイコンが表示されます。詳細を確認するには、各カタログの ［トラブルシューティング］タブに移動します。カタログの作成を再試行する前に、次の考慮事項を確認してください:

- まずトラブルシューティング情報を確認してから、問題を解決します。この情報は、見つかった問題について説明し、それらを解決するための推奨事項を提供します。
- オペレーティングシステムとマシンの管理に関連する設定は変更できません。カタログは、元のカタログからこれらの設定を継承します。
- 作成が完了するまでに時間がかかる場合があります。必要に応じて ［進行状況を隠す］を選択して、バックグラウンドで作成を実行します。

カタログの作成を再試行するには、次の手順を実行します:

1. Web Studio から、左側のペインで ［マシンカタログ］を選択します。
2. カタログを選択し、［トラブルシューティング］タブに移動します。
3. 再試行のハイパーリンクをクリックして、カタログの作成を再試行します。
4. 表示されるウィザードで、必要に応じて設定を変更します。変更を加える必要がない場合は、［概要］ページに直接移動できます。
5. 完了したら、［完了］を選択して作成を開始します。

トークンを使用した **MCS** 以外でプロビジョニングされた **VDA** の登録（**Technical Preview**）

MCS 以外でプロビジョニングされた VDA の登録トークンを生成および管理できるようになりました。この実装により、MCS を使用して VDA をプロビジョニングせずに、WebSocket 経由で VDA を登録できるようになります。この機能は、Linux Virtual Delivery Agent、Citrix Virtual Delivery Agent for macOS、および Citrix Virtual Apps and Desktops を使用したドメイン非参加の VDA もサポートします。

はじめに

1. サイトを構成します。詳しくは、「サイトの作成」を参照してください。

2. Delivery Controller に TLS 証明書をインストールします。詳しくは、「TLS サーバー証明書の Controller へのインストール」を参照してください。
3. Delivery Controller を信頼するには、VDA にルート CA と中間 CA をインストールします。
4. Delivery Controller で WebSocket 接続を有効にします。サイトにある各 Delivery Controller で次のコマンドを実行します:

```
New-ItemProperty "HKLM:\SOFTWARE\Citrix\DesktopServer\WorkerProxy"
    -Name "WebSocket_Enabled" -PropertyType "DWord" -Value 1 -
   Force
```

> 注:
>
> WebSocket を有効にした後は、必ず Delivery Controller を再起動してください。

登録トークンを生成する

Citrix でプロビジョニングされていないマシンに対してトークンベースの登録を有効にする必要がある場合、まずマシンカタログごとにトークンを生成し、それを VDA インストール管理者と共有する必要があります。

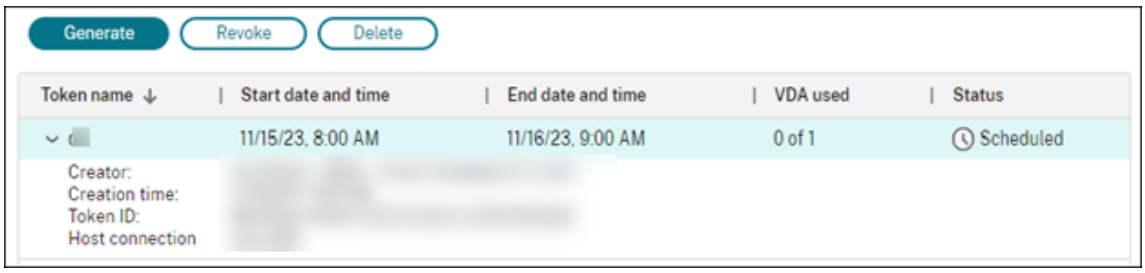
登録トークンの特徴は次のとおりです:

- 登録範囲: 1〜100 台の VDA マシン
- 有効期間: 最大 14 日間

Web Studio を使用してカタログのトークンを生成するには、次の手順を実行します:

1. [**Web Studio**] **>** [マシンカタログ] で MCS 以外でプロビジョニングされたカタログを見つけます。[マシンの数] 列に [プロビジョニング方法: 手動] が表示されています。
2. カタログを右クリックし、[登録トークンを管理する] を選択します。
3. 表示された [登録トークンを生成する] ページで、次のトークン情報を指定します:
   - トークンの名前を入力します。
   - 有効期間を入力します。期間は 14 日以内でなければなりません。トークンは指定された期間のみ有効です。
   - (オプション) トークンに登録された VDA の電源管理のホスト接続を選択します。オプションには、このカタログのゾーンにあるすべてのホスト接続が含まれます。
   - トークンの使用制限を入力します (1〜100)。
4. [生成] をクリックします。
5. 表示された [トークンが生成されました] ウィンドウでトークンをコピーして安全な場所に保存するか、[ダウンロード] をクリックしてダウンロードフォルダーにダウンロードします。

   トークンのレコードがトークン一覧に表示されます。



6. トークンを VDA インストール管理者と共有します。

   マシンへの VDA およびトークンのインストール方法について詳しくは、「VDA のインストール」を参照してください。

トークンを管理する

トークンを取り消して、VDA 登録に利用できないようにするには、2 つのオプションがあります:

- 取り消し: トークンを取り消しますが、ログ記録のために一覧に保持します。
- 削除: トークンを取り消し、一覧から削除します。

> 注:
>
> 期限切れのトークンは 14 日後に自動的に削除されます。

WebSocket VDA 登録ツールを使用してマシンをカタログに登録する

WebSocket VDA 登録ツールによって、VDA マシンのトークンベースの登録が容易になります。このツールは、登録トークンを使用して VDA をマシンカタログに追加することで、接続を WebSocket 接続に変換することができます。

> 注:
>
> このツールは、どのマシンカタログにも登録されていない VDA マシンを登録するために設計されています。

登録ツールを実行するには、次の手順に従います:

1. VDA にログインします。
2. `C:\Program Files\Citrix\Virtual Desktop Agent\Web Socket Vda Enrollment Tool`内でツール（`EnrollMachine.exe`）を見つけます。
3. 適切な入力パラメーターを使用してツールを実行します。たとえば、`EnrollMachine.exe -websocket_token_string:xxxxxxxxx`

次の表は、登録ツールの入力パラメーターについて説明しています:

パラメーター名	必須	説明	例
-websocket_token_stdin	はい	登録トークンを読み取ります。	.\EnrollMachine.exe -websocket_token_stdin
-websocket_token_string		コマンドラインパラメーターから直接登録トークンを読み取ります。	.\EnrollMachine.exe -websocket_token_string:<token>
-websocket_token_file:[token-file-path]		指定されたパスから登録トークンを読み取ります。	.\EnrollMachine.exe -websocket_token_file:C:\token\test2.txt
log:[log-file-path]	いいえ	登録ツールのログを表示します。	.\EnrollMachine.exe log:[C:\ProgramData\Citrix\EnrollMachine\EnrollMachine.txt]
-help	いいえ	簡単なヘルプテキストを表示します。	.\EnrollMachine.exe -help

登録が成功すると、ツールとログに成功メッセージが表示されます。必ず Web Studio にサインインして、VDA マシンがカタログに追加され、マシンのステータスが登録されていることを確認してください。

トラブルシューティング　デフォルトでは、登録ツールのログは次の場所にあります:

C:\ProgramData\Citrix\EnrollMachine\EnrollMachine.txt

ログに別のパスを指定した場合は、log:[log-file-path]を使用してログを取得できます。

次の表は、登録ツールによって返されるコードの一覧です:

コード	文字列	説明
0	成功	VDA がマシンカタログに正常に追加されました。
-1	InvalidArgument	登録トークンの入力パラメーターが無効です。
-2	BrokerAgentNotFound	ブローカーエージェントサービスが見つかりません。
-3	TokenInvalid	入力されたトークンは無効です。
-4	TokenMissingRequiredClaims	トークンに必要なクレーム（CustomerId や Enrollment URI など）がありません。
-5	InternalError	一般的なエラーが発生しました。
-6	TimedOut	タスクがタイムアウトになりました。
-7	FailedToDetermineMachineADJoinedStatus	VDA の AD 参加状態を返すサービスが失敗しました。
-8	ADMachineFailedToFindSid	AD マシンの SID を返すサービスが失敗しました。
-9	EnrollRequestFailed	HTTP エラーのため要求は失敗しました。
-10	EnrollResponseMissingRequiredFields	登録ツールの応答にパラメーター`VirtualSiteId`がありません。
-11	InsufficientPermission	タスクを実行するために必要な権限がありません。
-12	FailedToDetermineMachineAadJoinedStatus	VDA の AD 参加状態をチェックするサービスがエラーをスローします。
-13	AadMachineFailedToFindDeviceId	システムによって追加された追加パラメーター`AAD device id`が空です。
-14	AadDeviceIdNotValid	システムによって追加された追加パラメーター`AAD device id`は有効な GUID ではありません。
-15	NoValidMacAddress	無効な MAC アドレスです。
-16	FailedToGetComputerHostNameForVdaInstanceName	追加パラメーター`VdaInstanceName`を設定するためのコンピューターのホスト名を取得できませんでした。

コード	文字列	説明
-17	VirtualDesktopAgentRegistryKeyFailedToOpen	Delivery Controller の一覧を書き込むために VDA レジストリキーを開くことができませんでした。
-18	Failed Token reached the max count	失敗したトークンが最大数に達しました。

PowerShell の使用

このセクションでは、PowerShell を使用してカタログを管理する方法について説明します。

- カタログに関連した警告とエラーの取得
- 1 回限りの再起動スケジュールを有効にする
- イメージへの説明の追加
- OS ディスクのリセット
- 既存のプロビジョニングスキームのネットワーク設定を変更
- マシンカタログのバージョンの管理
- 非マシンプロファイルベースのマシンカタログをマシンプロファイルベースのマシンカタログに変換する
- アクティブなコンピューターアカウントの ID 情報を修復する
- 既存のマシンカタログのキャッシュ構成を変更する
- ローカルファイル共有アクセスによる VDA の更新をサポート

カタログに関連した警告とエラーの取得

MCS カタログの問題を把握して修正するために、エラーと警告の履歴を取得することができます。

PowerShell コマンドを使用すると、次のことができます:

- エラーまたは警告の一覧を取得する
- 警告ステータスを **New**（新規）から **Acknowledged**（確認済み）に変更する
- エラーまたは警告を削除する

PowerShell コマンドを実行するには:

1. PowerShell ウィンドウを開きます。
2. `asnp citrix*`を実行し、Citrix 固有の PowerShell モジュールをロードします。

エラーと警告の一覧を取得するには:

`Get-ProvOperationEvent`コマンドを実行します。

- パラメーターなし：すべてのエラーと警告を取得します

- LinkedObjectTypeおよびLinkedObjectUidパラメーターあり：特定のプロビジョニングスキームに関連付けられたすべてのエラーと警告を取得します
- EventIdパラメーターあり：このイベント ID に一致する特定のエラーまたは警告を取得します
- Filterパラメーターあり：カスタマイズされたフィルターによってエラーまたは警告を取得します

エラーまたは警告の状態を **New**（新規）から **Acknowledged**（確認済み）に変更するには：

Confirm-ProvOperationEventコマンドを実行します。

- EventIdパラメーターあり：このイベント ID に一致する特定のエラーまたは警告の状態を設定します。Get-ProvOperationEventコマンドからの出力として特定のエラーまたは警告のEventIdを取得できます
- LinkedObjectTypeおよびLinkedObjectUidパラメーターあり：特定のプロビジョニングスキームに関連付けられたすべてのエラーと警告の状態を設定します
- Allパラメーターあり：すべてのエラーと警告の状態を **Acknowledged**（確認済み）に設定します

エラーまたは警告を削除するには：

Remove-ProvOperationEventコマンドを実行します。

- EventIdパラメーターあり：このイベント ID に一致する特定のエラーまたは警告を削除します。Get-ProvOperationEventコマンドからの出力として特定のエラーまたは警告のEventIdを取得できます
- LinkedObjectTypeおよびLinkedObjectUidパラメーターあり：特定のプロビジョニングスキームに関連付けられたすべてのエラーと警告を削除します
- Allパラメーターあり：すべてのエラーと警告を削除します

詳しくは、「Citrix PowerShell SDK」を参照してください。

ハイパーバイザーにアクセスできないマシンの削除

VM またはプロビジョニングスキームを削除する場合、MCS は、削除オプションに含まれるリソースが MCS によって追跡または識別されなくなるように、VM から（場合によってはベース ディスクからも）タグを削除する必要があります。ただし、これらのリソースの一部は、ハイパーバイザーを介してのみアクセスできます。ハイパーバイザーにアクセスできない場合は、Remove-ProvVMPowerShell のPurgeDBOnlyオプションを使用して、VM、基本ディスク、ACG 内のイメージなどの VM リソースオブジェクトをデータベースから削除します。

このオプションは以下で有効になります：

- サポートされるすべてのハイパーバイザー
- 永続的および非永続的な VM

制限事項

コマンド-PurgeDBOnly と-ForgetVM を同時に使用することはできません。

PurgeDBOnly コマンドを使用する

PowerShell コマンド`Remove-ProvVM -ProvisioningSchemeName SCVMM-MC -VMName SCVMM01 -ForgetVM`を実行すると、次のシナリオで削除操作が失敗することがあります:

- ホスト接続がメンテナンス モードである
- 無効な資格情報
- 認証エラー
- 不正な操作
- ハイパーバイザーに到達できない

> 注:
>
> Remove-provVM -ForgetVM は、永続的な VM のみを対象としています。一覧にあるいずれかの VM が非永続的である場合、操作は失敗します。

ハイパーバイザーに到達できないために操作が失敗すると、次のプロンプトが表示されます:

`Try to use -PurgeDBOnly option to clean DDC database.`

`Remove-ProvVM`PowerShell コマンドで`-PurgeDBOnly`オプションを使用して、VM のリファレンスを MCS データベースから削除します。たとえば、

```
Remove-ProvVM -ProvisioningSchemeName SCVMM-MC -VMName SCVMM01 -
PurgeDBOnly
```

1 回限りの再起動スケジュールを有効にする

PowerShell を使用して 1 回限りの再起動スケジュールを有効にする場合は、以下の`BrokerCatalogRebootSchedule`の PowerShell コマンドを使用して、再起動スケジュールを作成、変更、および削除します:

- Get-BrokerCatalogRebootSchedule
- New-BrokerCatalogRebootSchedule
- Set-BrokerCatalogRebootSchedule
- Remove-BrokerCatalogRebootSchedule
- Rename-BrokerCatalogRebootSchedule

たとえば、

- **BankTellers** という名前のカタログ内の VM の再起動スケジュールを作成して、2022 年 2 月 3 日の午前 2 時から午前 4 時の間に開始します。

```
C:\PS> New-BrokerCatalogRebootSchedule -Name BankTellers -
    CatalogName BankTellers  -StartDate "2022-02-03" -StartTime "
    02:00" -Enabled $true -RebootDuration 120
```


- UID 17 を持つカタログ内の VM の再起動スケジュールを作成して、2022 年 2 月 3 日の午前 1 時から午前 5 時の間に開始します。再起動の 10 分前に、各 VM は、すべてのユーザーセッションで「**WARNING: Reboot pending**（警告：再起動保留中）」というタイトルのメッセージボックスと、「**Save your work**（作業を保存してください）」というメッセージを表示するように設定されています。

```
C:\PS> New-BrokerCatalogRebootSchedule -Name 'Update reboot' -
    CatalogUid 17 -StartDate "2022-02-03" -StartTime "01:00" -
    Enabled $true -RebootDuration 240 -WarningTitle "WARNING:
    Reboot pending" -WarningMessage "Save your work" -
    WarningDuration 10
```

- **Old Name** という名前のカタログ再起動スケジュールを **New Name** という名前に変更します。

```
C:\PS> Rename-BrokerCatalogRebootSchedule -Name "Old Name" -
    NewName "New Name"
```

- UID 1 のすべてのカタログ再起動スケジュールを表示し、UID 1 のカタログ再起動スケジュールの名前を **New Name** に変更します。

```
C:\PS> Get-BrokerCatalogRebootSchedule -Uid 1 | Rename-
    BrokerCatalogRebootSchedule -NewName "New Name" -PassThru
```

- **Accounting** という名前のカタログ再起動スケジュールを設定して、各仮想マシンの再起動の 10 分前に「**WARNING: Reboot pending**（警告：再起動保留中）」というタイトルのメッセージと、「**Save your work**（作業を保存してください）」というメッセージを表示します。このメッセージは、その VM のすべてのユーザーセッションに表示されます。

  “‘

  C:\PS> Set-BrokerCatalogRebootSchedule -Name Accounting -WarningMessage “Save your work” -WarningDuration 10 -WarningTitle “WARNING: Reboot pending”

- 無効になっているすべての再起動スケジュールを表示し、有効にします。

```
C:\PS> Get-BrokerCatalogRebootSchedule -Enabled $false | Set-
    BrokerCatalogRebootSchedule -Enabled $true
```

- UID 17 でカタログ再起動スケジュールを設定して、「**Rebooting in %m% minutes**（あと%m% 分で再起動）」というメッセージを表示します（各 VM の再起動の 15 分、10 分、5 分前）。

```
C:\PS> Set-BrokerCatalogRebootSchedule 17 -WarningMessage "
    Rebooting in %m% minutes." -WarningDuration 15 -
    WarningRepeatInterval 5
```

- **MyCatalog** という名前のカタログのタイムゾーンを構成します。

```
C:\PS> Set-BrokerCatalog -Name "MyCatalog" -TimeZone <TimeZone>
```


イメージへの説明の追加

マシンカタログイメージの更新に関連した変更に関する説明を追加できます。カタログを作成するとき、またはカタログの既存のマスターイメージを更新するときに、この機能を使用して説明を追加します。カタログ内の各マスターイメージの情報を表示することもできます。次のコマンドを使用して、イメージの説明を追加または表示します:

- マスターイメージでマシンカタログを作成するときにメモを追加するには、NewProvSchemeコマンドでMasterImageNoteパラメーターを使用します。例:

```
C:\PS>New-ProvScheme -ProvisioningSchemeName <name> -
    HostingUnitName <name> -IdentityPoolName <name> -MasterImageVM
XDHyp:\HostingUnits<hosting unit name><vm name>.vm\Base.snapshot
    -MasterImageNote "Note"
```

- マシンカタログに関連付けられているマスターイメージを更新するには、Publish-ProvMasterVMImageコマンドでMasterImageNoteパラメーターを使用します。例:

```
C:\PS>Publish-ProvMasterVMImage -ProvisioningSchemeName <name> -
    MasterImageVM XDHyp:\HostingUnits<hosting unit name><vm name>.
    vm\base.snapshot -MasterImageNote "Note"
```

- 各イメージの情報を表示するには、Get-ProvSchemeMasterVMImageHistory コマンドを使用します。例:

```
C:\PS>Get-ProvSchemeMasterVMImageHistory -ProvisioningSchemeName
    MyScheme -Showall
```

ロールバックの進行状況を追跡するには、[マシンカタログ] でカタログを見つけて、インラインの進行状況バーと手順ごとの進行状況グラフを表示します。

次のような場合、ロールバックできません（[マスターイメージのロール バック] オプションは表示されません）。

- ロールバックする権限がない。
- カタログが MCS を使用して作成されていない。
- カタログが、OS ディスクのイメージを使用して作成されている。
- カタログの作成に使用されたスナップショットが破損した。
- カタログ内のマシンに対してユーザーが行った変更が保持されない。
- カタログ内のマシンが実行中である。

OS ディスクのリセット

PowerShell コマンドReset-ProvVMDiskを使用して、MCS で作成されたマシンカタログ内の永続的な VM の OS ディスクをリセットします。現在この機能は、AWS、Azure、XenServer、Google Cloud に適用できます。SCVMM および VMware 仮想化環境。

PowerShell コマンドを正常に実行するには、次のことを確認してください:

- ターゲット VM が永続的な MCS カタログにある。

- MCS マシンカタログが正常に機能している。
- これは、プロビジョニングスキームとホストが存在し、プロビジョニングスキームに正しいエントリがあることを意味します。
- ハイパーバイザーはメンテナンスモードではない。
- ターゲット VM の電源がオフで、メンテナンスモードになっている。

OS ディスクをリセットするには、以下の手順を実行します:

1. PowerShell ウィンドウを開きます。
2. **asnp citrix*** を実行し、Citrix 固有の PowerShell モジュールをロードします。
3. 次のいずれかの方法で、PowerShell コマンド`Reset-ProvVMDisk`を実行します:

   - VM の一覧をコンマ区切りの一覧として指定し、各 VM でリセットを実行します:

     ```
     Reset-ProvVMDisk -ProvisioningSchemeName "xxx" -VMName ("abc"
         ,"def") -OS
     ```

   - `Get-ProvVM`コマンドからの出力として VM の一覧を指定し、各 VM でリセットを実行します:

     ```
     (Get-ProvVM -ProvisioningSchemeName "xxx") | Reset-ProvVMDisk
         "abc" -OS
     ```

   - 単一の VM を名前で指定します:

     ```
     Reset-ProvVMDisk -ProvisioningSchemeName "xxx" -VMName "abc"
         -OS
     ```

   - `Get-ProvVM`コマンドによって返される VM ごとに個別のリセットタスクを作成します。これは、VM ごとのハイパーバイザー機能チェック、接続チェックなど、各タスクが同じ冗長チェックを実行するため、効率が低下します。

     ```
     Get-ProvVM -ProvisioningSchemeName "xxx" | Reset-ProvVMDisk -
         ProvisioningSchemeName "xxx" -OS
     ```

4. リセットする VM を一覧表示する確認プロンプトと、回復不能な操作であるという警告メッセージが表示されます。回答を入力せずに **Enter** キーを押すと、それ以上のアクションは実行されません。

   > 注:
   >
   > リセットプロセスが完了するまで、VM のメンテナンスモードを解除したり、電源を入れたりしないでください。

   PowerShell コマンド`-WhatIf`を実行して、実行するアクションを出力し、アクションを実行せずに終了できます。

   次のいずれかの方法を使用して、確認プロンプトを回避することもできます:

   - `-Force`パラメーターを指定します:


```
Reset-ProvVMDisk -ProvisioningSchemeName "xxx" -VMName "abc"
    -OS -Force
```

- `-Confirm:$false`パラメーターを指定します:

```
Reset-ProvVMDisk -ProvisioningSchemeName "xxx" -VMName "abc"
    -OS -Confirm:$false
```

- `Reset-ProvVMDisk`を実行する前に、`$ConfirmPreference`を **None** に変更します:

```
PS C:\Windows\system32> $ConfirmPreference='None'
PS C:\Windows\system32> $ConfirmPreference
None
PS C:\Windows\system32> Reset-ProvVMDisk -
    ProvisioningSchemeName "xxx" -VMName "abc" -OS
```

5. `Reset-ProvVMDisk`コマンドで返されたタスクのステータスを取得するには、`Get-ProvTask`を実行します。

既存のプロビジョニングスキームのネットワーク設定を変更

新しい仮想マシンが新しいサブネットワーク上に作成されるように、既存のプロビジョニングスキームのネットワーク設定を変更できます。`Set-ProvScheme`コマンドのパラメーター`-NetworkMapping`を使用して、ネットワーク設定を変更します。

> 注:
>
> この機能は、Citrix Virtual Apps and Desktops 2203 LTSR CU3 以降のバージョンでサポートされています。

既存のプロビジョニングスキームのネットワーク設定を変更するには、以下を実行します:

1. PowerShell ウィンドウで、コマンド`asnp citrix*`を実行して PowerShell モジュールをロードします。
2. `(Get-Provscheme -ProvisioningSchemeName "name").NetworkMaps`を実行して、変更するネットワークパスにアクセスします。
3. 新しいネットワーク設定に変数を割り当てます。例:

```
$NewNetworkMap = @{
 "0"= "XDHYP:\HostingUnits\MyNetworks\Network 0.network" }
```

4. `Set-ProvScheme -ProvisioningSchemeName "name"-NetworkMapping $NewNetworkMap`を実行します。
5. `(Get-Provscheme -ProvisioningSchemeName "name").NetworkMaps`を実行して、既存のプロビジョニングスキームの新しいネットワーク設定を確認します。

マシンカタログのバージョンの管理

MCS マシンカタログが`Set-ProvScheme`コマンドで更新されると、現在の設定がバージョンとして保存されます。その後、PowerShell コマンドを使用してさまざまなバージョンのマシンカタログを管理できます。次の操作を実行できます:

- マシンカタログのバージョンの一覧を表示する
- 以前のバージョンを使用してマシンカタログを更新する
- そのマシンカタログの VM で使用されていないバージョンを手動で削除する
- マシンカタログによって保持されるバージョンの最大数を変更する（デフォルトは 99）

バージョンには、マシンカタログの次の情報が含まれます:

- VMCpuCount
- VMMemoryMB
- CustomProperties
- ServiceOffering
- MachineProfile
- NetworkMapping
- SecurityGroup

（例として提供された）次のコマンドを実行して、マシンカタログのさまざまなバージョンを管理します。

- マシンカタログのさまざまなバージョンの構成の詳細を表示する場合:

```
1  Get-ProvSchemeVersion -ProvisioningSchemeName AzureCatalog
```

- マシンカタログの特定のバージョンの構成の詳細を表示する場合:

```
1  Get-ProvSchemeVersion -ProvisioningSchemeName AzureCatalog -
       Version 2
```

- マシンカタログに関連付けられているバージョンの合計数を確認する場合:

  ‘‘‘

  (Get-ProvSchemeVersion -ProvisioningSchemeName AzureCatalog).Count

- 以前のバージョンを使用してマシンカタログを更新する場合:

```
1  Set-ProvScheme -ProvisioningSchemeName AzureCatalog -Version 2
```

- そのマシンカタログの VM で使用されていないバージョンを手動で削除する場合:

```
1  Remove-ProvSchemeVersion -ProvisioningSchemeName AzureCatalog -
       Version 3
```

- マシンカタログで保持されるバージョンの最大数を設定する場合（デフォルトは 99）。この設定はすべてのカタログに適用されます。たとえば、この場合、MCS でプロビジョニングされたすべてのカタログに対して最大

15 のバージョンが保持されます。

```
Set-ProvServiceConfigurationData -Name "MaxProvSchemeVersions" -
    Value 15
```

バージョン数が最大バージョン数に達した場合、マシンカタログ内のいずれかの VM で古いバージョンが使用されていると、新しいバージョンを作成できなくなります。その場合は、次のいずれかを実行します:

- マシンカタログで保持されるバージョンの最大数の上限を増やします。
- 古いバージョンの一部の VM を更新して、それらの古いバージョンがどの VM からも参照されなくなり、削除できるようにします。

非マシンプロファイルベースのマシンカタログをマシンプロファイルベースのマシンカタログに変換する

VM、テンプレートスペック（Azure の場合）、または起動テンプレート（AWS の場合）をマシンプロファイルの入力に使用して、非マシンプロファイルベースのマシンカタログをマシンプロファイルベースのマシンカタログに変換できます。カタログに追加された新しい VM は、明示的なカスタムプロパティによって上書きされない限り、マシンプロファイルからプロパティ値を取得します。

> 注:
>
> 既存のマシンプロファイルベースのマシンカタログを、非マシンプロファイルベースのマシンカタログに変更することはできません。

これを行うには、以下の手順に従います:

1. VM を使用し、マシンプロファイルを使用せずに、永続的または非永続的なマシンカタログを作成します。
2. **PowerShell** ウィンドウを開きます。
3. `Set-ProvScheme`コマンドを実行して、マシンプロファイルのプロパティ値をマシンカタログに追加された新しい VM に適用します。例:

   - Azure の場合:

   ```
   Set-ProvScheme = Set-ProvScheme -ProvisioningSchemeName xxxx
       -MachineProfile XDHyp:\HostingUnits<HostingUnitName>\
       machineprofile.folder<ResourceGroupName><TemplateSpecName
       ><VersionName>
   ```

   - AWS の場合:

   ```
   Set-ProvScheme = Set-ProvScheme -ProvisioningSchemeName xxxx
       -MachineProfile "XDHyp:\HostingUnits<hosting-unit><launch-
       template>.launchtemplate<launch-template-version>.
       launchtemplateversion"
   ```


アクティブなコンピューターアカウントの **ID** 情報を修復する

ID 関連の問題があるアクティブなコンピューターアカウントの ID 情報をリセットできます。マシンのパスワードと信頼キーのみをリセットするか、ID ディスクのすべての構成をリセットするかを選択できます。この実装は、永続および非永続の両方の MCS マシンカタログに適用できます。

> 注:
>
> 現在、この機能は AWS、GCP、Azure、XenServer、VMware 仮想化環境でサポートされています。

条件

ID ディスクを正常にリセットするには、次のことを確認してください:

- VM をオフにしてメンテナンスモードに設定する
- PowerShell コマンドにパラメーター「-OS」を含めない

ID ディスクをリセットする

ID ディスクをリセットするには:

1. **PowerShell** ウィンドウを開きます。
2. `asnp citrix*`を実行し、Citrix 固有の PowerShell モジュールをロードします。
3. ID 情報をリセットします。

    - マシンのパスワードと信頼キーのみをリセットするには、次のコマンドを次の順序で実行します:

    ```
    Repair-AcctIdentity -IdentityAccountName TEST\VM1 -
        PrivilegedUserName TEST\admin1 -PrivilegedUserPassword
        $password -Target IdentityInfo
    ```

    コマンドで使用されるパラメーターの説明は次のとおりです:

    - `IdentityAccountName`: 修復が必要な ID アカウントの名前。
    - `PrivilegedUserName`: ID プロバイダー（AD または AzureAD）に対する書き込み権限を持つユーザーアカウント。
    - `PrivilegedUserPassword`: PrivilegedUserName のパスワード。
    - `Target`: 修復作業のターゲット。これには、アカウントのパスワード/信頼キーを修復するための IdentityInfo、および Hybrid AzureAD に参加しているマシンの ID のユーザー証明書属性を修復するための UserCertificate があります。

    ```
    Reset-ProvVMDisk -ProvisioningSchemeName <name> -VMname <name
        > -Identity -ResetIdentityInfo
    ```

    `ResetIdentityInfo`パラメーターは以下をリセットします:

  - パスワードと信頼キー：VM が AD ドメインに参加している場合（DaaS ドキュメントのみ）
  - 信頼キーのみ：VM が AD ドメインに参加していない場合（DaaS ドキュメントのみ）
  - パスワードのみ：VM が AD ドメインに参加している場合（CVAD オンプレミスドキュメントのみ）

- ID ディスクのすべての構成をリセットするには、次のコマンドを次の順序で実行します：

```
Repair-AcctIdentity -IdentityAccountName TEST\VM1 -
    PrivilegedUserName TEST\admin1 -PrivilegedUserPassword
    $password -Target IdentityInfo
```

```
Reset-ProvVMDisk ProvisioningSchemeName <name> -VMName <name>
     -Identity
```

4. 「**y**」と入力してアクションを確認します。`-Force`パラメーターを使用して確認プロンプトをスキップすることもできます。例：

```
Reset-ProvVMDisk -ProvisioningSchemeName <name> -VMName <name> -
    Identity -Force
```

5. `Get-ProvVM -ProvisioningSchemeName <name -VMName <name>`を実行して、更新された ID ディスク設定を確認します。ID ディスクの属性（`IdentityDiskId`など）を更新する必要があります。`StorageId`と`IdentityDiskIndex`は変更しないでください。

既存のマシンカタログのキャッシュ構成を変更する

MCSIO を有効にして非永続カタログを作成した後、Set-ProvScheme コマンドを使用して次のパラメーターを変更できます：

- WriteBackCacheMemorySize
- WriteBackCacheDiskSize

この機能は現在、以下に適用されます：

- GCP および Microsoft Azure 環境、および
- MCSIO が有効になっている非永続カタログ

要件

キャッシュ構成を変更するための要件は次のとおりです：

- VDA の最新バージョン（2308 以降）に更新します。
- 既存のマシンカタログのパラメーター`UseWriteBackCache`を有効にします。`UseWriteBackCache`を有効にしてマシンカタログを作成するには、`New-ProvScheme`を使用します。例：


```
New-ProvScheme -ProvisioningSchemeName $CatalogName -
    HostingUnitUid $HostingUnitUid `
-IdentityPoolUid $acctPool.IdentityPoolUid -CleanOnBoot `
-MasterImageVM $MasterImage `
-ServiceOffering $ServiceOffering `
-NetworkMap $NetworkMap `
-SecurityGroup $SecurityGroup `
-UseWriteBackCache -WriteBackCacheDiskSize 8
```

キャッシュ構成を変更する

Set-ProvScheme コマンドを実行します。例:

```
Set-ProvScheme -ProvisioningSchemeName $provScheme.
    ProvisioningSchemeName -WriteBackCacheDisk32 -
    WriteBackCacheMemorySize 128
```

> 注:
>
> - 少なくとも 1GB のキャッシュディスクストレージが必要であるため、`WriteBackCacheDiskSize` の値は 0 より大きい必要があります。
> - `WriteBackCacheMemorySize`の値は、マシンカタログのメモリサイズより小さくなければなりません。
> - これらの変更は、変更後にカタログに追加された新しい VM にのみ影響します。既存の VM はこれらの変更の影響を受けません。

ローカルファイル共有アクセスによる **VDA** の更新をサポート

PowerShell コマンドレットを使用して VDA インストーラーの場所を指定すると、各 VDA が Citrix Managed Azure CDN から新しい VDA インストーラーを取得できるようにするためのネットワーク規則を提供する手間が軽減されます。

PowerShell コマンドレット

New-VusCatalogSchedule および **New-VusMachineUpgrade** コマンドレットに 2 つの新しいオプションのパラメーターが追加され、ローカルファイル共有からインストーラーを使用できるようになりました

- **VdaWorkstationPackageUri** - ワークステーション OS VDA インストーラーへの UNC パスを指定します
- **VdaServerPackageUri** - サーバー OS VDA インストーラーへの UNC パスを指定します

前提条件

- VDA 2311 に含まれる VUS エージェントインストーラー

- VDA Upgrade Agent をバージョン 7.40.0.35 以降にアップグレードします（VDA インストーラーバージョン 2311 以降を使用）
- Virtual Apps and Desktops Remote PowerShell SDK バージョン 7.40 以降（2024 年 1 月 10 日以降にリリース）

ファイル共有権限を設定する方法

VDA インストーラーパッケージを含むネットワーク共有には、ローカルシステム（NT AUTHORITY\SYSTEM プリンシパル）として実行される VDA Upgrade Agent サービスの読み取りアクセス権が必要です。

- ドメイン参加ファイルの共有権限

  VDA マシンがドメイン参加の場合、ローカル システムアカウント（VUA はローカルシステムとして実行されます）は、ネットワーク共有にアクセスするときにコンピューターの資格情報を使用します。

  ドメインコンピューターに読み取りアクセスを許可することで、最小限の権限を設定できます。

  1. ネットワーク上でファイルを共有するユーザーを選択します。
  2. ［共有の詳細設定］をクリックして、［ファイルとプリンターの共有］をオンにします。

- ドメイン非参加ファイルの共有権限

  VDA マシンがドメイン非参加の場合、ローカルシステムアカウント（VUA はローカルシステムとして実行されます）は、ネットワーク共有にアクセスするときに **ANONYMOUS LOGON** を使用します。

  1. 共有フォルダーを選択します。
  2. パスワード保護を無効にします。
     a) フォルダーの ［プロパティ］に移動します。
     b)［ネットワークと共有センター］を選択します。
     c)［パスワード保護共有］をオフにします。
  3. 共有権限を付与するには、［詳細な共有］をクリックします。
     a)［アクセス許可］を選択します。
     b) **ANONYMOUS LOGON** に読み取り共有権限を付与します。
  4. フォルダーの権限を付与するには ［セキュリティ］タブを選択します
     a) 共有フォルダーに権限を追加するには ［編集］をクリックします
     b) **ANONYMOUS LOGON** にフォルダー権限を付与する共有フォルダーを選択します。
  5.［詳細設定］をクリックして、［ファイルとプリンターの共有］をオンにします。
  6. 共有フォルダー名をネットワークアクセスセキュリティポリシーに追加します。

  > 注:
  >
  > 変更をすぐに有効にするには、マシンを再起動してください。

ローカルファイル共有から **VDA** を更新する

1. VDA インストーラーをダウンロードし、共有ファイルに格納します。

   > 注:
   >
   > 仮想アップグレードサービスでは、現在のリリーストラックまたは LTSR トラックのいずれかを選択できます。
   >
   > 例：マシンカタログが現在のリリース（2311）に設定されており、VDA バージョンが 2305 の場合、VDA をバージョン 2311 にアップグレードする必要があります。

   a) 当社 Web サイトのダウンロードページに移動します。
   b) 製品で **Citrix Virtual Apps and Desktops** を選択します。
   c) **Citrix Virtual Apps and Desktops 7 2311, All Editions** を選択します。
   d) 製品 **ISO** に含まれており、個別に展開可能なパッケージも用意されているコンポーネントから VDA インストーラーを選択します。

2. カタログの種類に基づいて、関連する VDA インストーラーを選択します。

   - カタログの種類がマルチセッションの場合は、マルチセッション **OS VDA** インストーラーをダウンロードします
   - カタログの種類がシングルセッションの場合は、シングルセッション **OS VDA** インストーラーをダウンロードします
   - カタログの種類がリモート **PC** アクセスの場合は、シングルセッション **OS** コアサービス **VDA** インストーラーをダウンロードします

> 注:
>
> ファイル共有インストーラーのバージョンは、VUS によってクラウドに公開された最新のインストーラーバージョンと完全に一致する必要があります。

トラブルシューティング

- マシンの状態が「Power State Unknown」の場合、CTX131267を参照してください。
- 継続的に不明な電源状態を示す仮想マシンを修正するには、How to fix VMs that continuously show an unknown power stateを参照してください。

次の手順

特定のクラウドサービスカタログの管理については、次を参照してください:

- AWS カタログの管理
- XenServer カタログの管理

- Google Cloud Platform カタログの管理
- Microsoft Azure カタログの管理
- Microsoft System Center Virtual Machine Manager カタログの管理
- VMware カタログの管理

AWS カタログの管理

August 17, 2024

「マシンカタログの管理」では、マシンカタログを管理するウィザードについて説明します。以下の情報は、AWS クラウド環境に固有の詳細について説明しています。

> 注:
>
> AWS カタログを管理する前に、AWS カタログの作成を完了する必要があります。「AWS カタログの作成」を参照してください。

タグの削除

カタログまたは仮想マシンを作成すると、次のリソースに MCS 作成のタグが作成されます:

- 仮想マシン
- ルートディスクボリューム
- ID ディスクボリューム
- NIC
- ルートディスクイメージ（AMI）
- 起動テンプレート
- AMI またはルートディスクのスナップショット

仮想マシンとマシンカタログを Citrix データベースから削除し、MCS 作成のタグを削除できます。以下を使用できます:

- `Remove-ProvVM`を`ForgetVM`パラメーターとともに使用して、マシンカタログの単一の仮想マシンまたは仮想マシンの一覧から仮想マシンと MCS 作成のタグを削除します。
- `Remove-ProvScheme`を`ForgetVM`パラメーターとともに使用して、Citrix データベースからマシンカタログを削除し、マシンカタログからタグを削除します。

この機能は、永続的な仮想マシンにのみ適用されます。

これを行うには、以下の手順に従います:

1. **PowerShell** ウィンドウを開きます。

2. `asnp citrix*`を実行し、Citrix 固有の PowerShell モジュールをロードします。
3. 仮想マシンを削除する前に、仮想マシンのロックを解除します。例:

```
1 Unlock-ProvVM -ProvisioningSchemeName "<name>" -VMID "<id"
```

4. 次のコマンドのいずれかを実行して、リソースから仮想マシン、マシンカタログ、および MCS 作成のタグを削除します。

   - `Remove-ProvVM`を`ForgetVM`とともに実行して、Citrix データベースから仮想マシンを削除し、仮想マシンからタグを削除します。例:

   ```
   1 Remove-ProvVM -ProvisioningSchemeName "<name>" -VMName "<name
       >" -ForgetVM
   ```

   - `Remove-ProvScheme`を実行して、Citrix データベースからマシンカタログを削除し、マシンカタログからリソースを削除します。例:

   ```
   1 Run Remove-ProvScheme -ProvisioningSchemeName "<name>" -
       ForgetVM
   ```

5. 仮想マシンが Delivery Controller から削除されていて、ハイパーバイザーからは削除されていないことを確認します。

   a) `Get-ProvVM -ProvisioningSchemeName "<name>"-VMName "<name>"`を実行します。これによって何も返されないことが必要です。

   b) AWS EC2 コンソールに移動します。仮想マシンが表示され、タグは削除されている必要があります。次のリソースのタグが削除されます:

   - 仮想マシン
   - ルートディスクボリューム
   - ID ディスクボリューム
   - NIC

6. マシンカタログを削除する場合は、カタログが Delivery Controller から削除されていることを確認してください。

   a) `Get-ProvScheme -ProvisioningSchemeName "forgetvmdemo"`を実行します。これによって、エラーが返される必要があります。

   b) AWS EC2 コンソールで、次のリソースが削除されていることを確認します。

   - ルートディスクイメージ（AMI）
   - 起動テンプレート
   - AMI またはルートディスクのスナップショット

MCS によって作成されたリソースの特定

以下は、MCS がリソースに追加するタグです。表のタグは、「”キー”:”値”」として表示されます。

リソース名	タグ
ID ディスク	“Name”: “VMName_IdentityDisk” “XdConfig”: “XdProvisioned=true” “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx”
イメージ	“XdConfig”: “XdProvisioned=true” “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx”
NIC	“Description”: “XD NIC” “XdConfig”: “XdProvisioned=true” “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx”
OS ディスク	“Name”: “VMName_rootDisk” “XdConfig”: “XdProvisioned=True” “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” [when AwsCaptureInstanceProperties = true] “Citrix Resource”: “” [when AwsCaptureInstanceProperties = true and AwsOperationalResourcesTagging = true] “CitrixOperationalResource”: “”
PrepVM	“Name”: “Preparation - CatalogName - xxxxxxxxxx” “XdConfig”: “XdProvisioned=true” “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” [when AwsCaptureInstanceProperties = true] “Citrix Resource”: “” [when AwsCaptureInstanceProperties = true and AwsOperationalResourcesTagging = true] “CitrixOperationalResource”: “”
公開されたスナップショット	“XdConfig”: “XdProvisioned=true”

リソース名	タグ
テンプレート	ボリュームワーカー AMI のスナップショットでない場合は、”CitrixProvisioningSchemeId”：“xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” [when AwsCaptureInstanceProperties = true] “XdConfig”： “XdProvisioned=true” [when AwsCaptureInstanceProperties = true] “CitrixProvisioningSchemeId”：“xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” [when AwsCaptureInstanceProperties = true] “CitrixResource”： “” [when AwsCaptureInstanceProperties = true and AwsOperationalResourcesTagging = true] “CitrixOperationalResource”： “”
カタログ内の VM	“XdConfig”： “XdProvisioned=true” “CitrixProvisioningSchemeId”：“xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” [when AwsCaptureInstanceProperties = true] “CitrixResource”： “” [when AwsCaptureInstanceProperties = true] “aws:ec2launchtemplate:id”:” lt-xxxx” [when AwsCaptureInstanceProperties = true] “aws:ec2launchtemplate:version”： “n” [when AwsCaptureInstanceProperties = true and AwsOperationalResourcesTagging = true] “CitrixOperationalResource”： “”
ボリュームワーカー AMI	“XdConfig”： “XdProvisioned=true”
ボリュームワーカーのブートストラッパー	“Name”： “XenDesktop Temp” “XdConfig”： “XdProvisioned=true” “CitrixProvisioningSchemeId”：“xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” [when AwsCaptureInstanceProperties = true and AwsOperationalResourcesTagging = true] “CitrixVolumeWorkerBootstrapper”： “”
ボリュームワーカーのインスタンス	“Name”：“Citrix.XD.Volumeworker-xxxx-xx-xx-xx-xxxx” “XdConfig”： “XdProvisioned=true”

追加情報

- 接続とリソースの作成と管理
- AWS への接続
- マシンカタログの作成
- AWS カタログの作成
- マシンカタログの管理

XenServer カタログの管理

August 17, 2024

「マシンカタログの管理」では、マシンカタログを管理するウィザードについて説明します。以下の情報は、XenServer 仮想化環境に固有の詳細について説明しています。

> 注:
>
> XenServer カタログを管理するには、その前に XenServer カタログの作成を完了しておく必要があります。「XenServer カタログの作成」を参照してください。

MCS によって作成されたリソースの特定

以下は、MCS がリソースに追加するタグです。表のタグは、「”キー”:”値”」として表示されます。

リソース名	タグ
各ネットワークまたはローカルストレージで公開された基本ディスクとそのコピー	“CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx”
ID ディスク	“CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx”
OS ディスク	“CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx”
VM の準備	“CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx”
カタログ内の VM	“CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx”
WBC ディスク	“CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx”

追加情報

- 接続とリソースの作成と管理
- XenServer への接続
- マシンカタログの作成
- XenServer カタログの作成
- マシンカタログの管理

Google Cloud Platform カタログの管理

August 17, 2024

「マシンカタログの管理」では、マシンカタログを管理するウィザードについて説明します。以下の情報は、Google クラウド環境に固有の詳細について説明しています。

> 注:
>
> Google Cloud Platform カタログを管理する前に、Google Cloud Platform カタログの作成を完了する必要があります。「Google Cloud Platform カタログの作成」を参照してください。

マシンカタログの管理

カタログへのマシンの追加、マシンの更新、更新のロールバックを実行するには、「マシンカタログの管理」を参照してください。

電源管理

Citrix DaaS を使用すると、Google Cloud マシンの電源管理が可能になります。左側のペインの ［検索］ノードを使用して、電源管理するマシンを検索します。次の電源操作が使用可能です:

- 削除
- 開始
- 再起動
- 強制再起動
- シャットダウン
- 強制シャットダウン
- デリバリーグループに追加
- タグの管理
- メンテナンスモードをオンにする

Autoscale を使用して Google Cloud マシンの電源を管理することもできます。これを行うには、Google Cloud マシンをデリバリーグループに追加し、そのデリバリーグループの Autoscale を有効にします。Autoscale について詳しくは、「Autoscale」を参照してください。

PowerShell を使用してプロビジョニングされたマシンを更新

Set-ProvSchemeコマンドは、プロビジョニングスキームを変更します。ただし、既存のマシンには影響しません。PowerShell コマンドのSet-ProvVMUpdateTimeWindowを使用して、現在のプロビジョニングスキームを既存の永続的マシンや非永続的マシン、またはマシンのセットに適用できるようになりました。現在 GCP では、マシンプロファイルがこの機能でサポートされているプロパティの更新です。

以下を更新できます:

- 単一の VM
- プロビジョニングスキーム ID に関連付けられている特定の VM またはすべての既存の VM のリスト
- プロビジョニングスキーム名に関連付けられている特定の VM またはすべての既存の VM のリスト

既存の VM を更新するには:

1. 既存のマシンの構成を確認します。たとえば、

```
Get-ProvScheme | select ProvisioningSchemeName,
    ProvisioningSchemeVersion
```

2. プロビジョニングスキームを更新します。たとえば、

```
`Set-ProvScheme  - ProvisioningSchemeName "my-catalog"  -
    MachineProfile "XDHyp:\HostingUnits<hosting-unit>\
    machineprofileinstance.vm"
```

3. VM の現在のプロパティが現在のプロビジョニングスキームと一致するかどうか、および VM に保留中の更新アクションがあるかどうかを確認します。たとえば、

```
Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
    ProvisioningSchemeVersion
```

   特定のバージョンのマシンを見つけることもできます。たとえば、

```
Get-ProvVM -Filter "ProvisioningSchemeVersion -eq 1" | select
    VMName, ProvisioningSchemeVersion
```

4. 既存のマシンを更新します。

   - すべての既存のマシンを更新するには:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
    -StartsNow -DurationInMinutes -1
```


- 特定のマシンのリストを更新するには:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
    -VMName <List-Of-Vm-Names> -StartsNow -DurationInMinutes
   -1
```

- Get-ProvVMの出力に基づいてマシンを更新するには:

```
Get-ProvVM -ProvisioningSchemeName "my-catalog" | Set-
   ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
   -StartsNow -DurationInMinutes -1
```

5. スケジュール済みの更新があるマシンを見つけます。たとえば、

```
Get-ProvVM -Filter "ProvisioningSchemeUpdateAfter" | select VMName
   , ProvisioningSchemeUpdateAfter
```

6. マシンを再起動します。次回の電源投入時に、プロパティの変更が既存のマシンに適用されます。次のコマンドを使用して、更新されたステータスを確認できます:

```
Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
   ProvisioningSchemeVersion
```

既存のカタログのディスクに関連したカスタムプロパティを変更する

既存のカタログおよびカタログの既存の VM で次のディスク関連のカスタムプロパティを変更できます:

- PersistOSDisk
- PersistWBC
- StorageType
- IdentityDiskStorageType
- WbcDiskStorageType

> 注:
>
> - StorageTypeプロパティは OS ディスク用です
> - PersistOsDiskプロパティは、ライトバックキャッシュを有効にした非永続カタログに対してのみ設定できます

この実装により、カタログを作成した後でも、異なるディスクに対して異なるストレージの種類を選択できるため、さまざまなストレージの種類を使用することと価格のバランスを取ることができます。

これを行うには、PowerShell コマンドSet-ProvSchemeおよびSet-ProvVMUpdateTimeWindowを使用します:

1. **PowerShell** ウィンドウを開きます。

2. `asnp citrix*`を実行します。
3. `Get-ProvVM -VMName <VM name>`を実行してカスタムプロパティを取得します。
4. カスタムプロパティ文字列を変更します:

   a) カスタムプロパティをメモ帳にコピーし、カスタムプロパティを変更します。

   b) **PowerShell** ウィンドウで、変更したカスタムプロパティをメモ帳から貼り付け、変更したカスタムプロパティに変数を割り当てます。例:

```
$cp =  '<CustomProperties xmlns=http://schemas.citrix.com
   /2014/xd/machinecreation xmlns:xsi="http://www.w3.org/2001/
   XMLSchema-instance">
<Property xsi:type="StringProperty" Name="CatalogZones" Value
   ="" />
<Property xsi:type="StringProperty" Name="PersistWBC" Value="
   true" />
<Property xsi:type="StringProperty" Name="PersistOSDisk" Value
   ="true" />
<Property xsi:type="StringProperty" Name="WBCDiskStorageType"
   Value="pd-standard" />
<Property xsi:type="StringProperty" Name="StorageType" Value="
   pd-standard" />
</CustomProperties>'
```

5. 既存のカタログを更新します。例:

```
Set-ProvScheme -ProvisioningSchemeName <yourCatalogName> -
   CustomProperties $cp
```

6. 既存の VM を更新します。例:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog -
   VMName <List-Of-Vm-Names> -StartsNow -DurationInMinutes -1
```

7. VM を再起動します。次回の電源投入時に、カスタムプロパティの変更が既存の VM に適用されます。

意図しないマシンの削除からの保護

Citrix DaaS を使用すると、Google Cloud 上の MCS リソースを保護し、誤って削除されないようにすることができます。`deletionProtection`フラグを TRUE に設定して、プロビジョニングされた VM を構成します。

デフォルトでは、MCS または Google Cloud プラグインを介してプロビジョニングされた VM は、InstanceProtection が有効な状態で作成されます。この実装は、永続カタログと非永続カタログの両方に適用できます。非永続カタログは、インスタンスがテンプレートから再作成されるときに更新されます。既存の永続マシンの場合、Google Cloud コンソールでフラグを設定できます。フラグの設定について詳しくは、Google のドキュメントのサイトを参照してください。永続カタログに追加された新しいマシンは、`deletionProtection`が有効な状態で作成されます。

deletionProtectionフラグを設定した VM インスタンスを削除しようとすると、その要求は失敗します。ただし、権限のcompute.instances.setDeletionProtectionが付与されているか、IAM の **Compute Admin** の役割が割り当てられている場合は、リソースの削除を許可するフラグをリセットできます。

MCS によって作成されたリソースの特定

以下は、MCS がリソースに追加するタグです。表のタグは、「”キー”:”値”」として表示されます。

リソース名	タグ
ID ディスク	“CitrixResource”： “internal” “CitrixProvisioningSchemeId”： “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx”
イメージ	“CitrixResource”： “internal” “CitrixProvisioningSchemeId”： “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx”
OS ディスク	“CitrixResource”： “internal” “CitrixProvisioningSchemeId”： “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx”
PrepVM	“CitrixResource”： “internal” “CitrixProvisioningSchemeId”： “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx”
公開されたスナップショット	“CitrixResource”： “internal”
ストレージバケット	“Citrixresource”： “internal”
テンプレート	“CitrixResource”： “internal”
カタログ内の VM	“CitrixResource”： “internal” “CitrixProvisioningSchemeId”： “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx”．プラグインは、MCS でプロビジョニングされた VM に次のラベルも追加します:”citrix-provisioning-scheme-id”： “provSchemeId”。このラベルは、GCP コンソールでカタログによるフィルタリングに使用できます。
WBC ディスク	“CitrixResource”： “internal” CitrixProvisioningSchemeId”： “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx”

> 注:
>
> MCS によって作成されたリソースとして識別するために **CitrixResource** タグが追加されている場合、VM は Citrix インベントリに表示されません。タグを削除するか名前を変更すると、表示できるようになります。

追加情報

- 接続とリソースの作成と管理
- Google クラウド環境への接続
- マシンカタログの作成
- Google Cloud Platform カタログの作成
- マシンカタログの管理

HPE Moonshot カタログを管理する

August 17, 2024

「マシンカタログの管理」では、マシンカタログを管理するウィザードについて説明します。以下の情報は、HPE Moonshot カタログに固有の詳細について説明しています。

> 注:
>
> HPE Moonshot カタログを管理する前に、HPE Moonshot カタログの作成を完了する必要があります。

電源管理

Citrix Virtual Apps and Desktops を使用すると、HPE Moonshot マシンの電源管理を行うことができます。ナビゲーションペインの ［検索］ノードを使用して、電源管理するマシンを検索します。次の電源操作が使用可能です:

- 開始
- シャットダウン
- 強制シャットダウン
- 再起動
- リセット

> 注:
>
> 電源操作の ［一時停止］および ［再開］はサポートされていません。

追加情報

- 接続とリソースの作成と管理
- HPE Moonshot への接続
- マシンカタログの作成
- HPE Moonshot マシンカタログの作成
- マシンカタログの管理

Microsoft Azure カタログの管理

August 17, 2024

> 注:
>
> 2023 年 7 月より、Microsoft は Azure Active Directory（Azure AD）の名前を Microsoft Entra ID に変更しました。このドキュメントでは、Azure Active Directory、Azure AD、または AAD への言及はすべて、Microsoft Entra ID を意味することになります。

「マシンカタログの管理」では、マシンカタログを管理するウィザードについて説明します。以下の情報は、Microsoft Azure Resource Manager クラウド環境に固有の詳細について説明しています。

> 注:
>
> Microsoft Azure カタログを管理する前に、Microsoft Azure カタログの作成を完了する必要があります。「Microsoft Azure カタログの作成」を参照してください。

仮想マシンのシャットダウン時にストレージの種類をダウングレードする

仮想マシンのシャットダウン時に管理対象ディスクのストレージの種類をダウングレードすると、ストレージコストを節約できます。これを行うには、カスタムプロパティ`StorageTypeAtShutdown`を使用します。

仮想マシンをシャットダウンすると、ディスクのストレージの種類が（カスタムプロパティ`StorageTypeAtShutdown`で指定されたものに）ダウングレードされます。仮想マシンの電源をオンにすると、ストレージの種類が（カスタムプロパティ`StorageType`またはカスタムプロパティ`WBCDiskStorageType`で指定された）元に戻ります。

> 重要:
>
> ディスクは、仮想マシンの電源を少なくとも 1 回オンにするまで存在しません。このため、仮想マシンの初回電源投入時にストレージの種類を変更することはできません。

要件

- 管理対象ディスクに適用できます。これは、カスタムプロパティ`UseManagedDisks`を true に設定することを意味します。
- 永続 OS ディスクがある永続カタログおよび非永続カタログに適用できます。これは、カスタムプロパティ`persistOsDisk`を true に設定することを意味します。
- 永続 WBC ディスクがある非永続カタログに適用できます。これは、カスタムプロパティ`persistWBC`を true に設定することを意味します。

制限事項

- Microsoft によると、ディスクの種類を変更できるのは 1 日に 2 回のみです。Microsoft ドキュメントを参照してください。Citrix に関しては、`StorageType`の更新は VM の開始または割り当て解除操作があるたびに行われます。したがって、VM ごとの電源操作の数を 1 日あたり 2 回に制限します。たとえば、朝に 1 回の電源操作で VM を起動し、夕方にもう 1 回の電源操作で VM の割り当てを解除します。

ストレージの種類をダウングレードするには

手順に進む前に、「要件」と「制限事項」を参照してください。

1. カスタムプロパティ`StorageTypeAtShutdown`を追加し、値を Standard_LRS（HDD）に設定し、`New-ProvScheme`を使用してカタログを作成します。PowerShell を使用してカタログを作成する方法については、「https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/」を参照してください。

   > 注:
   >
   > `StorageTypeAtShutdown`の値が空または Standard_LRS（HDD）以外の場合、操作は失敗します。

   永続カタログの作成中にカスタムプロパティを設定する例:

```
$customProperties='<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/machinecreation"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />
<Property xsi:type="StringProperty" Name="StorageType" Value="Premium_LRS" />
<Property xsi:type="StringProperty" Name="ResourceGroups" Value="" />
<Property xsi:type="StringProperty" Name="LicenseType" Value="Windows_Client" />
<Property xsi:type="StringProperty" Name="SchemaVersion" Value="2" />
```



```
<Property xsi:type="StringProperty" Name="OsType" Value="Windows"
    />
<Property xsi:type="StringProperty" Name="StorageTypeAtShutdown"
    Value="Standard_LRS" />
</CustomProperties>'
```

非永続カタログの作成中にカスタムプロパティを設定する例:

```
$customProperties='<CustomProperties xmlns="http://schemas.citrix.
    com/2014/xd/machinecreation"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="
    true" />
<Property xsi:type="StringProperty" Name="StorageType" Value="
    Premium_LRS" />
<Property xsi:type="StringProperty" Name="WbcDiskStorageType"
    Value="Standard_SSD_LRS" />
<Property xsi:type="StringProperty" Name="ResourceGroups" Value=""
    />
<Property xsi:type="StringProperty" Name="LicenseType" Value="
    Windows_Client" />
<Property xsi:type="StringProperty" Name="SchemaVersion" Value="2"
    />
<Property xsi:type="StringProperty" Name="OsType" Value="Windows"
    />
<Property xsi:type="BooleanProperty" Name="persistWBC" Value=true
    />
<Property xsi:type="BooleanProperty" Name="persistOsDisk" Value=
    true />
<Property xsi:type="StringProperty" Name="StorageTypeAtShutdown"
    Value="Standard_LRS" />
</CustomProperties>'
```

> 注:
>
> マシンプロファイルを使用する場合、カスタムプロパティは`MachineProfile`で定義されたプロパティよりも優先されます。

2. 仮想マシンをシャットダウンし、Azure Portal で仮想マシンのストレージの種類を確認します。ディスクのストレージの種類がカスタムプロパティ`StorageTypeAtShutdown`で指定されたものにダウングレードされます。
3. 仮想マシンの電源を入れます。ディスクのストレージの種類は、以下に記載されているストレージの種類に切り替わります:
   - OS ディスクのカスタムプロパティ`StorageType`
   - `CustomProperties`で指定した場合のみ WBC ディスクのカスタムプロパティ`WBCDiskStorageType`。それ以外の場合は、`StorageType`に記載されているストレージの種類に切り替わります。

StorageTypeAtShutdown を既存のカタログに適用する

手順に進む前に、「要件」と「制限事項」を参照してください。

`Set-ProvScheme`を使用して、既存のカタログに仮想マシンを追加します。この機能は、`Set-ProvScheme`の実行後に追加された新しい仮想マシンに適用されます。既存のマシンは影響を受けません。

仮想マシンを既存のカタログに追加するときにカスタムプロパティを設定する例:

```
$customProperties='<CustomProperties xmlns="http://schemas.citrix.com
    /2014/xd/machinecreation"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true"
     />
<Property xsi:type="StringProperty" Name="StorageType" Value="
    Premium_LRS" />
<Property xsi:type="StringProperty" Name="WbcDiskStorageType" Value="
    Standard_SSD_LRS" />
<Property xsi:type="StringProperty" Name="ResourceGroups" Value="" />
<Property xsi:type="StringProperty" Name="LicenseType" Value="
    Windows_Client" />
<Property xsi:type="StringProperty" Name="SchemaVersion" Value="2" />
<Property xsi:type="StringProperty" Name="OsType" Value="Windows" />
<Property xsi:type="BooleanProperty" Name="persistWBC" Value=true />
<Property xsi:type="BooleanProperty" Name="persistOsDisk" Value=true />
<Property xsi:type="StringProperty" Name="StorageTypeAtShutdown" Value
    ="Standard_LRS" />
</CustomProperties>'

$ProvScheme = Get-Provscheme -ProvisioningSchemeName $CatalogName

Set-ProvScheme -ProvisioningSchemeName $ProvScheme.
    ProvisioningSchemeName -CustomProperties $customProperties
```

シャットダウン時に既存の **VM** のストレージの種類を下位レベルに変更する

手順に進む前に、「要件」と「制限事項」を参照してください。

VM のシャットダウン時に、既存の VM のストレージの種類を下位レベルに変更することで、ストレージコストを節約できます。これを行うには、カスタムプロパティ`StorageTypeAtShutdown`を使用します。

VM のシャットダウン時に、カタログ内の既存のマシンのストレージの種類を下位レベルに変更するには、次の手順を実行します:

1. PowerShell ウィンドウを開きます。
2. `asnp citrix*`を実行し、Citrix 固有の PowerShell モジュールをロードします。
3. `Get-Provscheme -ProvisioningSchemeName $CatalogName`を実行します。
4. カスタムプロパティ文字列を変更します。


```
$customProperties = '<CustomProperties xmlns="http://schemas.
    citrix.com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.
    org/2001/XMLSchema-instance">
<Property xsi:type="StringProperty" Name="StorageTypeAtShutdown"
    Value="Standard_LRS" />
</CustomProperties>'
```

5. 既存のカタログのプロビジョニングスキームを更新します。この更新は、Set-ProvSchemeの実行後に追加された新しい仮想マシンに適用されます。

```
Set-ProvScheme -ProvisioningSchemeName $CatalogName -
    CustomProperties $customProperties
```

6. 既存の VM を更新してStorageTypeAtShutdownを有効にします。

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName $CatalogName -
    StartsNow -DurationInMinutes -1
```

7. 次にマシンの電源を入れると、マシンのStorageTypeAtShutdownプロパティが更新されます。ストレージの種類は、次回のシャットダウン時に変更されます。

8. 次のコマンドを実行して、カタログ内の各 VM のStorageTypeAtShutdown値を表示します:

```
Get-ProvVM -ProvisioningSchemeName <catalog-name> | foreach {
  $vmName = $_.VMName; $storageTypeAtShutdown = ($_.CustomVmData |
      ConvertFrom-Json).StorageTypeAtShutdown.
    DiskStorageAccountType; return New-Object psobject -Property
    @{
  "VMName" = $vmName; "StorageTypeAtShutdown" =
    $storageTypeAtShutdown  }
 }
```

プロビジョニングされたマシンを現在のプロビジョニングスキームの状態に更新する

Set-ProvSchemeコマンドは、プロビジョニングスキームを変更します。ただし、既存のマシンには影響しません。PowerShell コマンドのSet-ProvVMUpdateTimeWindowを使用して、現在のプロビジョニングスキームを既存の永続的マシンや非永続的マシン、またはマシンのセットに適用できます。既存の MCS プロビジョニング済みマシンの構成の更新について、時間枠をスケジュール設定できます。スケジュールされた時間枠内で電源をオンまたは再起動すると、スケジュールされたプロビジョニングスキームの更新がマシンに適用されます。現在、Azure では、ServiceOffering、MachineProfileおよび次のカスタムプロパティを更新できます:

- StorageType
- WBCDiskStorageType
- IdentityDiskStorageType
- LicenseType
- DedicatedHostGroupId

- PersistWBC
- PersistOsDisk
- PersistVm

> 注:
>
> - Azure 環境では、管理対象ディスクを使用してカタログのStorageType、WBCDiskStorageType、およびIdentityDiskStorageTypeのカスタムプロパティのみを更新できます。
> - Set-ProvVMUpdateTimeWindowを 2 回実行すると、最新のコマンドが有効になります。

以下を更新できます:

- 単一の VM
- プロビジョニングスキーム ID に関連付けられている特定の VM またはすべての既存の VM のリスト
- プロビジョニングスキーム名（マシンカタログ名）に関連付けられている特定の VM またはすべての既存の VM のリスト

プロビジョニングスキームに次の変更を加えた後、Azure の永続カタログの VM インスタンスが再作成されます:

- MachineProfileを変更
- LicenseTypeを削除
- DedicatedHostGroupIdを削除

> 注:
>
> 既存マシンの OS ディスクとそのすべてのデータはそのまま残り、新しい仮想マシンはディスクに接続されます。

既存の VM を更新する前に、以下を実行します:

1. 既存のマシンの構成を確認します。たとえば、

```
Get-ProvScheme | select ProvisioningSchemeName,
    ProvisioningSchemeVersion
```

2. プロビジョニングスキームを更新します。たとえば、

   - VM をマシンプロファイルの入力に使用する場合:

```
Set-ProvScheme -ProvisioningSchemeName "my-catalog" -
    MachineProfile "XDHyp:\HostingUnits<hosting-unit>\
    machineprofile.folder<resource-group>.resourcegroup<
    virtual-machine>.vm"
```

   - テンプレートスペックをマシンプロファイルの入力に使用する場合:

```
Set-ProvScheme -ProvisioningSchemeName "my-catalog"
```



```
2   -MachineProfile "XDHyp:\HostingUnits<hosting-unit>\
        machineprofile.folder<resource-group>.resourcegroup<
        template-spec>.templatespec<template-spec-version>.
        templatespecversion"
3   -ServiceOffering "XDHyp:\HostingUnits<hosting-unit>\
        serviceoffering.folder<service-offering>.serviceoffering"
```

- サービスオファリングだけを使用する場合:

```
1   Set-ProvScheme -ProvisioningSchemeName "my-catalog" -
        ServiceOffering "XDHyp:\HostingUnits<hosting-unit>\
        serviceoffering.folder<service-offering>.serviceoffering"
```

3. VM の現在のプロパティが現在のプロビジョニングスキームと一致するかどうか、および VM に保留中の更新アクションがあるかどうかを確認します。たとえば、

```
1  Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
       ProvisioningSchemeVersion
```

特定のバージョンのマシンを見つけることもできます。たとえば、

```
1  Get-ProvVM -Filter "ProvisioningSchemeVersion -eq 1" | select
       VMName, ProvisioningSchemeVersion
```

既存のマシンの更新を次回の再起動時に適用するように要求するには、次の手順を実行します:

1. 次のコマンドを実行して既存のマシンを更新し、次回の再起動時に更新を適用します。

   - すべての既存のマシンを更新するには、たとえば、

```
1   Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
        -StartsNow -DurationInMinutes -1
```

   - 特定のマシンのリストを更新するには: たとえば、

```
1   Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
        -VMName <List-Of-Vm-Names> -StartsNow -DurationInMinutes
       -1
```

   - Get-ProvVM の出力に基づいてマシンを更新するには、たとえば、

```
1   Get-ProvVM -ProvisioningSchemeName "my-catalog" | Set-
       ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
       -StartsNow -DurationInMinutes -1
```

> 注:
>
> - StartsNowは、スケジュールの開始時刻が現在時刻であることを指定します。
> - 負の数（-1 など）のDurationInMinutesは、スケジュールの期間に上限がないことを示します。

2. スケジュール済みの更新があるマシンを見つけます。たとえば、

```
Get-ProvVM -Filter "ProvisioningSchemeUpdateAfter" | select VMName
    , ProvisioningSchemeUpdateAfter
```

3. マシンを再起動します。次回の電源投入時に、プロパティの変更が既存のマシンに適用されます。次のコマンドを使用して、更新されたステータスを確認できます。たとえば、

```
Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
    ProvisioningSchemeVersion
```

次回、スケジュールされた時間帯に VM が起動したとき、最新のプロビジョニング設定に更新するようにスケジュールします:

1. 次のコマンドを実行します:

   - 開始時刻を現在時刻として更新をスケジュールするには

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
    -VMName vm1 -StartsNow -DurationInMinutes 120
```

   - 週末に更新をスケジュールするには

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName “ my-
    catalog “ -VMName “vm1” -StartTimeInUTC “10/15/2022
    9:00am” -DurationInMinutes (New - TimeSpan - Days 2).
    TotalMinutes
```

   > 注:
   >
   > - VMNameはオプションです。指定しない場合、更新はカタログ全体に対してスケジュールされます。
   > - StartTimeInUTCの代わりにStartsNowを使用して、スケジュールの開始時刻が現在時刻であることを指定します。
   > - DurationInMinutesはオプションです。デフォルトは 120 分です。負の数（-1 など）は、スケジュールの時間枠に上限がないことを示します。

2. 更新状況を確認します。

```
Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
    ProvisioningSchemeUpdateUntil, ProvisioningSchemeVersion
```

3. VM の電源を入れます。スケジュールされた時間枠の後にマシンの電源をオンにした場合、構成の更新は適用されません。スケジュールされた時間枠内にマシンの電源を入れた場合、

   - マシンの電源がオフになっていて、
     - マシンの電源をオンにしない場合、構成の更新は適用されません
     - マシンの電源をオンにする場合、構成の更新は適用されます

- マシンの電源がオンになっていて、
  - マシンを再起動しない場合、構成の更新は適用されません
  - マシンを再起動する場合、構成の更新は適用されます

構成の更新をキャンセルするには、以下の手順を実行します:

単一の VM、複数の VM、またはカタログ全体の構成の更新をキャンセルすることもできます。構成の更新をキャンセルするには:

1. `Clear-ProvVMUpdateTimeWindow`を実行します。例:
   - 単一の VM に対してスケジュールされた構成の更新をキャンセルするには:

```
Clear-ProvVMUpdateTimeWindow -ProvisioningSchemeName “my-catalog” -VMName “vm1”
```

   - 複数の VM に対してスケジュールされた構成の更新をキャンセルするには:

```
Clear-ProvVMUpdateTimeWindow -ProvisioningSchemeName "my-catalog" -VMName "vm1","vm2"
```

> 注:
>
> VM は同じカタログにある必要があります。

個別の **VM** のプロパティを更新する

PowerShell コマンド`Set-ProvVM`を使用して、永続的な MCS マシンカタログ内の個別の VM のプロパティを更新できるようになりました。ただし、更新はすぐには適用されません。更新を適用するには、PowerShell コマンド`Set-ProvVMUpdateTimeWindow`を使用して時間枠を設定する必要があります。

この実装により、マシンカタログ全体を更新することなく、個別の VM を効率的に管理できます。現在、この機能は Azure 環境にのみ適用されます。

以下は、現在更新できるプロパティです:

- `CustomProperties`
- `ServiceOffering`
- `MachineProfile`

この機能を使用することで、以下のことを実行できます:

- VM のプロパティを更新する
- マシンカタログが更新された後も、VM 上で更新されたプロパティを保持する
- VM に適用された構成の更新を元に戻す

VM のプロパティを更新する前に、以下を実行します:

1. **PowerShell** ウィンドウを開きます。
2. `asnp citrix*`を実行し、Citrix 固有の PowerShell モジュールをロードします。
3. 既存のマシンカタログの構成を確認します。例:

```
Get-ProvScheme -ProvisioningSchemeName AzureCatalog
```

4. 更新を適用する VM の構成を確認します。例:

```
Get-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
```

VM のプロパティを更新する

VM 上のプロパティを更新するには、次の手順を実行します:

1. 更新を適用する VM をオフにします。
2. VM のプロパティを更新します。たとえば、カスタムプロパティの VM のストレージの種類 (`StorageType`) を更新する場合は、次のコマンドを実行します:

```
Set-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1 -
    CustomProperties "...<Property Name='StorageType' Value='
    Premium_LRS' />..."
```

マシンカタログ内の 2 台の VM のプロパティを同時に更新できます。例:

```
Set-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1 -
    CustomProperties "...<Property Name='StorageType' Value='
    Premium_LRS' />..."
```

```
Set-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine2 -
    CustomProperties "...<Property Name='StorageType' Value='
    StandardSSD_LRS' />..."
```

> 注:
>
> 更新はすぐには適用されません。

3. 更新するように指定されたプロパティの一覧と構成バージョンを取得します。例:

```
Get-ProvVMConfiguration -ProvisioningSchemeName AzureCatalog -
    VMName machine1
```

`Version`のプロパティ値と更新するプロパティ（この場合は`StorageType`）を確認します。

4. 構成バージョンを確認します。例:

```
Get-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
```


ProvVMConfigurationVersionのプロパティ値を確認します。更新はまだ適用されていません。VM はまだ古い構成のままです。

5. スケジュールされた更新を要求します。例:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName AzureCatalog -
    StartsNow -DurationInMinutes -1
```

スケジュールされた更新について詳しくは、「プロビジョニングされたマシンを現在のプロビジョニングスキームの状態に更新する」を参照してください。

> 注:
>
> 保留中のプロビジョニングスキームの更新も適用されます。

6. 仮想マシンを再起動します。例:

```
New-BrokerHostingPowerAction -MachineName machine1 -Action TurnOn
```

7. 構成バージョンを確認します。例:

```
Get-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
```

ProvVMConfigurationVersionのプロパティ値を確認します。更新が適用されました。VM には新しい構成が適用されました。

8. VM にさらに構成の更新を適用するには、VM をオフにして、手順を繰り返します。

マシンカタログが更新された後も、**VM** 上で更新されたプロパティを保持する

VM 上の更新されたプロパティを保持するには、次の手順を実行します:

1. 更新を適用する VM をオフにします。
2. マシンカタログを更新します。たとえば、VM のサイズ（ServiceOffering）とストレージの種類（StorageType）を更新する場合は、次のコマンドを実行します:

```
Set-ProvScheme -ProvisioningSchemeName AzureCatalog -
    ServiceOffering Standard_E4_v3 -CustomProperties "...<Property
    Name='StorageType' Value='StandardSSD_LRS' />..."
```

3. マシンカタログの構成の詳細を取得します。例:

```
Get-ProvScheme -ProvisioningSchemeName AzureCatalog
```

ProvisioningSchemeVersionが 1 つ増えます。VM のサイズとストレージの種類も更新されます。

4. VM のプロパティを更新します。たとえば、マシンプロファイルを VM に提供します。


```
Set-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1 -
    MachineProfile "XDHyp:\HostingUnits<hosting-unit>\
    machineprofile.folder<resource-group>.resourcegroup<template-
    spec>.templatespec<template-spec-version>.templatespecversion"
```

> 注:
>
> マシンプロファイル入力にはタグがあり、別の VM サイズ（ServiceOffering）が指定されています。

5. VM 上の構成の更新をマシンカタログの更新とマージした後に VM のプロパティの一覧を取得します。例:

```
Get-ProvVMConfigurationResultantSet -ProvisioningSchemeName
    AzureCatalog -VMName machine1
```

> 注:
>
> VM 上の更新はすべて、マシンカタログ上で行われた更新を上書きします。

6. VM のスケジュールされた更新を要求します。例:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName AzureCatalog -
    VMName machine1 -StartsNow -DurationInMinutes -1
```

7. 仮想マシンを再起動します。例:

```
New-BrokerHostingPowerAction -MachineName machine1 -Action TurnOn
```

VM は、マシンプロファイルに基づいて更新された VM サイズを維持します。マシンプロファイルで指定されたタグ値も VM に適用されます。ただし、ストレージの種類は最新のプロビジョニングスキームに基づきます。

8. VM の構成バージョンを取得します。例:

```
Get-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
```

ProvisioningSchemeVersionとProvVMConfigurationVersionには最新バージョンが表示されるようになりました。

VM に適用された構成の更新を元に戻す

1. VM に更新を適用した後、VM をオフにします。
2. 次のコマンドを実行して、VM に適用されている更新を削除します。例:

```
Set-ProvVM -RevertToProvSchemeConfiguration -
    ProvisioningSchemeName AzureCatalog -VMName machine1
```

3. VM のスケジュールされた更新を要求します。例:


```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName AzureCatalog -
    VMName machine1 -StartsNow -DurationInMinutes -1
```

4. 仮想マシンを再起動します。例:

```
New-BrokerHostingPowerAction -MachineName machine1 -Action TurnOn
```

5. VM の構成バージョンを確認します。例:

```
Get-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
```

`ProvVMConfigurationVersion`の値は、マシンカタログの構成バージョンを表示するようになりました。

ディスク暗号化を変更する

Azure 仮想化環境でディスク暗号化を変更し、次の操作を実行できます:

- `New-ProvScheme`コマンドを使用して、マスターイメージのディスク暗号化セット（DES）とは異なる DES の MCS マシンカタログを作成します。例:

```
$customProperties = @"
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
    machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
    instance">
<Property xsi:type="DiskEncryptionSetId" Name="Zones" Value="/
    subscriptions/XXXXXXXXXXXXXXXXXXXXXXXXXXXXXX/resourceGroups/
    testrsg/providers/Microsoft.Compute/diskEncryptionSets/test-
    diskEncryptionSet"/>
</CustomProperties>
"@
New-ProvScheme -CleanOnBoot `
-ProvisioningSchemeName $provisioningSchemeName `
-HostingUnitName $hostingUnitName `
-IdentityPoolName $identityPoolName `
-InitialBatchSizeHint $numberOfVms `
-masterImagePath $masterImagePath `
-NetworkMapping $networkMapping `
-CustomProperties $customProperties
```

- `Set-ProvScheme` および`Set-ProvVMUpdateTimeWindow`コマンドを使用して、既存の MCS マシンカタログおよび既存の VM のディスク暗号化の種類を 1 つの DES キーから別の DES キーに変更します。VM を再起動すると、更新された DES キーが表示されます。例:

```
$customProperties = '<CustomProperties xmlns="http://schemas.
    citrix.com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.
    org/2001/XMLSchema-instance">
<Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
    Value="/subscriptions/456c683e2ed7/resourceGroups/testrg/
```



```
        providers/Microsoft.Compute/diskEncryptionSets/
        diskEncryptionSet1" />
3   </CustomProperties>'
4   Set-ProvScheme -ProvisioningSchemeName azure-catalog -
        CustomProperties $customProperties
5   Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName azure-catalog
        -VMName azu01, azu02 -StartsNow -DurationInMinutes -1
```

- Set-ProvSchemeおよびSet-ProvVMUpdateTimeWindowコマンドを使用して、以前に CMEK が有効になっていなかった MCS マシンカタログと VM を更新し、顧客管理の暗号化キー（CMEK）の暗号化（DES）、ホストでのディスク暗号化、または二重暗号化を有効にします。さまざまな暗号化の種類について詳しくは、「Azure サーバー側暗号化」、「ホストでの Azure ディスク暗号化」、および「管理対象ディスクの二重暗号化」を参照してください。
- Set-ProvSchemeおよびSet-ProvVMUpdateTimeWindowコマンドを使用して、以前に暗号化されていた既存の MCS マシンカタログと VM を暗号化されていない状態に更新します。例:

```
1   $customProperties = '<CustomProperties xmlns="http://schemas.
        citrix.com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.
        org/2001/XMLSchema-instance">
2   <Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
        Value="" />
3   </CustomProperties>'
4   Set-ProvScheme -ProvisioningSchemeName azure-catalog -
        CustomProperties $customProperties
5   Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName azure-catalog
        -VMName azu01, azu02 -StartsNow -DurationInMinutes -1
```

- プライベートエンドポイント（ProxyHypervisorTrafficThroughConnectorが有効になっているホスト接続を使用した MCS マシンカタログ）でディスク暗号化を有効にします。プライベートエンドポイントでディスク暗号化を有効にする方法について詳しくは、「プライベートエンドポイントでディスク暗号化を有効にする」を参照してください。

プライベートエンドポイントでディスク暗号化を有効にする

Azure の制限により、現在、プライベートエンドポイントに対して顧客管理キーを使用したサーバー側暗号化を行うことはできません。ただし、既存の MCS マシンカタログと VM をプライベートエンドポイントで更新して、DES キーで暗号化することができます。

プライベートエンドポイントを使用して既存のマシンカタログを更新する　既存のマシンカタログをプライベートエンドポイントで更新する詳細な手順は次のとおりです:

1. ProxyHypervisorTrafficThroughConnectorでディスク暗号化を使用せずにカタログを作成します。
2. Set-ProvSchemeを実行してDiskEncryptionSetIdでカタログを更新します。

> 注:
>
> DiskEcryptionSetIdはCustomPropertiesまたはMachineProfileで構成できます。CustomPropertiesとMachineProfileの両方で定義されている場合は、CustomPropertiesで定義されたプロパティが適用されます。

CustomPropertiesを使用する場合の例:

```
$customProperties = '<CustomProperties xmlns="http://schemas.
    citrix.com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.
    org/2001/XMLSchema-instance">
<Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
    Value="/subscriptions/456c683e2ed7/resourceGroups/testrg/
    providers/Microsoft.Compute/diskEncryptionSets/
    diskEncryptionSet1"/>
</CustomProperties>'
Set-ProvScheme -ProvisioningSchemeName azure-catalog -
    CustomProperties $customProperties
```

MachineProfile を使用する場合の例:ディスク暗号化が有効になっている VM か、ディスク暗号化設定を含むテンプレートスペックを使用します:

```
Set-ProvScheme -ProvisioningSchemeName azure-catalog -
    MachineProfile "XDHyp:\HostingUnits\azureunit\machineprofile.
    folder\testrg.resourcegroup\new-template.vm"
```

または、完全な構成インターフェイスを使用してマシンプロファイルを更新することもできます。

3. 既存のカタログ VM を更新するには、Set-ProvVMUpdateTimeWindowを実行します。例:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName azure-catalog -
    VMName azu01, azu02 -StartsNow -DurationInMinutes -1
```

4. VM を再起動すると、Azure Portal で VM のディスク上の更新されたディスク暗号化を確認できます。
5. 新しいカタログ VM を追加する前に、Set-ProvSchemeを実行してディスク暗号化を解除します。

> 注:
>
> プライベートエンドポイントカタログを更新するため、この手順は必須です。この手順を実行しないと、カタログに新しい VM を追加しようとしたときにエラーが発生します。

例:

```
$customProperties = '<CustomProperties xmlns="http://schemas.
    citrix.com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.
    org/2001/XMLSchema-instance">
<Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
    Value="" />
</CustomProperties>'
Set-ProvScheme -ProvisioningSchemeName azure-catalog -
    CustomProperties $customProperties
```


6. 新しい VM をカタログに追加します。

個々のカタログ **VM** を更新する　個々のカタログ VM を更新するための詳細な手順は次のとおりです:

1. ProxyHypervisorTrafficThroughConnectorでディスク暗号化を使用せずにカタログを作成します。
2. Set-ProvVMを実行してDiskEncryptionSetIdでカタログ VM を更新します。

   > 注:
   >
   > DiskEcryptionSetIdはCustomPropertiesまたはMachineProfileのいずれかで設定できます。

   CustomPropertiesを使用する場合の例:

   ```
   $customProperties = '<CustomProperties xmlns="http://schemas.
       citrix.com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.
       org/2001/XMLSchema-instance">
   <Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
       Value="/subscriptions/456c683e2ed7/resourceGroups/testrg/
       providers/Microsoft.Compute/diskEncryptionSets/
       diskEncryptionSet1" />
   </CustomProperties>'
   Set-ProvVM -ProvisioningSchemeName azure-catalog  -VMName azu01 -
       CustomProperties $customProperties
   ```

   MachineProfile を使用する場合の例:

   ```
   Set-ProvVM -ProvisioningSchemeName azure-catalog  -VMName azu01 -
       MachineProfile "XDHyp:\HostingUnits\azureunit\machineprofile.
       folder\testrg.resourcegroup\new-template.vm"
   ```

3. 既存のカタログ VM を更新するには、Set-ProvVMUpdateTimeWindowを実行します。例:

   ```
   Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName azure-catalog -
       VMName azu01 -StartsNow -DurationInMinutes -1
   ```

4. VM を再起動すると、Azure Portal で VM のディスク上の更新されたディスク暗号化を確認できます。
5. 新しい VM をカタログに追加します。

Azure VM、スナップショット、**OS** ディスク、およびギャラリーイメージ定義の情報の取得

OS ディスクと種類、スナップショット、ギャラリーイメージ定義など、Azure VM の情報を表示できます。この情報は、マシンカタログが割り当てられている場合にマスターイメージ上のリソースに関して表示されます。この機能を使用して、Linux または Windows イメージを表示および選択します。PowerShell プロパティTemplateIsWindowsTemplateがAdditionDatafieldパラメーターに追加されました。このフ

ィールドには、Azure 固有の情報（VM タイプ、OS ディスク、ギャラリーイメージ情報、OS の種類情報）が含まれます。TemplateIsWindowsTemplateを **True** に設定することで、OS の種類が Windows であることを示します。TemplateIsWindowsTemplateを **False** に設定することで、OS の種類が Linux であることを示します。

> ヒント：
>
> PowerShell プロパティTemplateIsWindowsTemplateによって表示される情報は、Azure API から取得されます。このフィールドが空の場合があります。たとえば、OS の種類をスナップショットから取得できないため、データディスクからのスナップショットにはTemplateIsWindowsTemplateフィールドが含まれません。

たとえば、PowerShell を使用して Windows OS の種類の Azure VM パラメーターAdditionDataを **True** に設定します：

```
PS C:\Users\username> (get-item XDHyp:\HostingUnits\mynetwork\image.
    folder\username-dev-testing-rg.resourcegroup\username-dev-tsvda.vm).
    AdditionalData
Key Value
ServiceOfferingDescription Standard_B2ms
HardDiskSizeGB 127
ResourceGroupName FENGHUAJ-DEV-TESTING-RG
ServiceOfferingMemory 8192
ServiceOfferingCores 2
TemplateIsWindowsTemplate True
ServiceOfferingWithTemporaryDiskSizeInMb 16384
SupportedMachineGenerations Gen1,Gen2
```

MCS によって作成されたリソースの特定

以下は、MCS がリソースに追加するタグです。表のタグは、「”キー”:”値”」として表示されます。

リソース名	タグ
ID ディスク	“CitrixProvisioningSchemeId” : “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” “CitrixResource” : “Internal”
イメージ	“CitrixProvisioningSchemeId” : “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” “CitrixResource” : “Internal”
NIC	“CitrixProvisioningSchemeId” : “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” “CitrixResource” : “Internal”

リソース名	タグ
OS ディスク	“CitrixProvisioningSchemeId” : “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” “CitrixResource” : “Internal”
PrepVM	“CitrixProvisioningSchemeId” : “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” “CitrixResource” : “Internal”
公開されたスナップショット	“CitrixProvisioningSchemeId” : “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” “CitrixResource” : “Internal”
リソースグループ	“CitrixResource” : “Internal” CitrixSchemaVersion: 2.0 “CitrixProvisioningSchemeId” : “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx”
ストレージアカウント	“CitrixProvisioningSchemeId” : “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” “CitrixResource” : “Internal”
カタログ内の VM	“CitrixProvisioningSchemeId” : “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” “CitrixResource” : “Internal”
WBC ディスク	“CitrixProvisioningSchemeId” : “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” “CitrixResource” : “Internal”

> 注:
>
> MCS によって作成されたリソースとして識別するために **CitrixResource** タグが追加されている場合、VM は Citrix インベントリに表示されません。タグを削除するか名前を変更すると、表示できるようになります。

タグの削除

カタログまたは 仮想マシンを作成すると、次のリソースにタグが作成されます:

- リソースグループ
- 仮想マシン
- OS ディスク
- ID ディスク

- ネットワークインターフェイス
- ストレージアカウント

仮想マシンとマシンカタログを Citrix データベースから削除し、タグを削除できます。以下を使用できます:

- Remove-ProvVMをForgetVMパラメーターとともに使用して、マシンカタログの単一の仮想マシンまたは仮想マシンの一覧から仮想マシンとタグを削除します。
- Remove-ProvSchemeをForgetVMパラメーターとともに使用して、Citrix データベースから単一のマシンカタログを削除し、マシンカタログ全体からタグを削除します。

この機能は、永続的な仮想マシンにのみ適用されます。

これを行うには、以下の手順に従います:

1. **PowerShell** ウィンドウを開きます。
2. **asnp citrix*** を実行し、Citrix 固有の PowerShell モジュールをロードします。
3. Remove-ProvVMを実行して、Citrix データベースから仮想マシンを削除し、仮想マシンからタグを削除します。
   例:

```
1 Remove-ProvVM -ProvisioningSchemeName “ProvisioningSchemeName” -
    VMName “vmname” -ForgetVM
```

4. Remove-ProvSchemeを実行して、Citrix データベースからマシンカタログを削除し、マシンカタログからタグを削除します。例:

```
1 Remove-ProvScheme -ProvisioningSchemeName “ProvisioningSchemeName
    ” -ForgetVM
```

> 注:
>
> Remove-ProvSchemeでForgetVMパラメーターを使用した後、プロビジョニングスキームが独自のリソースグループ（BYORG）または Citrix 管理のリソースグループのいずれかに存在する場合、MCS は基本ディスクのスナップショットを含むすべてのスナップショットを削除します。

追加情報

- 接続とリソースの作成と管理
- Microsoft Azure への接続
- マシンカタログの作成
- Microsoft Azure カタログの作成
- マシンカタログの管理

Microsoft System Center Virtual Machine Manager カタログの管理

August 17, 2024

「マシンカタログの管理」では、マシンカタログを管理するウィザードについて説明します。次の情報は、Microsoft System Center Virtual Machine Manager（VMM）仮想化環境に固有の詳細について説明しています。

> 注:
>
> VMM カタログを管理する前に、VMM カタログの作成を完了する必要があります。「Microsoft System Center Virtual Machine Manager カタログの作成」を参照してください。

MCS によって作成されたリソースの特定

以下は、MCS がリソースに追加するタグです。表のタグは、「”キー”:”値”」として表示されます。

リソース名	タグ
VM の準備	Tag string: “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” Custom property entry: “XdConfig:” XdProvisioned=True”
カタログ内の VM	Tag string: “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” Custom property entry: “XdConfig:” XdProvisioned=True”

追加情報

- 接続とリソースの作成と管理
- Microsoft System Center Virtual Machine Manager への接続
- マシンカタログの作成
- Microsoft System Center Virtual Machine Manager カタログの作成
- マシンカタログの管理

VMware カタログの管理

August 17, 2024

「マシンカタログの管理」では、マシンカタログを管理するウィザードについて説明します。以下の情報は、VMware 仮想化環境に固有の詳細について説明しています。

> 注:
>
> VMware カタログを管理する前に、VMware カタログの作成を完了する必要があります。「VMware カタログの作成」を参照してください。

マシンカタログのフォルダー **ID** の更新

`Set-ProvScheme`コマンドのカスタムプロパティで`FolderId`を指定することにより、MCS マシンカタログのフォルダー ID を更新できます。フォルダー ID の更新後に作成された仮想マシンは、この新しいフォルダー ID の下に作成されます。このプロパティが`CustomProperties`で指定されていない場合、仮想マシンはマスターイメージが配置されているフォルダーの下に作成されます。

マシンカタログのフォルダー ID を更新するには、次の手順を実行します。

1. Web ブラウザーを開き、**vSphere Web Client** の URL を入力します。
2. 資格情報を入力し、[**Login**] をクリックします。
3. **vSphere Web Client** で仮想マシンを配置するフォルダーを作成します。
4. PowerShell ウィンドウを開きます。
5. **asnp citrix*** を実行し、Citrix 固有の PowerShell モジュールをロードします。
6. `Set-ProvScheme`の`CustomProperties`に`FolderID`を指定します。この例では、フォルダー ID の値は`group-v2406`です。

```
Set-ProvScheme -ProvisioningSchemeUid "50bb319c-2e83-4a37-9ea1-94
    f630687372" -CustomProperties "<CustomProperties xmlns=""http
    ://schemas.citrix.com/2014/xd/machinecreation"" xmlns:xsi=""
    http://www.w3.org/2001/XMLSchema-instance""><Property xsi:type=
    ""StringProperty"" Name=""FolderId"" Value=""group-v2406"" /></
    CustomProperties>"
```

7. Studio を使用して仮想マシンをマシンカタログに追加します。
8. vSphere Web Client で新しい仮想マシンを確認します。新しい仮想マシンは、新しいフォルダーの下に作成されます。

vSphere でフォルダー **ID** を確認

任意の ESXi または vCenter サーバーシステムで管理対象オブジェクトブラウザー（MOB）にアクセスして、VM のフォルダー ID を見つけます。

MOB は、すべての ESX/ESXi および vCenter サーバーシステムに組み込まれている、Web ベースのサーバーアプリケーションです。この vSphere ユーティリティを使用すると、VM、データストア、リソースプールなどのオブジェクトに関する詳細情報を表示できます。

1. Web ブラウザーを開き、`http://x.x.x.x/mob`と入力します。ここで x.x.x.x は、vCenter Server の、または ESX/ESXi ホストの IP アドレスです。例：https://10.60.4.70/mob。
2. MOB のホームページで、プロパティ **content** の値をクリックします。
3. **rootFolder** の値をクリックします。
4. **childEntity** の値をクリックします。
5. **vmFolder** の値をクリックします。
6. フォルダー ID は、**childEntity** の値で確認できます。

VM のストレージ移行

既存の VM のディスクストレージを古いストレージから新しいストレージに移動できます。移行中、MCS は電源管理、OS ディスクのリセットなどの VM 機能を保持します。新しいディスクストレージを使用して、新しい VM をマシンカタログに追加することもできます。これを行うには、PowerShell コマンド`Move-ProvVMDisk`を使用します。

現在、移行できるのは完全なクローンの永続的な VM のみです。

新しいストレージは次の条件を満たしている必要があります：

- 古いストレージの同じクラスター内にある必要があります。
- VM が実行されているホストは、古いデータストアと新しいデータストアの両方にアクセスできる必要があります。

次のタスクを実行できます：

- ディスクストレージの移行
- 古いストレージの廃止

ディスクストレージの移行

ディスクストレージを移行するには、以下の手順を実行します：

1. 新しいストレージを既存のホスティングユニットに追加します。古いストレージを **Superseded** に変更します。このためには、Web Studio または PowerShell コマンドを使用できます。
    - Web Studio を使用する場合は、「ストレージの編集」を参照してください。
    - PowerShell コマンドを使用する場合：
        - `Add-Hyphostingunitstorage`を実行して、新しいストレージを既存のホスティングユニットに追加します。

- Set-Hyphostingunitstorageで **Superseded** を「true」に設定して、古いストレージでの新しい VM の作成を無効にします。

2. VM をオフにして、メンテナンスモードをオンにします。
3. VM のディスクストレージを新しいストレージに移動し、ストレージ情報を更新します。例:

```
Move-ProvVMDisk -ProvisioningSchemeName "myFullCloneProvScheme" -
    VMName ("VMware-TestVM01", "VMware-TestVM02") -DiskType OS,
    Identity -DestinationStorageId datastore1,datastore1
```

4. 移行のタスク ID を取得します。例:

```
,(Get-ProvVM -ProvisioningSchemeName xxxxx) | Move-ProvVMDisk -
    ProvisioningSchemeName xxxxx -DiskType OS,Identity -
    DestinationStorageId datastore1,datastore1
```

5. 移行の状態を確認します。

- (Get-ProvTask -TaskID xxxxxxxxx).DiskMovedVirtualMachines: 既に新しいストレージに移行されている VM を含む、ディスク移行が成功した VM の一覧を提供します。
- (Get-ProvTask -TaskID xxxxxxxxx).DiskMoveFailedVirtualMachines: 移行に失敗した VM の一覧を提供します。
- (Get-ProvTask -TaskID xxxxxxxxx).NotStartedVirtualMachines:移行がまだ開始されていない VM の一覧を提供します。
- Get-ProvVM -ProvisioningSchemeName xxxxx -VMName "VMware -TestVM01: 移行後に更新された VM プロパティを提供します。StorageId、AssignedImage、BootedImage、IdentityDiskId、IdentityDiskStorage、およびLastBootTimeなどのプロパティを確認します。

スナップショットを使用して MCS 作成の VM のディスクを移行した後、**VSphere Client** に統合が必要ですという警告が表示される場合があります。統合してデータの損失を回避するには、以下の手順を実行します:

1. VMware VM のバックアップを作成します。たとえば、すべての VM ファイルをデータストア上の別のフォルダーに転送します。
2. 警告が表示されたら、[**Consolidate**] をクリックし、[**OK**] をクリックして統合を確認します。

古いストレージの廃止

VM のディスク移行後に古いストレージを廃止するには、以下の手順を実行します:

1. ホスティングユニットの各ディスクストレージ内の基本ディスクとマシン数に関する情報を取得します。例:

```
$result=Get-ProvSchemeResourceInStorage -ProvisioningSchemeName
    xxxxx
```



```
$result
$result.ProvResourceInStorage | Format-List -Property *
```

移行が成功すると、MCS は古い基本ディスクを自動的に削除するため、古いストレージにはマシンがなくなります。したがって、コマンドの実行後、古いストレージにマシンと基本ディスクが存在しないことを確認してください。

2. Remove-Hyphostingunitstorageを実行して、ホスティングユニットから古いストレージを完全に削除します。Web Studio を使用して古いストレージを削除することもできます。

MCS によって作成されたリソースの特定

以下は、MCS がリソースに追加するタグです。表のタグは、「”キー”:”値”」として表示されます。

リソース名	タグ
VM の準備	“CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” “XdConfig:”XdProvisioned=True”
カタログ内の VM	“CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” “XdConfig:”XdProvisioned=True”

追加情報

- 接続とリソースの作成と管理
- VMware への接続
- マシンカタログの作成
- VMware カタログの作成
- マシンカタログの管理

電源管理

August 17, 2024

Citrix Virtual Apps and Desktops を使用すると、サポートされているさまざまなハイパーバイザーやクラウドサービスにわたって、MCS でプロビジョニングされた VM の電源管理を行うことができます。電源管理操作により、次のことが可能になります:

- 最適なユーザーエクスペリエンス
- コスト管理と省電力

利用可能な電源操作は次のとおりです:

- 開始
- シャットダウン
- 再起動
- 一時停止
- 再開
- 強制再起動
- 強制シャットダウン

> 注:
>
> - 非永続的な VM の場合は、電源サイクル（シャットダウン/起動および再起動）により、OS ディスクがリセットされます。
> - 電源操作の機能と動作は、ハイパーバイザーまたはクラウドサービスによって異なります。

この記事では、サポートされている特定のハイパーバイザーに関連する主要な電源管理機能について説明します。

- AWS VM の電源管理
- Azure VM の電源管理

AWS VM の電源管理

August 17, 2024

必要な権限については、「必要な AWS 権限」を参照してください。

インスタンスの休止

休止プロセスでは、インスタンスの状態がプライベート IP アドレスおよび Elastic IP アドレスとともにメモリ内に保存されるので、中断したところから正確に再開できます。

休止するように指示したインスタンスは、ルート EBS ボリューム内のファイルにメモリ内の状態を書き込み、その後、自身をシャットダウンします。Amazon EBS ボリュームは、インスタンスに接続できる、耐久性のあるブロックレベルのストレージデバイスです。インスタンスに接続した後のボリュームは、物理ハードドライブを使用するのと同じように使用できます。インスタンスのルート EBS ボリュームを暗号化します。暗号化により、メモリから EBS ボリュームにコピーされた機密データが適切に保護されるようになります。EBS 暗号化について詳しくは、「Amazon EBS 暗号化」を参照してください。

サポートされているインスタンスの休止に関する制限は、次のとおりです:

- 最大 150GB までのインスタンスメモリ（RAM）だけがサポートされます。
- UEFI ブートモードはサポートされていません。
- 汎用 SSD とプロビジョンド IOPS SSD は、EBS ボリュームタイプとしてのみサポートされます。

休止をサポートする **VM** の作成

休止をサポートする VM を作成するには:

1. ホスト接続を作成します。「AWS への接続」を参照してください。
2. EBS ルートを暗号化して **Stop-Hibernate** プロパティを有効にしたインスタンスを起動します。インスタンスの起動、ルート EBS ボリュームの暗号化、および休止の有効化について詳しくは、「https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/launching-instance.html/」を参照してください。このインスタンスをマスターイメージとして使用して、AMI を作成します。
3. マスターイメージを準備します:
   a) マスターイメージに VDA をインストールします。最新の機能を利用できるように、最新バージョンをインストールすることを Citrix ではお勧めします。マスターイメージに VDA をインストールできないと、カタログ作成が失敗します。VDA のインストール方法について詳しくは、「VDA のインストール」を参照してください。
   b) アプリケーションとデスクトップがメンバーとなっているドメインにマスターイメージを統合します。マスターイメージが、仮想マシンを作成するホスト上で使用できることを確認してください。
4. そのインスタンスから AMI を作成します。インスタンスから AMI を作成する方法については、「Amazon EC2 インスタンスからの AMI の作成」を参照してください。
5. `New-ProvScheme`コマンドを使用してマシンカタログを作成します。カスタムプロパティ`AwsCaptureInstanceProperties`を **True** に設定します。[完全な構成] インターフェイスで AWS インスタンスのプロパティを有効にする方法については、「完全な構成インターフェイスでの **AWS** インスタンスのプロパティの適用および運用リソースのタグ付け」を参照してください。

```
New-ProvScheme  -AdminAddress "xxx" -CleanOnBoot
-CustomProperties "AwsCaptureInstanceProperties,true;"
-HostingUnitName "xxx" -IdentityPoolName $catalog_name -
   InitialBatchSizeHint 1
-MasterImageVM "xyz.template" -NetworkMapping @{
 "0"="XDHyp:\HostingUnits\MyConn\us-east-2a.availabilityzone
    \10.0.0.0``/24 (vpc-0f1771e45671aedcd).network" }

-ProvisioningSchemeName $catalog_name
-RunAsynchronously -Scope @() -SecurityGroup @("xxx") -
   ServiceOffering "xxx"
```


PowerShell コマンドを使用してマシンカタログを作成する方法については、「https://developer-docs.citrix.com/projects/citrix-daas-sdk/en/latest/」を参照してください。

休止できる VM は、次の場合に作成されます:

- マスターイメージから作成された AMI のうち、**Stop-Hibernate** プロパティが有効になっている AMI を選択した場合
- マスター VM がドメインに参加しており、VDA がインストールされている場合
- 休止を処理できる正しい VM サイズ（サービスオファリング）を選択した場合

次の場合、**New-ProvScheme** コマンドは失敗し、該当するエラーメッセージが表示されます:

- マスター VM は休止が有効になっているが、サービスオファリングが休止を処理できない場合
- マスター VM がドメインに参加しておらず、VDA がインストールされていない場合

サービスオファリングと **AMI** の休止状態

サービスオファリングと AMI（テンプレート）の休止状態を表示するには、次のコマンドを実行します:

- `Get-HypConfigurationObjectForItem 'XDHyp:\HostingUnits\MyConn\WIN2016-ADDC-2021.09.10.145334-a1968709-10c4-47d5-9642-21e743159a7b (ami-0e6c5b33a52d2a6b6).template'`
- `Get-HypConfigurationObjectForItem 'XDHyp:\HostingUnits\MyConn\R6i Sixteen Extra Large Instance.serviceoffering'`

既存の休止でサポートされるプロビジョニングスキームに関するサービスオファリングの更新

1. `Set-ProvScheme`コマンドを実行します。たとえば、

```
1 Set-ProvScheme -ProvisioningSchemeName <String> -ServiceOffering <
    String>
```

サービス提供に互換性がない場合、システムは例外メッセージを表示します。

休止状態をサポートするマシンカタログを作成する

マシンカタログを作成する場合、休止状態をサポートするマシンプロファイルを使用できます。

1. カタログ作成ウィザードでは、マシンプロファイルの選択まで指示に従います。
2. ［マシンテンプレート］ページで、［マシンプロファイルを選択］をクリックしてマシンプロファイルを選択します。
3. ［仮想マシン］ページで、編集アイコンをクリックして VM を選択します。

> 注:
>
> マシンプロファイルで休止状態が有効になっている場合、システムは休止状態にできる VM のみを表示します。

4. 画面の指示に従ってすべての設定を完了してください。[概要] ページには、カタログの休止状態が表示されます。

> 注:
>
> [マシンカタログの編集] で、マシンプロファイルを休止状態が有効なプロファイルに変更すると、それに応じて VM を再構成するように求められます。

休止をサポートするマシンカタログの更新

休止をサポートしていないマシンカタログを使用して既存のマシンカタログを更新しようとすると、更新が失敗し、該当するエラーメッセージが表示されます。

休止状態の **VM** の電源管理

休止状態の VM に対して実行できる電源管理操作は、次のとおりです:

1. VM を実行状態から一時停止にする。
2. VM を一時停止状態から再開する。
3. VM を一時停止状態から再起動する。

Azure VM の電源管理

August 17, 2024

必要な権限については、「必要な Azure 権限」を参照してください。

Azure のオンデマンドプロビジョニング

Azure のオンデマンドプロビジョニングでは、VM は、プロビジョニング完了後、Citrix Virtual Apps and Desktops で電源投入操作が開始されたときにのみ作成されます。

MCS を使用して Azure Resource Manager でマシンカタログを作成する場合、Azure のオンデマンドプロビジョニング機能は次のことを実現します:

- ストレージコストを削減する。

- カタログ作成を高速化する

MCS カタログを作成すると、Azure Portal にリソースグループ内のネットワークセキュリティグループ、ネットワークインターフェイス、基本イメージ、ID ディスクが表示されます。

Azure Portal では、Citrix Virtual Apps and Desktops が VM の電源投入操作を開始するまで、その VM は表示されません。次のような違いがある 2 種類のマシンがあります:

- プールされたマシンの場合、オペレーティングシステムのディスクとライトバックキャッシュは、VM が存在する場合にのみ存在します。プールされたマシンをコンソールでシャットダウンすると、VM は Azure Portal に表示されません。マシンを定期的に（たとえば、勤務時間外に）シャットダウンすると、ストレージコストを大幅に節約できます。
- 専用マシンでは、VM の初回電源投入時にオペレーティングシステムのディスクが作成されます。Azure Portal の VM は、マシン ID が削除されるまでストレージに残ります。専用マシンをコンソールでシャットダウンすると、VM は引き続き Azure Portal に表示されます。

> 注:
>
> オンデマンドプロビジョニング機能（「レガシー」カタログ）が廃止される前に作成された Azure カタログのサポートは廃止されます。したがって、Azure レガシーカタログ VM を再作成してください。カタログはオンデマンドとしてプロビジョニングされるため、ストレージコストが節約されます。

電源を入れ直したときにプロビジョニングされた仮想マシンを保持する

電源を入れ直したときに、プロビジョニングされた仮想マシンを保持するかどうかを選択します。PowerShell パラメーター`New-ProvScheme CustomProperties`を使用します。このパラメーターではプロパティ`PersistVm`を追加することができ、これを使用して、電源を入れ直したときにプロビジョニングされた仮想マシンが保持されるかどうかを指定できます。`PersistVm`プロパティを **true** に設定して、電源がオフのときに仮想マシンが保持されるように設定するか、プロパティを **false** に設定して、電源がオフのときに仮想マシンが保持されないように設定します。

> 注:
>
> `PersistVm`プロパティは、`CleanOnBoot`および`UseWriteBackCache`のプロパティが有効なプロビジョニングスキームにのみ適用されます。非永続仮想マシンに`PersistVm`プロパティが指定されていない場合、非永続仮想マシンは電源がオフのときに Azure 環境から削除されます。

次の例では、`New-ProvScheme CustomProperties`パラメーターで`PersistVm`プロパティが **true** に設定されています:

```
1 <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
     machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
     instance">
2 <Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true"
      />
```



```
<Property xsi:type="StringProperty" Name="StorageType" Value="
    Standard_LRS" />
<Property xsi:type="StringProperty" Name="PersistWBC" Value="false" />
<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="true"
    />
<Property xsi:type="StringProperty" Name="PersistVm" Value="true" />
<Property xsi:type="StringProperty" Name="ResourceGroups" Value="demo-
    resourcegroup" />
<Property xsi:type="StringProperty" Name="LicenseType" Value="
    Windows_Client" />
</CustomProperties>
```

次の例では、New-ProvScheme CustomPropertiesパラメーターでPersistVMを **true** に設定することで、ライトバックキャッシュが維持されます:

```
New-ProvScheme
-AzureAdJoinType "None"
-CleanOnBoot
-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com
    /2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/
    XMLSchema-instance`"><Property xsi:type=`"StringProperty`" Name=`"
    UseManagedDisks`" Value=`"true`" /><Property xsi:type=`"
    StringProperty`" Name=`"StorageType`" Value=`"Standard_LRS`" /><
    Property xsi:type=`"StringProperty`" Name=`"PersistWBC`" Value=`"
    false`" /><Property xsi:type=`"StringProperty`" Name=`"
    PersistOsDisk`" Value=`"true`" /><Property xsi:type=`"
    StringProperty`" Name=`"PersistVm`" Value=`"true`" /><Property xsi:
    type=`"StringProperty`" Name=`"ResourceGroups`" Value=`"demo-
    resourcegroup`" /><Property xsi:type=`"StringProperty`" Name=`"
    LicenseType`" Value=`"Windows_Client`" /></CustomProperties>"
-HostingUnitName "demo"
-IdentityPoolName "NonPersistent-MCSIO-PersistVM"
-MasterImageVM "XDHyp:\HostingUnits\demo\image.folder\scale-test.
    resourcegroup\demo-snapshot.snapshot"
-NetworkMapping @ {
"0"="XDHyp:\HostingUnits\demo\virtualprivatecloud.folder\East US.
    region\virtualprivatecloud.folder\ji-test.resourcegroup\jitest-vnet
    .virtualprivatecloud\default.network" }

-ProvisioningSchemeName "NonPersistent-MCSIO-PersistVM"
-ServiceOffering "XDHyp:\HostingUnits\demo\serviceoffering.folder\
    Standard_B2ms.serviceoffering" -UseWriteBackCache
-WriteBackCacheDiskSize 127
-WriteBackCacheMemorySize 256
```

> ヒント:
>
> PersistVmプロパティは、プロビジョニングされた仮想マシンを保持するかどうかを決定します。PersistOsdiskプロパティは、OS ディスクを永続化するかどうかを決定します。プロビジョニングされた仮想マシンを保持するには、最初に OS ディスクを保持します。仮想マシンを削除する前に OS ディスクを削除しないでください。PersistVmパラメーターを指定せずにPersistOsdiskプロパティを使用する

> ことができます。

ストレージの種類の変更に失敗したときの電源投入時の動作をカスタマイズする

電源をオンにした際に、Azure での障害が原因で、管理対象ディスクのストレージの種類が目的の種類に変更されないことがあります。この場合、VM はオフのままになり、エラーメッセージが送信されます。ただし、設定した種類にストレージを復元できない場合でも、VM の電源をオンにするか、VM の電源をオフのままにするかを選択できます。

- カスタムプロパティの`FailSafeStorageType`を **true**（デフォルト設定）にするか、`New-ProvScheme`または`Set-ProvScheme`コマンドで値を指定しない場合:
  - 電源投入時、VM が正しくないストレージの種類でオンになります。
  - シャットダウン時、VM が正しくないストレージの種類でオフのままになります。
- `New-ProvScheme`または`Set-ProvScheme`コマンドでカスタムプロパティの`FailSafeStorageType`を **false** にした場合:
  - 電源投入時、VM が正しくないストレージの種類でオフのままになります。
  - シャットダウン時、VM が正しくないストレージの種類でオフのままになります。

マシンカタログを作成するには:

1. PowerShell ウィンドウを開きます。
2. `asnp citrix*`を実行し、Citrix 固有の PowerShell モジュールをロードします。
3. ID プールをまだ作成していない場合は作成します。
4. `New-ProvScheme`にカスタムプロパティを追加します。例:

```
New-ProvScheme -HostingUnitName "Azure-Resources-1" -
    IdentityPoolName "name" -InitialBatchSizeHint 1
-MasterImageVM "XDHyp:\HostingUnits\Azure-Resources-1\image.folder
    \abc.resourcegroup\def.snapshot"
-NetworkMapping @{
 "0"="XDHyp:\HostingUnits\Azure-Resources-1\ght.folder\abc.
     resourcegroup\abc-vnet.virtualprivatecloud\default.network" }

-ProvisioningSchemeName "name"
-ServiceOffering "XDHyp:\HostingUnits\Azure-Resources-1\
    serviceoffering.folder\Standard_DS2_v2.serviceoffering"
-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix
    .com/2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org
    /2001/XMLSchema-instance`">
<Property xsi:type=`"StringProperty`" Name=`"StorageType`" Value=`
    "Premium_LRS`" />
<Property xsi:type=`"StringProperty`" Name=`"StorageTypeAtShutdown
    `" Value=`"Standard_LRS`" />
```



```
<Property xsi:type=`"StringProperty`" Name=`"FailSafeStorageType`"
    Value=`"true`" />
</CustomProperties>"
```

5. マシンカタログを作成します。Remote PowerShell SDK を使用してカタログを作成する方法については、https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/を参照してください。

既存のマシンカタログを更新してカスタムプロパティのFailSafeStorageTypeを含めるようにします。この更新は、既存の VM には影響しません。

1. Set-ProvSchemeコマンドでカスタムプロパティを更新します。例:

```
Set-ProvScheme -ProvisioningSchemeName <String> -CustomProperties "
<CustomProperties xmlns=`"http://schemas.citrix.com/2014/xd/
    machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
    instance`">
<Property xsi:type=`"StringProperty`" Name=`"StorageType`" Value=`"
    Premium_LRS`" />
<Property xsi:type=`"StringProperty`" Name=`"IdentityDiskStorageType
    `" Value=`"Premium_LRS`" />
<Property xsi:type=`"StringProperty`" Name=`"FailSafeStorageType`"
    Value=`"false`" />
</CustomProperties>"
```

Set-ProvScheme で行った変更を既存の VM に適用するには、-StartsNowおよび-DurationInMinutes -1パラメーターを指定したSet-ProvVMUpdateTimeWindowコマンドを実行します。

1. Set-ProvVMUpdateTimeWindowコマンドを-StartsNowおよび-DurationInMinutes -1パラメーターとともに実行します。例:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog -
    VMName <List-Of-Vm-Names> -StartsNow -DurationInMinutes -1
```

2. VM を再起動します。

休止状態対応 **VM** の作成

Azure 環境では、休止状態をサポートする MCS マシンカタログを作成できます。この機能を使用すると、VM を一時停止し、ユーザーが再度サインインしたときに VM の以前の状態に再接続できます。

休止状態機能は以下に適用されます:

- シングルセッション OS
- 永続的および非永続的な VM
- 静的およびランダム（プール）VDI デスクトップ

VDI デスクトップが静的かランダムかに関係なく、VM を休止状態にした後に同じセッションを再開できます。

このセクションでは、以下を参照してください:

- 前提条件
- 制限事項
- 休止状態対応マシンカタログを作成および管理する
- 既存の休止状態対応 VM のマシンカタログを作成する
- MCS でプロビジョニングされた既存の VM で休止状態を有効にする
- 休止状態のプロパティを確認する
- VM の電源管理（手動および自動）

休止状態を使用するための前提条件

休止状態を使用するには、次のタスクを必ず完了してください:

- Windows と Linux の両方のマスターイメージに Azure VM エージェントをインストールします。Windows イメージのページファイルは一時ディスク上に置くことができます。マシンカタログで休止状態が有効になっている場合、MCS はページファイルの場所を基本ディスクの「C:」ドライブに設定します。
- MCS は、生成されたリソースの休止状態プロパティを自動的に設定します。休止状態をサポートするためにマスターリソースのプロパティを構成する必要はありません。
- 休止状態をサポートする VM サイズをサブスクリプションで使用します。
- VM が休止機能を継承できるように、休止状態対応マシンプロファイル（VM またはテンプレートスペック）を作成します。VM を作成するには、「休止機能の使用を開始する」を参照してください。

  > 注:
  >
  > Microsoft については、休止状態が有効な VM を OS ディスクから展開できます。この機能は現在、特定のリージョンでサポートされており、間もなくすべてのリージョンで利用できるようになる予定です。詳しくは、「休止機能が有効な VM を OS ディスクからデプロイする」を参照してください。

  テンプレートスペックを作成するには、次の手順を実行します:

  1. Azure Portal を開きます。テンプレートで使用する構成の VM を選択します。左側のペインで ［テンプレートのエクスポート］を選択します。
  2. ［パラメーターを含める］チェックボックスをオフにします。コンテキストをコピーし、JSON ファイルとして保存します（例: `VMExportTemplate.json`）。
  3. テンプレートのパラメーター`hibernationEnabled`が**`true`**であることを確認してください。パラメーターが**`true`**ではない場合は、使用した VM 構成を確認してください。サポートされる VM サイズをテンプレートファイルで指定できます。ただし、カタログの作成時にマシンのサイズを指定することもできます。
  4. ネットワークインターフェイスリソースのテンプレートを JSON ファイル`VMExportTemplate.json`に追加します。その結果、2 つのリソースを持つ ARM テンプレートファイルが作成されます。

5. [**Azure Portal**] > [テンプレートスペック] > [テンプレートのインポート] > [ローカルテンプレートファイルを選択] を選択して、このテンプレートファイルを ARM テンプレートスペックとしてインポートします。
6. ARM テンプレートスペックを作成したら、マシンプロファイルとして使用できます。

> 注:
>
> Citrix Studio と同期するまでに数分かかる場合があります。

詳しくは、Microsoft のドキュメント「休止状態を使用するための前提条件」を参照してください。

制限事項

- シングルセッション OS マシンカタログ（永続的および非永続的）のみがサポートされます。
- エフェメラル OS ディスクと MCS I/O 機能は Azure の休止状態をサポートしていません。
- Windows の自動更新中に休止機能が失敗する場合があります。

詳しくは、Microsoft のドキュメントを参照してください。

休止状態対応マシンカタログを作成および管理する

休止状態対応 VM を作成するために、以下を使用して休止状態対応マシンカタログを作成および管理できます:

- Web Studio、または
- PowerShell コマンド

Web Studio でのカタログの作成

1. [マシンカタログの作成] を選択します。カタログ作成ウィザードが開きます。
2. [マシンの種類] ページで、このカタログのマシンの種類 [シングルセッション **OS**] を選択します。
3. [マシン管理] ページで、次のように設定を選択します:

   a) 電源管理されているマシン（仮想マシン、ブレード **PC** など）を選択します。
   b) [**Citrix Machine Creation Services**（**MCS**）] を選択します。

4. [デスクトップエクスペリエンス] ページで、必要に応じてランダムまたは静的なデスクトップエクスペリエンスを選択します。
5. [イメージ] ページで、マスターイメージを選択します。[マシンプロファイルを使用する] チェックボックスを選択し、休止状態をサポートするマシンプロファイルを選択します。ヒントをクリックすると、マシンプロファイルが休止状態をサポートしているかどうかがわかります。
6. [ストレージとライセンスの種類] ページで、このカタログに使用するストレージとライセンスを選択します。
7. [仮想マシン] ページで、仮想マシンの数、仮想マシンのサイズ、およびアベイラビリティ ゾーンを選択します。

> 注:
>
> 休止状態をサポートするマシンサイズは、選択のためにのみ表示されます。

8. ［**NIC**］ページで、仮想マシンで使用する NIC を追加します。
9. ［ディスク設定］ページで、ライトバックキャッシュディスクのストレージの種類とサイズを選択します。
10. ［リソースグループ］ページで、仮想マシンをプロビジョニングするリソースグループを選択します。
11. ［マシン **ID**］ページで、［新しい **Active Directory** アカウントを作成する］を選択します。次に、アカウントの名前付けスキームを指定します。
12. ［ドメイン資格情報］ページで、［資格情報の入力］をクリックします。ドメイン資格情報を入力して、ターゲットの Active Directory ドメインでアカウント作成を実行します。
13. ［概要］ページで、マシンカタログの名前を入力し、［完了］をクリックします。

MCS マシンカタログの作成が完了したら、カタログ一覧でカタログを見つけて、［テンプレートのプロパティ］タブをクリックします。パラメーター **Hibernation** の値は **Supported** である必要があります。

マシンカタログを編集する場合は、次の制限を考慮してください:

- 現在のマシンカタログが休止状態をサポートしている場合、次のことはできません:
  - VM サイズを休止状態に対応しないサイズに変更する。
  - マシンプロファイルを休止状態に対応しないプロファイルに変更する。
- 現在のマシンカタログが休止状態をサポートしていない場合、次のことはできません:
  - 現時点で、Web Studio を使用してマシンプロファイルを休止状態対応プロファイルに変更すること。ただし、これは PowerShell コマンドを使用して行うことができます。「MCS でプロビジョニングされた既存の VM で休止状態を有効にする」を参照してください。

既存の休止状態対応の **VM** を管理するためのマシンカタログを作成する　既に休止状態対応の VM があり、それらを一時停止して再開したい場合は、マシンカタログを作成して、電源管理のためにそれらの VM をインポートします。

> 注:
>
> 休止状態対応の VM と休止状態に対応できない VM の両方を含むマシンカタログを作成できます。ただし、休止状態関連の機能が必要な場合は、休止状態対応の VM のみを含むマシンカタログを作成する必要があります。

Web Studio を使用して既存の休止状態対応の VM のカタログを作成するには、画面上の指示に従って手順を完了し、次の主要な設定に注意してください:

1. ［マシン管理］ページで、［電源管理されているマシン］を選択し、マシンを展開する方法として ［ほかのサービスまたはテクノロジ］を選択します。
2. ［仮想マシン］ページで、休止状態対応の VM のみを追加またはインポートします。

PowerShell コマンドを使用してマシンカタログを作成する　休止状態を使用するための要件をすべて満たしたら、New-ProvSchemeコマンドを使用して休止状態対応のマシンカタログを作成できます。Remote PowerShell SDK を使用してカタログを作成する方法については、「New-ProvScheme」を参照してください。

カタログの作成中に、次の PowerShell コマンドを使用して、VM サイズとマシンプロファイルが休止状態をサポートしているかどうかを確認できます:

- VM サイズについては、次のコマンドを実行し、プロパティsupportsHibernationが **True** であるかどうかを確認します。たとえば、

```
Get-ChildItem -AdminAddress "MyDDC.MyDomain.local" -LiteralPath @
    ("XDHyp:\HostingUnits\ <VirtualNetwork> \serviceoffering.
    folder") | select Name, AdditionalData | ConvertTo-Json
```

- マシンプロファイルについては、次のコマンドを実行し、プロパティsupportsHibernationが **True** であるかどうかを確認します。たとえば、

```
Get-ChildItem -AdminAddress "MyDDC.MyDomain.local" -LiteralPath @
    ("XDHyp:\HostingUnits\ <VirtualNetwork> \machineprofile.folder
    \abc.resourcegroup")|select Name, AdditionalData|ConvertTo-
    Json
```

マシンカタログを編集する場合は、次の制限を考慮してください:

- 現在のマシンカタログが休止状態をサポートしている場合、次のことはできません:
  - VM サイズを休止状態に対応しないサイズに変更する
  - マシンプロファイルを休止状態に対応しないプロファイルに変更する
- 現在のマシンカタログが休止状態をサポートしていない場合、次のことはできません:
  - 現時点で、Web Studio を使用してマシンプロファイルを休止状態対応プロファイルに変更すること。ただし、これは PowerShell コマンドを使用して行うことができます。「MCS でプロビジョニングされた既存の VM で休止状態を有効にする」を参照してください。

Remote PowerShell SDK を使用してカタログの VM サイズとマシンプロファイルを変更する方法については、https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/MachineCreation/Set-ProvScheme/を参照してください。

MCS でプロビジョニングされた既存の VM で休止状態を有効にする

以下の既存のもので Azure 休止状態を有効にできます:

- 一時ディスクを使用せずに作成された、Windows MCS によってプロビジョニングされたマシンカタログの VM。
- 一時ディスクを使用して、または使用せずに作成された、Linux MCS によってプロビジョニングされたマシンカタログの VM。

> 注:
>
> - MCS によってプロビジョニングされた既存の VM には、Azure VM エージェントがインストールされている必要があります。
> - 現在、この機能を有効にするには PowerShell コマンドのみを使用できます。

これを行うには、以下の手順に従います:

1. **PowerShell** ウィンドウを開きます。
2. `asnp citrix*`を実行し、Citrix 固有の PowerShell モジュールをロードします。
3. 既存のマシンの構成を確認します。例:

```
Get-ProvScheme | select ProvisioningSchemeName,
    ProvisioningSchemeVersion
```

4. `Set-ProvScheme`コマンドを使用して、このマシンカタログで休止状態を有効にします。例:

```
Set-ProvScheme -provisioningSchemeName xxxx
-machineprofile <path-to-machineprofile-with-hibernation-enabled>
-serviceoffering "XDHyp:\HostingUnits\msc-dev\serviceoffering.
    folder\Standard_D4as_v5.serviceoffering"
```

5. マシンカタログ内の既存の VM で更新を要求します。

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeUid xxxx -VMName <
    String[]
```

6. VM を再起動して、既存の VM での更新をトリガーします。例:

```
New-BrokerHostingPowerAction -machinename "<name>" -Action Restart
```

休止状態のプロパティを確認する

PowerShell コマンドを使用して、マシンカタログ、VM、およびブローカーマシンの休止状態プロパティを確認できます:

- プロビジョニングスキームの休止状態プロパティを確認するには、次の PowerShell コマンドを実行します。`HibernationEnabled` パラメーターは`True`である必要があります。

```
(Get-ProvScheme -provisioningSchemeName <YourSchemeName>).
    VMMetadata -join "" |  ConvertFrom-Json | Select
    HibernationEnabled
```

- プロビジョニング VM の休止状態プロパティを確認するには、次の PowerShell コマンドを実行します。`SupportsHibernation` パラメーターは`True`である必要があります。


```
(Get-ProvVM -VMName <YourVMName>).CustomVmData | ConvertFrom-Json
    | Select SupportsHibernation
```

- ブローカーマシンの休止状態を確認するには、次の PowerShell コマンドを実行します。電源操作の ［一時停止］および ［再開］は休止機能を示します。

```
(Get-BrokerMachine -MachineName <YourMachineName>).
   SupportedPowerActions
```

休止状態対応の **VM** の電源管理

休止状態対応の VM に対して実行できる電源管理操作は、次のとおりです:

- VM を実行状態から一時停止にする
- VM を一時停止状態から再開する
- VM を一時停止状態から強制的にシャットダウンする
- VM を一時停止状態から強制的に再起動する

詳しくは、以下を参照してください:

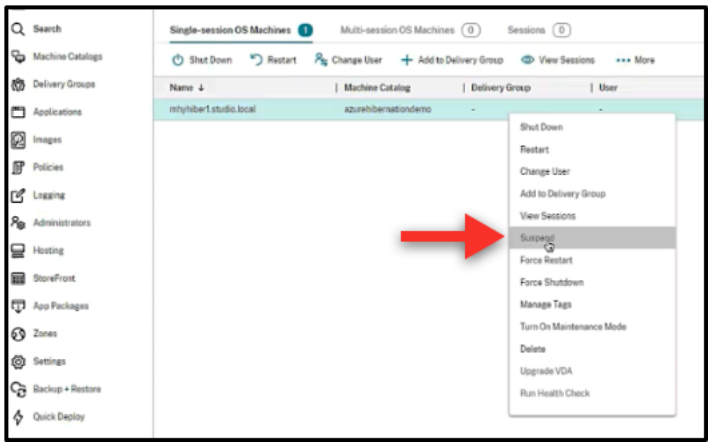
- 一時停止
- 再開

一時停止　次のいずれかの方法を使用して VM を一時停止できます:

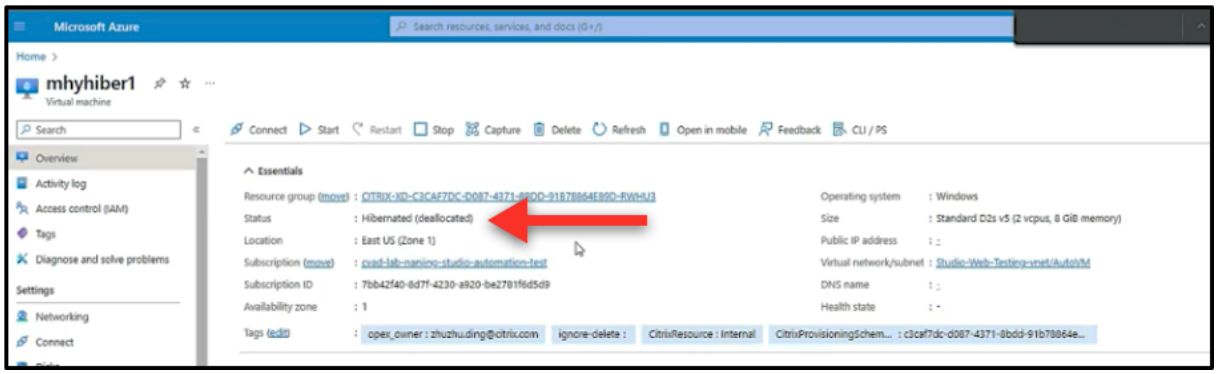
- Web Studio を使用して手動で行う
- タイムアウトポリシーを使用して自動的に行う: 詳しくは、「その他の設定」を参照してください。

VM を手動で一時停止するには:

1. VM を右クリックし、［一時停止］を選択します。［はい］をクリックしてアクションを確認します。［電源の状態］が ［一時停止中］から ［一時停止］に変わります。

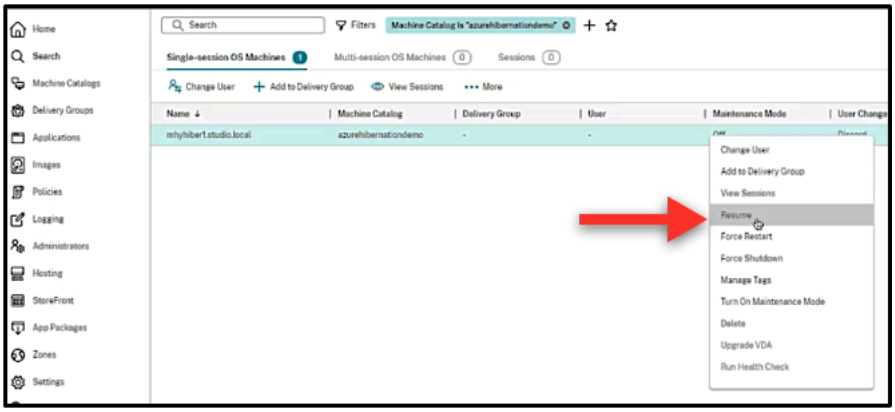


Azure Portal で VM のステータスを確認できます。

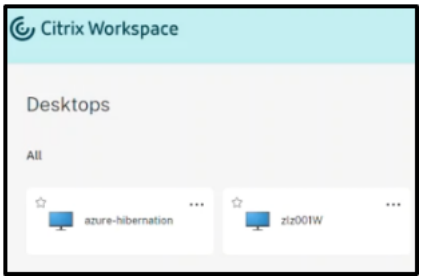


再開　休止状態の VM を再開するには、次のいずれかの方法を使用します:

- 手動:
  - 管理者は、Web Studio を使用して VM を再開できます。

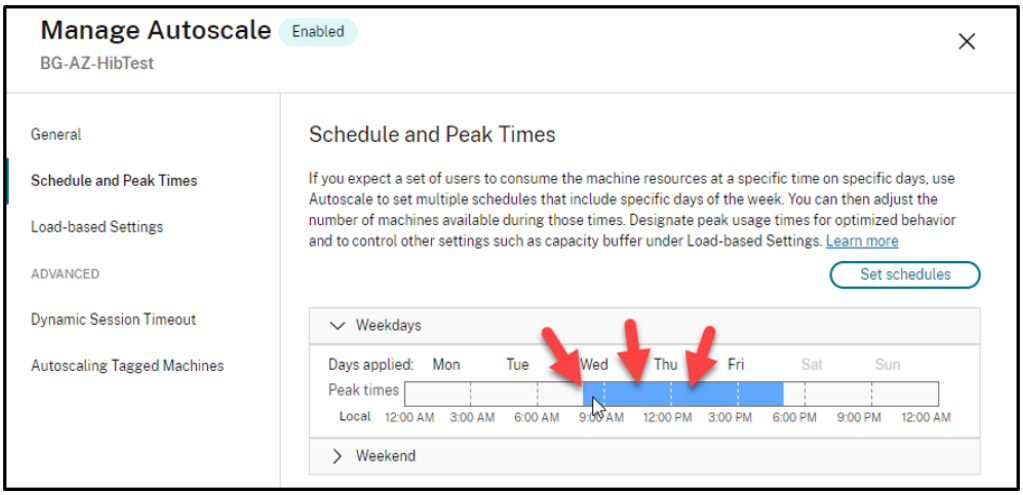


  - エンドユーザーは、デスクトップアイコンをクリックすると、Citrix Workspace メニューを使用して VM を起動できます。

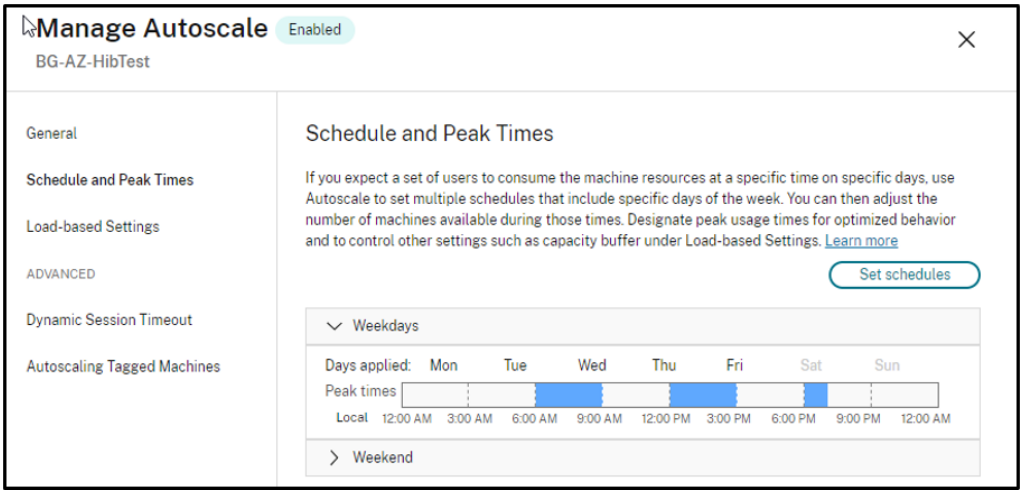


- 自動:
  - ピーク時間を正しく構成すると、Autoscale は休止状態のマシンの電源を自動的にオンにします。タイムスケジュールをクリックすると、ピーク時間を 30 分間隔で設定できます。青いフレームは、それぞれピーク時間としてマークされた時間枠を表します。ピーク時間には、連続した時間枠と連続しない時間枠があります。

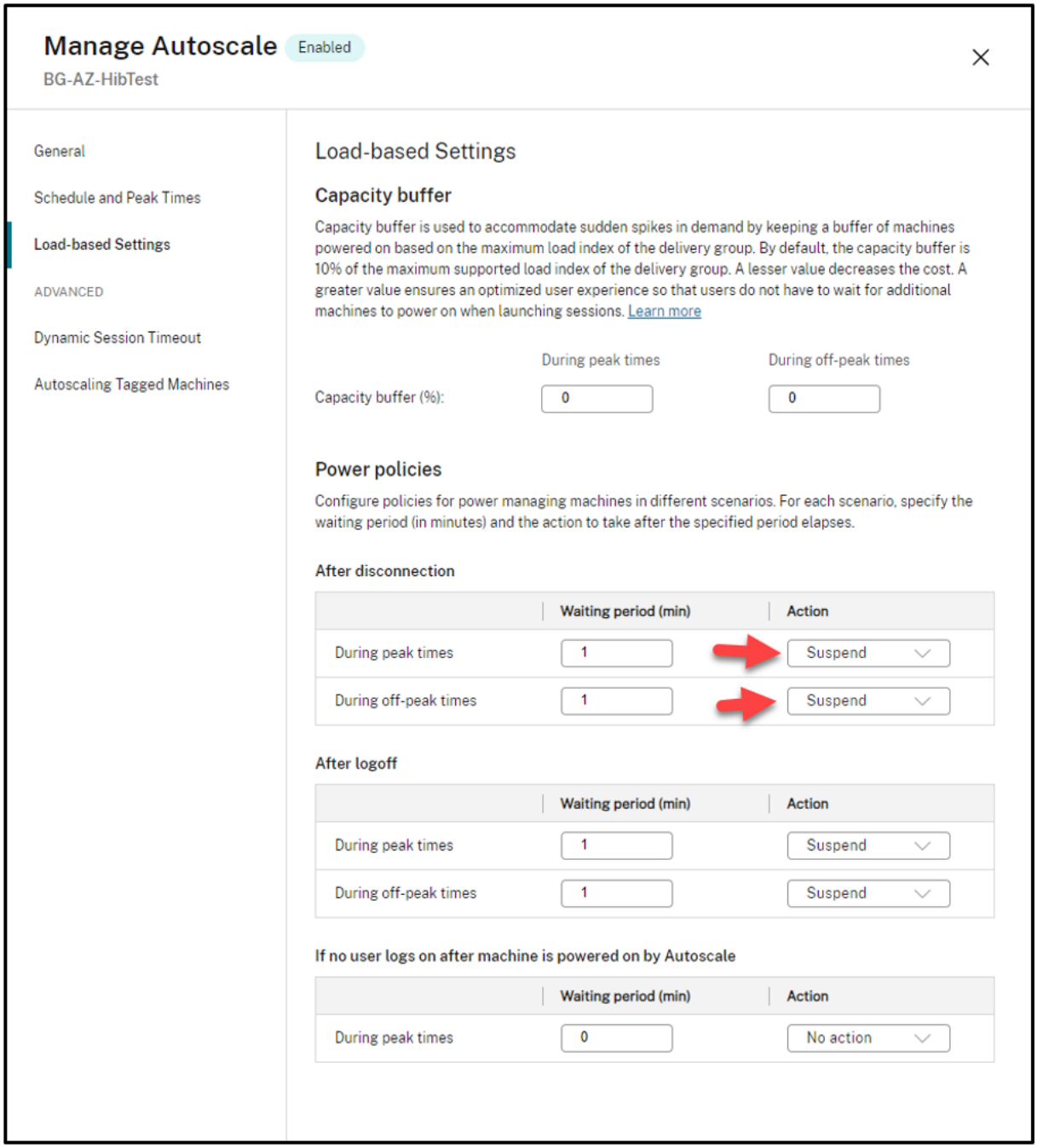
- 連続した時間枠



- 連続しない時間枠



> 注:
>
> [**Autoscale** の管理] > [負荷ベースの設定] で、[アクション] が [一時停止] として構成されている場合は、そのデリバリーグループ内のすべての VM に休止機能があることを確認してください。休止機能がないと、休止状態にできない VM は引き続き実行されます。



休止状態の失敗に関する警告メッセージを取得する

MCS でプロビジョニングされた、一時停止機能が有効な既存の仮想マシンの休止状態が失敗した場合は、PowerShell コマンド`Get-ProvOperationEvent`を使用して警告メッセージを表示できます。Powershell コマンドについて詳しくは、SDK ドキュメントGet-ProvOperationEventを参照してください。

これを行うには、以下の手順に従います:

1. PowerShell ウィンドウを開きます。
2. `asnp citrix*`を実行し、Citrix 固有の PowerShell モジュールをロードします。
3. 休止状態に失敗した場合に警告メッセージを表示するには、`Get-ProvOperationEvent`を実行します。

```
Get-ProvOperationEvent -filter {
  OperationName -eq "Suspend"  }
```

出力:

```
EventAdditionalData : Error code = OperationNotAllowed and Error message = The Hibernate-Deallocate Operation cannot be performed on a VM that has extension 'AzureHibernateExtension' in failed state. For more information, see https://aka.ms/hibernate-resume/errors. Error details from the extension : Enabling
                  hibernate failed. Response from the powercfg command. Exit Code: 1. Error message:
                  Hibernation failed with the following error: The request is not supported.

                  The following items are preventing hibernation on this system.
                    The current Device Guard configuration has disabled hibernation.
                    An internal system component has disabled hibernation.
                         Hypervisor
                  Status: 409
                  ErrorCode: OperationNotAllowed

                  Content:
                  {

                    "error": {

                      "code": "OperationNotAllowed",
                      "message": "The Hibernate-Deallocate Operation cannot be performed on a VM that has extension ' AzureHibernateExtension' in failed state. For more information, see https://aka.ms/hibernate-resume/errors. Error details from the extension : Enabling hibernate failed. Response from the
                  powercfg command. Exit Code: 1. Error message:\nHibernation failed with the following error: The request is not supported.\r\r\n\r\nThe following items are preventing hibernation on this system.\r\n\tThe current Device Guard configuration has disabled hibernation.\r\n\tAn internal system
```



```
                    component has disabled hibernation.\r\n\t\
                       tHypervisor"
                    }

                }

EventCategory       : Warning
EventDateTime       : 1/11/2024 4:18:31 AM
EventId             : 0
EventMessage        : Failed to suspend machine my-resource-group/
    my-vm.
EventSeverity       : Important
EventSource         : AzureRmPlugin
EventState          : New
LinkedObjectType    : ProvisioningScheme
LinkedObjectUid     : 589cb600-6e65-479f-9d47-9715c4732366
OperationName       : Suspend
OperationTargetName : my-resource-group/my-vm
OperationTargetType : VirtualMachine
OperationType       : PowerManagement
Recommendation      :
```

休止状態の問題のトラブルシューティング　休止状態とトラステッド起動の両方を仮想マシンで有効にしようとして、ゲスト OS の構成が正しくない場合、次のエラーメッセージが表示されます。

エラーコード	エラーメッセージ
OperationNotAllowed	拡張機能「AzureHibernateExtension」が失敗状態にある仮想マシンでは、Hibernate-Deallocate 操作を実行できません。詳しくは、https://aka.ms/hibernate-resume/errors/を参照してください。拡張機能からのエラーの詳細: 休止状態の有効化に失敗しました。powercfg コマンドからの応答。終了コード: 1。エラーメッセージ: 次のエラーにより休止状態に失敗しました: 要求はサポートされていません。次の項目により、このシステムでの休止状態が妨げられています。現在の **Device Guard** 構成では休止状態が無効になっています。内部システムコンポーネントによって休止状態が無効になっています。

この問題を解決するには、ゲスト仮想マシン内で仮想化が有効になっていることを確認します。たとえば、Windows 環境で Hyper-V が有効になっていることを確認します。Microsoft Windows の制限により、仮想マシンでトラステッド起動が有効になっている場合、休止状態は入れ子構造の仮想化でのみサポートされます。

警告メッセージについて詳しくは、Microsoft のドキュメント「休止状態のトラブルシューティング」を参照してく

ださい。

> 注:
>
> 仮想マシンの再開の失敗に関連するエラーメッセージは、将来のリリースで利用可能になります。

追加情報

Citrix Azure の休止状態について詳しくは、Citrix Tech Zone の記事を参照してください。

セキュリティポリシー

August 17, 2024

この記事では、サポートされているさまざまなクラウドサービスのセキュリティ機能について説明します。セキュリティ機能には以下が含まれます:

- セキュリティグループ
- セキュアブート
- 暗号化機能

セキュリティグループ

August 17, 2024

セキュリティグループは、仮想ネットワーク内のリソース間のネットワークトラフィックをフィルター処理するためのセキュリティ規則のグループです。セキュリティ規則は、さまざまなリソースの種類に対する受信ネットワークトラフィック、または送信ネットワークトラフィックを許可または拒否します。各規則は、次のプロパティを指定します:

- Name: ネットワークセキュリティグループ内の一意の名前
- Priority: 規則は優先度順に処理されます。数値が小さいほど優先度が高いため、数値が小さいほど大きい数値より先に処理されます
- Source または Destination: 任意の、または個別の IP アドレス、クラスレスドメイン間ルーティング（CIDR）ブロック（たとえば、10.0.0.0/24）、サービスタグ、またはアプリケーションセキュリティグループ
- Protocol: 各セキュリティグループの規則を追加する際の基準となるプロトコル
- Direction: 規則が受信または送信トラフィックに適用されるかどうか
- Port range: 個別のポートまたはポートの範囲を指定できます
- Action: 許可または拒否

サポートされているハイパーバイザーについて詳しくは、次を参照してください:

- AWS のセキュリティグループ
- Microsoft Azure のセキュリティグループ
- Google Cloud Platform のセキュリティグループ

AWS のセキュリティグループ

セキュリティグループは、VPC 内のインスタンスのトラフィックを制御する仮想ファイアウォールとして機能します。セキュリティグループにルールを追加することで、パブリックサブネット内のインスタンスがプライベートサブネット内のインスタンスと通信できるようになります。また、これらのセキュリティグループを仮想プライベートクラウド内の各インスタンスに関連付けることもできます。受信規則はインスタンスへの受信トラフィックを制御し、送信規則はインスタンスからの送信トラフィックを制御します。

イメージの準備中のネットワーク設定について詳しくは、「イメージの準備中のネットワーク設定」を参照してください。

インスタンスを起動するときに、1 つまたは複数のセキュリティグループを指定できます。セキュリティグループを構成するには、「セキュリティグループの構成」を参照してください。

Microsoft Azure のセキュリティグループ

Citrix Virtual Apps and Desktops は、Azure のネットワークセキュリティグループをサポートします。ネットワークセキュリティグループは、サブネットに関連付けられることが想定されています。詳しくは、「ネットワークセキュリティグループ」を参照してください。

ネットワークセキュリティグループについて詳しくは、「Azure Resource Manager イメージを使用してマシンカタログを作成する」を参照してください。

Google Cloud Platform のセキュリティグループ

マシンカタログの準備中に、カタログのマスターイメージシステムディスクとして機能するマシンイメージが準備されます。このプロセスが発生すると、ディスクは一時的に仮想マシンに接続されます。この VM は、すべての受信および送信ネットワークトラフィックが禁止された、分離された環境で実行する必要があります。これは、2 つの deny-all ファイアウォール規則によって実現されます。詳しくは、「ファイアウォール規則」を参照してください。

セキュアブート

August 17, 2024

セキュアブートは、信頼できるソフトウェアのみがシステムの起動に使用されるように設計されています。ファームウェアには、信頼できる証明書のデータベースがあり、ロードするイメージがいずれかの信頼できる証明書によって署名されていることを確認します。そのイメージがさらに別のイメージをロードする場合、その別のイメージも同じ方法で確認する必要があります。vTPM は、従来の物理 TPM モジュールを仮想化したソフトウェアインスタンスです。vTPM は、仮想マシンのブートチェーン全体（UEFI、OS、システム、およびドライバー）を測定することにより、構成証明を有効にします。

サポートされているクラウドサービスについて詳しくは、以下を参照してください:

- Google Cloud Platform でのセキュアブート
- Microsoft Azure でのセキュアブート
- VMware でのセキュアブート

Google Cloud Platform でのセキュアブート

シールドされた仮想マシンを GCP でプロビジョニングできます。シールドされた仮想マシンは、セキュアブート、仮想トラステッドプラットフォームモジュール、UEFI ファームウェア、整合性監視などの高度なプラットフォームセキュリティ機能を使用して、Compute Engine インスタンスの検証可能な整合性を提供する一連のセキュリティ制御によって強化されます。

PowerShell を使用してシールドされた VM でカタログを作成する方法について詳しくは、「PowerShell を使用してシールドされた VM でカタログを作成する」を参照してください。

> 注:
>
> マスターイメージに Windows 11 をインストールする場合は、マスターイメージの作成プロセス中に vTPM を有効にする必要があります。また、マシンプロファイルソース（VM またはインスタンステンプレート）で vTPM を有効にする必要があります。単一テナントノードで Windows 11 VM を作成する方法については、「単一テナントノードに Windows 11 VM を作成する」を参照してください。

Microsoft Azure でのセキュアブート

Azure 環境で、トラステッド起動を有効にしたマシンカタログを作成できます。Azure では、第 2 世代 VM のセキュリティをシームレスに向上させる方法として、トラステッド起動が提供されています。トラステッド起動は、高度かつ永続的な攻撃手法からの保護を提供します。トラステッド起動の根底にあるのは、VM のセキュアブートです。トラステッド起動は、vTPM を使用してクラウドによるリモート構成証明も実行します。これは、プラットフォームのヘルスチェックと、信頼ベースの決定を行うために使用されます。セキュアブートと vTPM を個別に有効にすることができます。トラステッド起動によるマシンカタログの作成について詳しくは、「トラステッド起動を使用したマシンカタログ」を参照してください。

VMware でのセキュアブート

MCS は、vTPM が組み込まれた VMware テンプレートをマシンプロファイルの入力のソースとして使用した、マシンカタログの作成をサポートします。Windows 11 がマスターイメージにインストールされている場合は、マスターイメージで vTPM を有効にすることが要件です。したがって、マシンプロファイルのソースである VMware テンプレートには、vTPM が組み込まれている必要があります。詳しくは、「マシンプロファイルを使用してマシンカタログを作成する」を参照してください。

暗号化機能

August 17, 2024

暗号化機能は、共有仮想マシンホスト上の悪意のあるゲストによる攻撃や、ホスト上のすべての仮想マシンを管理するハイパーバイザー制御ソフトウェアによって開始される攻撃から、仮想マシンのコンテンツを保護します。

サポートされているクラウドサービスについて詳しくは、以下を参照してください:

- AWS の暗号化機能
- Google Cloud Platform の暗号化機能
- Microsoft Azure の暗号化機能

AWS の暗号化機能

このセクションでは、AWS 仮想化環境の暗号化機能について説明します。

自動暗号化

新しい Amazon EBS Volume と、アカウントで作成されたコピーのスナップショットの自動暗号化をオンにすることができます。詳しくは、「自動暗号化」を参照してください。

Google Cloud Platform の暗号化機能

このセクションでは、Google Cloud Platform（GCP）仮想化環境の暗号化機能について説明します。

Google が管理する暗号キーよりもキーの操作を細かく制御する必要がある場合は、顧客管理暗号キーを使用できます。顧客管理暗号キーを使用する場合、オブジェクトはバケットに保存されるときに Cloud Storage によってキーで暗号化され、オブジェクトがリクエスタに提供されるときに Cloud Storage によって自動的に暗号化が解除されます。詳しくは、「顧客管理の暗号鍵」を参照してください。

MCS カタログでは、顧客管理暗号キー（CMEK：Customer Managed Encryption Keys）を使用できます。詳しくは、「顧客管理暗号キー（CMEK）の使用」を参照してください。

Microsoft Azure の暗号化機能

このセクションでは、Azure 仮想化環境の暗号化機能について説明します。

Azure サーバー側暗号化

ほとんどの Azure Managed Disks は、サーバー側暗号化（SSE）を使用してデータを保護し、セキュリティとコンプライアンスの必要性を満たすのに役立つ Azure Storage 暗号化で暗号化されています。Citrix Virtual Apps and Desktops は、Azure Key Vault を使用して Azure Managed Disks の顧客が管理する暗号化キーをサポートします。詳しくは、「Azure サーバー側暗号化」を参照してください。

ホストでの **Azure** ディスク暗号化

ホスト機能での暗号化を使用して、MCS マシンカタログを作成できます。

この暗号化方法は、Azure Storage でデータを暗号化しません。VM をホストするサーバーがデータを暗号化し、暗号化されたデータが Azure Storage サーバーを通過します。つまり、この暗号化方法はデータをエンドツーエンドで暗号化します。

ホストでの暗号化機能を使用した MCS マシンカタログの作成について詳しくは、「ホストでの Azure ディスク暗号化」を参照してください。

Azure の二重暗号化

二重暗号化とは、プラットフォーム側の暗号化（デフォルト）と顧客管理の暗号化（CMEK）です。したがって、暗号化アルゴリズム、実装、またはキーの侵害に関するリスクを懸念している、セキュリティに非常に敏感なお客様は、この二重暗号化を選択できます。永続的 OS ディスクとデータディスク、スナップショット、イメージはすべて二重暗号化により保存時に暗号化されます。詳しくは、「管理対象ディスクの二重暗号化」を参照してください。

Azure Confidential VM

Azure Confidential Computing VM によって、仮想デスクトップは確実にメモリ内で暗号化され、使用中に保護されます。

MCS を使用して、Azure Confidential VM を含むカタログを作成できます。このようなカタログを作成するには、マシンプロファイルワークフローを使用する必要があります。VM と ARM テンプレートスペックの両方をマシンプロファイル入力として使用できます。

詳しくは、「Azure Confidential VM」を参照してください。

デリバリーグループの作成

August 17, 2024

> 注:
>
> Web Studio（Web ベース）と Citrix Studio（Windows ベース）の 2 つの管理コンソールを使用して、Citrix Virtual Apps and Desktops の展開を管理できます。この記事では Web Studio のみを扱います。Citrix Studio について詳しくは、Citrix Virtual Apps and Desktops 7 2212 以前の同様の記事を参照してください。

デリバリーグループは、いくつかのマシンカタログから選択したマシンをグループ化したものです。デリバリーグループでは、それらのマシンを使用できるユーザーと、そのユーザーに提供するアプリケーションとデスクトップを指定します。

サイトおよびマシンカタログを作成した後、展開の構成における次の手順となるのが、デリバリーグループの作成です。その後、最初のデリバリーグループの初期設定を変更し、別のデリバリーグループを作成することができます。また、デリバリーグループの作成時ではなく、その編集時にのみ構成できる機能と設定もあります。

リモート PC アクセスでサイトを作成すると、「リモート PC アクセスデスクトップ」という名前のデリバリーグループが自動的に作成されます。

デリバリーグループを作成するには:

1. デリバリーグループなしでサイトとマシンカタログを作成した場合、デリバリーグループを作成するための説明が Web Studio に表示されます。
2. 既にデリバリーグループを作成済みで別のデリバリーグループを作成する場合は、次の手順に従います:
   a) ［デリバリー グループ］を選択します。操作ペインで ［デリバリーグループの作成］を選択します。
   b) フォルダーを使用してデリバリーグループを整理するには、デフォルトの ［**Delivery Groups**］フォルダーの下にフォルダーを作成します。詳しくは、「フォルダーの作成」を参照してください。
   c) グループを作成するフォルダーを選択し、［デリバリーグループの作成］をクリックします。グループ作成ウィザードが開きます。
3. ウィザードが起動され、［はじめに］ページが表示されます。このページは、今後このウィザードが起動されたときに開かないように設定できます。
4. 次に、ウィザードの指示に従って、以下のセクションで説明されているページの操作を行います。各ページの操作を終えたら、最後のページに到達するまで ［次へ］をクリックします。

手順 **1**: マシン

［マシン］ページでカタログを選択して、そのカタログから使用するマシンの番号を選択します。

ヒント:

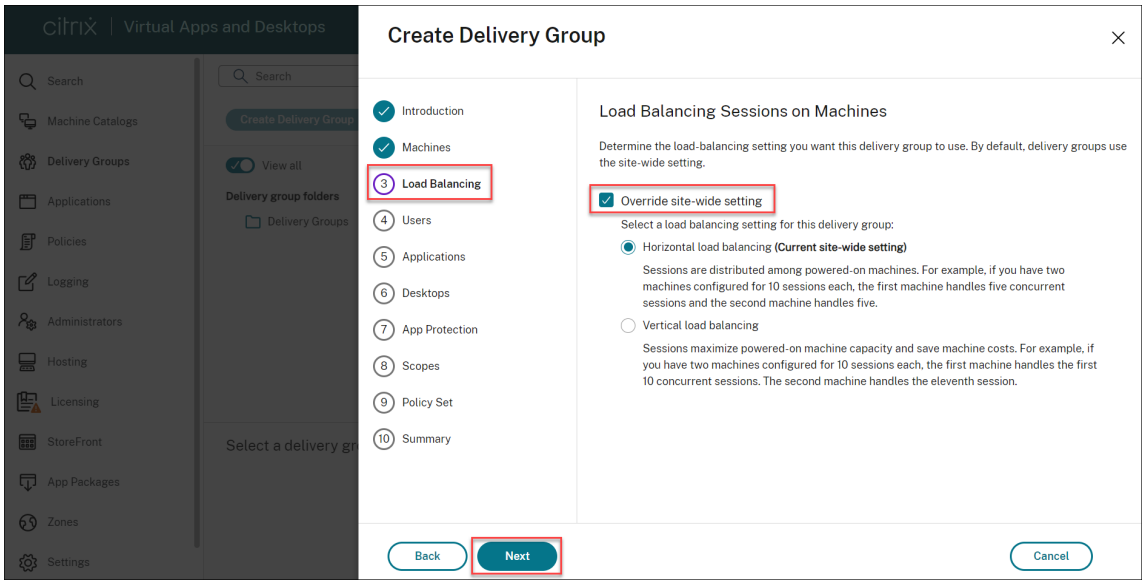
- マシンカタログに未使用のマシンが残っていない場合、そのカタログを選択することはできません。
- カタログは、複数のデリバリーグループで指定できます。マシンは 1 つのデリバリーグループでのみ使用できます。
- 1 つのデリバリーグループで、複数のマシンカタログのマシンを使用できますが、これらのマシンカタログに同じ種類のマシン（マルチセッション OS、シングルセッション OS、リモート PC アクセス）が含まれている必要があります。つまり、異なる種類のマシンをデリバリーグループに混在させることはできません。同様に、展開に Windows マシンのカタログと Linux マシンのカタログが含まれている場合、デリバリーグループには、両方ではなくいずれかの種類のオペレーティングシステムのマシンのみを含めることができます。
- すべてのマシンで最新の VDA バージョンをインストールする、またはアップグレードすることをお勧めします。必要に応じて、カタログとデリバリーグループをアップグレードします。デリバリーグループの作成時に、異なる VDA バージョンがインストールされたマシンを選択した場合、デリバリーグループは最も古いバージョンと互換性を持ちます。この最も古いバージョンが、グループの機能レベルとなります。たとえば、マシンの 1 つに VDA Version 7.1 がインストールされており、ほかのマシンには最新バージョンがインストールされている場合、グループ内のすべてのマシンで使用できるのは、VDA 7.1 でサポートされていた機能のみです。すなわち、より新しい VDA バージョンを必要とする機能を、このデリバリーグループで利用できない可能性があります。
- リモート PC アクセスカタログの各マシンは自動的にデリバリーグループに関連付けられます。リモート PC アクセスサイトを作成すると、「リモート PC アクセスマシン」という名前のカタログと、「リモート PC アクセスデスクトップ」という名前のデリバリーグループが自動的に作成されます。
- 次の互換性チェックが実行されます：
  - MinimumFunctionalLevel に互換性があること
  - SessionSupport に互換性があること
  - AllocationType は SingleSession に対する互換性があること
  - ProvisioningType に互換性があること
  - PersistChanges は MCS および Citrix Provisioning に対する互換性があること
  - RemotePC カタログは Remote PC カタログとのみ互換性があること
  - AppDisk 関連のチェック

手順 **2**：負荷分散

デリバリーグループの作成時に負荷分散設定を構成するには、次の手順を実行します：

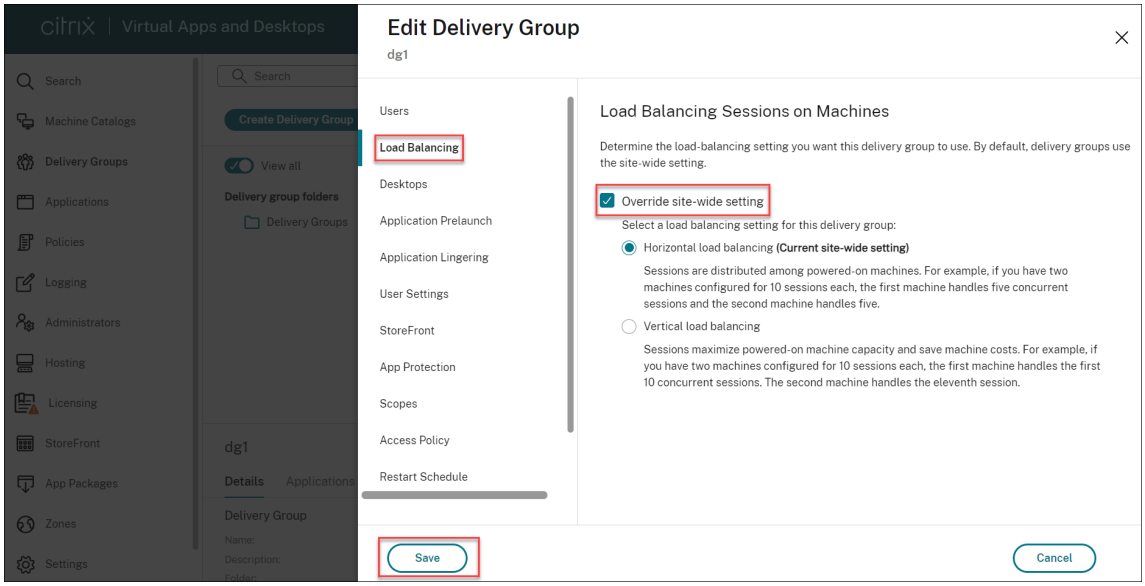
1. Web Studio にサインインします。
2. 左側のナビゲーションで、［デリバリーグループ］をクリックします。
3. ［デリバリーグループ］ページで、［デリバリーグループの作成］をクリックします。
4. デリバリーグループの作成ウィザードで、［次へ］をクリックします。［マシン］ウィザードが開きます。
5. ［マシン］ウィザードで、必要なマシンカタログを選択し、［次へ］をクリックします。負荷分散ウィザードが開きます。

6. 負荷分散 ウィザードで、［サイト全体の設定を上書きする］チェックボックスを選択します。
7. 必要に応じて ［水平負荷分散］または ［垂直負荷分散］オプションを選択し、［次へ］をクリックします。

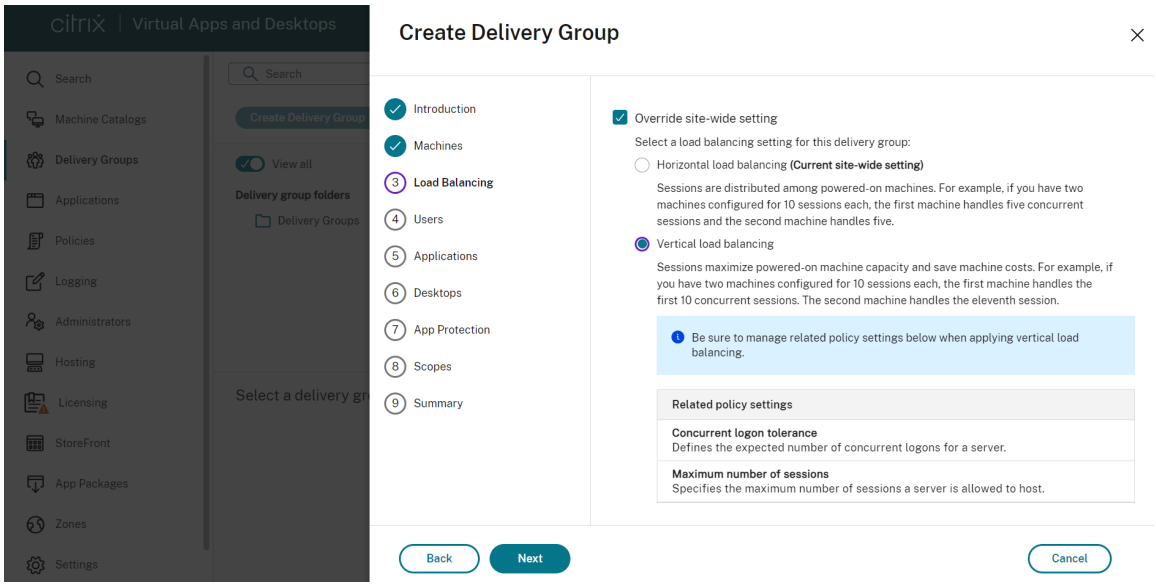


既存のデリバリーグループの編集中に負荷分散設定を構成するには、次の手順を実行します：

1. Web Studio にサインインします。
2. 左側のペインで、［デリバリーグループ］をクリックします。
3. 一覧から ［デリバリーグループ］を選択し、［編集］をクリックします。デリバリーグループの編集ウィザードが開きます。
4. ［デリバリーグループの編集］ページで、［負荷分散］をクリックします。
5. ［サイト全体の設定を上書きする］チェックボックスを選択します。
6. 必要に応じて ［水平負荷分散］または ［垂直負荷分散］オプションを選択し、［保存］をクリックします。



> 注:
>
> 垂直負荷分散設定が適用されている場合は、［同時ログオントレランス］と ［最大セッション数］ポリシーが適切に構成されていることを確認してください。



サイトおよびデリバリーグループレベルでの負荷分散について詳しくは、「マシンの負荷分散」を参照してください

手順 **3**: 配信の種類

このページは、静的な（割り当て済み）シングルセッションOS マシンを含むカタログを選択した場合にのみ開きます。

［配信の種類］ページで ［アプリケーション］か ［デスクトップ］を選択します。両方を有効にすることはできません。

マルチセッション OS またはシングルセッション OS ランダム（プール）カタログのマシンを選択した場合、配信の種類はアプリケーションとデスクトップと見なされます：この場合は、アプリケーションかデスクトップ、またはその両方を配信できます。

手順 **4**：ユーザー

このデリバリーグループで配信されるアプリケーションやデスクトップを使用できるユーザーおよびユーザーグループを指定します。

ユーザー一覧の指定場所

以下の作成時または編集時に、Active Directory ユーザー一覧を指定します。

- サイトのユーザーアクセス一覧（Web Studio では構成しません）。アプリケーション資格ポリシー規則には、デフォルトではすべてのユーザーが含まれます。詳しくは、PowerShell SDK の`BrokerAppEntitlementPolicyRule`コマンドレットを参照してください。
- アプリケーショングループ（構成されている場合）。
- デリバリーグループ。
- アプリケーション。

StoreFront 経由でアプリケーションにアクセスできるユーザーの一覧は、上記のユーザー一覧の共通部分になります。たとえば、ほかのグループに対して極端なアクセス制限をせずに、特定の部門に対してアプリケーション A の使用を構成するには次のように設定します。

- 全ユーザーが含まれる、デフォルトのアプリケーション資格ポリシー規則を使用します。
- デリバリーグループで指定されたすべてのアプリケーションをすべての本社ユーザーが使用できるよう、デリバリーグループのユーザー一覧を構成します。
- （アプリケーショングループが構成されている場合）アプリケーション A～L に管理部門および財務部門のメンバーがアクセスできるよう、アプリケーショングループのユーザー一覧を構成します。
- 管理部門と財務部門のアカウントを受信可能なユーザーのみに表示されるよう、アプリケーション A のプロパティを構成します。

認証が必要なユーザーおよび認証が不要なユーザー

ユーザーには、認証が必要なユーザーと認証が不要なユーザーの 2 種類があります（認証が不要なユーザーは「匿名ユーザー」とも呼ばれます）。いずれか一方または両方の種類のユーザーをデリバリーグループ内に構成できます。

- 認証が必要なユーザー：特定のアカウント名で指定したユーザーおよびグループメンバーは、アプリケーションとデスクトップにアクセスするときに、StoreFront または Citrix Workspace アプリで資格情報（スマートカード、またはユーザー名とパスワードなど）による認証を求められます。デリバリーグループにシングルセッションOS マシンが含まれる場合、後にそのデリバリーグループを編集することでユーザーデータ（ユーザーの一覧）をインポートできます。
- 認証が不要なユーザー（匿名ユーザー）：マルチセッション OS マシンを含むデリバリーグループでは、StoreFront または Citrix Workspace アプリでの認証が不要な匿名アクセスを許可できます。たとえば、キオスクのアプリケーションでは資格情報を必須にして、Citrix アクセスポータルやツールでは不要にできます。最初の Delivery Controller をインストールすると、匿名のユーザーグループが作成されます。

  認証が不要なユーザーのアクセスを許可するには、デリバリーグループの各マシンに VDA for Windows Server OS（Version 7.6 以降）がインストールされている必要があります。認証が不要なユーザーのアクセスを有効にする場合は、認証が不要な StoreFront ストアを作成しておく必要があります。

  認証が不要なユーザーアカウントはセッション開始時にオンデマンドで作成され、Anon*XYZ*（*XYZ* は一意の 3 桁の値）という名前が付けられます。

  認証が不要なユーザーセッションにはデフォルトで 10 分のアイドルタイムアウトが設定され、セッションを切断すると自動的にログオフされます。切断セッションへの再接続、デバイス間のローミング、およびワークスペースコントロールはサポートされません。

次の表に、［ユーザー］ページでの選択肢を示します：

アクセスを許可するユーザー	ユーザーおよびユーザーグループを追加/割り当てるかどうか	［認証が不要な（匿名）ユーザーのアクセスを許可する］チェックボックスをオンにするかどうか
認証が必要なユーザーのみ	はい	いいえ
認証が不要なユーザーのみ	いいえ	はい
認証が必要なユーザーおよび認証が不要なユーザー	はい	はい

手順 **5**：アプリケーション

ヒント：

- アプリケーションをデリバリーグループに追加すると、デフォルトで「アプリケーション」という名前のフォルダー内に表示されます。別のフォルダーを指定することもできます。詳しくは、「アプリケーションの管理」を参照してください。
- アプリケーションのプロパティは、デリバリーグループへの追加時、または後で変更できます。詳しくは、「アプリケーションの管理」を参照してください。

- アプリケーションの追加時にそのフォルダー内に同じ名前のアプリケーションが存在する場合、追加するアプリケーションの名前を変更するよう指示するメッセージが表示されます。名前の変更を拒否すると、アプリケーションはサフィックス付きで追加され、そのアプリケーションフォルダー内で名前が一意になります。
- アプリケーションを複数のデリバリーグループに追加する場合、そのすべてのデリバリーグループのアプリケーションを見ることができる十分な権限を有していなければ、表示上の問題が発生する可能性があります。そのような問題が発生した場合は、より上位の権限を持つ管理者に相談するか、または自身の権限を拡張して、アプリケーションを追加したデリバリーグループをすべて含めるようにします。
- 2 つのアプリケーションを同じ名前で同じユーザーに公開する場合は、Web Studio で［アプリケーション名（ユーザー用）］プロパティの名前を変更します。これを行わないと、ユーザーの Citrix Workspace アプリに同じ名前が 2 つ表示されます。
- パッケージアプリケーションを、シングルセッションの静的デリバリーグループおよびリモート PC アクセスのデリバリーグループに追加できます。これらのパッケージは、ユーザーがデスクトップまたはリモート PC にサインインするたびに自動的にマウントされます。

［追加］をクリックして、アプリケーションのソースを表示します。

- ［スタート］メニューから：選択したカタログのマスターイメージから作成されたマシンで検出されたアプリケーション。このソースを選択すると、新たなページが開き、検出されたアプリケーションが一覧表示されるので、追加するアプリケーションを選択して［**OK**］をクリックします。
- 手動：デリバリーグループまたはネットワーク内の別の場所にある VDA 上のアプリケーション。このソースを選択すると、次の方法により、追加するアプリケーションを指定する新しいページが開きます：
  - 実行可能ファイルのパス、作業ディレクトリ、コマンドライン引数（オプション）、管理者およびユーザー用の表示名を入力します。
  - デリバリーグループ内の VDA からアプリケーションを選択します。これを行うには、［参照］をクリックして、VDA にアクセスするための資格情報を入力し、VDA に接続されたあと、VDA からアプリケーションを選択します。選択したアプリケーションのプロパティが、ページ内のフィールドに自動的に入力されます。
- 既存：過去にサイトに追加された、おそらく別のデリバリーグループのアプリケーション。このソースを選択すると、新たなページが開き、検出されたアプリケーションが一覧表示されます。アプリケーションを追加し、［**OK**］をクリックします。
- アプリケーションパッケージ： App-V、MSIX、MSIX アプリのアタッチアプリケーションパッケージ内のアプリケーション。このソースを選択すると、新しいページが起動し、そこでソースの種類を選択して、結果の表示から追加するアプリケーションを選択できます。

あるアプリケーションのソースまたはアプリケーションが選択できない、または無効な場合、そのアプリケーションは見ることができないか、選択できないかのどちらかです。たとえば、サイトに追加されたアプリケーションがない場合、［既存］のソースを選択することはできません。アプリケーションが、選択したカタログのマシン上でサポートされるセッションタイプとの互換性を備えていない場合も同様です。

手順 **6**：デスクトップ

このページのタイトルは、［マシン］ページで選択したカタログによって異なります：

- プールされたマシンを含むマシンカタログを選択した場合、このページのタイトルは ［デスクトップ］になります。
- シングルセッションの静的マシンを含むマシンカタログを選択し、［配信の種類］ページで「デスクトップ」を指定した場合、このページのタイトルは「デスクトップユーザー割り当て」になります。
- シングルセッションの静的マシンを含むマシンカタログを選択し、［配信の種類］ページで「アプリケーション」を指定した場合、このページのタイトルは「アプリケーションマシンユーザー割り当て」になります。

［追加］をクリックします。ダイアログボックスで次の操作を実行します：

- ［表示名］フィールドと［説明］フィールドに、Citrix Workspace アプリで表示する情報を入力します。
- デスクトップにタグによる制限を追加するには、［タグでマシンの起動を制限します］をオンにして、ドロップダウンリストからタグを選択します。詳しくは、「タグ」を参照してください。
- ラジオボタンを使用して、デスクトップを起動するか、デスクトップの起動時にマシンを割り当てます。このデリバリーグループにアクセスできるあらゆるユーザー、または特定のユーザーやユーザーグループを指定できます。
- シングルセッションの静的マシンがグループに含まれる場合、ユーザーあたりの最大デスクトップ数を指定します。1 以上の値を入力する必要があります。
- （プールされたマシンの）デスクトップ、または（シングルセッションの静的マシンに対する）デスクトップ割り当て規則を有効または無効にします。デスクトップを無効にすると、デスクトップ配信が停止します。デスクトップ割り当て規則を無効にすると、ユーザーへのデスクトップの自動割り当てが停止されます。
- ダイアログボックスの操作を終了したら、［**OK**］をクリックします。

サイト内の最大デスクトップインスタンス数（**PowerShell** のみ）

サイト内の最大デスクトップインスタンス数を構成するには（PowerShell のみ）：

- PowerShell で、適切な BrokerEntitlementPolicyRule コマンドレットに MaxPerEntitlementInstances パラメーターを指定して実行します。たとえば、次のコマンドレットでは、`tsvda-desktop`ルールを変更して、サイト内で同時に実行できるデスクトップインスタンス数の上限を 2 に設定します。デスクトップインスタンスが 2 つ実行されている場合、3 人目のサブスクライバーがデスクトップを起動しようとするとエラーが発生します。

  ```
  Set-BrokerEntitlementPolicyRule -Name tsvda-desktop -MaxPerEntitlementInst
    2
  ```

- 詳しくは、Get-Help コマンドレットを使用してください。例：`Get-Help Set-BrokerEntitlementPolicyRu -Parameter MaxPerEntitlementInstances`。

手順 **7**：ローカルホストキャッシュ設定

この設定は、電源管理されたシングルセッションのプールされたマシンを含むデリバリーグループにのみ表示されます。

デフォルトでは、ローカルホストキャッシュ（LHC）モードの場合、漏えいの危険があるため、これらのマシンは使用できません。デフォルトの動作を変更して、LHC モードのときに新しいユーザー接続で使用できるようにするには、［リソースを使用可能な状態に維持する］を選択します。

または、PowerShell コマンドを使用してデフォルトの動作を変更することもできます。詳しくは、「アプリケーションおよびデスクトップのサポート」を参照してください。

> 重要：
>
> 電源管理された、シングルセッションのプールされたマシンへのアクセスを有効にすると、以前のユーザーセッションからのデータと変更が後続のセッションに残る可能性があります。

手順 **8**：まとめ

デリバリーグループの名前を入力します。オプションで、Citrix Workspace アプリと Web Studio に表示される説明を入力することもできます。

概要の情報を確認し、［完了］をクリックします。

デリバリーグループの管理

August 17, 2024

> 注：
>
> Web Studio（Web ベース）と Citrix Studio（Windows ベース）の 2 つの管理コンソールを使用して、Citrix Virtual Apps and Desktops の展開を管理できます。この記事では Web Studio のみを扱います。Citrix Studio について詳しくは、Citrix Virtual Apps and Desktops 7 2212 以前の同様の記事を参照してください。

はじめに

この記事では、管理コンソールでデリバリーグループを管理する手順について説明します。グループ作成時に指定した設定を変更できるほかに、デリバリーグループ作成時には使用できなかった設定を構成することも可能です。

手順のカテゴリには、全般、ユーザー、マシン、セッションなどがあります。タスクによっては複数のカテゴリに関係します。たとえば、「マシンへのユーザーの接続を禁止する」のタスクはマシン設定のカテゴリで説明されています

が、ユーザー設定のカテゴリにもかかわります。あるカテゴリで見つからないタスクがある場合は、関連するカテゴリを確認してください。

この他の記事にも関連情報が記載されています:

- 「アプリケーション」には、デリバリーグループでのアプリケーションの管理に関する情報が記載されています。
- デリバリーグループを管理するには、デリバリーグループ管理者の組み込みの役割権限が必要です。詳しくは、「委任管理」を参照してください。

一般

- グループの詳細の表示
- 配信方法の変更
- StoreFront アドレスの変更
- 機能レベルの変更
- リモート PC アクセスのデリバリーグループの管理
- フォルダーを使用したデリバリーグループの整理
- App Protection の管理

グループの詳細の表示

1. 検索機能を使用して、特定のデリバリーグループを見つけます。手順については、「インスタンスの検索」を参照してください。
2. 検索結果から必要に応じてグループを選択します。
3. グループ列の説明については、次の表を参照してください。
4. このグループの詳細については、下部の詳細ペインのタブをクリックしてください。

列	説明
デリバリーグループ	グループ名とセッションの種類。セッションの種類には、シングルセッション OS とマルチセッション OS があります。
配信	このグループから配信されるリソースの種類。設定可能な値には、アプリケーション、デスクトップ、およびアプリケーションとデスクトップが含まれます。デリバリーグループが専用マシンで構成されている場合、「静的マシン割り当て」が表示されます。
使用中のセッション	セットアップされているマシンの数と、切断状態にあるマシンの数。

列	説明
割り当て済み（個）	デリバリーグループに割り当てられたカタログ内のマシンの数。
フォルダー	デリバリーグループツリー内のグループの場所。グループが含まれているフォルダーの名前（末尾のバックスラッシュを含む）、またはグループがルートレベルにある場合は–が表示されます。

デリバリーグループの配信の種類の変更

配信の種類は、アプリケーション、デスクトップ、またはその両方のうち、そのグループが配信できるものを示します。

この種類を ［アプリケーションのみ］または ［デスクトップおよびアプリケーション］から ［デスクトップのみ］に変更する前に、グループからすべてのアプリケーションを削除します。

1. 左側のペインで ［デリバリーグループ］を選択します。
2. グループを選択して、操作バーの ［編集］をクリックします。
3. ［配信の種類］ページで、配信の種類を選択します。
4. ［適用］をクリックして、ウィンドウを閉じずに行った変更を適用します。または、［保存］をクリックして、変更を適用してウィンドウを閉じます。

StoreFront アドレスの変更

1. 左側のペインで ［デリバリーグループ］を選択します。
2. グループを選択して、操作バーの ［編集］をクリックします。
3. **StoreFront** ページで、StoreFront URL を選択または追加します。この URL は、デリバリーグループの各マシンにインストールされた Citrix Workspace アプリで使用されます。
4. ［適用］をクリックして、ウィンドウを閉じずに行った変更を適用します。または、［保存］をクリックして、変更を適用してウィンドウを閉じます。

StoreFront サーバーのアドレスは、後で指定することもできます。これを行うには、左側のペインで［**StoreFront**］を選択します。

機能レベルの変更

デリバリーグループの機能レベルの変更は、マシン上の VDA、およびデリバリーグループで使用されているマシンを含むマシンカタログをアップグレードしてから行ってください。

以下の点に注意してください：

- Citrix Provisioning（旧称 Provisioning Services）を使用している場合は、Citrix Provisioning コンソールで VDA をアップグレードします。
- アップグレードした VDA がインストールされているマシンを起動して、Delivery Controller に登録します。この処理によって、デリバリーグループで必要なアップグレードがコンソールで特定されます。
- 古いバージョンの VDA を使い続けると、新しい製品の機能を使用できません。詳しくは、アップグレードのドキュメントを参照してください。

デリバリーグループをアップグレードするには:

1. 左側のペインで ［デリバリーグループ］を選択します。
2. グループを選択して、操作バーの ［デリバリーグループのアップグレード］をクリックします。［機能レベルの変更］アクションは、アップグレードされた VDA が検出された場合にのみ表示されます。

ディスプレイには、機能レベルに変更できないマシンがある場合、そのマシンとその理由が表示されます。その後、変更アクションをキャンセルし、マシンの問題を解決してから変更アクションを再度実行できます。

変更が完了したら、マシンを以前の状態に戻すことができます。デリバリーグループを選択して、操作バーの ［機能レベルの変更を元に戻す］を選択します。

リモート **PC** アクセスのデリバリーグループの管理

リモート PC アクセスマシンカタログで割り当てられていないマシンは、そのカタログに関連付けられたデリバリーグループに一時的に割り当てられます。この一時的な割り当てにより、そのマシンを後でユーザーに割り当てられるようになります。

デリバリーグループとマシンカタログとの関連付けには優先度値があります。この優先度により、マシンをシステムに登録したとき、またはユーザーがマシンの割り当てを必要としたときに、マシンに割り当てられるデリバリーグループが決定されます。この値が小さいほど優先度が高くなります。リモート PC アクセスマシンカタログに複数のデリバリーグループ割り当てがある場合、優先度が最も高い割り当てが選択されます。この優先度値は設定するには PowerShell SDK を使用します。

リモート PC アクセス用のマシンカタログの初回作成時に、デリバリーグループが関連付けられます。このカタログに後から追加したマシンアカウントまたは組織単位を、このデリバリーグループに追加することができます。この関連付けは、必要に応じて有効にしたり無効にしたりできます。

リモート PC アクセスマシンカタログとデリバリーグループとの関連付けを追加または削除するには:

1. 左側のペインで ［デリバリーグループ］を選択します。
2. リモート PC アクセスのグループを選択します。
3. ［詳細］セクションで ［マシンカタログ］タブをクリックし、リモート PC アクセス用のカタログを選択します。
4. 関連付けを追加または復元するには、［デスクトップの追加］をクリックします。関連付けを削除するには、［関連付けの削除］をクリックします。

フォルダーを使用したデリバリーグループの整理

簡単にアクセスできるように、フォルダーを作成してデリバリーグループを整理できます。

必須の役割　デフォルトでは、デリバリーグループフォルダーを作成および管理するには、次の組み込みの役割が必要です：クラウド管理者、完全な管理者、またはデリバリーグループ管理者。必要に応じて、デリバリーグループフォルダーを作成および管理するための役割をカスタマイズできます。詳しくは、「必要な権限」を参照してください。

デリバリーグループフォルダーの作成　開始する前に、デリバリーグループを整理する方法を計画します。以下に注意してください：

- 最大で 5 レベルまでの階層構造でフォルダーをネストできます（デフォルトのルートフォルダーを除く）。
- フォルダーには、デリバリーグループとサブフォルダーを含めることができます。
- バックエンドのフォルダーツリーは、すべてのノード（［マシンカタログ］や ［アプリケーション］、および［デリバリーグループ］ノードなど）で共有されます。フォルダーの名前変更や移動時に他のノードと名前が競合しないように、異なるノードの第 1 レベルのフォルダーには異なる名前を付けることをお勧めします。

デリバリーグループフォルダーを作成するには、次の手順に従います：

1. 左側のペインで ［デリバリーグループ］を選択します。
2. フォルダー階層でフォルダーを選択し、［アクション］バーで ［フォルダーの作成］を選択します。
3. 新しいフォルダーの名前を入力し、［完了］をクリックします。

> ヒント：
>
> 意図しない場所にフォルダーを作成した場合は、それを正しい場所にドラッグできます。

デリバリーグループの移動

デリバリーグループはフォルダー間で移動できます。詳細な手順は次のとおりです：

1. 左側のペインで ［デリバリーグループ］を選択します。
2. フォルダー別にグループを表示します。フォルダー階層の上にある ［すべて表示］をオンにして、一度にすべてのグループを表示することもできます。
3. グループを右クリックしてから、［デリバリーグループの移動］を選択します。
4. グループの移動先のフォルダーを選択し、［完了］をクリックします。

> ヒント：
>
> グループはフォルダーにドラッグできます。

デリバリーグループフォルダーの管理

デリバリーグループフォルダーの削除、名前変更、および移動を行うことができます。

フォルダーの削除は、フォルダーとそのサブフォルダーにデリバリーグループが含まれていない場合にだけ可能となりますのでご注意ください。

フォルダーを管理するには、次の手順に従います:

1. 左側のペインで ［デリバリーグループ］を選択します。
2. フォルダー階層でフォルダーを選択し、必要に応じて ［アクション］バーでアクションを選択します:
   - フォルダーの名前を変更するには、［フォルダーの名前変更］を選択します。
   - フォルダーを削除するには、［フォルダーの削除］を選択します。
   - フォルダーを移動するには、［フォルダーの移動］を選択します。
3. 画面の指示に従って、残りの手順を完了します。

必要な権限　次の表に、デリバリーグループフォルダーでアクションを実行するために必要な権限を示します。

アクション	必要な権限
デリバリーグループフォルダーの作成	デリバリーグループフォルダーの作成
デリバリーグループフォルダーの削除	デリバリーグループフォルダーの削除
デリバリーグループフォルダーの移動	デリバリーグループフォルダーの移動
デリバリーグループフォルダー名の変更	デリバリーグループフォルダーの編集
デリバリーグループのフォルダーへの移動	デリバリーグループフォルダーの編集およびデリバリーグループプロパティの編集

App Protection の管理

次の情報は、「App Protection」の記事を補足するものです。次の詳細に注意してください:

- App Protection の有効な使用権が必要です。App Protection 機能を購入するには、Citrix の営業担当者にお問い合わせください。
- App Protection には XML 信頼が必要です。XML 信頼を有効にするには、［設定］**>** ［**XML** 信頼を有効にする］に移動します。
- 画面キャプチャ防止機能について:
  - Windows と macOS では、保護されたコンテンツのウィンドウのみが空白になります。保護されたウィンドウが最小化されていない場合に、App Protection がアクティブになります。

- Linux では、キャプチャ全体が空白になります。App Protection は、保護されたウィンドウが最小化されているかどうかに関係なくアクティブです。

デリバリーグループの App Protection 方法を選択するには、次の手順を実行します:

1. 左側のペインで ［デリバリーグループ］を選択します。
2. グループを選択して、操作バーの ［編集］を選択します。
3. [**App Protection**］ページには、次のオプションが表示されます:

オプション	説明
Do not apply	設定を適用しない場合はこのオプションを選択します。
Apply to this delivery group	［キーロガー対策］および/または ［スクリーンキャプチャ対策］オプションを選択します。各設定にマウスを合わせると、ツールヒントの詳細が表示されます。
Apply contextually	この設定を適用するには、［アクセスポリシー］設定ページでアクセスポリシーを構成します。 a) 左側ペインで ［アクセスポリシー］をクリックし、［追加］をクリックします。 b) ［ポリシーの追加］ページで、次の操作を行います • i. ［ポリシー名］を入力し、必要に応じて設定を構成します。 • ii. ［フィルター］フィールドと ［値］フィールドに詳細を入力し、［完了］をクリックします。新しいポリシーは、［**App Protection**］ページに表示されます。このポリシーに必要な設定を有効にします。 • iii. ［保存］をクリックします。

4. ［デリバリーグループ］ページで、［デリバリーグループ］を選択して ［詳細］をクリックします。適用された新しい **App Protection** 設定が表示されます。

ユーザー

このセクションでは以下のトピックについて説明します:

- ユーザー設定の変更
- ユーザーの追加と削除
- ユーザー割り当ての管理

デリバリーグループのユーザー設定を変更する

このページの名前には、［ユーザー設定］または ［基本設定］のどちらかが表示されます。

1. 左側のペインで ［デリバリーグループ］を選択します。
2. グループを選択して、操作バーの ［編集］をクリックします。
3. ［ユーザー設定］（または ［基本設定］）ページで、次の表のいずれかの設定を変更します。
4. ［適用］をクリックして、ウィンドウを閉じずに行った変更を適用します。または、［保存］をクリックして、変更を適用してウィンドウを閉じます。

設定	説明
説明	Citrix Workspace（または StoreFront）でユーザーに表示される説明です。
デリバリーグループの有効化	このデリバリーグループを有効にするかどうかを設定します。
タイムゾーン	このデリバリーグループのマシンが存在する必要があるタイムゾーン。このオプションにより、サイトでサポートされているタイムゾーンが一覧表示されます。注：デリバリーグループのタイムゾーンを変更すると、そのデリバリーグループ内のマシンが再起動される場合があります。これを回避するには、必ず運用時間外にタイムゾーン設定を変更してください。
SecureICA の有効化	デリバリーグループのマシンとの通信を、ICA プロトコルを暗号化する SecureICA を使用してセキュリティで保護します。デフォルトレベルは 128 ビットです。レベルは SDK を使用して変更できます。パブリックネットワークが使用される環境では、TLS などの暗号化方法を追加することを Citrix ではお勧めします。また、SecureICA では、メッセージの整合性チェックが行われません。

デリバリーグループのユーザーを追加または削除する

ユーザーについて詳しくは、「ユーザー」を参照してください。

1. 左側のペインで ［デリバリーグループ］を選択します。
2. グループを選択して、操作バーの ［編集］をクリックします。
3. ユーザーページで以下の手順を実行します：
    - ユーザーを追加するには、［追加］をクリックし、追加するユーザーを指定します。
    - ユーザーを削除する場合は、1 人または複数のユーザーを選択し、［削除］をクリックします。
    - 認証されていないユーザーによるアクセスを許可するかどうかを設定するチェックボックスを、オンまたはオフにします。

4. ［適用］をクリックして、ウィンドウを閉じずに行った変更を適用します。または、［保存］をクリックして、変更を適用してウィンドウを閉じます。

ユーザー一覧のインポートまたはエクスポート　物理シングルセッションOS マシン用のデリバリーグループでは、デリバリーグループを作成した後で CSV ファイルからユーザー情報をインポートできます。ユーザー情報を CSV ファイルにエクスポートすることもできます。以前の製品バージョンでのユーザー情報を CSV ファイルに含めることもできます。

CSV ファイルの最初の行には、コンマで区切られた 2 つの列ヘッダーが含まれている必要があります。最初のヘッダーが`Machine Account`で、2 番目のヘッダーが`User Names`であることを確認してください。（ヘッダーを追加することはできますがサポートされていません）。ファイル内の後続の行には、コンマ区切りのデータが含まれています。`Machine Account`エントリには、コンピューター SID（セキュリティ識別子）、FQDN（完全就職ドメイン名）、またはドメインとコンピューター名のペアを指定できます。

ユーザー情報をインポートまたはエクスポートするには、次の手順に従います。

1. 左側のペインで ［デリバリーグループ］を選択します。
2. グループを選択して、操作バーの ［編集］をクリックします。
3. ［マシン割り当て］ページで、［一覧のインポート］または ［一覧のエクスポート］を選択し、ファイルの場所を参照します。
4. ［適用］をクリックして、ウィンドウを閉じずに行った変更を適用します。または、［保存］をクリックして、変更を適用してウィンドウを閉じます。

ユーザー割り当ての管理

デリバリーグループ内のマシンのユーザー割り当てを管理します。デリバリーグループにデスクトップ割り当て規則が設定されている場合、最初のデスクトップ起動時にマシンがユーザーにランダムに割り当てられ、ユーザー割り当てが変更されない限り、ユーザーに割り当てられたままになります。未割り当てのマシンを特定のユーザーに手動で割り当てたり、マシンの既存のユーザー割り当てを変更したりする場合は、このトピックで説明されている手順に従って変更を加えます。これらの手順を使用すると、ユーザーに割り当てられたマシンの Citrix Workspace アプリに表示される名前を変更することもできます。

詳細な手順は次のとおりです：

1. コンソールの左側のペインで ［デリバリーグループ］を選択します。
2. グループを選択して、操作バーの ［編集］を選択します。
3. 左側のペインで ［マシン割り当て］を選択します。グループ内の各マシンの次の詳細が表示されます：
    - マシン名：マシンの名前を表示します。
    - 表示名： Citrix Workspace アプリでのマシンの表示名を表示します。

- ユーザー：このマシンに割り当てられているユーザーを表示します。デスクトップ割り当て規則が設定されている場合、最初のデスクトップ起動時にマシンがユーザーにランダムに割り当てられ、ユーザー割り当てが変更されない限り、ユーザーに割り当てられたままになります。

4. マシンを見つけて、そのマシンにユーザーを割り当てるか、ユーザーの割り当てを変更します。

   - ［ブラウザー］をクリックしてユーザーに移動します。
   - ［ユーザー］列に、セミコロンで区切られたユーザー名のリストを入力します。
   - ［**CSV** ファイルからインポート］をクリックすると、CSV ファイルを使用して設定の詳細をインポートできます。

5. （オプション）マシンがユーザーに割り当てられている場合は、必要に応じて表示名を変更します。

   > 注：
   >
   > 表示名フィールドは、マシンがユーザーに割り当てられている場合にのみ有効になります：
   >
   > - デスクトップ割り当て規則に基づいてマシンがユーザーに割り当てられている場合、このフィールドにはその規則で設定された表示名が表示されます。
   > - マシンがユーザーに手動で割り当てられ、フィールドが空白のままになっている場合、デリバリーグループの公開名（指定されている場合）がマシンの表示名として使用されます。公開名が指定されていない場合は、デリバリーグループの名前が使用されます。デリバリーグループの公開名は PowerShell を使用してのみ指定できることに注意してください。

6. ［適用］を選択して変更を適用し、ウィドウを開いたままにします。または、［**OK**］を選択し、変更を適用してウィンドウを閉じます。

マシン

- ユーザーへのマシン割り当ての変更
- 電源管理対象のプールされたシングルセッション VDA に対してローカルホストキャッシュ（LHC）を有効にする
- ユーザーあたりの最大マシン数の変更
- マシンの更新
- デスクトップのタグ制約の追加、変更、または削除
- マシンの削除
- マシンへのアクセス制限
- マシンへのユーザーの接続を禁止する（メンテナンスモード）
- マシンのシャットダウンと再起動
- マシンに対する再起動スケジュールの作成と管理
- 負荷管理マシン
- 電源管理マシン

デリバリーグループのユーザーへのマシン割り当ての変更

MCS でプロビジョニングされたシングルセッションOS マシンの割り当てを変更することができます。マルチセッション OS マシンや、Citrix Provisioning でプロビジョニングされたマシンの割り当てを変更することはできません。

1. 左側のペインで ［デリバリーグループ］を選択します。
2. グループを選択して、操作バーの ［編集］をクリックします。
3. ［デスクトップ］または ［デスクトップ割り当て規則］ページ（ページのタイトルは、デリバリーグループで使用されるマシンカタログの種類によって異なります）で、新しいユーザーを指定します。
4. ［適用］をクリックして、ウィンドウを閉じずに行った変更を適用します。または、［保存］をクリックして、変更を適用してウィンドウを閉じます。

電源管理対象のプールされたシングルセッション **VDA** に対してローカルホストキャッシュ（**LHC**）を有効にする

デフォルトでは、電源管理されたシングルセッションのプールされたマシンは、ローカルホストキャッシュモードでは使用できません。デフォルトの動作は、デリバリーグループごとに上書きできます。詳細な手順は次のとおりです:

1. ［管理］**>**［完全な構成］の左側ペインで ［デリバリーグループ］を選択します。

   グループ一覧では、MCS または Citrix Provisioning によってプロビジョニングされた、シングルセッションのプールされたマシンを含むグループには警告アイコンが表示されます。

2. 必要に応じてグループを選択して、操作バーの ［編集］を選択します。
3. ［ローカルホストキャッシュ］ページで、［リソースを使用可能な状態に維持する］を選択します。
4. ［適用］を選択して、ウィンドウを閉じずに行った変更を適用します。または、［**OK**］を選択し、変更を適用してウィンドウを閉じます。

または、PowerShell コマンドを使用してデフォルトの動作を上書きすることもできます。詳しくは、「アプリケーションおよびデスクトップのサポート」を参照してください。

> 重要:
>
> 電源管理された、シングルセッションのプールされたマシンへのアクセスを有効にすると、以前のユーザーセッションからのデータと変更が後続のセッションに残る可能性があります。

デリバリーグループのユーザーあたりの最大マシン数の変更

1. 左側のペインで ［デリバリーグループ］を選択します。
2. グループを選択して、操作バーの ［編集］をクリックします。
3. ［デスクトップ割り当て規則］ページで、ユーザーあたりのデスクトップの最大値を設定します。

4. ［適用］をクリックして、ウィンドウを閉じずに行った変更を適用します。または、［保存］をクリックして、変更を適用してウィンドウを閉じます。

デリバリーグループのマシンの更新

1. 左側のペインで ［デリバリーグループ］を選択します。
2. グループを選択し、操作バーの ［マシンの表示］をクリックします。
3. マシンを選択して、操作バーの ［マシンの更新］をクリックします。

別のイメージを選択するには、［イメージ］を選択し、スナップショットを選択します。

変更内容を適用し、マシンのユーザーに通知するには、［エンドユーザーへのロールアウト通知］を選択します。次に、以下を指定します：

- マスターイメージを更新するタイミング：今すぐ、または次の起動時
- 再起動分散時間（グループ内のすべてのマシンの更新を開始する合計時間）
- ユーザーに再起動を通知するかどうか
- ユーザーが受け取るメッセージ

デスクトップのタグ制約の追加、変更、または削除

タグによる制限を追加、変更、および削除すると、どのデスクトップが起動の対象となるかについて、予期しない結果を招くことがあります。「タグ」に記載されている考慮事項と注意を確認してください。

1. 左側のペインで ［デリバリーグループ］を選択します。
2. グループを選択して、操作バーの ［編集］をクリックします。
3. ［デスクトップ］ページでデスクトップを選択し、［編集］をクリックします。
4. タグによる制限を追加するには、［タグでマシンの起動を制限します］をオンにし、タグを選択します。
5. タグ制限を変更または削除するには、次のいずれかを行います：
    - 別のタグを選択する。
    - ［タグでマシンの起動を制限します］をオフにしてタグによる制限を削除する。
6. ［適用］をクリックして、ウィンドウを閉じずに行った変更を適用します。または、［保存］をクリックして、変更を適用してウィンドウを閉じます。

デリバリーグループからのマシンの削除

マシンを削除すると、そのマシンはデリバリーグループから削除されます。この場合でも、マシンはそのデリバリーグループで使用するマシンカタログからは削除されません。このため、そのマシンをほかのデリバリーグループに割り当てることができます。

マシンを削除する前に、マシンをシャットダウンする必要があります。デリバリーグループから削除せずにマシンを一時的に使用できなくする場合は、そのマシンをメンテナンスモードにしてからシャットダウンしてください。

マシンには個人データが保存されている可能性があるため、そのマシンを別のユーザーに割り当てる場合は注意が必要です。マシンをイメージから再作成することを検討してください。

1. 左側のペインで ［デリバリーグループ］を選択します。
2. グループを選択し、操作バーの ［マシンの表示］をクリックします。
3. マシンがシャットダウン状態であることを確認します。
4. マシンを選択し、操作バーの ［デリバリーグループから削除］をクリックします。

マシンが使用する接続からも、デリバリーグループからマシンを削除できます。

デリバリーグループのマシンへのアクセス制限

デリバリーグループでリソースへのアクセス制限を変更した場合、使用する方法にかかわらず既存の設定より優先されます。次の操作を実行できます:

- 管理者のアクセスを制限する場合は、委任管理スコープを使用します: すべてのアプリケーションへのアクセスを許可するスコープや、特定のアプリケーションへのアクセスのみを許可するスコープを作成して管理者に割り当てることができます。詳しくは、「委任管理」を参照してください。
- スマートアクセスポリシー式を使用してユーザーのアクセスを制限します: アクセスポリシー規則を構成して、特定のデリバリーグループへのユーザーアクセスを制御できます。以下に例を示します:
  - ユーザーのサブセットのアクセスを制限し、許可されたユーザーデバイスを指定できます。
  - （StoreFront ではなく）Workspace 経由で接続しているユーザーへのアクセスを制限します。
  - 特定の Workspace URL 経由で接続しているユーザーへのアクセスを制限します。

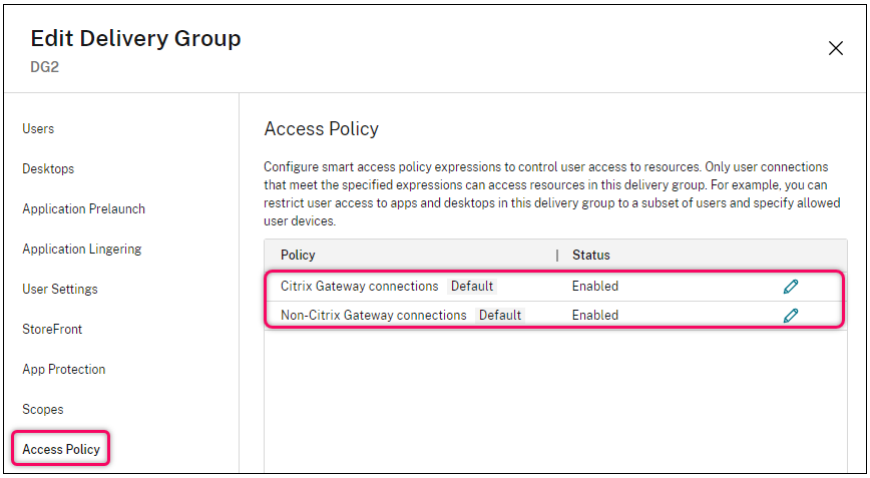
このセクションでは、アクセスポリシー規則を使用してデリバリーグループへのユーザーアクセスを制限する方法について説明します:

- アクセスポリシー規則について
- アクセスポリシー規則の追加
- Web Studio を使用したアクセスポリシー規則の管理
- PowerShell を使用したポリシー規則の追加および調整

アクセスポリシー規則について

デリバリーグループに対して複数のアクセスポリシー規則を設定できます。デリバリーグループ内のアプリとデスクトップは、ユーザーの接続がデリバリーグループに対して定義したアクセスポリシー規則と一致すると、順不同でユーザーの StoreFront または Workspace に表示されます。

各規則は個別に有効または無効にすることができます。無効な規則は、アクセスポリシーの評価時に無視されます。



Web Studio では、アクセスポリシー一覧に次のデフォルトの SmartAccess ポリシー規則が含まれます。必要に応じてさらに追加できます。

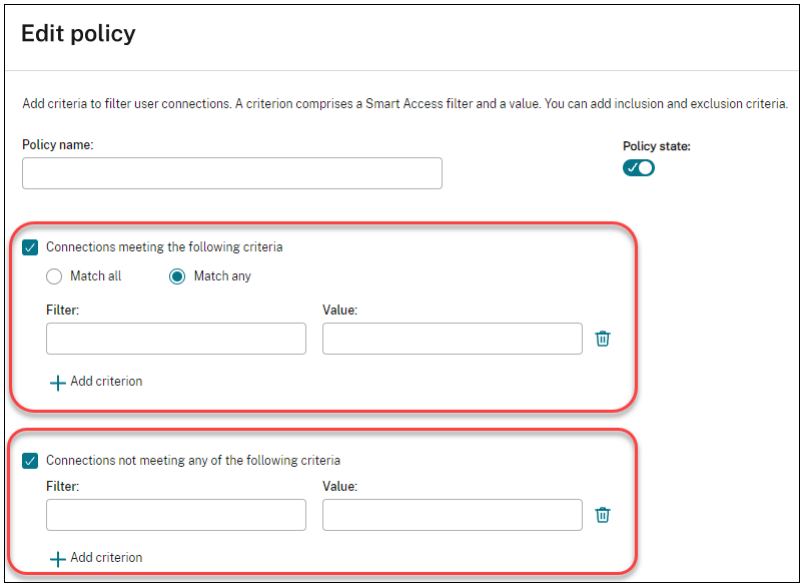
- **Citrix Gateway** 接続。このポリシーでは、Citrix Gateway 経由で行われたユーザー接続のみがデリバリーグループ内のリソースにアクセスできるようにします。デバイスポスチャ機能またはネットワークの場所機能が有効になっている場合に Workspace を介して行われたユーザー接続も、Citrix Gateway 経由の接続とみなされます。
- **Citrix Gateway** 以外の接続。このポリシーでは、Citrix Gateway を経由しないユーザー接続のみがデリバリーグループ内のリソースにアクセスできるようにします。

> 注:
>
> - デフォルトの規則が新しく構成された規則を上書きしないようにするには、デフォルトの規則を無効にするか、デフォルトの規則を調整して、新しいポリシーで使用されるフィルターを除外する必要があります。
> - デフォルトのポリシーは削除できませんが、無効にすることはできます。ポリシーを無効にするには、編集アイコンをクリックし、［ポリシーの状態］を ［無効］に変更します。
> - ポリシー一覧には、PowerShell コマンドを使用して追加された規則も表示されます。これらのポリシーは削除できますが、Web Studio では編集できません。

Web Studio を使用したアクセスポリシー規則の追加　アクセスポリシー規則は一連のフィルターで構成されています。フィルターについて詳しくは、こちらの記事を参照してください。アクセスポリシー規則を追加するときに、必要に応じて複数の条件フィルターを規則に追加します。

Web Studio を使用してデリバリーグループのポリシーを追加するには、次の手順を実行します:

1. コンソールの左側のペインで ［デリバリーグループ］を選択します。
2. グループを選択して、操作バーの ［編集］をクリックします。
3. ［アクセスポリシー］ページで、［追加］をクリックします。［ポリシーの追加］ページが開きます。



4. ［ポリシー名］フィールドに、ポリシーのわかりやすい名前を入力します。名前は展開内で一意である必要があります。
5. 許可されるユーザー接続の基準を定義するには、次の手順を実行します:
   a) ［次の条件に一致する接続］を選択します。
   b) ［条件の追加］をクリックします。
   c) ［フィルター］フィールドに、使用するフィルターの名前を入力します。［値］フィールドで、フィルターに必要な値を入力します。たとえば、（StoreFront ではなく）Workspace 経由で接続したユーザーのみがこのデリバリーグループ内のリソースにアクセスできるようにするには、［フィルター］に`Citrix-Via-Workspace`、［値］に`True`を入力します。
   d) さらに条件を追加するには、手順 b から c を繰り返します。
   e) 条件間の関係を選択します:
      - 一部が一致。受信ユーザー接続が構成されたフィルター基準のいずれかを満たしている場合にのみ、アクセスを許可します。
      - すべて一致。受信ユーザー接続が構成されたフィルター基準をすべて満たす場合にのみ、アクセスを許可します。
6. 禁止されるユーザー接続の条件を定義するには、次の手順を実行します:
   a) ［次の条件のいずれにも一致しない接続］を選択します。
   b) ［条件の追加］をクリックします。
   c) ［フィルター］フィールドに、使用するフィルターの名前を入力します。［値］フィールドで、フィルターに必要な値を入力します。たとえば、`example.cloud.com`Workspace URL 経由で接続しているユーザーがこのデリバリーグループ内のリソースにアクセスすることを禁止します。［フィルター］

にCitrix.Workspace.UsingDomainを入力し、［値］にexample.cloud.comを入力します。

d) さらに条件を追加するには、手順 b から c を繰り返します。

> 注:
>
> 構成された条件のいずれかを満たすユーザー接続は、このデリバリーグループ内のリソースへのアクセスが禁止されます。

7. ［完了］をクリックします。

   新しいポリシーがポリシー一覧に表示されます。

8. この新しいポリシーの対象となる接続との意図しない重複を避けるため、デフォルトのポリシー 規則を確認して調整します。既存のポリシーを調整するには、次の方法を使用します:

   - デフォルトのポリシー規則を無効にします。
   - 新しいポリシーの包含基準に追加した SmartAccess フィルターを除外するように、デフォルトのポリシー規則を構成します。詳しくは、「Web Studio を使用したポリシー規則の管理」および「PowerShell を使用したアクセスポリシー規則の追加および管理」を参照してください。

> 重要:
>
> 「アクセスポリシー規則について」で説明されているように、ユーザーの接続がデリバリーグループ内の 1 つ以上のポリシー規則に一致すると、ユーザーはそのリソースにアクセスできます。したがって、規則を作成した後、既存の規則を慎重に確認して調整し、新しい規則の対象となる接続との意図しない重複を避ける必要があります。

Web Studio を使用したアクセスポリシー規則の管理　包含基準と除外基準を使用して、デフォルトのポリシーを調整できます。たとえば、これらの接続のサブセットのアクセスを制限するには、次の手順を実行します:

1. デフォルトのポリシーを編集します。
2. ［次の条件のいずれかに一致する接続］を選択します。
3. 接続を許可するユーザーを特定する SmartAccess ポリシー式を追加、編集、または削除します。

詳しくは、Citrix Gateway のドキュメントを参照してください。

PowerShell を使用したアクセスポリシー規則の追加および管理　次の PowerShell コマンドレットを使用して、デリバリー グループのアクセスポリシー規則を追加および管理できます:

- New-BrokerAccessPolicyRule
- Get-BrokerAccessPolicyRule
- Set-BrokerAccessPolicyRule
- Rename-BrokerAccessPolicyRule

- Remove-BrokerAccessPolicyRule

詳しくは、Citrix 開発者向けドキュメントの関連する記事を参照してください。

デリバリーグループのマシンへのユーザーの接続を禁止する（メンテナンスモード）

一時的に新しい接続を停止する必要がある場合は、デリバリーグループの 1 台またはすべてのマシンに対してメンテナンスモードを有効にすることができます。パッチを適用したりメンテナンスツールを使用したりする場合は、メンテナンスモードを有効にしてから実行することをお勧めします。

- メンテナンスモードのマルチセッション OS マシンでは、既存のセッションに接続することはできますが、新しいセッションを開始することはできません。
- メンテナンスモードのシングルセッションOS マシン（またはリモート PC アクセスを使用している PC）では、新しいセッションを開始することも既存のセッションに再接続することもできません。実行中の接続は、ユーザーが切断またはログオフするまでは保持されます。

メンテナンスモードをオンまたはオフにするには、次の手順に従います。

1. 左側のペインで ［デリバリーグループ］を選択します。
2. グループを選択します。
3. デリバリーグループのすべてのマシンをメンテナンスモードにするには、操作バーの ［メンテナンスモードをオンにする］をクリックします。

   1 つのマシンをメンテナンスモードにするには、操作バーの ［マシンの表示］をクリックします。マシンを選択し、操作バーの ［メンテナンスモードをオンにする］をクリックします。
4. 特定のマシンまたはデリバリーグループのすべてのマシンのメンテナンスモードを解除するには、上記の手順に従って、操作バーで ［メンテナンスモードをオフにする］をクリックします。

Windows リモートデスクトップ接続（RDC）の設定も、マルチセッション OS マシンをメンテナンスモードにするかどうかに影響します。次の状態のいずれかが発生すると、サーバーがメンテナンスモードになります:

- 上記の手順で［メンテナンスモードをオンにする］が選択された。
- RDC が ［このコンピューターへの接続を許可しない］に設定された。
- RDC が ［このコンピューターへの接続を許可しない］に設定されていない。［リモートホスト構成のユーザーログオンモード］設定が ［再接続を許可するが、新しいログオンを許可しない］または ［再接続を許可するが、サーバーが再起動するまで新しいログオンを許可しない］に設定されている。

次のものについて、メンテナンスモードのオン/オフを切り替えることもできます:

- 接続。この接続を使用するマシンに影響が及びます。
- マシンカタログ。このカタログ内のマシンに影響が及びます。

デリバリーグループのマシンのシャットダウンと再起動

ここで説明する内容は、リモート PC アクセスマシンではサポートされません。

1. 左側のペインで ［デリバリーグループ］を選択します。
2. グループを選択し、操作バーの ［マシンの表示］をクリックします。
3. マシンを選択し、操作バーで以下のいずれかのエントリをクリックします:

    - 強制シャットダウン: マシンの電源を強制的に切って、マシン一覧を更新します。
    - 再起動: オペレーティングシステムに再起動を要求します。オペレーティングシステムで再起動を実行できない場合、マシンの状態は変更されません。
    - 強制再起動: オペレーティングシステムを強制的にシャットダウンしてから、マシンを再起動します。
    - 一時停止: マシンをシャットダウンすることなく一時的に停止して、マシン一覧を更新します。
    - シャットダウン: オペレーティングシステムにシャットダウンを要求します。

非強制操作の場合、マシンが 10 分以内にシャットダウンしないと、電源が切れ、強制的にシャットダウンされます。シャットダウン中に Windows が更新のインストールを開始すると、更新が完了する前にマシンの電源が切れる危険性があります。

セッション中はシングルセッションOS マシンのユーザーに ［シャットダウン］の選択を禁止することを Citrix ではお勧めします。詳しくは、Microsoft のポリシーのドキュメントを参照してください。

接続でマシンをシャットダウンし再起動することもできます。

デリバリーグループのマシンに対する再起動スケジュールの作成と管理

> 注:
>
> - Autoscale が有効になっているデリバリーグループに再起動スケジュールが適用されると、そのマシンの電源がオフになり、Autoscale が電源をオンにするまでそのままです。
> - 再起動スケジュールがランダムにシングルセッションマシンに適用される場合、コストを節約する場合に、それらのマシンは再起動されるのではなく電源がオフになります。Autoscale を使用してマシンの電源をオンにすることをお勧めします。
> - デリバリーグループのタイムゾーンを変更すると、そのデリバリーグループ内のマシンが再起動される場合があります。これを回避するには、必ず運用時間外にタイムゾーン設定を変更してください。

再起動のスケジュールにより、デリバリーグループ内のマシンを定期的に再起動するタイミングが指定されます。1 つのデリバリーグループに対して、1 つ以上のスケジュールを作成できます。スケジュールは次のいずれかに影響します:

- グループ内のすべてのマシン。
- グループ内の 1 つ以上のマシン（すべてではない）。マシンは、マシンに適用するタグで識別されます。これは、タグがあるアイテムのみタグによって操作が制限されるため「タグ制限」と呼ばれます。

たとえば、すべてのマシンが 1 つのデリバリーグループに属しているとします。すべてのマシンを毎週 1 回再起動し、経理チームが使用するマシンを毎日再起動するとします。これを実現するには、すべてのマシンに対して 1 つのスケジュールを設定し、経理チームのマシンのみ別途スケジュールを設定します。

スケジュールには、再起動が開始される日時と期間が含まれます。

スケジュールは有効または無効にできます。テストのときや、特別な間隔のとき、必要になる前にスケジュールを準備するときは、スケジュールを無効にすると役立ちます。

スケジュールは、管理コンソールからの自動パワーオンまたはシャットダウンには使用できません。再起動の場合にのみ使用できます。

スケジュールの重複　複数のスケジュールを重複させることができます。上記の例では、両方のスケジュールが経理チームのマシンに影響します。これらのマシンは、日曜日に 2 回再起動される可能性があります。スケジュールコードは、同じマシンを意図した回数より多く再起動しないよう設計されていますが、保証はされません。

- スケジュールで開始日時と期間が正確に一致する場合、マシンが一度だけ再起動される可能性が高くなります。
- スケジュールの開始日時と期間が異なるほど、再起動が複数回発生する可能性が高くなります。
- スケジュールの影響を受けるマシンの数は、重複の可能性にも影響します。例では、すべてのマシンに影響がある週次スケジュールは、経理チームのマシンの日次スケジュールより速く再起動を開始する可能性があります（それぞれに指定された期間により異なる）。

再起動スケジュールについて詳しくは、「Reboot schedule internals」を参照してください。

再起動スケジュールの表示

1. 左側のペインで ［デリバリーグループ］を選択します。
2. グループを選択して、操作バーの ［編集］をクリックします。
3. ［再起動スケジュール］ページを選択します。

［再起動スケジュール］ページには、構成された各スケジュールに関する次の情報が表示されます：

- スケジュール名。
- 使用されるタグ制限（ある場合）。
- マシンの再起動が発生する頻度。
- マシンのユーザーが通知を受信するかどうか。
- スケジュールが有効かどうか。

タグの追加（適用）　タグ制限を使用する再起動スケジュールを構成する場合、そのスケジュールの影響を受けるマシンにタグが追加されていることを確認してください。上記の例では、経理チームによって使用されるそれぞれのマシンにタグが適用されます。詳しくは、「タグ」を参照してください。

1 つのマシンに複数のタグを適用することもできますが、再起動スケジュールでは 1 つのタグしか指定できません。

1. 左側のペインで ［デリバリーグループ］を選択します。
2. スケジュールによって制御されるマシンを含むグループを選択します。
3. ［マシンの表示］をクリックし、タグを追加するマシンを選択します。
4. 操作バーの ［タグの管理］をクリックします。
5. タグが存在する場合は、タグ名の隣にあるチェックボックスをオンにします。タグが存在しない場合は、［作成］をクリックし、タグの名前を指定します。タグが作成されたら、新しく作成したタグ名の隣にあるチェックボックスをオンにします。
6. ［タグの管理］ダイアログボックスの ［保存］をクリックします。

再起動スケジュールの作成

1. 左側のペインで ［デリバリーグループ］を選択します。
2. グループを選択して、操作バーの ［編集］をクリックします。
3. ［再起動スケジュール］ページで、［追加］をクリックします。
4. ［再起動スケジュールの追加］ページで次の操作を行います：

    - スケジュールを有効にするには、［はい］を選択します。スケジュールを無効にするには、［いいえ］を選択します。
    - スケジュールの名前と説明を入力します。
    - ［タグに制限］では、タグの制限を適用します。
    - ［メンテナンスモードのマシンを含める］で、メンテナンスモードのマシンをこのスケジュールに含めるかどうかを選択します。代わりに PowerShell を使用する場合については、「メンテナンスモードのマシンのスケジュールされた再起動」を参照してください。
    - ［再起動の頻度］では、再起動の頻度を次の中から選択します：毎日、毎週、毎月、または一度だけ。［毎週］または ［毎月］を選択した場合は、1 つ以上の特定の曜日または日付を指定できます。
    - ［繰り返し間隔］には、スケジュールを実行する頻度を指定します。
    - ［開始日］には、スケジュールを設定する期間の最初の日を指定します。
    - ［再起動の開始］では、再起動の開始時刻を 24 時間形式で指定します。
    - ［再起動の間隔］の場合：
        - 自然な再起動を使用しない場合は、［すべてのマシンを同時に再起動する］または ［すべてのマシンを（一定期間内に）再起動する］を選択します。
        - 自然な再起動を使用する場合は、［セッションのドレイン後にすべてのマシンを再起動する］を選択します。

          自然再起動を使用するように構成された再起動スケジュールを開始すると、次のようになります：

            * デリバリーグループに属するすべてのアイドル状態のマシンがすぐに再起動されます

* 1 つまたは複数のアクティブなセッションがあるデリバリーグループに属する各マシンは、すべてのセッションがログオフされると再起動されます。

> 注:
>
> このオプションは、電源管理されているマシンと、電源管理されていないマシンに使用できます。

- ［ユーザーへ通知を送信］で、再起動を開始する前に、該当するマシンに通知メッセージを表示するかどうかを選択します。デフォルトでは、メッセージは表示されません。
- 再起動開始の 15 分前にメッセージが表示されるように選択した場合、最初のメッセージの後、5 分ごとにメッセージが繰り返し送信されるように ［通知の頻度］で選択できます。デフォルトでは、メッセージは繰り返して送信はされません。
- 通知のタイトルと本文を入力します。デフォルトのテキストはありません。

  メッセージに再起動までのカウントダウンを含める場合は、変数 **%m%** を入れます。すべてのマシンを同時に再起動することを選択した場合を除き、メッセージは、再起動前の適切なタイミングで各マシンに表示されます。

5. ［完了］をクリックして変更を適用し、［再起動スケジュールの追加］ウィンドウを閉じます。
6. ［適用］をクリックすると、ウィンドウは閉じずに、行った変更が適用されます。または、［保存］をクリックして、変更を適用してウィンドウを閉じます。

ドレイン後の再起動　PowerShell を使用してマシンの再起動スケジュールを作成または更新する場合は、再起動の間隔にもう 1 つ別の値を使用できます（`New-BrokerRebootSchedulev2`または`Set-BrokerRebootSchedulev2`）。

`-UseNaturalReboot <Boolean>`パラメーターを指定してドレイン後の再起動機能を有効にすると、すべてのセッションがドレインされた後、すべてのマシンが再起動されます。再起動時間に達し、すべてのセッションがログオフされると、マシンはドレイン状態になり再起動されます。

この機能は、シングルセッションまたはマルチセッションのマシンを含むデリバリーグループでサポートされています。このオプションは、電源管理されているマシンと、電源管理されていないマシンに使用できます。

オンプレミス環境では、この機能は PowerShell を使用している場合にのみサポートされます。この機能は Web Studio では使用できません。

再起動スケジュールの編集、削除、有効化、無効化

1. 左側のペインで ［デリバリーグループ］を選択します。
2. グループを選択して、操作バーの ［編集］をクリックします。
3. ［再起動スケジュール］ページで、スケジュールのチェックボックスをオンにします。

- スケジュールを編集するには、［編集］をクリックします。スケジュール設定を更新します。更新の方法については、「再起動スケジュールの作成」を参照してください。
- スケジュールを有効または無効にするには、［編集］をクリックします。［再起動スケジュールを有効にする］チェックボックスを、オンまたはオフにします。
- スケジュールを削除するには、［削除］をクリックします。削除を確認します。スケジュールを削除しても、影響を受けるマシンに適用済みのタグには影響しません。

データベースの停止によるスケジュールされた再起動の遅延

> 注:
>
> この機能は、PowerShell のみで利用可能です。

デリバリーグループ内のマシン（VDA）に対してスケジュールされた再起動が開始される前にサイトデータベースの停止が発生した場合、停止が終了すると再起動が開始されます。これは意図しない結果につながる可能性があります。

たとえば、デリバリーグループの再起動が実稼働時間外に（03:00 から）行われるようにスケジュールしたとします。スケジュールされた再起動開始時間の 1 時間前（02:00）に、サイトデータベースの停止が発生します。この停止は 6 時間続きます（08:00 まで）。Delivery Controller とサイトデータベース間の接続が復元されると、再起動スケジュールが開始されます。VDA の再起動は、元のスケジュールの 5 時間後に開始されたため、実稼働時間中に VDA が再起動することになります。

この状況を回避するには、`New-BrokerRebootScheduleV2`および`Set-BrokerRebootScheduleV2`コマンドレットの`MaxOvertimeStartMins`パラメーターを使用できます。この値により、スケジュールされた開始時間の最大何分後に再起動スケジュールを開始できるかを指定します。

- その時間（スケジュールされた時間 + `MaxOvertimeStartMins`）内にデータベース接続が復元された場合、VDA の再起動が開始されます。
- その時間内にデータベース接続が復元されない場合には、VDA の再起動は開始されません。
- このパラメーターを省略するか値に 0 を設定すると、停止時間に関係なく、スケジュールされた再起動はデータベースへの接続の復元時に開始されます。

詳しくは、コマンドレットのヘルプを参照してください。この機能は、PowerShell のみで利用可能です。再起動スケジュールを Web Studio で構成する場合には、この値を設定できません。

メンテナンスモードのマシンのスケジュールされた再起動

> 注:
>
> この機能は、PowerShell のみで利用可能です。`IgnoreMaintenanceMode`オプションは、Citrix Virtual Apps and Desktops 7 2006 以降でサポートされています。

再起動スケジュールがメンテナンスモードのマシンを影響を与えるかを指定するには、`BrokerRebootScheduleV2`コマンドレットで`IgnoreMaintenanceMode`オプションを使用します。

たとえば、次のコマンドレットは、メンテナンスモードのマシン（およびメンテナンスモードではないマシン）を再起動するスケジュールを作成します。

```
New-Brokerrebootschedulev2 rebootSchedule1 -DesktopGroupName <myDesktopGroup> -IgnoreMaintenanceMode $true
```

次のコマンドレットは、既存の再起動スケジュールを変更します。

```
Set-Brokerrebootschedulev2 rebootSchedule1 -IgnoreMaintenanceMode $true
```

詳しくは、コマンドレットのヘルプを参照してください。この機能は、PowerShell のみで利用可能です。

デリバリーグループの負荷管理マシン

負荷管理できるのはマルチセッション OS マシンのみです。

負荷管理機能では、測定されたサーバー負荷に基づいて最適なサーバーが選択されます。この選択は、以下の基準により行われます。

- サーバーのメンテナンスモードの状態：メンテナンスモードがオフのマルチセッション OS マシンだけが負荷分散の対象として選択されます。
- サーバー負荷指数：マルチセッション OS マシンの配信サーバーの負荷に基づいて、そのサーバーがどれだけの接続を受け入れられるかが決定されます。サーバー負荷指数は、セッション数とパフォーマンス測定値（CPU、ディスク、メモリ使用量など）で計算される負荷評価基準の組み合わせを指します。負荷評価基準は、ポリシーの負荷管理に関する設定項目で指定します。

  ［負荷指数］列に値 10000 が表示される場合、そのサーバーが負荷限界状態であることを示しています。ほかに使用可能なサーバーがない場合は、ユーザーがセッションを起動したときに、デスクトップまたはアプリケーションを使用できないという内容のメッセージが表示されることがあります。

  Director（監視）、Web Studio（管理）の［検索］ノード、および SDK を使用して負荷指数を監視できます。

  コンソールで ［サーバー負荷インデックス］列（デフォルトでは非表示）を表示するには、マシンを選択し、列見出しを右クリックして ［列の選択］を選択します。［マシン］カテゴリ の ［負荷指数］を選択します。

  SDK では、`Get-BrokerMachine`コマンドレットを使用します。詳しくは、CTX202150を参照してください。

- 同時ログオントレランスのポリシー設定：サーバーが同時に処理できるログオン要求の最大数です。この設定項目は、XenApp バージョン 6.x の「負荷調整」に相当します。

  すべてのサーバーが同時ログオントレランスの設定値に達した場合、それ以降のログオン要求は保留中のログオン数が最も少ないサーバーに割り当てられます。同時ログオントレランスの設定値に達しないサーバーがいくつか存在する場合は、負荷指数が最小のサーバーにログオン要求が割り当てられます。

デリバリーグループの電源管理マシン

電源を管理できるのは、仮想シングルセッションOS マシンのみです。物理マシンの電源を管理することはできません（リモート PC アクセスマシンを含む）。GPU 機能が有効なシングルセッションOS マシンは一時停止できないため、電源を切ることはできません。マルチセッション OS マシンでは、再起動のスケジュールを作成できます。

プールされたマシンが含まれるデリバリーグループでは、仮想シングルセッションOS マシンは次のうちいずれかの状態になります：

- ランダムに割り当てられ、使用中
- 未割り当て、未接続

静的なマシンが含まれるデリバリーグループでは、仮想シングルセッションOS マシンは次のうちいずれかの状態になります：

- 永続的に割り当てられ、使用中
- 永続的に割り当てられ、未接続（準備は完了）
- 未割り当て、未接続

通常、静的なデリバリーグループには、永続的に割り当てられたマシンと未割り当てマシンの両方が含まれています。はじめに、すべてのマシンは未割り当て状態です（デリバリーグループ作成時に手動で割り当てられたマシンを除く）。ユーザーが接続すると、マシンが永続的に割り当てられます。静的なデリバリーグループでは未割り当てマシンの電源を完全に管理できますが、永続的に割り当てられたマシンでは一部の電源管理のみを実行できます。

- プールおよびバッファー：未割り当てマシンが含まれる静的なデリバリーグループ、およびプールされたデリバリーグループの場合、（ここでの）「プール」は、電源が入っていてユーザーが接続可能な、未割り当てまたは一時的に割り当てられたマシンのセットを指します。ユーザーがログオンすると、マシンがすぐに割り当てられます。プールサイズ（電源が入った状態のマシンの数）は時刻によって構成できます。静的なデリバリーグループの場合、SDK を使用してプールを構成します。

  「バッファー」は、プール内のマシンの数がしきい値を下回ると電源がオンになる、別の未割り当てマシンの「待機」セットを指します。このしきい値は、デリバリーグループのサイズの割合で指定します。大規模なデリバリーグループの場合、しきい値を上回ると、非常に多くの数のマシンがオンになることがあります。こうした場合には、デリバリーグループのサイズを慎重に計画するか、または SDK を使用してデフォルトのバッファーサイズを調整してください。

- 電源状態タイマー：電源状態タイマーを使用して、ユーザーが切断してから一定の時間が経過したマシンを一時停止にすることができます。たとえば、業務時間終了後にユーザーが切断してから 10 分が経過したマシンを自動的に一時停止状態にできます。

  平日と週末、ピーク期間とオフピーク期間のタイマーを構成できます。

- 永続的に割り当てられたマシンの部分的な電源管理：永続的に割り当てられたマシンでは、電源の状態タイマーを設定することはできますが、プールまたはバッファーを設定することはできません。各ピーク時間の開始時にマシンの電源がオンになり、各オフピーク時間の開始時に電源がオフになります。このため、未割り当てマシンの場合とは異なり、使用中のマシンを補うためのマシンの数を詳細に調整できません。

仮想シングルセッション**OS** マシンの電源管理

1. 左側のペインで ［デリバリーグループ］を選択します。
2. グループを選択して、操作バーの ［デリバリーグループの編集］をクリックします。
3. ［電源管理］ページの ［マシンの電源管理］で、［**1 -** 平日］を選択します平日は、デフォルトで月曜日から金曜日です。
4. ランダムなデリバリーグループの場合、［電源をオンするマシン］で ［編集］をクリックして、平日のプールサイズを指定します。次に、電源をオンにするマシンの数を選択します。
5. ［ピーク時］で、平日のピーク時間とオフピーク時間を設定します。
6. 平日のピーク時間およびオフピーク時間の電源状態タイマーを設定します：［ピーク時の電源管理］**>** ［切断時］で、ユーザーが切断してからマシンを一時停止状態にするまでの時間（分）を指定して、［一時停止］を選択します。［オフピーク時の電源管理］**>** ［切断時］で、ユーザーがログオフしてからマシンの電源をオフにするまでの時間を指定して、［シャットダウン］を選択します。このタイマーはランダムマシンのデリバリーグループでは使用できません。
7. ［マシンの電源管理］で ［**2 -** 週末］を選択し、週末のピーク時間と電源状態タイマーを構成します。
8. ［適用］をクリックして、ウィンドウを閉じずに行った変更を適用します。または、［保存］をクリックして、変更を適用してウィンドウを閉じます。

SDK を使用すると、以下の設定が可能です。

- 電源状態タイマーの設定に基づいてマシンを（一時停止ではなく）シャットダウンする場合や、ユーザーの（切断時ではなく）ログオフ時にタイマーが起算されるように設定する。
- デフォルトの平日と週末の定義を変更する。
- 電源管理を無効にする。CTX217289を参照してください。

セッションが切断された状態で異なる期間に移行する **VDI** マシンの電源管理

> 重要：
>
> この拡張機能は、セッションが切断された VDI マシンにのみ適用されます。セッションがログオフされている VDI マシンには適用されません。

以前のリリースでは、アクション（切断アクション =「一時停止」または「シャットダウン」）が必要な期間に移行する VDI マシンは、電源がオンのままになっていました。このシナリオは、操作（切断アクション =「何もしない」）が不要な期間（ピーク時またはオフピーク時）にマシンが切断された場合に発生しました。

Citrix Virtual Apps and Desktops 7 1909 以降では、指定した切断時間が経過すると、マシンは一時停止または電源をオフにされます。これは、その期間に対して構成された切断アクションによって異なります。

たとえば、VDI デリバリーグループに対して次の電源ポリシーを構成するとします：

- `PeakDisconnectAction`を「何もしない」に設定
- `OffPeakDisconnectAction`を「シャットダウン」に設定
- `OffPeakDisconnectTimeout`を「10」に設定

電源ポリシーの切断アクションについて詳しくは、「https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/about_Broker_PowerManagement/#power-policy」および「https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/Get-BrokerDesktopGroup/」を参照してください。

以前のリリースでは、ピーク時にセッションが切断された VDI マシンは、ピークからオフピークに移行しても電源がオンのままでした。Citrix Virtual Apps and Desktops 7 1909 以降、`OffPeakDisconnectAction`および`OffPeakDisconnectTimeout`ポリシーのアクションは、期間移行時に VDI マシンに適用されます。その結果、オフピークに移行してから 10 分後にマシンの電源がオフになります。

以前の動作に戻す（つまり、セッションが切断された状態でピークからオフピークまたはオフピークからピークに移行するマシンでは何も実行しない）場合は、次のいずれかの操作を行います：

- `LegacyPeakTransitionDisconnectedBehaviour`レジストリ値を1に設定します。これは、以前の動作を有効にする *true* と同等です。デフォルトでは値は0、または *false* です。これは、期間の移行時に電源ポリシーの切断アクションをトリガーします。
  - パス：`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\DesktopServer`
  - 値の名前：`LegacyPeakTransitionDisconnectedBehaviour`
  - 種類：`REG_DWORD`
  - データ：`0x00000001 (1)`
- `Set-BrokerServiceConfigurationData` PowerShell コマンドを使用して設定を構成します。例：
  - ```
    PS C:\> Set-BrokerServiceConfigurationData HostingManagement.
    LegacyPeakTransitionDisconnectedBehaviour -SettingValue $true
    ```

期間移行時に電源ポリシーアクションを適用するには、マシンが次の条件を満たす必要があります：

- 切断されたセッションがある。
- 保留中の電源操作がない。
- 異なる期間に移行する VDI（シングルセッション）デリバリーグループに属している。
- 特定の期間（ピーク時またはオフピーク時）に切断し、電源操作が割り当てられている期間に移行するセッションがある。

カタログで電源オン状態にする **VDA** の割合の変更

1. ［デリバリーグループ］の ［電源管理］セクションで、デリバリーグループのピーク時間を調整します。
2. デスクトップグループの名前を書き留めます。
3. 管理者権限で PowerShell を起動し、次のコマンドを実行します。「Desktop Group Name」は、実行する VDA の割合を変更したデスクトップグループの名前に置き換えてください。

   ```
   asnp Citrix*
   ```

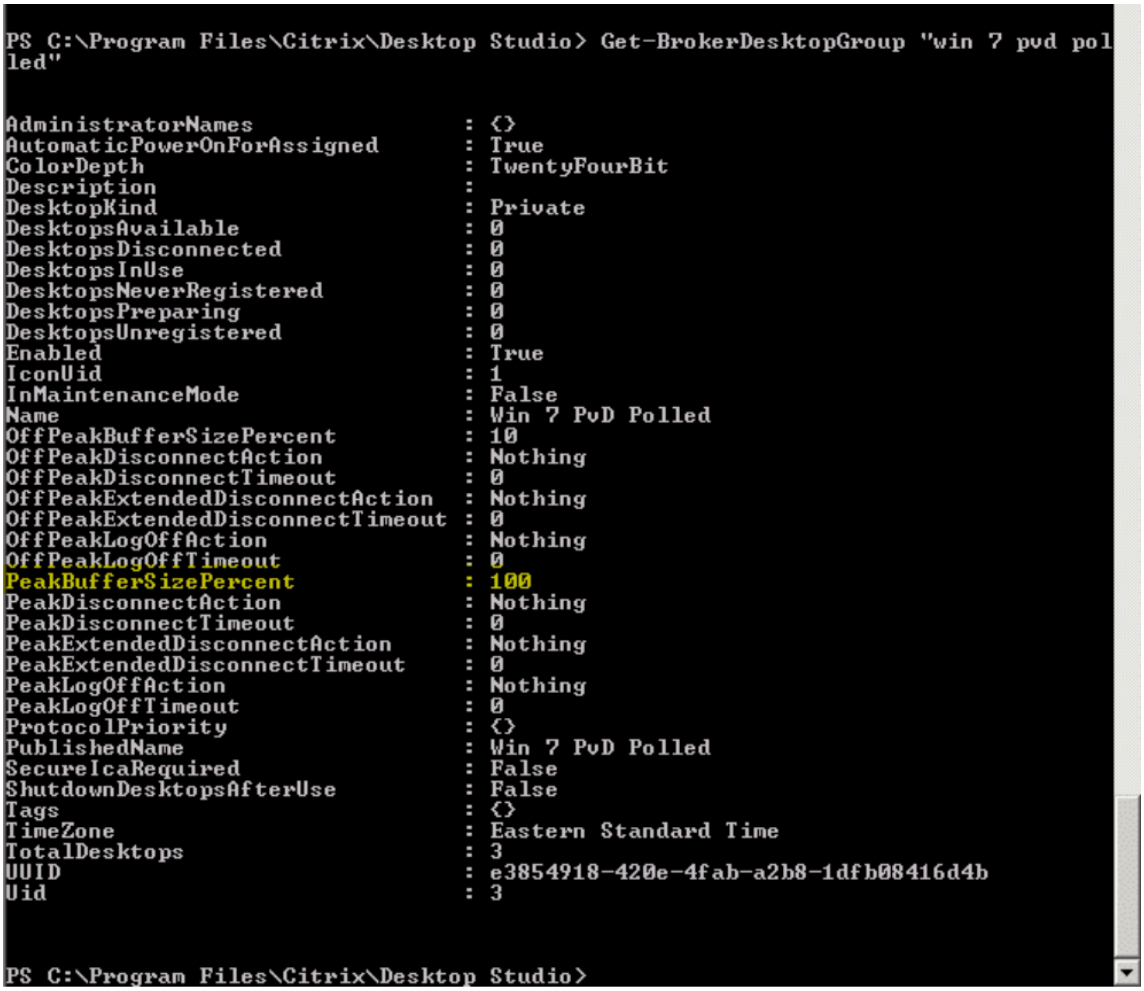

   ```

```
Set-BrokerDesktopGroup "Desktop Group Name"-PeakBufferSizePercent
 100
```

この数値の 100 により、100% の VDA が準備完了状態になるように設定されます。

4. 次のコマンドを実行して、ソリューションを確認します:

```
#Get-BrokerDesktopGroup "Desktop Group Name"
```



変更が反映されるまでには最大 1 時間かかることがあります。

ユーザーがログオフした後に VDA をシャットダウンするには、次のように入力します:

```
# Set-BrokerDesktopGroup "Desktop Group Name"-ShutDownDesktopsAfterUse
 $True
```

ログオフ後も準備完了状態になるようにピーク時に VDA を再起動するには、次のように入力します:

```
# Set-BrokerDesktopGroup "Desktop Group Name"-AutomaticPowerOnForAssignedDurin
 $True
```


セッション

- セッションのログオフ/切断、またはユーザーへのメッセージ送信
- セッションの事前起動およびセッション残留の構成
- メンテナンスモードでマシンから切断されたときのセッションの再接続の制御
- セッションローミングを構成する

セッションをログオフまたは切断する

1. 左側のペインで ［デリバリーグループ］を選択します。
2. デリバリーグループを選択して、操作バーの ［マシンの表示］を選択します。
3. 中央のペインでマシンを選択し、操作バーで ［セッションの表示］を選択して、セッションを選択します。
    - または、中央のペインで ［セッション］タブを選択し、セッションを選択します。
4. ユーザーをセッションからログオフするには、操作バーの ［ログオフ］をクリックします。セッションが終了し、ユーザーがログアウトされます。ほかのユーザーがそのマシンを使用できるようになります（そのマシンが特定のユーザーに割り当てられてない場合）。
5. セッションを切断するには、操作バーの ［切断］を選択します。ユーザーのアプリケーションは引き続きセッション内で実行され、マシンはそのユーザーに割り当てられたままになります。ユーザーは同じマシンに再接続できます。

シングルセッションOS マシンでは、電源状態タイマーを使用して、ユーザーが切断してから一定の時間が経過したマシンを一時停止にしたりシャットダウンしたりすることができます。詳しくは、「電源管理マシン」を参照してください。

デリバリーグループへのメッセージの送信

1. 左側のペインで ［デリバリーグループ］を選択します。
2. デリバリーグループを選択して、操作バーの ［マシンの表示］を選択します。
3. 中央のペインで、メッセージを送信するマシンを選択します。
4. 操作バーで ［セッションの表示］を選択します。
5. 中央のペインですべてのセッションを選択し、操作バーで ［メッセージの送信］を選択します。
6. メッセージを入力して ［**OK**］をクリックします。必要に応じて、重要度のレベルを指定できます。オプションには ［重要］、［質問］、［警告］、［情報］があります。

または、Citrix Director を使用してメッセージを送信することもできます。詳しくは、「ユーザーへのメッセージの送信」を参照してください。

デリバリーグループのセッションの事前起動および残留セッションの構成

これらの機能は、マルチセッション OS マシンでのみサポートされます。

セッションの事前起動機能とセッション残留機能を使用すると、セッションが要求される前にセッションを開始したり（セッションの事前起動）、ユーザーがすべてのアプリケーションを閉じた後もアプリケーションセッションをアクティブな状態で保持したり（セッション残留）できます。これにより、ユーザーがアプリケーションにすばやくアクセスできるようになります。

デフォルトでは、セッションの事前起動とセッション残留は無効になっています。セッションはユーザーがアプリケーションを開始すると開始（起動）され、セッションで開いていた最後のアプリケーションを閉じるまでアクティブな状態で保持されます。

注意事項:

- これらの機能を使用するには、デリバリーグループでアプリケーションが配信されている必要があります。また、マシンでマルチセッション OS 対応 VDA バージョン 7.6 以降が動作している必要があります。
- これらの機能は Windows 向け Citrix Workspace アプリを使用している場合にのみサポートされ、Citrix Workspace アプリ側での構成も必要になります。詳しくは、使用中のバージョンの Windows 向け Citrix Workspace アプリに関する製品ドキュメントで、「セッションの事前起動」を検索してください。
- HTML5 向け Citrix Workspace アプリはサポートされません。
- セッションの事前起動を使用するときに、ユーザーのマシンが一時停止状態または休止状態の場合は、（セッションの事前起動設定にかかわらず）事前起動は機能しません。ユーザーはマシン/セッションをロックできます。ただし、ユーザーが Citrix Workspace アプリからログオフすると、セッションが終了し、事前起動は適用されなくなります。
- セッションの事前起動を使用するときは、物理クライアントマシンでは一時停止または休止状態の電源管理機能を使用できません。クライアントマシンのユーザーはセッションをロックすることはできますが、ログオフすることはできません。
- 事前起動セッションと残留セッションは、接続されている間のみ同時使用ライセンスを消費します。ユーザーライセンスまたはデバイスライセンスを使用する場合、ライセンスは 90 日間有効です。使用されない事前起動セッションと残留セッションは、デフォルトで 15 分後に切断されます。この値は PowerShell（`New`/`Set-BrokerSessionPreLaunch`コマンドレット）で構成できます。
- これらの機能が相互に補完し合うよう調整するには、ユーザーの使用状況を監視して慎重に計画することが重要です。最適に構成することで、ライセンス消費やリソース割り当ての効率化とユーザーの利便性を両立させることができます。
- Citrix Workspace アプリ側で、セッションの事前起動を有効にする時間帯を構成できます。

使用されない事前起動セッションや残留セッションがアクティブのまま保持される時間　ユーザーがアプリケーションを起動しない場合に、使用されないセッションをどのくらい保持するかを指定するには、タイムアウトおよびサーバー負荷のしきい値を構成します。これらのすべてを設定することができます。最初に発生したイベントによって未使用のセッションが終了します。

- タイムアウト：使用されない事前起動セッションや残留セッションを保持する日数、時間数、または分数を指定できます。この値が短すぎると事前起動セッションがすぐに終了してしまい、ユーザーがアプリケーションにすばやくアクセスできるというメリットが活かされません。また、タイムアウト値が長すぎると、サーバーのリソースが足りなくなり、ユーザーの接続要求が拒否される場合があります。

このタイムアウトの設定は、管理コンソールではなく SDK からのみ(`New-BrokerSessionPreLaunch` / `Set-BrokerSessionPreLaunch` コマンドレット）有効にできます。タイムアウトを無効にすると、コンソールや ［デリバリーグループの編集］ページにそのデリバリーグループのタイムアウトが表示されなくなります。

- しきい値：サーバーの負荷が高くなったときに事前起動セッションや残留セッションを自動的に終了することができます。これにより、サーバーの負荷が低い間は可能な限りセッションが保持されます。新しいユーザーセッション用のリソースが必要になったときに事前起動セッションや残留セッションが自動的に終了するため、これらのセッションが原因で接続が拒否されることはありません。

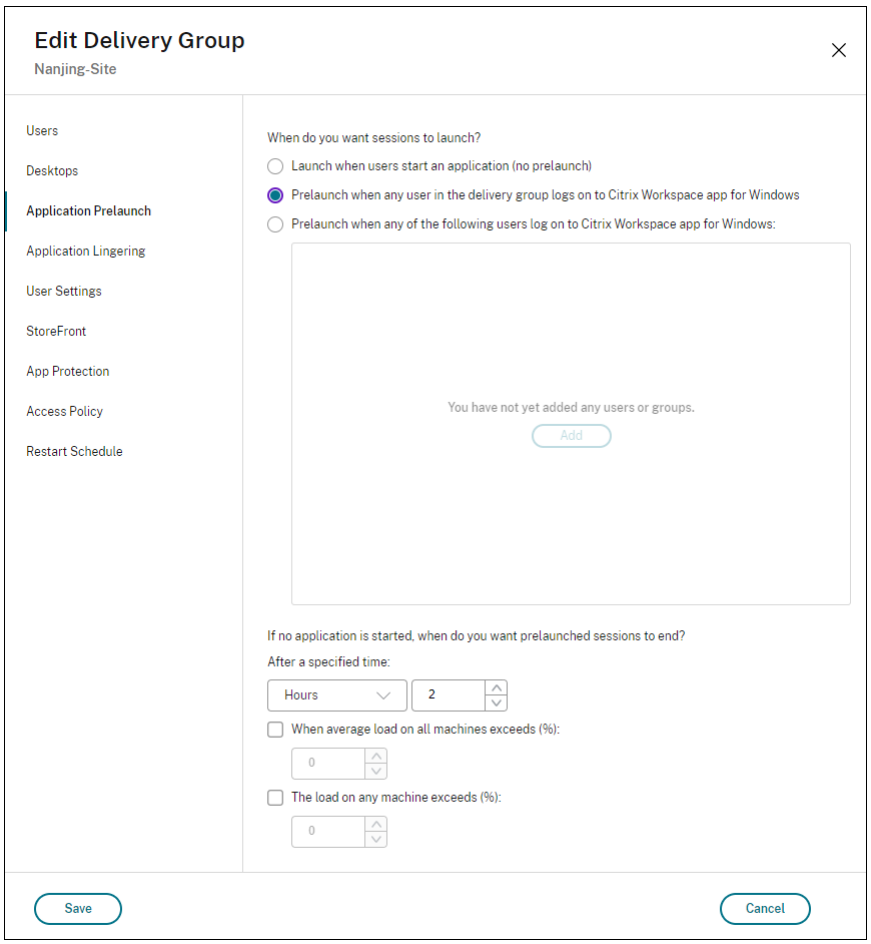
  次の 2 つのしきい値を構成できます：デリバリーグループ内の全サーバーの平均負荷パーセンテージと、グループ内のいずれかのサーバーの最大負荷パーセンテージ。サーバーの負荷がいずれかのしきい値を超えると、最も長い時間保持された事前起動セッションまたは残留セッションが終了します。その後、負荷がしきい値を下回るまで、分間隔で 1 つずつセッションが終了します。しきい値を超えている間は、新たな事前起動セッションは開始されません。

Controller に登録されていない VDA が動作するサーバーやメンテナンスモードのサーバーは、負荷限界状態として認識されます。サーバーで計画外の停止状態が発生した場合、事前起動セッションや残留セッションは自動的に終了してリソースが解放されます。

セッションの事前起動を有効にするには、次の手順に従います

1. グループを選択して、操作バーの ［デリバリーグループの編集］をクリックします。
2. ［アプリケーションの事前起動］ページで、セッションを起動するタイミングを選択します：

   - アプリケーションの起動時にセッションを起動する。これがデフォルトの設定です。セッションの事前起動機能は無効になっています。
   - デリバリーグループ内のすべてのユーザーで、Windows 向け Citrix Workspace アプリへのログオン時に事前起動する。
   - 一覧に含まれるユーザーおよびユーザーグループでのみ、Windows 向け Citrix Workspace アプリへのログオン時に事前起動する。このオプションを選択する場合は、ユーザーまたはユーザーグループを一覧に追加してください。



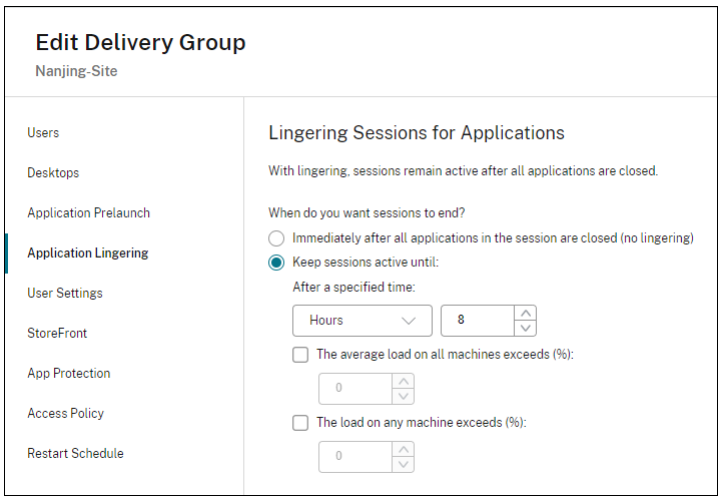
3. 事前起動セッションは、ユーザーがアプリケーションを起動すると通常のセッションに置き換わります。ユーザーがアプリケーションを起動しない場合（事前起動セッションが使用されない場合）、以下の設定に従って事前起動セッションが終了します。

    - この時間が経過したときにセッションを終了する。セッションを自動的に終了するまでの時間を指定します（1～99 日間、1～2,376 時間、または 1～142,560 分）。
    - デリバリーグループ内のすべてのマシンの平均負荷が指定上限値 1%～99% を超えたときに終了する。
    - デリバリーグループ内のいずれかのマシンの負荷が指定上限値 1%～99% を超えたときに終了する。

    事前起動セッションは、ユーザーがいずれかのアプリケーションを起動したとき、指定した時間が経過したとき、または指定した負荷のしきい値を超えたときのいずれかの状態が発生するまで保持されます。

セッション残留を有効にするには、次の手順に従います

1. 左側のペインで ［デリバリーグループ］を選択します。
2. グループを選択して、操作バーの ［デリバリーグループの編集］をクリックします。
3. ［アプリケーションの残留］ページで、［セッションをアクティブのまま保持する期間を指定する］をクリックします。



4. ユーザーが別のアプリケーションを起動しない場合、残留セッションを保持する時間は複数の設定によって決定されます。

   - この時間が経過したときにセッションを終了する。セッションを自動的に終了するまでの時間を指定します（1〜99 日間、1〜2,376 時間、または 1〜142,560 分）。
   - デリバリーグループ内のすべてのマシンの平均負荷が指定上限値 1%〜99% を超えたときに終了する。
   - デリバリーグループ内のいずれかのマシンの負荷が指定上限値 1%〜99% を超えたときに終了する。

   要約：残留セッションは、次のいずれかの状態が発生するまで保持されます：ユーザーがいずれかのアプリケーションを起動したとき、指定した時間が経過したとき、または指定した負荷のしきい値を超えたとき。

メンテナンスモードでマシンから切断されたときのセッションの再接続の制御

> 注:
>
> この機能は、PowerShell のみで利用可能です。

メンテナンスモードのマシンで切断されたセッションが、デリバリーグループ内のマシンに再接続できるかどうかを制御できます。

2106 より前のバージョンでは、メンテナンスモードでマシンから切断されたシングルセッションのプールされたデスクトップセッションについて、再接続は許可されていませんでした。バージョン 2106 からは、メンテナンスモードでマシンから切断された後、（セッションの種類に関係なく）再接続を許可または禁止するようにデリバリーグループを構成できるようになりました。

デリバリーグループを作成または編集する場合(`New-BrokerDesktopGroup`、`Set-BrokerDesktopGroup`）は、`-AllowReconnectInMaintenanceMode <boolean>`パラメーターを使用して、メンテナンスモードでマシンから切断されたマシンの再接続を許可または禁止します。

- true に設定すると、セッションはグループ内のマシンに再接続できます。
- false に設定すると、セッションはグループ内のマシンに再接続できません。

デフォルト値:

- シングルセッション：無効
- マルチセッション：有効

セッションローミングを構成する

デフォルトでは、デリバリーグループでセッションローミングが有効になっています。ユーザーのクライアントデバイス間でセッションローミングが行われます。ユーザーがセッションを開始した後に別のデバイスに移動した場合、同じセッションが使用され、両方のデバイスで同時にアプリケーションを使用することができます。複数のデバイスでアプリケーションを表示できます。デバイスや、現在のセッションが存在するかどうかに関係なく、アプリケーションが引き継がれます。たいていの場合、アプリケーションに割り当てられたプリンターやそのほかのリソースも引き継がれます。または、PowerShell を使用することもできます。詳しくは、「セッションローミング」を参照してください。

アプリケーションのセッションローミングを構成する　アプリケーションのセッションローミングを構成するには、次の手順に従います:

1. コンソールの左側のペインで ［デリバリーグループ］を選択します。
2. グループを選択して、操作バーの ［デリバリーグループの編集］を選択します。
3. ［ユーザー］ページで、［ユーザーがデバイス間を移動するときにセッションローミングを行う］チェックボックスをオンにして、セッションローミングを有効にします。
    - 有効にすると、ユーザーがアプリケーションセッションを開始した後に別のデバイスに移動した場合、同じセッションが使用され、両方のデバイスでアプリケーションを使用することができます。無効にすると、セッションはデバイス間でローミングしなくなります。
4. ［**OK**］を選択して、変更を適用してウィンドウを閉じます。

デスクトップのセッションローミングを構成する　デスクトップのセッションローミングを構成するには、次の手順に従います:

1. コンソールの左側のペインで ［デリバリーグループ］を選択します。
2. グループを選択して、操作バーの ［編集］を選択します。
3. ［デスクトップ］ページでデスクトップを選択し、［編集］を選択します。
4. ［セッションローミング］チェックボックスをオンにして、セッションローミングを有効にします。

- 有効にすると、ユーザーがデスクトップを開始した後に別のデバイスに移動した場合、同じセッションが使用され、両方のデバイスでアプリケーションを使用することができます。無効にすると、セッションはデバイス間でローミングしなくなります。

［**OK**］を選択して、変更を適用してウィンドウを閉じます。

アプリケーション

アプリケーションを表示し、デリバリーグループに追加します。

1. コンソールの左側のペインで ［デリバリーグループ］を選択します。
2. グループを選択します。このグループにアプリケーションが含まれている場合は、操作バーに ［アプリケーションの表示］が表示されます。
3. ［アプリケーションの表示］を選択します。このグループで利用可能なすべてのアプリケーションが表示される［アプリケーション］ノードに移動します。
4. このグループにさらにアプリケーションを追加するには、［デリバリーグループ］ノードに移動し、グループを選択して、操作バーで ［アプリケーションの追加］を選択します。

トラブルシューティング

- 仲介セッションを起動する場合、Delivery Controller に登録されていない VDA は考慮されません。これにより、登録されていれば使用されるはずのリソースが使用されない場合があります。VDA が登録されない理由はさまざまですが、その多くは管理者がトラブルシューティングできます。詳細画面ではカタログ作成ウィザードで、またはカタログをデリバリーグループに登録した後に、トラブルシューティング情報を提供します。

  デリバリーグループを作成すると、デリバリーグループの［詳細］ペインに、登録できるのに登録されていないマシンの数が表示されます。たとえば、1 台または複数台のマシンの電源が入っておりメンテナンスモードではないのに、Controller に現在登録されていない場合があります。「未登録だが登録する必要がある」のマシンが表示された場合は、［詳細］ペインの ［トラブルシューティング］タブで、考えられる原因と推奨される修正アクションを確認します。

  機能レベルに関するメッセージについては、「VDA バージョンと機能レベル」を参照してください。

  VDA 登録のトラブルシューティングについて詳しくは、CTX136668を参照してください。

- デリバリーグループの表示では、［詳細］ペインの ［インストール済み **VDA** のバージョン］が、マシンにインストールされている実際のバージョンと異なる可能性があります。マシンの Windows の［プログラムと機能］には、VDA の実際のバージョンが表示されます。
- マシンの状態が「**Power State Unknown**」の場合、CTX131267を参照してください。

アプリケーショングループの作成

August 17, 2024

> 注:
>
> Web Studio（Web ベース）と Citrix Studio（Windows ベース）の 2 つの管理コンソールを使用して、Citrix Virtual Apps and Desktops の展開を管理できます。この記事では Web Studio のみを扱います。Citrix Studio について詳しくは、Citrix Virtual Apps and Desktops 7 2212 以前の同様の記事を参照してください。

はじめに

アプリケーショングループを使用すると、アプリケーションのコレクションを管理できます。異なるデリバリーグループ間で共有されているアプリケーションのアプリケーショングループを作成します。または、デリバリーグループ内のユーザーのサブセットが使用するアプリケーションを作成します。アプリケーショングループはオプションです。複数のデリバリーグループに同じアプリケーションを追加する代わりの手段となります。デリバリーグループを複数のアプリケーショングループに関連付け、アプリケーショングループを複数のデリバリーグループに関連付けます。

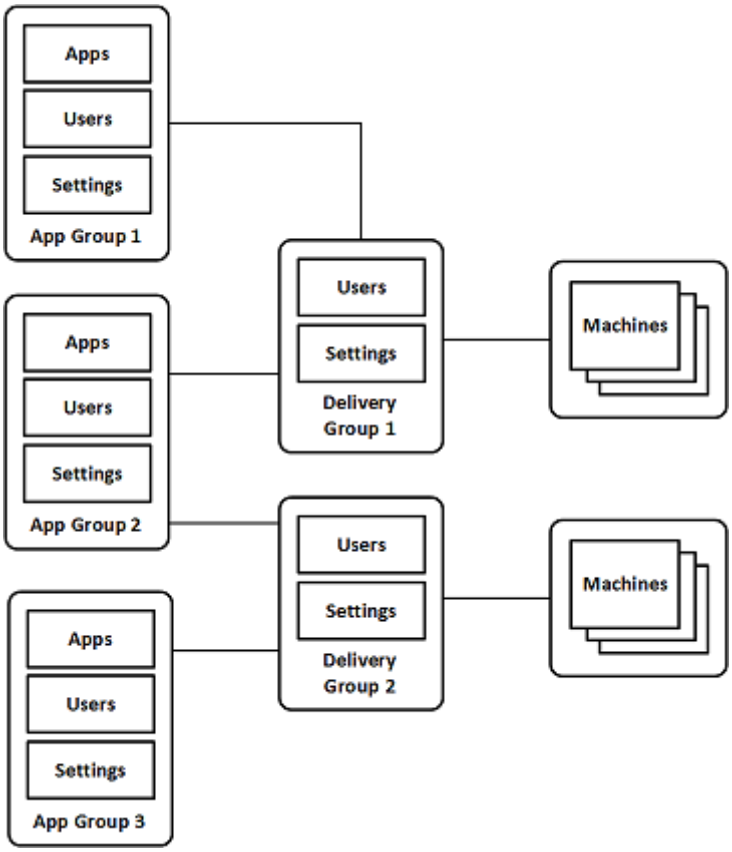
アプリケーショングループの使用は、さらに多くのデリバリーグループを使用するのに比べて、アプリケーション管理とリソース制御に利点をもたらします:

- アプリケーションおよびその設定を論理的にグループ化することで、アプリケーションを 1 つの単位として管理することができます。たとえば、同じアプリケーションをそれぞれのデリバリーグループに 1 つずつ追加（公開）する必要はありません。
- アプリケーショングループ間でのセッション共有により、リソースの消費を削減できます。また、アプリケーショングループ間のセッション共有を無効にすることが有益な場合もあります。
- タグ制限機能を使用すると、選択したデリバリーグループ内のマシンのサブセットだけを対象にして、アプリケーショングループからアプリケーションを公開できます。タグによる制限で、複数の公開タスクに既存のマシンを使用できるので、追加のマシンを展開、管理するコストを節約できます。タグ制限は、デリバリーグループのマシンをさらに分割（またはパーティション化）するものと考えることができます。タグ制限のあるアプリケーショングループやデスクトップを使用すると、デリバリーグループ内のマシンのサブセットを分離してトラブルシューティングするときに便利です。

構成例

例 **1**:

次の図に、アプリケーショングループを含む Citrix Virtual Apps and Desktops 環境を示します:



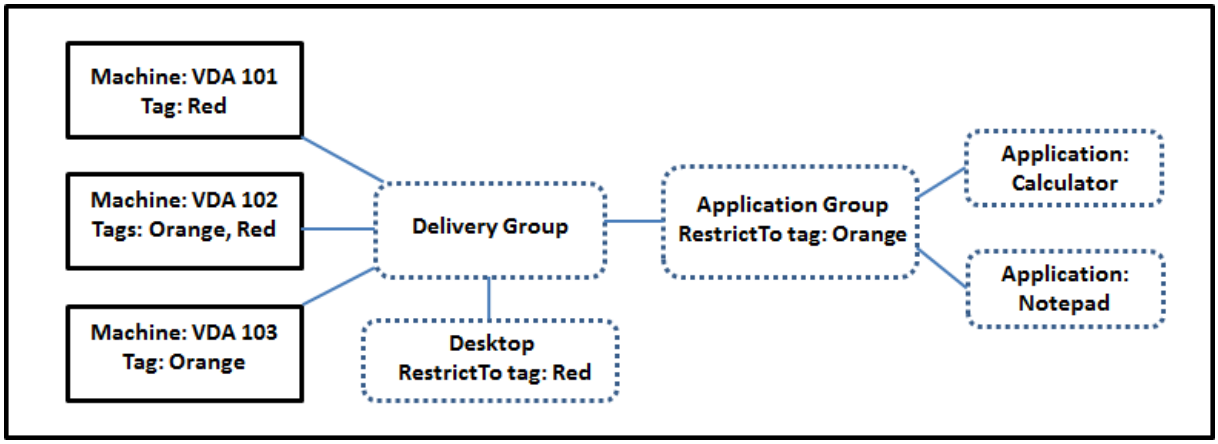
この構成では、アプリケーションはデリバリーグループではなくアプリケーショングループに追加されます。デリバリーグループでは、使用するマシンを指定します。（表示されていませんが、マシンはマシンカタログに含まれています。）

アプリケーショングループ 1 はデリバリーグループ 1 に関連付けられています。アプリケーショングループ 1 に指定されたユーザーは、アプリケーショングループ 1 のアプリケーションにアクセスします。これらのグループは、デリバリーグループ 1 のユーザーリストにも含まれている場合にのみ表示されます。この構成は、アプリケーショングループのユーザー一覧が、関連付けられているデリバリーグループのユーザー一覧のサブセット（制限）であるというガイダンスに従っています。アプリケーショングループ 1 の設定（アプリケーショングループ間で共有されるアプリケーションセッション、関連付けられているデリバリーグループなど）は、このグループのアプリケーションとユーザーに適用されます。デリバリーグループ 1 の設定は、アプリケーショングループ 1 および 2 のユーザーに適用されます。この 2 つのアプリケーショングループがこのデリバリーグループに関連付けられているためです。

アプリケーショングループ 2 は、デリバリーグループ 1 と 2 に関連付けられています。この 2 つのデリバリーグループそれぞれにアプリケーショングループ 2 の優先度を割り当てることで、アプリケーション起動時にデリバリーグループをチェックする順序が指定されます。同等の優先度が割り当てられたデリバリーグループ間では、負荷が分散されます。アプリケーショングループ 2 に指定されたユーザーは、アプリケーショングループ 2 のアプリケーションにアクセスします。ただし、デリバリーグループ 1 とデリバリーグループ 2 のユーザーリストにも表示される必要があります。

例 **2**:

この単純なレイアウトでは、あるデスクトップおよびアプリケーションの起動に関係するマシンを、タグを使用して制限します。サイトには、1 つの共有デリバリーグループ、1 つの公開デスクトップ、および 2 つのアプリケーションで構成された 1 つのアプリケーショングループがあります。



3 台のマシン（VDA 101～103）それぞれにタグが追加されています。

アプリケーショングループは、「オレンジ」タグの制限付きで作成されました。各アプリケーションは、「オレンジ」タグが付いたデリバリーグループ内のマシン、VDA 102 および 103 でのみ起動されます。

アプリケーショングループ（およびデスクトップ）でのタグ制限の使用に関する包括的な例やガイダンスは、「タグ」を参照してください。

ガイダンスおよび考慮事項

Citrix では、アプリケーショングループとデリバリーグループの両方ではなく、どちらか一方にアプリケーションを追加することをお勧めします。両方に追加すると、アプリケーションを 2 種類のグループに追加することにより複雑度が増加し、管理が困難になる可能性があります。

デフォルトでは、アプリケーショングループが有効になっています。アプリケーショングループ作成後、グループを編集してこの設定を変更できます。「アプリケーショングループの管理」を参照してください。

デフォルトでは、アプリケーショングループ間でのアプリケーションセッションの共有が有効になっています。「アプリケーショングループ間のセッション共有」を参照してください。

Citrix では、デリバリーグループを最新のバージョンにアップグレードすることをお勧めします。このプロセスには以下が必要です:

1. デリバリーグループで使用されているマシン上の VDA のアップグレード
2. それらのマシンを含むマシンカタログのアップグレード
3. デリバリーグループのアップグレード

詳しくは、「デリバリーグループの管理」を参照してください。

アプリケーショングループを使用するには、コアコンポーネントがバージョン 7.9 以上である必要があります。

アプリケーショングループを作成するには、デリバリーグループ管理者組み込みの役割の配信管理者権限が必要です。詳しくは、「委任管理」を参照してください。

この記事では、アプリケーションを複数のアプリケーショングループに「関連付ける」ことについて説明します。このアクションは、利用可能なソースからそのアプリケーションのインスタンスを追加することとは異なります。同様に、デリバリーグループはアプリケーショングループに関連付けられます。追加されるのでも、お互いのコンポーネントになるのでもありません。

アプリケーショングループを使用したセッション共有

アプリケーションセッション共有を有効にすると、すべてのアプリケーションが同一のアプリケーションセッションで起動されるようになります。これにより、さらなるアプリケーションセッションの起動にかかるコストが抑えられるとともに、クリップボードを使用するアプリケーション機能（コピーアンドペーストなど）を使用できます。ただし、セッション共有を解除できる場合もあります。

アプリケーショングループを使用する場合、以下の 3 通りの方法でアプリケーションセッション共有を構成して、デリバリーグループのみを使用ときに利用できる標準的なセッション共有の動作を拡張できます：

- アプリケーショングループ間でセッション共有を有効にする。
- 同一のアプリケーショングループに含まれるアプリケーション間でのみセッション共有を有効にする。
- セッション共有を無効にする。

アプリケーショングループ間のセッション共有

アプリケーショングループ間のアプリケーションセッション共有を有効にすることも、この共有を無効化して、アプリケーションセッション共有を同一のアプリケーショングループに含まれるアプリケーションのみに限定することもできます。

- アプリケーショングループ間のセッション共有を有効にすることが役立つ例：

  アプリケーショングループ 1 には、Word や Excel などの Microsoft Office アプリケーションが含まれています。アプリケーショングループ 2 にはメモ帳や電卓などその他のアプリケーションが含まれており、両方のアプリケーショングループは同じデリバリーグループに接続されています。両方のアプリケーショングループへのアクセス権を持つユーザーが、Word を起動してアプリケーションセッションを開始してから、メモ帳を起動するとします。Controller により、このユーザーの Word が実行されている既存のセッションがメモ帳の実行にも適していると判断されると、メモ帳は既存のセッション内で起動されます。メモ帳を既存のセッションで実行できない場合（タグによる制限でセッションの実行元のマシンが除外されている場合など）、セッション共有を使用せず適切なマシン上に新しいセッションが作成されます。

- アプリケーショングループ間のセッション共有を無効にすることが役立つ例：

  同じマシンにインストールされている他のアプリケーションとうまく相互運用できない一連のアプリケーションを含む構成。同じソフトウェアスイートの 2 つの異なるバージョンや、同じ Web ブラウザーの 2 つの異な

るバージョンなど。管理者は、同じセッションで両方のバージョンを起動することをユーザーに許可しないほうがいいと考えました。

ソフトウェアスイートの各バージョン用にアプリケーショングループを 1 つ作成し、ソフトウェアスイートの各バージョンのアプリケーションを対応するアプリケーショングループに追加します。これらの各アプリケーショングループでグループ間のセッション共有を無効にすると、各グループで指定されたユーザーは同じセッションで同じバージョンのアプリケーションを実行できます。ユーザーは引き続き他のアプリケーションを同時に実行できますが、同じセッションでは実行できません。異なるバージョンのアプリケーションを起動するか、アプリケーショングループには含まれていないアプリケーションを起動すると、そのアプリケーションは新しいセッションで起動されます。

このアプリケーショングループ間のセッション共有機能は、セキュリティサンドボックス機能ではありません。完全に信頼することはできず、ユーザーが別の手段（Windows エクスプローラーなど）を使用してセッションにアプリケーションを起動することは防げません。

マシンがフル稼働の場合、そのマシンで新しいセッションは開始されません。新しいアプリケーションは、セッション共有を使用して、必要に応じてマシン上の既存のセッションで開始されます。

事前起動セッションは、アプリケーションセッション共有が許可されているアプリケーショングループでのみ利用できます（残留セッション機能を使用するセッションは、すべてのアプリケーショングループで利用できます）。これらの機能は、アプリケーショングループに関連付けるデリバリーグループごとに有効にして構成する必要があります。アプリケーショングループでは設定できません。

デフォルトでは、アプリケーショングループの作成時、アプリケーショングループ間のアプリケーションセッション共有は有効になっています。グループを作成するときにこれを変更することはできません。アプリケーショングループ作成後、グループを編集してこの設定を変更できます。「アプリケーショングループの管理」を参照してください。

アプリケーショングループ内でのセッション共有の無効化

同一のアプリケーショングループに含まれるアプリケーション間で、アプリケーションセッション共有を無効にすることができます。

- アプリケーショングループ内のセッション共有を無効にすることが役立つ例:

  ユーザーが別々のモニターで、アプリケーションの複数の全画面セッションへ同時にアクセスできるようにする場合。

  アプリケーショングループを作成して、そのグループにアプリケーションを追加する場合。

デフォルトでは、アプリケーショングループ作成時にはアプリケーションセッションの共有が有効になっています。グループを作成するときにこの設定を変更することはできません。アプリケーショングループ作成後、グループを編集してこの設定を変更できます。「アプリケーショングループの管理」を参照してください。

アプリケーショングループの作成

アプリケーショングループを作成するには:

1. Web Studio にサインインします。
2. 左側のペインで ［アプリケーション］を選択し、［アプリケーショングループ］タブを選択します。
3. フォルダーを使用してアプリケーショングループを整理するには、**Application Groups** ルートフォルダーの下にフォルダーを作成します。
4. グループを作成するフォルダーを選択し、［アプリケーショングループの作成］をクリックします。グループ作成ウィザードが起動し、［はじめに］ページが表示されます。このウィザードで、今後このページが表示されないようにできます。
5. ウィザードに従って、以下に説明するページで設定を構成します。各ページの操作を終えたら、［概要］ページに到達するまで ［次へ］を選択します。

手順 **1**: デリバリーグループ

［デリバリーグループ］ページには、すべてのデリバリーグループが、各グループに含まれるマシンの数とともに表示されます。

- ［互換性のあるデリバリーグループ］リストには、選択可能なデリバリーグループが含まれています。互換性のあるデリバリーグループには、ランダムな（永続的ではない、つまり静的に割り当てられていない）マルチセッション OS マシンまたはシングルセッションOS マシンが含まれます。
- ［互換性のないデリバリーグループ］リストには、選択できないデリバリーグループが含まれています。各エントリで、静的に割り当てられたマシンを含む、などの互換性がない理由が説明されます。

アプリケーショングループは、アプリケーションを配信可能な共有（プライベートではない）マシンが含まれるデリバリーグループに関連付けることができます。

次の両方の条件が満たされている場合は、デスクトップのみを配信する共有マシンが含まれるデリバリーグループを選択することもできます:

- デリバリーグループは、共有マシンが含まれ、7.9 より前のバージョンの XenDesktop で作成されたものです。
- デリバリーグループの編集権限があります。

アプリケーショングループの作成ウィザードをコミットすると、デリバリーグループの種類が自動的に「デスクトップおよびアプリケーション」に変換されます。

おそらくはアプリケーションを整理したり現在は使用されていないアプリケーションのストレージとして使用したりするために、デリバリーグループに関連付けないアプリケーショングループを作成することができますが、アプリケーショングループで少なくとも 1 つのデリバリーグループを指定するまでは、そのアプリケーショングループを使用してアプリケーションを配信することはできませんまた、デリバリーグループが指定されていない場合は、［スタート］メニューから のソースからアプリケーショングループにアプリケーションを追加することもできません。

選択するデリバリーグループで、アプリケーションの配信に使用するマシンを指定します。アプリケーショングループに関連付けるデリバリーグループの横にあるチェックボックスをオンにします。

タグによる制限を追加するには、［タグでマシンの起動を制限します］をオンにし、ドロップダウンリストからタグを選択します。

手順 **2**：ユーザー

アプリケーショングループでアプリケーションユーザーを指定します。1 つ前のページで選択したデリバリーグループのすべてのユーザーとユーザーグループに許可するか、これらのデリバリーグループから特定のユーザーとユーザーグループを選択します。指定したユーザーの使用を制限した場合は、デリバリーグループとアプリケーショングループで指定したユーザーだけが、このグループのアプリケーションにアクセスできます。基本的に、アプリケーショングループのユーザー一覧は、デリバリーグループのユーザー一覧のフィルターとして機能します。

認証されていないユーザーによるアプリケーション使用の有効化または無効化は、デリバリーグループでのみ行えます。アプリケーショングループではできません。

展開内のユーザー一覧が指定されている場所については、「ユーザー一覧の指定場所」を参照してください。

手順 **3**：アプリケーション

ヒント：

- アプリケーションをデリバリーグループに追加すると、デフォルトで「アプリケーション」という名前のフォルダー内に表示されます。別のフォルダーを指定することもできます。アプリケーションの追加時にそのフォルダー内に同じ名前のアプリケーションが存在する場合、追加するアプリケーションの名前を変更するよう指示するメッセージが表示されます。提案された一意の名前を受け入れると、アプリケーションにその新しい名前が追加されます。それ以外の場合は、追加する前に名前を変更する必要があります。詳しくは、「アプリケーションフォルダーの管理」を参照してください。
- アプリケーションのプロパティ（設定）は、追加時、または後で変更できます。「アプリケーションプロパティの変更」を参照してください。同じ名前の 2 つのアプリケーションを同じユーザーに公開する場合は、Web Studio の ［アプリケーション名（ユーザー用）］プロパティを変更します。これを行わないと、Citrix Workspace アプリで同じ名前が 2 つ表示されます。
- アプリケーションを複数のアプリケーショングループに追加する場合、そのすべてのアプリケーショングループのアプリケーションを見ることができる十分な権限を有していなければ、表示上の問題が発生する可能性があります。そのような問題が発生した場合は、より上位の権限を持つ管理者に相談するか、または自身の権限を拡張して、アプリケーションを追加したグループをすべて含めるようにします。

ドロップダウンメニューから ［追加］をクリックして、アプリケーションのソースを表示します。

- ［スタート］メニューから：選択したデリバリーグループのマシンで検出されたアプリケーション。このソースを選択すると、新たなページが開き、検出されたアプリケーションが一覧表示されます。追加するアプリケーションのチェックボックスをオンにし、［**OK**］をクリックします。

このソースは、次のいずれかを選択した場合は選択できません：

- 関連するデリバリーグループのないアプリケーショングループ。
- マシンを含まないデリバリーグループが関連付けられたアプリケーショングループ。
- マシンを含まないデリバリーグループ。

- 手動で定義：サイトまたはネットワーク内の別の場所にあるアプリケーション。このソースを選択すると、新たなページが開くので、そのページで実行可能ファイルのパス、作業ディレクトリ、オプションのコマンドライン引数、管理者およびユーザー用の表示名を入力します。これらの情報を入力したら、［**OK**］をクリックします。
- 既存：以前サイトに追加したアプリケーション。このソースを選択すると、新たなページが開き、検出されたアプリケーションが一覧表示されます。追加するアプリケーションのチェックボックスをオンにし、［**OK**］をクリックします。このソースは、サイトにアプリケーションが含まれていない場合は選択できません。
- **App-V**：App-V パッケージのアプリケーション。このソースを選択すると、新しいページが開くので、そのページで **App-V** サーバーまたはアプリケーションライブラリを選択します。結果表示で、追加するアプリケーションのチェックボックスをオンにし、［**OK**］をクリックします。詳しくは、「App-V アプリケーションの展開および配信」を参照してください。このソースは、サイトで App-V を構成していない場合は選択および表示できません。

上述のとおり、［追加］ドロップダウンメニューの特定のエントリは、そのタイプの有効なソースがない場合は選択できません。互換性のないソースは、一切表示されません。たとえば、アプリケーショングループにアプリケーショングループは追加できないため、このソースはアプリケーショングループ作成時には表示されません。

手順 **4**：スコープ

このページは、カスタムスコープを作成済みの場合にのみ表示されます。デフォルトでは、すべてのスコープが選択されています。詳しくは、「管理者権限の委任」を参照してください。

手順 **5**：まとめ

アプリケーショングループの名前を入力します。必要に応じて説明も入力できます。

概要の情報を確認し、［完了］をクリックします。

アプリケーショングループの管理

August 17, 2024

> 注:
>
> Web Studio（Web ベース）と Citrix Studio（Windows ベース）の 2 つの管理コンソールを使用して、Citrix Virtual Apps and Desktops の展開を管理できます。この記事では Web Studio のみを扱います。Citrix Studio について詳しくは、Citrix Virtual Apps and Desktops 7 2212 以前の同様の記事を参照してください。

はじめに

この記事では、作成済みのアプリケーショングループの管理方法について説明します。

以下の操作方法を含む、アプリケーショングループまたはデリバリーグループでのアプリケーションの管理について詳しくは、「アプリケーション」を参照してください:

- アプリケーショングループのアプリケーションの追加または削除
- アプリケーショングループの関連付けの変更

アプリケーショングループの管理には、組み込みの役割であるデリバリーグループ管理者の委任管理権限が必要です。詳しくは、「委任管理」を参照してください。

アプリケーショングループの有効化または無効化

アプリケーショングループを有効にすると、このグループに追加されたアプリケーションを配信できます。アプリケーショングループを無効にすると、グループ内のアプリケーションもすべて無効になります。ただし、これらのアプリケーションが他の有効なアプリケーショングループにも関連付けられている場合は、これらの他のアプリケーショングループから配信できます。アプリケーションが、アプリケーショングループに関連付けられているデリバリーグループに明示的に追加された場合は、アプリケーショングループを無効にしても、これらのデリバリーグループ内のアプリケーションには影響しません。

アプリケーショングループは、作成すると有効になります。グループを作成するときにこの構成を変更することはできません。

1. 左側のペインで ［アプリケーション］を選択し、［アプリケーショングループ］タブを選択します。
2. アプリケーショングループを選択し、操作バーで ［アプリケーショングループを編集します］を選択します。
3. ［設定］ページで、［アプリケーショングループを有効にする］チェックボックスをオンまたはオフにします。
4. ［適用］をクリックしてウィンドウを開いたままにするか、［保存］をクリックして変更を適用しウィンドウを閉じます。

アプリケーショングループ間でのアプリケーションセッション共有の有効化または無効化

アプリケーショングループの作成時、アプリケーショングループ間でのセッション共有は有効になっています。グループを作成するときにこの構成を変更することはできません。詳しくは、「アプリケーショングループを使用したセッション共有」を参照してください。

1. 左側のペインで ［アプリケーション］を選択し、［アプリケーショングループ］タブを選択します。
2. アプリケーショングループを選択し、操作バーで ［アプリケーショングループを編集します］を選択します。
3. ［設定］ページで、［アプリケーショングループ間のアプリケーションのセッション共有を有効にします］チェックボックスをオンまたはオフにします。
4. ［適用］をクリックしてウィンドウを開いたままにするか、［保存］をクリックして変更を適用しウィンドウを閉じます。

アプリケーショングループ内でのアプリケーションセッション共有の無効化

アプリケーショングループを作成すると、同じアプリケーショングループのアプリケーション間のセッション共有がデフォルトで有効になります。アプリケーショングループ間でのアプリケーションセッション共有を無効化しても、同じアプリケーショングループのアプリケーション間のセッション共有は引き続き有効です。

PowerShell SDK を使用して、所属するアプリケーション間のセッション共有を無効化したアプリケーショングループを構成できます。状況によっては、このオプションが望ましい場合もあります。たとえば、ユーザーが複数の非シームレスアプリケーションを個別のモニターのフルサイズのアプリケーションウィンドウで起動できるようにする場合などです。

アプリケーショングループ内でのアプリケーションセッション共有を無効にした場合、そのグループ内の各アプリケーションは新しいアプリケーションセッションで起動します。適切な切断されたセッションで同じアプリケーションが動作中の利用可能なセッションがあれば、そのセッションが再接続されます。たとえば、Notepad が動作中の切断されたセッションで Notepad を起動する場合、そのセッションは新しく作成されるのではなく再接続されます。複数の適切な切断セッションが利用可能なときは、そのうちの 1 つのセッションが再接続先として、ランダムだが決定的な方法で選択されます。同じ状況で同じ状態が再現したときは、同じセッションが選択されます。しかし、そうでない場合は再接続されるセッションは、予測できるとは限りません。

PowerShell SDK を使用して、既存のアプリケーショングループのすべてのアプリケーションでアプリケーションセッション共有を無効化するか、アプリケーションセッション共有を無効化したグループを作成します。

PowerShell コマンドレット例

セッション共有を無効にするには、Broker PowerShell コマンドレット`New-BrokerApplicationGroup`を使用するか、パラメーター`SessionSharingEnabled`を`False`に設定し、パラメーター`SingleAppPerSession`を`True`に設定した`Set-BrokerApplicationGroup`を使用します。

- たとえば、グループ内のすべてのアプリケーションでアプリケーションセッション共有が無効のアプリケーショングループを作成するには、以下を実行します:

  ```
  New-BrokerApplicationGroup AppGr1 -SessionSharingEnabled $False -
  SingleAppPerSession $True
  ```

- たとえば、既存のアプリケーショングループ内のすべてのアプリケーション間でアプリケーションセッション共有を無効化するには、以下を実行します:


```
Set-BrokerApplicationGroup AppGR1 -SessionSharingEnabled $False -
SingleAppPerSession $True
```

注意事項

- SingleAppPerSessionプロパティを有効にするには、SessionSharingEnabledプロパティを False に設定する必要があります。この 2 つのプロパティは、同時に有効化してはなりません。SessionSharingEnabledパラメーターは、アプリケーショングループ間のセッション共有に関するものです。
- アプリケーションセッション共有は、アプリケーショングループに関連付けられているが、デリバリーグループには関連付けられていないアプリケーションに対してのみ有効です。デリバリーグループに直接関連付けられているアプリケーションはすべてデフォルトでセッションを共有します。
- 1 つのアプリケーションが複数のアプリケーショングループに割り当てられている場合、グループどうしで設定が矛盾しないようにしてください。たとえば、同じオプションを一方のグループではTrueに、他方のグループではFalseに設定していると、予想のつかない動作を引き起こします。

アプリケーショングループ名の変更

1. 左側のペインで ［アプリケーション］を選択し、［アプリケーショングループ］タブを選択します。
2. アプリケーショングループを選択し、操作バーで ［アプリケーショングループ名を変更します］を選択します。
3. 新しい一意の名前を指定し、［**OK**］をクリックします。

アプリケーショングループとデリバリーグループの関連付けの追加、削除、または優先度変更

アプリケーショングループは、アプリケーションを配信可能な共有（プライベートではない）マシンが含まれるデリバリーグループに関連付けることができます。

次の両方の条件が満たされている場合は、デスクトップのみを配信する共有マシンが含まれるデリバリーグループを選択することもできます:

- デリバリーグループは、共有マシンが含まれ、7.9 より前のバージョンで作成されたものです。
- デリバリーグループの編集権限があります。

デリバリーグループの種類は、［アプリケーショングループを編集します］ダイアログボックスが表示されると、自動的に「デスクトップとアプリケーション」に変換されます。

1. 左側のペインで ［アプリケーション］を選択し、［アプリケーショングループ］タブを選択します。
2. アプリケーショングループを選択し、操作バーで ［アプリケーショングループを編集します］を選択します。
3. ［デリバリーグループ］ページを選択します。

4. デリバリーグループを追加するには、[追加] をクリックします。使用可能なデリバリーグループのチェックボックスをオンにします（互換性のないデリバリーグループは選択できません）。選択が完了したら、[**OK**] をクリックします。
5. デリバリーグループを削除するには、削除するグループのチェックボックスをオンにして、[削除] をクリックします。確認のメッセージが表示されたら、削除を確定します。
6. デリバリーグループの優先度を変更するには、デリバリーグループのチェックボックスをオンにして、[優先度の編集] をクリックします。優先順位（0 が最高）を入力し、[**OK**] をクリックします。
7. [適用] をクリックして行った変更を適用しウィンドウを開いたままにするか、[保存] をクリックして変更を適用しウィンドウを閉じます。

アプリケーショングループのタグ制限の追加、変更、または削除

タグによる制限を追加、変更、および削除すると、どのマシンがアプリケーション起動の対象となるかについて、予期しない結果を招くことがあります。「タグ」に記載されている考慮事項と注意を確認してください。

1. 左側のペインで [アプリケーション] を選択し、[アプリケーショングループ] タブを選択します。
2. アプリケーショングループを選択し、操作バーで [アプリケーショングループを編集します] を選択します。
3. [デリバリーグループ] ページを選択します。
4. タグによる制限を追加するには、[タグでマシンの起動を制限します] をオンにし、ドロップダウンリストからタグを選択します。
5. タグによる制限を変更または削除するには、異なるタグを選択するか、[タグでマシンの起動を制限します] をオフにして、タグによる制限を完全に削除します。
6. [適用] をクリックして行った変更を適用しウィンドウを開いたままにするか、[保存] をクリックして変更を適用しウィンドウを閉じます。

アプリケーショングループのユーザーの追加または削除

ユーザーについて詳しくは、「アプリケーショングループの作成」を参照してください。

1. 左側のペインで [アプリケーション] を選択し、[アプリケーショングループ] タブを選択します。
2. アプリケーショングループを選択し、操作バーで [アプリケーショングループを編集します] を選択します。
3. [ユーザー] ページを選択します。アプリケーショングループ内のアプリケーションの使用を、関連付けられたデリバリーグループ内のすべてのユーザーに許可するか、特定のユーザーおよびグループにのみ許可するかを指定します。ユーザーを追加するには、[追加] をクリックし、追加するユーザーを指定します。ユーザーを削除する場合は、1 人または複数のユーザーを選択し、[削除] をクリックします。
4. [適用] をクリックして行った変更を適用しウィンドウを開いたままにするか、[保存] をクリックして変更を適用しウィンドウを閉じます。

アプリケーショングループのアプリケーションアイコンの追加、変更、または削除

アプリケーションアイコンを追加、変更、または削除するには、次の手順を実行します。

1. 左側のペインで ［アプリケーション］を選択します。
2. ［アプリケーション］タブでアプリケーションを選択してから ［プロパティ］を選択します。

   アプリケーショングループレベルで変更を加えるには、［アプリケーショングループ］タブに移動し、グループ内のアプリケーションを選択して、［プロパティ］を選択します。
3. ［デリバリー］ページを選択してから、［変更］を選択します。［アイコンの選択］ウィンドウが開きます。
4. ［アイコンの選択］ウィンドウで、次のいずれかを実行します:

   - アイコンを追加するには、［追加］を選択して、対象のアイコンを参照します。
   - アイコンを削除するには、対象のアイコンを選択して、［削除］を選択します。
   - アイコンを変更するには、対象アプリケーション用のアイコンを選択します。

   > 重要:
   >
   > - サイズが 200KB を超えるアイコンを追加することはできません。
   > - 追加できるのは.icon ファイルのみです。
   > - 組み込みのアイコンは削除できません。
   > - 使用中のアプリケーションのアイコンを削除することはできません。
5. ［保存］を選択して、変更を適用してウィンドウを閉じます。

アプリケーショングループのスコープの変更

スコープの変更は、スコープを作成済みの場合のみ行うことができます（［すべて］のスコープを編集することはできません）。詳しくは、「管理者権限の委任」を参照してください。

1. 左側のペインで ［アプリケーション］を選択し、［アプリケーショングループ］タブを選択します。
2. アプリケーショングループを選択し、操作バーで ［アプリケーショングループを編集します］を選択します。
3. ［スコープ］ページを選択します。スコープの横にあるチェックボックスをオンまたはオフにします。
4. ［適用］をクリックして行った変更を適用しウィンドウを開いたままにするか、［保存］をクリックして変更を適用しウィンドウを閉じます。

アプリケーショングループのスコープの変更

スコープの変更は、スコープを作成済みの場合のみ行うことができます（［すべて］のスコープを編集することはできません）。詳しくは、「管理者権限の委任」を参照してください。

1. 左側のペインで ［アプリケーション］を選択し、［アプリケーショングループ］タブを選択します。

2. アプリケーショングループを選択し、操作バーで ［アプリケーショングループを編集します］を選択します。
3. ［スコープ］ページを選択します。変更するスコープの横にあるチェックボックスをオンまたはオフにします。
4. ［適用］を選択して行った変更を適用しウィンドウを開いたままにするか、［保存］を選択して変更を適用しウィンドウを閉じます。

アプリケーショングループの削除

アプリケーションは、デリバリーグループかアプリケーショングループの少なくとも 1 つに割り当てる必要があります。アプリケーショングループの削除により 1 つまたは複数のアプリケーションがグループに属していない状態になる場合は、グループを削除するとこれらのアプリケーションも削除されることを通知する警告メッセージが表示されます。削除を確定またはキャンセルすることができます。

アプリケーションを削除しても、元のソースからは削除されません。ただし、再度使用可能にする場合は、再度追加する必要があります。

1. 左側のペインで ［アプリケーション］を選択し、［アプリケーショングループ］タブを選択します。
2. アプリケーショングループを選択し、操作バーで ［グループの削除］を選択します。
3. 確認のメッセージが表示されたら、削除を確定します。

フォルダーを使用したアプリケーショングループの整理

簡単にアクセスできるように、フォルダーを作成してアプリケーショングループを整理できます。

必須の役割

デフォルトでは、次の組み込みの役割のいずれかがある場合、アプリケーショングループのフォルダーを作成および管理できます:

- クラウド管理者
- 完全な管理者
- アプリケーショングループ管理者

カスタム役割を作成することで、管理アクションを他のユーザーに委任できます。次の表に、各アクションに必要な権限を示します。

アクション	必要な権限
アプリケーショングループフォルダーを作成する	アプリケーショングループフォルダーの作成
アプリケーショングループフォルダーを削除する	アプリケーショングループフォルダーの削除
アプリケーショングループフォルダーを移動する	アプリケーショングループフォルダーの移動

アクション	必要な権限
アプリケーショングループフォルダーの名前を変更する	アプリケーショングループフォルダーの編集
アプリケーショングループをフォルダーに移動する	アプリケーショングループフォルダーの編集、アプリケーショングループのプロパティの編集

詳しくは、「役割の作成と管理」を参照してください。

フォルダーの作成と管理

操作バーまたは右クリックメニューを使用して、アプリケーショングループフォルダーを作成および管理できます。さらに、アプリケーショングループまたはフォルダーをフォルダーツリー内の目的の場所にドラッグできます。

ヒント:

- 最大で 5 レベルまでの階層構造でフォルダーをネストできます（デフォルトのルートフォルダーを除く）。
- フォルダーには、アプリケーショングループとサブフォルダーを含めることができます。フォルダーの削除は、フォルダーとそのサブフォルダーにアプリケーショングループが含まれていない場合にのみ可能となります。
- バックエンドのフォルダーツリーは、すべてのノード（マシンカタログ、デリバリーグループ、アプリケーション、およびアプリケーショングループなど）で共有されます。フォルダーの名前変更や移動時に他のリソースフォルダーと名前が競合しないように、異なるフォルダーツリーの第 1 レベルのフォルダーには異なる名前を付けることをお勧めします。

リモート PC アクセス

August 17, 2024

> 注:
>
> Web Studio（Web ベース）と Citrix Studio（Windows ベース）の 2 つの管理コンソールを使用して、Citrix Virtual Apps and Desktops の展開を管理できます。この記事では Web Studio のみを扱います。Citrix Studio について詳しくは、Citrix Virtual Apps and Desktops 7 2212 以前の同様の記事を参照してください。

リモート PC アクセスは Citrix Virtual Apps and Desktops の機能であり、組織で従業員が安全な方法でリモートから企業リソースに簡単にアクセスできるようにします。Citrix プラットフォームでは、ユーザーが社内の物理的な PC にアクセスできるようにすることで、この安全なアクセスを可能にします。ユーザーが社内 PC にアクセスできる場合、作業に必要なすべてのアプリケーション、データ、リソースにアクセスできます。リモート PC アクセスによ

り、テレワークに対応するために他のツールを導入したり提供したりする必要がなくなります。たとえば、仮想デスクトップまたはアプリケーション、および関連するインフラストラクチャなどです。

リモート PC アクセスでは、仮想デスクトップとアプリケーションを配信するのと同じ Citrix Virtual Apps and Desktops コンポーネントが使用されます。その結果、リモート PC アクセスの展開と構成の要件およびプロセスは、仮想リソースの配信のために Citrix Virtual Apps and Desktops の展開に必要なものと同じです。この統一性により、一貫性のある統一された管理エクスペリエンスが実現されます。ユーザーは、Citrix HDX を使用して社内 PC セッションを提供することで、最高のユーザーエクスペリエンスを実現できます。

この機能は、種類がリモート **PC** アクセスのマシンカタログで構成され、提供されます:

- OU を指定してマシンを追加する機能。この機能によって PC の一括追加を円滑に実行できます。
- 社内の Windows PC にログインするユーザーに基づいた自動ユーザー割り当て。単一ユーザーおよび複数ユーザーの割り当てをサポートしています。デフォルトでは、複数のユーザーが次の未割り当てのマシン: に自動的に割り当てられます。自動割り当てを 1 人のユーザーに制限するには、Web Studio にサインインし、［設定］に移動して、［リモート **PC** アクセスの複数ユーザー自動割り当てを有効にする］設定をオフにします。

Citrix Virtual Apps and Desktops では、他の種類のマシンカタログを使用することで、物理 PC のユースケースが増えます。これらのユースケースには次のようなものがあります:

- 物理 Linux PC
- プールされた物理 PC（ランダムに割り当てられ、専用ではありません）

> 注:
>
> サポートされている OS バージョンについて詳しくは、VDA のシステム要件（「シングルセッション OS」と「Linux VDA」）を参照してください。
>
> オンプレミス展開の場合、リモート PC アクセスは、Citrix Virtual Apps and Desktops の Advanced または Premium ライセンスでのみ有効です。セッションでは、他の Citrix Virtual Desktops セッションと同様にライセンスが消費されます。Citrix Cloud の場合、Citrix DaaS（旧称 Citrix Virtual Apps and Desktops サービス）および Workspace Premium Plus で有効です。

注意事項

Citrix Virtual Apps and Desktops 全般に適用される技術的要件および考慮事項はすべて、リモート PC アクセスにも適用されますが、一部は物理 PC のユースケースに対してより関連性があるか、または排他的な場合もあります。

> 重要:
>
> Windows 11（と一部の Windows 10 を実行している）物理システムには仮想化ベースのセキュリティ機能が含まれているため、VDA ソフトウェアがそれらを仮想マシンとして誤って検出します。この問題を緩和するには、次のオプションがあります。

> - VDA コマンドラインを使用したインストールで、「/physicalmachine」オプションを「/remotepc」オプションとともに使用します。
> - 前述のオプションを使用しなかった場合は、VDA のインストール後に次のレジストリ値を追加します
> `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`
>
> - 名前：ForceEnableRemotePC
> - 種類：DWORD
> - データ：1

展開に関する考慮事項

リモート PC アクセスの導入を計画する際は、以下の全般的な項目について判断してください。

- 既存の Citrix Virtual Apps and Desktops 展開にリモート PC アクセスを追加できます。このオプションを選択する前に、以下の点を考慮してください：
  - リモート PC アクセスの VDA に関連する追加の負荷をサポートするために、現在の Delivery Controller または Cloud Connector のサイズは適切か?
  - オンプレミスのサイトデータベースとデータベースサーバーは、リモート PC アクセスの VDA に関連する追加の負荷をサポートするために適切なサイズか?
  - 既存の VDA と新しいリモート PC アクセスの VDA は、サイトあたりサポートされる VDA の最大数を超えているか?
- VDA は、自動プロセスによって社内 PC に展開する必要があります。以下は、使用できるオプションです：
  - SCCM などの電子ソフトウェア配信（ESD）ツール：SCCM を使用した VDA のインストール。
  - 展開スクリプト：スクリプトを使用した VDA のインストール。
- 「リモート PC アクセスのセキュリティに関する考慮事項」を確認してください。

> 注：
>
> リモート PC アクセスを設計するときは、リモート PC の GPU に接続されている物理モニターの数と、現在設定されている/動作中の物理モニターの数を考慮する必要があります。モニターが Citrix セッションで使用されていないのに、GPU によって検出された場合、このモニターの存在は、GPU によってサポートされるモニターの最大制限にカウントされます。

マシンカタログに関する考慮事項

必要なマシンカタログの種類は、ユースケースによって異なります：

- リモート PC アクセスのマシンカタログ
  - Windows 専用 PC

  - Windows 専用のマルチユーザー PC。このユースケースは、複数のユーザーが異なるシフトでリモートアクセスできる物理的なオフィス PC に当てはまります。
  - プールされた Windows PC。このユースケースは、コンピューターラボなど、複数のランダムユーザーがアクセスできる物理 PC に適用されます。

- シングルセッション OS のマシンカタログ
  - 静的 - 専用 Linux PC
  - ランダム - プールされた Linux PC

マシンカタログの種類を特定したら、次の点を考慮してください:

- リモート PC アクセスでは、1 つのマシンを複数のマシンカタログに同時に関連付けることはできません。
- 委任管理を円滑に進めるために、各カタログの管理を適切な管理者に容易に委任できる地理的な場所、部署、またはその他のグループに基づいて、マシンカタログを作成することを検討してください。
- マシンアカウントが存在する OU を選択する場合は、より細分化するために下位レベルの OU を選択します。このような細分性が必要ない場合は、上位レベルの OU を選択できます。たとえば、Bank/Officers/Tellers の場合、より細分性を高めるために **Tellers** を選択します。それ以外の場合は、要件に基づいて ［役員］または ［銀行］を選択できます。
- リモート PC アクセスマシンカタログに割り当てた後に OU を移動または削除すると、VDA の関連付けに影響し、今後の割り当てで問題が発生します。したがって、マシンカタログの OU 割り当ての更新が Active Directory 変更計画で考慮されるように、適切な計画を立ててください。
- OU 構造のため、マシンカタログにマシンを追加する OU を選択することが容易でない場合は、OU を選択する必要はありません。後で PowerShell を使用してマシンをカタログに追加できます。デリバリーグループでデスクトップ割り当てが正しく構成されていれば、ユーザーの自動割り当ては引き続き機能します。ユーザー割り当てと併せてマシンカタログにマシンを追加するサンプルスクリプトについては、「GitHub」を参照してください。
- 統合された Wake on LAN は、リモート **PC** アクセスタイプのマシンカタログでのみ使用できます。

Linux VDA に関する考慮事項

次の考慮事項は、Linux VDA に固有のものです:

- Linux VDA は、非 3D モードの物理マシンでのみ使用します。NVIDIA のドライバーの制限により、HDX 3D モードが有効になっている場合、PC のローカル画面はブラックアウトせず、画面にはセッションのアクティビティが表示されます。この画面の表示は、セキュリティ上のリスクです。
- 物理 Linux マシンには、シングルセッション OS タイプのマシンカタログを使用します。
- Linux マシンでは、自動ユーザー割り当ては使用できません。
- ユーザーが既にローカルで PC にログオンしている場合、StoreFront から PC を起動しようとすると失敗します。
- Linux マシンでは、省電力オプションは使用できません。

技術的な要件および考慮事項

このセクションでは、物理 PC の技術要件と考慮事項について説明します。

- 以下はサポートされていません:
  - KVM スイッチ、またはセッションを切断する可能性のあるそのほかのコンポーネント。
  - ハイブリッド PC（オールインワンおよび NVIDIA Optimus ノートブックおよび PC を含む）。
  - デュアルブートマシン。
- キーボードとマウスを PC に直接接続します。電源を切ったり接続を切断したりできるモニターなどのコンポーネントに接続すると、これらの周辺機器が使用できなくなることがあります。キーボードやマウスをモニターなどのデバイス経由で接続する必要がある場合は、それらのコンポーネントの電源をオフにしないでください。
- PC は Active Directory ドメインサービスドメインに参加している必要があります。
- セキュアブートは Windows 10 および Windows 11 でのみサポートされています。
- PC にはアクティブなネットワーク接続が必要です。信頼性と帯域幅を高めるには、有線接続をお勧めします。
- Wi-Fi を使用する場合、以下の点を確認します:
  1. 電源設定でワイヤレスアダプターの電源を入れたままにするようにします。
  2. ユーザーがサインインする前にワイヤレスネットワークに自動的に接続できるように、ワイヤレスアダプターとネットワークプロファイルを構成します。そうしないと、ユーザーがログオンするまで VDA は登録されません。ユーザーがログオンするまで、PC ではリモートアクセスを使用できません。
  3. Wi-Fi ネットワークから Delivery Controller または Cloud Connector にアクセスできることを確認してください。
- リモート PC アクセスはノートブックコンピューターで使用できます。ノートブックがバッテリーで動作しているのではなく、電源に接続されていることを確認します。デスクトップ PC のオプションに合わせて、ノートブックの電源オプションを構成します。例:
  1. 休止機能を無効にする。
  2. スリープ機能を無効にする。
  3. カバーを閉じた場合の動作を ［何もしない］ に設定する。
  4. 電源ボタンを押したときの操作を ［シャットダウン］ に設定する。
  5. ビデオカードおよび NIC の省電力設定を無効にする。
- リモート PC アクセスは、Surface Pro デバイス上の Windows 10 でサポートされます。前述のノートブックと同じガイドラインに従います。
- ドッキングステーションを使用している場合、ノートブックをドッキング解除して再接続できます。ドッキング解除すると、VDA は Wi-Fi で Delivery Controller または Cloud Connector に再登録されます。ただし、ノートブックを再接続した場合、ワイヤレスアダプターを外さない限り、VDA は有線接続を使用するように切

り替わりません。有線接続が確立されると、組み込まれた機能がワイヤレスアダプターを切断するデバイスもあります。それ以外のデバイスでは、ワイヤレスアダプターを切断するためのカスタムソリューションかサードパーティ製のユーティリティが必要です。前述の Wi-Fi に関する考慮事項を確認してください。

デバイスのリモート PC アクセスでドッキングとドッキング解除を有効にするには、以下の操作を実行します:

1. ［スタート］メニューの ［設定］**>** ［システム］**>** ［電源とスリープ］で ［スリープ］を ［なし］に設定します。
2. ［デバイスマネージャー］**>** ［ネットワーク アダプター］**>** ［イーサネットアダプター］の［電源管理］で［電力の節約のために、コンピューターでこのデバイスの電源をオフにできるようにする］に移動します。［このデバイスで、コンピューターのスタンバイ状態を解除できるようにする］チェックボックスがオンになっていることを確認します。

- 同じ社内 PC にアクセスする複数のユーザーには、Citrix Workspace で同じアイコンが表示されます。ユーザーが Citrix Workspace にログオンすると、そのリソースが他のユーザーによって既に使用されている場合は使用不可と表示されます。
- 社内 PC へアクセスする各クライアントデバイス（自宅の PC など）に、Citrix Workspace アプリをインストールします。

構成の順序

このセクションでは、リモート **PC** アクセスタイプのマシンカタログを使用する場合にリモート PC アクセスを構成する方法の概要について説明します。他のタイプのマシンカタログを作成する方法については、「マシンカタログの作成」を参照してください。

1. オンプレミスサイトのみ - 統合された Wake on LAN 機能を使用するには、「Wake on LAN」で説明されている前提条件を構成します。
2. リモート PC アクセス用に新しい Citrix Virtual Apps and Desktops サイトが作成された場合:

   a) リモート **PC** アクセスサイトの種類を選択します。
   b) 管理者は、［電源管理］ページで、デフォルトのリモート PC アクセスマシンカタログのマシンの電源管理機能を有効または無効にできます。この設定は、後でマシンカタログのプロパティを編集して変更できます。Wake on LAN の構成について詳しくは、「Wake on LAN」を参照してください。
   c)「ユーザー」ページと「マシンアカウント」ページの情報を入力します。

   これらの手順を完了すると、「リモート **PC** アクセスマシン」という名前のマシンカタログと、「リモート **PC** アクセスデスクトップ」という名前のデリバリーグループが作成されます。

3. 既存の Citrix Virtual Apps and Desktops サイトに追加する場合:

   a) リモート **PC** アクセスタイプのマシンカタログを作成します（ウィザードの［オペレーティングシステム］ページ）。マシンカタログの作成方法について詳しくは、「マシンカタログの作成」を参照してくだ

さい。ターゲットの PC をリモート PC アクセスで使用できるように、正しい組織単位が割り当てられていることを確認します。

b) デリバリーグループを作成して、ユーザーがマシンカタログの PC にアクセスできるようにします。デリバリーグループの作成方法について詳しくは、「デリバリーグループの作成」を参照してください。PC へのアクセスが必要なユーザーが含まれる Active Directory グループにこのデリバリーグループを割り当てます。

4. VDA を社内 PC に展開します。

   - シングルセッション OS コア VDA インストーラー（VDAWorkstationCoreSetup.exe）を使用することをお勧めします。
   - シングルセッションのフル VDA インストーラー（VDAWorkstationSetup.exe）を /`remotepc`/`physicalmachine`オプションで使用することもできます。これにより、コア VDA インストーラーを使用する場合と同じ結果が得られます。

     > 注:
     >
     > リモート PC のインストールでは、/`physicalmachine`引数を/`remotepc`で使用して、VDA が特定のユーザーシナリオで正常に動作するようにします。

   - ヘルプデスクチームが Citrix Director を通じてリモートサポートを提供できるように、Windows リモートアシスタンスを有効にすることを検討してください。そのために、/`enable_remote_assistance`オプションを使用します。詳しくは、「コマンドラインを使ったインストール」を参照してください。
   - Director でログオン時間情報を表示するには、シングルセッション完全版 VDA インストーラーを使用して **Citrix User Profile Management WMI Plugin** コンポーネントを含める必要があります。/`includeadditional`オプションを使用してこのコンポーネントを含めます。詳しくは、「コマンドラインを使ったインストール」を参照してください。
   - SCCM を使用した VDA の展開については、「SCCM を使用した VDA のインストール」を参照してください。
   - 展開スクリプトを使用した VDA の展開については、「スクリプトを使用した VDA のインストール」を参照してください。

   手順 2〜4 を正常に完了すると、ユーザーが PC にローカルでログインしたときに、自動的にマシンが割り当てられます。

5. 社内 PC へのリモート接続で使用する各クライアントデバイスに、Citrix Workspace アプリをダウンロードしインストールするようユーザーに指示します。Citrix Workspace アプリは`https://www.citrix.com/downloads/`から、またはサポートされるモバイルデバイス向けのアプリストアから入手できます。

レジストリで管理される機能

> 注意:
>
> レジストリエディターの使用を誤ると、深刻な問題が発生する可能性があり、オペレーティングシステムの再インストールが必要になる場合もあります。レジストリエディターの誤用による障害に対して、Citrix では一切責任を負いません。レジストリエディターは、お客様の責任と判断の範囲でご使用ください。また、レジストリファイルのバックアップを作成してから、レジストリを編集してください。

複数ユーザーの自動割り当てを無効化

Delivery Controller ごとに、次のレジストリ設定を追加します:

`HKEY_LOCAL_MACHINE\Software\Citrix\DesktopServer`

- 値の名前: AllowMultipleRemotePCAssignments
- 種類: DWORD
- データ: 0

スリープモード（バージョン **7.16** 以降）

リモート PC アクセスマシンがスリープ状態に入ることを許可するには、このレジストリ設定を VDA に追加してからマシンを再起動します。再起動後は、オペレーティングシステムの省電力設定が優先されます。設定済みのアイドルタイマー間隔が経過すると、マシンはスリープモードに入ります。マシンがスリープモードから復帰すると、Delivery Controller に再登録されます。

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`

- 値の名前: DisableRemotePCSleepPreventer
- 種類: DWORD
- データ: 1

セッション管理

デフォルトでは、ローカルユーザーがそのマシンで Ctrl+Alt+Del キーを押してセッションを開始すると、リモートユーザーのセッションは自動的に切断されます。自動的に切断されないようにするには、社内 PC に次のレジストリエントリを追加してから、マシンを再起動します。

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA\RemotePC`

- 値の名前: SasNotification
- 種類: DWORD
- データ: 1

デフォルトでは、接続メッセージがタイムアウト期間内に承認されなかった場合にリモートユーザーがローカルユーザーより優先されます。この動作を構成するには、次の設定を使用します:

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA\RemotePC`

- 値の名前: RpcaMode
- 種類: DWORD
- データ:
  - 1 - 指定のタイムアウト期間に Messaging UI へ応答しない場合、リモートユーザーが常に優先されます。この設定が構成されていない場合、この動作がデフォルトです。
  - 2 - ローカルユーザーが優先されます。

リモート PC アクセスモードを強制するまでのタイムアウト期間はデフォルトでは 30 秒です。このタイムアウト期間は変更できますが、30 秒より短く設定しないでください。タイムアウトを構成するには、次のレジストリ設定を使用します:

`HKLM\SOFTWARE\Citrix\PortICA\RemotePC`

- 値の名前: RpcaTimeout
- 種類: DWORD
- データ: 10 進数のタイムアウト値（秒単位）

ユーザーがコンソールに強制的にアクセスできるようにするには: ローカルユーザーが Ctrl+Alt+Del キーを 10 秒以内に 2 回押すことによって、リモートセッションのローカル制御を取得して切断イベントを強制的に発生します。

レジストリを変更してマシンを再起動した後に、リモートユーザーが使用中の PC にローカルユーザーが Ctrl+Alt+Del キーを押してログオンすると、プロンプトがリモートユーザーに表示されます。このプロンプトは、ローカルユーザーの接続を許可するか拒否するかを尋ねます。接続を許可すると、リモートユーザーのセッションは切断されます。

セッション管理ログ

リモート PC アクセスにログ機能（アクティブな ICA セッションで誰かが PC にアクセスしようとしたときにログに記録する機能）が追加されました。この機能により、ご使用の環境で不要なアクティビティまたは予期しないアクティビティがないかどうかを監視し、インシデントを調査する必要がある場合にそうしたイベントを監査できます。

イベントは、Windows イベントビューアーでログに記録され、［アプリケーションとサービス］**>**［**Citrix**］**>**［**HostCore**］**>**［**ICA Service**］**>**［**Admin**］で確認できます。

リモート PC アクセスを使用するときにログに記録される 3 つの異なるイベントがあります。

Ctrl+Alt+Del イベント

このイベントは、ローカルユーザーがアクティブなリモートセッションにおいてコンソールキーボードで Ctrl+Alt+Del キーを押すと表示されます。

イベントの詳細

- ログの名前：アプリケーションとサービス
- イベント ID：43、44、45
- ソース：ICA Service

イベント **ID 43**　このイベント ID は、SasNotification レジストリ値が存在しない場合、または SasNotification レジストリ値が 0 の場合に表示されます。

- メッセージ：

```
Ctrl+Alt+Del has been pressed on the endpoint.
The session management behavior is set to automatically
    disconnect the remote session.
```

イベント **ID 44**　このイベント ID は、SasNotification レジストリ値が 1 で RpcaMode レジストリ値が 1 の場合、または RpcaMode レジストリ値が存在しない場合に表示されます。

- メッセージ：

```
Ctrl+Alt+Del has been pressed on the endpoint.
The session management behavior is set to notify the
    remote user. The user preference is set to remote user
    .
```

イベント **ID 45**　このイベント ID は、SasNotification レジストリ値が 1 で RpcaMode レジストリ値が 2 の場合に表示されます。

- メッセージ：

```
Ctrl+Alt+Del has been pressed on the endpoint.
The session management behavior is set to notify the
    remote user.
The user preference is set to local user.
```

リモートセッション切断イベント

このイベントは、さまざまな理由でリモートセッションが切断された場合に表示されます。

イベントの詳細

- ログの名前：アプリケーションとサービス
- イベント ID：46、47、48
- ソース：ICA Service

イベント **ID 46**　このイベント ID は、リモートセッションが切断されたとき、SasNotification レジストリ値が存在しない場合、または SasNotification レジストリ値が 0 の場合に表示されます。

- メッセージ:

```
The remote session for <remoteUserName> has been
    disconnected.
```

イベント **ID 47**　このイベント ID は、リモートユーザーがセッションの切断に同意したとき、SasNotification レジストリ値が 1 で RpcaMode レジストリ値が 1 の場合、または RpcaMode レジストリ値が 2 または存在しない場合に表示されます。

- メッセージ:

```
The remote session for <remoteUserName> has been
    disconnected because the user accepted the request to
    disconnect the session.
```

イベント **ID 48**　このイベント ID は、リモートユーザーが特定のタイムアウト期間内に切断要求を拒否しなかったとき、SasNotification レジストリ値が 1 で RpcaMode レジストリ値が 2 の場合に表示されます。

- メッセージ:

```
The remote session for <remoteUserName> has been
    disconnected because the user did not decline the
    disconnection request within the configured timeout
    period (<timeout period>).
```

Ctrl+Alt+Del が **2** 回押されたイベント　このイベントは、Ctrl+Alt+Del キーが 10 秒以内に 2 回押されたときに表示されます。

イベントの詳細

- ログの名前：アプリケーションとサービス
- イベント ID：49
- ソース：ICA Service

イベント **ID 49**　このイベント ID は、Ctrl+Alt+Del キーが 10 秒以内に 2 回押されたときに表示されます。

- メッセージ:

```
The remote session for <remoteUserName> has been forcibly
    disconnected.
```


Wake-on-LAN

リモート PC アクセスでは Wake on LAN がサポートされ、物理 PC をリモートから起動できます。この機能により、ユーザーが退社時に PC の電源をオフにできるようになるため、消費電力を節約できます。また、電源が突然オフになった PC にもリモートアクセスできるようになります。

Wake on LAN 機能を使用すると、Delivery Controller の指示に従って、PC 上で実行中の VDA から PC が存在するサブネットにマジックパケットが直接送信されます。これによって、マジックパケットを配信するために追加のインフラストラクチャコンポーネントまたはサードパーティ製ソリューションに依存する必要がなくなります。

Wake on LAN 機能は、従来の SCCM ベースの Wake on LAN 機能とは異なります。SCCM ベースの Wake on LAN については、「Wake on LAN –SCCM 統合」を参照してください。

システム要件

以下は、Wake on LAN 機能を使用するためのシステム要件です:

- コントロールプレーン:
  - Citrix DaaS
  - Citrix Virtual Apps and Desktops 2009 以降
- 物理 PC:
  - VDA バージョン 2009 以降
  - Windows10 または Windows11。サポートの詳細については、「VDA のシステム要件」を参照してください。
  - BIOS/UEFI で Wake on LAN が有効になっている
  - Windows 構成内のネットワークアダプターのプロパティで Wake on LAN が有効になっている

Wake on LAN の構成

オンプレミスで Citrix Virtual Apps and Desktops を使用している場合、統合された Wake on LAN の構成は PowerShell を使用した場合のみサポートされます。

Wake on LAN を構成するには:

1. リモート PC アクセスマシンカタログをまだ作成していない場合は作成します。
2. Wake on LAN ホスト接続をまだ作成していない場合は作成します。

> 注:
>
> Wake on LAN 機能を使用するには、「Microsoft Configuration Manager Wake on LAN」タイプのホスト接続がある場合は、新しいホスト接続を作成します。

3. Wake on LAN ホスト接続の一意の識別子を取得します。
4. Wake onLAN ホスト接続をマシンカタログに関連付けます。

Wake on LAN ホスト接続を作成するには:

```
# Load Citrix SnapIns
Add-PSSnapIn -Name "*citrix*"

# Provide the name of the Wake on LAN host connection
[string]$connectionName = "Remote PC Access Wake on LAN"

# Create the hypervisor connection
$hypHc = New-Item -Path xdhyp:\Connections `
                -Name $connectionName `
                -HypervisorAddress "N/A" `
                -UserName "woluser" `
                -Password "wolpwd" `
                -ConnectionType Custom `
                -PluginId VdaWOLMachineManagerFactory `
                -CustomProperties "<CustomProperties></CustomProperties
                   >" `
                -Persist

$bhc = New-BrokerHypervisorConnection -HypHypervisorConnectionUid
   $hypHc.HypervisorConnectionUid

# Wait for the connection to be ready before trying to use it
while (-not $bhc.IsReady)
{

    Start-Sleep -s 5
    $bhc = Get-BrokerHypervisorConnection -HypHypervisorConnectionUid
       $hypHc.HypervisorConnectionUid
 }
```

ホスト接続の準備ができたら、次のコマンドを実行して、ホスト接続の一意の識別子を取得します:

```
$bhc = Get-BrokerHypervisorConnection -Name "<WoL Connection Name>"
$hypUid = $bhc.Uid
```

接続の一意の識別子を取得したら、次のコマンドを実行して、その接続をリモート PC アクセスマシンカタログに関連付けます:

```
Get-BrokerCatalog -Name "<Catalog Name>" | Set-BrokerCatalog -
   RemotePCHypervisorConnectionUid $hypUid
```

設計上の考慮事項

リモート PC アクセスで Wakeon LAN を使用する場合は、次の点を考慮してください:

- 複数のマシンカタログでは同じ Wake on LAN ホスト接続を使用できます。
- PC が別の PC をウェイクアップするには、両方の PC が同じサブネット内にあり、同じ Wake on LAN ホスト接続を使用する必要があります。PC が同じマシンカタログにあるか、別のマシンカタログにあるかは関係ありません。
- ホスト接続は特定のゾーンに割り当てられます。環境に複数のゾーンがある場合は、各ゾーンに Wake on LAN ホスト接続が必要です。同じことがマシンカタログにも当てはまります。
- マジックパケットは、グローバルブロードキャストアドレス 255.255.255.255 を使用してブロードキャスト配信されます。このアドレスがブロックされていないことを確認してください。
- そのサブネット内のマシンをウェイクアップできるようにするには、サブネット内で（Wake on LAN 接続ごとに）少なくとも 1 台の PC がオンになっている必要があります。

運用上の考慮事項

以下は、Wake on LAN 機能を使用する場合の考慮事項です：

- 統合された Wake on LAN 機能を使用して PC をウェイクアップするには、VDA を少なくとも 1 回登録する必要があります。
- Wake on LAN は、PC のウェイクアップにのみ使用できます。再起動やシャットダウンなど、他の電源操作はサポートしていません。
- Wake on LAN 接続が作成されると、Web Studio に表示されます。ただし、オンプレミスで Citrix Virtual Apps and Desktops を使用している場合、Web Studio 内でのプロパティの編集はサポートされません。
- マジックパケットは、次の 2 つの方法のいずれかで送信されます：

  1. ユーザーが PC へのセッションを開始しようとしたときに、VDA が登録解除されている場合
  2. 管理者が Web Studio または PowerShell から電源オンのコマンドを手動で送信する場合

- Delivery Controller は PC の電源の状態を認識しないため、Web Studio では電源の状態のところに ［サポートされていません］と表示されます。Delivery Controller は、VDA 登録状態を使用して PC がオンかオフかを判断します。

Wake on LAN –SCCM 統合

SCCM 統合 Wake on LAN は、リモート PC アクセスの代替 Wake on LAN オプションであり、オンプレミスの Citrix Virtual Apps and Desktops でのみ使用できます。

システム要件

以下は、SCCM 統合 Wake on LAN 機能を使用するためのシステム要件です：

- Citrix Virtual Apps and Desktops 1912 以降
- 物理 PC：

  - VDA バージョン 1912 以降
  - Windows 10。サポートの詳細については、「VDA のシステム要件」を参照してください。
  - BIOS/UEFI で Wake on LAN が有効になっている
  - Windows 構成内のネットワークアダプターのプロパティで Wake on LAN が有効になっている

- System Center Configuration Manager（SCCM）2012 R2 以降

SCCM 統合 Wake on LAN の構成

次の前提条件を満たす必要があります:

1. 組織内で SCCM 2012 R2、2016、または 2019 を構成します。リモート PC アクセス用のすべてのマシンに SCCM クライアントを展開し、スケジュールされている SCCM インベントリサイクルが実行されるのを待ちます。または必要に応じて、手動で強制的に実行することもできます。
2. ウェイクアッププロキシの場合は、SCCM でウェイクアッププロキシを有効にします。リモート PC アクセスの Wake on LAN 機能を使用する PC が属する各サブネットで、センチネルマシンとして動作可能なマシンが 3 台以上あることを確認します。
3. マジックパケットの場合は、サブネット宛てのブロードキャストまたはユニキャストを使用して、ネットワーク経路およびファイアウォールでパケットの転送がブロックされないようにします。
4. 各 PC の BIOS/UEFI 設定で、Wake on LAN 機能を有効にします。
5. まだ実行していない場合は、VDA を物理 PC に展開します。

前提条件を満たした後、次の手順を実行して Delivery Controller が SCCM と通信できるようにします:

1. SCCM のホスト接続を作成します。詳しくは、「接続およびリソース」を参照してください。
   - **Microsoft Configuration Manager Wake on LAN** を接続の種類として選択します。
   - 入力された資格情報は、スコープのコレクションにアクセス可能で、リモートツールオペレーターの役割が割り当てられている必要があります。
2. Web Studio で接続を選択して、［接続の編集］を選択し、［詳細設定］をクリックします。
3. Wake on LAN を処理するための適切なオプションを選択します:
   - ウェイクアッププロキシを使用している場合は、最初のオプションを選択します: **Microsoft System Center Configuration Manager** のウェイクアッププロキシ。
   - マジックパケットを使用している場合は、2 番目のオプションを選択します: **Delivery Controller** が送信する **Wake On LAN** パケット。
     - 適切な送信方法を選択します: サブネット向けのブロードキャスト または ユニキャスト。

ホスト接続を作成後、接続をリモート PC アクセスカタログに関連付けます:

- 新しいリモート PC アクセスカタログを作成する場合は、カタログ作成ウィザードの ［オペレーティングシステム］ページで、カタログの種類として ［リモート **PC** アクセス］を選択し、ドロップダウンリストから適切な接続を選択します。

- Wake on LAN を既存のリモート PC アクセスカタログに追加するには、次の手順を実行します:

  1. Web Studio の ［マシンカタログ］ノードに移動し、マシンカタログを選択して ［マシンカタログの編集］を選択します。
  2. ［電源管理］タブを選択し、［はい］を選択してマシンカタログの電源管理を有効にします。
  3. ボックスの一覧から適切な接続を選択して ［**OK**］をクリックします。

トラブルシューティング

モニターのブランキングが機能しない

アクティブな HDX セッションがあるときに Windows PC のローカルモニターが空白になっていない場合（ローカルモニターはセッションで発生していることを表示します）、GPU ベンダーのドライバーに問題があることが原因である可能性があります。この問題を解決するには、次のレジストリ値を設定して、Citrix Indirect Display ドライバー（IDD）にグラフィックカードのベンダードライバーよりも高い優先度を与えます:

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics\AdapterMerits`

- 名前: CitrixIDD
- 種類: DWORD
- データ: 3

ディスプレイアダプターの優先度とモニターの作成について詳しくは、Knowledge Center のCTX237608を参照してください。

セッション管理通知が有効になっているマシンで **Ctrl+Alt+Del** を選択すると、セッションが切断される

レジストリ値 **SasNotification** によって制御されるセッション管理通知は、VDA でリモート PC アクセスモードが有効になっている場合にのみ機能します。物理 PC で Hyper-V の役割または仮想化ベースのセキュリティ機能が有効になっている場合、PC は仮想マシンとして報告します。VDA が仮想マシン上で実行されていることを検出すると、リモート PC アクセスモードが自動的に無効になります。リモート PC アクセスモードを有効にするには、次のレジストリ値を追加します:

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`

- 名前: ForceEnableRemotePC
- 種類: DWORD
- データ: 1

設定を有効にするには、PC を再起動します。

診断情報

リモート PC アクセスの診断情報は、Windows のアプリケーションイベントログに書き込まれます。情報メッセージは調整されません。エラーメッセージは重複メッセージの破棄により調整されます。

- 3300（情報）：マシンカタログへのマシンの追加
- 3301（情報）：デリバリーグループへのマシンの追加
- 3302（情報）：ユーザーへのマシンの割り当て
- 3303（エラー）：例外の発生

電源管理

リモート PC アクセス用の電源管理を有効にすると、サブネット向けのブロードキャストでのマシンの起動に失敗することがあります。この問題は、Controller とマシンが異なるサブネット上に存在する場合に発生します。AMT がサポートされない場合に異なるサブネット間でサブネット向けのブロードキャストを使用するには、ウェイクアッププロキシまたはユニキャストを使用してください。これらの詳細設定は、電源管理接続のプロパティで有効にできます。

アクティブなリモートセッションは、ローカルのタッチスクリーン入力を記録します

VDA でリモート PC アクセスモードを有効にすると、アクティブなセッション中にローカルタッチスクリーン入力が無視されます。物理 PC で Hyper-V の役割または仮想化ベースのセキュリティ機能が有効になっている場合、PC は仮想マシンとして報告します。VDA が仮想マシン上で実行されていることを検出すると、リモート PC アクセスモードが自動的に無効になります。リモート PC アクセスモードを有効にするには、次のレジストリ設定を追加します：

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`

- 名前：ForceEnableRemotePC
- 種類：DWORD
- データ：1

設定を有効にするには、PC を再起動します。

その他のリソース

リモート PC アクセスのその他のリソースは次のとおりです：

- ソリューション設計ガイダンス：「リモート PC アクセス設計の決定」。
- リモート PC アクセスアーキテクチャの例：「Citrix のリモート PC アクセスソリューションのリファレンスアーキテクチャ」。

コンテンツの公開

August 17, 2024

> 注:
>
> Web Studio（Web ベース）と Citrix Studio（Windows ベース）の 2 つの管理コンソールを使用して、Citrix Virtual Apps and Desktops の展開を管理できます。この記事では Web Studio のみを扱います。Citrix Studio について詳しくは、Citrix Virtual Apps and Desktops 7 2212 以前の同様の記事を参照してください。

Microsoft Word ドキュメントや Web リンクなどのリソースへの URL または UNC パスを、アプリケーションとして公開できます。この機能は、コンテンツの公開と呼ばれています。コンテンツの公開機能を使用することで、ユーザーへのコンテンツの配信をより柔軟に行うことができるようになります。既存のアプリケーションのアクセス制御と管理機能を使用できるというメリットもあります。コンテンツを開くのにローカルアプリケーションと公開アプリケーションのどちらを使用するかも指定できます。

公開したコンテンツは、ほかのアプリケーションと同様に StoreFront および Citrix Workspace アプリに表示されます。ユーザーは、アプリケーションと同じようにこれらのコンテンツにアクセスできます。クライアントでは、リソースは通常どおりに開かれます。

- ローカルにインストールされているアプリケーションが適している場合は、こうしたアプリケーションが起動されリソースが開かれます。
- ファイルタイプの関連付けが定義されている場合は、公開アプリケーションが起動されリソースが開かれます。

コンテンツの公開には PowerShell SDK を使用します。Web Studio を使用してコンテンツを公開することはできませんが、アプリケーションの公開後に Web Studio を使用してそのプロパティを編集することはできます。

構成の概要と準備

コンテンツの公開では、`New-BrokerApplication`コマンドレットに以下のキープロパティを指定して使用します（すべてのコマンドレットプロパティの説明についてはこのコマンドレットのヘルプを参照してください）。

```
1 New-BrokerApplication -ApplicationType PublishedContent -
      CommandLineExecutable location -Name app-name -DesktopGroup delivery
      -group-name
```

`ApplicationType`プロパティは`PublishedContent`にする必要があります。

`CommandLineExecutable`プロパティで、公開コンテンツの場所を指定します。以下の形式を使用でき、最大文字数は 255 文字です。

- HTML Web サイトアドレス（例：http://www.citrix.com）

- Web サーバー上のドキュメントファイル（例: https://www.citrix.com/press/pressrelease.doc）
- FTP サーバー上のディレクトリ（例: ftp://ftp.citrix.com/code）
- FTP サーバー上のドキュメントファイル（例: ftp://ftp.citrix.com/code/Readme.txt>）
- UNC ディレクトリパス（たとえば、file://myServer/myShare or \\\\\myServer\\myShare）
- UNC ファイルパス（たとえば、file://myServer/myShare/myFile.asfまたは\\myServer\myShare\myFile.asf）

適切な SDK があることを確認します。

- 展開環境が Citrix DaaS（旧称 Citrix Virtual Apps and Desktops サービス）の場合は、Citrix Virtual Apps and Desktops のリモート PowerShell SDK をダウンロードして、インストールします。
- 展開環境がオンプレミスの Citrix Virtual Apps and Desktops の場合は、Delivery Controller とともにインストールされている PowerShell SDK を使用します。公開コンテンツアプリケーションの追加には Delivery Controller のバージョン 7.11 以上が必要です。

以下の手順ではサンプルを利用しています。このサンプルの詳細は次のとおりです。

- マシンカタログを作成しています。
- PublishedContentAppsという名前のデリバリーグループを作成しています。このデリバリーグループでは、カタログのマルチセッション OS マシンを使用しています。このデリバリーグループには、ワードパッドアプリケーションが追加されています。
- デリバリーグループ名、CommandLineExecutableの場所、およびアプリケーション名用の変数を作成しています。

開始

PowerShell SDK をインストール済みのマシンで PowerShell を開きます。

次のコマンドレットにより、適切な PowerShell スナップインを追加し、返されたデリバリーグループレコードを変数に代入します。

```
Add-PsSnapin Citrix\* $dg = Get-BrokerDesktopGroup -Name PublishedContentApps
```

Citrix DaaS を使用している場合は、Citrix Cloud 資格情報を入力して認証を行います。ユーザーが複数存在する場合は 1 人を選択します。

URL の公開

次のコマンドレットでは、場所とアプリケーション名を変数に代入してから Citrix ホームページをアプリケーションとして公開します。


```
$citrixUrl = "https://www.citrix.com/"
$appName = "Citrix Home Page"

New-BrokerApplication -ApplicationType PublishedContent -
    CommandLineExecutable $citrixURL -Name $appName -DesktopGroup $dg.
    Uid
```

次の手順を実行して、成功したことを確認します:

- StoreFront を開き、PublishedContentApps デリバリーグループのアプリケーションにアクセスできるユーザーとしてログオンします。新しく作成したアプリケーションが、デフォルトのアイコンで表示されます。アイコンのカスタマイズ方法については、https://www.citrix.com/blogs/2013/08/21/xd-tipster-changing-delivery-group-icons-revisited-xd7/を参照してください。
- **Citrix Home Page** アプリケーションをクリックします。ローカルで実行されているデフォルトブラウザーのインスタンスの新しいタブで、指定した URL が開かれます。

UNC パスに配置されているリソースの公開

この例では、管理者が共有名PublishedResourcesを既に作成しています。次のコマンドレットで、場所とアプリケーション名を変数に代入してから、この共有に含まれる RTF ファイルと DOCX ファイルをリソースとして公開します。

```
$rtfUNC = "\GMSXJ-EDGE0.xd.local\PublishedResources\PublishedRTF.rtf"
$rtfAppName = "PublishedRTF"

New-BrokerApplication -ApplicationType PublishedContent
 -CommandLineExecutable $rtfUNC -Name $rtfAppName
-DesktopGroup $dg.Uid

$docxUNC = "\GMSXJ-EDGE0.xd.local\PublishedResources\PublishedDOCX.docx
    "
$docxAppName = "PublishedDOCX"

New-BrokerApplication -ApplicationType PublishedContent
 -CommandLineExecutable $docxUNC -Name $docxAppName
-DesktopGroup $dg.Uid
```

次の手順を実行して、成功したことを確認します:

- StoreFront ウィンドウを更新して、新しく公開したドキュメントが表示されることを確認します。
- **PublishedRTF** アプリケーションおよび **PublishedDOCX** アプリケーションをクリックします。各ドキュメントが、ローカルで実行されるワードパッドで開きます。

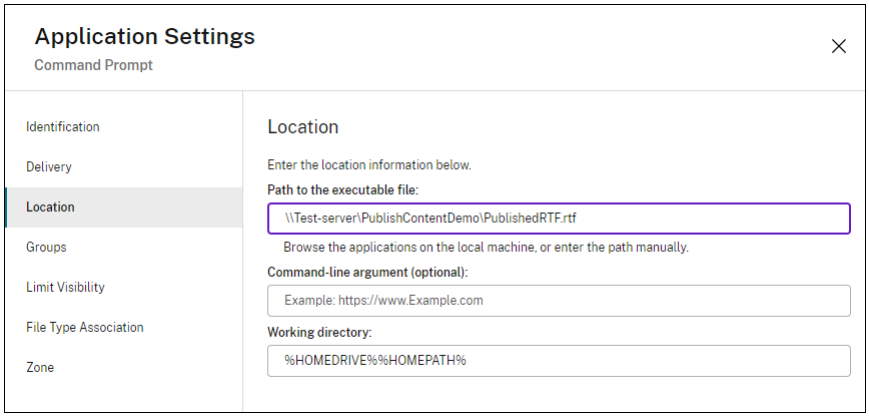
PublishedContent アプリケーションの確認と編集

公開コンテンツは、他の種類のアプリケーションと同じ方法で管理できます。

PublishedContentアプリケーションを表示および編集するには、次の手順に従います:

1. Web Studio にサインインし、左側のペインで ［アプリケーション］をクリックします。
2. ［アプリケーション］タブで PublishedContent アプリケーションを選択し、［プロパティ］を選択します。

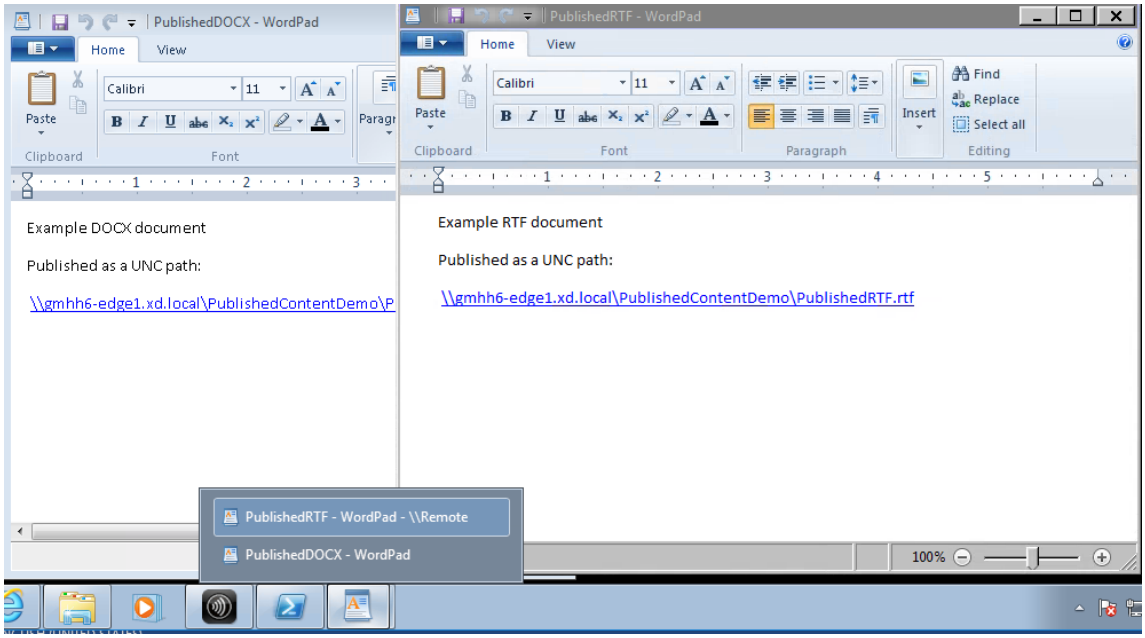
   公開コンテンツには、アプリケーションのプロパティ（表示できるユーザー、グループ割り当て、ショートカットなど）が適用されます。ただし、［場所］ページでコマンドライン引数や作業ディレクトリプロパティを変更することはできません。
3. リソースを変更するには、［場所］ページの ［実行可能ファイルのパス］を変更します。



4. 公開アプリケーションを使用してPublishedContentアプリケーション（ローカルアプリケーションではなく）を開くには、次の手順に従います:

   この例では、公開済みのワードパッドアプリケーションを編集して、.rtf ファイルに対するファイルタイプの関連付けを作成しています。

   a) デリバリーグループのメンテナンスモードを有効にします。
   b) ファイルタイプの関連付けプロパティを編集します。
   c) 完了したら、メンテナンスモードを無効にします。
   d) StoreFront を更新してファイルタイプの関連付けに対する変更を反映させ、**PublishedRTF** アプリケーションおよび **PublishedDOCX** アプリケーションをクリックします。違いに注目してください。**PublishedDOCX** は以前と同様にローカルのワードパッドで開かれますが、**PublishedRTF** は、ファイルタイプの関連付けにより公開済みのワードパッドアプリケーションで開かれるようになりました。



詳細情報

- マシンカタログの作成
- デリバリーグループの作成
- アプリケーションプロパティの変更

サーバー VDI

August 17, 2024

サーバー VDI（Virtual Desktop Infrastructure）機能を使用すると、サーバーオペレーティングシステムからユーザーにデスクトップを配信できます。

- エンタープライズ管理者は、エンジニアやデザイナーなどのユーザーにサーバーオペレーティングシステムを VDI デスクトップとして配信できます。
- サービスプロバイダーは、デスクトップをクラウドから提供できます。これらのデスクトップは、Microsoft Services Provider License Agreement（SPLA）に準拠します。

サポート：

- Citrix Virtual Apps and Desktops および Citrix DaaS（旧称 Citrix Virtual Apps and Desktops サービス）の展開では、Windows Server 2022、Windows Server 2019、Windows Server 2016 で、サーバー VDI がサポートされています。

- すべての Server VDI 展開では、ユーザー個人設定レイヤーテクノロジがサポートされています。
- スキャナのような TWAIN デバイスと連携するサーバー VDI には、Windows Server のデスクトップエクスペリエンス機能をインストールする必要があります。
- サーバー VDI では、次の機能を使用できません:
  - ホストされるアプリケーション
  - ローカルアプリアクセス
  - 直接（非仲介）デスクトップ接続
  - リモート PC アクセス

サーバー **VDI** のインストールと構成

1. Windows サーバーでのインストールの準備
   - Windows サーバーマネージャーを使って、リモートデスクトップサービスの役割サービスがインストールされていないことを確認します。既にインストールされている場合は、それを削除します。これらの役割サービスがインストールされていると、VDA のインストールに失敗します。
   - [**1** ユーザーにつき **1** セッションに制限する] プロパティが有効であることを確認します。Windows サーバー上で、ターミナルサーバー設定のレジストリを編集します:

     ```
     HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server
     ```

     ```
     DWORD fSingleSessionPerUser = 1
     ```

2. Citrix Virtual Apps and Desktops インストーラーのコマンドラインインターフェイスで、「`/quiet`」および「`/servervdi`」オプションを指定して、VDA をサポート対象のサーバーまたはサーバーマスターイメージ上にインストールします。（デフォルトでインストーラーのグラフィカルユーザーインターフェイスでは、サーバーオペレーティングシステム上の Windows シングルセッション OS 対応 VDA はブロックされます。コマンドラインを使用すると、この動作が無効になります）。次のいずれかのコマンドを使用します:
   - Citrix Virtual Apps and Desktops 環境の場合:
     - `XenDesktopVdaSetup.exe /quiet /servervdi`
     - `VDAWorkstationSetup.exe /quiet /servervdi`
   - Citrix DaaS 展開:
     - `VDAWorkstationSetup.exe /quiet /servervdi`

   その他のオプション:
   - 「`/controllers`」を使用して、Delivery Controller または Cloud Connector を指定します。
   - ファイアウォールが手動で構成されていない限りは、「`/enable_hdx_ports`」を使用してファイアウォールのポートを開いてください。

- イメージに VDA をインストールしており、MCS を使用してそのイメージからサーバー仮想マシンを作成する場合は、/`mastermcsimage`（または/`masterimage`）を使用します。
- 全オプションについて詳しくは、「コマンドラインを使用したインストール」を参照してください。

3. サーバー VDI のマシンカタログを作成します。カタログ作成ウィザードで次の操作を行います：

   - ［オペレーティングシステム］ページで、［シングルセッション **OS**］を選択します。
   - ［概要］ページで、管理者がサーバー VDI 用のマシンカタログを識別できるようにマシンカタログ名と説明を指定します。これは、Studio においてそのマシンカタログがサーバー VDI 用であることを示す唯一のインジケーターになります。

   VDA はマルチセッションマシン上にインストールされていますが、Studio で検索すると、このサーバー VDI カタログは ［シングルセッション**OS** マシン］タブに表示されます。

4. デリバリーグループを作成し、作成したサーバー VDI カタログを選択します。

VDA のインストール中に Delivery Controller または Cloud Connector を指定しなかった場合、必ずあとから指定します。詳しくは、「VDA 登録」を参照してください。

ユーザー個人設定レイヤー

August 17, 2024

> 注：
>
> Web Studio（Web ベース）と Citrix Studio（Windows ベース）の 2 つの管理コンソールを使用して、Citrix Virtual Apps and Desktops の展開を管理できます。この記事では Web Studio のみを扱います。Citrix Studio について詳しくは、Citrix Virtual Apps and Desktops 7 2212 以前の同様の記事を参照してください。

Citrix Virtual Apps and Desktops のユーザー個人設定レイヤー機能は、非永続マシンカタログの機能を拡張し、セッション間でユーザーのデータとローカルにインストールされたアプリケーションを保持します。基盤となる Citrix App Layering テクノロジを活用して、ユーザー個人設定レイヤー機能は、永続的ではないマシンカタログの Citrix Provisioning と Machine Creation Services（MCS）をサポートします。

このユーザー個人設定レイヤーコンポーネントを、マスターイメージ内の Virtual Delivery Agent と一緒にインストールします。VHD ファイルには、ユーザーがインストールしたアプリケーションがローカルに格納されます。イメージにマウントされている VHD は、ユーザー独自の仮想ハードドライブとして機能します。

> 重要：
>
> Citrix Virtual Apps and Desktops にユーザー個人設定レイヤーを展開するか、イメージテンプレートで有

> 効な App Layering ユーザーレイヤーを展開することができます。両方ではありません。App Layering 内のレイヤーにユーザー個人設定レイヤー機能をインストールしないでください。

これは、Personal vDisk（PvD）に代わる機能で、プールされた非永続的なデスクトップ環境のユーザーに、永続的なワークスペース環境を提供します。

ユーザー個人設定レイヤー機能を展開するには、この記事で説明されている手順を使用してユーザー個人設定レイヤー機能をインストールして構成します。

アプリケーションサポート

次の例外を除き、ユーザーがローカルでデスクトップにインストールするすべてのアプリケーションは、ユーザー個人設定レイヤーでサポートされます。

例外

次のアプリケーションは例外であり、ユーザー個人設定レイヤーでサポートされません：

- MS Office や Visual Studio などのエンタープライズアプリケーション。
- ネットワークスタックまたはハードウェアを変更するアプリケーション。例：VPN クライアント。
- ブートレベルのドライバーを備えたアプリケーション。例：ウイルススキャナー。
- ドライバーストアを使用するドライバーを備えたアプリケーション。例：プリンタードライバー。

  > 注：
  >
  > Windows グループポリシーオブジェクト（GPO）を使用して、プリンターを使用可能にすることができます。

ユーザーがサポートされていないアプリケーションをローカルでインストールできないようにしてください。このようなアプリケーションは、マスターイメージに直接インストールします。

ローカルユーザーまたは管理者アカウントを必要とするアプリケーション

ユーザーがアプリケーションをローカルにインストールすると、そのアプリケーションはユーザーレイヤーに入ります。その後、ユーザーがローカルユーザーやローカルグループを追加または編集した場合、その変更はセッションを超えて保持されません。

> 重要：
>
> 必要なローカルユーザーまたはグループをマスターイメージに追加します。

要件

ユーザー個人設定レイヤー機能には、次のコンポーネントが必要です:

- Citrix Virtual Apps and Desktops 7 1909 以降
- Virtual Delivery Agent（VDA）、バージョン 1912 以降
- Citrix Provisioning バージョン 1909 以降
- Windows ファイル共有（SMB）、またはオンプレミス AD 認証が有効な Azure ファイル

OS がシングルセッションとして展開されている場合、次の Windows バージョンにユーザー個人設定レイヤー機能を展開できます。サポートは、1 セッションの 1 ユーザーに制限されています。

- Windows 11 Enterprise x64
- Windows 10 Enterprise x64 バージョン 1607 以降
- Windows Server 2019（Azure ファイルをサポート）
- Windows Server 2022（Azure ファイルをサポート）

Citrix Virtual Apps and Desktops 7 では、ユーザー個人設定レイヤーを持つ Azure ファイルの使用が、Windows Server 2022、Windows Server 2019、および Windows 10 クライアントでサポートされています。

> 注:
>
> サーバー OS を使用している場合は、サーバー VDI のみがサポートされます。展開について詳しくは、「サーバー VDI」の記事を参照してください。
>
> ユーザー個人設定レイヤーは、マシンごとに一度に 1 人のユーザーのみをサポートします。その後、マシンを再起動してディスクをリセットする必要があります。マルチセッションサーバー OS ではユーザー個人設定レイヤーを使用することはできません。シングルセッションサーバーシステムでのみ使用できます。ユーザー個人設定レイヤーは、非永続デスクトップでのみサポートされます。

ユーザー個人設定レイヤー機能がインストールされている場合は、アンインストールします。最新リリースをインストールする前に、マスターイメージを再起動してください。

ファイル共有の設定

ユーザー個人設定レイヤー機能には、Windows サーバーメッセージブロック（SMB）ストレージが必要です。Windows ファイル共有を作成するには、使用している Windows オペレーティングシステムの通常の手順に従います。

Azure ベースのカタログで Azure ファイルを使用する方法について詳しくは、「ユーザー個人設定レイヤー用の Azure Files ストレージの設定」を参照してください。

推奨事項

ユーザー個人設定レイヤーを展開するには、このセクションの推奨事項に従ってください。

Microsoft System Center Configuration Manager（SCCM）

ユーザー個人設定レイヤー機能を SCCM とともに使用している場合は、VDI 環境でイメージを準備するための Microsoft ガイドラインに従ってください。詳しくは、このMicrosoft TechNet の記事を参照してください。

ユーザーレイヤーサイズ

ユーザーレイヤーは、ディスク上の領域が使用されると拡張するシンプロビジョニングされたディスクです。ユーザーレイヤーのデフォルトのサイズは 10GB で、Citrix で推奨される最小サイズです。

> 注:
>
> インストール時にこの値がゼロ（0）に設定されている場合、デフォルトのユーザーレイヤーサイズは 10GB に設定されます。

ユーザーレイヤーサイズを変更する場合は、［ユーザーレイヤーサイズ］ポリシーに別の値を入力してください。「オプション：ユーザーレイヤーサイズ（**GB**）の横の［選択］をクリックします」の「手順 **5**：デリバリーグループのカスタムポリシーの作成」を参照してください。

ユーザーレイヤーサイズを上書きするためのツール（オプション）

Windows のツールを使用して、ユーザーレイヤーファイル共有のクォータを定義することにより、ユーザーレイヤーサイズを上書きできます。

次の Microsoft クォータツールのいずれかを使用して、**Users** という名前のユーザーレイヤーディレクトリにハードクォータを設定します:

- ファイルサーバーリソースマネージャー（FSRM）
- クォータマネージャー

> 注:
>
> クォータを増やすと、新しいユーザーレイヤーに影響し、既存のユーザーレイヤーが拡張されます。クォータを減らすと、新しいユーザーレイヤーにのみ影響します。既存のユーザーレイヤーのサイズが小さくなることはありません。

ユーザー個人設定レイヤーの展開

ユーザー個人設定機能を展開する場合は、Web Studio 内でポリシーを定義します。次に、この機能が展開されているマシンカタログにバインドされているデリバリーグループにポリシーを割り当てます。

マスターイメージにユーザー個人設定レイヤーを構成しない場合、サービスはアイドル状態のままになり、オーサリングアクティビティに干渉しません。

マスターイメージでポリシーを設定すると、サービスが実行されてユーザーレイヤーをマスターイメージ内にマウントしようとします。この場合、マスターイメージは予期しない動作と不安定性を示します。

ユーザー個人設定レイヤー機能を展開するには、次の手順をこの順序で実行します:

- 手順 1: Citrix Virtual Apps and Desktops 環境の可用性を検証します。
- 手順 2: マスターイメージを準備します。
- 手順 3: マシンカタログを作成します。
- 手順 4: デリバリーグループを作成します。
- 手順 5: デリバリーグループのカスタムポリシーを作成します。

> 注:
>
> イメージで Windows 10 をアップグレードした後に初めてログオンすると、通常よりも時間がかかります。ユーザーのレイヤーを新しいバージョンの Windows 10 に合わせて更新する必要があるため、ログオン時間が長くなります。

手順 **1**: **Citrix Virtual Apps and Desktops** 環境の可用性を検証

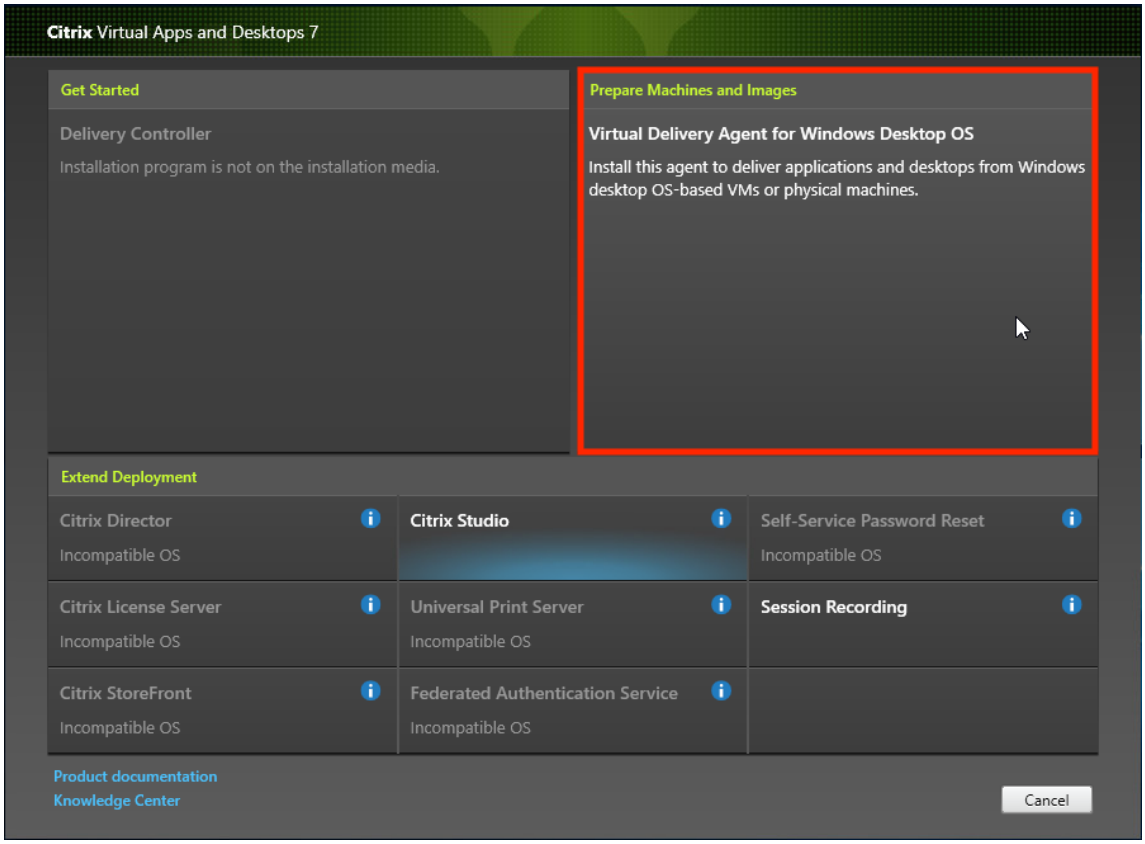
Citrix Virtual Apps and Desktops 環境でこの新機能を使用できることを確認してください。セットアップについて詳しくは、「Citrix Virtual Apps and Desktops のインストールと構成」を参照してください。

手順 **2**: マスターイメージの準備

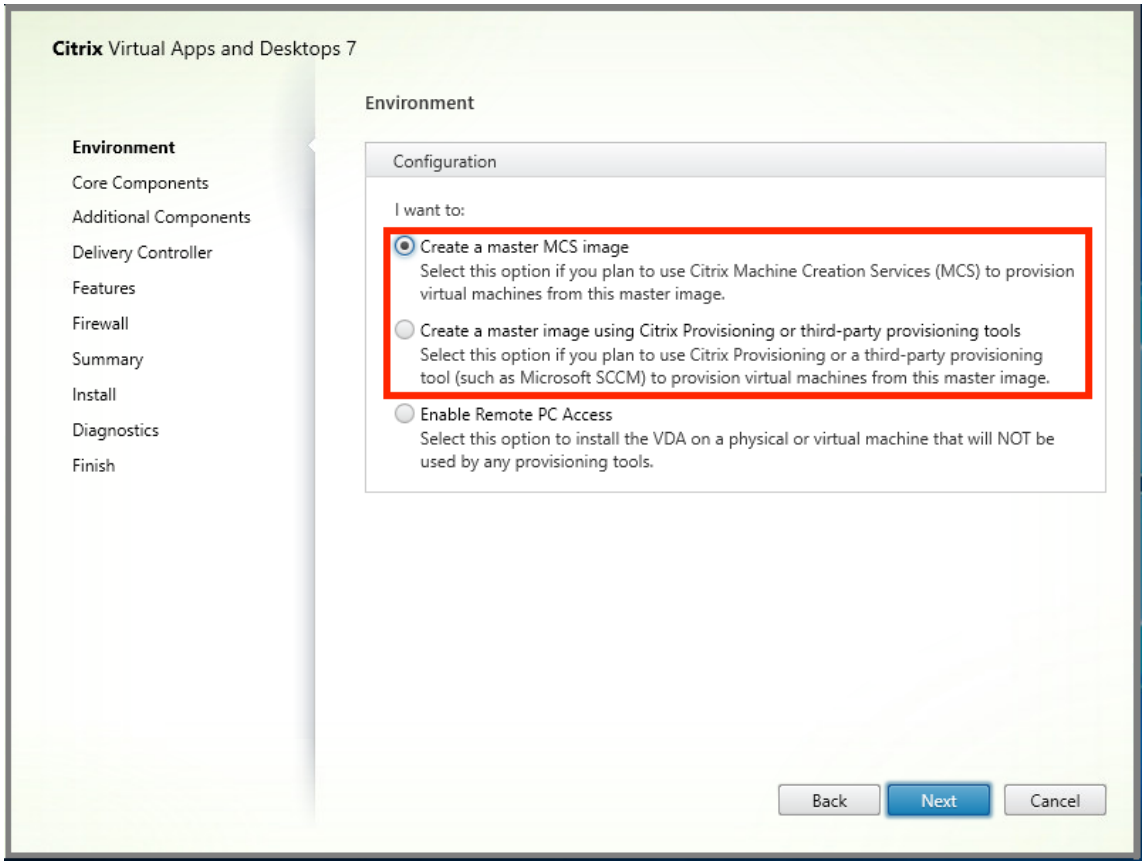
マスターイメージを準備するには:

1. マスターイメージを見つけます。組織のエンタープライズアプリケーションと、一般的にユーザーが有用だと見なすその他のアプリをインストールします。
2. サーバー VDI を展開する場合は、「サーバー VDI」に記載の手順に従ってください。オプションのコンポーネントであるユーザー個人設定レイヤーが含まれていることを確認します。詳しくは、「VDA のインストールで使用するコマンドラインオプション」を参照してください。
3. Windows 10 を使用している場合は、Virtual Delivery Agent（VDA）1912 以降をインストールします。古いバージョンの VDA が既にインストールされている場合は、最初に古いバージョンをアンインストールします。新しいバージョンをインストールするときは、次のようにオプションのコンポーネントである **Citrix** ユーザー個人設定レイヤーを選択してインストールしてください:

    a) [**Virtual Delivery Agent for Windows Desktop OS**] のタイルをクリックします:

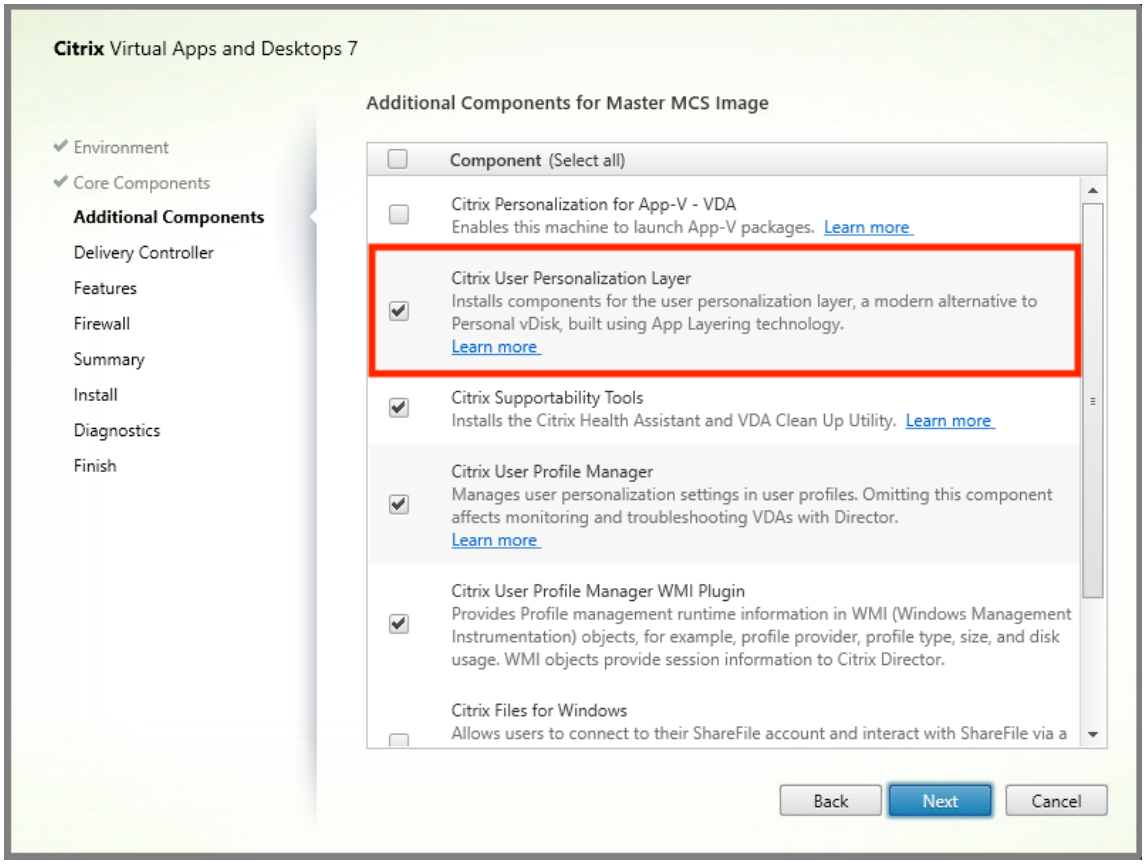


a) 環境：［マスター **MCS** イメージを作成する］か、［**Citrix Provisioning** またはサードパーティのプロビジョニングツールを使用してマスターイメージを作成する］を選択します。



a) コアコンポーネント：［次へ］をクリックします。

b) 追加のコンポーネント：［**Citrix User Personalization Layer**］をオンにします。



a) 残りのインストール画面をクリックして進みながら、必要に応じて VDA を構成し、［インストール］をクリックします。イメージはインストール中に 1 回または複数回再起動します。

4. **Windows** の更新プログラムは無効のままにします。ユーザー個人設定レイヤーインストーラーは、イメージの Windows の更新プログラムを無効にします。更新プログラムを無効のままにします。

イメージを Web Studio にアップロードする準備ができました。

> 注:
>
> ユーザーパーソナライズレイヤー（UPL）をアップグレードしたいだけの場合は、新しいバージョンの UPL とスタンドアロンパッケージを使用してアップグレードできます。VDA をアップグレードする必要はありません。

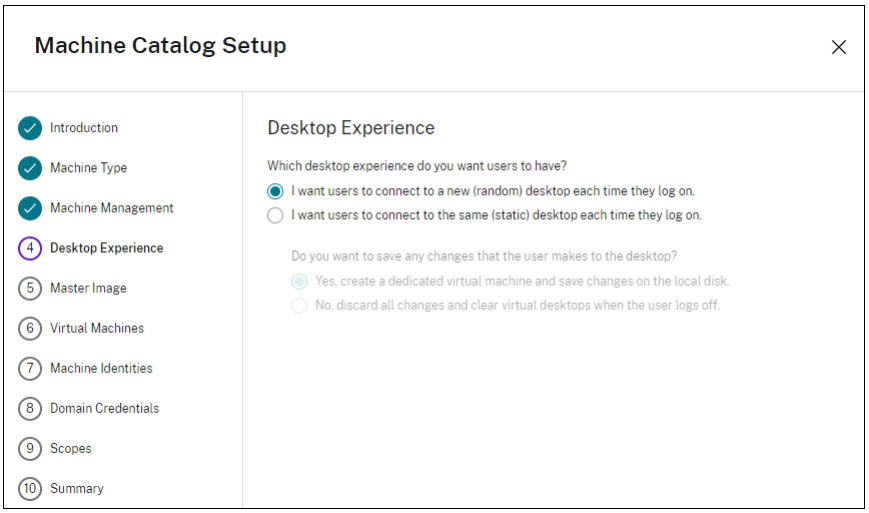
手順 **3**：マシンカタログの作成

Web Studio で、手順に従ってマシンカタログを作成します。カタログの作成時に次のオプションを使用します:

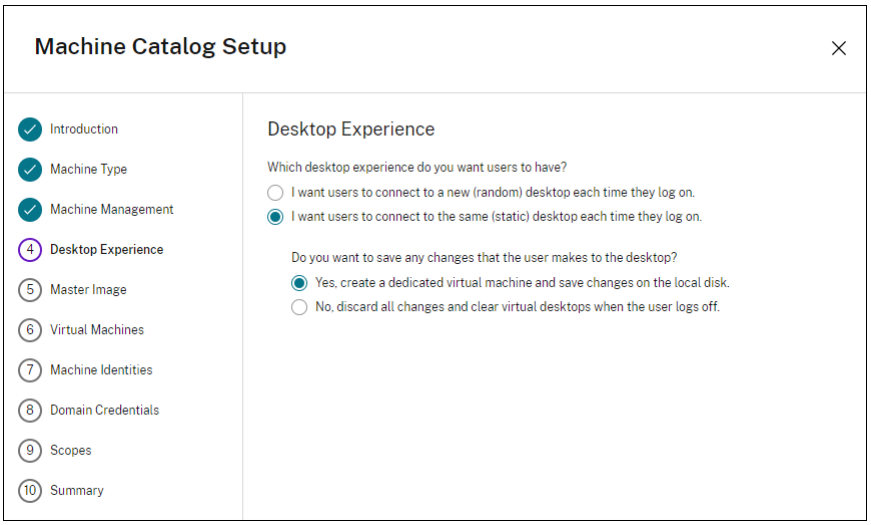
1. ［オペレーティングシステム］を選択して ［シングルセッション **OS**］に設定します。
2. ［マシン管理］を選択して ［電源管理されているマシン］に設定します。たとえば、仮想マシンまたはブレード PC などです。

3. ［デスクトップエクスペリエンス］を選択して、次の例のようにカタログの種類 **Pooled-random** または **Pooled-static** を選択します：

   - **Pooled-random**：



   - **Pooled-static**：Pooled-static を選択する場合、デスクトップを構成して、以下のスクリーンショットのようにユーザーのログオフ時にすべての変更を破棄して仮想デスクトップを消去するようにします：



   > 注：
   >
   > ユーザー個人設定レイヤーは、Citrix Personal vDisk を使用するように構成された、または専用仮想マシンとして割り当てられた Pooled-static カタログをサポートしていません。

4. MCS を使用している場合、イメージと前述のセクションで作成されたイメージのスナップショットを選択します。

5. 環境で必要な場合、残りのカタログプロパティを構成します。

手順 **4**：デリバリーグループの作成

作成したマシンカタログのマシンも含めて、デリバリーグループを作成して構成します。詳しくは、「デリバリーグループの管理」を参照してください。

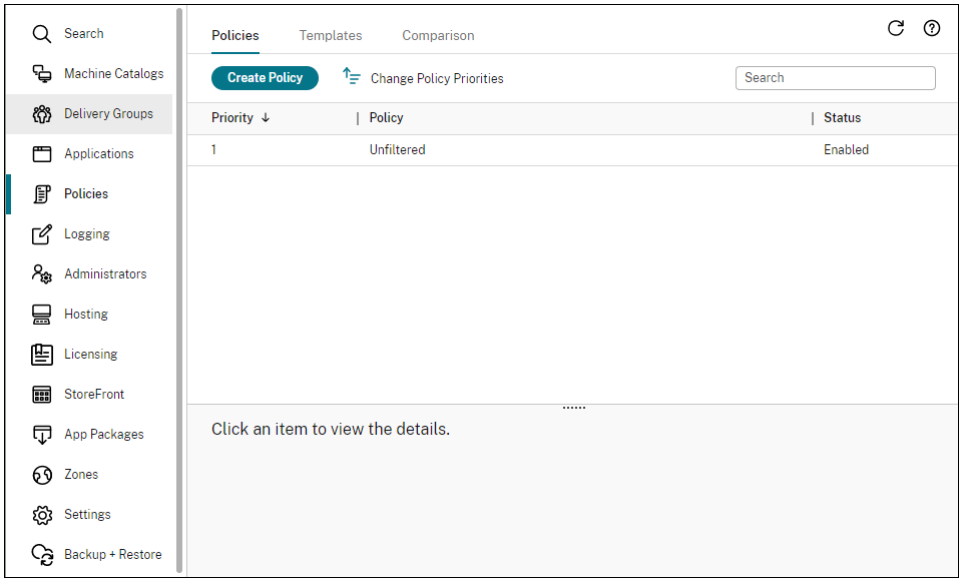
手順 **5:** デリバリーグループのカスタムポリシーの作成

Virtual Delivery Agent 内のユーザーレイヤーのマウントを有効にするには、構成パラメーターを使用して以下を指定します：

- ユーザーレイヤーにアクセスするネットワーク上の場所。
- ユーザーレイヤーディスクの拡大上限。

Web Studio でパラメーターをカスタム Citrix ポリシーとして定義し、デリバリーグループに割り当てる方法を説明します。

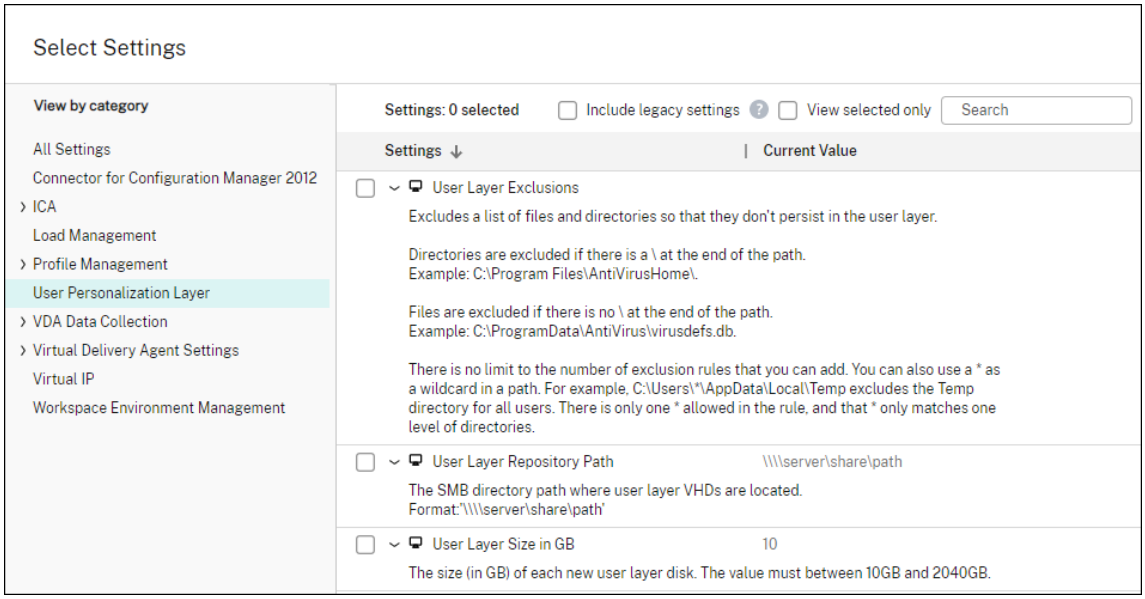
1. Web Studio にサインインし、左側のペインで ［ポリシー］をクリックします：



2. 操作バーの ［ポリシーの作成］を選択します。［ポリシーの作成］ウィンドウが開きます。
3. 検索フィールドに「`user layer`」と入力します。次の 3 つのポリシーが利用可能なポリシーの一覧に表示されます：

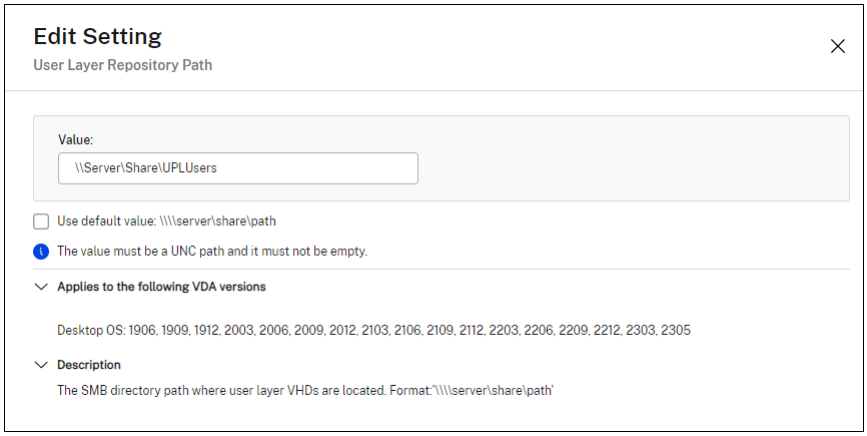
    - ユーザー レイヤーからの除外
    - ユーザーレイヤーリポジトリパス
    - ユーザーレイヤーサイズ（GB）

> 注:
>
> サイズを大きくすると、新しいユーザーレイヤーに影響し、既存のユーザーレイヤーが拡張されます。サイズを小さくすると、新しいユーザーレイヤーにのみ影響します。既存のユーザーレイヤーのサイズが小さくなることはありません。



4. [ユーザーレイヤーリポジトリパス] の横にあるチェックボックスをオンにして、[編集] をクリックします。[設定の変更] ウィンドウが開きます。
5. [値] フィールドに次の形式でパスを入力し、[保存] をクリックします:

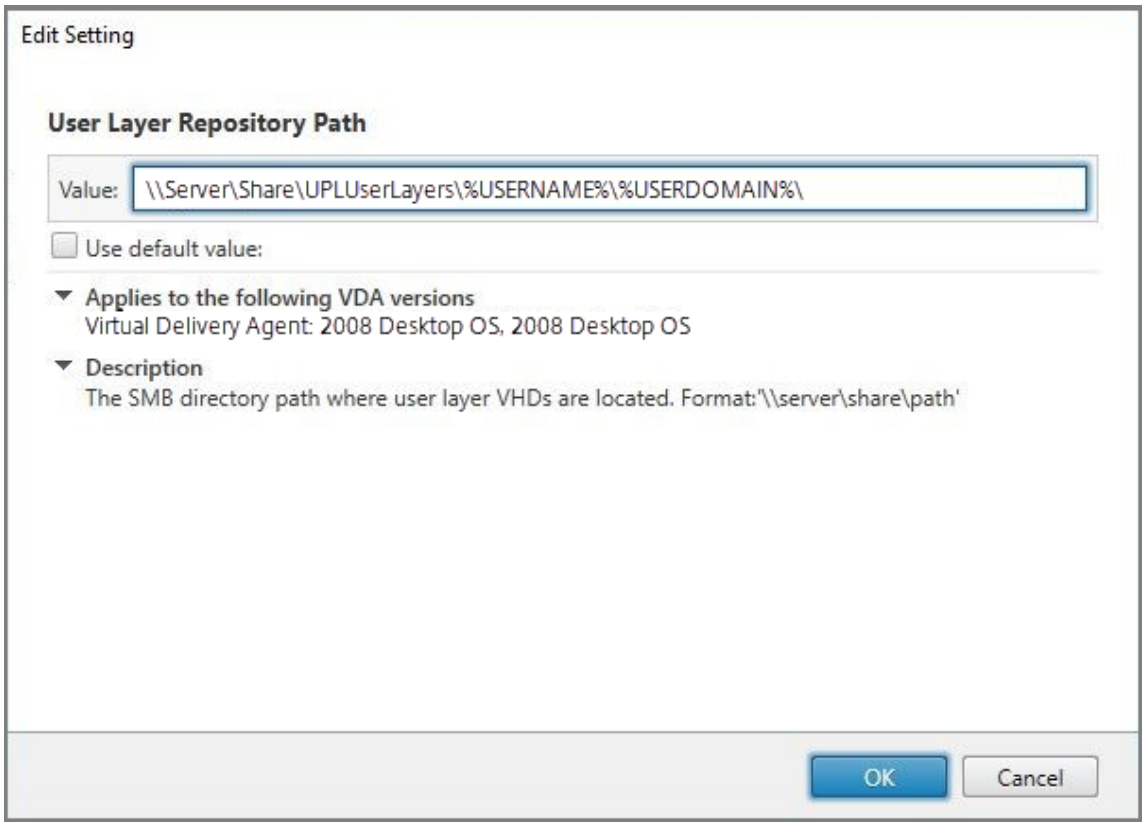
   - パスの形式: `\\server-name-or-address\share-name\folder`
   - パスの例: `\\Server\Share\UPLUsers`
   - 結果のパスの例: **CoolCompanyDomain** の **Alex** という名前のユーザーの場合、パスは次のようになります: `\\Server\Share\UPLUsers\Users\CoolCompanyDomain_Alex\A_OK`



%USERNAME%および%USERDOMAIN%変数、マシン環境変数、Active Directory（AD）属性を使用してパスをカスタマイズできます。これらの変数を展開すると、明示的なパスになります。

環境変数の例:

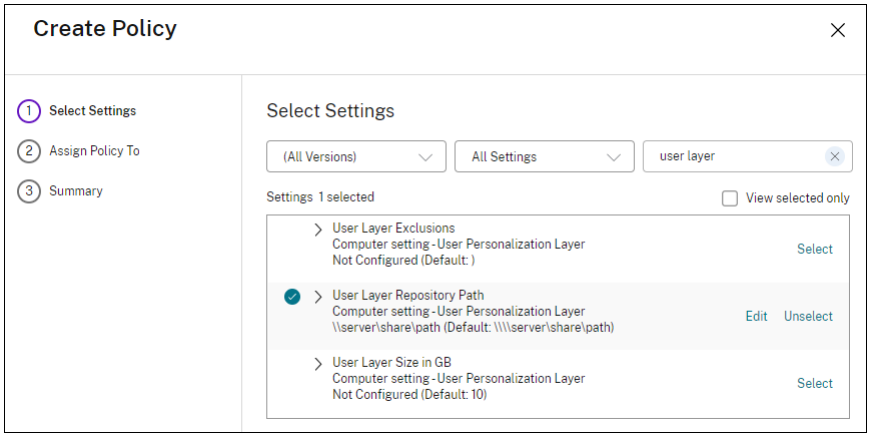
- パスの形式: \\Server-name-or-address\share-name\folder-with-environment-variables
- パスの例: \\Server\Share\UPLUserLayers\\%USERNAME%\\%USERDOMAIN%
- 結果のパスの例: **CoolCompanyDomain** の **Alex** という名前のユーザーの場合、パスは次のようになります: \\Server\Share\UPLUserLayers\Alex\CoolCompanyDomain\A_OK



カスタム AD 属性の例:

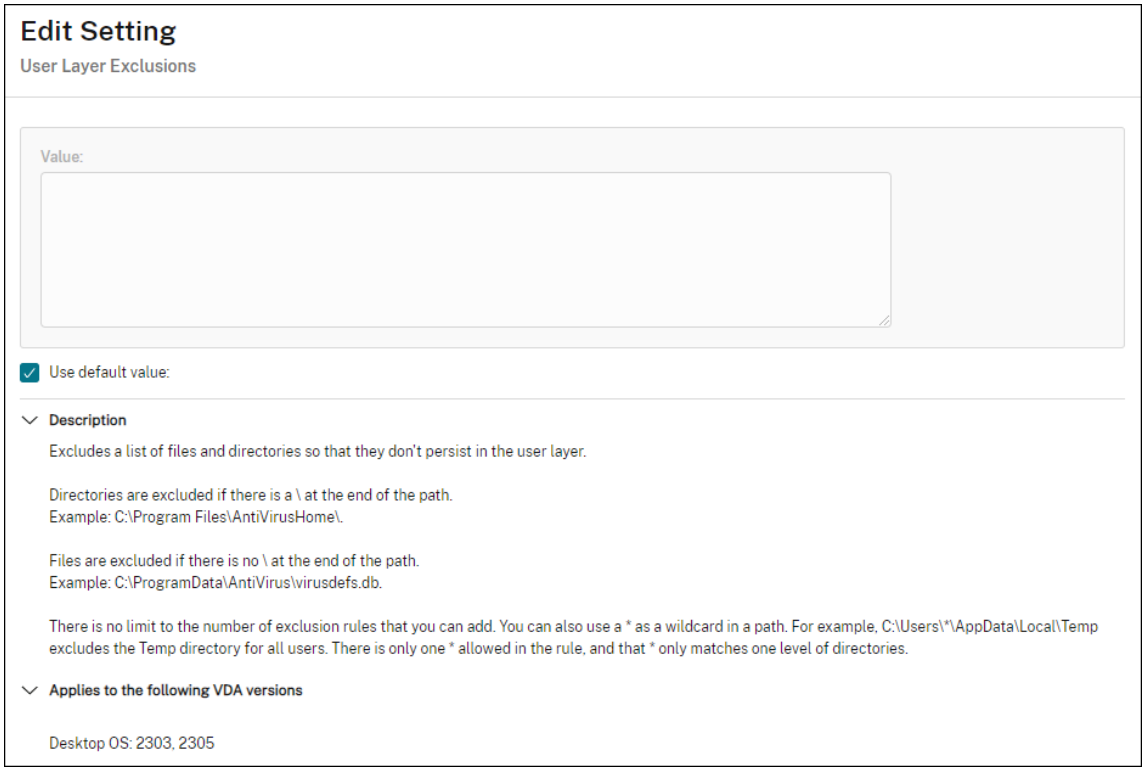
- パスの形式: \\Server-name-or-address\share-name\AD-attribute
- パスの例: \\Server\share\\#sAMAccountName#
- 結果のパスの例: \\Server\share\JohnSmith（#sAMAccountName# が現在のユーザーの JohnSmith に解決される場合）

6. オプション:［ユーザーレイヤーサイズ（**GB**）］の横にあるチェックボックスをオンにして、［編集］をクリックします:

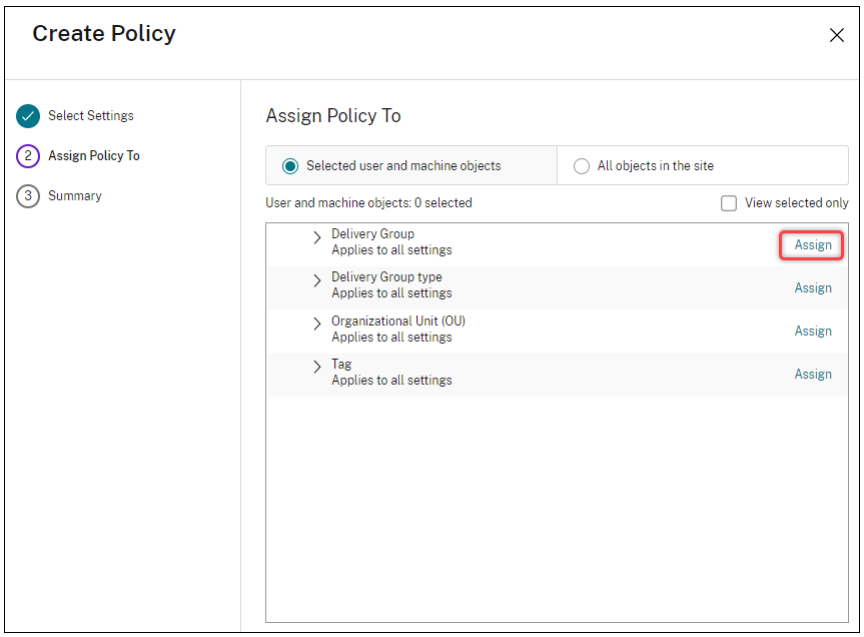


［設定の編集］ウィンドウが開きます。

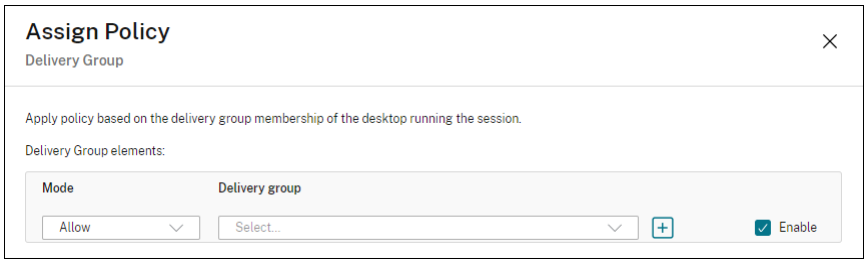
7. オプション：デフォルト値の **10GB** からユーザーレイヤーが拡大できる最大サイズに変更します。［保存］をクリックします。
8. オプション：［ユーザーレイヤーからの除外］の横にあるチェックボックスをオンにして、［編集］をクリックします。



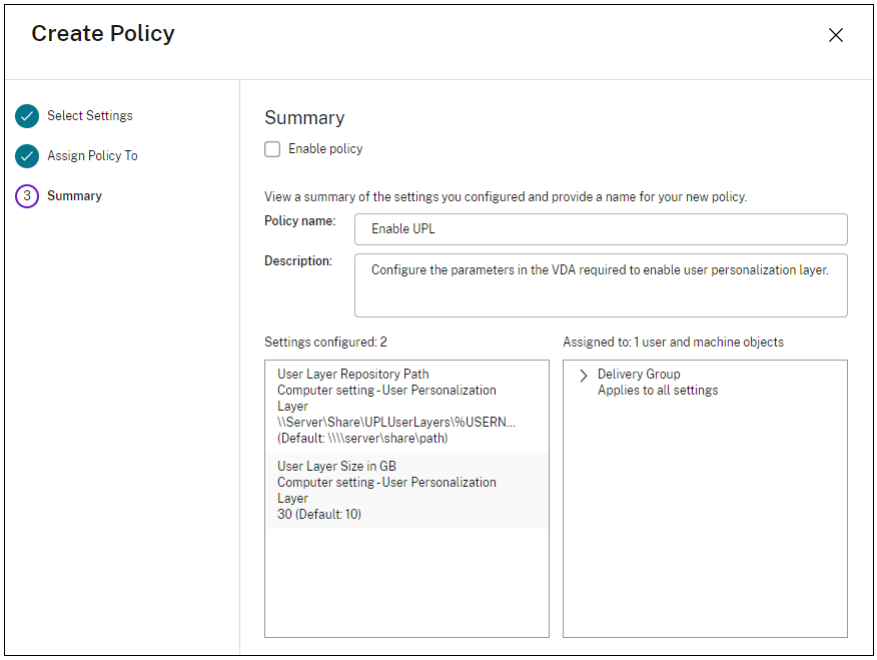
9. オプション：除外するファイルとフォルダーを指定し、［保存］をクリックします。詳しくは、Citrix App Layering のドキュメントを参照してください。
10. ［次へ］をクリックして、割り当てるユーザーとマシンを構成します。この画像で強調表示されている ［デリバリーグループ割り当て］リンクをクリックします：



11. ［デリバリーグループ］メニューで、前のセクションで作成したデリバリーグループを選択します。［**OK**］をクリックします。



12. ポリシーの名前を入力します。チェックボックスをクリックしてポリシーを有効にし、［完了］をクリックします。



ユーザーレイヤーフォルダーのセキュリティ設定の構成

ドメイン管理者は、ユーザーレイヤーに複数のストレージの場所を指定できます。各ストレージの場所（デフォルトの場所を含む）に対して、「\Users」サブフォルダーを作成します。次の設定を使用して各場所を保護します。

設定名	値	適用先
作成所有者	変更	サブフォルダーおよびファイルのみ
所有者の権利	変更	サブフォルダーおよびファイルのみ
ユーザーまたはグループ:	フォルダーの作成/データの追加; フォルダーのスキャン/ファイルの実行; フォルダーの一覧化/データの読み取り; 属性の読み取り	選択したフォルダーのみ
システム	フルコントロール	選択したフォルダー、サブフォルダーおよびファイル
ドメイン管理者、および選択した管理者グループ	フルコントロール	選択したフォルダー、サブフォルダーおよびファイル

ユーザーレイヤーメッセージ

ユーザーがユーザーレイヤーにアクセスできない場合、これらの通知メッセージのいずれかを受信します。

- 使用中のユーザーレイヤー


```
We were unable to attach your user layer because it is in use.
Any changes you make to application settings or data will not be
saved. Be sure to save any work to a shared network location.
```

- 利用できないユーザーレイヤー

```
We were unable to attach your user layer. Any changes you make to
 application settings or data will not be saved. Be sure to save
any work to a shared network location.
```

- ユーザーのサインアウト後にリセットされないシステム

```
This system was not shut down properly. Please log off immediately
 and contact your system administrator.
```

トラブルシューティング時に使用するログファイル

ログファイル ulayersvc.log には、変更が記録されたユーザー個人設定レイヤーソフトウェアの出力が含まれています。

```
1 C:\ProgramData\Unidesk\Logs\ulayersvc.log
```

ユーザーレイヤー/UPL 領域の解放

ユーザーレイヤー/UPL 領域の解放を使用して、ユーザーのログオフのたびに自動的に VHDX ファイルを圧縮できます。
詳しくは、「ユーザーレイヤー/UPL 領域の解放」を参照してください

制限事項

ユーザー個人設定レイヤー機能をインストールして使用する場合、次の制限に留意してください。

- App Layering 内のレイヤーにユーザー個人設定レイヤーソフトウェアを展開しようとしないでください。Citrix Virtual Apps and Desktops にユーザー個人設定レイヤーを展開するか、App Layering イメージテンプレートでユーザーレイヤーを有効にします。両方ではありません。どちらのプロセスでも、必要なユーザーレイヤーが生成されます。
- 永続マシンカタログを使用してユーザー個人設定レイヤー機能を構成しないでください。
- セッションホストは使用しないでください。
- (Windows 10 のバージョンが同じ場合であっても) 新しい OS インストールを実行しているイメージのマシンカタログを更新しないでください。ベストプラクティスは、マシンカタログの作成時に使用したものと同じマスターイメージ内の OS に更新を適用することです。

- 起動時ドライバー、または以前の起動用個人設定を使用しないでください。
- Personal vDisk データをユーザー個人設定レイヤー機能に移行しないでください。
- App Layering 完全製品から既存のユーザーレイヤーをユーザー個人設定レイヤー機能に移行しないでください。
- 別のマスター OS イメージを使用して作成されたユーザーレイヤーにアクセスするためにユーザーレイヤーの SMB パスを変更しないでください。
- ユーザーがセッションからログアウトしてから再度ログインすると、新しいセッションはプール内の別のマシンで実行されます。VDI 環境において、Microsoft Software Center は最初のマシンではアプリケーションをインストール済みと表示しますが、2 番目のマシンでは使用不可と表示します。

  アプリケーションの実際のステータスを確認するには、ソフトウェアセンターでアプリケーションを選択して［インストール］をクリックするよう、ユーザーに指示します。次に、SCCM はステータスを true の値に更新します。
- ソフトウェアセンターは、ユーザー個人設定レイヤー機能が有効になっている VDA 内で起動した直後に停止することがあります。この問題を回避するには、XenDesktop VDI 環境での SCCM の実装についての Microsoft の推奨事項に従ってください。また、ソフトウェアセンターを開始する前に、`ccmexec`サービスが実行されていることを確認してください。
- グループポリシー（コンピューター設定）では、ユーザーレイヤー設定はマスターイメージに適用された設定を上書きします。そのため、GPO を使用して［コンピューターの設定］で行った変更が、次のセッションログインまで保持されるとは限りません。

  この問題を回避するには、コマンドを発行するユーザーログオンスクリプトを作成します：

  ```
  gpupdate /force
  ```

  たとえば、ある顧客は各ユーザーログインで実行するように次のコマンドを設定します：

  ```
  gpudate /Target:Computer /force
  ```

  最適な結果を得るには、ユーザーのログイン後、ユーザーレイヤーで［コンピューターの設定］に直接変更を適用します。
- ドメインユーザーアカウントが、マスターイメージにログインした最後のユーザーにならないようにします。これを怠ると、そのイメージからプロビジョニングされたマシンに問題が発生します。
- 純粋な Azure AD 環境で UPL が有効になっている場合、Azure 上で実行されている Windows が原因の問題によって、カスタム証明書が保持されません。Microsoft による将来の機能強化でこの問題が修正された場合、この記事を更新します。

コンポーネントの削除

August 20, 2024

製品のコンポーネントを削除するには、プログラムの削除（アンインストール）や変更を行う Windows の機能を使用することをお勧めします。または、コマンドラインや、インストールメディアに収録されているスクリプトを使用してコンポーネントをアンインストールすることもできます。

コンポーネントをアンインストールしても、そのコンポーネントと一緒にインストールされたサードパーティ製ソフトウェアはアンインストールされず、ファイアウォール設定も変更されません。たとえば、Delivery Controller をアンインストールしても、SQL Server ソフトウェアおよびデータベースは削除されません。

Controller をアップグレードする前の環境で Web Interface を使用していた場合は、Web Interface コンポーネントを別途アンインストールする必要があります。この製品のインストーラーを使って Web Interface をアンインストールすることはできません。

以下に記載されていない機能の削除については、機能のドキュメントを参照してください。

準備

Controller をアンインストールする前に、サイトからその Controller を削除してください。詳しくは、「Controller の削除」を参照してください。

Studio と Director を終了してから削除してください。

プログラムの削除や変更を行う **Windows** の機能を使用してコンポーネントをアンインストールする

プログラムの削除や変更を行うための Windows 機能（コントロールパネルの［プログラムと機能］など）を開き、以下の操作を行います:

- Controller、Studio、Director、ライセンスサーバー、または StoreFront をアンインストールするには、**Citrix Virtual Apps *version*** または **Citrix Virtual Desktops and Desktops *version*** を選択してから右クリックし、［アンインストール］を選択します。インストーラーが起動します。アンインストールするコンポーネントを選択します。

  StoreFront は、［**Citrix StoreFront**］を右クリックしてから ［アンインストール］を選択して削除することもできます。

- VDA をアンインストールするには、［**Citrix Virtual Delivery Agent *version***］を選択し、右クリックしてから ［アンインストール］を選択します。インストーラーが起動したら、アンインストールするコンポーネントを選択します。アンインストール後にデフォルトでマシンが自動的に再起動します。

- ユニバーサルプリントサーバーをアンインストールするには、［**Citrix** ユニバーサルプリントサーバー］を右クリックし、［アンインストール］を選択します。

コマンドラインを使ってコアコンポーネントをアンインストールする

\x64\XenDesktop Setupディレクトリから`XenDesktopServerSetup.exe`コマンドを実行します。

- 特定のコンポーネントのみをアンインストールするには、`/remove`および`/components`オプションを指定します。
- すべてのコンポーネントをアンインストールするには、`/removeall`オプションを指定します。

コマンドおよびパラメーターについて詳しくは、「コマンドラインを使ったインストール」を参照してください。

たとえば、Web Studio をアンインストールするには次のコマンドを実行します。

```
\x64\XenDesktop Setup\XenDesktopServerSetup.exe /remove /components
webstudio
```

コマンドラインを使って **VDA** をアンインストールする

\x64\XenDesktop Setupディレクトリから`XenDesktopVdaSetup.exe`コマンドを実行します。

- 特定のコンポーネントのみをアンインストールするには、`/remove`および`/components`オプションを使用します。たとえば、VDA と Citrix Workspace アプリをアンインストールするには、`/remove /components vda,plugin`を使用します。
- `/removeall`オプションは、VDA のみを削除します。Citrix Workspace アプリは削除されません。

コマンドおよびパラメーターについて詳しくは、「コマンドラインを使ったインストール」を参照してください。

アンインストール後にデフォルトでマシンが自動的に再起動します。

Active Directory のスクリプトを使用して VDA を削除するには、「スクリプトを使った VDA のインストールまたは削除」を参照してください。

アップグレードと移行

August 17, 2024

はじめに

新しいバージョンのマシンやサイトをセットアップしなくても、既存の環境をアップグレードすることで Citrix Virtual Apps and Desktops 7 最新リリース（**CR**）を使用できます。これをインプレースアップグレードと呼びます。

アップグレード後は、ライセンス対象の最新機能やテクノロジを利用できるようになります。さらに、以前のバージョンからの修正や機能拡張も使用することができます。

アップグレードの概要

1. アップグレードを開始する前に、「環境のアップグレード」の記事を確認してください。これは、アップグレードの準備と実装方法を学ぶための主要な情報源です。
2. 現在のカスタマーサクセスサービスの日付が有効であり、有効期限が切れていないことを確認してください。詳しくは、「カスタマーサクセスサービスの更新ライセンス」を参照してください。
3. 準備ガイダンスを完了します。
4. インストーラーを実行して、コアコンポーネントをアップグレードします。
5. データベースとサイトをアップグレードします。
6. イメージ上で（またはマシン上で直接）VDA をアップグレードします。
7. 他のコンポーネントをアップグレードします。

各準備とアップグレードの手順については、「環境のアップグレード」を参照してください。

アップグレードできるバージョン

以下から Citrix Virtual Apps and Desktops 2402 LTSR にアップグレードできます:

- Virtual Apps and Desktops 2203 LTSR（CU の有無は問わない/CU4 まで）
- Virtual Apps and Desktops 1912 LTSR（CU の有無は問わない/CU8 まで）
- Citrix Virtual Apps and Desktops：現在サポートされている最新リリースバージョン

アップグレードできる Citrix Virtual Apps and Desktops（および XenApp と XenDesktop）のバージョンの一覧については、[Citrix アップグレードガイド](/en-us/upgrade.html) も参照できます。

> 注:
>
> - アップグレードプロセスを開始する前に、Citrix は、管理された環境でアップグレードをテストし、特定の要件を満たしていることを確認することをお勧めします。さらに、スムーズな移行を確実に行うために、廃止機能一覧や既知の問題など、関連するすべての製品ドキュメントを確認することをお勧めします。このアプローチは、実稼働システムの中断の可能性を軽減し、全体的なアップグレードエクスペリエンスを向上させるのに役立ちます。
> - Citrix Virtual Apps and Desktops 1912 LTSR はまもなくサポート終了となります。
>   サポートされているバージョンの一覧については、「製品マトリクス」を参照してください。

よく寄せられる質問

このセクションでは、Citrix Virtual Apps and Desktops のアップグレードに関するよくある質問に回答します。

- **Virtual Apps and Desktops** 環境をアップグレードするための正しい順序はありますか

  推奨のアップグレード順序の図と説明については、「アップグレードの順序」と「アップグレード手順」を参照してください。

- サイトには、いくつかの **Delivery Controller** が（異なるゾーンに）あります。一部のみをアップグレードするとどうなりますか? 同じメンテナンスウィンドウ中にサイト内のすべての **Controller** をアップグレードする必要がありますか?

  各 Controller のさまざまなサービスが相互に通信するため、ベストプラクティスは、同じメンテナンスウィンドウ中にすべての Delivery Controller をアップグレードすることです。異なるバージョンを保持すると、問題が発生する場合があります。メンテナンスウィンドウ中に、半分の Controller をアップグレードし、サイトをアップグレードしてから、残りの Controller をアップグレードすることをお勧めします。詳しくは、「アップグレード手順」を参照してください。

- 最新バージョンに直接アップグレードできますか。それとも増分アップグレードが必要ですか。

  アップグレードするバージョンのドキュメントの「新機能」に別途明記されていない限り、常に中間リリースを省略して最新バージョンにアップグレードすることができます。
  「[アップグレードガイド](/en-us/upgrade)」を参照してください。

- お客様は長期サービスリリース（**LTSR**）環境から最新リリースにアップグレードできますか

  はい。お客様が長期間にわたって長期サービスリリースを継続して使用する必要はありません。ビジネス上の要件および機能に基づいて、LTSR 環境を最新リリースに移行できます。

- コンポーネントのバージョンを混在させることはできますか

  Citrix では各サイト内ですべてのコンポーネントを同じバージョンにアップグレードすることをお勧めします。コンポーネントによっては以前のバージョンを使用できますが、最新バージョンの機能を一部使用できない場合があります。詳しくは、「混在環境に関する考慮事項」を参照してください。

- どのくらいの頻度で最新リリースをアップグレードする必要がありますか。

  最新リリースは、リリース日の 6 か月後にメンテナンス終了（EOM）になります。Citrix では、常に最新リリースを採用することをお勧めします。最新リリースは、リリース日の 18 か月後に製品終了（EOL）になります。

  詳しくは、「[最新リリースのライフサイクル](https://www.citrix.com/support/product-lifecycle/milestones/citrix-virtual-apps-and-desktops.html)」を参照してください。

- **LTSR** または **CR** のどちらにアップグレードすべきしょうか。

  最新リリース（CR）は、最新の画期的なアプリ、デスクトップ、サーバー仮想化機能を提供します。CR を導入することによって、最新テクノロジを活用し、競合に差をつけることができます。

  長期サービスリリース（LTSR）は、長期間にわたって同じ基本バージョンを維持する必要がある大企業の実稼働環境に最適です。

For details, see [Servicing Options](https://www.citrix.com/support/citrix-customer-success-services/citrix-virtual-apps-and-desktops-servicing-options.html).

- 使用しているライセンスはアップグレードが必要でしょうか。

  現在のライセンス日が期限切れになっていないこと、およびアップグレード対象のリリースに対して有効であることを確認してください。CTX111618を参照してください。更新について詳しくは、「カスタマーサクセスサービスの更新ライセンス」を参照してください。

- アップグレードにはどれくらい時間がかかりますか。

  展開のアップグレードに必要な時間は、インフラストラクチャとネットワークによって異なります。そのため、正確な時間は不明です。

- ベストプラクティスについて教えてください。

  準備に関するガイドに目を通し、それに従ってください。

- どのオペレーティングシステムがサポートされていますか。

  アップグレードするバージョンに関する「システム要件」の記事に、サポート対象の OS が記載されています。

  現在の展開で、サポートされていないオペレーティングシステムを使用している場合は、「以前のオペレーティングシステム」を参照してください。

- どのバージョンの **VMware vSphere**（**vCenter + ESXi**）がサポートされていますか。

  CTX131239に、サポートされているホストとバージョン、および既知の問題へのリンクが記載されています。

- 使用中のバージョンの **EOL** スケジュールを教えてください。

  「製品マトリクス」を確認してください。

- 最新のリリースにはどのような既知の問題がありますか。

  - Citrix Virtual Apps and Desktops
  - StoreFront
  - Citrix Provisioning
  - Citrix ライセンスサーバー
  - Windows 向け Citrix Workspace アプリ

追加情報

[長期サービスリリース（LTSR）](https://www.citrix.com/support/citrix-customer-success-services/citrix-virtual-apps-and-desktops-servicing-options.html)

長期サービスリリース（**LTSR**）展開の更新には、累積更新プログラム（CU）を使用します。CU は LTSR のベースラインコンポーネントを更新します。各 CU には、独自の Metainstaller が含まれます。

また、それぞれに専用のドキュメントがあります。たとえば 2203 LTSR の場合、LTSR の「新機能」ページで最新 CU のリンクを確認してください。各 CU ページには、サポートされているバージョンの情報、手順、CU のダウンロードパッケージへのリンクが含まれています。

移行

クラウドへの移行

Citrix Virtual Apps and Desktops の自動構成ツールを使用して、オンプレミス展開をクラウドに移行できます。詳しくは、「クラウドへの移行」を参照してください。

従来からの移行

以前のバージョンの環境から、より新しいバージョンの環境にデータを移行できます。移行処理により、より新しいコンポーネントのインストール、新しいサイトの作成、既存のファームからのデータのエクスポート、および新しいサイトへのデータのインポートが行われます。

XenApp および XenDesktop のバージョンの移行、または以前の Citrix Virtual Apps and Desktops のバージョンの移行用に、サポートされているツールやスクリプトはありません。アップグレードは、長期サービスリリース (LTSR) Citrix アップグレードガイドに記載されている Citrix Virtual Apps and Desktops バージョンでサポートされており、<!–> この製品ドキュメントで説明しています。

以前の XenApp 6.x の移行コンテンツについては、以下を参照してください。スクリプトや記事は用意しておらず、保持もされていません。

- XenApp 6.x バージョンのオープンソース移行スクリプトは、https://github.com/citrix/xa65migrationtoolから入手できます。Citrix ではこれらの移行スクリプトに対応しておらず、保持もしていません。
- 7.x での変更点
- XenApp 6.5 ワーカーから新しい VDA へのアップグレード
- XenApp 6.x からの移行

環境のアップグレード

August 17, 2024

はじめに

新しいバージョンのマシンやサイトをセットアップせずに、一部の環境をアップグレードすることができます。これはインプレースアップグレードと呼ばれます。

アップグレードできる Citrix Virtual Apps and Desktops のバージョンについては、Citrix アップグレードガイドを参照してください。

任意の Citrix Virtual Apps and Desktops リリースにアップグレードする前に、現在のカスタマーサクセスサービスの日付が有効で期限切れではないことを確認します。詳しくは、「カスタマーサクセスサービスの更新ライセンス」を参照してください。

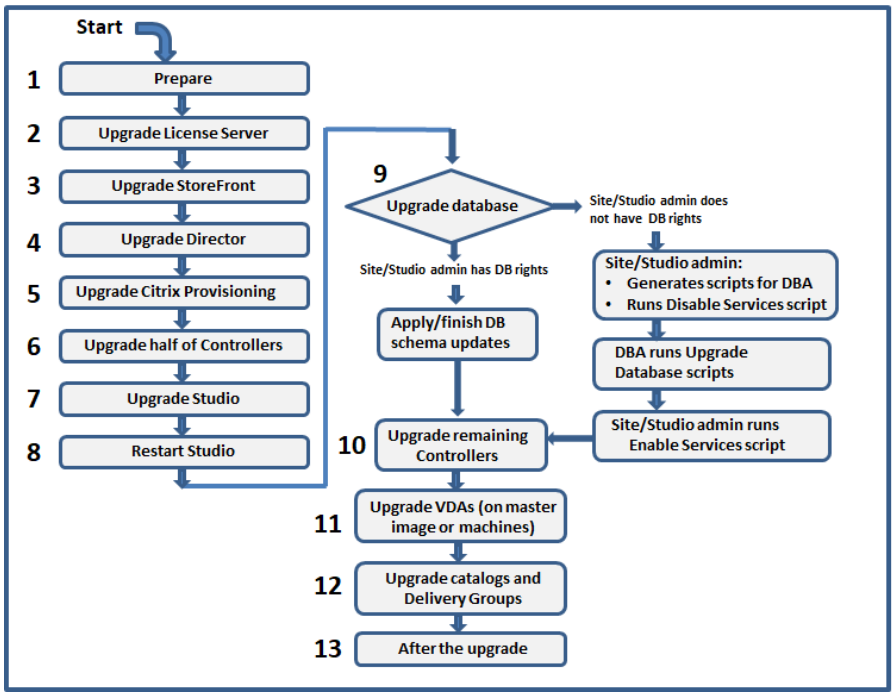
アップグレードを開始するには、新しいバージョンでインストーラーを実行して、以前にインストールされたコアコンポーネント、VDA、およびその他の特定のコンポーネントをアップグレードします。その後に、データベースとサイトをアップグレードします。

全製品インストーラー（およびスタンドアロン VDA インストーラー）でインストールできるコンポーネントの新しいバージョンが提供されている場合は、そのコンポーネントをアップグレードできます。全製品インストーラーでインストールされていない他のコンポーネント（Citrix Provisioning や Profile Management など）については、そのコンポーネントのマニュアルを参照してください。ホストのアップグレードについては、該当するドキュメントを参照してください。

アップグレードを開始する前に、この記事の情報をすべて確認してください。

アップグレードの順序

次の図に、アップグレードの順序を示します。「アップグレード手順」には、図の各手順の詳細が記載されています。



> 注:
>
> 失敗を回避するには、新しいマシンカタログの作成、マシンカタログの削除、デリバリーグループ内のマシ

> ンの更新などのプロビジョニングおよびデリバリーグループ関連タスクを実行する前に、すべての Delivery Controller とデータベースをアップグレードする必要があります。

ハイブリッド権利ライセンス

ハイブリッド権利ライセンスは、お客様が永続的ライセンスからクラウドサービスサブスクリプションに移行またはトレードアップするときに、クラウドサービスサブスクリプションに加えて提供される、期間ベースのサブスクリプションライセンスです。DaaS サブスクリプションでハイブリッド権利アドオンを購入することもできます。

SaaS 属性を持つハイブリッド権利ライセンスをお持ちの場合、Citrix Virtual Apps and Desktops LTSR 2203 以降にアップグレードすると、Citrix Virtual Apps and Desktops LTSR 1912 で利用できない機能にアクセスできるようになります。これらの機能には、Microsoft Azure、AWS EC2、Google Cloud などのパブリッククラウドでのワークロードに関するプロビジョニングとホストが含まれます。新しいライセンスファイルを展開する前に、ライセンスサーバーを最新バージョンに更新してください。

SaaS 属性のないハイブリッド権利ライセンスにアクセスできる場合は、次の手順に従って、SaaS 属性を持つ新しいハイブリッド権利ライセンスにアクセスできます:

> 注:
>
> - 新しいライセンスコードが記載されたメールが届きます。詳しくは、「ライセンスアクセスコードを使用」を参照してください。
> - 既存のライセンスは破棄されます。不要になったライセンスはライセンスサーバーから削除し、新しいライセンスをインストールする必要があります。詳しくは、「ライセンスファイルの削除」を参照してください。

1. citrix.comの［Manage Licenses］のポータルにアクセスし、クラウドプロビジョニング権利が有効になっている新しいハイブリッド権利ライセンスファイルをダウンロードします（SaaS 属性）。詳しくは、「ライセンスのダウンロード」を参照してください。次の画像は、増分セクションに SaaS 属性を持つハイブリッド権利ライセンスファイルを示しています。

```
INCREMENT XDT_PLT_CCS CITRIX 2022.1201 01-dec-2022 5 \
    VENDOR_STRING=;LT=RetailS;GP=720;PSL=10;CL=VDS,VDA,VDE,VDP,SaaS:SA=0;ODP=0;NUDURMIN=2880;NUDURMAX=525600;AP=ADMIN/INT/14
    OVERDRAFT=1 DUP_GROUP=V ISSUED=18-dec-2005 NOTICE="Citrix \
    Systems Inc." SN=RetailSSaaS SIGN="..."
```

2. ハイブリッド権利ライセンスファイルをライセンスサーバーにインストールします。詳しくは、「ライセンスのインストール」を参照してください。
3. ライセンスエディションまたはモデルに変更がある場合は、ブローカーコマンドを実行してエディションとモデルを設定してから、インプレースアップグレードを開始するようにします。Broker コマンドについて詳しくは、「Broker PowerShell SDK」セクションを参照してください。

Citrix Virtual Apps and Desktops の最新リリースおよび長期サービスリリースでのパブリッククラウドサポートについて詳しくは、CTX270373を参照してください。

アップグレード手順

主な製品コンポーネントのほとんどは、そのコンポーネントを含むマシンで製品インストーラーを実行するとアップグレードできます。

1 つのマシンに複数のコンポーネント（Studio や License Server など）が含まれている場合、製品メディアに新しいバージョンのソフトウェアが含まれていれば、そのマシン上のすべてのコンポーネントがアップグレードされます。

インストーラーを使用するには、次の手順に従います:

- 全製品インストーラーのグラフィカルインターフェイスを実行するには、マシンにログオンし、メディアを挿入するか、新しいリリース用の ISO ドライブをマウントします。**AutoSelect** をダブルクリックします。
- コマンドラインインターフェイスを使用するには、該当するコマンドを発行します。「コマンドラインを使用したインストール」を参照してください。

手順 **1**: 準備

アップグレードを開始する前に、準備ができていることを確認します。次の必要なタスクについて読み、完了します:

- PvD、AppDisk、およびサポートされていないホストの削除
- PvD または AppDisk コンポーネントを持つ VDA
- 制限事項
- 混在環境に関する考慮事項
- 以前のオペレーティングシステム
- 準備
- 事前サイトテスト
- SQL Server のバージョンチェック

手順 **2**: ライセンスサーバーのアップグレード

新しいバージョンの Citrix License Server ソフトウェアがインストールされている場合は、他のコンポーネントよりも先にこのコンポーネントをアップグレードします。

新しいバージョンでライセンスサーバーに互換性があるか確認できない場合、他のコアコンポーネントをアップグレードする前にライセンスサーバーでインストーラーを実行する必要があります。

手順 **3**: **StoreFront** のアップグレード

インストールメディアに新しいバージョンの StoreFront ソフトウェアが含まれている場合は、StoreFront サーバーが存在するマシンでインストーラーを実行します。

- グラフィカルインターフェイスで、［拡張展開］セクションから ［**Citrix StoreFront**］を選択します。
- コマンドラインから`CitrixStoreFront-x64.exe`を実行します。これは Citrix Virtual Apps and Desktops のインストールメディアの`x64`フォルダーにあります。

手順 **4**：**Director** のアップグレード

インストールメディアに新しいバージョンの Director ソフトウェアが含まれている場合は、Director が含まれているマシンでインストーラーを実行します。

手順 **5**：**Citrix Provisioning** のアップグレード

Citrix Provisioning のインストールメディアは、Citrix Virtual Apps and Desktops のインストールメディアとは別に入手します。Citrix Provisioning サーバーおよびターゲットデバイスのソフトウェアをインストールおよびアップグレードする方法については、Citrix Provisioning の製品ドキュメントを参照してください。

手順 **6**：**Delivery Controller** の半分のアップグレード

たとえば、サイトに 4 つの Controller がある場合、そのうちの 2 つでインストーラーを実行します。

半数の Controller をアクティブなままにしておくことによって、ユーザーがそのサイトにアクセスできます。VDA はこれらの残りの Controller に登録されます。使用可能な Controller の数が減少するため、サイトの処理能力が低下する場合があります。データベースのアップグレードの最終段階で新しいクライアント接続を確立するときに、ほんの短い間だけサイトの動作が中断されます。アップグレード済みの Controller では、サイト全体がアップグレードされるまで要求を処理できません。

サイトに Controller が 1 つしかない場合、アップグレード中はサイトが動作しなくなります。

実際のアップグレードが開始される前に、最初の Controller で事前サイトテストが実行されます。詳しくは、「事前サイトテスト」を参照してください。

手順 **7**：**Studio** のアップグレード

Web Studio をまだアップグレードしていない場合（別のコンポーネントと同じマシン上にあったため）、Studio を含むマシンでインストーラーを実行します。

> 注：
>
> Web Studio をアップグレードした後、バージョン情報がすぐに更新されない場合があります。Web Studio がすでに最新の状態であっても、アップグレードするように求められる場合があります。この問題に対応するには、Web Studio サーバーに移動し、インターネットインフォメーションサービス（IIS）マネージャーを開

> き、［スタートページ］>［サイト］>［Default Web Site］に移動し、［Web サイトの管理］ペインで ［再起動］を選択します。

手順 **8**：**Studio** の再起動

アップグレードした Web Studio を再起動します。アップグレードプロセスが自動的に再開されます。

手順 **9**：データベースとサイトのアップグレード

> 注：
>
> 失敗を回避するには、新しいマシンカタログの作成、マシンカタログの削除、デリバリーグループ内のマシンの更新などのプロビジョニングおよびデリバリーグループ関連タスクを実行する前に、すべての Delivery Controller とデータベースをアップグレードする必要があります。

SQL Server データベースのスキーマを更新するために必要な権限について、「準備」で確認します。

- SQL Server データベーススキーマを更新するために十分な権限がある場合は、データベースの自動アップグレードを開始できます。「データベースとサイトの自動アップグレード」に進みます。
- 十分なデータベース権限がない場合は、スクリプトを使用する手動アップグレードを開始し、データベース管理者（必要な権限を持つ誰か）の支援によって続行できます。手動アップグレードの場合、Studio ユーザーはスクリプトを生成し、サービスを有効または無効にするスクリプトを実行します。データベース管理者は、SQLCMD ユーティリティ、または SQL Server Management Studio を SQLCMD モードで使用して、データベーススキーマを更新するその他のスクリプトを実行します。「データベースとサイトの手動アップグレード」に進みます。
- マルチゾーン展開をしており、データベースとサイトを自動的にアップグレードする場合は、Citrix ではサイトの SQL サーバーデータベースをホストするのと同じゾーンで、dbschema のアップグレードを実行することをお勧めします。そうしないと、データベースとサイトの自動アップグレードが失敗する場合があります。

アップグレードする前にデータベースをバックアップしておくことを Citrix では強くお勧めします。CTX135207 を参照してください。データベースのアップグレード中は製品サービスが無効になります。その間は、Controller がサイトへの接続要求を仲介できなくなるため、慎重に計画しておく必要があります。

データベースとサイトの自動アップグレード

1. 新しくアップグレードした Studio を起動します。
2. サイトのアップグレードを自動的に開始するよう指定して、準備ができていることを確認します。

データベースとサイトのアップグレードが続行されます。

データベースとサイトの手動アップグレード

1. 新しくアップグレードした Studio を起動します。
2. サイトを手動でアップグレードするよう指定します。ウィザードでライセンスサーバーの互換性がチェックされ、確認メッセージが表示されます。
3. データベースがバックアップされたことを確認します。

   スクリプトとアップグレード手順のチェックリストが生成され、表示されます。製品バージョンのアップグレード後にデータベースのスキーマが変更されていない場合、該当するスクリプトは生成されません。たとえば、App Orchestration ログデータベーススキーマが変更されていない場合、`UpgradeLoggingDatabase.sql`スクリプトは生成されません。
4. 以下のスクリプトを順番に実行します。

   - `DisableServices.ps1`: Studio ユーザーはこの PowerShell スクリプトを Controller で実行して、製品サービスを無効にします。
   - `UpgradeSiteDatabase.sql`: データベース管理者は、サイトデータベースを格納しているサーバー上でこの SQL スクリプトを実行します。
   - `UpgradeMonitorDatabase.sql`: データベース管理者は、モニターデータベースを格納しているサーバー上でこの SQL スクリプトを実行します。
   - `UpgradeLoggingDatabase.sql`: データベース管理者は、構成ログデータベースを格納しているサーバー上でこの SQL スクリプトを実行します。このスクリプトは、このデータベースが変更された場合にのみ実行します（Hotfix の適用後など）。
   - `EnableServices.ps1`: Studio ユーザーは、この PowerShell スクリプトを Controller で実行して、製品サービスを有効にします。

   データベースのアップグレードが完了し、製品サービスが有効になると、Studio で自動的に環境と構成がテストされて HTML レポートが生成されます。問題が見つかった場合は、データベースのバックアップを復元できます。問題を解決した後で、データベースのアップグレードを再試行します。
5. チェックリストのタスクを完了したら、［アップグレードを完了する］を選択します。

手順 **10**: 残りの **Delivery Controller** のアップグレード

アップグレードした Studio のナビゲーションペインで、［**Citrix Studio**（サイト名）］を選択し、［よく使用するタスク］タブで、［残りの **Delivery Controller** のアップグレード］を選択します。

> 注:
>
> ［残りの **Delivery Controller** のアップグレード］を利用するには、サイト用に少なくとも 1 つのマシンカタログと 1 つのデリバリーグループを作成します。

アップグレードが完了したら、Studio をいったん閉じてから再度開きます。Controller のサービスをサイトに登録するため、またはゾーン ID が存在しない場合に作成するために、追加のサイトアップグレードを要求するメッセージ

が Studio によって表示されることがあります。

手順 **11**：**VDA** のアップグレード

> 重要：
>
> VDA をバージョン 1912 以降にアップグレードする場合には、「VDA を 1912 以降にアップグレードする」を参照してください。

アップグレードする VDA のマシン上で製品インストーラーを実行します。

Machine Creation Services とマスターイメージを使用してマシンを作成した場合は、ホストに移動し、マスターイメージの VDA をアップグレードします。使用可能な任意の VDA インストーラーを使用できます。

- グラフィカルインターフェイスのガイダンスについては、「VDA のインストール」を参照してください。
- コマンドラインのガイダンスについては、「コマンドラインを使用したインストール」を参照してください。

Citrix Provisioning を使用してマシンを作成した場合、アップグレードに関するガイダンスについては、Citrix Provisioning の製品ドキュメントを参照してください。

手順 **12**：マシンカタログとデリバリーグループの更新

- VDA がアップグレードされたマシンを使用するカタログを更新します。
- VDA がアップグレードされたマシンを使用するカタログをアップグレードします。
- VDA がアップグレードされたマシンを使用するデリバリーグループをアップグレードします。

手順 **13**：アップグレード後

アップグレードが完了したら、新しくアップグレードしたサイトをテストできます。Studio のナビゲーションペインで、**Citrix Studio** のサイト名を選択します。［よく使用するタスク］タブの ［サイトのテスト］を選択します。これらのテストはデータベースのアップグレード後に自動的に実行されますが、必要に応じて再実行できます。

サイトデータベースにローカルの Microsoft SQL Server Express を使用している場合に、SQL Server Browser サービスが開始されてないと、Windows Server 2016 上の Controller に対するテストが失敗する可能性があります。これを回避するには、以下の操作を行います：

- （必要に応じて）SQL Server Browser サービスを有効にして開始します。
- SQL Server（SQLEXPRESS）サービスを再開始します。

展開の他のコンポーネントをアップグレードします。ガイダンスについては、以下の製品ドキュメントを参照してください：

- StoreFront
- AppDNA

- Citrix App Layering
- HDX RealTime Optimization Pack
- Profile Management
- Citrix Provisioning
- Session Recording
- Workspace Environment Management

Microsoft SQL Server Express LocalDB ソフトウェアを新しいバージョンに置き換える必要がある場合は、「SQL Server Express LocalDB の置き換え」を参照してください。

Dbschema のアップグレード

環境を更新すると、一部のデータベーススキーマがアップグレードされることがあります。このプロセスでアップグレードされるデータベーススキーマについては、次の表を参照してください:

From\To	1912 CU1	1912 CU2	1912 CU3	1912 CU4	1912 CU5	2203
7.15 RTM or 7.15 CU releases	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config; Logging
1912 RTM	Config	Site, Config	Site, Config	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config; Logging
1912 CU1		Site	Site, Config	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config; Logging
1912 CU2			Site, Config	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config; Logging
1912 CU3				Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config; Logging
1912 CU4					Site, Config	Site; Monitor; Config; Logging
1912 CU5						Site; Monitor; Config; Logging
2112						Site; Monitor; Config

用語の定義:

- サイト: サイトデータストア。サイトデータストアに対して Dbschema の更新が行われます。
- モニター: モニターデータストア。モニターデータストアに対して Dbschema の更新が行われます。
- 構成: 構成テーブル。Desktop Studio のバージョン、ライセンス情報、またはその両方が構成テーブルで更新されます。
- ログ: ログデータストア。ログデータストアに対して Dbschema の更新が行われます。

VDA を 2203 以降にアップグレード

Personal vDisk（PvD）コンポーネントを VDA にインストールしたことがある場合、その VDA をバージョン 2203 以降にアップグレードすることはできません。新しい VDA を使用するには、現在の VDA をアンインストールしてから新しくインストールする必要があります

この手順は、PvD を使用したことがない場合でも適用されます。

PvD コンポーネントが以前のバージョンでどのようにインストールされていたかは次のとおりです:

- VDA インストーラーのグラフィカルインターフェイスでは、PvD は ［追加コンポーネント］ページのオプションです。
- コマンドラインでは、`/baseimage`オプションによって PvD がインストールされます。このオプションを指定した場合、またはこのオプションを含むスクリプトを使用した場合、PvD がインストールされました。

VDA に PvD がインストールされているかどうかわからない場合は、マシンまたはイメージで新しい VDA（2203 以降）のインストーラーを実行します。

- PvD がインストールされている場合、互換性のないコンポーネントがあることを示すメッセージが表示されます。
  - グラフィカルインターフェイスから、メッセージが表示されるページで ［キャンセル］をクリックして、インストーラーを閉じます。
  - CLI では、コマンドが失敗してメッセージが表示されます。
- PvD がインストールされていない場合、アップグレードが続行されます。

必要なアクション

VDA に PvD がインストールされていない場合は、通常のアップグレード手順に従ってください。

VDA に PvD がインストールされている場合:

1. 現在の VDA をアンインストールします。
2. 新しい VDA をインストールします。

Windows 10（1607 以前、更新なし）マシンで PvD を引き続き使用する場合、使用できる最新バージョンは VDA 7.15 LTSR です。

> 注:
>
> *XenApp および XenDesktop 7.15 LTSR の Windows 7 デスクトップで Personal vDisk を使用できますか?*
>
> Citrix は、2016 年 1 月に発表された XenApp および XenDesktop 7.6 LTSR から Personal vDisk（PvD）を除外しました。さらに、Citrix は PvD テクノロジの廃止を発表し、今後は Citrix App Layering の使用を開始することを推奨しています。Citrix App Layering（バージョン 4.4 以降）は、XenApp および XenDesktop 7.15 LTSR の互換性のあるコンポーネントです。ただし、Windows 7 での既存の PvD 展開を Citrix App Layering テクノロジに移行できるように、Citrix は、2020 年 1 月 14 日までの期間限定で XenApp および XenDesktop 7.15 LTSR 累積更新プログラム（CU）を介して Windows 7 デスクトップで PvD 展開をサポートすることを決定しました。PvD コンポーネントは LTSR CU から削除され、2020 年 1 月 14 日より後はサポートされなくなります。さらに、2020 年 1 月 14 日を超えて Windows 7 で PvD を使用すると、LTSR サイトのレンダリングが非準拠になります。また、Windows 10 用の PvD は引き続き 7.15 LTSR から除外されます。したがって、お客様は 7.15 LTSR サイトで PvD を使用しないでください。

PvD、**AppDisk**、およびサポートされていないホストの削除

以下のテクノロジとホストタイプは、Citrix Virtual Apps and Desktops 7 の現在のリリース展開ではサポートされていません:

- **Personal vDisk**（**PvD**） - ユーザーの VM の隣にあるデータをカタログに保存するためのもの。現在は、ユーザー個人設定レイヤー機能が、ユーザーの永続性を処理します。
- **AppDisk** - デリバリーグループで使用されるアプリケーションを管理するためのもの。
- ホストタイプ： Azure Classic、CloudPlatform（元の Citrix 製品）。
  - このリリースでサポートされるホストタイプについては、「システム要件」を参照してください。
  - ARM と AWS を引き続き使用できる別の方法については、CTX270373を参照してください。

現在の展開環境で PvD または AppDisk を使用している場合、またはサポートされていないホストタイプ（たとえば、Microsoft Azure Classic）への接続がある場合、それらのテクノロジを使用するアイテムを削除した後でのみ、バージョン 2006（またはそれ以降のサポートされているバージョン）にアップグレードできます。現在の展開でパブリッククラウドホスト接続（AWS など）を使用している場合は、アップグレードする前にハイブリッド権利ライセンスがあることを確認してください。1 つまたは複数のサポートされていないテクノロジ、またはハイブリッド権利ライセンスなしのホスト接続をインストーラーが検出すると、アップグレードが一時停止または停止し、説明メッセージが表示されます。インストーラーログに詳細が記載されています。

アップグレードを確実に成功させるには、サポートされていないアイテムを削除するための適切なガイダンスを確認し、それに従ってください。

- PvD を削除する
- AppDisk を削除する
- サポートされていないホストアイテムを削除する

展開で PvD または AppDisk を使用しなかった場合でも、関連する MSI が以前の VDA のインストールまたはアップグレードに含まれていることがあります。VDA をバージョン 2006（またはそれ以降のサポートされているバージョン）にアップグレードする前に、そのソフトウェアを使用したことがなくても削除する必要があります。グラフィカルユーザーインターフェイスを使用する場合、その削除は自動的に実行できます。または、CLI を使用するときに削除オプションを含めることができます。詳しくは、「PvD または AppDisks コンポーネントを持つ VDA のアップグレード」を参照してください。

PvD を削除する

PvD を使用するように構成されているすべてのマシンを削除するまで、展開のアップグレードは成功しません。削除をすると、カタログとデリバリーグループに影響します。

グループとカタログから PvD を削除するには：

1. Studio で、PvD を使用するカタログのマシンがデリバリーグループに含まれている場合は、それらのマシンをグループから削除します。
2. Studio で、PvD を使用するマシンを含むカタログをすべて削除します。

VDA のアップグレード：展開のアップグレードでは、VDA に AppDisk または PvD コンポーネントがインストールされているかどうかは検出されません。ただし、VDA インストーラーでは、それが検出されます。詳しくは、「PvD または AppDisks コンポーネントを持つ VDA」を参照してください。

PvD の代わりに App Layering を使用する場合は、データの移動について、「PvD から App Layering への移行」を参照してください。

AppDisk を削除する

AppDisk を使用するすべてのデリバリーグループから AppDisk を削除して AppDisk 自体を削除するまで、展開のアップグレードは続行できません。

1. Studio のナビゲーションペインで ［デリバリーグループ］を選択します。
2. グループを選択し、［操作］ペインの ［**AppDisks** の管理］をクリックします。
3. グループから AppDisk を削除する操作をクリックします。
4. AppDisk を使用するデリバリーグループごとに手順 2 と 3 を繰り返します。
5. Studio のナビゲーションペインで ［**AppDisks**］を選択します。
6. AppDisk を選択し、AppDisk を削除する操作をクリックします。
7. AppDisk ごとに手順 5 と 6 を繰り返します。

VDA のアップグレード: 展開のアップグレードでは、VDA に AppDisk または PvD コンポーネントがインストールされているかどうかは検出されません。ただし、VDA インストーラーでは、それが検出されます。詳しくは、「PvD または AppDisks コンポーネントを持つ VDA」を参照してください。

サポートされていないホストアイテムを削除する

サイトに Citrix CloudPlatform や Microsoft Azure Classic などのサポートされていないホストタイプへの接続がある場合、バージョン 2006（またはそれ以降のサポートされているバージョン）への展開のアップグレードは続行できません。アップグレードを試みる前に、次のタスクを完了してください。

Studio で以下の操作を行います。

- サポートされていないホストへの接続をすべて削除します。
- デリバリーグループに、サポートされていないホストのマスターイメージで作成されたカタログのマシンが含まれている場合は、それらのマシンをグループから削除します。
- サポートされていないホストのマスターイメージを使用して作成されたカタログをすべて削除します。

PvD または **AppDisks** コンポーネントを持つ **VDA**

PvD および AppDisks テクノロジを有効にするコンポーネントが VDA にインストールされている場合、それらのコンポーネントが削除されるまで、その VDA はアップグレードできません。

> 注:
>
> バージョン 1912 にアップグレードする場合、現在の VDA をアンインストールしてから新しい VDA をインストールする必要がありました。このバージョンでは、Citrix でコンポーネントを削除してアップグレードを続

> 行するかどうかを尋ねられます。

AppDisk および PvD コンポーネントは、これらのテクノロジを使用したことがない場合でも、以前の VDA バージョンにインストールされていることがあります:

- グラフィカルユーザーインターフェイス: VDA インストーラーでは、[追加コンポーネント] ページに［**Citrix AppDisk** または **Personal vDisk**］オプションがあります。7.15 LTSR およびそれ以前の 7.x リリースでは、デフォルトでこのオプションが有効になっています。そのため、デフォルトを変更しない場合（またはこのオプションがあるリリースでオプションを有効にすることを明示的に選択した場合）、そのコンポーネントがインストールされました。
- CLI: `/baseimage`オプションを指定すると、コンポーネントがインストールされました。

必要なアクション　VDA インストーラーが現在インストールされている VDA 内の AppDisks または PvD コンポーネントを検出しない場合、アップグレードは通常どおり続行されます。

インストーラーが現在インストールされている VDA で AppDisks または PvD コンポーネントを検出した場合:

- グラフィカルインターフェイス: アップグレードが一時停止します。サポートされていないコンポーネントを自動的に削除するかどうかを尋ねるメッセージが表示されます。［**OK**］をクリックすると、コンポーネントが自動的に削除され、アップグレードが続行されます。
- CLI: コマンドの失敗を回避するには、コマンドに次のオプションを含めます:
  - `/remove_appdisk_ack`
  - `/remove_pvd_ack`

制限事項

アップグレードには以下の制限があります。

- コンポーネント選択インストール: コンポーネントを新しいバージョンをインストールまたはアップグレードしていて、アップグレードが必要な他のコンポーネント（別のマシン上）をアップグレードしないことを選択している場合、Studio によって確認メッセージが表示されます。たとえば、アップグレードに Controller と Studio の新しいバージョンが含まれるとします。Controller をアップグレードしますが、Studio がインストールされているマシン上でインストーラーを実行しません。Studio をアップグレードするまではサイトを管理できません。

  VDA をアップグレードする必要はありませんが、利用できる機能をすべて使用できるようにするために、すべての VDA をアップグレードすることを Citrix ではお勧めします。
- **Early Release** または **Technology Preview** バージョン: Early Release、Technology Preview、またはプレビューバージョンから、アップグレードすることはできません。

- 以前のオペレーティングシステム上のコンポーネント： Microsoft または Citrix でサポートされなくなったオペレーティングシステムに、現行の VDA をインストールすることはできません。詳しくは、「以前のオペレーティングシステム」を参照してください。
- 混在環境またはサイト：以前のバージョンのサイトと現行バージョンのサイトの実行を継続する必要がある場合は、「混在環境での考慮事項」を参照してください。
- 製品選択：以前のバージョンからアップグレードする場合、インストール時に設定されていた製品（Citrix Virtual Apps または Citrix Virtual Apps and Desktops）を選択または指定しないでください。

混在環境に関する考慮事項

アップグレードするときには、Citrix ではすべてのコンポーネントおよび VDA をアップグレードすることをお勧めします。そうすることにより、そのエディションおよびバージョンで追加および強化された機能をすべて使用できるようになります。

たとえば、以前のバージョンの Controller を含む環境で最新の VDA を使用できますが、最新リリースの新機能を使用できない場合があります。最新でないバージョンを使用すると、VDA 登録で問題が発生する可能性もあります。

環境によっては、すべての VDA を最新バージョンにアップグレードできない場合があります。マシンカタログを作成する際に、マシンにインストールされている VDA バージョンを指定できます（これは機能レベルと呼ばれます）。デフォルトでは、VDA の推奨最小バージョンを指定します。ほとんどの展開では、デフォルト値で十分です。カタログにデフォルトより以前の VDA が含まれている場合にのみ、設定を以前のバージョンに変更することを検討してください。マシンカタログで複数のバージョンの VDA を混在させることは推奨されていません。

デフォルトの最小 VDA バージョンの設定を使用してカタログが作成されていて、デフォルトバージョンより以前の VDA を格納するマシンが複数ある場合は、それらのマシンは Controller に登録できず、動作しません。

詳しくは、「VDA バージョンと機能レベル」を参照してください。

バージョンが異なる複数のサイト

環境内に製品バージョンが異なるサイトがある（たとえば、XenDesktop 7.18 のサイトと Citrix Virtual Apps and Desktops 1909 のサイト）場合は、Citrix では、StoreFront を使用して異なる製品バージョンからアプリケーションとデスクトップを集約することをお勧めします。詳しくは、StoreFrontのドキュメントを参照してください。

混在環境では、異なるバージョンの Studio や Director を同一マシン上にインストールすることはできません。

以前のオペレーティングシステム

コンポーネントの以前のバージョンを、サポートされているオペレーティングシステム（OS）バージョンを実行していたマシンにインストールしたとします。新しいコンポーネントバージョンを使用したい場合でも、現行バージョンのコンポーネントでその OS がサポートされなくなっています。

たとえば、Windows Server 2016 マシンにサーバー VDA をインストールしたとします。VDA を現在のリリースにアップグレードしたいものの、アップグレード後の現在のリリースでは Windows Server 2016 はサポートされていません。

許容されなくなったオペレーティングシステム上にコンポーネントをインストールまたはアップグレードしようとすると、「このオペレーティング システムにはインストールできません。」などのエラーメッセージが表示されます。

以上の考慮事項を、最新リリースおよび長期サービスリリースのバージョンのアップグレードで検討します（LTSR バージョンへの CU の適用には影響しません）。

サポートされている OS については、リンク先を参照してください：

- Citrix Virtual Apps and Desktops（最新リリース）：
  - Delivery Controller、Studio、Director、VDA、ユニバーサルプリントサーバー
  - フェデレーション認証サービス
  - StoreFront、セルフサービスパスワードリセット、およびSession Recordingについては、現行リリースのシステム要件を参照してください。
- LTSR については、LTSR バージョンおよび CU のコンポーネントリストを参照してください（Citrix Virtual Apps and Desktops の製品ドキュメントのメインページで、お使いの LTSR バージョンを選択します）。

無効なオペレーティングシステム

次の表に、現行リリースのコンポーネントのインストールまたはアップグレードに対して有効でない、以前のオペレーティングシステムの一覧を示しています。記載されている各 OS でサポートされている最新の有効なコンポーネントのバージョンと、インストールおよびアップグレードが無効になったときのコンポーネントのバージョンを示しています。

表のオペレーティングシステムには、サービスパックと更新プログラムが含まれています。

オペレーティングシステム	コンポーネント/機能	最新の有効バージョン	インストール/アップグレードが不可能になるバージョン
Windows 7 および Windows 8	VDA	7.15 LTSR	7.16
Windows 7 および Windows 8	その他のインストーラーコンポーネント	7.17	7.18
1607 より前の Windows 10 バージョン	VDA	7.15 LTSR	7.16
Windows 10 x86 のバージョン	VDA	1906.2.0	1909
Windows Server 2008 R2	VDA	7.15 LTSR	7.16

オペレーティングシステム	コンポーネント/機能	最新の有効バージョン	インストール/アップグレードが不可能になるバージョン
Windows Server 2008 R2	その他のインストーラーコンポーネント	7.17	7.18
Windows Server 2012	VDA	7.15 LTSR	7.16
Windows Server 2012	その他のインストーラーコンポーネント	7.17	7.18
Windows Server 2012 R2	その他のインストーラーコンポーネント *	1912 LTSR	2003
Windows Server 2012 R2	サーバー VDI	7.15 LTSR	7.16
Windows Server 2016	サーバー VDI	7.15 LTSR	7.16

Windows XP および Windows Vista は、7.x のコンポーネントまたはテクノロジでは無効です。

* Delivery Controller、Studio、Director、VDA などがあります。

対応の手順

選択肢があります。次の操作を実行できます:

- 現在の OS を引き続き使用する
- マシンを再イメージ化またはアップグレードする
- 新しいマシンを追加してから古いマシンを削除する

現在の **OS** を引き続き使用する　この方法は、VDA では実現可能です。以前の OS のマシンを引き続き使用する場合は、次のいずれかを選択できます。

- インストールされているコンポーネントバージョンを使用し続ける
- 最新の有効なコンポーネントバージョンをダウンロードし、コンポーネントをそのバージョンにアップグレードする（最新の有効なコンポーネントバージョンがまだインストールされていないことを前提としています）

たとえば、Windows 7 SP1 マシンで 7.14 VDA を使用しているとします。Windows 7 OS マシン上で最新の有効な VDA バージョンは、XenApp および XenDesktop 7.15 LTSR です。7.14 を使用し続けるか、または 7.15 LTSR VDA をダウンロードして VDA をそのバージョンにアップグレードします。以前のバージョンの VDA は、新しいバージョンの Delivery Controller がある展開で動作します。たとえば、7.15 LTSR VDA は、Citrix Virtual Apps and Desktops 7 1808 の Controller に接続できます。

マシンを再イメージ化またはアップグレードする　これらの方法は、VDA、およびコアコンポーネント（Delivery Controller など）がインストールされていない他のマシンで実現可能です。次のいずれかのオプションを選択します:

- メンテナンスモードをオンにしてすべてのセッションを終了できるようにして、マシンのサービスを停止した後に、サポートされている Windows OS バージョンにマシンを再イメージ化してから、コンポーネントの最新バージョンをインストールできます。
- 再イメージ化せずに OS をアップグレードするには、OS をアップグレードする前に Citrix ソフトウェアをアンインストールします（これには、OS に対する内部のアップグレードが含まれます。たとえば、Windows 10 バージョン 1903 から Windows 10 バージョン 1909 へのアップグレードなどです）。そうしないと、Citrix ソフトウェアはサポートされなくなります。次に、新しいコンポーネントをインストールします。
- 再イメージ化せずに VDA マシンの OS をアップグレードするには、まずアップグレード先の OS でサポートされているバージョンの VDA をインストールするか、OS のアップグレード後に VDA をアップグレードする必要があります。そうしないと、Citrix ソフトウェアはサポートされなくなります。VDA をアンインストールせずにインプレースアップグレードを実行する場合は、次の最小 OS バージョンにアップグレードできます:
  - Windows 11 向けの 2023-07 累積更新プログラム（KB5028185）以降（ビルド 22621.1992 以降）がインストールされた Windows 11。
  - Windows 10 向けの 2023-07 動的更新プログラム（KB5028311）がインストールされた Windows 10。
- アップグレードする予定の Windows バージョンが前述のガイドラインに準拠していない場合は、OS をアップグレードする前に VDA をアンインストールし、OS のアップグレードが完了した後にサポートされている VDA バージョンをインストールする必要があります。

新しいマシンを追加してから古いマシンを削除する　この方法は、Delivery Controller などのコアコンポーネントがあるマシンで OS をアップグレードする必要がある場合に適しています。

Citrix ではサイト内のすべての Controller が同じ OS であることをお勧めします。次のアップグレードシーケンスでは、複数の Controller の OS が異なる間隔を最小限に抑えています。

1. サイト内のすべての Delivery Controller のスナップショットを作成し、サイトデータベースをバックアップします。
2. サポートされているオペレーティングシステムを搭載したクリーンなサーバーに新しい Delivery Controller をインストールします。
3. 新しい Controller をサイトに追加します。
4. 現行リリースで有効でないオペレーティングシステムを実行している Controller を取り外します。「Delivery Controller」に記載されている、Controller を取り外すための推奨事項に従います。

準備

アップグレードを開始する前に、次の情報を確認し、必要な作業を完了してください。

> 注:
>
> VDA のアップグレードはアップグレード手順の後半で行われますが、アップグレードが開始する前にインストーラーを選択して手順を確認し、行う操作を把握してください。

インストーラーとインターフェイスを選択する

製品 ISO から全製品インストーラーを使用して、コンポーネントをアップグレードします。全製品インストーラーまたはスタンドアロンの VDA インストーラーを使用して、VDA をアップグレードできます。すべてのインストーラーで、グラフィカルおよびコマンドラインインターフェイスが提供されます。

詳しくは、「インストーラー」を参照してください。

インストールの詳細：インストーラーを開始するために必要な準備の完了後は、インストールに関する記事で表示される画面（グラフィカルユーザーインターフェイスを使用している場合）や入力画面（コマンドラインインターフェイスを使用している場合）を確認できます。

- グラフィカルインターフェイスを使用したコアコンポーネントのインストールまたはアップグレード
- コマンドラインを使用したコアコンポーネントのインストールまたはアップグレード
- グラフィカルインターフェイスを使用した VDA のインストールまたはアップグレード
- コマンドラインを使用した VDA のインストールまたはアップグレード

シングルセッション VDA の最初のインストールに`VDAWorkstationCoreSetup.exe`インストーラーを使用した場合は、アップグレードするときもそのインストーラーを使用することを Citrix では推奨しています。全製品 VDA インストーラーまたは`VDAWorkstationSetup.exe`インストーラーを使用して VDA をアップグレードする場合、明示的にアップグレードを省略または除外していない限り、元は除外されていたコンポーネントがインストールされることがあります。

VDA を現行リリースにアップグレードする場合、アップグレード処理中にマシンの再起動が発生します（この要件は 7.17 リリースから導入されました）。この再起動は回避できません。再起動後に、アップグレードが再開されます（コマンドラインで`/noresume`を指定していない場合）。

データベースのアクション

サイト、監視、および Configuration Logging データベースをバックアップします。CTX135207の指示に従います。アップグレード後に問題を検出した場合は、バックアップを回復できます。

サポート対象外となったバージョンの SQL Server のアップグレードについて詳しくは、「SQL Server のバージョンチェック」を参照してください（これは、サイト、モニター、および構成ログデータベースに使用される SQL Server に言及しています）。

ローカルホストキャッシュ機能と連携して使用するために、自動で Microsoft SQL Server Express LocalDB がインストールされます以前のバージョンを置き換える必要がある場合、新しいバージョンは SQL Server Express LocalDB 2019 であることが必要です。コンポーネントとサイトのアップグレード後に、SQL Server Express

LocalDB を新しいバージョンに置き換える方法については、「SQL Server Express LocalDB の置き換え」を参照してください。

Citrix ライセンスが最新であることを確認する

Citrix ライセンスの管理に関する総合的な情報は、「Citrix ライセンスのアクティブ化、アップグレード、管理」を参照してください。

全製品インストーラーを使用して、ライセンスサーバーをアップグレードできます。または、ライセンスコンポーネントを個別にダウンロードしてアップグレードすることもできます。「アップグレード 」を参照してください。

アップグレードする前に、Customer Success Services / Software Maintenance / Subscription Advantage 日が新しい製品バージョンに対して有効であることを確認してください。日付は少なくとも 2021.11.15 である必要があります。

Citrix ライセンスサーバーに互換性があることを確認してください

Citrix ライセンスサーバーに新しいバージョンとの互換性があることを確認します。次のいずれかの方法を使用します:

- 他の Citrix コンポーネントをアップグレードする前に、Delivery Controller があるマシンで ISO ファイルに収録されている`XenDesktopServerSetup.exe`インストーラーを実行します。互換性に問題がある場合は、問題を解決するための推奨手順がインストーラーから提示されます。
- インストールメディアの`XenDesktop Setup`ディレクトリから、次のコマンドを実行します: `.\LicServVerify.exe -h <license-server-fqdn> -p 27000 -v`。ライセンスサーバーに互換性があるかどうかが表示されます。ライセンスサーバーに互換性がない場合は、ライセンスサーバーをアップグレードします。

StoreFront の変更のバックアップ

アップグレードを開始する前に、*default.ica* や *usernamepassword.tfrm* など、`C:\inetpub\wwwroot\Citrix\<StoreName>\App_Data`のファイルを変更した場合は、ストアごとにバックアップを作成します。アップグレード後はそれらを復元して、変更内容を元に戻すことができます。

アプリケーションとコンソールを閉じる

アップグレードを開始する前に、管理コンソールや PowerShell セッションなど、ファイルのロックの原因になりうるすべてのプログラムを終了してください。

マシンを再起動すると、ロックされているファイルや保留中の Windows 更新プログラムがない状態になります。

アップグレードの開始前に、サードパーティの監視エージェントサービスを停止し、無効にしてください。

適切な権限があることを確認する

製品コンポーネントをアップグレードするには、ドメインユーザーであることに加えて、そのマシンのローカル管理者である必要があります。

サイトデータベースおよびサイトは、自動または手動でアップグレードできます。データベースの自動アップグレードでは、SQL Server データベーススキーマを更新できる権限（`db_securityadmin`または`db_owner`データベースロールなど）が Studio ユーザーに必要です。詳しくは、「データベース」を参照してください。

Studio ユーザーにこれらの権限がない場合は、データベースの手動アップグレードを開始するとスクリプトが生成されます。Studio ユーザーは Studio が生成したスクリプトをいくつか実行します。データベース管理者は、SQL Server Management Studio などのツールを使用して、その他のスクリプトを実行します。

その他の準備作業

- 必要に応じて、テンプレートをバックアップし、ハイパーバイザーをアップグレードします。
- 他の準備タスクが事業継続計画に記載されていれば、それも完了します。

事前サイトテスト

Delivery Controllers およびサイトをアップグレードする場合は、実際のアップグレードが開始される前に事前サイトテストが実行されます。このテストでは、次のことが確認されます：

- サイトデータベースにアクセスでき、バックアップされている
- 基本的な Citrix サービスへの接続が正しく機能している
- Citrix ライセンスサーバーのアドレスが使用可能である
- 構成ログデータベースにアクセスできる
- パブリッククラウドホスト接続（AWS など）を追加する場合は、ハイブリッド権利ライセンスがあることを確認してください。そうしないと、事前のサイトテストが一時停止または停止し、説明メッセージが表示されます。

テストの実行後に、その結果のレポートを表示できます。検出された問題を修正し、テストを再実行できます。事前サイトテストを実行して問題を解決できない場合、サイトの仕組みに影響を与える可能性があります。

テスト結果が含まれているレポートは、インストールログと同じディレクトリにある HTML ファイル（`PreliminarySiteTestResult.html`）です。そのファイルが存在しない場合は作成されます。ファイルが存在する場合は、その内容が上書きされます。

テストの実行

- インストーラーのグラフィカルインターフェイスを使用してアップグレードする場合、ウィザードにはテストを開始してレポートを表示できるページがあります。テストの実行後、レポートを表示して見つかった問題が

解決されたら、テストを再実行できます。テストが正常に完了したら、［次へ］をクリックしてウィザードを続行します。
- コマンドラインインターフェイスを使用してアップグレードする場合、テストは自動的に実行されます。デフォルトでは、テストが失敗した場合、アップグレードは実行されません。レポートを表示して問題を解決したら、コマンドを再実行します。

Citrix では Controller およびサイトのアップグレードを続行する前に、事前サイトテストを実行して問題を解決しておくことをお勧めします。テストを実行する時間に比べて十分な利点があります。ただし、この推奨アクションは無効にできます。

- グラフィカルインターフェイスを使用してアップグレードする場合、テストをスキップしてアップグレードを続行できます。
- コマンドラインでアップグレードする場合、テストはスキップできません。デフォルトでは、サイトテストが失敗すると、インストーラーが失敗し、アップグレードは実行されません。ほとんどの場合、`/ignore_site_test_failure`オプションが含まれているとサイトテストの失敗は無視され、アップグレードが進行します（例外については、「SQL Server のバージョンチェック」を参照してください）。

複数の **Controller** をアップグレードする場合

1 つの Controller でアップグレードを開始した後、（最初のアップグレードが完了する前に）同じサイトの別の Controller のアップグレードを開始した場合：

- 最初の Controller で事前サイトテストが完了した場合、他の Controller のウィザードに事前サイトテストページは表示されません。
- 他の Controller でアップグレードを開始したときに、最初の Controller でテストが進行中の場合、他の Controller のウィザードにサイトテストページが表示されます。ただし、最初の Controller のテストが終了すると、最初の Controller のテスト結果のみが保持されます。

サイトの正常性に関係しないテストの失敗

- メモリ不足のために事前サイトテストが失敗した場合は、使用可能なメモリを増やしてからテストを再実行してください。
- ユーザーにアップグレードの権限があり、サイトテストを実行していない場合は、事前サイトテストが失敗します。これを解決するには、テストを実行する権限を持つユーザーアカウントでインストーラーを再実行します。

SQL Server のバージョンチェック

正常な Citrix Virtual Apps and Desktops 展開では、Microsoft SQL Server のバージョンがサイト、モニター、構成ログデータベースでサポートされている必要があります。サポート対象外のバージョンの SQL Server で Citrix 展開をアップグレードすると、機能的な問題が発生する可能性があり、サイトがサポートされなくなります。

アップグレードする Citrix リリースでサポートされている SQL Server のバージョンについては、「システム要件」で対象リリースについて参照してください。

Controller をアップグレードする場合、サイト、モニター、構成ログデータベースで使用する現在インストールされている SQL Server のバージョンを Citrix インストーラーがチェックします。

- 現在インストールされている SQL Server のバージョンがアップグレードする Citrix リリースでサポートされたバージョンではないと判断した場合:
  - グラフィカルインターフェイス: メッセージが表示されアップグレードが停止します。[**I understand**]、[**Cancel**] を順にクリックして Citrix インストーラーを閉じます（アップグレードを続行することはできません）。
  - コマンドラインインターフェイス:（コマンドに/`ignore_db_check_failure`オプションが含まれていても）コマンドは失敗します。

  SQL Server のバージョンをアップグレードした後、再度 Citrix アップグレードを開始します。
- チェックで現在インストールされている SQL Server のバージョンが判断できなかった場合、アップグレードするバージョンで現在インストールされているバージョンがサポートされているかを確認してください（「システム要件」）。
  - グラフィカルインターフェイス: メッセージが表示されアップグレードが停止します。
    - 現在インストールされている SQL Server のバージョンがサポートされている場合、[**I understand**] をクリックしてメッセージを閉じ、[**Next**] をクリックして Citrix アップグレードを続行します。
    - 現在インストールされている SQL Server のバージョンがサポートされていない場合、[**I understand**] をクリックしてメッセージを閉じ、[**Cancel**] をクリックして Citrix アップグレードを終了します。SQL Server のバージョンをサポート対象のバージョンにアップグレードした後、再度 Citrix アップグレードを開始します。
  - コマンドラインインターフェイス: メッセージが表示され、コマンドは失敗します。メッセージを閉じた後:
    - 現在インストールされている SQL Server のバージョンがサポートされている場合は、/`ignore_db_check_failure`オプションで再度コマンドを実行します。
    - 現在インストールされている SQL Server のバージョンがサポートされていない場合、サポートされているバージョンにアップグレードしてください。再度コマンドを実行して Citrix アップグレードを開始します。

SQL Server のアップグレード

新しい SQL Server を起動してサイトデータベースを移行する場合、接続文字列を更新する必要があります。

サイトが現在、SQL Server Express（サイト作成時に Citrix 製品により自動的にインストールされる）を使用している場合:

1. 最新の SQL Server Express バージョンをインストールします。
2. データベースを接続解除します。
3. 新しい SQL Server Express にデータベースを接続します。
4. 接続文字列を移行します。

詳しくは、「接続文字列の構成」および Microsoft SQL Server の製品ドキュメントを参照してください。

SQL Server Express LocalDB の置き換え

Microsoft SQL Server Express LocalDB は、ローカルホストキャッシュがスタンドアロンで使用する SQL Server Express の機能です。ローカルホストキャッシュでは、SQL Server Express LocalDB 以外の SQL Server Express のコンポーネントは必要ありません。

Delivery Controller の 1912 より前のバージョンをインストールしてから、バージョン 1912 以降にアップグレードすると、SQL Server Express LocalDB のバージョンは Citrix により自動的にアップグレードされません。なぜでしょうか。それは、SQL Server Express LocalDB に依存する Citrix 以外のコンポーネントがある可能性があるためです。SQL Server Express LocalDB を使用している Citrix 以外のコンポーネントがある場合は、SQL Server Express LocalDB のアップグレードでこれらのコンポーネントが中断されないことを確認してください。SQL Server Express LocalDB のバージョンをアップグレード（リプレース）するには、このセクションのガイダンスに従ってください。

- **Delivery Controller** を **Citrix Virtual Apps and Desktops** バージョン **1912** または **2003** にアップグレードする場合：SQL Server Express LocalDB のアップグレードはオプションです。SQL Server Express LocalDB をアップグレードするかどうかにかかわらず、ローカルホストキャッシュは機能を失うことなく、正常に動作します。Microsoft の SQL Server Express LocalDB 2014 サポートの終了に関する懸念がある場合のために、SQL Server Express LocalDB の新しいバージョンに移行するオプションを追加しました。
- **Delivery Controller** を **Citrix Virtual Apps and Desktops 2003** より新しいバージョンにアップグレードする場合：サポートされるバージョンは、SQL Server Express LocalDB 2019 です。バージョン 1912 より前のバージョンの Delivery Controller をインストールし、SQL Server Express LocalDB を新しいバージョンに置き換えていない場合は、データベースソフトウェアを今すぐ置き換える必要があります。置き換えない場合、ローカルホストキャッシュは機能しません。

必要な準備：

- （アップグレードするバージョンの）Citrix Virtual Apps and Desktops インストールメディア。メディアには Microsoft SQL Server Express LocalDB 2019 のコピーが含まれています。
- Windows Sysinternals ツールを Microsoft サイトからダウンロード。

手順：

1. Citrix Virtual Apps and Desktops コンポーネント、データベース、サイトのアップグレードを完了します（これらのアップグレードによって、サイトデータベース、監視データベース、構成ログデータベースが影響を

受けます。SQL Server Express LocalDB を使用するローカルホストキャッシュデータベースは影響を受けません)。

2. Microsoft サイトから Delivery Controller にPsExecをダウンロードします。Microsoft のドキュメント「PsExec v2.2」を参照してください。
3. Citrix High Availability Service を停止します。
4. コマンドプロンプトでPsExecを実行し、Network Service アカウントに切り替えます。

   ```
   psexec -i -u "NT AUTHORITY\NETWORKSERVICE"cmd
   ```

   必要な場合、whoamiを使用してコマンドプロンプトが Network Service アカウントとして動作しているかを確認できます。

   ```
   whoami
   ```

   ```
   nt authority\networkservice
   ```

5. SqlLocalDB が含まれるフォルダーに移動します。

   ```
   cd "C:\Program Files\Microsoft SQL Server\120\Tools\Binn"
   ```

6. CitrixHA（LocalDB）を停止して削除します。

   ```
   SqlLocalDB stop CitrixHA
   ```

   ```
   SqlLocalDB delete CitrixHA
   ```

7. C:\Windows\ServiceProfiles\NetworkServiceで関連ファイルを削除します。

   ```
   1 HADatabaseName.*
   2 HADatabaseName_log.*
   3 HAImportDatabaseName.*
   4 HAImportDatabaseName_log.*
   ```

   ヒント: 展開にHAImportDatabaseName.*およびHAImportDatabaseName_log.*が含まれていないことがあります。

8. Windows のプログラムを削除する機能でサーバーから SQL Server Express LocalDB 2014 をアンインストールします。
9. SQL Server Express LocalDB 2019 をインストールします。Citrix Virtual Apps and Desktops インストールメディアのSupport > SQLLocalDBフォルダーでsqllocaldb.msiをダブルクリックします。インストールを完了するために、再起動が要求されることがあります。（新しい SQLLocalDB はC:\Program Files\Microsoft SQL Server\150\Tools\Binnにあります。）
10. Citrix High Availability Service を起動します。
11. 各 Delivery Controller にローカルホストキャッシュデータベースが作成されていることを確認します。これにより、必要に応じて High Availability Service（セカンダリブローカー）が処理を引き継げるようになります。

- Controller サーバーで、C:\Windows\ServiceProfiles\NetworkServiceに移動します。
- HaDatabaseName.mdfおよびHaDatabaseName_log.ldfが作成されたことを確認します。

VDA Upgrade Agent のプロキシサポート

July 4, 2024

VDA Upgrade Agent のプロキシサポートが 2311 VDA に追加されました。

2311 VDA 以降の VDA Upgrade Agent（つまりバージョン 7.40）は、プロキシ経由でトラフィックを認識し、送信できます。

VDA Upgrade Agent（VUA）は、「ホスト名: ポート（IP: ポート）」の形式および PAC ファイルでプロキシをサポートします。

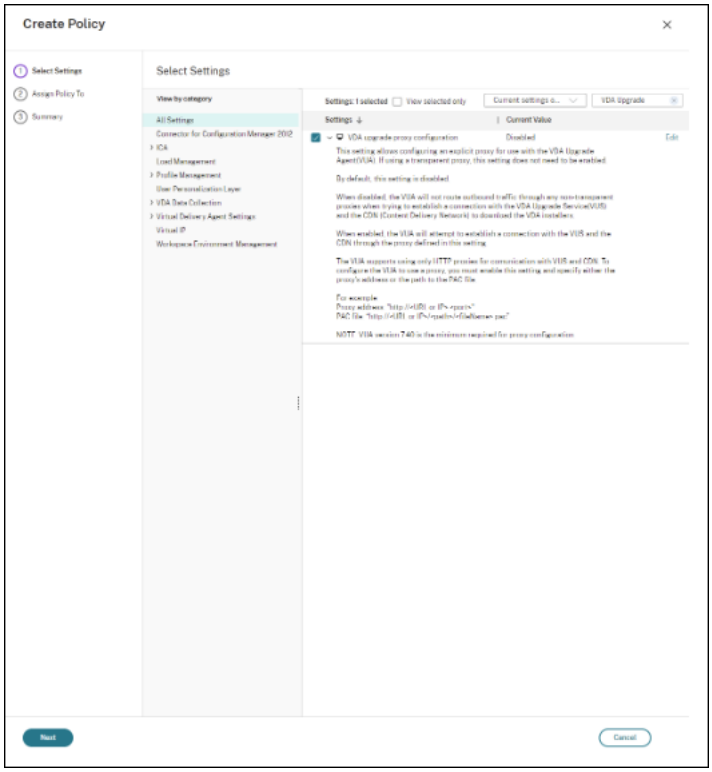
HTTP プロキシのみがサポートされています。
パケットの暗号化解除と検査はサポートされていません。

プロキシ認証はサポートされていません。
SOCKS5 はサポートされていません。

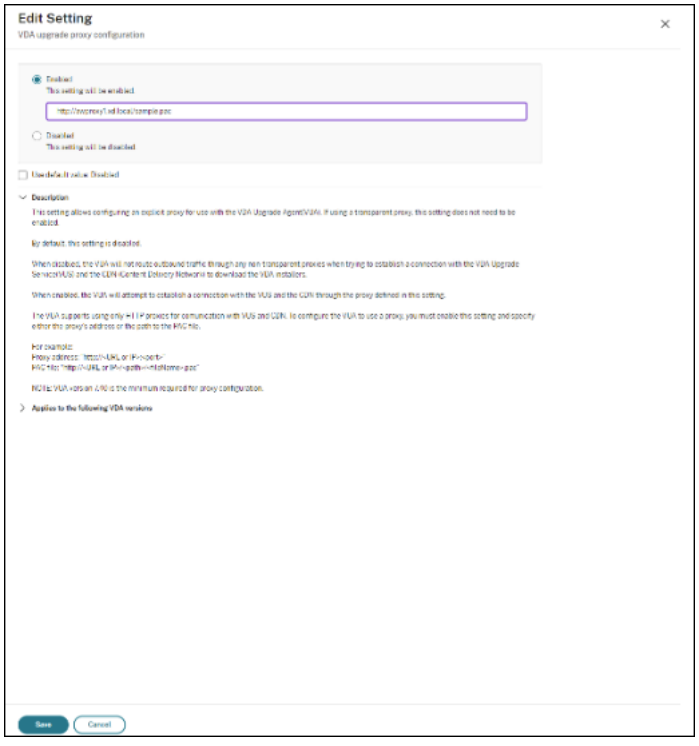
VDA Upgrade Agent プロキシの構成

VDA Upgrade Agent プロキシは、次の 2 つの方法で構成できます:

1. **Webstudio** ポリシーを使用して **VDA Upgrade Agent** ポリシーを構成します。
2. ［ポリシーの作成］ページの ［設定］から ［**VDA upgrade proxy configuration**］を選択します。



3. 設定を有効にします。この設定は、デフォルトでは、無効になっています。



4. レジストリキーを使用して VDA Upgrade Agent を構成します。

   VDA のインストール中にレジストリ キーがメタインストーラーに設定されます。

レジストリ:

キー: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\VirtualDesktopAgent

値の種類: 文字列

値の名前: ProxySettings

値のデータ: プロキシアドレスまたは PAC ファイルへのパス。

たとえば、次のように設定します:

a) プロキシアドレス: http://<URL or IP>:<port>
b) PAC ファイル: http://<URL or IP>/<path/<filename>.pac

構成のバックアップまたは移行

July 4, 2024

この機能は、DaaS の構成のバックアップを作成するのに役立ちます。バックアップにより、あるクラウドサイトから別のクラウドサイトに構成を移行するプロセスが容易になります。また、緊急時にサイトをすぐに回復することもできます。
次の方法を使用してバックアップを作成できます:

1. バックアップと復元
    a) WebStudio に統合されました。
2. 自動構成ツール (ACT)
    a) Powershell ベースのツール。このツールをインストールして使用します。

バックアップは次の用途に使用できます:

1. 復元
2. 移行

Citrix では、ユースケースごとに次のツールの使用を推奨します。

バックアップ

環境	使用例	推奨ツール	特別な考慮事項	リンク
DaaS	オンデマンドおよびスケジュールされたバックアップ	バックアップと復元	Citrix がバックアップを保持しており、ユーザーは必要に応じてダウンロードできます	バックアップ + Studio で復元
オンプレミス	オンデマンドバックアップ	ACT	ユーザーがバックアップを保持します	バックアップと自動構成ツールを使用した復元

移行

環境	使用例	推奨ツール	特別な考慮事項	リンク
オンプレミスからクラウドへ	1 つのオンプレミスサイトを DaaS に移行	ACT		オンプレミスからクラウドへの移行
	複数のオンプレミスサイトを 1 つの DaaS サイトに統合	ACT	サイトマージ	1 つのクラウドサイトへの複数のオンプレミスサイトのマージ
オンプレミスからオンプレミスへ	1 つのオンプレミスサイトを別のオンプレミスサイトに移行	ACT		概念実証ガイド：自動構成ツール - オンプレミスからオンプレミスへの移行
	複数のオンプレミスサイトを別のオンプレミスサイトに統合	ACT	サイトマージ	概念実証ガイド：自動構成ツール - オンプレミスからオンプレミスへの移行 1 つのクラウドサイトへの複数のオンプレミスサイトのマージ
クラウドからクラウドへ	1 つの DaaS サイトを別の DaaS サイトに移行	ACT		クラウドからクラウドへの移行

環境	使用例	推奨ツール	特別な考慮事項	リンク
複数の DaaS サイトを 1 つの DaaS サイトに統合	ACT	サイトマージ		クラウドからクラウドへの移行 複数のオンプレミスサイトを 1 つのクラウドサイトに移行

セキュリティ

August 17, 2024

Citrix Virtual Apps and Desktops では、セキュリティニーズに合わせて環境をカスタマイズできる、セキュアバイデザイン（セキュリティに配慮した設計）ソリューションが提供されます。

モバイルワーカーへの対応で IT 部門が直面するセキュリティ上の問題に、データの紛失や盗難があります。Citrix Virtual Apps and Desktops では、アプリケーションとデスクトップがホストされ、すべてのデータがデータセンターに保持されるため、機密データや知的財産がエンドポイントデバイスから安全に分離されます。データ転送を許可するポリシーを有効にしている場合でも、すべてのデータが暗号化されます。

また、Citrix Virtual Apps and Desktops のデータセンターでは、一元的な監視と管理サービスを利用できるため、インシデント対応が容易になります。Director では、ネットワーク経由でアクセスされたデータを監視して分析できます。また、Studio ではデータセンターにパッチを適用して多くの脆弱性を解決できるため、エンドユーザーデバイスごとにローカルで問題を解決する必要がありません。

Citrix Virtual Apps and Desktops では、一元化された監査記録を使用して、どのアプリケーションやデータにどのユーザーがアクセスしたかを判別できるため、監査と法規制順守も簡素化されます。Director では、構成ログと OData API にアクセスして、システムに適用された更新とユーザーのデータ使用状況に関する履歴データが収集されます。

委任管理によって、管理者の役割を設定して、Citrix Virtual Apps and Desktops へのアクセスを詳細に制御できます。これにより、ほかの管理者のアクセス権は制限したままで、特定の管理者に対してタスク、操作、およびスコープへの完全なアクセス権を組織内で柔軟に付与できます。

Citrix Virtual Apps and Desktops では、ローカルレベルから組織単位レベルまで、ネットワークのさまざまなレベルでポリシーを適用してユーザーを制御できます。このポリシー制御によって、ユーザー、デバイス、またはユーザーやデバイスのグループが実行できる操作（接続、印刷、コピーと貼り付け、ローカルドライブのマップ）を指定できるため、社外作業者に対するセキュリティ上の問題を最小限に抑えることができます。Desktop Lock 機能を使用すると、エンドユーザーデバイスのローカルのオペレーティングシステムにアクセスできないようにして、エンドユーザーによる使用を仮想デスクトップのみに制限することも可能です。

管理者は、Controller で、またはエンドユーザーと VDA（Virtual Delivery Agent）間で TLS（Transport Layer Security）プロトコルが使用されるように構成して、Citrix Virtual Apps または Citrix Virtual Desktops のセキュリティを強化できます。このプロトコルを有効にして、TCP/IP 接続に対してサーバー認証、データストリームの暗号化、およびメッセージの整合性チェックが行われるようにすることもできます。

さらに、Citrix Virtual Apps and Desktops では、Windows や特定のアプリケーションでの複数要素認証がサポートされています。多要素認証を使用して、Citrix Virtual Apps and Desktops で配信されるすべてのリソースを管理することもできます。以下の認証方法を使用できます：

- トークン
- スマートカード
- RADIUS
- kerberos
- 生体認証

Citrix Virtual Desktops は、ID 管理からウイルス対策ソフトウェアまで、さまざまなサードパーティセキュリティソリューションを統合できます。サポートされている製品の一覧については、http://www.citrix.com/readyを参照してください。

Citrix Virtual Apps and Desktops の一部リリースは、情報セキュリティ国際評価基準（コモンクライテリア）の認定を受けています。これらの基準の一覧については、https://www.commoncriteriaportal.org/cc/を参照してください。

FIDO2 および WebAuthn 認証

August 17, 2024

FIDO2 および WebAuthn を使用したローカル認証と仮想認証

ユーザーは、TPM 2.0 および Windows Hello を搭載したデバイスで FIDO2 セキュリティキーまたは統合された生体認証を使用することで、仮想セッションで FIDO2 または WebAuthn を活用するアプリケーションに認証できます。

FIDO2 について詳しくは、「FIDO2: WebAuthn & CTAP」を参照してください。

この機能の使用について詳しくは、「FIDO2 リダイレクト」を参照してください。

> 注
>
> この機能は、WebAuthn または FIDO2 を使用した仮想セッションへのログインをサポートしていないことに

> 注意してください。仮想セッション内のアプリケーションでのみこれらの認証方法を使用できます。
>
> この機能は、ダブルホップのシナリオではサポートされません。

サポートに関するマトリックス

セッションホストのオペレーティングシステム	Web アプリケーション認証	UWP アプリケーションの認証
Windows Server 2016	USB リダイレクト経由でサポート	未サポート
Windows Server 2019	サポート対象	未サポート
Windows Server 2022	サポート対象	サポート対象
Windows 10	サポート対象	サポート対象
Windows 11	サポート対象	サポート対象

追加情報については、以下の要件をご確認ください。

Web アプリケーション認証

要件

Web アプリケーションで FIDO2 および WebAuthn 認証を使用するための要件は次のとおりです:

Citrix コントロールプレーン

- Citrix Virtual Apps and Desktops 2009 以降

セッションホスト

- オペレーティングシステム
  - Windows 10 1809 以降
  - Windows Server 2019 以降
- VDA
  - Windows: バージョン 2009 以降

クライアントデバイス

- オペレーティングシステム
  - Windows 10 1809 以降
  - Linux：Linux のシステム要件については、Workspace アプリを参照してください。
- Workspace アプリ
  - Windows：バージョン 2009.1 以降
  - Linux：2303 以降

Web ブラウザーの要件

- 64 ビットブラウザーのみ

サポートされている認証方法

- FIDO2 セキュリティキー
- Windows Hello
  - TPM 2.0
  - 統合された生体認証
    - 顔認識
    - 指紋スキャナー
  - WebAuthn

UWP アプリケーションの認証

Citrix Virtual Apps and Desktops 2112 のリリースから、UWP アプリケーションで、WebAuthn および FIDO2 がサポートされます。

Microsoft Teams、Microsoft Outlook for Office 365、OneDrive などのアプリケーションは、Azure Active Directory へのリンクとして認証に UWP アプリケーションを使用します。Citrix は、FIDO2 を使用したこれらのアプリケーションの認証をサポートします。

要件

UWP アプリケーションで FIDO2 および WebAuthn 認証を使用するための要件は次のとおりです：

Citrix コントロールプレーン

- Citrix Virtual Apps and Desktops 2112 以降

セッションホスト

- オペレーティングシステム
  - Windows 10 1809 以降
  - Windows Server 2022 以降
- VDA
  - Windows：バージョン 2112 以降

クライアントデバイス

- オペレーティングシステム
  - Windows 10 1809 以降
  - Linux：Linux のシステム要件については、Workspace アプリを参照してください。
- Workspace アプリ
  - Windows：バージョン 2009.1 以降
  - Linux：2303 以降

サポートされている認証方法

- FIDO2 セキュリティキー
- Windows Hello
  - TPM 2.0
  - 統合された生体認証
    - 顔認識
    - 指紋スキャナー
  - WebAuthn

> 注：
>
> FIDO2 リダイレクトがクライアント、VDA、またはオペレーティングシステムでサポートされていないために利用できない場合は、USB リダイレクトを使用することで、USB ベースの FIDO2 キーをリダイレクトすることができます。
> また、FIDO2 リダイレクトが利用可能な場合でも、USB リダイレクトの使用による USB ベースの FIDO2 キーのリダイレクトは、行うことができます。ただし、その場合、FIDO2 リダイレクトを無効にし、必要な USB リダイレクト規則を構成しておく必要があります。
> USB リダイレクト規則を使用した FIDO2 キーの構成方法について詳しくは、USB redirection device rulesに関するドキュメントを参照してください。

msedgewebview2.exe ベースのアプリケーションの詳細な構成

> 注:
>
> レジストリエディターの使用を誤ると、深刻な問題が発生する可能性があり、オペレーティングシステムの再インストールが必要になる場合もあります。レジストリエディターの誤用による障害に対して、Citrix では一切責任を負いません。
> レジストリエディターは、お客様の責任と判断の範囲でご使用ください。また、レジストリファイルのバックアップを作成してから、レジストリを編集してください。

msedgewebview2.exe ベースの Web アプリケーションを持つ企業の場合、HDX セッション内で FIDO2 リダイレクトが機能するには、VDA にさらにレジストリ値を追加する必要があります -

AllowedProcesses レジストリ値に msedgewebview2.exe のフルパスを追加します:

- キー: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\WebAuthnAllowedProcesses
- 値の名前: AllowedProcesses
- 値の種類: REG_MULTISZ
- 値のデータ: <add full path of the msedgewebview2.exe here >

64 ビットアプリケーションの場合、次の値を設定する必要があります:

- キー:HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxHook\AppInit_DLLs\CtxWebAuthnHook\msedgewebvie
- キー: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxHook\AppInit_DLLs\CtxWebAuthnHook
- 値の名前: FilePathName
- 値の種類: REG_SZ
- 値のデータ: C:\Program Files\Citrix\HDX\bin\CtxWebAuthnHook.dll
- キー: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxHook\AppInit_DLLs\CtxWebAuthnHook
- 値の名前: Flag
- 値の種類: DWORD
- 値データ: 00000002

32 ビットアプリケーションの場合、次の値を設定する必要があります:

- キー:HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\CtxHook\AppInit_DLLs\CtxWebAuthnHook
- キー:HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\CtxHook\AppInit_DLLs\CtxWebAuthnHook
- 値の名前: FilePathName
- 値の種類: REG_SZ
- 値のデータ: C:\Program Files\Citrix\HDX\bin\CtxWebAuthnHook.dll

- キー：HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\CtxHook\AppInit_DLLs\CtxWebAuthnHook
- 値の名前：Flag
- 値の種類：DWORD
- 値データ：00000002

msedgewebview2.exe ベースのアプリケーションで FIDO2 リダイレクトを有効にするためにレジストリ値を設定した後、VDA を再起動します。

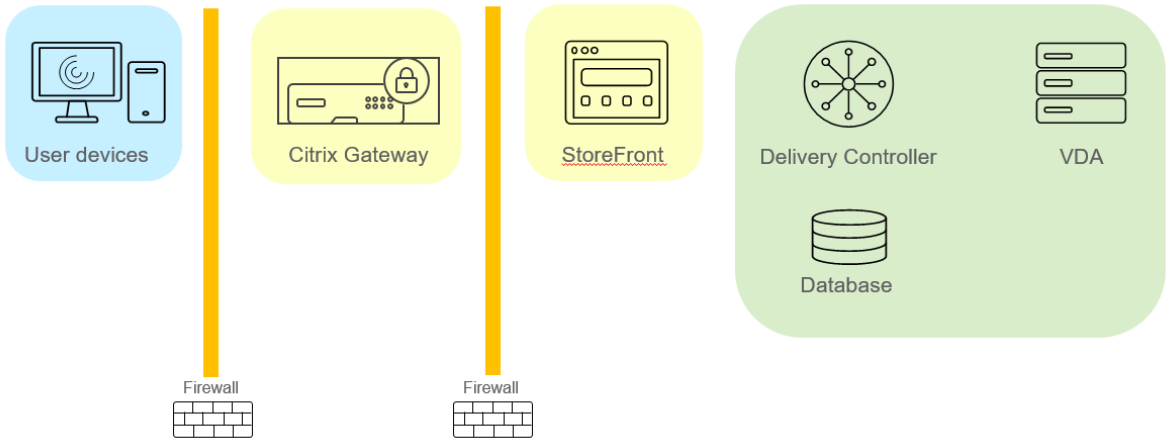
Citrix Virtual Apps and Desktops と Citrix Gateway の統合

August 17, 2024

公開リソースおよびデータへのアクセスを管理するには、StoreFront サーバーを展開および構成します。リモートアクセスの場合は、Citrix Gateway を StoreFront の前に追加することをお勧めします。

> 注：
>
> Citrix Virtual Apps and Desktops を Citrix Gateway と統合する構成手順については、StoreFront のドキュメントを参照してください。

次の図に、Citrix Gateway を含む簡略化された Citrix の展開例を示します。Citrix Gateway は StoreFront と通信して、Citrix Virtual Apps and Desktops が配信するアプリやデータを保護します。ユーザーデバイスは Citrix Workspace アプリを実行してセキュリティで保護された接続を構築し、アプリ、デスクトップ、ファイルにアクセスします。



ユーザーは、Citrix Gateway を使用してログオンおよび認証を行います。Citrix Gateway は、DMZ で展開およびセキュリティ保護されます。2 要素認証が構成されます。ユーザーの資格情報に基づいて、ユーザーに該当のリソースおよびアプリケーションが提供されます。アプリケーションとデータは適切なサーバー上に存在します（図には表示されていません）。セキュリティ上機微なアプリケーションとデータについては、別のサーバーが使用されます。

セキュリティに関する考慮事項およびベストプラクティス

August 17, 2024

> 注:
>
> 組織によっては、法的規制の要件を満たすために特定のセキュリティ基準への準拠が要求される場合があります。このようなセキュリティ基準は変更されることがあるため、ここでは説明しません。セキュリティ標準と Citrix 製品に関する最新情報については、「http://www.citrix.com/security/」を参考にしてください。

セキュリティに関する推奨事項

セキュリティパッチを適用して、環境内にあるすべてのマシンを最新の状態にします。この製品の利点の 1 つは、シンクライアントをターミナルとして使用することによってこの作業を簡略化できることです。

環境内にあるすべてのマシンを、アンチウイルスソフトウェアで保護します。

プラットフォーム特定のアンチマルウェアソフトウェアの使用を検討します。

ソフトウェアをインストールするときは、指定されたデフォルトパスにインストールします。

- 指定されたデフォルトパス以外のファイルの場所にソフトウェアをインストールする場合は、権限を制限するなどさらにセキュリティ対策をファイルの場所に追加することを検討してください。

すべてのネットワーク通信が正しく保護され、セキュリティポリシーに従って暗号化されている必要があります。IPSec を使用して、Microsoft Windows コンピューターの間でのすべての通信を保護できます。その方法について詳しくは、使用するオペレーティングシステムのドキュメントを参照してください。さらに、ユーザーデバイスとデスクトップ間の通信は、デフォルトで 128 ビット暗号化を行う Citrix SecureICA で保護できます。SecureICA は、デリバリーグループの作成または更新時に設定できます。

> 注:
>
> Citrix SecureICA は、ICA/HDX プロトコルの一部ですが、Transport Layer Security（TLS）のような標準に準拠したネットワークセキュリティプロトコルではありません。TLS を使用して、ユーザーデバイスとデスクトップ間のネットワーク通信を保護することもできます。TLS を構成する方法については、「Transport Layer Security（TLS）」を参照してください。

Windows ベストプラクティスをアカウント管理に適用します。Machine Creation Services または Provisioning Services によって複製される前に、アカウントをテンプレートやイメージに作成しないでください。保存された、権限が付与されているドメインアカウントを使用して、タスクをスケジュールしないでください。共有 Active Directory マシンアカウントを手動で作成しないでください。こうすることにより、ローカルの永続アカウントのパスワードがマシンへの攻撃によって取得され、他者所有の MCS/PVS 共有イメージへのログオンに使用されるのを阻止することができます。

ファイアウォール

環境内にあるすべてのマシンを、境界ファイアウォール（必要に応じてエンクレーブ境界を含む）で保護します。

環境内にあるすべてのマシンは、パーソナルファイアウォールで保護する必要があります。コアコンポーネントと VDA をインストールするときに Windows Firewall サービスが検出された場合は（ファイアウォールが無効であったとしても）、コンポーネントと機能の通信に必要なポートが自動的に開放されるように設定できます。また、それらのファイアウォールポートを手作業で構成することもできます。Windows 以外のファイアウォールを使用している場合は、手作業でファイアウォールを構成する必要があります。

従来の環境を新しいバージョンに移行する場合は、既存の境界ファイアウォールを移動するか、新しい境界ファイアウォールを追加する必要があります。たとえば、従来のクライアントとデータセンター内のデータベースサーバーとの間に境界ファイアウォールがあるとします。このリリースを使用するときは、仮想デスクトップおよびユーザーデバイスと、データセンター内のデータベースサーバーおよび Delivery Controller との間に境界ファイアウォールを設定する必要があります。したがって、データベースサーバーと Controller を含むエンクレーブをデータセンター内に作成することを検討します。また、ユーザーデバイスと仮想デスクトップ間のセキュリティについても考慮する必要があります。

> 注:
>
> TCP ポート 1494 および 2598 は ICA および CGP に使用され、ファイアウォールで開放されているため、データセンター外のユーザーはこれらのポートにアクセスできます。管理インターフェイスが不注意で開いたままになって攻撃を受ける可能性を避けるため、Citrix ではこれらの TCP ポートをほかの目的で使用しないでください。ポート 1494 および 2598 は、Internet Assigned Number Authority（http://www.iana.org/）に正規登録されています。

アプリケーションのセキュリティ

管理者以外のユーザーが悪意のある操作を実行するのを防ぐために、VDA ホストとローカル Windows クライアントで、インストーラー、アプリケーション、実行可能ファイル、スクリプトに対して Windows AppLocker の規則を構成することをお勧めします。

ユーザー権限の管理

ユーザーには、必要な権限だけを付与します。デスクトップのユーザーには、Microsoft Windows での権限（グループポリシーの［ユーザー権利の割り当て］およびグループメンバーシップ）がそのまま適用されます。このリリースの利点の 1 つは、仮想デスクトップが格納されているコンピューターに対する物理的な制御を許可せずに、デスクトップに対するユーザーの管理権限を付与できることです。

デスクトップ権限を計画するときは、以下の点に注意してください。

- デフォルトでは、権限を持たないユーザーがデスクトップに接続すると、ユーザーデバイスのタイムゾーンではなく、そのデスクトップを実行しているシステムのタイムゾーンが表示されます。デスクトップの使用時に

ローカルの時刻が表示されるようにする方法については、「デリバリーグループの管理」を参照してください。

- デスクトップの管理者権限を持つユーザーは、そのデスクトップを完全に制御することができます。デスクトップが専用デスクトップではなくプールデスクトップの場合、管理者権限を持つユーザーはそのデスクトップのすべてのユーザー（将来のユーザーを含む）に信頼されている必要があります。このため、プールデスクトップのすべてのユーザーは、この状況によってデータのセキュリティに永続的な危険性が存在することを認識する必要があります。これは、1 人のユーザーに対してのみ割り当てられるデスクトップには当てはまりません。つまり、このユーザーはほかのデスクトップの管理者になることはできません。
- 通常、デスクトップの管理者であるユーザーはそのデスクトップにソフトウェアをインストールできます。インストールできるソフトウェアには悪意のあるものも含まれます。またユーザーが、そのデスクトップに接続しているすべてのネットワーク上のトラフィックを監視または制御することも可能です。

ログオン権限の管理

ユーザーアカウントとコンピューターアカウントの両方にログオン権限が必要です。Microsoft Windows の権限では、ログオン権限は引き続き、［ユーザー権限の割り当て］で権限を設定し［グループポリシー］でグループメンバーシップを設定するという通常の方法で、デスクトップに適用されます。

Windows のログオン権限には次の種類があります。ローカルログオン、リモートデスクトップサービスを使ったログオン、ネットワーク経由でのログオン（ネットワーク経由でコンピューターへアクセス）、バッチジョブとしてログオン、サービスとしてログオン。

コンピューターアカウントでは、必要なログオン権限だけをコンピューターに付与します。次のアカウントに、ログオン権限「ネットワーク経由でコンピューターへアクセス」が必要です。

- VDA で、Delivery Controller のコンピューターアカウント
- Delivery Controller で、VDA のコンピューターアカウント。「Active Directory OU ベースの Controller 検出」を参照してください。
- StoreFront サーバーで、同じ StoreFront サーバーグループ内の他のサーバーのコンピューターアカウント

ユーザーアカウントでは、必要なログオン権限だけをユーザーに付与します。

Microsoft によると、デフォルトで Remote Desktop Users グループに［リモート デスクトップ サービスを使ったログオンを許可］でログオン権限が付与されています（ドメインコントローラを除く）。

組織のセキュリティポリシーによっては、このグループがこのログオン権限から除外されることを明示的に設定している場合もあります。次の方法を検討してください。

- マルチセッション OS 対応 Virtual Delivery Agent（VDA）は Microsoft リモートデスクトップサービスを使用します。Remote Desktop Users グループを制限されたグループとして構成し、Active Directory グループポリシー経由でグループのメンバーシップを制御できます。詳しくは、Microsoft 社のドキュメントを参照してください。
- シングルセッション OS 対応 VDA を含む Citrix Virtual Apps and Desktops の他のコンポーネントでは、Remote Desktop Users グループは必要ありません。このため、これらのコンポーネントでは Remote

Desktop Users グループにログオン権限［リモート デスクトップ サービスを使ったログオンを許可］の必要はなく、削除できます。さらに、以下を確認します。

- リモートデスクトップサービスでこれらのコンピューターを管理する場合、すべての必要な管理者が既に Administrators グループのメンバーであることを確認してください。
- リモートデスクトップサービスでこれらのコンピューターを管理しない場合、コンピューター上でリモートデスクトップサービスを無効にすることを検討してください。

ユーザーとグループをログオン権限［リモートデスクトップサービスによるログオンを拒否］に追加することは可能ですが、ログオン権限の拒否の使用は、通常推奨されません。詳しくは、Microsoft 社のドキュメントを参照してください。

ユーザー権利の構成

Delivery Controller をインストールすると、次の Windows サービスが作成されます。

- Citrix AD Identity Service（NT SERVICE\CitrixADIdentityService）: 仮想マシンの Microsoft Active Directory コンピューターアカウントを管理します。
- Citrix Analytics（NT SERVICE\CitrixAnalytics）: Citrix が使用するサイト構成の使用状況情報の収集がサイト管理者によって承認されている場合、この情報を収集します。その後、製品の改善に役立てるために、この情報を Citrix に送信します。
- Citrix App Library（NT SERVICE\CitrixAppLibrary）: AppDisk の管理とプロビジョニング、AppDNA 統合、および App-V の管理をサポートします。
- Citrix Broker Service（NT SERVICE\CitrixBrokerService）: ユーザーが使用できる仮想デスクトップやアプリケーションを選択します。
- Citrix Configuration Logging Service（NT SERVICE\CitrixConfigurationLogging）: すべての構成の変更と、管理者がサイトに対して行ったそのほかの状態の変更を記録します。
- Citrix Configuration Service（NT SERVICE\CitrixConfigurationService）: 共有される構成のサイト全体のリポジトリです。
- Citrix Delegated Administration Service（NT SERVICE\CitrixDelegatedAdmin）: 管理者に与えられた権限を管理します。
- Citrix Environment Test Service（NT SERVICE\CitrixEnvTest）: そのほかの Delivery Controller サービスのセルフテストを管理します。
- Citrix Host Service（NT SERVICE\CitrixHostService）: Citrix Virtual Apps または Citrix Virtual Desktops 環境で使用されているハイパーバイザーインフラストラクチャに関する情報を保存します。また、コンソールで使用される、ハイパーバイザープールのリソースを列挙する機能を提供します。
- Citrix Machine Creation Services（NT SERVICE\CitrixMachineCreationService）: デスクトップ仮想マシンの作成をオーケストレーションします。
- Citrix Monitor Service（NT SERVICE\CitrixMonitor）: Citrix Virtual Apps または Citrix Virtual Desktops のメトリックスを収集し、履歴情報を保存して、トラブルシューティングのためのクエリインターフェイスと各種のレポートツールを提供します。

- Citrix Storefront Service（NT SERVICE\ CitrixStorefront）： StoreFront の管理をサポートします（StoreFront コンポーネント自体には含まれていません）。
- Citrix Storefront Privileged Administration Service（NT SERVICE\CitrixPrivilegedService）: StoreFront の特権管理操作をサポートします（StoreFront コンポーネント自体には含まれていません）。
- Citrix Config Synchronizer Service（NT SERVICE\CitrixConfigSyncService）: メインサイトデータベースからローカルホストキャッシュに構成データを反映させせす。
- Citrix High Availability Service（NT SERVICE\CitrixHighAvailabilityService）: メインサイトデータベースが使用できない場合に、ユーザーが使用できる仮想デスクトップやアプリケーションを選択します。

Delivery Controller をインストールすると、次の Windows サービスも作成されます。これらは、そのほかの Citrix コンポーネントをインストールしたときにも作成されます。

- Citrix Diagnostic Facility COM Server（NT SERVICE\CdfSvc）: Citrix サポートが使用するための診断情報の収集をサポートします。
- Citrix Telemetry Service（NT SERVICE\CitrixTelemetryService）: Citrix が分析するための診断情報を収集することで、管理者が分析結果と推奨事項を確認してサイトの問題解決に役立てることができるようにします。

Delivery Controller をインストールすると、次の Windows サービスも作成されます。これは現在使用されていません。有効だった場合、無効にしてください。

- Citrix Remote Broker Provider（NT SERVICE\XaXdCloudProxy）

Delivery Controller をインストールすると、次の Windows サービスも作成されます。これらは現在使用されていませんが、有効にする必要があります。無効にしないでください。

- Citrix オーケストレーションサービス（NT SERVICE\CitrixOrchestration）
- Citrix 信頼サービス（NT SERVICE\CitrixTrust）

Citrix Storefront Privileged Administration Service を除く、これらのサービスには、［サービスとしてログオン］のログオン権限と［プロセスのメモリクォータの増加］、［セキュリティ監査の生成］、［プロセスレベルトークンの置き換え］の権限が付与されます。通常、これらのユーザー権利を変更する必要はありません。これらの権限は Delivery Controller では使用されないため、自動的に無効にされています。

サービス設定の構成

Citrix StoreFront Privileged Administration Service と Citrix Telemetry Service を除く、上述の「ユーザー権利の構成」セクションに示す Delivery Controller Windows サービスは、ネットワークサービス ID でログオンするように構成されます。このサービス設定は変更しないでください。

Citrix Config Synchronizer Service では、ネットワークサービスアカウントが Delivery Controller のローカル管理者グループに属している必要があります。これにより、ローカルホストキャッシュが正しく機能します。

Citrix Storefront Privileged Administration Service は、ローカルシステム（NT AUTHORITY\SYSTEM）にログオンするように構成されます。これは、通常はサービスで実行できない Delivery Controller StoreFront 操作（Microsoft IIS サイトの作成など）に必要な構成です。このサービス設定は変更しないでください。

Citrix Telemetry Service は、このサービス自体のサービス固有の ID でログオンするように構成されます。

Citrix Telemetry Service は、無効にすることができます。このサービスと、既に無効にされているサービス以外のそのほかの Delivery Controller Windows サービスは、無効にしないでください。

レジストリ設定の構成

VDA ファイルシステムで 8.3 ファイル名およびフォルダーの作成を有効にする必要はなくなりました。レジストリキー **NtfsDisable8dot3NameCreation** は、8.3 ファイル名およびフォルダーの作成が無効になるように構成できます。これは、「**fsutil.exe behavior set disable8dot3**」コマンドを使用しても構成できます。

展開シナリオのセキュリティ

ユーザー環境は、組織に管理されずにユーザーにより完全に制御されるユーザーデバイス、または組織により管理されたユーザーデバイスで構成できます。通常、これら 2 つの環境に対するセキュリティ上の考慮事項は異なります。

管理されるユーザーデバイス

「管理されるユーザーデバイス」とは、管理者または信頼されたほかの組織によって管理されるユーザーデバイスを指します。この場合、ユーザーデバイスを管理者が構成してユーザーに直接提供したり、全画面のみを実行するモードで単一のデスクトップを実行する端末を提供したりできます。管理されるユーザーデバイスに対しては、前述の一般的なセキュリティ構成を実装します。この製品の長所は、ユーザーデバイス上に最低限のソフトウェアしか必要としないという点です。

管理されるユーザーデバイスでは、仮想デスクトップの実行モードとして、全画面のみを実行するモードまたはウィンドウモードを構成できます。

- 全画面のみを実行するモード：ユーザーは通常の［Windows へのログオン］画面からユーザーデバイスにログオンします。すると、同じユーザー資格情報で自動的にこのリリースへのログオンが実行されます。
- 一方、ウィンドウモードを使用する場合、ユーザーは最初にユーザーデバイスにログオンし、次にこのリリースで提供された Web サイトを介してこの製品にログオンします。

管理されていないユーザーデバイス

「管理されていないユーザーデバイス」とは、管理者または信頼された組織によって管理されていないユーザーデバイスを指します。たとえば、ユーザーが自分のデバイスを使用する場合、上記のセキュリティ上の推奨事項にユーザーが従わないことがあります。このリリースでは、このような管理されていないユーザーデバイスにも、デスクトップ

を安全に配信できます。ただし、これらのユーザーデバイスでも、キーロガーやそれに類似した入力攻撃を阻止するための基本的なウイルス対策が施されている必要があります。

データストレージの考慮事項

このリリースを使用しているときに、ユーザーが自分のユーザーデバイスにデータを保存できないように構成できます。ただし、ユーザーが仮想デスクトップにデータを保存することを許可するかどうかも考慮する必要があります。ユーザーによるデスクトップ上へのデータ保存は推奨されません。データはファイルサーバー、データベースサーバー、またはデータが適切に保護されるそのほかのリポジトリに保存する必要があります。

デスクトップ環境は、プールデスクトップや専用デスクトップなど、さまざまな種類のデスクトップで構成される場合があります。ユーザーは、プールデスクトップなど、複数のユーザーで共有されるデスクトップ上にデータを保存するべきではありません。また、専用デスクトップでも、そのデスクトップをほかのユーザーが使用することになった場合に、保存されているデータを削除する必要があります。

バージョン混在環境

アップグレード処理のある時点においては、バージョンが混在する環境は不可避なものです。ベストプラクティスに従い、異なるバージョンの Citrix コンポーネントが同時に存在する時間を最短化させます。たとえばバージョン混在環境ではセキュリティポリシーが一律には適用されない可能性があります。

> 注:
>
> これは、ほかのソフトウェア製品では一般的な問題です。Active Directory の以前のバージョンを使用すると、最近のバージョンの Windows にはグループポリシーが部分的にしか適用されません。

次のシナリオでは、特定のバージョン混在 Citrix 環境で発生する可能性があるセキュリティ問題について説明します。XenApp および XenDesktop 7.6 Feature Pack 2 の Virtual Delivery Agent を実行している仮想デスクトップへの接続に Citrix Receiver 1.7 が使用されている場合、ポリシー設定 ［デスクトップとクライアント間におけるファイル転送の許可］はサイトでは有効ですが、XenApp および XenDesktop 7.1 を実行している Delivery Controller によっては無効にできません。製品のより新しいバージョンでリリースされたポリシーの設定は認識されません。このポリシーにより、ユーザーはファイルを自分の仮想デスクトップにアップロードしてダウンロードできます–セキュリティ問題。この問題を回避するには、Delivery Controller あるいは Studio のスタンドアロンインスタンスをバージョン 7.6 Feature Pack 2 にアップグレードし、その後でグループポリシーを使ってポリシーを無効にします。または、すべての該当する仮想デスクトップでローカルポリシーを使用します。

リモート **PC** アクセスのセキュリティに関する考慮事項

リモート PC アクセスでは、次のセキュリティ機能がサポートされます。

- スマートカードの使用がサポートされます。

- リモートセッションの間、社内の PC のモニターは非表示になります。
- リモート PC アクセスでは、すべてのキーボードおよびマウスの入力がリモートセッションにリダイレクトされます（Ctrl+Alt+Del キー入力、および USB 対応スマートカードや生体認証デバイスを除く）。
- SmoothRoaming は 1 人のユーザーに対してのみサポートされます。
- リモートセッションで接続していた社内の PC にローカルでアクセスを再開できるのはそのユーザーのみです。ローカルでのアクセスを再開するには、ローカルのキーボードで Ctrl+Alt+Del キーを押して、リモートセッションと同じ資格情報を使ってログオンします。システムに適切なサードパーティ製の資格情報プロバイダー統合が構成されている場合は、スマートカードを挿入したり生体認証を使用したりしてローカルアクセスを再開することもできます。グループポリシーオブジェクト（GPO）やレジストリキーでユーザーの簡易切り替え機能を有効にして、このデフォルトの動作設定を上書きすることができます。

> 注:
>
> Citrix では VDA 管理者特権を一般のセッションユーザーに割り当てないことをお勧めします。

自動割り当て

リモート PC アクセスでは、デフォルトで単一 VDA への複数ユーザーの自動割り当てがサポートされます。XenDesktop 5.6 Feature Pack 1 では、PowerShell スクリプト RemotePCAccess.ps1 を使ってこの動作を上書きできました。このリリースでは、レジストリキーを使って複数ユーザーの自動割り当てを許可または禁止できます。この設定はサイト全体に適用されます。

> 注意:
>
> レジストリエディターの使用を誤ると、深刻な問題が発生する可能性があり、オペレーティングシステムの再インストールが必要になる場合もあります。レジストリエディターの誤用による障害に対して、Citrix では一切責任を負いません。レジストリエディターは、お客様の責任と判断の範囲でご使用ください。また、レジストリファイルのバックアップを作成してから、レジストリを編集してください。

自動割り当てを 1 人のユーザーのみに制限するには、以下の手順に従います。

サイト上の各 Controller で、以下のレジストリエントリを設定します。

```
1 HKEY\_LOCAL\_MACHINE\Software\Citrix|DesktopServer
2 Name: AllowMultipleRemotePCAssignments
3 Type: REG_DWORD
4 Data: 0 = Disable multiple user assignment, 1 = (Default) Enable
     multiple user assignment.
```

既存のユーザー割り当てを削除するには、SDK コマンドを使用します。これにより、VDA に単一ユーザーが割り当てられるようになります。

- 割り当てられているすべてのユーザーを VDA から削除するには以下のコマンドを実行します。
  `$machine.AssociatedUserNames | %{ Remove-BrokerUser-Name $_ -Machine $machine`

- デリバリーグループから VDA を削除するには、次のコマンドを実行します: `$machine | Remove-BrokerMachine -DesktopGroup $desktopGroup`

社内の物理 PC を再起動します。

XML 信頼

XML 信頼設定は、以下を使用する展開に適用されます:

- オンプレミス StoreFront。
- パスワードを必要としない利用者（ユーザー）認証テクノロジ。このようなテクノロジの例がドメインパススルー、スマートカード、SAML、Veridium ソリューションです。

XML 信頼設定を有効にすると、ユーザーはアプリケーションを正常に認証して起動できます。Delivery Controller は、StoreFront から送信された資格情報を信頼します。Delivery Controller と StoreFront 間の通信を、セキュリティキー、またはファイアウォールや IPsec などの別のメカニズムを使用して保護している場合にのみ、この設定を有効にします。

このチェックボックスは、デフォルトでオフになっています。

Citrix Virtual Apps and Desktops PowerShell SDK を使用して、XML 信頼設定を確認、有効化、または無効化します。

- XML 信頼設定の現在の値を確認するには、`Get-BrokerSite`を実行して`TrustRequestsSentToTheXMLServ`の値を調べます。
- XML 信頼を有効にするには、`Set-BrokerSite -TrustRequestsSentToTheXmlServicePort $true`を実行します。
- XML 信頼を無効にするには、`Set-BrokerSite -TrustRequestsSentToTheXmlServicePort $false`を実行します。

スマートカード

August 17, 2024

スマートカードおよび同等のテクノロジは、このアーティクルに記載されているガイドライン内でサポートされています。Citrix Virtual Apps または Citrix Virtual Desktops でスマートカードを使用するには:

- 所属する組織における、スマートカードの使用に関するセキュリティポリシーを理解します。たとえば、スマートカードがどのように発行され、ユーザーがそれをどのように保護するかについてこれらのポリシーで規定してあることがあります。Citrix Virtual Apps または Citrix Virtual Desktops の環境では、これらのポリシーの一部の変更が必要になる場合があります。

- どのユーザーデバイスの種類、オペレーティングシステム、および公開アプリケーションがスマートカードとともに使用されるかを決定します。
- スマートカードテクノロジ全般および選択したスマートカードベンダーのハードウェアとソフトウェアについて理解します。
- 分散環境でのデジタル証明書の展開管理方法について理解します。

> 注:
>
> 高速スマートカードではスマートカードの登録はサポートされていません。スマートカードの登録は、高速スマートカードが無効になっている場合に機能する可能性がありますが、スマートカードとミドルウェアの種類によって異なります。Citrix Virtual Apps and Desktops との統合、および仮想セッションでのスマートカード登録のサポートについては、スマートカードおよびミドルウェアのベンダーにお問い合わせください。

スマートカードの種類

エンタープライズ向けとコンシューマー向けのスマートカードは、寸法も電気コネクタも同じで、同じスマートカードリーダーを使用できます。

エンタープライズ向けのスマートカードにはデジタル証明書が含まれています。これらのスマートカードは Windows ログオンをサポートし、ドキュメントやメールのデジタル署名と暗号化のためのアプリケーションと連携して使用できます。Citrix Virtual Apps and Desktops は、こうした用途に対応しています。

コンシューマー向けのスマートカードにはデジタル証明書は含まれていませんが、共有シークレットが含まれています。これらのスマートカードは、支払い（チップと署名、チップと PIN クレジットカードなど）をサポートできます。これらのスマートカードは、Windows ログインや一般的な Windows アプリケーションをサポートしていません。これらのスマートカードと合わせて使用するには、特別な Windows アプリケーションと、適切なソフトウェアインフラストラクチャ（支払いカードネットワークへの接続など）が必要です。Citrix Virtual Apps または Citrix Virtual Desktops でのこのような特別なアプリケーションのサポートについて詳しくは、Citrix 担当者にお問い合わせください。

エンタープライズ向けスマートカードには、互換性のある同等のものが存在し、類似した方法で使用できます。

- スマートカードと同等の USB トークンは USB ポートに直接接続します。これらの USB トークンは通常 USB フラッシュドライブのサイズですが、携帯電話で使用される SIM カードと同じくらい小さいものもあります。それらは、スマートカードと USB スマートカードリーダーの組み合わせとして表示されます。
- Windows トラステッドプラットフォームモジュール（TPM：Trusted Platform Module）を使用する仮想スマートカードは、スマートカードとして表示されます。これらの仮想スマートカードは、Citrix Workspace アプリ（Citrix Receiver 4.3 以降）を使用して、Windows 8 および Windows 10 でサポートされます。
  - Citrix Virtual Apps and Desktops（旧称 XenApp および XenDesktop）の XenApp および XenDesktop 7.6 FP3 よりも前のバージョンは、仮想スマートカードをサポートしていません。
  - 仮想スマートカードについて詳しくは、「Virtual Smart Card Overview」を参照してください。

> 注:「仮想スマートカード」という用語は、ユーザーコンピューターに保存されたデジタル証明書についても使用されます。これらのデジタル証明書は、厳密にはスマートカードと同等ではありません。

Citrix Virtual Apps and Desktops のスマートカードのサポートは、Microsoft の PC/SC（Personal Computer/Smart Card）標準仕様に基づいています。スマートカードおよびスマートカードデバイスは、使用する Windows オペレーティングシステムでサポートされており、Microsoft WHQL（Windows Hardware Quality Lab）により承認されている必要があります。PC/SC に準拠しているハードウェアについては、Microsoft 社のドキュメントを参照してください。その他のタイプのユーザーデバイスは、PS/SC 標準に準拠していることがあります。詳しくは、Citrix Ready プログラムを参照してください。

通常、各ベンダーのスマートカードまたは同等のものには、別々のデバイスドライバーが必要です。ただし、スマートカードが NIST Personal Identity Verification（PIV）標準などの標準に準拠している場合、一定範囲のスマートカードに単一のデバイスドライバーを使用できる場合があります。デバイスドライバーをユーザーデバイスと Virtual Delivery Agent（VDA）の両方にインストールする必要があります。多くの場合、デバイスドライバーは Citrix パートナーから入手可能なスマートカードミドルウェアパッケージの一部として提供されます。スマートカードミドルウェアパッケージにより、高度な機能が提供されます。デバイスドライバーは、暗号化サービスプロバイダー（CSP：Cryptographic Service Provider）、キーストレージプロバイダー（KSP：Key Storage Provider）、ミニドライバーとして説明されることもあります。

Windows システムでは、以下のスマートカードとミドルウェアでの Citrix の動作確認が行われています。ただし、そのほかのスマートカードおよびミドルウェアも使用できます。Citrix 互換のスマートカードとミドルウェアについて詳しくは、http://www.citrix.com/readyを参照してください。

ミドルウェア	スマートカード
GemAlto Mini Driver for .NET カード	Gemalto .NET v2+

他の種類のデバイスでのスマートカード使用法について詳しくは、そのデバイスに関する Citrix Workspace アプリのドキュメントを参照してください。

リモート **PC** アクセス

オフィスで動作する、物理的な Window 10、Windows 8、または Windows 7 マシンにリモートアクセスする場合にのみ、スマートカードがサポートされます。

以下のスマートカードが、リモート PC アクセス機能でテストされています。

ミドルウェア	スマートカード
Gemalto .NET ミニドライバー	Gemalto .NET v2+

高速スマートカード

高速スマートカードは、既存の HDX PC/SC ベースのスマートカードリダイレクトの改良版です。遅延が大きい WAN 環境でスマートカードを使用する場合のパフォーマンスが向上しています。待ち時間が長い場合、パフォーマンスが大幅に向上する可能性があります（たとえば、Windows の高速スマートカードログオンの場合は 15 秒であるのに対して、PC/SC ベースのスマートカードリダイレクトの場合は 1 分）。

高速スマートカードは、現在サポートされている Windows 用の VDA がインストールされたホストマシン上ではデフォルトで有効になっています。高速スマートカードを、たとえば診断する目的でホスト側で無効にするには、「暗号化リダイレクトを無効にする」レジストリを任意のゼロ以外の値に設定します：

```
HKLM\SOFTWARE\Citrix\SmartCard
CryptographicRedirectionDisable (DWORD)
```

クライアント側では、高速スマートカードを有効にするには、関連する StoreFront サイトの *default.ica* ファイルに SmartCardCryptographicRedirection ICA パラメーターを含めます：

```
[WFClient]
SmartCardCryptographicRedirection=On
```

さらに、クライアント側では次のレジストリ設定を使用して、高速スマートカードを（診断目的などで）強制的に有効または無効にすることができます。

- HKEY_LOCAL_MACHINE\SOFTWARE[\WOW6432Node]\Citrix\ICA Client\SmartCard\ForceEnableCryptograp
  （DWORD はゼロ以外）

または

- HKEY_LOCAL_MACHINE\SOFTWARE[\WOW6432Node]\Citrix\ICA Client\SmartCard\ForceDisableCryptograp
  （DWORD はゼロ以外）

クライアントマシンが 64 ビットの場合は、32 ビットのレジストリハイブを指定する必要があります（WOW6432Nodeを使用）。

制限事項：

- 高速スマートカードをサポートしているのは Windows 向け Citrix Workspace アプリのみです。default.ica ファイルで高速スマートカードを設定している場合、Windows 向け以外の Citrix Workspace アプリは、引き続き既存の PC/SC リダイレクトを使用します。
- 高速スマートカードがサポートされているダブルホップシナリオは、両方のホップで高速スマートカードが有効になっている ICA > ICA のみです。高速スマートカードでは ICA > RDP のダブルホップシナリオはサポートされていないため、これらのシナリオでは動作しません。
- 高速スマートカードでは Cryptography Next Generation はサポートされていません。したがって、高速スマートカードでは楕円曲線暗号（ECC）スマートカードはサポートされていません。
- 高速スマートカードでは、読み取り専用キーコンテナ操作のみがサポートされています。
- 高速スマートカードでは、スマートカード PIN の変更はサポートされていません。

VDA バージョン 2203 および Windows 向け Citrix Workspace アプリバージョン 2202 以降、高速スマートカードは Cryptography Next Generation（CNG）と互換性があります。さらに、楕円曲線暗号（ECC）スマートカードは、次の曲線でサポートされます：ECDSA と ECDH の両方で P-256、P-384、P-521 ビット。

VDA バージョン 2203 以降、高速スマートカードで、同一ユーザーのログオンセッションのアプリケーション間でスマートカード PIN をキャッシュする機能が追加されています。たとえば、セッション **PIN** キャッシュ が有効になっていて、エンドユーザーが以前にスマートカード PIN を Outlook に提供した場合、Word を使用してドキュメントに署名すると、Word は既にキャッシュされているスマートカード PIN（Outlook に送信されたもの）を使用します。セッション **PIN** キャッシュ は、ユーザーがスマートカードの PIN を入力する回数を減らすことで、ユーザーエクスペリエンスを向上させます。さらに、スマートカードを使用して VDA にログオンする場合、Windows スマートカードのログオン PIN をオプションでセッション **PIN** キャッシュに保存できます。これにより、ユーザーエクスペリエンスをさらに向上させることができます。

セッション **PIN** キャッシュはデフォルトで無効になっています。VDA の次のレジストリ設定を使用して有効化、制御することができます：

場所：HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartCard

- `EnablePinSessionCache`を DWORD として設定（有効にする場合はゼロ以外）
- `EnableLogonPinSessionCache`を DWORD として設定（有効にする場合はゼロ以外）
- `PinSessionCacheEntryStaleTimeout`を DWORD として設定（エントリが古くなるまでの秒数。デフォルトは 1 時間）

スマートカードリーダーの種類

スマートカードリーダーはユーザーデバイス内に作成されることもありますし、別にユーザーデバイスに（通常は USB または Bluetooth で）接続することもあります。USB Chip/Smart Card Interface Devices（CCID）仕様に準拠する接触カードリーダーがサポートされます。これらのカードリーダーでは、ユーザーがスマートカードをスロットに挿入したりスワイプしたりします。Deutsche Kreditwirtschaft（DK）標準は、接触カードリーダーの 4 つのクラスを定義しています。

- Class 1 スマートカードリーダーは最も一般的で、通常 1 つのスロットを備えています。Class 1 スマートカードリーダーは通常、オペレーティングシステム付属の標準 CCID デバイスドライバーでサポートされます。
- Class 2 スマートカードリーダーには、ユーザーデバイスがアクセスできない安全なキーパッドも含まれています。Class 2 スマートカードリーダーは、内蔵の安全なキーパッドがあるキーボードに搭載される場合があります。Class 2 スマートカードリーダーについては、Citrix の担当者に連絡してください。安全なキーパッドの機能を有効化するには、リーダー固有のデバイスドライバーが必要になる場合があります。
- Class 3 スマートカードリーダーには、安全なディスプレイも含まれます。Class 3 スマートカードリーダーはサポートされません。
- Class 4 スマートカードリーダーには、安全なトランザクションモジュールも含まれます。Class 4 スマートカードリーダーはサポートされません。

> 注:
>
> スマートカードリーダーのクラスは、USB デバイスのクラスには無関係です。

スマートカードリーダーは、対応するデバイスドライバーとともにユーザーデバイスにインストールする必要があります。

サポートされているスマートカードリーダーについては、使用している Citrix Workspace アプリのマニュアルを参照してください。サポートされているバージョンは、Citrix Workspace アプリのドキュメントでスマートカードの記事でまたはシステム要件に関する記事に掲載されています。

ユーザーエクスペリエンス

スマートカードのサポートは、デフォルトで有効な特定の ICA/HDX スマートカード仮想チャネルを使用して、Citrix Virtual Apps and Desktops に統合されています。

重要: スマートカードリーダーでは汎用 USB リダイレクトを使用しないでください。一部のスマートカードリーダーではこれはデフォルトで無効にされており、有効化した場合サポートされなくなります。

同一ユーザーデバイス上で、複数のスマートカードやスマートカードリーダーを使用することは可能ですが、パススルー認証を使用する場合は 1 枚のスマートカードを挿入した状態で仮想デスクトップまたはアプリケーションを開始する必要があります。アプリケーション内でスマートカードを使用する場合（デジタル署名または暗号化機能など）、スマートカードの挿入または PIN の入力を求める別のメッセージが表示されることがあります。これは、同時に複数のスマートカードが挿入されている場合に発生します。

- 適切なスマートカードを挿入しているにもかかわらずスマートカードの挿入を求めるメッセージが表示された場合は、［キャンセル］を選択するよう通知します。
- ただし、PIN の入力が求められた場合は、PIN を再入力する必要があります。

カード管理システムまたはベンダーのユーティリティを使って PIN をリセットできます。

> 重要:
>
> Citrix Virtual Apps または Citrix Virtual Desktops セッションでは、Microsoft リモートデスクトップ接続アプリケーションでのスマートカードの使用はサポートされません。これは「ダブルホップ」の使用と呼ばれることがあります。

スマートカードを展開する前の確認事項

- スマートカードリーダーのデバイスドライバーを入手して、ユーザーデバイスにインストールする必要があります。Microsoft により提供される CCID デバイスドライバーは、多くのスマートカードリーダーで使用できます。

- スマートカードベンダーからデバイスドライバーと暗号化サービスプロバイダー（CSP）ソフトウェアを入手して、ユーザーデバイスと仮想デスクトップの両方にインストールします。このドライバーと CSP ソフトウェアは、Citrix Virtual Apps and Desktops と互換性がある必要があります。詳しくは、ベンダーのドキュメントを参照してください。ミニドライバーモデルのスマートカードを使用する仮想デスクトップでは、スマートカードミニドライバーが自動的にダウンロードされます。また、http://catalog.update.microsoft.comまたはベンダーから入手することもできます。さらに、PKCS#11 ミドルウェアが必要な場合は、カードベンダーから入手してください。
- 重要：Citrix ソフトウェアをインストールする前に、物理的なコンピューターにドライバーと CSP ソフトウェアをインストールしてテストすることをお勧めします。
- Windows 10 で実行する Internet Explorer でスマートカードを使用するユーザーの信頼済みサイトの一覧に Citrix Receiver for Web URL を追加します。Windows 10 では、Internet Explorer は信頼済みサイトのデフォルトで保護モードでは実行しません。
- PKI（Public Key Infrastructure：公開キー基盤）が適切に構成されていることを確認します。つまり、アカウントマッピングのための証明書が Active Directory 環境に対して正しく構成されており、ユーザー証明書の検証を正しく実行できることを確認します。
- Citrix Workspace アプリや StoreFront など、スマートカードで使用するほかの Citrix コンポーネントのシステム要件を満たしていることを確認します。
- サイト内の以下のサーバーにアクセスできることを確認します。
  - スマートカード上のログオン証明書に関連付けられているユーザーアカウント用の Active Directory ドメインコントローラー
  - Delivery Controller
  - Citrix StoreFront
  - Citrix Gateway/Citrix Access Gateway 10.x
  - VDA
  - Microsoft Exchange Server（リモート PC アクセスの場合はオプション）

スマートカード使用の有効化

手順 **1**：カードの発行ポリシーに従って、ユーザーにスマートカードを発行します。

手順 **2**：必要に応じて、ユーザーがリモート PC アクセスを実行できるようにスマートカードをセットアップします。

手順 **3**：Delivery Controller と StoreFront をインストールして（未インストールの場合）、スマートカードのリモート処理用に構成します。

手順 **4**：StoreFront で、スマートカードの使用を有効にします。詳しくは、StoreFront ドキュメントの「スマートカード認証の構成」を参照してください。

手順 **5**：Citrix Gateway/Access Gateway で、スマートカードの使用を有効にします。詳しくは、NetScaler ドキュメントの「認証と承認の構成」および「Web Interface でのスマートカードアクセスの構成」を参照してください。

手順 **6**：VDA で、スマートカードの使用を有効にします。

- VDA に必要なアプリケーションおよび更新がインストール済みであることを確認します。
- ミドルウェアをインストールします。
- ユーザーデバイス上の Citrix Workspace アプリと仮想デスクトップセッション間でスマートカードデータ通信が行われるように、スマートカードのリモート処理をセットアップします。

手順 **7**：ユーザーデバイス（ドメインに属しているマシンと属していないマシンを含む）でスマートカードの使用を有効にします。詳しくは、StoreFront ドキュメントの「スマートカード認証の構成」を参照してください。

- 証明機関のルート証明書とその証明機関の証明書をデバイスのキーストア内にインポートします。
- ベンダーが提供するスマートカードミドルウェアをインストールします。
- Windows 向け Citrix Workspace アプリをインストールおよび構成して、グループポリシー管理コンソールを使って icaclient.adm をインポートします。また、スマートカード認証を有効にします。

手順 **8**：展開をテストします。テストユーザーのスマートカードで仮想デスクトップを起動して、展開が正しく構成されていることを確認します。すべてのアクセス方法（たとえば、Internet Explorer および Citrix Workspace アプリを介したデスクトップアクセスなど）をテストします。

スマートカードリーダー挿入回数の追跡

スマートカードのリモート処理では、SCardGetStatusChange 関数を使用して、スマートカードがリーダーに対して挿入または削除された回数を追跡できます。この関数は、監視するリーダーごとに SCARD_READERSTATE データ構造の配列 1 つを更新します。各 SCARD_READERSTATE の dwEventState フィールドの上位ワード（16 ビット）には、リーダーの回数が含まれます。詳しくは、Microsoft の記事SCardGetStatusChangeA functionおよびSCARD_READERSTATEA structureを参照してください。

Reader Insert Count Reporting 設定はデフォルトで無効になっています。有効にするには、次のレジストリキーを追加します：

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartCard

名前：EnableReaderInsertCountReporting

種類：DWORD

値：ゼロ（0）以外の任意の数

セッションが切断されると、カウントはゼロにリセットされます。

Reader Insert Count Reporting は、サードパーティのスマートカードミドルウェアと互換性があります。

スマートカード展開

August 17, 2024

この製品バージョンおよびこのバージョンと以前のバージョンとの混在環境では、以下の種類のスマートカード展開がサポートされます。そのほかの構成でも使用できる場合がありますが、サポートの対象外です。

種類	StoreFront への接続
ローカルのドメイン参加コンピューター	直接接続
ドメイン参加コンピューターからのリモートアクセス	Citrix Gateway 経由で接続
ドメイン不参加コンピューター	直接接続
ドメイン不参加コンピューターからのリモートアクセス	Citrix Gateway 経由で接続
デスクトップアプライアンスサイトにアクセスするドメイン不参加コンピューターおよびシンクライアント	デスクトップアプライアンスサイト経由の接続
XenApp Services サイト経由で StoreFront にアクセスするドメイン参加コンピューターおよびシンクライアント	XenApp Services サイト経由の接続

展開の種類は、スマートカードリーダーが接続されているユーザーデバイスの特徴により定義されます。

- デバイスがドメインに参加しているか参加していないか。
- デバイスが StoreFront にどのように接続するか。
- 仮想デスクトップやアプリケーションの表示にどのソフトウェアを使用するか。

これらの展開では、Microsoft Word や Microsoft Excel など、スマートカード対応のアプリケーションを使用できます。ユーザーは、これらのアプリケーションを使用してドキュメントにデジタル署名を追加したり、ドキュメントを暗号化したりできます。

2 モード認証

これらの各展開で可能な箇所では、スマートカードを使用するのか、ユーザー名およびパスワードを入力するのかをユーザーに選択させる 2 モード認証を Receiver がサポートします。この機能は、ユーザーがスマートカードを使用できない場合（スマートカードを自宅に忘れた場合や資格情報の有効期限が切れた場合など）に便利です。

ドメイン不参加デバイスのユーザーは Receiver for Windows に直接ログオンするため、管理者は指定ユーザー認証へのフォールバックを有効にすることができます。2 モード認証を構成した場合、ユーザーは最初にスマートカードと PIN を使ったログオンを要求されますが、スマートカードでログオンできない場合は指定ユーザー認証を選択することができます。

Citrix Gateway を使用する環境では、ユーザーはデバイスにログオンし、Citrix Gateway の認証を受けるように Receiver for Windows から要求されます。これはドメイン参加デバイスとドメイン不参加デバイスの両方に適用されます。ユーザーは、スマートカードと PIN を使って、または指定ユーザーの資格情報を使って Citrix Gateway にログオンできます。これにより、Citrix Gateway にログオンするときの 2 モード認証をユーザーに提供できます。

ユーザーが StoreFront に透過的に認証されるように、Citrix Gateway から StoreFront へのパススルー認証を構成し、スマートカードユーザーの資格情報の検証を Citrix Gateway に委任します。

複数 **Active Directory** フォレストでの考慮事項

Citrix 環境では、スマートカードは単一のフォレスト内でサポートされます。フォレスト間でのスマートカード認証には、すべてのユーザーアカウントに対する直接の双方向の信頼関係が必要です。より複雑なマルチフォレスト展開（一方向のみまたはそのほかの信頼関係が設定された複数フォレスト展開）はサポートされていません。

リモートデスクトップを含む Citrix 環境でスマートカードを使用できます。この機能は、（スマートカードが接続されるユーザーデバイス上に）ローカルにインストールしたり、（ユーザーデバイスが接続するリモートデスクトップ上に）リモートにインストールしたりできます。

スマートカード取り出し時の動作ポリシー

スマートカード取り出し時の動作ポリシーの設定により、セッション中にスマートカードリーダーからカードを取り出したときの処理が制御されます。このポリシーは、Windows オペレーティングシステムで設定します。

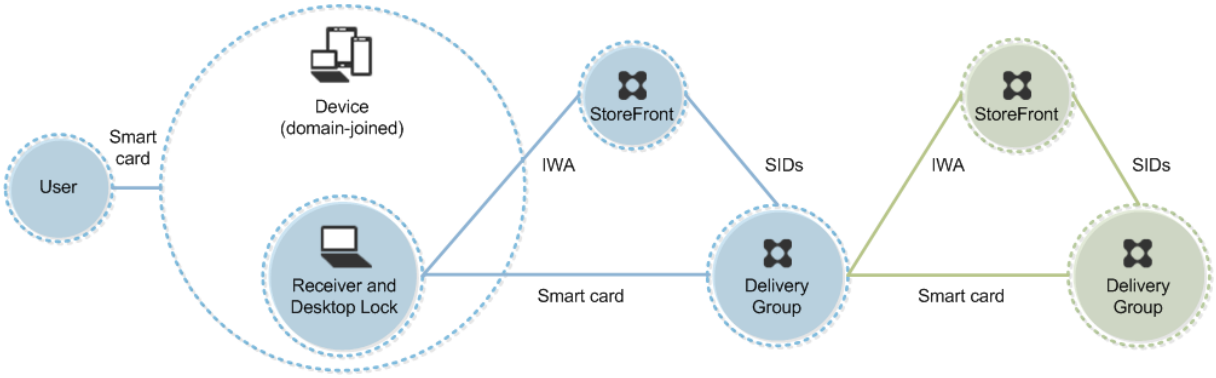
ポリシー設定	デスクトップの動作
何もしない	何もしない。
ワークステーションをロック	デスクトップセッションは切断され、仮想デスクトップはロックされます。
ログオフを強制する	ユーザーは強制的にログオフされます。ネットワーク接続が失われ、この設定が有効な場合、セッションはログオフされてユーザーのデータは消失します。
リモートターミナルサービスセッションの場合に切断	セッションは切断され、仮想デスクトップはロックされます。

証明書失効のチェック

証明書失効のチェックが有効な場合、スマートカードの証明書が有効かどうか検出されます。証明書が無効な場合、ユーザー認証に失敗したり、その証明書に関連付けられているデスクトップやアプリケーションへのアクセスが拒否されたりします。たとえば、メールの復号化用の証明書が無効な場合、暗号化されたメールを復号化できなくなります。同じスマートカード上に有効なほかの証明書がある場合、その機能については有効なままとなります。たとえば、認証用の証明書が有効な場合、ユーザー認証に成功します。

展開例：ドメイン参加コンピューター

この展開には、Desktop Viewer を実行し、StoreFront に直接接続する、ドメインに参加しているユーザーデバイスが含まれています。

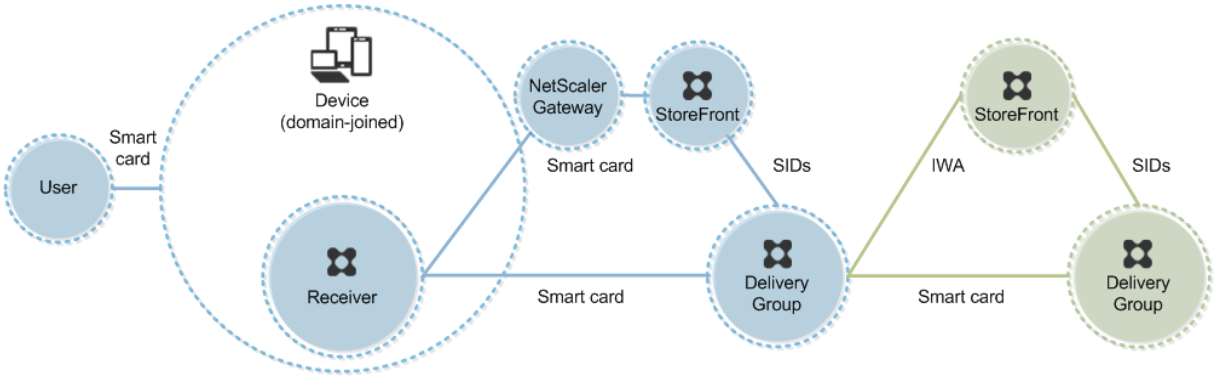


ユーザーは、スマートカードと PIN を使ってデバイスにログオンします。Receiver は、StoreFront サーバーにアクセスするユーザーを統合 Windows 認証（IWA）で認証します。StoreFront により、ユーザーのセキュリティ識別子（SID）が Citrix Virtual Apps または Citrix Virtual Desktops に渡されます。Receiver でシングルサインオン機能が構成されているため、ユーザーが仮想デスクトップやアプリケーションを起動するときに PIN を再入力する必要はありません。

この展開は、2 つ目の StoreFront サーバーとアプリケーションをホストするサーバーを追加してダブルホップ形式に拡張できます。仮想デスクトップの Receiver は、2 つ目の StoreFront サーバーへの認証を実行します。この 2 つ目の接続では任意の認証方法を使用できます。最初の接続で使用した認証方法を 2 つ目の接続で再使用したり、または 2 つ目の接続で異なる方法を使用したりできます。

展開例：ドメイン参加コンピューターからのリモートアクセス

この展開には、Desktop Viewer を実行し、Citrix Gateway/Access Gateway を介して StoreFront に接続する、ドメインに参加しているユーザーデバイスが含まれています。



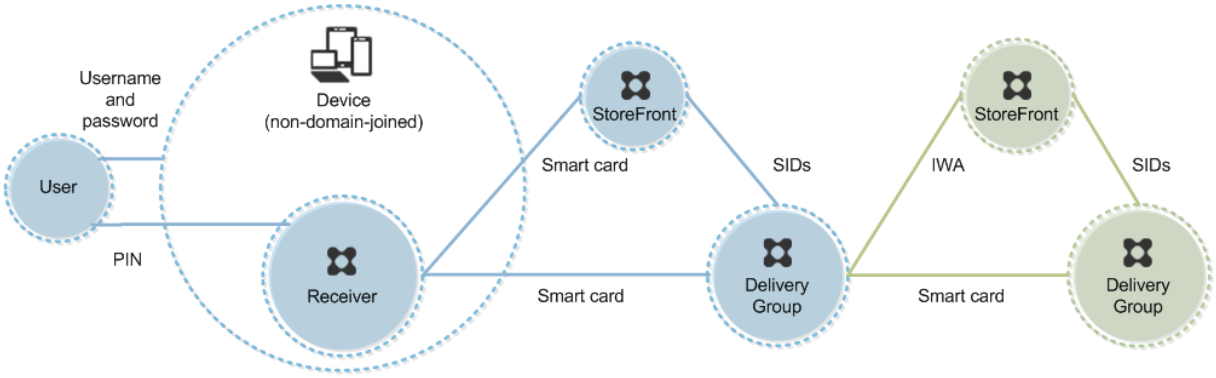
ユーザーはスマートカードと PIN を使ってデバイスにログオンし、次に Citrix Gateway/Access Gateway にもう一度ログオンします。この展開では Receiver で 2 モード認証を使用できるため、この 2 つ目のログオンではスマートカードと PIN を使用したりユーザー名とパスワードを入力したりできます。

ユーザーは自動的に StoreFront にログオンし、ユーザーセキュリティ識別子（SID）が Citrix Virtual Apps または Citrix Virtual Desktops に渡されます。Receiver でシングルサインオン機能が構成されているため、ユーザーが仮想デスクトップやアプリケーションを起動するときに PIN を再入力する必要はありません。

この展開は、2 つ目の StoreFront サーバーとアプリケーションをホストするサーバーを追加してダブルホップ形式に拡張できます。仮想デスクトップの Receiver は、2 つ目の StoreFront サーバーへの認証を実行します。この 2 つ目の接続では任意の認証方法を使用できます。最初の接続で使用した認証方法を 2 つ目の接続で再使用したり、または 2 つ目の接続で異なる方法を使用したりできます。

展開例：ドメイン不参加コンピューター

この展開には、Desktop Viewer を実行し、StoreFront に直接接続する、ドメイン不参加のユーザーデバイスが含まれています。



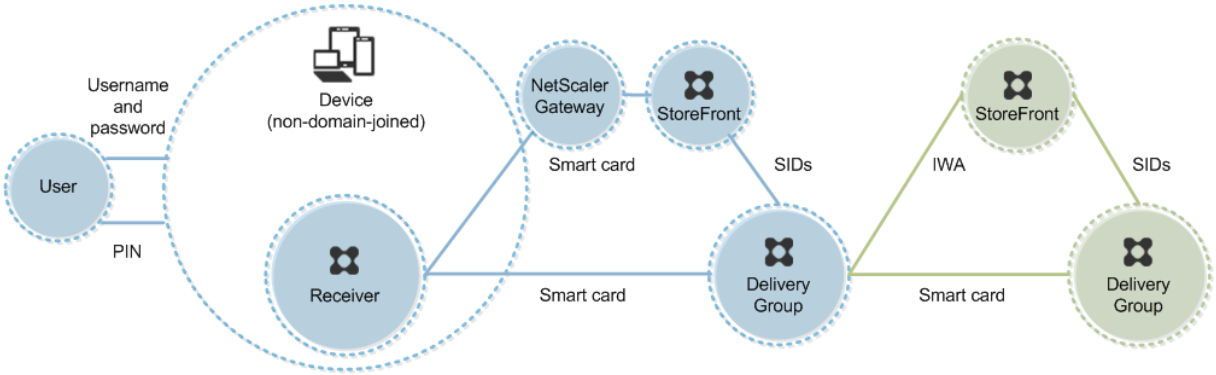
ユーザーがデバイスにログオンします。通常はユーザー名とパスワードを入力しますが、デバイスがドメインに参加していないため、このログオンでの資格情報の入力は必須ではありません。この展開では 2 モード認証を使用できるため、Receiver ではスマートカードと PIN、またはユーザー名とパスワードのいずれかの入力が求められます。その後、Receiver が Storefront への認証を実行します。

StoreFront により、ユーザーのセキュリティ識別子（SID）が Citrix Virtual Apps または Citrix Virtual Desktops に渡されます。この展開ではシングルサインオン機能を使用できないため、ユーザーが仮想デスクトップやアプリケーションを起動するときに PIN を再入力する必要があります。

この展開は、2 つ目の StoreFront サーバーとアプリケーションをホストするサーバーを追加してダブルホップ形式に拡張できます。仮想デスクトップの Receiver は、2 つ目の StoreFront サーバーへの認証を実行します。この 2 つ目の接続では任意の認証方法を使用できます。最初の接続で使用した認証方法を 2 つ目の接続で再使用したり、または 2 つ目の接続で異なる方法を使用したりできます。

展開例：ドメイン不参加コンピューターからのリモートアクセス

この展開には、Desktop Viewer を実行し、StoreFront に直接接続する、ドメイン不参加のユーザーデバイスが含まれています。



ユーザーがデバイスにログオンします。通常はユーザー名とパスワードを入力しますが、デバイスがドメインに参加していないため、このログオンでの資格情報の入力は必須ではありません。この展開では 2 モード認証を使用できるため、Receiver ではスマートカードと PIN、またはユーザー名とパスワードのいずれかの入力が求められます。その後、Receiver が Storefront への認証を実行します。

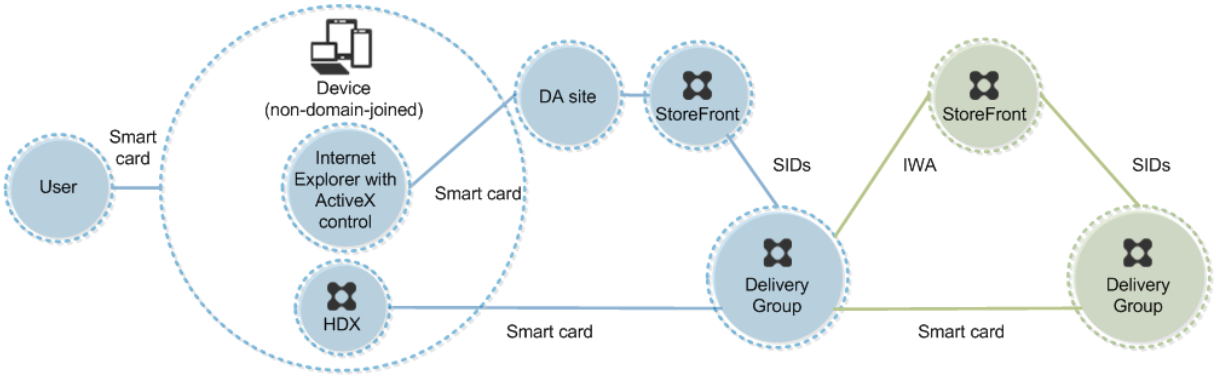
StoreFront により、ユーザーのセキュリティ識別子（SID）が Citrix Virtual Apps または Citrix Virtual Desktops に渡されます。この展開ではシングルサインオン機能を使用できないため、ユーザーが仮想デスクトップやアプリケーションを起動するときに PIN を再入力する必要があります。

この展開は、2 つ目の StoreFront サーバーとアプリケーションをホストするサーバーを追加してダブルホップ形式に拡張できます。仮想デスクトップの Receiver は、2 つ目の StoreFront サーバーへの認証を実行します。この 2 つ目の接続では任意の認証方法を使用できます。最初の接続で使用した認証方法を 2 つ目の接続で再使用したり、または 2 つ目の接続で異なる方法を使用したりできます。

展開例：デスクトップアプライアンスサイトにアクセスするドメイン不参加コンピューターおよびシンクライアント

この展開には、Desktop Lock を実行し、デスクトップアプライアンスサイトを介して StoreFront に接続する、ドメイン不参加のユーザーデバイスが含まれています。

Desktop Lock は、Citrix Virtual Apps、Citrix Virtual Desktops、および Citrix VDI-in-a-Box と一緒にリリースされる個別のコンポーネントです。Desktop Viewer の代替として使用でき、主に再目的化された Windows コンピューターおよび Windows シンクライアント向けに設計されています。Desktop Lock はユーザーデバイス上の Windows Shell とタスクマネージャーを置き換えるもので、これによりユーザーはそのデバイスに直接アクセスできなくなります。Desktop Lock により、ユーザーには Windows Server および Windows Desktop のデスクトップが提供されます。Desktop Lock のインストールは必須ではありません。



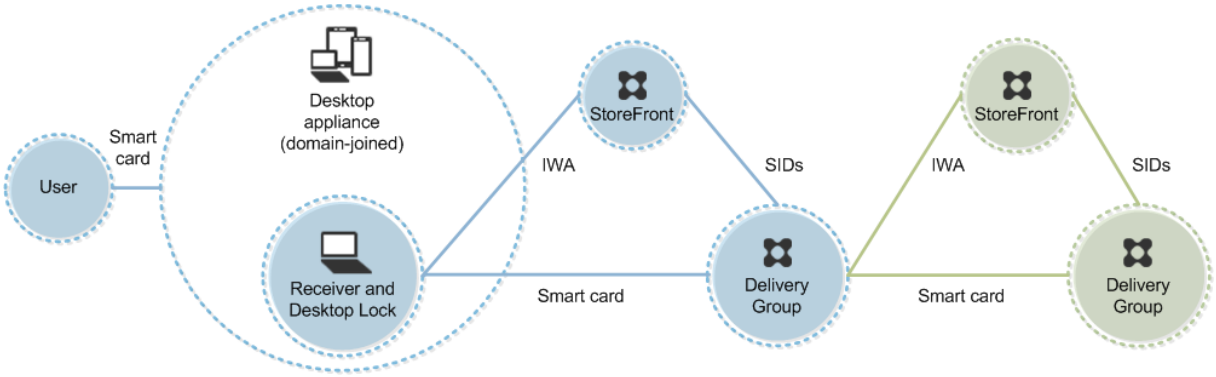
ユーザーは、スマートカードを使ってデバイスにログオンします。Desktop Lock を実行するデバイスは、キオスクモードで動作する Internet Explorer を介してデスクトップアプライアンスサイトを起動するように構成されます。サイトの ActiveX コントロールにより PIN の入力が求められ、それが StoreFront に送信されます。StoreFront により、ユーザーのセキュリティ識別子（SID）が Citrix Virtual Apps または Citrix Virtual Desktops に渡されます。割り当てられたデスクトップグループ一覧で使用可能な（アルファベット順で）最初のデスクトップが起動します。

この展開は、2 つ目の StoreFront サーバーとアプリケーションをホストするサーバーを追加してダブルホップ形式に拡張できます。仮想デスクトップの Receiver は、2 つ目の StoreFront サーバーへの認証を実行します。この 2 つ目の接続では任意の認証方法を使用できます。最初の接続で使用した認証方法を 2 つ目の接続で再使用したり、または 2 つ目の接続で異なる方法を使用したりできます。

展開例：**XenApp Services** サイト経由で **StoreFront** にアクセスするドメイン参加コンピューターおよびシンクライアント

この展開には、Desktop Lock を実行し、XenApp Services URL を介して StoreFront に接続する、ドメインに参加しているユーザーデバイスが含まれています。

Desktop Lock は、Citrix Virtual Apps、Citrix Virtual Desktops、および Citrix VDI-in-a-Box と一緒にリリースされる個別のコンポーネントです。Desktop Viewer の代替として使用でき、主に再目的化された Windows コンピューターおよび Windows シンクライアント向けに設計されています。Desktop Lock はユーザーデバイス上の Windows Shell とタスクマネージャーを置き換えるもので、これによりユーザーはそのデバイスに直接アクセスできなくなります。Desktop Lock により、ユーザーには Windows Server および Windows Desktop のデスクトップが提供されます。Desktop Lock のインストールは必須ではありません。



ユーザーは、スマートカードと PIN を使ってデバイスにログオンします。デバイス上で Desktop Lock が動作している場合は、StoreFront サーバーでのユーザー認証に統合 Windows 認証（IWA）が使用されます。StoreFront により、ユーザーのセキュリティ識別子（SID）が Citrix Virtual Apps または Citrix Virtual Desktops に渡されます。Receiver でシングルサインオン機能が構成されているため、ユーザーが仮想デスクトップを起動するときに PIN を再入力する必要はありません。

この展開は、2 つ目の StoreFront サーバーとアプリケーションをホストするサーバーを追加してダブルホップ形式に拡張できます。仮想デスクトップの Receiver は、2 つ目の StoreFront サーバーへの認証を実行します。この 2 つ目の接続では任意の認証方法を使用できます。最初の接続で使用した認証方法を 2 つ目の接続で再使用したり、または 2 つ目の接続で異なる方法を使用したりできます。

スマートカードを使用したパススルー認証とシングルサインオン

August 17, 2024

パススルー認証

仮想デスクトップへのスマートカードによるパススルー認証は、Windows 10、Windows 8、Windows 7 Service Pack 1 Enterprise エディション、および Professional エディションが動作するユーザーデバイスでサポートされます。

サーバーでホストされるアプリケーションへのスマートカードによるパススルー認証は、Windows Server 2012 および Windows Server 2008 R2 SP1 が動作するサーバーでサポートされます。

サーバーでホストされるアプリケーションへのスマートカードパススルー認証を使用するには、サイトの認証方法としてスマートカードパススルーを構成するときに Kerberos を有効にする必要があります。

注：スマートカードによるパススルー認証を使用できるかどうかは、次の例のようなさまざまな要因により決定されます。

- パススルー認証に関する組織のセキュリティポリシー。

- ミドルウェアの種類と構成。
- スマートカードリーダーの種類。
- ミドルウェアの PIN キャッシュポリシー。

スマートカードによるパススルー認証は、Citrix StoreFront 上で構成します。詳しくは、StoreFront のドキュメントを参照してください。

シングルサインオン

「シングルサインオン」とは、仮想デスクトップやアプリケーションの起動時にパススルー認証を実行する機能を指します。この機能を「ドメイン参加の StoreFront 直接アクセス」および「ドメイン参加の NetScaler 経由の StoreFront アクセス」のスマートカード展開で使用して、ユーザーが PIN を入力する回数を減らすことができます。これらの種類の展開でシングルサインオンを使用するには、StoreFront サーバー上 default.ica で以下のパラメーターを編集します。

- ドメイン参加の StoreFront 直接アクセス—DisableCtrlAltDel を Off に設定します。
- ドメイン参加の NetScaler 経由の StoreFront アクセス—UseLocalUserAndPassword を On に設定します。

これらのパラメーター設定について詳しくは、StoreFront または Citrix Gateway のドキュメントを参照してください。

シングルサインオン機能を使用できるかどうかは、以下を含むさまざまな要因により決定されます。

- シングルサインオンに関する組織のセキュリティポリシー。
- ミドルウェアの種類と構成。
- スマートカードリーダーの種類。
- ミドルウェアの PIN キャッシュポリシー。

> 注:
>
> スマートカードリーダーが接続されたマシン上の Virtual Delivery Agent（VDA）にユーザーがログオンすると、前回使用された認証方法（スマートカードまたはパスワードなど）の画面が開く場合があります。この結果、シングルサインオンが有効な場合はシングルサインオン用のタイルが表示されます。この画面ではログオンできないため、ユーザーは［ユーザーの切り替え］をクリックしてほかの画面を開く必要があります。

Transport Layer Security（TLS）

August 17, 2024

Citrix Virtual Apps and Desktops は、コンポーネント間の TCP ベースの接続で TLS（Transport Layer Security）プロトコルをサポートしています。Citrix Virtual Apps and Desktops は、アダプティブトランスポートを使用し

て、UDP ベースの ICA/HDX 接続用の DTLS（Datagram Transport Layer Security）プロトコルもサポートしています。

TLS と DTLS は似ており、同じデジタル証明書をサポートします。TLS を使用するように Citrix Virtual Apps サイトまたは Citrix Virtual Desktops サイトを設定すると、DTLS も使用するように設定されます。次の手順を使用します。これらの手順は、TLS と DTLS の両方に共通していますが、以下の点が異なります。

- サーバー証明書を入手して、すべての Delivery Controller 上にインストールして登録します。さらに、TLS 証明書のポート構成を行います。詳しくは、「TLS サーバー証明書の Controller へのインストール」を参照してください。

  必要な場合は、Controller で HTTP および HTTPS トラフィック用に使用されるポートを変更することもできます。

- Citrix Workspace アプリと Virtual Delivery Agent（VDA）間の TLS 接続を有効にします。これを行うには、以下のタスクを実行する必要があります：

  – VDA がインストールされたマシン上で TLS を構成します（便宜上、VDA がインストールされたマシンをここでは「VDA」と呼びます）。概要については、「VDA 上の TLS 設定」を参照してください。TLS/DTLS を設定するには、Citrix 提供の PowerShell スクリプトを使用することを強くお勧めします。詳しくは、「VDA 上の TLS 構成：PowerShell スクリプトの使用」を参照してください。ただし、TLS/DTLS を手動で構成する場合は、「VDA 上の TLS 構成：手作業による構成」を参照してください。

  – VDA が追加されているデリバリーグループで TLS を構成します。これを行うには、Studio でいくつかの PowerShell コマンドレットを実行します。詳しくは、「デリバリーグループの TLS の構成」を参照してください。

    以下の要件および考慮事項があります：

    * ユーザーと VDA 間の TLS 接続を有効にするのは、XenApp 7.6 サイト、XenDesktop 7.6 サイト、およびこれ以降のリリースでのみ必要です。
    * デリバリーグループおよび VDA 上の TLS は、コンポーネントのインストール、サイトの作成、およびマシンカタログとデリバリーグループの作成を行った後で構成します。
    * デリバリーグループで TLS を構成するには、Controller のアクセス規則を変更するための権限が必要です。すべての管理権限を実行できる管理者には必要な権限が付与されています。
    * VDA 上の TLS を構成するには、そのマシン上の Windows 管理者権限が必要です。
    * Machine Creation Services または Provisioning Services によってプロビジョニングされたプールされた VDA では、VDA マシンイメージは再起動時にリセットされ、以前の TLS 設定は失われます。VDA を再起動するたびに PowerShell スクリプトを実行して、TLS 設定を再構成してください。

> 警告：
>
> Windows レジストリの編集を含むタスクの場合：レジストリの編集を誤ると、深刻な問題が発生する可能性があり、オペレーティングシステムの再インストールが必要になる場合もあります。レジストリエディターの

> 誤用による障害に対して、Citrix では一切責任を負いません。レジストリエディターは、お客様の責任と判断の範囲でご使用ください。また、レジストリファイルのバックアップを作成してから、レジストリを編集してください。

サイトデータベース接続の TLS を有効にする方法については、CTX137556を参照してください。

TLS サーバー証明書の Controller へのインストール

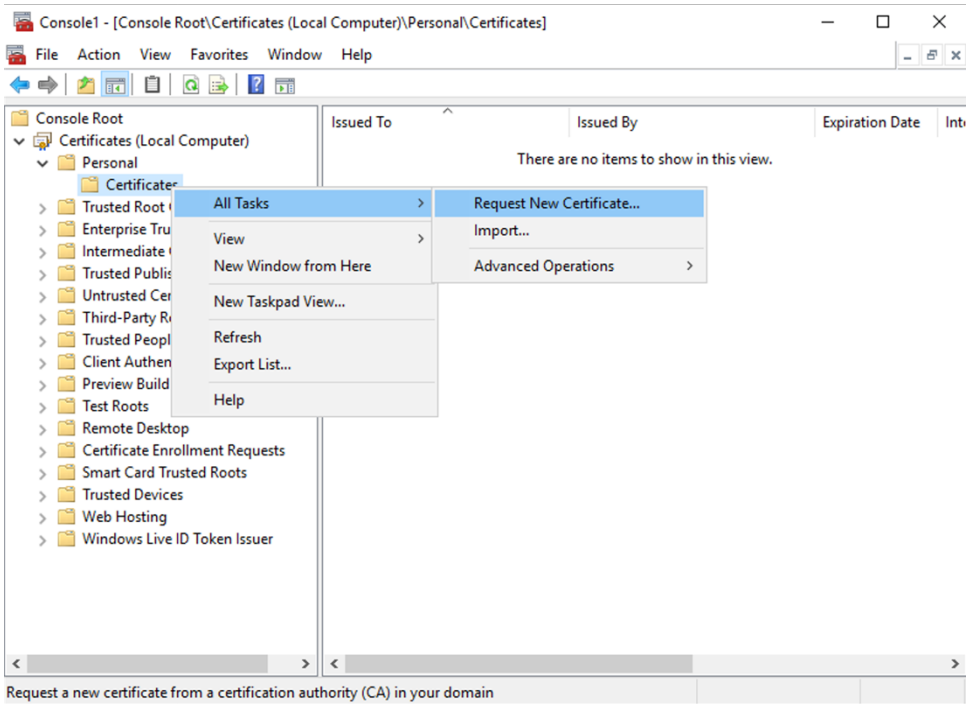
HTTPS 接続を使用する場合、XML Service はサーバー証明書を使用することで TLS 機能をサポートしますが、クライアント証明書はサポートしません。このセクションでは、Delivery Controller での TLS 証明書の取得とインストールについて説明します。同じ手順を Cloud Connector に適用して、STA および XML トラフィックを暗号化できます。

証明機関にはさまざまな種類があり、そこに証明書を要求する方法もさまざまですが、この資料では Microsoft 証明機関について説明します。Microsoft 証明機関は、サーバー認証の目的で発行された証明書テンプレートを保有している必要があります。

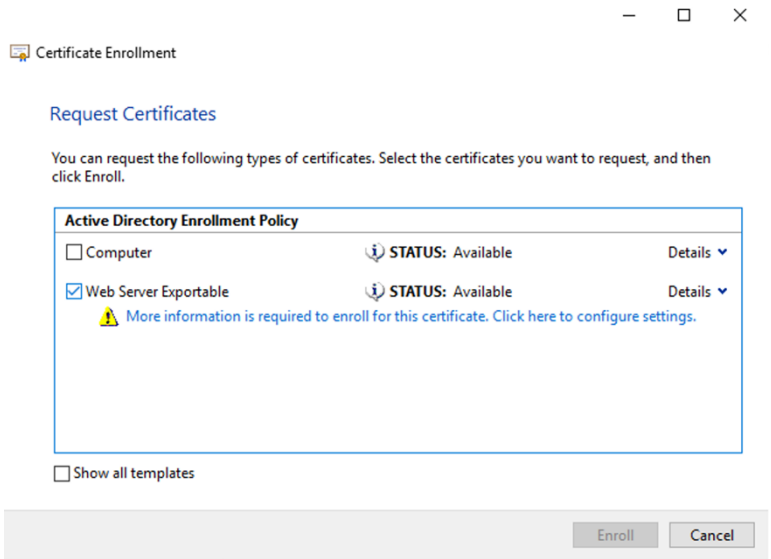
Microsoft 証明機関が、Active Directory ドメインまたは Delivery Controller が参加している信頼されたフォレストに統合されている場合は、証明書 MMC スナップインの証明書登録ウィザードから証明書を取得できます。

証明書の要求とインストール

1. Delivery Controller で、MMC コンソールを開き、証明書スナップインを追加します。プロンプトが表示されたら、［コンピューターアカウント］を選択します。
2. ［個人］**>**［証明書］を展開し、［すべてのタスク］**>**［新しい証明書の要求］コンテキストメニューコマンドを使用します。



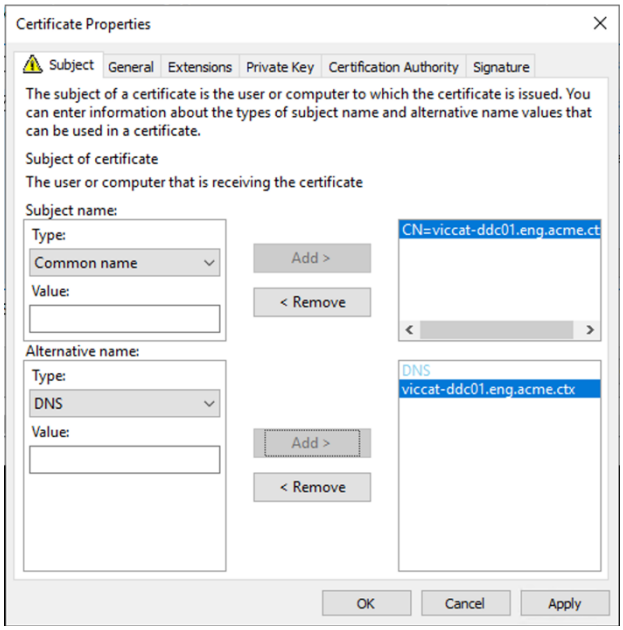
3. ［次へ］をクリックして開始し、［次へ］をクリックして、Active Directory の登録から証明書を取得していることを確認します。
4. サーバー認証証明書のテンプレートを選択します。［件名］の値が自動的に入力されるようにテンプレートが設定されている場合は、詳細を指定せずに ［登録］をクリックできます。



5. 証明書テンプレートの詳細情報を入力するには、［詳細］矢印ボタンをクリックし、次の項目を構成します：

   サブジェクト名：共通名を選択し、Delivery Controller の完全修飾ドメイン名を追加します。

   代替名： DNS を選択し、Delivery Controller の完全修飾ドメイン名を追加します。



SSL/TLS リスナーポートの構成

1. マシンの管理者として PowerShell コマンドウィンドウを開きます。
2. ブローカーサービスアプリケーション GUID を取得するには、次のコマンドを実行します:

```
New-PSDrive -Name HKCR -PSProvider Registry -Root
    HKEY_CLASSES_ROOT

$Service_Guid = Get-ChildItem HKCR:\Installer\Products -Recurse -
    Ea 0 | Where-Object {
  $key = $_; $_.GetValueNames() | ForEach-Object {
  $key.GetValue($_)  }
  | Where-Object {
  $_ -like 'Citrix Broker Service'  }
   }
  | Select-Object Name

$Service_Guid.Name -match "[A-Z0-9]*$"

$Guid = $Matches[0]

[GUID]$Formatted_Guid = $Guid

Remove-PSDrive -Name HKCR

Write-Host "Broker Service Application GUID: $($Formatted_Guid)" -
    ForegroundColor Yellow
```

3. 同じ PowerShell ウィンドウで次のコマンドを実行して、以前にインストールした証明書の拇印を取得します:


```
$HostName = ([System.Net.Dns]::GetHostByName(($env:computerName)))
    .Hostname

$Thumbprint = (Get-ChildItem -Path Cert:\LocalMachine\My | Where-
    Object {
 $_.Subject -match ("CN=" + $HostName) }
 ).Thumbprint -join ';'

Write-Host -Object "Certificate Thumbprint for $($HostName): $(
    $Thumbprint)" -Foreground Yellow
```

4. 同じ PowerShell ウィンドウで次のコマンドを実行して、ブローカーサービスの SSL/TLS ポートを構成し、暗号化用の証明書を使用します:

```
$IPV4_Address = Test-Connection -ComputerName $HostName -Count 1
    | Select-Object -ExpandProperty IPV4Address

$IPPort = "$($IPV4_Address):443"

$SSLxml = "http add sslcert ipport=$IPPort certhash=$Thumbprint
    appid={
 $Formatted_Guid }
 "

$SSLxml | netsh

. netsh http show sslcert
```

正しく構成された場合、最後のコマンド`.netsh http show sslcert`の出力に、リスナーが正しい`IP:port`を使用していること、および`Application ID`がブローカーサービスアプリケーション GUID と一致していることが示されます。

サーバーが Delivery Controller にインストールされた証明書を信頼している場合、StoreFront Delivery Controller および Citrix Gateway STA バインディングで、HTTP ではなく HTTPS を使用するように構成できます。

暗号の組み合わせの順序一覧には、`TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384`または`TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256`の暗号の組み合わせ（またはこの両方）を含める必要があります。これらの暗号の組み合わせは、`TLS_DHE_`の暗号の組み合わせより前に配置する必要があります。

1. Microsoft のグループポリシーエディターを使用して、［コンピューターの構成］**>**［管理用テンプレート］**>**［ネットワーク］**>**［**SSL** 構成設定］の順に参照します。
2.「SSL 暗号の順位」ポリシーを編集します。デフォルトでは、このポリシーは［未構成］に設定されています。このポリシーを［有効］に設定します。
3. 暗号の組み合わせを適切な順序に並び替え、使用しない暗号の組み合わせを削除します。

`TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384`または`TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256`

のどちらかがすべてのTLS_DHE_暗号の組み合わせより前に配置されていることを確認します。

Microsoft MSDN の「Prioritizing Schannel Cipher Suites」も参照してください。

HTTP または HTTPS ポートの変更

デフォルトでは、XML Service は HTTP トラフィックにはポート 80 を、HTTPS トラフィックにはポート 443 を使用します。これらのポート番号を変更することもできますが、信頼されないネットワークに Controller を露出させる場合のセキュリティ上のリスクについて考慮してください。デフォルト構成を変更する場合は、スタンドアロンの StoreFront サーバーを使用することをお勧めします。

Controller で使用されるデフォルトの HTTP または HTTPS ポートを変更するには、Studio で次のコマンドを実行します:

```
BrokerService.exe -WIPORT \<http-port> -WISSLPORT \<https-port>
```

ここで、<http-port>は HTTP トラフィックのポート番号で、<https-port>は HTTPS トラフィックのポート番号です。

> 注:
>
> ポートが変更されると、ライセンスの互換性およびアップグレードに関するメッセージが Studio に表示されます。この問題を解決するには、以下の PowerShell コマンドレットを順に実行してサービスインスタンスを再登録してください:

```
1 Get-ConfigRegisteredServiceInstance -ServiceType Broker -Binding
     XML_HTTPS |
2 Unregister-ConfigRegisteredServiceInstance
3 Get-BrokerServiceInstance | where Binding -eq "XML_HTTPS" |
4 Register-ConfigServiceInstance
```

HTTPS トラフィックのみに制限する

HTTP トラフィックが XML Service で無視されるように構成するには、Controller 上の HKEY_LOCAL_MACHINE\Software\Cit
以下のレジストリ設定を作成してから Broker Service を再起動します。

HTTP トラフィックを無視するには、DWORD XmlServicesEnableNonSsl を作成して 0 に設定します。

同様に、HTTPS トラフィックを無視するために作成できるレジストリの DWORD 値も存在します: DWORD XmlServicesEnableSsl これは 0 に設定しないでください。

VDA 上の TLS 設定

TLS を構成した VDA と構成していない VDA を同一デリバリーグループ内で混在させることはできません。デリバリーグループの TLS を構成する前に、そのグループに属しているすべての VDA 上で TLS 構成を完了しておいてください。

VDA 上に TLS を構成すると、インストールされている TLS 証明書の権限が変更され、その証明書の秘密キーに対する読み取り権限が ICA Service に付与されます。ICA Service には、以下の情報が提供されます:

- **TLS** で使用される証明書ストア内の証明書。
- **TLS** 接続で使用される **TCP** ポート番号。

  Windows ファイアウォールを使用する環境では、この TCP での着信接続が許可されている必要があります。PowerShell スクリプトを使用する場合は、このファイアウォール規則が自動的に構成されます。
- どのバージョンの **TLS** プロトコルが許可されるのか。

  > 重要:
  >
  > SSLv3 の使用状況を確認し、必要に応じ、それらの展開を再構成して SSLv3 のサポートを削除することを Citrix ではお勧めします。CTX200238を参照してください。

  サポートされる TLS プロトコルのバージョンは次の通りです:(低いものから)SSL 3.0、TLS 1.0、TLS 1.1、TLS 1.2、および TLS 1.3。サポートされる SSL プロトコルを指定するときは、許可する最低バージョンを指定します。

  たとえば、最低バージョンとして TLS 1.1 を指定すると、TLS 1.1 および TLS 1.3 のプロトコルを使用した接続が許可されます。最低バージョンとして SSL 3.0 を指定すると、サポートされる SSL プロトコルのすべてのバージョンが許可されます。最低バージョンとして TLS 1.3 を指定すると、TLS 1.3 の接続のみが許可されます。

  DTLS 1.0 は TLS 1.1 に対応し、DTLS 1.3 は TLS 1.3 に対応します。
- どの **TLS** 暗号の組み合わせが許可されるのか。

  暗号の組み合わせにより、この接続において使用する暗号化が選択されます。クライアントと VDA は、暗号スイートの異なる組み合わせをサポートできます。クライアント(Citrix Workspace アプリまたは StoreFront)が VDA に接続するときは、そのクライアントがサポートする TLS 暗号スイートの一覧を VDA に送信します。VDA 側では、構成済みの暗号スイートの独自の一覧内にクライアントのいずれかの暗号スイートと一致するものがあるかどうかがチェックされ、あった場合にのみ接続が確立されます。一致する暗号スイートがない場合、その接続は VDA により拒否されます。

  VDA は、GOV(ernment)、COM(mercial)、および ALL の 3 つの暗号の組み合わせ(コンプライアンスモードとも呼ばれます)をサポートします。確立できる暗号スイートは、Windows の FIPS モードによっても異なります。Windows の FIPS モードについては、http://support.microsoft.com/kb/811833を参照してください。次の表は、各セットの暗号の組み合わせを示しています:

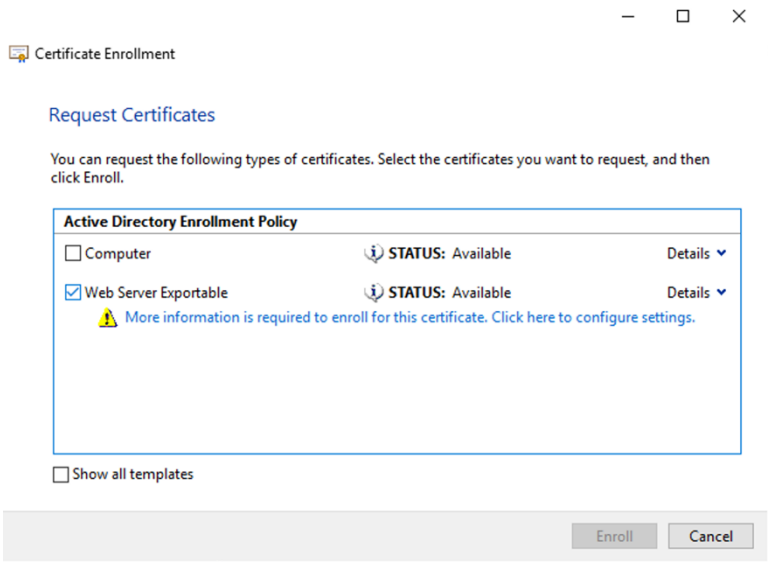
TLS/DTLS						
暗号の組み合わせ	**ALL**	**COM**	**GOV**	**ALL**	**COM**	**GOV**
FIPS モード	オフ	オフ	オフ	On	On	On

TLS/DTLS 暗号の組み合わせ	ALL	COM	GOV	ALL	COM	GOV
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	X		X	X		X
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	X		X	X		X
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	X			X	X	

> 注:
>
> VDA では、DHE 暗号スイート（例：TLS_DHE_RSA_WITH_AES_256_GCM_SHA384、TLS_DHE_RSA_WITH_AES_256_CB TLS_DHE_RSA_WITH_AES_128_GCM_SHA256、TLS_DHE_RSA_WITH_AES_128_CBC_SHA）はサポートされません。これらの暗号スイートが Windows で選択されても、Citrix Receiver では使用できません。
>
> Citrix Gateway を使用している場合、バックエンド通信に対する暗号の組み合わせのサポートについては、Citrix ADC のドキュメントを参照してください。TLS がサポートする暗号の組み合わせについては、「Citrix ADC アプライアンスで利用可能な暗号」を参照してください。DTLS がサポートする暗号の組み合わせについては、「DTLS 暗号サポート」を参照してください。

証明書の要求とインストール

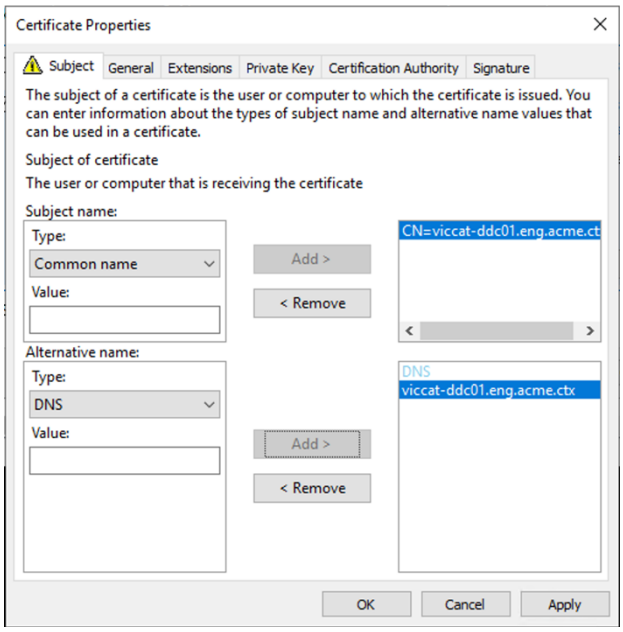
1. VDA で、MMC コンソールを開き、証明書スナップインを追加します。プロンプトが表示されたら、［コンピューターアカウント］を選択します。
2. ［個人］**>**［証明書］を展開し、コンテキストメニューコマンドの ［すべてのタスク］**>**［新しい証明書の要求］を使用します。
3. ［次へ］をクリックして開始し、［次へ］をクリックして、Active Directory の登録から証明書を取得していることを確認します。
4. サーバー認証証明書のテンプレートを選択します。デフォルトの Windows の **Computer** または **Web Server Exportable** の両方が使用できます。［件名］の値が自動的に入力されるようにテンプレートが設定されている場合は、詳細を指定せずに ［登録］をクリックできます。



5. 証明書テンプレートの詳細情報を入力するには、［詳細］をクリックし、次の項目を構成します：

   サブジェクト名—種類は ［共通名］を選択し、VDA の完全修飾ドメイン名を追加します。

   代替名—種類は ［**DNS**］を選択し、VDA の完全修飾ドメイン名を追加します。

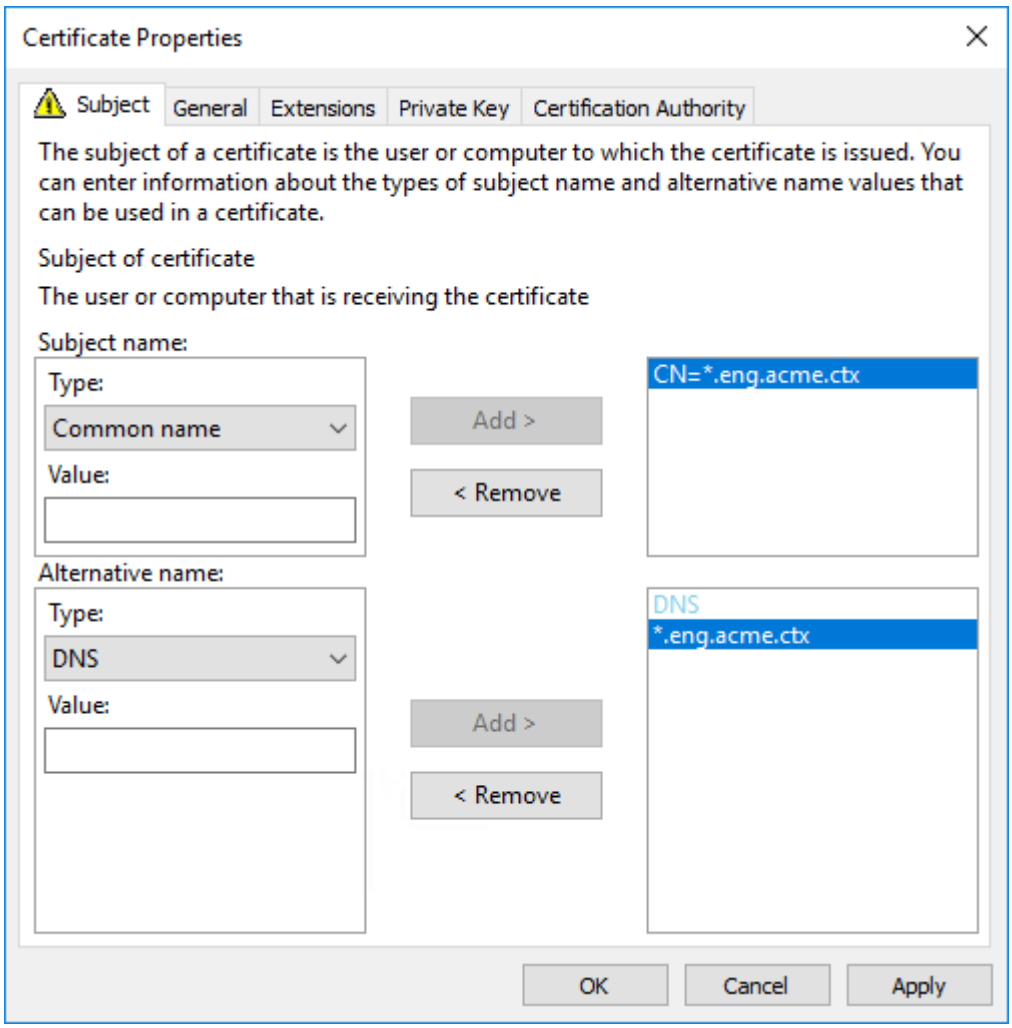


> 注：
>
> Active Directory 証明書サービスの証明書の自動登録を使用して、VDA への証明書の発行と展開を自動化します。これについては、https://support.citrix.com/article/CTX205473に説明があります。

ワイルドカード証明書を使用して、単一の証明書で複数の VDA を保護するように設定できます：

サブジェクト名—種類は ［共通名］を選択し、VDA の「*.primary.domain」を入力します。

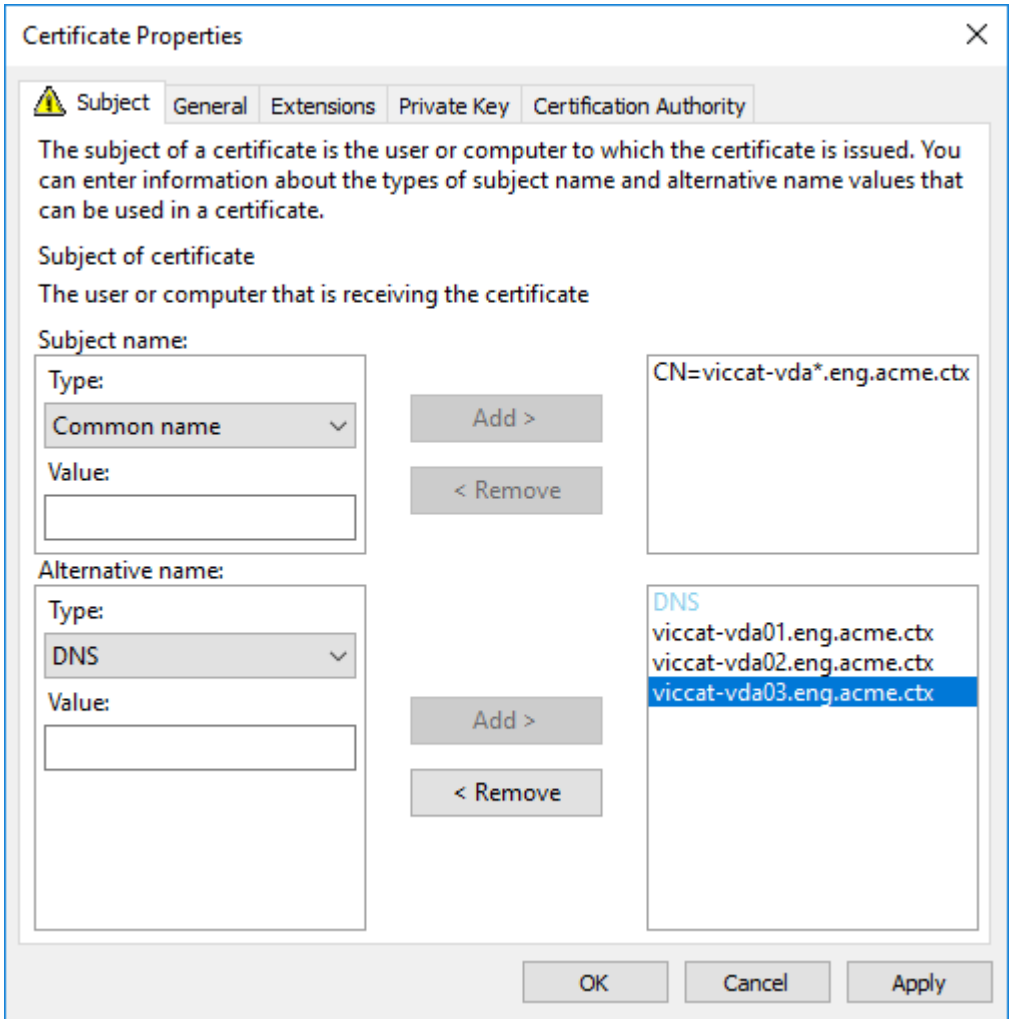
代替名—種類は ［**DNS**］を選択し、VDA の「*.primary.domain」を追加します。



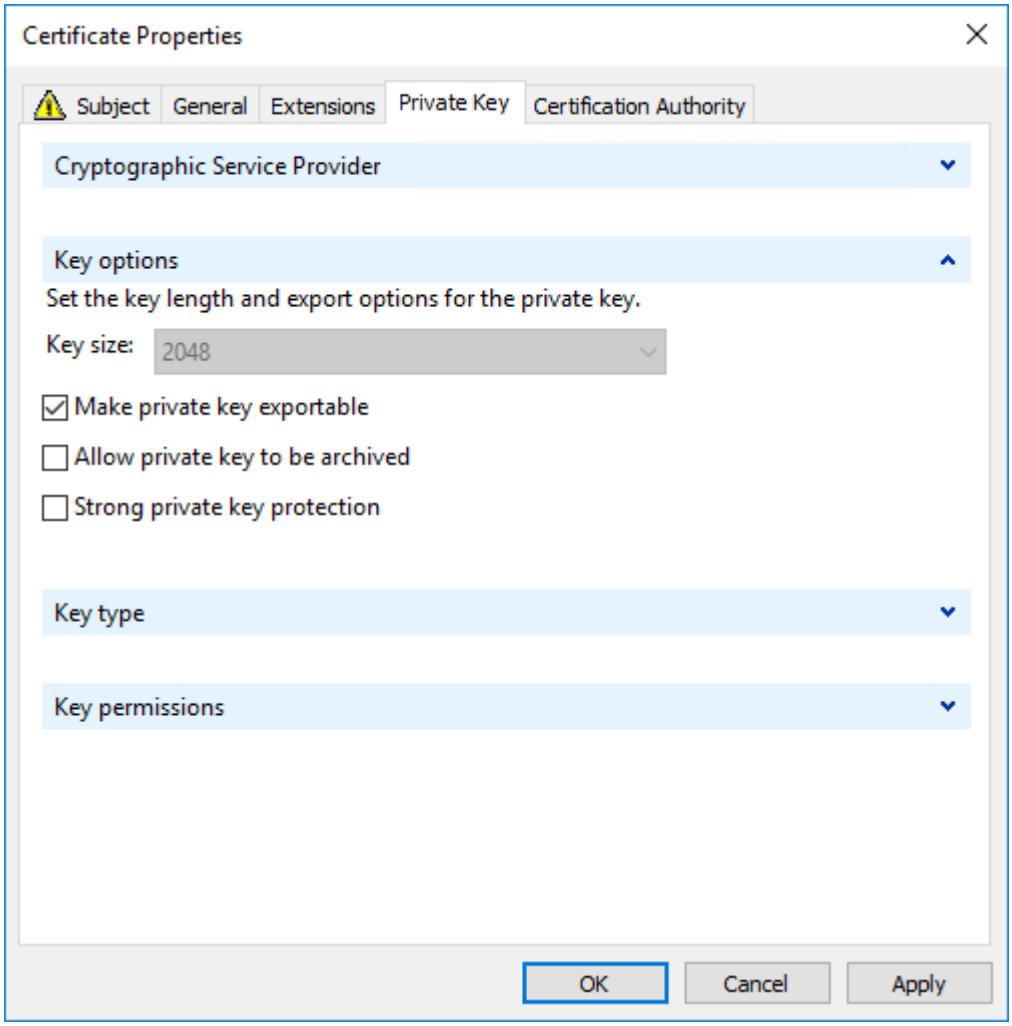
SAN 証明書を使用して、単一の証明書で複数の指定の VDA を保護するように設定できます:

サブジェクト名—種類は ［共通名］を選択し、証明書の使用方法を識別するのに役立つ文字列を入力します。

代替名—種類は ［**DNS**］を選択し、各 VDA の完全修飾ドメイン名を入力します。最適な TLS ネゴシエーションを確保するために、代替名の数を最小限にします。



> 注:
>
> ワイルドカード証明書と SAN 証明書の両方で、［秘密キー］タブの ［秘密キーをエクスポート可能にする］をオンにする必要があります:



VDA 上の **TLS** 構成：**PowerShell** スクリプトの使用

証明書ストアの［ローカルコンピューター］>［個人］>［証明書］領域にある TLS 証明書をインストールします。その場所に複数の証明書が存在する場合は、証明書の拇印を PowerShell スクリプトに指定します。

> 注：
>
> PowerShell スクリプトは、XenApp および XenDesktop 7.16 LTSR から、VDA の完全修飾ドメイン名に基づいて正しい証明書を検索します。VDA の完全修飾ドメイン名に 1 つの証明書のみが存在する場合は、拇印を指定する必要はありません。

VDA 上で Enable-VdaSSL.ps1 スクリプトを実行すると、その VDA での TLS リスナーを有効または無効にできます。このスクリプトは、インストールメディアの *Support* > *Tools* > *SslSupport* フォルダーに収録されています。

TLS を有効にすると、DHE の暗号の組み合わせは無効になります。ECDHE の暗号の組み合わせは影響を受けません。

TLS を有効にすると、スクリプトは指定された TCP ポートの既存の Windows ファイアウォール規則をすべて無効にします。その後、ICA サービスが TLS TCP および UDP ポートでのみ着信接続を受け入れることを許可する新しい規則を追加します。また、スクリプトにより以下の Windows ファイアウォール規則が無効になります:

- Citrix ICA（デフォルトで 1494）
- Citrix CGP（デフォルトで 2598）
- Citrix WebSocket（デフォルトで 8008）

ユーザーは TLS または DTLS を使用した場合にのみ接続できるようになります。TLS または DTLS を使用しないと、ICA/HDX、セッション画面を保持した ICA/HDX、WebSocket を介した HDX を使用することはできません。

> 注:
>
> DTLS は、ICA/HDX の UDP でのオーディオリアルタイムトランスポート、または ICA/HDX Framehawk ではサポートされていません。

「ネットワークポート」を参照してください。

このスクリプト内には、以下の構文および使用例が記載されています。Notepad++ などのツールを使用してこれらを参照できます。

> 重要:
>
> Enable または Disable パラメーターと CertificateThumbPrint パラメーターを指定します。その他のパラメーターはオプションです。

構　文 `Enable-VdaSSL { -Enable | -Disable } -CertificateThumbPrint "<thumbprint>"[-SSLPort <port>] [-SSLMinVersion "<min-ssl-version>"] [-SSLCipherSuite"\<suite>"]`

パラメーター	説明
Enable	TLS リスナーを VDA 上にインストールして有効にします。このパラメーターまたは Disable パラメーターのいずれかを指定する必要があります。
Disable	VDA 上の TLS リスナーを無効にします。このパラメーターまたは Enable パラメーターのいずれかを指定する必要があります。このパラメーターを指定した場合、ほかのパラメーターは無視されます。
CertificateThumbPrint “”	証明書ストア内の TLS 証明書の拇印を二重引用符で囲んで指定します。スクリプトは、指定された拇印によって使用する証明書を選択します。このパラメーターを省略すると、不正な証明書が選択されます。
SSLPort	TLS ポート指定します。デフォルト：443

パラメーター	説明
SSLMinVersion “”	許可される TLS プロトコルの最低バージョンを二重引用符で囲んで指定します。有効な値:「TLS_1.0」(デフォルト)、「TLS_1.1」、「TLS_1.3」。
SSLCipherSuite “”	TLS 暗号スイートを二重引用符で囲んで指定します。使用できる値は、「GOV」、「COM」、および「ALL」(デフォルト)です。

例　次のスクリプトでは、TLS プロトコルバージョン値をインストールして有効にします。拇印(この例の場合、「12345678987654321」)を指定して、使用する証明書を選択します。

```
Enable-VdaSSL -Enable -CertificateThumbPrint "12345678987654321"
```

次のスクリプトでは、TLS リスナーをインストールして有効化し、TLS ポートとして 400、暗号スイート GOV、および SSL プロトコルの最低バージョンとして TLS 1.2 を設定します。拇印(この例の場合、「12345678987654321」)を指定して、使用する証明書を選択します。

```
Enable-VdaSSL -Enable
-CertificateThumbPrint "12345678987654321"
-SSLPort 400 -SSLMinVersion "TLS_1.3"
-SSLCipherSuite "All"
```

次のスクリプトでは、VDA 上の TLS リスナーを無効にします。

```
Enable-VdaSSL -Disable
```

VDA 上の **TLS** 構成:手作業による構成

VDA 上の TLS を手作業で構成するには、TLS 証明書の秘密キーに対する読み取り権限を VDA 上の NT SERVICE\PorticaService(Windows シングルセッション OS 対応 VDA の場合)または NT SERVICE\TermService(Windows マルチセッション OS 対応 VDA の場合)に付与します。VDA がインストールされたマシン上で、以下の手順を行います:

手順 **1**: Microsoft 管理コンソール(MMC)を起動します:[スタート]>[ファイル名を指定して実行]>mmc.exe。

手順 **2**:MMC に証明書スナップインを追加します。

1. [ファイル]>[スナップインの追加と削除]の順に選択します。
2. [証明書]を選択して[追加]をクリックします。
3. [このスナップインで管理する証明書]で[コンピューターアカウント]をクリックし、[次へ]をクリックします。
4. [このスナップインで管理するコンピューター]で[ローカルコンピューター]をクリックし、[完了]をクリックします。

手順 **3**: コンソールツリーの［証明書（ローカルコンピューター）］>［個人］>［証明書］で証明書を右クリックして、［すべてのタスク］>［秘密キーの管理］の順に選択します。

手順 **4**: アクセス制御リストエディターで［(FriendlyName）プライベートキーのアクセス許可］ダイアログボックスが開きます。ここで（FriendlyName）は、TLS 証明書の名前です。以下のいずれかのサービスを追加して、［読み取り］アクセスを許可します。

- Windows シングルセッション OS 対応 VDA では「PORTICASERVICE」
- Windows マルチセッション OS 対応 VDA では「TERMSERVICE」

手順 **5**: インストールした TLS 証明書をダブルクリックします。［証明書］ダイアログボックスの［詳細］タブをクリックして、一番下までスクロールします。［拇印］をクリックします。

手順 **6**: regedit を実行して、HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd を開きます。

1. SSL Thumbprint キーを編集して、TLS 証明書の拇印の値をバイナリ値にコピーします。［バイナリ値の編集］ダイアログボックスでは、不明な項目（「0000」や特殊文字など）は無視して構いません。
2. SSLEnabled キーを編集して、DWORD 値を 1 に変更します（この DWORD 値を 0 にすると SSL が無効になります)。
3. このレジストリパスでは、必要に応じて以下のデフォルト値を変更できます。

   SSLPort の DWORD 値–SSL ポート番号。デフォルト: 443。

   SSLMinVersion の DWORD 値–1 = SSL 3.0、2 = TLS 1.0、3 = TLS 1.1、4 = TLS 1.3。デフォルト: 2 (TLS 1.0)。

   SSLCipherSuite の DWORD 値–1 = GOV、2 = COM、3 = ALL。デフォルト: 3（ALL)。

手順 **7**: デフォルトの 443 以外の TLS TCP ポートおよび UDP ポートを使用する場合は、そのポートが Windows ファイアウォールで開放されていることを確認します（Windows ファイアウォールで受信規則を作成するときは、［接続を許可する］および［有効］が選択されていることを確認してください)。

手順 **8**: ほかのアプリケーションやサービスなど（IIS など）がその TLS TCP ポートを使用していないことを確認します。

手順 **9**: Windows マルチセッション OS 対応 VDA の場合は、変更を適用するためのマシンを再起動します (Windows シングルセッション OS 対応 VDA のマシンを再起動する必要はありません)。

> 重要:
>
> VDA が、Windows 10 Anniversary Edition 以降のサポートリリースにインストールされている場合は、追加の手順が必要になります。これは、Citrix Receiver for Windows（バージョン 4.6～4.9)、HTML5 向け Citrix Workspace アプリ、および Chrome 向け Citrix Workspace アプリからの接続に影響します。これには、Citrix Gateway を使用した接続も含まれます。
>
> この手順は、Citrix Gateway と VDA 間の TLS が設定されている場合、すべての VDA バージョンで Citrix

> Gateway を使用するすべての接続にも必要です。これは Citrix Receiver のすべてのバージョンに影響します。

グループポリシーエディターを使用する VDA（Windows 10 Anniversary Edition 以降）上で、［コンピューターの構成］>［ポリシー］>［管理用テンプレート］>［ネットワーク］>［SSL 構成設定］>［SSL 暗号の順位］と移動します。以下の順に選択します：

```
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384_P384
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384_P256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P384
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P384
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P256
```

> 注：
>
> 最初の 6 つの項目は、楕円曲線、P384、または P256 も指定します。［curve25519］が選択されていないことを確認します。FIPS モードは、「curve25519」の使用を妨げません。

このグループポリシー設定が構成されると、VDA は、暗号の組み合わせを、グループポリシーの一覧と選択されたコンプライアンスモード（COM、GOV または ALL）の一覧の両方に表示されている場合のみ選択します。また、暗号の組み合わせは、クライアント（Citrix Workspace アプリまたは StoreFront）が送信する一覧にも記載されている必要があります。

このグループポリシー構成は、VDA 上の他の TLS アプリケーションおよびサービスにも影響します。アプリケーションが特定の暗号スイートを必要とする場合、このグループポリシーの一覧に追加する必要がある場合があります。

> 重要：
>
> グループポリシーの変更が適用されたときに表示されても、TLS 構成のグループポリシーの変更は、オペレーティングシステムの再起動後にのみ有効になります。したがって、プールデスクトップの場合、TLS 構成のグループポリシーの変更は基本イメージに適用してください。

デリバリーグループの **TLS** の構成

TLS 接続を構成した VDA を含んでいるすべてのデリバリーグループで、以下の手順を行います。

1. Studio から PowerShell コンソールを開きます。
2. **asnp Citrix.*** を実行して Citrix 製品のコマンドレットをロードします。
3. **Get-BrokerAccessPolicyRule -DesktopGroupName '*<delivery-group-name>*' | Set-BrokerAccessPolicyRule -HdxSslEnabled $true** を実行します。
4. **Set-BrokerSite -DnsResolutionEnabled $true** を実行します。

トラブルシューティング

接続エラーが発生した場合は、VDA のシステムイベントログを確認してください。

Windows 向け Citrix Workspace アプリで TLS 関連の接続エラーが発生した場合は、Desktop Viewer を無効にしてから接続を再試行してください。接続エラーは解決されないままでも、TLS の問題についての情報が表示される場合があります。たとえば、証明機関に証明書を要求したときに正しくないテンプレートを使用したなどがあります。

HDX アダプティブトランスポートを使用するほとんどの構成は、DTLS で正常に機能します（最新バージョンの Citrix Workspace アプリ、Citrix Gateway、および VDA を使用する DTLS など）。Citrix Workspace アプリと Citrix Gateway との間で DTLS を使用する構成、および Citrix Gateway と VDA との間で DTLS を使用する構成には、追加で操作が必要な場合があります。

次の場合は、追加で操作が必要になります。

- HDX アダプティブトランスポートおよび DTLS をサポートする Citrix Receiver バージョン：Receiver for Windows（4.7、4.8、4.9）、Receiver for Mac（12.5、12.6、12.7）、Receiver for iOS（7.2、7.3.x）、または Receiver for Linux（13.7）

および、次のいずれかにも該当する場合：

- Citrix Gateway バージョンで VDA への DTLS がサポートされていますが、VDA バージョンで DTLS（バージョン 7.15 以前）がサポートされていません。
- VDA バージョンで DTLS（バージョン 7.16 以降）がサポートされていますが、Citrix Gateway バージョンで VDA への DTLS がサポートされていません。

Citrix Receiver からの接続が失敗しないようにするには、次のいずれかを実行します。

- Citrix Receiver を、Receiver for Windows Version 4.10 以降、Receiver for Mac 12.8 以降、または Receiver for iOS Version 7.5 以降に更新します。または、
- Citrix Gateway を、VDA への DTLS をサポートしているバージョンに更新します。または、
- VDA をバージョン 7.16 以降に更新します。または、
- VDA で DTLS を無効にします。または、
- HDX アダプティブトランスポートを無効にします。

> 注：
>
> Receiver for Linux 用の適切な更新プログラムは、まだ利用できません。Receiver for Android（バージョン 3.12.3）は、HDX アダプティブトランスポート、および Citrix Gateway を介した DTLS をサポートしていないため、影響を受けません。
>
> VDA で DTLS を無効にするには、VDA ファイアウォール構成を変更して UDP ポート 443 を無効にします。「ネットワークポート」を参照してください。

Controller と VDA の間の通信

Windows Communication Framework（WCF）のメッセージレベルの保護によって、Controller と VDA との間の通信がセキュリティで保護されます。TLS を使用した追加の移送レベルの保護は必要ありません。WCF 構成で

は、Controller と VDA 間の相互認証に Kerberos が使用されます。暗号化には、CBC モードでの AES が 256 ビットキーで使用されます。メッセージの整合性には SHA-1 が使用されます。

Microsoft によると、WCF で使用されるセキュリティプロトコルは、WS-SecurityPolicy 1.2 を含む OASIS（Organization for the Advancement of Structured Information Standards）による標準に準拠しています。さらに、WCF は『Security Policy 1.2』に表記されているアルゴリズムスイートすべてをサポートしていることも明言されています。

Controller と VDA 間の通信には、上述のアルゴリズムによる basic256 アルゴリズムスイートが使用されます。

TLS および **HTML5** ビデオリダイレクション、およびブラウザーコンテンツリダイレクト

HTML5 ビデオリダイレクションおよびブラウザーコンテンツリダイレクトを使用して、HTTPS Web サイトをリダイレクトできます。これらの Web サイトに挿入された JavaScript は、VDA で動作する Citrix HDX HTML5 ビデオリダイレクトサービスへの TLS 接続を確立する必要があります。これを達成するために、HTML5 ビデオリダイレクトサービスは VDA の証明書ストアで 2 つのカスタム証明書を生成します。このサービスを停止すると、証明書が削除されます。

HTML5 ビデオリダイレクションポリシーはデフォルトで無効になっています。

Web ブラウザーコンテンツリダイレクトは、デフォルトで有効になっています。

HTML5 ビデオリダイレクトについて詳しくは、「マルチメディアのポリシー設定」を参照してください。

ユニバーサルプリントサーバーの **Transport Layer Security**（**TLS**）

August 17, 2024

Transport Layer Security（TLS）プロトコルは、Virtual Delivery Agent（VDA）とユニバーサルプリントサーバーとの間の TCP ベースの接続でサポートされています。

> 警告：
>
> Windows レジストリの編集を含むタスクの場合：レジストリの編集を誤ると、深刻な問題が発生する可能性があり、オペレーティングシステムの再インストールが必要になる場合もあります。レジストリエディターの誤用による障害に対して、Citrix では一切責任を負いません。レジストリエディターは、お客様の責任と判断の範囲でご使用ください。また、レジストリファイルのバックアップを作成してから、レジストリを編集してください。

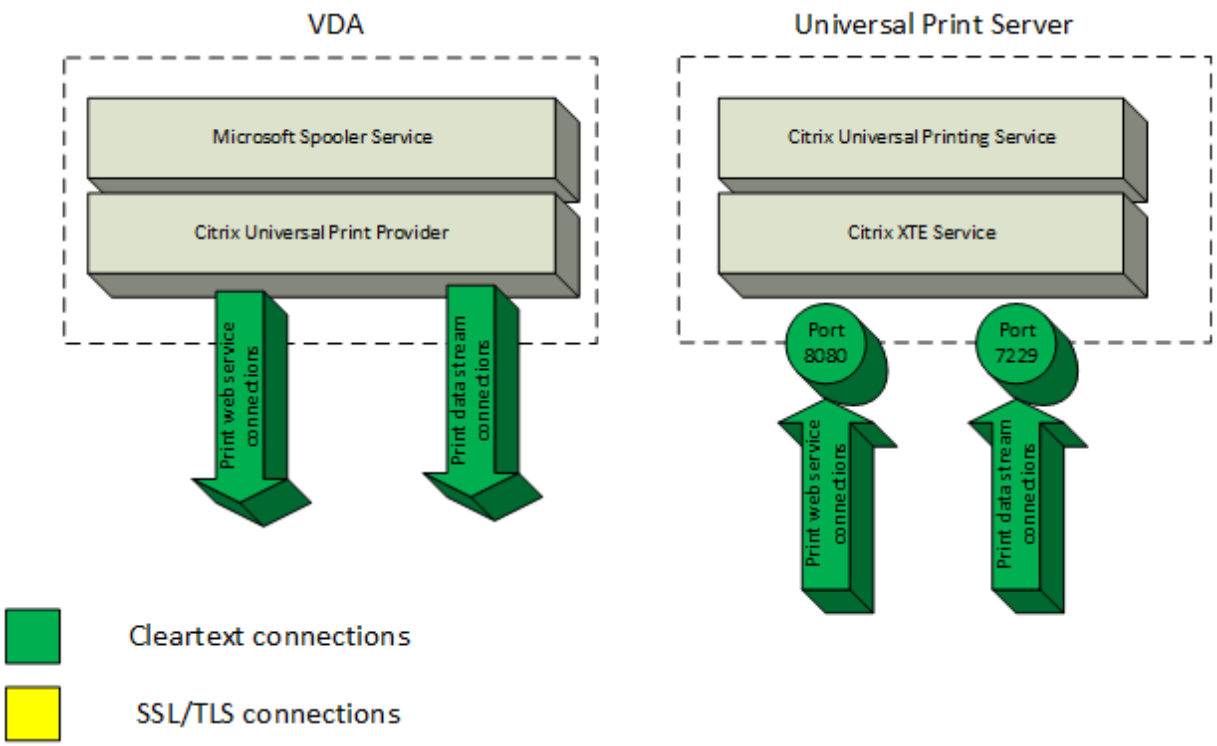
VDA とユニバーサルプリントサーバー間の印刷接続の種類

クリアテキスト接続

印刷に関連する次の接続は VDA から開始され、ユニバーサルプリントサーバーのポートに接続します。これらの接続は、［**SSL** が有効］ポリシー設定が **Disabled**（デフォルト）に設定されている場合のみ確立されます。

- クリアテキスト印刷 Web サービス接続（TCP ポート：8080）
- クリアテキスト印刷データストリーム（CGP）接続（TCP ポート：7229）

Microsoft Windows 印刷スプーラーサービスで使用されるポートについては、Microsoft のサポート記事Service overview and network port requirements for Windowsを参照してください。このドキュメントの SSL/TLS 設定は、NetBIOS および Windows 印刷スプーラーサービスで確立された RPC 接続には適用されません。［ユニバーサルプリントサーバーの有効化］ポリシー設定が ［有効。**Windows** のリモート印刷機能にフォールバックする］に設定されている場合、VDA は Windows ネットワーク印刷プロバイダー（win32spl.dll）をフォールバックとして使用します。

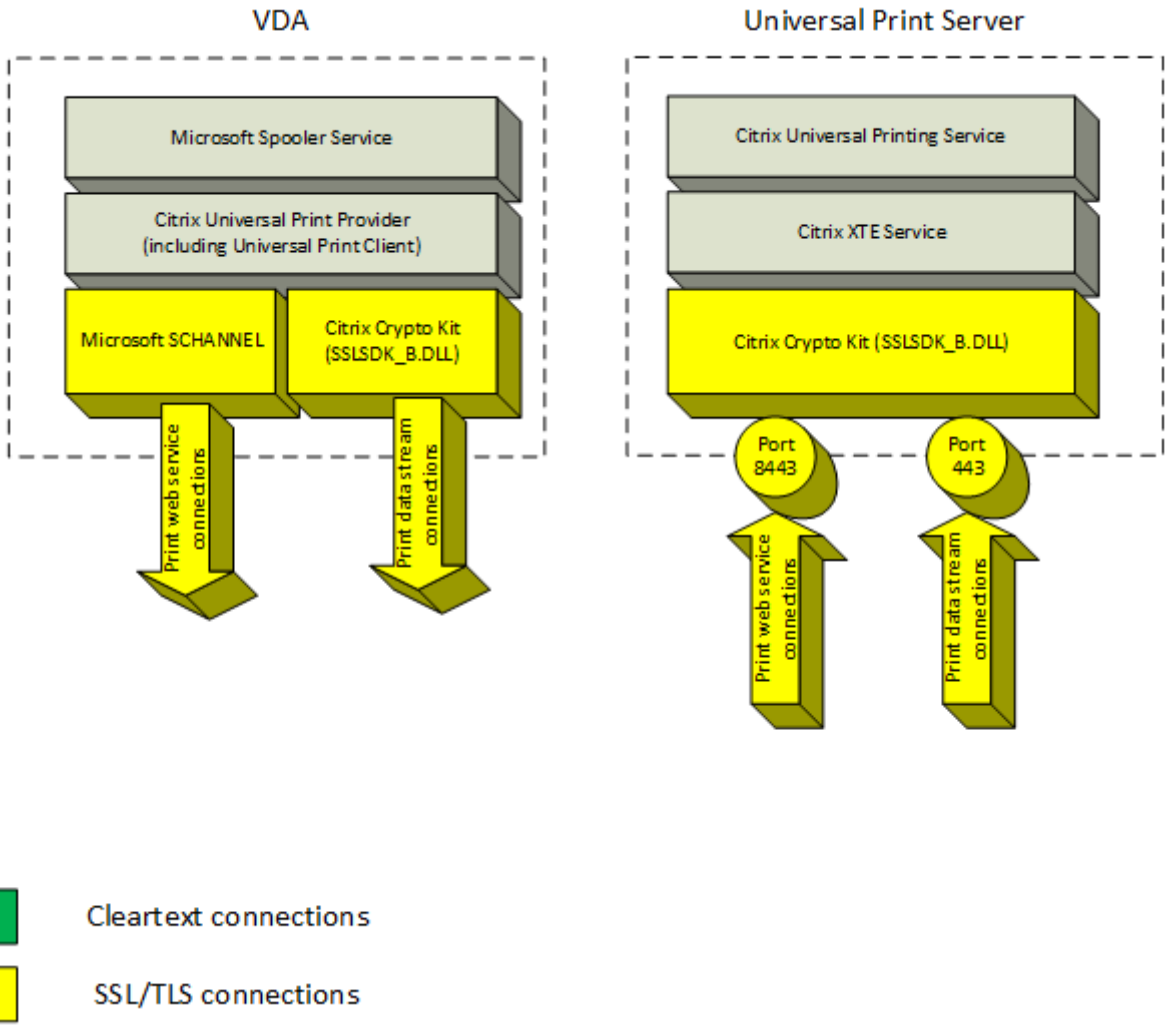


暗号化された接続

印刷に関連する SSL/TLS 接続は、VDA から開始されユニバーサルプリントサーバーのポートに接続します。これらの接続は、［**SSL** が有効］ポリシー設定が **Enable** に設定されている場合のみ確立されます。

- 暗号化印刷 Web サービス接続（TCP ポート：8443）

- 暗号化印刷データストリーム（CGP）接続（TCP ポート：443）



SSL/TLS クライアント構成

VDA は SSL/TLS クライアントとして機能します。

Microsoft のグループポリシーとレジストリを使用して、暗号化印刷 Web サービス接続（TCP ポート：8443）で Microsoft SCHANNEL SSP を構成します。Microsoft SCHANNEL SSP のレジストリ設定については、Microsoft のサポート記事TLS Registry Settingsを参照してください。

グループポリシーエディターを使用する VDA 上で、［コンピューターの構成］**>**［管理用テンプレート］**>**［ネットワーク］**>**［**SSL** 構成設定］**>**［**SSL** 暗号の順位］と移動します。TLS 1.3 が設定されている場合、以下の順に選択します：

TLS_AES_256_GCM_SHA384
TLS_AES_128_GCM_SHA256

TLS 1.2 が設定されている場合、以下の順に選択します:

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384_P384
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384_P256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P384
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P384
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P256

> 注:
>
> このグループポリシー設定が構成されている場合、暗号化印刷 Web サービス接続（デフォルトポート：8443）が両方の SSL 暗号の組み合わせ一覧に表示されているときのみ、VDA は暗号の組み合わせを選択します:
>
> - グループポリシーの SSL 暗号の組み合わせ順一覧
> - 選択した SSL 暗号の組み合わせポリシー設定（COM、GOV、または ALL）に関連した一覧
>
> このグループポリシー構成は、VDA 上の他の TLS アプリケーションおよびサービスにも影響します。アプリケーションが特定の暗号の組み合わせを必要とする場合、このグループポリシーの暗号の組み合わせ順一覧に追加することが必要な場合があります。
>
> 重要:
>
> TLS 構成のグループポリシーの変更は、オペレーティングシステムの再起動後にのみ有効になります。
>
> Citrix ポリシーを使用して暗号化印刷データストリーム（CGP）接続（TCP ポート：443）の SSL/TLS 設定を構成します。

SSL/TLS サーバー構成

ユニバーサルプリントサーバーは、SSL/TLS サーバーとして機能します。

`Enable-UpsSsl.ps1` PowerShell スクリプトを使用して SSL/TLS 設定を構成します。

ユニバーサルプリントサーバーに **TLS** サーバー証明書をインストールする

HTTPS 接続を使用する場合、ユニバーサルプリントサーバーはサーバー証明書を使用することで TLS 機能をサポートします。クライアント証明書はサポートしません。Microsoft Active Directory 証明書サービスまたは他の証明機関を使用して、ユニバーサルプリントサーバーの証明書を要求します。

Microsoft Active Directory 証明書サービスを使用して証明書を登録/要求する場合、次の点に注意してください:

1. 証明書をローカルコンピューターの個人証明書ストアに配置します。
2. 証明書のサブジェクト識別名（Subject DN）のコモンネーム属性をユニバーサルプリントサーバーの完全修飾ドメイン名（FQDN）に設定します。証明書テンプレートでこれを指定します。

3. 証明書要求や秘密キーの生成に使用される暗号化サービスプロバイダー（CSP）を **Microsoft Enhanced RSA** および **AES Cryptographic Provider**（暗号）に設定します。証明書テンプレートでこれを指定します。
4. キーサイズを 2048 ビット以上に設定します。証明書テンプレートでこれを指定します。

ユニバーサルプリントサーバーで **SSL** を構成する

ユニバーサルプリントサーバー上の XTE サービスは、受信接続を待機します。SSL が有効な場合は、SSL サーバーとして機能します。受信接続には、印刷コマンドを含む印刷 Web サービス接続と、印刷ジョブを含む印刷データストリーム接続の 2 種類があります。これらの接続で SSL を有効にできます。SSL はこれらの接続の機密性と完全性を保護します。デフォルトでは、SSL は無効になっています。

SSL の構成に使用される PowerShell スクリプトはインストールメディアにあり、次のファイル名です：`\Support\Tools\SslSupport\Enable-UpsSsl.ps1`.

ユニバーサルプリントサーバーでリスニングポート番号を構成する

以下は XTE サービス用のデフォルトのポートです：

- クリアテキスト印刷 Web サービス（HTTP）TCP ポート：8080
- クリアテキスト印刷データストリーム（CGP）TCP ポート：7229
- 暗号化印刷 Web サービス（HTTPS）TCP ポート：8443
- 暗号化印刷データストリーム（CGP）TCP ポート：443

ユニバーサルプリントサーバー上の XTE サービスで使用されるポートを変更するには、管理者として次の PowerShell コマンドを実行します（Enable-UpsSsl.ps1 PowerShell スクリプトの使用に関する注意事項については後述を参照してください）：

1. `Stop-Service CitrixXTEServer, UpSvc`
2. `Enable-UpsSsl.ps1 -Enable -HTTPSPort <port> -CGPSSLPort <port>` または `Enable-UpsSsl.ps1 -Disable -HTTPPort <port> -CGPPort <port>`
3. `Start-Service CitrixXTEServer`

ユニバーサルプリントサーバーの **TLS** 設定

負荷分散構成で複数のユニバーサルプリントサーバーがある場合、すべてのユニバーサルプリントサーバー上で一貫した **TLS** 設定を構成するようにしてください。

ユニバーサルプリントサーバー上に TLS を構成すると、インストールされている TLS 証明書の権限が変更され、その証明書の秘密キーに対する読み取り権限がユニバーサルプリントサーバーに付与されます。ユニバーサルプリントサーバーには、以下の情報が提供されます：

- TLS で使用される証明書ストア内の証明書。
- TLS 接続でどの TCP ポートが使用されるのか。

Windows ファイアウォールを使用する環境では、これらの TCP ポートでの受信接続が許可されている必要があります。Enable-UpsSsl.ps1 PowerShell スクリプトを使用する場合は、このファイアウォール規則が自動的に構成されます。

- どのバージョンの TLS プロトコルが許可されるのか。

ユニバーサルプリントサーバーは TLS プロトコルバージョン 1.3 および 1.2 をサポートしています。許可する最小バージョンを指定します。

デフォルトの TLS プロトコルバージョンは 1.2 です。

> 注:
>
> TLS 1.1 および 1.0 は、Citrix Virtual Apps and Desktops バージョン 2311 以降サポートされなくなりました。

- どの TLS 暗号の組み合わせが許可されるのか。

暗号の組み合わせにより、接続において使用する暗号化アルゴリズムが選択されます。VDA とユニバーサルプリントサーバーは、暗号の組み合わせのさまざまなセットをサポートできます。VDA が接続を開始して、サポートする TLS 暗号の組み合わせの一覧を送信すると、ユニバーサルプリントサーバー側では、構成済みの暗号の組み合わせの一覧内に VDA のいずれかの暗号の組み合わせと一致するものがあるかどうかがチェックされます。一致した場合、接続が確立されます。一致する暗号の組み合わせがない場合、ユニバーサルプリントサーバーは接続を拒否します。

ユニバーサルプリントサーバーは、OPEN、FIPS、および SP800-52 ネイティブ暗号キットモードに対し、GOV（政府）、COM（商業）、ALL という以下の暗号の組み合わせをサポートします。使用できる暗号の組み合わせは、**SSL FIPS** モードポリシー設定や Windows の FIPS モードによっても異なります。Windows FIPS モードについて詳しくは、Microsoft のサポート記事を参照してください。

暗号の組み合わせ（優先度の高い順）	OPEN ALL	OPEN COM	OPEN GOV	FIPS ALL	FIPS COM	FIPS GOV	SP800-52 ALL	SP800-52 COM	SP800-52 GOV
TLS_ECDHE_RSA_AES256_GCM_SHA384	X			X		X	X		X
TLS_ECDHE_RSA_AES256_CBC_SHA384	X			X		X	X		X
TLS_ECDHE_RSA_AES256_CBC_SHA	X	X		X	X		X	X	

PowerShell スクリプトを使用したユニバーサルプリントサーバー上の **TLS** 構成

証明書ストアの［ローカルコンピューター］**>**［個人］**>**［証明書］領域にある TLS 証明書をインストールします。その場所に複数の証明書が存在する場合は、証明書の拇印を`Enable-UpsSsl.ps1` PowerShell スクリプトに指定します。

> 注:
>
> PowerShell スクリプトは、ユニバーサルプリントサーバーの完全修飾ドメイン名を基にして正しい証明書を見つけます。ユニバーサルプリントサーバーの完全修飾ドメイン名に 1 つの証明書のみが存在する場合は、証明書の拇印を指定する必要はありません。

`Enable-UpsSsl.ps1`スクリプトは VDA からユニバーサルプリントサーバーへの TLS 接続を有効または無効にします。このスクリプトは、インストールメディアの **Support > Tools > SslSupport** フォルダーに収録されています。

TLS を有効にすると、スクリプトはユニバーサルプリントサーバーの TCP ポートで既存の Windows ファイアウォール規則をすべて無効にします。その後、XTE サービスが TLS TCP および UDP ポートでのみ受信接続を受け入れることを許可する新しい規則を追加します。また、スクリプトにより以下の Windows ファイアウォール規則が無効になります:

- クリアテキスト印刷 Web サービス接続（デフォルト：8080）
- クリアテキスト印刷データストリーム（CGP）接続（デフォルト：7229）

その結果、VDA は TLS を使用している場合にのみこれらの接続を確立できます。

> 注:
>
> TLS を有効にしても、VDA からユニバーサルプリントサーバーへの Windows 印刷スプーラーの RPC/SMB 接続には影響しません。
>
> 重要:
>
> 最初のパラメーターとして、**Enable** か **Disable** のどちらかを指定します。CertificateThumbprint パラメーターは、ローカルコンピューターの個人証明書ストアの 1 つの証明書のみがユニバーサルプリントサーバーの完全修飾ドメイン名を持つ場合、オプションです。その他のパラメーターはオプションです。

構文

```
Enable-UpsSSL.ps1 -Enable [-HTTPPort <port>] [-CGPPort <port>] [-
    HTTPSPort <port>] [-CGPSSLPort <port>] [-SSLMinVersion <version>] [-
    SSLCipherSuite <name>] [-CertificateThumbprint <thumbprint>] [-
    FIPSMode <Boolean>] [-ComplianceMode <mode>]
Enable-UpsSSL.ps1 -Disable [-HTTPPort <portnum>] [-CGPPort <portnum>]
```


パラメーター	説明
Enable	XTE サーバーで SSL/TLS を有効にします。このパラメーターまたは Disable パラメーターのいずれかを指定する必要があります。
Disable	XTE サーバー上で SSL/TLS を無効にします。このパラメーターまたは Enable パラメーターのいずれかを指定する必要があります。
CertificateThumbprint "<thumbprint>"	ローカルコンピューターの個人証明書ストア内にある TLS 証明書の拇印を二重引用符で囲んで指定します。スクリプトは、指定された拇印によって使用する証明書を選択します。
HTTPPort <port>	クリアテキスト印刷 Web サービス（HTTP/SOAP）ポート。デフォルト：8080
CGPPort <port>	クリアテキスト印刷データストリーム（CGP）ポート。デフォルト：7229
HTTPSPort <port>	暗号化印刷 Web サービス（HTTPS/SOAP）ポート。デフォルト：8443
CGPSSLPort <port>	暗号化印刷データストリーム（CGP）ポート。デフォルト：443
SSLMinVersion "<version>"	許可される TLS プロトコルの最低バージョンを二重引用符で囲んで指定します。有効な値:”TLS_1.2”および”TLS_1.3”。デフォルト：TLS_1.2。
SSLCipherSuite "<name>"	TLS 暗号の組み合わせパッケージの名前。二重引用符で囲みます。使用できる値は、「GOV」、「COM」、および「ALL」（デフォルト）です。
FIPSMode <Boolean>	XTE サーバーで FIPS 140 モードを有効または無効にします。有効な値：$true で FIPS 140 モードを有効にし、$falseFIPS 140 モードを無効にします。

例

次のスクリプトは TLS を有効にします。拇印（この例の場合、「12345678987654321」）を指定して、使用する証明書を選択します。

```
Enable-UpsSsl.ps1 -Enable -CertificateThumbprint "12345678987654321"
```

次のスクリプトは TLS を無効にします。

```
Enable-UpsSsl.ps1 -Disable
```


FIPS モードの構成

米国の Federal Information Processing Standards（FIPS）モードを有効にすると、FIPS 140 準拠の暗号化のみがユニバーサルプリントサーバーの暗号化接続に使用されるようにできます。

クライアントで FIPS モードを構成する前に、サーバーで FIPS モードを構成してください。

Windows FIPS モードを有効/無効にする方法については、Microsoft のドキュメントサイトを参照してください。

クライアントで **FIPS** モードを有効にする

Delivery Controller で Web Studio を実行して、Citrix ポリシー設定 ［**SSL FIPS** モード］を **Enabled** に設定します。Citrix ポリシーを有効にします。

各 VDA でこの操作を繰り返します:

1. Windows の FIPS モードを有効にします。
2. VDA を再起動します。

サーバーで **FIPS** モードを有効にする

各ユニバーサルプリントサーバーでこの操作を繰り返します:

1. Windows の FIPS モードを有効にします。
2. この PowerShell コマンドを管理者として実行します: `stop-service CitrixXTEServer, UpSvc`
3. `Enable-UpsSsl.ps1`スクリプトを`-Enable -FIPSMode $true`パラメーターで実行します。
4. ユニバーサルプリントサーバーを再起動します。

クライアントで **FIPS** モードを無効にする

Web Studio で、Citrix ポリシー設定 ［**SSL FIPS** モード］を **Disabled** に設定します。Citrix ポリシーを有効にします。Citrix ポリシー ［**SSL FIPS** モード］設定を削除することもできます。

各 VDA でこの操作を繰り返します:

1. Windows の FIPS モードを無効にします。
2. VDA を再起動します。

サーバーで **FIPS** モードを無効にする

各ユニバーサルプリントサーバーでこの操作を繰り返します:

1. Windows の FIPS モードを無効にします。
2. この PowerShell コマンドを管理者として実行します: `stop-service CitrixXTEServer, UpSvc`
3. `Enable-UpsSsl.ps1`スクリプトを`-Enable -FIPSMode $false`パラメーターで実行します。
4. ユニバーサルプリントサーバーを再起動します。

> 注:
>
> SSL プロトコルのバージョンが TLS 1.3 に設定されている場合、FIPS モードはサポートされません。

SSL/TLS プロトコルバージョンを構成する

デフォルトの SSL/TLS プロトコルバージョンは TLS 1.2 です。TLS 1.2 および TLS 1.3 は、実稼働環境で推奨される SSL/TLS プロトコルバージョンです。トラブルシューティングのためには、実稼働環境以外で一時的に SSL/TLS プロトコルバージョンの変更が必要な場合があります。

SSL 2.0 と SSL 3.0 は、ユニバーサルプリントサーバーではサポートされていません。

サーバーで SSL/TLS プロトコルバージョンを設定する

各ユニバーサルプリントサーバーでこの操作を繰り返します:

1. この PowerShell コマンドを管理者として実行します: `stop-service CitrixXTEServer, UpSvc`
2. `Enable-UpsSsl.ps1`スクリプトを`-Enable -SSLMinVersion`バージョンパラメーターで実行します。テストの終了後は、TLS 1.2 または TLS 1.3 に戻すことを忘れないようにしてください。
3. ユニバーサルプリントサーバーを再起動します。

クライアントで SSL/TLS プロトコルバージョンを設定する

各 VDA でこの操作を繰り返します:

1. Delivery Controller でポリシー設定 ［**SSL** プロトコルバージョン］を必要なプロトコルバージョンに設定して、ポリシーを有効にします。
2. Microsoft SCHANNEL SSP のレジストリ設定については、Microsoft のサポート記事TLS Registry Settingsを参照してください。レジストリ設定を使用して、クライアント側の **TLS 1.2** または **TLS 1.3** を有効にします。

   > 重要:
   >
   > テストの終了後は、レジストリ設定を元の値に戻すのを忘れないでください。

3. VDA を再起動します。

トラブルシューティング

接続エラーが発生した場合は、ユニバーサルプリントサーバーで C:\Program Files (x86)\Citrix\XTE\logs\error.log ファイルをチェックしてください。

SSL/TLS ハンドシェイクが失敗した場合は、このログファイルに「**SSL handshake from client failed**」というメッセージが表示されます。このような失敗は、VDA とユニバーサルプリントサーバーの SSL/TLS プロトコルバージョンが一致しない場合に発生することがあります。

ユニバーサルプリントサーバーのホスト名を含む次のポリシー設定でユニバーサルプリントサーバーの完全修飾ドメイン名を使用します:

- セッションプリンター
- プリンター割り当て
- 負荷分散のためのユニバーサルプリントサーバー

ユニバーサルプリントサーバーと VDA のシステムクロック（日付、時刻、およびタイムゾーン）が正しいことを確認してください。

仮想チャネルの許可リスト

August 17, 2024

仮想チャネル許可リストは、環境内で許可される Citrix 以外の仮想チャネルを制御できる機能です。デフォルトでは、仮想チャネル許可リスト機能が有効になっています。その結果、Citrix 仮想チャネルのみが Citrix Virtual Apps and Desktops セッションで開けるようになっています。自社製、サードパーティ製を問わず、カスタム仮想チャネルを使用する必要がある場合は、これらを許可リストに明示的に追加する必要があります。

構成

仮想チャネル許可リストがデフォルトで有効になっています。この機能は、Citrix ポリシーの次の設定を使用して構成できます:

- 仮想チャネル許可リスト：機能を有効または無効にし、仮想チャネルをリストに追加します。
- 仮想チャネルの許可リストのログ調整：仮想チャネル許可リストのイベント ログの調整期間を設定します。
- 仮想チャネル許可リストのログ：仮想チャネル許可リストのログレベルを設定します。

許可リストへの仮想チャネルの追加

仮想チャネルを許可リストに追加するには、次の情報が必要です:

1. コードで定義されている仮想チャネル名。最大 7 文字の長さにすることができます。例: CTXCVC1。
2. VDA マシンで仮想チャネルを開くプロセスのパス。例: C:\Program Files\Application\run.exe。

必要な情報を取得したら、仮想チャネルの許可リストポリシー設定を使用して、仮想チャネルを許可リストに追加する必要があります。仮想チャネルをリストに追加するには、仮想チャネル名のあとにコンマを入力してから、その仮想チャネルにアクセスするプロセスへのパスを入力します。プロセスが複数ある場合は、各プロセスをコンマで区切って追加できます。

単一プロセスの場合

前の例を使用して、以下のエントリをリストに追加します:

```
CTXCVC1,C:\Program Files\Application\run.exe
```

複数プロセスの場合

複数のプロセスがある場合は、以下のエントリをリストに追加します:

```
CTXCVC1,C:\Program Files\Application\run.exe,C:\Program Files\Application
\run2.exe
```

ワイルドカード文字の使用

ワイルドカードの使用（*）がサポートされています。アプリケーションのバージョンに基づいてディレクトリまたは実行可能ファイルの名前が変更された場合、またはサードパーティコンポーネントがユーザーのプロファイルにインストールされている場合は、ワイルドカードを使用できます。

ワイルドカードは次のシナリオで使用できます:

- 完全なディレクトリ名を置き換える場合。
  例: C:\Program Files\Application*\run1.exe
- ディレクトリ名の一部を置き換える場合。
  例: C:\Program Files\Application\v*\run1.exe
- 実行可能ファイルの名前を置き換える場合。
  例: C:\Program Files\Application\v1.2*.exe
- 実行可能ファイルの名前の一部を置き換える場合。
  例: C:\Program Files\Application\v1.2\run*.exe

次の制限事項が適用されます:

- ワイルドカードは、単一のディレクトリを置き換えるためにのみ使用できます。たとえば、実行可能ファイルがC:\Program Files\Application\v1.2\run1.exeにある場合、以下のようになります

  - 使用可能: C:\Program Files\Application*\run1.exe
  - 使用不可: C:\Program Files*\run1.exe

- エントリにはファイル拡張子が含まれている必要があります。
  - 使用可能: C:\Program Files\Application\v1.2*.exe
  - 使用不可: C:\Program Files\Application\v1.2*

- すべてのパスはローカルである必要があります。

> 注:
>
> - ネットワークパスの使用は許可されていません。
> - ワイルドカードのサポートは、Citrix Virtual Apps and Desktops 2206 から利用できます。
> - ワイルドカードのサポートは、Citrix Virtual Apps and Desktops 2203 LTSR の CU2 から利用できます。

システム環境変数の使用

システム環境変数を使用すると、許可リスト内の信頼できるプロセスの定義を簡素化できます。%programfiles%、%programfiles(x86)%、%systemdrive%、%systemroot%などの通常の変数を使用できます。

システムレベルで定義されている限り、カスタム環境変数を使用することもできます。

次の例は、通常の環境変数を示しています:

- %programfiles%\Application\v1.2\run.exe
- %programfiles%\Application*\run.exe
- %programfiles(x86)%\Application\v1.*\run.exe

次の例は、カスタムのシステム環境変数を示しています:

- カスタム変数名: app
- カスタム変数値: %programfiles%\Application\
- 許可リストのエントリ: CTXCVC1,%app%\run.exe

> 注:
>
> ユーザー環境変数はサポートされていません。
>
> 環境変数のサポートは、Citrix Virtual Apps and Desktops バージョン 2209 から利用できます。

仮想チャネル名とプロセスの取得

仮想チャネルの名前と VDA マシンで仮想チャネルを開くプロセスを取得する最も簡単な方法は、仮想チャネルを提供した開発者またはサードパーティベンダーから情報を取得することです。

別の方法としては、機能のログを適用し、次の手順に従うことで情報を取得することもできます:

1. カスタム仮想チャネルのクライアントコンポーネントとサーバーコンポーネントを配置したら、仮想アプリケーションまたは仮想デスクトップを起動します。
2. VDA マシンのシステムイベントログにて、開こうとしたカスタム仮想チャネルの名前とプロセスを探します。利用可能なイベントについて詳しくは、「イベントログ」を参照してください。
3. セッションからログアウトします。
4. 仮想チャネル許可リストポリシー設定に、識別された仮想チャネルとプロセスに関するエントリを追加します。
5. マシンを再起動してください。
6. VDA が登録されたら、仮想アプリケーションまたは仮想デスクトップを実行して、カスタム仮想チャネルが正常に開くことを確認します。

Citrix 仮想チャネルに関する考慮事項

組み込みの Citrix 仮想チャネルはすべて信頼されており、追加の構成なしで開くことができます。ただし、次の 2 つの機能は、外部の依存関係のために許可リストに明示的なエントリを必要とします:

- マルチメディアリダイレクト
- HDX RealTime Optimization Pack for Skype for Business

マルチメディアリダイレクト

Windows Media Player 以外のメディアプレーヤーをシステムメディアプレーヤーとして使用する場合は、信頼できるプロセスとして許可リストに追加する必要があります。次の情報は、許可リストのエントリに必要です:

- 仮想チャネル名: `CTXMM`
- プロセス: VDA マシンで使用されているメディアプレーヤーのパス。例: `C:\Program Files (x86)\Windows Media Player\wmplayer.exe`。
- 許可リストのエントリ: `CTXMM,C:\Program Files (x86)\Windows Media Player\wmplayer.exe`

HDX RealTime Optimization Pack for Skype for Business

次の情報は、許可リストのエントリに必要です:

- 仮想チャネル名: `CTXRMEP`
- プロセス: VDA マシン内の Skype for Business 実行可能ファイルのパス。Skype for Business のバージョンや、カスタムインストールパスの使用の有無によって異なる場合があります。例: `C:\Program Files\Microsoft Office\root\Office16\lync.exe`.
- 許可リストのエントリ: `CTXRMEP,C:\Program Files\Microsoft Office\root\Office16\lync.exe`

VDA と Delivery Controller 間の WebSocket 通信

August 17, 2024

この記事では、VDA と Delivery Controller 間の通信用に WebSocket 接続を設定する方法について説明します。

概要

WebSocket プロトコルは Citrix Brokering Protocol 上で動作し、Delivery Controller と VDA 間の安定した通信を実現します。
通信に WebSocket プロトコルを使用すると、次のようなメリットがあります:

- VDA から Delivery Controller への通信には TLS ポート 443 のみが必要です。
- VDA と Delivery Controller 間のシームレスで信頼性の高い通信チャネルを提供します。

機能

次のセクションでは、Delivery Controller と VDA 間の WebSocket 接続のワークフローについて説明します:

1. Citrix Virtual Apps and Desktops 管理者は、Machine Creation Service（MCS）を使用して VDA をプロビジョニングすることによりプロセスを開始します。
2. MCS プロビジョニングプロセス中に、MCS は各 VDA の公開キーと秘密キーのペアを生成し、その公開キーを Delivery Controller 上の FMA トラストサービスに登録します。MCS は、公開キーと秘密キーのペアを VDA の ID ディスクの下にファイルとして保存します。
3. VDA マシンが起動すると、VDA マシンにインストールされた MCS エージェントが ID ディスクからキーペアを読み取り、この情報を VDA レジストリの場所に書き込みます。
4. VDA にインストールされたブローカーエージェントは、レジストリからキーペアを読み取り、秘密キーで署名されたサービスキーを使用して、Delivery Controller への SSL を有効にした WebSocket 要求を生成します。
5. Delivery Controller は、署名されたサービスキー認証ヘッダーを FMA トラストサービスからの公開キーで検証します。
6. 検証が完了すると、システムは VDA と Delivery Controller 間の WebSocket 接続を確立します。

AD 参加済み VDA の WebSocket サポート

はじめに

1. サイトを構成します。詳しくは、「サイトの作成」を参照してください。
2. Delivery Controller に TLS 証明書をインストールします。詳しくは、「TLS サーバー証明書の Controller へのインストール」を参照してください。

3. Delivery Controller を信頼するには、VDA にルート CA と中間 CA をインストールします。

手順

WebSocket 接続を設定するには、次の手順に従ってください:

1. Delivery Controller で WebSocket 接続を有効にします。サイトにある各 Delivery Controller で次のコマンドを実行します:

   ```
   New-ItemProperty "HKLM:\SOFTWARE\Citrix\DesktopServer\WorkerProxy
   "-Name "WebSocket_Enabled"-PropertyType "DWord"-Value 1 -Force
   ```

   > 注:
   >
   > WebSocket を有効にした後は、必ず Delivery Controller を再起動してください。

2. MCS プロビジョニングを使用して、AD 参加済み VDA のマシンカタログを作成します。詳しくは、「マシンカタログの作成」を参照してください。
3. デリバリーグループを作成し、そこに VDA を追加します。詳しくは、「デリバリーグループの作成」を参照してください。
4. VDA で WebSocket 接続を有効にします。VDA で次のコマンドを実行します:

   ```
   `New-ItemProperty "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\
      Services\CitrixBrokerAgent\WebSocket" -Name "Enabled" -
      PropertyType "DWord" -Value 1 -Force`
   ```

   - VDA が WebSocket 経由でサーバーに接続されているかどうかを確認するには、次のレジストリキーの値を確認します。

     キー:

     ```
     HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\
        CitrixBrokerAgent\WebSocket
     ```

     値の名前: Connected

     種類: REG_DWORD

     値: 1 または 0

     1: VDA は WebSocket を使用してサーバーに接続しました。

     0: VDA は WebSocket 経由でサーバーにアクセスできないか、WebSocket が有効になっていません。

   - WebSocket が有効になっているかどうかを確認するには、次のレジストリキーの値を確認します。`Enabled`の値は 1 でなければなりません。

     キー:


```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\
   CitrixBrokerAgent\WebSocket
```

値の名前：Enabled

種類：REG_DWORD

値：1

HDX 接続

August 17, 2024

Citrix HDX には、デバイス上とネットワーク上で一元化されたアプリケーションとデスクトップの高品位なユーザーエクスペリエンスを実現する幅広いテクノロジが搭載されています。

HDX は、次の 3 つの技術原則に基づいて設計されています：

- インテリジェントリダイレクト
- 連続文字圧縮
- データ重複排除

これらの原則をさまざまに組み合わせて適用することで、IT 部門およびユーザーの操作を最適化し、帯域幅の消費量を抑えてホストサーバーあたりのユーザー密度を増やすことができます。

HDX オファリング内では、独自の専用トランスポートプロトコルを介して接続し、セッションを確立するときに最大転送ユニットを利用し、Citrix SD-WAN との接続を最適化できます。

アダプティブトランスポート

August 17, 2024

アダプティブトランスポートは、Citrix Virtual Apps and Desktops のメカニズムであり、優先トランスポートプロトコルを使用して HDX セッションの接続を確立し、優先プロトコルによる接続が利用できない場合に TCP へのフォールバックを提供します。

次のトランスポートプロトコルがサポートされています：

- Enlightened Data Transport（EDT）
- 伝送制御プロトコル（TCP）

構成

アダプティブトランスポートはデフォルトで有効になっています。アダプティブトランスポートを次のモードで動作するように構成できます:

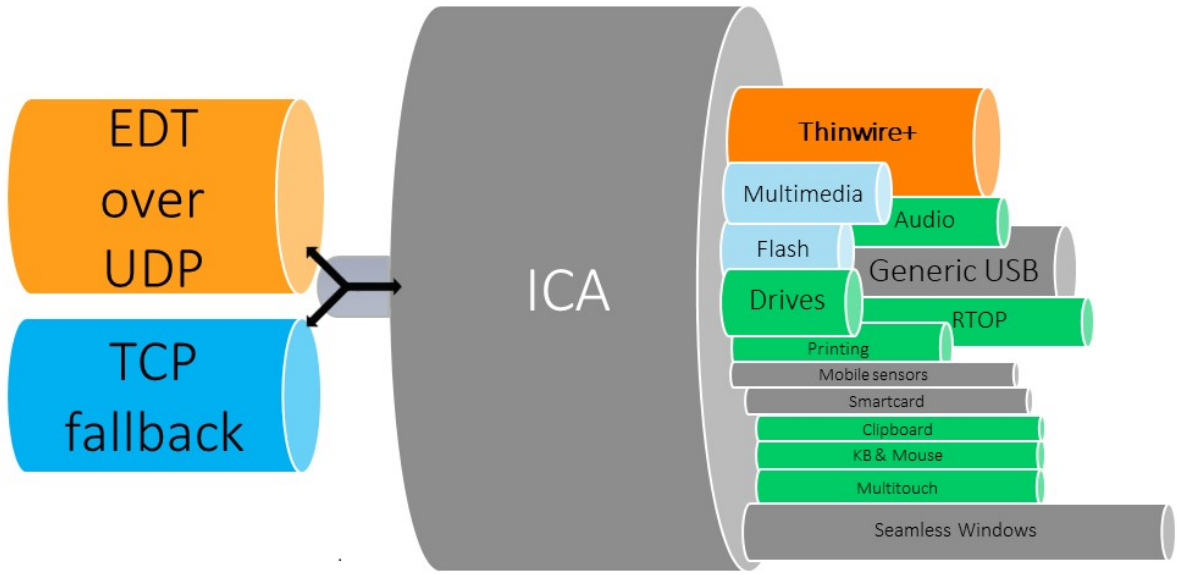
- 優先:（デフォルト）クライアントは優先プロトコルで接続を試み、優先プロトコルで接続できない場合は TCP にフォールバックします。
- 診断モード:クライアントは、優先プロトコルを使用してのみ接続を試行します。[Fall back to TCP] は無効です。
- オフ:クライアントは TCP を使用してのみ接続を試行します。

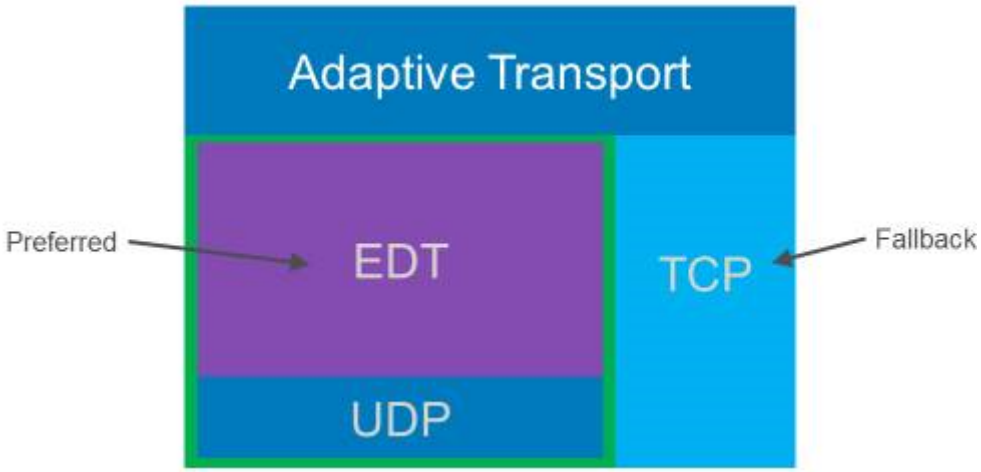
機能

アダプティブトランスポートが`Preferred`に設定されている場合、クライアントは優先プロトコルと TCP の両方を並行してセッションに接続しようとします。これにより、優先プロトコルで接続できず、クライアントが TCP の使用にフォールバックする必要がある場合に、接続時間を最適化できます。TCP を使用して接続が確立された場合、クライアントは 5 分ごとにバックグラウンドで優先プロトコルを使用して接続を試行します。

アダプティブトランスポートが`Diagnostic mode`に設定されている場合、クライアントは優先プロトコルのみを使用してセッションに接続します。クライアントが優先プロトコルを使用して接続を確立できない場合、TCP の使用にフォールバックせず、接続は失敗します。

アダプティブトランスポートが`Off`に設定されている場合、アダプティブトランスポート は無効になり、クライアントは TCP のみを使用してセッションに接続します。





システム要件

アダプティブトランスポートと EDT を使用するための要件は次のとおりです:

- コントロールプレーン
  - Citrix DaaS（旧称：Citrix Virtual Apps and Desktops サービス）
  - Citrix Virtual Apps and Desktops：現在サポートされているバージョン
- Virtual Delivery Agent
  - Windows：現在サポートされているバージョン（2402 以降を推奨）
  - Linux：現在サポートされているバージョン（2402 以降を推奨）
- Citrix Workspace アプリ
  - Windows：現在サポートされているバージョン（2402 以降を推奨）
  - Linux：現在サポートされているバージョン（2402 以降を推奨）
  - Mac：現在サポートされているバージョン（2402 以降を推奨）
  - iOS：Apple App Store で入手可能な最新バージョン
  - Android：Google Play で利用可能な最新バージョン
- Citrix NetScaler Gateway
  - 14.1.12.30 以降（推奨）
  - 13.1.17.42 以降（13.1-52.19 以降を推奨）

> 注:
>
> Linux VDA の詳細については、Linux Virtual Delivery Agentのドキュメントを参照してください。

ネットワークの要件

次のセクションは、アダプティブトランスポートで EDT を使用するためのネットワーク要件です:

セッションホスト

セッションホストに Windows Defender ファイアウォールなどのファイアウォールがある場合は、内部接続に対して次の受信トラフィックを許可する必要があります。

説明	接続元	プロトコル	ポート
内部接続 - セッション画面の保持が有効	クライアント	UDP	2598
内部接続 - セッション画面の保持が無効			1494
内部接続 - HDX Direct または VDA SSL			443

> 注:
>
> VDA インストーラーは、適切な受信規則を Windows Defender ファイアウォールに追加します。別のファイアウォールを使用する場合は、上記の規則を追加する必要があります。

内部ネットワーク

次の表は、ネットワークで EDT を使用するために必要なファイアウォール規則を示しています:

説明	プロトコル	接続元	接続先	接続先ポート
直接内部接続 - セッションの信頼性が有効	UDP	クライアント側ネットワーク	VDA ネットワーク	2598
直接内部接続 - セッションの信頼性が有効				1494
直接内部接続 - HDX Direct または SSL				443
VDA		NetScaler SNIP		2598
NetScaler Gateway				

説明	プロトコル	接続元	接続先	接続先ポート
NetScaler Gateway - VDA SSL				443

> 注:
>
> Citrix Gateway サービスを使用している場合は、**Rendezvous** が EDT をトランスポートプロトコルとして使用できるようにする必要があります。システムおよびネットワークの要件については、Rendezvousのドキュメントを参照してください。

クライアント側ネットワーク

次の表は、クライアントデバイスの接続要件を示しています:

説明	プロトコル	接続元	接続先	接続先ポート
内部接続 - セッション画面の保持が有効	UDP	クライアント IP	VDA ネットワーク	2598
内部接続 - セッション画面の保持が無効				1494
内部接続 - HDX Direct または SSL VDA				443
外部接続 - NetScaler Gateway			NetScaler Gateway パブリック IP アドレス	443
外部接続 - Citrix Gateway サービス			Citrix Gateway サービス	443

> 注:
>
> Citrix Gateway サービスを使用している場合、クライアントはhttps://*.*.nssvc.netにアクセスできる必要があります。https://*.*.nssvc.netを使用してすべてのサブドメインを許可できない場合、代わりにhttps://*.c.nssvc.netおよびhttps://*.g.nssvc.netを使用します。詳しくは、Knowledge CenterのCTX270584を参照してください。

Enlightened Data Transport

August 17, 2024

Enlightened Data Transport（EDT）は、ユーザーデータグラムプロトコル（UDP）上に構築された Citrix 独自のトランスポートプロトコルです。サーバーのスケーラビリティを維持しながら、要求の厳しい長距離接続で優れたユーザーエクスペリエンスを提供します。EDT は、信頼性の低いネットワーク上のすべての ICA 仮想チャネルのデータスループットを向上させ、より優れた、より一貫性のあるユーザーエクスペリエンスを提供します。

アダプティブトランスポートが有効になっている場合、EDT が優先プロトコルになります。

知っておくべきこと

- NetScaler Gateway および Citrix Gateway サービスで **MTU Discovery** と EDT を使用するには、セッション画面の保持を有効にする必要があります。
- パケットの断片化により、パフォーマンスが低下したり、場合によってはセッションの起動に失敗したりすることがあります。これを防ぐには、EDT MTU をネットワークに適した値に調整する必要があります。EDT MTU Discovery を使用するか、「How to configure MSS when using EDT on networks with non-standard MTU」の説明に従って手動の回避策を使用できます。
- NetScaler Gateway で EDT の使用を有効にする方法の詳細については、「Enlightened Data Transport をサポートするように NetScaler Gateway を構成する」を参照してください。

EDT MTU Discovery

MTU Discovery により、セッション確立時に EDT が最大伝送単位（MTU）を自動的に決定できるようにします。これにより、パフォーマンスの低下やセッションの確立失敗となる可能性のある、EDT パケットのフラグメンテーションが防止されます。

MTU Discovery はデフォルトで有効になっています。無効にする必要がある場合、詳細は「レジストリで管理される HDX 機能」を参照してください。

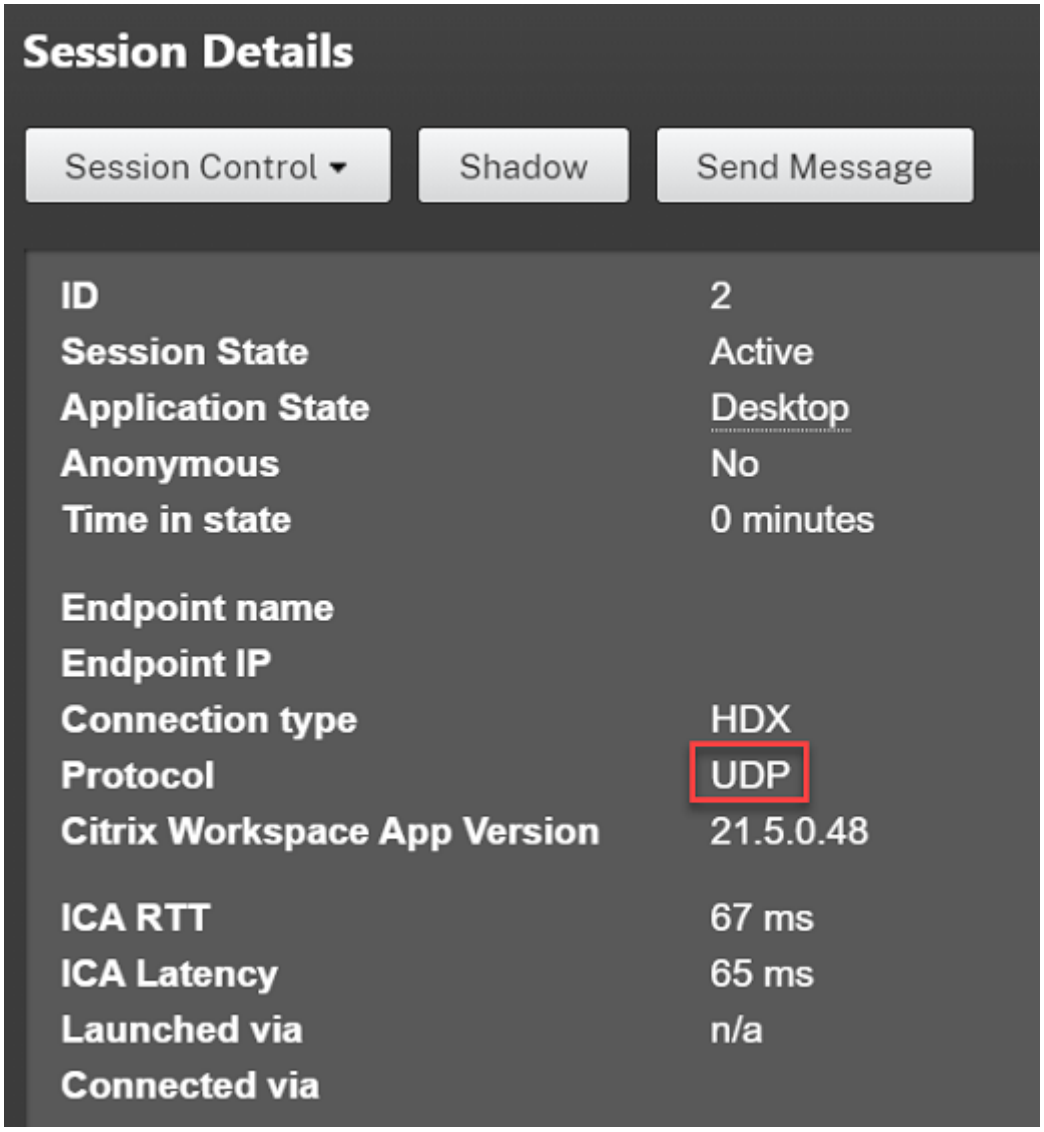
> 注:
>
> - MTU Discovery が機能するには、［セッション画面の保持］を有効にする必要があります。
> - マルチストリーム ICA を使用した MTU Discovery は、VDA バージョン 2209 以降で利用できます。

トラブルシューティング

August 17, 2024

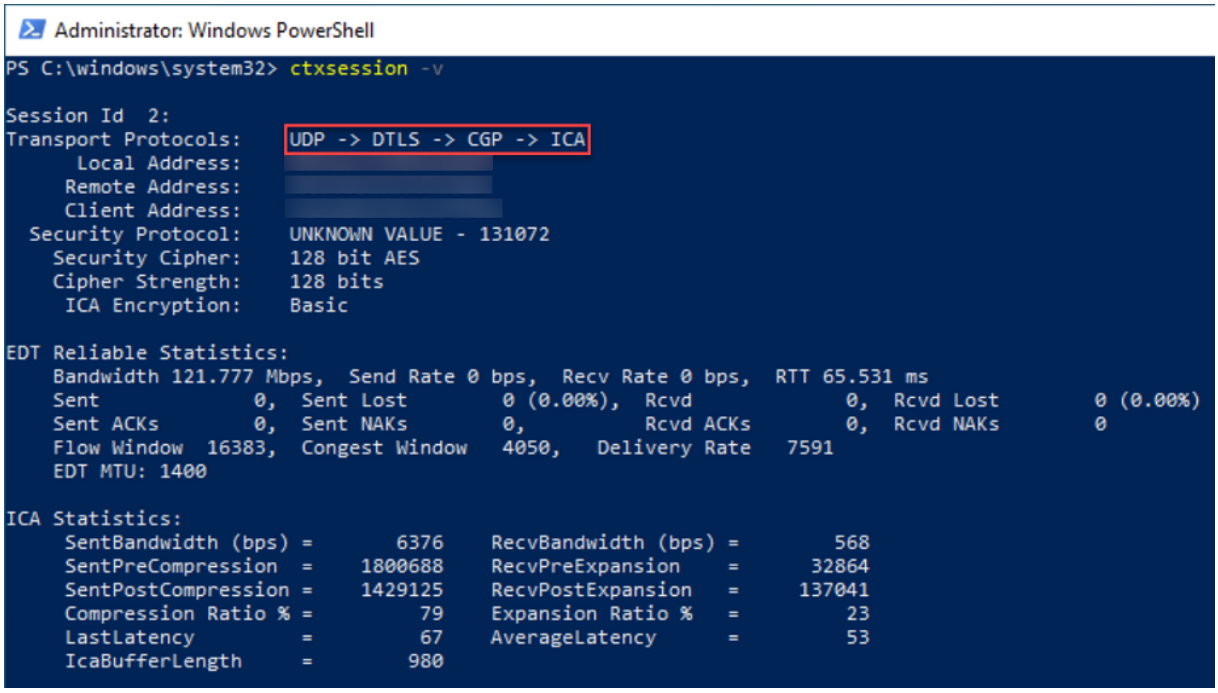
EDT がセッションのトランスポートプロトコルとして使用されていることを確認するために、VDA で Director または`CtxSession.exe`コマンドラインユーティリティを使用できます。

Director でセッションを検索し、［詳細］を選択します。［接続の種類］が`HDX`で ［プロトコル］が`UDP`の場合、セッションのトランスポートプロトコルとして EDT が使用されています。



CtxSession.exe ユーティリティを使用するには、セッション内でコマンドプロンプトまたは PowerShell を起動し、`ctxsession.exe`を実行します。詳細な統計を表示するには、`ctxsession.exe -v`を実行します。EDT が使用されている場合、トランスポートプロトコルは次のいずれかを示します:

- **UDP > ICA**（セッション画面の保持が無効）
- **UDP > CGP > ICA**（セッション画面の保持が有効）
- **UDP > DTLS > CGP > ICA**（ICA は DTLS で暗号化されたエンドツーエンド）



EDT でセッションが接続に失敗した場合

アダプティブトランスポートと **EDT** のトラブルシューティングを行うには、次のことをお勧めします:

1. システム要件、ネットワーク要件、既知の問題、および知っておくべきことを確認し、すべての項目に対応していることを確認します。
2. Studio または GPO に Citrix ポリシーがあり、目的の **HDX** アダプティブトランスポート設定を上書きしていないかどうかを確認します。
3. 目的の HDX アダプティブトランスポート設定を上書きする設定がクライアントにあるかどうかを確認します。上書きする設定とは、GPO 設定、オプションの Workspace アプリ管理テンプレートを使用して構成された設定、またはレジストリやクライアントの構成ファイルで手動で構成された **HDXoverUDP** 設定などです。
4. マルチセッション VDA マシンでは、UDP リスナーがアクティブであることを確認してください。VDA マシンでコマンドプロンプトを開き、`netstat -a -p udp`を実行します。詳しくは、「How to Confirm HDX Enlightened Data Transport Protocol」を参照してください。
5. ネットワークファイアウォールと VDA マシンで実行されているファイアウォールの両方で適切なファイアウォール規則が構成されているかどうかを確認します。
6. NetScaler Gateway または Citrix Gateway サービスをバイパスして内部で直接セッションを開始し、使用中のプロトコルを確認します。セッションで EDT を使用する場合、VDA は NetScaler Gateway または Citrix Gateway サービスを介した外部接続に EDT を使用するよう準備しています。
7. EDT が直接の内部接続では機能し、NetScaler Gateway または Citrix Gateway サービスを経由するセッションでは機能しない場合は、次の手順を実行します:

- セッション画面の保持が有効になっていることを確認します。
- NetScaler Gateway を使用する場合は、「Enlightened Data Transport および HDX Insight をサポートするように NetScaler Gateway を構成する」に記載されている必須構成に準拠していることを確認してください。

8. Citrix Gateway サービスを使用している場合は、Rendezvous が有効になっていて動作していることを確認します。
9. ユーザーの接続に非標準の MTU が必要かどうかを確認します。有効 MTU が 1500 バイト未満の接続は、EDT パケットの断片化を引き起こし、パフォーマンスに影響を与えたり、セッションの起動に失敗したりすることがあります。この問題は、VPN、一部の Wi-Fi アクセスポイント、および 4G や 5G などのモバイルネットワークを使用している場合によく発生します。MTU Discovery が有効になっているか、または「標準以外の MTU を持つネットワークで EDT を使用する場合に MSS を構成する方法」で説明されているようにカスタム MTU を設定していることを確認します。

既知の問題

- 非対称ネットワークパスにより、MTU Discovery が、NetScaler Gateway または Citrix Gateway サービスを介さない接続に失敗することがあります。この問題に対処するには、VDA バージョン 2103 以降にアップグレードします。[CVADHELP-16654]
- NetScaler Gateway を使用している場合、非対称ネットワークパスが原因で MTU Discovery が失敗することがあります。これは、Gateway で EDT パケットのヘッダーの Don’t Fragment（DF）ビットが伝播されないことが原因です。この問題の修正は、ファームウェアリリース 13.1 ビルド 17.42 以降で利用できます。修正プログラムを有効にする方法について詳しくは、NetScaler Gatewayのドキュメントを参照してください。[CGOP-18438]
- DS-Lite ネットワークを介して接続するユーザーの場合、MTU Discovery が失敗することがあります。一部のモデムでは、パケット処理が有効になっていると DF ビットを正しく処理できず、MTU Discovery が断片化を検出できなくなります。この状況では、次のオプションを使用できます:
  - ユーザーのモデムでパケット処理を無効にします。
  - **MTU Discovery** を無効にして、「How to configure MSS when using EDT on networks with non-standard MTU」の説明に従ってハードコードされた MTU を使用します。
  - アダプティブトランスポートを無効にして、セッションに TCP の使用を強制します。ユーザーのサブセットのみが影響を受ける場合は、他のユーザーが引き続き EDT を使用できるように、クライアント側でそれを無効にすることを検討してください。

HDX Direct（Technical Preview）

August 17, 2024

Citrix が提供するリソースにアクセスする場合、HDX Direct を使用すると、内部および外部の両方のクライアントデバイスはセッションホストとのセキュアな直接接続を確立できます（直接通信が可能な場合）。

> 重要：
>
> HDX Direct は現在、Technical Preview 段階にあります。この機能はサポートなしで提供されているため、運用環境での使用はまだ推奨されていません。フィードバックを送信したり、問題を報告したりする場合は、このフォームを使用してください。

システム要件

HDX Direct を使用するためのシステム要件は次のとおりです：

- コントロールプレーン
  - Citrix DaaS
  - Citrix Virtual Apps and Desktops 2402 以降
- Virtual Delivery Agent（VDA）
  - Windows：バージョン 2402 以降
- Workspace アプリ
  - Windows：バージョン 2402 以降
- アクセス層
  - Citrix Workspace（Citrix Gateway Service 使用）
  - Citrix Workspace（NetScaler Gateway 使用）
- その他
  - 外部直接接続に対してアダプティブトランスポートを有効にする必要がある

ネットワークの要件

HDX Direct を使用するためのネットワーク要件は次のとおりです：

セッションホスト

セッションホストに Windows Defender ファイアウォールなどのファイアウォールがある場合は、内部接続に対して次の受信トラフィックを許可する必要があります。

説明	接続元	プロトコル	ポート
内部直接接続	クライアント	TCP	443
内部直接接続	クライアント	UDP	443

> 注:
>
> VDA インストーラーは、適切な受信規則を Windows Defender ファイアウォールに追加します。別のファイアウォールを使用する場合は、上記の規則を追加する必要があります。

クライアント側ネットワーク

次の表に、内部ユーザーと外部ユーザーのクライアントネットワークを示します。

内部ユーザー

説明	プロトコル	接続元	送信元ポート	接続先	接続先ポート
内部直接接続	TCP	クライアント側ネットワーク	1024～65535	VDA ネットワーク	443
内部直接接続	UDP	クライアント側ネットワーク	1024～65535	VDA ネットワーク	443

外部ユーザー

説明	プロトコル	接続元	送信元ポート	接続先	接続先ポート
STUN（外部ユーザーのみ）	UDP	クライアント側ネットワーク	1024～65535	インターネット（下記の注を参照）	3478、19302
外部ユーザー接続	UDP	クライアント側ネットワーク	1024～65535	データセンターのパブリック IP アドレス	1024～65535

データセンターネットワーク

次の表に、内部ユーザーと外部ユーザーのデータセンターネットワークを示します。

内部ユーザー

説明	プロトコル	接続元	送信元ポート	接続先	接続先ポート
内部直接接続	TCP	クライアント側ネットワーク	1024～65535	VDA ネットワーク	443
内部直接接続	UDP	クライアント側ネットワーク	1024～65535	VDA ネットワーク	443

外部ユーザー

説明	プロトコル	接続元	送信元ポート	接続先	接続先ポート
STUN（外部ユーザーのみ）	UDP	VDA ネットワーク	1024～65535	インターネット（下記の注を参照）	3478、19302
外部ユーザー接続	UDP	DMZ/内部ネットワーク	1024～65535	VDA ネットワーク	55000～55250
外部ユーザー接続	UDP	VDA ネットワーク	55000～55250	クライアントのパブリック IP	1024～65535

> 注:
>
> VDA と Workspace アプリは両方とも、STUN 要求を以下のサーバーにこの順序で送信しようとします:
>
> - stunserver.stunprotocol.org:3478
> - employees.org:3478
> - stun.l.google.com:19302
>
> [**HDX Direct** のポート範囲] ポリシー設定を使用して外部ユーザー接続のデフォルトのポート範囲を変更する場合、カスタムポート範囲が対応するファイアウォール規則を満たしている必要があります。

構成

デフォルトでは、HDX Direct は無効になっています。この機能を構成するには、Citrix ポリシーの [**HDX Direct**] 設定を使用します。

- **HDX Direct**: 機能を有効または無効にします。
- **HDX Direct** モード: **HDX Direct** を内部クライアントのみで使用可能にするか、内部クライアントと外部クライアントの両方で使用可能にするかを設定します。
- **HDX Direct** のポート範囲: VDA が外部クライアントからの接続に使用するポート範囲を定義します。

注意事項

HDX Direct を使用するための注意事項は次のとおりです：

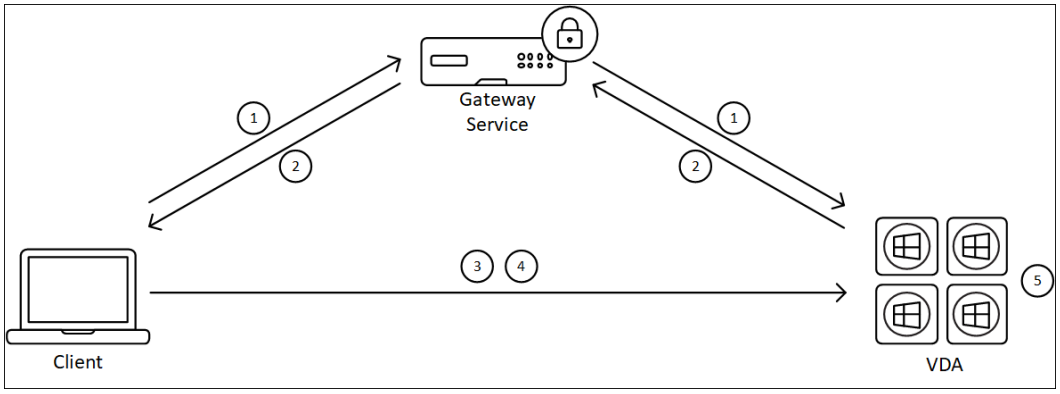
- HDX Direct を外部ユーザーが使用できるようにするには、トランスポートプロトコルとして EDT（UDP）を使用する必要があります。このため、［アダプティブトランスポート］を有効にする必要があります。
- **HDX Insight** を使用している場合は、**HDX Direct** を使用すると、セッションが NetScaler Gateway の仲介によるアクセス対象にされなくなるため、HDX Insight のデータ収集が妨げられることに注意してください。
- Virtual Apps and Desktops に非永続マシンを使用する場合、各マシンが独自の証明書を生成できるように、**HDX Direct** をマスター/テンプレートイメージ内ではなくセッションホスト上で有効にすることをお勧めします。
- HDX Direct での独自の証明書の使用は現在サポートされていません。

機能

HDX Direct を使用すると、直接通信が利用できる場合、クライアントはセッションホストへの直接接続を確立できます。HDX Direct で直接接続を行うと、自己署名証明書により、ネットワークレベルの暗号化（TLS/DTLS）で直接接続が保護されます。

内部ユーザー

次の図は、内部ユーザーの HDX Direct 接続プロセスの概要を示しています。



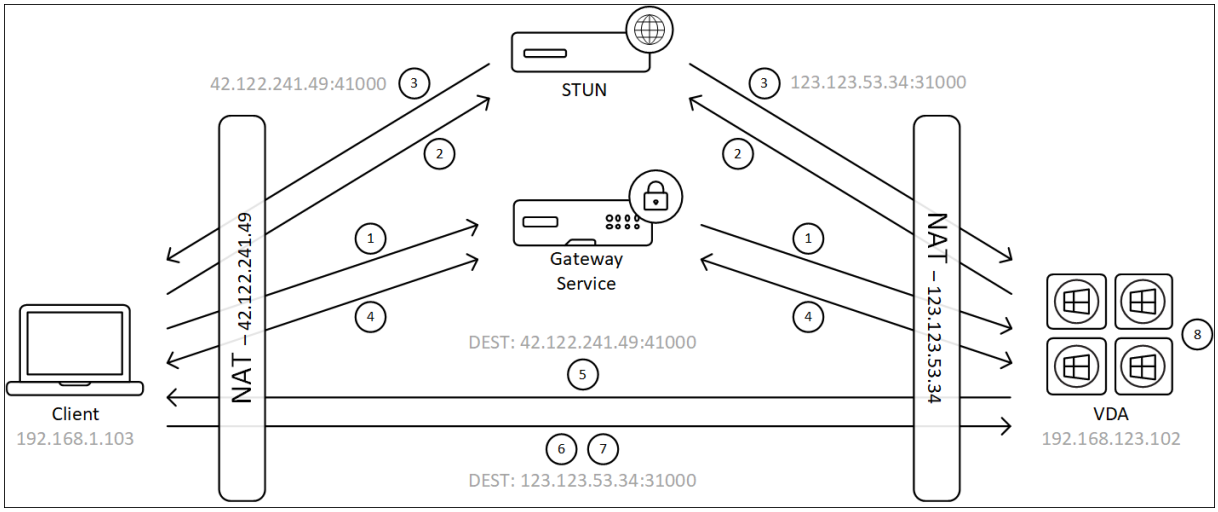
1. クライアントは、Gateway Service を通じて HDX セッションを確立しようとします。
2. 接続が成功すると、VDA は、VDA マシンの FQDN、その IP アドレスの一覧、および VDA マシンの証明書を HDX 接続経由でクライアントに送信します。
3. クライアントは IP アドレスをプローブして、VDA に直接アクセスできるかどうかを確認します。
4. クライアントは共有 IP アドレスのいずれかを使用して VDA に直接接続できる場合、手順（2）で交換した証明書と一致する証明書を使用して、（D）TLS で保護された、VDA との直接接続を確立しようとします。

5. 直接接続が正常に確立されると、セッションが新しい接続に転送されるので、Gateway Service への接続は終了します。

> 注:
>
> 上記の手順 2 で接続が確立されると、セッションがアクティブになります。後続の手順を実行しても、仮想アプリケーションまたはデスクトップを使用しようとする場合に遅延や妨害が生じることはありません。後続の手順のいずれかが失敗した場合でも、Gateway を介した接続はユーザーのセッションを中断することなく維持されます。

外部ユーザー

次の図は、外部ユーザーの HDX Direct 接続プロセスの概要を示しています:



1. クライアントは、Gateway Service を通じて HDX セッションを確立しようとします。
2. 接続が成功すると、クライアントと VDA の両方がパブリックな IP アドレスとポートを検出するための STUN 要求を送信します。
3. STUN サーバーは、対応するパブリックな IP アドレスとポートを使用してクライアントと VDA に応答します。
4. HDX 接続を通じて、クライアントと VDA はパブリックな IP アドレスと UDP ポートを交換し、VDA は証明書をクライアントに送信します。
5. VDA は、クライアントのパブリックな IP アドレスと UDP ポートに UDP パケットを送信します。クライアントは、UDP パケットを VDA のパブリックな IP アドレスと UDP ポートに送信します。
6. クライアントは VDA からメッセージを受信すると、セキュリティで保護された接続の要求で応答します。
7. DTLS ハンドシェイク中に、クライアントは証明書が手順（4）で交換された証明書と一致するかどうかを検証します。検証後、クライアントは承認トークンを送信します。これで、セキュリティで保護された直接接続が確立されました。
8. 直接接続が正常に確立されると、セッションが新しい接続に転送されるので、Gateway Service への接続は終了します。

> 注:
>
> 上記の手順 2 で接続が確立されると、セッションがアクティブになります。後続の手順を実行しても、仮想アプリケーションまたはデスクトップを使用しようとする場合に遅延や妨害が生じることはありません。後続の手順のいずれかが失敗した場合でも、Gateway を介した接続はユーザーのセッションを中断することなく維持されます。

証明書管理

セッションホスト

VDA マシン上の次の 2 つのサービスは証明書の作成と管理を処理します。どちらのサービスもマシンの起動時に自動的に実行されるように設定されています:

- Citrix ClxMtp サービス: CA 証明書キーを生成・ローテーションします。
- Citrix Certificate Manager サービス: 自己署名のルート CA 証明書とマシン証明書を生成・管理します。

次の手順は、証明書管理プロセスを示しています:

1. サービスは、マシンの起動時に開始されます。
2. キーがまだ作成されていない場合、`Citrix ClxMtp Service`によってキーが作成されます。
3. Citrix Certificate Manager サービスは、**HDX Direct** が有効になっているかどうかを確認します。有効になっていない場合、サービスは自動的に停止します。
4. **HDX Direct** が有効になっている場合、Citrix Certificate Manager サービスは、自己署名のルート CA 証明書が存在するかどうかをチェックします。存在しない場合は、自己署名のルート証明書が作成されます。
5. ルート CA 証明書が使用できるようになると、Citrix Certificate Manager サービスは、自己署名のマシン証明書が存在するかを確認します。存在しない場合は、サービスはキーを生成し、マシンの FQDN を使用して新しい証明書を作成します。
6. Citrix Certificate Manager サービスによって作成された既存のマシン証明書があり、サブジェクト名がマシンの FQDN と一致しない場合、新しい証明書が生成されます。

> 注:
>
> Citrix Certificate Manager サービスは、2048 ビットキーを利用する RSA 証明書を生成します。

クライアントデバイス

セキュリティで保護された **HDX Direct** 接続の確立を成功させるには、クライアントはセッションの保護に使用される証明書を信頼できる必要があります。そのため、クライアントは ICA ファイル（Workspace によって提供される）を使用してセッションの CA 証明書を受信します。したがって、CA 証明書をクライアントデバイスの証明書ストアに配布する必要はありません。

NAT の互換性

August 17, 2024

外部ユーザーのデバイスとセッションホスト間の直接接続を確立するために、HDX Direct は STUN と NAT トラバーサルのホールパンチングを利用して、クライアントデバイスとセッションホストの間でパブリックな IP アドレスとポートのマッピングを交換できるようにします。これは、VoIP、統合コミュニケーション、P2P ソリューションの仕組みと似ています。

ファイアウォールおよびその他のネットワークコンポーネントが HDX セッションおよび STUN 要求の UDP トラフィックを許可するように構成されている限り、外部ユーザー向けの HDX Direct は機能することが期待できます。ただし、ユーザーネットワークの NAT タイプとセッションホストネットワークの NAT タイプに互換性がない場合に HDX Direct が失敗する場合もあります。

検証

クライアントの NAT タイプとセッションホストの NAT タイプを検証するには、STUNTMAN の STUN クライアントユーティリティを使用します:

1. ターゲットプラットフォームに適切なパッケージを stunprotocol.org からダウンロードし、内容を抽出します。
2. コマンドウィンドウを開き、内容が抽出されたディレクトリに移動します。
3. 次のコマンドを実行します:
   ```
   .\stunclient.exe stunserver.stunprotocol.org --mode behavior
   ```
4. 出力をメモします。

バインドテストと動作テストが成功した場合、**binding test** と **behavior test** の両方によって成功が報告され、NAT の動作が指定されます:

テストが失敗した場合、**binding test** と **behavior test** の両方によって失敗が報告されます。

次の表を参照すると、外部ユーザー向けの HDX Direct が動作することを期待できるかどうかを、クライアントテストとセッションホストテストの両方の結果に基づいて判断することができます:

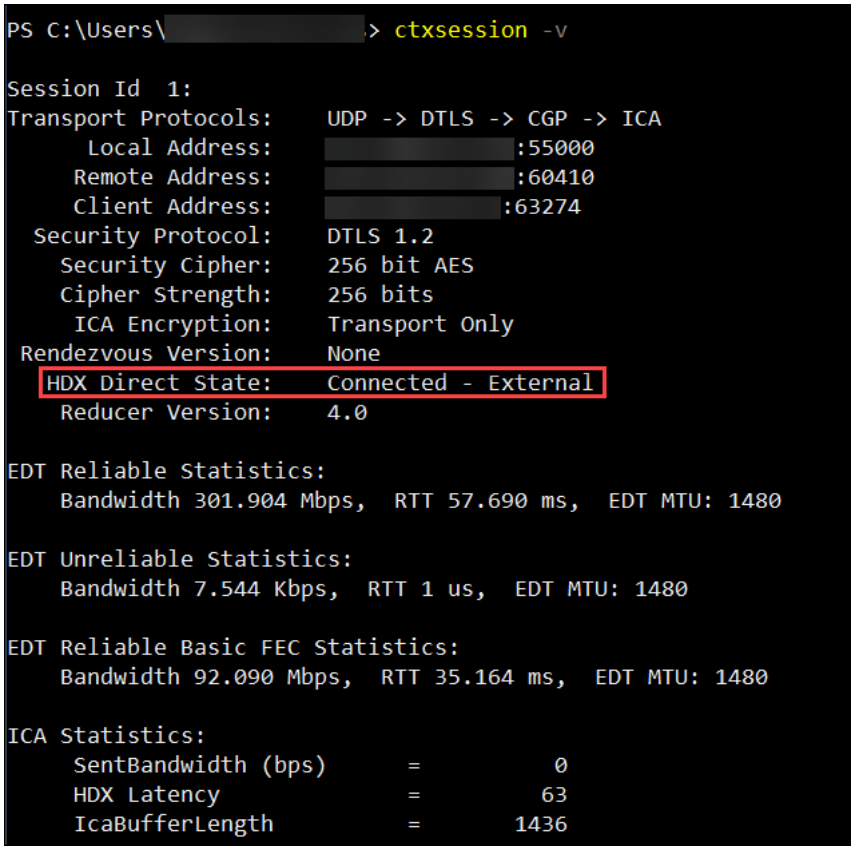
クライアントデバイス	セッションホスト	機能しますか?
エンドポイントに依存しないマッピング	エンドポイントに依存しないマッピング	はい
エンドポイントに依存しないマッピング	エンドポイントに依存したマッピング	はい
エンドポイントに依存したマッピング	エンドポイントに依存しないマッピング	はい
エンドポイントに依存したマッピング	エンドポイントに依存したマッピング	いいえ
アドレスとポートに依存したマッピング	任意の NAT タイプ	いいえ
任意の NAT タイプ	アドレスとポートに依存したマッピング	いいえ
失敗	任意の NAT タイプ	いいえ
任意の NAT タイプ	失敗	いいえ
失敗	失敗	いいえ

トラブルシューティング

August 17, 2024

HDX Direct が直接接続の確立に成功したことを確認するには、VDA マシンで`CtxSession.exe`ユーティリティを使用します。

`CtxSession.exe`ユーティリティを使用するには、セッション内でコマンドプロンプトまたは PowerShell を起動し、`ctxsession.exe -v`を実行します。**HDX Direct** 接続の確立が成功した場合、［**HDX Direct Status**］が`Connected`と表示されます。



HDX Direct 接続の確立が成功したか失敗したかを確認する別の方法としては、セッションホストのイベントログを確認するという方法もあります。詳しくは、「イベントログ」セクションを参照してください。

> 注:
>
> セッションホストで使用できる IP アドレスの数と環境によっては、HDX Direct 接続が確立されるまでに最大 5 分かかる場合があります。

HDX Direct が直接接続を確立できない場合

HDX Direct が直接接続を確立できない場合は、次の手順を確認してください:

1. 使用している VDA のバージョンと Workspace アプリのバージョンがシステム要件に応じた機能をサポートしていることを確認します。
2. HDX Direct を有効にするポリシーが VDA に適用されていること、およびこの機能を無効にする優先度の高いポリシーが他にないことを確認します。
3. 必要な HDX Direct モードを設定するポリシーが VDA に適用されていること、および構成を上書きする優先度の高いポリシーが他にないことを確認します。
4. Citrix ClxMtp サービスがセッションホストで実行されていることを確認します。
5. Citrix Certificate Manager サービスがセッションホストで実行されていることを確認します。実行されていない場合は、手動で開始してください。HDX Direct を無効にすると、このサービスは自動的に停止します。

6. セッションホストに自己署名のルート CA 証明書があるかどうかを確認します:
    a) 発行先: CA-<hostname>（例: CA-FTLW11-001）
    b) 発行者: CA-<hostname>（例: CA-FTLW11-001）
    c) 発行者の詳細: Citrix Systems, Inc.（組織名）
7. セッションホストに自己署名のサーバー証明書があるかどうかを確認します:
    a) 発行先: <host FQDN>（例: FTLW11-001.ctxlab.net）
    b) 発行者: CA-<hostname>（例: CA-FTLW11-001）
    c) 発行者の詳細: Citrix Systems, Inc.（組織名）
8. 証明書が見つからない場合は、Citrix 技術サポートにお問い合わせください。
9. 証明書が存在する場合:
    a) セッションホストで実行されている Citrix Certificate Manager サービスを停止します。
    b) 自己署名のルート CA 証明書と自己署名のサーバー証明書を両方とも削除します。
    c) セッションホストで Citrix Certificate Manager サービスを開始します。本サービスは開始されると新しい証明書を作成します。
10. 内部ユーザーの場合:
    a) セッションホストのファイアウォールが、HDX over EDT および HDX over TCP の TCP 443 または UDP 443 での受信トラフィックをブロックしていないことを確認します。
    b) ネットワークファイアウォールが、クライアントのネットワークとセッションホストのネットワーク間の UDP 443 および TCP 443 のトラフィックをブロックしていないことを確認します。
11. 外部ユーザーの場合:
    a) クライアントの NAT タイプとセッションホストの NAT タイプを確認し、これらの NAT タイプの組み合わせが正常に機能することを確認します。詳しくは、「NAT の互換性」セクションを参照してください。
    b) クライアントまたはセッションホストのいずれかで NAT のテストが失敗した場合:
        i. ファイアウォールがシステムで実行されている場合は、UDP 3478 の送信トラフィックをブロックしていないことを確認します。
        ii. ネットワークファイアウォールが UDP 3478 の送信トラフィックをブロックしていないことを確認します。
        iii. ファイアウォールが STUN サーバーの応答をブロックしていないことを確認します。
    c) ネットワークファイアウォールに、必要なトラフィックをすべて許可する適切な規則が構成されていることを確認します。詳しくは、「ネットワーク要件」セクションを参照してください。
    d) [HDX Direct のポート範囲] ポリシー設定を使用してデフォルトのポート範囲を変更する場合は、カスタムポート範囲に対してファイアウォール規則が設定されていることを確認します。

イベントログ

VDA マシンのイベントログに記録されるイベントは、次のとおりです。

ログ	ID	接続元	レベル	説明
[アプリケーションとサービスログ] > [Citrix-HostCore-HDX Direct/Operational]	1	HDX Direct	情報	内部ユーザー <username>の HDX Direct 接続が確立されました。
[アプリケーションとサービスログ] > [Citrix-HostCore-HDX Direct/Operational]	2	HDX Direct	情報	外部ユーザー <username>の HDX Direct 接続が確立されました。
[アプリケーションとサービスログ] > [Citrix-HostCore-HDX Direct/Operational]	3	HDX Direct	情報	ユーザー< username>の HDX Direct 接続に失敗しました。

既知の問題

HDX Direct が既に有効になっているマシンで VDA のインプレースアップグレードを実行すると、**HDX Direct** が動作しなくなる場合があります。
この問題を解決するには、次の手順を実行します:

1. セッションホストで実行されている Citrix Certificate Manager サービスを停止します。
2. 自己署名のルート CA 証明書と自己署名のサーバー証明書を削除します。
3. レジストリを開きます。
4. `HKLM\Software\Citrix\HDX-Direct`キーを削除します。
5. `HKLM\SYSTEM\CurrentControlSet\Control\TerminalServer\Wds\icawd`に 移動します。
6. **SSLEnabled** 値を0に設定します。
7. **SSLThumbprint** 値の内容を削除します。
8. **Citrix Certificate Manager** サービスを開始します。

Secure HDX（Technical Preview）

August 17, 2024

Secure HDX は、トラフィックパス内のネットワーク要素が HDX トラフィックを検査できないようにするアプリケーションレベルの暗号化（ALE）ソリューションです。これは、AES-256-GCM 暗号化を使用して、Citrix Workspace アプリ（クライアント）と VDA（セッションホスト）間のアプリケーションレベルで真のエンドツーエンド暗号化（E2EE）を提供することで実現します。

> 重要:
>
> Secure HDX は現在、Technical Preview 段階にあります。この機能はサポートなしで提供されているため、運用環境での使用はまだ推奨されていません。フィードバックを送信したり、問題を報告したりする場合は、このフォームを使用してください。

システム要件

Secure HDX を使用するためのシステム要件は次のとおりです。

- コントロールプレーン
  - Citrix DaaS
  - Citrix Virtual Apps and Desktops 2402 以降
- Virtual Delivery Agent（VDA）
  - Windows：バージョン 2402 以降
- Workspace アプリ
  - Windows：バージョン 2402 以降
- アクセス層
  - Citrix Workspace
  - Citrix StoreFront 2402 以降

構成

デフォルトでは、Secure HDX は無効になっています。この機能は、Citrix ポリシーの Secure HDX 設定を使用して構成できます:

Secure HDX：機能をすべてのセッションに対して有効にするか、直接接続に対してのみ有効にするか、無効にするかを定義します。

注意事項

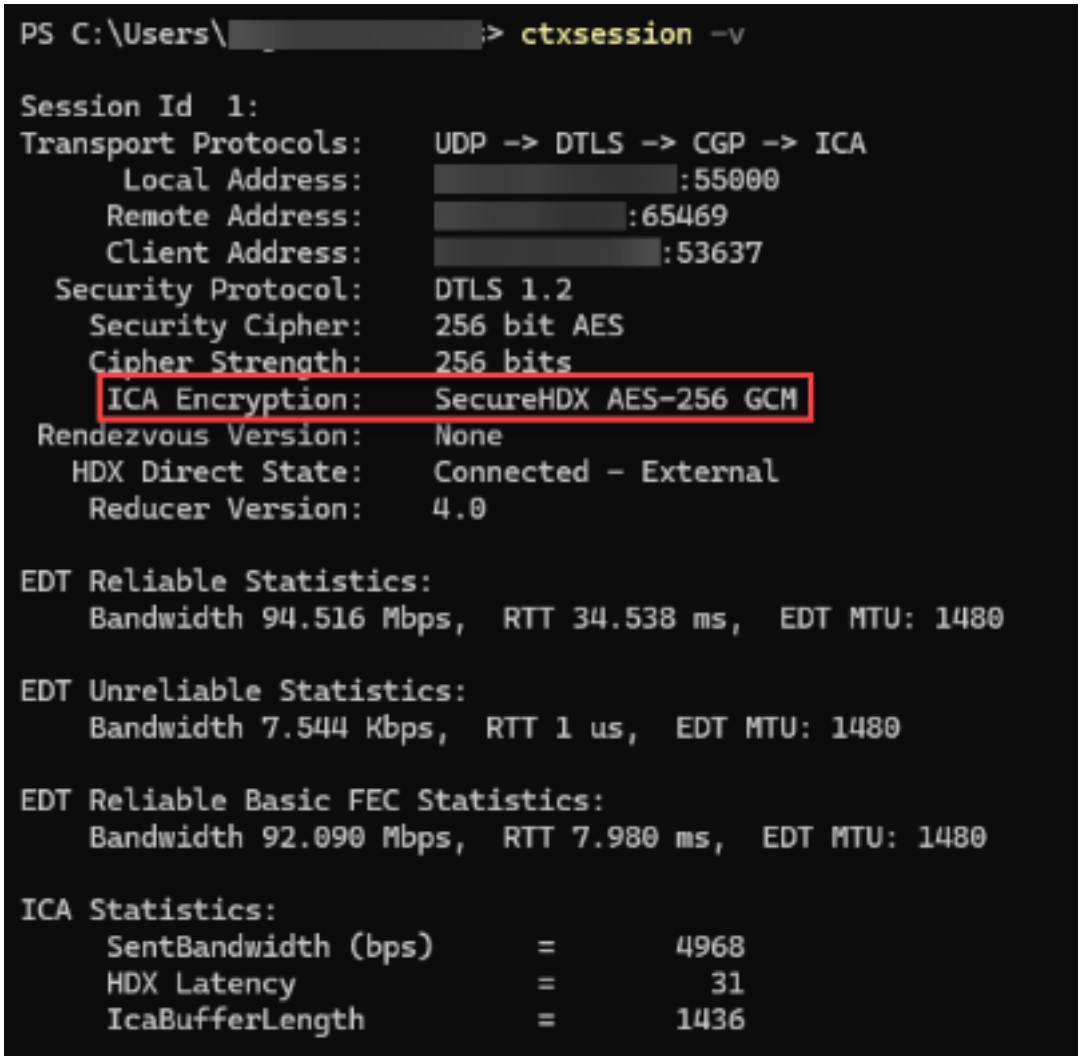
Secure HDX を使用するための注意事項は次のとおりです:

- ユーザーが、機能をサポートしていないクライアントを使用して、Secure HDX が有効になっているセッションホストに接続しようとすると、接続は拒否されます。
- サービス継続性は現在、Secure HDX ではサポートされていません。Citrix Cloud 環境でサービス継続性を有効にしている場合、クラウドサービスが停止すると、Secure HDX が有効になっているセッションホストに接続できなくなる可能性があります。
- HDX Insight を使用する場合、NetScaler は暗号化された HDX トラフィックを検査できないため、Secure HDX を使用すると HDX Insight データの収集が妨げられることに注意してください。HDX Insight を使用する必要がある場合は、直接接続に対してのみ Secure HDX を有効にするように設定できます。
- SmartControl を使用する場合、Secure HDX を使用すると、NetScaler が暗号化された HDX トラフィックを検査できないため、SmartControl が機能しなくなることに注意してください。SmartControl を使用する必要がある場合は、直接接続に対してのみ Secure HDX を有効にするように設定できます。
- Secure HDX が有効になっている場合、マルチストリーム ICA はサポートされません。
- HDX トラフィックの検査に依存するサードパーティソリューションを使用している場合、HDX トラフィックは暗号化されているため、Secure HDX を有効にするとそれらのソリューションは機能しなくなります。

トラブルシューティング

Secure HDX がアクティブであることを確認するには、VDA マシンで `ctxsession.exe`ユーティリティを使用できます。

`CtxSession.exe`ユーティリティを使用するには、セッション内でコマンドプロンプトまたは PowerShell を開き、`ctxsession.exe -v`を実行します。Secure HDX が使用されている場合、ICA 暗号化には`SecureHDX AES-256 GCM`が表示されます。



セッションで **Secure HDX** が有効にならない場合

- 使用中の VDA のバージョンがシステム要件に応じた機能をサポートしていることを確認します。
- Secure HDX を有効にするポリシーが VDA に適用されていること、およびこの機能を無効にする優先度の高いポリシーが他にないことを確認します。
- クライアントデバイスが NetScaler Gateway または Gateway Service 経由で接続している場合は、Secure HDX が「直接接続のみ」に設定されていないことを確認してください。
- Secure HDX を構成したときにセッションホストが既に実行されていた場合は、変更を有効にするためにマシンを再起動します。

仮想チャネルの許可リスト

August 17, 2024

仮想チャネル許可リストは、環境内で許可される Citrix 以外の仮想チャネルを制御できる機能です。デフォルトでは、仮想チャネル許可リスト機能が有効になっています。その結果、Citrix 仮想チャネルのみが Citrix Virtual Apps and Desktops セッションで開けるようになっています。自社製、サードパーティ製を問わず、カスタム仮想チャネルを使用する必要がある場合は、これらを許可リストに明示的に追加する必要があります。

構成

仮想チャネル許可リストがデフォルトで有効になっています。この機能は、Citrix ポリシーの次の設定を使用して構成できます:

- 仮想チャネル許可リスト: 機能を有効または無効にし、仮想チャネルをリストに追加します。
- 仮想チャネルの許可リストのログ調整: 仮想チャネル許可リストのイベント ログの調整期間を設定します。
- 仮想チャネル許可リストのログ: 仮想チャネル許可リストのログレベルを設定します。

許可リストへの仮想チャネルの追加

仮想チャネルを許可リストに追加するには、次の情報が必要です:

1. コードで定義されている仮想チャネル名。最大 7 文字の長さにすることができます。例: `CTXCVC1`。
2. VDA マシンで仮想チャネルを開くプロセスのパス。例: `C:\Program Files\Application\run.exe`。

必要な情報を取得したら、仮想チャネルの許可リストポリシー設定を使用して、仮想チャネルを許可リストに追加する必要があります。仮想チャネルをリストに追加するには、仮想チャネル名のあとにコンマを入力してから、その仮想チャネルにアクセスするプロセスへのパスを入力します。プロセスが複数ある場合は、各プロセスをコンマで区切って追加できます。

単一プロセスの場合

前の例を使用して、以下のエントリをリストに追加します:

```
CTXCVC1,C:\Program Files\Application\run.exe
```


複数プロセスの場合

複数のプロセスがある場合は、以下のエントリをリストに追加します:

```
CTXCVC1,C:\Program Files\Application\run.exe,C:\Program Files\Application
\run2.exe
```

ワイルドカード文字の使用

ワイルドカードの使用（*）がサポートされています。アプリケーションのバージョンに基づいてディレクトリまたは実行可能ファイルの名前が変更された場合、またはサードパーティコンポーネントがユーザーのプロファイルにインストールされている場合は、ワイルドカードを使用できます。

ワイルドカードは次のシナリオで使用できます:

- 完全なディレクトリ名を置き換える場合。
  例: `C:\Program Files\Application\*\run1.exe`
- ディレクトリ名の一部を置き換える場合。
  例: `C:\Program Files\Application\v*\run1.exe`
- 実行可能ファイルの名前を置き換える場合。
  例: `C:\Program Files\Application\v1.2\*.exe`
- 実行可能ファイルの名前の一部を置き換える場合。
  例: `C:\Program Files\Application\v1.2\run*.exe`

次の制限事項が適用されます:

- ワイルドカードは、単一のディレクトリを置き換えるためにのみ使用できます。たとえば、実行可能ファイルが`C:\Program Files\Application\v1.2\run1.exe`にある場合、以下のようになります
  - 使用可能: `C:\Program Files\Application\*\run1.exe`
  - 使用不可: `C:\Program Files\*\run1.exe`
- エントリにはファイル拡張子が含まれている必要があります。
  - 使用可能: `C:\Program Files\Application\v1.2\*.exe`
  - 使用不可: `C:\Program Files\Application\v1.2\*`
- すべてのパスはローカルである必要があります。

> 注:
>
> - ネットワークパスの使用は許可されていません。
> - ワイルドカードのサポートは、Citrix Virtual Apps and Desktops 2206 から利用できます。
> - ワイルドカードのサポートは、Citrix Virtual Apps and Desktops 2203 LTSR の CU2 から利用できます。

システム環境変数の使用

システム環境変数を使用すると、許可リスト内の信頼できるプロセスの定義を簡素化できます。%programfiles%、%programfiles(x86)%、%systemdrive%、%systemroot%などの通常の変数を使用できます。

システムレベルで定義されている限り、カスタム環境変数を使用することもできます。

次の例は、通常の環境変数を示しています:

- %programfiles%\Application\v1.2\run.exe
- %programfiles%\Application*\run.exe
- %programfiles(x86)%\Application\v1.*\run.exe

次の例は、カスタムのシステム環境変数を示しています:

- カスタム変数名: app
- カスタム変数値: %programfiles%\Application\
- 許可リストのエントリ: CTXCVC1,%app%\run.exe

> 注:
>
> ユーザー環境変数はサポートされていません。
>
> 環境変数のサポートは、Citrix Virtual Apps and Desktops バージョン 2209 から利用できます。

仮想チャネル名とプロセスの取得

仮想チャネルの名前と VDA マシンで仮想チャネルを開くプロセスを取得する最も簡単な方法は、仮想チャネルを提供した開発者またはサードパーティベンダーから情報を取得することです。

別の方法としては、機能のログを適用し、次の手順に従うことで情報を取得することもできます:

1. カスタム仮想チャネルのクライアントコンポーネントとサーバーコンポーネントを配置したら、仮想アプリケーションまたは仮想デスクトップを起動します。
2. VDA マシンのシステムイベントログにて、開こうとしたカスタム仮想チャネルの名前とプロセスを探します。利用可能なイベントについて詳しくは、「イベントログ」を参照してください。
3. セッションからログアウトします。
4. 仮想チャネル許可リストポリシー設定に、識別された仮想チャネルとプロセスに関するエントリを追加します。
5. マシンを再起動してください。
6. VDA が登録されたら、仮想アプリケーションまたは仮想デスクトップを実行して、カスタム仮想チャネルが正常に開くことを確認します。

Citrix 仮想チャネルに関する考慮事項

組み込みの Citrix 仮想チャネルはすべて信頼されており、追加の構成なしで開くことができます。ただし、次の 2 つの機能は、外部の依存関係のために許可リストに明示的なエントリを必要とします:

- マルチメディアリダイレクト
- HDX RealTime Optimization Pack for Skype for Business

マルチメディアリダイレクト

Windows Media Player 以外のメディアプレーヤーをシステムメディアプレーヤーとして使用する場合は、信頼できるプロセスとして許可リストに追加する必要があります。次の情報は、許可リストのエントリに必要です:

- 仮想チャネル名: `CTXMM`
- プロセス: VDA マシンで使用されているメディアプレーヤーのパス。例: `C:\Program Files (x86)\Windows Media Player\wmplayer.exe`。
- 許可リストのエントリ: `CTXMM,C:\Program Files (x86)\Windows Media Player\wmplayer.exe`

HDX RealTime Optimization Pack for Skype for Business

次の情報は、許可リストのエントリに必要です:

- 仮想チャネル名: `CTXRMEP`
- プロセス: VDA マシン内の Skype for Business 実行可能ファイルのパス。Skype for Business のバージョンや、カスタムインストールパスの使用の有無によって異なる場合があります。例: `C:\Program Files\Microsoft Office\root\Office16\lync.exe`.
- 許可リストのエントリ: `CTXRMEP,C:\Program Files\Microsoft Office\root\Office16\lync.exe`

トラブルシューティング

August 17, 2024

カスタム仮想チャネルが開かない場合は、次の手順を確認してください:

1. 正しい VDA バージョンを使用していることを確認します。
2. 仮想チャネル許可リストでポリシーがカスタム仮想チャネルを含む VDA に適用されていること、およびこの構成を上書きする優先度の高い他のポリシーがないことを確認します。

3. VDA のイベントログを確認し、報告された仮想チャネル名が許可リストで定義されているものと一致していることを確認します。

   a) 複数のプロセスがある場合は、「許可リストへの仮想チャネルの追加」の説明に従って、これらが適切に定義されていることを確認してください。
   b) 定義されたプロセスパスでワイルドカードを使用している場合は、「ワイルドカード文字の使用」のガイドラインに従っていることを確認してください。
   c) 定義されたプロセス パスで環境変数を使用している場合は、「システム環境変数の使用」のガイドラインに従っていることを確認してください。

イベントログ

VDA マシンのイベントログに記録されるイベントは、次のとおりです。

シングルセッション **VDA**

次のイベントは、シングルセッション VDA マシンのイベントログに記録されます:

ログ名	Id	接続元	レベル	説明
システム	2001	Picadd	情報	カスタム仮想チャネル<vcName>がプロセス<processName>によって開かれました
システム	2002	Picadd	警告	カスタム仮想チャネル<vcName>をプロセス<processName>で開くことはできません
システム	2003	Picadd	情報	<username>がカスタム仮想チャネル<vcName>を開きました
システム	2004	Picadd	警告	<username>がカスタム仮想チャネル<vcName>を開こうとしました

ログ名	Id	接続元	レベル	説明
システム	2005	Picadd	エラー	ポリシー<pathInPolicy>で指定されたパスは、プロセスパスに解決できません
システム	2007	Picadd	情報	読み込まれたプロセスパスは<processPath>です
システム	2008	Picadd	エラー	VC ポリシー パスに環境変数<varName>が見つかりません

マルチセッション **VDA**

次のイベントは、マルチセッション VDA マシンのイベントログに記録されます:

ログ名	Id	接続元	レベル	説明
システム	13	Rpm	情報	カスタム仮想チャネル<vcName>がプロセス<processName>によって開かれました
システム	14	Rpm	警告	カスタム仮想チャネル<vcName>をプロセス<processName>で開くことはできません
システム	15	Rpm	情報	<username>がカスタム仮想チャネル<vcName>を開きました

ログ名	Id	接続元	レベル	説明
システム	16	Rpm	警告	<username>がカスタム仮想チャネル<vcName>を開こうとしました
システム	17	Rpm	エラー	ポリシー<pathInPolicy>で指定されたパスは、プロセスパスに解決できません
システム	18	Rpm	情報	読み込まれたプロセスパスは<processPath>です
システム	19	Rpm	エラー	VC ポリシー パスに環境変数<varName>が見つかりません

既知のサードパーティ仮想チャネル

August 17, 2024

以下は、カスタム Citrix 仮想チャネルを使用する既知のサードパーティソリューションです。このリストには、カスタム Citrix 仮想チャネルを使用するすべてのソリューションが含まれているわけではありません。

- Cerner
- ControlUp
- Cisco WebEx Teams
- Cisco WebEx Meetings 仮想デスクトップソフトウェア
- deviceTrust
- Epic Warp Drive
- Epic Slingshot
- Imprivata OneSign
- Midmark IQPath クライアント拡張機能
- Nuance PowerMic クライアント拡張機能

- Nuance Dragon Medical Network Edition 360 vSync
- Zoom Meetings for VDI
- Ultima IA-Connect

関連する仮想チャネルを許可リストに追加することについて詳細を取得するには、ソリューションのベンダーに連絡してください。または、「仮想チャネル名とプロセスの取得」に記載されている手順に従ってください。

デバイス

August 17, 2024

HDX は、どんな場所にあるどんなデバイスでも高品位なユーザーエクスペリエンスを提供します。「デバイス」セクションの記事では、以下のデバイスについて説明します:

- スキャン
- 一般的な USB デバイス
- クライアントドライブマッピング
- モバイルおよびタッチスクリーンデバイス
- シリアルデバイス
- 特殊キーボード
- Web カメラ

最適化された **USB** デバイスと一般的な **USB** デバイス

最適化された USB デバイスとは、Citrix Workspace アプリが特定のサポートを提供しているデバイスです。たとえば、HDX マルチメディア仮想チャネルを使用して Web カメラをリダイレクトする機能などのサポートです。一般的なデバイスとは、Citrix Workspace アプリで特定のサポートがない USB デバイスのことです。

一般的な USB のリダイレクト機能では、一般モードに設定されていなければ、最適化された仮想チャネルをサポートする USB デバイスをデフォルトではリダイレクトできません。

一般的に、USB デバイスは一般モードよりも最適化モードで優れたパフォーマンスを発揮します。ただし、USB デバイスが最適化モードでの機能を完全に備えていない場合があります。そのデバイスの機能を完全に利用するには、一般モードに切り替える必要がある場合もあります。

USB 大容量記憶装置デバイスでは、Citrix ポリシーによって制御されるクライアントドライブマッピングまたは一般的な USB のリダイレクト機能のどちらか、またはその両方を使用できます。主な違いは次のとおりです。

一般的な USB のリダイレクト機能とクライアントドライブマッピングのポリシーの両方が有効な場合、セッション開始前または後に挿入された大容量記憶装置デバイスがクライアント側ドライブのマッピングによりリダイレクトされます。

これらの条件が満たされると、大容量記憶装置は一般的な USB のリダイレクト機能を使用してリダイレクトされます。

- 一般的な USB のリダイレクト機能とクライアントドライブマッピングのポリシーの両方が有効になっています。
- デバイスが自動リダイレクトに構成されています。
- 大容量記憶装置がセッションの開始前または後に挿入されます。

詳しくは、http://support.citrix.com/article/CTX123015を参照してください。

機能	クライアントドライブマッピング	汎用 USB リダイレクト
デフォルトで有効	はい	いいえ
読み取り専用アクセスの構成が可能	はい	いいえ
デバイスアクセスが暗号化される	はい（仮想セッションでデバイスにアクセスする前に暗号化のロックを解除した場合）。	Citrix Virtual Desktops のみ

スキャン

August 17, 2024

スキャナーは、画像、印刷されたテキスト、手書き文字、またはオブジェクトを光学的にスキャンし、デジタル画像に変換するデバイスです。

スキャナーを使用しており、コンピューターが Windows を実行している場合は、WIA スキャナードライバーを使用している可能性が高いです。このドライバーは、コンピューターとスキャナー間の通信を担当します。

- **Windows Image Acquisition**（WIA）は、ソフトウェアがスキャナーなどのイメージ作成ハードウェアと通信できるようにする Microsoft のドライバーモデルおよびアプリケーションプログラミングインターフェイス（API）です。
- **TWAIN**（Windows および Mac）は、もう 1 つのプロトコルであり、標準インターフェイスを提供することでスキャナーとアプリケーションを接続するスキャンプロトコルです。TWAIN を使用すると、アプリケーションは TWAIN 準拠のデバイス（スキャナー、デジタルカメラなど）から画像を取得できます。

TWAIN Redirection

August 17, 2024

はじめに

TWAIN は、画像ソフトウェアをスキャナーまたはデジタルカメラにリンクするために使用されるスキャンプロトコルです。

TWAIN の仕組み

- Citrix セッション内のいずれかの 32 ビットアプリケーションを使用してドキュメントをスキャンします。

  > 注:
  >
  > ローカルに接続された TWAIN 準拠のスキャナーを使用してドキュメントをスキャンします。

- Citrix スキャンモジュールは、TWAIN の要求をクライアントのスキャナーにリダイレクトします。
- スキャンが完了すると、セッションホストに通知されます。

要件

Citrix コントロールプレーン

- Citrix Virtual Apps and Desktops 1912 以降
- Citrix DaaS

セッションホスト

- オペレーティングシステム
  - Windows 10 1809 以降
  - Windows 11
  - Windows Server 2022 以降
- VDA
  - Version 1912 or later
- アプリケーション
  - 32 ビットアプリケーション

クライアントデバイス

- オペレーティングシステム
  - Windows 10 1809 以降
  - Windows 11
- Workspace アプリ
  - Windows：バージョン 1912 以降
- スキャナー
  - TWAIN 準拠スキャナー

構成

- クライアントエンドポイントに TWAIN ドライバーをインストールします。
- デバイスまたはアプリケーションが TWAIN と WIA の両方をサポートしている場合は、必要なスキャンプロトコルを選択するように設定してください。
- スキャナーをクライアントエンドポイントにローカルで接続します（USB 経由）。
- 必要に応じて、USB リダイレクト経由で TWAIN デバイスをセッションにリダイレクトします。

  > 注:
  >
  > TWAIN デバイスは USB リダイレクトでは適切に動作しないため、スキャン品質が低下します。

ポリシー設定

TWAIN リダイレクトを設定し、スキャン機能を向上させるためのポリシー設定。

- クライアント **TWAIN** デバイスリダイレクト： TWAIN リダイレクトを有効または無効にします。

  > 注:
  >
  > デフォルトでは、TWAIN リダイレクトは有効になっています。

- **TWAIN** 圧縮レベル：クライアントからホストへの画像の圧縮レベルを設定します。

詳しくは、「Twain デバイスのポリシー設定」を参照してください。

トラブルシューティング

このURLからダウンロードできる公開テストアプリ Twacker を使用して、TWAIN を試してみてください。

公開されたデスクトップセッション内で TWAIN を検証するには、次の手順を実行します:

1. VDA に **Twacker** をインストールします。
2. **Twacker**（32 ビットバージョン）を起動します。
3. [**File**] > [**Select Source**] をクリックして、一覧からスキャナーを選択します。
4. [**File**] > [**Acquire**] をクリックします。
5. スキャナーをテストするには、[スキャン] ボタンをクリックします。

Twacker が正常にスキャンできる場合、**Citrix Virtual Apps and Desktops** のセットアップが次の状態であることが確認されます:

- 構成された USB リダイレクトの設定
- TWAIN デバイスの使用
- すべてのローカルクライアントデバイス要件を満たす

特定のアプリケーション内でスキャンの問題がまだ発生する場合は、ソフトウェアの問題である可能性があります。

WIA デバイス

August 17, 2024

要件

- スキャナーは WIA 準拠である必要があります。
- ローカルデバイスに WIA ドライバーをインストールします。サーバー上には TWAIN ドライバーは必要ありません。
- スキャナーをローカルに接続します（USB 経由など）。
- スキャナーが TWAIN ドライバーではなくローカルの Windows Image Acquisition サービスを使用していることを確認します。
- テストに使用するユーザーアカウントに、ICA セッション内の帯域幅を制限しているポリシー（たとえば、クライアント USB デバイスリダイレクトの最大帯域幅）が適用されていないことを確認します。

Windows Image Acquisition アプリケーションの許可リスト

許可リストにより、VDA 上のどのアプリケーションに Windows Image Acquisition スキャナーのリダイレクトへのアクセスを許可するかを制御できます。レジストリエディターでは、Windows Image Acquisition を含む各

VDA の許可リスト設定からの入力を使用します。デフォルトでは、Windows Image Acquisition にアクセスできるアプリケーションはありません。

VDA 上のアプリケーションの Windows Image Acquisition を調整するには、レジストリで管理される機能の一覧にある「Windows Image Acquisition アプリケーションの許可リスト」の設定を参照してください。

ポリシー設定について詳しくは、「WIA デバイスのポリシー設定」を参照してください。

汎用 **USB** デバイス

August 17, 2024

はじめに

汎用 USB リダイレクト機能を使用すると、クライアントマシンから HDX セッションに USB デバイスをリダイレクトできるため、エンドユーザーは HDX セッションでさまざまな汎用 USB デバイスを操作できるようになります。これは、最適化されたサポートがない特殊なデバイスをユーザーが使用する必要がある場合や、サポートが適切でない場合に便利です。

> 注：仮想チャネルのサポート用に最適化されていない USB デバイスは、汎用 USB 仮想チャネルを使用してリダイレクトされます。

どのように動作するのですか**?**

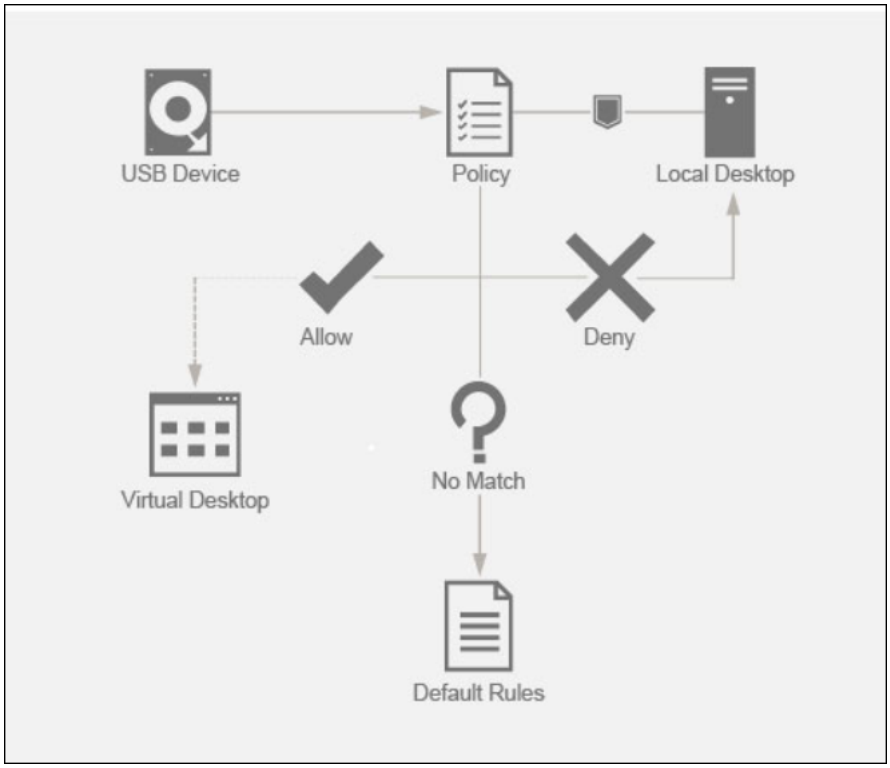
汎用 USB リダイレクトは低レベルで動作し、クライアントマシンと XenDesktop 仮想デスクトップ間で USB 要求メッセージと応答メッセージをリダイレクトします。

クライアントマシンに互換性のあるデバイスは必要ありません。ドライバーは仮想デスクトップでのみサポートされます。USB リダイレクトポリシー規則は特定の優先順位に従い、DDC ポリシー規則が評価および適用された後にクライアント側のポリシーとデフォルトの規則が優先されるようにします。これにより、Citrix 管理者は認証されていない/なりすましのデバイスがセッション内でリダイレクトされるのを防ぎます。

さらに、リモートセッションにアクセスしようとする不正なデバイスのイベントログを監査してフラグを付けることができ、管理者はデータの流出を防ぐための追加のアクションを実行できます。

ユーザーが USB デバイスを装着すると、一致が見つかるまで、セッションホストで各ポリシー規則が順に確認されます。マッチする最初の規則でリダイレクトが許可されているかどうかがチェックされます。

- 最初の一致が Allow 規則の場合、USB デバイスは仮想デスクトップにリダイレクトされます。
- 最初の一致が Deny 規則の場合、デバイスはセッションにリダイレクトされず、ローカルユーザーデバイスでのみ使用できるようになります。一致する規則がない場合、デフォルトの規則が使用されます。



構成

August 17, 2024

URL リダイレクトはデフォルトで無効になっています。Citrix ポリシーの次の設定を使用して、汎用 USB リダイレクトを構成できます:

- クライアント **USB** デバイスリダイレクト: USB リダイレクトを有効または無効にする
- クライアント **USB** デバイスリダイレクト規則: 特定のデバイス操作を指定する（つまり、特定のデバイスへのアクセスを許可または拒否する）
- クライアント **USB** デバイス リダイレクト規則（バージョン **2**）: USB デバイスのフィルタリング、分割、自動接続の規則を指定する
- クライアント **USB** デバイス最適化規則: 最適化を無効にする、または最適化モードを変更する
- 既存の **USB** デバイスの自動接続を許可する: HDX セッション開始時にクライアントエンドポイントに接続された既存の USB デバイスの自動接続を許可または禁止する
- 新しく受信した **USB** デバイスの自動接続を許可する: HDX セッション中にクライアントエンドポイントに接続された既存の USB デバイスの自動接続を許可または禁止する

詳しくは、「USB ポリシー設定」を参照してください。

USB リダイレクトの構成方法

デフォルトでは、USB リダイレクトの構成は無効になっています。これを使用するには、DDC で USB リダイレクトポリシーと特定のリダイレクト規則を有効にして構成する必要があります。

> 注:
>
> バージョン 2212 より古いコンポーネントを使用している場合、または Linux/Mac 向け Workspace アプリを使用している場合、USB リダイレクトを構成する方法の詳細については、「レガシー USB リダイレクト構成」を参照してください。

汎用 **USB** リダイレクトの有効化

1. **Citrix Web Studio** ポリシーを開き、［ポリシー］タブをクリックします。
2. ［ポリシーの作成］をクリックし、［**ICA**］**>** ［**USB Devices policies**］を展開します。
3. クライアント **USB** デバイスリダイレクトポリシーを編集します。
4. ［許可］を選択し、［保存］をクリックします。

USB リダイレクトポリシー規則の作成

ユーザーが USB デバイスを仮想デスクトップにリダイレクトしようとすると、一致するものが見つかるまで各 USB ポリシー規則に対して順番にチェックされます。どのデバイスでも、最初に一致したものが最終的な一致と見なされます。最初の一致が **Allow** 規則である場合、一致したデバイスは仮想デスクトップにリダイレクトされることが許可されます。最初の一致が **Deny** 規則の場合、一致したデバイスはローカルデスクトップでのみ使用可能になります。一致する規則がない場合、デフォルトの規則が使用されます。

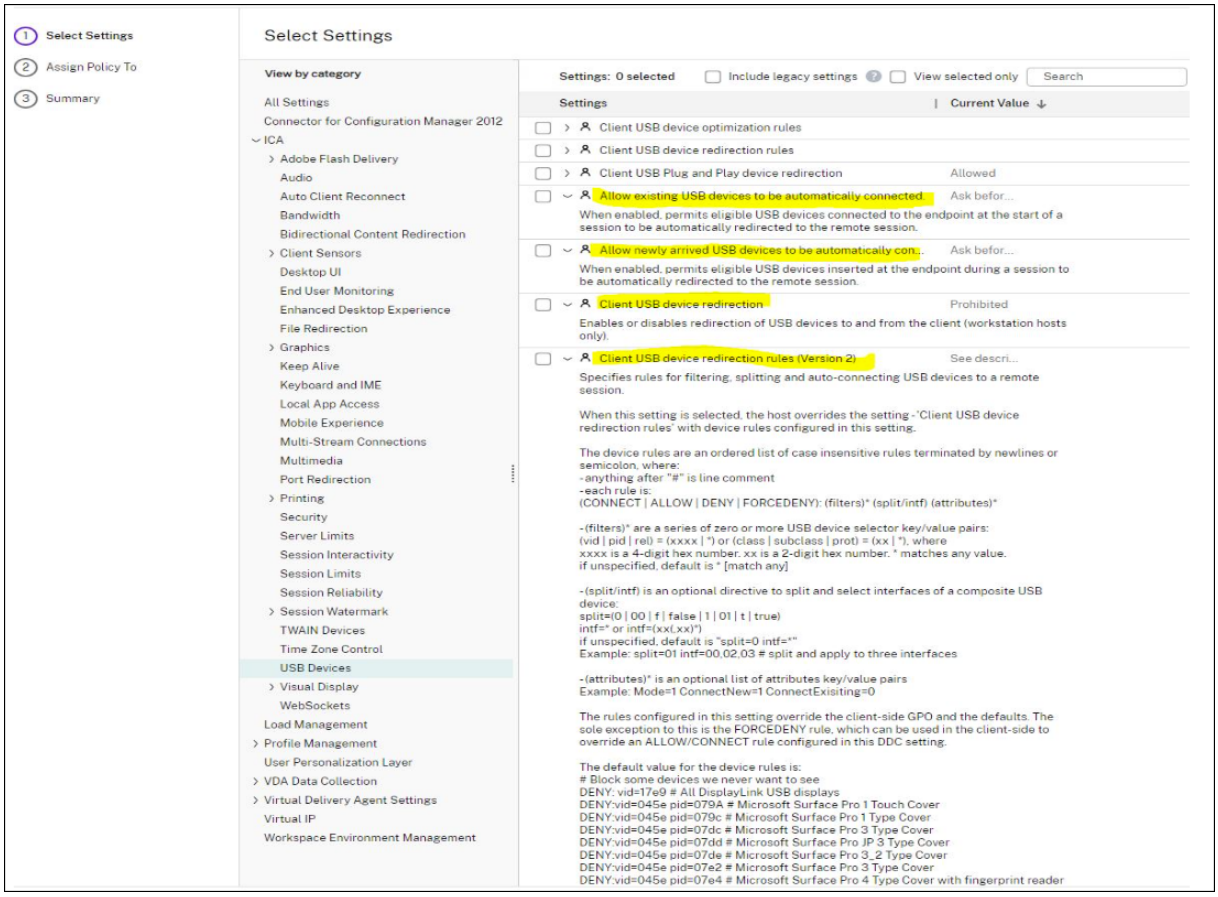
デバイス規則　通常の USB デバイスと同様に、エンドポイントのポリシーまたはクライアント Citrix Workspace アプリ構成で設定されたデバイス規則は、転送するデバイスを選択します。Citrix Workspace アプリは、これらの規則を使用して、リモートセッションへの転送を許可または禁止する USB デバイスを決定します。

各規則は、アクションキーワード（**Allow**、**Connect**、または **Deny**）、コロン（:）、およびエンドポイント USB サブシステムの実際のデバイスと一致する 0 個以上のフィルターパラメーターで構成されています。これらのフィルターパラメーターは、すべての USB デバイスが自身を識別するために使用する USB デバイスの記述子メタデータに対応します。

デバイス規則はクリアテキストであり、各規則は 1 行に表示され、オプションのコメントは # 文字の後に記載されています。規則はトップダウンで照合されます（優先度の降順）。デバイスまたは子インターフェイスに一致する最初の規則が適用されます。同じデバイスまたはインターフェイスを選択する後続の規則は無視されます。

例： ALLOW VID=1050 PID=0421 #Device1
例： CONNECT VID=xxxx PID=yyyy Class=03 #Device2

キーワード	説明
CONNECT	このキーワードを使用すると、デバイスを USB 仮想チャネル経由でリダイレクトできるだけでなく、セッションの起動時や挿入時に自動的にリダイレクトできるようになります。
ALLOW	このキーワードを使用して、USB 仮想チャネル経由でデバイスがリダイレクトされるのを許可します
DENY	このキーワードを使用して、USB 仮想チャネル経由でデバイスがリダイレクトされるのを拒否します



DDC のポリシーの設定:

1. **Citrix Web Studio** ポリシーを開き、［ポリシー］タブをクリックします。
2. ［ポリシーの作成］をクリックし、［**ICA**］**>** ［**USB Devices policies**］を展開します。
3. クライアント **USB** デバイスリダイレクト規則（バージョン **2**）を編集します。
4. リダイレクトする必要がある各 USB デバイスの説明に記載されている例に基づいて値を設定し、［保存］をクリックします。

例：Allow: VID=056A PID=00A4 #STU-430
Deny: Class=08 subclass=05 # 大容量記憶装置

> 注：
>
> Citrix 管理者が ［デフォルト値を使用する］をチェックし、［保存］をクリックすると、デフォルトの規則は VDA の次のレジストリで見つかります。
>
> 注意
>
> レジストリエディターを使用する前に、この記事の最後に記載されている免責事項を参照してください。

`HKLM\SOFTWARE\Wow6432Node\Citrix\PortICA\GenericUSB\DeviceRules`

> 注：
>
> グループポリシーデバイス規則を使用してクライアントデバイスにポリシーを設定することは引き続き可能ですが、Citrix Virtual Apps and Desktops および Citrix Workspace アプリの新しいバージョンではその必要はありません。
>
> USB デバイスのレガシー構成については、「レガシー USB リダイレクト構成」を参照してください。

USB デバイスの自動リダイレクトを構成する（オプション）

USB サポート機能が有効になっており、USB 関連のユーザー設定で USB デバイスに自動接続するように設定されている場合は、USB デバイスが自動的にリダイレクトされます。一部の USB デバイスはリダイレクトしない方が良い場合もあります。ユーザーは、USB デバイスリストから、自動的にリダイレクトされないデバイスを明示的にリダイレクトすることができます。USB デバイスのリスト表示とリダイレクトを禁止するには、クライアントエンドポイントまたは Desktop Delivery Controller ポリシーで DeviceRules を適用します。
このポリシーは、DDC、GPO を使用するクライアント、Citrix Workspace 環境設定、または CDViewer の［接続］タブを使用して設定できます。これらすべての方法について以下に説明します：

DDC のポリシーの設定：

DDC には USB デバイスの自動リダイレクトを許可するために設定できるポリシーが 2 つあります。

- 既存の USB デバイスの自動接続を許可する
- 新しく受信した USB デバイスの自動接続を許可する

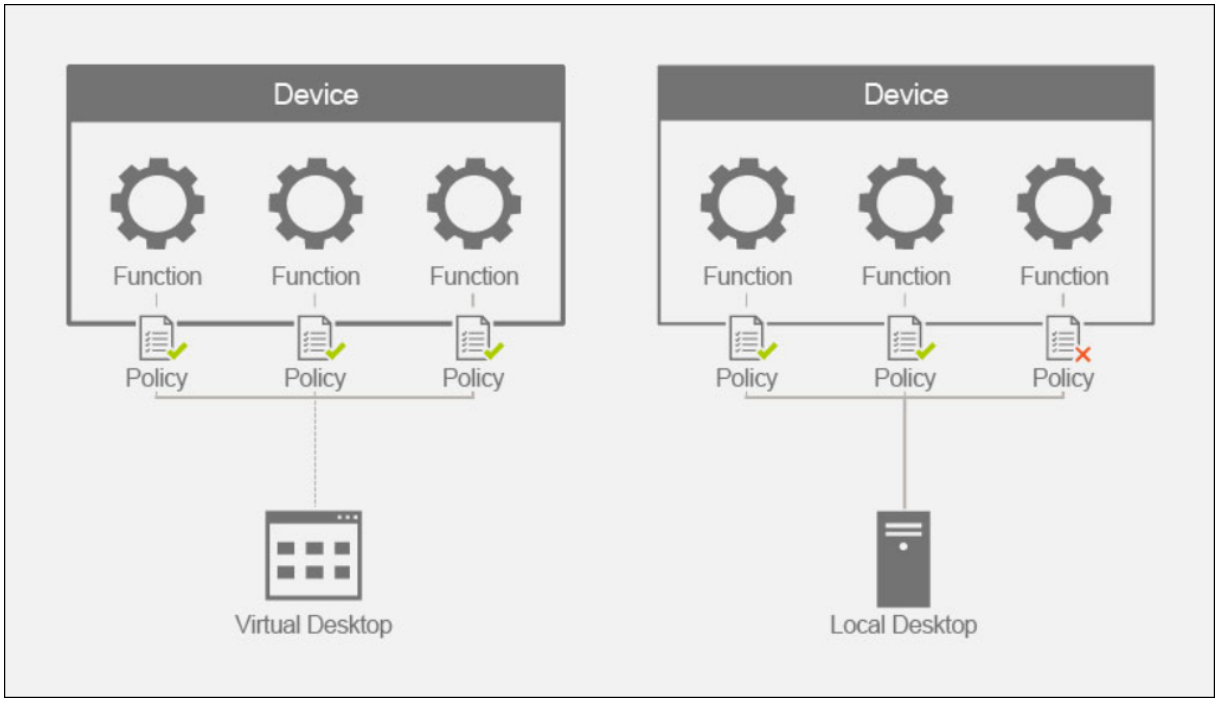
1. **Citrix Web Studio** ポリシーを開き、［ポリシー］タブをクリックします。
2. ［ポリシーの作成］をクリックし、［**ICA**］**>** ［**USB Devices policies**］を展開します。
3. 既存の **USB** デバイスの自動接続を許可する設定を編集します。
4. ［デフォルト値を使用する］チェックボックスをオフにし、ドロップダウンメニューから ［使用可能な **USB** デバイスを自動的にリダイレクトする］を選択して ［保存］をクリックします。

5. 新しく受信した **USB** デバイスの自動接続を許可する設定を編集します。
6. ［デフォルト値を使用する］チェックボックスをオフにし、ドロップダウンメニューから ［使用可能な **USB** デバイスを自動的にリダイレクトする］を選択して ［保存］をクリックします。

複合デバイスとデバイス分割

August 17, 2024

複合 USB デバイスは、コンピューターに接続された複数の独立した USB デバイスのように動作する単一のデバイスです。USB コネクタは 1 つだけですが、それぞれ独自の機能セットを持つ複数のインターフェイスをコンピューターに公開できます。ユーザーが複合 USB デバイスを接続すると、ホストデバイスは各ポリシー規則に対してすべての機能（インターフェイス）をチェックします。いずれかの機能（インターフェイス）の最初の一致が Deny 規則である場合、その規則が複合デバイスの決定的な一致として見なされ、デバイスは拒否されます。機能（インターフェイス）の最初の一致が Allow 規則である場合、ホストデバイスは次の機能（インターフェイス）に対して規則の一致を続行します。ポリシー規則によって機能（インターフェイス）が拒否されていない場合、複合デバイスは許可されます。複合デバイスの決定的な一致が Deny 規則である場合、デバイスはローカルデスクトップでのみ使用可能になり、それ以外の場合はデバイスは仮想デスクトップにリモートで接続されます。一致する規則がない場合、デフォルトの規則が使用されます。



デバイスリダイレクト規則（バージョン 2）ポリシーの適切な規則を使用して複合デバイスを分割し、複合デバイスの特定の機能のみを許可できます。たとえば、FIDO2 キーの HID 機能のみを使用し、スマートカード機能は使用したくない場合があります。その場合、以下のように規則を設定します:

1. Connect: VID=1050 PID=0407 class=03 split=01 intf=00,01 #Yubikey シリーズ 5 では FIDO2 HID 機能が許可されました。
2. Deny: VID=1050 PID=0407 split=01 intf=02 # Yubikey シリーズ 5 スマートカード機能がブロックされました。

> ヒント:
>
> 新しいポリシー規則を作成する場合、USB Web サイトでUSB クラスコードを参照してください。

署名パッドの構成

1. VDA ホストに適切なデバイスドライバーをインストールします。
2. **Citrix Web Studio** でクライアント **USB** デバイスリダイレクトポリシーをオンにします。
3. クライアント **USB** デバイスリダイレクト規則（バージョン **2**）ポリシーを編集します。
    a) リダイレクトする必要がある署名パッドの **VID** と **PID** 情報を設定し、［保存］をクリックします。例: 接続: VID=056A PID=00A4 #STU-430
4. ポリシーのクライアント **USB** デバイス最適化規則を編集します。
    a) 他のデバイス情報とともにモードを設定します。例: Mode=00000004 VID=056A PID=00A4 class=03 # キャプチャモードで動作する入力デバイス
5. 既存の **USB** デバイスの自動接続を許可するポリシーを編集します。
6. ［デフォルト値を使用する］チェックボックスをオフにし、ドロップダウンメニューから ［使用可能な **USB** デバイスを自動的にリダイレクトする］を選択して ［保存］をクリックします。
7. 新しく受信した **USB** デバイスの自動接続を許可するポリシーを編集します。
8. ［デフォルト値を使用する］チェックボックスをオフにし、ドロップダウンメニューから ［使用可能な **USB** デバイスを自動的にリダイレクトする］を選択して ［保存］をクリックします。

Studio コンソールでこれらのポリシーが設定されると、以降のセッションの起動時にデバイスが自動的にリダイレクトされ、エンドユーザーによる追加の操作は必要ありません。

> 注:
>
> VID と PID を、リダイレクトするデバイスの実際の VID と PID に置き換えます。

USB リダイレクトを使用した **Bloomberg** キーボードの構成

1. **Citrix Web Studio** でクライアント **USB** デバイスリダイレクトポリシーをオンにします。
2. Bloomberg 5 キーボードは、クライアント USB デバイスリダイレクト規則（バージョン 2）ポリシーでデフォルトで設定されており、追加の管理者の操作は必要ありません。

3. 既存の **USB** デバイスの自動接続を許可するポリシーを編集します。
4. ［デフォルト値を使用する］チェックボックスをオフにし、ドロップダウンメニューから ［使用可能な **USB** デバイスを自動的にリダイレクトする］を選択して ［保存］をクリックします。
5. 新しく受信した **USB** デバイスの自動接続を許可するポリシーを編集します。
6. ［デフォルト値を使用する］チェックボックスをオフにし、ドロップダウンメニューから ［使用可能な **USB** デバイスを自動的にリダイレクトする］を選択して ［保存］をクリックします。

Studio コンソールでこれらのポリシーが設定されると、Bloomberg キーボードは後続の HDX セッションで自動的に表示され、エンドユーザーによる追加の操作は必要ありません。

USB リダイレクトを使用した **FIDO2** キーの構成

Citrix では、HDX セッションで FIDO2 キーを使用する場合は FIDO2 リダイレクトを使用することをお勧めします。ただし、代わりに USB リダイレクトを使用して FIDO2 キーをリダイレクトする必要がある状況もあります。これには、クライアント、VDA、またはオペレーティングシステム（Windows Server 2016 など）で機能がサポートされていないために FIDO2 リダイレクトが利用できないシナリオが含まれます。

キーに複数のモードが有効になっているものの、HDX セッションではそれらのモードのサブセットのみを許可したいという状況も考えられます。たとえば、FIDO2 と OTP を許可し、スマートカードはブロックしたい場合があります。

次の手順は、USB リダイレクトを使用して FIDO2 キーを構成する方法を示しています（Yubikey vid=1050、pid=0407）。

1. **Citrix Web Studio** でクライアント **USB** デバイスリダイレクトポリシーをオンにします。
2. クライアント **USB** デバイスリダイレクト規則（バージョン 2）ポリシーを編集します。
    a) セッションでリダイレクトされる FIDO2 キーの **VID** と **PID** 情報、および分割デバイス構成を設定し、［保存］をクリックします。
    b) **Connect**: VID=1050 PID=0407 class=03 split=01 intf=00,01 #Yubikey シリーズ 5 では FIDO2 HID 機能が許可されました。
    c) **Deny**: VID=1050 PID=0407 split=01 intf=02 # Yubikey シリーズ 5 スマートカード機能がブロックされました。
3. 既存の **USB** デバイスの自動接続を許可するポリシーを編集します。
4. ［デフォルト値を使用する］チェックボックスをオフにし、ドロップダウンメニューから ［使用可能な **USB** デバイスを自動的にリダイレクトする］を選択して ［保存］をクリックします。
5. 新しく受信した **USB** デバイスの自動接続を許可するポリシーを編集します。
6. ［デフォルト値を使用する］チェックボックスをオフにし、ドロップダウンメニューから ［使用可能な **USB** デバイスを自動的にリダイレクトする］を選択して ［保存］をクリックします。

Studio コンソールでこれらのポリシーが設定されると、FIDO2 キーは後続の HDX セッションで自動的に表示され、エンドユーザーによる追加の操作は必要ありません。

USB リダイレクトを使用した 3D マウスの構成

現在、3dConnexion SpaceMouse ドライバーはワークステーション OS（Windows 10 および 11）でのみサポートされています。サーバー OS では動作しません。ワークステーション OS 上で SpaceMouse Enterprise を構成する手順は次のとおりです（vid=046D、pid=C016）。

1. VDA ホストに最新のWindows ドライバーをインストールします。
2. **Citrix Web Studio** でクライアント **USB** デバイスリダイレクトポリシーをオンにします。
3. クライアント **USB** デバイスリダイレクト規則（バージョン **2**）ポリシーを編集します。
    a) リダイレクトする必要がある署名パッドの **VID** と **PID** 情報を設定し、［保存］をクリックします。例: 接続: VID=046D PID=C016 #SpaceMouse Enterprise
4. ポリシーのクライアント **USB** デバイス最適化規則を編集します。
    a) 他のデバイス情報とともにモードを設定します。例: Mode=00000004 VID=046D PID=C016 class=03 # キャプチャモードで動作する入力デバイス
5. 既存の **USB** デバイスの自動接続を許可するポリシーを編集します。
6. ［デフォルト値を使用する］チェックボックスをオフにし、ドロップダウンメニューから ［使用可能な **USB** デバイスを自動的にリダイレクトする］を選択して ［保存］をクリックします。
7. 新しく受信した **USB** デバイスの自動接続を許可するポリシーを編集します。
8. ［デフォルト値を使用する］チェックボックスをオフにし、ドロップダウンメニューから ［使用可能な **USB** デバイスを自動的にリダイレクトする］を選択して ［保存］をクリックします。

トラブルシューティング

August 17, 2024

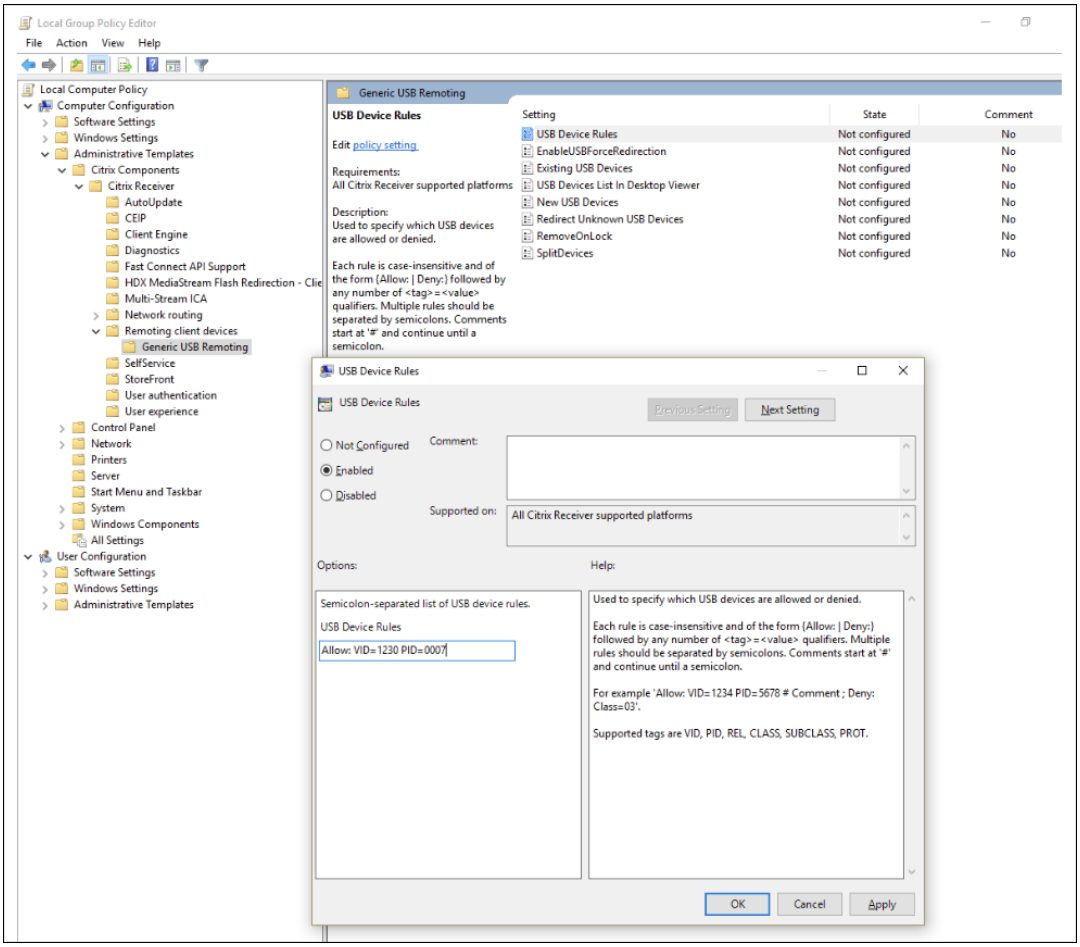
USB リダイレクト関連の問題をトリアージするには、次の手順を実行する必要があります:

1. USB リダイレクトのシステム要件が満たされていることを確認します。これには、検討中の OS プラットフォームに対して正しい Citrix Virtual Apps and Desktops および Citrix Workspace アプリのバージョン、サポートされているデバイス、デバイス ドライバーが含まれます。

2. 環境で使用されているコンポーネントのバージョンとプラットフォームに基づいて、構成が適切であることを確認します。レガシー構成設定を必要とするコンポーネントの詳細については、「レガシー USB リダイレクト構成」の注記を参照してください。
3. クライアントが列挙した一覧の下にデバイスが表示されていることを確認します。
    a) Workspace の基本設定ツールバー：［Workspace アプリの基本設定］ツールバーのデバイスタブに列挙されているデバイスを確認します（**Citrix Workspace** アプリアイコンを右クリックして［コネクションセンター］**>**［基本設定］…［デバイス］タブをクリックします）。
    b) `CtxUsbDiagnostics.exe`（推奨）：コマンドプロンプトウィンドウでこのツールを実行します。出力には、特定のセッションのデバイス固有の情報が表示されます。デバイスがリダイレクトされているかどうかがわかります。また、デバイス規則セットが原因でデバイスがリダイレクトされないかどうかも通知されます。詳しくは、「診断ツール」を参照してください。
    c) USBView またはその他のサードパーティツール：エンドポイント/クライアントマシンで USBView などのサードパーティツールを実行し、デバイスがエンドポイントで検出されることを確認します。
4. デバイスが列挙されている場合：
    a) 特定のデバイスの CtxUsbDiagnostics ツールの出力に Deny 規則が表示される場合は、Studio で構成されているポリシーを確認し、バージョン 2 ポリシーで規則が正しく設定されていることを確認します。Studio ポリシーに Deny 規則が表示されない場合は、クライアント側のポリシーを確認し、最後にクライアント側のデフォルト設定の順序で確認して、一致する Deny 規則を見つけます。
    b) CtxUsbDiagnostics の出力に Deny 規則がない場合、Citrix Workspace アプリは［基本設定］ウィンドウ（［デバイス］> ［デバイスの管理］）のデバイスタブで適切なボタンをチェック/クリックして、デバイスのリダイレクトを許可します。リダイレクトされたデバイスはセッションで使用できるようになります。これはデバイスマネージャー/USBView、または HDX セッション内の同様のアプリケーションで確認できます。
5. セッション内でデバイスが表示されない場合は、次の手順を実行します：
    a) VDA ホストに正しいデバイスドライバーが正しくインストールされていない可能性があります。最新バージョンのデバイスドライバーが VDA ホストに正しくインストールされていることを確認します。一部のデバイスドライバーはターミナルサーバーマシンではサポートされていないため、リダイレクトしようとしているデバイスがサポートされていることを確認してください。
    b) デバイスがクライアントエンドポイントで使用されていないことを確認します。一部のデバイスでは、クライアントエンドポイントにもドライバーをインストールする必要があり、これが原因でセッションでリダイレクトされなくなる可能性があります。
6. クライアントエンドポイントで USB 関連の規則が正しく設定されていることを確認します：
    a) **Windows** 向け **Citrix Workspace** アプリ：

i. クライアントのグループポリシー（これに関する詳細と SS を追加）が適切に設定されており、Studio で設定された規則と競合していないことを確認します。

ii. クライアントのレジストリ内のデフォルト規則を確認します。



(HKLM\SOFTWARE\Wow6432Node\Citrix\PortICA\GenericUSB\DeviceRules)are appropriately set and not in conflict with the rules set in Studio and client group policy.

b) Linux 向け Citrix Workspace アプリ - Linux 向け Citrix Workspace アプリの問題をトリアージするには、USB ドキュメントで「Linux 向け Citrix Workspace アプリ」を参照してください

c) Mac 向け Citrix Workspace アプリ - Mac 向け Citrix Workspace アプリの問題をトリアージするには、「Mac 向け Citrix Workspace アプリ」を参照してください

> 注:
>
> - TSVDA では、オーディオデバイスはデフォルトで USB リダイレクトの使用をブロックされます。これらのデバイスを使用するには、最適化された Audio VC を使用することをお勧めします。
> - 場合によっては、デバイスを分割するように正しいデバイスリダイレクト規則が設定されている場合で

> も、USB 複合デバイスが自動的に分割されないことがあります。この問題は、デバイスが省電力モードであるために発生します。このような場合、省電力モードになった子デバイスはデバイス一覧に存在しない可能性があります。この問題を解決するには、次の回避策を使用できます:
>
> - セッションを切断し、USB デバイスを挿入して、セッションに再接続します。
>
> - USB デバイスを取り外し、再度差し込みます。この操作により、デバイスの省電力モードが解除されます。
>
> • 場合によっては、バッテリー寿命を最適化するために、USB バッテリー節約設定が有効になっていることがあります。クライアントエンドポイントがスリープ状態になると、USB デバイスが切断される可能性があります。このようなシナリオでは、セッションでデバイスを再度表示する場合、デバイスを切断して再接続する必要がある場合があります。

イベントログ

管理者は、ユーザーがリダイレクトしようとする可能性のある不正なデバイスを監視し、適切なアクションを実行できるようになりました。以下は、リダイレクトが許可されているデバイスと許可されていないデバイスについて、VDA ホストのイベントビューアーに記録されるイベントメッセージの一部です。

Id	1000
Name	UsbEventAcceptDevice
Severity	Informational
Facility	System
Text	The Citrix USB Service allows the USB Device with Product ID: %2, Vendor ID: %3, and Device ID: %4 to be remoted.
Comment	This message logs the device info of a device redirected in an HDX session

Id	1001
Name	UsbEventPolicyRejectsDeviceV1
Severity	Warning
Facility	System
Text	The USB device with Product ID: 0x%2, Vendor ID: 0x%3, and Device ID: 0x%4 is not being redirected because the Citrix USB policy, "DENY: ...%5..." is in effect. If you wish to redirect the device, please set an allow rule that matches the device in the "Client USB device redirection rules" policy in Citrix Studio.
Comment	This message displays a message of the device not getting redirected if a DENY rule is being enforced by the legacy “Client USB device redirection rules” policy rule.
Arguments	

Id	1002
Name	UsbEventPolicyRejectsDeviceV2
Severity	Warning
Facility	System
Text	The USB device with Product ID: 0x%2, Vendor ID: 0x%3, and Device ID: 0x%4 is not being redirected because the Citrix USB policy, "DENY: ...%5..." is in effect. If you wish to redirect the device, please set an allow rule that matches the device in the "Client USB device redirection rules (Version 2)" policy in Citrix Studio.
Comment	This message displays a message of the device not getting redirected if a DENY rule is being enforced by the "Client USB device redirection rules (Version 2)" policy rule. For instance, if the studio policy rule allows an approved set of devices and denies all other devices and an end user tries to create a new rule on the client endpoint via group policy, this event will get logged. This message would be indicative of an unauthorized device redirection attempt.
Arguments	

USB 診断ツール

August 17, 2024

`CtxUsbDiagnostics.exe`は、Citrix 管理者が、クライアントで発生した USB デバイスのリダイレクトの問題を迅速に診断して解決するのに役立つ、VDA 上のコマンドラインツールです。このユーティリティツールは、クライアントに接続されている USB デバイスが HDX セッション内でリダイレクトに失敗することに関連した構成の問題をトリアージするために必要な、重要な情報を収集します。

```
> **Note :**
>
> Running Command Prompt or Powershell as an administrator is required to ensure the tool has the necessary permissions to perform system-level operations.
```


要件

セッションホスト

- オペレーティングシステム
  - Windows 10 1809 以降
  - Windows 11 21H2 以降
  - Windows Server 2016 以降
- VDA
  - Windows：Citrix Virtual Apps and Desktops バージョン 2311 以降

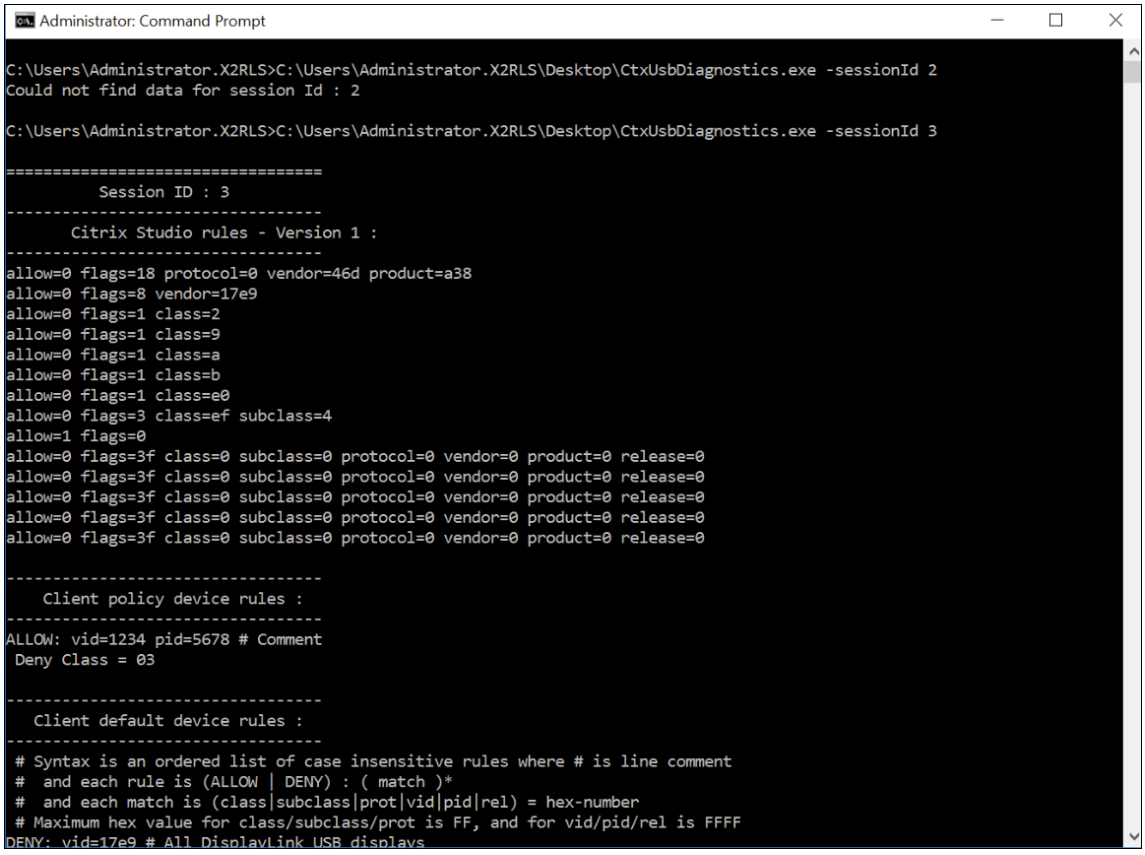
クライアントデバイス

- オペレーティングシステム
  - Windows 10 1809 以降
- Workspace アプリ
  - Windows：バージョン 2311 以降

このツールの概要

このツールは、現在以下を提供します：

- SessionID
- VDA デバイスポリシー（Studio で設定されたデバイス規則）
- クライアントデバイスとクライアントデバイスポリシー（デバイス規則）
- デバイスの一覧、そのリダイレクト状態、およびそれらが許可または拒否された理由



> 注
>
> :
>
> 管理者は、すべてのアクティブなセッションのデバイス情報を確認できます。

表示される情報

- **Citrix Studio** 規則 **-** バージョン **1/2**
  - DDC 規則は、Studio で従来の「クライアント **USB** デバイスリダイレクト規則」または「クライアント **USB** デバイスリダイレクト規則（バージョン **2**）」ポリシーを使用することを示します。このセクションに記載されている情報には、Citrix 管理者によって構成されたすべての規則が表示されています。

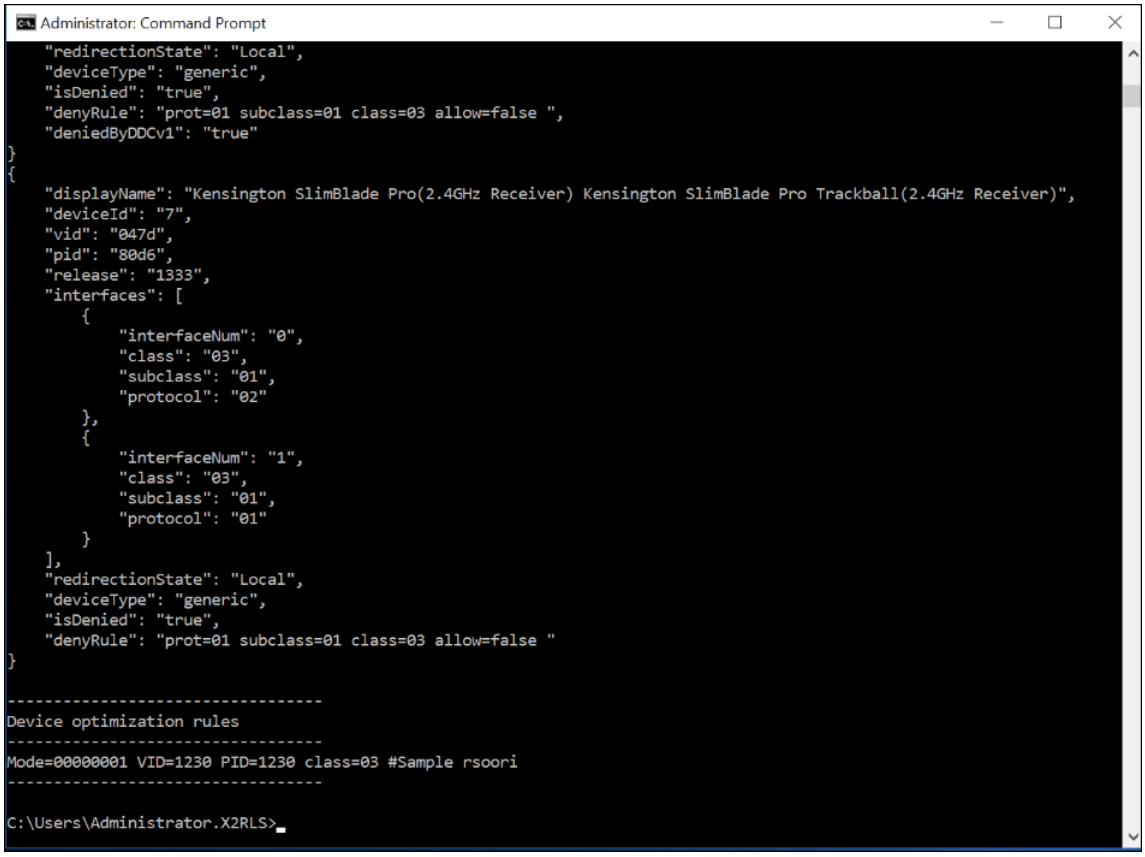

```
C:\Program Files\Citrix\HDX\bin>CtxUsbDiagnostics.exe

-----------------------------------
          Session ID : 1
-----------------------------------
       Citrix Studio rules - Version 2 :
-----------------------------------
DENY: vid=046D pid=0A38
# Block some devices we never want to see
DENY: vid=17e9 # All DisplayLink USB displays
```

- クライアントのデフォルトのデバイス規則
  - このセクションでは、クライアントのレジストリで設定されている規則を表示します。

```
---------------------------------
  Client default device rules :
---------------------------------
 # Syntax is an ordered list of case insensitive rules where # is line comment
 #  and each rule is (ALLOW | DENY) : ( match )*
 #  and each match is (class|subclass|prot|vid|pid|rel) = hex-number
 # Maximum hex value for class/subclass/prot is FF, and for vid/pid/rel is FFFF
DENY: vid=17e9 # All DisplayLink USB displays
CONNECT: vid=1188 pid=A101 # Bloomberg 5 Biometric module
DENY: vid=1188 pid=A001 split=01 intf=00 # Bloomberg 5 Primary keyboard
CONNECT: vid=1188 pid=A001 split=01 intf=01 # Bloomberg 5 Keyboard HID
DENY: vid=1188 pid=A301 split=01 intf=02 # Bloomberg 5 Keyboard Audio Channel
CONNECT: vid=1188 pid=A301 split=01 intf=00,01 # Bloomberg 5 Keyboard Audio HID
DENY: class=02 # Communications and CDC-Control
DENY: class=09 # Hub devices
DENY:vid=045e pid=079A # Microsoft Surface Pro 1 Touch Cover
DENY:vid=045e pid=079c # Microsoft Surface Pro 1 Type Cover
DENY:vid=045e pid=07dc # Microsoft Surface Pro 3 Type Cover
DENY:vid=045e pid=07dd # Microsoft Surface Pro JP 3 Type Cover
DENY:vid=045e pid=07de # Microsoft Surface Pro 3_2 Type Cover
DENY:vid=045e pid=07e2 # Microsoft Surface Pro 3 Type Cover
DENY:vid=045e pid=07e4 # Microsoft Surface Pro 4 Type Cover with fingerprint reader
DENY:vid=045e pid=07e8 # Microsoft Surface Pro 4_2 Type Cover
DENY:vid=03eb pid=8209 # Surface Pro Atmel maXTouch Digitizer
ALLOW:vid=056a pid=0315 class=03 # Wacom Intuos tablet
ALLOW:vid=056a pid=0314 class=03 # Wacom Intuos tablet
ALLOW:vid=056a pid=00fb class=03 # Wacom DTU tablet
DENY: class=03 subclass=01 prot=01 # HID Boot keyboards
DENY: class=03 subclass=01 prot=02 # HID Boot mice
DENY: class=0a # CDC-Data
DENY: class=0b # Smartcard
DENY: class=e0 # Wireless controller
DENY: class=ef subclass=04 # Miscellaneous network devices
ALLOW: # Otherwise allow everything else
```

- デバイス最適化規則
  - このセクションでは、「クライアント USB デバイス最適化規則」で設定されたデバイス最適化規則を一覧表示します。



デバイス一覧

このセクションには、クライアントエンドポイントに接続されている各デバイスの情報、ハードウェア情報、リダイレクトされているかどうか、正しいデバイスのリダイレクト規則が設定されているかどうかなどに関する重要な情報が表示されます。

タグ名	説明
displayName	デバイスの一般名を一覧表示します。
vid	ベンダー ID
pid	製品 ID
インターフェイス	このサブセクションでは、複合デバイスが複数の子デバイスに分割されている場合のすべてのインターフェイスを一覧表示します。
InterfaceNum	インターフェイス記述子のインデックスを示します
class	クラスコード
subclass	サブクラスコード

タグ名	説明
プロトコル	プロトコル
redirectionState	**Local** は、デバイスが ICA セッションでリダイレクトされないことを示します。**ThisSession** は、デバイスが ICA セッションでリダイレクトされることを示します。**OtherSession** は、デバイスが別の ICA セッションでリダイレクトされることを示します。
optiEnabled	**true** は、デバイスが最適化されていることを示します。**false** は、デバイスが最適化されておらず、データ転送は USB 仮想チャネル経由で行われることを示します。
deviceType	**generic** は、デバイスに最適化された仮想チャネルがなく、トラフィックフローが USB 仮想チャネルを経由していることを示します。**optimized** は、デバイスに関連付けられたデータ転送が専用の仮想チャネル上で行われることを意味します。
isDenied	**true** は、管理者が設定したポリシー規則によりデバイスがリダイレクトされないことを示します。`false`は、適用されたポリシーによりデバイスがリダイレクトされることを示します。
denyRule	このフィールドは、**isDenied** が`true`に設定されている場合に役立ちます。これにより、デバイスがリダイレクトされなくなる原因のポリシーに設定された特定の規則が、管理者に通知されます。

レガシー **USB** リダイレクト構成

August 17, 2024

バージョン 2212 より古いコンポーネントを使用している場合、または Linux 向け Citrix Workspace アプリを使用している場合は、このガイドに従って、環境で USB リダイレクトを構成してください。

汎用 **USB** リダイレクトの有効化

1. **Citrix Web Studio** ポリシーを開き、［ポリシー］タブをクリックします。

2. ［ポリシーの作成］をクリックし、［**ICA**］**>**［**USB Devices policies**］を展開します。
3. クライアント **USB** デバイスリダイレクトポリシーを編集します。
4. ［許可］を選択し、［保存］をクリックします。

USB リダイレクトポリシー規則の作成

ユーザーが USB デバイスを仮想デスクトップにリダイレクトしようとすると、一致するものが見つかるまで各 USB ポリシー規則に対して順番にチェックされます。どのデバイスでも、最初に一致したものが最終的な一致と見なされます。最初の一致が Allow 規則である場合、一致したデバイスは仮想デスクトップにリダイレクトされることが許可されます。最初の一致が Deny 規則の場合、一致したデバイスはローカルデスクトップでのみ使用可能になります。一致する規則がない場合、デフォルトの規則が使用されます。

DDC のポリシーの設定:

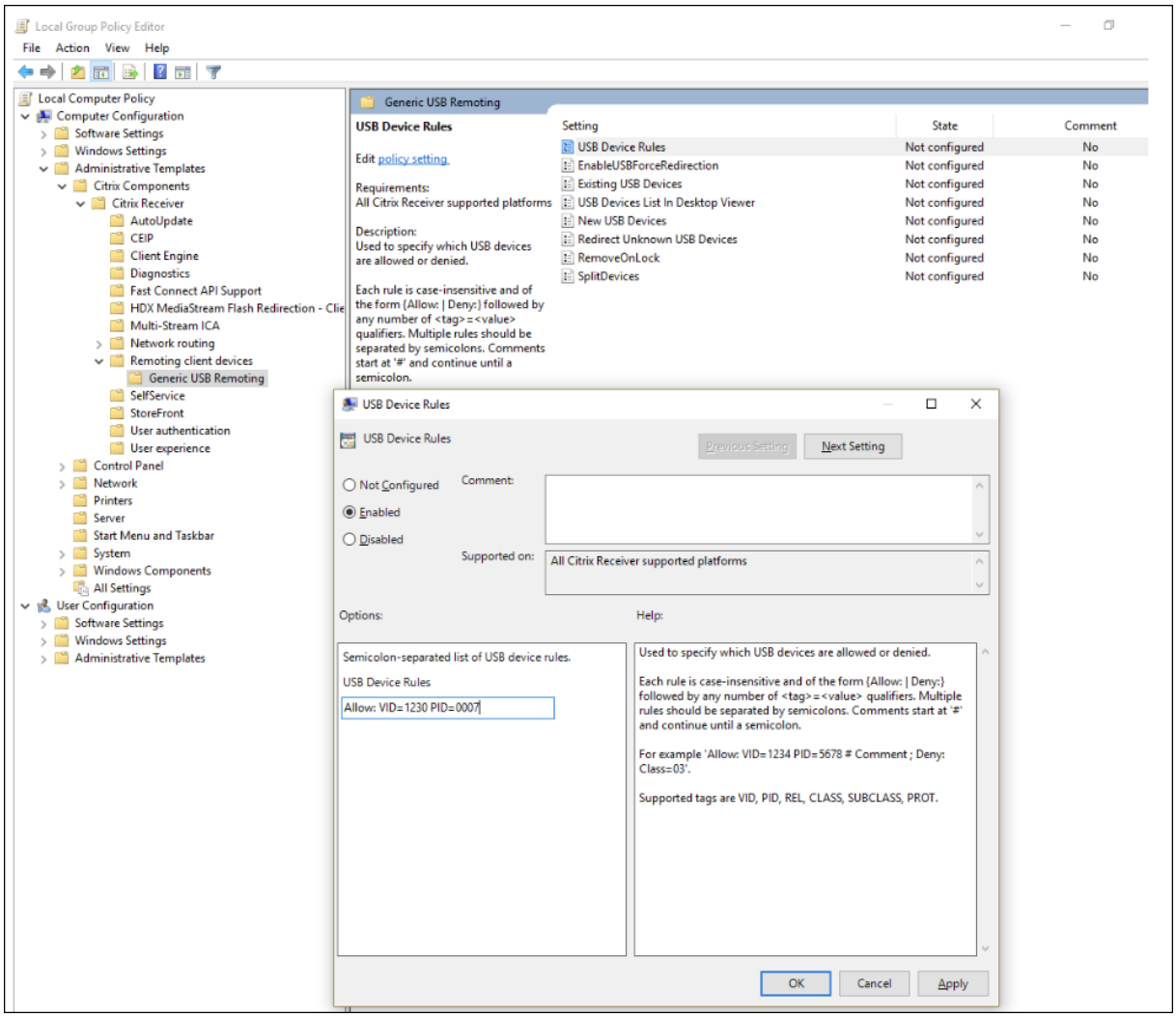
1. **Citrix Web Studio** ポリシーを開き、［ポリシー］タブをクリックします。
2. ［ポリシーの作成］をクリックし、［**ICA**］**>**［**USB Devices policies**］を展開します。
3. クライアント **USB** デバイスのリダイレクト規則を編集します。
4. リダイレクトする必要がある各 USB デバイスの説明に記載されている例に基づいて値を設定し、［保存］をクリックします。
   例:
   Allow: VID=056A PID=00A4 #STU-430
   Deny: Class=08 subclass=05 # 大容量記憶装置

   > 注:
   >
   > Citrix 管理者が［デフォルト値を使用する］をチェックし、［保存］をクリックすると、デフォルトの規則は VDA の次のレジストリで見つかります。
   >
   > 注意
   >
   > レジストリエディターを使用する前に、この記事の最後に記載されている免責事項を参照してください。
   > `HKLM\SOFTWARE\Wow6432Node\Citrix\PortICA\GenericUSB\DeviceRules`

クライアントで **GPO** を使用する:

1. ローカルグループポリシーエディターを開き、［管理用テンプレート］**>**［**Citrix** コンポーネント］**>**［**Citrix Receiver**］**>**［クライアントデバイスをリモート処理します］**>**［一般的な **USB** のリモート処理］の順に選択します。
2. **USB** デバイス規則設定を開き、設定を有効にします。この例のように USB デバイス規則を追加します。
   「Allow: VID=1230 PID=0007」規則により、Vendor ID 1230 および Product ID 0007 のデバイスが許可されます。

> 注:
>
> 特定のデバイスをデバイス規則一覧の一番上にする必要がある場合、「Allow: VID=xxxx PID=xxxx」規則を使用します。



> 注:
>
> USBView などのツールや接続ツールバーを使用して、VID や PID（ここでは SS を含める）などのデバイスの詳細を確認できます。

USB デバイスの自動リダイレクトを構成する

USB サポート機能が有効になっており、USB 関連のユーザー設定で USB デバイスに自動接続するように設定されている場合は、USB デバイスが自動的にリダイレクトされます。一部の USB デバイスはリダイレクトしない方が良い場合もあります。ユーザーは、USB デバイスリストから、自動的にリダイレクトされないデバイスを明示的にリダ

イレクトすることができます。USB デバイスのリスト表示とリダイレクトを禁止するには、クライアントエンドポイントまたは Desktop Delivery Controller ポリシーで DeviceRules を適用します。

このポリシーは、DDC、GPO を使用するクライアント、Citrix Workspace 環境設定、または CDViewer の［接続］タブを使用して設定できます。これらすべての方法について以下に説明します：

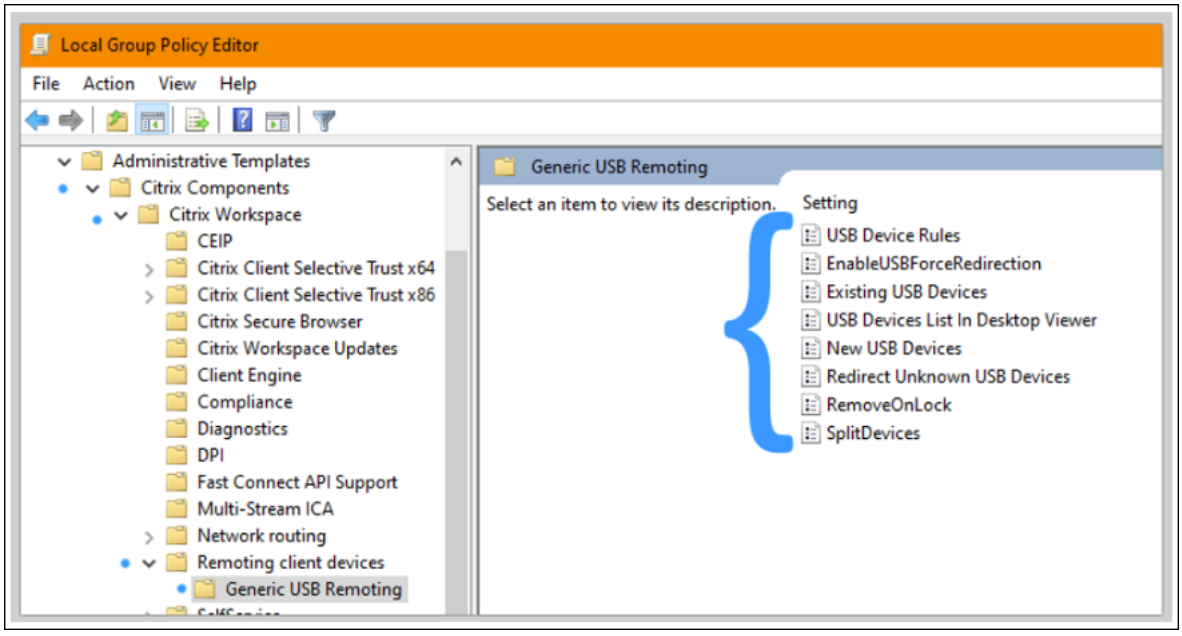
DDC のポリシーの設定：

DDC には、USB デバイスの自動リダイレクトを許可するために設定できるポリシーが 2 つあります。「既存の USB デバイスの自動接続を許可する」と「新しく受信した USB デバイスの自動接続を許可する」です

1. **Citrix Web Studio** ポリシーを開き、［ポリシー］タブをクリックします。
2. ［ポリシーの作成］をクリックし、［**ICA**］**>** ［**USB Devices policies**］を展開します。
3. 既存の **USB** デバイスの自動接続を許可する設定を編集します。
4. ［デフォルト値を使用する］チェックボックスをオフにし、ドロップダウンメニューから ［使用可能な **USB** デバイスを自動的にリダイレクトする］を選択して ［保存］をクリックします。
5. 新しく受信した **USB** デバイスの自動接続を許可する設定を編集します。
6. ［デフォルト値を使用する］チェックボックスをオフにし、ドロップダウンメニューから ［使用可能な **USB** デバイスを自動的にリダイレクトする］を選択して ［保存］をクリックします。

クライアントで **GPO** を使用する：

1. ローカルグループポリシーエディターを開き、［管理用テンプレート］**>** ［**Citrix** コンポーネント］**>** ［**Citrix Receiver**］**>** ［クライアントデバイスをリモート処理します］**>** ［一般的な **USB** のリモート処理］の順に選択します。
2. ［新しい **USB** デバイス］を開いて ［有効］を選択し、［**OK**］をクリックします。
3. ［既存の **USB** デバイス］を開いて ［有効］を選択し、［**OK**］をクリックします。



Citrix コネクションセンターを使用する：

1. [**Citrix Workspace** の基本設定] > [接続] に移動します。
2. 次のオプションを選択します:

    a) セッションの開始時に、デバイスを自動的に接続します
    b) セッションの実行中に新しいデバイスが接続されると、自動的にデバイスに接続します

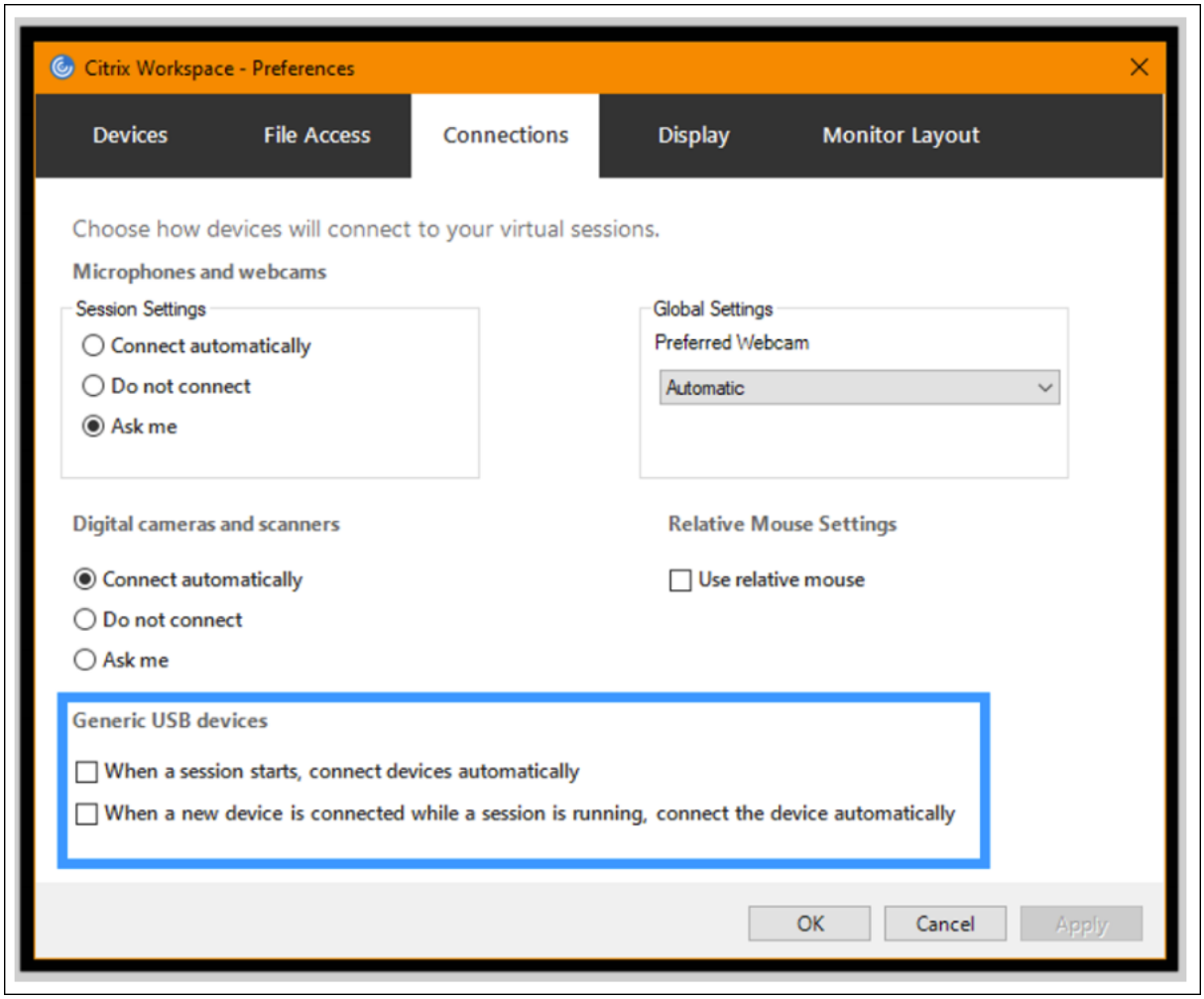
3. [**OK**] をクリックします。

CDViewer の **Connection** の接続ツールバーを使用する:

1. セッションが開始したら、**CDViewer** ドロップダウンをクリックし、[**Citrix Workspace** の基本設定] > [接続] タブを選択します。
2. 次のオプションを選択します:

    a) セッションの開始時に、デバイスを自動的に接続します
    b) セッションの実行中に新しいデバイスが接続されると、自動的にデバイスに接続します

3. [適用] および [**OK**] をクリックしてポリシーを保存します。



クライアント ベースの構成の場合、レジストリキーはクライアントデバイスの次の場所に設定されます:

> 注意
>
> レジストリエディターを使用する前に、この記事の最後に記載されている免責事項を参照してください。
> `HKLM\SOFTWARE\Wow6432Node\Citrix\ICA Client\GenericUSB`

クライアントドライブマッピング（**CDM**）

August 17, 2024

クライアントドライブマッピングは、クライアントエンドポイントのストレージドライブを Citrix HDX セッション内で利用できるようにすることで、ファイルやフォルダーをクライアントからセッションホストに、またはその逆方向に転送できるようになります。この機能はデフォルトで読み取り権限と書き込み権限の両方で有効になっています。マップされたクライアント側デバイス上でのフォルダーおよびファイルの追加や変更を禁止するには、［クライアント側ドライブへの読み取り専用アクセス］設定を有効にします。この設定項目をポリシーに追加するときは、［クライアントドライブのリダイレクト］設定も追加されており、［許可］が選択されていることを確認してください。

セキュリティ上の予防措置として、デフォルトでは、エンドポイントドライブは実行権限なしでマップされます。マップされたクライアントドライブから実行可能ファイルをユーザーが直接実行できるようにするには、セッションホストの **ExecuteFromMappedDrive** レジストリ値を編集します。詳しくは、「レジストリを介して管理される機能」にある「マップされたクライアントドライブ」を参照してください。

要件

CDM を使用するための要件は以下のとおりです。

Citrix コントロールプレーン

- Citrix Virtual Apps and Desktops 1912 以降
- Citrix DaaS

セッションホスト

- オペレーティングシステム
  - Windows 10 1809 以降
  - Windows Server 2016 以降
  - Linux：Linux Virtual Delivery Agent の「システム要件」を参照してください。
- VDA

  - Windows：Citrix Virtual Apps and Desktops 1912 以降
  - Linux：Linux Virtual Delivery Agent のドキュメントを参照してください。

クライアントデバイス

- オペレーティングシステム
  - Windows 10 1809 以降
  - Linux：Linux のシステム要件については、Workspace アプリを参照してください。

関連ポリシー

CDM の設定については、「ポリシー設定リファレンス」セクションを参照してください。

ダブルホップのシナリオ

CDM はダブルホップのシナリオでサポートされます。デフォルトでは、クライアントエンドポイントのドライブは 2 番目のホップセッションにマップされ、最初のホップのドライブは使用できません。ただし、これは、クライアントエンドポイントのドライブでなく最初のホップのドライブが 2 番目のホップのセッションにマップされるように設定することもできます。

この機能を構成するには、次のレジストリ値を編集します。

- キー：HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ICA Client\Engine\Configuration\Advanced
- 値の名前：NativeDriveMapping
- 値の種類：REG_SZ
- 値のデータ：
  - True - 最初のホップセッションのドライブを 2 番目のホップセッションにマッピングします。
  - False - クライアント エンドポイントのドライブを 2 番目のホップセッションにマッピングします。

> 注：
>
> レジストリエディターの使用を誤ると、深刻な問題が発生する可能性があり、オペレーティングシステムの再インストールが必要になる場合もあります。レジストリエディターの誤用による障害に対して、Citrix では一切責任を負いません。レジストリエディターは、お客様の責任と判断の範囲でご使用ください。また、レジストリファイルのバックアップを作成してから、レジストリを編集してください。

モバイルおよびタッチスクリーンクライアントデバイスのサポート

August 17, 2024

Citrix Virtual Apps and Desktops を使用すると、ユーザーはモバイルデバイスやタッチスクリーンクライアントデバイスから公開アプリケーションやデスクトップにアクセスできます。

要件

Citrix コントロールプレーン

- Citrix Virtual Apps and Desktops 1912 以降
- Citrix DaaS

セッションホスト

- オペレーティングシステム
  - Windows 10 1903 以降
  - Windows 11 21H2 以降
- VDA
  - Windows：Citrix Virtual Apps and Desktops バージョン 7.15 以降

クライアントデバイス

- オペレーティングシステム
  - Windows 10 1809 以降
  - Windows 11 21H2 以降
- Windows 向け Citrix Workspace アプリバージョン 1808 以降

Windows Continuum を使用したタッチスクリーンデバイス用タブレットモード

Continuum は、クライアントデバイスの使用方法に対応する Windows 10 の機能です。VDA がタッチ対応クライアントのキーボードまたはマウスの存在を検出すると、クライアントをデスクトップモードにします。キーボードまたはマウスが存在しない場合、VDA はクライアントをタブレット/モバイルモードにします。この検出は、セッションの接続時と再接続時に行われます。また、セッション中にキーボードまたはマウスが接続または切断されたときにも行われます。

この機能はデフォルトで有効にされています。この機能を無効にするには、ポリシー設定で ［タブレットモードの切り替え］ を構成します。

上記のタッチスクリーンデバイスの要件に加えて、Windows Continuum では次の要件があります:

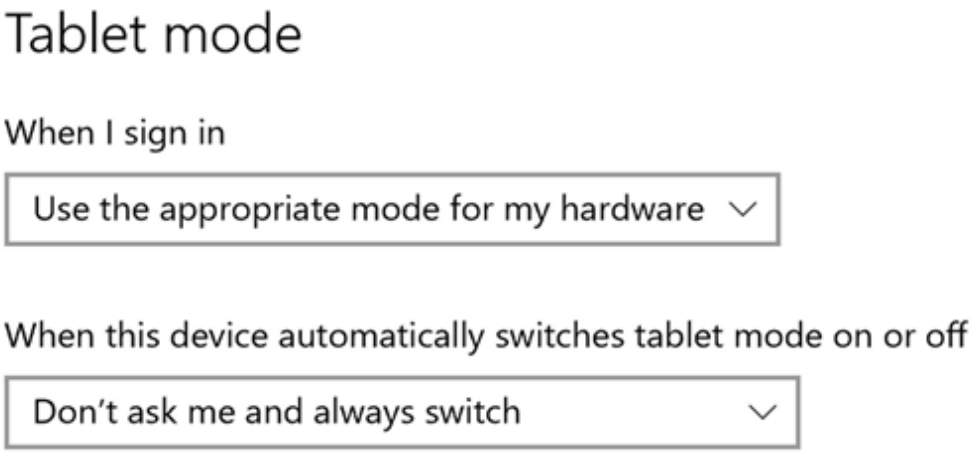
XenServer（旧称 **Citrix Hypervisor**）

- Citrix Hypervisor 8.2 以降
- ノートブック/タブレットの切り替えを許可するには、XenServer CLI コマンドを実行します:
  xe vm-param-set uuid=<VM_UUID> platform:acpi_laptop_slate=1

> 重要:
>
> メタデータ設定を変更した後で既存のマシンカタログの基本イメージを更新しても、以前にプロビジョニングされた VM には影響しません。XenServer VM の基本イメージを変更した後、カタログを作成し、基本イメージを選択し、新しい MCS（Machine Creation Services）マシンをプロビジョニングします。

セッションホスト

- オペレーティングシステム
  - Windows 10 1903 以降
  - Windows 11 21H2 以降
- VDA
  - Windows: バージョン 7.16 以降
  - オペレーティング システム構成の現在の制限により、ユーザーは最初の **ICA** セッションを開始して **VDA** を再起動した後、ドロップダウンメニューから次のオプションを設定する必要があります:
    * ［設定］ **>** ［システム］ **>** ［タブレットモード］
      - ハードウェアに適切なモードを使用する
      - 確認なしで常に切り替える



タブレットモードでは、タッチスクリーンにより適した以下のユーザーインターフェイスが提供されます:

- やや大きめのボタン
- スタート画面や開始したアプリケーションを全画面で開く
- タスクバーに［戻る］ボタンを表示
- タスクバーからアイコンを削除

File Explorer にアクセスできます。

Windows 10 は、この更新された BIOS を基にターゲット仮想マシンに GPIO ドライバーをロードします。これは、仮想マシン内でタブレットモードとデスクトップモードを切り替えるのに使用されます。

HTML5 向け Citrix Workspace アプリは、Windows Continuum 機能をサポートしていません。

デスクトップモードでは、PC とキーボードとマウスを使用するのと同じ方法で対話する従来のユーザーインターフェイスが提供されます。

Microsoft Surface Pro および **Surface Book** のペン

Windows Ink を使用するアプリケーションで標準のペン機能をサポートします。サポートされるペン機能には、ポインティング、消去、筆圧、Bluetooth 信号、オペレーティングシステムのファームウェアやペンモデルによって異なるその他の機能が含まれます。たとえば、筆圧は最大 4096 レベルまで可能です。この機能はデフォルトで有効になっています。

ペン機能のサポートの要件は次のとおりです:

Citrix コントロールプレーン

- Citrix Virtual Apps and Desktops 1903 以降
- Citrix DaaS

セッションホスト

- オペレーティングシステム
  - Windows 10 1809 以降
  - Windows 11 21H2 以降
- VDA
  - Windows：Citrix Virtual Apps and Desktops 1903 以降

クライアントデバイス

- オペレーティングシステム
  - Windows 10 1809 以降
  - Windows 11 21H2 以降
- Windows 向け Citrix Workspace アプリバージョン 1902 以降

Windows Ink とペン機能のデモを見るには、以下の画像をクリックしてください：

この機能を無効または有効にするには、レジストリを介して管理される機能の一覧にある「Microsoft Surface Pro および Surface Book のペン」を参照してください。

既知の問題

ペン機能のサポートに関する既知の問題は次のとおりです：

- Windows Server 2k22 の OS の制限により、2k22 サーバーまたはデスクトップに接続している場合、ユーザーは［コントロールパネル］でペンのショートカットを設定したり、ペン/Ink の設定に調整を加えたりすることができません。
- OS の制限のため、ペン機能に対応した Windows 11 クライアントでペンのショートカットが機能しません。

シリアルポート

August 17, 2024

ほとんどの新しい PC には、シリアル（COM）ポートは内蔵されていません。シリアルポートは USB コンバーターを使用して簡単に追加できます。シリアルポートに適したアプリケーションには、センサー、コントローラー、旧式のチェックリーダー、パッドなどがあります。一部の USB 仮想 COM ポートデバイスでは、Windows 提供のドライバー（usbser.sys）の代わりにベンダー固有のドライバーが使用されます。これらのドライバーを使用すると、USB デバイスの仮想 COM ポートを別の USB ソケットに接続しても変更されないように強制することができます。これは、［デバイスマネージャー］**>**［ポート（**COM** & **LPT**）］**>**［プロパティ］から、またはデバイスを制御するアプリケーションから設定できます。

クライアント側 COM ポートのマッピングを使用すると、ユーザーのエンドポイント上の COM ポートに接続されているデバイスを仮想セッション中に使用できるようになります。これらのマッピングは他のネットワークマッピングと同様に使用できます。

各 COM ポートには、オペレーティングシステムのドライバーによって COM1 や COM2 などのシンボリックリンク名が割り当てられます。アプリケーションはそのリンクを使用してポートにアクセスします。

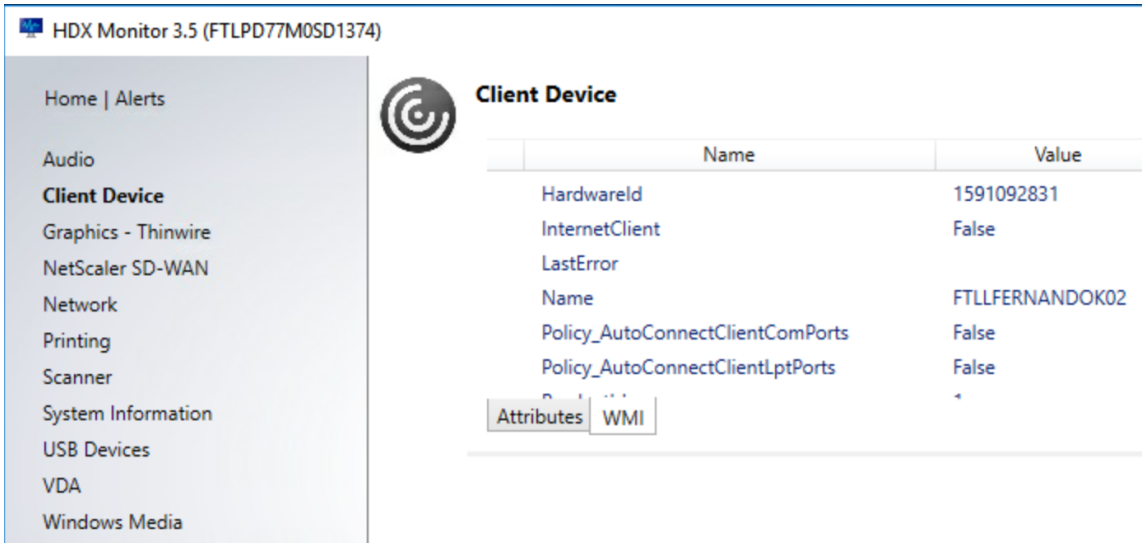
> 重要:
>
> デバイスは USB を直接使用してエンドポイントに接続できるため、汎用 USB リダイレクトを使用してデバイスをリダイレクトすることはできません。一部の USB デバイスは仮想 COM ポートとして機能し、アプリケーションは物理シリアルポートと同じ方法でそのポートにアクセスできます。オペレーティングシステムは、COM ポートを抽象化して、ファイル共有のように扱うことができます。仮想 COM でよく使用されるプロトコルは CDC ACM と MCT の 2 つです。RS-485 ポート経由で接続すると、アプリケーションがまったく機能しないことがあります。RS-485 を COM ポートとして使用するには、RS-485-to-RS232 コンバーターを入手してください。
>
> 重要:
>
> 一部のアプリケーションは、デバイス（たとえば、署名パッド）がクライアントワークステーションの COM1 または COM2 に接続されている場合に限り、そのデバイスを一貫して認識します。

クライアント **COM** ポートをサーバーの **COM** ポートにマップする

クライアントの COM ポートを Citrix セッションにマップするには、次の 3 つの方法があります。

- Studio ポリシー。ポリシーについて詳しくは、「ポートリダイレクトのポリシー設定」を参照してください。
- VDA コマンドプロンプト。
- リモートデスクトップ（ターミナルサービス）構成ツール。

1. ［クライアント **COM** ポートリダイレクト］と ［クライアント **COM** ポートを自動接続する］の Studio ポリシーを有効にします。適用すると、一部の情報が HDX Monitor で利用可能になります。



2. ［クライアント **COM** ポートを自動接続する］でポートのマッピングに失敗した場合は、そのポートを手動でマップするか、またはログオンスクリプトを使用します。VDA にログオンし、コマンドプロンプトウィンドウで次のように入力します:

   NET USE COMX: \\CLIENT\COMZ:

   または

   NET USE COMX: \\CLIENT\CLIENTPORT:COMZ:

   < X > は VDA 上の COM ポートの番号です（マッピングに使用できるのはポート 1～9 です）。**< Z >** は、マップするクライアント COM ポートの番号です。

   その操作が成功したことを確認するには、VDA コマンドプロンプトで **NET USE** と入力します。マップされているドライブ、LPT ポート、およびマップされている COM ポートの一覧が表示されます。

```
C:\Windows\system32>net use
New connections will be remembered.


Status       Local     Remote                    Network

-------------------------------------------------------------------------------
             COM3      \\Client\COM3:            Citrix Client Network
```

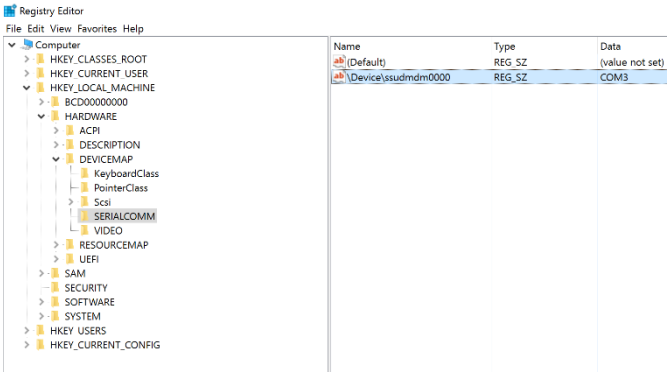
3. その COM ポートを仮想デスクトップやアプリケーションで使用するには、ユーザーデバイスアプリケーションをインストールし、マップされている COM ポート名を指すようにします。たとえば、クライアントの

COM1 をサーバーの COM3 にマップしている場合は、COM ポートデバイスアプリケーションを VDA にインストールし、セッション中に COM3 を指すようにします。この方法でマップした COM ポートは、ユーザーデバイスの COM ポートと同じように使用できます。

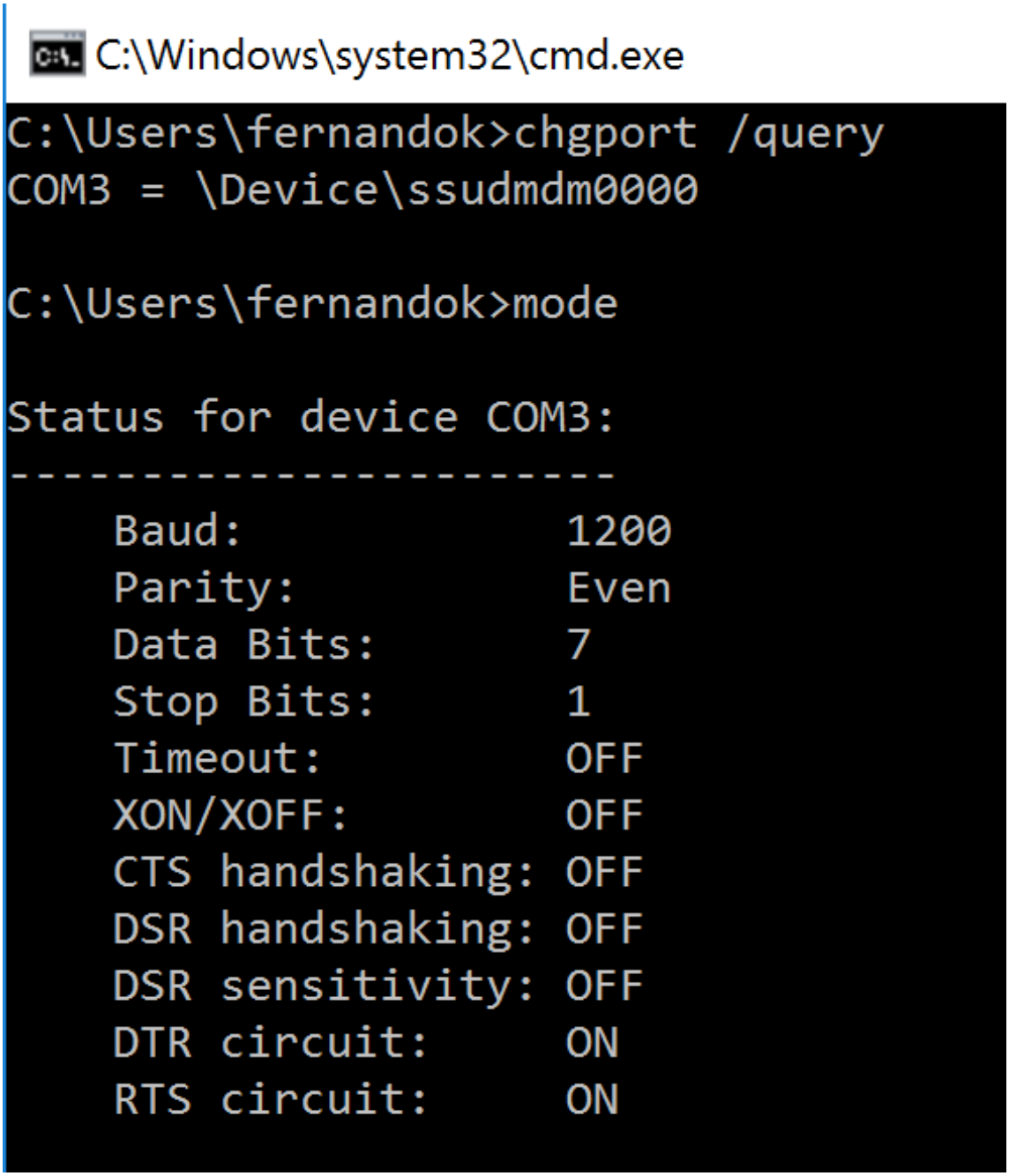
> 重要:
>
> COM ポートマッピングは TAPI 対応ではありません。Windows テレフォニーアプリケーションプログラミングインターフェイス（TAPI）デバイスをクライアント COM ポートにマップすることはできません。TAPI は、アプリケーションがデータ、ファックス、および音声通話のテレフォニー機能を制御するための標準的な方法を定義します。TAPI は、ダイヤル、応答、通話終了などのシグナリングを管理します。また、保留、転送、会議通話などの付加的サービスも管理します。

トラブルシューティング

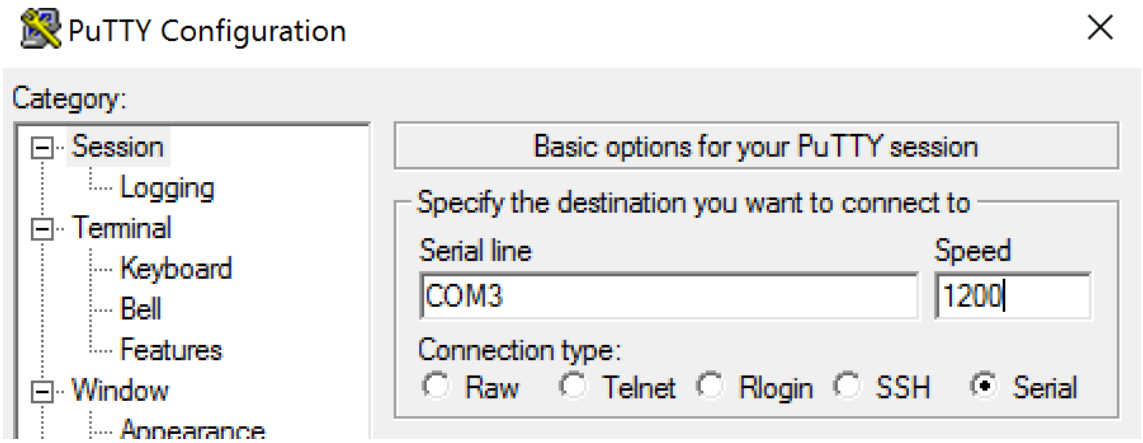
1. Citrix をバイパスしてエンドポイントからデバイスに直接アクセスできることを確認します。ポートが VDA にマップされていない間は、Citrix セッションに接続していません。デバイスに付属しているトラブルシューティングの指示に従って、まずデバイスがローカルに動作することを確認します。
   デバイスがシリアル COM ポートに接続されている場合は、次のハイブにレジストリキーが作成されています:



   この情報は、コマンドプロンプトで **chgport /query** を実行して確認することもできます。



デバイスのトラブルシューティングの手順を利用できない場合は、PuTTY セッションを開いてみます。［セッション］を選択し、［シリアル回線］で COM ポートを指定します。



ローカルのコマンドウィンドウで **MODE** コマンドを実行すると、その出力に、使用中の COM ポート、および PuTTY セッションで必要なボーレート/パリティ/データビット/ストップビットの情報が表示されます。PuTTY 接続に成功した場合は、**Enter** キーを押すとデバイスからのフィードバックが表示されます。入力した文字が画面上で繰り返されるか、または応答が返されます。この手順が正常に行われない場合、仮想セッションからデバイスにアクセスすることはできません。

2. ローカル COM ポートを VDA にマップし（ポリシーまたは **NET USE COM< X >: \\CLIENT\COM< Z >** を使用）、今回は VDA PuTTY から、前と同じ PuTTY 手順を繰り返します。PuTTY が「**Unable to open connection to COM1. Unable to open serial port**」というエラーで失敗する場合は、別のデバイスが COM1 を使用している可能性があります。

3. **chgport /query** を実行します。VDA 上の Windows の組み込みシリアルドライバーによって、VDA の COM1 ポートに\Device\Serial0 が自動的に割り当てられている場合は、次のようにします：
   A. VDA でコマンドウィンドウを開いて、次のコマンドを入力します：**NET USE**

   B. VDA の既存のマッピング（たとえば、COM1）を削除します。

   NET USE COM1 /DELETE

   C. そのデバイスを VDA にマップします。

   NET USE COM1: \\CLIENT\COM3:

   D. VDA 上のアプリケーションが COM3 を指すようにします。

   最後に、ローカル COM ポート（COM3 など）を VDA の別の COM ポート（COM1 以外の COM3 など）にマップしてみます。アプリケーションがそのポートを指すようにします：
   NET USE COM3: \\CLIENT\COM3

4. この時点でポートがマップされていることを確認できた場合、PuTTY は動作していますがデータは渡されていないため、競合状態である可能性があります。ポートがマップされる前にアプリケーションがそのポートに接続して開き、ロックしているためにマップできない可能性があります。次のいずれかを試してみます。

   - 同じサーバーで公開されている別のアプリケーションを開きます。ポートがマップされるまで数秒待ってから、そのポートを使用しようとする実際のアプリケーションを開きます。

- Studio ではなく Active Directory のグループポリシーエディターから、COM ポートリダイレクトポリシーを有効にします。有効にするポリシーは、［クライアント **COM** ポートリダイレクト］と ［クライアント **COM** ポートを自動接続する］です。この方法で適用されるポリシーは、Studio ポリシーより前に処理され、COM ポートがマップされることが保証される可能性があります。Citrix ポリシーは VDA にプッシュされ、次の場所に格納されています。
  `HKLN\SOFTWARE\Policies\Citrix \<user session ID\>`
- このログオンスクリプトをユーザーに対して使用するか、またはアプリケーションを公開する代わりに使用して、VDA の任意のマッピングを削除した後に仮想 COM ポートを再マッピングしてから、そのアプリケーションを起動する.bat スクリプトを公開します。

```
@echo off
NET USE COM1 /delete
NET USE COM2 /delete
NET USE COM1: \\CLIENT\COM1:
NET USE COM2: \\CLIENT\COM2:
MODE COM1: BAUD=1200（など必要な値なら何でも）
MODE COM2: BAUD=9600 PARITY=N Data=8 Stop=1（など必要な値なら何でも）
START C:\Program Files\< ソフトウェアのパス >\\< ソフトウェアの.exe ファイル > ソフトウェアの.exe ファイル > ソフトウェアのパス >
```

5. 最後の手段としては、Sysinternals の Process Monitor があります。VDA でこのツールを実行するときは、COM3、picaser.sys、CdmRedirector など（特に、<your_app>.exe）のオブジェクトを検索してフィルタリングします。「アクセスが拒否されました」などのエラーが表示されることがあります。

特殊キーボード

August 17, 2024

Bloomberg キーボード

> 警告:
>
> レジストリエディターの使用を誤ると、深刻な問題が発生する可能性があり、オペレーティングシステムの再インストールが必要になる場合もあります。レジストリエディターの誤用による障害に対して、Citrix では一切責任を負いません。レジストリエディターは、お客様の責任と判断の範囲でご使用ください。また、レジストリファイルのバックアップを作成してから、レジストリを編集してください。

Citrix Virtual Apps and Desktops では、Bloomberg のモデル 5、モデル 4 の Starboard キーボード（およびそれ以前のモデル 3）がサポートされています。このキーボードを使用すると、金融分野の顧客は、キーボードの特殊機能を使用して金融市場データにアクセスし、取引を迅速に実行できます。

> 重要:
>
> Bloomberg キーボードは 1 つのセッションのみで使用することをお勧めします。複数の同時セッション（1 つのクライアントからのマルチセッション）でこのキーボードを使用することはお勧めしません。

Bloomberg キーボードは、1 つの物理シェル内に次の複数の USB デバイスを備える、USB 複合デバイスです:

- キーボード。
- 指紋リーダー。
- 音量を増減するためのキーおよびスピーカーとマイクをミュートするためのキーが付いているオーディオデバイス。このデバイスには、オンボードスピーカー、マイク、およびマイクとヘッドセット用のジャックが備わっています。
- これらのすべてのデバイスをシステムに接続するための USB ハブ。

要件:

- Windows 向け Citrix Workspace アプリが接続するセッションで、USB デバイスがサポートされている必要があります。
- Bloomberg キーボードモデル 5 は、Linux 向け Citrix Workspace アプリ 2207 以降でサポートされています。
- Bloomberg キーボードモデル 5 は、Windows 向け Citrix Workspace アプリ 2109 以降でサポートされています。
- Bloomberg キーボードモデル 3 および 4 は、Windows 向け Citrix Workspace アプリ 1808 以降および Citrix Receiver for Windows 4.8 以降でサポートされています。
- モデル 4 の KVM モード（USB ケーブル 2 本、1 本は KVM 経由）を使用するには、Windows 向け Citrix Workspace アプリ 1808 以降または Citrix Receiver for Windows 4.12 以降が必要です。

Windows 向け Citrix Workspace アプリでの Bloomberg キーボードの構成について詳しくは、「Bloomberg キーボードの構成」を参照してください。

Bloogberg キーボードのサポートを有効にするには、レジストリを介して管理される機能の一覧にある「Bloomberg キーボード」を参照してください。

サポートを確認する:

Bloomberg キーボードのサポートが Citrix Workspace アプリで有効になっているかどうかを確認するには、Desktop Viewer で Bloomberg キーボードのデバイスが正しく報告されているかどうかを確認します。

デスクトップの場合:

Desktop Viewer を開きます。Bloomberg キーボードのサポートが有効になっている場合は、Desktop Viewer で USB アイコンの下に次の 3 つのデバイスが表示されています:

Bloomberg 5 キーボードの場合:

- Bloomberg LP Bloomberg Biometric Module

- Bloomberg LP Keyboard（2 つのインターフェイスを備えた複合デバイス）
- Bloomberg LP Keyboard Audio（3 つのインターフェイスを備えた複合デバイス）

Bloomberg 3 および 4 キーボードの場合：

- Bloomberg Fingerprint Scanner
- Bloomberg Keyboard Features
- Bloomberg LP Keyboard 2013

シームレスアプリケーションのみの場合：

Citrix Workspace アプリの通知領域アイコンから ［コネクションセンター］メニューを開きます。Bloomberg キーボードのサポートが有効になっている場合は、［デバイス］メニューに 3 つのデバイスが表示されています。

各デバイスに付いているチェックマークは、そのデバイスがそのセッションでリモートであることを示しています。

Web カメラ

August 17, 2024

高品位 Web カメラストリーミング

Web カメラは、仮想セッション内で実行されているビデオ会議アプリケーションで使用できます。サーバーのアプリケーションは、サポートされている形式の種類に基づいて Web カメラの形式と解像度を選択します。セッションが開始されると、クライアントは Web カメラ情報をサーバーに送信します。ビデオ会議アプリケーションから Web カメラを選択します。Web カメラとアプリケーションがどちらも高品位レンダリングをサポートする場合、アプリケーションは高品位解像度を使用します。1920x1080 までの Web カメラ解像度がサポートされています。

この機能を使用するには、Citrix Receiver for Windows の最小バージョン 4.10 が必要です。HDX Web カメラリダイレクトをサポートする Citrix Workspace アプリプラットフォームの一覧については、「Citrix Workspace アプリの機能マトリックス」を参照してください。

高品位 Web カメラでのストリーミングについて詳しくは、「HDX ビデオ会議と Web カメラビデオ圧縮」を参照してください。

レジストリキーを使用してこの機能を無効または有効にすることで、特定の解像度を設定することができます。詳しくは、レジストリを介して管理される機能の一覧にある「高品位 Web カメラストリーミングと高品位 Web カメラ解像度」を参照してください。

グラフィック

August 17, 2024

Citrix HDX グラフィックは広範囲な一連のグラフィックアクセラレーションと、Citrix Virtual Apps and Desktops からのリッチグラフィックアプリケーションの配信を最適化するエンコード技術を備えています。このグラフィック技術は、グラフィックを多用する仮想アプリケーションをリモートで使用する際に、物理デスクトップを使う場合と同じ操作性を提供します。

グラフィックにはハードウェアまたはソフトウェアレンダリングが使用できます。ソフトウェアレンダリングには、ソフトウェアラスタライザーと呼ばれるサードパーティのライブラリが必要です。たとえば、Windows には DirectX ベースのグラフィックのための WARP ラスタライザーが含まれています。他のソフトウェアレンダラーを使うことも可能です。ハードウェアレンダリング（ハードウェアアクセラレーション）にはグラフィックプロセッサ（GPU）が必要です。

HDX グラフィックは、一般的なユースケースのほとんどの場合に最適化された、デフォルトのエンコーディング構成を備えています。Citrix ポリシーを使用すると、IT 管理者は異なる要件を満たすさまざまなグラフィック関連の設定を構成し、望ましいユーザーエクスペリエンスを実現することもできます。

Thinwire

Thinwire とは、Citrix Virtual Apps and Desktops で使用される、Citrix のデフォルトのディスプレイリモートテクノロジです。

ディスプレイリモートテクノロジを使用すると、あるマシンで生成されたグラフィックが、通常はネットワークを経由して、別のマシンに転送され、表示されます。グラフィックは、ユーザー入力（たとえば、キー入力やマウス操作）の結果として生成されます。

HDX 3D Pro

Citrix Virtual Apps and Desktops の HDX 3D Pro 機能を使用すると、ハードウェアアクセラレーションにグラフィック処理装置（GPU）を使用して最高の性能を発揮するデスクトップとアプリケーションを配信できます。たとえば、OpenGL や DirectX を使用する 3D プロフェッショナルグラフィックアプリケーションでこの機能を使用します。標準 VDA では、DirectX の GPU アクセラレーションのみがサポートされます。

Windows シングルセッション OS のための GPU アクセラレーション

HDX 3D Pro を使用することで、グラフィックアプリケーションを仮想デスクトップ上で提供したりシングルセッションOS マシン上のアプリケーションとして配信したりできます。HDX 3D Pro は、物理コンピューター（デスクトップ、ブレード、およびラックワークステーションなど）と、XenServer、vSphere、および Hyper-V（パススルーのみ）ハイパーバイザーが提供する GPU パススルーおよび GPU 仮想化技術をサポートします。

GPU パススルー機能を使用すると、グラフィック処理ハードウェアに排他的にアクセスする仮想マシンを作成できます。ハイパーバイザーに複数の GPU を装着して、各仮想マシンに GPU を 1 つずつ割り当てることができます。

GPU 仮想化を使用すると、複数の仮想マシンで単一の物理 GPU によるグラフィック処理能力に直接アクセスできるようになります。

Windows マルチセッション OS のための GPU アクセラレーション

HDX 3D Pro 機能により、Windows マルチセッション OS のセッションで実行しているグラフィック処理アプリケーションで、サーバー上の GPU（Graphics Processing Unit）リソースを使用できるようになります。OpenGL、DirectX、Direct3D、および Windows Presentation Foundation（WPF）の処理をサーバーの GPU に移すことで、グラフィック処理によりサーバーの CPU 速度が低下することを回避できます。また、ワークロードが CPU と GPU で分担されるため、サーバーでより多くのグラフィック処理が可能になります。

Framehawk

> 重要：
>
> Citrix Virtual Apps and Desktops 7 1903 以降、Framehawk はサポートされなくなりました。代わりに、アダプティブトランスポートが有効なThinwireを使用します。

Framehawk は、ブロードバンドワイヤレス接続（Wi-Fi および 4G/LTE セルラーネットワーク）でのモバイルワーカー向けディスプレイリモートテクノロジです。Framehawk はスペクトル干渉や多重伝搬による課題を克服し、仮想アプリおよびデスクトップのユーザーに、滑らかで対話的なユーザーエクスペリエンスを提供します。

テキストベースのセッションウォーターマーク

テキストベースのセッションウォーターマークは、データ盗難を防止し、追跡できるようにするために役立ちます。この情報は追跡可能であり、セッションデスクトップに表示されることで、データを盗むために写真やスクリーンキャプチャを使用する場合の抑止力になります。テキストのレイヤーであるウォーターマークは自分で指定できます。ウォーターマークは元のドキュメントのコンテンツを変更することなく、セッション画面全体に表示されます。テキストベースのセッションウォーターマークには、VDA サポートが必要です。

アダプティブリフレッシュレート

新しくスケーラビリティが向上したことにより、HDX は仮想モニターのリフレッシュレートをターゲットの FPS ポリシーセットに合わせます。アダプティブリフレッシュレート（ARR）は、シングルセッション VDA とマルチセッション VDA の両方で利用でき、GPU でアクセラレートされたシナリオと非 GPU のシナリオの両方で機能します。

損失耐性モード

損失耐性モードは徹底的に見直され、パケット損失が検出されたときにセッションが通信可能のままであることが保証されます。

関連情報

- HDX 3D Pro
- Windows シングルセッション OS のための GPU アクセラレーション
- Windows マルチセッション OS のための GPU アクセラレーション
- Framehawk
- Thinwire
- テキストベースのセッションウォーターマーク

10 ビットハイダイナミックレンジ（HDR）

August 17, 2024

10 ビットのハイダイナミック レンジ（HDR）仮想デスクトップセッションでは、強化されたエンコーディングおよびデコーディング機能を使用して、色の範囲を広げ、コントラストと明るさを向上させた高品質の画像とビデオをレンダリングできます。また、白色輝度レベル、Extended Display Identification Data（EDID）、および視覚品質をカスタマイズして、ユーザーエクスペリエンスを向上させることもできます。

システム要件

エンドポイント：

- NVIDIA GPU 用の Windows 向け Citrix Workspace アプリ 2209 以降
- エンドポイントでの 10 ビット HEVC（H.,265）444 デコードに対応した NVIDIA GPU
- 10 ビット HDR 対応モニター。ディスプレイ設定を使用しているすべてのモニターで 10 ビット HDR を有効にする必要があります。

サーバー：

- NVIDIA GPU 用 Windows シングルセッション OS の場合は VDA 2209 以降、Intel GPU の場合は VDA 2308 以降
- VDA での 10 ビット HEVC 444 エンコードに対応した NVIDIA GPU

必要なポリシー

エンドポイント：

- グラフィックの H.265 デコードを有効にする

サーバー：

- 3D 画像ワークロードの最適化
- グラフィックス状態インジケーター（オプション）

サーバー構成

10 ビット HDR 対応エンドポイントモニターで Citrix セッションを起動すると、デフォルトで HDR セッションが有効になります。複数モニターの HDR セッションでは、すべてのエンドポイントモニターで 10 ビット HDR が有効になっている必要があります。HDR セッションは、ウィンドウモードと全画面モードの両方でサポートされています。

基準の白色輝度レベル

この設定は、nit 値で白色輝度レベルを定義します。セッション内の相対的な HDR 画面の明るさを制御します。デフォルト値は 80nit です。次のレジストリ キーを設定して、別の nit 値を定義します:

- HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics
- 種類: REG_DWORD
- 名前: RefWhiteLevel

設定を有効にするには、セッションのサイズを変更するか、セッションを切断して再起動する必要があります。

EDID のオーバーライド

HDR セッションにエンドポイントモニター EDID を使用するように VDA を構成できます。これにより、色域と輝度範囲を一致させることで、モニターの表示機能を最大限に活用できます。デフォルトでは、HDR セッションは HDR1000 対応ディスプレイを前提としています。
NVIDIA またはその他のツールを使用して、エンドポイントモニターの EDID をエクスポートできます。次のレジストリ キーを使用して VDA に適用します:

- HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics
- 種類: REG_BINARY
- 名前: EDIDOverride

EDID をレジストリに保存するときは、コンマ、スペース、または特殊文字を含めることはできません。オーバーライド EDID を有効にするには、サインアウトして新しいセッションを開始します。

視覚的無損失圧縮エクスペリエンス

視覚的に損失のないエクスペリエンスを実現するには、次のポリシーを有効にします:

- 視覚的無損失圧縮を許可
- 表示品質:［常に無損失］または［操作時は低品質］

ポリシーを設定後、画質スライダーを使用するか、ピクセル単位での精密なモードに切り替えることで、グラフィックス状態インジケーターを使用して HDR セッションの品質を制御できます。

Windows の画面ロックを許可する

このポリシーを使用すると、画面ロックを含むすべての Windows ディスプレイタイムアウトを Workstation OS 上の Citrix Virtual Desktops セッションに適用できます。この設定は、Citrix Studio の Citrix グループポリシーオブジェクトを使用して設定できます。

デフォルトでは、この設定が有効になっていない場合、Citrix Virtual Desktops は、アクティブなセッション中に、セッションロック、スクリーンセーバー、または画面オフのタイムアウトに応答しません。

Workstation VDA でパスワードで保護されたスクリーンセーバーが構成されている場合、スクリーンセーバーのタイムアウトに達したときに Citrix Virtual Desktops セッションが自動的にロックされるようにするには、この設定を有効にする必要があります。

VDA で画面オフのタイムアウトが構成されている場合にこの設定を有効にすると、タイムアウトの期限が切れても、ユーザーがセッションの操作を再開するまでセッションが更新されなくなります。たとえば、表示されている時刻は更新されず、新しい通知も表示されません。

そのほかの考慮事項

- 仮想 GPU では、最大 4 台のモニターで 10 ビット HDR セッションを起動できます。
- 次の場合、Citrix セッションは 8 ビットの非 HDR モードに戻ります:
  - エンドポイントモニターで 10 ビット HDR が有効になっていない場合
  - 画面共有を有効にします。
  - VDA で仮想ディスプレイレイアウトを設定します。
  - 視覚的無損失圧縮を許可ポリシーを設定せずにピクセル単位の精密なモードに切り替えます。

HDX 3D Pro

August 17, 2024

Citrix Virtual Apps and Desktops の HDX 3D Pro 機能を使用すると、グラフィック処理装置（GPU）によるハードウェアアクセラレーションで最高の性能を発揮するデスクトップとアプリケーションを配信できます。たとえば、OpenGL や DirectX を使用する 3D プロフェッショナルグラフィックアプリケーションでこの機能を使用します。標準 VDA では、DirectX の GPU アクセラレーションのみがサポートされます。

HDX 3D Pro のポリシー設定については、「3D 画像ワークロードの最適化」を参照してください。

サポート対象の Citrix Workspace アプリすべてで、3D グラフィックを使用できます。複雑な 3D ワークロード、高解像度モニター、マルチモニター構成、および高フレームレートアプリケーションで最高のパフォーマンスを得るには、Windows 向け Citrix Workspace アプリおよび Linux 向け Citrix Workspace アプリを最新バージョンにすることをお勧めします。サポート対象の Citrix Workspace アプリのバージョンについて詳しくは、「Citrix Workspace アプリのライフサイクルマイルストーン」を参照してください。

これらの 3D グラフィック処理アプリケーションとして次のものがあります:

- コンピューター支援設計（CAD）、コンピューター支援製造（CAM）、およびコンピューター支援エンジニアリング（CAE）アプリケーション

- 地理情報システム（GIS）ソフトウェア
- 医療画像処理のための画像保存通信システム（PACS）
- 最新バージョンの OpenGL、DirectX、NVIDIA CUDA、OpenCL、および WebGL を使用するアプリケーション
- 並列計算に NVIDIA Compute Unified Device Architecture（CUDA）GPU を使用する計算集約型の非グラフィックアプリケーション

HDX 3D Pro では、さまざまな帯域幅において最適なユーザーエクスペリエンスが提供されます。

- WAN 接続の場合：帯域幅が 1.5Mbps の WAN 接続でもインタラクティブなユーザーエクスペリエンスが提供されます。
- LAN 接続の場合：LAN 接続ではローカルデスクトップに匹敵するユーザーエクスペリエンスが提供されます。

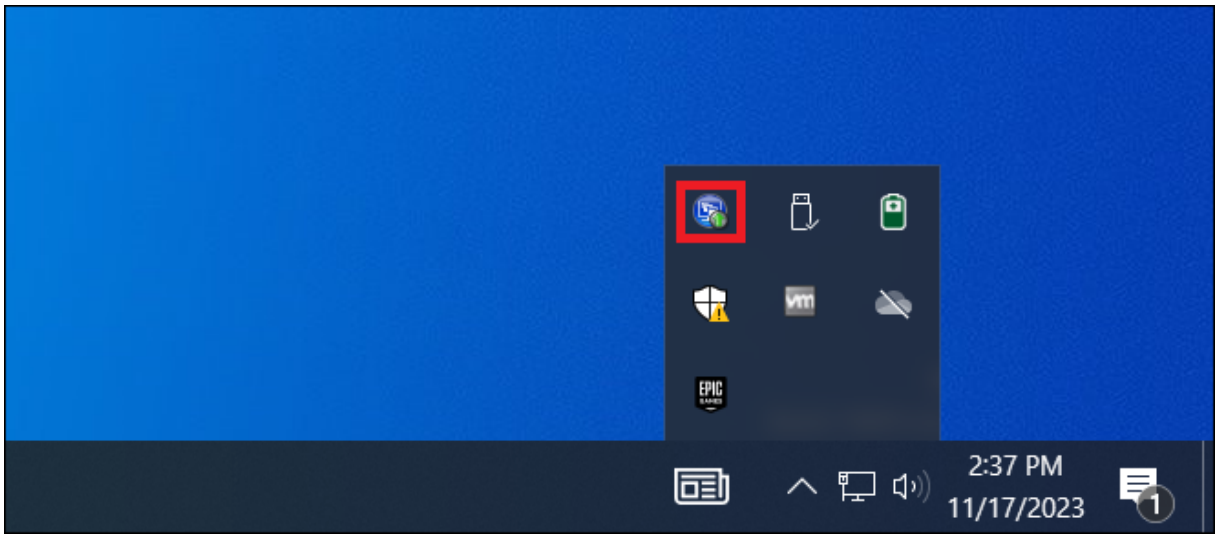
  ユーザーが使用する複雑で高価なワークステーションをよりシンプルなユーザーデバイスに置き換えて、グラフィック処理をユーザー側から中央管理が可能なデータセンター内に移管できます。

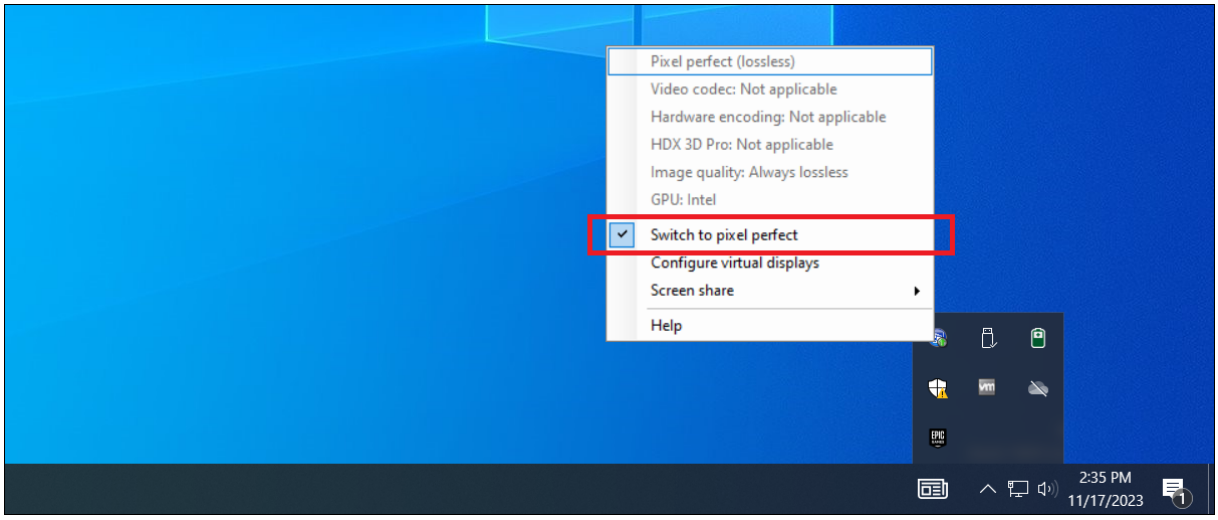
特殊なユースケースのための無損失圧縮オプション

HDX 3D Pro では CPU ベースの無損失コーデックも提供され、医療用画像処理などピクセル単位での精密なグラフィックが求められるアプリケーションがサポートされます。真の無損失圧縮はネットワークおよび処理リソースに対する負荷が非常に高いため、特殊なユースケースでのみ使用することをお勧めします。

無損失圧縮を使用すると、以下のように動作します：

- 表示しているフレームに非可逆圧縮が適用されているのか無損失圧縮が適用されているのかを示すグラフィックス状態インジケーターの無損失インジケーター（システムトレイアイコン）がユーザーの通知領域に表示されます。このアイコンは、ポリシーの ［表示品質］設定で ［操作時は低品質］が選択されている場合に便利です。送信されたフレームが無損失の場合、このインジケーターが緑色になります。





- ユーザーは、無損失スイッチを使ってセッション内でいつでも ［常に無損失］モードを有効にできます。セッション内で ［無損失］を選択または選択解除するには、アイコンを右クリックして ［完全に無損失に切り替える］をクリックするか、ショートカット Alt+Shift+1 を使用します。
  - 無損失圧縮の場合：HDX 3D Pro では、ポリシーで指定されているコーデックに関係なく、無損失コーデックが使用されます。
  - 非可逆圧縮の場合：HDX 3D Pro では、デフォルトのコーデックまたはポリシーで指定されているコーデックが使用されます。
    無損失スイッチの設定は保持されず、次回のセッションではリセットされます。すべてのセッションで無損失コーデックが使用されるようにするには、ポリシーの ［表示品質］設定で ［常に無損失］を選択します。

デフォルトのショートカットである ALT+SHIFT+1 を無効にし、セッション内で無損失を選択または選択解除できます。`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HDX3D\LLIndicator`で新しいレジストリ設定を構成します。

- 値の名前：HKEY_LOCAL_MACHINE_HotKey、種類：String

ショートカットの組み合わせを構成する形式は、C=0	1, A=0	1, S=0	1, W=0	1, K=val。キーはコンマ「,」で区切る必要があります。キーの順番は関係ありません。

-

- A、C、S、W、および K はキーです。ここで、C=Control、A=ALT、S=SHIFT、W=Win、および K=a が有効なキーです。K に対して使用できる値は、0～9、a～z、およびすべての仮想キーコードです。

- 例:
  F10 の場合、K=0x79 を設定
  Ctrl + F10 の場合、C=1、K=0x79 を設定
  Alt + A の場合、A=1、K=a または A=1、K=A または K=A、A=1 を設定
  Ctrl + Alt + 5 の場合、C=1、A=1、K=5 または A=1、K=5、C=1 を設定
  Ctrl + Shift + F5 の場合、A=1、S=1、K=0x74 を設定

HDX 3D Pro のユーザーエクスペリエンスの最適化

ブランチオフィスなど、帯域幅が制限された接続を複数のユーザーで共有している場合、ポリシーの［セッション全体の最大帯域幅］設定を使用して、各ユーザーが使用できる帯域幅を制限することをお勧めします。この設定により、ユーザーがログオンしたりログオフしたりするときに、使用可能な帯域幅が大きく変動しなくなります。HDX 3D Pro では使用可能なすべての帯域幅が使用されるため、ユーザーのセッション中に使用可能な帯域幅が大きく増減するとパフォーマンスが低下します。
たとえば、60Mbps の接続を 20 人のユーザーで共有する場合、各ユーザーが使用できる帯域幅は、同時接続ユーザーの数に応じて 3Mbps～60Mbps の間で変動します。この場合におけるユーザーエクスペリエンスを最適化するには、各ユーザーがピーク時に必要とする帯域幅を調べて、常時この値でユーザーを制限します。
ユーザーが 3D マウスを使用する場合は、汎用 USB リダイレクト仮想チャネルの優先度を 0 にすることをお勧めします。仮想チャネルの優先度を変更する方法については、Knowledge Center の記事 CTX128190 を参照してください。
HDX Monitor を使用すると、HDX 視覚化テクノロジの操作と構成を検証して、HDX の問題を診断して解決できます。このツールは、Citrix Virtual Apps and Desktops インストールメディアの **Support** フォルダーにあります。

Windows マルチセッション **OS** のための **GPU** アクセラレーション

August 17, 2024

Citrix Virtual Apps and Desktops では、Windows マルチセッション OS のセッションで実行しているグラフィック処理アプリケーションで、サーバー上の GPU（Graphics Processing Unit）リソースを使用できます。OpenGL、DirectX、Direct3D、および Windows Presentation Foundation（WPF）の処理をサーバーの GPU に移すことで、サーバーの CPU をより効率的に使用できます。

Windows Server はマルチユーザーオペレーティングシステムなので、GPU 仮想化（vGPU）を行わなくても、Citrix Virtual Apps がアクセスする GPU を複数のユーザーで共有できます。

このトピックの説明にはレジストリの編集が含まれています。レジストリエディターの使用を誤ると、深刻な問題が発生する可能性があり、Windows の再インストールが必要になる場合もあります。レジストリエディターの誤用による障害に対して、Citrix では一切責任を負いません。レジストリエディターは、お客様の責任と判断の範囲でご使用ください。また、レジストリファイルのバックアップを作成してから、レジストリを編集してください。

GPU 共有

GPU 共有により、リモートデスクトップセッションで動作する OpenGL アプリケーションおよび DirectX アプリケーションで GPU ハードウェアによるレンダリング処理が可能になります。GPU 共有には、以下の特徴があります:

- ベアメタルまたは仮想マシン上で使用でき、アプリケーションのスケーラビリティとパフォーマンスが向上します。
- 複数の同時接続セッションで GPU リソースを共有できます（ほとんどのユーザーは専用 GPU のレンダリングパフォーマンスを必要としません）。
- 特別な設定は必要ありません。

GPU は、ハイパーバイザーと GPU ベンダーの要件に従って、完全パススルーモードまたは仮想 GPU（vGPU）モードのいずれかで、Windows Server 仮想マシンに割り当てることができます。物理 Windows Server マシンでのベアメタル展開もサポートされています。

GPU 共有は、特定のグラフィックカードに依存するものではありません。

- 仮想マシンの場合は、使用中のハイパーバイザーと互換性のあるグラフィックカードを選択します。XenServer のハードウェア互換性リストについては、「Hypervisor ハードウェア互換性リスト」を参照してください。
- ベアメタルを実行するときは、オペレーティングシステムで単一のディスプレイアダプターを有効にすることをお勧めします。複数の GPU がハードウェアに取り付けられている場合は、デバイスマネージャーを使用して 1 つだけ残して無効にします。

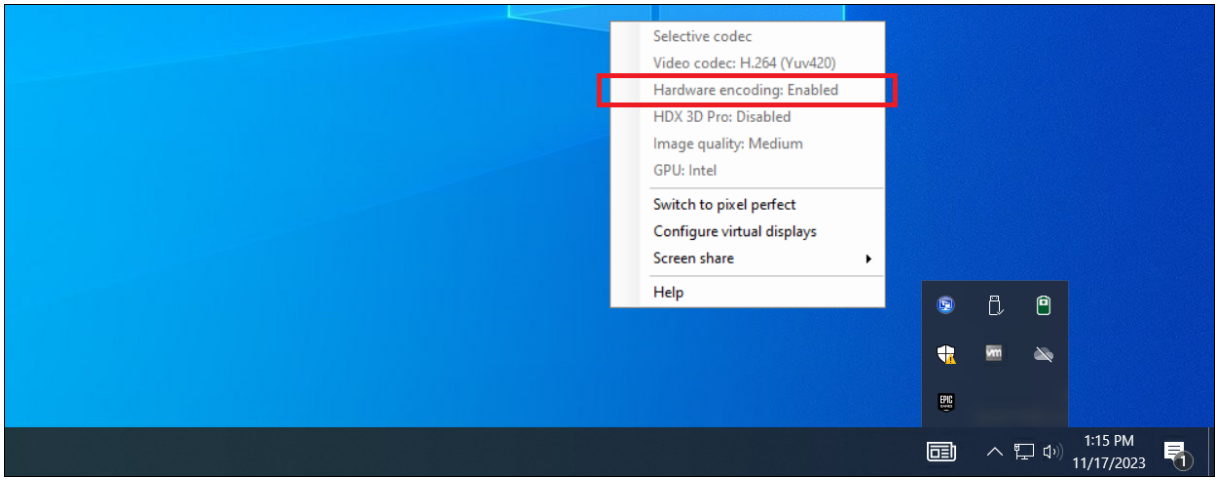
GPU 共有でのスケーラビリティは、以下の要素により異なります。

- 実行するアプリケーション
- 消費されるビデオ RAM の量
- グラフィックカードの処理能力

一部のアプリケーションでは、ビデオ RAM の不足をより効果的に処理できます。ハードウェアが過負荷になると、グラフィックカードドライバーが不安定になるか、クラッシュが発生する可能性があります。このような問題を避けるには、同時接続ユーザーの数を制限してください。

- NVIDIA GPU の高パフォーマンスビデオエンコーダーと Intel Iris Pro グラフィックプロセッサへのアクセス。ポリシー設定（デフォルトで有効）によりこの機能を制御し、H.264 エンコーディングのハードウェアエンコーディングを許可します（利用可能な場合）。該当するハードウェアが利用可能でない場合、VDA はソフトウェアビデオコーデックを使用して、CPU ベースのエンコーディングにフォールバックします。詳しくは、「グラフィックのポリシー設定」を参照してください。

GPU アクセラレーションが発生していることを確認するには、グラフィックス状態インジケーターを使用できます:



DirectX、Direct3D、および WPF レンダリング

DirectX、Direct3D、および WPF レンダリングは、DDI（Display Driver Interface）Version 9ex、10、または 11 をサポートする GPU が搭載されたサーバーでのみ使用可能です。

- Windows Server 2016 以降の RD Session Host サーバー上のリモートデスクトップサービス（RDS）セッションでは、デフォルトのアダプターとして Microsoft 基本レンダリングドライバーが使用されます。Windows Server 2016 以降の RDS セッションで GPU を使用するには、グループポリシーの［**Local Computer Policy**］>［**Computer Configuration**］>［**Administrative Templates**］>［**Windows Components**］>［**Remote Desktop Services**］>［**Remote Desktop Session Host**］>［**Remote Session Environment**］で［**Use the hardware default graphics adapter**］を有効にします。
- WPF アプリケーションでのレンダリングにサーバーの GPU を使用するようにするには、Windows マルチセッション OS セッションを実行するサーバー上でレジストリキーを設定します。レジストリの設定について詳しくは、レジストリを介して管理される機能の一覧にある「Windows Presentation Foundation（WPF）のレンダリング」を参照してください。

CUDA または OpenCL アプリケーション用の GPU アクセラレーション機能

ユーザーセッションで実行中の CUDA および OpenCL アプリケーションの GPU アクセラレーションは、デフォルトで無効です。

CUDA アクセラレーション機能を使用するには、レジストリ設定を有効にします。詳しくは、レジストリを介して管理される機能の一覧にある「CUDA または OpenCL アプリケーション用の GPU アクセラレーション機能」を参照してください。

Windows シングルセッション OS のための GPU アクセラレーション

August 17, 2024

HDX 3D Pro を使用することで、グラフィックアプリケーションを仮想デスクトップ上で提供したりシングルセッションOS マシン上のアプリケーションとして配信したりできます。HDX 3D Pro は、物理ホストコンピューター（デスクトップ、ブレード、ラックワークステーションなど）と、XenServer、vSphere、Nutanix および Hyper-V（パススルーのみ）ハイパーバイザーが提供する GPU パススルーおよび GPU 仮想化技術をサポートします。

HDX 3D Pro の機能は以下のとおりです：

- WAN およびワイヤレス接続でのパフォーマンスを最適化する Adaptive H.264 ベースまたは H.265 ベースの深圧縮。HDX 3D Pro のデフォルトでは、CPU ベースの全画面 H.264 圧縮が使用されます。H.264 によるハードウェアエンコーディングは、NVENC をサポートする NVIDIA、Intel、AMD カードで使用されます。H.265 によるハードウェアエンコーディングは、NVENC をサポートする NVIDIA カードで使用されます。
- 特殊なユースケースのための無損失圧縮オプション。HDX 3D Pro では CPU ベースの無損失コーデックも提供され、医療用画像処理などピクセル単位での精密なグラフィックが求められるアプリケーションがサポートされます。真の無損失圧縮はネットワークおよび処理リソースに対する負荷が非常に高いため、特殊なユースケースでのみ使用することをお勧めします。

> 注意：
>
> レジストリエディターの使用を誤ると、深刻な問題が発生する可能性があり、オペレーティングシステムの再インストールが必要になる場合もあります。レジストリエディターの誤用による障害に対して、Citrix では一切責任を負いません。レジストリエディターは、お客様の責任と判断の範囲でご使用ください。また、レジストリファイルのバックアップを作成してから、レジストリを編集してください。

- 複数および高解像度モニターのサポート。シングルセッション OS マシンの場合、最大 8 台の 4K モニターがサポートされます。ユーザーはそれらのモニターを自由に配置でき、解像度や向きが異なるモニターを組み合わせて使用できます。モニターの数は、ホストコンピューターの GPU、ユーザーデバイス、および使用できる帯域幅による制限を受けます。HDX 3D Pro では、ホストコンピューター上の GPU でサポートされるすべてのモニター解像度がサポートされます。
- 動的解像度仮想デスクトップまたはアプリケーションのウィンドウのサイズを任意に変更できます。注：解像度は、VDA のセッションウィンドウのサイズを変更することでのみ変更できます。VDA セッション内での解像度の変更（[コントロールパネル] > [デスクトップのカスタマイズ] > [ディスプレイ] > [画面の解像度] で変更）はサポートされていません。
- NVIDIA vGPU アーキテクチャのサポート。HDX 3D Pro は、NVIDIA vGPU カードをサポートしています。GPU パススルーと GPU 共有については「NVIDIA vGPU」を参照してください。NVIDIA vGPU を使用すると、複数の仮想マシンで単一の物理 GPU に同時に直接アクセスできます。このとき、仮想化されていないオペレーティングシステムで動作するものと同じ NVIDIA グラフィックドライバーが使用されます。

- Virtual Direct Graphics Acceleration（vDGA）を使った VMware vSphere および VMware ESX のサポート - RDS および VDI の両方のワークロードで、vDGA を使用する HDX 3D Pro がサポートされます。
- VMware vSphere/ESX のサポート。
- Windows Server 2016 の Discrete Device Assignment を使用した Microsoft HyperV のサポート。
- Intel Xeon Processor E3 ファミリおよび Intel Data Center GPU Flex シリーズによるデータセンターグラフィックのサポート。詳しくは、https://www.intel.com/content/www/us/en/products/details/discrete-gpus/data-center-gpu/flex-series.htmlを参照してください。
- AMD GPU のサポート。

> 注:
>
> AMD MxGPU（GPU 仮想化）のサポートに対応しているのは、VMware vSphere の vGPU のみです。GPU パススルーに対応しているのは、Citrix Hypervisor と Hyper-V です。詳しくは、https://www.amd.com/en/graphics/workstation-virtual-graphicsを参照してください。

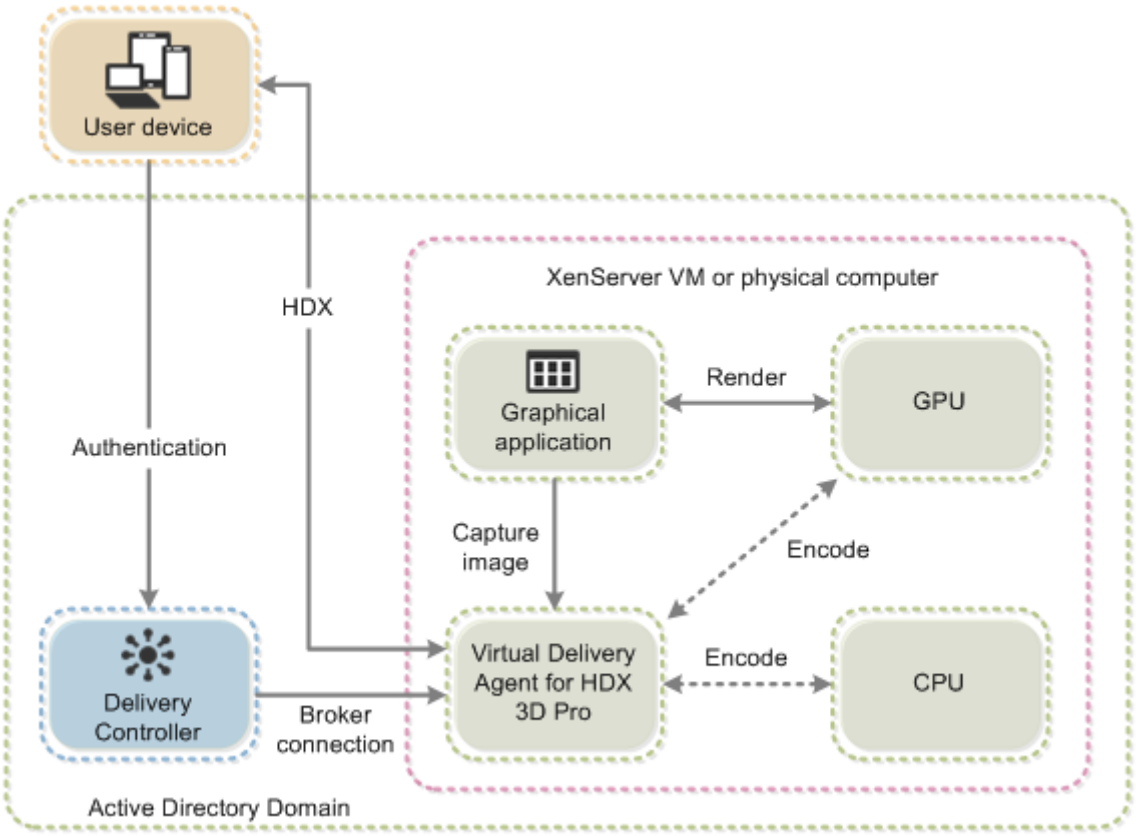
- NVIDIA GPU、AMD GPU、Intel GPU の高パフォーマンスビデオエンコーダーへのアクセス。この機能はポリシー設定（デフォルトで有効）によって制御されます。この機能により H.264、H.265、または AV1 エンコーディングのハードウェアエンコーディングが許可されます（利用可能な場合）。該当するハードウェアが利用可能でない場合、VDA はソフトウェアビデオコーデックを使用して、CPU ベースのエンコーディングにフォールバックします。詳しくは、「グラフィックのポリシー設定」を参照してください。

以下の図を参照してください:

- ユーザーが Citrix Workspace アプリにログオンして仮想アプリケーションまたはデスクトップにアクセスすると、Controller でユーザーが認証されます。Controller は VDA for HDX 3D Pro にアクセスし、グラフィカルアプリケーションをホストしているコンピューターへの接続を仲介します。

VDA for HDX 3D Pro はホスト上の適切なハードウェアを使って、デスクトップ全体またはグラフィックアプリケーションだけのビューを圧縮します。

- デスクトップまたはアプリケーションのビューおよびそれに対するユーザーの応答は、ホストコンピューターとユーザーデバイス間で転送されます。この転送は、Citrix Workspace アプリと VDA for HDX 3D Pro の間の直接 HDX 接続を介して行われます。



HDX 3D Pro のユーザーエクスペリエンスの最適化

ブランチオフィスなど、帯域幅が制限された接続を複数のユーザーで共有している場合、ポリシーの ［セッション全体の最大帯域幅］設定を使用して、各ユーザーが使用できる帯域幅を制限することをお勧めします。この設定により、ユーザーがログオンしたりログオフしたりするときに、使用可能な帯域幅が大きく変動しなくなります。HDX 3D Pro では使用可能なすべての帯域幅が使用されるため、ユーザーのセッション中に使用可能な帯域幅が大きく増減するとパフォーマンスが低下します。

たとえば、60Mbps の接続を 20 人のユーザーで共有する場合、各ユーザーが使用できる帯域幅は、同時接続ユーザーの数に応じて 3Mbps～60Mbps の間で変動します。この場合におけるユーザーエクスペリエンスを最適化するには、各ユーザーがピーク時に必要とする帯域幅を調べて、常時この値でユーザーを制限します。

ユーザーが 3D マウスを使用する場合は、汎用 USB リダイレクト仮想チャネルの優先度を 0 にすることをお勧めします。仮想チャネルの優先度を変更する方法については、Knowledge Center の記事CTX128190を参照してください。

無損失圧縮

無損失圧縮を使用すると、以下のように動作します:

- 表示しているフレームに非可逆圧縮が適用されているのか無損失圧縮が適用されているのかを示すインジケーター（システムトレイアイコン）がユーザーの通知領域に表示されます。このアイコンは、ポリシーの ［表示品質］設定で ［操作時は低品質］が選択されている場合に便利です。送信されたフレームが無損失の場合、このインジケーターが緑色になります。
- ユーザーは、無損失スイッチを使ってセッション内でいつでも ［常に無損失］モードを有効にできます。セッション内で［無損失］を選択または選択解除するには、アイコンを右クリックして ［完全に無損失に切り替える］をクリックするか、ショートカット Alt+Shift+1 を使用します。
- 無損失圧縮の場合：HDX 3D Pro では、ポリシーで指定されているコーデックに関係なく、無損失コーデックが使用されます。
- 非可逆圧縮の場合：HDX 3D Pro では、デフォルトのコーデックまたはポリシーで指定されているコーデックが使用されます。
- 無損失スイッチの設定は保持されず、次回のセッションではリセットされます。すべてのセッションで無損失コーデックが使用されるようにするには、ポリシーの ［表示品質］設定で ［常に無損失］を選択します。

無損失のホットキー

デフォルトのショートカット **ALT + SHIFT + 1** を使用すると、セッション中いつでもホットキーを使用して無損失を選択または選択解除することができます。

Windows レジストリ内で、デフォルトのショートカット **ALT + SHIFT + 1** を上書きすることができます。
新しいレジストリ設定を構成するには、次のレジストリ値を設定します：

- キー：`HKEY_CURRENT_USER\SOFTWARE\Citrix\Graphics`
- 名前：`HKLM_HotKey`
- 種類：`String`

ショートカットの組み合わせの構成形式は、`C=0|1, A=0|1, S=0|1, W=0|1, K=val`です。キーはスペースなしでコンマ（,）で区切る必要があります。キーの順番は関係ありません。

A、C、S、W、K はキーであり、C=Control、A=ALT、S=SHIFT、W=Win、および K= 有効なキー（使用できる値は 0～9、a～z、および任意の仮想キーコード）です。

たとえば、

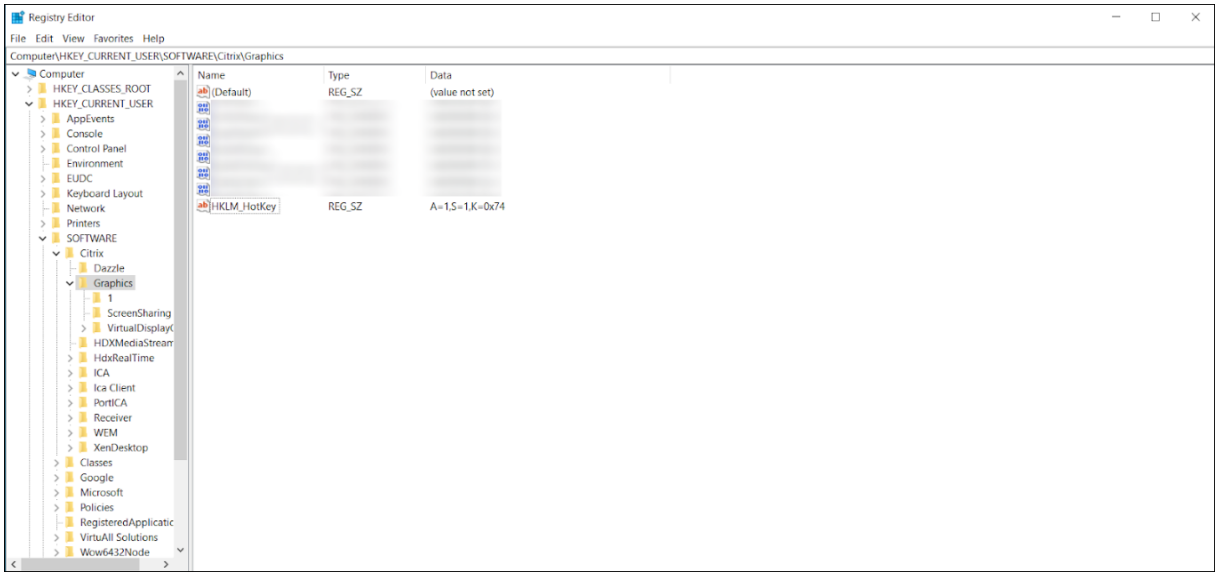
- **F10** に、K=0x79 を設定
- **Ctrl + F10** に、C=1, K=0x79 を設定
- **Alt + A** には、次を設定します：A=1, K=a または A=1, K=A または K=A, A=1
- **Ctrl + Alt + 5** には、次を設定します：C=1, A=1, K=5 または A=1, K=5, C=1
- **Ctrl + Shift + F5** には、次を設定します：A=1, S=1, K=0x74

次の表は、仮想キーコードの例を示しています：

キー	値
F1	0x70
F2	0x71
F3	0x72
F4	0x73
F5	0x74
F6	0x75
F7	0x76
F8	0x77
F9	0x78
F10	0x79
F11	0x7A
F12	0x7B
PAGE UP キー	0x21
PAGE DOWN キー	0x22
END キー	0x23
HOME キー	0x24
左方向キー	0x25
上方向キー	0x26
右方向キー	0x27
下方向キー	0x28

ショートカットの組み合わせの間にスペースがないことを確認してください。例:

正:
C=1,K=0x74
誤:
C=1, K=0x74



> 注意:
>
> レジストリエディターの使用を誤ると、深刻な問題が発生する可能性があり、オペレーティングシステムの再インストールが必要になる場合もあります。レジストリエディターの誤用による障害に対して、Citrix では一切責任を負いません。レジストリエディターは、お客様の責任と判断の範囲でご使用ください。また、レジストリファイルのバックアップを作成してから、レジストリを編集してください。

Thinwire

August 17, 2024

はじめに

Thinwire は Citrix HDX テクノロジの一部で、Citrix Virtual Apps and Desktops で使用される、Citrix のデフォルトのディスプレイリモートテクノロジです。

ディスプレイリモートテクノロジを使用すると、あるマシンで生成されたグラフィックが、通常はネットワークを経由して、別のマシンに転送され、表示されます。

正常なディスプレイリモートソリューションでは、ローカル PC と同様の、高度にインタラクティブなユーザーエクスペリエンスが提供されます。Thinwire では、幅広く複合的、効果的な画像解析および圧縮技術の使用により、これを実現しています。Thinwire ではサーバーのスケーラビリティが最大化され、消費する帯域幅は他のディスプレイリモートテクノロジより少なくできます。

このようなバランスの良さから、Thinwire は大部分の一般的なビジネスユースケースに合致しており、Citrix Virtual Apps and Desktops のデフォルトのディスプレイリモートテクノロジとして使用されています。

HDX 3D Pro

デフォルト設定では、Thinwire は 3D または高度にインタラクティブなグラフィックを提供し、グラフィック処理装置（GPU）を使用できます（存在する場合）。ただし、GPU を使用するシナリオでは、Citrix ポリシーの ［**3D** グラフィックの負荷の最適化］または ［表示品質］**>**［操作時は低品質］ポリシーを使用して、HDX 3D Pro モードを有効にすることをお勧めします。これらのポリシーは、GPU が存在する場合、ハードウェアアクセラレーションを使用して、Thinwire がビデオコーデック（H.264、H.265、または AV1）で画面全体をエンコードできるよう構成します。これにより、3D Pro グラフィックは、より滑らかなエクスペリエンスを実現できます。詳しくは、「H.264 の［操作時は低品質］」、「HDX 3D Pro」および「Windows シングルセッション OS のための GPU アクセラレーション」を参照してください。

要件

Thinwire は、Windows Server 2022、Windows Server 2019、Windows 10、および Windows 7 など、最新のオペレーティングシステムに最適化されています。Windows Server 2008 R2 には、従来のグラフィックモードをお勧めします。ビルトインのCitrix ポリシーテンプレートである「高サーバースケーラビリティ - レガシ OS」と「WAN の最適化 - レガシ OS」を使用して、これらのユースケースに推奨されるポリシー設定の組み合わせを提供します。

- Thinwire の動作を制御する ［圧縮にビデオコーデックを使用する］ポリシー設定は、Citrix Virtual Apps and Desktops 7 1808 以降と XenApp および XenDesktop 7.6 FP3 以降の VDA バージョンで利用できます。Citrix Virtual Apps and Desktops 7 1808 以降と XenApp および XenDesktop 7.9 以降の VDA バージョンでは、［選択された場合ビデオコーデックを使用する］オプションがデフォルト設定になっています。
- Thinwire はすべての Citrix Workspace アプリでサポートされています。ただし、8 ビットまたは 16 ビットグラフィックで帯域幅の使用量が少なくなるなど、Thinwire の機能は Citrix Workspace アプリによってサポートの有無が異なることがあります。こうした機能のサポートは、Citrix Workspace アプリによって自動的にネゴシエートされます。
- Thinwire は、マルチモニターおよび高解像度のシナリオで、より多くのサーバーリソース（CPU、メモリ）を使用します。Thinwire が使用するリソース量は調整可能ですが、帯域幅の使用状況がその結果増大することがあります。
- 低帯域幅または高遅延のシナリオでは、8 または 16 ビットグラフィックを有効にして対話操作性を改善することを検討できます。表示品質は、特に 8 ビットの色数で影響を受けることがあります。

エンコーディング方法

Thinwire は、ポリシーとクライアントの機能に応じて、2 つの異なるエンコーディングモードで動作できます：

- アダプティブ JPEG を使用した Thinwire
  圧縮にビデオコーデックを使用するポリシー設定：ビデオコーデックを使用しない

- 選択的な H.264、H.265、または AV1 を使用した Thinwire
  圧縮にビデオコーデックを使用するポリシー設定：選択された場合ビデオ コーデックを使用するまたは 領域をアクティブに変更
- 全画面 H.264、H.265、または AV1 を使用した Thinwire
  圧縮にビデオコーデックを使用するポリシー設定：画面全体に使用

H.265

H.265 としても知られる High Efficiency Video Coding（HEVC）は、H.264 の後継版です。
H.265 ビデオコーデックによるハードウェアエンコーディングは、次の GPU でサポートされています：

- NVIDIA Maxwell ベース以降の GPU
- Intel 第 6 世代以降の GPU
- AMD Raven ベース以降の GPU

AV1

Citrix は、AV1 ビデオコーデックのサポートを追加しました。AV1 のメリットは、H.264 や H.265 と比較して、画像圧縮に優れ、画質が良く、帯域幅の使用量が少ないことです。

AV1 では、次の要件を満たす必要があります：

- NVIDIA GPU で VDA 2305 以降、または
- Intel GPU で VDA 2308 以降

次の GPU はエンコーディングで互換性があります：

- NVIDIA Ada Lovelace ベースの GPU
- Intel ARC または Intel Data Center GPU Flex シリーズの GPU

NVIDIA の Ada Lovelace GPU について詳しくは、ADA アーキテクチャを参照してください。

Intel の ARC ワークステーションおよびデータセンター Flex シリーズの GPU について詳しくは、Flex シリーズおよび概要を参照してください。

ビデオコーデックの自動選択

VDA で圧縮にビデオ コーデックを使用するポリシーが有効になっているか、または 3D 画像ワークロードの最適化が有効になっている場合、使用する最適なビデオコーデックを自動的に検出できます。Windows 向け Citrix Workspace アプリのインストール中に、エンドポイントのデコード機能が評価されます。この情報に基づいて、Windows 向け Citrix Workspace アプリは、セッションの開始時に VDA で使用する最適なコーデックをネゴシエートします。以下は、ビデオコーデックが評価される順序です：

- AV1
- H.265
- H.264

自動選択は、これらのコーデックの 4:2:0 バリアントにのみ適用されます。表示品質設定が［操作時は低品質］または［常に無損失］に設定されており、視覚的無損失の圧縮が［有効］に設定されている場合、ビデオコーデックの自動選択は無効になります。

リソースに接続するときに、Citrix Workspace アプリはエンドポイントの H.265 および AV1 をデコードする機能をテストし、その機能をレジストリに保存します。Citrix Workspace アプリは使用する最適なビデオコーデックを自動的に選択し、このコーデックを VDA とネゴシエートします。VDA とクライアントの両方が H.265 と AV1 を使用できる場合、AV1 がビデオコーデックとして選択されます。AV1 が VDA またはクライアントのいずれでも利用できない場合は、H.265 がネゴシエートされます。どちらでも H.265 が利用できない場合、セッションはビデオコーデックとして H.264 を使用します。

> 注:
>
> この機能はデフォルトで有効になっています。この動作は、新しいクライアント側レジストリ設定DisableDecoderCapsを設定することで変更できます。

ビデオコーデックの自動選択を無効にするには、「DisableDecoderCaps」を HKLM\Software\WOW6432Node\Policies\Citrix\ICA Client\Graphics Engine DWORD DisableDecoderCaps = 1ま た はHKCU\Software\Policies\Citrix\ICA Client\Graphics Engine DWORD DisableDecoderCaps = 1に設定します。

これらの値のいずれかが 1 に設定されている場合、ビデオコーデックの自動選択は使用されません。
グラフィック状態インジケーターと HDX モニターは、ビデオコーデックを監視できます。

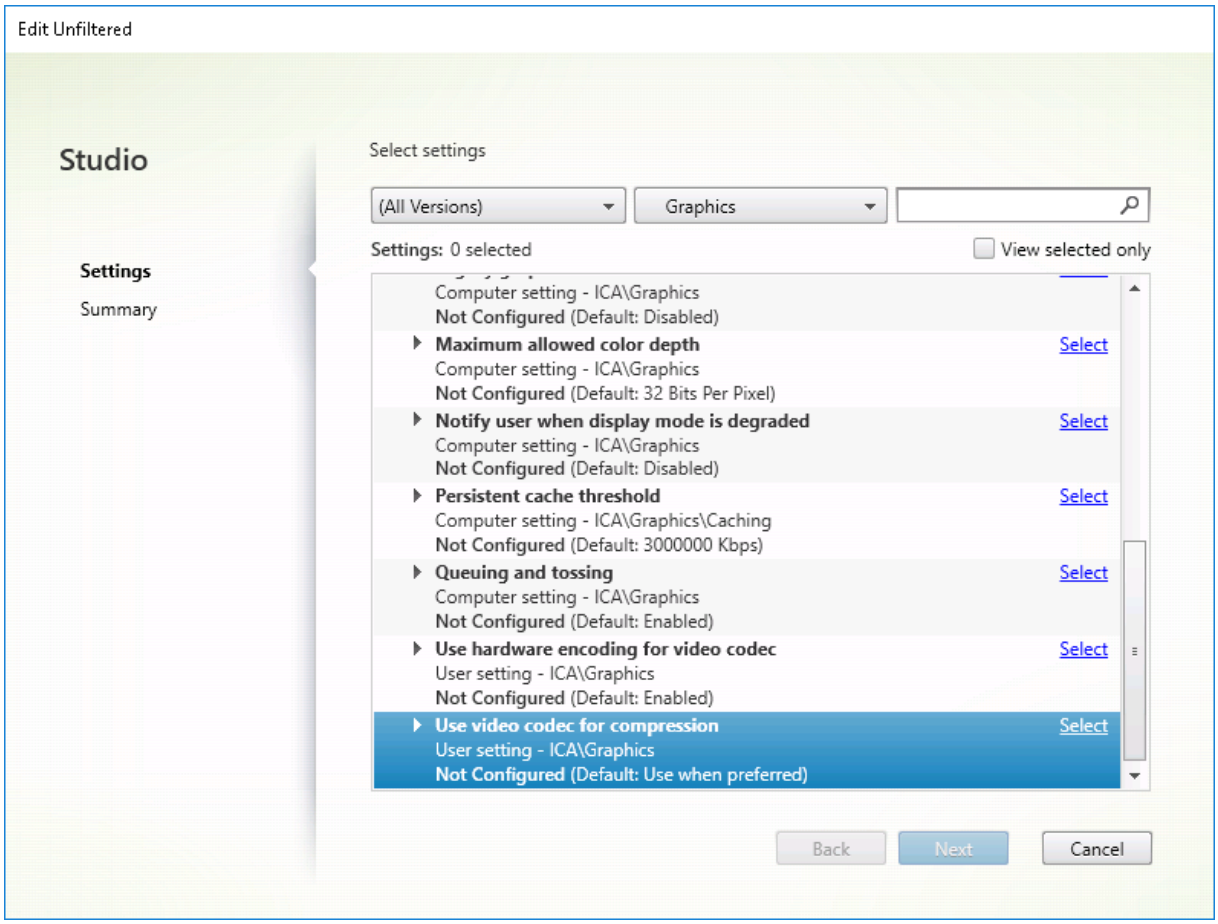
構成

Thinwire はデフォルトのディスプレイリモートテクノロジです。

次のグラフィックポリシー設定はデフォルトを設定し、さまざまなユースケースに代替選択肢を提供します:

- 圧縮にビデオコーデックを使用する
  - 選択された場合ビデオコーデックを使用するこれがデフォルトの設定です。追加の構成は必要ありません。この設定をデフォルトとして保持することにより、すべての Citrix 接続で Thinwire が選択され、デスクトップの一般的なワークロードで、スケーラビリティ、帯域幅、および優れた画質の点で、確実に最適化されます。これは、機能的に ［領域をアクティブに変更］と同等です。
- このポリシー設定の他のオプションは、さまざまなユースケースで他のテクノロジと組み合わせて Thinwire を使用し続けます。例:
  - ［領域をアクティブに変更］。Thinwire の状況に応じたディスプレイテクノロジは、動画（ビデオ、3D インモーション）を識別し、画像が動く画面の部分でのみ H.264、H.265、または AV1 を使用します。

– ［画面全体に使用］。特に 3D グラフィックを多用する事例で、Thinwire を全画面 H.264、H.265、または AV1 を使用して配信し、ユーザーエクスペリエンスと帯域幅を最適化します。H.264 4:2:0（［視覚的無損失］ポリシーが無効）の場合、最終イメージは完全に無損失ではなく、特定のシナリオには適さないことがあります。このような場合は、代わりに H.264 の［操作時は低品質］または H.265 の［操作時は低品質］を使用することを検討してください。



次の視覚表示ポリシー設定など、いくつかの他のポリシー設定は、ディスプレイリモートテクノロジのパフォーマンスを微調整するために使用できます。Thinwire はこれらすべてをサポートします。

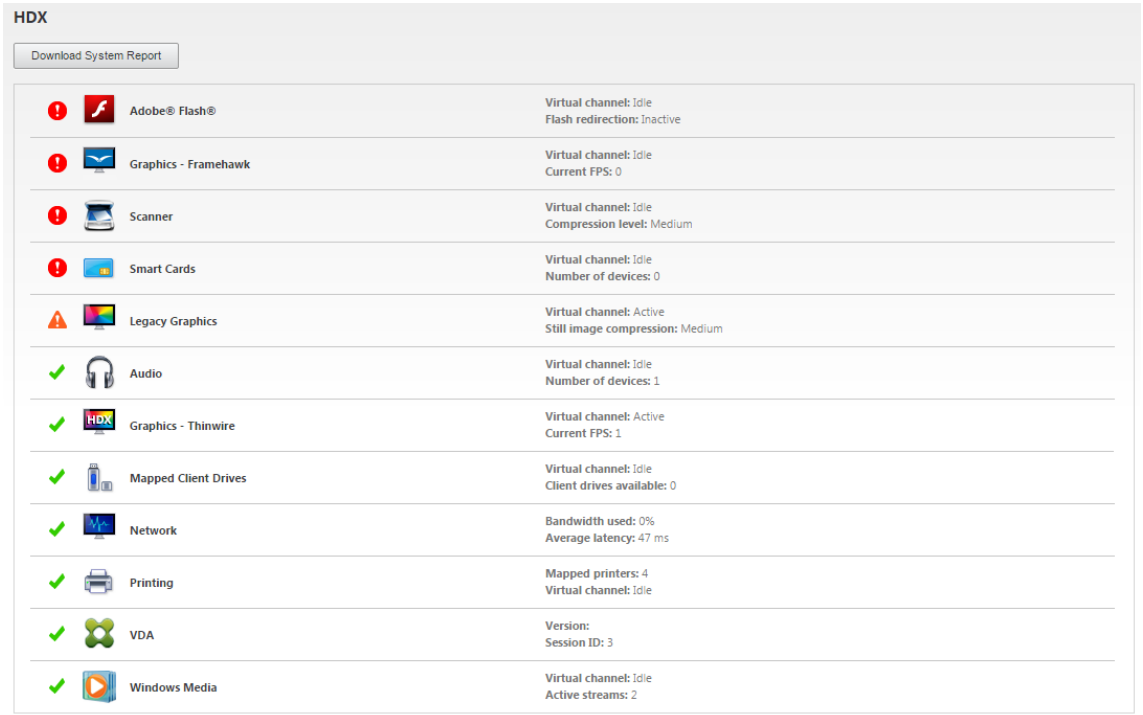
- 簡素なグラフィックに対する優先的色の解像度
- ターゲットフレーム数
- 表示品質

さまざまなビジネスユースケースに対して Citrix で推奨されるポリシー設定の組み合わせを取得するには、組み込みの Citrix ポリシーテンプレートを使用します。「高サーバースケーラビリティ」および「最高品位ユーザーエクスペリエンス」テンプレートは、組織の優先順位やユーザーの予期に最も適したポリシー設定との組み合わせで Thinwire を使用します。

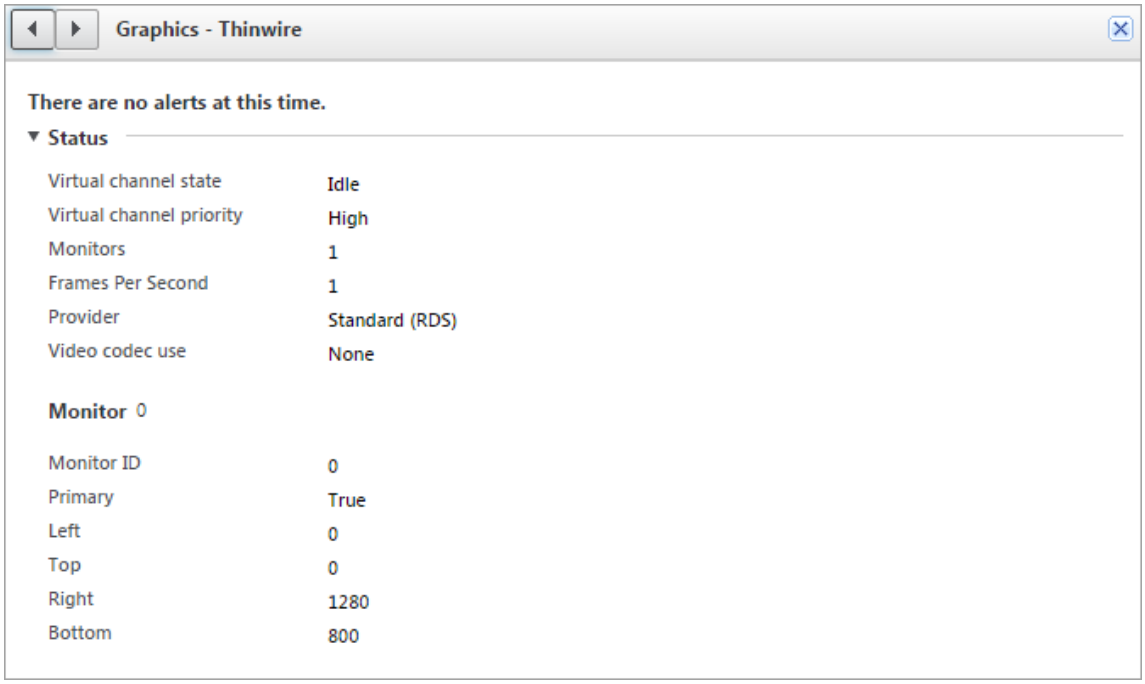
Thinwire のモニター

Citrix Director から Thinwire の利用状況とパフォーマンスをモニターすることができます。HDX 仮想チャネル詳細ビューには、あらゆるセッションで、Thinwire のトラブルシューティングやモニターに役立つ情報が表示されます。Thinwire 関連の測定基準を表示するには:

1. Director で、ユーザー、マシン、またはエンドポイントを検索し、アクティブなセッションを開いて ［詳細］をクリックします。または、［フィルター］>［セッション］>［すべてのセッション］を選択し、アクティブなセッションを開いて［詳細］をクリックすることもできます。
2. ［**HDX**］パネルまで下にスクロールします。



3. ［グラフィック **- Thinwire**］を選択します。



無損失圧縮コーデック（**MDRLE**）

通常のデスクトップセッションでは、画面の大半が単純なグラフィックまたはテキスト領域です。Thinwire はこれらの領域の範囲を決定し、2DRLE コーデックを使用して無損失エンコーディングの領域を選択します。Citrix Workspace アプリのクライアント側では、これらの要素は、セッション表示時に Citrix Workspace アプリ側の 2DRLE デコーダーを使用してデコードされます。

XenApp および XenDesktop 7.17 では、より高い圧縮率の MDRLE コーデックが追加されており、通常のデスクトップセッションでは 2DRLE コーデックよりも少ない帯域幅しか消費しません。この新しいコーデックは、サーバーの拡張性には影響を与えることはありません。

消費帯域幅が抑えられるため、通常、（特に共有リンクまたは制約付きリンクで）セッションのインタラクティブ性が向上するとともに、コストを削減できます。

MDRLE コーデックには構成は不要です。Citrix Workspace アプリで MDRLE デコードがサポートされている場合、VDA では、VDA の MDRLE エンコードと Citrix Workspace アプリの MDRLE デコードが使用されます。Citrix Workspace アプリで MDRLE デコードがサポートされていない場合、VDA では、自動的に 2DRLE エンコードにフォールバックされます。

MDRLE の要件:

- Citrix Virtual Apps and Desktops: VDA バージョン 7 1808 以降
- XenApp および XenDesktop: VDA バージョン 7.17 以降
- Windows 向け Citrix Workspace アプリ: バージョン 1808 以降
- Citrix Receiver for Windows バージョン 4.11 以降

プログレッシブモード

Citrix Virtual Apps and Desktops 1808 では、プログレッシブモードが導入され、デフォルトで有効になっています。制約のあるネットワーク環境（デフォルト：帯域幅 <2Mbps、または遅延 >200 ミリ秒）では、Thinwire が圧縮するテキストや静止画の量が増えて、画面アクティビティの対話操作性が改善されます。画面アクティビティが停止すると、大幅に圧縮されたテキストや画像は、その後徐々に、ランダムなブロック単位でシャープになります。このような方法で圧縮およびシャープ化して総合的な対話操作性を改善しながら、キャッシュ使用を低減し帯域幅の使用を増やしていきます。

Citrix Virtual Apps and Desktops 1906 の場合、プログレッシブモードはデフォルトで無効になっています。現在は、別のアプローチを使用しています。静止画の画質は、現在、ネットワーク状況に基づいて ［表示品質］設定ごとに事前定義された最小値および最大値の間で変化します。明示的なシャープ化の手順が存在しないため、Thinwire は、プログレッシブモードの利点をほぼすべて提供しながら画像配信を最適化し、キャッシュ効率を維持します。

プログレッシブモードの動作を変更する

プログレッシブモードの状態は、レジストリキーを使用して変更できます。詳しくは、レジストリを介して管理される機能の一覧にある「プログレッシブモード」を参照してください。

操作時は低品質

［操作時は低品質］は、対話操作性のために画像配信や最終イメージの品質を最適化する Thinwire の特別な構成です。［表示品質］ポリシーを ［操作時は低品質］に設定することで有効にできます。

［操作時は低品質］の設定は画面のアクティビティ中に H.264、H.265、または AV1 を使用して画面を圧縮し、アクティビティが停止すると完全な無損失へシャープ化します。可能な限り最高のフレーム数を維持するために、使用可能なリソースの非可逆圧縮画質に適応します。シャープ化の手順は徐々に実行されます。たとえば、モデルを選択してから、それを回転させる場合などです。

［操作時は低品質］では、ハードウェアアクセラレーションなど、画面全体用のビデオコーデックのすべての利点を利用できますが、最終的な、無損失画面は保証されていません。これは、完全に無損失な最終イメージが必要な 3D タイプのワークロードにとって重要なポイントです。たとえば、医療画像を操作する場合です。また、H.264 の ［操作時は低品質］は全画面 H.264 4:4:4 よりも少ないリソースを使用します。その結果、［操作時は低品質］を使用すると通常、視覚的無損失 H.264 4:4:4 よりもフレーム数が多くなります。

> 注:
>
> ［操作時は低品質］を使用する場合、ビデオコーデックの使用を無効にすることができます。［ビデオ コーデックを使用する］ポリシーを`Do not use video codec`に設定するだけです。これによって動画は代わりにアダプティブ JPEG でエンコードされます。

視覚的無損失エンコーディング

視覚的無損失エンコーディングは、ビデオコーデック圧縮にクロマサブサンプリングされた YUV 4:2:0 色空間ではなく、YUV 4:4:4 色空間を使用します。これにより、色空間の変換中に色情報が失われることはなく、デコードされると元の RGB 画像からは視覚的に認識できなくなります。

次の例について考えてみましょう。ビデオコーデックを使用して画面全体を圧縮する場合、4:2:0 色圧縮により、テキストなどのハイコントラストの細部が劣化し、ぼやけて読みにくくなる可能性があります。対照的に、4:4:4 ではほぼすべての色情報が保持され、視覚的に認識できる劣化は見られません。

完全に無損失な画質や正確な色表示が必要とされるワークロードでは、視覚的無損失エンコーディングのメリットを生かすことができます。

視覚的無損失エンコーディングは、H.264 と H.265 の両方で使用できます。H.264 4:4:4 エンコーディングは純粋にソフトウェアベースのソリューションであるため、VDA とクライアントの両方の CPU 使用率に重大な影響を与える可能性があります。これはフレームレートにも影響する可能性があります。

Citrix Workspace アプリ 2305 リリースで H.265 4:4:4 のサポートが追加され、Thinwire で VDA 上の GPU とクライアントの両方で H.265 4:4:4 エンコーディングを使用できるため、パフォーマンスが大幅に向上します。

視覚的無損失 4:4:4 エンコーディングを可能にするには、次の 2 つのポリシーを有効にする必要があります:

- 表示品質: `Build to Lossless`または`Always Lossless`に設定
- 視覚的無損失を許可する: `Enabled`に設定

> 注:
>
> 視覚的無損失を許可するが有効になっていない場合、`Build to lossless`または`Always Lossless`で Thinwire エンコーダーに切り替えます。

H.265 4:4:4 の視覚的無損失には追加の要件があります:

- NVIDIA GPU には VDA バージョン 2209 以降が必要です
- Intel GPU には VDA バージョン 2308 以降が必要です

H.265 4:4:4 では次の GPU がサポートされています:

- NVIDIA Pascal 世代以降の GPU
- Intel 第 10 世代以降の GPU

クライアントの場合、Windows 向け Citrix Workspace アプリバージョン 2305 が必要です（バージョン 2309.1 が推奨されます）。

H.265 4:4:4 のハードウェアデコーディングは、次のクライアントデバイス GPU で可能になります:

- NVIDIA Turing 世代以降の GPU
- Intel 第 10 世代以降の GPU

テキストベースのセッションウォーターマーク

August 17, 2024

テキストベースのセッションウォーターマークは、データ盗難を防止し、追跡できるようにするために役立ちます。この情報は追跡可能であり、セッションデスクトップに表示されることで、データを盗むために写真やスクリーンキャプチャを使用する場合の抑止力になります。テキストのレイヤーであるウォーターマークは自分で指定できます。ウォーターマークは元のドキュメントのコンテンツを変更することなく、セッション画面全体に表示されます。テキストベースのセッションウォーターマークには、VDA サポートが必要です。

> 重要:
>
> テキストベースのセッションウォーターマーキングは、セキュリティ機能ではありません。このソリューションは、データ盗難を完全に防止するものではありませんが、ある程度の抑止力とトレーサビリティを提供します。この機能の使用時の完全な情報トレーサビリティが保証されるわけではありませんが、この機能を他のセキュリティソリューションと適切に組み合わせることをお勧めします。

セッションウォーターマークはテキストであり、ユーザーに配信されるセッションに適用されます。セッションウォーターマークによって、データ盗難を追跡するための情報が伝えられます。最も重要なデータは、画面イメージが撮影された現在のセッションのログオンユーザーの ID です。データ漏洩をより効果的に追跡するには、サーバーまたはクライアントのインターネットプロトコルアドレスや接続時間などのその他の情報を含めます。

ユーザーエクスペリエンスを調整するには、［セッションウォーターマーク］ポリシー設定を使用して、画面上の配置とウォーターマークの外観を構成します。

要件:

Virtual Delivery Agent:

マルチセッション OS 7.17
シングルセッション OS 7.17

制限事項:

- セッションウォーターマークは、ローカルアプリケーションアクセス、Windows Media リダイレクト、MediaStream、Web ブラウザーコンテンツリダイレクト、および HTML5 ビデオリダイレクトが使用されるセッションではサポートされていません。セッションウォーターマークを使用するには、これらの機能が無効になっていることを確認してください。

- 全画面ハードウェアアクセラレーションモード（全画面 H.264 または H.265 エンコーディング）でセッションが実行されている場合は、セッションウォーターマークはサポートされておらず、表示されません。
- これらの HDX ポリシーを設定すると、ウォーターマーク設定が有効にならず、ウォーターマークがセッション画面に表示されません。

［ビデオコーデックにハードウェアエンコーディングを使用します］を ［有効］
［圧縮にビデオコーデックを使用する］を ［画面全体に使用］

- これらの HDX ポリシーを設定すると、動作が不確定となり、ウォーターマークが表示されないことがあります。

  ［ビデオコーデックにハードウェアエンコーディングを使用します］を ［有効］
  ［圧縮にビデオコーデックを使用する］を ［画面全体に使用］

  ウォーターマークが表示されるようにするには、［ビデオコーデックにハードウェアエンコーディングを使用します］を ［無効］に設定するか、または ［圧縮にビデオコーデックを使用する］を ［領域をアクティブに変更］か ［ビデオコーデックを使用しない］に設定します。
- セッションウォーターマークは、Thinwire グラフィックモードのみをサポートします。
- ［Session Recording］を使用する場合、録画されたセッションにウォーターマークは含まれません。
- Windows リモートアシスタンスを使用している場合、ウォーターマークは表示されません。
- ユーザーが **Print Screen** キーを押して画面をキャプチャした場合、VDA 側でキャプチャされる画面にウォーターマークは含まれません。キャプチャされたイメージがコピーされるのを防ぐために対策を講じることをお勧めします。

画面共有

August 17, 2024

画面共有により、ユーザーは Citrix Virtual Desktop セッションと、画面コンテンツ、キーボード、マウスコントロールなどを共有できます。

システム要件

- Windows：シングルセッションまたはマルチセッションの OS VDA
- Linux：Linux セッションの共有について詳しくは、Linux VDA のドキュメントを参照してください。
- デスクトップセッションのみを共有できます。
- セッションをホストしている VDA と共有セッションに接続しているマシンとの間にネットワーク接続が必要です。ネットワークポートの要件は、使用中の ICA ポート（TCP/UDP 1494 または 2598）と、［画面共有ポリシー］ 構成（デフォルトでは TCP 52525～52625）に基づいています。

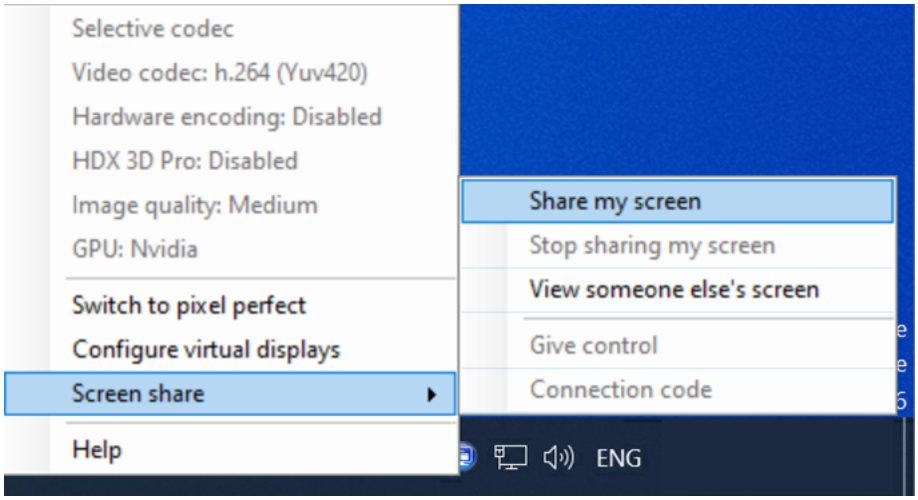
構成

画面共有は、Citrix ポリシーを使用して有効にする必要があります。画面共有はデフォルトで無効になっています。［画面共有ポリシー］ を構成して、機能を有効または無効にし、使用可能なネットワークポート範囲を割り当てます。

［グラフィック状態インジケーター］ ポリシーを有効にして、セッションの共有とセッションへの接続のコントロールなど、ユーザーインターフェイスを表示します。

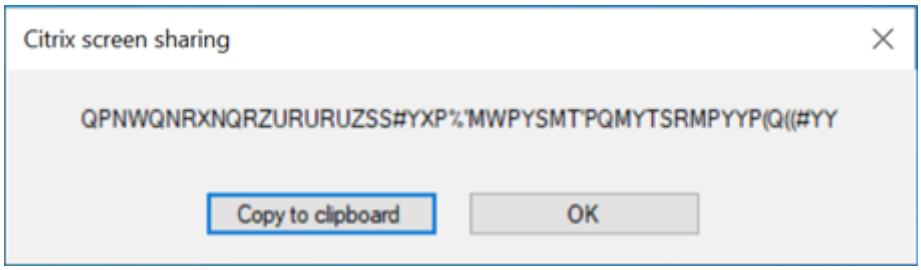
セッションの共有

セッションを共有するには、Windows の通知領域にある HDX グラフィック状態インジケーターアイコンを探します。それを右クリックしてメニューを表示し、［画面共有］ **>** ［自分の画面を共有］を選択します。



［クリップボードにコピー］をクリックするか、ダイアログボックスに表示されている文字列すべてを手動で選択してコピーします。次に、選択したアプリケーション（メール、IM クライアントなど）に文字列を貼り付けて、他のユーザーに配布できます。

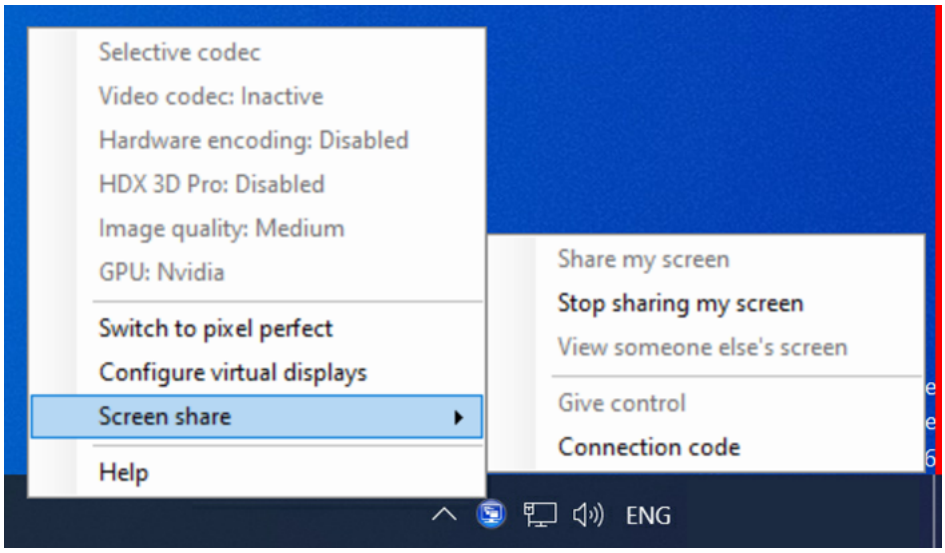
［**OK**］または［**x**］をクリックしてダイアログボックスを閉じます。接続コードは、セッション共有中はいつでも、［画面共有］ **>** ［接続コード］メニューオプションから取得できます。



画面の周りに赤い枠線が表示され、現在セッションが共有中であることと他のユーザーに表示されていることを示します。

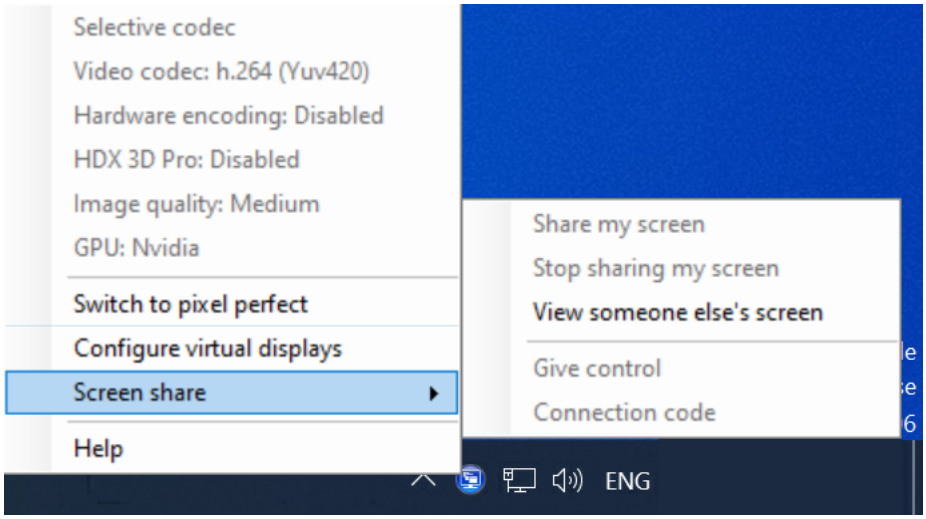
キーボードとマウスのコントロールは、［画面共有］**>**［制御を渡す］メニューオプションを使用して、他のユーザーと共有することもできます。

［画面共有］**>**［画面の共有を停止］メニューオプションで、セッションの共有を停止し、すべてのユーザーを切断できます。

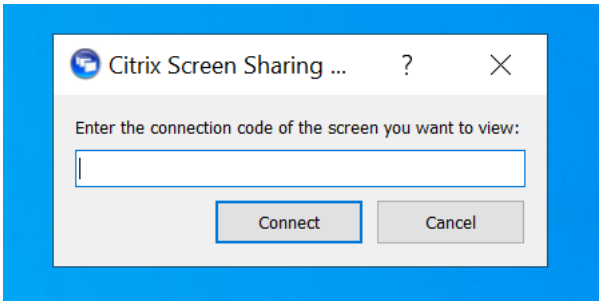


共有セッションへの接続

他の人のセッションに接続するには、Windows の通知領域にある HDX グラフィック状態インジケーターアイコンを探します。それを右クリックしてメニューを表示し、［画面共有］**>**［他のユーザーの画面を表示］を選択します。

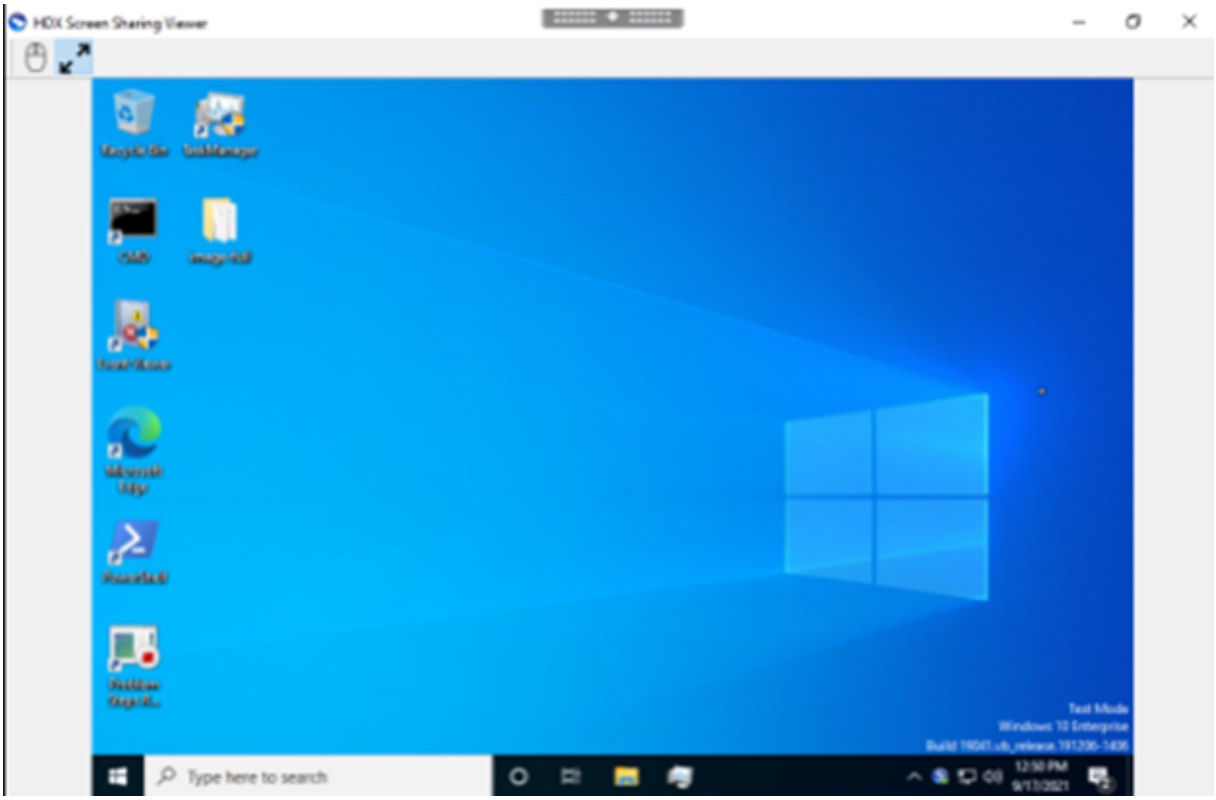


セッションを共有しているユーザーが入力した接続文字列をテキストボックスに入力する、または貼り付けます。［接続］をクリックして接続を確立します。



［**HDX** 画面共有ビューアー］ウィンドウの左上隅にあるマウスアイコンをクリックして、キーボードとマウスのコントロールを要求できます。

［**HDX** 画面共有ビューアー］ウィンドウを閉じて、いつでも共有セッションを切断できます。



そのほかの考慮事項

- 画面共有ビューアーアプリケーションは、*C:\Program Files\Citrix\HDX\bin\TwPlayer.exe* の VDA に含まれており、Virtual Apps サーバーを使用して、公開アプリケーションとして展開することもできます。この代替の展開モデルにより、仮想デスクトップにアクセスできないユーザーとの共同作業が可能になります。
- 画面共有ポリシーのネットワークポート範囲を使用して、共有セッションへの接続を許可するユーザーの数を制限できます。ユーザーごとに 1 つのポートが必要です。デフォルトの範囲では、最大 100 ユーザーを許可できます。
- セッションに接続されているすべてのモニターが共有されます。個々のモニターを選択することはできません。

- H.265 ビデオコーデックはサポートされていません。

仮想ディスプレイレイアウト

August 17, 2024

仮想ディスプレイの設定 UI を使用すると、ライブセッション内の VDA のセッションモニターごとに仮想ディスプレイレイアウトを定義できます。この機能を使用すると、各セッションモニターを個別に複数の仮想モニターに分割できます。リモートデスクトップ上で、合計 8 台の仮想モニターに分割できます。また、セッションのプライマリモニターとディスプレイの DPI 設定を更新できます。

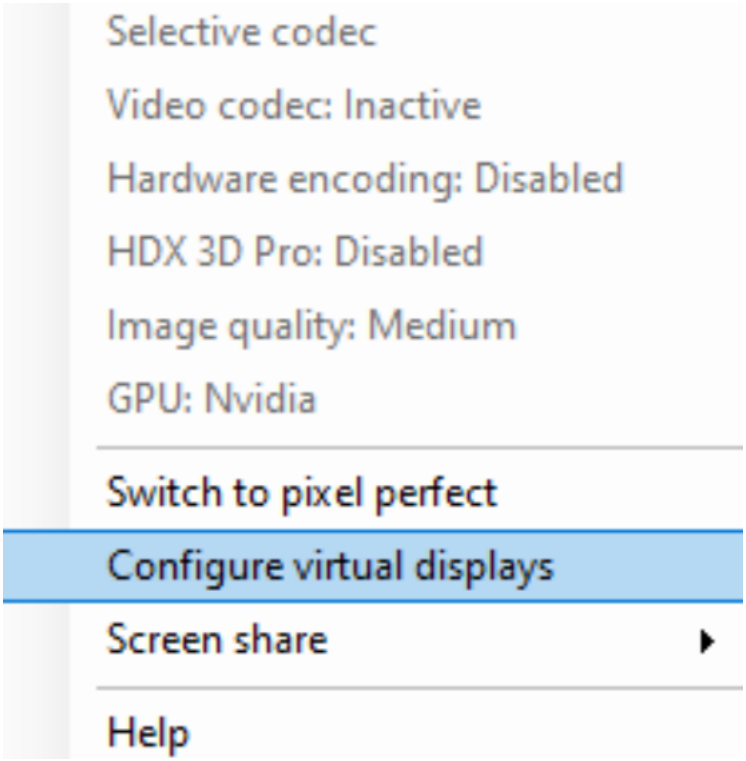
仮想ディスプレイの設定は、各クライアントデバイスのユーザーごとに保存されます。この設定は、特定のユーザーの特定のクライアントから、後続のすべての接続に適用されます。セッションのサイズ変更、セッションの切断または再接続、セッションのログオフまたはログオン間で保持されます。構成された仮想ディスプレイレイアウトは、セッションのサイズ変更時とセッションモニターの数の変更時にリセットされます。

システム要件

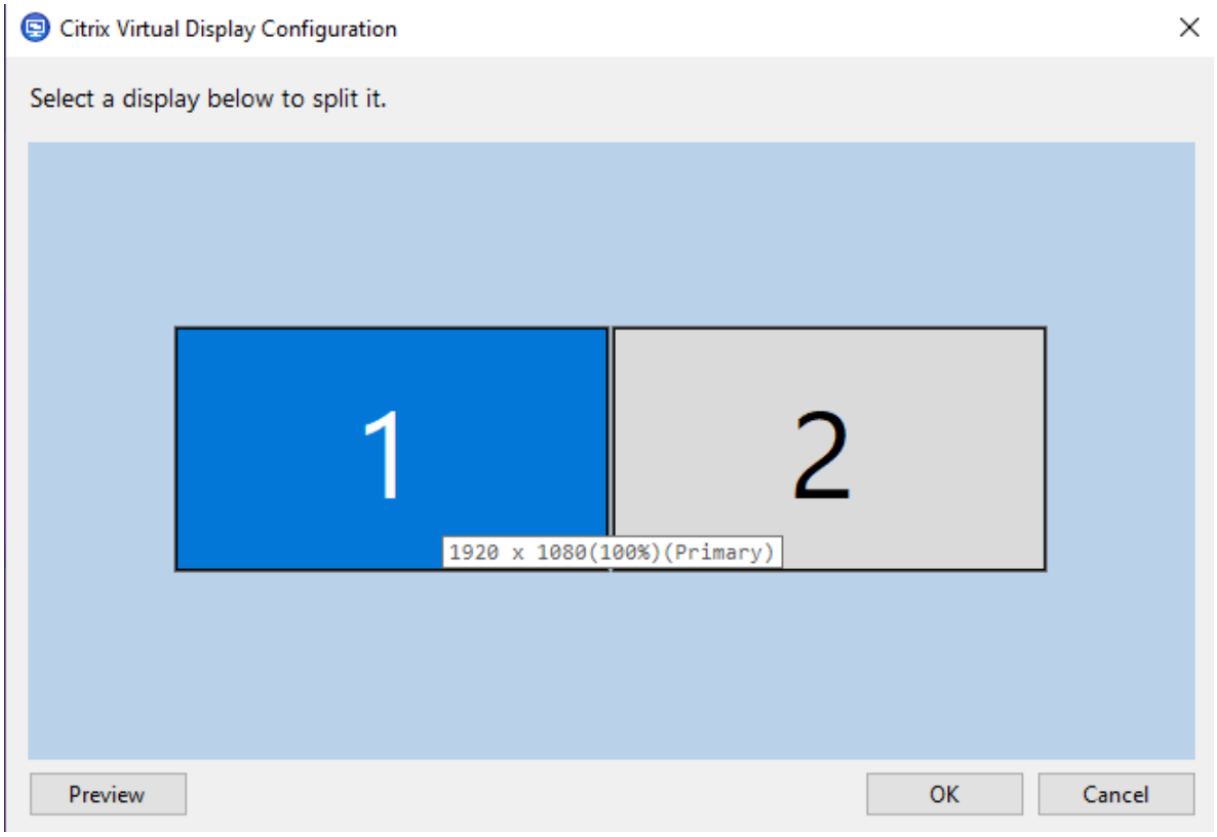
- Windows：シングルセッションまたはマルチセッションの OS VDA
- グラフィック状態インジケーターポリシーを有効にする必要があります
- デスクトップセッションのみを構成できます。

構成

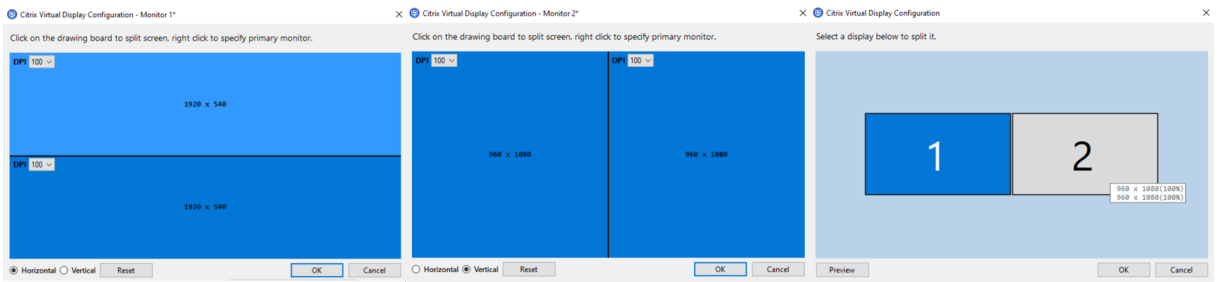
仮想ディスプレイレイアウトを構成するには、グラフィックス状態インジケーターアイコンを右クリックし、［仮想ディスプレイの設定］オプションを選択します。仮想ディスプレイの設定 UI が起動します。



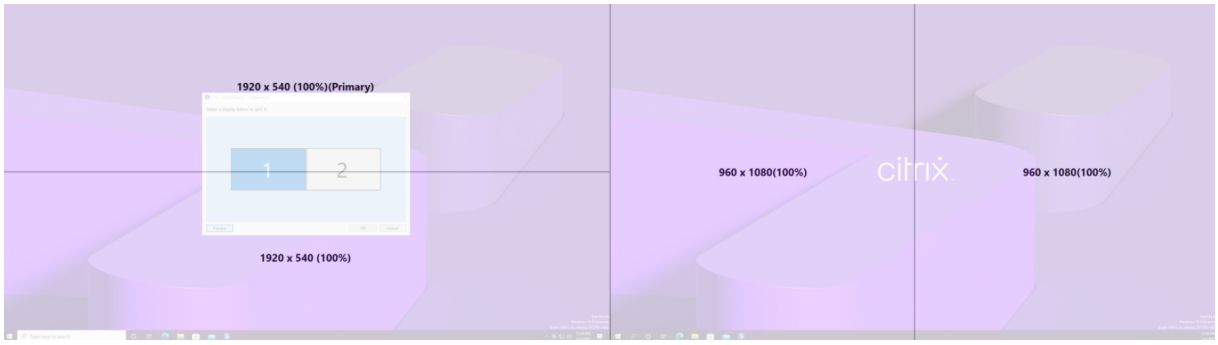
UI には、現在のセッションのディスプレイレイアウトが表示されます。青色はセッションのプライマリモニターを示します。ディスプレイにカーソルを合わせると、ディスプレイ設定のツールチップが表示されます。ツールチップは、特定のセッションモニターで定義されている、現在の仮想ディスプレイレイアウトに関する情報を提供します。



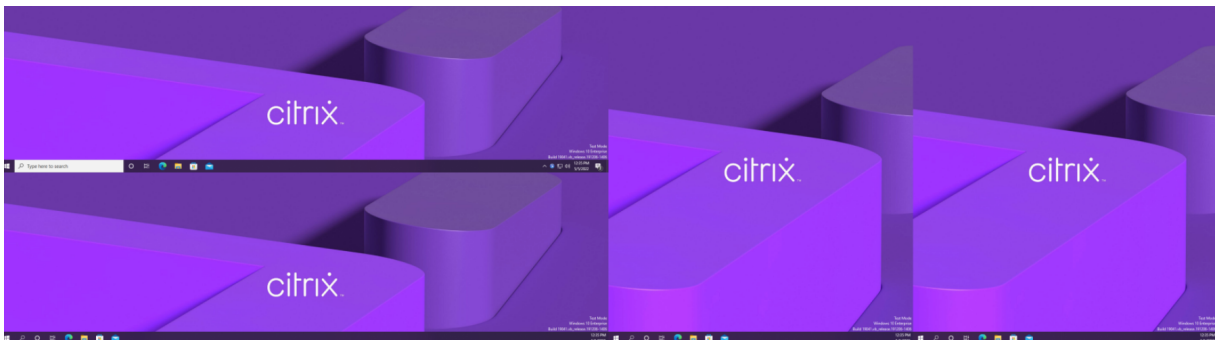
ディスプレイを選択してインタラクティブ UI に移行します。これにより、選択したセッションモニターの仮想ディスプレイを構成できます。垂直または水平の線で画面を仮想モニターに分けることができます。画面は、セッションのモニター解像度で指定されたパーセンテージに従って分割されます。仮想ディスプレイを右クリックしてプライマリモニターとしてマークし、DPI ドロップダウンリストを使用して、仮想ディスプレイの優先スケールファクターを設定します。仮想ディスプレイレイアウトを定義したら、[**OK**] をクリックしてレイアウトを一時的に保存するか、[キャンセル] をクリックして変更を破棄します。[リセット] を使用すると、構成を元に戻し、セッションモニターの元のレイアウトを復元できます。



現在構成されている仮想ディスプレイレイアウトをプレビューするには、[プレビュー] ボタンをクリックします。セッション内の仮想ディスプレイの予想される位置と解像度が強調表示されたウィンドウが表示されます。



[**OK**] をクリックして、仮想ディスプレイレイアウトをすぐに適用して保存します。[キャンセル] をクリックして UI を閉じ、すべての変更を破棄します。



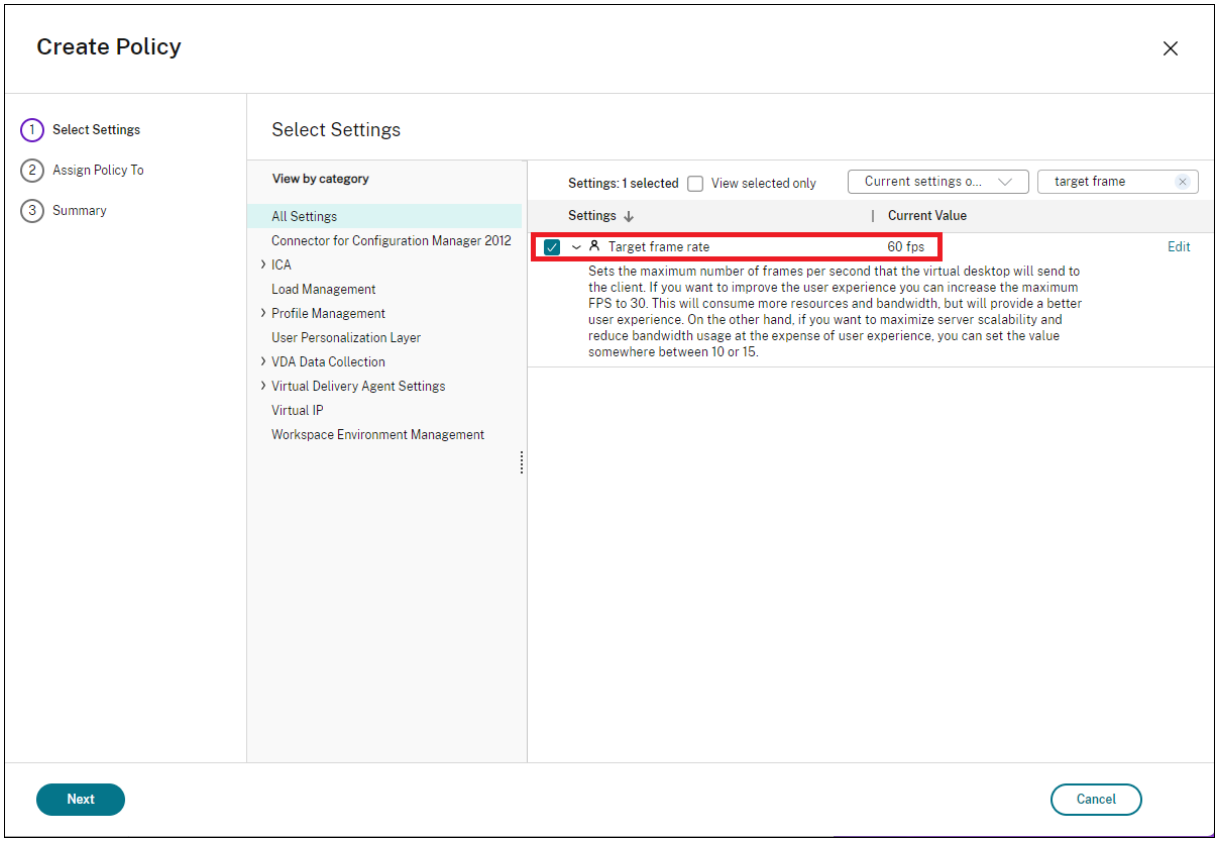
そのほかの考慮事項

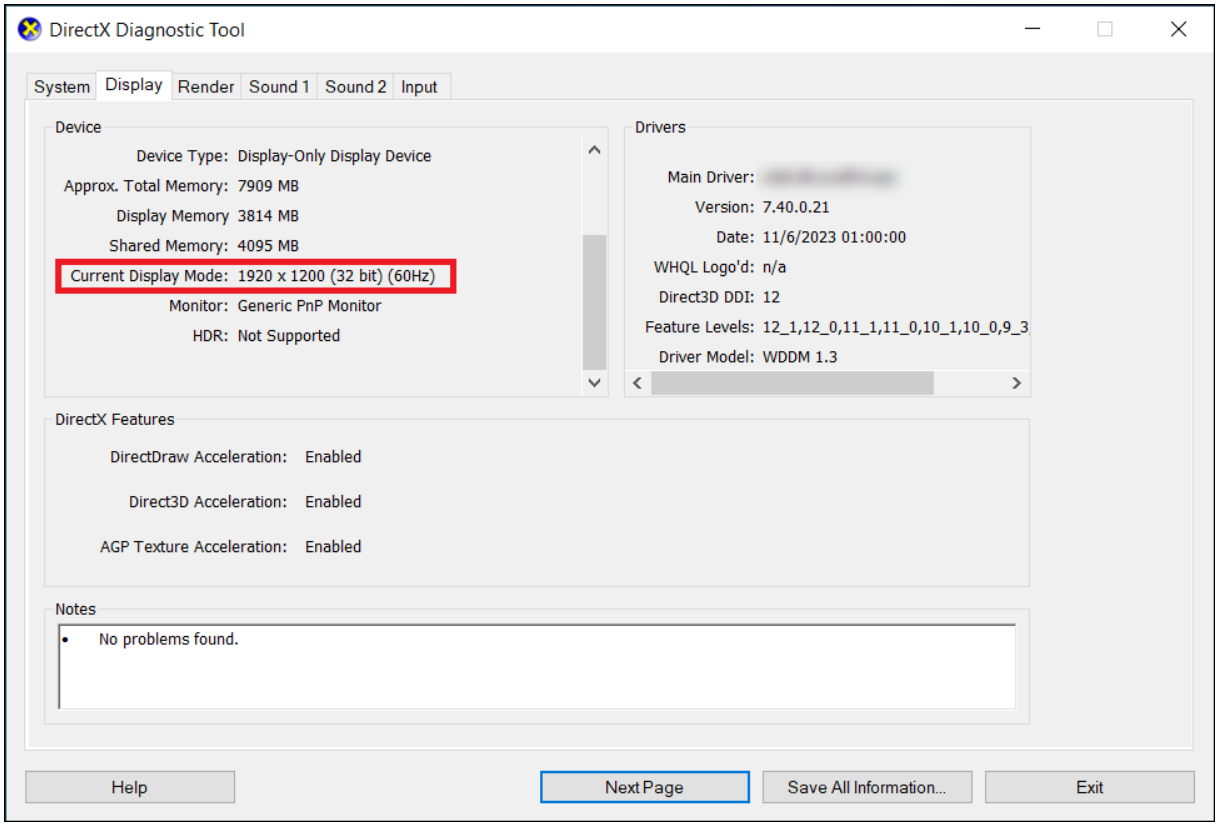
- 仮想ディスプレイの必要な最小解像度は 640 x 480 です。
- UI を介して定義された仮想ディスプレイの DPI は、指定された画面解像度を OS がサポートしているかによって異なります。
- この機能を、Citrix Workspace アプリの既存の仮想ディスプレイ機能と同時に使用しないでください。
- プレビュー機能は Server 2016 ではサポートされていません。

アダプティブリフレッシュレート

August 17, 2024

新しくスケーラビリティが向上したことにより、HDX は仮想モニターのリフレッシュレートをターゲットの FPS ポリシーセットに合わせます。アダプティブリフレッシュレート（ARR）は、シングルセッション VDA とマルチセッション VDA の両方で利用でき、GPU でアクセラレートされたシナリオと非 GPU のシナリオの両方で機能します。





> 注
>
> アダプティブリフレッシュレートは、（Citrix Virtual Apps and Desktops のデフォルトに従って）Citrix Indirect Display または IDD が使用されている場合にのみ使用でき、ベンダー提供のディスプレイアダプターを使用している場合は使用できません。

グラフィックの損失耐性モード

August 17, 2024

グラフィックの損失耐性モードは徹底的に見直され、パケット損失が検出されたときにセッションが通信可能のままであることが保証されます。ネットワークの状態が事前に定義された帯域幅、遅延、およびパケット損失のしきい値を超えて悪化すると、Citrix グラフィックエンコーダーはパケット損失の影響を抑えるために、より積極的なパケット配信モードに自動的に切り替わります。その結果、帯域幅の使用量はパケット損失の量に比例して増加します。その後状況が改善すると、Citrix グラフィックエンコーダーはシームレスに元に戻ります。しきい値はポリシーで構成でき、デフォルトは 300 ミリ秒の遅延で、5% のパケット損失です。

Windows 向け Citrix Workspace アプリ 2311 は、現在サポートされています。他のプラットフォームのサポートは、今後の Citrix Workspace アプリのリリースで追加される予定です。以前のバージョンと同様、この機能が動作するには HDX アダプティブトランスポート（EDT）が有効になっている必要があります。さらに、Citrix Gateway サービス経由で接続する場合は、Gateway 上でグラフィックの損失耐性モードも有効にする必要があります。

マルチメディア

August 17, 2024

HDX 技術スタックは、マルチメディアアプリケーションの配信を次の 2 つの相補的なアプローチでサポートします。

- サーバー側でレンダリングするマルチメディア配信
- クライアント側でレンダリングするマルチメディアリダイレクト

これにより、良好なユーザーエクスペリエンスを保ちながら、サーバースケーラビリティを向上させ、ユーザーごとのコストを削減するあらゆる種類のマルチメディアフォーマットを配信できます。

サーバー側でレンダリングするマルチメディア配信で、オーディオとビデオコンテンツは、アプリケーションによって Citrix Virtual Apps and Desktops サーバー上でデコードおよびレンダリングされます。コンテンツは圧縮され、ICA プロトコルでユーザーデバイス上の Citrix Workspace アプリに配信されます。この方法は、さまざまなアプリケーションとメディア形式に対して、最大レートの互換性を提供します。ビデオ処理は数値計算であるため、サーバ

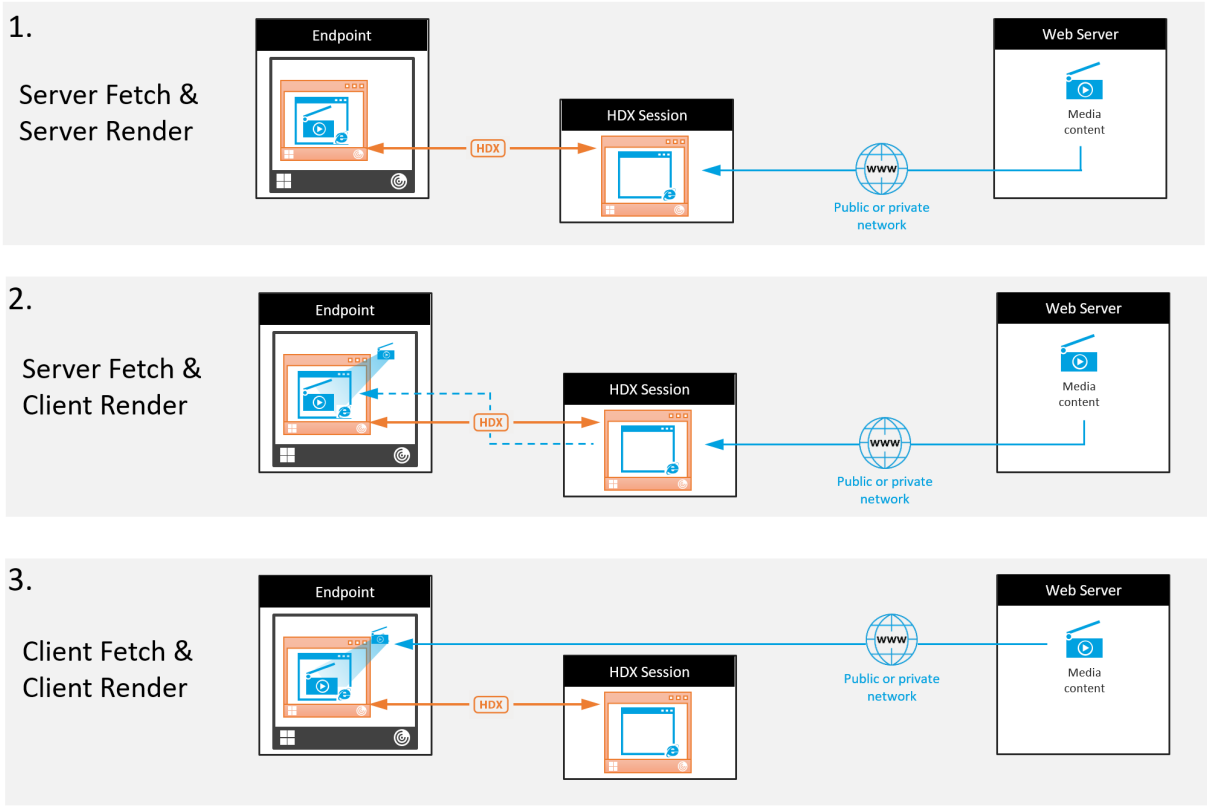
ー側でレンダリングされたマルチメディア配信はオンボードのハードウェアアクセラレーションの利点を大幅に活かすことがきます。たとえば、DirectX Video Acceleration（DXVA）のサポートは、H.264 デコーディングを別のハードウェアで実行することで、CPU をオフロードします。Intel Quick Sync、AMD RapidFire、NVIDIA NVENC の機能により、ハードウェアアクセラレーション用の H.264 エンコーディングが利用できるようになりました。

ほとんどのサーバーにビデオ圧縮用のハードウェアアクセラレーションがないため、すべてのビデオ処理をサーバーの CPU で実行する場合は、サーバースケーラビリティに悪影響を及ぼします。多くのマルチメディア形式をユーザーデバイスにリダイレクトしてローカル側でレンダリングするようにすれば、高サーバースケーラビリティを維持できます。

- Windows Media リダイレクトは、一般的に Windows Media Player に関連した、さまざまな種類のメディア形式に対してサーバーをオフロードします。
- HTML5 ビデオが普及し、Citrix はこのタイプのコンテンツに対してリダイレクトテクノロジを導入しました。HTML5、HLS、DASH、または WebRTC を使用している Web サイトについては、Web ブラウザーコンテンツのリダイレクトをお勧めします。
- 一般的な連絡先リダイレクト機能である、ホストからクライアントへのリダイレクトとローカルアプリアクセスを、マルチメディアコンテンツに応用できます。

これらの機能を含めて、リダイレクトを構成しない場合は、HDX はサーバー側でのレンダリングを実行します。
リダイレクトを構成する場合、HDX はサーバー側でフェッチし、クライアント側でレンダリング、またはクライアント側でフェッチし、クライアント側でレンダリングのいずれかを実行します。これらの方法が失敗した場合、HDX は必要に応じてサーバー側でのレンダリングにフォールバックし、フォールバック防止ポリシーの対象になります。

サンプルシナリオ



シナリオ **1.**（サーバー側でフェッチし、サーバー側でレンダリング）**:**

1. サーバーはメディアファイルをソースからフェッチし、デコードし、コンテンツをオーディオデバイスまたはディスプレイデバイスに対して再生します。
2. サーバーは再生されたイメージまたはサウンドをディスプレイデバイスまたはオーディオデバイスからそれぞれ抽出します。
3. オプションとしてサーバーが抽出されたファイルを圧縮し、クライアントに送信します。

このアプローチでは、（抽出されたイメージやサウンドが効率的に圧縮されていない場合は）高 CPU コストと高帯域幅コストを負担することになり、サーバースケーラビリティは低くなります。

Thinwire とオーディオの仮想チャネルがこのアプローチを処理します。このアプローチの利点により、クライアントのハードウェアとソフトウェアの要件が削減されます。このアプローチでは、デコーディングはサーバーで実行され、より多くの種類のデバイスとフォーマットに対応します。

シナリオ **2.**（サーバー側でフェッチし、クライアント側でレンダリング）**:**

このアプローチは、オーディオまたはディスプレイデバイスに対してデコードおよび再生される前に、メディアコンテンツをインターセプトできることを前提としています。圧縮されたオーディオ/ビデオコンテンツは、クライアントに送信され、ローカルでデコードおよび再生されます。このアプローチの利点により、クライアントデバイスにオフロードされ、サーバーの CPU サイクルが節約されます。

ただし、このアプローチでは、クライアントにハードウェアとソフトウェアの要件が一部追加されます。クライアントは、受信する可能性のあるそれぞれのフォーマットをデコードできる必要があります。

シナリオ **3.**（クライアント側でフェッチし、クライアント側でレンダリング）**:**

このアプローチは、ソースからフェッチされる前に、メディアコンテンツの URL をインターセプトできることを前提としています。URL は、メディアコンテンツがローカルでフェッチ、デコード、および再生されたクライアントに送信されます。このアプローチは概念的に単純です。この利点により、制御コマンドのみがサーバーから送信されるため、サーバーの CPU サイクルと帯域幅の両方が節約されます。ただし、メディアコンテンツは、クライアントに常にアクセスできるわけではありません。

フレームワークとプラットフォーム**:**

シングルセッションオペレーティングシステム（Windows、Mac OS X、および Linux）は、マルチメディアアプリケーションのよりすばやい開発を可能にする、マルチメディアフレームワークを提供します。次の表に、より一般的なマルチメディアフレームワークの一部を示します。各フレームワークはメディア処理を複数の段階に分割して、パイプラインベースのアーキテクチャを使用します。

フレームワーク	プラットフォーム
DirectShow	Windows（98 以降）
Media Foundation	Windows（Vista 以降）
Gstreamer	Linux
Quicktime	Mac OS X

メディアリダイレクト機能によるダブルホップのサポート

	オーディオリダイレクト	いいえ
	ブラウザーコンテンツリダイレクト	いいえ
	HDX Web カメラリダイレクト	はい
	HTML5 ビデオリダイレクト	はい
	Windows Media リダイレクト	はい

オーディオ機能

August 17, 2024

ポリシーに以下の Citrix 設定項目を追加して、HDX のオーディオ機能を最適化できます。これらの設定項目の使用方法、およびほかのポリシー設定項目との依存関係について詳しくは、「オーディオのポリシー設定」、「帯域幅のポリシー設定」、「マルチストリーム接続のポリシー設定」を参照してください。

アダプティブオーディオ

アダプティブオーディオを使用すれば、VDA でオーディオ品質ポリシーを手動で構成する必要がありません。アダプティブオーディオは環境の設定を最適化し、古いオーディオ圧縮形式を置き換えることで、優れたユーザーエクスペリエンスを提供します。

アダプティブオーディオはデフォルトで有効になっています。アダプティブオーディオを無効にするには、「オーディオのポリシー設定」を参照してください。

> 重要:
>
> リアルタイムオーディオアプリケーションが必要な場合には、TCP ではなくユーザーデータグラムプロトコル（UDP）を使用してオーディオを配信することをお勧めします。UDP では、次のオーディオ転送オプションが利用できます:
>
> - UDP を使用したオーディオ
> - HDX アダプティブ トランスポート（Enlightened Data Transport）
>
> DTLS を使用した UDP オーディオ暗号化は、Citrix Gateway と Citrix Workspace アプリ間でのみ有効です。このため、TCP トランスポートを使用した方が望ましい場合もあります。TCP では、VDA と Citrix Workspace アプリ間の、エンドツーエンドの TLS 暗号化がサポートされます。
>
> アダプティブオーディオと UDP オーディオについて詳しくは、「UDP でのオーディオリアルタイムトランスポートとオーディオ UDP ポートの範囲」を参照してください。

オーディオの損失耐性モード

損失耐性モードはオーディオをサポートします。この機能により、リアルタイムストリーミングのユーザーエクスペリエンスが向上し、ユーザーが遅延やパケット損失が大きいネットワーク経由で接続している場合に、EDT と比較して音質が向上します。この機能はデフォルトでは無効になっています。

> 注:
>
> この機能が動作するには、**HDX** アダプティブトランスポート（**EDT**）ポリシーとオーディオの損失耐性モードポリシーの両方を有効にする必要があります。

システム要件

次の製品が損失耐性モードをサポートする最小バージョンであることに注意してください:

- Citrix Virtual Delivery Agent（VDA）2308
- Windows 向け Citrix Workspace アプリ 2309

さらに、次の機能を有効にする必要があります:

- HDX アダプティブトランスポートポリシー。
- （オプション）リモート接続の場合は、Citrix Gateway サービスが必要です。

> 注:
>
> 上記の条件が満たされない場合、オーディオは EDT Reliable トランスポート経由で送信されます。

追加情報

損失耐性モードは、マルチメディアコンテンツを再送信せずに送信中のパケット損失を許容する損失耐性のあるトランスポートプロトコルであり、その結果、ユーザーはよりリアルタイムなエクスペリエンスを得ることができます。

Enlightened Data Transport（EDT）は Citrix 独自のトランスポートプロトコルであり、サーバーのスケーラビリティを維持しながら要求の厳しい長距離接続で優れたユーザーエクスペリエンスを提供します。損失耐性モードは、ネットワークが輻輳している場合でも安定した接続を維持するために、トランスポートプロトコルとして損失耐性モードを使用する Citrix Gateway サービスの機能です。これにより、リモートワーカーに一貫して安定したエクスペリエンスが保証されます。通常の状態では、EDT と損失耐性モードの両方で同様の結果が得られます。ただし、パケット損失のあるネットワーク状態では、損失耐性モードは EDT と比較して優れたオーディオエクスペリエンスを提供します。このため、リアルタイムマルチメディアに依存して作業をするリモートワーカーにとって、不可欠な機能です。

音質

一般的に、音質を高くするほど、オーディオデータの転送に必要な帯域幅が大きくなり、サーバーの CPU にも負担がかかります。オーディオデータを圧縮すると、セッションのパフォーマンスと音質とのバランスを考慮しながら、ユーザーの操作感を最適化できます。これを行うには、サウンドファイルに適用する圧縮レベルを制御するには、Citrix ポリシーを使用します。

デフォルトでは、TCP トランスポート使用時の ［音質］ポリシー設定は［高 - 高品位オーディオ］に設定されています。UDP トランスポート使用時（推奨）は［中 - スピーチに最適化］に設定されています。高品位オーディオ設定では HiFi ステレオオーディオが提供されますが、ほかの品質設定よりも多くの帯域幅が消費されます。最適化されていないボイスチャットアプリケーションやビデオチャットアプリケーション（ソフトフォンなど）では、この音質を使用しないでください。リアルタイム通信に適していないオーディオパスに遅延が発生する可能性があるためです。選

択されたトランスポートプロトコルに関係なく、リアルタイムオーディオには「スピーチに最適化」ポリシー設定をお勧めします。

衛星、ダイヤルアップ接続など帯域幅が制限されている場合、音質を ［低］に設定することで、帯域幅の消費を最小限に抑えることができます。この状況では、低帯域幅接続のユーザーに対して別のポリシーを作成し、高帯域幅接続のユーザーに影響しないようにします。

設定について詳しくは、「オーディオのポリシー設定」を参照してください。ユーザーデバイス側の［クライアント側オーディオ設定］が有効になっていることを確認してください。

オーディオの再生と録音の帯域幅ガイドライン:

- アダプティブオーディオ（デフォルト）
  - ビットレート：バリアブルアダプティブ
  - チャンネル数：再生用 2（ステレオ）、マイクキャプチャ用 1（モノラル）
  - 周波数：48000Hz
  - ビット深度：16 ビット
- 高品質
  - ビットレート：再生では約 100kbps（最小 75、最大 175kbps）、マイクキャプチャでは約 70kbps
  - チャンネル数：再生用 2（ステレオ）、マイクキャプチャ用 1（モノラル）
  - 周波数：44100Hz
  - ビット深度：16 ビット
- 中品質（VoIP 用に推奨）
  - ビットレート：再生では約 16kbps（最小 20、最大 40kbps）、マイクキャプチャでは約 16kbps
  - チャンネル数：再生とキャプチャの両方で 1（モノラル）
  - 周波数：16000Hz（ワイドバンド）
  - ビット深度：16 ビット
- 低品質
  - ビットレート：再生では約 11kbps（最小 10、最大 25kbps）、マイクキャプチャでは約 11kbps
  - チャンネル数：再生とキャプチャの両方で 1（モノラル）
  - 周波数：8000Hz（狭帯域）
  - ビット深度：16 ビット

クライアントオーディオリダイレクト

サーバー上で実行しているアプリケーションからユーザーデバイス上のスピーカーまたはサウンドデバイスでオーディオが再生されるようにするには、［クライアントオーディオリダイレクト］設定を ［許可］のままにしておきます。これがデフォルトの設定です。

クライアントオーディオマッピングを使用すると、サーバーとネットワークに大きな負荷がかかります。ただし、［クライアントオーディオリダイレクト］設定で［禁止］を選択すると、すべての HDX オーディオ機能が無効になります。

設定について詳しくは、「オーディオのポリシー設定」を参照してください。ユーザーデバイス側の［クライアント側オーディオ設定］が有効になっていることを確認してください。

クライアントマイクリダイレクト

ユーザーデバイス上のマイクなどのサウンド入力デバイスを使って録音できるようにするには、［クライアントマイクリダイレクト］設定をデフォルトのまま（［許可］）にします。

セキュリティ上の理由から、ユーザーデバイスとの信頼関係が設定されていないサーバーがマイクを使用しようとすると、警告メッセージが表示されます。ユーザーは、マイクを使用する前にアクセスを許可するか拒否するかを選択できます。この警告は、ユーザーが Citrix Workspace アプリ側で無効にできます。

設定について詳しくは、「オーディオのポリシー設定」を参照してください。ユーザーデバイス側の［クライアント側オーディオ設定］が有効になっていることを確認してください。

オーディオプラグアンドプレイ

ポリシーの［オーディオプラグアンドプレイ］設定では、録音やサウンド再生のための複数のオーディオデバイスの使用を許可または禁止します。この設定項目は、デフォルトで［有効］になっています。［オーディオプラグアンドプレイ］の機能を使用すると、ユーザーのセッションが開始されるまでプラグを差し込んだ状態にしなくても、オーディオデバイスを認識できます。

この設定項目は、Windows マルチセッション OS マシンのみに適用されます。

設定について詳しくは、「オーディオのポリシー設定」を参照してください。

オーディオリダイレクトの最大帯域幅（**Kbps**）とオーディオリダイレクトの最大帯域幅（**%**）

ポリシーの［オーディオリダイレクトの最大帯域幅（Kbps）］設定では、クライアント側デバイスによるオーディオの再生や録音で使用可能な最大帯域幅を、キロビット/秒（Kbps）単位で指定します。

ポリシーの［オーディオリダイレクトの最大帯域幅（%）］設定では、クライアント側デバイスによるオーディオの再生や録音で使用可能な最大帯域幅を、セッション全体に対する割合で指定します。

これらの設定には、デフォルトで 0 が指定されており、帯域幅に制限はありません。両方の設定を構成した場合、より高い制限（より小さい値）の設定が適用されます。

設定について詳しくは、「帯域幅のポリシー設定」を参照してください。ユーザーデバイス側の［クライアント側オーディオ設定］が有効になっていることを確認してください。

UDP でのオーディオリアルタイムトランスポートとオーディオ UDP ポートの範囲

ポリシーの［UDP でのオーディオリアルタイムトランスポート］設定は、デフォルトで［有効］が選択されています(インストール時に選択した場合)。これにより、サーバーの UDP ポートが開き、［UDP でのオーディオリアルタイムトランスポート］設定が有効な接続でそのポートが使用されます。ネットワークで輻輳やパケット損失が生じる場合、最適なユーザーエクスペリエンスを提供するために、オーディオの UDP/RTP を構成することをお勧めします。ソフトフォンアプリケーションなどのリアルタイムオーディオでは、EDT より UDP オーディオが優先されます。UDP は再送のないパケット損失が認められており、パケット損失が頻繁な場合でも接続に遅延が発生しません。

> 重要:
>
> Citrix Gateway がパス上にない場合、UDP で転送されるオーディオデータは暗号化されません。Citrix Gateway が Citrix Virtual Apps and Desktops のリソースにアクセスするよう構成されている場合、エンドポイントデバイスと Citrix Gateway 間のオーディオトラフィックは DTLS プロトコルで保護されます。

ポリシーの［オーディオ UDP ポートの範囲］設定では、Windows VDA でユーザーデバイスとのオーディオパケットデータの送受信に使用されるポート番号の範囲を指定します。

デフォルトでは、16500～16509 の範囲が指定されています。

> 注:
>
> アダプティブオーディオに UDP でのオーディオリアルタイムトランスポートが必要ない場合は、ポリシー設定を［無効］に設定することをお勧めします。これにより、Citrix Workspace アプリクライアントが UDP 接続を要求したり、Citrix Workspace アプリクライアントのファイアウォール構成ダイアログウィンドウが必要ではない場合に開いたりするのを防ぐことができます。

［UDP でのオーディオリアルタイムトランスポート］について詳しくは、「オーディオポリシーの設定」を参照してください。［オーディオ UDP ポートの範囲］について詳しくは、「マルチストリーム接続のポリシー設定」を参照してください。ユーザーデバイス側の［クライアント側オーディオ設定］が有効になっていることを確認してください。

UDP を使用したオーディオには、Windows VDA が必要です。Linux VDA でサポートされているポリシーについては、「ポリシーサポート一覧」を参照してください。

ユーザーデバイス側のオーディオ設定ポリシー

1. 「グループポリシーオブジェクトテンプレート管理用テンプレートの構成」の手順に従って、グループポリシーテンプレートをロードします。
2. グループポリシーエディターで、［管理用テンプレート］**>** ［**Citrix Components**］**>** ［**Citrix Workspace**］**>** ［ユーザーエクスペリエンス］の順に開きます。
3. ［**Client audio settings**］を開き、［**Not Configured**］、［**Enabled**］、または［**Disabled**］をクリックします。

    - **Not Configured**。デフォルトでは、オーディオリダイレクトは高品質オーディオ、または以前に構成したカスタムのオーディオ設定で有効になります。

- **Enabled**。オーディオリダイレクトは、選択したオプションで有効になります。
- 無効。オーディオリダイレクトは無効化されます。

4. [**Enabled**] をクリックした場合は、音質を選択します。UDP オーディオでは、[中]（デフォルト）を使用してください。
5. UDP オーディオでは、[**Enable Real-Time Transport**] チェックボックスをオンにして、ローカルの Windows ファイアウォールを通過するための着信ポートの範囲を指定します。
6. Citrix Gateway で UDP オーディオを使用するには、[**Allow Real-Time Transport Through gateway**] チェックボックスをオンにします。Citrix Gateway で DTLS を構成します。詳しくは、こちらの記事を参照してください。

エンドポイントデバイスで上記の変更を行う制御権を持っていない場合、管理者として StoreFront の default.ica 属性を使用して UDP オーディオを有効にします。たとえば、自分のデバイスや家庭のコンピューターを持ち込む場合などです。

1. StoreFront マシンで、メモ帳などのエディターを使用して C:\inetpub\wwwroot\Citrix\< ストア名 >\App_Data\default.ica を開きます。ストア名 >
2. [アプリケーション] セクションで以下の項目を入力します。

   ; リアルタイム転送を有効にします

   EnableRtpAudio=true

   ; ゲートウェイを介したリアルタイム転送を有効にします

   EnableUDPThroughGateway=true

   ;Audio quality を「Medium」に設定します

   AudioBandwidthLimit=1

   ;UDP ポートの範囲を表します

   RtpAudioLowestPort=16500

   RtpAudioHighestPort=16509

ユーザーデータグラムプロトコル（UDP）オーディオは、default.ica の編集で有効になっている場合、そのストアを使用するすべてのユーザーに対して有効化されます。

マルチメディア会議でのエコーの解消

オーディオまたはビデオ会議にユーザーが参加したときに、音声にエコーがかかって聞こえることがあります。通常、この問題はスピーカーとマイクが近すぎる場合に発生します。このため、オーディオまたはビデオ会議ではヘッドセットを使用することをお勧めします。

HDX には、会議中のエコーを最小限に抑えるためのエコーキャンセル機能が用意されており、デフォルトで有効になっています。エコーキャンセル機能の効果は、スピーカーとマイクとの距離により異なります。デバイスが互いに近すぎたり遠すぎたりしないように注意してください。

エコーキャンセル機能を無効にするには、レジストリ設定を変更します。詳しくは、レジストリを介して管理される機能の一覧にある「マルチメディア会議でのエコーの解消」を参照してください。

ソフトフォン

ソフトフォンは、電話インターフェイスとして動作するソフトウェアです。コンピューターや他のスマートデバイスからインターネット経由で電話するには、ソフトフォンを使用します。ソフトフォンを使うことにより、画面を使って電話番号をダイヤルしたり、他の電話関連の機能を実行したりできます。

Citrix Virtual Apps and Desktops は、ソフトフォンの配信に対するいくつかの代替手段をサポートします。

- 制御モード。ホストされたソフトフォンが物理的な電話セットを制御します。このモードでは、Citrix Virtual Apps and Desktops サーバーを通過するオーディオトラフィックはありません。
- **HDX RealTime** に最適化されたソフトフォンのサポート（推奨）。このメディアエンジンはユーザーデバイス上で実行され、ボイスオーバー IP トラフィックがピアツーピアで流れます。たとえば、以下を参照してください：
  - Microsoft Teams の HDX 最適化
  - Microsoft Skype for Business の配信を最適化するHDX RealTime Optimization Pack
  - Cisco Jabber Softphone for VDI（旧称 VXME）
  - Cisco Webex Meetings for VDI
  - Avaya VDI Equinox（旧称 VDI Communicator）
  - Zoom VDI プラグイン
  - Genesys PureEngage Cloud
  - Nuance Dragon PowerMic ディクテーションデバイス
- ローカルアプリケーションアクセス。Citrix Virtual Apps and Desktops の機能により、ソフトフォンなどのアプリケーションは、Windows ユーザーのデバイス上ではローカルで実行されますが、その仮想/公開デスクトップとはシームレスに統合されています。これにより、ユーザーデバイスへのすべてのオーディオ処理の負荷が軽減されます。詳しくは、「ローカルアプリアクセスと URL リダイレクト」を参照してください。
- **HDX RealTime** の汎用ソフトフォンのサポート。ICA を介したボイスオーバー IP。

汎用ソフトフォンのサポート

汎用ソフトフォンのサポートにより、データセンターの XenApp または XenDesktop 上に、未変更のソフトフォンをホストすることができます。オーディオトラフィックは、Citrix ICA プロトコルを介して（UDP/RTP を優先的に使用して）、Citrix Workspace アプリを実行しているユーザーデバイスに送信されます。

汎用ソフトフォンのサポートは、HDX RealTime の機能です。ソフトフォンの配信に対するこのアプローチは、以下の場合に特に有効です。

- ソフトフォンの配信に最適なソリューションがなく、ローカルアプリケーションアクセスが可能な Windows デバイス上にユーザーがいない。
- ソフトフォンの最適化された配信に必要とされるメディアエンジンが、ユーザーデバイスにインストールされていないか、ユーザーデバイス上で実行しているオペレーティングシステムのバージョンで利用できない。このシナリオでは、汎用 HDX RealTime が価値のあるフォールバックソリューションを提供します。

Citrix Virtual Apps and Desktops を使用したソフトフォンの配信には、考慮事項が 2 つあります:

- ソフトフォンアプリケーションがどのように仮想/公開デスクトップに配信されるか。
- ユーザーのヘッドセット、マイクロフォン、およびスピーカー、または USB 電話セット間でオーディオがどのように配信されるか。

Citrix Virtual Apps and Desktops には、汎用ソフトフォンの配信をサポートする多くのテクノロジが含まれています:

- リアルタイムオーディオの高速エンコードと帯域幅の効率性のための、スピーチに最適化されたコーデック。
- 遅延の少ないオーディオスタック。
- ネットワーク遅延が変動する場合、オーディオをスムーズにするサーバー側のジッターバッファー。
- QoS のパケットのタグ付け（DSCP および WMM）
  - RTP パケットの DSCP タグ付け（レイヤー 3）
  - WiFi の WMM タグ付け

Windows、Linux、Chrome、および Mac 向けの Citrix Workspace アプリの各バージョンは、ボイスオーバー IP にも対応しています。Windows 向け Citrix Workspace アプリは以下の機能を提供します:

- クライアント側のジッターバッファー - ネットワーク遅延が変動する場合でもオーディオを確実にスムーズにします。
- エコーキャンセル - ヘッドセットを使用しないユーザー向けに、マイクとスピーカの距離を調整します。
- オーディオプラグアンドプレイ - オーディオデバイスは、セッション開始前にプラグインする必要はありません。いつでもプラグインできます。
- オーディオデバイスルーティング - ユーザーはヘッドセットの音声通信以外に、スピーカーに着信音を直接送信できます。
- マルチストリーム ICA - ネットワーク上で柔軟なサービス品質ベースのルーティングを有効にします。
- ICA は、4 つの TCP と 2 つの UDP ストリームをサポートします。UDP ストリームの 1 つは、RTP 上でリアルタイムオーディオをサポートします。

Citrix Workspace アプリの機能の概要については、『Citrix Receiver Feature Matrix』を参照してください。

システム構成の推奨事項

クライアントのハードウェアとソフトウェア: 音質の最適化のために、最新バージョンの Citrix Workspace アプリとアコースティックエコーキャンセル（AEC）付きの高品質なヘッドセットをお勧めします。
Windows、Linux、および Mac 向けの Citrix Workspace アプリの各バージョンは、ボイスオーバー IP に対応しています。また、Dell Wyse は ThinOS（WTOS）のボイスオーバー IP サポートを提供します。

CPU 検討事項：VDA 上の CPU 使用率を監視して、それぞれの仮想マシンに 2 つの仮想 CPU を割り当てる必要があるかどうかを決定します。
リアルタイムの音声およびビデオはデータ量が多いです。2 つの仮想 CPU を構成すると、スレッドの切り替え遅延を減らすことができます。そのため、Citrix Virtual Desktops VDI 環境で 2 つの vCPU を構成することをお勧めします。

物理 CPU はセッションを超えて共有できるため、2 つの仮想 CPU を持つことは、必ずしも物理 CPU の数を倍にすることではありません。

セッション画面の保持機能に使われる Citrix Gateway Protocol（CGP）により、CPU の消費も増加します。高品質のネットワーク接続では、この機能を無効にして、VDA の CPU 消費を削減することができます。前述のいずれの手順も、強力なサーバーでは必要ないかもしれません。

UDP オーディオ：UDP によるオーディオは、ネットワークの輻輳やパケット損失に対する強力な耐性を提供します。利用できるのであれば、TCP から代えることをお勧めします。

LAN/WAN の設定：ネットワークの適切な設定は、リアルタイムオーディオの高い品質にはきわめて重要です。
通常、過度のブロードキャストパケットはジッターを発生させる場合があるため、仮想 LAN（VLAN）を構成する必要があります。IPv6 が有効なデバイスでは、大量のブロードキャストパケットが発生する場合があります。IPv6 のサポートが不要な場合は、それらのデバイスで IPv6 を無効にできます。QoS（サービス品質）をサポートするように構成してください。

WAN 接続使用時の設定：LAN および WAN 接続を経由したボイスチャットを使用できます。
WAN 接続では、音質は接続の遅延、パケット損失、およびジッターにより異なります。WAN 接続を経由してソフトフォンを配信する場合、データセンターとリモートオフィス間には NetScaler SD-WAN を使用することをお勧めします。これにより、高いサービス品質が維持されます。NetScaler SD-WAN は、UDP を含むマルチストリーム ICA をサポートします。また、単一の TCP ストリームの場合は、さまざまな ICA 仮想チャネルの優先度を識別し、優先度の高いリアルタイムの音声データを優先的に扱うことができます。

HDX 構成を検証するには、Director またはHDX Monitorを使用してください。

リモートユーザーの接続：Citrix Gateway は DTLS をサポートし、UDP/RTP トラフィックをネイティブに（TCP でカプセル化せずに）送信します。

ポート 443 を介した UDP トラフィックに対してファイアウォールを双方向に開きます。

コーデックの選択と帯域幅の消費：
ユーザーデバイスとデータセンターの VDA 間には、中品質オーディオとも呼ばれる、スピーチに最適化されたコーデック設定を使用することをお勧めします。VDA プラットフォームと IP-PBX 間では、ソフトフォンは構成またはネゴシエートされたコーデックを使用します。例：

- G711 の音質は高いものの、通話で 1 秒あたり 80〜100 キロビットの帯域幅（ネットワークのレイヤー 2 のオーバーヘッドにより異なる）が必要になります。
- G729 の音質は高く、通話で 1 秒あたり 30〜40 キロビットの低帯域幅（ネットワークのレイヤー 2 のオーバーヘッドにより異なる）が必要になります。

ソフトフォンアプリケーションの仮想デスクトップへの配信

XenDesktop 仮想デスクトップにソフトフォンを配信するには、次の 2 つの方法があります。

- アプリケーションは、仮想デスクトップイメージにインストールできます。
- アプリケーションは、Microsoft App-V を使用して、仮想デスクトップにストリーム配信できます。このアプローチでは、仮想デスクトップイメージに手が加えられないため、管理上の利点があります。仮想デスクトップにストリーム配信された後、アプリケーションはその環境で、通常の方法でインストールされたかのように実行されます。すべてのアプリケーションが App-V 互換であるわけではありません。

ユーザーデバイスとのオーディオの配信

汎用 HDX RealTime は、ユーザーデバイスとのオーディオの配信を次の 2 つの方法でサポートします。

- **Citrix** オーディオ仮想チャネル。オーディオ転送専用に設計されているため、通常は Citrix オーディオ仮想チャネルをお勧めします。
- 汎用 **USB** リダイレクト。ユーザーデバイスが Citrix Virtual Apps and Desktops サーバーへの LAN または LAN のような接続上にある場合は、ボタンまたはディスプレイ（またはその両方）などのヒューマンインターフェイスデバイス（HID）を持つオーディオデバイスをサポートします。

Citrix オーディオ仮想チャネル

双方向の Citrix オーディオ仮想チャネル（CTXCAM）は、ネットワーク上でオーディオを効率的に配信することができます。汎用 HDX RealTime は、ユーザーのヘッドセットまたはマイクからオーディオを取り出して圧縮します。その後、ICA 経由で仮想デスクトップ上のソフトフォンアプリケーションに送信します。同様に、ソフトフォンのオーディオ出力も圧縮され、ユーザーのヘッドセットまたはスピーカーに向けて反対方向に送信されます。この圧縮は、ソフトフォン自体で使われる圧縮（G.729、G.711 など）とは関係ありません。スピーチに最適化されたコーデック（中品質）で行われます。その特性はボイスオーバー IP に最適です。高速エンコード機能を備え、ピーク時でもおよそ 1 秒間に 56 キロビット（それぞれの方向で 28Kbps ずつ）しかネットワーク帯域幅を消費しません。このコーデックはデフォルトのオーディオコーデックではないため、Studio のコンソールで明示的に選択する必要があります。デフォルトは、HD オーディオコーデック（高品質）です。このコーデックは HiFi ステレオ録音には最適ですが、スピーチに最適化されたコーデックと比較してエンコードが遅くなります。

汎用 ***USB*** リダイレクト

Citrix 汎用 USB リダイレクトテクノロジ（CTXGUSB 仮想チャネル）は、複合デバイス（オーディオプラス HID）とアイソクロナス USB デバイスを含む、USB デバイスのリモート処理に一般的な手段を提供します。このアプローチは LAN 接続のユーザーに制限されます。USB プロトコルはネットワークの遅延に影響を受けやすく、相当量のネットワーク帯域幅を必要とするためです。ソフトフォンによっては、アイソクロナス USB リダイレクトが有効です。このリダイレクトは、優れた音声品質と低遅延を実現します。ただし、オーディオトラフィックに最適化されているため、Citrix オーディオ仮想チャネルが優先されます。主な例外は、ボタンが付いたオーディオデバイスを使う場合です。たとえば、データセンターに LAN 接続されているユーザーデバイスに取り付けられた USB 電話などです。この場合は、汎用 USB リダイレクトが、信号をソフトフォンに送ることで機能を制御する電話セットまたはヘッドセットのボタンをサポートします。デバイス上でローカルに動作するボタンでは問題ありません。

オーディオ診断コマンドラインツール

VDA 上のオーディオ診断コマンドラインツールを使用して、オーディオ ポリシー、構成、データ転送に関連するセッション データを照会できます。

使用状況

コマンドプロンプトを開き、`C:\Program Files\Citrix\HDX\bin`フォルダーから`CtxAudio.exe`を実行します。

- 管理者としてツールを実行すると、アクティブな ICA セッションのオーディオ情報がすべて表示されます。
- 非管理者としてツールを実行すると、現在のユーザーの ICA セッションのオーディオ情報が表示されます。

出力

このツールは、セッション内のオーディオ関連の問題の診断に役立つさまざまな構成設定を出力します。

セクション	説明
Policy information（ポリシー情報）	現在のセッションに適用されるオーディオポリシー。
Settings information（設定情報）	レジストリに保存されるオーディオ関連の構成設定。
State information（状態情報）	現在のセッションに適用されるオーディオの状態、バージョン、コーデック、および転送。
Devices information（デバイス情報）	セッションで使用されるデバイス名、その役割およびステータス。

> 注:
>
> 出力は、ツールをマルチセッション（TS）VDA で実行するか、シングルセッション VDA（WSVDA）で実行するかによって異なります。

制限事項

クライアントにオーディオデバイスをインストールし、オーディオリダイレクトを有効にして、RDS セッションを開始します。オーディオファイルが再生されず、エラーメッセージが表示されることがあります。

回避策として、レジストリキーを RDS マシンに追加し、マシンを再起動します。詳しくは、レジストリを介して管理される機能の一覧にある「オーディオ制限」を参照してください。

ブラウザーコンテンツリダイレクト

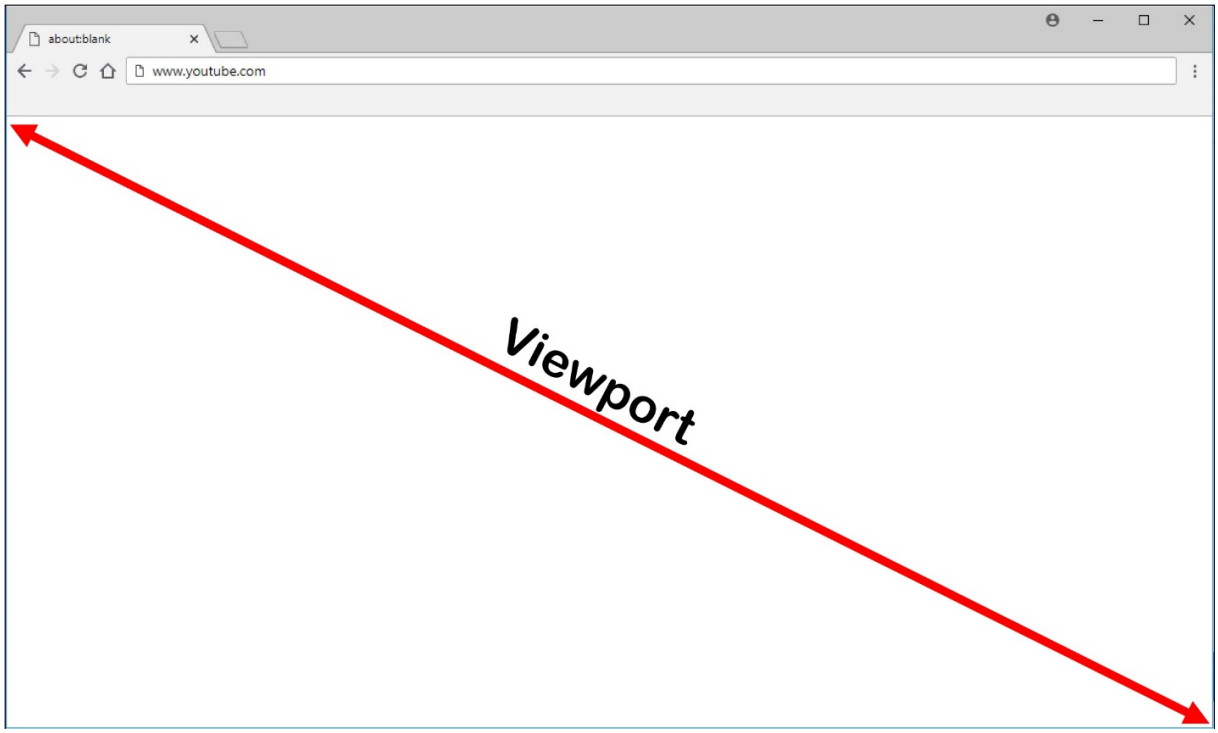
August 17, 2024

ブラウザーコンテンツリダイレクトによって、VDA 側の許可リストに登録された Web ページのレンダリングができません。この機能は、Windows 向け Citrix Workspace アプリと Linux 向け Citrix Workspace アプリを使用して、クライアント側の対応するレンダリングエンジンをインスタンス化し、URL から HTTP および HTTPS コンテンツを取得します。

> 注:
>
> 禁止リストを使用することで、Web ページを VDA 側にリダイレクトする（クライアント側ではリダイレクトされない）ように指定できます。

このオーバーレイ Web レイアウトエンジンは、VDA 上ではなくエンドポイントデバイス上で実行され、エンドポイントの CPU、GPU、RAM、およびネットワークを使用します。

ブラウザーのビューポートだけがリダイレクトされます。ビューポートは、コンテンツが表示されるブラウザー内の長方形の領域です。ビューポートには、アドレスバー、お気に入りツールバー、ステータスバーなどは含まれません。これらの項目はユーザーインターフェイス内にあり、リダイレクト時も VDA のブラウザーで実行されます。



1. リダイレクト用に許可リストに登録された URL、または特定の URL パスのリダイレクトを無効にする禁止リストを含む、アクセス制御リストを指定する Studio ポリシーを構成します。ユーザーがナビゲートしている URL が許可リストと一致することや禁止リストと一致しないことを、VDA 上のブラウザーで検出するために、ブラウザーの拡張機能によって比較が実行されます。Chrome 向けのブラウザー拡張機能は Chrome ウェブ

ストアで提供されており、グループポリシーと ADMX ファイルを使用して展開できます。Chrome の拡張機能は、ユーザーごとにインストールします。拡張機能を追加または削除する場合に、ゴールデンイメージを更新する必要はありません。Microsoft Edge の場合、拡張機能は直接利用できません。Chrome ストアの拡張機能を見つけてインストールできるようにする必要があります。

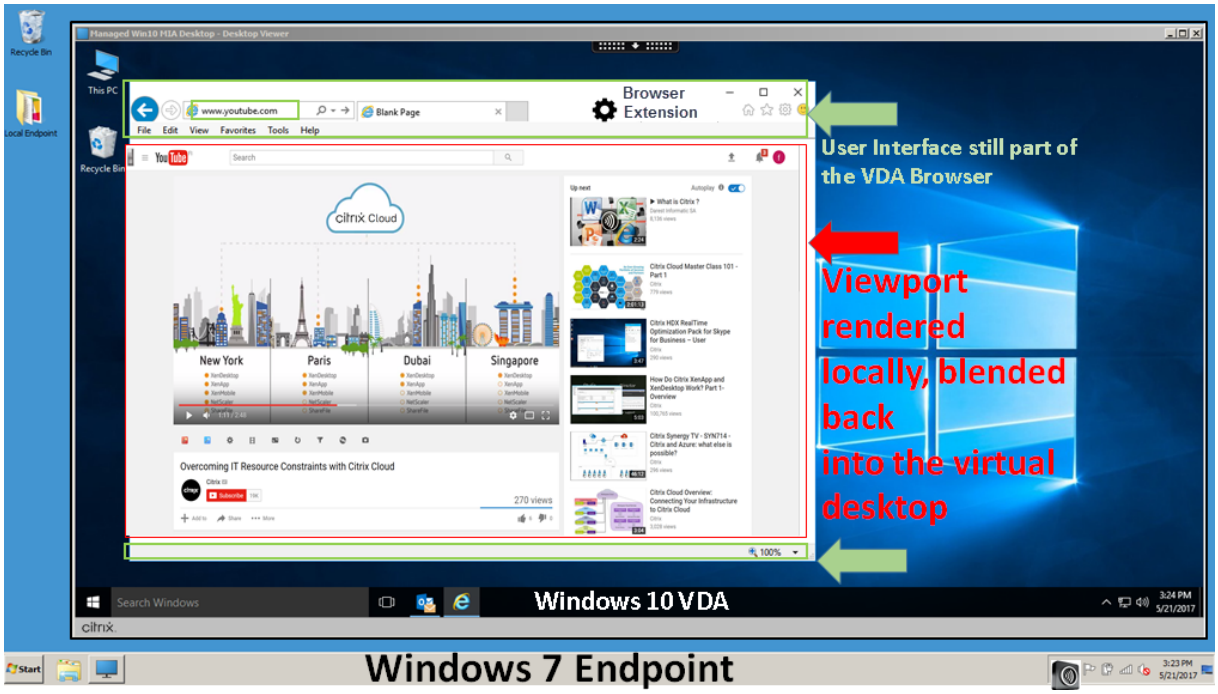
2. 許可リスト内に一致するものがあり（例：`https://www.mycompany.com/`）、禁止リスト内の URL と一致するもの（例：`https://www.mycompany.com/engineering`）がない場合、仮想チャネル（CTXCSB）は、リダイレクトが必要であることを Citrix Workspace アプリに指示し、URL をリレーします。Citrix Workspace アプリは、ローカルレンダリングエンジンをインスタンス化し、Web サイトを表示します。
3. Citrix Workspace アプリは、Web サイトを仮想デスクトップブラウザーのコンテンツ領域にシームレスにブレンドします。

> 注：
>
> ブラウザーコンテンツリダイレクト拡張機能の新機能と修正について詳しくは、Chrome ウェブストアにアクセスし、「`citrix bcr`」で検索して、この拡張機能の説明を参照してください。

ロゴの色は、Chrome 拡張機能のステータスを指定します。それは、以下の 3 つの色のいずれかです：

- 緑：アクティブで接続されています。
- グレー：現在のタブではアクティブではないかアイドル状態です。
- 赤：壊れているか動作していません。

拡張機能メニューの ［オプション］を使用して、ログをデバッグできます。



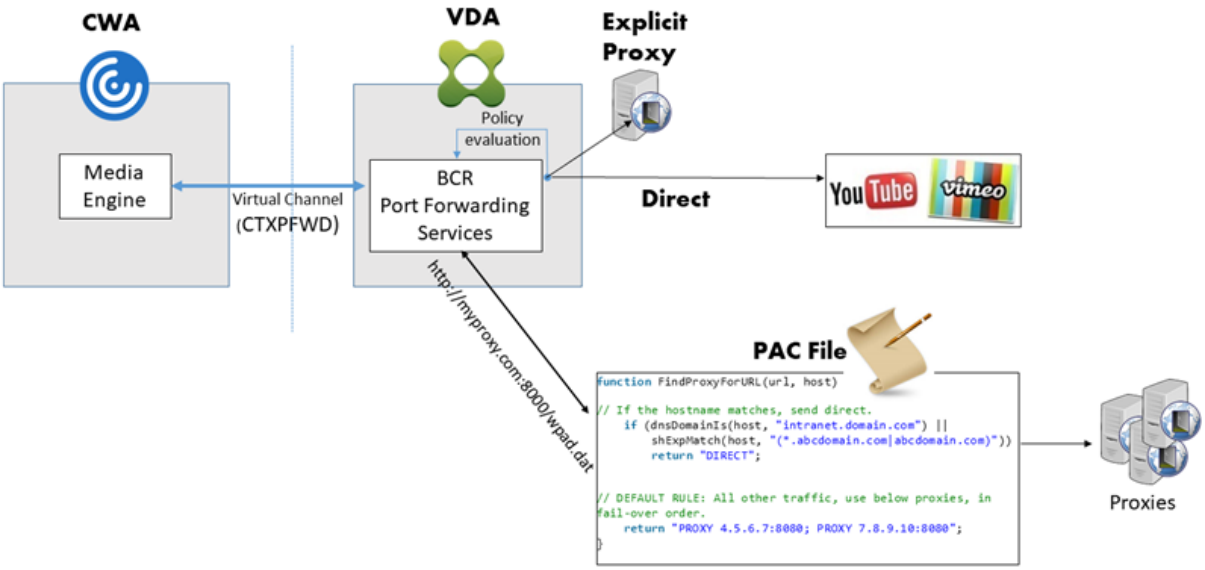
Citrix Workspace アプリがコンテンツをどのようにフェッチするかのシナリオを次に示します：

- サーバーフェッチとサーバーレンダリング：サイトを許可リストに登録していないか、リダイレクトに失敗したため、リダイレクトはありません。VDA 上での Web ページのレンダリングに戻り、Thinwire を使用してグラフィックスを遠隔操作します。ポリシーを使用してフォールバックの動作を制御します。VDA での CPU、RAM、および帯域幅の消費量が多い
- サーバーフェッチとクライアントレンダリング：Citrix Workspace アプリは仮想チャネル（CTXPFWD）を使用して、Web サーバーから VDA を通じてコンテンツに接続し、フェッチします。このオプションは、クライアントにインターネットアクセスがない場合（シンクライアントなど）に便利です。VDA では CPU と RAM の消費量は少なくなりますが、ICA 仮想チャネルでは帯域幅が消費されます。

  このシナリオには 3 つの動作モードがあります。プロキシという用語は、VDA がインターネットアクセスのためにアクセスするプロキシデバイスを意味します。

  選択可能なポリシーオプション：

  - **Explicit Proxy** - データセンターに単一の明示的なプロキシがある場合。
  - **Direct or Transparent** - プロキシがない場合、または透過プロキシを使用している場合。
  - **PAC files** - PAC ファイルに依存して、指定された URL のフェッチに VDA のブラウザーが適切なプロキシサーバーを自動で選択できる場合。

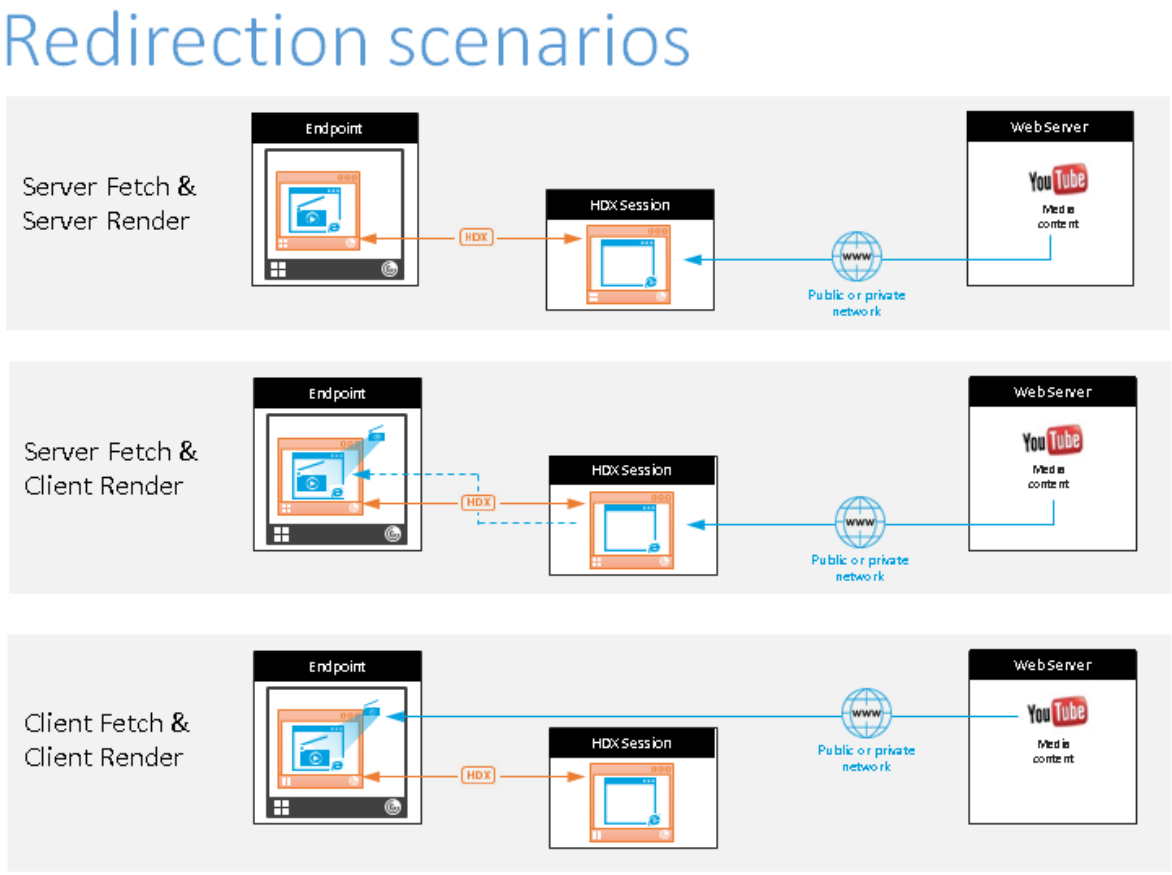


- クライアントフェッチとクライアントレンダリング：Citrix Workspace アプリは Web サーバーに直接接続するため、インターネットにアクセスする必要があります。このシナリオでは、XenApp および XenDesktop サイトからネットワーク、CPU、および RAM の使用量をすべてオフロードします。

  長所：

  - エンドユーザーエクスペリエンスの向上（アダプティブビットレート（ABR））

- VDA リソース使用量の削減（CPU/RAM/IO）
- 消費帯域幅の削減



フォールバックのメカニズム:

クライアントのリダイレクトが失敗することがあります。たとえば、クライアントマシンでインターネットに直接アクセスできない場合、エラー応答が VDA に返される可能性があります。このような場合、VDA 上のブラウザーは、サーバー上のページをリロードしてレンダリングできます。

既存の［**Windows** メディアフォールバック防止］ポリシーを使用することで、ビデオ要素のサーバーレンダリングを抑制できます。このポリシーを、［クライアントにあるすべてのコンテンツのみを再生］または［クライアント上のクライアントがアクセスできるコンテンツのみを再生］に設定します。これらの設定は、クライアントのリダイレクトが失敗した場合に、サーバー上でのビデオ要素の再生を禁止します。このポリシーは、Web ブラウザーコンテンツリダイレクトが有効になっており、［アクセス制御リスト］ポリシーにフォールバックする URL がある場合にのみ有効です。URL を禁止リストポリシーで指定することはできません。

システム要件

Citrix Virtual Apps and Desktops

- Citrix Virtual Apps and Desktops 7 1808 以降

- XenApp および XenDesktop 7.15 CU5 以降
- VDA OS：Windows 10 および 11、Windows Server 2016/2019/2022
- VDA 上のブラウザー：
  - 最新バージョンの Google Chrome
  - 最新バージョンの Microsoft Edge
- Chrome ウェブストアから VDA のブラウザーにインストールされた BCR 拡張機能

Windows endpoints

- Windows 10 および 11
- Windows 向け Citrix Workspace アプリ 1809 以降

> 注：
>
> ブラウザーコンテンツリダイレクトは、Citrix Workspace アプリ LTSR リリース 1912 および 2203.1 ではサポートされていません。

Linux エンドポイント

- Linux 向け Citrix Workspace アプリ 1808 以降
- シンクライアント端末には WebKitGTK+ が必要です

Mac エンドポイント（Technical Preview）

- macOS 11 Big Sur
- macOS 12 Monterey
- macOS 13 Ventura
- macOS 14 Sonoma（14.2.1 まで）、Citrix Workspace アプリの最小バージョン 2311

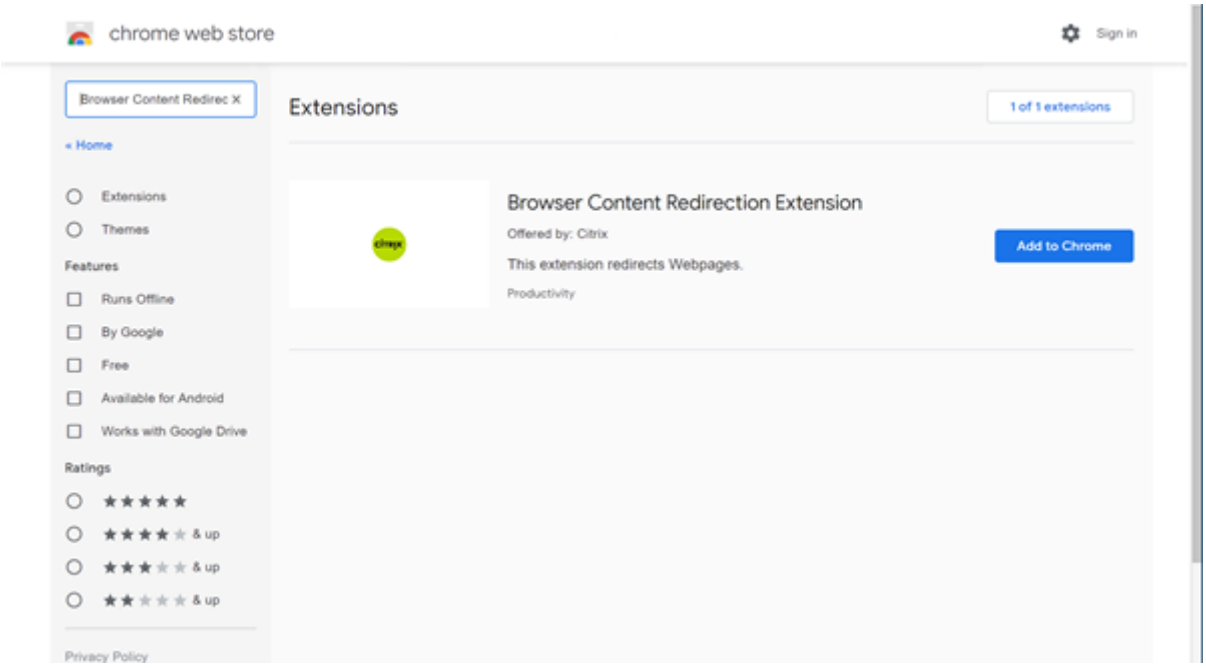
トラブルシューティング

トラブルシューティング情報については、ナレッジセンターの記事「How to troubleshoot browser content redirection」 を参照してください。

Chrome 向けの Web ブラウザーコンテンツリダイレクト拡張機能

Chrome で Web ブラウザーコンテンツリダイレクトを使用するには、Chrome ウェブストアから Browser Content Redirection Extension を追加します。Citrix Virtual Apps and Desktops 環境で、[**Chrome** に追加] をクリックします。

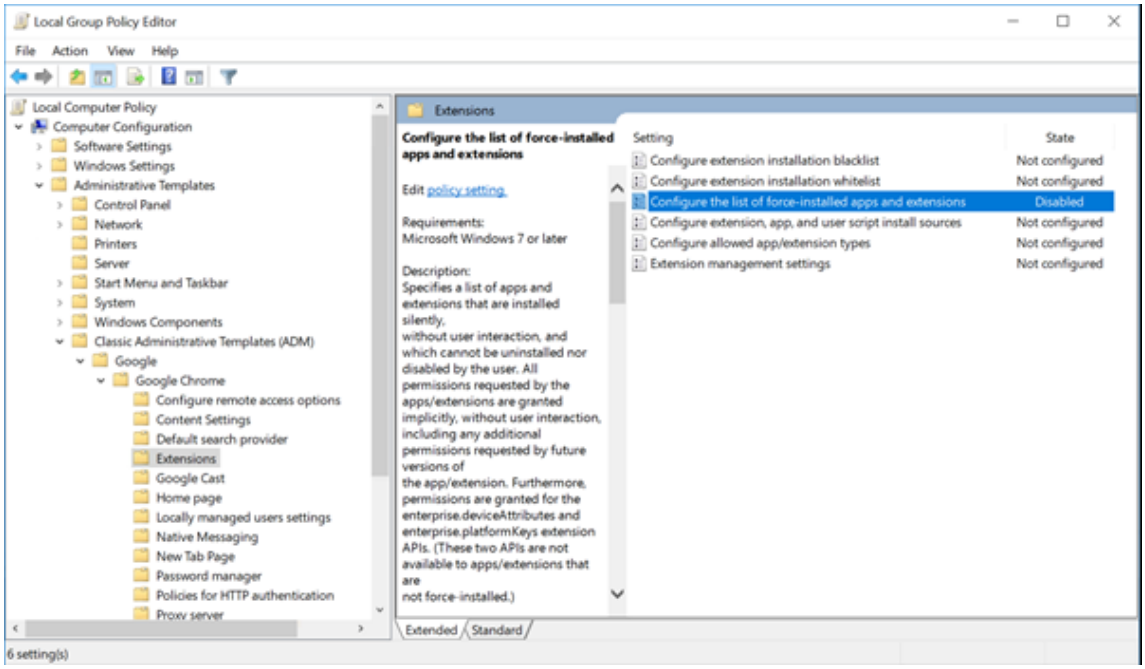
この拡張機能は VDA にのみ必要であり、ユーザーのクライアントマシンには不要です。



この方法は、ユーザーごとに行います。組織内の大規模なユーザーグループにこの拡張機能を展開するには、グループポリシーを使用して展開します。

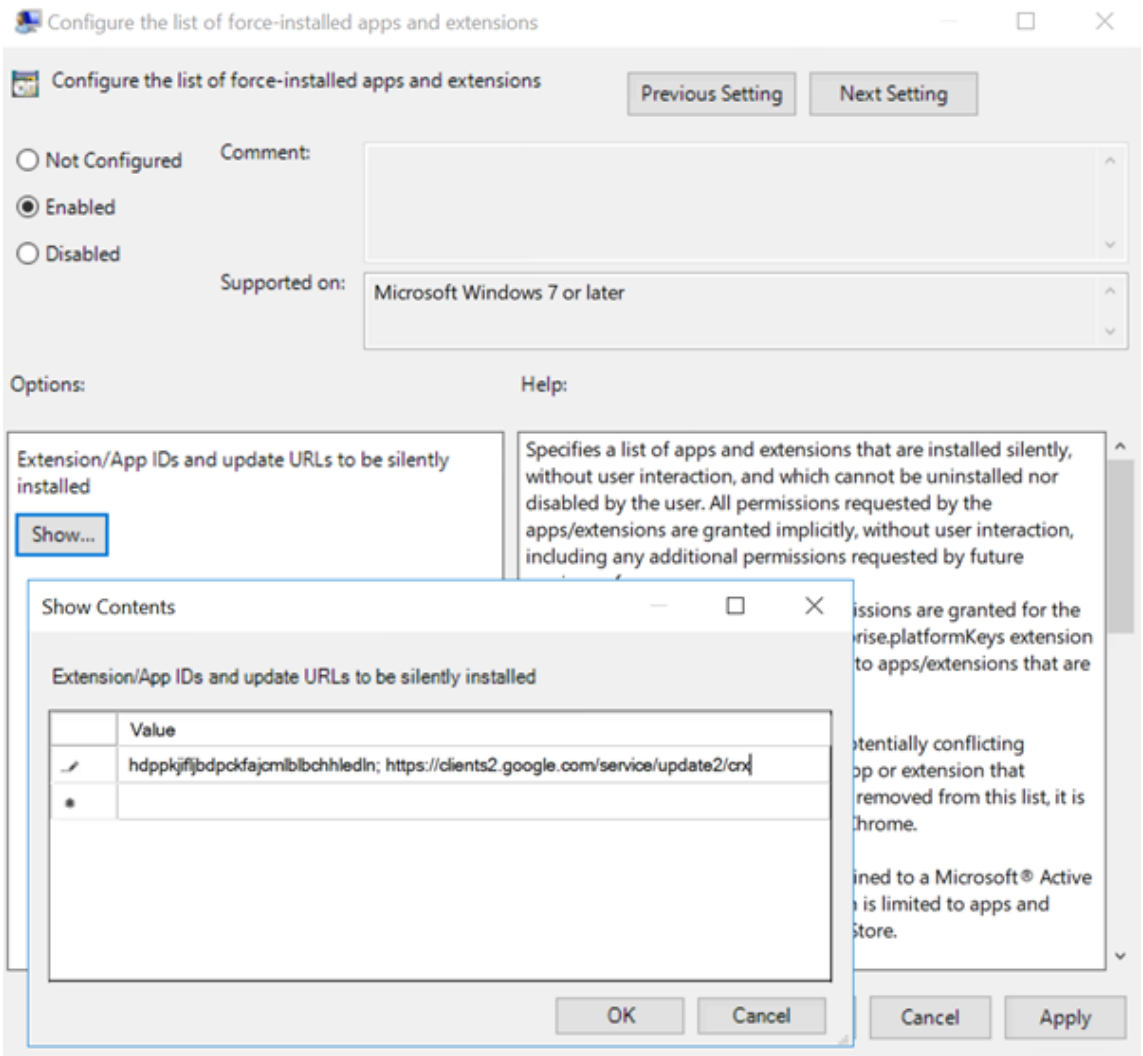
グループポリシーを使用して拡張機能を展開する

1. 現在の環境に Google Chrome ADMX ファイルをインポートします。ポリシーテンプレートをダウンロードしてグループポリシーエディターにインストールし、構成を行う方法については、管理対象パソコンに Chrome ブラウザーのポリシーを設定するを参照してください。
2. グループポリシー管理コンソールを開き、［ユーザーの構成］**>**［管理用テンプレート］**>**［従来の管理用テンプレート（**ADM**）］**>**［**Google**］**>**［**Google Chrome**］**>**［拡張機能］の順に選択します。［強制インストールするアプリと拡張機能のリストを設定します］設定を有効にします。



3. ［表示］をクリックして、拡張機能 ID に対応する文字列と、Browser Content Redirection Extension の更新用 URL を次のように指定します。

   ```
   hdppkjifljbdpckfajcmlblbchhledln; https://clients2.google.com/service/update2/crx
   ```

4. 設定を適用し、**gpudate** が更新されると、ユーザーへこの拡張機能が自動で配信されます。ユーザーのセッションで Chrome ブラウザーを起動すると、この拡張機能が既に適用されています。ユーザーがこの機能を削除することはできません。

   拡張機能の更新は、設定で指定した更新用 URL を通じて、ユーザーのマシンに自動でインストールされます。

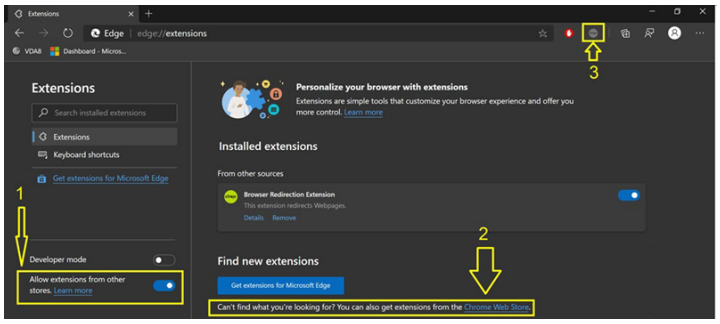
   [強制インストールするアプリと拡張機能のリストを設定します] 設定を [無効] に設定すると、この拡張機能はすべてのユーザーの Chrome から削除されます。

Chromium 版 **Edge** 向けの **Web** ブラウザーコンテンツリダイレクト拡張機能

Edge にブラウザーコンテンツリダイレクト拡張機能をインストールするため、Edge ブラウザーのバージョン **83.0.478.37** 以降がインストールされていることを確認してください。

1. [拡張機能] オプションをクリックします。[拡張機能の管理] を選択します。[他のストアからの拡張機能を許可する] をオンにします。

2. **Chrome** ウェブストアリンクをクリックすると、拡張機能が右上のバーに表示されます。
   Microsoft Edge の拡張機能について詳しくは、「拡張機能」を参照してください。



ブラウザーコンテンツリダイレクトと **DPI**

ユーザーのマシン上で Web ブラウザーコンテンツのリダイレクトの DPI（スケール）を 100% を超えて設定して使用すると、リダイレクトされたブラウザーコンテンツ画面が正しく表示されません。この問題を回避するため、ブラウザーコンテンツリダイレクトを使用するときに DPI を設定しないでください。この問題を回避するもう 1 つの方法は、ユーザーのマシン上でレジストリキーを作成して、Chrome で Web ブラウザーコンテンツのリダイレクトの GPU アクセラレーションを無効にすることです。詳しくは、レジストリを介して管理される機能の一覧にある「ブラウザーコンテンツリダイレクトと DPI」を参照してください。

統合 **Windows** 認証によるシングルサインオン

Web ブラウザーコンテンツリダイレクト機能は、VDA と同じドメイン内の統合 Windows 認証（IWA）で構成された Web サーバーへの認証に **Negotiate** スキームを使用するオーバーレイを拡張します。

Web ブラウザーコンテンツリダイレクトでは、デフォルトで、ユーザーが Web サーバーにアクセスするたびに VDA 資格情報を使って認証することを要求する基本認証スキームを使用します。シングルサインオンの場合、[**Web** ブラウザーコンテンツリダイレクト統合 **Windows** 認証サポート］ポリシー設定を有効にするか、VDA でレジストリキーを作成することができます。

シングルサインオンを有効にする前に、次の手順を完了します:

- ホスト名から構築されたサービスプリンシパル名（SPN）のチケットを発行するように、Kerberos インフラストラクチャを構成します。例: `HTTP/serverhostname.com`。
- サーバーフェッチの場合: サーバーフェッチモードで Web ブラウザーコンテンツリダイレクトを使用する場合は、VDA で DNS が正しく構成されていることを確認してください。
- クライアントフェッチの場合: クライアントフェッチモードで Web ブラウザーコンテンツリダイレクトを使用する場合は、クライアントデバイスで DNS が正しく構成されていること、およびオーバーレイから Web サーバーの IP アドレスへの TCP 接続が許可されていることを確認してください。

Web ブラウザーコンテンツリダイレクトポリシーを使用してシングルサインオンを構成するには、「Web ブラウザーコンテンツリダイレクト統合 Windows 認証サポート」の設定を参照してください。

または、VDA にレジストリキーを追加して、Web サーバーへのシングルサインオンを有効にすることもできます。詳しくは、レジストリを介して管理される機能の一覧にある「Web ブラウザーコンテンツリダイレクトの統合 Windows 認証によるシングルサインオン」を参照してください。

user-agent 要求ヘッダー

user-agent ヘッダーは、ブラウザーコンテンツリダイレクトから送信された HTTP 要求を識別するのに役立ちます。この設定は、プロキシ規則とファイアウォール規則を構成するときに役立ちます。たとえば、サーバーがブラウザーコンテンツリダイレクトから送信された要求を禁止する場合、user-agent ヘッダーを含む規則を作成して、特定の要件をバイパスできます。

Windows デバイスでのみ、user-agent 要求ヘッダーがサポートされています。

デフォルトでは、user-agent 要求ヘッダー文字列は無効になっています。クライアント側でレンダリングされたコンテンツの user-agent ヘッダーを有効にするには、レジストリエディターを使用します。詳しくは、レジストリを介して管理される機能の一覧にある「user-agent 要求ヘッダー」を参照してください。

Web ブラウザーコンテンツリダイレクトとクライアントの互換性

WMI を使用して、ご使用のクライアントが Web ブラウザーコンテンツリダイレクトと互換性があるかどうかを確認できます。WMI にアクセスするいずれかの方法を使用すると機能します。以下は、PowerShell を使用した場合の例です。

1. PowerShell を開きます。
2. `Get-WmiObject -Class CTXBCRStatus`を実行します。
3. `BCR_Capable`パラメーターを確認します。
    - `True`の場合、クライアントは Web ブラウザーコンテンツリダイレクトと互換性があります。
    - `False`の場合、クライアントは Web ブラウザーコンテンツリダイレクトと互換性がありません。

追加情報

- `CtxBrowserSvc`が使用できない場合、コマンドの実行時に結果は表示されません。
- `CtxBrowserSvc`が実行されたことがない場合、結果は無効なクラスエラーを返します。

ブラウザーコンテンツリダイレクトの制限

ブラウザーコンテンツリダイレクトでは、次のユースケースはサポートされません:

- ポップアップウィンドウを必要とする Web アプリケーションはサポートされていません。

- セッション Cookie の保持を必要とする Web アプリケーションもサポートされていません。Google 認証サービスに依存するアプリケーション（Google Meet など）はブロックされる可能性があります。
- 拡張プラグインは、Microsoft Edge ストアで正式に公開されていません。ただし、Chrome ストアを使用して拡張機能をインストールすることはできます。
- ブラウザーコンテンツリダイレクトが使用されている場合は、HTML5 ビデオリダイレクトポリシーを無効にする必要があります。
- ブラウザーコンテンツリダイレクトは、ARMhf（ARM ハード フロート）フレームワークではサポートされていません。
- ネットワークの状態が不安定であったり、待ち時間が非常に変わりやすかったりする場合、また、無線デバイスの伝送距離に制限がある場合に、セッションが切断されてしまうことがあります。現在、BCR にはこのようなシナリオに対応する十分なフォールバックまたはレポートメカニズムがありません。
- BCR オーバーレイブラウザーではファイルをダウンロードしたり印刷したりすることはできません。

HDX ビデオ会議と Web カメラビデオ圧縮

August 17, 2024

> 警告:
>
> レジストリエディターの使用を誤ると、深刻な問題が発生する可能性があり、オペレーティングシステムの再インストールが必要になる場合もあります。レジストリエディターの誤用による障害に対して、Citrix では一切責任を負いません。レジストリエディターは、お客様の責任と判断の範囲でご使用ください。また、レジストリファイルのバックアップを作成してから、レジストリを編集してください。

Web カメラは、HDX Web カメラビデオ圧縮または HDX プラグアンドプレイ汎用 USB リダイレクトにより、仮想セッション内で実行されるアプリケーションで使用できます。各モードの切り替えは、［**Citrix Workspace** アプリ］**>**［基本設定］**>**［デバイス］で行えます。可能であれば常に、HDX Web カメラビデオ圧縮を使用することをお勧めします。HDX 汎用 USB リダイレクトは、HDX ビデオ圧縮に関するアプリケーション互換性の問題がある場合、または Web カメラの高度なネイティブ機能が必要な場合にのみお勧めします。パフォーマンスを向上させるためには、Virtual Delivery Agent に少なくとも 2 つの仮想 CPU を用意することを Citrix ではお勧めします。

ユーザーが［HDX Web カメラビデオ圧縮］から切り替えられないようにするには、［**ICA** ポリシーの設定］**>**［**USB** デバイスのポリシー］のポリシー設定を使用して、USB デバイスのリダイレクトを無効にします。このデフォルト設定は、Citrix Workspace アプリユーザーが Desktop Viewer の［マイクと Web カメラ］設定で、［マイクおよび **Web** カメラを使用しない］を選択すると無効になります。

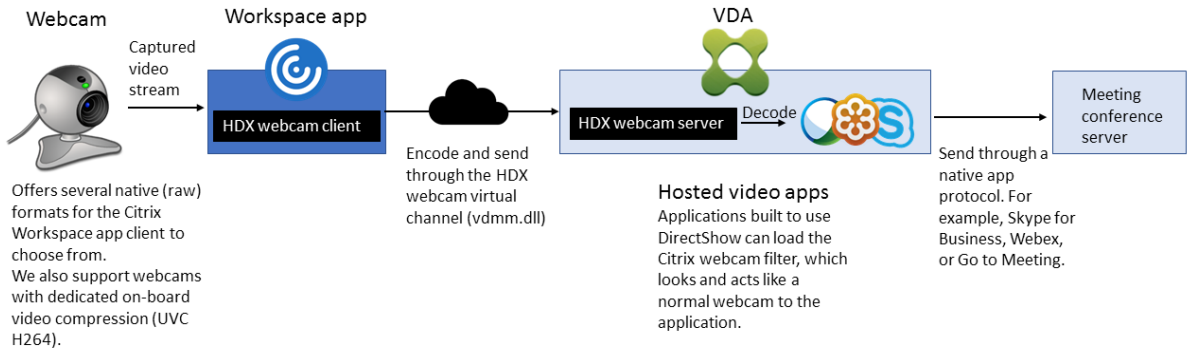
HDX Web カメラビデオ圧縮

HDX Web カメラビデオ圧縮は、最適化 Web カメラモードとも呼ばれます。このタイプの Web カメラビデオ圧縮では、仮想セッションで実行されているビデオ会議アプリケーションに H.264 ビデオを直接送信します。VDA リソースを最適化するため、HDX Web カメラ圧縮では Web カメラビデオをエンコード、トランスコード、およびデコードしません。この機能はデフォルトで有効になっています。

サーバーからビデオ会議アプリへの直接ビデオストリーミングを無効にするには、VDA でレジストリキーを 0 に設定します。詳しくは、レジストリを介して管理される機能の一覧にある「Web カメラビデオ圧縮」を参照してください。

ストリーミングビデオリソースのデフォルト機能を無効にすると、HDX Web カメラビデオ圧縮では、クライアントオペレーティングシステムに含まれるマルチメディアフレームワークテクノロジにより、キャプチャデバイスのビデオをインターセプトし、トランスコードおよび圧縮します。各キャプチャデバイスの製造元から、OS カーネルのストリーミングアーキテクチャに組み込まれるドライバーが提供されています。

クライアントは、Web カメラとの通信を処理します。その後、サーバーで適切に表示できるビデオのみを、サーバーに送信します。サーバーが Web カメラと直接やり取りをするわけではありませんが、統合によりデスクトップでも同様のエクスペリエンスが得られます。Citrix Workspace アプリがビデオを圧縮するため、帯域幅が節約され、WAN シナリオでの回復性の向上します。



マルチメディア会議ポリシーは、HDX Web カメラビデオ圧縮で有効にする必要があります。このポリシーはデフォルトで有効になっています。

Web カメラでハードウェアエンコード機能がサポートされる場合、HDX Web カメラビデオ圧縮ではデフォルトでそのハードウェアエンコードが使用されます。ハードウェアエンコード機能は、ソフトウェアエンコードより多くの帯域幅を消費する場合があります。ソフトウェア圧縮が使用されるようにするには、クライアントのレジストリキーを編集します。詳しくは、レジストリを介して管理される機能の一覧にある「Web カメラソフトウェア圧縮」を参照してください。

HDX Web カメラビデオ圧縮の要件

HDX Web カメラのビデオ圧縮は、次のバージョンの Citrix Workspace アプリをサポートします:

プラットフォーム	プロセッサ
Windows 向け Citrix Workspace アプリ	Windows 向け Citrix Workspace アプリは、XenApp および XenDesktop 7.17 以降上の 32 ビットおよび 64 ビットアプリの Web カメラビデオ圧縮をサポートします。以前のバージョンでは、Windows 向け Citrix Workspace アプリは 32 ビットアプリのみをサポートしていました。
Mac 向け Citrix Workspace アプリ	Mac 向け Citrix Workspace アプリ 2006 は、XenApp および XenDesktop 7.17 以降上の 64 ビットアプリの Web カメラビデオ圧縮をサポートします。以前のバージョンでは、Mac 向け Citrix Workspace アプリは 32 ビットアプリのみをサポートしていました。
Linux 向け Citrix Workspace アプリ	Linux 向け Citrix Workspace アプリは、仮想デスクトップの 32 ビットアプリと 64 ビットアプリの両方をサポートします。
Chrome 向け Citrix Workspace アプリ	一部の ARM Chromebook は H.264 エンコーディングをサポートしていないため、最適化された HDX Web カメラビデオ圧縮を使用できるのは 32 ビットアプリのみです。

メディアファンデーション形式のビデオアプリケーションは、Windows 10 以降および Windows Server 2019 以降での HDX Web カメラビデオ圧縮をサポートします。詳しくは、Knowledge Center の記事CTX132764を参照してください。

そのほかのユーザーデバイス要件:

- サウンド再生のためのハードウェア
- DirectShow 対応の Web カメラ（Web カメラのデフォルト設定を使用してください）。Web カメラ側のハードウェアエンコーディング機能を使用すると、クライアント側の CPU 使用率が軽減されます。
- HDX Web カメラを使用する場合、可能であれば、Web カメラの製造元から入手した Web カメラドライバーをクライアントにインストールしてください。サーバーにデバイスドライバーをインストールする必要はありません。

Web カメラが異なれば、フレームレートや、明るさとコントラストのレベルも異なります。Web カメラのコントラストを調整すると、アップストリームトラフィックを大幅に減らすことができます。Citrix 製品では、初期の機能検証に次の Web カメラを使用します:

- Microsoft LifeCam VX モデル（2000、3000、5000、7000）
- Creative Live! Cam Optia Pro
- Logitech QuickCam Messenger

- Logitech C600、C920
- HP Deluxe Webcam

最適なビデオフレームレートを調整するには、クライアントでレジストリキーを編集します。詳しくは、レジストリを介して管理される機能の一覧にある「Web カメラビデオ圧縮フレームレート」を参照してください。

高品位 **Web** カメラストリーミング

サーバーのビデオ会議アプリケーションは、サポートされている形式の種類に基づいて Web カメラの形式と解像度を選択します。セッションが開始されると、クライアントは Web カメラ情報をサーバーに送信します。アプリケーションから Web カメラを選択します。Web カメラとビデオ会議アプリケーションが高品位レンダリングをサポートする場合、アプリケーションは高品位解像度を使用します。Web カメラのすべての解像度をサポートしています。

この機能を使用するには、Windows 向け Citrix Workspace アプリバージョン 1808 以降、または Citrix Receiver for Windows バージョン 4.10 以降が必要です。

レジストリキーを使用してこの機能を無効または有効にすることができます。詳しくは、レジストリを介して管理される機能の一覧にある「高品位 Web カメラストリーミング」を参照してください。

メディアの種類のネゴシエーションが失敗した場合、HDX はデフォルトの VGA 解像度（640 x 480 ピクセル）に戻ります。クライアントのレジストリキーを使用して、デフォルトの解像度を設定することができます。カメラが指定された解像度をサポートしていることを確認してください。詳しくは、レジストリを介して管理される機能の一覧にある「高品位 Web カメラの解像度」を参照してください。

HDX Web カメラのビデオ圧縮は、プラグアンドプレイの汎用 USB リダイレクトと比較して、使用する帯域幅が大幅に少なく、WAN 接続で適切に動作します。帯域幅を調整するには、クライアントでレジストリキーを設定します。詳しくは、レジストリを介して管理される機能の一覧にある「高品位 Web カメラの帯域幅」を参照してください。

1 秒あたりのビット数で値を入力します。帯域幅を指定しない場合、ビデオ会議アプリケーションはデフォルトで 350000bps を使用します。

HDX プラグアンドプレイ汎用 **USB** リダイレクト

HDX プラグアンドプレイ汎用 USB リダイレクト（アイソクロナス）は、汎用 Web カメラモードとも呼ばれます。HDX プラグアンドプレイ汎用 USB リダイレクトの利点は、シンクライアントやエンドポイントにドライバーをインストールする必要がないことです。USB スタックは仮想化されており、ローカルクライアントに接続した周辺機器はすべてリモート VM へ送信されます。リモートデスクトップは、ネイティブ接続の場合と同じように動作します。Windows デスクトップがハードウェアとのやり取りをすべて処理し、プラグアンドプレイロジックにより適切なドライバーが検出されます。ドライバーがサーバー上に存在し、ICA に対応する場合、ほとんどの Web カメラを使用できます。汎用 Web カメラモードでは、USB プロトコルにより未圧縮のビデオをネットワーク上で送信するため、はるかに多くの帯域幅（大量の Mbps）が使用されます。

HTML5 マルチメディアリダイレクション

August 17, 2024

HTML5 マルチメディアリダイレクションは、HDX MediaStream のマルチメディアリダイレクト機能を拡張し、HTML5 のオーディオとビデオを含むようにしたものです。マルチメディアコンテンツのオンライン配信の拡大、特にモバイルデバイスへの拡大により、ブラウザー業界はオーディオやビデオを再生するより効率的な方法を開発してきました。

Flash が標準となりましたが、Flash はプラグインが必要で、すべてのデバイスで稼働するわけではなく、また、モバイルデバイスでは大量のバッテリーを消費します。YouTube や NetFlix などの企業、および Mozilla、Google、Microsoft の Web ブラウザーの新バージョンは HTML5 に移行しており、これが新しい標準になっています。

HTML5 ベースのマルチメディアには、専用プラグインを超える以下のような多数の利点があります:

- 企業非依存型の標準（W3C）
- 簡素化されたデジタル著作権管理（DRM）ワークフロー
- プラグインが原因のセキュリティの問題がないことによる優れたパフォーマンス

HTTP プログレッシブダウンロード

HTTP プログレッシブダウンロードは、HTML5 をサポートする、HTTP ベースの疑似ストリーミング方式です。プログレッシブダウンロードでは、（単一品質でエンコードされた）1 つのファイルが HTTP Web サーバーからダウンロードされている間に、ブラウザーがそれを再生します。ビデオは受け取られるとドライブに保存され、ドライブから再生されます。ビデオを再度視聴する場合、ブラウザーがキャッシュからビデオをロードします。

プログレッシブダウンロードの例については、「HTML5 ビデオリダイレクションのテストページ」を参照してください。Web ページ内のビデオエレメントを調べ、以下のような HTML5 ビデオタグ内のソース（MP4 コンテナフォーマット）を探すには、使用するブラウザーの開発者ツールを使用します。

HTML5 と Flash の比較

機能	HTML5	Flash
専用のプレーヤーが必要	いいえ	はい
モバイルデバイスで実行	はい	一部
異なるプラットフォームでの実行速度	High	低速
iOS でサポート	はい	いいえ
リソース使用率	比較的少ない	比較的多い

機能	HTML5	Flash
より高速なロード	はい	いいえ

要件

MP4 フォーマットでのプログレッシブダウンロードのリダイレクトのみがサポートされます。WebM、および DASH/HLS などのアダプティブビットレートストリーミングのテクノロジはサポートされません。

以下がサポートされており、ポリシーを使用してこれらを制御します。詳しくは、「マルチメディアのポリシー設定」を参照してください。

- サーバー側でレンダリング
- サーバー側でフェッチし、クライアント側でレンダリング
- クライアント側でフェッチしレンダリング

Citrix Workspace アプリおよび Citrix Receiver の最小バージョン:

- Windows 向け Citrix Workspace アプリ 1808
- Citrix Receiver for Windows 4.5
- Linux 向け Citrix Workspace アプリ 1808
- Citrix Receiver for Linux 13.5

VDA ブラウザーの最小バージョン	Windows OS のバージョン/ビルド/SP
Internet Explorer 11.0	Windows 10 x86（1607 RS1）および x64（1607 RS1）、Windows 7 x86 および x64、Windows Server 2016 RTM 14393（1607）、Windows Server 2012 R2
Firefox 47。Firefox 証明書ストアに証明書を手動で追加するか、Windows の信頼された機関からの証明書ストアで証明書を探すように Firefox を構成します。詳しくは、`https://wiki.mozilla.org/CA:AddRootToFirefox`を参照してください:	Windows 10 x86（1607 RS1）および x64（1607 RS1）、Windows 7 x86 および x64、Windows Server 2016 RTM 14393（1607）、Windows Server 2012 R2
Chrome 51	Windows 10 x86（1607 RS1）および x64（1607 RS1）、Windows 7 x86 および x64、Windows Server 2016 RTM 14393（1607）、Windows Server 2012 R2

HTML5 ビデオリダイレクションソリューションのコンポーネント

- **HdxVideo.js** - Web サイト上のビデオコマンドを傍受する JavaScript フック。HdxVideo.js は、セキュア WebSocket（SSL/TLS）を使用して WebSocketService と通信します。
- **WebSocket SSL** 証明書
  - CA（ルート）の場合：**Citrix XenApp/XenDesktop HDX In-Product CA**（C = US、S = Florida、L = Fort Lauderdale、O = Citrix Systems, Inc.、OU = XenApp and XenDesktop Engineering、CN = Citrix XenApp and XenDesktop HDX In-Product CA）
    場所：［証明書 **-** ローカルコンピューター］**>**［信頼されたルート証明機関］**>**［証明書］。
  - エンドエンティティ（リーフ）の場合：**Citrix XenApp/XenDesktop HDX Service**（C = US、S = Florida、L = Fort Lauderdale、O = Citrix Systems, Inc.、OU = XenApp and XenDesktop Engineering、CN = Citrix XenApp and XenDesktop HDX Service）
    場所：［証明書 **-** ローカルコンピューター］**>**［個人］**>**［証明書］。
- **WebSocketService.exe** - ローカルシステムで稼働し、SSL の終了とユーザーセッションマッピングを実行します。127.0.0.1 ポート 9001 でリッスンする TLS Secure WebSocket です。
- **WebSocketAgent.exe** - ユーザーセッションで稼働し、WebSocketService コマンドの指示に従ってビデオをレンダリングします。

HTML5 ビデオリダイレクションを有効にするには

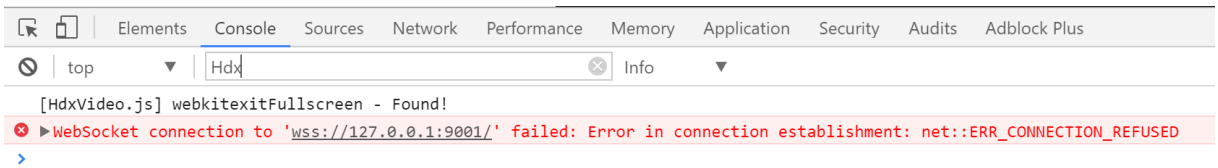
このリリースでは、この機能は管理対象 Web ページでのみ利用できます。HTML5 マルチメディアコンテンツが利用可能な Web ページに HdxVideo.js JavaScript（Citrix Virtual Apps and Desktops のインストールメディアに含まれています）を追加する必要があります。たとえば、社内研修サイトのビデオなどです。

youtube.com のようにアダプティブビットレート技術（HTTP ライブストリーミング（HLS）、Dynamic Adaptive Streaming over HTTP（DASH）など）をベースにした Web サイトは、サポートされていません。

詳しくは、「マルチメディアのポリシー設定」を参照してください。

トラブルシューティングのヒント

Web ページで HdxVideo.js を実行しようとすると、エラーが発生する場合があります。JavaScript が読み込みに失敗した場合、HTML5 リダイレクションメカニズムはエラーになります。使用するブラウザーの開発者ツールウィンドウでコンソールを調べて、HdxVideo.js に関連するエラーがないことを確認してください。例：



Microsoft Teams の最適化

August 17, 2024

> 注:
>
> 新しい Microsoft Teams 2.1 が VDA で一般提供されるようになりました。この Microsoft Teams のバージョンは、WebRTC（VDI 1.0）を使用した Citrix Microsoft Teams の最適化と互換性があります。
>
> Citrix Virtual Apps and Desktops 2402 以降では、`msedgewebview2.exe`レジストリエントリはデフォルトで許可リストに登録されているため、手動で構成する必要はありません。
>
> 公開アプリは、新しい Microsoft Teams でサポートされるようになりました。

Citrix では Citrix Virtual Apps and Desktops および Citrix Workspace アプリを通じてデスクトップベースの Microsoft Teams の最適化を提供します。必要なコンポーネントはデフォルトで Citrix Workspace アプリと Virtual Delivery Agent（VDA）に付属しています。

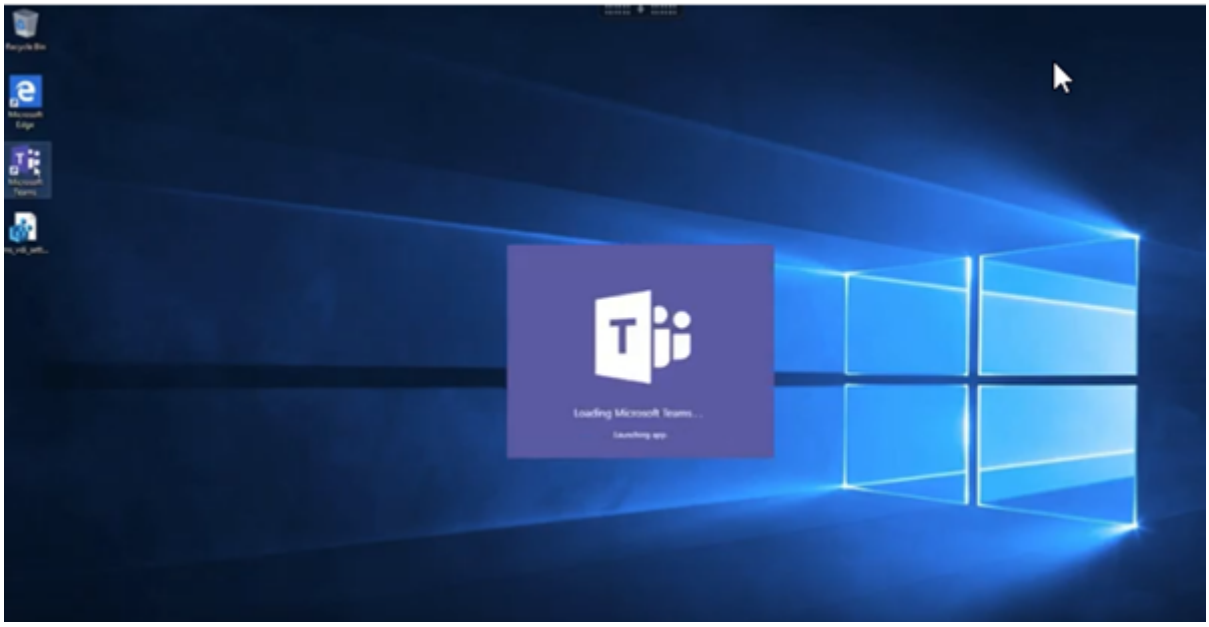
Microsoft Teams の最適化には、Microsoft Teams のホストアプリとのインターフェイスとしてコマンドを受信する、VDA 側の HDX サービスと API が含まれます。これらのコンポーネントにより Citrix Workspace アプリ側のメディアエンジンにつながる制御用の仮想チャネル（CTXMTOP）が開かれます。エンドポイントではマルチメディアがローカルでデコーディングおよび提供され、Citrix Workspace アプリのウィンドウはホストされている Microsoft Teams アプリに渡されます。

認証とシグナリングは他の Microsoft Teams サービス（チャットやコラボレーションなど）と同様に、Microsoft Teams のホストアプリでネイティブに行われます。これらのアプリはオーディオやビデオのリダイレクトによる影響を受けません。

`CTXMTOP`はコマンドであり、制御用の仮想チャネルです。つまり、Citrix Workspace アプリと VDA の間でメディアは交換されません。

クライアント側で取得またはクライアント側でレンダリングのみを利用できます。

このデモ動画をご覧いただければ、Microsoft Teams が Citrix の仮想環境でどのように機能するのかを確認できます。



Microsoft Teams のインストール

Citrix と Microsoft は、利用可能な最新バージョンの Microsoft Teams を使用し、最新の状態に保つことを推奨します。
リリース日が、現在のバージョンより 90 日を超えて古い Microsoft Teams デスクトップアプリのバージョンは、サポートされていません。
サポートされていない Microsoft Teams デスクトップアプリのバージョンでは、ユーザーをブロックするページが表示され、アプリの更新が要求されます。

利用可能な最新バージョンについては、「Microsoft Teams アプリの更新履歴（デスクトップと Mac）」を参照してください。

Microsoft Teams のマシン全体のインストールガイドラインに従うことをお勧めします。AppDataに Microsoft Teams をインストールする.exe インストーラーの使用は避けてください。代わりに、コマンドラインでALLUSER=1フラグを使用してC:\Program Files (x86)\Microsoft\Teamsにインストールします。

```
msiexec /i <path_to_msi> /l*v <install_logfile_name> ALLUSER=1
ALLUSERS=1
```

この例では、ALLUSERS=1パラメーターも使用しています。このパラメーターを設定すると、Microsoft Teams のマシン全体のインストーラーが、［コントロールパネル］の［プログラムと機能］に表示されます。また、Windows の設定の ［アプリと機能］にも表示されます。これはそのコンピューターの全ユーザーが対象です。管理者の資格情報があれば、すべてのユーザーが Microsoft Teams をアンインストールできます。

ALLUSERS=1とALLUSER=1の違いを理解することが重要です。ALLUSERS=1パラメーターは、非 VDI 環境と VDI 環境で使用できます。マシンごとのインストールを指定するには、VDI 環境でのみALLUSER=1パラメーターを使用します。

ALLUSER=1モードでは、Microsoft Teams アプリケーションのバージョンが新しくなるたびに自動更新されることはありません。Windows Server または Windows 10 のランダム/プールカタログからホストされた共有アプリまたは共有デスクトップなど、非永続環境ではこのモードをお勧めします。詳しくは、「MSI を使用して Microsoft Teams をインストールする」（VDI インストールセクション）を参照してください。

Windows 10 専用の永続 VDI 環境を想定します。Microsoft Teams アプリケーションを自動更新し、ユーザーごとにAppdata/Localに Microsoft Teams をインストールするこの場合、.exeインストーラーを使用するか、ALLUSER=1を設定せずに MSI を使用します。

> 注:
>
> ゴールデンイメージで Microsoft Teams をインストールする前に、VDA をインストールすることをお勧めします。このインストール順序は、ALLUSER=1フラグを有効にするために必要です。VDA をインストールする前に仮想マシンに Microsoft Teams がインストールされている場合は、Microsoft Teams をアンインストールして再インストールします。

リモート **PC** アクセス向け

VDA のインストール後に Microsoft Teams バージョン 1.4.00.22472 以降をインストールすることをお勧めします。そうしない場合は、Microsoft Teams で想定どおりに VDA が検出されるように、サインアウトしてから再度サインインする必要があります。バージョン 1.4.00.22472 以降には、VDA 検出のために Microsoft Teams の起動時およびサインイン時に実行される、拡張されたロジックが含まれています。これらのバージョンには、アクティブなセッションタイプの識別（HDX、RDP、またはクライアントマシンへのローカル接続）も含まれています。ローカル接続の場合、以前のバージョンの Microsoft Teams は、特定の機能または UI 要素の検出と無効化に失敗する可能性があります。たとえば、ブレークアウトルームでの、会議用やチャット用、または会議のリアクション用のウィンドウの表示などです。

> 重要:
>
> ローカルセッションから HDX セッションにローミングし、Microsoft Teams を開いてバックグラウンドで実行している場合は、Microsoft Teams を終了して再起動し、HDX で正しく最適化する必要があります。
> 逆に、最適化された HDX セッションを介してリモートで Microsoft Teams を使用する場合は、HDX セッションを切断し、デバイスのローカルで同じ Windows セッションに再接続します。オフィスから作業する場合は、Microsoft Teams を再起動して、リモート PC アクセスの状態（HDX またはローカル）を正しく検出できるようにする必要があります。Microsoft Teams は、アプリの起動時にのみ VDI モードを評価でき、バックグラウンドで既に実行されている間は評価できないためです。再起動しないと、Microsoft Teams はポップアウトウィンドウ、ブレークアウトルーム、会議のリアクションなどの機能の読み込みに失敗する可能性があります。

App Layering の場合

Citrix App Layering を使用して VDA と Microsoft Teams を異なるレイヤーで管理する場合、コマンドラインからALLUSER=1フラグを使用して Microsoft Teams をインストールする前に、Windows VDA でレジストリキー

を作成する必要があります。詳しくは、「マルチメディア」の「*Citrix App Layering* による *Microsoft Teams* の最適化」セクションを参照してください。

Profile Management の推奨事項

Windows Server 環境およびプールされた VDI Windows 10 環境では、マシン全体のインストーラーを使用することをお勧めします。

コマンドラインで **ALLUSER=1** フラグを MSI に渡すと、Microsoft Teams アプリは`C:\Program Files (x86)`（約 300MB）にインストールされます。このアプリはログに`AppData\Local\Microsoft\TeamsMeetingAddin`を、ユーザー独自の構成、ユーザーインターフェイスの要素のキャッシュなどに`AppData\Roaming\Microsoft\Teams`（約 600～700MB）を使用します。

> 重要:
>
> **ALLUSER=1** フラグを渡さない場合、MSI は Teams.exe インストーラーと`setup.json`を`C:\Program Files (x86)\Teams Installer`に配置します。レジストリキー（TeamsMachine-Installer）が次の場所に追加されます: `HKEY_LOCAL_MACHINE \SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run`
>
> 後続のユーザーログオンは、代わりに **AppData** の最終インストールをトリガーします。

マシン全体のインストーラー

以下は、任意の Windows Server 64 ビット仮想マシンに、Microsoft Teams のマシン全体のインストーラーをインストールすることによって作成されるフォルダー、デスクトップショートカット、およびレジストリの例です:

フォルダー:

- `C:\Program Files (x86)\Microsoft\Teams`
- `C:\Users\<username>\AppData\Roaming\Microsoft\Teams`

デスクトップのショートカット:

`C:\Program Files (x86)\Microsoft\Teams\current\Teams.exe`

レジストリ:

- `HKEY_LOCAL_MACHINE \SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run`
- `HKEY_LOCAL_MACHINE \SOFTWARE\Microsoft\Windows\CurrentVersion\Run`
- `HKEY_CURRENT_USER \SOFTWARE\Microsoft\Windows\CurrentVersion\Run`
- 値の名前: `Teams`
- 種類: `REG_SZ`
- 値: `C:\Program Files (x86)\Microsoft\Teams\current\Teams.exe`

> 注:
>
> レジストリの場所は、基盤となるオペレーティングシステムとビットによって異なります。

推奨事項

- Microsoft Teams のレジストリキーを削除して、自動起動を無効にすることをお勧めします。そうすることで、多数のログオンが同時に行われる場合（たとえば、就業日の開始時刻）に、VM の CPU 使用量が急上昇するのを防ぎます。
- 仮想デスクトップに GPU または vGPU がない場合は、Microsoft Teams の［設定］で［**GPU** ハードウェアアクセラレーションを無効にする］を選択し、パフォーマンスを改善します。この設定（`"disableGpu":true`）は`desktop-config.json`の`%Appdata%\Microsoft\Teams`に格納されています。ログオンスクリプトを使用してファイルを編集し、値を`true`に設定できます。
- Citrix Workspace Environment Management（WEM）を使用している場合は、［**CPU** スパイク保護］を有効にして、Microsoft Teams のプロセッサ消費を管理します。

ユーザーごとのインストーラー

`.exe`インストーラーを使用する場合は、インストールプロセスが異なります。すべてのファイルは AppData に配置されます。

フォルダー:

- `C:\Users\<username>\AppData\Local\Microsoft\Teams`
- `C:\Users\<username>\AppData\Local\Microsoft\TeamsPresenceAddin`
- `C:\Users\<username>\AppData\Local\Microsoft\TeamsMeetingAddin`
- `C:\Users\<username>\AppData\Local\SquirrelTemp`
- `C:\Users\<username>\AppData\Roaming\Microsoft\Teams`

デスクトップのショートカット:

```
C:\Users\<username>\AppData\Local\Microsoft\Teams\Update.exe --
processStart "Teams.exe"
```

レジストリ:

```
HKEY_CURRENT_USER \SOFTWARE\Microsoft\Windows\CurrentVersion\Run
```

ベストプラクティス

ベストプラクティスの推奨事項は、ユースケースのシナリオに基づいています。
非永続的な設定で Microsoft Teams を使用するには、Microsoft Teams ランタイムのデータ同期を効率的に実行するために、プロファイルキャッシュマネージャーが必要です。プロファイルキャッシュマネージャーを使用すると、

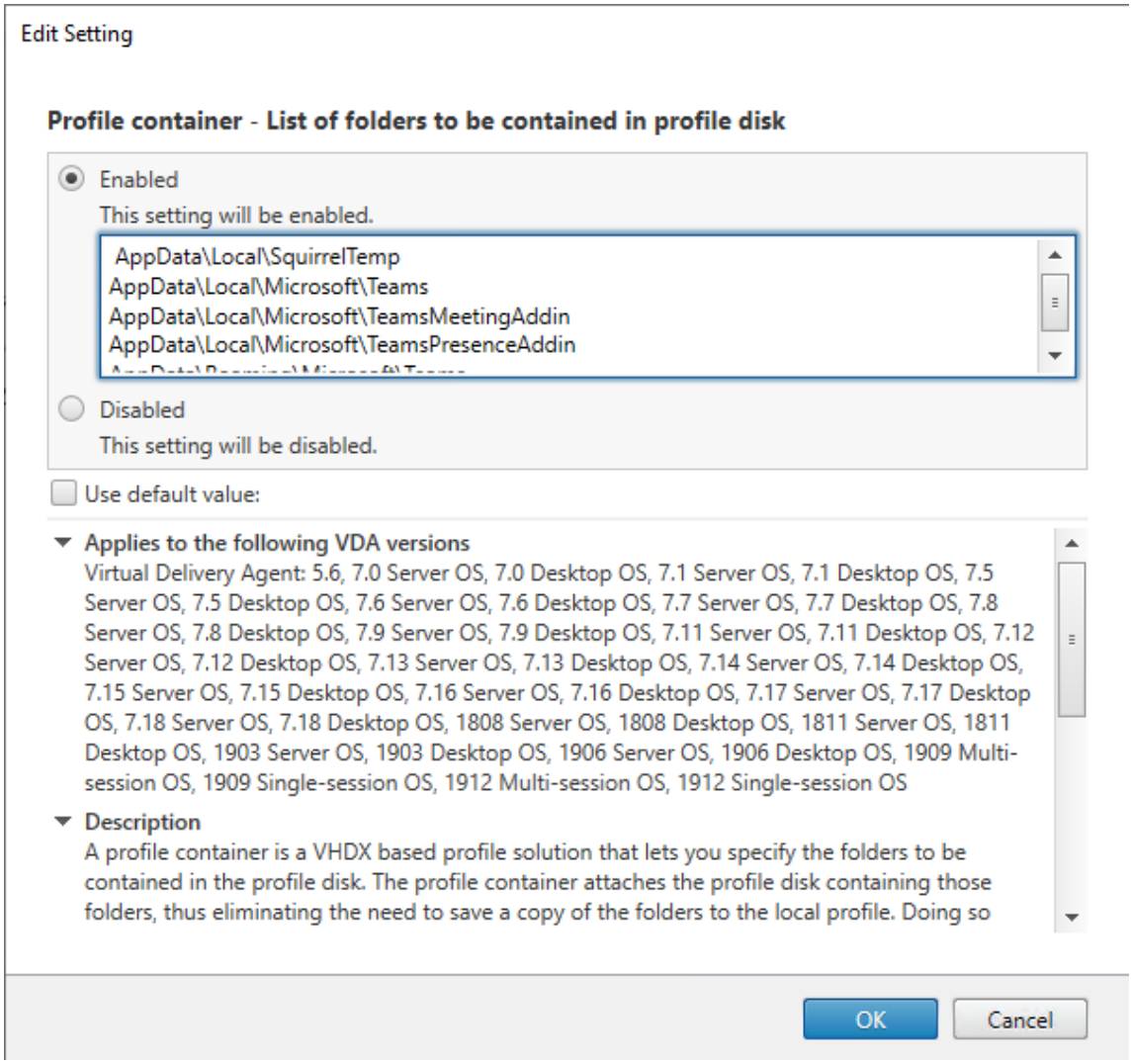
適切なユーザー固有の情報がユーザーセッション中にキャッシュされます。たとえば、ユーザー固有の情報には、ユーザーデータ、プロファイル、設定が含まれます。次の 2 つのフォルダー内のデータを同期してください:

- C:\Users\<username>\AppData\Local\Microsoft\IdentityCache
- C:\Users\<username>\AppData\Roaming\Microsoft\Teams

非永続的な設定用の、**Microsoft Teams** でキャッシュしたコンテンツ除外一覧　Microsoftのドキュメントで説明されているように、ファイルとディレクトリを Microsoft Teams のキャッシュフォルダーから除外します。この操作は、ユーザーのキャッシュサイズを減らして、非永続的な設定をさらに最適化するのに役立ちます。

ユースケース: シングルセッションシナリオ　このシナリオでは、エンドユーザーは、一度に 1 つの場所で Microsoft Teams を使用します。2 つの Windows セッションで同時に Microsoft Teams を実行する必要はありません。共通の仮想デスクトップ展開では、各ユーザーが 1 つのデスクトップに割り当てられ、Microsoft Teams は 1 つのアプリケーションとして仮想デスクトップに展開されます。
Citrix Profile コンテナを有効にして、ユーザーごとのインストーラーに表示されるユーザーごとのディレクトリをコンテナにリダイレクトすることをお勧めします。

1. Microsoft Teams のマシン全体のインストーラー（**ALLUSER=1**）をゴールデンイメージで展開します。
2. Citrix Profile Management を有効にし、適切な権限でユーザープロファイルストアを設定します。
3. 次の Profile Management ポリシー設定を有効にします:［ファイルシステム］**>**［同期］**>**［プロファイルコンテナ **-** プロファイルディスクに含まれるフォルダー一覧］。



この構成でユーザーごとのすべてのディレクトリを一覧表示します。Citrix Workspace Environment Management（WEM）サービスを使用して、これらの設定を構成することもできます。

4. 設定を適切なデリバリーグループに適用します。
5. ログインして展開を検証します。

システム要件

推奨の最小バージョン **- Delivery Controller（DDC）1906.2**

以前のバージョンを使用している場合は、「Microsoft Teams の最適化を有効にする」を参照してください：

以下のオペレーティングシステムがサポートされています：

- Windows Server 2022、2019、2016、2012 R2 の Standard およびデータセンターエディション、および Server Core オプション付き

最小バージョン **- Virtual Delivery Agent**（**VDA**）**1906.2**

以下のオペレーティングシステムがサポートされています：

- Windows 11
- Windows 10 64 ビット版、バージョン 1607 以降。VM Hosted Apps は、Windows 向け Citrix Workspace アプリ 2109.1 以降でサポートされます
- Windows Server 2022、2019、2016、2012 R2（Standard およびデータセンターエディション）

要件：

- BCR_x64.msi - Microsoft Teams の最適化コードが格納された MSI ファイルです。自動的に GUI で起動します。VDA のインストールにコマンドラインインターフェイスを使用する場合は、このファイルを除外しないでください。

推奨バージョン **- Windows** 向け **Citrix Workspace** アプリの最新 **CR** および最小バージョン **- Windows** 向け **Citrix Workspace** アプリ **1907**

- Windows 11。
- Windows 10（Embedded エディションを含む 32 ビットおよび 64 ビットエディション）（Windows 7 のサポートはバージョン 2006 で終了しました）（Windows 8.1 のサポートはバージョン 2204.1 で終了しました）。
- Windows 10 IoT Enterprise 2016 LTSB（v1607）および 2019 LTSC（v1809）。
- サポートされているプロセッサ（CPU）アーキテクチャ：x86 および x64（ARM はサポートされていません）。
- エンドポイントの要件：2.2～2.4GHz 程度のデュアル CPU を搭載し、ピアツーピアのビデオ会議通話で 720p HD の解像度に対応していること。
- デュアルまたはクアッドコア CPU、低い基本速度（約 1.5GHz）で Intel Turbo Boost または AMD Turbo Core を搭載し、少なくとも 2.4GHz までブーストできる。
- 検証済みの HP シンクライアント：t630/t640、t730/t740、mt44/mt45。
- 検証済みの Dell シンクライアント：5070、5470 モバイル TC、AIO。
- 検証済みの 10ZiG シンクライアント：4510 および 5810q。
- 検証済みエンドポイントの全一覧については、「シンクライアント」を参照してください。
- Citrix Workspace アプリでは、少なくとも 600MB の空きディスクスペースと 1GB の RAM が必要です。
- Microsoft .NET Framework の最小要件はバージョン 4.8 です。システムに.NET Framework が導入されていない場合は、Citrix Workspace アプリにより自動的にダウンロードとインストールが行われます。

管理者は Microsoft Teams 最適化ポリシーを変更することにより、最適化モードで開始する Microsoft Teams を有効にするか無効にするかを選択できます。Citrix Workspace アプリで最適化モードで開始するユーザーは、Microsoft Teams を無効にできません。

最小バージョン **- Linux** 向け **Citrix Workspace** アプリ **2006**

詳しくは、Linux 向け Citrix Workspace アプリドキュメントの「Microsoft Teams の最適化」を参照してください。

ソフトウェア:

- `GStreamer` 1.0 以降または Cairo 2
- `libc++-9.0`以降
- `libgdk` 3.22 以降
- OpenSSL 1.1.1d
- `libnsl`
- Ubuntu 20.04 以降

認証の強化:

- libsecret ライブラリ
- libunwind-12 ライブラリ。詳しくは、「llvm-12 に libunwind-12 ライブラリの依存関係を追加」を参照してください。

ハードウェア:

- 1.8GHz 以上のデュアル CPU を搭載し、ピアツーピアのビデオ会議通話で 720p HD の解像度に対応している
- デュアルまたはクアッドコア CPU、基本速度 1.8GHz で、2.9GHz 以上の高速 Intel Turbo Boost を搭載している

検証済みエンドポイントの全一覧については、「シンクライアント」を参照してください。

詳しくは、「Citrix Workspace アプリをインストールする前提条件」を参照してください。

`/opt/Citrix/ICAClient/config/module.ini`ファイル内の **VDWEBRTC** フィールドの値をオフに更新して、Microsoft Teams の最適化機能を無効にすることができます。デフォルトでは VDWEBRTC がオンになっています。更新が完了したら、セッションを再開します。(ルート権限が必要です)。

最小バージョン **- Mac** 向け **Citrix Workspace** アプリ **2012**

以下のオペレーティングシステムがサポートされています:

- macOS Catalina(10.15)。
- macOS Big Sur 11.0.1 以降。
- macOS Monterey。

サポートされる機能:

- オーディオ
- ビデオ

- 画面共有の最適化（受信および送信）

> 注:
>
> Citrix Viewer アプリでは、画面共有を機能させるために macOS の［セキュリティとプライバシー］の環境設定にアクセスする必要があります。この環境設定を行うには、アップルメニュー **>** ［システム環境設定］ **>** ［セキュリティとプライバシー］ **>** ［プライバシー］タブ **>** ［画面収録］の順に進み、［**Citrix Viewer**］を選択します。

Microsoft Teams の最適化は、Citrix Workspace アプリ 2012 以降および macOS 10.15 とデフォルトで機能します。

Microsoft Teams の最適化を無効にする場合は、ターミナルで次のコマンドを実行し、Citrix Workspace アプリを再起動します:

```
defaults write com.citrix.receiver.nomas mtopEnabled -bool NO
```

最小バージョン- 最新バージョンの **ChromeOS** で実行されている **ChromeOS** 向け **Citrix Workspace** アプリ

ハードウェア:

- パフォーマンスが Intel i3、クアッドコア 2.4GHz と同等またはそれ以上のプロセッサ。

サポートされる機能:

- オーディオ
- ビデオ
- 画面共有の最適化（受信および送信）- デフォルトで無効有効にする方法については、これらの設定を参照してください。

単一サーバーのスケーラビリティ

このセクションでは、単一の物理ホストでサポートできるユーザーまたは仮想マシン（VM）の数を見積もる際の推奨事項等を説明します。これは一般的に、Citrix Virtual Apps and Desktops の単一サーバーのスケーラビリティ（Single Server Scalability：SSS）と呼ばれます。Citrix Virtual Apps（CVA）またはセッション仮想化の文脈では、一般的にユーザー密度とも呼ばれます。これは、主要なハイパーバイザーを実行している単一のハードウェアで実行可能なユーザーまたは VM の数を調べることを意味します。

> 注:
>
> このセクションには、SSS を見積もるためのガイダンスがあります。このガイダンスは概要の説明であり、必ずしも特定の状況や環境に固有のことではないことがあります。Citrix Virtual Apps and Desktops の SSS を深く理解する唯一の方法は、Login VSI などのスケーラビリティまたは負荷テストツールを使用することです。ここに記載されているガイダンスと簡単な規則を用いて、すばやく SSS のみを見積もることをお勧めしま

> す。ただし、ハードウェアを購入したり、財務上の決定を行う前に、Login VSI または負荷テストツールを使用して結果を検証することをお勧めします。

ハードウェア（テスト対象のシステム）

- Dell PowerEdge R740
- Intel Xeon（Gold）6126 @ 2.60GHz（最大 Turbo 3.70GHz）、ソケットあたり 12 コア、Hyperthreading が有効なデュアルソケット
- 382GB の RAM
- ローカル SSD RAID 0 ストレージ（11 ディスク）6 TB

ソフトウェア

Citrix Virtual Apps and Desktops 2106
VMware ESXi 6.7 を実行している Windows 2019（TSVDA）の単一の仮想マシン（40 個の論理プロセッサ）

用語

- ナレッジワーカーのワークロード：Acrobat Reader、Freemind/Java、Photo viewer、Edge、および Excel、Outlook、PowerPoint、Word などの MS Office アプリ。
- 基準：サーバーのスケーラビリティのテストは、ナレッジワーカーのワークロード（Microsoft Teams なし）で実行されます。
- Microsoft Teams ワークロード：ナレッジワーカーの一般的なワークロード + Microsoft Teams。

Microsoft Teams のストレステスト方法

- Microsoft Teams は HDX で最適化されています。したがって、すべてのマルチメディア処理は、エンドポイントまたはクライアントにオフロードされ、測定の一部にはなりません。
- ワークロードが開始する前に、すべての Microsoft Teams プロセスが停止または強制終了されます。
- Microsoft Teams が開きます（コールドスタート）。
- Microsoft Teams がプライマリウィンドウを読み込んでフォーカスを取得するのにかかる時間を測定します。
- キーボードショートカットを使用して、チャットウィンドウに切り替えます。
- キーボードショートカットを使用して、カレンダーウィンドウに切り替えます。
- キーボードショートカットを使用して、特定のユーザーにチャットメッセージを送信します。
- キーボードショートカットを使用して、Microsoft Teams ウィンドウに切り替えます。

結果

- 基準（137 ユーザー）と比較した場合、Microsoft Teams ワークロード（81 ユーザー）によるスケーラビリティへの影響は 40% です。
- サーバー容量を 40% 以下（CPU 内）の範囲で増やすと、基準ワークロードと同じユーザー数を復元します。
- 基準と比較した場合、Microsoft Teams ワークロードでは 20% の追加メモリが必要です。
- 1 ユーザーあたりのストレージサイズを 512～1024MB の範囲で増やします。
- IOPS 書き込みは 50% 以下の範囲で増加、IOPS 読み取りは 100% 以下の範囲で増加。Microsoft Teams は、ストレージの速度が遅い環境に深刻な影響を与える可能性があります。

機能マトリックスとバージョンのサポート

機能	Microsoft Teams（最小バージョン）	VDA（最小バージョン）	Windows 向け Citrix Workspace アプリ CR（最小バージョン）	Mac 向け Citrix Workspace アプリ（最小バージョン）	Linux 向け Citrix Workspace アプリ（最小バージョン）	ChromeOS 向け Citrix Workspace アプリ（最小バージョン）
オーディオ/ビデオ (P2P および会議)	最新バージョンから 90 日を引いたバージョン	1906	1907	2009	2004	2105.5
画面共有	最新バージョンから 90 日を引いたバージョン	1906	1907	2012	2006	2105.5
i. 赤い枠線を画面に表示	最新バージョンから 90 日を引いたバージョン	1906	2002	2012	2006	いいえ
ii. キャプチャを Desktop Viewer に制限	最新バージョンから 90 日を引いたバージョン	1906	2009.5	2012	2006	いいえ
iii. マルチモニター	最新バージョンから 90 日を引いたバージョン	1912 CU6 以降	2106 (1)	2106	2106	いいえ

機能	Microsoft Teams（最小バージョン）	VDA（最小バージョン）	Windows 向け Citrix Workspace アプリ CR（最小バージョン）	Mac 向け Citrix Workspace アプリ（最小バージョン）	Linux 向け Citrix Workspace アプリ（最小バージョン）	ChromeOS 向け Citrix Workspace アプリ（最小バージョン）
DTMF	最新バージョンから 90 日を引いたバージョン	-	2102	2101	2101	2111.1
プロキシサーバーのサポート	最新バージョンから 90 日を引いたバージョン	-	2012 (2)	2104 (3)	2101 (3)	2305
アプリの共有	最新バージョンから 90 日を引いたバージョン	2109	2109.1	2203.1	2209	いいえ
ライブキャプション	最新バージョンから 90 日を引いたバージョン	-（4）	2109.1	2109	2109	2303
動的緊急通報（Dynamic e911）	最新バージョンから 90 日を引いたバージョン	-	2112.1	2112	2112	2112
制御を渡す	最新バージョンから 90 日を引いたバージョン	-	2112.1	2203.1	いいえ	いいえ
制御を要求	最新バージョンから 90 日を引いたバージョン	-	2112.1	2203.1	2203	2303
マルチウィンドウ	1.5.00.11865	2112、1912 CU6（5）	2112.1	2203.1	2203	2303

機能	Microsoft Teams（最小バージョン）	VDA（最小バージョン）	Windows 向け Citrix Workspace アプリ CR（最小バージョン）	Mac 向け Citrix Workspace アプリ（最小バージョン）	Linux 向け Citrix Workspace アプリ（最小バージョン）	ChromeOS 向け Citrix Workspace アプリ（最小バージョン）
会議のトランスクリプト	最新バージョンから 90 日を引いたバージョン	2112.1、1912 CU6 以降	2112	2203.1	2203	2303
背景のぼかし	最新バージョンから 90 日を引いたバージョン	2112、1912 CU6 以降	2207	2301	2212	2303

1. CD ビューアはフルスクリーンモードでのみ使用できます。SHIFT+F2 はサポートされていません。
2. Negotiate/Kerberos、NTLM、Basic、およびダイジェスト。Pacファイルもサポートされています。
3. 匿名のみ。
4. VDA が 2112 以降の場合、ライブキャプションは、Mac 向け Citrix Workspace アプリではバージョン 2203.1、Linux 向けでは 2203、Windows 向けでは 2112 の場合にのみ機能します。これは、Microsoft Teams がシングルウィンドウ UI モードまたはマルチウィンドウモードの場合で、ライブキャプションの動作が異なるためです。
5. マルチウィンドウは 2112 VDA で導入されましたが、VDA 1912 LTSR CU6 リリースにバックポートされました。

> 注:
>
> - 「**Windows** 向け **Citrix Workspace** アプリ **1912 CU6** 以降」に記載されているすべての機能は、Windows 向け Citrix Workspace アプリ 2203.1 LTSR CU1 に適用されます。
> - Microsoft は、Microsoft Teams でのシングルウィンドウモードのサポートを廃止しました。準拠するには、VDA を 1912 CU6 以降の LTSR および Citrix Workspace アプリ 2203 CU2 以降にアップグレードする必要があります。

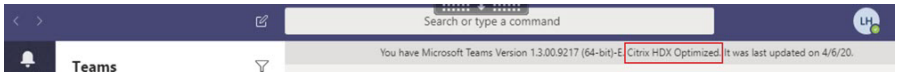
Microsoft Teams の最適化を有効にする

Microsoft Teams の最適化を有効にするには、「Microsoft Teams リダイレクト」で説明されている［管理］コンソールのポリシーを使用します。このポリシーは、デフォルトでは有効になっています。HDX はこのポリシーが有効になっていることと、Citrix Workspace アプリのバージョンが最低限必要とされるバージョン以上であることを確認します。ポリシーが有効で Citrix Workspace アプリがサポート対象のバージョンである場合は、VDA で

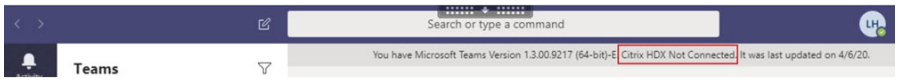
HKEY_CURRENT_USER\Software\Citrix\HDXMediaStream\MSTeamsRedirSupport の値が **1** に自動的に設定されます。Microsoft Teams はこのレジストリキーを VDI モードで読み取ってロードします。

> 注:
>
> ［管理］コンソール（Studio）で使用可能なポリシーがない古いバージョンのコントローラー（たとえばバージョン 7.15）でバージョン 1906.2 以降の VDA を使用している場合、その VDA では引き続き最適化が有効になっています。Microsoft Teams の HDX 最適化は、VDA ではデフォルトで有効になっています。

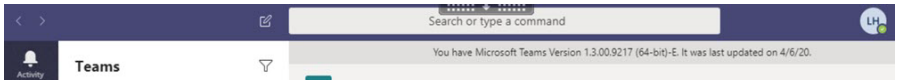
［バージョン情報］をクリックすると、**Citrix HDX Optimized** と表示されます:



Citrix HDX Not Connected と表示される場合は、Citrix API は Microsoft Teams に読み込まれています。API の読み込みは、リダイレクトへの最初の手順です。しかし、スタックの後半部分にエラーがあります。このエラーは、VDA サービスまたは Citrix Workspace アプリで発生する可能性があります。



凡例が表示されない場合、Microsoft Teams が Citrix API の読み込みに失敗しています。通知領域のアイコンを右クリックして Microsoft Teams を終了し、再起動します。［管理］コンソールのポリシーが ［禁止］に設定されていないこと、および Citrix Workspace アプリのバージョンがサポートされていることを確認します。



> 重要：セッションは再接続されます
>
> - 接続が変更されたときに、HDX で最適化されたセッションを取得するには、Microsoft Teams の再起動が必要な場合があります。たとえば、サポートされていないエンドポイント（iOS 用、Android 用、または古いバージョンの Windows/Linux/Mac 用の Workspace アプリ）から、サポートされているエンドポイント（Windows/Linux/Mac/ChromeOS/HTML5 用の Workspace アプリ）にローミングしている場合、またはその逆の場合。
> - VDA で Microsoft Teams の.exe インストーラーを使用してアプリをインストールした場合も、Microsoft Teams の再起動が必要です。永続する VDI 展開には、.exe インストーラーをお勧めします。この場合、Microsoft Teams は、HDX セッションが切断された状態のときに自動更新できます。そのため、HDX セッションに再接続するユーザーは、Microsoft Teams が最適化された状態で実行されていないことに気付きます。
> - ローカルセッションから HDX セッションにローミングする場合、HDX で最適化するには Microsoft Teams を再起動する必要があります。この操作は、リモート PC アクセスのシナリオで必要です。

ネットワークの要件

Microsoft Teams は、会議またはマルチパーティ通話で Microsoft 365 のメディアプロセッササーバーに依存します。また、次のシナリオで Microsoft Teams は Microsoft 365 トランスポートリレーに依存します:

- ピアツーピア通話の 2 つのピアが直接接続できない。
- 参加者がメディアプロセッサに直接接続できない。

そのため、ピアと Microsoft 365 クラウドの間のネットワークの状態が通話のパフォーマンスを左右します。ネットワーク計画に関する詳細なガイドラインについては、「Microsoft 365 ネットワーク接続の原則」を参照してください。

環境を評価し、クラウド全体のオーディオおよびビデオ環境に影響を与える可能性のあるリスクと要件を特定することをお勧めします。
Skype for Business ネットワーク評価ツールを使用して、ネットワークが Microsoft Teams に対応できるかどうかをテストします。サポート情報については、「サポート」を参照してください。

リアルタイムプロトコル（**RTP**）トラフィックに関する主要なネットワーク推奨事項の要約

- 可能な限りブランチオフィスから直接 Microsoft 365 ネットワークに接続します。
- ブランチオフィスで十分な帯域幅を計画して提供します。
- 各ブランチオフィスのネットワークの接続性と品質について確認してください。
- ブランチオフィスで次のいずれかを使用する必要がある場合は、（Citrix Workspace アプリの HdxRtcEngine.exe で処理される）RTP/UDP のトラフィックが妨げられないことを確認してください。
  - プロキシサーバーのバイパス
  - ネットワークの SSL インターセプト
  - ディープパケットインスペクションデバイス
  - VPN ヘアピン（可能な場合は分割トンネリングを使用）

> 重要：**VPN** 分割トンネリング構成
>
> HdxRtcEngine.exe トラフィックは VPN トンネルから迂回させ、ユーザーのローカルインターネット接続を使用してサービスに直接接続できるようにする必要があります。これを実現する方法は、使用する VPN 製品とマシンプラットフォームによって異なりますが、ほとんどの VPN ソリューションでは、簡単にポリシーを設定してこのロジックを適用できます。VPN プラットフォーム固有の分割トンネルガイダンスについて詳しくは、この Microsoft の記事を参照してください。

Workspace アプリ（HdxRtcEngine.exe）の WebRTC メディアエンジンは、クライアントにオフロードされるマルチメディアストリームの Secure Real-time Transport Protocol（SRTP）を使用します。SRTP は、RTP に機密性と認証を提供します。この機能では、対称キー（DTLS とネゴシエート）を使用してメディアを暗号化し、AES 暗号化を使用してメッセージを制御します。

ポジティブなユーザーエクスペリエンスのために、次の測定基準をお勧めします:

メトリック	エンドポイントから Microsoft 365
遅延（片道）	50 ミリ秒未満
遅延（RTT）	100 ミリ秒未満
パケット損失	15 秒間隔で 1% 未満
パケット到着間ジッター	15 秒間隔で 30 ミリ秒未満

詳しくは、「Microsoft Teams 用に組織のネットワークを準備する」を参照してください。

帯域幅の要件に関して、Microsoft Teams 用の最適化では、オーディオ（OPUS/G.722/PCM G711）およびビデオ（H264）用にさまざまなコーデックを使用できます。

ピアは、セッション記述プロトコル（SDP）のオファー/アンサーを使用して、通話の確立プロセス中にこれらのコーデックをネゴシエートします。
Citrix のユーザーごとの最低推奨要件は次のとおりです:

種類	帯域幅	コーデック
オーディオ（片道）	約 90kbps	G.722
オーディオ（片道）	約 60kbps	Opus*
ビデオ（片道）	約 700kbps	H264 360p @ 30 fps 16:9
画面共有	約 300kbps	H264 1080p @ 15 fps

* Opus は、6kbps～510kbps の固定および可変ビットレートのエンコードをサポートしています。

Opus と H264 は、ピアツーピアおよび電話会議に推奨されるコーデックです。

> 重要:
>
> パフォーマンスに関しては、クライアントマシンでの CPU 使用率のために、エンコードにはデコードよりもコストがかかります。Linux および Windows 用の Citrix Workspace アプリで最大エンコーディング解像度をハードコーディングできます。「エンコーダーのパフォーマンス見積もりツール」と「Microsoft Teams の最適化」を参照してください。

プロキシサーバー

プロキシの場所に応じて、次のことを考慮してください:

- VDA でのプロキシ構成:

VDA で明示的なプロキシサーバーを構成し、プロキシ経由でローカルホストに接続をルーティングすると、リダイレクトは失敗します。プロキシを正しく構成するには、［インターネットオプション］**>**［接続］**>**［**LAN** の設定］**>**［プロキシサーバー］で ［ローカルアドレスにはプロキシサーバーを使用しない］を選択し、`127.0.0.1:9002`がバイパスされるようにする必要があります。

PAC ファイルを使用する場合、PAC ファイルの VDA プロキシ構成スクリプトは`wss://127.0.0.1:9002`に対して **DIRECT** を返す必要があります。そうでない場合、最適化は失敗します。このスクリプトが **DIRECT** を返すようにするには、`shExpMatch(url, "wss://127.0.0.1:9002/*")`を使用します。

- Citrix Workspace アプリでのプロキシ構成:

  ブランチオフィスがプロキシを介してインターネットにアクセスするように構成されている場合、以下のバージョンはプロキシサーバーをサポートします:

  - Windows 向け Citrix Workspace アプリバージョン 2012（Negotiate または Kerberos、NTLM、Basic、および Digest。Pacファイルもサポートされています）
  - Windows 向け Citrix Workspace アプリバージョン 1912 CU5(Negotiate または Kerberos、NTLM、Basic、および Digest。Pacファイルもサポートされています）
  - Linux バージョン 2101 向け Citrix Workspace アプリ（匿名認証）
  - Mac バージョン 2104 向け Citrix Workspace アプリ（匿名認証）

クライアントデバイスで以前のバージョンの Citrix Workspace アプリを使用している場合、プロキシ構成を読み取ることができません。これらのデバイスは、トラフィックを Microsoft 365 TURN サーバーに直接送信します。

> 重要:
>
> - クライアントデバイスが DNS サーバーに接続して DNS 解決を実行できることを確認します。クライアントデバイスは、次の Microsoft Teams Relay サーバーの FQDN を解決できる必要があります:
>
>   ```
>   - worldaz.relay.teams.microsoft.com
>   - inaz.relay.teams.microsoft.com
>   - uaeaz.relay.teams.microsoft.com
>   - euaz.relay.teams.microsoft.com
>   - usaz.relay.teams.microsoft.com
>   - turn.dod.teams.microsoft.us
>   - turn.gov.teams.microsoft.us
>   ```
>
> DNS 要求が失敗した場合、外部ユーザーとの P2P 通話および電話会議でのメディアの確立は失敗します。
>
> - 会議サーバーの場所は、最初の参加者の仮想デスクトップの場所（クライアントではない）に基づいて選択されます。

通話の確立とメディアフローパス

可能な場合、Citrix Workspace アプリの HDX WebRTC メディアエンジン（HdxRtcEngine.exe）は、ピアツーピア通話で、ユーザーデータグラムプロトコル（UDP）上で、直接ネットワーク Secure Real-time Transport Protocol（SRTP）接続を確立しようとします。高 UDP ポートがブロックされている場合、メディアエンジンは TCP/TLS 443 にフォールバックします。

HDX メディアエンジンは、ICE、Session Traversal Utilities for NAT（STUN）、Traversal Using Relays around NAT（TURN）をサポートして、候補の検出と接続の確立を行います。このサポートは、エンドポイントで DNS 解決を実行できる必要があることを意味します。

2 つのピア間、またはピアと会議サーバー間に直接パスがなく、ユーザーがマルチパーティ通話または会議に参加しているとします。HdxRtcEngine.exe は、Microsoft 365 の Microsoft Teams トランスポートリレーサーバーを使用して、会議がホストされているほかのピアまたはメディアプロセッサに到達します。クライアントマシンには、3 つの Microsoft 365 サブネット IP アドレス範囲と 4 つの UDP ポート（または、UDP がブロックされている場合のフォールバックとしての TCP/TLS 443）にアクセスする権限が必要です。詳しくは、「通話のセットアップ」のアーキテクチャの図と「Office 365 の URL と IP アドレスの範囲 ID 11」を参照してください。

ID	カテゴリ	アドレス	ターゲットポート
11	最適化が必要	13.107.64.0/18、52.112.0.0/14、52.122.0.0/15	**UDP**：3478、3479、3480、3481、**TCP**：443（フォールバック）

これらの範囲には、Azure Load Balancer によって前処理されたトランスポートリレーとメディアプロセッサの両方が含まれます。
Microsoft Teams トランスポートリレーは、STUN および TURN 機能を提供しますが、ICE エンドポイントではありません。また、Microsoft Teams トランスポートリレーはメディアや TLS を終了せず、トランスコード処理も実行しません。ほかのピアまたはメディアプロセッサにトラフィックを転送するときに、TCP（HdxRtcEngine.exe が TCP を使用している場合）を UDP に中継できます。

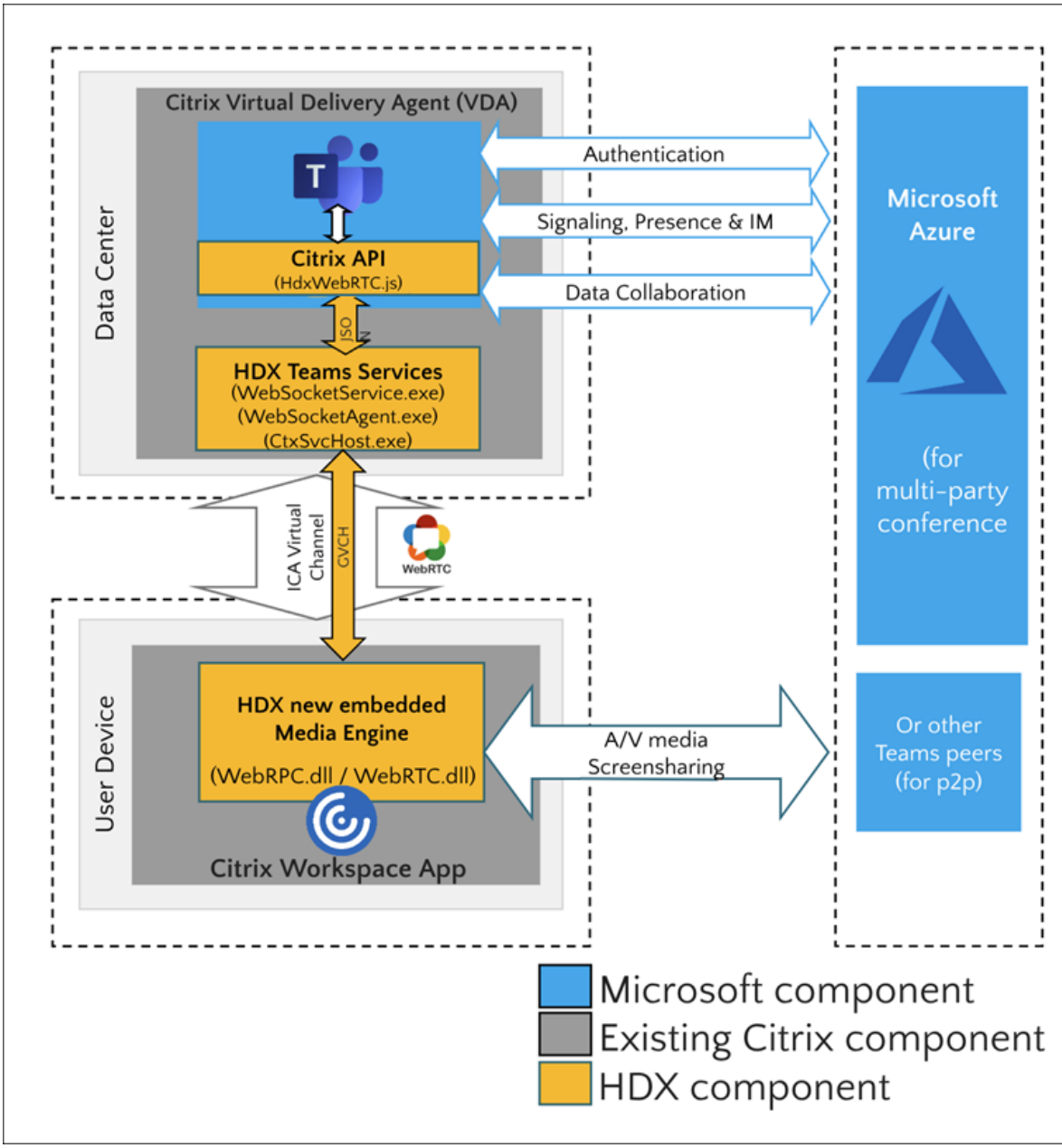
Workspace アプリの WebRTC メディアエンジンは、Microsoft 365 クラウド内の最も近い Microsoft Teams トランスポートリレーと通信します。メディアエンジンは、エニーキャスト IP とポート 3478～3481 UDP（ワークロードごとに異なる UDP ポート、多重化によって発生する場合あり）またはフォールバックに 443 TCP/TLS を使用します。通話品質は、基盤となるネットワークプロトコルによって異なります。UDP は常に TCP よりも推奨されるため、ブランチオフィスの UDP トラフィックに対応するようネットワークを設計することをお勧めします。

Microsoft Teams が最適化モードで読み込まれ、HdxRtcEngine.exe がエンドポイントで実行されている場合、ICE の失敗により、通話のセットアップエラーが発生するか、オーディオ/ビデオが一方通行になります。通話を完了できない場合、またはメディアストリームが全二重でない場合は、最初にエンドポイントの **Wireshark** トレースを確認してください。ICE 候補の収集プロセスについて詳しくは、「サポート」セクションの「ログの収集」を参照してください。

> 注:
>
> エンドポイントにインターネットアクセスがない場合でも、エンドポイントの両方が同じ LAN 上にあれば、ユーザーはピアツーピア通話ができる可能性があります。会議は失敗します。この場合、通話のセットアップが始まる前に 30 秒のタイムアウトがあります。

通話のセットアップ

このアーキテクチャ図は、通知フローシーケンスの視覚的なリファレンスとして使用します。対応する手順が図に示されています。



アーキテクチャ

1. Microsoft Teams を起動します。
2. Microsoft Teams が O365 に認証します。テナントポリシーが Microsoft Teams クライアントにプッシュダウンされ、関連する TURN およびシグナリングチャネル情報がアプリに中継されます。
3. Microsoft Teams は VDA で実行されていることを検出し、Citrix JavaScript API への API 呼び出しを行います。
4. Microsoft Teams 内の Citrix JavaScript は、VDA 上で実行されている WebSocketService.exe へのセキュアな WebSocket 接続を開き、ユーザーセッション内で実行される WebSocketAgent.exe を起動します。
5. WebSocketAgent.exe は、Citrix HDX Microsoft Teams リダイレクトサービス（CtxSvcHost.exe）を呼

び出すことによって、汎用仮想チャネルをインスタンス化します。

6. Citrix Workspace アプリの wfica32.exe（HDX エンジン）は、Microsoft Teams の最適化に使用される新しい WebRTC エンジンである HdxRtcEngine.exe という新しいプロセスを生成します。
7. Citrix メディアエンジンと Teams.exe は、双方向仮想チャネルパスを持ち、マルチメディア要求の処理を開始できます。

   ––ユーザー呼び出し――

8. ピア **A** が 呼び出し ボタンをクリックします。Teams.exe は Microsoft 365 の Microsoft Teams サービスと通信し、ピア **B** とのエンドツーエンドのシグナリングパスを確立します。Microsoft Teams は、サポートされている一連の呼び出しパラメーター（コーデック、解像度など、セッション記述プロトコル（SDP）サービスとして知られています）を HdxRtcEngine に要求します。これらの呼び出しパラメーターは、Microsoft 365 の Microsoft Teams サービスへのシグナリングパスを使用して、そこからほかのピアに中継されます。
9. SDP オファーまたは応答（シングルパスネゴシエーション）はシグナリングチャネル経由で実行され、ICE 接続チェック（STUN バインド要求を使用した NAT およびファイアウォールトラバーサル）が完了します。次に、Secure Real-time Transport Protocol（SRTP）メディアは、HdxRtcEngine.exe とほかのピア（または会議の場合は Microsoft 365 会議サーバー）の間で直接やり取りされます。

Microsoft 電話システム

電話システムは、Microsoft Teams を使用して Microsoft 365 クラウドで通話制御および PBX を有効にする Microsoft のテクノロジです。Microsoft Teams の最適化は、Microsoft 365 通話プランまたはダイレクトルーティングを使用する電話システムをサポートします。ダイレクトルーティングを使用すると、オンプレミスのソフトウェアを追加しなくても、サポートされている独自のセッションボーダーコントローラーを Microsoft 電話システムに直接接続できます。
通話キュー、転送、自動転送、保留、ミュート、および通話の再開がサポートされています。

DTMF

デュアルトーンマルチ周波数（DTMF）機能は、次のバージョン以降の Citrix Workspace アプリでサポートされています:

- Windows 向け Citrix Workspace アプリバージョン 2102
- Windows 向け Citrix Workspace アプリ LTSR 1912 CU5（Windows 10 OS のみ）
- Linux 向け Citrix Workspace アプリバージョン 2101
- Mac 向け Citrix Workspace アプリバージョン 2101
- ChromeOS 向け Citrix Workspace アプリバージョン 2111.1

動的緊急通報（**Dynamic e911**）のサポート

バージョン 2112 以降、Citrix Workspace アプリは動的な緊急通報をサポートしています。Microsoft 通話プラン、Operator Connect、ダイレクトルーティングで使用すると、以下を実行できます：

- 緊急電話の構成とルーティング
- セキュリティ担当者への通知。

通知は、VDA で実行されている Microsoft Teams クライアントではなく、エンドポイントで実行されている Citrix Workspace アプリの現在の場所に基づいて送信されます。

Ray Baum 法では、緊急車両を派遣可能な 911 発信者の位置情報を、適切な公衆安全応答ポイント（PSAP）に送信する必要があります。以下のバージョンの Citrix Workspace アプリで使用する場合、HDX を使用した Microsoft Teams 最適化は Ray Baum 法に準拠しています：

- Windows 向け Citrix Workspace アプリバージョン 2112.1 以降
- Linux 向け Citrix Workspace アプリバージョン 2112 以降
- Mac 向け Citrix Workspace アプリバージョン 2112 以降
- ChromeOS 向け Citrix Workspace アプリバージョン 2112 以降

動的緊急通報を有効にするには、管理者は Microsoft Teams 管理センターを使用し、以下を構成して、ネットワークまたは緊急事態発生位置マップを作成する必要があります：

- ネットワーク設定
- 位置情報サービス（Location Information Service：LIS）

動的緊急通報について詳しくは、Microsoft 社のドキュメントを参照してください。

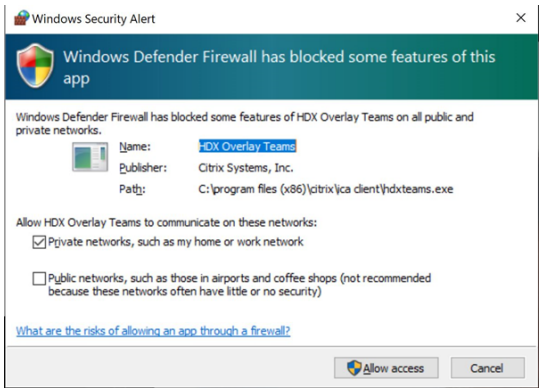
Citrix Workspace アプリが Microsoft Teams に送信する派遣可能な位置情報は次のとおりです：

- イーサネット/スイッチ接続にリンク層検出プロトコル（Link Layer Discovery Protocol：LLDP）を使用するシャーシ ID/ポート ID イーサネット/スイッチ（LLDP）は、以下でサポートされています：
  - Windows バージョン 8.1 および 10
  - macOS（LLDP 対応ソフトウェアが必要です）LLDP 対応ソフトウェアをダウンロードするには、`www.microsoft.com`にアクセスして、LLDP 対応ソフトウェアを検索してください。
  - Linux（LLDP ライブラリが、シンクライアントのオペレーティングシステム（OS）ディストリビューションに含まれている必要があります）。
- WLAN BBSID および Citrix Workspace アプリがインストールされているエンドポイントの {IPv4-IPv6; サブネット; MAC アドレス}。
  - サブネットおよび WiFi ベースの場所情報は、Windows、Linux、および Mac 用の Workspace アプリでサポートされています。
- 緯度と経度（Citrix Workspace アプリがインストールされている OS レベルにおいてユーザー権限が付与されている場合。権限は HDX RTC Engine に設定されている）

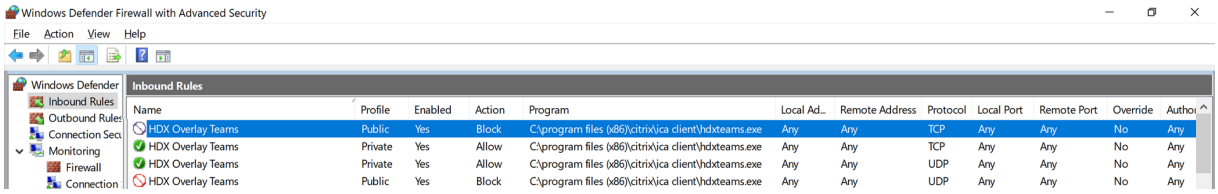
- すべての Workspace アプリプラットフォームでサポートされています。ただし、Linux 向け Citrix Workspace の場合、シンクライアントの OS ディストリビューションに`libgps`ライブラリを含める必要があります（>sudo apt-get install libgps23 gpsd lldpd）。

ファイアウォールについての考慮事項

ユーザーが初めて Microsoft Teams クライアントを使用して最適化された呼び出しを開始すると、**Windows** ファイアウォール設定の警告が表示されることがあります。この警告は、HdxTeams.exe または HdxRtcEngine.exe（HDX Overlay Microsoft Teams）の通信を許可するようユーザーに求めます。



以下の 4 つのエントリが ［セキュリティが強化された **Windows Defender** ファイアウォール］コンソールの ［受信規則］に追加されます。必要に応じて、より制限的な規則を適用できます。

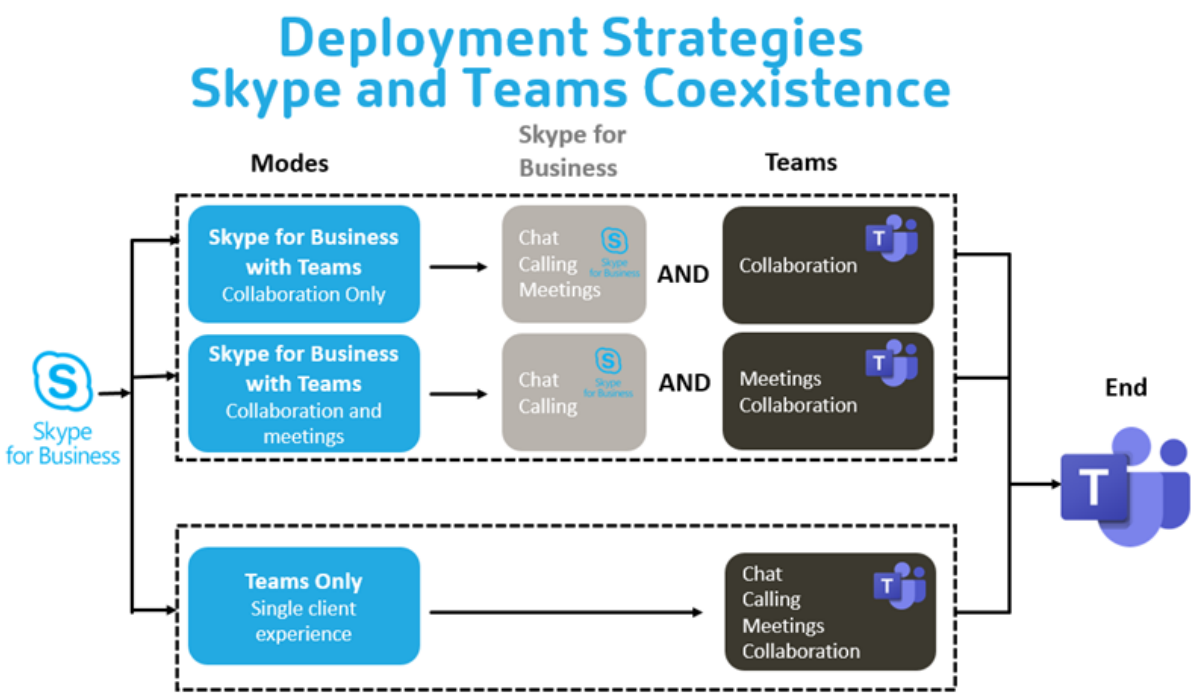


Microsoft Teams と **Skype for Business** の共存

Microsoft Teams と Skype for Business を、機能が重複する 2 つの個別のソリューションとして並べて展開できます。
詳しくは、「Microsoft Teams と Skype for Business の共存と相互運用性の理解」を参照してください。

Microsoft Teams マルチメディアエンジン用の Citrix RealTime Optimization Pack および HDX 最適化は、環境で設定された構成を尊重します。例としては、アイランドモードや Skype for Business と Microsoft Teams のコラボレーションがあります。また、Skype for Business と Microsoft Teams のコラボレーションと会議もあります。

周辺機器アクセス権限は、一度に 1 つのアプリケーションにのみ付与されます。たとえば、通話中に RealTime Media Engine が Web カメラにアクセスすると、通話の間、イメージデバイスがロックされます。デバイスがリリースされると、Microsoft Teams で使用できるようになります。



Citrix SD-WAN：**Microsoft Teams** 向けに最適化されたネットワーク接続

オーディオとビデオの最適な品質には、Microsoft 365 クラウドへのネットワーク接続で低遅延、低ジッター、低パケット損失が必要です。Citrix Workspace アプリユーザーによるブランチオフィスからデータセンターへの Microsoft Teams 音声ビデオ RTP トラフィックのバックホールで追加の遅延が発生することがあります。また、WAN リンクで輻輳が発生することがあります。Citrix SD-WAN は Microsoft 365 ネットワーク接続の原則に従って、Microsoft Teams の接続を最適化します。Citrix SD-WAN は、Microsoft REST ベースの Microsoft 365 IP アドレスと Web サービス、および近接 DNS を使用します。この用途は、Microsoft Teams のトラフィックを識別、分類、誘導するためのものです。

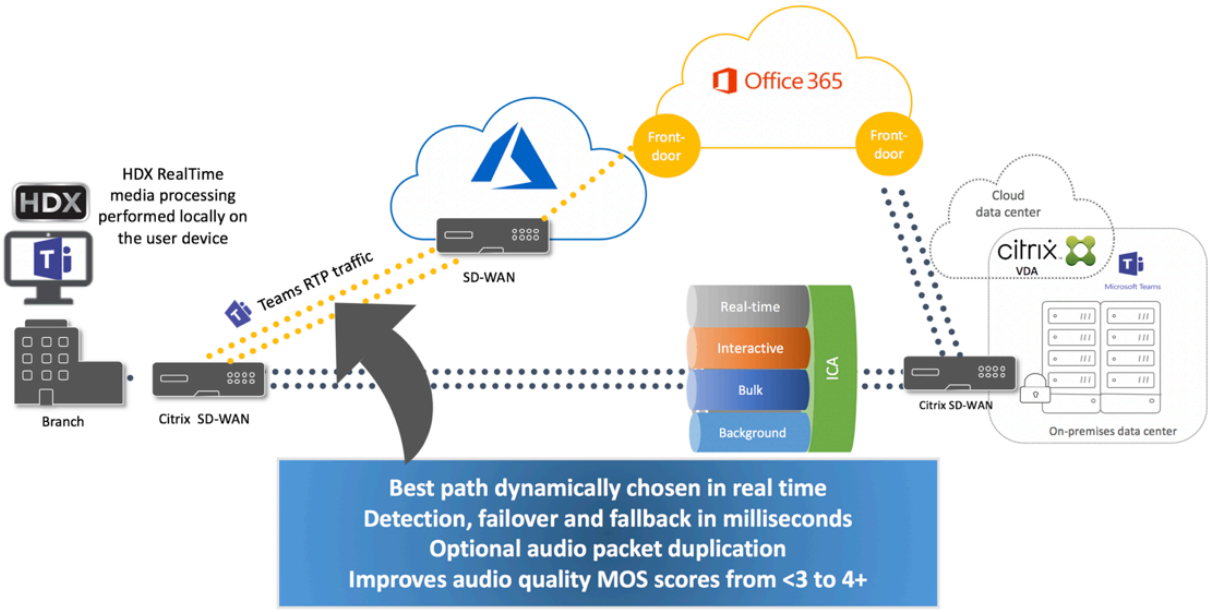
多くの地域のビジネス用ブロードバンドインターネット接続は、断続的なパケット損失、過度のジッター期間、停止に悩まされています。

Citrix SD-WAN は、ネットワークの状態がさまざまに異なる場合、または低下している場合、Microsoft Teams のオーディオ/ビデオ品質を保持する 2 つのソリューションを提供します。

- Microsoft Azure を使用している場合、Azure VNET で導入された Citrix SD-WAN 仮想アプライアンス（VPX）は、高度な接続の最適化を提供します。これらの最適化には、シームレスなリンクフェールオーバーとオーディオパケットトレースが含まれます。
- Citrix SD-WAN のお客様は Citrix Cloud Direct サービスを介して Microsoft 365 に接続できます。このサービスは、すべてのインターネットのトラフィックに信頼できる安全な配信を提供します。

ブランチオフィスのインターネット接続の品質が問題にならない場合は、遅延を最小限に抑えるのに十分な可能性があります。Microsoft Teams のトラフィックを、Citrix SD-WAN ブランチアプライアンスから一番近い Microsoft

365 フロントドアに直接誘導して、遅延を最小限に抑えます。詳しくは、「Citrix SD-WAN Office 365 の最適化」を参照してください。



マルチウィンドウ会議とチャット

Windows の Microsoft Teams では、複数の会議またはチャットウィンドウを使用できます。ポップアウト機能について詳しくは、Microsoft 365 サイトのMicrosoft Teams のチャットおよび会議でのポップアウトウィンドウに関する記事を参照してください。

> 注:
>
> この機能は、Windows 2112.1、Mac 2203、Linux 2203、および ChromeOS 2303 向けの Citrix Workspace アプリでサポートされています。この場合 VDA 2112 以降が必要であり、1912 CU6 以降 LTSR にバックポートされました。

背景のぼかしと効果

Windows 向け、Mac 向け、Linux 向けおよび ChromeOS/HTML5 向け Citrix Workspace アプリで、HDX を使用した Microsoft Teams の最適化における背景のぼかしと効果がサポートされます。

背景をぼかしたり、デフォルト画像に置き換えたりして、会話中にシルエット（体と顔）に集中できるようにすることで、集中力が乱されることを回避できます。この機能は、P2P 通話または電話会議で使用できます。

> 注:
>
> この機能は、Microsoft Teams の UI/ボタンと統合されています。マルチウィンドウのサポートは、VDA を 2112 以降に更新するときに必要な前提条件です。詳しくは、「マルチウィンドウ会議とチャット」を参照して

> ください。

背景のぼかしと効果に関する Microsoft Teams UI コントロールを利用するには、次の最小バージョンが必要です:

- Windows 向け Citrix Workspace アプリ 2207
- Mac 向け Citrix Workspace アプリ 2301
- Linux 向け Citrix Workspace アプリ 2307
- ChromeOS 向け Citrix Workspace アプリ 2303

制限事項:

- クライアントで背景画像を Microsoft Teams のデフォルト画像に置き換えるときは、デバイスをインターネットに接続する必要があります。
- 管理者およびユーザーが定義した背景画像の置き換えは Microsoft Teams の UI ではサポートされていません。カスタムの背景画像は、画像がクライアントにも保存されている限り、構成設定を使用して設定できます。

カスタムの背景画像の設定

次のレジストリキーは、Microsoft Teams UI を使用して機能を制御する予定がない場合、または管理者がデフォルトの動作を上書きしたい場合にのみ必要です。たとえば、エンドポイントの性能が十分ではないため、背景のぼかしを無効にするなど。

Windows の場合　カスタムの背景画像を設定するには、管理者またはエンドユーザーがクライアントまたはエンドポイントで次のレジストリキーを構成する必要があります:

場所: `HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXMediaStream`

- 値の名前: VideoBackgroundEffect
- 種類: DWORD
- 値: 0（無効）、1（有効）、2（背景画像の置換）

値を 1 に設定すると、背景がぼやけます。エンドユーザーまたは管理者がこの値を設定できます。

値を 2 に設定するには、**VideoBackgroundImage** キーも存在する必要があります。この値を設定できるのは管理者だけです。次のキーは、背景画像を置き換えたい場合にのみ必要であり、ぼかしには必要ありません:

- 値の名前: VideoBackgroundImage
- 種類: REG_SZ
- 値: my_image_name.jpeg

ビデオの背景画像は`C:\Program Files (x86)\Citrix\ICA Client`ディレクトリに格納されている必要があります。

このレジストリ構成によって、Microsoft Teams UI セレクターを使用せずに、Citrix Workspace アプリ 2206 で背景のぼかしまたは画像の置換を有効にすることもできます。つまり、環境または VDA がマルチウィンドウをサポートしていない場合でも、Citrix Workspace アプリ 2206 以降で HKEY_CURRENT_USER レジストリによる回避策を適用して同様の結果を得ることができます。ただし、ユーザーは HDX セッションまたは Microsoft Teams 通話中に機能を制御することはできません。

レジストリキーの変更は、HDX セッションが接続されたときにのみ有効になります。

Mac の場合　ユーザーがダウンロードした画像の場所：*/Users/username/Downloads/any_image.png*

次のコマンドを実行して、カスタム画像をデフォルトの画像として設定します：

```
defaults write com.citrix.HdxRtcEngine VideoBackgroundEffect -int 2

defaults write com.citrix.HdxRtcEngine VideoBackgroundImage -string "
/Users/username/Downloads/any_image.png"
```

Linux の場合　ユーザーがダウンロードした画像の場所：*/home/username/Downloads/any_image.jpg*

ファイル*/var/.config/citrix/hdx_rtc_engine/config.json* を作成して、次の構成キーを JSON 形式で追加します。たとえば、

```
{


"VideoBackgroundEffect":2,

"VideoBackgroundImage":"/home/username/Downloads/any_image.jpg"

 }
```

HTML5 の場合

1. **HTML5Client** フォルダーの **configuration.js** ファイルに移動します。
2. **backgroundEffects** 属性を追加し、この属性を **true** に設定します。たとえば、

```
'features' : {

    'msTeamsOptimization' :
    {

        'backgroundEffects' : true
     }

 }
```

3. 変更を保存します。

クライアントの **CPU** 消費に関する考慮事項

ぼかし機能による CPU への影響はわずかですが、消費量の増加が予想されます。たとえば、最大 2.8GHz のターボブーストを利用した 4 コア、1.5GHz の Intel® Pentium® Silver チップを搭載したシンクライアントでは、背景のぼかしによって CPU 使用率が約 2% 上昇します。平均 CPU 使用率は 20% 未満です。

Microsoft Teams のギャラリービューとアクティブスピーカー

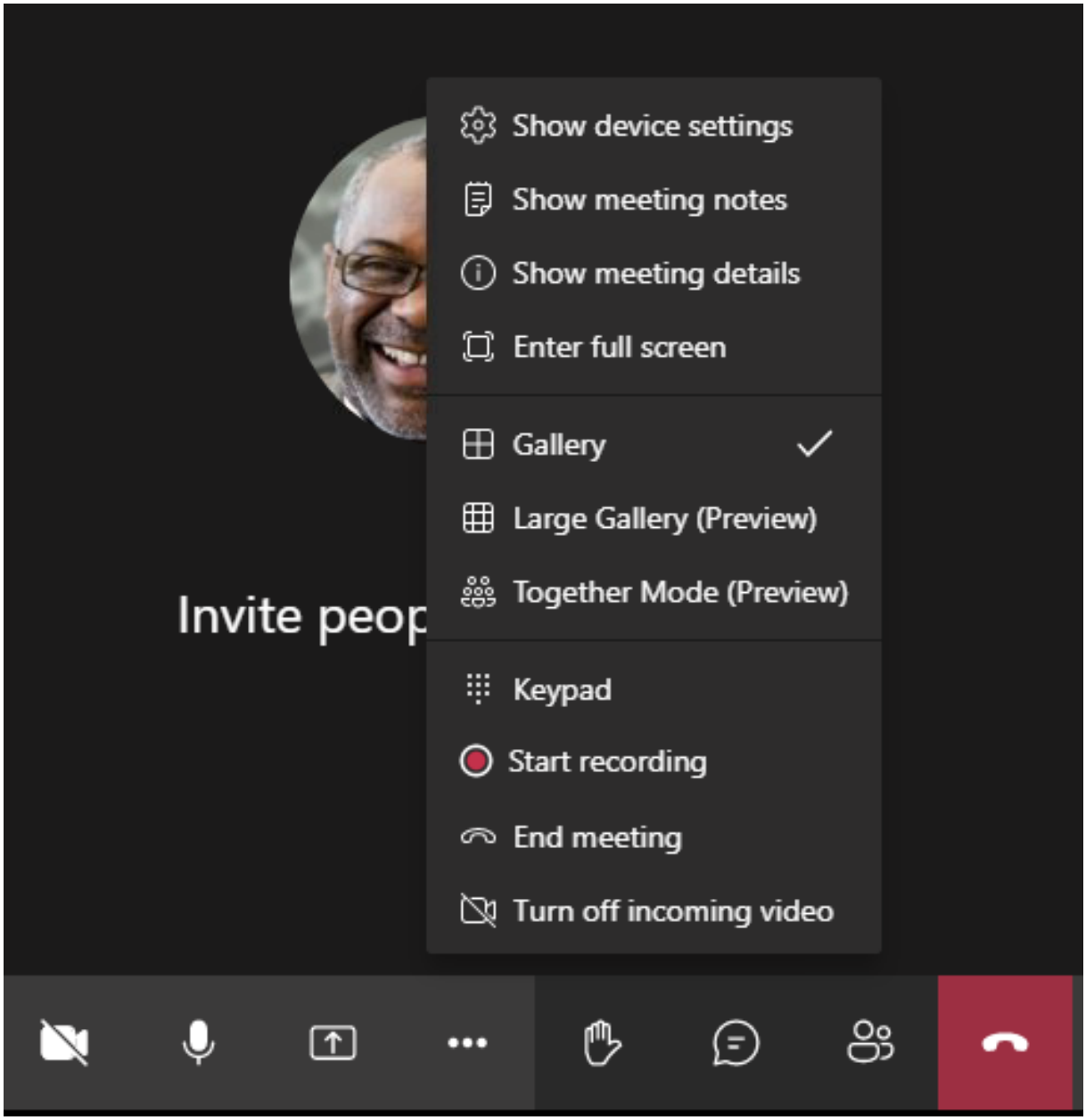
Microsoft Teams は、［ギャラリー］、［大きいギャラリー］、および［集合モード］のレイアウトをサポートしています。

Microsoft Teams は、4 人の参加者のビデオストリームによる 2x2 グリッドを表示します（ギャラリーと呼ばれます）。この場合、Microsoft Teams はデコードのために 4 つのビデオストリームをクライアントデバイスに送信します。ビデオを共有している参加者が 4 人を超える場合、最新の 4 人のうち最もアクティブなスピーカーのみが画面に表示されます。

Microsoft Teams は、最大 7x7 のグリッドを表示する大きなギャラリービューも提供します。その結果、Microsoft Teams 会議サーバーは単一のビデオフィードを合成し、それをデコードのためにクライアントデバイスに送信するため、CPU 消費量を抑えられます。この単一のマス目形式のフィードには、ユーザーのセルフプレビュービデオも含まれることがあります。

最後に、Microsoft Teams は、新しい会議エクスペリエンスの一部である集合モードをサポートしています。Microsoft Teams は、AI セグメンテーションテクノロジを使用して参加者を共有の背景にデジタルで配置し、すべての参加者を同じホールの客席に表示します。

ユーザーは、省略記号メニューで［ギャラリー］、［大きいギャラリー］、または［集合モード］のレイアウトを選択することにより、会議中にこれらのモードを制御できます。



ビデオのアスペクト比の制限のサポート（Windows 向け Citrix Workspace アプリ 2102、Linux 向け Citrix Workspace アプリ 2106、MAC 向け Citrix Workspace アプリ 2106 以降）:

- ［**Fill to frame**］オプションは、［Gallery］ビューまたは［Large Gallery］ビューで使用できます。このオプションにより、サブウィンドウに収まるようにビデオサイズがトリミングされます。一方、［**Fit to frame**］を使用すると、ビデオの側面に黒いバー（レターボックス）が表示され、トリミングが行われません。

次の表に、［ギャラリー］と［大きいギャラリー］のレイアウトの比較を示します:

	［ギャラリー］ビュー 2x2（デフォルト）	［大きいギャラリー］ビュー
レイアウト/グリッド	4 人の参加者がいるビデオストリームでは 2x2 のグリッドが表示されます。直近の最もアクティブなスピーカー 4 人のみが画面に表示され、他の参加者はグリッドに表示されません。	49 人の参加者がいるビデオストリームでは 7x7 のグリッドが表示されます。
ミキシング技法	メディアルーターは、各参加者からすべてのユーザーに個々のストリームを転送します。	中央会議サーバーは、すべてのオーディオまたはビデオをミキシングおよびトランスコードして、参加者ごとに調整した複合レイアウトを作成します。この操作により、さらに遅延が発生します。
アクティブなスピーカー	新しいアクティブなスピーカーは、グリッド内で最もアクティブでないスピーカーに取って代わります。	アクティブか非アクティブかに関係なく、すべての参加者が表示されます。
エンドポイントでのエンコード	サイマルキャストが有効な場合、1 つまたは複数のビデオストリームがエンドポイントでエンコードされる可能性があります。サイマルキャストのサポートについて詳しくは、「サイマルキャスト」を参照してください。	サイマルキャストが有効な場合、1 つまたは複数のビデオストリームがエンドポイントでエンコードされる可能性があります。サイマルキャストのサポートについて詳しくは、「サイマルキャスト」を参照してください。
エンドポイントでのデコード	各参加者は、最大 4 つの個別のメディアストリームを取得します。これにより、HdxRtcEngine.exe によるエンドポイントでの CPU 消費量が増加します（デコードおよびレンダリングのため）。	各参加者は、オーディオとビデオのストリームを 1 つだけ取得します。この設定により、エンドポイントでの CPU 消費量が減少します。
最大解像度	720p。4 人の参加者がビデオを共有している場合、最大解像度はビデオフィードあたり 360p です。参加者 4 人未満でビデオを共有している場合は、ビデオフィードあたりの解像度が高くなる可能性があります。	複合レイアウトまたはミキシングの場合は 720p です。複合レイアウトでは、参加者ごとに高品質のビデオストリームは必要ありません。この条件のため、各送信者が解像度やアップロードのビットレートを下げます。

	［ギャラリー］ビュー 2x2（デフォルト）	［大きいギャラリー］ビュー
「低速ユーザー」の問題	送信者は、各モダリティ（オーディオ、ビデオ、および画面共有）の品質を、参加者間で最も低い共通ネットワーク品質に変更します。このマルチメディアストリームは、その後、他のすべての参加者に転送されます。その結果、ネットワーク状態が悪い参加者が、その通話に参加している他のすべての人の品質に影響を与えます。	最も低品質な共通ネットワークのシナリオには左右されません。会議サーバーは、個々の参加者のネットワーク状態に基づいてさまざまな品質を提供します。
セルフプレビュー	自分自身を小さなサムネイルでリアルタイムで表示します。	自分自身をサムネイルで表示し、残りのビデオフィードとは区別しません。その結果、メインのビデオレイアウトに自分が含まれ、多少の遅延がさらに発生する場合があります。

Microsoft Teams の画面共有

Microsoft Teams は、H264 のようなビデオコーデックで共有されているデスクトップを効果的にエンコードし高画質ストリームを作成する、ビデオベースの画面共有（VBSS）に依存しています。HDX 最適化により、受信画面共有はビデオストリームとして扱われます。

Windows、Linux、または Mac 向けの Citrix Workspace アプリ 2109 以降および ChromeOS 向け Citrix Workspace アプリ 2303 以降のユーザーは画面とビデオカメラを同時に共有できます。

以前のバージョンでは、ビデオ通話の最中にほかのピアがデスクトップの共有を開始すると、元のカメラのビデオフィードが一時停止されます。代わりに、画面共有ビデオフィードが表示されます。その後、このピアは手動でカメラ共有を再開する必要があります。

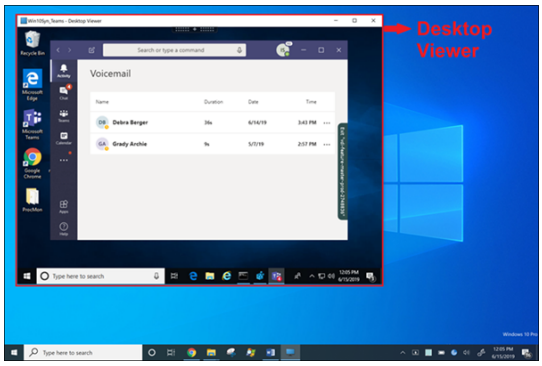
> **PowerPoint Live** に関するメモ
>
> PowerPoint Live のコンテンツを共有している場合、この制限はありません。その場合でも、他のピアは Web カメラとコンテンツを確認し、前後に移動して他のスライドを確認できます。このシナリオでは、スライドは VDA でレンダリングされています。PowerPoint Live スライドデッキにアクセスするには、共有トレイボタンをクリックして提案された PowerPoint スライドの 1 つを選択するか、［参照］をクリックしてコンピューターまたは OneDrive で PowerPoint ファイルを検索します。

発信画面共有も最適化され Citrix Workspace アプリにオフロードされます。この場合、メディアエンジンは、周りに赤い境界線が描画された Citrix Desktop Viewer（CDViewer.exe）ウィンドウのみをキャプチャして送信します。Desktop Viewer と重複するローカルアプリケーションはキャプチャされません。

> 注
>
> Mac 向け Citrix Workspace アプリでの特定の権限を設定して、画面共有を有効にします。詳しくは、「システム要件」を参照してください。

既知の制限事項:

- Desktop Viewer が無効になっている場合、または Desktop Lock が使用されている場合は、マルチモニターは Microsoft Teams のスクリーンピッカーで選択できません。Desktop Viewer は、`.ICA`ファイルテンプレートと`StoreFront web.config`のいずれかを編集したことで、無効になっている可能性があります。SHIFT+F2 ホットキーはマルチモニターの画面共有と互換性がありません。
- Workspace アプリの 2106 より前のバージョンでは、プライマリモニターのみが共有されます。仮想デスクトップ上のアプリケーションを、通話中のほかのピアのプライマリモニターにドラッグして表示します。
- 仮想モニターレイアウト機能（単一の物理モニターの論理パーティション）を使用して Citrix Workspace アプリを構成した場合は、マルチモニター画面共有が機能しないことがあります。この場合、すべての仮想モニターが 1 つの合成画像として共有されます。
- 古いバージョンの Windows 向け Citrix Workspace アプリ（1907 から 2008）では、クライアントマシンで実行されているローカルアプリケーションも共有されます。この共有は、ローカルアプリが Desktop Viewer の上に重なっている場合にのみ可能です。この動作は、2009.6 以降、および 1912 CU5 以降で削除されました。
- 画面共有中にウィンドウモードから全画面に変更すると、画面共有が停止します。画面共有を機能させるには、停止して再度共有する必要があります。
- 最適化された Microsoft Teams の特定の場所に共有制御を固定することはできません。
- 最小化されたアプリを共有する場合、アプリのタイトルバーも共有されることがあります。



シームレスアプリケーションからの画面共有:

Microsoft Teams をスタンドアロンのシームレスアプリケーションとして公開している場合、画面共有は、物理エンドポイントのローカルデスクトップをキャプチャします。Citrix Workspace アプリのバージョンは 1909 以降である必要があります。

アプリの共有

Windows 向け Citrix Workspace アプリ 2112.1 以降、および VDA 向け Citrix Workspace アプリ 2112 以降、Microsoft Teams はアプリ共有をサポートしています。

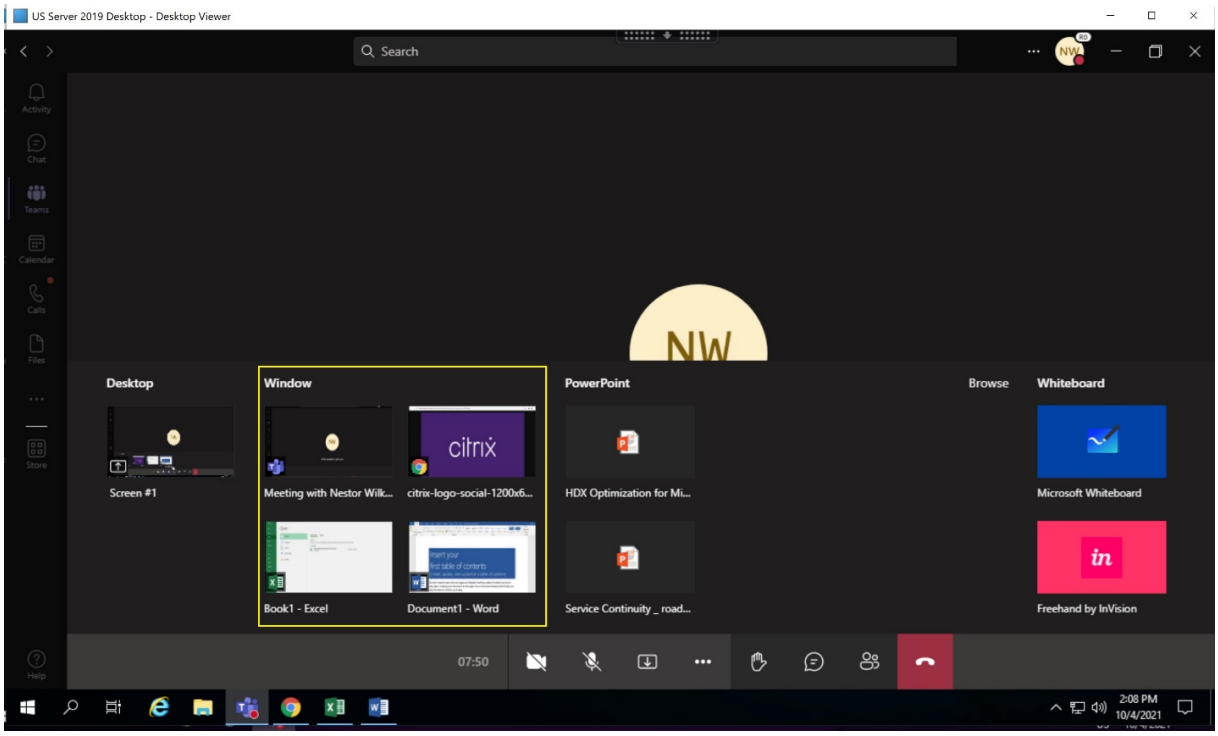
Citrix Workspace アプリの Windows 向け 2109、Mac 向け 2203、Linux 向け 2209、および VDA 向け 2109 以降では、Microsoft Teams が仮想セッションで実行されている特定のアプリの画面共有をサポートしています。最適化された Microsoft Teams を使用して、Java などのカスタム社内アプリケーションを共有することもできます。特定のアプリを共有するには:

1. リモートセッション内の Microsoft Teams アプリに移動します。
2. Microsoft Teams UI の ［コンテンツの共有］をクリックします。
3. 会議で共有するアプリを選択します。選択したアプリの周りに赤い枠線が表示され、通話中の同僚は共有アプリを確認できます。

別のアプリを共有するには、もう一度 ［コンテンツの共有］をクリックして、新しいアプリを選択します。

アプリの共有を無効にする場合は、`HKLM\SOFTWARE\Citrix\Graphics`の VDA に次のレジストリキーを作成します:
名前: `UseWsProvider`
種類: `DWORD`
値: 0

> 注:
>
> - アプリを最小化すると、Microsoft Teams は共有アプリの最後のイメージを表示します。ウィンドウを最大化すると、画面共有を再開できます。
> - 画面共有は、ウィンドウの VDA 側のキャプチャに依存します。その後、コンテンツは最大速度で Citrix Workspace アプリに中継されます。最大速度は毎秒 30 フレームです。Citrix Workspace アプリは、コンテンツをピアまたは会議サーバーに転送します。



特定のアプリの画面共有に関する既知の制限:

- アプリを画面共有しているときは、マウスポインターは表示されません。
- アプリを共有しているときにアプリを最小化すると、アプリアイコンのみがスクリーンピッカーに表示されます。アプリのサムネイルはスクリーンピッカーでプレビューされません。そのコンテンツを共有することはできず、アプリを最大化するまで赤い枠線は表示されません。
- LAA アプリは、VDA の最適化された Microsoft Teams のデスクトップアプリと共有できるアプリの一覧を表示します。ただし、一覧からアプリを選択すると、想定した結果にならない場合があります。

App Protection との互換性

特定のアプリの画面共有は、HDX 最適化の Microsoft Teams のアプリ保護機能と互換性があります。App Protection が有効になっているデリバリーグループからアプリまたはデスクトップを起動した場合は、特定のアプリを画面共有できます。

Microsoft Teams UI で ［コンテンツの共有］をクリックすると、画面選択メニューから ［デスクトップ］オプションが削除されます。開いているアプリを共有するために選択できるオプションは ［ウィンドウ］だけです。

> 注:
>
> アプリ保護が有効になっているデリバリーグループからアプリまたはデスクトップを起動すると、Windows 向け Citrix Workspace アプリ 2202 以前を使用している場合に、着信ビデオや画面共有を表示できません。

Microsoft Teams での制御の付与と要求　この機能は、Citrix Workspace アプリの以下のバージョンでサポートされています（VDA バージョンやオペレーティングシステム、シングルセッションかマルチセッションかには依存しません）:

- Windows 向け Citrix Workspace アプリバージョン 2112.1 以降
- Mac 向け Citrix Workspace アプリバージョン 2203.1 以降
- Linux 向け Citrix Workspace アプリバージョン 2203 以降
- ChromeOS 向け Citrix Workspace アプリバージョン 2303 以降

参加者が画面を共有しているときに、Microsoft Teams の通話中に制御を要求できます。制御できるようになると、共有画面に対して選択、編集、またはその他のキーボードとマウスのアクティビティを実行できます。

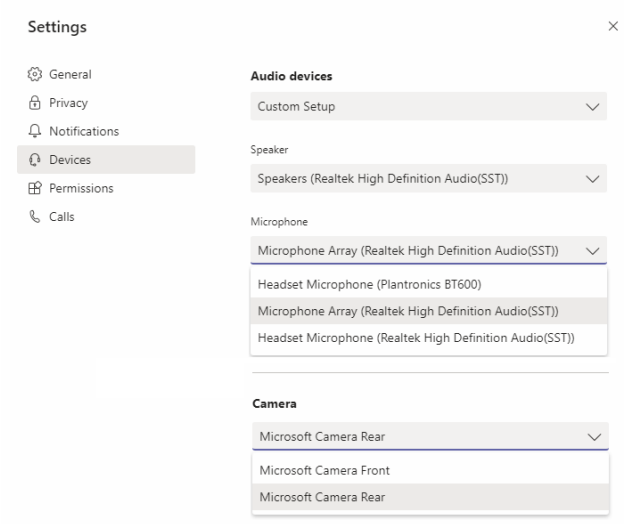
画面が共有されているときに制御を取得するには、Microsoft Teams UI の ［制御を要求］ボタンをクリックします。画面を共有している会議参加者は、要求を許可または拒否できます。

制御中は、共有画面に対して選択、編集、その他の変更を実行できます。これらの操作には、キーボードとマウスの両方を使用できます。入力が完了したら、［制御を要求］をクリックします。

> 制限事項:
>
> - ユーザーが単一のアプリを共有している場合（アプリ共有）、制御を渡したり要求したりはできません。デスクトップまたはモニター全体を共有する必要があります。
> - コントロールバーを特定の場所に固定する機能は使用できません。

Microsoft Teams の周辺機器

Microsoft Teams の最適化がアクティブな場合、Citrix Workspace アプリは周辺機器に（ヘッドセット、マイク、カメラ、スピーカーなど）にアクセスします。その後、周辺機器は Microsoft Teams UI に正しく表示されます（[設定] **>** ［デバイス］）。



Microsoft Teams はデバイスに直接アクセスしません。メディアの取得、キャプチャ、処理には、代わりに Workspace アプリの WebRTC メディアエンジンが使用されます。Microsoft Teams では、ユーザーが選択できるデバイスが一覧表示されます。

Microsoft Teams がアクティブなときに挿入される周辺機器は、デフォルトでは選択されていません。Microsoft Teams UI の ［設定］ > ［デバイス］画面で、周辺機器を手動で選択する必要があります。周辺機器が選択されると、Microsoft Teams は周辺機器の情報をキャッシュします。これにより、同じエンドポイントからセッションに再接続すると、周辺機器が自動的に選択されます。

推奨事項:

- エコーキャンセル機能が組み込まれた Microsoft Teams 認定ヘッドセット。マイクとスピーカーが別のデバイスにある複数周辺機器セットアップでは、エコーが発生することがあります。これは、マイクが Web カメラに内蔵されており、スピーカーがモニターに搭載されている場合などです。外部スピーカーを使用する場合は、マイクからできるだけ離して配置してください。また、マイクに音を反響させる可能性のある表面からも離して配置してください。詳しくは、www.microsoft.comにアクセスして、Microsoft Teams 認定ヘッドセットを検索してください。
- Microsoft Teams 認定のカメラ。ただし、Skype for Business 認定の周辺機器は Microsoft Teams と互換性があります。詳しくは、にアクセスして、Microsoft Teams 認定カメラと Skype for Business 認定周辺機器を検索してください。
- Citrix Workspace アプリのメディアエンジンは、オンボード H.264 エンコーディング-UVC 1.1 および 1.5 を実行する Web カメラで CPU オフロードを利用できません。

> 注:
>
> Windows 向け Workspace アプリ 2009.6 では、24 ビットのオーディオ形式または 96kHz を超える周波数のオーディオ形式の周辺機器を取得できるようになりました。
>
> HdxTeams.exe（Windows 2009 以前の Citrix Workspace アプリ内）は、次の特定のオーディオデバイス形式（チャネル、ビット深度、およびサンプルレート）のみをサポートします:
>
> - 再生デバイス：最大 2 チャネル、16 ビット、最大 96,000Hz の周波数
> - 録音デバイス：最大 4 チャネル、16 ビット、最大 96,000Hz の周波数
>
> 1 つのスピーカーまたはマイクが通常の設定と一致しない場合でも、Microsoft Teams のデバイス列挙は失敗し、［設定］**>**［デバイス］になしが表示されます。
> **HdxTeams.exe** の
> **Webrpc** ログはこのような情報を表示します:
>
> ```
> Mar 27 20:58:22.885 webrtcapi.WebRTCEngine Info: init. initializing
> ...
> Mar 27 20:58:23.190 webrtcapi.WebRTCEngine Error: init. couldn't
> create audio module!
> ```
>
> 回避策として、特定のデバイスを無効にするか、以下を実行します:
>
> 1. サウンドコントロールパネル（mmsys.cpl）を開きます。
> 2. 再生デバイスまたは録音デバイスを選択します。

> 3.［プロパティ］>［詳細設定］に移動し、サポートされているモードに設定を変更します。

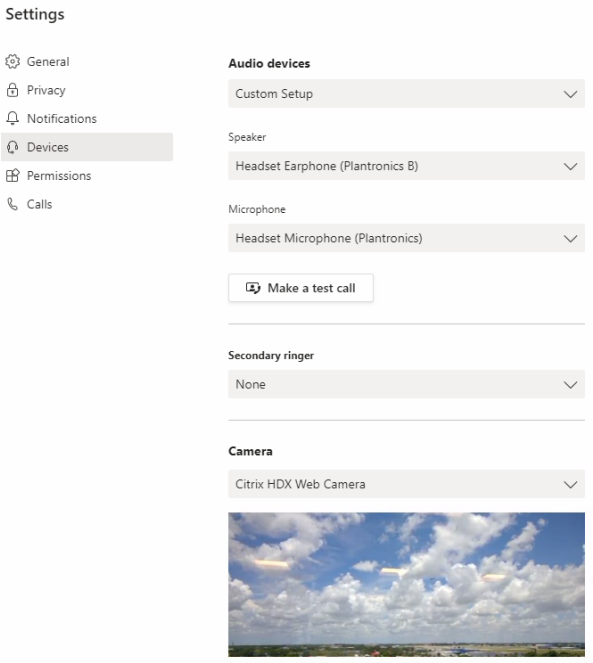
フォールバックモード

最適化された VDI モードで Microsoft Teams が読み込めない場合（Microsoft Teams/About/Version で「Citrix HDX Not Connected」と表示）、VDA では従来の HDX テクノロジにフォールバックされます。従来の HDX テクノロジとしては、Web カメラリダイレクトやクライアントのオーディオとマイクのリダイレクトなどが挙げられます。Microsoft Teams の最適化をサポートしていない Workspace アプリのバージョンまたはプラットフォーム OS を使用している場合は、フォールバックレジストリキーが適用されません。
フォールバックモードでは、周辺機器が VDA にマップされます。周辺機器は、Microsoft Teams アプリには仮想デスクトップにローカルで接続されているように表示されます。

VDA でレジストリキーを設定することで、フォールバックメカニズムを細かく制御できるようになりました。詳しくは、レジストリを使用して管理される機能の一覧にある「Microsoft Teams フォールバックモード」を参照してください。

この機能を使用するには、Microsoft Teams バージョン 1.3.0.13565 以降が必要です。

Microsoft Teams アプリの ［設定］>［デバイス］タブで表示されるカメラ名の違いで、最適化モードか非最適化モードかを判断できます。Microsoft Teams が非最適化モードで読み込まれた場合、従来の HDX テクノロジが起動します。以下の画像のように、Web カメラ名の冒頭には **Citrix HDX** が表示されます。スピーカーとマイクのデバイス名は、最適化モードと比べてわずかに異なる（または省略される）場合があります。



従来の HDX テクノロジを使用する場合、Microsoft Teams はオーディオ、ビデオ、および画面共有処理をエンドポイントの Citrix Workspace アプリ WebRTC メディアエンジンにオフロードしません。代わりに、HDX テクノロジでサーバー側でのレンダリングが使用されます。ビデオをオンにすると、VDA の CPU 消費量が高くなることが予想されます。リアルタイムのオーディオパフォーマンスは最適ではない場合があります。

既知の制限事項

Citrix の制限

Citrix Workspace アプリでの制限:

- HID ボタン - 応答と通話終了はサポートされていません。音量の増減はサポートされています。
- Microsoft Teams の管理センターの QoS（サービス品質）設定は、VDI ユーザーには適用されません。
- VDA で Snipping Tool を使用している場合、ユーザーは Microsoft Teams コンテンツのスクリーンショットを撮ることができません。ただし、Snipping Tool をクライアント側で使用した場合は、コンテンツをキャプチャできます。

VDA での制限:

- **Citrix Workspace** アプリの高 **DPI** 設定を「`Yes`」にすると、リダイレクトされたビデオウィンドウがずれて表示されます。この制限は、モニターの DPI スケールファクターが 100% を超えて設定されている場合に発生します。

Citrix Workspace アプリと VDA での制限:

- 最適化された通話の音量は、VDA ではなくクライアントマシンの音量バーでのみ制御できます。

サイマルキャスト

サイマルキャストのサポートは、Windows および Mac での最適化された Microsoft Teams ビデオ会議通話に対して有効になっています。Linux の場合は、シンクライアントのベンダーに確認してください。
サイマルキャストでは、すべての発信者に最適な通話エクスペリエンスを提供できる適切な解像度に適応しているため、さまざまなエンドポイントでのビデオ会議通話の品質とエクスペリエンスが向上します。

この向上したエクスペリエンスにより、各ユーザーは、エンドポイントの機能、ネットワークの状態などのいくつかの要因に応じて、複数のビデオ ストリームを異なる解像度（720p、360p など）で配信できます。次に、受信側のエンドポイントは、可能な範囲で最高品質の解像度を要求します。これにより、すべてのユーザーに最適なビデオ体験を提供できます。

> 注:
>
> この機能は、Microsoft Teams からの更新のロールアウト後にのみ使用できます。ETA については、https://www.microsoft.com/にアクセスし、Microsoft 365 ロードマップを検索してください。Microsoft によって更新プログラムがロールアウトされたら、ドキュメントのアップデートおよび発表内容について、CTX253754を確認することができます。

Microsoft の制限

- 3x3 ギャラリービューはサポートされていません。Microsoft Teams の依存関係 - 3x3 グリッドの実装予定については、Microsoft にお問い合わせください。

- Skype for Business との相互運用性は音声通話に限定され、ビデオのモダリティはありません。
- 受信および発信ビデオストリームの最大解像度は 720p です。
- PSTN 通話の呼び出し音はサポートされていません。
- ダイレクトルーティングのメディアバイパスはサポートされていません。
- ブロードキャストおよびライブイベントのプロデューサーの役割とプレゼンターの役割はサポートされていません。参加者の役割はサポートされていますが、最適化されていません（代わりに VDA でレンダリングされます）。
- Microsoft Teams のズームインおよびズームアウト機能はサポートされていません。
- 場所ベースのルーティング（LBR）およびメディアバイパスはサポートされていません。
- 通話の結合はサポートされていません（このオプションはユーザーインターフェイスに表示されません）。

Citrix と **Microsoft** の制限

- 画面共有を行うと ［システムオーディオを含める］オプションを使用できません。
- サイマルキャストは ChromeOS ではサポートされていません。

EOL 予定の **Microsoft Teams** シングルウィンドウ

2024 年 1 月 31 日、Microsoft は VDI で Microsoft Teams 最適化を使用した場合のシングルウィンドウ UI に対するサポートを終了し、マルチウィンドウ エクスペリエンスのみをサポートします。Microsoft は、この機能廃止について M365 管理センターで 2023 年 9 月 8 日（投稿 ID：MC674419）に発表しました。
マルチウィンドウ機能について公開された詳細情報については、Tech Community の記事「New Meeting and Calling Experience in Microsoft Teams」を参照してください。

> 注:
>
> Citrix は、引き続きビデオと画面共有が最適化されたモードで Microsoft Teams を使用するには、VDA および Citrix Workspace アプリをサポートされているバージョンにアップグレードすることをお勧めします。マルチウィンドウをサポートするためにインフラストラクチャとエンドポイントをアップグレードしない場合、通話、ビデオ通話、画面共有が最適化されなくなります。これにより、通話品質の問題、遅延の増加、サーバーの負荷の増加が発生する可能性があります。

次の表は、Citrix VDI 上の Microsoft Teams で最適化された通話を引き続き使用するために必要な VDA および Citrix Workspace アプリの最小バージョン、LTSR バージョン、および推奨バージョンを示しています:

コンポーネント	最小バージョン（1）	LTSR でサポートされているバージョン（2）	推奨バージョン（3）
Microsoft Teams	1.5.00.11865	該当なし	最新バージョン
VDA	1912 CU6 LTSR、2109 CR、2203 LTSR	1912 CU8 以降、2203 LTSR CU2 以降（4）	2308 CR 以降

コンポーネント	最小バージョン（1）	LTSR でサポートされているバージョン（2）	推奨バージョン（3）
Windows 向け Citrix Workspace アプリ	2112.1 CR	2203 CU2 以降（4）	2309 CR 以降
Mac 向け Citrix Workspace アプリ	2203 CR	該当なし	2308 CR 以降
Linux 向け Citrix Workspace アプリ	2202 CR	該当なし	2308 CR 以降
ChromeOS または HTML5 向け Citrix Workspace アプリ	2303 CR	該当なし	2309 CR 以降

> 注：
>
> 1. 最小バージョン：これは、マルチウィンドウが最初に導入されたバージョンです。ここに記載されている最小バージョンの一部は、製品終了になっている可能性があります。
> 2. サポートされている LTSR バージョン：これは、Citrix によってマルチウィンドウがサポートされている LTSR バージョンです。これらの LTSR リリースの古いバージョンは動作する可能性がありますが、新しい LTSR CU バージョンがリリースされると、それらのバージョンのサポートは利用できなくなります。LTSR サポートポリシーについて詳しくは、「https://support.citrix.com/article/CTX205549/faq-citrix-virtual-apps-and-desktops-and-citrix-hypervisor-long-term-service-release-ltsr」を参照してください。
> 3. 推奨バージョン：これは、ユーザー/顧客がソフトウェアのアップグレードを選択する場合に Citrix が推奨するソフトウェアのバージョンです。これらはすべて CR バージョンです。
> 4. VDA のバージョン 2203 LTSR および Citrix Workspace アプリの基本バージョンには、マルチウィンドウ機能が含まれています。これらのバージョンは、正式にサポートされているバージョンである最新の CU に置き換えられました。お客様は、これらのサポートされていないバージョンを自らの裁量で引き続き使用することができます。Citrix は、LTSR リリースを使用しているお客様が最新の CU にアップグレードすることをお勧めします。

WebRTC による **SDP** 形式（**Plan B**）の廃止に関する情報

Citrix は、将来のリリースで WebRTC による現在の SDP 形式（Plan B）のサポートを廃止する予定です。最適化された Microsoft Teams 機能をサポートするには、WebRTC で Unified Plan を使用する必要があります。

影響を受ける製品

Citrix Workspace アプリケーションの今後のリリースのいずれかでは、Citrix Workspace アプリの次期リリースのエンドポイントと Citrix Workspace アプリ 2108 以前のバージョンのエンドポイント間の通話はサポートされな

くなります。互換性がなくなる通話には、1912 LTSR Citrix Workspace アプリ クライアント (CWA) が含まれます。次の Citrix Workspace アプリクライアントが影響を受けます:

- Windows 向け Citrix Workspace アプリ
- Linux 向け Citrix Workspace アプリ
- Mac 向け Citrix Workspace アプリ
- Chrome 向け Citrix Workspace アプリ

Plan B を置き換える

2109 よりも古いバージョンの Citrix Workspace アプリを実行している場合は、サポートされているバージョン（可能であれば最新の CR リリース）にアップグレードする必要があります。そうしないと、将来のリリースまたは新しいエンドポイントで通話が接続できません。連携パートナーが Citrix Workspace をアップグレードしていない場合、将来のリリースと連携通信パートナー間の通話も失敗する可能性があります。

Citrix Workspace アプリバージョン 2108 のサポート期限は 2023 年 3 月に終了しているため、新しいバージョンにアップグレードする必要があります。詳しくは、Workspace アプリで Citrix Workspace アプリのバージョンサポートの詳細を参照してください。

Plan B の廃止について詳しくは、WebRTCのドキュメントを参照してください。

追加情報

- Microsoft Teams の監視、トラブルシューティング、およびサポート
- Microsoft Teams デスクトップアプリの仮想マシンへの展開
- MSI を使用した Microsoft Teams のインストール（VDI インストールセクション）
- シンクライアント
- Skype for Business ネットワーク評価ツール
- Microsoft Teams と Skype for Business の共存と相互運用性の理解

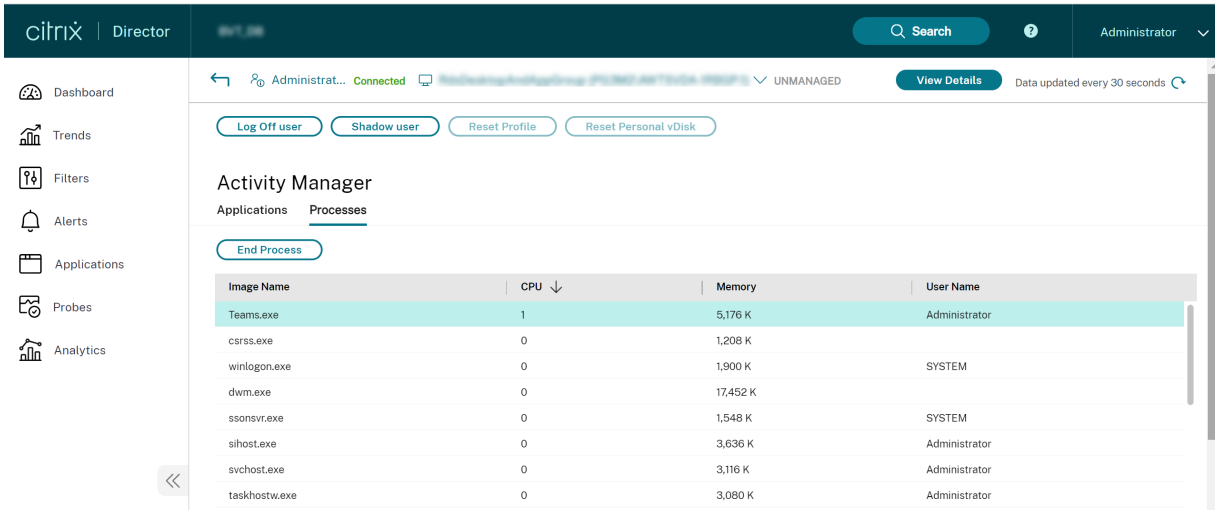
Microsoft Teams の監視、トラブルシューティング、およびサポート

August 17, 2024

Teams の監視

このセクションでは、HDX による Microsoft Teams の最適化を監視するためのガイドラインを提供します。
最適化モードで実行していて、`HdxRtcEngine.exe`がクライアントマシンで実行されている場合、

WebSocketAgent.exeと呼ばれる VDA のプロセスがセッションで実行されています。Director で ［アクティビティマネージャー］を使用してアプリケーションを表示します。



Microsoft Teams 最適化の状態は、Director の ［ユーザーの詳細］ページ >［セッションの詳細］>［**MS Teams** の最適化］フィールドで表示できます。Microsoft Teams の最適化は、クリアな音声やビデオなどのユーザーエクスペリエンスを向上させるために重要です。この機能は、VDA バージョン 2311 以降で利用できます。サポートされている Citrix Workspace アプリのバージョンは、「Microsoft Teams の最適化」に記載されています。Director は、Microsoft Teams が公開アプリとして実行されている場合、または公開デスクトップ内で実行されている場合にのみ、Microsoft Teams の最適化の状態を表示します。
詳しくは、「Microsoft Teams の最適化の状態」を参照してください。

VDA バージョン 1912 以降では、Citrix HDX Monitor（最小バージョン 3.11）を使用してアクティブな Teams 通話を監視できます。Citrix Virtual Apps and Desktops 製品の ISO には、フォルダーlayout\image-full\Support\HDX Monitorに最新のhdxmonitor.msiが含まれます。
VDA バージョン 1912 以降では、Citrix HDX Monitor（最小バージョン 3.11）を使用してアクティブな Microsoft Teams 通話を監視できます。Citrix Virtual Apps and Desktops 製品の ISO には、フォルダーlayout\image-full\Support\HDX Monitorに最新のhdxmonitor.msiが含まれます。

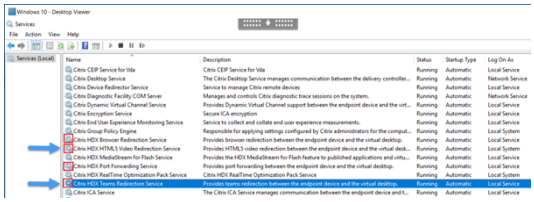
詳しくは、Knowledge Center のCTX253754の「*Monitoring*」を参照してください。

トラブルシューティング

このセクションでは、Microsoft Teams の最適化を実施する際に想定される問題に対処するためのヒントを提供します。詳しくは、CTX253754を参照してください。

Virtual Delivery Agent の状態

BCR_x64.msi. により 4 つのサービスがインストールされています。そのうちの 2 つが、VDA での Microsoft Teams のリダイレクトを担当します。



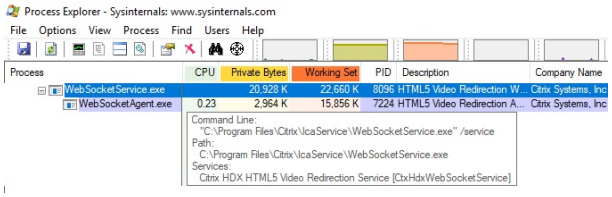
- **Citrix HDX Teams** リダイレクトサービスは Microsoft Teams が使用する仮想チャネルを確立します。このサービスは CtxSvcHost.exe に依存します。
- **Citrix HDX HTML 5** ビデオリダイレクトサービスは WebSocketService.exe として実行され、127.0.0.1 の TCP ポート 9002 をリッスンします。WebSocketService.exe には主に 2 つの機能があります。

  i. Microsoft Teams アプリのコンポーネントとして組み込まれている vdiCitrixPeerConnection.js から **WebSocket** のセキュリティを確保する **TLS** ターミネーションに対して、安全な WebSocket 接続が渡されます。この接続はプロセスモニターで追跡可能です。証明書について詳しくは、「Controller と VDA の間の通信」の「TLS および HTML5 ビデオリダイレクション、およびブラウザーコンテンツリダイレクト」を参照してください。

  一部のウイルス対策ソフトウェアおよびデスクトップセキュリティソフトウェアは、`WebSocketService.exe`およびその証明書の適切な動作を妨げます。Citrix HDX HTML5 ビデオリダイレクトサービスは、`services.msc`コンソールで動作している可能性がありますが、localhost `127.0.0.1:9002` TCP ソケットが netstat で表示されるようにリスニングモードになることはありません。サービスを再起動しようとすると、サービスがハングします（「停止しています…」）。`WebSocketService.exe`プロセスで適切な除外を適用するようにしてください。

  ii. ユーザーセッションのマッピング。Microsoft Teams アプリケーションが起動すると、WebSocketService.exe は VDA のユーザーセッションで WebSocketAgent.exe プロセスを起動します。WebSocketService.exe は LocalSystem アカウントの動作として、セッション 0 で実行されます。

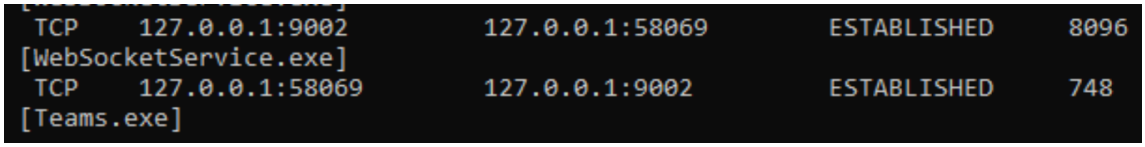
  

  `netstat`を使用して、WebSocketService.exe サービスが VDA でアクティブなリッスン状態であるかどうかを確認できます。

  管理者特権でのコマンドプロンプトウィンドウから`netstat -anob -p tcp`を実行します：

```
  TCP    127.0.0.1:9001         0.0.0.0:0              LISTENING       11740
[WebSocketService.exe]
  TCP    127.0.0.1:9002         0.0.0.0:0              LISTENING       11740
[WebSocketService.exe]
```

  接続が成功すると、状態が ESTABLISHED に変わります：



> 重要:
>
> WebSocketService.exe は 127.0.0.1:9001 と 127.0.0.1:9002 の 2 つの TCP ソケットでリッスンします。ポート 9001 はブラウザーコンテンツのリダイレクトと HTML5 ビデオのリダイレクトに、ポート 9002 は Microsoft Teams のリダイレクトにそれぞれ使用されます。VDA の Windows OS に、Teams.exe と WebSocketService.exe の間の直接通信を妨げる可能性があるプロキシ構成がないことを確認してください。Internet Explorer 11（[インターネットオプション] > [接続] > [**LAN** の設定] > [プロキシサーバー]）で明示的なプロキシを構成すると、接続は割り当てられたプロキシサーバーを経由する場合があります。手動および明示的なプロキシ設定を使用する場合、[ローカルアドレスにはプロキシサーバーを使用しない] がオンになっていることを確認します。

サービスの場所と説明

サービス	Windows Server OS の実行可能ファイルへのパス	ログオン名	説明
Citrix HTML5 ビデオリダイレクトサービス	“C:\Program Files (x86)\Citrix\System32\WebSocketService.exe” /service	ローカルシステムアカウント	仮想デスクトップとエンドポイントデバイス間でメディアのリダイレクトを実行する場合に必要な、複数の HDX マルチメディアサービスの初期のフレームワークを提供します。
Citrix HDX ブラウザーリダイレクトサービス	“C:\Program Files (x86)\Citrix\System32\CtxSvcHost.exe” -g BrowserRedirSvcs	使用アカウント（ローカル）	エンドポイントデバイスと仮想デスクトップ間で Web ブラウザーコンテンツのリダイレクトを実行します。
Citrix ポート フォワーディングサービス	“C:\Program Files (x86)\Citrix\System32\CtxSvcHost.exe” -g PortFwdSvcs	使用アカウント（ローカル）	エンドポイントデバイスと仮想デスクトップ間で Web ブラウザーコンテンツのリダイレクトのポートフォワーディングを実行します。

サービス	Windows Server OS の実行可能ファイルへのパス	ログオン名	説明
Citrix HDX Teams リダイレクトサービス	“C:\Program Files (x86)\Citrix\System32\CtxSvcHost.exe” -g TeamsSvcs	ローカルシステムアカウント	エンドポイントデバイスと仮想デスクトップ間で Microsoft Teams のリダイレクトを実行します。

Citrix Workspace アプリ

Windows 向け Citrix Workspace アプリは、ユーザーのエンドポイント上で HdxTeams.exe または HdxRtcEngine.exe という名前の新しいサービスをインスタンス化します。これは、Microsoft Teams が VDA で起動し、ユーザーがセルフプレビューで周辺機器の呼び出しやアクセスを試みたときに行われます。このサービスが表示されない場合は、次の点を確認してください:

1. Windows 向け Workspace アプリのバージョン 1905 以上がインストールされていることを確認します。Workspace アプリのインストールパスに HdxTeams.exe または HdxRtcEngine.exe と webrpc.dll バイナリがあるかを確認します。
2. 手順 1 の確認ができたら、次の手順を実行して HdxTeams.exe または HdxRtcEngine.exe が起動するかを確認してください。

    a) VDA で Microsoft Teams を終了します。
    b) VDA で services.msc を起動します。
    c) Citrix HDX Teams リダイレクトサービスを停止します。
    d) ICA セッションを切断します。
    e) ICA セッションを接続します。
    f) Citrix HDX チームリダイレクトサービスを起動します。
    g) Citrix HDX HTML5 ビデオリダイレクトサービスを再起動します。
    h) VDA で Microsoft Teams を起動します。

3. これでもクライアントエンドポイントで HdxTeams.exe または HdxRtcEngine.exe が起動しない場合は、次の手順を実行してください:

    a) VDA を再起動します。
    b) クライアントエンドポイントを再起動します。

サポート

Citrix と Microsoft は Citrix Virtual Apps and Desktops での Microsoft Teams の提供について、Microsoft Teams の最適化を通じて共同でサポートしています。この共同サポートは両社の緊密な協力関係により実現したものです。サポート契約の有効期間にこのソリューションで問題が発生した場合は、原因と考えられるコードの担当べ

ンダーのサポートチケットを開いてください。つまり Teams の場合は Microsoft の、最適化コンポーネントの場合は Citrix のサポートチケットを開きます。
Citrix または Microsoft はチケットを受け取り、問題を優先順位付けし、必要に応じてエスカレーションします。管理者が各社のサポートチームに連絡する必要はありません。

問題がある場合は、Teams UI の ［**Help**］**>** ［**Report a Problem**］にアクセスすることをお勧めします。VDA 側のログは Citrix と Microsoft の間で自動的に共有されるため、技術的な問題をより迅速に解決できます。

ログの収集

HDX メディアエンジンのログは、VDA ではなくユーザーのマシンにあります。問題が発生した場合は、必ずサポートケースにログを添付してください。

Windows ログ:

Windows ログは、%TEMP%**HDXTeams** フォルダー（AppData/Local/Temp/HDXTeams または AppData/Local/Temp/HdxRtcEngine）内にあります。「webrpc_Day_Month_timestamp_Year.txt」という名称の.txt ファイルを探します。Citrix Workspace アプリ 2009.5 以降など、新しいバージョンの Citrix Workspace アプリを使用している場合は、ログを AppData\Local\Temp\HdxRtcEngine に保存します。

各セッションは、ログ用に個別のフォルダーを作成します。

Mac ログ:

1. VDWEBRTC ログ - 仮想チャネルの実行を記録します。

   場所: /Users/<User Name>/Library/Logs/Citrix Workspace/CitrixViewer_<Y_M_D_H_M_S>.txt

2. HdxRtcEngine ログ - HdxRtcEngine でのプロセスの実行を記録します。

   場所: $TMPDIR/hdxrtcengine/<W_M_D_H_M_S_Y>/hdxrtcengine.log

   HdxRtcEngine ログは、デフォルトで有効になっています。

3. WebRTC ログ - WebRTC ライブラリのラップアップの実行を記録する最も重要なログです。

   場 所: /Users/<USERNAME>/Library/Logs/HdxRtcEngine/<W_M_D_H_M_S_Y>/webrpc.log

Linux ログ:

Linux ログは、/tmp/webrpc/<current date>/ and /tmp/hdxrtcengine/<current date>/フォルダーにあります。
WebRTC ログ: /tmp/webrpc/<current date>/webrtc.log
カーネルログ: /var/log/syslog

ICE/STUN/TURN/ログ:

通話を確立する場合、次の 4 つの ICE フェーズが必要です:

- 候補の収集
- 候補の交換
- 接続性チェック（STUN バインド要求）
- 候補のプロモーション

HdxRtcEngine.exe のログでは、以下のエントリが関連の対話型接続確立（ICE）エントリです。通知のセットアップを成功させるには、次のエントリが必要です。収集のフェーズについては、次のサンプルスニペットを参照してください:

```
RPCStubs Info: -> device id = \?\display#int3470#4&1835d135&0&uid13424
    #{
 65e8773d-8f56-11d0-a3b9-00a0c9223196 }
 {
 bf89b5a5-61f7-4127-a279-e187013d7caf }
  label = Microsoft Camera Front groupId =

webrtcapi.RTCPeerConnection Info: createOffer. audio = 1 video = 1
webrtcapi.RTCPeerConnection Info: setLocalDescription.
>>> begin:sdp
[…]

webrtcapi.RTCPeerConnection Info: OnSignalingChange. signaling state =
    HaveLocalOffer

webrtcapi.RTCPeerConnection Info: OnIceGatheringChange. state =
    Gathering

[…]
>>> begin:sdp
candidate:840548147 1 udp 2122194687 10.108.124.215 56927 typ host
    generation 0 ufrag oVk6 network-id 1
<<< end:sdp
[…]
>>> begin:sdp
candidate:1938109490 1 udp 24911871 52.114.xxx.xxx 52786 typ relay
    raddr 73.205.xxx.x rport 25651 generation 0 ufrag dDML network-id 1
    network-cost 10
<<< end:sdp
[…]
>>> begin:sdp
candidate:4271145120 1 udp 1685987071 66.xxx.xxx.xxx 55839 typ srflx
    raddr 10.108.124.215 rport 55839 generation 0 ufrag uAVH network-id
    1
<<< end:sdp
[…]

webrtcapi.RTCPeerConnection Info: OnIceGatheringChange. state =
    Complete webrtcapi.RTCPeerConnection Info: setRemoteDescription.
>>> begin:sdp
[…]

webrtcapi.RTCPeerConnection Info: OnSignalingChange. signaling state =
```



```
        HaveRemotelOffer
```

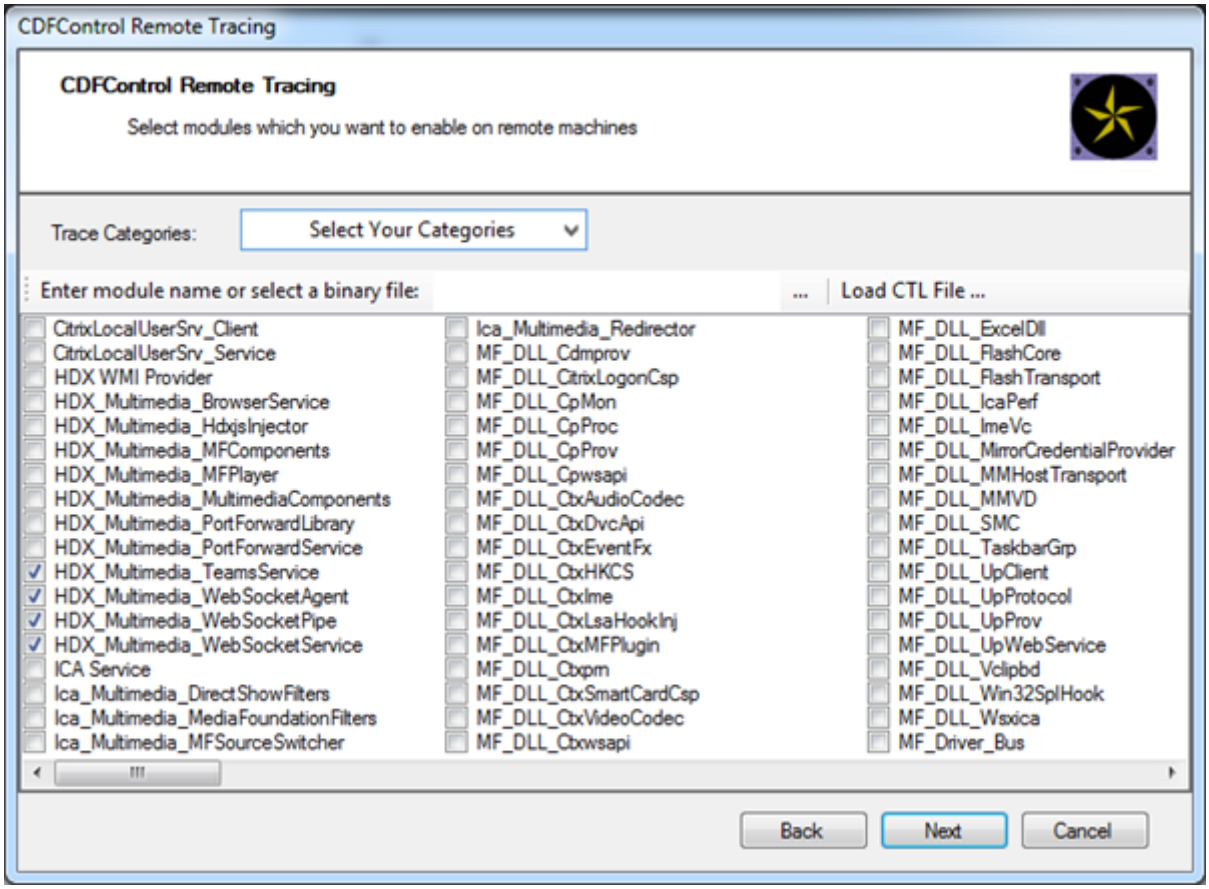
複数の ICE 候補がある場合、優先順位は次のとおりです:

1. host
2. peer reflexive
3. server reflexive
4. transport relay

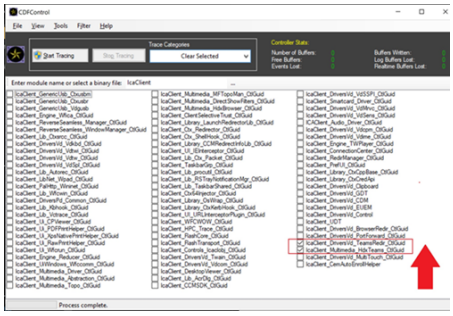
問題が発生し、一貫して再現できる場合は、Microsoft Teams で［**Help**］**>**［**Report a problem**］にアクセスすることをお勧めします。Microsoft でケースを開いた場合の技術的な問題を解決するために、Citrix と Microsoft の間でログが共有されます。
Citrix サポートに連絡する前に CDF トレースをキャプチャすることもお勧めします。詳しくは、Knowledge Center の「CDFcontrol」を参照してください。

CDF トレースを収集する際の推奨事項については、Knowledge Center の「Recommendations for Collecting the CDF Traces」を参照してください。

VDA 側の **CDF** トレース **-** 次の **CDF** トレースプロバイダーを有効にします:



Workspace アプリ側の **CDF** トレース **-** 次の **CDF** トレースプロバイダーを有効にします:



- IcaClient_DriversVd_TeamsRedir（オプション）
- IcaClient_Multimedia_HdxTeams （Citrix Workspace アプリ 2012 以降が必要です）

Windows Media リダイレクト

August 17, 2024

Windows Media リダイレクトは、サーバーでのユーザーへのオーディオとビデオのストリーム配信方法を制御および最適化します。サーバーではなくクライアントデバイスでメディアランタイムファイルを再生することで、Windows Media リダイレクトはマルチメディアファイルの再生に必要な帯域幅を減少させます。Windows Media リダイレクトは、仮想 Windows デスクトップで実行中の Windows Media Player および互換プレーヤーのパフォーマンスを向上させます。

Windows メディアのクライアント側でのコンテンツ取得の要件が満たされない場合、メディア配信は自動的にサーバー側での取得を使用します。その方法はユーザーにとって透過的です。Citrix Scout を使用して、HostMMTransport.dll から Citrix Diagnosis Facility（CDF）トレースを実行すると、その使用方法を決定できます。詳しくは、「Citrix Scout」を参照してください。

Windows Media リダイレクトは、ホストサーバーでのメディアパイプラインをインターセプトし、ネイティブの圧縮フォーマットでメディアデータをキャプチャし、コンテンツをクライアントデバイスにリダイレクトします。クライアントデバイスはパイプラインを再作成し、ホストサーバーから受信したメディアデータの展開およびレンダリングを行います。Windows Media リダイレクトは Windows オペレーティングシステムを実行中のクライアントデバイスで正しく動作します。これらのデバイスは、ホストサーバーに存在したパイプラインを再構築するために必要なマルチメディアフレームワークを備えています。Linux クライアントは、メディアパイプラインを再構築するために、同様のオープンソースメディアフレームワークを使用します。

[**Windows Media** リダイレクト］ポリシー設定で、この機能を制御します。デフォルトは ［許可］です。この設定は、通常、セッション内で再生されるオーディオおよびビデオの品質が向上して、クライアントデバイス上のファイルを再生しているときの品質に近くなります。まれに、Windows Media リダイレクトによるメディアの再生品質が、基本的な ICA 圧縮および通常のオーディオ機能での品質よりも悪い場合があります。その場合は、[**Windows Media** リダイレクト］設定をポリシーに追加し、その値を ［禁止］にすることで、機能を無効にできます。

ポリシーの設定について詳しくは、「マルチメディアのポリシー設定」を参照してください。

制限事項:

セッション内でリモート音声およびビデオ拡張機能（RAVE）を有効にして Windows Media Player を使用しているときに、画面表示が黒くなることがあります。この黒い画面は、ビデオコンテンツを右クリックし、［プレイビューを常に手前に表示］を選択すると表示されることがあります。

一般コンテンツリダイレクト

August 17, 2024

コンテンツのリダイレクト機能では、ユーザーが特定の種類のコンテンツにアクセスするときに、公開アプリケーションを使うのか、ユーザーデバイス上のアプリケーションを使うのかを制御できます。

クライアントフォルダーのリダイレクト

クライアントフォルダーのリダイレクトは、クライアント側のファイルがホスト側のセッションのへアクセスする方法を変更します。

- サーバー上でクライアント側ドライブのマッピングのみを有効にすると、クライアントの側の全ボリュームが UNC（Universal Naming Convention）リンクとしてセッションに自動的にマップされます。
- 管理者がサーバー上でクライアントフォルダーのリダイレクトを有効にして、ユーザーがそれを Windows デスクトップデバイス上で構成すると、ユーザーが指定したローカルボリュームの一部がリダイレクトされます。

ホストからクライアントへのリダイレクト

一般的ではないユースケースでの、ホストからクライアントへのリダイレクト機能の使用を検討します。通常は、ほかのコンテンツリダイレクト機能を使用することをお勧めします。この種類のリダイレクト機能は、マルチセッション OS VDA でのみサポートされ、シングルセッション OS VDA ではサポートされません。

ローカルアプリアクセスと URL リダイレクト

ローカルアプリアクセスを有効にすると、ローカルにインストールされている Windows アプリケーションが仮想デスクトップ環境にシームレスに統合されます。コンピューター間で切り替えるはありません。

HDX テクノロジは、特殊デバイスに次のような最適化されたサポートがないとき、または不適切なときに汎用 **USB** リダイレクトを提供します。

クライアントフォルダーのリダイレクト

August 17, 2024

クライアントフォルダーのリダイレクトは、クライアント側のファイルがホスト側のセッションのへアクセスする方法を変更します。サーバー上でクライアント側ドライブのマッピングのみを有効にすると、クライアントの側の全ボ

リュームが UNC（Universal Naming Convention）リンクとしてセッションに自動的にマップされます。管理者がサーバー上でクライアントフォルダーのリダイレクトを有効にして、ユーザーがそれをユーザーデバイス上で構成すると、ユーザーが指定したローカルボリュームの一部がリダイレクトされます。

セッション内でユーザー指定のフォルダーのみが UNC リンクとして表示されます。つまり、ユーザーデバイス上のファイルシステム全体が表示されるわけではありません。レジストリで UNC リンクを無効にすると、クライアントフォルダーはマップされたドライブとしてセッション内で表示されます。

クライアントフォルダーのリダイレクトは Windows シングルセッションOS マシンでのみサポートされます。

外部 USB ドライブに対するクライアントフォルダーのリダイレクトは、デバイスを解除して再接続しても保存されません。

サーバー側でクライアントフォルダーのリダイレクトを有効にします。次に、クライアントデバイス上でリダイレクト対象フォルダーを指定します。クライアントフォルダーオプションの指定に使用するアプリケーションは、このリリースで提供される Citrix Workspace アプリに含まれています。

要件:

サーバーの場合:

- Windows Server 2022
- Windows Server 2019、Standard、および Datacenter エディション

クライアントの場合:

- Windows 10 32 ビット版および 64 ビット版（バージョン 1607 以降）
- Windows 8.1 32 ビット版および 64 ビット版（Embedded エディションを含む）
- Windows 7 32 ビット版および 64 ビット版（Embedded エディションを含む）

サーバーでクライアントフォルダーのリダイレクトを有効にするには、レジストリを介して管理される機能の一覧にある「クライアントフォルダーのリダイレクト」を参照してください。

ユーザーデバイスで、リダイレクトするフォルダーを指定します:

1. 最新バージョンの Citrix Workspace アプリがインストールされていることを確認します。
2. Citrix Workspace アプリのインストール先ディレクトリで、CtxCFRUI.exe を実行します。
3. [カスタム] ラジオボタンをクリックし、フォルダーを追加、編集、または削除します。
4. セッションを切断してから再接続すると、変更が適用されます。

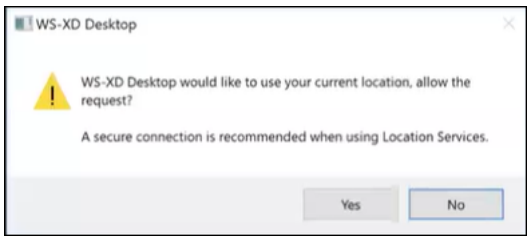
クライアントの場所へのリダイレクト

August 17, 2024

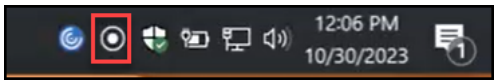
クライアントの場所へのリダイレクトを有効にすると、VDA でホストされるアプリとデスクトップセッションがクライアントの現在の場所にシームレスにアクセスできるようになります。マルチセッションオペレーティング システム（TS VDA またはマルチセッション WS VDA）では、各セッションに、接続されたクライアントによって提供される独自の一意の場所があります。この機能を使用すると、場所に依存する VDA 上のアプリケーションはクライアントの正確な場所を知ることができます。

詳しくは、Microsoftのドキュメントを参照してください。

クライアントの場所へのリダイレクトが有効になり、サーバー側とクライアント側の両方で場所へのアクセスが許可された後、場所にアクセスするアプリケーションまたはデスクトップを起動すると、クライアントは次のダイアログボックスで現在の場所を共有するように求めます：



クライアントの場所へのリダイレクトを有効にすると、VDA でホストされるアプリまたはデスクトップが現在の場所を照会した場合、クライアントのタスクバーに次のアイコンが表示されます。



システム要件

サーバーの場合：

- シングルセッション（Win10/11）またはマルチセッション（Win 11 22H2 および Server 2022 23H2 以降）OS VDA
- Windows、iOS、または Android 向け Citrix Workspace アプリ

構成

この機能が動作するには、Citrix ポリシーを使用してクライアントの場所へのリダイレクトを有効にする必要があります。クライアントの場所へのリダイレクトはデフォルトでは無効になっています。

クライアントの場所へのリダイレクトを有効にするには、次の手順を完了します：

Windows VDA およびクライアント側：

1. ［設定］**>**［プライバシー］**>**［場所］で、次のオプションを有効にします：
    - このデバイスでの位置情報へのアクセスを許可する

- アプリが位置情報にアクセスできるようにする
- デスクトップアプリが位置情報にアクセスできるようにする

2. マルチセッション OS の場合は、［場所の上書き］設定を有効にします。

Controller/DDC 側:

［**Studio**］**>**［ポリシー］**>**［位置情報］**>**［設定］**>**［クライアントデバイスの位置情報をアプリケーションで使用する］ポリシーを有効にします。
詳しくは、「クライアントセンサーのポリシー設定」を参照してください。

コンテンツの双方向リダイレクト

August 17, 2024

コンテンツの双方向リダイレクトにより、Web ブラウザーの HTTP または HTTPS の URL、あるいはアプリケーションに埋め込まれた URL を、Citrix VDA セッションとクライアントエンドポイントの間で双方向に転送できます。Citrix セッションで実行されているブラウザーに入力された URL は、クライアントのデフォルトのブラウザーを使用して開くことができます。逆に、クライアントで実行されているブラウザーに入力された URL は、公開アプリケーションまたはデスクトップのいずれかを使用して、Citrix セッションで開くことができます。コンテンツの双方向リダイレクトの一般的なユースケースは次のとおりです:

- 起動ブラウザーがソースへのネットワークアクセス権を持っていない場合の Web URL のリダイレクト。
- ブラウザーの互換性とセキュリティ上の理由からの Web URL のリダイレクト。
- Citrix セッションまたはクライアントで Web ブラウザーを実行する必要がない場合の、アプリケーションに埋め込まれた Web URL のリダイレクト。

システム要件

- シングルセッションまたはマルチセッションの OS VDA
- Windows 向け Citrix Workspace アプリ

ブラウザー:

- Citrix Browser Redirection Extension を備えた Google Chrome（Google Chrome ウェブストアで入手可能）
- Citrix Browser Redirection Extension を備えた Microsoft Edge（Chromium）（Google Chrome ウェブストアで入手可能）

構成

Citrix Virtual Apps and Desktops バージョン 2311 以降、コンテンツの双方向リダイレクトは Citrix Studio を通じてのみ構成されます。以前のリリースでは、クライアントエンドポイントと Studio の両方でポリシー設定が構成されていました。コンテンツの双方向リダイレクトはデフォルトで有効になっています。

最新のポリシー設定については、「**ICA** ポリシー設定」の「コンテンツの双方向リダイレクトの構成」を参照してください。

ブラウザーのリダイレクトが機能するためには、次に示すコマンドを使用して、ブラウザー拡張機能を元のブラウザー（URL のリダイレクト元）に登録する必要があります。使用中のブラウザーに基づいて、VDA およびクライアントで、必要に応じてコマンドを実行します。

ブラウザー	VDA	クライアント
Google Chrome	%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirect.exe /regChrome	%ProgramFiles(x86)%\Citrix\ICA Client\redirector.exe /regChrome
Microsoft Edge	%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirect.exe /regEdge	%ProgramFiles(x86)%\Citrix\ICA Client\redirector.exe /regEdge
利用可能なすべてのブラウザー	%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirect.exe /regall	%ProgramFiles(x86)%\Citrix\ICA Client\redirector.exe /regall

ブラウザー拡張機能の登録を解除するには：

ブラウザー	VDA	クライアント
Google Chrome	%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirect.exe /unregChrome	%ProgramFiles(x86)%\Citrix\ICA Client\redirector.exe /unregChrome
Microsoft Edge	%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirect.exe /unregEdge	%ProgramFiles(x86)%\Citrix\ICA Client\redirector.exe /unregEdge
利用可能なすべてのブラウザー	%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirect.exe /unregall	%ProgramFiles(x86)%\Citrix\ICA Client\redirector.exe /unregall

> 注：
>
> 登録コマンドを使用すると、Chrome および Edge ブラウザーは、最初の起動時に Citrix Browser Redirection Extension を有効にするようにユーザーに促します。ブラウザー拡張機能は、Google Chrome ウェブストアから手動でインストールすることもできます。Microsoft Edge については、「Chrome ウェブストアか

> ら Microsoft Edge に拡張機能を追加する」も参照してください。

Citrix VDA からクライアントへのワイルドカードリダイレクト

コンテンツの双方向リダイレクトでは、リダイレクトされる URL を定義するときにワイルドカードを使用できます。コンテンツの双方向リダイレクトを構成するには、「構成」手順を参照してください。

VDA からクライアントへのカスタムプロトコルリダイレクト

コンテンツの双方向リダイレクトは、Citrix VDA からクライアントへのカスタムプロトコルのリダイレクトをサポートします。HTTP または HTTPS 以外のプロトコルがサポートされています。コンテンツの双方向リダイレクトを構成するには、「構成」手順を参照してください。

Web Studio の ［コンテンツの双方向リダイレクト］でカスタムプロトコルを設定します。

> 注:
>
> - これらのコマンドを実行するには、管理者権限が必要です。
> - クライアントには、プロトコルを処理するためのアプリケーションが登録されている必要があります。登録されていない場合、URL はクライアントにリダイレクトされ、起動に失敗します。
> - Chrome および Edge ブラウザーで入力または起動するカスタムプロトコル URL はサポートされておらず、リダイレクトは機能しません。
> - 次のプロトコルはサポートされていません: `rtsp://`, `rtspu://`, `pnm://`, `mms://`。

そのほかの考慮事項

- ブラウザーの要件と構成は、リダイレクトを開始するブラウザーにのみ適用されます。リダイレクトが成功した後に URL が開く宛先ブラウザーは、サポートの対象とは見なされません。URL を VDA からクライアントにリダイレクトする場合、サポートされているブラウザー構成は VDA でのみ必要です。逆に、URL をクライアントから VDA にリダイレクトする場合、サポートされているブラウザー構成はクライアントでのみ必要です。リダイレクトされた URL は、方向に応じて、クライアントまたは VDA のいずれかの宛先マシン上で構成されたデフォルトのブラウザーに渡されます。VDA とクライアントで同じブラウザーの種類を使用する必要はありません。
- リダイレクト規則がループした構成になっていないことを確認してください。たとえば、VDA ポリシーが`https://www.citrix.com`をリダイレクトするように設定され、クライアントポリシーが同じ URL をリダイレクトするように設定されていると、無限ループが発生します。
- URL の短縮はサポートされていません。
- クライアントから VDA にリダイレクトするには、Windows クライアントを管理者権限でインストールする必要があります。

- 宛先ブラウザーが既に開いている場合は、リダイレクトされた URL が新しいタブで開きます。それ以外の場合、URL は新しいブラウザーウィンドウで開きます。
- ローカルアプリアクセス（LAA）が有効になっている場合、コンテンツの双方向リダイレクトは機能しません。

ホストからクライアントへのリダイレクト

August 17, 2024

ホストからクライアントへのリダイレクトにより、Citrix セッションで実行中のアプリケーションにハイパーリンクとして埋め込まれている URL を、ユーザーエンドポイントデバイスにある対応するアプリケーションを使用して開くことができます。ホストからクライアントへのリダイレクトの一般的なユースケースは次のとおりです：

- Citrix サーバーにソースへのインターネットまたはネットワークアクセスがない場合の Web サイトのリダイレクト。
- Citrix セッション内で Web ブラウザーを実行している場合の Web サイトのリダイレクトは、セキュリティ、パフォーマンス、互換性、またはスケーラビリティの観点から望ましくありません。
- URL を開くために必要なアプリケーションが Citrix サーバーにインストールされていない場合の特定の URL タイプのリダイレクト。

ホストからクライアントへのリダイレクトは、Web ページでアクセスする URL、または Citrix セッションで実行されている Web ブラウザーのアドレスバーに入力する URL を対象としていません。Web ブラウザーでの URL のリダイレクトについては、「双方向の URL のリダイレクト」または「Web ブラウザーコンテンツのリダイレクト」を参照してください。

システム要件

- マルチセッション OS VDA
- サポートされているクライアント：
  - Windows 向け Citrix Workspace アプリ
  - Mac 向け Citrix Workspace アプリ
  - Linux 向け Citrix Workspace アプリ
  - HTML5 向け Citrix Workspace アプリ
  - Chrome 向け Citrix Workspace アプリ

クライアントデバイスには、URL タイプのリダイレクトを処理するためのアプリケーションがインストールおよび構成されている必要があります。

構成

「ホストからクライアントへのリダイレクト」の Citrix ポリシーを使用して、この機能を有効にします。ホストからクライアントへのリダイレクトはデフォルトで無効になっています。ホストからクライアントへのリダイレクトポリシーを有効にすると、Citrix Launcher アプリケーションが Windows サーバーに登録され、URL をインターセプトしてクライアントデバイスに送信できるようになります。

次に、必要な URL タイプのデフォルトアプリケーションとして Citrix Launcher を使用するように、Windows グループポリシーを構成する必要があります。Citrix サーバー VDA で、ServerFTAdefaultPolicy.xml ファイルを作成し、次の XML コードを挿入します。

```
<?xml version="1.0" encoding="UTF-8"?>

<DefaultAssociations>

<Association Identifier="http" ProgId="ServerFTAHTML" ApplicationName="
    ServerFTA" />

<Association Identifier="https" ProgId="ServerFTAHTML" ApplicationName=
    "ServerFTA" />

</DefaultAssociations>
```

グループポリシー管理コンソールから、[コンピューターの構成] **>** [管理用テンプレート] **>** [**Windows** コンポーネント] **>** [エクスプローラー] **>** [既定の関連付け構成ファイルの設定] の順に移動し、ServerFTAdefaultPolicy.xml ファイルを保存します。

> 注:
>
> Citrix サーバーにグループポリシー設定がない場合、URL を開くためのアプリケーションを選択するよう求める Windows プロンプトが表示されます。

デフォルトでは、次の URL タイプのリダイレクトをサポートしています:

- HTTP
- HTTPS
- RTSP
- RTSPU
- PNM
- MMS

リダイレクト用の一覧に追加の標準 URL タイプまたはカスタム URL タイプを含めるには、前に参照した ServerFTAdefaultPolicy.xml ファイルに新しい **Association Identifier**（関連付け識別子）行を作成します。例:

```
<Association Identifier="ftp"ProgId="ServerFTAHTML"ApplicationName="
ServerFTA"/>
```



```
<Association Identifier="mailto"ProgId="ServerFTAHTML"ApplicationName
="ServerFTA"/>

<Association Identifier="customtype1"ProgId="ServerFTAHTML"ApplicationName
="ServerFTA"/>

<Association Identifier="customtype2"ProgId="ServerFTAHTML"ApplicationName
="ServerFTA"/>
```

一覧に URL タイプを追加するには、クライアントの構成も必要です。Windows クライアントで次のレジストリキーと値を作成します。

> 注:
>
> レジストリエディターの使用を誤ると、深刻な問題が発生する可能性があり、オペレーティングシステムの再インストールが必要になる場合もあります。レジストリエディターの誤用による障害に対して、Citrix では一切責任を負いません。レジストリエディターは、お客様の責任と判断の範囲でご使用ください。また、レジストリファイルのバックアップを作成してから、レジストリを編集してください。

- キー: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Policies\Citrix\ICA Client\SFTA
- 値の名前: ExtraURLProtocols
- 値の種類: REG_SZ
- 値のデータ: 必要な URL タイプをセミコロンで区切って指定します。URL の権限部分の前にすべてを含めます。例:
  `ftp://;mailto:;customtype1://;custometype2://`

Windows クライアントに対してのみ URL タイプを追加できます。上記のレジストリ設定がないクライアントは、Citrix セッションへ戻るリダイレクトを拒否します。クライアントには、指定された URL タイプを処理するようにアプリケーションがインストールおよび構成されている必要があります。

デフォルトのリダイレクト一覧から URL タイプを削除するには、サーバー VDA で次のレジストリキーと値を作成します。

- キー: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\SFTA
- 値の名前: DisableServerFTA
- 値の種類: DWORD
- 値のデータ: 1
- 値の名前: NoRedirectClasses
- 値の種類: REG_MULTI_SZ
- 値のデータ: 値の組み合わせを指定します: `http`、`https`、`rtsp`、`rtspu`、`pnm`、または`mms`。1 つの行に 1 つの値を入力してください。例:

```
http
```


`https`

`rtsp`

特定の Web サイトのセットについてホストからクライアントへのリダイレクト機能を有効にするには、サーバー VDA でレジストリキーと値を作成します。

- キー：HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\SFTA
- 値の名前：ValidSites
- 値の種類：REG_MULTI_SZ
- 値のデータ：FQDN（完全修飾ドメイン名：Fully-Qualified Domain Name）の組み合わせを指定します。1 つの行に 1 つの FQDN を入力してください。プロトコル（`http://`または`https://`）を使用せずに、FQDN のみを含めます。FQDN には、左端にのみワイルドカード文字としてアスタリスク（*）を含めることができます。このワイルドカードは単一レベルのドメインと照合されます。これは RFC 6125 の規則に準拠しています。例：

`www.exmaple.com`

`*.example.com`

> 注：
>
> **ValidSites** キーを **DisableServerFTA** キーおよび **NoRedirectClasses** キーと使用することはできません。

サーバー **VDA** のデフォルトの **Web** ブラウザー構成

このセクションで参照されているようにホストからクライアントへのリダイレクトを有効にすると、サーバー VDA の以前のデフォルトの Web ブラウザー構成が置き換えられます。Web URL がリダイレクトされない場合、Citrix Launcher は URL を`command_backup`レジストリキーで構成された Web ブラウザーに渡します。キーはデフォルトで Internet Explorer を指定しますが、これを変更して別の Web ブラウザーへのパスを含めることができます。詳しくは、レジストリを介して管理される機能の一覧にある「サーバー VDA のデフォルトの Web ブラウザー構成」を参照してください。

ローカルアプリアクセスと **URL** リダイレクト

August 17, 2024

はじめに

ローカルアプリアクセスを有効にすると、ローカルにインストールされている Windows アプリケーションが仮想デスクトップ環境にシームレスに統合されます。ローカルアプリアクセスにより、以下の操作が可能になります。

- ラップトップや PC などの物理コンピューター上にローカルにインストールされたアプリケーションに仮想デスクトップからアクセスする。
- フレキシブルなアプリケーション配信ソリューションをユーザーに提供する。仮想化できないアプリケーションや IT 担当者が管理しないアプリケーションをユーザーのローカルにインストールして、仮想デスクトップ上にインストールされたアプリケーションのように使用できます。
- アプリケーションが仮想デスクトップから個別にホストされている場合、ダブルホップによる遅延を排除します。このために、ユーザーの Windows デバイス上で公開アプリケーションのショートカットを作成します。
- 次のようなアプリケーションを使用する。
  - GoToMeeting などのビデオ会議ソフトウェア。
  - 仮想化されていない特殊なアプリケーション。
  - ユーザーデバイスとサーバー間で大量のデータ転送が発生するアプリケーションや周辺機器。たとえば、DVD バーナーや TV チューナーなどです。

Citrix Virtual Apps and Desktops では、URL のリダイレクトにより、ホストされたデスクトップセッションからローカルアプリケーションアクセスアプリケーションを起動できます。URL リダイレクトでは、複数の URL アドレスでアプリケーションを起動できます。デスクトップセッションで、Web ブラウザー内に埋め込まれたリンクをクリックすると、Web ブラウザーの URL 禁止リストに基づいてローカルの Web ブラウザーが起動します。禁止リストにない URL をクリックすると、その URL がデスクトップセッションで再度開きます。

URL リダイレクトはデスクトップセッションでのみ機能し、アプリケーションセッションでは機能しません。アプリケーションセッションで使用できるリダイレクト機能は、サーバー FTA（File Type Association：ファイルタイプの割り当て）リダイレクトの 1 つである「ホストからクライアントへのコンテンツのリダイレクト」のみです。この FTA では、HTTP、HTTPS、RTSP、MMS など、特定のプロトコルがクライアント側に転送されます。たとえば、HTTP の埋め込みリンクを開くときに、クライアント側のアプリケーションが使用されます。URL 禁止リストまたは許可リストのサポートはありません。

ローカルアプリケーションアクセスを有効にすると、ローカルで実行されるアプリケーション、ホストされるアプリケーション、またはデスクトップ上のショートカットからアクセスされた URL を、以下のいずれかの方法でリダイレクトできます。

- ユーザーのコンピューターから、ホストされているデスクトップへ
- Citrix Virtual Apps and Desktops サーバーからユーザーのコンピューターへ
- 起動された環境内で処理（リダイレクトなし）

特定の Web サイトでのリダイレクト方法を指定するには、Virtual Delivery Agent 上の URL 許可リストおよび URL 禁止リストを構成します。これらのリストでは、URL リダイレクトのポリシー設定を指定する複数行文字列値を設定します。詳しくは、「ローカルアプリアクセスのポリシー設定」を参照してください。

すべての URL を VDA 側の Web ブラウザーで開くこともできますが、以下の URL についてはエンドポイント上の Web ブラウザーで開くためのポリシーを構成できます。

- ジオ/ロケール情報—ユーザーの現在位置の情報に基づいて適切なページを自動的に表示する msn.com や news.google.com などの Web サイト。たとえば、イギリスにあるデータセンターで提供される VDA にイ

ンドのクライアントから接続する場合、in.msn.com が表示されるはずですが、代わりに、uk.msn.com が表示されます。

- マルチメディアコンテンツ—メディアリッチな Web サイト。クライアント側で処理されるように設定すると、ユーザーエクスペリエンスが向上し、狭帯域幅接続での使用帯域幅や処理能力が改善されます。この機能は、Silverlight などの他のメディアの種類のサイトをリダイレクトします。これにより、環境のセキュリティも向上します。つまり、管理者により許可された URL だけがクライアント側で処理され、ほかの URL はすべて VDA 側で処理されます。

URL リダイレクトに加えて、FTA リダイレクトも使用できます。FTA により、セッションで特定のファイルを開くときにローカルのアプリケーションが使用されます。ローカルアプリケーションでファイルを開くには、そのローカルアプリケーションがそのファイルにアクセスできる必要があります。つまり、ローカルアプリケーションで開くことができるのは、ネットワーク共有上またはクライアントドライブ上にあるファイル（クライアント側ドライブのマッピング機能）のみです。たとえば、PDF ファイルを開く場合、ローカルにインストールされている PDF リーダーでファイルが表示されます。ローカルアプリケーションはファイルに直接アクセスできるため、ファイルを開くときに ICA によるネットワーク転送は発生しません。

要件、考慮事項、および制限事項

ローカルアプリアクセスは、Windows マルチセッション OS 対応 VDA および Windows シングルセッション OS 対応 VDA でサポートされるオペレーティングシステムでサポートされています。ローカルアプリケーションアクセスには、バージョン 4.1 以降の Windows 向け Citrix Workspace アプリが必要です。次の Web ブラウザーがサポートされています:

- Edge：最新バージョン
- Firefox：最新バージョンおよび延長サポートリリース
- Chrome：最新バージョン

ローカルアプリアクセスや URL リダイレクトを使用するときは、以下の考慮事項および制限事項について確認してください。

- ローカルアプリアクセスは全画面モード用に設計されています。このため、以下の制限事項があります。
  - ローカルアプリケーションアクセスをウィンドウ表示モードの仮想デスクトップで使用するなど、単一の仮想デスクトップをすべてのモニター上で表示しない場合、ユーザーエクスペリエンスに混乱が生じます。
  - マルチモニター環境で、アプリケーションの表示を 1 つのモニターで最大化すると、すべてのアプリケーションがそのモニター上に表示されます。このデフォルトの状態は、以降のアプリケーションが通常は他のモニターに表示される場合でも発生します。
  - この機能は、単一 VDA での使用を想定して設計されています。複数の同時接続 VDA を対象とするものではありません。
- 一部のアプリケーションでは、以下の予期されない問題が発生する場合があります。

  - ドライブ文字により、ユーザーが仮想デスクトップの C ドライブとローカルの C ドライブを混同する場合があります。
  - 仮想デスクトップで使用できるプリンターは、ローカルアプリケーションでは使用できません。
  - 管理者特権が必要なアプリケーションは、ローカルアプリケーションアクセスでは起動できません。
  - 単一インスタンスアプリケーション（Windows Media Player など）もほかのアプリケーションと同等に処理されます。
  - ローカルアプリケーションはローカルマシンの Windows テーマで表示されます。
  - 全画面アプリケーションはサポートされません。これらのアプリケーションには、PowerPoint のスライドショーやデスクトップ全体で表示されるフォトビューアーなど、全画面で開くアプリケーションが含まれます。
  - ローカルアプリケーションアクセスでは、VDA 上のローカルアプリケーションのプロパティ（デスクトップや［スタート］メニューのショートカットなど）が複製されます。ただし、ショートカットキーや読み取り専用属性などの他のプロパティはコピーされません。
  - 一部のアプリケーションで、各ウィンドウが正しい重なり順で表示されない場合があります。これにより、一部のウィンドウが非表示になることがあります。
  - マイコンピューター、ごみ箱、コントロールパネル、ネットワークドライブ、フォルダーなどのショートカットはサポートされません。
  - カスタムのファイルタイプ、関連付けられたプログラムのないファイル、ZIP ファイル、および隠しファイルはサポートされません。
  - ビット数の異なるローカルアプリケーションと VDA アプリケーションのタスクバーでのグループ化はサポートされません。つまり、32 ビットのローカルアプリケーションと 64 ビットの VDA アプリケーションは、タスクバーでグループ化されません。
  - アプリケーションは COM を使って起動できません。たとえば、Office アプリケーション内に埋め込まれている Office ドキュメントをクリックしても、プロセス起動が検出されないため、ローカルアプリケーション統合に失敗します。

- ユーザーが、仮想デスクトップセッション内から別の仮想デスクトップを起動するダブルホップシナリオはサポートされていません。
- 明示的な URL リダイレクトのみがサポートされます。つまり、Web ブラウザーのアドレスバーに表示される URL や、ブラウザー内ナビゲーションによる URL だけが正しくリダイレクトされます。
- URL リダイレクトはデスクトップセッションでのみ機能し、アプリケーションセッションでは機能しません。
- VDA セッションのローカルデスクトップフォルダーにユーザーがファイルを作成することはできません。
- ローカルアプリケーションの複数のインスタンスのタスクバーアイコンは、仮想デスクトップのタスクバー設定に基づいて表示されます。ただし、ローカルで実行されているアプリケーションのショートカットは、このアプリケーションの実行インスタンスのアイコンとはグループ化されません。また、ホストされているアプリケーションの実行インスタンスや、そのアプリケーションのピン留めアイコンともグループ化されません。タスクバー上のアイコンでは、ローカルで実行されているアプリケーションのウィンドウのみを閉じることができます。ローカルアプリケーションのショートカットをデスクトップタスクバーや［スタート］メニューに固定することもできますが、そのショートカットからアプリケーションを起動できなくなる場合があります。
- ［ローカルアプリアクセスを許可する］ポリシー設定 ［有効］に設定した場合、ブラウザーコンテンツリダイレ

クトはサポートされません。デフォルトでは、ローカルアプリアクセスは禁止されています。

Windows 上での動作

ローカルアプリアクセスは、Windows 上で次のように動作します。

- Windows 8 および Windows Server 2012 のショートカットの動作
  - クライアント上にインストールされた Windows ストアアプリケーションは、ローカルアプリケーションアクセスのショートカットとして列挙されません。
  - イメージファイルとビデオファイルは、デフォルトで Windows ストアアプリケーションで開きます。ただし、ローカルアプリケーションアクセスでは、Windows ストアアプリケーションが列挙され、ショートカットがデスクトップアプリケーションで開かれます。
- Local Programs フォルダー
  - Windows 7 の場合、［スタート］メニューに Local Programs フォルダーが表示されます。
  - Windows 8 の場合、ユーザーがスタート画面のカテゴリとして ［すべてのアプリ］を選択した場合のみ、Local Programs フォルダーが表示されます。Local Programs フォルダーにすべてのサブフォルダーが表示されるわけではありません。
- アプリケーション用の Windows 8 グラフィック機能
  - デスクトップアプリケーションはデスクトップ領域に制限され、スタート画面および Windows 8 スタイルアプリケーションの背面に表示されます。
  - ローカルアプリアクセスは、マルチモニターモードでデスクトップアプリケーションのようには動作しません。マルチモニターモードでは、スタート画面とデスクトップは別のモニター上で表示されます。
- Windows 8 およびローカルアプリアクセスの URL リダイレクト
  - Windows 8 上の Internet Explorer ではアドオンを使用できないため、URL リダイレクトを有効にする場合はデスクトップ版の Internet Explorer を使用する必要があります。
  - Windows Server 2012 上の Internet Explorer では、デフォルトでアドオンが無効になっています。URL リダイレクトを実装するには、Internet Explorer の拡張構成を無効にしてください。標準ユーザーに対してアドオンが有効になるように、Internet Explorer のオプションを再設定して再起動します。

ローカルアプリアクセスと URL リダイレクトの構成

Citrix Workspace アプリでローカルアプリケーションアクセスと URL リダイレクトを使用するには:

- ローカルクライアントマシンに Citrix Workspace アプリをインストールします。Citrix Workspace アプリのインストール時に両方の機能を有効することも、グループポリシーエディターを使ってローカルアプリケーションアクセステンプレートを有効にすることも可能です。

- ポリシーの ［ローカルアプリアクセスを許可する］設定を ［有効］に設定します。URL リダイレクトの URL 許可リストおよび禁止リストのポリシー設定を構成することもできます。詳しくは、「ローカルアプリアクセスのポリシー設定」を参照してください。

ローカルアプリアクセスと **URL** リダイレクトの有効化

すべてのローカルアプリケーションのローカルアプリアクセスを有効にするには、次の手順を実行します:

1. Web Studio にサインインし、左側のペインで ［ポリシー］をクリックします。
2. 操作バーで ［ポリシーの作成］をクリックします。
3. ［ポリシーの作成］ウィンドウで、検索ボックスに「ローカルアプリアクセスを許可する」と入力して、［選択］をクリックします。
4. ［設定の編集］ウィンドウで、［許可］を選択します。デフォルトでは、［ローカルアプリアクセスを許可する］ポリシーは禁止されます。この設定が許可されている場合、VDA により、公開アプリケーションおよびローカルアプリアクセスのショートカットを有効にするかをエンドユーザーが指定できます。（この設定が禁止されている場合、公開アプリケーションおよびローカルアプリケーションアクセスのショートカットのいずれも VDA で機能しません。）このポリシー設定は、URL リダイレクトのポリシー設定だけではなく、マシン全体に適用されます。
5. ［ポリシーの作成］ウィンドウで、検索ボックスに「URL リダイレクトの許可リスト」と入力して、［選択］をクリックします。URL リダイレクトの許可リストは、リモートセッションのデフォルトの Web ブラウザーで開く URL を指定します。
6. ［設定の編集］ウィンドウで ［追加］をクリックして URL を追加し、［**OK**］を選択します。
7. ［ポリシーの作成］ウィンドウで、検索ボックスに「URL リダイレクトの禁止リスト」と入力して、［選択］をクリックします。URL リダイレクトの禁止リストは、エンドポイント上で実行されているデフォルトの Web ブラウザーにリダイレクトされる URL を指定します。
8. ［設定の編集］ウィンドウで ［追加］をクリックして URL を追加し、［**OK**］を選択します。
9. ［設定］ページで、［次へ］をクリックします。
10. ［ユーザーおよびマシン］ページでポリシーを該当のデリバリーグループに割り当てて、［次へ］をクリックします。
11. ［概要］ページで、設定を確認して ［完了］をクリックします。

Citrix Workspace アプリのインストール中、すべてのローカルアプリケーションで URL リダイレクトを有効にするには、以下の手順を実行します:

1. Citrix Workspace アプリのインストール時に、マシンのすべてのユーザーに対して URL リダイレクトを有効にします。これにより、URL リダイレクト機能で使用される Web ブラウザーアドオンも登録されます。
2. コマンドプロンプトで次のいずれかのオプションを付けて適切なコマンドを実行し、Citrix Workspace アプリをインストールします:

   - CitrixReceiver.exe の場合、/`ALLOW_CLIENTHOSTEDAPPSURL`=1を使用します。
   - CitrixReceiverWeb.exe の場合、/`ALLOW_CLIENTHOSTEDAPPSURL`=1を使用します。

グループポリシーエディターを使ってローカルアプリアクセステンプレートを有効にするには

> 注:
>
> - グループポリシーエディターを使用してローカルアプリアクセステンプレートを有効にする前に、receiver.admx/adml テンプレートファイルをローカルグループポリシーオブジェクト（GPO）に追加します。
> - Windows 向け Citrix Workspace アプリのテンプレートファイルは、[管理用テンプレート] > [**Citrix** コンポーネント] > [**Citrix Workspace**] フォルダーのローカル GPO にあります（ユーザーが CitrixBase.admx/CitrixBase.adml を%systemroot%\policyDefinitions フォルダーに追加する場合のみ）。

グループポリシーエディターを使ってローカルアプリアクセステンプレートを有効にするには、以下の手順を実行します:

1. **gpedit.msc** を実行します。
2. [コンピューターの構成] > [管理用テンプレート] > [従来の管理用テンプレート（**ADM**）] > [**Citrix** コンポーネント] > [**Citrix Workspace**] > [ユーザーエクスペリエンス] の順に移動します。
3. [ローカルアプリケーションアクセス設定] を選択します。
4. [有効] を選択し、[**URL** のリダイレクトを許可します] チェックボックスをオンにします。URL リダイレクト機能を使用するには、この記事の「*Web* ブラウザーアドオンの登録」セクションに記載されているコマンドラインを使用して、Web ブラウザーアドオンを登録してください。

公開アプリケーションへのアクセスのみを提供する

レジストリエディターまたは PowerShell SDK を使用して、公開アプリケーションへのアクセスを管理できます。

レジストリの設定については、レジストリを介して管理される機能の一覧にある「公開アプリケーションのローカルアプリアクセス」を参照してください。

PowerShell SDK を使用するには:

1. Delivery Controller が実行されているマシンで PowerShell を開きます。
2. コマンド:`set-configsitemetadata -name "studio_clientHostedAppsEnabled" -value "true"`を実行します。

クラウドサービス展開で ［ローカルアプリアクセスアプリケーションの追加］ にアクセスするには、Citrix DaaS Remote PowerShell SDK を使用します。詳しくは、「Citrix DaaS Remote PowerShell SDK」を参照してください。

1. インストーラーをダウンロードします:

   https://download.apps.cloud.com/CitrixPoshSdk.exe

2. 次のコマンドを実行します:

a) `asnp citrix.*`
b) `Get-XdAuthentication`

3. コマンド:`set-configsitemetadata -name "studio_clientHostedAppsEnabled "-value "true"`を実行します。

上記の手順を完了したら、以下の手順に従って続行します。

1. Web Studio にサインインし、左側のペインで ［アプリケーション］をクリックします。
2. 中央上部のペインで空白の領域を右クリックし、コンテキストメニューから ［ローカルアプリアクセスアプリケーションの追加］を選択します。また、操作バーで ［ローカルアプリアクセスアプリケーションの追加］をクリックすることもできます。操作バーで［ローカルアプリアクセスアプリケーションの追加］オプションを表示させるには、［更新］をクリックします。
3. ローカルアプリアクセスアプリケーションを公開します。

   - ローカルアプリケーションアクセスウィザードが起動され、［はじめに］ページが表示されます。このページは、今後このウィザードが起動されたときに開かないように設定できます。
   - ウィザードの指示に従って、［グループ］、［場所］、［識別］、［配信］、［概要］の各ページで操作を行います。各ページの操作を終えたら、［概要］ページに到達するまで ［次へ］をクリックします。
   - ［グループ］ページで、アプリケーションが追加されるデリバリーグループを選択して ［次へ］をクリックします。
   - ［場所］ページで、ユーザーのローカルマシン上にあるアプリケーションの実行可能ファイルのフルパスを入力し、アプリケーションが存在するフォルダーへのパスを入力します。Citrix ではシステム環境変数のパスを使用することをお勧めします（例: %ProgramFiles(x86)%\Internet Explorer\iexplore.exe）。
   - ［識別］ページで、既定値をそのまま使用するか、必要な情報を入力して ［次へ］をクリックします。
   - ［配信］ページで、このアプリケーションをユーザーに配信する方法を構成して ［次へ］をクリックします。選択したアプリケーションのアイコンを指定できます。このローカルアプリケーションのショートカットを仮想デスクトップの［スタート］メニューやデスクトップに追加するかどうかを指定することもできます。
   - ［概要］ページで、設定を確認して ［完了］をクリックし、ローカルアプリケーションアクセスウィザードを閉じます。

Web ブラウザーアドオンの登録

> 注:
>
> URL リダイレクト機能に必要な Web ブラウザーアドオンは、コマンドラインでの Citrix Workspace アプリのインストール時に/ALLOW_CLIENTHOSTEDAPPSURL=1 オプションを指定すると自動的に登録されます。

以下のコマンドを実行して、適切な Web ブラウザーにアドオンを登録したり登録解除したりできます。

- クライアントデバイスにアドオンを登録する場合: <*client-installation-folder*>\redirector.exe /reg<*browser*>
- クライアントデバイスのアドオンの登録を解除する場合: <*client-installation-folder*>\redirector.exe /unreg<*browser*>
- VDA にアドオンを登録する場合: <*VDAinstallation-folder*>\VDARedirector.exe /reg<*browser*>
- VDA のアドオンの登録を解除する場合: <*VDAinstallation-folder*>\VDARedirector.exe /unreg<*browser*>

ここで <*browser*> は、「Internet Explorer」、「Firefox」、「Chrome」、または「All」です。

たとえば、Citrix Workspace アプリを実行するデバイスに、Internet Explorer 用のアドオンを登録するには、次のコマンドを実行します。

C:\Program Files\Citrix\ICA Client\redirector.exe/regIE

また、Windows マルチセッション OS VDA が動作するサーバー上ですべてのアドオンを登録するには、次のコマンドを実行します。

C:\Program Files (x86)\Citrix\HDX\bin\VDARedirector.exe /regAll

さまざまな **Web** ブラウザーでの **URL** リダイレクト

- Internet Explorer では、入力された URL がデフォルトでリダイレクトされます。禁止リストに追加されていない URL が Web ブラウザーや Web サイトによりほかの URL にリダイレクトされた場合、最終的な URL はリダイレクトされません。禁止リストにあってもリダイレクトされません。

URL リダイレクトが正しく機能するためには、Web ブラウザーに表示されるメッセージに従ってアドオンを有効にする必要があります。インターネットオプションを使用するアドオンやメッセージで示されたアドオンが無効の場合、URL リダイレクトは正しく機能しません。

- Firefox アドオンでは、URL が常にリダイレクトされます。

Firefox では、アドオンのインストールを許可するかどうかを確認するメッセージが新しいタブに表示されます。URL リダイレクトが正しく機能するためには、アドオンのインストールを許可します。

- Chrome のアドオンでは、ユーザーがナビゲーションにより開いた最終的な URL（ユーザーが入力したものでない URL）は常にリダイレクトされます。

拡張機能が外部的にインストールされます。この拡張機能を無効にすると、Chrome で URL リダイレクトが動作しなくなります。シークレットモードで URL リダイレクトを使用するには、Web ブラウザーの設定でシークレットモードでの拡張機能の実行を許可する必要があります。

ログオフおよび切断時のローカルアプリケーションの動作の構成

> 注:
>
> 以下の手順どおりに設定を構成しなかった場合、ユーザーが仮想デスクトップからログオフまたは切断しても、デフォルトで、ローカルアプリケーションは実行したまま保持されます。仮想デスクトップに再接続すると、そのローカルアプリケーションが再統合されます（仮想デスクトップで使用可能な場合）。

ログオフおよび切断時のローカルアプリケーションの動作を構成するには、レジストリを介して管理される機能の一覧にある「ログオフおよび切断時のローカルアプリケーションの動作」を参照してください。

汎用 **USB** リダイレクトとクライアント側ドライブの考慮事項

August 17, 2024

HDX テクノロジは、一般的な USB デバイスのほとんどに最適化されたサポートを提供します。最適化されたサポートにより、パフォーマンスが良くなることでユーザーエクスペリエンスが向上し、WAN 経由の帯域幅効率が改善されます。最適化されたサポートは通常、遅延が多い環境やセキュリティが厳しい環境で最善のオプションです。

HDX テクノロジにより、特殊デバイスに次のような最適化されたサポートがないときや、不適切なときに汎用 **USB** リダイレクトを使用できます:

- USB デバイスに追加の高度な機能があり（追加ボタンがあるマウスや Web カメラなど）、それらの機能が最適化されたサポートに含まれていないとき。
- ユーザーが最適化されたサポートに含まれない機能を必要とするとき。
- USB デバイスが特殊なデバイス（テスト用機器、測定用機器、工業用コントローラーなど）であるとき。
- アプリケーションが USB デバイスとしてデバイスに直接アクセスする必要があるとき。
- USB デバイスで Windows ドライバーしか使用できないとき。たとえば、スマートカードリーダーには、Android 向け Citrix Workspace アプリで使用できるドライバーがないことがあります。
- 使用しているバージョンの Citrix Workspace アプリで、該当するタイプの USB デバイスに最適化されたサポートを利用できないとき。

汎用 USB リダイレクトでは、以下に注意してください。

- ユーザーデバイスにデバイスドライバーをインストールする必要はありません。
- USB クライアントドライバーは VDA マシン上にインストールされます。

> 重要:
>
> - 汎用 USB リダイレクトは、最適化されたサポートと併用できます。汎用 USB リダイレクトを有効にする場合は、Citrix の「USB デバイスのポリシー設定」で汎用 USB リダイレクトと最適化されたサポートの両方を構成します。
> - 一部の USB デバイスでは、クライアント USB デバイス最適化規則の Citrix ポリシー設定が、汎用 USB

> リダイレクト専用の設定となります。ここで説明したような、最適化されたサポートには該当しません。

USB デバイスのパフォーマンスに関する考慮事項

一部のタイプの USB デバイスで汎用 USB リダイレクトを使用する場合、ネットワークの遅延と帯域幅がユーザーエクスペリエンスと USB デバイスの操作に影響を与えます。たとえば、遅延が多く低帯域幅のリンクでタイミングが重要なデバイスが正しく動作しないことがあります。可能な場合は、代わりに最適化されたサポートを使用してください。

3D マウスなどの一部の USB デバイスは、高い帯域幅を使用できる必要があります（通常、これも高帯域幅を必要とする 3D アプリとともに使用）。帯域幅を増やすことができない場合には、帯域幅ポリシー設定を使用して他のコンポーネントの帯域幅使用状況を調整することで、問題を緩和できます。詳しくは、「帯域幅のポリシー設定」（クライアント USB デバイスリダイレクトの場合）および「マルチストリーム接続のポリシー設定」を参照してください。

USB デバイスのセキュリティに関する考慮事項

スマートカードリーダーやフィンガープリントリーダー、署名パッドなどの一部の USB デバイスは、もともとセキュリティを重視します。USB ストレージデバイスなどの他の USB デバイスは、機密扱いである可能性のあるデータの受け渡しに使用できます。

USB デバイスは、しばしばマルウェアの配信に使用されます。このような USB デバイスのリスクは、Citrix Workspace アプリと Citrix Virtual Apps and Desktops の構成により減らすことはできますが、すべて取り除くことはできません。こうした状況は、汎用 USB リダイレクトを使用しているか最適化されたサポートを使用しているかにかかわらず発生します。

> 重要:
>
> セキュリティを重視するデバイスやデータを扱う場合は、TLSまたは IPsec のどちらかを使用して、常に HDX 接続をセキュリティで保護してください。
>
> 必要な USB デバイスのサポートのみを有効にしてください。汎用 USB リダイレクトと最適化されたサポートの両方で、このニーズを満たしてください。
>
> USB デバイスの安全な使用についての以下のようなガイダンスをユーザーに提供してください。
>
> - 信頼できるソースから入手した USB デバイスのみを使用する。
> - USB デバイスを人がいないオープンな環境に置きっぱなしにしない（例: インターネットカフェに Flash ドライブを置きっぱなしにしない）。
> - また、複数のコンピューターで 1 つの USB デバイスを使用することのリスクを説明してください。

汎用 USB リダイレクトの互換性

汎用 USB リダイレクトは、USB 2.0 以前のデバイスでサポートされます。USB 3.0 デバイスを USB 2.0 または USB 3.0 ポートに接続した場合も、汎用 USB リダイレクトがサポートされます。汎用 USB リダイレクトは、USB3.0 に

導入された超高速などの USB 機能はサポートしません。

汎用 USB リダイレクトは、次の Citrix Workspace アプリでサポートされます:

- Windows 向け Citrix Workspace アプリ。「アプリケーション配信の構成」を参照してください。
- Mac 向け Citrix Workspace アプリ。「Mac 向け Citrix Workspace アプリ」を参照してください。
- Linux 向け Citrix Workspace アプリ。「最適化」を参照してください。
- Chrome OS 向け Citrix Workspace アプリ。「Chrome 向け Citrix Workspace アプリ」を参照してください。

Citrix Workspace アプリのバージョンについては、『Citrix Workspace app feature matrix』を参照してください。

過去のバージョンの Citrix Workspace アプリを使用している場合は、Citrix Workspace アプリのドキュメントを参照して、汎用 USB リダイレクトがサポートされていることを確認してください。サポート対象の USB デバイスのタイプに関する制限事項については、Citrix Workspace アプリのドキュメントを参照してください。

汎用 USB リダイレクトはシングルセッション OS 対応 VDA のバージョン 7.6 以上のデスクトップセッションでサポートされます。

汎用 USB リダイレクトはマルチセッション OS 対応 VDA のバージョン 7.6 以上のデスクトップセッションでサポートされますが、以下の制限事項があります:

- VDA は Windows Server 2012 R2、Windows Server 2016、Windows Server 2019、Windows Server 2022 のいずれかで動作している必要があります。
- USB デバイスドライバーには、完全仮想化サポートなど、VDA OS（Windows 2012 R2）のリモートデスクトップセッションホスト（RDSH）との完全な互換性がある必要があります。

次のような一部のタイプの USB デバイスは、リダイレクトしても役に立たないため、汎用 USB リダイレクトをサポートしません。

- USB モデム。
- USB ネットワークアダプター。
- USB ハブ。USB ハブに接続した USB デバイスは、個別に扱われます。
- USB 仮想 COM ポート。汎用 USB リダイレクトではなく、COM ポートリダイレクトを使用します。

汎用 USB リダイレクトでテストされた USB デバイスについては、Citrix Ready Marketplaceを参照してください。一部の USB デバイスは、汎用 USB リダイレクトを使用すると正しく動作しません。

汎用 **USB** リダイレクトの設定

汎用 USB リダイレクトを使用する USB デバイスのタイプを制御し、個別に構成できます。

- Citrix ポリシー設定を使って VDA で設定します。詳しくは、「ポリシー設定リファレンス」の「クライアントドライブやデバイスのリダイレクト」、および「USB デバイスのポリシー設定」を参照してください。

- Citrix Workspace アプリで、Citrix Workspace アプリに依存するメカニズムを使用して設定します。たとえば、管理用テンプレートは、Windows 向け Citrix Workspace アプリを構成するレジストリ設定を制御できます。USB リダイレクトのデフォルトでは、特定のクラスの USB デバイスでのみ許可され、ほかのクラスのデバイスはリダイレクトされません。詳しくは、Windows 向け Citrix Workspace アプリのドキュメントの「構成」を参照してください。

別々に設定できることで柔軟性が提供されます。例:

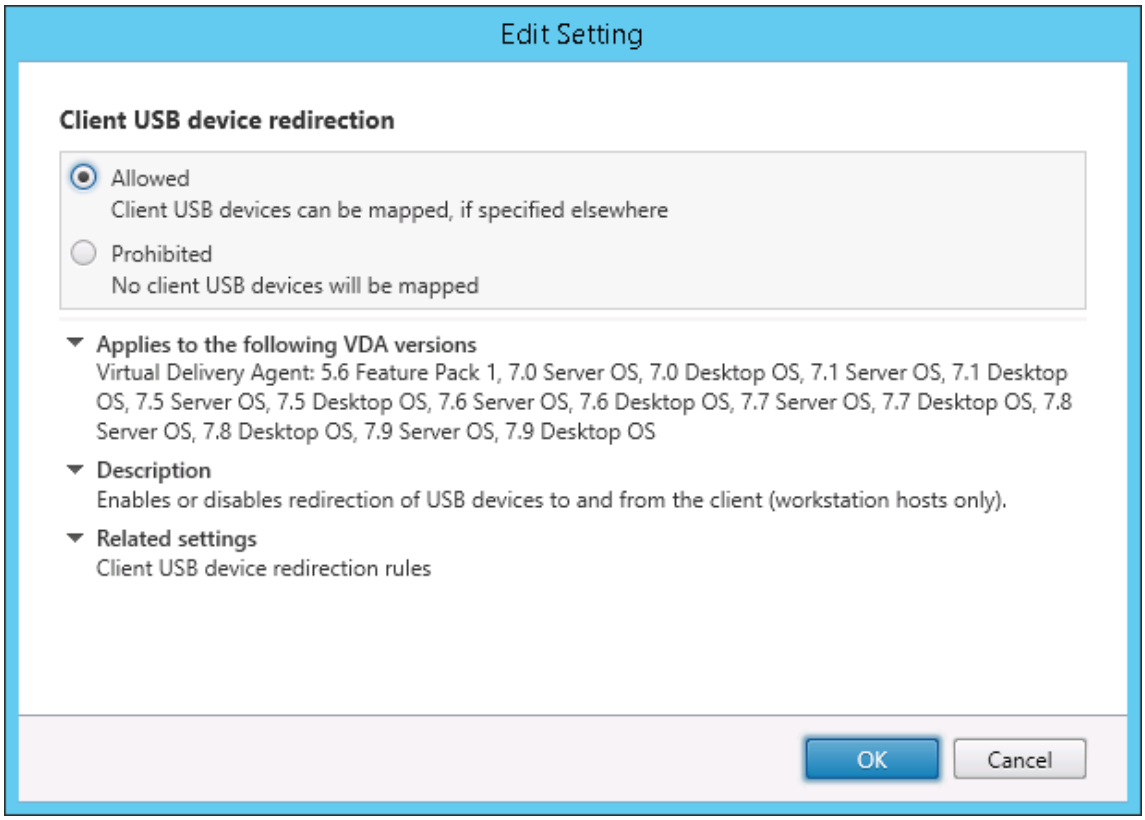
- 2 つの異なる組織または部門が Citrix Workspace アプリと VDA を担当している場合に、それぞれが別に制御を実行できます。この構成は、ある組織のユーザーが別の組織のアプリケーションにアクセスするときにも適用されます。
- Citrix ポリシー設定では、特定のユーザー、または（Citrix Gateway 経由ではなく）LAN 経由で接続しているユーザーのみに許可された USB デバイスを制御できます。

汎用 **USB** リダイレクトの有効化

汎用 USB リダイレクトを有効化して、ユーザーの手動リダイレクトを不要にするには、Citrix ポリシー設定と Citrix Workspace アプリの接続設定の両方を構成します。

Citrix ポリシー設定で、次の手順に従います:

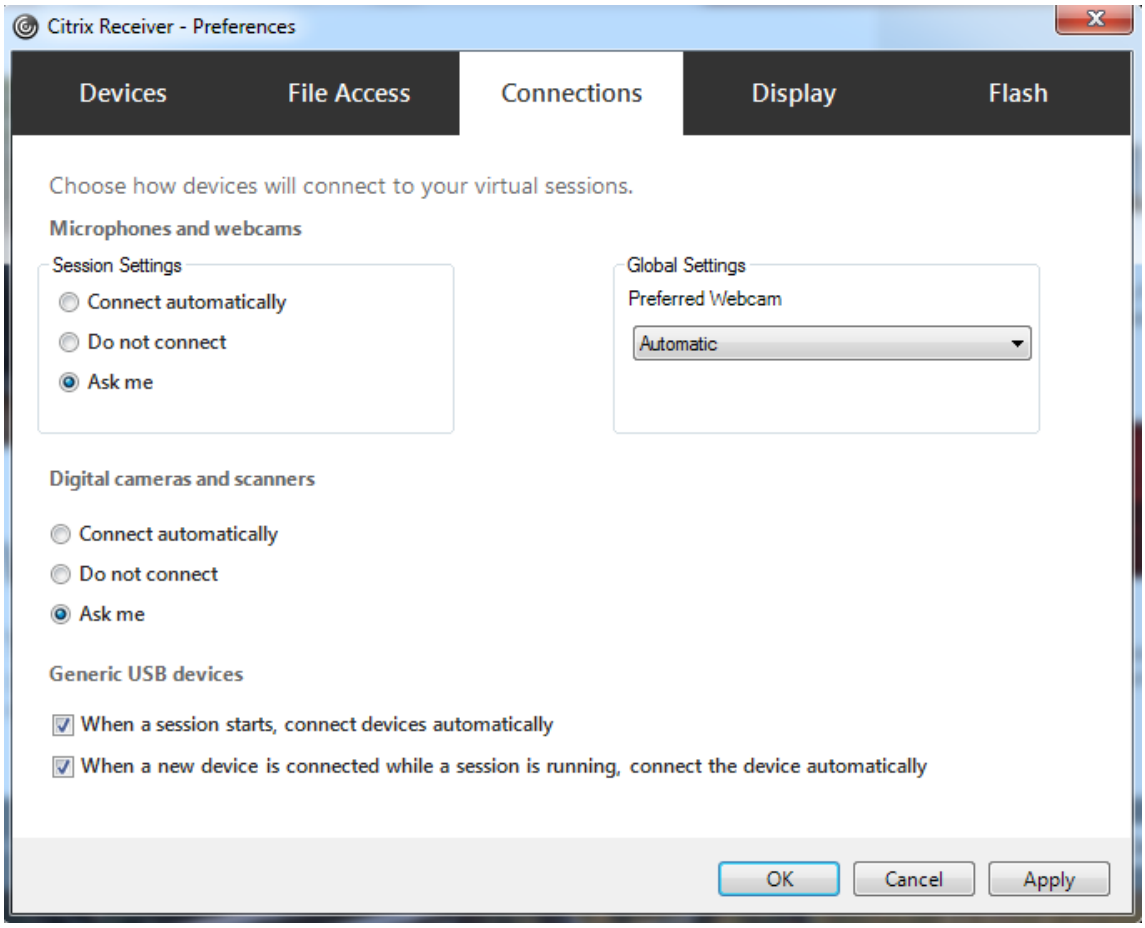
1. ポリシーに ［クライアント USB デバイスリダイレクト］ を追加して、値を ［許可］ に設定します。



2. 必要な場合は、ポリシーに ［クライアント USB デバイスリダイレクト規則］ 設定を追加して USB ポリシー規則を指定し、リダイレクトする USB デバイスの一覧を変更します。

   ポリシー設定が完了したら、Citrix Workspace アプリで以下を実行します:

3. デバイスが手動リダイレクトなしで自動的に接続されるように設定します。この設定は、管理用テンプレートを使うか、Windows 向け Citrix Workspace アプリの ［基本設定］ > ［接続］ で実行できます。



前の手順で VDA の USB ポリシー規則を指定した場合は、Citrix Workspace アプリにも同じポリシー規則を指定します。

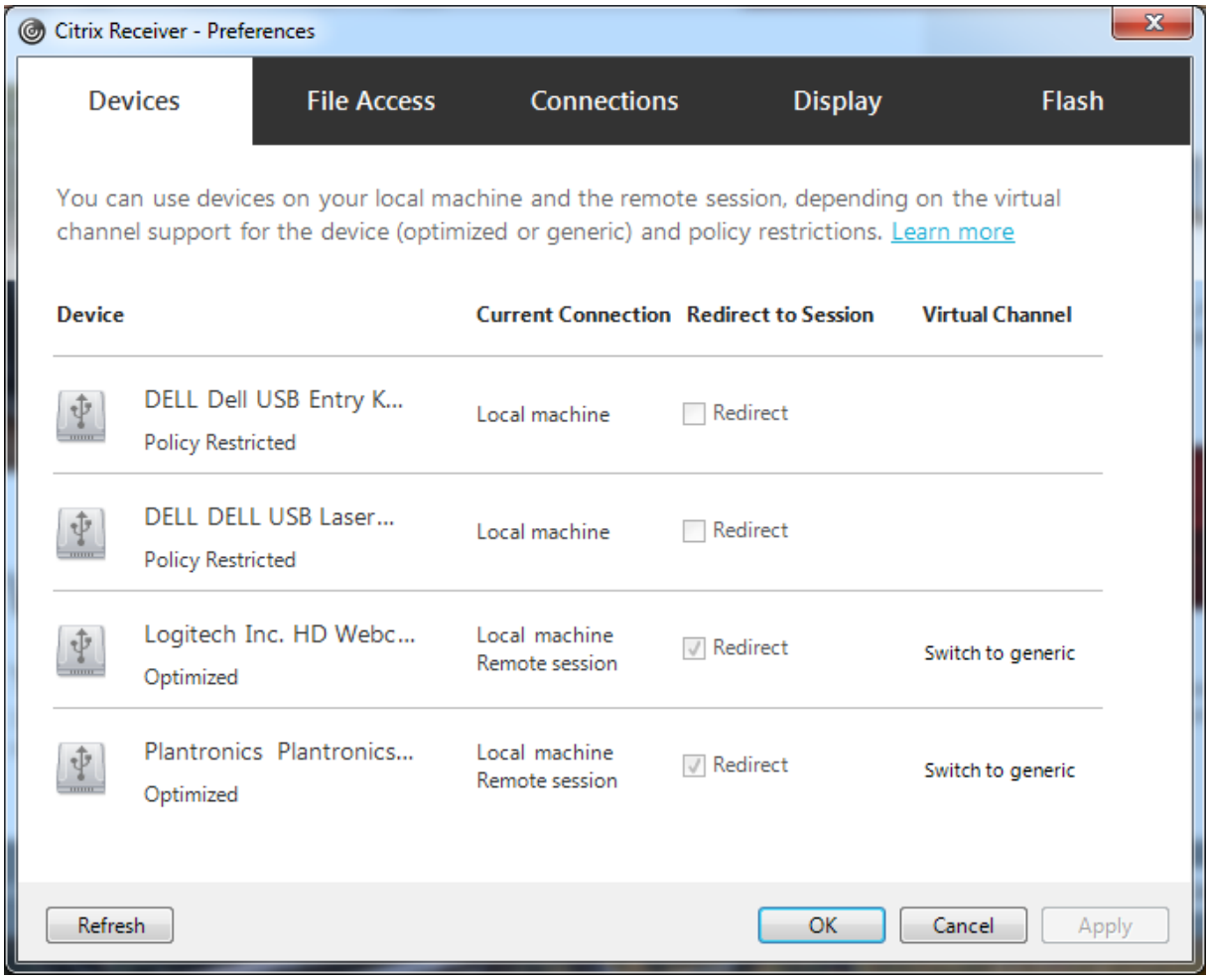
シンクライアントでの USB サポートおよびその構成方法については、デバイスの製造元に問い合わせてください。

汎用 **USB** リダイレクトで使用できる **USB** デバイスタイプの設定

USB サポート機能が有効になっており、USB 関連のユーザー設定で USB デバイスに自動接続するように設定されている場合は、USB デバイスが自動的にリダイレクトされます。接続バーが表示されていない場合も、USB デバイスは自動的にリダイレクトされます。

ユーザーは、USB デバイスの一覧からデバイスを選択することによって、自動的にリダイレクトされないデバイスを明示的にリダイレクトすることができます。詳しくは、Windows 向け Citrix Workspace アプリのユーザーヘルプ

の「Desktop Viewer でのデバイスの表示」を参照してください。



最適化されたサポートではなく汎用 USB リダイレクトを使用するには、次のどちらかの手順を実行します。

- Citrix Workspace アプリで、汎用 USB リダイレクトを使う USB デバイスを手動で選択し、［基本設定］ダイアログボックスの［デバイス］タブで ［汎用に切り替え］をオンにします。
- USB デバイスタイプの自動リダイレクトを設定することで（たとえば AutoRedirectStorage=1）、汎用 USB リダイレクトを使う USB デバイスを自動選択して、USB ユーザー基本設定を自動接続 USB デバイスに設定します。詳しくは、「USB デバイスの自動リダイレクトの設定」を参照してください。

> 注:
>
> Web カメラと HDX マルチメディアリダイレクトの互換性がない場合は、Web カメラで使用する汎用 USB リダイレクトのみを設定します。

Citrix Workspace アプリおよび VDA のデバイス規則を定義して、USB デバイスを一覧に表示しないようにしたり、リダイレクトできないようにしたりできます。

汎用 USB リダイレクトでは、少なくとも USB デバイスクラスとサブクラスを知っておく必要があります。すべての USB デバイスが明確な USB デバイスクラスとサブクラスを持つわけではありません。例:

- ペンはマウスデバイスクラスを使用します。
- スマートカードリーダーはベンダー定義のクラスまたは HID デバイスクラスを使用できます。

より正確な制御のためには、ベンダー ID、製品 ID、およびリリース ID を知っておく必要があります。この情報はデバイスベンダーから入手できます。

> 重要:
>
> 悪意のある USB デバイスが、意図された使用状況にマッチしない USB デバイス特性を示すことがあります。デバイス規則は、この動作を防ぐことを目的としていません。

USB デバイスリダイレクト規則を指定し、デフォルトの USB ポリシー規則よりも優先することで、汎用 USB リダイレクトを使用できる USB デバイスを制御できます。

Citrix DaaS（旧称 Citrix Virtual Apps and Desktops サービス）:

- ほとんどの場合、Citrix グループポリシー管理コンソール MSI(`CitrixGroupPolicyManagement_x64.msi`）をダウンロードして Active Directory システムにインストールしてから、AD グループポリシーを管理します（MSI を VDA にインストールしないでください）。
- Windows 向け Citrix Workspace アプリの場合、ユーザーデバイスレジストリを編集します。インストールメディアに収録されている管理テンプレート（ADM ファイル）により、Active Directory のグループポリシーを使用してユーザーデバイスを変更できます：DVD のルート`\os\lang\Support\Configuration\icaclient_usb.adm`

オンプレミス Citrix Virtual Apps and Desktops:

- VDA については、グループポリシー規則を介して、マルチセッション OS マシン上の OS の管理者による上書き規則を編集します。グループポリシー管理コンソールは、インストールメディアにあります。
  - x64:DVD のルート `\os\lang\x64\Citrix Policy\CitrixGroupPolicyManagement_x64.msi`
  - x86:DVD のルート `\os\lang\x86\Citrix Policy\CitrixGroupPolicyManagement_x86.msi`
- Windows 向け Citrix Workspace アプリの場合、ユーザーデバイスレジストリを編集します。インストールメディアに収録されている管理テンプレート（ADM ファイル）により、Active Directory のグループポリシーを使用してユーザーデバイスを変更できます：DVD のルート`\os\lang\Support\Configuration\icaclient_usb.adm`

> 警告:
>
> レジストリエディターの使用を誤ると、深刻な問題が発生する可能性があり、オペレーティングシステムの再インストールが必要になる場合もあります。レジストリエディターの誤用による障害に対して、Citrix では一切責任を負いません。レジストリエディターは、お客様の責任と判断の範囲でご使用ください。また、レジストリファイルのバックアップを作成してから、レジストリを編集してください。

製品のデフォルトの規則は、HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ICA Client\GenericUSB に保存されます。このデフォルトの規則は変更しないでください。ただし、以下で説明しているように、製品のデフォルトの規則を参照して管理者による上書き規則を作成できます。管理者による上書き規則は、製品のデフォルトの規則よりも先に評価されます。

管理者による上書き規則は、HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\PortICA\GenericUSB\DeviceRules に保存されます。GPO ポリシー規則は、**{Allow: | Deny:}** の後にスペースで区切った一連の「*tag=value*」式の形式で設定します。

以下のタグがサポートされます。

タグ	説明
VID	デバイス記述子のベンダー ID
PID	デバイス記述子の製品 ID
REL	デバイス記述子のリリース ID
クラス	デバイス記述子またはインターフェイス記述子のクラス。使用可能な USB クラスコードについては、USB Web サイトhttp://www.usb.org/を参照してください
SubClass	デバイス記述子またはインターフェイス記述子のサブクラス
Prot	デバイス記述子またはインターフェイス記述子のプロトコル

ポリシー規則を作成する場合、以下の点に注意してください。

- 大文字と小文字は区別されません。
- 規則の末尾に、「#」で始まる任意のコメントを追加できます。区切り文字は不要で、コメントは無視されます。
- 空白行およびコメントのみの行は無視されます。
- 区切り文字にはスペースが使用されますが、番号または識別子の間には使用できません。たとえば、「Deny: Class = 08 SubClass=05」は有効ですが、「Deny: Class=0 Sub Class=05」は無効です。
- タグには等号（=）を使用する必要がありますたとえば、VID=1230 とします。
- 各規則を 1 行ずつ記述するか、同一行に記述する場合はセミコロンで区切られたリスト形式である必要があります。

> 注:
>
> - Citrix Virtual Apps and Desktops バージョン 2212 以降、一部の USB デバイスで汎用 USB リダイレクト機能の使用が無効になっています。これらのデバイスは、それぞれのベンダー ID（VID）と製品 ID（PID）を使用して明示的に追加する必要があります。
> - ADM テンプレートを使用する場合は、規則を単一行に（セミコロン区切りのリストとして）作成する必

> 要があります。

例:

- 次の例に、ベンダー ID と製品 ID に関する管理者定義の USB ポリシー規則を示します。

```
Allow: VID=046D PID=C626 # Allow Logitech SpaceNavigator 3D Mouse
 Deny: VID=046D # Deny all Logitech products
```

- 次の例に、クラス、サブクラス、およびプロトコルに関する管理者定義の USB ポリシー規則を示します。

```
Deny: Class=EF SubClass=01 Prot=01 # Deny MS Active Sync devices
Allow: Class=EF SubClass=01 # Allow Sync devices Allow: Class=EF
# Allow all USB-Miscellaneous devices
```

USB デバイスの装着と取り外し

ユーザーは、仮想セッションの開始前および開始後に USB デバイスを装着できます。

Windows 向け Citrix Workspace アプリでは、以下の点について考慮してください:

- セッションを開始した後で装着したデバイスは、Desktop Viewer の［USB］メニューに直ちに追加されます。
- USB デバイスが正しくリダイレクトされない場合、仮想セッションが開始されてからデバイスを装着することで問題が解決される場合があります。
- データの損失を避けるため、Windows で推奨される手順（［ハードウェアの安全な取り外し］アイコンの使用など）に従って USB デバイスを取り外してください。

USB マスストレージデバイスのセキュリティ制御

USB マスストレージデバイスでは最適化されたサポートが提供されます。このサポートは、Citrix Virtual Apps and Desktops のクライアント側ドライブのマッピング機能に含まれています。ユーザーのログオン時にユーザーデバイス上のドライブが自動的に仮想デスクトップのドライブ文字にマップされます。これらのドライブは、マップされたドライブ文字を持つ共有フォルダーとして表示されます。クライアント側ドライブのマッピングを構成するには、［クライアント側リムーバブルドライブ］設定を使用します。この設定は、ICA ポリシー設定の［ファイルリダイレクトポリシー設定］セクションにあります。

USB マスストレージデバイスでは、Client 側ドライブのマッピングまたは汎用 USB リダイレクトのどちらか、またはこの両方を使用できます。これらは Citrix ポリシーを使って制御されます。主な違いは次のとおりです。

機能	クライアントドライブマッピング	汎用 USB リダイレクト
デフォルトで有効	はい	いいえ
読み取り専用アクセスの構成が可能	はい	いいえ

機能	クライアントドライブマッピング	汎用 USB リダイレクト
デバイスアクセスが暗号化される	はい、デバイスにアクセスする前に暗号化のロックを解除した場合	はい
BitLocker To Go デバイス	いいえ	いいえ
セッション中にデバイスを安全に取り外せる	いいえ	はい（ユーザーがオペレーティングシステムで推奨される手順に従う場合）

汎用 USB リダイレクトとクライアント側ドライブのマッピングのポリシーの両方が有効な場合、セッション開始前または後に装着されたマスストレージデバイスがクライアント側ドライブのマッピングによりリダイレクトされます。汎用 USB リダイレクトとクライアント側ドライブのマッピングのポリシーの両方が有効で、自動リダイレクトが構成されている場合、セッション開始前または後に装着されたマスストレージデバイスが汎用 USB リダイレクトによりリダイレクトされます。詳しくは、Knowledge Center のCTX123015を参照してください。

> 注:
>
> USB リダイレクトはより低い帯域幅の接続（50Kbps など）でもサポートされます。ただし、大きなファイルはコピーできません。

印刷

August 17, 2024

環境でのプリンター管理には、以下の複数の段階があります。

1. 印刷の概念を理解します。
2. 印刷アーキテクチャを計画します。これには、業務上のニーズや既存の印刷インフラストラクチャについての分析と、ユーザーやアプリケーションが現状でどのように印刷を行っているか、および理想的な印刷管理モデルは何かについての評価が含まれます。
3. プリンタープロビジョニングの方法を選択し、印刷設計を展開するためのポリシーを作成して印刷環境を構成します。新しい従業員またはサーバーが追加されたときにポリシーを更新します。
4. 新しい印刷環境を実務環境に展開する前に、その環境をテストします。
5. プリンタードライバーを管理し、印刷のパフォーマンスを最適化して Citrix の印刷環境を維持します。
6. 発生する問題をトラブルシューティングします。

印刷の概念

印刷環境の構築を計画する前に、Citrix 環境での印刷処理の主な概念について理解しておく必要があります。

- 使用できるプリンタープロビジョニングの種類
- 印刷ジョブをどのようにルーティングするか
- プリンタードライバーの基本的な管理方法

印刷の概念は、Windows の印刷概念上に構成されています。環境での印刷設定を正しく管理するには、Windows でのネットワークやクライアント印刷のしくみについて熟知しており、それが実際の環境にどのように適用されるのかを理解する必要があります。

印刷プロセス

この環境では、ユーザーによる印刷はすべてアプリケーションをホストするマシン上で開始されます。印刷ジョブはネットワークプリントサーバーまたはユーザーデバイスを介して印刷装置にリダイレクトされます。

仮想デスクトップやアプリケーションのユーザーに提供されるワークスペースは永続的ではありません。ユーザーのセッションが終了すると、そのユーザーのワークスペースはサーバーから削除されます。このため、各セッションの開始時にすべての設定を再構築する必要があります。この結果、ユーザーが新しいセッションを開始するたびに、ユーザーのワークスペースが再構築されます。

ユーザーが印刷を実行すると、以下の処理が行われます。

- ユーザーに提供するプリンターを決定します。この処理は、プリンタープロビジョニングと呼ばれます。
- ユーザーの印刷設定を復元します。
- セッションのデフォルトプリンターを決定します。

管理者は、プリンタープロビジョニング、印刷ジョブの送信経路、プリンタープロパティの保存、およびプリンタードライバー管理に関するオプションを変更して、上記の処理をカスタマイズできます。これらのオプションの変更によって環境での印刷パフォーマンスやユーザーエクスペリエンスがどのように変化するのかを検証してください。

プリンタープロビジョニング

セッション用のプリンターを準備する処理は、プリンタープロビジョニングと呼ばれます。通常、この処理は動的に行われます。つまり、セッションで提供されるプリンターは事前定義されておらず、非永続的です。プリンターは、セッションへのログオン時または再接続時にポリシーに基づいて構成されます。このため、ポリシー、ユーザーの場所、およびネットワークに基づいて、異なるプリンターをユーザーに提供できます。つまり、ユーザーが別の場所に移動すると、そのユーザーの印刷環境が変更されます。

この Citrix 製品の環境では、クライアント側のプリンターが監視され、クライアント側プリンターの追加、削除、および変更に応じてセッションの自動作成プリンターが動的に変更されます。この動的プリンター検出は、さまざまなデバイスを使用するモバイルユーザーにとって便利な機能です。

プリンターのプロビジョニングには、主に以下の方法があります:

- ユニバーサルプリントサーバー - Citrixユニバーサルプリントサーバーは、ネットワークプリンターでのユニバーサル印刷をサポートします。ユニバーサルプリントサーバーでは、ユニバーサルプリンタードライバーが

使用されます。これにより、マルチセッション OS マシン上の単一のドライバーを使って、任意のデバイスからネットワーク印刷を実行できます。

リモートの印刷サーバーを使う環境では、Citrix ユニバーサルプリントサーバーの使用をお勧めします。ユニバーサルプリントサーバーで送信される印刷ジョブは最適化および圧縮されるため、ネットワーク消費を抑えてユーザーエクスペリエンスを向上させることができます。

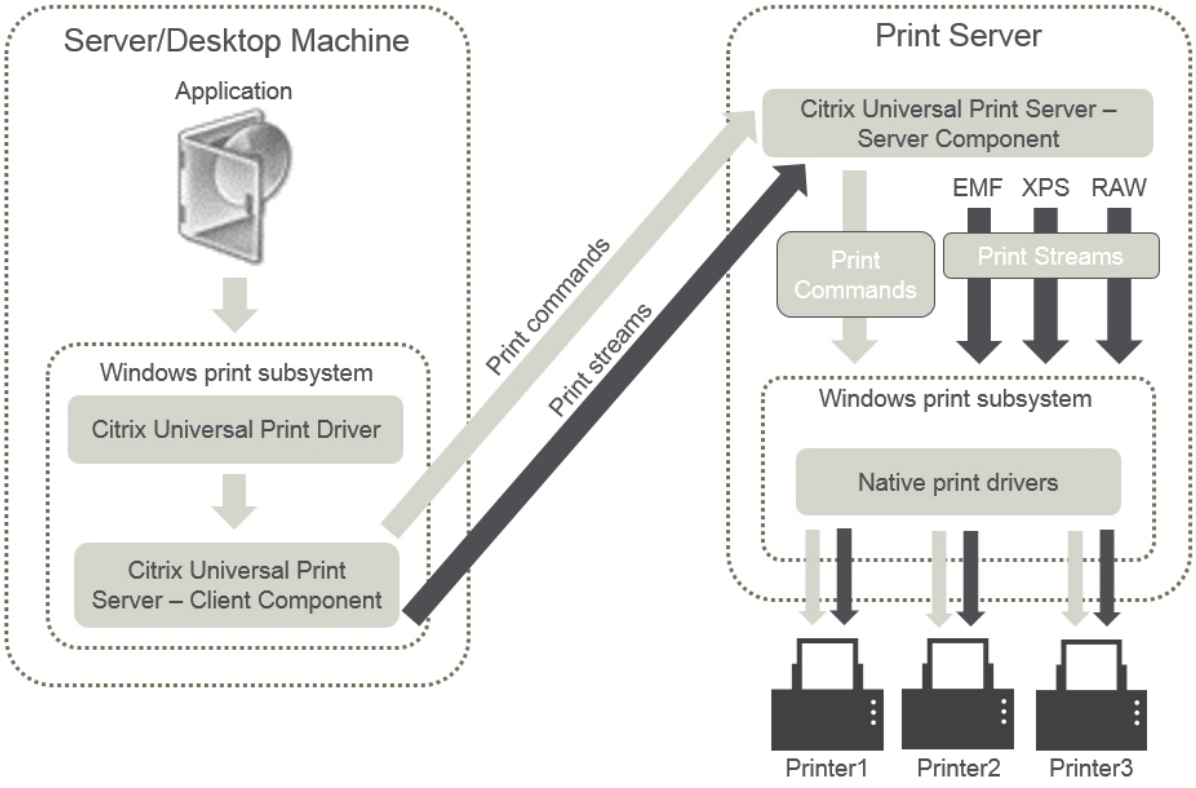
ユニバーサルプリントサーバーの機能は以下のコンポーネントで構成されます。

クライアントコンポーネント、ユニバーサルプリントクライアント - 各マルチセッション OS マシンでユニバーサルプリントクライアントを有効にして、セッションネットワークプリンターをプロビジョニングし、ユニバーサルプリントドライバーを使用します。

サーバーコンポーネント、ユニバーサルプリントサーバー - 各プリントサーバーにユニバーサルプリントサーバーをインストールして、セッションネットワークプリンターをプロビジョニングし、（セッションプリンターが一元的にプロビジョニングされているかどうかにかかわらず）セッションプリンターにユニバーサルプリントドライバーを使用します。

ユニバーサルプリントサーバーの要件とセットアップ詳細については、システム要件およびインストールに関する説明を参照してください。

次の図は、ユニバーサルプリントサーバーを使用する環境におけるネットワークベースのプリンターの一般的なワークフローを示しています。



Citrix ユニバーサルプリントサーバーを有効にすると、接続されているすべてのネットワークプリンターでユニバー

サルプリントサーバーが自動検出されて使用されます。

- 自動作成—自動作成とは、各セッションの開始時に自動的に作成されるプリンターを指します。リモートネットワークプリンターとローカルに接続されたクライアントプリンターの両方を自動作成できます。ユーザーあたりのプリンター数が多い環境では、デフォルトのクライアントプリンターだけが自動作成されるように構成することを検討します。自動作成するプリンターの数を最小限にすることで、マルチセッション OS マシンの負荷（メモリや CPU）を軽減できます。また、これによりユーザーログオン時間も短縮されます。

  以下の項目に基づいてプリンターが自動作成されます。

  - ユーザーデバイス上にインストールされたプリンター。
  - セッションに適用されるポリシー。

    管理者は、自動作成に関するポリシーを設定して、作成されるプリンターの数や種類を制御できます。デフォルトでは、ユーザーデバイス上で設定されているすべてのプリンター（ローカル接続のプリンターおよびネットワークプリンター）が自動作成され、ユーザーに提供されます。

  ユーザーがセッションを終了すると、これらのプリンターは削除されます。

  クライアントプリンターおよびネットワークプリンターの自動作成機能を使用する場合、保守作業が必要です。たとえば、プリンターを追加した場合は以下の設定が必要になります:

  - ポリシーの［セッションプリンター］設定を更新します。
  - ポリシーの［プリンタードライバーのマッピングと互換性］設定ですべてのマルチセッション OS マシンにドライバーを追加します。

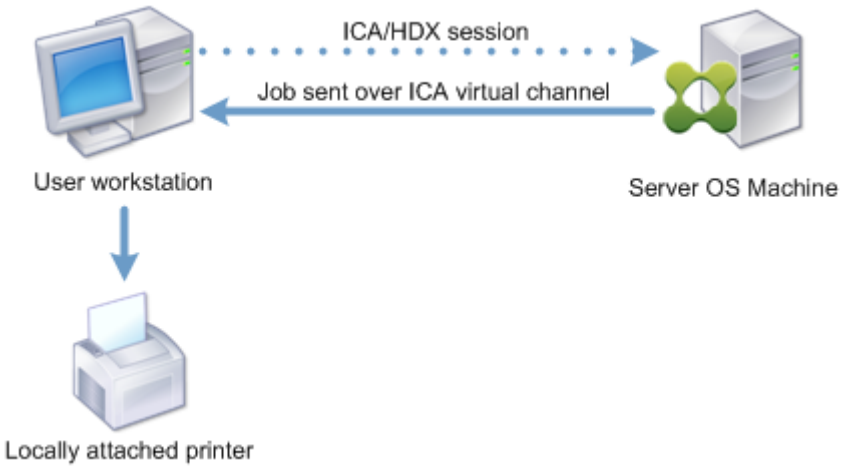
印刷ジョブの送信

印刷経路という語は、印刷ジョブがどのような経路で印刷装置に転送されるのか、および印刷ジョブがどこにスプールされるのかという概念を含んでいます。印刷環境を管理する場合、これらの概念を理解することは重要です。印刷ジョブのルーティング経路はネットワークトラフィックに影響し、スプール場所は印刷ジョブを処理するコンピューターの負荷に影響します。

この環境では、印刷装置への印刷ジョブの転送経路として、クライアント経由とネットワーク上のプリントサーバー経由の 2 つがあります。これらの転送経路は、「クライアント印刷経路」および「ネットワーク印刷経路」と呼ばれます。デフォルトでどちらの印刷経路が使用されるかは、使用されるプリンターの種類により異なります。

ローカル接続のプリンター

印刷ジョブは、マルチセッション OS マシンからクライアントに送信され、さらにローカル接続のプリンターに転送されます。この場合、ICA プロトコルにより最適化および圧縮された印刷ジョブがネットワーク上に送信されます。印刷装置がユーザーデバイスにローカルに接続されている場合、印刷ジョブが ICA 仮想チャネルで転送されます。



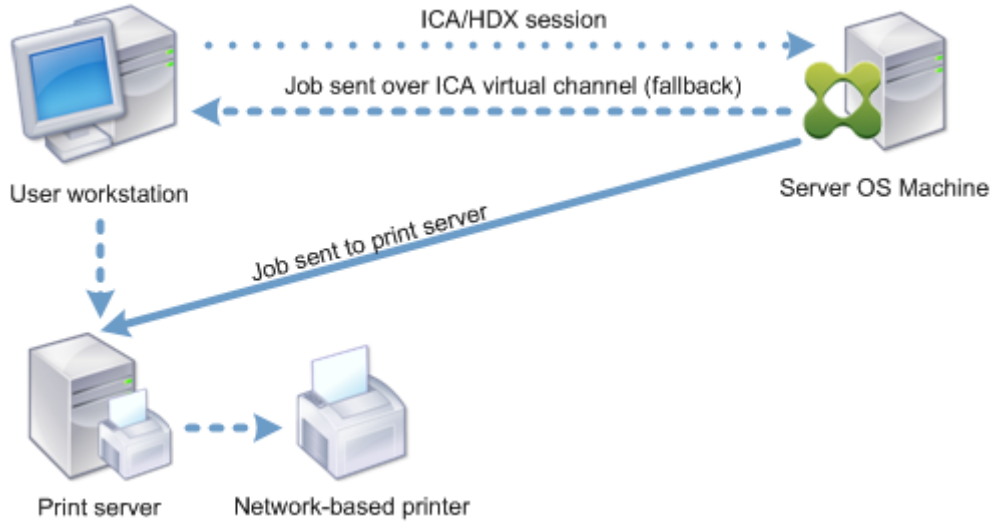
ネットワークベースのプリンター

デフォルトでは、マルチセッション OS マシンからのすべての印刷ジョブがネットワークを介してプリントサーバーに直接転送されます。ただし、以下の状況では印刷ジョブが自動的に ICA 仮想チャネルで転送されます。

- 仮想デスクトップまたはアプリケーションがプリントサーバーにアクセスできない場合。
- プリンター固有のドライバーがマルチセッション OS マシン上にない場合。

ユニバーサルプリントサーバーが無効な場合、ICA 仮想チャネルを介して送信される印刷ジョブは最適化および圧縮されるため、WAN などの狭帯域幅接続で隔たれたサーバーとクライアント間でクライアント印刷経路が使用されるように構成するとネットワークトラフィックへの負担が軽減されます。

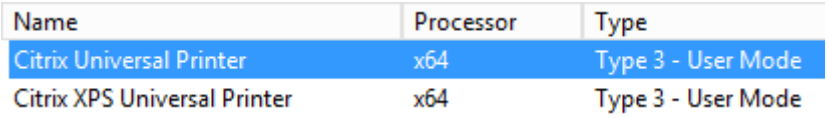
また、クライアント印刷経路では、印刷ジョブに割り当てられる帯域幅を制限できます。印刷機能がないシンクライアントなど、ユーザーデバイスを介して印刷ジョブを転送できない場合は、QoS 設定で ICA/HDX トラフィックを優先させて、セッションで良好なユーザーエクスペリエンスが提供されるように構成してください。



プリンタードライバーの管理

Citrix ユニバーサルプリンタードライバー（UPD）は、デバイスに依存しないプリンタードライバーで、大部分のプリンターに対して互換性があります。Citrix UPD は、以下の 2 つのコンポーネントで構成されています。

サーバーコンポーネント。Citrix UPD は、Citrix Virtual Apps and Desktops VDA のインストールの一部としてインストールされます。VDA は、Citrix UPD とともに次のドライバーをインストールします：Citrix ユニバーサルプリンター（EMF ドライバー）および Citrix XPS ユニバーサルプリンター（XPS ドライバー）。



VDA インストーラーでは、ユニバーサルプリントサーバー PDF プリンタードライバーのインストールを制御するオプションは提供されなくなりました。PDF プリンタードライバーは、必ず自動的にインストールされるようになりました。7.17 VDA（またはそれ以降のサポートされているバージョン）にアップグレードすると、以前にインストールされた Citrix PDF プリンタードライバーが自動的に削除されて最新バージョンに置き換えられます。

印刷ジョブが開始されると、ドライバーは、エンドポイントデバイスをいっさい変更せずに、アプリケーションの出力を記録して送信します。

クライアントコンポーネント。Citrix UPD は、Citrix Workspace アプリのインストールの一部としてインストールされます。それによって、Citrix Virtual Apps and Desktops セッションの着信する印刷ストリームがフェッチされます。印刷ストリームはローカルの印刷サブシステムに転送され、そこで印刷ジョブがデバイス固有のプリンタードライバーを使用してレンダリングされます。

Citrix UPD は次の印刷形式をサポートします。

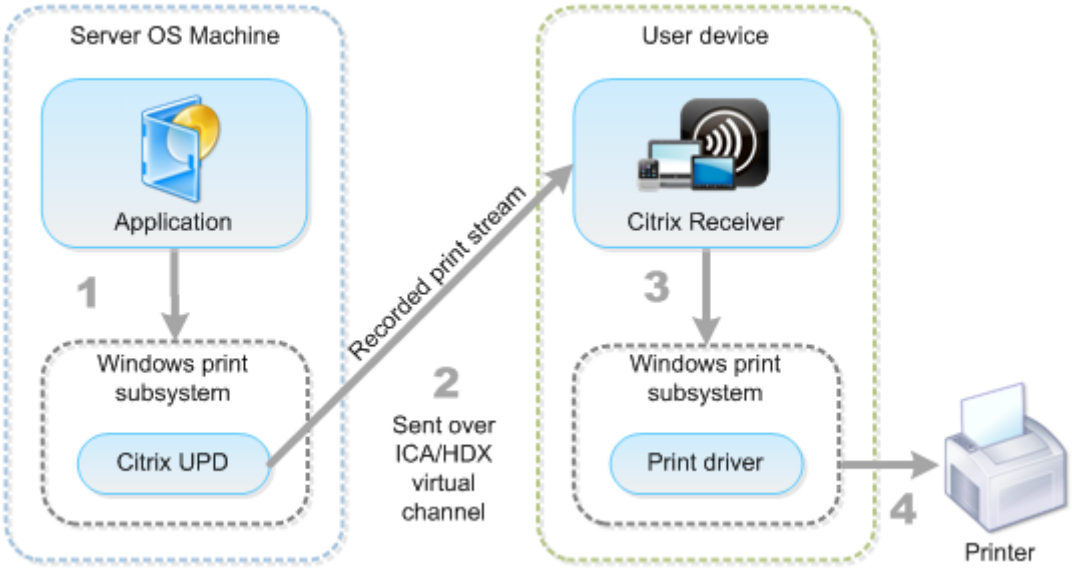
- 拡張メタファイル形式（**EMF**）、デフォルト。EMF は 32 ビットバージョンの Windows Metafile（WMF）形式です。EMF ドライバーは、Windows ベースのクライアントでのみ使用できます。
- XML Paper Specification（**XPS**）。XPS ドライバーでは XML が使用され、Adobe PDF に似た、プラットフォームに依存しない「電子ペーパー」が作成されます。
- プリンターコマンド言語（**PCL5c** および **PCL4**）。PCL は、もともとインクジェットプリンターのために Hewlett-Packard によって開発された印刷プロトコルです。基本的なテキストおよびグラフィックを印刷するために使用され、HP LaserJet および複合機で広くサポートされています。
- PostScript（**PS**）。PostScript は、テキストおよびベクターグラフィックスを印刷するために使用できるコンピューター言語です。ドライバーは、低コストのプリンターや複合機で広く使われています。

PCL および PS ドライバーは、Mac や UNIX クライアントなど、非 Windows ベースのデバイスを使用する場合に最適です。Citrix UPD がドライバーを使用する順序は、ユニバーサルドライバーの優先度ポリシー設定を使用して変更できます。

Citrix UPD（EMF および XPS ドライバー）は、ホチキス留めや給紙方法の選択など、詳細なプリンター機能をサポートします。これらの機能は、ネイティブドライバーが Microsoft の印刷機能テクノロジを使用して利用可能としている場合にのみ、利用できます。ネイティブドライバーでは、印刷機能 XML で、標準化された印刷スキーマキーワー

ドを使用する必要があります。標準化されていないキーワードを使用すると、Citrix のユニバーサルプリンタードライバーでは詳細な印刷機能を使用できなくなります。

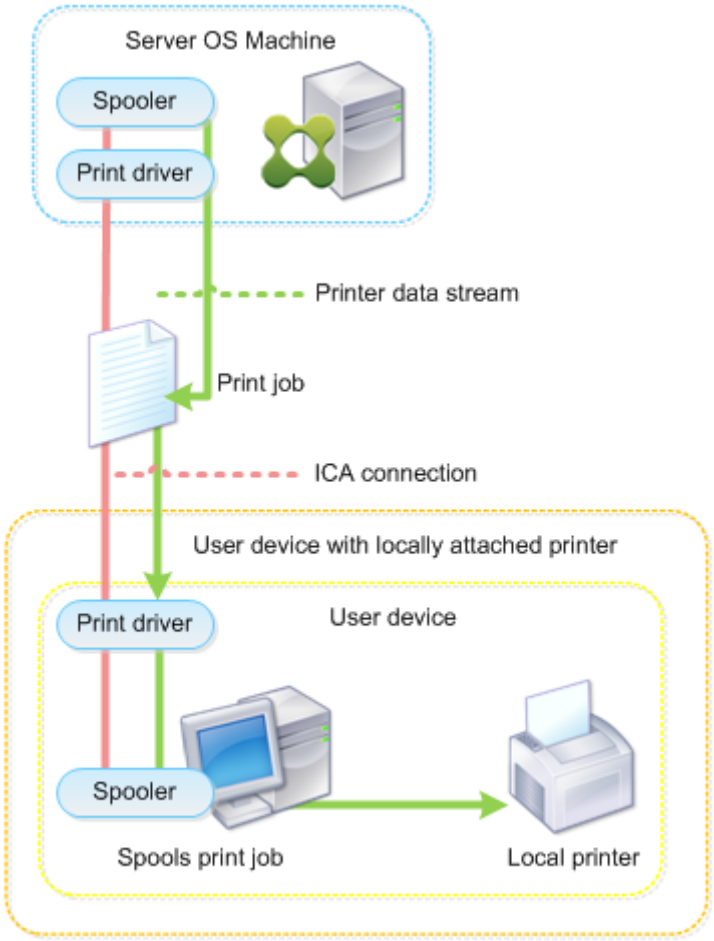
次の図は、ユニバーサルプリンタードライバーコンポーネントとデバイスにローカル接続されたプリンターの一般的なワークフローを示しています。



プリンタードライバーの管理方法を計画する場合、ユニバーサルプリンタードライバーを使用するか、デバイス固有のドライバーを使用するか、またはその両方を使用するかを決定する必要があります。標準ドライバーをサポートする場合は、以下の点を検討する必要があります。

プリンターの自動作成時に、ユーザーデバイスに接続された新しいローカルプリンターが検出されると、必要なプリンタードライバーについてマルチセッション OS マシンがチェックされます。デフォルトでは、Windows ネイティブドライバーが使用できない場合は、ユニバーサルプリンタードライバーが使用されます。

正しく印刷するには、マルチセッション OS マシン上のプリンタードライバーとユーザーデバイス上のドライバーが一致する必要があります。次の図は、クライアント印刷経路でサーバーとクライアント上のプリンタードライバーがどのように使用されるかを示しています。



- サポートするドライバーの種類。
- マルチセッション OS マシンにプリンタードライバーがない場合に自動的にインストールされるように設定するかどうか。
- プリンタードライバーの互換性リストを作成するかどうか。

関連トピック

- 印刷構成の例
- ベストプラクティス、セキュリティに関する考慮事項、およびデフォルトの操作
- 印刷に関するポリシーと設定
- プリンターのプロビジョニング
- 印刷環境の保守

印刷構成の例

August 17, 2024

組織のコンピューティング環境やユーザーのニーズに適した印刷環境を設定すると、管理が容易になります。通常、デフォルトの印刷構成でも正しく印刷できますが、ユーザーエクスペリエンスが低下したり、ネットワーク使用が最適化されなかったり、管理上のオーバーヘッドが生じたりする場合もあります。

印刷環境を設定するときは、以下の事項を考慮します。

- 業務上のニーズと既存の印刷インフラストラクチャ。

  組織のニーズに基づいて、印刷環境を設計します。既存の印刷環境（ユーザーが自分でプリンターを追加できるかどうか、どのユーザーがどのプリンターにアクセスできるか、など）を確認し、それに沿って印刷環境を構成できます。

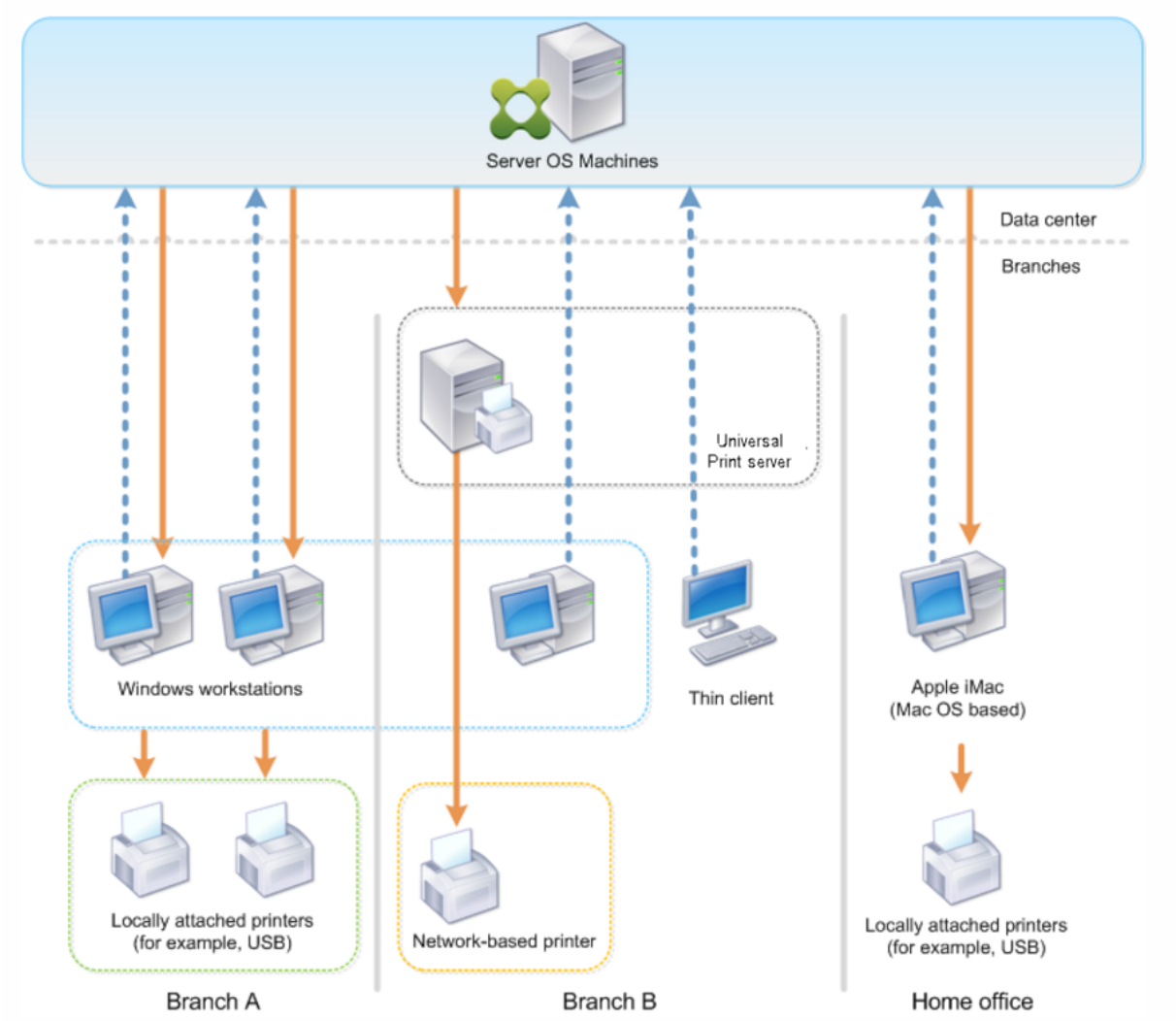
- 組織のセキュリティポリシー。人事部用のプリンターなど、特定のユーザー用に予約されたプリンターがあるかどうかを確認します。
- メインのワークステーションとは離れた場所で印刷するユーザーがいるかどうか。たとえば、複数のワークステーション間を移動しながら作業したり、出張先で印刷したりするユーザーがいるかどうかを確認します。

印刷環境を設計するにあたり、ユーザーがローカルのユーザーデバイス上で印刷するときと同様なユーザーエクスペリエンスを提供することを目標にします。

印刷展開の例

次の図は、以下の環境での印刷展開を示しています。

- 支社 **A** - 数台の Windows ワークステーションがある海外の小さなブランチオフィス。すべてのユーザーワークステーションは共有されていないプリンターにローカルで接続されています。
- 支社 **B** - シンクライアントおよび Windows ベースのワークステーションが複数台ある大規模なブランチオフィス。効率を上げるため、この支社のユーザーはネットワーク上のプリンターを（各階で 1 台）共有しています。支社内に置かれている Windows ベースのプリントサーバーが印刷キューを管理します。
- 社員の自宅 - Mac OS ベースのユーザーデバイスで自宅から会社の Citrix インフラストラクチャにアクセスしています。ユーザーデバイスはプリンターにローカルで接続されています。



以降のセクションでは、各印刷環境をシンプルにして簡単に管理するための構成について説明します。

自動作成されるクライアントプリンターと **Citrix** ユニバーサルプリンタードライバー

ブランチオフィス A のすべてのユーザーは Windows ベースのワークステーションを使用しており、自動作成されたクライアントプリンターとユニバーサルプリンタードライバーが使用されます。この構成には以下のメリットがあります。

- パフォーマンス - 印刷ジョブは ICA 印刷チャネル上で配信されます。このため、印刷データの圧縮により帯域幅を節約できます。

  サイズの大きなドキュメントを印刷しているユーザーがほかのユーザーのセッションパフォーマンスを低下させることがないように、最大印刷帯域幅を指定する Citrix ポリシーを構成します。

  代替策として、マルチストリーム ICA 接続を使用して、印刷トラフィックが優先度の低い専用の TCP 接続で転送されるように構成することもできます。マルチストリーム ICA は、WAN 接続にサービス品質（QoS）が

実装されていない場合のオプションです。

- 柔軟性 - Citrix ユニバーサルプリンタードライバーを使用しているため、新しいプリンタードライバーをデータセンターに追加することなく、クライアントに接続されているすべてのプリンターを仮想デスクトップや仮想アプリケーションのセッションでも使用できます。

Citrix ユニバーサルプリントサーバー

ブランチオフィス B のすべてのプリンターはネットワークに接続されており、その印刷キューは Windows プリントサーバー上で管理されます。このため、Citrix ユニバーサルプリントサーバーが最も効果的な構成になります。

必要なすべてのプリンタードライバーは、ローカルの管理者によりプリントサーバー上にインストールされて管理されます。ネットワーク上のプリンターは、以下のように仮想デスクトップやアプリケーションセッションにマップされます。

- Windows ベースのワークステーションの場合 - ローカルの IT チームの支援により、ユーザーの Windows ワークステーションを適切なネットワークプリンターに接続します。これにより、ユーザーはローカルにインストールされたアプリケーションから印刷できるようになります。

  仮想デスクトップやアプリケーションのセッションを開始すると、ローカルで構成されたプリンターがセッション内で自動作成されます。仮想デスクトップまたはアプリケーションは、可能であれば直接ネットワーク接続としてプリントサーバーに接続します。

  Citrix ユニバーサルプリントサーバーコンポーネントが構成されているため、ネイティブのプリンタードライバーは不要です。ドライバーをアップデートしたりプリンターキューを変更したりしても、データセンターで何らかの構成を行う必要はありません。

- シンクライアントの場合 - シンクライアントデバイスのユーザーは、仮想デスクトップやアプリケーションのセッション内でプリンターを接続する必要があります。ユーザーに最もシンプルな印刷構成を提供するには、管理者が Citrix ポリシーの［セッションプリンター］設定を階ごとに構成して、各階のプリンターがデフォルトのプリンターとして接続されるようにします。

  ユーザーが階を移動しても正しいプリンターが接続されるようにするには、シンクライアントのサブセットまたは名前に基づいてポリシーが適用されるように構成します。この構成は「近接プリンター機能」と呼ばれ、ローカルプリンタードライバーのメンテナンスを委任管理モデルに基づいて実行できます。

  プリンターキューを変更または追加する必要がある場合は、Citrix 管理者が環境内でそれぞれの［セッションプリンター］設定を変更する必要があります。

ネットワーク印刷トラフィックは ICA 仮想チャネルの外側で送信されるため、サービス品質（QoS）が実装されます。ICA/HDX トラフィックにより使用されるポート上の送受信ネットワークトラフィックは、ほかのすべてのネットワークトラフィックよりも優先されます。この構成により、大きな印刷ジョブがユーザーセッションに影響を及ぼすことがなくなります。

自動作成されるクライアントプリンターと **Citrix** ユニバーサルプリンタードライバー

ユーザーが自宅で非標準的なワークステーションを使用し、管理されていない印刷装置を使用する場合、ユニバーサルプリンタードライバーを使用してクライアントプリンターを自動作成する構成が最適です。

展開の要約

要約すると、展開例は以下のように構成されています。

- マルチセッション OS マシン上にはプリンタードライバーがインストールされていません。Citrix ユニバーサルプリンタードライバーのみを使用します。ネイティブのプリンタードライバーへのフォールバックおよびプリンタードライバーの自動インストールは無効です。
- すべてのクライアントプリンターを自動作成するためのポリシーがすべてのユーザーに適用されます。マルチセッション OS マシンはデフォルトでプリントサーバーに直接アクセスします。必要な構成タスクは、ユニバーサルプリントサーバーコンポーネントの有効化のみです。
- ブランチオフィス B の各階に個別の［セッションプリンター］設定が構成されており、その階のすべてのシンクライアントに適用されます。
- 支社 B には QoS が実装され、優れたユーザーエクスペリエンスが提供されています。

ベストプラクティス、セキュリティに関する考慮事項、およびデフォルトの操作

August 17, 2024

ベストプラクティス

環境での最適な印刷ソリューションは、さまざまな要因により決定されます。以下のベストプラクティスの中には、特定のサイトに適用されない場合があります。

- Citrix ユニバーサルプリントサーバーを使用します。
- ユニバーサルプリンタードライバーまたは Windows ネイティブドライバーを使用します。
- マルチセッション OS マシン上にインストールされるプリンタードライバー数を最小化します。
- ネイティブドライバーへのドライバーマッピングを使用します。
- 動作検証されていないプリンタードライバーを実稼働環境サイトにインストールしないようにします。
- ドライバーのアップデートインストールを避け、常にドライバーをアンインストールしてからプリントサーバーを再起動して、その後で新しいドライバーをインストールしてください。

- 未使用のドライバーをアンインストールするか、［プリンター ドライバーのマッピングと互換性］ポリシーを行使して、プリンターがそのドライバーで作成されないようにします。
- Version 2 のカーネルモードドライバーを使用しないようにします。
- 特定のプリンターがサポートされるかどうかについては、製造元に問い合わせるか、Citrix Ready 製品に関する情報（www.citrix.com/ready）を参照してください。

  一般的に、Microsoft 社より提供されるプリンタードライバーはすべて Terminal Services でテストされ、Citrix 環境での動作が確認されています。ただし、サードパーティ製のプリンタードライバーを使う前に、ターミナルサービスでの動作が Windows Hardware Quality Labs（WHQL）プログラムで認定されているかどうかをプリンタードライバーのベンダーに確認してください。Citrix ではプリンタードライバーの動作を保証しません。

セキュリティに関する注意事項

Citrix の印刷ソリューションは、これ自体がセキュアに設計されています。

- Citrix Print Manager Service は、ログオンやログオフ、切断、再接続、およびセッション終了などのセッションイベントを常に監視してそれらに応答します。実際のセッションユーザーを偽装して、サービス要求を処理します。
- Citrix の印刷ソリューションでは、セッション内の一意な名前空間に各プリンターが割り当てられます。
- Citrix の印刷ソリューションでは、自動作成プリンターにデフォルトのセキュリティ記述子が設定されます。これにより、あるセッションで自動作成されたクライアントプリンターにほかのセッションのユーザーがアクセスできないようになります。デフォルトでは、クライアントプリンターのアクセス権を変更するための管理者権限を持つユーザーでも、ほかのセッションのクライアントプリンターに誤って出力してしまうということはありません。

デフォルトの印刷動作

印刷に関するポリシーを設定しない場合、デフォルトで次のように処理されます。

- ユニバーサルプリントサーバーが無効になります。
- ユーザーデバイス上で設定されているすべてのプリンターが、各セッションの開始時にサーバー上に自動作成されます。

  この動作は、Citrix ポリシーの［クライアント プリンターを自動作成する］設定で［すべてのクライアント プリンターを自動作成する］を構成した場合と同等です。
- クライアントデバイスにローカル接続されたプリンターへのすべての印刷ジョブは、ICA チャネルを介してユーザーデバイスに送信され、プリンターに転送されます（クライアント印刷経路）。

- ネットワークプリンターへのすべての印刷ジョブは、マルチセッション OS マシンからプリントサーバーに直送されます。印刷ジョブをネットワーク上に送信できない場合は、ユーザーコンピューターを介して転送されます（リダイレクトされるクライアント印刷ジョブ）。

  この動作は、Citrix ポリシーの［プリント サーバーへの直接接続］設定で［無効］を選択した場合と同等です。

- デフォルトでは、印刷プロパティ（ユーザーの印刷設定とデバイス設定）はユーザーデバイス上に格納されます。クライアント側でこの処理がサポートされない場合、マルチセッション OS マシン上のユーザープロファイルに印刷プロパティが格納されます。

  この動作は、Citrix ポリシーの［プリンター プロパティの保存］設定で［クライアントに保存できない場合にのみユーザー プロファイルに保存する］を選択した場合と同等です。

- VDA バージョン 7.16 以降では、V3 インボックスプリンタードライバーがオペレーティングシステムに含まれていないため、Citrix ポリシー設定「受信トレイプリンタードライバーの自動インストール」は Windows 8 以降の Windows オペレーティングシステムのバージョンには影響しません。

- 7.16 より前の VDA では、セッション内でプリンターが自動作成されるときに、そのマルチセッション OS マシン上にインストールされている Windows バージョンのプリンタードライバーが使用されます。適切なドライバーがインストールされていない場合、Windows オペレーティングシステムからドライバーがインストールされます。Windows オペレーティングシステムから適切なドライバーをインストールできない場合、Citrix ユニバーサルプリンタードライバーが使用されます。

  この動作は、Citrix ポリシーの［付属のプリンタードライバーの自動インストール］設定で［有効］を選択し、［ユニバーサル印刷］設定で［要求されたドライバーを使用できない場合にのみユニバーサル印刷を使用する］を選択した場合と同等です。

  ただし、［付属のプリンタードライバーの自動インストール］を有効にすると、必要以上に多くのプリンタードライバーがインストールされる可能性があります。

> 注:
>
> 印刷に関するデフォルト設定を確認するには、新しい Citrix ポリシーを作成し、印刷に関するすべての設定項目で［デフォルト値を使用する］チェックボックスをオンにします。これにより、デフォルトの設定が適用されます。

Always-On ログ

VDA にはプリントサーバーおよび印刷サブシステムのための Always-On ログ機能があります。

ログを ZIP としてまとめてメールで送信、または自動的に Citrix Insight Services にアップロードするには、**Start-TelemetryUpload**PowerShell コマンドレットを使用します。

印刷に関するポリシーと設定

August 17, 2024

Citrix ポリシーでは、ユーザーが公開アプリケーションからプリンターにアクセスするときの以下の動作を制御できます。

- どのようにプリンターを提供するか（どのようにセッションに追加するか）
- 印刷ジョブをどのようにルーティングするか
- プリンタードライバーをどのように管理するか

Citrix ポリシーでは、ユーザーが使用するユーザーデバイスやユーザーアカウントなどの条件に応じて、異なる印刷環境を構成できます。

印刷機能の多くは、Citrix の「印刷のポリシー設定」で設定できます。印刷の設定は、Citrix ポリシーの標準的な動作に基づいて適用されます。

プリンター設定は、セッション終了時にプリンターオブジェクトまたは（ユーザーのネットワークアカウントに適切な権限がある場合は）クライアントの印刷装置に格納されます。Citrix Workspace アプリのデフォルトでは、プリンターオブジェクトに格納された設定がまずチェックされ、見つからない場合はほかの場所に格納されている設定が使用されます。

デフォルトでは、ユーザーデバイス（デバイスがこれをサポートする場合）またはマルチセッション OS マシン上のユーザープロファイルにプリンターのプロパティが格納（または保持）されます。セッションでの作業中にユーザーがプリンターのプロパティを変更すると、その内容はそのマシン上のユーザープロファイルに反映されます。ユーザーがそのマシンに再ログオンしたり再接続したりすると、ユーザープロファイルに保持されたプロパティがユーザーデバイスに継承されます。つまり、ユーザーデバイス上のプリンタープロパティの変更は、ユーザーの次回ログオン時まで反映されません。

印刷設定の場所

Windows の印刷環境では、印刷設定に対する変更をローカルコンピューターに格納したり、ドキュメントファイルに格納したりできます。この環境では、ユーザーが変更した印刷設定を以下の場所に格納できます。

- ユーザーデバイス上 - Windows ユーザーは、ユーザーデバイス側の印刷設定を自分で変更できます。これを行うには、コントロールパネルでプリンターを右クリックして、［印刷設定］を選択します。たとえば、印刷の方向として［横］を選択すると、そのプリンターのデフォルトの方向として横向きが設定されます。
- ドキュメント内 - ワードプロセッサやデスクトップパブリッシングのプログラムでは、印刷の向きなどのドキュメント設定はそのドキュメントファイル内に格納されます。たとえば、Microsoft Word ドキュメントを印刷キューに送ると、ユーザーが指定した印刷の向きやプリンター名などの印刷設定がそのドキュメントファイル内に格納されます。これらのオプションは、次回そのドキュメントを印刷するときのデフォルト設定として表示されます。

- セッションでのユーザーによる変更 - 自動作成されたプリンターでは、ユーザーがセッション内のコントロールパネルで変更したオプション、つまりマルチセッション OS マシン上で変更されたオプションだけが保持されます。
- マルチセッション **OS** マシン上 - マルチセッション OS マシン上の特定のプリンタードライバーに対するデフォルト設定は、そのマシン上に格納されます。

Windows ベースの環境で保持される設定は、ユーザーがどのようにその設定を変更したかにより異なります。つまり、スプレッドシートプログラムなどに表示される印刷設定が、ドキュメントなどほかの場所に格納されている設定と異なることがあります。この結果、特定のプリンターに適用される設定は、セッション内で変化することがあります。

ユーザーの印刷設定の階層構造

印刷に関するユーザー設定はさまざまな場所に格納されるため、特定の優先順位でそれらの設定が処理されます。また、デバイス設定はドキュメント設定とは区別され、より優先されることに注意してください。

デフォルトでは、ユーザーがセッション内で変更したすべての印刷設定、つまり保持された設定が適用され、その後でそのほかの設定がチェックされます。ユーザーが印刷を行うと、マルチセッション OS マシン上に格納されたデフォルトの設定と、保持された設定やクライアントプリンター設定が統合されます。

ユーザーの印刷設定の保存

プリンタープロパティの格納場所を変更することは推奨されません。デフォルトの格納場所（つまりユーザーデバイス上）を使用すると、ユーザーの印刷に一貫したプロパティが適用されるようになります。ユーザーデバイス上にプロパティを保存できない場合は、自動的にマルチセッション OS マシン上のユーザープロファイルが格納場所として使用されます。

以下の環境では、［プリンタープロパティの保存］設定の内容を確認してください。

- ユーザーデバイス上へのプリンタープロパティの格納をサポートしない従来のプラグインソフトウェアが使用されている。
- 固定プロファイルを使用する Windows ネットワーク環境で、ユーザーのプリンタープロパティが保持されるように設定する。

プリンターのプロビジョニング

August 17, 2024

Citrix ユニバーサルプリントサーバー

環境に最適の印刷ソリューションを決定するときは、以下の点について検討します。

- ユニバーサルプリントサーバーにより提供されるイメージとフォントのキャッシュ、高度圧縮、最適化、QoS サポートなどの機能は、Windows の印刷プロバイダーでは提供されません。
- ユニバーサルプリンタードライバーでは、Microsoft によって定義されているパブリックな非デバイス依存の設定がサポートされます。ユーザーがプリンターの製造元固有のデバイス設定を使用する必要がある場合は、ユニバーサルプリントサーバーと Windows ネイティブドライバーの両方を提供します。この構成では、ユニバーサルプリントサーバーの長所を維持したままでユーザーに特殊なプリンター機能へのアクセスが提供されます。ここで考慮すべきことは、Windows ネイティブドライバーではメンテナンスが必要になるということです。
- Citrix ユニバーサルプリントサーバーは、ネットワークプリンターでのユニバーサル印刷をサポートします。ユニバーサルプリントサーバーではユニバーサルプリンタードライバーが使用されます。このドライバーはマルチセッション OS マシン上の単一のドライバーで、シンクライアントやタブレットを含むあらゆるデバイスからのローカル印刷またはネットワーク印刷が可能になります。

ユニバーサルプリントサーバーを Windows ネイティブドライバーと一緒に使うには、ユニバーサルプリントサーバーを有効にします。デフォルトでは、Windows ネイティブドライバーが使用可能な場合はそれが使用されます。使用できない場合は、ユニバーサルプリンタードライバーが使用されます。Windows ネイティブドライバーのみ、またはユニバーサルプリンタードライバーのみを使用するなど、ユニバーサル印刷機能の動作を変更するには、ポリシーの［ユニバーサル印刷の使用］設定を使用します。

ユニバーサルプリントサーバーのインストール

ユニバーサルプリントサーバーを使用するには、製品のインストールに関するドキュメントの説明に従って、プリントサーバー上に UpsServer コンポーネントをインストールして構成します。詳しくは、「コアコンポーネントのインストール」および「コマンドラインを使ったインストール」を参照してください。

XenApp 6.5 など、UPClient コンポーネントを別個に展開する環境の場合:

1. Windows シングルセッション OS または Windows マルチセッション OS 用の Citrix Virtual Apps and Desktops Virtual Delivery Agent（VDA）スタンドアロンパッケージをダウンロードします。
2. 「コマンドラインを使ったインストール」の説明に従って、コマンドラインを使って VDA を展開します。
3. \Image-Full\Support\VcRedist_2013_RTM から前提条件をインストールします
    - Vcredist_x64 / vcredist_x86
        - 32 ビット展開に対しては x86 のみ、64 ビット展開に対しては両方を実行
4. \Image-Full\x64\Virtual Desktop Components または\Image-Full\x86\Virtual Desktop Components から、cdf の必須コンポーネントをインストールします。
    - Cdf_x64 / Cdf_x86

- 32 ビット展開に対しては x86、64 ビット展開に対しては x64

5. \Image-Full\x64\Virtual Desktop Components または\Image-Full\x86\Virtual Desktop Components で UPClient コンポーネントを見つけます。
6. 展開して UPClient コンポーネントをインストールし、コンポーネントの MSI を実行します。
7. UPClient コンポーネントのインストール後には再起動する必要があります。

ユニバーサルプリントサーバーの **CEIP** からの登録解除

ユニバーサルプリントサーバーをインストールすると、自動的に Citrix カスタマーエクスペリエンス向上プログラム（CEIP）に登録されます。インストール日時から 7 日後に最初のデータアップロードが行われます。

CEIP の登録を解除するには、**HKEY_LOCAL_MACHINE\Software\Citrix\Universal Print Server\CEIPEnabled** を編集して、**DWORD** 値を **0** に設定します。

もう一度参加するには、この DWORD 値を 1 に設定します。

注意：レジストリエディターの使用を誤ると、深刻な問題が発生する可能性があり、Windows の再インストールが必要になる場合もあります。レジストリエディターの誤用による障害に対して、Citrix では一切責任を負いません。レジストリエディターは、お客様の責任と判断の範囲でご使用ください。また、レジストリファイルのバックアップを作成してから、レジストリを編集してください。

詳しくは、「Citrix Insight Services」を参照してください。

ユニバーサルプリントサーバーの構成

以下の Citrix ポリシー設定を使用してユニバーサルプリントサーバーを構成します。詳しくは、画面に表示される各ポリシー設定のヘルプを参照してください。

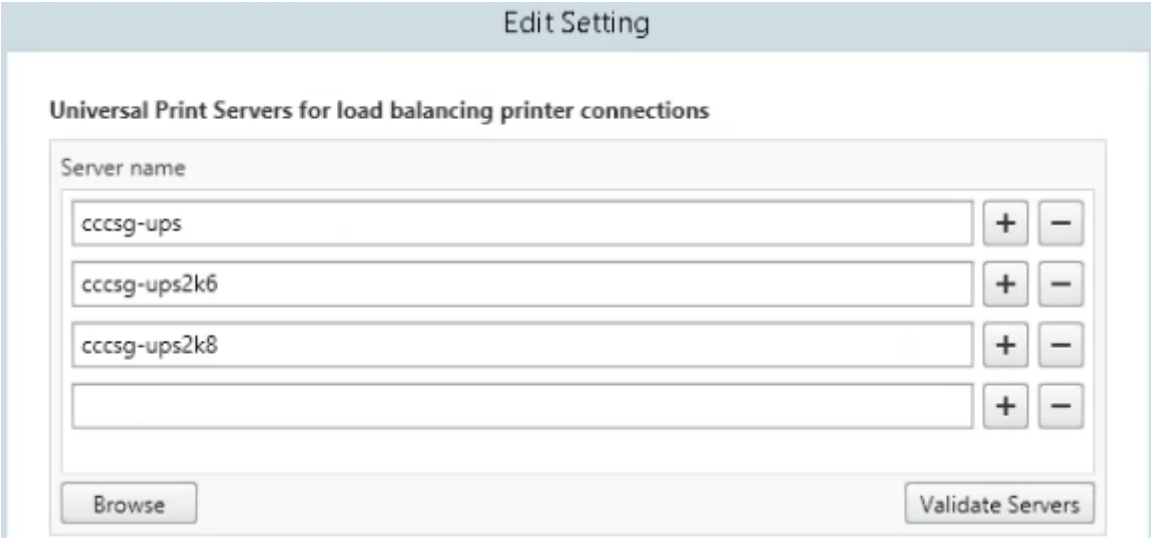
- ユニバーサルプリントサーバーの有効化。ユニバーサルプリントサーバーはデフォルトでは無効になっています。ユニバーサルプリントサーバーを有効にする場合、ユニバーサルプリントサーバーを使用できないときに Windows 印刷プロバイダーにフォールバックするかどうかを選択できます。ユニバーサルプリントサーバーを有効にすると、Windows 印刷プロバイダーと Citrix プロバイダーのインターフェイスを介してネットワークプリンターを追加して列挙できます。
- ユニバーサルプリントサーバー印刷データストリーム（**CGP**）ポート。ユニバーサルプリントサーバー印刷データストリーム CGP（Common Gateway Protocol）リスナーが使用する TCP ポート番号を指定します。デフォルトは **7229** です。
- ユニバーサルプリントサーバー **Web** サービス（**HTTP/SOAP**）ポート。ユニバーサルプリントサーバーのリスナーで使用される、HTTP/SOAP 要求の受信 TCP ポート番号を指定します。デフォルトは **8080** です。

Citrix Virtual Apps and Desktops VDA へのユニバーサルプリントサーバーの通信用ポートをデフォルトの HTTP 8080 から変更するには、次のレジストリを作成し、ユニバーサルプリントサーバーコンピューターでポート番号値を変更する必要があります：

HKEY_LOCAL_MACHINE\\SOFTWARE\\Policies\\Citrix\\PrintingPolicies
“UpsHttpPort” =DWORD:<portnumber>

このポート番号は、Studio で HDX ポリシー、ユニバーサルプリントサーバー Web サービス（HTTP/SOAP）ポートと一致する必要があります。

- ユニバーサルプリントサーバー入力データストリームの最大帯域幅（**Kbps**）。各印刷ジョブからユニバーサルプリントサーバーに CGP で配信される印刷データの転送速度の上限をキロビット/秒単位で指定します。デフォルトは 0（無制限）です。
- 負荷分散のためのユニバーサルプリントサーバー。この設定には、Citrix のほかの印刷ポリシー設定を評価した後、セッション起動時に確立されるプリンター接続の負荷分散に使用するユニバーサルプリントサーバーの一覧が表示されます。プリンターの作成時間を最適化するには、すべてのプリントサーバーに同じ共有プリンターを設定することをお勧めします。



- ユニバーサルプリントサーバーのサービス停止のしきい値。ロードバランサーが、反応しないプリントサーバーの復旧を待機する時間を指定します。タイムアウト後、ロードバランサーはそのサーバーが永続的にオフラインであると判定し、その負荷をほかの利用可能なプリントサーバーに再分散します。デフォルト値は 180 秒です。

Delivery Controller で印刷ポリシーを変更した後、そのポリシーの変更が VDA に適用されるまでに数分かかることがあります

ほかのポリシー設定との相互作用—ユニバーサルプリントサーバーは、ほかの Citrix 印刷ポリシー設定とも相互作用します。次の表では、ユニバーサルプリントサーバーコンポーネントをインストールしてポリシーで有効にした場合に、ほかのポリシー設定がどのような影響を受けるかについて説明します。

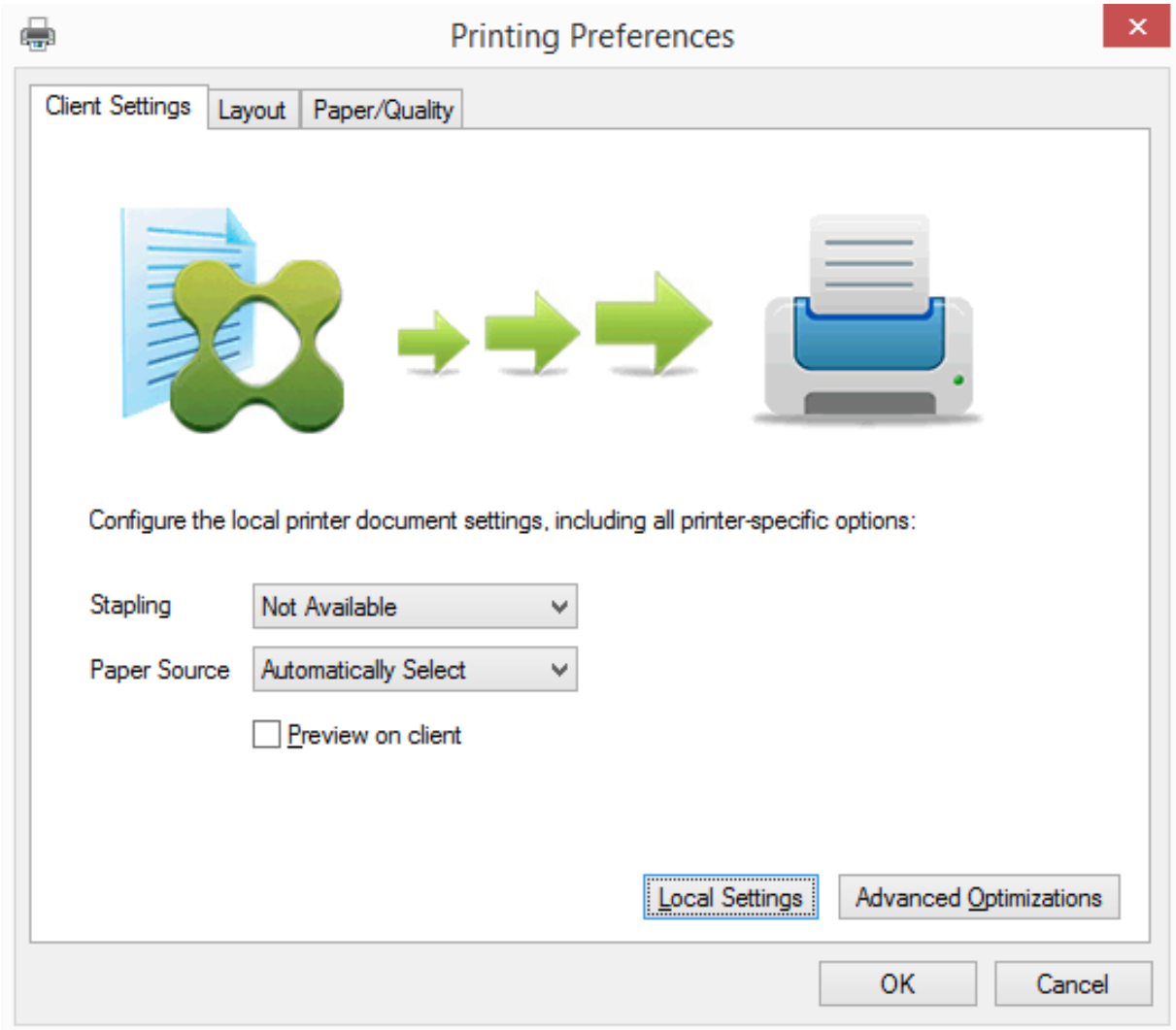
ポリシー設定	相互作用

クライアントプリンターリダイレクト、クライアントプリンターを自動作成する	ユニバーサルプリントサーバーが有効な場合、ネイティブドライバーの代わりにユニバーサルプリンタードライバーを使ってクライアントネットワークプリンターが作成されます。ユーザー側には、同じプリンター名が表示されます。
セッションプリンター	Citrix ユニバーサルプリントサーバーソリューションを使用する場合、ユニバーサルプリンタードライバー関連のポリシー設定によりセッションプリンターが構成されます。
プリントサーバーへの直接接続	ユニバーサルプリントサーバーが有効で、［ユニバーサル印刷の使用］ポリシー設定で［ユニバーサル印刷のみを使用する］が構成されている場合、ユニバーサルプリンタードライバーでプリントサーバーに直接ネットワークプリンターの接続を作成できます。
ユニバーサルドライバーの優先度	EMF および XPS ドライバーがサポートされます。

ユーザーインターフェイスに対する影響—ユニバーサルプリントサーバーにより使用される Citrix ユニバーサルプリンタードライバーにより、以下のユーザーインターフェイスコントロールが無効になります。

- ［プリンターのプロパティ］ダイアログボックスの［ローカルプリンター設定］ボタン
- ［ドキュメントのプロパティ］ダイアログボックスの［ローカルプリンター設定］ボタンおよび［クライアントでのプレビュー］ボタン

Citrix ユニバーサルプリンタードライバー（EMF および XPS ドライバー）は、ホチキス留めや給紙方法の選択など、詳細なプリンター機能をサポートします。ホチキス留めや給紙方法などのオプションは、セッションの UPD にマップされるクライアントまたはネットワークプリンターがこれらの機能をサポートしている場合に、カスタム UPD の印刷ダイアログボックスから選択できます。



ホチキス留めや安全な PIN などの非標準のプリンター設定を設定するには、Citrix UPD EMF または XPS ドライバーを使用するあらゆるクライアントマッピングされたプリンターに対して、カスタムの UPD 印刷ダイアログで［ローカル設定］を選択します。マップされたプリンターの［プリンターの設定］ダイアログがクライアント上のセッションの外部に表示されるので、ユーザーはあらゆるプリンターオプションを変更でき、アクティブなセッションでそのドキュメントを印刷する場合、変更されたプリンター設定が使用されます。

これらの機能は、ネイティブドライバーが Microsoft の印刷機能テクノロジを使用して利用可能としている場合にのみ、利用できます。ネイティブドライバーでは、印刷機能 XML で、標準化された印刷スキーマキーワードを使用する必要があります。標準化されていないキーワードを使用すると、Citrix のユニバーサルプリンタードライバーでは詳細な印刷機能を使用できなくなります。

ユニバーサルプリントサーバーを使用するときの Citrix 印刷プロバイダーのプリンターの追加ウィザードは、Windows 印刷プロバイダーのプリンターのものとほぼ同じです。ただし、以下の違いがあります。

- 名前またはアドレスを指定してプリンターを追加する場合、プリントサーバーの HTTP/SOAP ポート番号を指定できます。このポート番号は、プリンター名の一部として表示されます。

- Citrix ユニバーサルプリンタードライバーに関するポリシーでユニバーサル印刷が常に使用されるように設定すると、プリンターを選択するときにユニバーサルプリンタードライバー名が表示されます。Windows 印刷プロバイダーはユニバーサルプリンタードライバーを使用できません。

Citrix 印刷プロバイダーはクライアント側でのレンダリングをサポートしません。

ユニバーサルプリントサーバーについて詳しくは、CTX200328を参照してください。

クライアントプリンターの自動作成

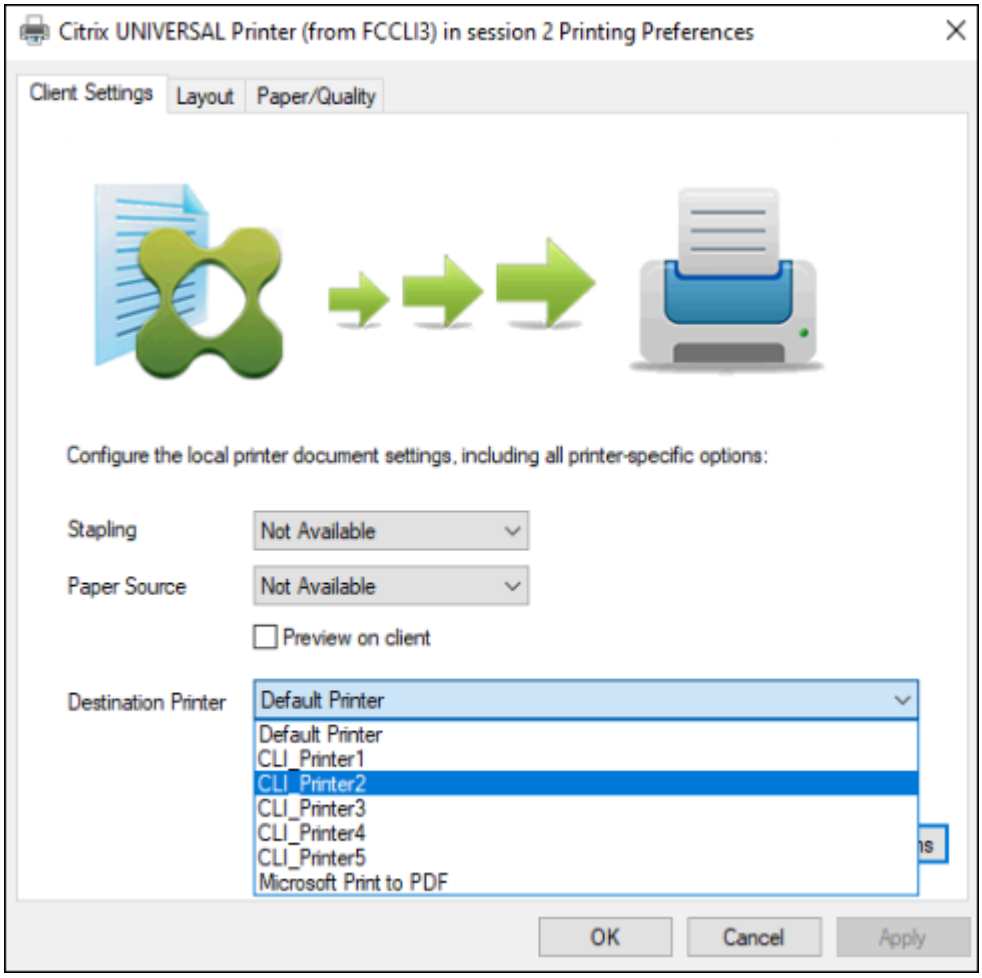
ユニバーサル印刷ソリューションにより、クライアントプリンターに以下の機能が提供されます。

- **Citrix** ユニバーサルプリンター - セッションの開始時に作成される汎用プリンターで、特定の印刷装置に関連付けられるものではありません。Citrix ユニバーサルプリンターのみを自動作成して使用すると、リソース使用量とユーザーのサインイン時間が減少することがあります。ユニバーサルプリンターでは、クライアント側のあらゆる印刷装置を使用できます。

  Citrix ユニバーサルプリンターは、ユーザーが使用するユーザーデバイスや Citrix Workspace アプリによっては正しく動作しない場合があります。Citrix ユニバーサルプリンターは Windows 環境で動作し、Citrix Offline Plug-in や、クライアント上にストリーム配信されるアプリケーションをサポートしません。このような環境では、クライアントプリンターの自動作成機能とユニバーサルプリンタードライバーの使用を検討してください。

  Windows 以外の Citrix Workspace アプリのユーザーにユニバーサル印刷ソリューションを提供するには、Postscript または PCL ベースのユニバーサル印刷ドライバーを使用してください。

  Citrix ユニバーサルプリンターを使用すると、クライアントの通常使うプリンターまたは特定のクライアントプリンターを印刷先として選択できます。印刷ジョブ用に特定のプリンターを選択するには、[プリンターの設定] ダイアログボックスを開きます。[出力先プリンター] ドロップダウンを選択します。[通常使うプリンター] オプションは、印刷ジョブをクライアントの通常使うプリンターに送信します。セッション実行中のエンドポイントに接続されているクライアントリダイレクトプリンターも表示されます。選択したプリンターは、今後の印刷ジョブの出力先プリンターとして保存されます。



- **Citrix** ユニバーサルプリンタードライバー - デバイスに依存しないプリンタードライバー。Citrix ユニバーサルプリンタードライバーを構成すると、デフォルトで EMF ベースのユニバーサルプリンタードライバーが使用されます。

  Citrix ユニバーサルプリンタードライバーによる印刷ジョブのサイズは、古いバージョンなどのプリンタードライバーのものよりも小さい場合があります。ただし、特殊なプリンターでの印刷ジョブを最適化するには、デバイス固有のドライバーが必要になる場合があります。

ユニバーサル印刷の構成—以下の Citrix ポリシー設定を使用してユニバーサル印刷を構成します。詳しくは、画面に表示される各ポリシー設定のヘルプを参照してください。

- ユニバーサル印刷の使用：ユニバーサル印刷を使用する条件を指定します。
- 汎用ユニバーサルプリンターを自動作成する：ユニバーサル印刷と互換性があるユーザーデバイスが使用されたセッションで、汎用的な Citrix ユニバーサルプリンターオブジェクトの自動作成を有効または無効にします。デフォルトでは、汎用ユニバーサルプリンターオブジェクトは自動作成されません。
- ユニバーサルドライバーの優先度：ユニバーサルプリンタードライバーの使用優先順位を指定します。一覧の上位にあるドライバーから順に使用されます。この一覧では、ドライバーを追加、編集、または削除したり、優先順位を変更したりできます。

- ユニバーサル印刷プレビューの設定：自動作成プリンターおよび汎用ユニバーサルプリンターの印刷プレビュー機能を使用するかどうかを指定します。
- ユニバーサル印刷 EMF 処理モード：Windows ユーザーデバイス上での EMF スプールファイルの処理方法を制御します。デフォルトでは、EMF スプールファイルがクライアント上のスプールキューに直接挿入されます。これにより、EMF 形式の印刷を高速に実行でき、CPU リソースの消費も少なくなります。

ポリシーについて詳しくは、「印刷パフォーマンスの最適化」を参照してください。用紙サイズ、印刷品質、色設定、両面印刷、部数などのデフォルト設定を変更する方法については、CTX114420を参照してください。

ユーザーデバイスからのプリンターの自動作成—デフォルトでは、セッションの開始時にユーザーデバイス上で設定されているすべてのプリンターが自動作成されます。管理者は、セッション内でユーザーに提供するプリンターの種類を制御して、自動作成を無効にできます。

自動作成機能を制御するには、Citrix ポリシーの［クライアントプリンターを自動作成する］設定を使用します。以下のオプションを選択できます。

- ローカル接続されているプリンターやネットワークプリンターを含め、ユーザーデバイス上で設定されているすべてのプリンターがセッション開始時に自動作成されるようにする（デフォルト）。
- ユーザーデバイスに物理的に接続されているすべてのローカルプリンターが自動作成されるようにする。
- ユーザーデバイス上で設定されているデフォルトプリンターだけが自動作成されるようにする。
- すべてのクライアントプリンターに対する自動作成を無効にする。

［クライアントプリンターを自動作成する］設定を使用する場合は、［クライアントプリンターリダイレクト］設定を［許可］（デフォルト）にする必要があります。

ユーザーへのネットワークプリンターの割り当て

デフォルトでは、クライアントデバイス上で設定されているすべてのネットワークプリンターが、セッション開始時に自動作成されます。管理者は、列挙およびマップされるプリンターの数を最小限にするために、各セッションで特定のネットワークプリンターだけが作成されるように構成することができます。このようなプリンターをセッションプリンターと呼びます。

IP アドレスによりセッションプリンターポリシーをフィルターして、近接プリンター機能を提供できます。この機能を使用すると、ユーザーの IP アドレスの範囲に応じて、特定のネットワークプリンターが自動的に割り当てられるようになります。近接プリンター機能は Citrix ユニバーサルプリントサーバーにより提供され、このセクションで説明する構成は必要ありません。

近接プリンター機能は、以下の環境で使用できます。

- 企業の社内ネットワークでユーザーの IP アドレスが DHCP サーバーにより自動的に割り当てられる。
- 組織内のすべての部署で、それぞれ異なる IP アドレス範囲が割り当てられる。
- 各部署の IP アドレス範囲内にネットワークプリンターが存在する。

近接プリンター機能を構成すると、従業員がある部署から別の部署に移動する場合でも追加の印刷装置の構成は必要ありません。移動先の部署の IP アドレス範囲でユーザーデバイスが認識されると、その範囲内のすべてのネットワークプリンターへのアクセスが可能になります。

セッションで特定のプリンターがリダイレクトされるように構成する - 管理者割り当てのプリンターを作成するには、Citrix ポリシーの［セッションプリンター］設定を構成します。この設定では、以下のいずれかの方法でネットワークプリンターを追加します。

- プリンターの UNC パスを\\<servername>\<printername> 形式で入力します。
- ネットワーク上でプリンターの場所を参照します。
- 特定サーバー上のプリンターを参照します。サーバー名を\\<servername> 形式で入力して［参照］をクリックします。

重要：特定のセッションに複数のポリシーが適用される場合、それらのポリシー（優先度の高いものから低いものまですべて）の［セッションプリンター］設定で指定されているすべてのネットワークプリンターが自動作成されます。複数のポリシーにより同じプリンターの自動作成が適用される場合、最も優先度の高いポリシーの設定だけがそのプリンターのカスタムデフォルト設定として使用されます。

［セッションプリンター］設定を使用すると、サブネットなどの条件により異なるポリシーが適用されるように構成して、ユーザーがセッションを開始した場所によって異なるネットワークプリンターが自動作成されるように制御できます。

セッションのデフォルトネットワークプリンターを指定する—デフォルトでは、ユーザーの現在のデフォルトプリンター（通常使うプリンター）がセッションのデフォルトプリンターとして使用されます。セッションのデフォルトのクライアントプリンターとして設定するプリンターを指定するには、Citrix ポリシーの［デフォルトプリンター］設定を構成します。

1. ［デフォルトプリンター］設定で、［デフォルトのクライアントプリンター］ボックスの一覧から、以下のいずれかのオプションを選択します。
    - ネットワークプリンター名。［セッションプリンター］ポリシー設定で追加されたプリンターがこのメニューに表示されます。デフォルトプリンターとして指定するネットワークプリンターを選択します。
    - デフォルトプリンターの設定を変更しない。ターミナルサービスまたは Windows のユーザープロファイルで設定されているデフォルトプリンターが使用されます。詳しくは、画面に表示される各ポリシー設定のヘルプを参照してください。
2. このポリシーの適用先として、ユーザーグループ（またはそのほかのフィルターオブジェクト）を指定します。

近接プリンター機能を構成する—Citrix ユニバーサルプリントサーバーでは、近接プリンター機能も提供されます。この場合、ここで説明されている構成は必要ありません。

1. 各サブネット（またはプリンターが設定されている場所）に応じて、異なるポリシーを作成します。
2. 各ポリシーの［セッションプリンター］設定で、そのサブネットの場所に設置されているプリンターを追加します。
3. ［デフォルトプリンター］設定で、［デフォルトプリンターの設定を変更しない］を選択します。

4. 各ポリシーの適用先として、クライアントの IP アドレスを指定します。DHCP IP アドレス範囲が変更された場合は、これらのポリシーも更新する必要があります。

印刷環境の保守

August 17, 2024

印刷環境では、以下の保守作業を行います。

- プリンタードライバーを管理する。
- 印刷パフォーマンスを最適化する。
- プリンターを表示して印刷キューを管理する。

プリンタードライバーの管理

管理上のオーバーヘッドや潜在的な問題を最小化するため、Citrix ユニバーサルプリンタードライバーの使用をお勧めします。

自動作成に失敗すると、デフォルトで、Windows で提供されている Windows ネイティブのプリンタードライバーがインストールされます。ドライバーが使用できない場合は、ユニバーサルプリンタードライバーが使用されます。プリンタードライバーのデフォルトについて詳しくは、「ベストプラクティス、セキュリティに関する考慮事項、およびデフォルトの操作」を参照してください。

Citrix ユニバーサルプリンタードライバーが適さない環境では、マルチセッション OS マシン上にインストールするドライバーの数を少なくするためにプリンタードライバーをマップします。プリンタードライバーをマップすることで、以下のことが可能になります。

- 特定のプリンターで Citrix ユニバーサルプリンタードライバーだけが使用されるようにする
- 特定のドライバーによるプリンターの作成を許可または禁止する
- 問題が生じるプリンタードライバーの代わりに正しく動作するプリンタードライバーを割り当てる
- クライアント側のプリンタードライバーの代わりに Windows サーバー上で使用可能なドライバーを割り当てる

プリンタードライバーの自動インストールを無効にする—マルチセッション OS マシン間で一貫したプリンター構成を保つため、プリンタードライバーの自動インストールを無効にします。これは Citrix のポリシー、Microsoft のポリシー、またはその両方で設定できます。Windows ネイティブドライバーが自動的にインストールされないようにするには、Citrix ポリシーの［付属のプリンタードライバーの自動インストール］設定を無効にします。

クライアントプリンタードライバーのマップ—ユーザーがセッションにログオンするときに、プリンタードライバー名など、クライアント側のプリンターの情報が提供されます。クライアントプリンターの自動作成時に、クライアントから提供されたプリンターのモデル名に基づいて、Windows サーバーのプリンタードライバーの名前が選択され

ます。次に、選択されたプリンタードライバーが自動作成プロセスで使用され、リダイレクトされるクライアント印刷キューが作成されます。

次の手順で、ドライバー置換規則を定義して、マップされたクライアントプリンタードライバーの印刷設定を編集します。

1. 自動作成クライアントプリンターのドライバー置換規則を指定するには、Citrix ポリシーの［プリンタードライバーのマッピングと互換性］設定を構成して、クライアント側のプリンタードライバーの名前を追加し、それに割り当てるサーバー側プリンタードライバーを指定します（［サーバー側プリンタードライバー］を選択して［ドライバーの検索］をクリック）。ここでは、ワイルドカード文字を使用できます。たとえば、すべての HP 社製プリンターで特定のドライバーを使用する場合は、「HP*」と入力します。
2. プリンタードライバーの使用を禁止するには、ドライバー名を選択して［作成しない］を選択します。
3. 必要に応じて、既存のマッピングを編集したり、マッピングを削除したり、一覧のドライバーエントリの順位を変更したりできます。
4. マップされたクライアントプリンタードライバーの印刷設定を編集するには、［設定］をクリックして印刷品質、印刷の向き、印刷カラーなどの設定を指定します。プリンタードライバーでサポートされないオプションを選択した場合、そのオプションは無視されます。ここで選択するオプションは、ユーザーが前回のセッションで指定し、保持されていた設定よりも優先されます。
5. 一部のプリンター機能は特定のドライバーでのみ使用可能であるため、ドライバーをマップした後でプリンターの動作を詳細にテストすることをお勧めします。

ユーザーがログオンすると、クライアントプリンタードライバーの互換性一覧がチェックされ、その後でクライアントプリンターがセットアップされます。

印刷パフォーマンスの最適化

印刷パフォーマンスを最適化するには、ユニバーサルプリントサーバーとユニバーサルプリンタードライバーを使用します。以下のポリシー設定を構成して、印刷の最適化と圧縮を制御します。

- ユニバーサル印刷最適化デフォルト：セッションで作成されるユニバーサルプリンターに適用されるデフォルト設定を指定します。
  - ［必要なイメージ品質］では、ユニバーサル印刷に適用されるイメージ圧縮レベルの上限を指定します。デフォルトでは［標準品質］が選択されており、ユーザーは標準品質または低品質（最大圧縮）を使ってイメージを印刷できます。
  - ［ヘビーウェイト圧縮を有効にする］では、ヘビーウェイト圧縮を有効または無効にします。この機能では、画質を損なわずに［必要なイメージ品質］での圧縮レベルよりも高い帯域幅削減が提供されます。デフォルトでは、ヘビーウェイト圧縮は無効になっています。
  - ［イメージおよびフォントのキャッシュ］では、印刷ストリームで使用されているイメージやフォントをキャッシュするかどうかを指定します。キャッシュを有効にすると、同一のイメージやフォントがプリンターに複数回送信されることを防ぐことができます。デフォルトでは、埋め込みイメージおよびフォントがキャッシュされます。

  - ［非管理者によるこれらの設定の変更を許可する］では、非管理者ユーザーがセッション内でこれらの最適化設定を変更することを許可または禁止します。デフォルトでは、禁止されています。

- ユニバーサル印刷イメージ圧縮制限：ユニバーサルプリンタードライバーでのイメージ印刷で使用できる品質レベルの上限を指定します。デフォルトでは、イメージ品質の上限が［最高品質（無損失圧縮）］に設定されています。
- ユニバーサル印刷品質制限：セッションでの印刷出力で使用できる最大 DPI 値（インチあたりのドット数）を指定します。デフォルトでは、DPI 値に上限はありません。

デフォルトでは、マルチセッション OS マシンからのすべての印刷ジョブがネットワークを介してプリントサーバーに直接転送されます。ネットワークで遅延が発生したり帯域幅に制限があったりする場合は、ICA 仮想チャネルでの印刷ジョブの送信を検討します。これを行うには、Citrix ポリシー設定の［プリントサーバーへの直接接続］設定で［無効］を選択します。ICA 仮想チャネルで送信されるデータは圧縮されるため、データが WAN を横断するときに消費される帯域幅が少なくなります。

印刷帯域幅を制限してセッションのパフォーマンスを改善する—マルチセッション OS マシンからユーザープリンターで印刷すると、帯域幅消費によりビデオなどほかの仮想チャネルのパフォーマンスが低下することがあります。この問題は、ユーザーが低速のネットワークを介してサーバーにアクセスする場合に顕著です。このような低下を防ぐために、ユーザープリンターでの印刷に使用される帯域幅を制限できます。転送される印刷データの量を制限すると、ビデオ、キーストローク、およびマウスデータ転送のため HDX データストリームで使用できる帯域幅が大きくなります。

> 重要：
>
> プリンター帯域幅の制限設定は、ほかのチャネルが使用されていない場合でも常に適用されます。

セッションでの印刷帯域幅制限を構成するには、Citrix ポリシーで［帯域幅］カテゴリの以下の設定項目を使用します。サイトでの制限を設定するには、Studio を使ってポリシーを構成します。個々のサーバーでの制限を設定するには、各マルチセッション OS マシン上でローカルの Windows グループポリシー管理コンソールを使ってポリシーを構成します。

- ［プリンターリダイレクトの最大帯域幅（Kbps）］設定で、印刷に使用される最大帯域幅をキロビット/秒（Kbps）で指定します。
- ［プリンターリダイレクトの最大帯域幅（%）］設定で、印刷に使用される最大帯域幅を、セッション全体に対する割合で指定します。

  注：［プリンターリダイレクトの最大帯域幅（%）］設定を使って帯域幅をパーセンテージで指定する場合は、［セッション全体の最大帯域幅］設定でセッション全体で使用可能な総帯域幅の最大値をキロビット/秒（Kbps）で指定します。

  最大帯域幅を Kbps およびセッション全体に対する割合（%）で指定した場合、より高い制限（より低い値）の設定が適用されます。

印刷帯域幅に関する情報をリアルタイムに取得するには、Citrix Director を使用します。

ユニバーサルプリントサーバーの負荷分散

ユニバーサルプリントサーバーソリューションは、負荷分散ソリューションにプリントサーバーを追加することによって拡張できます。VDA にはそれぞれ、印刷の負荷をすべてのプリントサーバーに分散する独自のロードバランサーがあるため、単一の障害点はありません。

負荷分散ソリューションでプリントサーバー全体の印刷負荷を分散するには、ポリシー設定「負荷分散のためのユニバーサルプリントサーバー」および「ユニバーサルプリントサーバーのサービス停止のしきい値」を使用します。

プリントサーバーで予期しない障害が発生した場合、各 VDA のロードバランサーのフェールオーバーメカニズムにより、既存の受信セッションがすべてユーザーエクスペリエンスに影響せず管理者の介入も必要とせずに通常どおり機能するように、障害が発生したプリントサーバーに割り当てられているプリンター接続が他の使用可能なプリントサーバーに自動的に再分散されます。

管理者は、一連のパフォーマンスカウンターを使用して VDA の以下の項目を追跡し、負荷分散されたプリントサーバーのアクティビティを監視できます。

- VDA 上の負荷分散されたプリントサーバーおよびそのステータス（使用可能、使用不可）の一覧
- 各プリントサーバーで許可されたプリンター接続の数
- 各プリントサーバー上で失敗したプリンター接続の数
- 各プリントサーバー上で有効なプリンター接続の数
- 各プリントサーバー上で保留中のプリンター接続の数

印刷キューの表示と管理

次の表は、プリンターを表示したり印刷キューを管理したりするためのツールの一覧です。

		印刷経路
クライアントプリンター（ユーザーデバイスに接続されたプリンター）	クライアント印刷経路	UAC が有効な場合、Microsoft 管理コンソール内にある［印刷の管理］スナップイン。UAC が無効な場合は、Windows 8 以前では［コントロールパネル］、Windows 8 では［印刷の管理］スナップイン。
ネットワークプリンター（ネットワークプリントサーバー上のプリンター）	ネットワーク印刷経路	UAC が有効な場合は Microsoft 管理コンソール内の［プリントサーバー］>［印刷の管理］スナップイン。UAC が無効な場合は［プリントサーバー］>［コントロールパネル］。

		印刷経路
ネットワークプリンター（ネットワークプリントサーバー上のプリンター）	クライアント印刷経路	UAC が有効な場合、Microsoft 管理コンソール内にある［プリントサーバー］>［印刷の管理］スナップイン。UAC が無効な場合は、Windows 8 以前では［コントロールパネル］、Windows 8 では［印刷の管理］スナップイン。
ローカルのネットワークサーバープリンター（マルチセッション OS マシンに追加されたネットワークプリントサーバー上のプリンター）	ネットワーク印刷経路	UAC が有効な場合は［プリントサーバー］>［コントロールパネル］、UAC が無効な場合は［プリントサーバー］>［コントロールパネル］

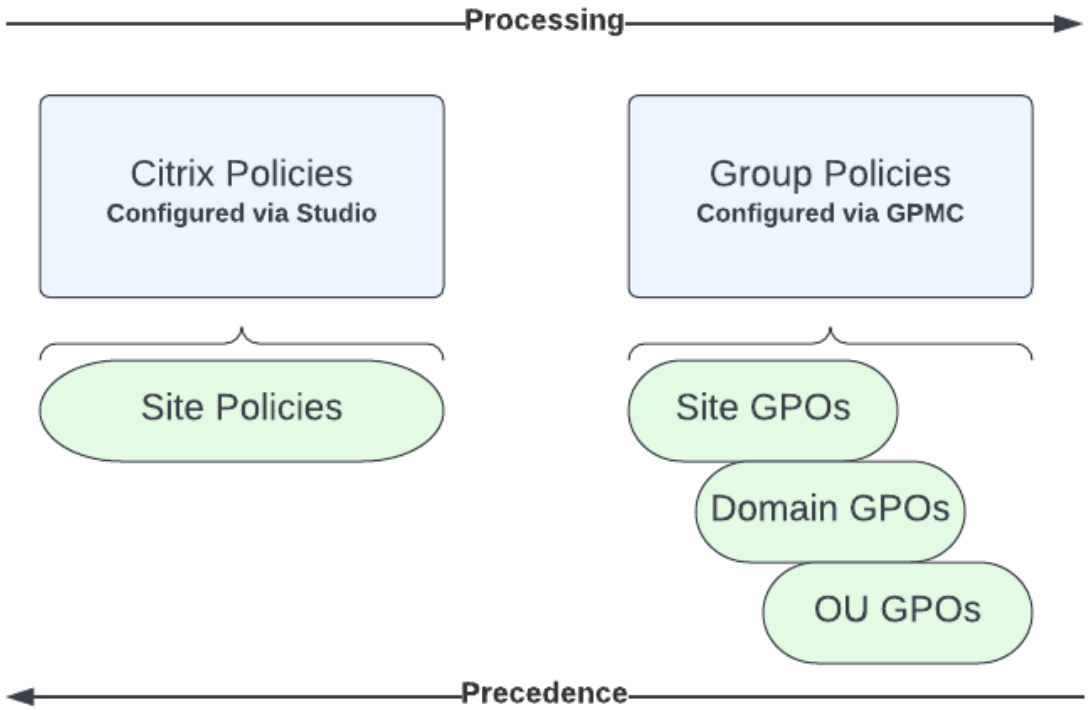
> 注:
>
> ネットワーク印刷経路で実行されたネットワークプリンターへの印刷キューは「プライベート」であり、システムで管理することはできません。

ポリシー

August 17, 2024

ポリシーは構成可能な設定項目をグループ化したもので、特定のユーザー、デバイス、または接続の種類に対して特定のセッション、帯域幅、およびセキュリティ構成が適用されるように制御する目的で使用します。

これらのポリシーは、特定の物理マシン、仮想マシン、またはユーザーに割り当てることができます。ユーザーに適用する場合、ローカルレベルのアカウントを指定したり Active Directory のセキュリティグループを指定したりできます。この構成では、特定の条件や規則を定義します。ポリシーを特定のオブジェクトに明示的に割り当てない場合、その設定はすべての接続に適用されます。



ポリシーは、ネットワークのさまざまなレベルに割り当てることができます。組織単位の GPO レベルに割り当てられたポリシーは、そのネットワークで最も優先されます。ドメイン GPO レベルのポリシーは、サイトグループポリシーオブジェクトレベルのポリシーよりも優先されます。サイトグループポリシーオブジェクトレベルは、Microsoft や Citrix のローカルポリシーレベルの競合ポリシーよりも優先されます。

すべての Citrix ローカルポリシーは、Web Studio コンソールで作成および管理され、サイトデータベースに格納されます。グループポリシーは、Microsoft グループポリシー管理コンソール（GPMC）を使用して作成および管理され、Active Directory に格納されます。Microsoft ローカルポリシーは Windows 上で作成され、レジストリ内に格納されます。

Studio のモデル作成ウィザードを使用すると、複数のテンプレートやポリシーの設定項目とその構成内容を比較してポリシーの競合や重複を避けることができます。管理者は、GPMC を使用して GPO を設定できます。また、それらの設定を、ネットワークのさまざまなレベルのユーザーのターゲットセットに適用します。

これらの GPO は Active Directory に保存されます。セキュリティ上の理由から、IT 担当者のみがこれらの設定を管理できるよう制限されています。

複数のポリシーの設定内容は、ポリシーの優先度や条件に基づいて統合されます。優先度のより高いポリシーの設定で［無効］または［禁止］が選択されている場合、優先度の低いポリシーで［有効］または［許可］が選択されていても、その設定内容は無視されます。未構成の設定項目は無視され、優先度の低いポリシーでの設定を上書きすることはありません。

ローカルポリシーと Active Directory 内のグループポリシーの設定内容が競合する場合、優先されるポリシーは状

況により異なります。

すべてのポリシーは、以下の順番で処理されます。

1. エンドユーザーがドメインの資格情報を使用してマシンにログオンする。
2. 資格情報がドメインコントローラーに送信される。
3. Active Directory によりすべてのポリシー（エンドユーザー、エンドポイント、組織単位、およびドメイン）が適用される。
4. エンドユーザーが Citrix Workspace アプリにログオンしてアプリケーションまたはデスクトップにアクセスする。
5. そのエンドユーザー、およびアプリケーションまたはデスクトップのホストマシンに適用される Citrix ポリシーと Microsoft ポリシーが処理される。
6. Active Directory により各ポリシー設定の優先度が決定され、エンドポイントデバイスのレジストリやリソースをホストしているマシンに適用される。
7. エンドユーザーがアプリケーションまたはデスクトップからログオフする。そのエンドユーザー、およびアプリケーションまたはデスクトップのホストマシンに適用される Citrix ポリシーが非アクティブになる。
8. エンドユーザーがユーザーデバイスからログオフし、GPO ユーザーポリシーが非アクティブになる。
9. エンドユーザーがユーザーデバイスをシャットダウンし、GPO マシンポリシーが非アクティブになる。

ユーザー、ユーザーデバイス、およびマシンのグループに割り当てるポリシーを作成する場合、グループの一部のメンバーで要件が異なるために一部の設定項目で例外が必要になることがあります。この例外は、Studio と GPMC におけるフィルターとして作成され、このフィルターにより、だれにどのポリシーが適用されるのかが決定されます。

> 注:
>
> 1 つの GPO に Windows ポリシーと Citrix ポリシーを混在させることはできません。

ポリシーの使用

August 17, 2024

> 注:
>
> Web Studio（Web ベース）と Citrix Studio（Windows ベース）の 2 つの管理コンソールを使用して、Citrix Virtual Apps and Desktops の展開を管理できます。この記事では Web Studio のみを扱います。Citrix Studio について詳しくは、Citrix Virtual Apps and Desktops 7 2212 以前の同様の記事を参照してください。

ユーザーのアクセスやセッション環境を制御するには、Citrix ポリシーを構成します。Citrix ポリシーを使用して、接続、セキュリティ、および帯域幅の設定を効率的に制御できます。ポリシーは、特定のグループのユーザー、デバイス、または接続の種類を対象に適用できます。1 つのポリシーに複数の設定を選択して構成できます。

Citrix ポリシーを構成するツール

Citrix ポリシーでは、以下のツールを使用できます。

- **Web Studio**。グループポリシーの管理権限が付与されていない Citrix 管理者は、Web Studio を使ってサイトのポリシーを作成します。Web Studio を使って作成されたポリシーはそのサイトのデータベースに保存され、VDA をブローカーに登録するとき、またはユーザーが VDA に接続するときにその VDA に適用されます。
- ローカルグループポリシーエディター（Microsoft 管理コンソールのスナップイン）。ネットワーク環境で Active Directory が使用されており、グループポリシーの管理権限が付与されている場合は、グループポリシーエディターを使用してサイトのポリシーを作成できます。ここでの設定内容は、グループポリシー管理コンソールで指定するグループポリシーオブジェクト（GPO）に反映されます。

> 重要:
>
> 一部のポリシー設定を構成する場合、ローカルグループポリシーエディターの使用をお勧めします。これには、コントローラーへの VDA の登録に関連する設定や、Microsoft App-V サーバーに関連する設定などが含まれます。
> さらにポリシー検証が追加されます。その結果、無効なポリシー設定が存在する場合、インプレースアップグレードを実行するとポリシーデータが失われる可能性があります。Web Studio 以外の方法を使用してポリシーを作成または編集する場合は、最新バージョンの SDK とスナップインを使用することをお勧めします。

ポリシーの処理順序と優先順位

グループポリシーの設定は、以下の順で処理されます。

1. ローカルの GPO
2. Virtual Apps and Desktops サイトの GPO（サイトのデータベースに格納される）
3. サイトレベルの GPO
4. ドメインレベルの GPO
5. 組織単位

ただし、設定内容に競合が発生すると、最後に処理されるポリシーの設定により、先に処理されるポリシーの設定が上書きされます。ポリシー設定の優先順位は次のとおりです:

1. 組織単位
2. ドメインレベルの GPO
3. サイトレベルの GPO
4. Virtual Apps and Desktops サイトの GPO（サイトのデータベースに格納される）
5. ローカルの GPO

たとえば、営業部のユーザーがクライアント側のファイルをセッション内で使用できるようにするポリシー（Policy A）を Citrix 管理者が Web Studio で作成し、同じユーザーに対してこの機能を禁止するポリシー（Policy B）を

ほかの管理者がグループポリシーエディターで作成したとします。営業担当者が仮想デスクトップにログオンすると、Policy B が適用され、Policy A は無視されます。Policy B がドメインレベルで処理され、Policy A が Virtual Apps and Desktops サイトの GPO レベルで処理されたためです。

ただし、ユーザーが ICA またはリモートデスクトッププロトコル（RDP）セッションを開始する場合は、Active Directory や Windows のリモートデスクトップセッションホストの構成ツールでの設定よりも、Citrix ポリシーでの設定の方が優先されることに注意してください。この設定には、一般的な RDP のクライアント接続設定に関連する設定などがあります。RDP クライアント接続の例として、デスクトップの壁紙、メニューのアニメーション化、ウィンドウの内容を表示したままドラッグする機能があります。

複数のポリシーを適用する場合は、競合する設定項目が正しく処理されるように優先順位を設定できます。詳しくは、「ポリシーの比較、優先度、モデル作成、およびトラブルシューティング」を参照してください。

Citrix ポリシーの設定工程

ポリシーを設定する工程は次のとおりです。

1. ポリシーを作成します。
2. ポリシー設定を構成します。
3. ポリシーをマシンやユーザーオブジェクトに割り当てます。
4. ポリシーの優先度を設定します。
5. Citrix グループポリシーモデル作成ウィザードを実行して、ポリシーの効果を確認します。

   > 注:
   >
   > ［ポリシー］>［モデル作成］タブに移動して操作バーの ［モデル作成ウィザードの起動］をクリックすると、Citrix グループポリシーモデル作成ウィザードが開きます。［モデル作成］タブは、Web Studio で（顧客の要求ごとに）使用できます。

Citrix ポリシーと設定の使用

ローカルグループポリシーエディターでは、ポリシーと設定項目が［コンピューターの構成］ノードと［ユーザーの構成］ノードに表示されます。これらのそれぞれに［Citrix Policies］ノードがあります。このスナップインの使用方法については、Microsoft 社のドキュメントを参照してください。

Web Studio では、ポリシーやテンプレートの設定項目が機能に基づいて分類されています。たとえば、［**Profile Management**］セクションには、Profile Management のポリシー設定が含まれています。

- 「コンピューター設定」（マシンに適用される設定項目）は仮想デスクトップの動作を制御し、仮想デスクトップの起動時に適用されます。これらの設定項目は、仮想デスクトップにアクティブなユーザーセッションがない場合でも適用されます。

- 「ユーザー設定」は、仮想デスクトップに ICA 接続する場合のユーザーエクスペリエンスを制御します。これらの設定項目は、ユーザーが ICA を使って接続または再接続するたびに適用されます。ユーザーポリシーは、ユーザーが RDP を使って接続したりコンソールに直接ログオンしたりする場合は適用されません。

  ポリシー、設定項目、およびテンプレートを管理するには、Web Studio の左側のペインで ［ポリシー］を選択します。

  - ［ポリシー］タブには、すべての既存のポリシーが表示されます。ポリシーを選択すると、下のタブが表示されます:
    * 概要 - 名前、優先度、有効/無効ステータス、および説明の一覧
    * 設定 - 構成されたすべての設定項目の一覧
    * 割り当て先 - ポリシーが割り当てられているユーザーおよびマシンオブジェクトの一覧。
      詳しくは、「ポリシーの作成」を参照してください。
  - ［テンプレート］タブには、組み込みおよびカスタムのテンプレートが表示されます。テンプレートを選択すると、下のタブが表示されます:
    * 説明（テンプレートを使用する理由）
    * 設定（構成された設定項目の一覧）。詳しくは、「ポリシーテンプレート」を参照してください。
  - ［比較］タブでは、複数のポリシーやポリシーテンプレートの設定項目を比較することができます。環境に適した設定項目が構成されているかどうかを確認するときに、この機能を使用できます。詳しくは、「ポリシーの比較、優先度、モデル作成、およびトラブルシューティング」を参照してください。

  ポリシーやテンプレートの設定項目を検索するには、以下の手順に従います:

  1. ポリシーまたはテンプレートを選択します。
  2. 操作バーの ［ポリシーの編集］または ［テンプレートの編集］を選択します。
  3. ［設定］ページの ［検索］フィールドで、設定項目の名前を入力します。

     以下を選択して、検索を絞り込むことができます:

     - 特定の製品バージョン
     - カテゴリ（帯域幅など）
     - 設定名のキーワード
     - ［選択項目のみを表示する］チェックボックス
     - 選択したポリシーに追加された設定項目のみを検索します。

  すべての設定項目を検索対象にするには、［すべての設定］を選択します。

- ポリシーの設定項目を検索するには、以下の手順に従います:

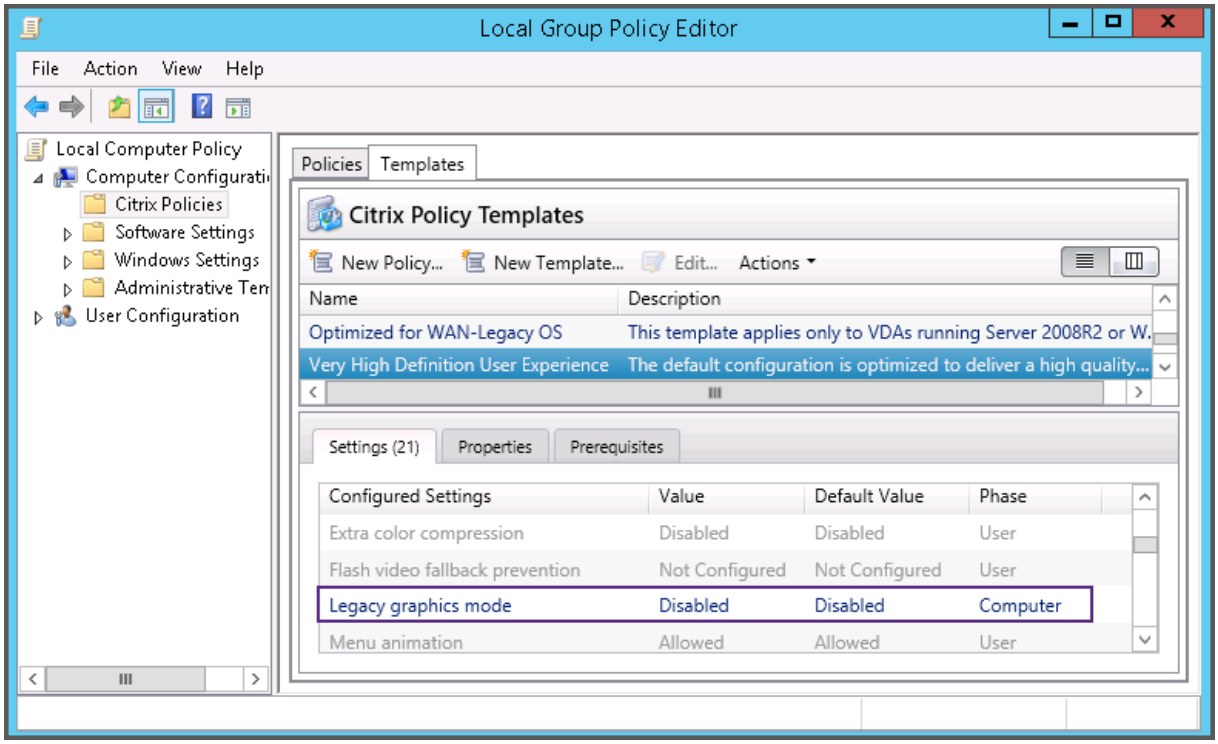
  1. ポリシーを選択します。
  2. ［設定］タブを選択し、設定項目の名前を入力します。

特定の製品バージョンや設定項目のカテゴリを選択することで、検索範囲を限定できます。すべての設定項目を検索対象にするには、［すべての設定］を選択します。

いったんポリシーを作成したら、それは使用されるテンプレートとは無関係です。新しいポリシーの ［説明］フィールドを使って、使用されるソーステンプレートを追跡できます。

グループポリシーエディターでは、コンピューターとユーザーの両方の種類の設定を含むテンプレートから作成された場合でも、コンピューターとユーザーは別々に適用される必要があります。この例では、［コンピューターの構成］で［最高品位ユーザー エクスペリエンス］を使用することを選択しています。

- 従来のグラフィックモードは、このテンプレートから作成されるポリシーで使用されるコンピューター設定です。
- 灰色表示のユーザー設定は、このテンプレートから作成されるポリシーでは使用されません。



ポリシーテンプレート

August 17, 2024

> 注:
>
> Web Studio（Web ベース）と Citrix Studio（Windows ベース）の 2 つの管理コンソールを使用して、Citrix Virtual Apps and Desktops の展開を管理できます。この記事では Web Studio のみを扱います。Citrix Studio について詳しくは、Citrix Virtual Apps and Desktops 7 2212 以前の同様の記事を参照してください。

テンプレートは、特定の結果を達成するためのポリシーを作成する場合に使用することが推奨される設定のコレクシ

ョンです。たとえば、エンドユーザーに高品位ユーザーエクスペリエンスを提供するためのポリシーを作成するには、最高品位ユーザーエクスペリエンスのテンプレートで定義された設定を、そのようなポリシーを作成するためのリファレンスおよびスタートポイントとして使用できます。

テンプレートはポリシーではありません。テンプレートは、Citrix ポリシー設定の補足ドキュメントです。これらは、特定のユーザー関連設定がまとめられた機能を示します。

テンプレートの使用はオプションです。管理者はテンプレートを使用せずにポリシーを作成できます。テンプレートは、サイトの構成方法について大まかなアイデアはあるものの、希望する構成を実現するためにどの設定を使用すればよいかわからない管理者にとって便利です。

管理者は、既存のテンプレートや既存のポリシーを使用して、または一から、テンプレートを作成できます。

ADMX/ADML

ここで説明する Citrix グループポリシーテンプレートは、Windows ポリシーテンプレートとは関係ありません。ここで説明するテンプレートと Windows ポリシーテンプレートは、2 つの異なる概念です。Citrix グループポリシーテンプレートは ADMX ファイルではありません。

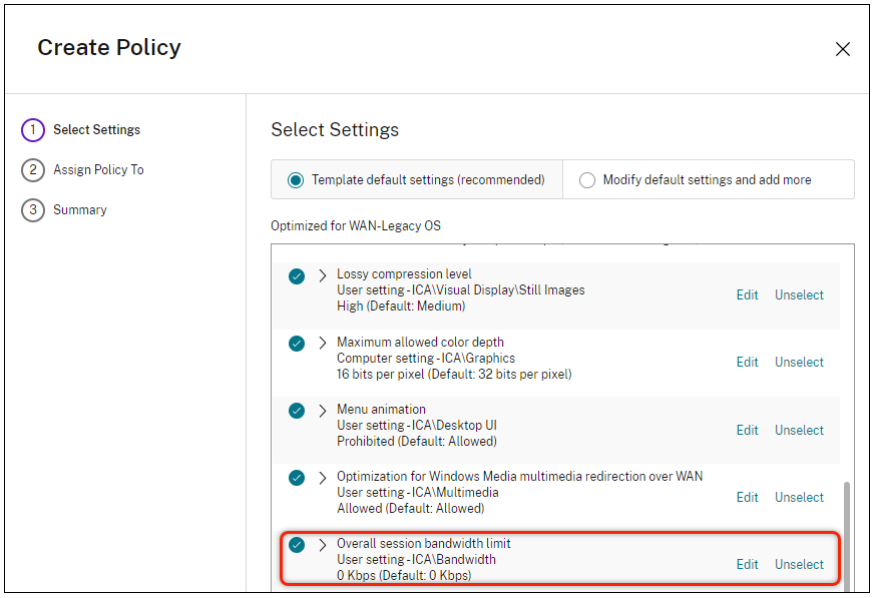
組み込みの **Citrix** テンプレート

使用できるポリシーテンプレートは以下のとおりです。

- 最高品位ユーザーエクスペリエンス。このテンプレートは、デフォルトの設定を適用してユーザーエクスペリエンスを最大化します。このテンプレートは、複数のポリシーが優先順に処理されるシナリオで使用します。
- 高サーバースケーラビリティ。サーバーリソースの浪費を避けるには、このテンプレートを適用します。このテンプレートはユーザーエクスペリエンスとサーバーのスケーラビリティの均衡をとります。単一のサーバー上でホストできるユーザー数を増大させながら、良質のユーザーエクスペリエンスを提供します。このテンプレートは、グラフィックの圧縮にビデオコーデックを使用せず、サーバー側のマルチメディアレンダリングを防ぎます。
- 高サーバースケーラビリティ **-** レガシ **OS**。この高サーバースケーラビリティテンプレートは、Windows Server 2008 R2 または Windows 7 以前が動作する VDA にのみ適用されます。このテンプレートは、これらのオペレーティングシステムでより効率的に機能する従来のグラフィックモードに依存します。
- **NetScaler SD-WAN** に最適化。これは、NetScaler SD-WAN が展開されたブランチオフィスユーザーに適用して Citrix Virtual Desktops の配信を最適化するテンプレートです。（NetScaler SD-WAN は、CloudBridge の新しい名前です）。
- **WAN** の最適化。このテンプレートは、共有 WAN 接続を使用しているブランチオフィスなどの遠隔や、低帯域幅接続を実行する遠隔地にいて、マルチメディアコンテンツがほとんどない視覚的に簡素なユーザーインターフェイスのアプリケーションにアクセスするタスクワーカーを対象としたものです。このテンプレートでは、ビデオ再生エクスペリエンスと一部のサーバースケーラビリティが帯域幅の効率性を最適化するため犠牲にされます。

- **WAN** の最適化 **-** レガシ **OS**。この *WAN* の最適化テンプレートは、Windows Server 2008 R2 または Windows 7 以前が動作する VDA にのみ適用されます。このテンプレートは、これらのオペレーティングシステムでより効率的に機能する従来のグラフィックモードに依存します。
- セキュリティと制御。許容率が低い環境でのこのテンプレートの使用にはリスクがあります。Citrix Virtual Apps and Desktops ではデフォルトで有効な機能が最小化することになります。このテンプレートには、印刷、クリップボード、周辺デバイス、ドライブマッピング、ポートのリダイレクト、およびユーザーデバイス上の Flash アクセラレーションへのアクセスを無効にする設定があります。このテンプレートを適用すると、より多くの帯域幅が消費され、サーバーごとのユーザー密度が減ります。

組み込み Citrix テンプレートはそのデフォルトの設定のままで使用することをお勧めしますが、その設定には特定の推奨値はありません。たとえば、WAN の最適化テンプレートにはセッション全体の最大帯域幅があります。この場合、テンプレートにより設定が公開され、これによって管理者はこの設定がそのシナリオに適用されようとしていることを理解します。



XenApp および XenDesktop 7.6 FP3 より前のバージョン（ポリシー管理および VDA）を使用していて、高サーバースケーラビリティおよび WAN の最適化テンプレートを必要とする場合、これらのテンプレートを適用するときはそのレガシ OS バージョンを使用してください。

> 注:
>
> Citrix が組み込みテンプレートを開発およびアップデートします。これらのテンプレートを変更したり削除したりすることはできません。

Web Studio 使ったテンプレートの作成と管理

テンプレートをベースにしたテンプレートを作成するには:

1. Web Studio にサインインし、左側のペインで ［ポリシー］をクリックします。

2. ［テンプレート］タブを選択し、作成元のテンプレートを選択します。
3. ［テンプレートの作成］タブを選択します。［設定項目の選択］画面が表示されます。
4. テンプレートのポリシー設定を選択して構成します。
5. ［次へ］をクリックします。［概要］画面が開きます。
6. テンプレートの名前を入力します。
7. ［完了］をクリックします。新しいテンプレートが ［テンプレート］タブに表示されます。

ポリシーをベースにテンプレートを作成するには:

1. Web Studio にサインインし、左側のペインで ［ポリシー］をクリックします。
2. ［ポリシー］タブを選択し、作成元のポリシーを選択します。
3. ［詳細］タブをクリックします。
4. ［テンプレートとして保存］を選択します。［設定項目の選択］画面が表示されます。
5. テンプレートに含める新しいポリシー設定を追加して構成します。
6. ［次へ］をクリックします。［概要］画面が開きます。
7. 新しいテンプレートの名前と説明を入力し、［完了］をクリックします。

テンプレートと委任管理

Web Studio のテンプレートは、Citrix Studio のテンプレートとは異なり、サイトデータベースに保存されます。Citrix Studio のテンプレートは、現在の管理者のユーザープロファイルフォルダーに `.gpt` 拡張子のファイルとして保存されます。ある管理者によって作成された Citrix Studio テンプレートは、他の管理者や別のマシン上の同じ管理者には表示されません。Web Studio テンプレートは、権限と委任管理の対象となるすべての管理者に表示されます。

ポリシーの作成

August 17, 2024

> 注:
>
> Web Studio（Web ベース）と Citrix Studio（Windows ベース）の 2 つの管理コンソールを使用して、Citrix Virtual Apps and Desktops の展開を管理できます。この記事では Web Studio のみを扱います。Citrix Studio について詳しくは、Citrix Virtual Apps and Desktops 7 2212 以前の同様の記事を参照してください。

ポリシーを作成する前に、そのポリシーが適用される可能性があるユーザーまたはデバイスのグループを決定します。ユーザーの担当業務、接続の種類、ユーザーデバイス、または作業場所に応じたポリシーを作成できます。また、Windows の Active Directory のグループポリシーと同じ基準を使用できます。

グループに適用するポリシーを作成済みの場合は、別のポリシーを作成するのではなく、そのポリシーを編集することを検討してください。ポリシーを編集した後、適切な設定を構成します。特定の設定内容を変更するため、または特定のユーザーを適用対象から除外するためだけにポリシーを作成することは避けてください。

既存のポリシーテンプレートを基にポリシーを作成し、必要に応じて設定項目をカスタマイズできます。テンプレートを使用せずに作成し、必要なすべての設定を追加することもできます。

Web Studio では、新しいポリシーを作成すると、［ポリシーの有効化］チェックボックスが明示的にオンになっていない限り［無効］に設定されます。

ポリシーの作成時および設定の構成時に、システムによって設定の種類を表示するオプションが提供されます。表示できる設定の種類は以下のとおりです:

- すべての設定 - すべての VDA バージョンに適用できるすべての設定を表示します
- 現在の設定のみ - 現在の VDA バージョン固有の設定を表示します
- 従来の設定のみ - 廃止された VDA バージョンにのみ適用できる設定を表示します

設定の構成中に設定を表示するには、以下の手順に従います:

1. Web Studio にサインインし、左側のペインで ［ポリシー］をクリックします。
2. ［ポリシー］タブで、［ポリシーの作成］をクリックします。
3. ［設定の選択］テーブルで、［設定］の横にあるドロップダウンをクリックします。
4. ドロップダウンから次のいずれかのオプションを選択します:

- すべての設定 - すべての VDA バージョンのすべての設定を表示します
- 現在の設定のみ - 現在の VDA バージョンのみの設定を表示します
- 従来の設定のみ - 廃止された VDA バージョンのみの設定を表示します

1. ［設定］テーブルには、前の手順に基づいて使用可能な設定がリストされます。

ポリシー設定

ポリシーを設定するには、適用するポリシー設定を選択して値を構成します。デフォルトでは、ポリシーに追加されている設定項目はありません。設定を適用するには、ポリシーに追加する必要があります。

ポリシーのいくつかの設定では、次のオプションを指定します。

- ［許可］または［禁止］を選択して、その設定項目により制御されるアクションを許可または禁止します。これらのアクションには、セッション内でのユーザーによる管理を許可したり禁止したりできるものがあります。たとえば、メニューをアニメーション化する設定で［許可］を選択した場合、ユーザーがクライアント環境内でメニューのアニメーション化を制御できるようになります。
- ［有効］または［無効］を選択して、その設定項目の機能を有効または無効にします。ここで無効にすると、より優先度の低いポリシーで［有効］を選択しても、その設定は有効になりません。

また、一部の設定は、それに依存する設定の効果を制御します。たとえば、[クライアントドライブのリダイレクト] 設定により、クライアントデバイス側のドライブへのアクセスが制御されます。この設定と ［クライアントネットワークドライブ］設定の両方がポリシーに追加され、ユーザーのネットワークドライブへのアクセスが許可されている必要があります。この場合、[クライアントドライブのリダイレクト］設定で［禁止］を選択すると、[クライアントネットワークドライブ］設定で［許可］を選択しても、ユーザーがネットワークドライブにアクセスできなくなります。

通常、マシンの動作を制御するポリシー設定に対する変更内容は、仮想デスクトップが再起動したときまたはユーザーがログオンしたときに適用されます。また、ユーザーの機能を制御する設定項目は、そのユーザーの次回ログオン時に適用されます。Active Directory 環境では、ポリシーが 90 分間隔で再評価されるときに、ポリシー設定が更新されます。また、ポリシー設定は、仮想デスクトップの再起動時、またはユーザーのログオン時に適用されます。

一部の設定項目では、ポリシーに追加するときに値を入力または選択します。[デフォルト値を使用する］チェックボックスをオンにすると、設定の構成を制限できます。この選択によって設定の構成が無効になり、ポリシーが適用されると、設定項目のデフォルト値しか使用できなくなります。[デフォルト値を使用する］をオンにする前に入力した値は無視されます。

セキュアなデフォルト設定が有効になっている場合、VDA のインストール中に、ポリシー設定の優先順位は次のように影響を受けます:

- カスタマイズされた設定が最優先されます
- セキュアなデフォルト設定が 2 番目に優先されます
- デフォルト設定の優先順位が最も低くなります

ポリシーのセキュアなデフォルト設定を確認するには、以下の手順を実行します:

1. Web Studio にログインします。
2. 左側のナビゲーションで ［ポリシー］をクリックします。
3. [ポリシー］タブで、[ポリシーの作成］をクリックします。
4. [設定項目の選択］テーブルで、現在の値として ［許可］が設定されている設定にマウスを移動すると、[セキュアなデフォルト値は禁止です］が表示されます。

   セキュアなデフォルト設定

ベストプラクティス:

- ポリシーの適用先として、個々のユーザーアカウントではなくグループアカウントを使用します。ポリシーの対象ユーザーを個々に追加したり削除したりするよりも、そのユーザーがグループアカウントに属しているかどうかで管理した方が効率的です。
- Windows のリモートデスクトップセッションホストの構成ツールと重複または競合する設定を使用しないでください。リモートデスクトップセッションホストの構成ツールと Citrix ポリシーで、同様の機能に対して異なる動作が設定されていると、予期せぬ問題が生じる場合があります。設定の有効/無効をできる限り統一しておくと、問題解決が容易になります。
- 使用しないポリシーは無効にしておきます。ポリシーに設定を追加しない場合でも、そのポリシーにより不要な処理が行われます。

ポリシーの割り当て

ポリシーを作成するときに、特定のユーザーとマシンオブジェクトにポリシーを割り当てます。そのポリシーは、特定の基準または規則に従って接続に適用されます。通常、1 つのポリシーに複数の割り当てを指定して、複数の条件を組み合わせることができます。

割り当てを指定しない場合、または指定しても無効にしている場合、そのポリシーはすべての接続に適用されます。

> 注:
>
> ポリシーの割り当ては、ポリシーフィルターとも呼ばれます。詳しくは、次のトピックを参照してください:
>
> - ポリシーフィルターの作成、変更、または削除
> - フィルターはどのように適用されますか?

次の表は、使用可能な割り当ての一覧です。

割り当て名	ポリシーの適用対象
アクセス制御	セッションに接続するときのアクセス制御条件。接続の種類 - 接続が NetScaler Gateway 経由かどうかを指定します。*NetScaler Gateway* ファーム名 - NetScaler Gateway 仮想サーバーの名前を指定します。アクセス条件 - 使用するエンドポイント解析ポリシーまたはセッションポリシーの名前を入力します。
NetScaler SD-WAN	ユーザーセッションで NetScaler SD-WAN が使用されているかどうか。注: ポリシーに追加できる NetScaler SD-WAN 割り当ては 1 つのみです。
クライアント IP アドレス	セッションに接続するクライアントデバイスの IP アドレス。IPv4 の場合は 12.0.0.0、12.0.0.*、12.0.0.1-12.0.0.70、12.0.0.1/24 など。IPv6 の場合は、2001:0db8:3c4d:0015:0:0:abcd:ef12、2001:0db8:3c4d:0015::/54 など。
クライアント名	ユーザーデバイスの名前。完全一致の場合、ClientABCName。ワイルドカード文字を使用する場合、Client*Name。
デリバリーグループ	所属するデリバリーグループ。

割り当て名	ポリシーの適用対象
デリバリー グループの種類	実行されるデスクトップまたはアプリケーションの種類。プライベートデスクトップ、共有デスクトップ、プライベートアプリケーション、または共有アプリケーションから選択します。注：プライベートデスクトップと共有デスクトップのフィルターオプションは、Citrix Virtual Apps and Desktops 7.x でのみ使用できます。詳しくは、CTX219153を参照してください。
組織単位（OU）	組織単位。
タグ	タグ。注：このポリシーをすべてのタグ付きマシンに適用します。アプリケーションタグは含まれていません。
ユーザーまたはグループ	ユーザー名またはグループ名。

ユーザーがログオンするときに、その接続の条件に一致するすべてのポリシーが検出されます。検出されたポリシーは優先度順に処理されます。このとき、ポリシー間で重複している設定がある場合は、最も優先度の高いポリシーの内容が適用されます。たとえば、優先度の高いポリシーの設定で［無効］が選択されている場合、優先度の低いポリシーの同じ設定で［有効］が選択されていても、その設定には［無効］が適用されます。構成されていないポリシー設定は無視されます。

> 重要：
>
> グループポリシー管理コンソールを使って Active Directory ポリシーと Citrix ポリシーの両方を構成する場合、割り当ておよび設定が意図したとおりに適用されない場合があります。詳しくは、CTX127461を参照してください。

「Unfiltered」という名前のポリシーはデフォルトで提供されています。

- Web Studio を使用して Citrix ポリシーを管理する場合は、Unfiltered ポリシーに追加する設定がそのサイトのすべてのサーバー、仮想デスクトップ、および接続に適用されます。
- ローカルグループポリシーエディターを使用して Citrix ポリシーを管理する場合は、すべてのサイトおよび接続に Unfiltered ポリシーの設定が適用されます。このサイトと接続は、ポリシーを含むグループポリシーオブジェクト（GPO）のスコープ内にある必要があります。たとえば、営業部署の組織単位に大阪支社のすべての営業メンバーを含んでいる Sales-OSK という GPO がある場合に、いくつかのユーザーポリシー設定を追加した Unfiltered ポリシーを Sales-OSK に設定します。ここで大阪支社の営業部長がサイトにログオンすると、Unfiltered ポリシーのすべての設定が自動的にセッションに適用されます。この構成は、ユーザーが Sales-OSK GPO のメンバーであるためです。

割り当ての［モード］によっても、そのポリシーの適用先が異なります。割り当てのモードとして［許可］（デフォルト）が設定されている場合、その割り当て条件にマッチした接続にのみポリシーが適用されます。割り当てのモードとして［拒否］が設定されている場合、その割り当て条件にマッチしない接続にのみポリシーが適用されます。以下

の例では、複数の割り当てを追加した Citrix ポリシーで、割り当てのモードがどのように適用されるかについて説明します。

- 例：同じ種類の割り当てでモードが異なる場合 - ポリシーに同じ種類の割り当てを 2 つ追加し、一方を［許可］にしてもう一方を［拒否］にした場合、［拒否］を設定した割り当てが優先されます。例：

  Policy 1 に以下の割り当てを追加します：

  - Assignment A は営業部署のグループアカウントに適用されます。［許可］を設定します。
  - Assignment B は営業部長のアカウントに適用されます。［拒否］を設定します。

  ここで営業部長がログオンした場合、営業部長が営業部署のグループアカウントに属していても、Assignment B が［拒否］モードなのでこの Policy 1 は適用されません。

- 例：異なる種類の割り当てでモードが同じ場合 - ポリシーに異なる種類の複数の割り当てを追加し、すべての割り当てに［許可］を設定した場合、すべての種類の割り当てに一致しないとポリシーは適用されません。例：

  Policy 2 に以下の割り当てを追加します：

  - Assignment C は営業部署のグループアカウントに適用される［ユーザーまたはグループ］割り当てです。［許可］を設定します。
  - Assignment D は 10.8.169.*（企業ネットワーク）を指定するクライアント IP アドレス割り当てです。［許可］を設定します。

  ここで営業部長が社内のオフィスからログオンした場合、上記 2 つの割り当てに合致するので、この Policy 2 が適用されます。

  Policy 3 に以下の割り当てを追加します：

  - Assignment E は営業部署のグループアカウントに適用される［ユーザーまたはグループ］割り当てです。［許可］を設定します。
  - Assignment F は特定の NetScaler Gateway 接続に適用される［アクセス制御］割り当てです。［許可］を設定します。

  ここで営業部長が社内のオフィスからログオンした場合、Assignment F に合致しないので、この Policy 3 は適用されません。

Web Studio でテンプレートからポリシーを作成する

1. Web Studio にサインインし、左側のペインで ［ポリシー］をクリックします。
2. ［テンプレート］タブを選択し、テンプレートを選択します。
3. 操作バーの ［テンプレートからのポリシーの作成］を選択します。
4. デフォルトでは、新しいポリシーはテンプレートのすべてのデフォルト設定を使用します。この場合、［テンプレートのデフォルトの設定項目（推奨）］がオンになっています。設定項目を変更する場合は、［デフォルトの設定項目を変更および追加する］をクリックして、必要に応じて設定項目を追加または削除します。

5. ポリシーの割り当て先として、以下のいずれかを選択します。

    - 選択したユーザーおよびマシンオブジェクト。選択したユーザーおよびマシンオブジェクトにポリシーを適用するには、［割り当て］をクリックしてポリシーを適用する必要があるユーザーおよびマシンオブジェクトを選択します。
    - サイト内のすべてのオブジェクト。サイト内のすべてのユーザーやマシンオブジェクトにこのポリシーが適用されます。

6. ポリシーの名前を入力します。経理部やリモートユーザーなど、ポリシーの適用対象に基づいて名前を付けると便利です。また、必要に応じて説明を入力します。

    ポリシーはデフォルトで無効になりますが、有効にすることもできます。ポリシーを作成して有効にすると、新たにログオンするユーザーに直ちに適用されます。既存のセッションには適用されません。無効にしたポリシーは適用されません。作成済みのポリシーに優先度を設定したり、設定項目を追加したりする必要がある場合は、そのポリシーを一時的に無効にすることを検討してください。

Web Studio でポリシーを作成する

1. Web Studio にサインインし、左側のペインで ［ポリシー］をクリックします。
2. ［ポリシー］タブをクリックします。
3. 操作バーの ［ポリシーの作成］を選択します。
4. 必要な設定項目を追加して構成します。
5. ポリシーの割り当て先として、以下のいずれかを選択します。

    - ［選択したユーザーおよびマシンオブジェクト］をクリックして、ポリシーを適用する必要があるユーザーおよびマシンオブジェクトを選択します。
    - ［サイト内のすべてのオブジェクトに割り当てる］をクリックします。これにより、サイト内のすべてのユーザーやマシンオブジェクトにこのポリシーが適用されます。

6. ポリシーの名前を入力します。またはデフォルトを使用します。経理部やリモートユーザーなど、ポリシーの適用対象に基づいて名前を付けると便利です。また、必要に応じて説明を入力します。

    新しいポリシーはデフォルトで有効になりますが、無効にすることもできます。ポリシーを作成して有効にすると、新たにログオンするユーザーに直ちに適用されます。既存のセッションには適用されません。無効にしたポリシーは適用されません。作成済みのポリシーに優先度を設定したり、設定項目を追加したりする必要がある場合は、そのポリシーを一時的に無効にすることを検討してください。

グループポリシーエディターでポリシーを作成および管理する

グループポリシーエディターで、［コンピューターの構成］または［ユーザーの構成］を展開します。［ポリシー］ノードを開き、［**Citrix** ポリシー］を選択します。適切な操作を行います：

タスク	手順
ポリシーを作成する	［ポリシー］タブの ［新規］をクリックします。
既存のポリシーを編集する	［ポリシー］タブでポリシーを選択して ［編集］をクリックします。
既存のポリシーの優先度を変更する	［ポリシー］タブでポリシーを選択して ［上げる］または ［下げる］をクリックします。
ポリシーの要約情報を表示する	［ポリシー］タブでポリシーを選択して ［情報］タブをクリックします。
ポリシーの設定項目を表示して変更する	［ポリシー］タブでポリシーを選択して ［設定］タブをクリックします。
ポリシーの割り当て先を表示して変更する	［ポリシー］タブでポリシーを選択して ［フィルター］タブをクリックします。ポリシーに複数のフィルターを追加する場合、適用するポリシーですべてのフィルター条件が満たされている必要があります。
ポリシーを有効または無効にする	［ポリシー］タブでポリシーを選択して ［操作］**>**［有効］または ［操作］**>**［無効］の順に選択します。
既存のテンプレートからポリシーを作成する	［テンプレート］タブでテンプレートを選択して ［新規ポリシー］をクリックします。

ポリシーセット

August 17, 2024

ポリシーセットとは、Citrix Virtual Apps and Desktops のオブジェクトであり、シンプルな役割ベースのアクセスと容易な管理を可能にするポリシーを集約したものです。ポリシーセットを作成して、管理者チームと会社の論理的な部門をミラーリングできます。たとえば、地理的地域、事業単位、または特定のユースケースごとにポリシー セットを作成できます。ポリシーセットが作成されると、スコープとデリバリーグループが割り当てられるため、権限のある管理者のみが関連するユーザーとマシンに適用されるポリシーを管理できます。

> 注:
>
> ポリシーセットを有効にする前に、Citrix では次の点に注意することをお勧めします:
>
> - さらにポリシー検証が追加されます。その結果、無効なポリシー設定が存在する場合、インプレースアップグレードを実行するとポリシーデータが失われる可能性があります。

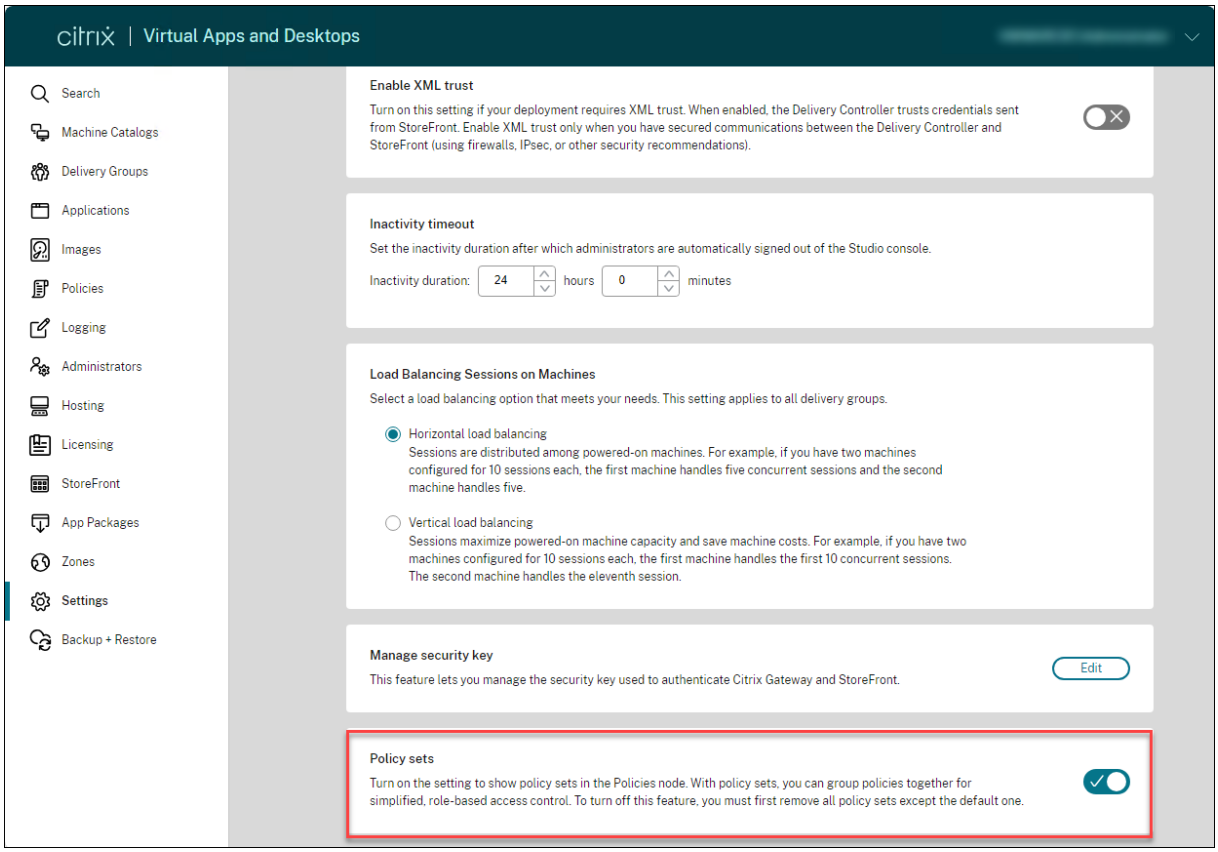
- 無効なデータを検出するには、GPO スキャナーツールを使用して、アップグレードする前に必要な編集を行ってください。詳しくは、CTX676686を参照してください。
- 今後のすべてのアップグレードでは、Citrix は最新の SDK を使用することをお勧めします。ポリシーの更新に古い SDK を使用すると、ポリシー設定に無効なデータが追加され、ポリシーデータが失われる危険性があります。

メリット

- 分散された管理者チームに対応した役割ベースのアクセス制御
- 合併、買収、統合の簡素化
- 障害ドメインの限定
- ポリシーのマルチテナントのサポート

ポリシーセットの有効化

Virtual Apps and Desktops の ［管理］タブから ［設定］に移動し、［ポリシーセット］設定をオンにします。



注:

ポリシーセットを作成する前に、ポリシーセットを有効にする必要があります。

機能比較

ポリシーセットの適用前	ポリシーセットの適用後
サイト全体のポリシー、設定、フィルター、およびポリシーの優先順位は、Citrix Studio 内の 1 か所で構成されます。	ポリシー、設定、フィルター、およびポリシーの優先順位は、ポリシーセットごとに個別に構成されます。
1 つのポリシーを管理する場合は、すべてのポリシーを管理する必要があります。	すべての管理権限を実行できる管理者は、特定のポリシーセットを個別に管理する権限を下位レベルの管理者に委任できます。
大規模な分散環境のポリシーは複雑になり、管理が困難になります。	大規模な分散環境のポリシーは分割して簡単に管理できます。

ポリシーセットはどのように機能しますか?

一般的な概要

- ポリシーセットはデリバリーグループに割り当てられます
- ポリシーセットには 1 つまたは複数のスコープがあります
- ポリシーセットが割り当てられていないデリバリーグループは、デフォルトのポリシーセットを受け取ります
- 1 つのデリバリーグループにはポリシーセットを 1 つだけ割り当てることができます
- 複数のデリバリーグループが同じポリシーセットを使用できます
- ポリシーセットがデリバリー グループに割り当てられている場合でも、ポリシーはそれぞれのフィルターを維持します

詳しくは、「フィルターはどのように適用されますか?」を参照してください。ポリシーセットに関するポリシー割り当てまたはポリシーフィルターの動作に変更はありません。つまり、ポリシーの場合と同じように機能します。

デフォルトポリシーセット

- ポリシーセット設定がオンになっている場合、既存のポリシーはすべてデフォルトのポリシーセット内でグループ化されます。
- 管理者チームがポリシーセットを作成してデリバリーグループに割り当てない限り、すべてのデリバリーグループはデフォルトのポリシーセットを受け取ります。
- デリバリーグループに別のポリシーセットが割り当てられると、デフォルトのポリシーセットからポリシーを取得できなくなります。

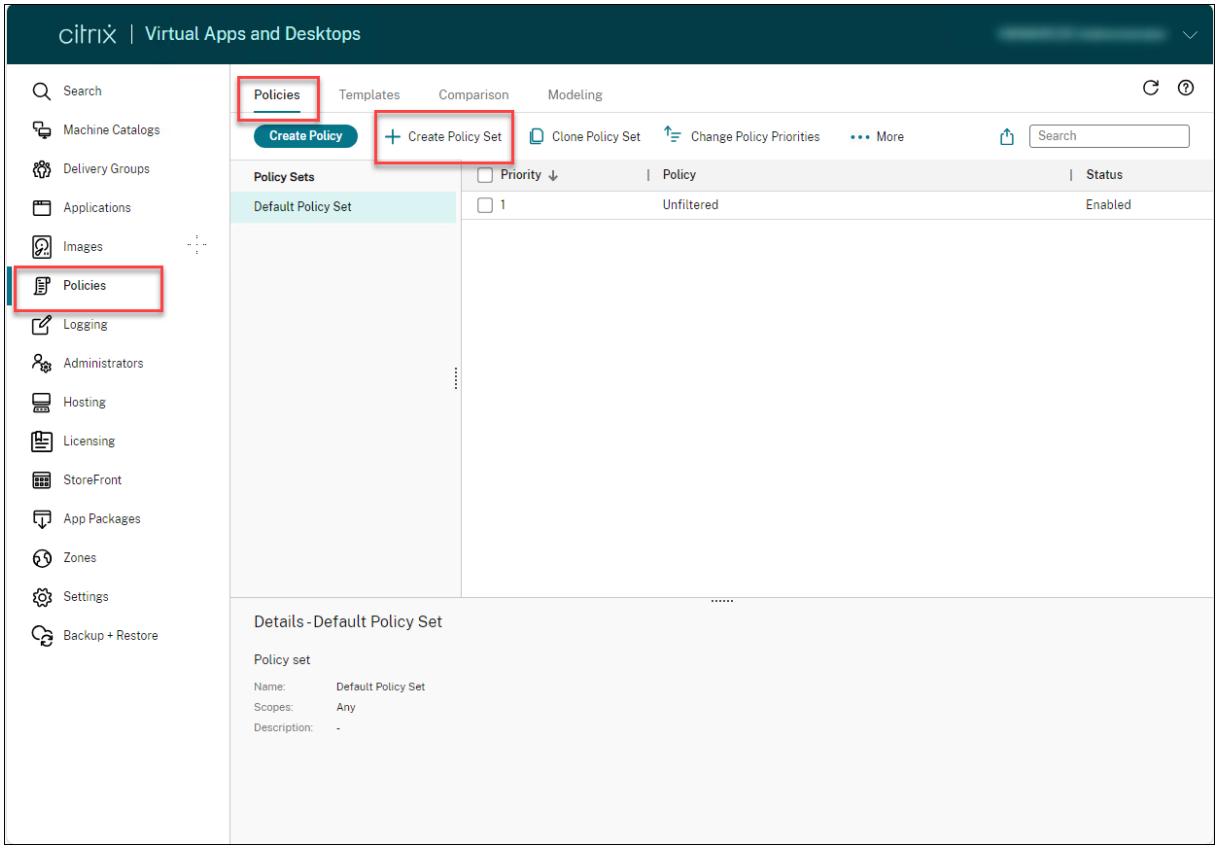
ポリシーセットの作成

ポリシーセットは、次の 2 つの方法で作成できます:

- ポリシーセットの作成 - この操作により、空のポリシーセットが作成されます。
- ポリシーセットの複製 - この操作により、既存のポリシーセットに基づいてポリシーセットが作成されます。

ポリシーセットの作成

1. Web Studio にサインインし、左側のペインで ［ポリシー］をクリックします。



1. ［ポリシーセットの作成］を選択します。［はじめに］タブが表示されます。
2. ［次へ］をクリックするか、［名前と説明］タブをクリックします。
3. ポリシーセットの名前と説明を入力します。
4. ［次へ］をクリックするか、［割り当て］タブをクリックします。
5. ポリシーセットを割り当てるデリバリーグループを 1 つまたは複数選択します。
6. ［次へ］をクリックするか、［スコープ］タブをクリックします。
7. ポリシーセットのスコープを選択します。
8. ［作成］をクリックします。ポリシーセットは、定義された割り当てとスコープを使用して作成されます。

ポリシーセットの複製

1. Web Studio にサインインし、左側のペインで ［ポリシー］をクリックします。
2. ［ポリシーセットの複製］を選択します。
3. ポリシーセットの名前を変更します。

4. ポリシーセットの割り当てを変更または作成し、［次へ］をクリックします。
5. 複製されたポリシーセットに含めるポリシーを選択または選択解除します。
6. ポリシーのスコープを変更します。
7. ［作成］をクリックします。ポリシーセットが作成されます。

ポリシーセットの編集

1. Web Studio にサインインし、左側のペインで ［ポリシー］をクリックします。
2. ［ポリシーセットの編集］を選択します。
3. ポリシーセットの名前を変更し、［次へ］をクリックします。
4. ポリシーセットの割り当てを変更または作成し、［次へ］をクリックします。
5. ポリシーのスコープを変更します。
6. ［作成］をクリックします。

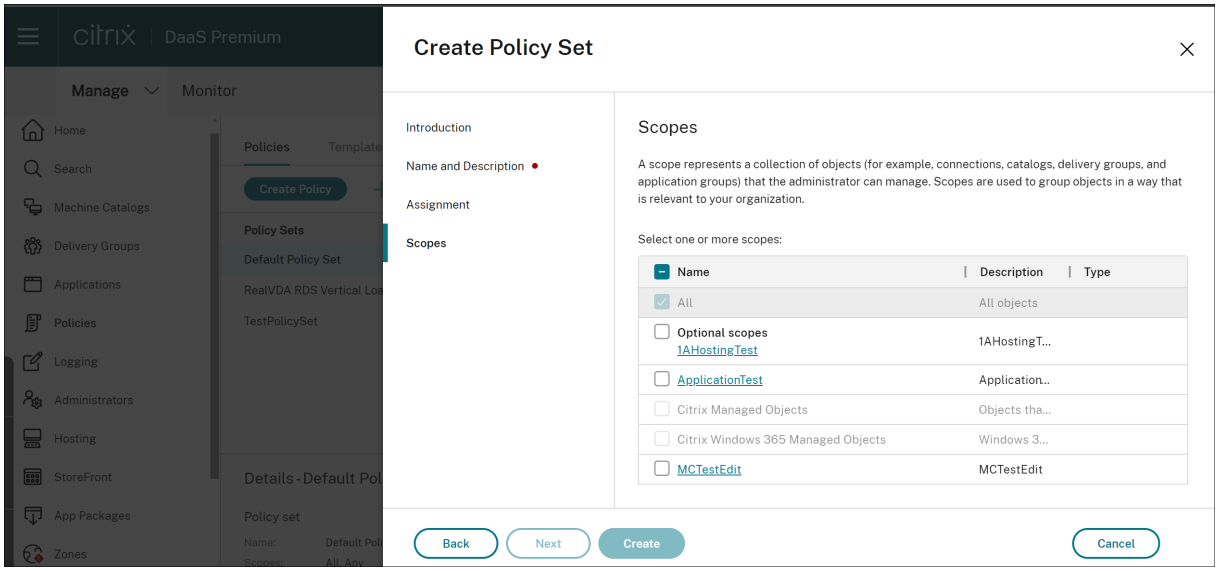
ポリシーセットの割り当て

ポリシーセットはデリバリーグループに割り当てられます。ポリシーセットの作成または編集時に割り当てを構成できます。また、デリバリーグループの作成または編集時に割り当てを構成することもできます。

ポリシーセットのスコープ

管理者は、権限のある管理者のみが表示または編集できるようにポリシーセットのスコープを定義できます。ポリシーセットの作成または編集時にスコープを構成できます。

ポリシーセットの導入により、API を使用して Citrix ポリシーを作成および管理することもできます。詳しくは、「How to create a policy set in Citrix DaaS」を参照してください。



ポリシーの比較、優先度、およびトラブルシューティング

August 17, 2024

> 注:
>
> Web Studio（Web ベース）と Citrix Studio（Windows ベース）の 2 つの管理コンソールを使用して、Citrix Virtual Apps and Desktops の展開を管理できます。この記事では Web Studio のみを扱います。Citrix Studio について詳しくは、Citrix Virtual Apps and Desktops 7 2212 以前の同様の記事を参照してください。

ユーザーの担当業務、作業場所、または接続の種類などのユーザーのニーズに応じて、複数のポリシーを作成できます。たとえば、セキュリティ強化を目的として、機密データを日常的に取り扱うユーザーグループのアクセスに、一定の制限を適用したい場合があります。

また、この場合、ユーザーがローカルのクライアントドライブ上に機密データファイルを保存することを禁止するポリシーを作成できます。また、そのユーザーグループの中にローカルドライブへのアクセスが必要なユーザーがいる場合は、そのユーザー専用のポリシーを作成してほかのポリシーよりも高い優先度を設定します。同じユーザーに複数のポリシーが適用される場合は、それらのポリシーに優先度を設定して、適用される設定内容を制御できます。複数のポリシーを使用する場合は、次のことを決定する必要があります:

- ポリシーに優先順位を付ける方法
- 例外を作成する方法
- ポリシーが競合する場合に効果的なポリシーを表示する方法。

通常、Citrix ポリシーの設定は、サイト全体、または Delivery Controller やユーザーデバイス側で構成されている同様の設定よりも優先されます。ただし、ご使用の環境で最高レベルの暗号化設定が、他の設定やポリシーよりも常に優先されます。最高レベルの暗号化設定には、オペレーティングシステムや最も制限の厳しいシャドウ機能の設定などがあります。

Citrix ポリシーは、オペレーティングシステム側で設定されているほかのポリシーとも関連して機能します。Citrix 環境では、Active Directory や Windows のリモートデスクトップセッションホストの構成ツールでの設定よりも、Citrix ポリシーでの設定の方が優先されます。この設定には、一般的なリモートデスクトッププロトコル（RDP）のクライアント接続設定に関連する設定などがあります。一般的な RDP 設定には、デスクトップの壁紙、メニューのアニメーション化、ウィンドウの内容を表示したままドラッグする機能などの設定があります。

また、［Secure ICA の最低暗号化レベル］など、オペレーティングシステム側の設定と合致していなければならないものもあります。Citrix ポリシー以外の機能でより高い暗号化レベルが設定されている場合、［**Secure ICA** の最低暗号化レベル］設定やアプリケーションやデスクトップごとに指定されている配信設定は無視されます。

たとえば、デリバリーグループを作成するときに指定する暗号化レベルは、その環境全体に対して設定されているレベルと同じである必要があります。

> 注:
>
> ダブルホップシナリオの 2 つ目のホップでは、シングルセッション OS VDA をマルチセッション OS VDA に接続することを検討してください。この場合、Citrix ポリシーは、ユーザーデバイスであるかのように、シングルセッション OS VDA に作用します。たとえば、ポリシーがユーザーデバイスにイメージをキャッシュするように設定されているとします。この例では、ダブルホップ環境における 2 つ目のホップに対してキャッシュされたイメージは、シングルセッション OS VDA マシンでキャッシュされます。

ポリシーのモデル作成ウィザードの使用

ポリシーのモデル作成は、計画およびテストのために、フィルターを使用してポリシーを有効にするシミュレーションを行うのに役立ちます。フィルターを使用して有効にしたポリシーのみがモデル化されます。無効にしたポリシーは適用されず、フィルターなしで有効にしたポリシーは常に適用されます。

ポリシーのモデル作成ウィザードを開くには、次の手順を実行します:

1. 左側のナビゲーションから ［ポリシー］を選択します。
2. ［モデル作成］タブを選択します。
3. 操作バーの ［ポリシーのモデル作成］を選択します。
4. ［はじめに］ページで ［次へ］をクリックします。
5. ユーザーまたはコンピューターを選択します。コンテナまたは特定のユーザーまたはコンピューターを参照できます。［次へ］をクリックします。
6. フィルター値を選択します。オプションで、デリバリーグループ、タグ、クライアント **IP** アドレスなどの追加の詳細を入力することで、シミュレーションをより詳細にすることができます。［次へ］をクリックします。
7. 選択した内容の概要を確認し、［実行］をクリックします。

［実行］をクリックすると、モデル作成の結果のレポートが生成されます。このレポートを表示している間、次のことができます:

- ドロップダウン メニューで ［すべての設定］、［コンピューター設定］、または ［ユーザー設定］を表示するかどうかを選択します。
- 検索バーを使用して、特定の設定を探します。
- 特定の設定をクリックして、その設定の詳細を表示します。たとえば、すべてのユーザー設定が特定のポリシーに適用されなかった場合、［詳細］ペインに設定が適用されなかった理由が表示されます。
- ［エクスポート］をクリックして、モデル作成結果を JSON 形式、HTML 形式、またはその両方でエクスポートします。

ポリシーのモデル作成を実行すると、より多くのオプションを利用できるようになります。次の操作を実行できます:

- モデル作成レポートの表示: このオプションにより、上と同じモデル作成レポートが開き、再度表示したり、エクスポートしたりできます。

- ポリシーのモデル作成の再実行：これにより、以前に選択した同じ一連の基準を使用してポリシーのモデル作成を再実行し、新しいモデル作成の結果を生成できます。これは、一部のポリシーが変更され、それらの変更が現在のモデルにどのように影響するかを確認したい場合に役立ちます。
- モデル作成レポートの削除：これにより、現在のモデル作成レポートが削除されます。

ポリシーおよびテンプレートの比較

Studio では、1 つのポリシーまたはテンプレートの設定を、複数のポリシーまたはテンプレートの設定と比較することができます。たとえば、ベストプラクティスのコンプライアンス状態を維持できる値に設定されているかどうかを確認する必要が生じることがあります。また、そのポリシーまたはテンプレートの各設定項目の設定値を、デフォルトの値と比較する必要が生じることもあります。

1. Web Studio にサインインし、左側のペインで ［ポリシー］をクリックします。
2. ［比較］タブをクリックし、［選択］をクリックします。
3. 比較するポリシーまたはテンプレートのチェックボックスをオンにします。［設定項目のデフォルト値と比較する］チェックボックスをオンにすると、各設定項目のデフォルト値が比較結果に追加されます。
4. ［比較］をクリックすると、構成された設定項目とその設定値が一覧表示されます。
5. すべての設定項目を表示するには、［すべての設定項目を表示］を選択します。元の表示に戻るには、［共通の設定項目を表示］を選択します。

ポリシーの優先度

複数のポリシーで設定内容が競合することを防ぐために、ポリシーに優先度を設定できます。ユーザーがログオンするときに、その接続の条件に一致するすべてのポリシーが検出されます。検出されたポリシーは優先度順に処理されます。このとき、ポリシー間で重複している設定がある場合は、最も優先度の高いポリシーの内容が適用されます。

ポリシーの優先度は数値で示されます。デフォルトでは、新しいポリシーに最低の優先度が設定されます。複数のポリシーで設定内容に矛盾が生じた場合は、優先度の高いポリシー（最高の優先度は「1」です）の設定が適用されます。複数のポリシーの設定内容は、ポリシーの優先度や設定の条件に基づいて統合されます。たとえば、設定が無効か有効かなどです。優先度のより高いポリシーの設定で［無効］が選択されている場合、優先度の低いポリシーで［有効］が選択されていても、その設定内容は無視されます。ただし、［設定しない］が選択されたポリシー設定は無視されるため、優先度の高いポリシーで［設定しない］が設定されている場合、その設定内容は無視され、優先度の低いポリシーの内容が適用されます。

1. 左ペインで ［ポリシー］を選択します。［ポリシー］タブを選択していることを確認します。
2. ［ポリシー］タブで、操作バーの ［ポリシーの優先度の変更］を選択します。［ポリシーの優先度の変更］ページが開きます。
3. 優先度一覧で、次のいずれかの方法を使用してポリシーの優先度を変更します：
    - ポリシーを目的の位置にドラッグします。

- 位置を 1 つずつ上または下に移動するには、それぞれ上方向アイコンまたは下方向アイコンをクリックします。
- 一覧の最上部または最下部に移動するには、それぞれ上部矢印アイコンまたは下部矢印アイコンをクリックします。
- 優先度の番号を変更するには、［編集］アイコンをクリックし、必要に応じた番号を入力し、［保存］をクリックします。

4. ［保存］をクリックします。

例外

ユーザー、ユーザーデバイス、またはマシンに対して作成したポリシーの中に、そのグループの特定のユーザーに適用したくない設定内容が含まれている場合は、以下の方法で例外を設定します。

- 例外処理が必要なグループメンバー用に新しいポリシーを作成して、ほかのポリシーより高い優先度を設定します。
- ポリシーに追加する割り当てのモードとして［拒否］を選択します

割り当てのモードとして［拒否］を選択すると、その条件にマッチしない接続にのみポリシーが適用されます。たとえば、ポリシーには次の割り当てが含まれます：

- Assignment A は、［クライアントの IP アドレス］割り当てで「208.77.88.*」を指定します。［許可］を設定します。
- Assignment B は、ユーザー割り当てで特定のユーザーアカウントを指定します。［拒否］を設定します。

この 2 つのフィルターが設定されたポリシーは、Assignment A で指定した範囲の IP アドレスを持つサイトにログオンするすべてのユーザーに適用されます。ただし、Assignment B で指定したユーザーアカウントを使用してこのサイトにログオンするユーザーには、このポリシーは適用されません。

接続に適用されるポリシーの確認

複数のポリシーが適用されているため、接続が応答しないことがあります。作成したポリシーよりも優先度の高いポリシーがあると、意図した設定内容が上書きされてしまいます。管理者は、ポリシーの結果セットを算出でき、接続のために最終的にポリシー設定をどのようにマージするかを決定できます。

以下の方法で、ポリシーの結果セットを算出できます：

- **Citrix** グループポリシーモデル作成ウィザードを使用して、接続シナリオをシミュレートし、Citrix ポリシーがどのように適用されるかを確認する。次のような接続シナリオの条件を指定できます：
  - ドメインコントローラー
  - ユーザー
  - Citrix ポリシーの割り当ての証拠値

  - 低速ネットワーク接続などのシミュレートされた環境設定
    ウィザードが生成するレポートには、このシナリオで機能する Citrix ポリシーが一覧表示されます。ドメインユーザーとして Controller にログオンしている場合は、サイトポリシー設定と Active Directory グループポリシーオブジェクト（GPO）の両方を使ってポリシーの結果が算出されます。

- グループポリシーの結果で、特定のユーザーや Controller に適用される Citrix ポリシーのレポートを作成する。グループポリシー結果ツールは、環境内の GPO の現在の状態を評価し、レポートを生成するのに役立ちます。生成されたレポートは、Citrix ポリシーなどのオブジェクトが、特定のユーザーおよびコントローラーに現在どのように適用されているかを示します。

Citrix グループポリシーモデル作成ウィザードは、Web Studio で起動できます。または、Windows のグループポリシー管理コンソールからグループポリシー結果ツールを起動することもできます。

Web Studio を使用して作成したサイトポリシー設定は、次の場合、ポリシーの結果セットに含まれません:

- グループポリシー管理コンソールから Citrix グループポリシーモデル作成ウィザードを実行する場合
- グループポリシー管理コンソールからグループポリシー結果ツールを実行する場合

ポリシーの管理にグループポリシー管理コンソールのみを使用している場合を除き、最も包括的なポリシーの結果セットを確実に取得するためには、Web Studio から Citrix グループポリシーモデル作成ウィザードを起動することをお勧めします。

ポリシーのトラブルシューティング

複数のポリシーで、適用先として同じ割り当て（ユーザーアカウントやクライアントの IP アドレスなど）を指定することも可能です。このシナリオでは、ポリシーの設定が別のポリシーの設定と競合すると、ポリシーが意図したとおりに適用されない可能性があります。最終的に適用されるポリシーを確認するために Citrix グループポリシーモデル作成ウィザードやグループポリシーの結果ウィザードを使用する場合、ユーザー接続にいずれのポリシーも適用されないことが判明することがあります。このようなシナリオでは、ポリシー評価基準に合致する条件でアプリケーションおよびデスクトップに接続するユーザーに、ポリシー設定が適用されません。この状況は、次の場合に発生します:

- 割り当て条件に合致するポリシーがない場合。
- 割り当て条件に合致したポリシーに設定項目が追加されていない場合。
- 割り当て条件に合致したポリシーが無効になっている場合。

指定した条件の接続にポリシーが適用されるようにするには、以下の内容を確認します。

- そのポリシーが有効になっている。
- そのポリシーに追加した設定項目の内容が適切である。

デフォルトのポリシー設定

August 17, 2024

次の表は、ポリシーの各設定項目のデフォルト設定と、適用される Virtual Delivery Agent（VDA）のバージョンの一覧です。

ICA

名前	デフォルト設定	VDA
アダプティブトランスポート	オフ。可能であれば使用	VDA 7.13～7.15、VDA 7.16 以降
クライアントクリップボードリダイレクト	許可	すべてのバージョンの VDA
クライアントクリップボードに書き込みを許可する形式	形式の指定なし	VDA 7.6 以降
デスクトップの起動	禁止	マルチセッション OS 対応 VDA 7 以降
ICA リスナーポートの番号	1494	すべてのバージョンの VDA
クライアント接続での非公開アプリケーションの起動	禁止	マルチセッション OS 対応 VDA 7 以降
クリップボードのクライアントからセッションへの転送サイズを制限する	無効	VDA 2009
クリップボードのセッションからクライアントへの転送サイズを制限する	無効	VDA 2009
損失耐性モード	許可	VDA 2003。注：損失耐性モードはまだ利用できません。利用可能になった際、VDA のこのバージョンでサポートされます。
損失耐性モードのしきい値	損失耐性モードが利用可能な場合：パケット損失：5%、遅延：300 ミリ秒（RTT）	VDA 2003 以降
Rendezvous プロトコル	無効	Citrix Cloud 経由で確立された HDX セッションにのみ適用されます。
クライアントクリップボードの書き込み制限	禁止	VDA 7.6 以降

名前	デフォルト設定	VDA
セッションクリップボードの書き込み制限	禁止	VDA 7.6 以降
セッションクリップボードに書き込みを許可する形式	形式の指定なし	VDA 7.6 以降
タブレットモードの切り替え	有効	VDA 7.16 以降。VDA 7.14 および 7.15 LTSR では、この設定はレジストリで構成します。
仮想チャネルの許可リスト	有効	VDA 2109 以降
セッションメトリックの収集	許可	7.42 以降

ICA/Adobe Flash デリバリー**/Flash** リダイレクト

名前	デフォルト設定	VDA
Flash ビデオフォールバック防止	未構成	VDA 7.6 FP3 以降
Flash ビデオフォールバック防止エラー *.swf		VDA 7.6 FP3 以降

ICA/オーディオ

名前	デフォルト設定	VDA
アダプティブオーディオ	有効	Citrix Virtual Apps and Desktops 2109 以降を使用する VDA のシングルセッション OS セッションとマルチセッション OS セッションの両方に適用されます。
UDP でのオーディオリアルタイムトランスポート	許可	すべてのバージョンの VDA
オーディオプラグアンドプレイ	許可	マルチセッション OS 対応 VDA 7 以降
音質	高 - 高品位オーディオ	すべてのバージョンの VDA
クライアントオーディオリダイレクト	許可	すべてのバージョンの VDA
クライアントマイクリダイレクト	許可	すべてのバージョンの VDA

名前	デフォルト設定	VDA
オーディオの損失耐性モード	禁止	VDA バージョン 2402 以降

ICA/クライアントの自動再接続

名前	デフォルト設定	VDA
クライアントの自動再接続	許可	すべてのバージョンの VDA
クライアントの自動再接続時の認証	認証を必要としない	すべてのバージョンの VDA
クライアントの自動再接続のログ	自動再接続イベントをログに記録しない	すべてのバージョンの VDA
クライアントの自動再接続のタイムアウト	120 秒	VDA 7.13 以降
再接続 UI の透過レベル	80%	VDA 7.13 以降

ICA/帯域幅

名前	デフォルト設定	VDA
オーディオリダイレクトの最大帯域幅（Kbps）	0Kbps	すべてのバージョンの VDA
オーディオリダイレクトの最大帯域幅（%）	0	すべてのバージョンの VDA
USB デバイスリダイレクトの最大帯域幅（Kbps）	0Kbps	VDA 5.5、5.6 FP1、マルチセッション OS 対応 VDA 7 以降、シングルセッション対応 VDA 7 以降
USB デバイスリダイレクトの最大帯域幅（%）	0	VDA 5.5、5.6 FP1、マルチセッション OS 対応 VDA 7 以降、シングルセッション対応 VDA 7 以降
クリップボードリダイレクトの最大帯域幅（Kbps）	0Kbps	すべてのバージョンの VDA
クリップボードリダイレクトの最大帯域幅（%）	0	すべてのバージョンの VDA
COM ポートリダイレクトの最大帯域幅 (Kbps)	0Kbps	すべてのバージョンの VDA。VDA 7.0 から 7.8 ではレジストリで構成します。

名前	デフォルト設定	VDA
COM ポートリダイレクトの最大帯域幅（%）	0	すべてのバージョンの VDA。VDA 7.0 から 7.8 ではレジストリで構成します。
ファイルリダイレクトの最大帯域幅（Kbps）	0Kbps	すべてのバージョンの VDA
ファイルリダイレクトの最大帯域幅（%）	0	すべてのバージョンの VDA
HDX MediaStream マルチメディアアクセラレーションの最大帯域幅	0Kbps	VDA 5.5、5.6 FP1、マルチセッション OS 対応 VDA 7 およびシングルセッション OS 対応 VDA 7 から最新のマルチセッション OS 対応 VDA およびシングルセッション OS 対応 VDA
HDX MediaStream マルチメディアアクセラレーションの最大帯域幅（%）	0	VDA 5.5、5.6 FP1、マルチセッション OS 対応 VDA 7 以降、シングルセッション対応 VDA 7 以降
LPT ポートリダイレクトの最大帯域幅（Kbps）	0Kbps	すべてのバージョンの VDA。VDA 7.0 から 7.8 ではレジストリで構成します。
LPT ポートリダイレクトの最大帯域幅（%）	0	すべてのバージョンの VDA。VDA 7.0 から 7.8 ではレジストリで構成します。
セッション全体の最大帯域幅	0Kbps	すべてのバージョンの VDA
プリンターリダイレクトの最大帯域幅（Kbps）	0Kbps	すべてのバージョンの VDA
プリンターリダイレクトの最大帯域幅（%）	0	すべてのバージョンの VDA
TWAIN デバイスリダイレクトの最大帯域幅（Kbps）	0Kbps	VDA 5.5、5.6 FP1、マルチセッション OS 対応 VDA 7 以降、シングルセッション対応 VDA 7 以降
TWAIN デバイスリダイレクトの最大帯域幅（%）	0	VDA 5.5、5.6 FP1、マルチセッション OS 対応 VDA 7 以降、シングルセッション対応 VDA 7 以降

ICA/コンテンツの双方向リダイレクト

名前	デフォルト設定	VDA
コンテンツの双方向リダイレクトを許可する	禁止	VDA 7.13 以降
クライアントへのリダイレクトを許可する URL	empty	VDA 7.13 以降
VDA へのリダイレクトを許可する URL	empty	VDA 7.13 以降
コンテンツの双方向リダイレクトの構成	無効	VDA 2311 以降

ICA/Web ブラウザーコンテンツのリダイレクト

名前	デフォルト設定	VDA
ブラウザーコンテンツリダイレクト	許可	VDA 7.16 以降
Web ブラウザーコンテンツリダイレクトの ACL 構成	`https://www.youtube.com/*`	VDA 7.16 以降
Web ブラウザーコンテンツリダイレクト統合 Windows 認証サポート	禁止	VDA 2106 以降
Web ブラウザーコンテンツリダイレクトのプロキシ構成	empty	VDA 7.16 以降
Web ブラウザーコンテンツリダイレクトのサーバー側での取得のプロキシ認証	禁止	VDA 2012 以降

ICA/クライアントセンサー

名前	デフォルト設定	VDA
クライアントデバイスの位置情報をアプリケーションで使用する	禁止	VDA 5.6 FP1、マルチセッション OS 対応 VDA 7 以降、シングルセッション対応 VDA 7 以降

ICA/デスクトップ **UI**

名前	デフォルト設定	VDA
デスクトップコンポジションリダイレクト	無効（7.6 FP3 以降）、有効（5.6～7.6 FP2）	VDA 5.6、シングルセッション OS 対応 VDA 7～7.15
デスクトップコンポジションリダイレクトの画質	中	VDA 5.6、シングルセッション OS 対応 VDA 7～7.15
デスクトップの壁紙	許可	すべてのバージョンの VDA
メニューをアニメーション化する	許可	すべてのバージョンの VDA
ドラッグ中にウィンドウの内容を表示する	許可	すべてのバージョンの VDA

ICA/エンドユーザーモニタリング

名前	デフォルト設定	VDA
ICA 往復測定	有効	すべてのバージョンの VDA
ICA 往復測定間隔	15 秒	すべてのバージョンの VDA
アイドル接続の ICA 往復測定	無効	すべてのバージョンの VDA

ICA/拡張デスクトップエクスペリエンス

名前	デフォルト設定	VDA
拡張デスクトップエクスペリエンス	許可	マルチセッション OS 対応 VDA 7 以降

ICA/ファイルリダイレクト

名前	デフォルト設定	VDA
クライアントドライブに自動接続する	許可	すべてのバージョンの VDA
クライアントドライブリダイレクト	許可	すべてのバージョンの VDA
クライアント側固定ドライブ	許可	すべてのバージョンの VDA
クライアント側フロッピードライブ	許可	すべてのバージョンの VDA

名前	デフォルト設定	VDA
クライアント側ネットワークドライブ	許可	すべてのバージョンの VDA
クライアント側光学式ドライブ	許可	すべてのバージョンの VDA
クライアント側リムーバブルドライブ	許可	すべてのバージョンの VDA
ホストからクライアントへのリダイレクト	無効	マルチセッション OS 対応 VDA 7 以降
クライアント側のドライブ文字を保持する	無効	VDA 5、5.5、5.6 FP1、シングルセッション OS 対応 VDA 7 以降
クライアント側ドライブへの読み取り専用アクセス	無効	VDA 5.5、5.6 FP1、マルチセッション OS 対応 VDA 7 以降、シングルセッション対応 VDA 7 以降
ユーザーフォルダーのリダイレクト	許可	Web Interface 環境でのみ。マルチセッション OS 対応 VDA 7 以降
非同期書き込みを使用する	無効	すべてのバージョンの VDA

ICA/グラフィック

名前	デフォルト設定	VDA
視覚的無損失の圧縮を使用する	無効	VDA 7.6 以降
表示メモリの制限	65,536KB	VDA 5、5.5、5.6 FP1、シングルセッション OS 対応 VDA 7 以降
メモリが不足したときの表示モード	色数を下げる	すべてのバージョンの VDA
動的ウィンドウプレビュー	有効	VDA 5.5、5.6 FP1、マルチセッション OS 対応 VDA 7 以降、シングルセッション対応 VDA 7 以降
グラフィックス状態インジケーター	無効	VDA 7.16 以降
イメージキャッシュ	有効	VDA 5.5、5.6 FP1、マルチセッション OS 対応 VDA 7 以降、シングルセッション対応 VDA 7 以降
従来のグラフィックモード	無効	マルチセッション OS 対応 VDA 7 以降、シングルセッション対応 VDA 7 以降
許可される最大表示色数	32 ビット/ピクセル	すべてのバージョンの VDA

名前	デフォルト設定	VDA
メモリ不足による表示品質の低下をユーザーに通知する	無効	マルチセッション OS 対応 VDA 7 以降
3D 画像ワークロードの最適化	無効	VDA 7.17 以降
キューイメージの破棄	有効	すべてのバージョンの VDA
画面共有	無効	VDA 2112
圧縮にビデオコーデックを使用する	選択された場合ビデオコーデックを使用する	VDA 7.6 FP3 以降
ビデオ コーデックにハードウェアエンコーディングを使用します	有効	VDA 7.11 以降

ICA/グラフィック**/**キャッシュ

名前	デフォルト設定	VDA
固定キャッシュしきい値	3,000,000bps	マルチセッション OS 対応 VDA 7 以降

ICA/グラフィック**/Framehawk**

名前	デフォルト設定	VDA
Framehawk ディスプレイチャネル	無効	VDA 7.6 FP2 以降
Framehawk 表示チャネルポートの範囲	3224、3324	VDA 7.6 FP2 以降

ICA/Keep-Alive

名前	デフォルト設定	VDA
ICA Keep-Alive タイムアウト	60 秒	すべてのバージョンの VDA
ICA Keep-Alive	ICA Keep-Alive メッセージを送信しない	すべてのバージョンの VDA

ICA/キーボードおよび **IME**

名前	デフォルト設定	VDA
クライアントキーボードレイアウトの同期と IME の改善	無効	1912 LTSR CU2 以降にのみ適用されます。
Unicode キーボードレイアウトのマッピングの有効化	禁止	1912 LTSR CU2 以降にのみ適用されます。
キーボード レイアウトの切り替えポップアップメッセージを非表示にする。	禁止	1912 LTSR CU2 以降にのみ適用されます。

ICA/ローカルアプリアクセス

名前	デフォルト設定	VDA
ローカルアプリアクセスを許可する	禁止	マルチセッション OS 対応 VDA 7 以降、シングルセッション対応 VDA 7 以降
URL のリダイレクトの禁止リスト	サイトの指定なし	マルチセッション OS 対応 VDA 7 以降、シングルセッション対応 VDA 7 以降
URL のリダイレクトの許可リスト	サイトの指定なし	マルチセッション OS 対応 VDA 7 以降、シングルセッション対応 VDA 7 以降

ICA/モバイルデバイスでの動作

名前	デフォルト設定	VDA
キーボードの自動表示	禁止	VDA 5.6 FP1、マルチセッション OS 対応 VDA 7 以降、シングルセッション対応 VDA 7 以降

名前	デフォルト設定	VDA
タッチパネルでの操作に最適化されたデスクトップ	許可	VDA 5.6 FP1、マルチセッション OS 対応 VDA 7 以降、シングルセッション OS 対応 VDA 7 以降。この設定は無効になっており、Windows 10 および Windows Server 2016 マシンでは使用できません。
コンボボックスをデバイス側で表示する	禁止	VDA 5.6 FP1、マルチセッション OS 対応 VDA 7 以降、シングルセッション対応 VDA 7 以降

ICA/マルチメディア

名前	デフォルト設定	VDA
HTML5 ビデオリダイレクト	禁止	VDA 7.12 以降
ビデオ品質の制限	未構成	マルチセッション OS 対応 VDA 7 以降、シングルセッション対応 VDA 7 以降
Microsoft Teams リダイレクト	許可	マルチセッション OS 対応 VDA 1906 以降、シングルセッション対応 VDA 1906 以降
マルチメディア会議	許可	すべてのバージョンの VDA
WAN 接続での Windows Media マルチメディアリダイレクトの最適化	許可	マルチセッション OS 対応 VDA 7 以降、シングルセッション対応 VDA 7 以降
WAN 接続での Windows Media マルチメディアリダイレクトでの GPU の使用	禁止	マルチセッション OS 対応 VDA 7 以降、シングルセッション対応 VDA 7 以降
Windows メディアフォールバック防止	未構成	VDA 7.6 FP3 以降
Windows Media のクライアント側でのコンテンツ取得	許可	マルチセッション OS 対応 VDA 7 以降、シングルセッション対応 VDA 7 以降
Windows Media リダイレクト	許可	すべてのバージョンの VDA
Windows Media リダイレクトのバッファーサイズ	5 秒	VDA 5、5.5、5.6 FP1 以降

名前	デフォルト設定	VDA
Windows Media リダイレクトのバッファーサイズ使用	無効	VDA 5、5.5、5.6 FP1 以降

ICA/マルチストリーム接続

名前	デフォルト設定	VDA
UDP を使用したオーディオ	許可	マルチセッション OS 対応 VDA 7 以降
オーディオ UDP ポートの範囲	16500、16509	VDA 5.5、5.6 FP1、マルチセッション OS 対応 VDA 7 以降、シングルセッション対応 VDA 7 以降
マルチポートポリシー	プライマリポート（2598）に優先度［高］	VDA 5.5、5.6 FP1、マルチセッション OS 対応 VDA 7 以降、シングルセッション対応 VDA 7 以降
マルチストリームコンピューター設定	無効	VDA 5.5、5.6 FP1、マルチセッション OS 対応 VDA 7 以降、シングルセッション対応 VDA 7 以降
マルチストリームユーザー設定	無効	VDA 5.5、5.6 FP1、マルチセッション OS 対応 VDA 7 以降、シングルセッション対応 VDA 7 以降
マルチストリーム仮想チャネルのストリーム割り当て設定	デフォルトのストリーム割り当てについては、「マルチストリーム仮想チャネルの割り当て設定」を参照してください。	VDA 2003

ICA/ポートリダイレクト

名前	デフォルト設定	VDA
クライアント COM ポートを自動接続する	無効	すべてのバージョンの VDA。VDA 7.0 から 7.8 ではレジストリで構成します。
クライアント LPT ポートを自動接続する	無効	すべてのバージョンの VDA。VDA 7.0 から 7.8 ではレジストリで構成します。

名前	デフォルト設定	VDA
クライアント COM ポートリダイレクト	禁止	すべてのバージョンの VDA。VDA 7.0 から 7.8 ではレジストリで構成します。
クライアント LPT ポートリダイレクト	禁止	すべてのバージョンの VDA。VDA 7.0 から 7.8 ではレジストリで構成します。

ICA/印刷

名前	デフォルト設定	VDA
クライアントプリンターリダイレクト	許可	すべてのバージョンの VDA
デフォルトプリンター	クライアントのメイン プリンターをデフォルトに設定する	すべてのバージョンの VDA
プリンター割り当て	ユーザーの現在のプリンター	すべてのバージョンの VDA
プリンター自動作成イベントログの設定	エラーおよび警告をログに記録する	すべてのバージョンの VDA
セッションプリンター	プリンターの指定なし	すべてのバージョンの VDA
プリンターの自動作成を待機する (デスクトップ)	無効	すべてのバージョンの VDA

ICA/印刷**/**クライアントプリンター

名前	デフォルト設定	VDA
クライアントプリンターを自動作成する	すべてのクライアントプリンターを自動作成する	すべてのバージョンの VDA
汎用ユニバーサルプリンターを自動作成する	無効	すべてのバージョンの VDA
クライアントプリンター名	標準のプリンター名	VDA 5.6
プリントサーバーへの直接接続	有効	すべてのバージョンの VDA
プリンタードライバーのマッピングと互換性	規則の指定なし	すべてのバージョンの VDA

名前	デフォルト設定	VDA
プリンタープロパティの保存	クライアントに保存できない場合にのみユーザープロファイルに保存する	すべてのバージョンの VDA
クライアントプリンターの保持と復元	許可	VDA 5、5,5、5.6 FP1

ICA/印刷**/**ドライバー

名前	デフォルト設定	VDA
付属のプリンタードライバーの自動インストール	有効	すべてのバージョンの VDA
ユニバーサルドライバーの優先度	EMF; XPS; PCL5c; PCL4; PS	すべてのバージョンの VDA
ユニバーサル印刷の使用	要求されたドライバーを使用できない場合にのみユニバーサル印刷を使用する	すべてのバージョンの VDA

ICA/印刷**/**ユニバーサルプリントサーバー

名前	デフォルト設定	VDA
ユニバーサルプリントサーバーの有効化	無効	すべてのバージョンの VDA
ユニバーサルプリントサーバー印刷データストリーム（CGP）ポート	7229	すべてのバージョンの VDA
ユニバーサルプリントサーバー入力データストリームの最大帯域幅 (kbps)	0	すべてのバージョンの VDA
ユニバーサルプリントサーバー Web サービス（HTTP/SOAP）ポート	8080	すべてのバージョンの VDA
負荷分散のためのユニバーサルプリントサーバー		VDA バージョン 7.9 以降
ユニバーサルプリントサーバーのサービス停止のしきい値	180（秒）	VDA バージョン 7.9 以降

ICA/印刷**/**ユニバーサル印刷

名前	デフォルト設定	VDA
ユニバーサル印刷 EMF 処理モード	EMF スプール ファイルを直接挿入する	すべてのバージョンの VDA
ユニバーサル印刷イメージ圧縮制限	最高品質（無損失圧縮）	すべてのバージョンの VDA
ユニバーサル印刷最適化デフォルト	[イメージ圧縮］の各項目は［必要なイメージ品質］=［標準品質]、[ヘビーウェイト圧縮を有効にする］=［いいえ]。[イメージおよびフォントのキャッシュ］の各項目は、[埋め込みイメージのキャッシュを許可する］=[はい]、[非管理者によるこれらの設定の変更を許可する］=［いいえ]。	すべてのバージョンの VDA
ユニバーサル印刷プレビューの設定	自動作成プリンターまたは汎用ユニバーサルプリンターの印刷プレビューを使用しない	すべてのバージョンの VDA
ユニバーサル印刷品質制限	制限なし	すべてのバージョンの VDA

ICA/セキュリティ

名前	デフォルト設定	VDA
SecureICA の最低暗号化レベル	基本	マルチセッション OS 対応 VDA 7 以降

ICA/サーバーの制限

名前	デフォルト設定	VDA
サーバーのアイドルタイマーの間隔	0 ミリ秒	マルチセッション OS 対応 VDA 7 以降

ICA/セッションの制限

名前	デフォルト設定	VDA
切断セッションタイマー	無効	VDA 5、5.5、5.6 FP1、シングルセッション OS 対応 VDA 7 以降
リモート PC アクセス切断セッションタイマー	無効	シングルセッション OS 対応 VDA 7 以降
切断セッションタイマーの間隔	1,440 分	VDA 5、5.5、5.6 FP1、シングルセッション OS 対応 VDA 7 以降
セッション接続タイマー	無効	VDA 5、5.5、5.6 FP1、シングルセッション OS 対応 VDA 7 以降
セッション接続タイマーの間隔	1,440 分	VDA 5、5.5、5.6 FP1、シングルセッション OS 対応 VDA 7 以降
セッションアイドルタイマー	有効	VDA 5、5.5、5.6 FP1、シングルセッション OS 対応 VDA 7 以降
セッションアイドルタイマーの間隔	1,440 分	VDA 5、5.5、5.6 FP1、シングルセッション OS 対応 VDA 7 以降

ICA/セッション画面の保持

名前	デフォルト設定	VDA
セッション画面の保持	許可	すべてのバージョンの VDA
セッション画面の保持のポート番号	2598	すべてのバージョンの VDA
セッション画面の保持のタイムアウト	180 秒	すべてのバージョンの VDA

ICA/タイムゾーン制御

名前	デフォルト設定	VDA
レガシークライアントのローカルタイムゾーンを検出する	有効	マルチセッション OS 対応 VDA 7 以降
セッションの切断時またはログオフ時にシングルセッション OS のタイムゾーンを復元する	有効	最新の VDA バージョン
クライアントのローカルタイムゾーンを使用する	サーバーのタイムゾーンを使用する	すべてのバージョンの VDA

ICA/TWAIN デバイス

名前	デフォルト設定	VDA
クライアント TWAIN デバイスリダイレクト	許可	VDA 5.5、5.6 FP1、マルチセッション OS 対応 VDA 7 以降、シングルセッション対応 VDA 7 以降
TWAIN 圧縮レベル	中	VDA 5.5、5.6 FP1、マルチセッション OS 対応 VDA 7 以降、シングルセッション対応 VDA 7 以降

ICA/USB デバイス

名前	デフォルト設定	VDA
クライアント USB デバイス最適化規則	[有効]（VDA 7.6 FP3 以降）、[無効]（VDA 7.11 以降）。デフォルトでは規則は指定されていません。	VDA 7.6 FP3 以降
クライアント USB デバイスリダイレクト	禁止	すべてのバージョンの VDA
クライアント USB デバイスリダイレクト規則	規則の指定なし	すべてのバージョンの VDA
クライアント USB プラグアンドプレイデバイスリダイレクト	許可	マルチセッション OS 対応 VDA 7 以降、シングルセッション対応 VDA 7 以降

ICA/視覚表示

名前	デフォルト設定	VDA
簡素なグラフィックに対する優先的色の解像度	24 ビット/ピクセル	VDA 7.6 FP3 以降
ターゲットフレーム数	30fps	すべてのバージョンの VDA
表示品質	中	マルチセッション OS 対応 VDA 7 以降、シングルセッション対応 VDA 7 以降

ICA/視覚表示/動画

名前	デフォルト設定	VDA
画質の下限レベル	Normal（通常）	VDA 5.5、5.6 FP1、マルチセッション OS 対応 VDA 7 以降、シングルセッション対応 VDA 7 以降
動画圧縮	有効	VDA 5.5、5.6 FP1、マルチセッション OS 対応 VDA 7 以降、シングルセッション対応 VDA 7 以降
プログレッシブ圧縮のレベル	なし	VDA 5.5、5.6 FP1、マルチセッション OS 対応 VDA 7 以降、シングルセッション対応 VDA 7 以降
プログレッシブ圧縮のしきい値	2,147,483,647Kbps	VDA 5.5、5.6 FP1、マルチセッション OS 対応 VDA 7 以降、シングルセッション対応 VDA 7 以降
保持する最低フレーム数	10fps	VDA 5.5、5.6 FP1、マルチセッション OS 対応 VDA 7 以降、シングルセッション対応 VDA 7 以降

> 注:
>
> 保持する最低フレーム数ポリシーは廃止されました。

ICA/視覚表示/静止画

名前	デフォルト設定	VDA
エクストラ色圧縮	無効	すべてのバージョンの VDA
エクストラ色圧縮しきい値	8,192Kbps	すべてのバージョンの VDA
ヘビーウェイト圧縮	無効	すべてのバージョンの VDA
非可逆圧縮のレベル	中	すべてのバージョンの VDA
非可逆圧縮のしきい値	2,147,483,647Kbps	すべてのバージョンの VDA

ICA/WebSocket

名前	デフォルト設定	VDA
WebSocket 接続	禁止	マルチセッション OS 対応 VDA 7 以降、シングルセッション対応 VDA 7 以降
WebSocket ポート番号	8008	マルチセッション OS 対応 VDA 7 以降、シングルセッション対応 VDA 7 以降
WebSocket 信頼される接続元サーバー一覧	*（すべての Receiver for Web サイト URL が信頼されます）	マルチセッション OS 対応 VDA 7 以降、シングルセッション対応 VDA 7 以降

負荷管理

名前	デフォルト設定	VDA
同時ログオントレランス	2	マルチセッション OS 対応 VDA 7 以降
CPU 使用率	無効	マルチセッション OS 対応 VDA 7 以降
CPU 使用率から除外するプロセスの優先順位	通常以下および低	マルチセッション OS 対応 VDA 7 以降
ディスク使用率	無効	マルチセッション OS 対応 VDA 7 以降
最大セッション数	250	マルチセッション OS 対応 VDA 7 以降
メモリ使用率	無効	マルチセッション OS 対応 VDA 7 以降
基本メモリ使用量	ゼロ負荷：768MB	マルチセッション OS 対応 VDA 7 以降

Profile Management/上級設定

名前	デフォルト設定	VDA
自動構成を無効にする	無効	すべてのバージョンの VDA
問題が発生する場合にユーザーをログオフ	無効	すべてのバージョンの VDA

名前	デフォルト設定	VDA
ロックされたファイルにアクセスする場合の試行数	5	すべてのバージョンの VDA
ログオフ時にインターネット Cookie ファイルを処理	無効	すべてのバージョンの VDA

Profile Management/基本設定

名前	デフォルト設定	VDA
アクティブライトバック	無効	すべてのバージョンの VDA
Profile Management の有効化	無効	すべてのバージョンの VDA
除外グループ	無効。すべてのユーザーグループのプロファイルが処理されます。	すべてのバージョンの VDA
オフライン プロファイル サポート	無効	すべてのバージョンの VDA
ユーザーストアへのパス	Windows	すべてのバージョンの VDA
ローカル管理者のログオン処理	無効	すべてのバージョンの VDA
処理済みグループ	無効。すべてのユーザーグループのプロファイルが処理されます。	すべてのバージョンの VDA

Profile Management/クロスプラットフォーム設定

名前	デフォルト設定	VDA
クロスプラットフォーム設定ユーザーグループ	無効。［処理済みグループ］で指定したすべてのユーザーグループのプロファイルが処理されます。	すべてのバージョンの VDA
クロスプラットフォーム設定の有効化	無効	すべてのバージョンの VDA
クロスプラットフォーム定義へのパス	無効。パスは指定されていません。	すべてのバージョンの VDA
クロスプラットフォーム設定ストアへのパス	無効。Windows\PM_CM が使用されます。	すべてのバージョンの VDA
クロスプラットフォーム設定を作成するためのソース	無効	すべてのバージョンの VDA

Profile Management/ファイルシステム**/**除外

名前	デフォルト設定	VDA
除外の一覧 - ディレクトリ	無効。ユーザープロファイルのすべてのフォルダーが同期されます。	すべてのバージョンの VDA
除外の一覧 - ファイル	無効。ユーザープロファイルのすべてのファイルが同期されます。	すべてのバージョンの VDA

Profile Management/ファイルシステム**/**同期

名前	デフォルト設定	VDA
同期するディレクトリ	無効。除外されていないフォルダーのみが同期されます。	すべてのバージョンの VDA
同期するファイル	無効。除外されていないファイルのみが同期されます。	すべてのバージョンの VDA
ミラーリングするフォルダー	無効。フォルダーはミラーリングされません。	すべてのバージョンの VDA

Profile Management/フォルダーのリダイレクト

名前	デフォルト設定	VDA
管理者アクセスを許可	無効	すべてのバージョンの VDA
ドメイン名を包含	無効	すべてのバージョンの VDA

Profile Management/フォルダーのリダイレクト**/AppData**（**Roaming**）

名前	デフォルト設定	VDA
AppData（Roaming）パス	無効。パスは指定されていません。	すべてのバージョンの VDA
AppData(Roaming) のリダイレクト設定	［AppData（Roaming）パス］で指定した UNC パスにリダイレクト	すべてのバージョンの VDA

Profile Management/フォルダーのリダイレクト**/**連絡先

名前	デフォルト設定	VDA
アドレス帳パス	無効。パスは指定されていません。	すべてのバージョンの VDA
アドレス帳のリダイレクト設定	［連絡先パス］で指定した UNC パスにリダイレクト	すべてのバージョンの VDA

Profile Management/フォルダーのリダイレクト**/**デスクトップ

名前	デフォルト設定	VDA
デスクトップパス	無効。パスは指定されていません。	すべてのバージョンの VDA
デスクトップのリダイレクト設定	［デスクトップパス］で指定した UNC パスにリダイレクト	すべてのバージョンの VDA

Profile Management/フォルダーのリダイレクト**/**ドキュメント

名前	デフォルト設定	VDA
ドキュメントパス	無効。パスは指定されていません。	すべてのバージョンの VDA
ドキュメントのリダイレクト設定	［ドキュメントパス］で指定した UNC パスにリダイレクト	すべてのバージョンの VDA

Profile Management/フォルダーのリダイレクト**/**ダウンロード

名前	デフォルト設定	VDA
ダウンロードパス	無効。パスは指定されていません。	すべてのバージョンの VDA
ダウンロードのリダイレクト設定	［ダウンロードパス］で指定した UNC パスにリダイレクト	すべてのバージョンの VDA

Profile Management/フォルダーのリダイレクト**/**お気に入り

名前	デフォルト設定	VDA
お気に入りパス	無効。パスは指定されていません。	すべてのバージョンの VDA
お気に入りのリダイレクト設定	［お気に入りパス］で指定した UNC パスにリダイレクト	すべてのバージョンの VDA

Profile Management/フォルダーのリダイレクト**/**リンク

名前	デフォルト設定	VDA
リンクパス	無効。パスは指定されていません。	すべてのバージョンの VDA
リンクのリダイレクト設定	［リンクパス］で指定した UNC パスにリダイレクト	すべてのバージョンの VDA

Profile Management/フォルダーのリダイレクト**/**ミュージック

名前	デフォルト設定	VDA
ミュージックパス	無効。パスは指定されていません。	すべてのバージョンの VDA
ミュージックのリダイレクト設定	［ミュージックパス］で指定した UNC パスにリダイレクト	すべてのバージョンの VDA

Profile Management/フォルダーのリダイレクト**/**ピクチャ

名前	デフォルト設定	VDA
ピクチャパス	無効。パスは指定されていません。	すべてのバージョンの VDA
ピクチャのリダイレクト設定	［ピクチャパス］で指定した UNC パスにリダイレクト	すべてのバージョンの VDA

Profile Management/フォルダーのリダイレクト**/**保存したゲーム

名前	デフォルト設定	VDA
保存したゲームパス	無効。パスは指定されていません。	すべてのバージョンの VDA
保存したゲームのリダイレクト設定	［保存したゲームパス］で指定した UNC パスにリダイレクト	すべてのバージョンの VDA

Profile Management/フォルダーのリダイレクト**/**検索

名前	デフォルト設定	VDA
検索パス	無効。パスは指定されていません。	すべてのバージョンの VDA
検索のリダイレクト設定	［検索パス］で指定した UNC パスにリダイレクト	すべてのバージョンの VDA

Profile Management/フォルダーのリダイレクト**/**スタートメニュー

名前	デフォルト設定	VDA
スタートメニューパス	無効。パスは指定されていません。	すべてのバージョンの VDA
スタートメニューのリダイレクト設定	［スタートメニューパス］で指定した UNC パスにリダイレクト	すべてのバージョンの VDA

Profile Management/フォルダーのリダイレクト**/**ビデオ

名前	デフォルト設定	VDA
ビデオパス	無効。パスは指定されていません。	すべてのバージョンの VDA
ビデオのリダイレクト設定	［ビデオパス］で指定した UNC パスにリダイレクト	すべてのバージョンの VDA

Profile Management/ログ設定

名前	デフォルト設定	VDA
Active Directory 操作	無効	すべてのバージョンの VDA
一般的な情報	無効	すべてのバージョンの VDA
一般的な警告	無効	すべてのバージョンの VDA
ログの有効化	無効	すべてのバージョンの VDA
ファイルシステム操作	無効	すべてのバージョンの VDA
ファイルシステム通知	無効	すべてのバージョンの VDA
ログオフ	無効	すべてのバージョンの VDA
ログオン	無効	すべてのバージョンの VDA
ログファイルの最大サイズ	1048576	すべてのバージョンの VDA
ログファイルへのパス	無効。%System-Root%\System32\Logfiles\UserProfileManager に生成されます	すべてのバージョンの VDA
個人用ユーザー情報	無効	すべてのバージョンの VDA
ログオンおよびログオフ時のポリシー値	無効	すべてのバージョンの VDA
レジストリ操作	無効	すべてのバージョンの VDA
ログオフ時のレジストリ差分	無効	すべてのバージョンの VDA

Profile Management/プロファイル制御

名前	デフォルト設定	VDA
キャッシュしたプロファイルを削除する前の待ち時間	0	すべてのバージョンの VDA
ログオフ時にローカルでキャッシュしたプロファイルの削除	無効	すべてのバージョンの VDA
ローカルプロファイル競合の制御	ローカル プロファイルを使用	すべてのバージョンの VDA
既存のプロファイルの移行	ローカルおよび移動	すべてのバージョンの VDA

名前	デフォルト設定	VDA
テンプレートプロファイルへのパス	無効。ユーザーが最初にログオンするコンピューター上のデフォルトのユーザープロファイルから新しいユーザープロファイルが作成されます。	すべてのバージョンの VDA
テンプレートプロファイルがローカル プロファイルを上書きする	無効	すべてのバージョンの VDA
テンプレートプロファイルが移動プロファイルを上書きする	無効	すべてのバージョンの VDA
すべてのログオンで Citrix 固定プロファイルとして使用されるテンプレートプロファイル	無効	すべてのバージョンの VDA

Profile Management/レジストリ

名前	デフォルト設定	VDA
除外の一覧	無効。HKEY_CURRENT_USER ハイブのすべてのレジストリキーがユーザーのログオフ時に処理されます。	すべてのバージョンの VDA
包含の一覧	無効。HKEY_CURRENT_USER ハイブのすべてのレジストリキーがユーザーのログオフ時に処理されます。	すべてのバージョンの VDA

Profile Management/ストリーム配信ユーザープロファイル

名前	デフォルト設定	VDA
常時キャッシュ	無効	すべてのバージョンの VDA
常時キャッシュサイズ	0Mb	すべてのバージョンの VDA
プロファイルストリーミング	無効	すべてのバージョンの VDA
ストリーム配信ユーザープロファイルグループ	無効。OU 内のすべてのユーザープロファイルが処理されます。	すべてのバージョンの VDA
待機領域のロックファイルのタイムアウト（日）	1 日	すべてのバージョンの VDA

Receiver

名前	デフォルト設定	VDA
StoreFront アカウント一覧	ストアの指定なし	マルチセッション OS 対応 VDA 7 以降、シングルセッション対応 VDA 7 以降

ユーザー個人設定レイヤー

名前	デフォルト設定	VDA
ユーザーレイヤーリポジトリパス	無効。パスは指定されていません。	VDA 19.12 以降のバージョン
ユーザーレイヤーサイズ（GB）	10GB。ユーザーレイヤーは、設定したサイズまで拡張するシンプロビジョニングされたディスクです。ユーザーレイヤーのサイズが小さくなることはありません。	VDA 19.12 以降のバージョン

Virtual Delivery Agent

名前	デフォルト設定	VDA
コントローラー登録の IPv6 ネットマスク	ネットマスクの指定なし	マルチセッション OS 対応 VDA 7 以降、シングルセッション対応 VDA 7 以降
コントローラー登録ポート	80	すべてのバージョンの VDA
コントローラー SID	SID の指定なし	すべてのバージョンの VDA
Controller	Controller の指定なし	すべてのバージョンの VDA
コントローラーの自動更新を有効にする	有効	マルチセッション OS 対応 VDA 7 以降、シングルセッション対応 VDA 7 以降
IPv6 コントローラー登録のみを使用する	無効	マルチセッション OS 対応 VDA 7 以降、シングルセッション対応 VDA 7 以降
サイト GUID	GUID の指定なし	すべてのバージョンの VDA

Virtual Delivery Agent/HDX 3D Pro

名前	デフォルト設定	VDA
無損失を有効にする	有効	VDA 5.5、5.6 FP1
HDX 3D Pro 品質レベル		VDA 5.5、5.6 FP1

Virtual Delivery Agent/Monitoring

名前	デフォルト設定	VDA
プロセスの監視を有効にします	無効	VDA 7.11 以降
リソースの監視を有効にします	有効	VDA 7.11 以降

仮想 IP

名前	デフォルト設定	VDA
仮想 IP ループバックサポート	無効	VDA 7.6 以降
仮想 IP ループバックプログラム一覧	なし	VDA 7.6 以降

ポリシー設定リファレンス

August 17, 2024

ポリシーには、対象のセッションを制御するための設定項目があります。ここでは、その設定項目が依存するほかの設定項目や、関連する設定項目についても説明します。

クイックリファレンス

次の各表は、ポリシー内で構成できる設定の一覧です。これらの表では、左側の列がポリシーで制御するセッションの機能を示し、右側の列がその機能に対応する設定を示します。

すべてのポリシー設定の完全な一覧は、.CHM（コンパイル済み HTML）形式と.CSV 形式で利用できます。これらのファイルは、ブローカー（Delivery Controller）がインストールされているサーバー上の`\program files\citrix\grouppolicy`フォルダーにあります。また、こちらをクリックして、ポリシー設定の最新バージョンをダウンロードすることもできます。

オーディオ

目的	使用するポリシー設定
複数オーディオデバイスの使用を制御する	オーディオプラグアンドプレイ
クライアント側のマイクからのオーディオ入力を制御する	クライアントマイクリダイレクト
クライアント側のオーディオの音質を制御する	音質
クライアント側のスピーカーの使用を制御する	クライアントオーディオリダイレクト

帯域幅の制限

目的	使用するポリシー設定
クライアントオーディオマッピングで使用される帯域幅を制限する	[オーディオリダイレクトの最大帯域幅（Kbps）]または[オーディオリダイレクトの最大帯域幅（%）]
クリップボードマッピングで使用される帯域幅を制限する	[クリップボードリダイレクトの最大帯域幅（Kbps）]または［クリップボード リダイレクトの最大帯域幅（%）]
クライアント側ドライブへのアクセスで使用される帯域幅を制限する	[ファイルリダイレクトの最大帯域幅（Kbps）]または[ファイルリダイレクトの最大帯域幅（%）]
HDX MediaStream マルチメディアアクセラレーション	[HDX MediaStream マルチメディアアクセラレーションの最大帯域幅]または［HDX MediaStream マルチメディアアクセラレーションの最大帯域幅（%）]
クライアントセッションで使用される帯域幅を制限する	セッション全体の最大帯域幅
印刷	[プリンターリダイレクトの最大帯域幅（Kbps）]または[プリンターリダイレクトの最大帯域幅（%）]
カメラやスキャナーなどの TWAIN デバイスで使用される帯域幅を制限する	[TWAIN デバイスリダイレクトの最大帯域幅（Kbps）]または［TWAIN デバイスリダイレクトの最大帯域幅（%）]
USB デバイス	[USB デバイスリダイレクトの最大帯域幅]または[USB デバイスリダイレクトの最大帯域幅（%）]

クライアント側のドライブやデバイスのリダイレクト

目的	使用するポリシー設定
ログオン時にクライアント側ドライブに接続する機能を制御する	クライアントドライブに自動接続する
サーバーとローカルのクリップボード間でのデータ転送を制御する	クライアントクリップボードリダイレクト
クライアント側ドライブのマッピングを制御する	クライアントドライブリダイレクト
クライアント側ハードディスクドライブの使用を制御する	[クライアント側固定ドライブ] および [クライアントドライブリダイレクト]
クライアント側フロッピーディスクドライブの使用を制御する	[クライアント側フロッピードライブ] および [クライアントドライブリダイレクト]
クライアント側ネットワークドライブの使用を制御する	[クライアント側ネットワークドライブ] および [クライアントドライブリダイレクト]
クライアント側 CD、DVD、およびブルーレイドライブの使用を制御する	[クライアント側光学式ドライブ] および [クライアントドライブリダイレクト]
クライアント側リムーバブルドライブの使用を制御する	[クライアント側リムーバブルドライブ] および [クライアントドライブリダイレクト]
デジタルカメラやスキャナーなどのクライアント側 TWAIN デバイスの使用および転送されるイメージデータの圧縮レベルを制御する	[クライアント TWAIN デバイスリダイレクト]、[TWAIN 圧縮リダイレクト]
クライアント側 USB デバイスの使用を制御する	[クライアント USB デバイスリダイレクト] および [クライアント USB デバイスリダイレクト規則]
WAN を介した接続でのクライアント側ドライブへの書き込み速度を改善する	非同期書き込みを使用する

コンテンツリダイレクト

目的	使用するポリシー設定
サーバーからユーザーデバイス側にコンテンツをリダイレクトするかどうかを制御する	ホストからクライアントへのリダイレクト

デスクトップ **UI**

目的	使用するポリシー設定
セッションでの壁紙の表示を制御する	デスクトップの壁紙
ウィンドウの内容を表示したままドラッグする機能を制御する	ドラッグ中にウィンドウの内容を表示する

グラフィック/マルチメディア

> 重要:
>
> Flash ポリシーは、以前の VDA を使用しているお客様が新しい Controller（バージョン 1912 Controller など）を使用し、引き続き Flash を使用できるようにするためにのみ残されます。この VDA バージョンは Flash をサポートしていません。

目的	使用するポリシー設定
仮想デスクトップがクライアント側に送信されるときの、1 秒あたりのフレームの最大数を設定する	ターゲットフレーム数
ユーザーデバイス側に表示されるイメージの表示品質を制御する	表示品質
セッションで特定の Web ページ上の Flash コンテンツを表示するかどうかを制御する	[Flash サーバー側でのコンテンツ取得 URL リスト]、[Flash URL 互換性リスト]、[Flash ビデオフォールバック防止］ポリシー設定、[Flash ビデオフォールバック防止エラー *.swf]
サーバー側でレンダリングするビデオの圧縮の制御	[圧縮にビデオコーデックを使用する]、[ビデオコーデックにハードウェアエンコーディングを使用します]
HTML5 マルチメディア Web コンテンツのユーザーへの配信の制御	HTML5 ビデオリダイレクト

マルチストリームネットワークトラフィックの優先度

目的	使用するポリシー設定
マルチストリーム接続の ICA トラフィックのポートを指定して、各ポートのネットワーク 優先度を定義する	マルチポートポリシー
サーバーとユーザーデバイス間のマルチストリーム接続のサポートを有効にする	マルチストリーム（コンピューターポリシーおよびユーザーポリシー）

印刷

目的	使用するポリシー設定
ログオン時のクライアントプリンターの自動作成を制御する	[クライアント プリンターを自動作成する] および [クライアントプリンターリダイレクト]
プリンタープロパティの保存先を制御する	プリンタープロパティの保存
印刷ジョブをサーバーから直接プリンターに送信するか、クライアント経由で送信するかを制御する	プリントサーバーへの直接接続
クライアント側プリンターの使用を制御する	クライアントプリンターリダイレクト
クライアントプリンターおよびネットワークプリンターの自動作成時に、Windows に付属のプリンタードライバーを自動的にインストールするかどうかを制御する	付属のプリンタードライバーの自動インストール
ユニバーサルプリンタードライバーの使用を制御する	ユニバーサル印刷の使用
ローミングユーザーの接続方法に応じて自動作成されるプリンターを制御する	デフォルトプリンター
負荷を分散し、ユニバーサルプリントサーバーのフェールオーバーしきい値を設定する	[負荷分散のためのユニバーサルプリントサーバー]、[ユニバーサルプリントサーバーのサービス停止のしきい値]

> 注:
>
> デスクトップセッションおよびアプリケーションセッションでは、ポリシーを使用してスクリーンセーバーを有効にすることはできません。スクリーンセーバーが必要なユーザーの場合は、ユーザーデバイスにスクリーンセーバーを実装できます。

ICA のポリシー設定

August 17, 2024

> 注:
>
> このページでは、ICA ポリシー設定の説明と、サポートされている構成の値を示します。ポリシーの操作について詳しくは、「ポリシーの使用」セクションを参照してください。

アダプティブトランスポート

この設定では、EDT 上のデータトランスポートをプライマリとして TCP にフォールバックすることを、許可または禁止します。

デフォルトでは、アダプティブトランスポートが有効になり（[優先]）、可能な場合は EDT が使用されて、TCP にフォールバックします。必要に応じて設定を変更できます：

- 優先。可能な場合、Adaptive transport over EDT が使用され、TCP にフォールバックします。
- 診断モード。EDT が強制的にオンになり、TCP へのフォールバックは無効になります。この設定はトラブルシューティングでのみお勧めします。
- オフ。TCP が強制的にオンになり、EDT が無効になります。

詳しくは、「アダプティブトランスポート」を参照してください。

ドラッグアンドドロップ設定

この設定では、クライアントと仮想アプリケーションまたはデスクトップ間でのファイルのドラッグを許可または禁止します。デフォルトでは、ドラッグアンドドロップポリシーは無効になっています。必要に応じて、このポリシーを有効にすることができます。

アプリケーションの起動待機タイムアウト

この設定では、セッションで最初のアプリケーションの起動を待機する待機タイムアウトの値をミリ秒単位で指定します。この時間を超えた後にアプリケーションが起動されると、セッションは終了します。

デフォルトの時間（10,000 万ミリ秒）を選択するか、数値をミリ秒単位で指定できます。

クライアントクリップボードリダイレクト

この設定項目では、クライアント側のクリップボードをサーバーのクリップボードにマップすることを許可または禁止します。

デフォルトでは許可されます。

セッションとローカルのクリップボード間でデータを転送できなくするには、[禁止] を選択します。ただし、セッション内で動作するアプリケーション間でのクリップボードを介したデータ転送は無効になりません。

[許可] に設定した場合は、クライアント接続でクリップボードが使用できる最大帯域幅を構成します。これには、[クリップボードリダイレクトの最大帯域幅（**Kbps**）] 設定または [クリップボード リダイレクトの最大帯域幅（**%**）] を使用します。

クライアントクリップボードに書き込みを許可する形式

[クライアントクリップボードの書き込み制限] が [有効] に設定されている場合、ホスト側のクリップボードデータはクライアントエンドポイント側に共有されません。この [クライアント クリップボードに書き込みを許可する形式]

設定では、特定の種類のクリップボードデータの共有を許可します。これを行うには、この設定項目を有効にして、許可するデータ形式を追加します。

以下のシステム定義のクリップボードデータ形式を追加できます。

- CF_TEXT
- CF_BITMAP
- CF_METAFILEPICT
- CF_SYLK
- CF_DIF
- CF_TIFF
- CF_OEMTEXT
- CF_DIB
- CF_PALETTE
- CF_PENDATA
- CF_RIFF
- CF_WAVE
- CF_UNICODETEXT
- CF_ENHMETAFILE
- CF_HDROP
- CF_LOCALE
- CF_DIBV5
- CF_OWNERDISPLAY
- CF_DSPTEXT
- CF_DSPBITMAP
- CF_DSPMETAFILEPICT
- CF_DISPENHMETAFILE
- CF_HTML

また、以下の XenApp および XenDesktop、Citrix Virtual Apps and Desktops 用のカスタム定義のデータ形式を追加できます:

- CFX_RICHTEXT
- CFX_OfficeDrawingShape
- CFX_BIFF8
- CFX_FILE

HTML 形式はデフォルトでは無効になっています。この機能を有効にするには:

- [クライアントクリップボードリダイレクト] が [許可] に設定されていることを確認します。
- [クライアントクリップボードの書き込み制限] が [有効] に設定されていることを確認します。
- [クライアントクリップボードに書き込みを許可する形式] で、[**CF_HTML**]（およびサポートを希望するほかの形式）のエントリを追加します。

カスタム定義のデータ形式を追加できます。この場合、データ形式の名前がシステムに登録されたものと一致する必要があります。また、形式名の大文字と小文字は区別されます。

［クライアントクリップボードリダイレクト］ポリシーで ［禁止］が設定されている場合、または ［クライアントクリップボードの書き込み制限］ポリシーで ［無効］が設定されている場合、この設定項目は無視されます。

> 注:
>
> HTML 形式のクリップボードコピーのサポート（CF_HTML）を有効にすると、コピーされたコンテンツのソースに含まれるあらゆるスクリプトが、コピー先にコピーされます。コピーを実行する前に、ソースの信頼性を確認してください。スクリプトを含むコンテンツをコピーする場合、コピー先のファイルを HTML ファイルとして保存して実行する場合に限り、ライブになります。

クリップボードのクライアントからセッションへの転送サイズを制限する

この設定項目では、コピーして貼り付ける 1 回の操作でクライアントエンドポイントから仮想セッションに転送できるクリップボードデータの最大サイズを指定します。

クリップボード転送サイズを制限するには、［クリップボードのクライアントからセッションへの転送サイズを制限する］設定を有効にします。次に、［サイズ制限］フィールドに、ローカルクリップボードとセッション間のデータ転送のサイズを定義する値をキロバイト単位で入力します。

デフォルトでは、この設定は無効になっており、クライアントからセッションへの転送に制限はありません。

HDX Direct

HDX Direct を使用すると、直接通信が利用できる場合、クライアントはセッションホストへの直接接続を自動的に確立できます。接続はネットワークレベルの暗号化を使用してセキュアに確立されます。

HDX Direct モード

HDX Direct を使用すると、内部および外部クライアントのセッションホストとの直接接続を確立できます。この設定は、HDX Direct を内部クライアントのみで使用可能にするか、内部クライアントと外部クライアントの両方で使用可能にするかを決定します。

内部のみに設定すると、HDX Direct は内部ネットワーク内のクライアントに対してのみ直接接続を確立しようとします。

内部および外部に設定すると、HDX Direct は内部および外部クライアントに対して直接接続を確立しようとします。

デフォルトでは、HDX Direct は内部クライアントのみに設定されています。

HDX Direct のポート範囲

このポート範囲は、外部ユーザーへの接続に HDX Direct で使用されます。
デフォルトでは、HDX Direct はポート範囲 55000～55250 を使用します。

クリップボードのセッションからクライアントへの転送サイズを制限する

この設定項目では、コピーして貼り付ける 1 回の操作で仮想セッションからクライアントエンドポイントに転送できるクリップボードデータの最大サイズを指定します。

クリップボード転送サイズを制限するには、[クリップボードのセッションからクライアントへの転送サイズを制限する] 設定を有効にします。次に、[サイズ制限] フィールドに、セッションとローカルクリップボード間のデータ転送のサイズを定義する値をキロバイト単位で入力します。

デフォルトでは、この設定は無効になっており、セッションからクライアントへの転送に制限はありません。

クライアントクリップボードの書き込み制限

この設定項目を [有効] に設定すると、ホスト側のクリップボードデータがクライアントエンドポイント側に共有されなくなります。この場合、特定のデータの共有を許可するには、[クライアントクリップボードに書き込みを許可する形式] 設定を使用します。

デフォルトでは、この設定は [無効] になっています。

セッションクリップボードの書き込み制限

この設定項目を [有効] に設定すると、クライアント側のクリップボードデータがユーザーセッション側に共有されなくなります。この場合、特定のデータの共有を許可するには、[セッションクリップボードに書き込みを許可する形式] 設定を使用します。

デフォルトでは、この設定は [無効] になっています。

セッションクリップボードに書き込みを許可する形式

[セッションクリップボードの書き込み制限] 設定が [有効] の場合、クライアント側のクリップボードデータはセッション内のアプリケーション側に共有されません。この [セッション クリップボードに書き込みを許可する形式] 設定では、特定の種類のクリップボードデータの共有を許可します。

以下のシステム定義のクリップボードデータ形式を追加できます。

- CF_TEXT
- CF_BITMAP

- CF_METAFILEPICT
- CF_SYLK
- CF_DIF
- CF_TIFF
- CF_OEMTEXT
- CF_DIB
- CF_PALETTE
- CF_PENDATA
- CF_RIFF
- CF_WAVE
- CF_UNICODETEXT
- CF_ENHMETAFILE
- CF_HDROP
- CF_LOCALE
- CF_DIBV5
- CF_OWNERDISPLAY
- CF_DSPTEXT
- CF_DSPBITMAP
- CF_DSPMETAFILEPICT
- CF_DISPENHMETAFILE
- CF_HTML

また、以下の XenApp および XenDesktop、Citrix Virtual Apps and Desktops 用のカスタム定義のデータ形式を追加できます:

- CFX_RICHTEXT
- CFX_OfficeDrawingShape
- CFX_BIFF8

HTML 形式はデフォルトでは無効になっています。この機能を有効にするには:

- [クライアントクリップボードリダイレクト] が [許可] に設定されていることを確認します。
- [セッションクリップボードの書き込み制限] が [有効] に設定されていることを確認します。
- [セッションクリップボードに書き込みを許可する形式] で、[**CF_HTML**]（およびサポートを希望するほかの形式）のエントリを追加します。

カスタム定義のデータ形式を追加できます。この場合、データ形式の名前がシステムに登録されたものと一致する必要があります。また、形式名の大文字と小文字は区別されます。

[クライアントクリップボードリダイレクト] ポリシーで [禁止] が設定されている場合、または [セッションクリップボードの書き込み制限] ポリシーで [無効] が設定されている場合、この設定項目は無視されます。

> 注:
>
> HTML 形式のクリップボードコピーのサポート（CF_HTML）を有効にすると、コピーされたコンテンツのソースに含まれるあらゆるスクリプトが、コピー先にコピーされます。コピーを実行する前に、ソースの信頼性を確認してください。スクリプトを含むコンテンツをコピーする場合、コピー先のファイルを HTML ファイルとして保存して実行する場合に限り、ライブになります。

デスクトップを起動する

この設定により、VDA の Direct Access Users グループの非管理者ユーザーによる ICA コネクションでの VDA 上セッションへの接続を許可または禁止します。

デフォルトでは、管理者以外のユーザーはこれらのセッションに接続できません。

この設定は、RDP 接続を使用している VDA の Direct Access Users グループの非管理者ユーザーには影響がありません。これらのユーザーは、この設定が有効または無効になっている場合、VDA に接続できます。この設定は、VDA の Direct Access Users グループではない非管理者ユーザーには影響がありません。これらのユーザーは、この設定が有効または無効になっている場合、VDA に接続できます。

FIDO2 リダイレクト

この設定では、FIDO2 リダイレクトを有効または無効にします。FIDO2 リダイレクトにより、ユーザーは仮想マシンでローカルエンドポイントの FIDO2 コンポーネントを利用できます。ユーザーは、TPM 2.0 および Windows Hello を搭載したデバイスで FIDO2 セキュリティキーまたは統合された生体認証を使用して、仮想セッションを認証できます。

この設定が ［許可］の場合、ユーザーはローカルエンドポイント機能を使用して FIDO2 認証を行うことができます。デフォルトでは、［許可］に設定されています。

ICA リスナー接続タイムアウト

この設定では、ICA プロトコルによる接続が完了するまでの最大待機時間を指定します。

デフォルトの最大待機時間は、120,000 ミリ秒（2 分）です。

ICA リスナーポートの番号

この設定では、サーバー上の ICA プロトコルで使用される TCP/IP ポートを指定します。

デフォルトのポート番号は、1494 に設定されています。

ほかのポートを指定する場合は、0 から 65535 の範囲で、ほかのウェルノウンポート番号と競合しない番号を使用してください。変更したポート番号を有効にするには、サーバーを再起動する必要があります。サーバー上のポート番

号を変更した場合は、そのサーバーに接続する Citrix Workspace アプリやプラグインソフトウェア側でもポート番号を変更する必要があります。

キーボードと入力システム（**IME**）

この設定により、以下を有効または無効にできます:

- 動的なキーボードレイアウトの同期
- 入力システム（IME）
- Unicode キーボードレイアウトマッピング
- キーボードレイアウトの切り替え通知ダイアログメッセージを表示または非表示にする

1. Web Studio で ［キーボードと **IME**］を選択します。
2. VDA の動的キーボードレイアウト同期機能と汎用クライアント入力システム（IME）機能を制御するには、［クライアントキーボードレイアウトの同期と **IME** の改善］を選択します。以下の項目を構成できます。

   無効 - 動的なキーボードレイアウト同期と汎用クライアント入力システム（IME）。

   動的クライアントキーボードレイアウト同期をサポート - 動的キーボードレイアウト同期を有効にします。

   動的クライアントキーボードレイアウトの同期と **IME** の改善をサポート -動的キーボードレイアウトの同期と汎用クライアント入力システム（IME）の両方を有効にします。
3. Unicode キーボードマッピングを有効または無効にするには、［**Unicode** キーボードレイアウトマッピングを有効にする］を選択します。
4. ユーザーがクライアントのキーボードレイアウトを変更したときに、キーボードレイアウトが同期中であることをメッセージで表示するかを制御するには、［キーボードレイアウトの切り替えポップアップメッセージを非表示にする］を選択します。このメッセージが表示されないようにすると、ユーザーは誤った文字入力を避けるために、入力前にしばらく待つ必要があります。

デフォルト設定:

- クライアントキーボードレイアウトの同期と **IME** の改善
  - Windows Server 2016 と Windows Server 2019 では無効。
  - Windows Server 2012 および Windows 2010 での動的なクライアントキーボードレイアウトの同期と IME の改善をサポートします。
- **Unicode** キーボードレイアウトのマッピングを無効にします。
- キーボードレイアウトの切り替えポップアップメッセージを表示します。

このポリシーは、ポリシー設定の ［説明］セクションに一覧表示されているレジストリ設定を置き換えます。

ログオフチェッカー起動遅延

この設定では、ログオフチェッカー起動の遅延時間を指定します。このポリシーを使用して、クライアントセッションがセッション切断を待機する時間（秒単位）を設定します。

この設定により、ユーザーがサーバーからログオフするのにかかる時間を長くすることもできます。

損失耐性モード

> 重要:
>
> - この機能は、Windows 向け Citrix Workspace アプリ 2002 以降が必要です。利用可能になった際、VDA のこのバージョンでサポートされます。
> - グラフィックの損失耐性モードは、Citrix Gateway および Citrix Gateway サービスでサポートされています。このモードでは、直接接続でのみ使用可能です。

この設定は、グラフィックの損失耐性のモードを有効または無効にします。

デフォルトでは、グラフィックの損失耐性のモードは ［許可］になっています。

許可の場合、パケット損失および遅延がしきい値を超えると、このモードに移行します。損失耐性モードのしきい値ポリシーを使用してしきい値を設定できます。

損失耐性モードのしきい値

損失耐性モードを使用できる場合、この設定はセッションがグラフィックの損失耐性モードに切り替わるネットワーク指標のしきい値を指定します。

デフォルトのしきい値は次のとおりです:

- パケット損失：5%
- 遅延：300 ミリ秒（RTT）

詳しくは、「損失耐性モード」を参照してください。

オーディオの損失耐性モード

この設定は、オーディオの損失耐性モードを有効または無効にします。

有効にすると、オーディオは損失耐性モードで送信されます。

デフォルトでは、オーディオの損失耐性モードは **Prohibited** になっています。

ポリシーを有効にするには、オーディオポリシーの損失耐性モードのレジストリを **Allowed** に変更します。

オーディオの損失耐性モードを有効にするには、EDT トランスポートが必要です。

Rendezvous プロトコル

この設定により、Citrix Gateway Service の使用時に HDX セッションがプロキシ接続される方法が変更されます。この設定を有効にすると、HDX トラフィックは Citrix Cloud Connector を経由しなくなります。代わりに、VDA の発信接続は、Citrix Gateway サービスに対して直接確立されるようになります（Cloud Connector のスケーラビリティが向上します）。

> 重要:
>
> Citrix Cloud のフィーチャートグルと HDX ポリシー設定により、この機能が制御されます。HDX 設定はデフォルトで無効ですが、Citrix Cloud の機能トグルはデフォルトで有効になっています。HDX 設定の影響を受けるのは、Citrix Gateway サービスを介して確立された HDX セッションのみです。クライアントと VDA との間で直接確立されたセッション、またはオンプレミス Citrix Gateway 経由のセッションは、この設定の影響を受けません。

詳しくは、「Rendezvous プロトコル」を参照してください。

Rendezvous プロキシの構成

この設定により、Rendezvous プロトコルで使用する明示的なプロキシを構成できます。透過プロキシを使用する場合は、この設定を有効にする必要はありません。

デフォルトでは、この設定は無効になっています。

無効にすると、VDA は、Gateway サービスとの Rendezvous 接続を確立しようとしたときに、非透過プロキシを介して送信トラフィックをルーティングしません。

有効にすると、VDA は、この設定で定義したプロキシを介して Gateway サービスとの Rendezvous 接続を確立しようとします。

VDA は、Rendezvous 接続での HTTP プロキシおよび SOCKS5 プロキシの使用をサポートしています。Rendezvous 接続にプロキシを使用するよう VDA を構成するには、この設定を有効にする必要があります。また、プロキシのアドレスまたは PAC ファイルへのパスのいずれかを指定します。例:

- プロキシアドレス: `http://<URL or IP>:<port>` または `socks5://<URL or IP>:<port>`
- PAC ファイル: `http://<URL or IP>/<path>/<filename>.pac`

  VDA バージョン 2103 は、PAC ファイルを使用したプロキシ構成でサポートされている最小バージョンです。SOCKS5 プロキシの PAC ファイルスキーマについて詳しくは、「プロキシ構成」を参照してください。

> 注:
>
> EDT を介したデータ転送をサポートしているのは、SOCKS5 プロキシのみです。HTTP プロキシの場合、ICA のトランスポートプロトコルとして TCP を使用します。

詳しくは、「Rendezvous プロトコル」を参照してください。

クライアント接続での非公開アプリケーションの起動

この設定項目では、サーバー上のリモートデスクトッププロトコルを介した開始アプリケーションの起動を許可するかどうかを指定します。

デフォルトでは、サーバー上のリモートデスクトッププロトコルを介した開始アプリケーションの起動は許可されません。

セッションメトリックの収集

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

Citrix は、オペレーティングシステム、稼働時間、コンピューターシステム情報、ビデオコントローラの詳細、VDA のバージョン、展開の種類、ドメイン参加のステータスなどのデータを収集します。さらに、パフォーマンスと信頼性のデータとともにいくつかのセッション構成を収集して、製品の品質向上に役立てることもできます。カスタマーエクスペリエンス向上プログラムについて詳しくは、以下を参照してください:

- https://more.citrix.com/XD-CEIP
- https://docs.citrix.com/en-us/linux-virtual-delivery-agent/current-release/configure/administration/linux-vda-data-collection-program
- https://docs.citrix.com/en-us/mac-vda/configure/session/supportability-service

デフォルトでは、有効になっています。

タブレットモードの切り替えのポリシー設定

タブレットモードの切り替えでは、VDA 上でのストアアプリ、Win32 アプリ、および Windows シェルの外観と動作を最適化します。これは、電話やタブレット（またはタッチ対応デバイス）などの小型のフォームファクタデバイスから接続するときに、仮想デスクトップからタブレットモードに自動的に切り替えることによって行われます。

このポリシーを無効にすると、VDA はクライアントの種類に関係なく、ユーザーが設定したモードになり、ずっと同じモードを維持します。

クライアントの自動再接続のポリシー設定

August 17, 2024

［クライアントの自動再接続］カテゴリには、セッションの自動再接続の制御に関するポリシー設定項目が含まれています。

クライアントの自動再接続

この設定では、接続が中断した後で同じクライアントから自動再接続することを許可または禁止します。

Citrix Receiver for Windows 4.7 以降および Citrix Workspace アプリ 1808 以降のクライアントの自動再接続では、Citrix Studio からのポリシー設定のみを使用します。Studio でこれらのポリシーを更新すると、サーバーからクライアントにクライアントの自動再接続が同期されます。以前のバージョンの Citrix Receiver for Windows では、クライアントの自動再接続を構成するのには、Studio ポリシーを使用してレジストリまたは default.ica ファイルを変更します。

クライアントの自動再接続を許可すると、ユーザーは接続が切断された時点の状態に戻って作業を再開できます。自動再接続機能では、切断された接続が検出されてそのセッションにユーザーが再接続されます。

セッション ID と資格情報のキーが含まれている Citrix Workspace アプリの Cookie を使用していない場合は、自動再接続によって新しいセッションが開始されることがあります。つまり、既存のセッションに再接続されるのではありません。有効期限が切れている場合、Cookie は使用されません。たとえば、再接続に時間がかかって Cookie の有効期限が切れた場合や、ユーザーが資格情報を再入力する必要がある場合です。また、ユーザーが自分で切断した場合、クライアントの自動再接続はトリガーされません。

再接続中は、セッションウィンドウが灰色になります。セッションを再接続するまでの残り時間がカウントダウンタイマーで表示されます。セッションがタイムアウトになると、接続は切断されます。

アプリケーションセッションで自動再接続が許可されている場合は、カウントダウンタイマーが通知領域に表示されます。セッションを再接続するまでの残り時間がカウントダウンタイマーで表示されます。Citrix Workspace アプリによる再接続は、接続に成功するかユーザーがキャンセルするまで繰り返し試行されます。

ユーザーセッションでは、自動再接続が許可されている場合、Citrix Workspace アプリは、指定された時間、接続に成功するかユーザーがキャンセルするまで再接続を繰り返し試行します。デフォルトでは、この時間は 2 分です。この期間を変更するには、ポリシーを編集します。

デフォルトでは、クライアントの自動再接続が許可されます。ポリシーを ［禁止］に設定することで無効にできます。

クライアントの自動再接続時の認証

この設定では、自動再接続時に認証処理を必要とするかどうかを指定します。［認証を必要とする］を選択すると、クライアントの自動再接続時に認証のためのダイアログボックスが開きます。

ユーザーが最初にログオンすると、そのユーザーの資格情報は暗号化されてメモリに格納され、その暗号キーを含んだ Cookie が作成されます。この Cookie は Citrix Workspace アプリに送信されます。この設定を構成すると、Cookie は使用されなくなります。その代わりに、Citrix Workspace アプリが切断セッションに再接続するときに、ユーザーの資格情報を入力するためのダイアログボックスが開きます。

デフォルトでは、認証は要求されません。

クライアントの自動再接続のログ

この設定では、クライアントの自動再接続イベントをログに記録するかどうかを制御します。

ログを有効にすると、サーバーのシステムログに自動再接続の成功および失敗イベントが記録されます。これらのイベントは、そのイベントが発生した個々のサーバーのシステムログに記録されます。

デフォルトでは、ログは無効になっています。

クライアントの自動再接続のタイムアウト

デフォルトでは、クライアントの自動再接続タイムアウトは 120 秒に設定されます。自動クライアント接続の構成可能なタイムアウトの最大値は 300 秒です。このポリシーを使用して、タイムアウト値を設定します。

再接続 **UI** の透過レベル

この設定では、セッション画面の保持の再接続時に、XenApp または XenDesktop のセッションウィンドウに適用される不透明度レベルを指定できます。

デフォルトでは、再接続 UI の透明度は、80 に設定されています。

オーディオのポリシー設定

August 17, 2024

[オーディオ] カテゴリには、ユーザーデバイスがパフォーマンスを低下させずにセッションでオーディオを送受信することを許可するための設定項目が含まれています。

アダプティブオーディオ

この設定により、アダプティブオーディオを有効または無効にします。このポリシーを有効にすると、最良のユーザーエクスペリエンスを提供するように音質設定が動的に調整されます。この設定は、Citrix Virtual Apps and Desktops 2109 以降を使用する VDA のシングルセッション OS セッションとマルチセッション OS セッションの両方に適用されます。

この設定が禁止されている場合は、音質ポリシーが適用されます。詳しくは、「音質」を参照してください。

デフォルトでは、アダプティブオーディオポリシーは有効になっています。

UDP でのオーディオリアルタイムトランスポート

この設定では、ホストとユーザーデバイス間のユーザーデータグラムプロトコル（UDP）を使用したオーディオリアルタイムトランスポート（RTP）でのオーディオ転送を許可または禁止します。この設定を無効にすると、オーディオが TCP 上で送受信されます。

デフォルトでは許可されます。

オーディオプラグアンドプレイ

この設定では、録音やサウンド再生のための複数のオーディオデバイスの使用を許可または禁止します。

デフォルトでは許可されます。

この設定項目は、Windows マルチセッション OS マシンのみに適用されます。

音質

この設定では、ユーザーセッション内で受信されるサウンドの品質を指定します。

デフォルトでは、［高 - 高品位オーディオ］が指定されています。

音質を制御するには、次のオプションから 1 つを選択します。

- 狭帯域接続には［低 - 低速接続用］を選択します。この設定では、サウンドデータが最大 16Kbps まで圧縮されてから転送されます。この圧縮により、音質が大幅に低下します。ただし、低帯域幅の接続でも妥当なパフォーマンスが得られます。
- ［中］を選択 - スピーチ用に最適化され、ボイスオーバー IP アプリケーションを配信します。512Kbps 未満の低速なネットワーク接続回線でメディアアプリケーションを配信する場合、または輻輳やパケット損失が生じる環境では、［中］を選択します。高速にエンコーディングされるため、ソフトフォンや統合コミュニケーションアプリケーションなどのメディア処理をサーバー側で行う場合に適しています。

  この設定では、オーディオデータが最大 64Kbps まで圧縮されてからユーザーデバイスに転送されます。この圧縮により、ユーザーデバイス上でのオーディオ再生の品質はやや低下しますが、遅延は少なくなり、帯域幅の消費も少なくなります。ボイスオーバー IP アプリケーションで十分な音質が得られない場合は、［UDP でのオーディオリアルタイムトランスポート］設定で［許可］を選択します。

  現在、この音質が設定されている場合のみ、UDP 上のリアルタイムトランスポート（RTP）がサポートされています。この音質は、低速なネットワーク接続（512Kbps 未満）でメディアアプリケーションを配信するときに使用します。また、ネットワークに輻輳やパケット損失がある場合に使用します。
- 帯域幅が十分で、サウンドの音質が重要である場合は、［高 - 高品位オーディオ］を選択します。この設定では、ネイティブのサウンドデータを再生または録音できます。サウンドデータは、CD レベルの音質が維持される 112Kbps の高品質レベルで圧縮されます。ただし、大量のネットワークデータ転送が要求されるため、CPU およびネットワークに負担がかかる場合があります。

録音と再生を同時に行った場合、消費帯域幅は 2 倍になります。

帯域幅の上限を指定するには、［オーディオリダイレクトの最大帯域幅（**Kbps**）］設定または ［オーディオリダイレクトの最大帯域幅（**%**）］設定を使用します。

クライアントオーディオリダイレクト

この設定では、サーバーでホストされているアプリケーションから、ユーザーデバイスにインストールされているサウンドデバイスを介してサウンドを再生したり、オーディオ入力を録音したりすることを許可または禁止します。

デフォルトでは許可されます。

この設定を許可したら、オーディオの再生や録音で使用できる帯域幅の上限を設定します。これにより、アプリケーションのパフォーマンスが向上しますが、音質が低下することがあります。録音と再生を同時に行った場合、消費帯域幅は 2 倍になります。帯域幅の上限を指定するには、［オーディオリダイレクトの最大帯域幅（**Kbps**）］設定または ［オーディオリダイレクトの最大帯域幅（**%**）］設定を使用します。

Windows マルチセッション OS マシンで複数のオーディオデバイスをサポートするには、［オーディオプラグアンドプレイ］設定がオンになっていることも確認してください。

重要:［クライアントオーディオリダイレクト］設定で［禁止］を選択すると、すべての HDX オーディオ機能が無効になります。

クライアントマイクリダイレクト

この設定では、クライアント側のマイクのリダイレクトを有効または無効にします。この設定を有効にすると、セッション内でクライアント側のマイクを使ってオーディオを録音できるようになります。

デフォルトでは許可されます。

セキュリティの設定により、ユーザーデバイスに信頼されていないサーバーからユーザーデバイス側のマイクにアクセスしたときに、警告メッセージが表示されます。ユーザーは、このメッセージに対してアクセスを許可したり拒否したりできます。この警告は、ユーザーが Citrix Workspace アプリ側で無効にできます。

Windows マルチセッション OS マシンで複数のオーディオデバイスをサポートするには、［オーディオプラグアンドプレイ］設定で［有効］が選択されていることも確認してください。

ユーザーデバイス側で ［クライアントオーディオリダイレクト］設定が無効になっている場合、この設定は無視されます。

帯域幅のポリシー設定

August 17, 2024

［帯域幅］カテゴリには、クライアントセッションでの消費帯域幅に関する問題を避けるための設定項目が含まれています。

重要：これらのポリシー設定を ［マルチストリーム］設定と一緒に使用すると、意図したとおりに動作しなくなる場合があります。ポリシーで［マルチストリーム］設定を使用する場合は、帯域幅を制限するポリシー設定を追加しないようにしてください。

オーディオリダイレクトの最大帯域幅（**Kbps**）

この設定では、クライアント側デバイスによるオーディオの再生や録音で使用可能な最大帯域幅を指定します。最大帯域幅は、キロビット/秒（Kbps）で指定されます。

デフォルトでは、上限なし（0）が指定されています。

この設定および ［オーディオリダイレクトの最大帯域幅（**%**）］設定の両方を指定した場合、より高い制限（より小さい値）の設定が適用されます。

オーディオリダイレクトの最大帯域幅（**%**）

この設定では、クライアント側デバイスによるオーディオの再生や録音で使用可能な最大帯域幅を、セッション全体に対する割合で指定します。

デフォルトでは、上限なし（0）が指定されています。

この設定および ［オーディオリダイレクトの最大帯域幅（**Kbps**）］設定の両方を指定した場合、より高い制限（より小さい値）の設定が適用されます。

この設定を使用する場合は、セッションで使用可能な総帯域幅の最大値を指定する ［セッション全体の最大帯域幅］設定も使用する必要があります。

USB デバイスリダイレクトの最大帯域幅（**Kbps**）

この設定項目では、クライアント側の USB デバイスにアクセスするときに使用可能な最大帯域幅を指定します。最大帯域幅は、キロビット/秒（Kbps）で指定されます。

デフォルトでは、上限なし（0）が指定されています。

この設定および ［**USB** デバイスリダイレクトの最大帯域幅（**%**）］設定の両方を指定した場合、より高い制限（より小さい値）の設定が適用されます。

USB デバイスリダイレクトの最大帯域幅（**%**）

この設定では、クライアント側の USB デバイスにアクセスするときに使用可能な最大帯域幅を、セッション全体に対する割合で指定します。

デフォルトでは、上限なし（0）が指定されています。

この設定および［**USB** デバイスリダイレクトの最大帯域幅（**Kbps**）］設定の両方を指定した場合、より高い制限（より小さい値）の設定が適用されます。

この設定を使用する場合は、セッションで使用可能な総帯域幅の最大値を指定する ［セッション全体の最大帯域幅］設定も使用する必要があります。

クリップボードリダイレクトの最大帯域幅（**Kbps**）

この設定項目では、セッションとローカルのクリップボード間でのデータ転送で使用可能な最大帯域幅を指定します。最大帯域幅は、キロビット/秒（Kbps）で指定されます。

デフォルトでは、上限なし（0）が指定されています。

この設定および［クリップボードリダイレクトの最大帯域幅（**%**）］設定の両方を指定した場合、より高い制限（より小さい値）の設定が適用されます。

クリップボードリダイレクトの最大帯域幅（**%**）

この設定項目では、セッションとローカルのクリップボード間でのデータ転送で使用可能な最大帯域幅を、セッション全体に対する割合で指定します。

デフォルトでは、上限なし（0）が指定されています。

この設定および ［クリップボードリダイレクトの最大帯域幅（**Kbps**）］設定の両方を指定した場合、より高い制限（より小さい値）の設定が適用されます。

この設定を使用する場合は、セッションで使用可能な総帯域幅の最大値を指定する ［セッション全体の最大帯域幅］設定も使用する必要があります。

COM ポートリダイレクトの最大帯域幅 **(Kbps)**

注: Virtual Delivery Agent 7.0～7.8 では、レジストリを使ってこの設定を構成します。「レジストリを使った COM ポートおよび LPT ポートリダイレクト設定の構成」を参照してください。

この設定では、クライアント側 COM ポートにアクセスするときに使用可能な最大帯域幅を、キロビット/秒（Kbps）単位で指定します。この設定および ［**COM** ポートリダイレクトの最大帯域幅（**%**）］設定の両方を指定した場合、より高い制限（より小さい値）の設定が適用されます。

COM ポートリダイレクトの最大帯域幅（**%**）

注: Virtual Delivery Agent 7.0～7.8 では、レジストリを使ってこの設定を構成します。「レジストリを使った COM ポートおよび LPT ポートリダイレクト設定の構成」を参照してください。

この設定では、クライアント側 COM ポートにアクセスするときに使用可能な最大帯域幅を、セッション全体に対する割合で指定します。

デフォルトでは、上限なし（0）が指定されています。

この設定および［**COM** ポートリダイレクトの最大帯域幅（**Kbps**）］設定の両方を指定した場合、より高い制限（より小さい値）の設定が適用されます。

この設定を使用する場合は、セッションで使用可能な総帯域幅の最大値を指定する ［セッション全体の最大帯域幅］設定も使用する必要があります。

ファイルリダイレクトの最大帯域幅（**Kbps**）

この設定では、クライアント側ドライブにアクセスするときに使用可能な最大帯域幅を指定します。最大帯域幅は、キロビット/秒（Kbps）で指定されます。

デフォルトでは、上限なし（0）が指定されています。

この設定および［ファイルリダイレクトの最大帯域幅（**%**）］設定の両方を指定した場合、より高い制限（より小さい値）の設定が適用されます。

ファイルリダイレクトの最大帯域幅（**%**）

この設定では、クライアント側ドライブにアクセスするときに使用可能な最大帯域幅を、セッション全体に対する割合で指定します。

デフォルトでは、上限なし（0）が指定されています。

この設定および［ファイルリダイレクトの最大帯域幅（**Kbps**）］の両方を指定した場合、より高い制限（より小さい値）の設定が適用されます。

この設定を使用する場合は、セッションで使用可能な総帯域幅の最大値を指定する ［セッション全体の最大帯域幅］設定も使用する必要があります。

HDX MediaStream マルチメディアアクセラレーションの最大帯域幅

この設定では、HDX MediaStream マルチメディアアクセラレーションによりストリーム配信されるオーディオやビデオで使用可能な最大帯域幅を指定します。最大帯域幅は、キロビット/秒（Kbps）で指定されます。

デフォルトでは、上限なし（0）が指定されています。

この設定および［**HDX MediaStream** マルチメディアアクセラレーションの最大帯域幅（**%**）］設定の両方を指定した場合、より高い制限（より小さい値）の設定が適用されます。

HDX MediaStream マルチメディアアクセラレーションの最大帯域幅（**%**）

この設定では、HDX MediaStream マルチメディアアクセラレーションによりストリーム配信されるオーディオやビデオで使用可能な最大帯域幅を、セッション全体に対する割合で指定します。

デフォルトでは、上限なし（0）が指定されています。

この設定および［**HDX MediaStream** マルチメディアアクセラレーションの最大帯域幅（**Kbps**）］設定の両方を指定した場合、より高い制限（より小さい値）の設定が適用されます。

この設定を使用する場合は、セッションで使用可能な総帯域幅の最大値を指定する ［セッション全体の最大帯域幅］設定も使用する必要があります。

LPT ポートリダイレクトの最大帯域幅（**Kbps**）

注: Virtual Delivery Agent 7.0～7.8 では、レジストリを使ってこの設定を構成します。「レジストリを使った COM ポートおよび LPT ポートリダイレクト設定の構成」を参照してください。

この設定では、クライアント側 LPT ポートを使用する印刷ジョブで使用可能な最大帯域幅を指定します。最大帯域幅は、キロビット/秒（Kbps）で指定されます。

デフォルトでは、上限なし（0）が指定されています。

この設定および ［**LPT** ポートリダイレクトの最大帯域幅（**%**）］設定の両方を指定した場合、より高い制限（より小さい値）の設定が適用されます。

LPT ポートリダイレクトの最大帯域幅（**%**）

注: Virtual Delivery Agent 7.0～7.8 では、レジストリを使ってこの設定を構成します。「レジストリを使った COM ポートおよび LPT ポートリダイレクト設定の構成」を参照してください。

この設定では、クライアント側 LPT ポートを使用する印刷ジョブで使用可能な最大帯域幅を、セッション全体に対する割合で指定します。

デフォルトでは、上限なし（0）が指定されています。

この設定および［**LPT** ポートリダイレクトの最大帯域幅（**Kbps**）］設定の両方を指定した場合、より高い制限（より小さい値）の設定が適用されます。

この設定を使用する場合は、セッションで使用可能な総帯域幅の最大値を指定する ［セッション全体の最大帯域幅］設定も使用する必要があります。

セッション全体の最大帯域幅

この設定では、セッションで使用可能な総帯域幅の最大値を、キロビット/秒（Kbps）単位で指定します。

適用できる帯域幅の上限は、20Mbps（20,000Kbps）です。デフォルトでは、上限なし（0）が指定されています。

狭帯域幅接続で、セッションでの使用帯域幅が原因でほかのアプリケーションでのデータ転送パフォーマンスが低下する場合に、この設定を使用します。

プリンターリダイレクトの最大帯域幅（**Kbps**）

この設定では、クライアント側プリンターにアクセスするときに使用可能な最大帯域幅を指定します。最大帯域幅は、キロビット/秒（Kbps）で指定されます。

デフォルトでは、上限なし（0）が指定されています。

この設定および［プリンターリダイレクトの最大帯域幅（**%**）］設定の両方を指定した場合、より高い制限（より小さい値）の設定が適用されます。

プリンターリダイレクトの最大帯域幅（**%**）

この設定では、クライアント側プリンターにアクセスするときに使用可能な最大帯域幅を、セッション全体に対する割合で指定します。

デフォルトでは、上限なし（0）が指定されています。

この設定および［プリンターリダイレクトの最大帯域幅（**Kbps**）］設定の両方を指定した場合、より高い制限（より小さい値）の設定が適用されます。

この設定を使用する場合は、セッションで使用可能な総帯域幅の最大値を指定する ［セッション全体の最大帯域幅］設定も使用する必要があります。

TWAIN デバイスリダイレクトの最大帯域幅（**Kbps**）

この設定では、クライアント側 TWAIN デバイスにアクセスするときに使用可能な最大帯域幅を指定します。最大帯域幅は、キロビット/秒（Kbps）で指定されます。

デフォルトでは、上限なし（0）が指定されています。

この設定および［**TWAIN** デバイスリダイレクトの最大帯域幅（**%**）］設定の両方を指定した場合、より高い制限（より小さい値）の設定が適用されます。

TWAIN デバイスリダイレクトの最大帯域幅（**%**）

この設定では、クライアント側 TWAIN デバイスにアクセスするときに使用可能な最大帯域幅を、セッション全体に対する割合で指定します。

デフォルトでは、上限なし（0）が指定されています。

この設定および［**TWAIN** デバイスリダイレクトの最大帯域幅（**Kbps**）］設定の両方を指定した場合、より高い制限（より小さい値）の設定が適用されます。

この設定を使用する場合は、セッションで使用可能な総帯域幅の最大値を指定する ［セッション全体の最大帯域幅］設定も使用する必要があります。

双方向のコンテンツリダイレクトのポリシー設定

August 17, 2024

［コンテンツの双方向リダイレクト］セクションには、クライアントから VDA および VDA からクライアントへの URL リダイレクトを有効にするか無効にするかのポリシー設定項目があります。

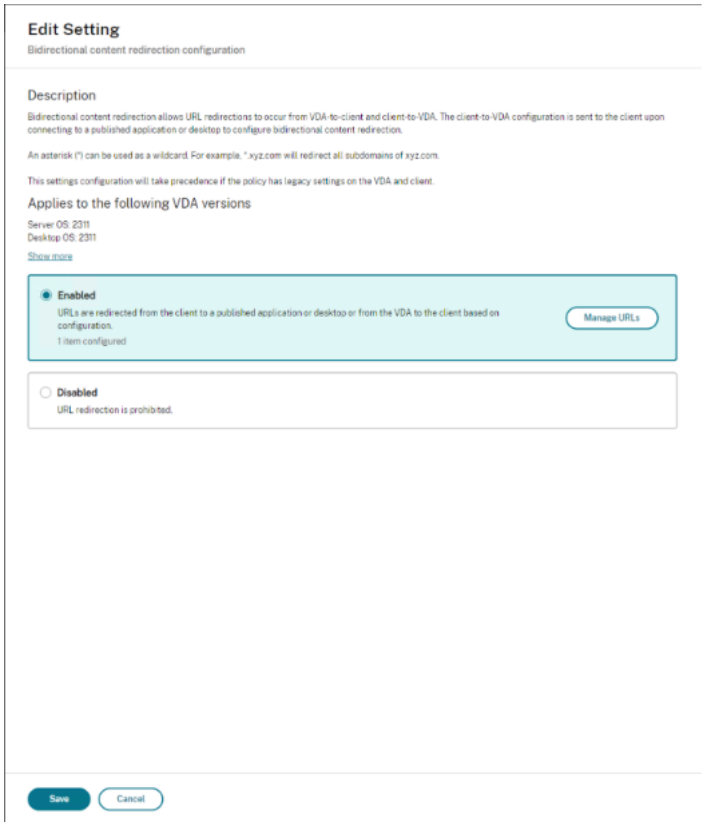
サーバーポリシーは Web Studio で設定されます。Citrix Workspace アプリのバージョン 2311 以降、この設定は Web Studio の廃止された次の 3 つの従来の設定を置き換えます:

- コンテンツの双方向リダイレクトを許可する
- VDA へのリダイレクトを許可する URL
- クライアントへのリダイレクトを許可する URL

また、Windows クライアント上の次の 3 つのローカルグループポリシーオブジェクト（GPO）設定も置き換えられます:

- コンテンツの双方向リダイレクト
- コンテンツの双方向リダイレクトでの上書き
- OAuth リダイレクト

この設定が有効になっている場合、公開アプリまたはデスクトップへの接続時にクライアントから VDA への設定が送信され、コンテンツの双方向リダイレクトが構成されます。



この設定が構成されている場合、Web Studio およびクライアントの従来の設定よりも優先されます。予期しない動作を避けるために、新しいポリシー設定のみを使用し、従来の設定は削除することをお勧めします。

VDA および Desktop Delivery Controller がバージョン 2311 以降を実行している場合は、クライアントポリシーを設定しないでください。または、クライアントポリシーを、Citrix Workspace アプリのグループポリシーオブジェクト管理用テンプレートで設定します。

Citrix は、ホストからクライアントへのリダイレクトと、クライアントから URL へのリダイレクトのためのローカルアプリアクセスを提供します。ただし、ドメイン参加済みの Windows クライアントについては、コンテンツの双方向リダイレクトを使用することをお勧めします。

Citrix は、Desktop Studio ではなく、Web Studio の新しい UI を使用して機能を構成することをお勧めします。

ワイルドカードリダイレクト

コンテンツの双方向リダイレクトでは、リダイレクトされる URL を定義するときにワイルドカードを使用できます。詳細とコンテンツの双方向リダイレクトを構成する方法については、「構成」手順を参照してください。
Web Studio で、`hostToClientUrls`配列または`clientToHostUrls`配列の`url`キーの値として JSON 文字列を編集して、ワイルドカード URL を設定します。

> 注:
>
> - 無限ループを避けるため、`hostToClientUrls`と`clientToHostUrls`に同じ URL を設定しないでください。
> - 最上位ドメインはサポートされていません。たとえば、https://www.citrix.*またはhttp://www.citrix.co*はリダイレクトされません。

コンテンツの双方向リダイレクトの構成

機能の構成を開始するには、このポリシーを`Enabled`に設定し、[**URL** を管理する] をクリックします。次の構成を設定します:

- **VDA** からクライアントへのリダイレクト
- クライアントから **VDA** へのリダイレクト

VDA からクライアントへのリダイレクト

VDA からクライアントに URL をリダイレクトするには、1 行に 1 つの URL を入力します。ワイルドカードを使用できます。
OAuth リダイレクトを使用すると、クライアントエンドポイントでブラウザーを使用して認証を実行し、トークンを VDA に送り返すことができます。

長所:

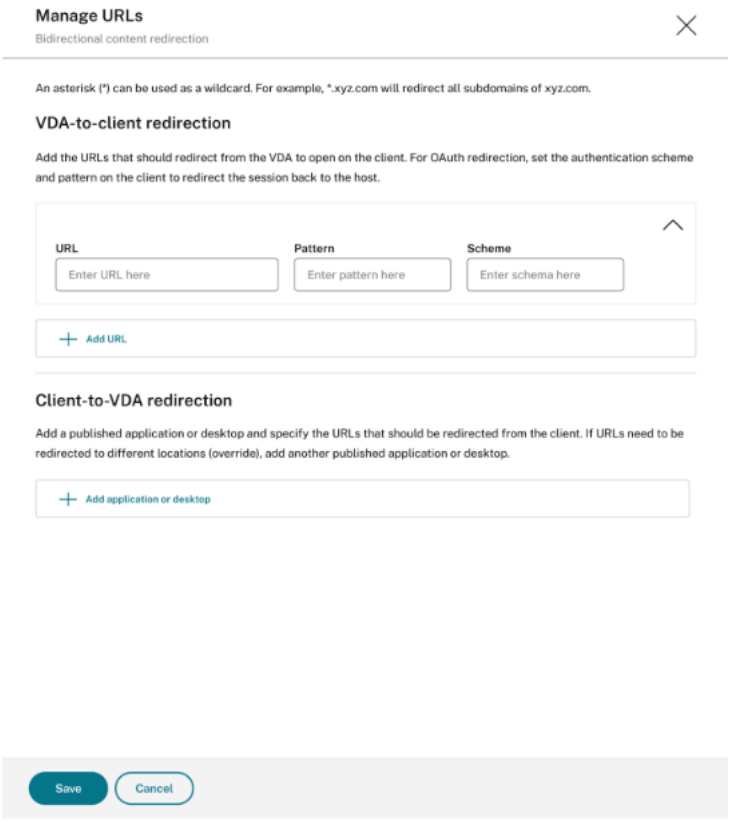
- これらの資格情報をホスト環境に保存するのを避けることができます。
- 利用可能な生体認証機能を、VDA ではなくエンドポイントで使用できます。

構成:

URL で VDA からクライアントへのリダイレクトを構成するには、以下を指定します:

- **URL**(必須):クライアントで開くために VDA からリダイレクトする URL を追加します。**OAuth** リダイレクトの場合、セッションをホストにリダイレクトするようにクライアントで認証スキームとパターンを設定します。
- パターン:(オプション)ホストからクライアントへの URL リダイレクトを介してクライアントにリダイレクトされると OAuth 認証フローが開始されたかのように追跡され、フローが完了すると(結果のスキームまたは開かれたリダイレクト URL パターンによって検出)、結果の URL がフローを開始したホスト VDA にリダイレクトされる URL 正規表現です。
- スキーム:(オプション)スキームが指定されている場合、終了 URL は「<`scheme`>://<`something`>」の形式である必要があります。スキームが指定されていない(空)とみなします。この場合、元の結果の URL パターンが正規表現キャプチャグループを介してパターンから抽出されます(パターンで指定されている必要があります)。元の URL は`citrix-oauth-redir:`//リダイレクト URL を使用するように書き換え

られます。フローが完了すると、元のリダイレクト URL がホスト（VDA）に再度リダイレクトされます。この場合、OAuth 認証サーバーは`citrix-oauth-redir://byIndex/1 (2, 3, ... N)`リダイレクト URL を許可するように設定する必要があります。

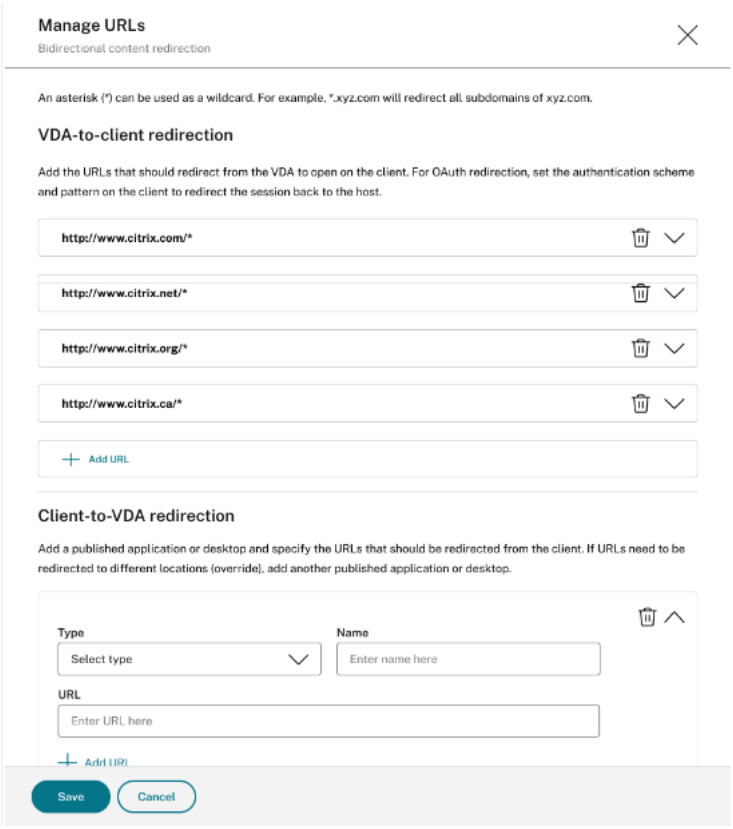


> 注:
>
> パターンとスキームはどちらもオプションですが、パターンが指定されている場合は、スキームも指定する必要があります。

クライアントから **VDA** へのリダイレクト

クライアントから VDA に URL をリダイレクトするには、次の手順を実行します:

1. クライアント URL のリダイレクト先を構成します。
2. 公開アプリケーションまたは公開デスクトップのいずれかを選択します。
3. そのリソースの名前を指定します。
4. そのリソースにリダイレクトする必要があるすべての URL を追加します。
   新しいアプリケーションまたはデスクトップを追加し、そのリソースにリダイレクトする URL を指定することにより、このデフォルトのリソースを上書きできます。



Desktop Studio

> 注:
>
> Citrix では、Citrix Virtual Apps and Desktops バージョン 2402 以降では、Web Studio を使用してこの機能を構成することをお勧めします。

2311 で双方向コンテンツリダイレクトを構成するには、次の形式で JSON 文字列を作成します:

```
{

  "version": 1,
  "hostToClientConfig": [
    {

      "hostToClientUrls": [
        {

          "url": "http://www.citrix.com/*"
        }
,
        {

          "url": "www.example.com"
        }
```



```
,
        {

          "url": "https://login.example.org/*",
          "oAuthRedirectionPattern": "https://login.example.org/oauth2
             ?.*",
          "oAuthScheme": "idm.desktop-authentication"
         }

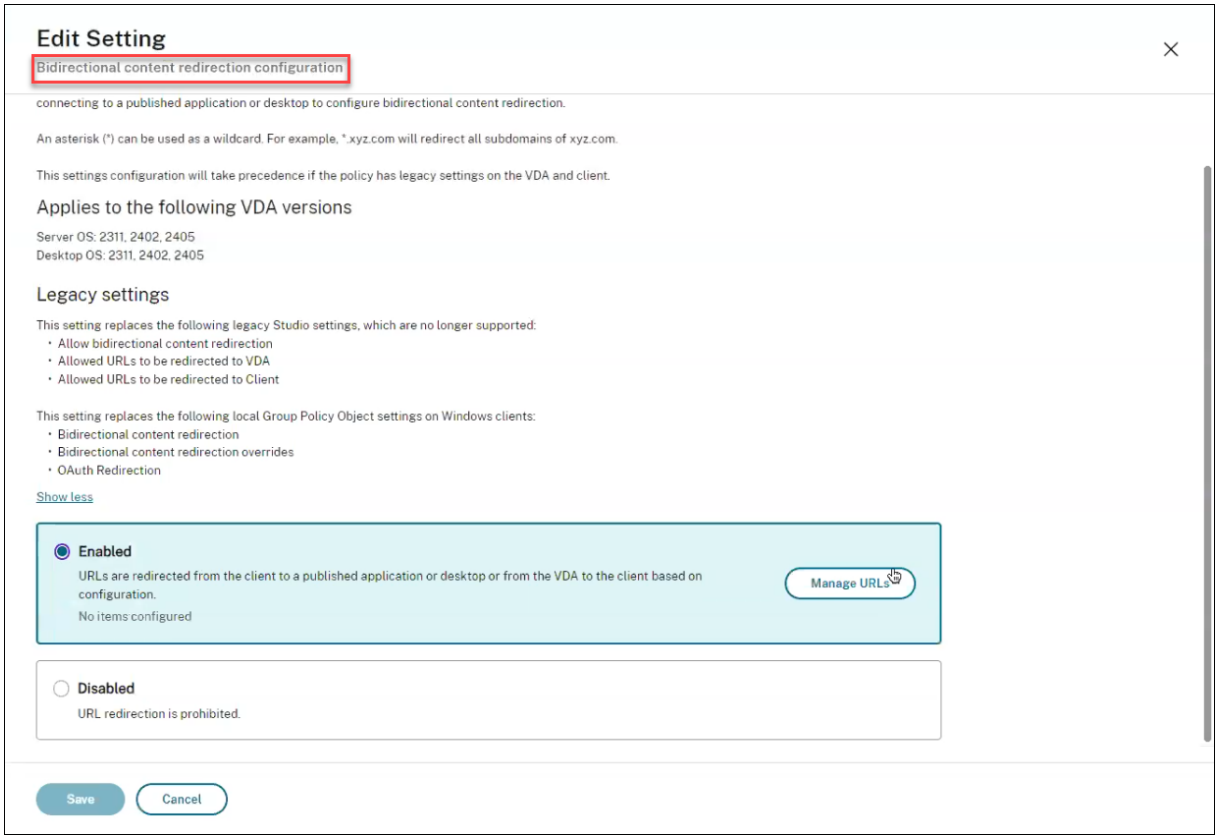
      ]
     }

 ],
 "clientToHostConfig": [
   {

     "publishedAppOrDesktopNameType": "Desktop",
     "publishedAppOrDesktopName": "Win11Desktop",
     "clientToHostUrls": [
       "https://www.example.net",
       "https://*.citrix.example"
     ]
    }
,
   {

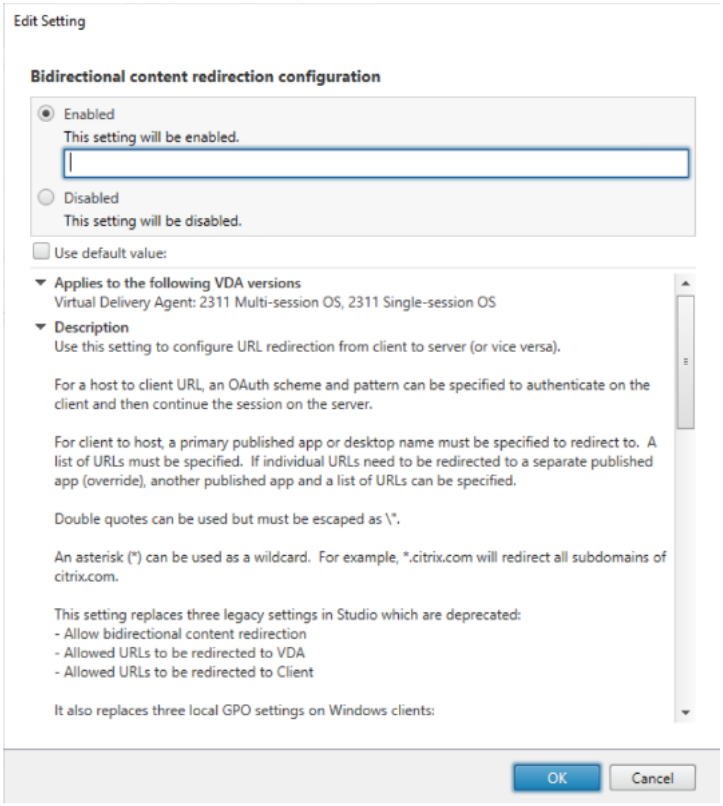
     "publishedAppOrDesktopNameType": "Application",
     "publishedAppOrDesktopName": "Chrome",
     "clientToHostUrls": [
       "https://tibco.example"
     ]
    }

 ]
}
```

次のパラメーターを設定する必要があります:

- **version**:（必須）1 に設定します。
- VDA からクライアントへの URL リダイレクトの場合は、単一の`hostToClientConfig`を作成します。
- **hostToClientUrls**:（必須）ホスト（VDA）からクライアントにリダイレクトされる URL の一覧。ワイルドカードを使用できます。「*」が指定されている場合、`clientToHostConfig`は`publishedAppOrDesktopNameType`、空の`publishedAppOrDesktopName`、および空の`clientToHostUrls`とともに指定する必要があります。



OAuth リダイレクト

OAuth リダイレクトを使用すると、クライアントエンドポイントのブラウザーを使用して認証を実行し、トークンを VDA に送り返すことができます。

メリット:

- これらの資格情報をホスト環境に保存するのを避けることができます。
- 利用可能な生体認証機能を、VDA ではなくエンドポイントで使用できます。

URL の OAuth リダイレクトを構成するには、次のパラメーターを指定します:

- **oAuthRedirectionPattern**:(オプション)ホストからクライアントへの URL リダイレクトを介してクライアントにリダイレクトされると OAuth 認証フローが開始されたかのように追跡され、フローが完了すると(結果のスキームまたは開かれたリダイレクト URL パターンによって検出)、結果の URL がフローを開始したホスト VDA にリダイレクトされる URL 正規表現です。
- **oAuthScheme**:(オプション)スキームが指定されている場合、終了 URL は「<scheme>://<something>」の形式である必要があります。スキームが指定されていない(空)とみなします。この場合、元の結果の URL パターンが正規表現キャプチャグループを介してパターンから抽出されます(パターンで指定されている必要があります)。元の URL は`citrix-oauth-redir://`リダイレクト URL を使用するように書き換えられます。フローが完了すると、元のリダイレクト URL がホスト(VDA)に再度リダイレクトされます。こ

の場合、OAuth 認証サーバーは`citrix-oauth-redir://byIndex/1 (2, 3, ... N)`リダイレクト URL を許可するように設定する必要があります。

クライアントから VDA へのリダイレクトの場合は、リダイレクトするリソースごとに **clientToHostConfig** を作成します。
各リソースに次のパラメーターを含めます:

- **publishedAppOrDesktopNameType**:（必須）Studio で構成された公開デスクトップ（「Desktop」）または公開アプリケーション（「Application」）のいずれか。リソースが有効でない場合、リダイレクトは正しく機能しません。
- **publishedAppOrDesktopName**:（必須）Web Studio で構成されたリソース名。
- **clientToHostUrls**:（必須）クライアントからホスト（VDA）にリダイレクトされる URL の一覧。ワイルドカードを使用できます。

既知の制限事項

PowerShell を使用してカスタム URL スキーム（HTTP または HTTPS ではない）でブラウザーを起動すると、カスタム URL はクライアントにリダイレクトされません。

ブラウザーコンテンツリダイレクトのポリシー設定

August 17, 2024

[Web ブラウザーコンテンツリダイレクト］には、この機能を構成するためのポリシー設定が含まれています。

Web ブラウザーコンテンツのリダイレクトでは、Citrix Virtual Apps and Desktops が Web ブラウザーコンテンツ（HTML5 など）をユーザーに配信する方法を制御し、最適化します。コンテンツが表示されている Web ブラウザーの表示領域のみがリダイレクトされます。

HTML5 ビデオリダイレクションと Web ブラウザーコンテンツリダイレクトは、独立した機能です。この機能を使用するために、HTML5 ビデオのリダイレクトのポリシーは不要です。ただし、Web ブラウザーコンテンツのリダイレクトには Citrix HDX HTML5 ビデオリダイレクトサービスが使用されます。詳しくは、「ブラウザーコンテンツリダイレクト」を参照してください。

> 注:
>
> Web Studio で利用可能なポリシー設定は VDA 上でレジストリキーにより上書きできますが、レジストリキーはオプションです。

TLS および **Web** ブラウザーコンテンツリダイレクト

Web ブラウザーコンテンツリダイレクトを使用して、HTTPS Web サイトをリダイレクトできます。これらの Web サイトに挿入された JavaScript は、VDA で動作する Citrix HDX HTML5 ビデオリダイレクションサービス (WebSocketService.exe）への TLS 接続を確立する必要があります。このリダイレクションを実現し、Web ページの TLS 整合性を維持するために、Citrix HDX HTML5 ビデオリダイレクションサービスは VDA の証明書ストアで 2 つのカスタム証明書を生成します。

HdxVideo.js は、Secure Web ソケットを使用して VDA で動作する WebSocketService.exe と通信します。このプロセスはローカルシステムで動作し、SSL の終了とユーザーセッションマッピングを実行します。

WebSocketService.exe は 127.0.0.1 ポート 9001 でリスンします。

ブラウザーコンテンツリダイレクト

デフォルトでは、Citrix Workspace アプリはクライアントフェッチとクライアントレンダリングを試行します。クライアントフェッチとクライアントレンダリングが失敗すると、サーバー側のレンダリングが試行されます。Web ブラウザーコンテンツのリダイレクトプロキシ設定ポリシーも有効にすると、Citrix Workspace アプリはサーバーフェッチとクライアントレンダリングだけを試みます。

デフォルトでは、［許可］に設定されています。

Web ブラウザーコンテンツリダイレクト統合 **Windows** 認証サポート設定

Web ブラウザーコンテンツリダイレクトにより、認証に Negotiate スキームを使用するオーバーレイが有効になります。この機能拡張は、VDA と同じドメイン内の統合 Windows 認証（IWA）で構成された Web サーバーへのシングルサインオンを提供します。

Allowed に設定すると、Web ブラウザーコンテンツリダイレクトオーバーレイは、ユーザーの VDA 資格情報を使用して Negotiate チケットを取得します。次に、ユーザーはシングルサインオンで Web サーバーへの認証を行います。

Prohibited に設定すると、Web ブラウザーコンテンツリダイレクトオーバーレイは、VDA からの Negotiate チケットを要求しません。ユーザーは、基本認証方法を使用して、Web サーバーに対して認証を行います。この認証方法では、ユーザーは Web サーバーにアクセスするたびに VDA 資格情報を入力する必要があります。

デフォルトでは、この設定は禁止されています。

Web ブラウザーコンテンツリダイレクトのサーバー側での取得のプロキシ認証設定

この設定では、オーバーレイから発信された HTTP トラフィックをダウンストリーム Web プロキシ経由でルーティングします。ダウンストリーム Web プロキシは、Negotiate 認証スキームにより VDA ユーザーのドメイン資格情報を使用し、HTTP トラフィックを承認および認証します。

Web ブラウザーコンテンツリダイレクトプロキシ設定ポリシーを使用して、PAC ファイルでサーバーフェッチモードのブラウザーコンテンツリダイレクトを設定する必要があります。PAC スクリプトで、ダウンストリーム Web プロキシを介してオーバーレイトラフィックをルーティングする手順を指定します。次に、ネゴシエート認証スキームを介して VDA ユーザーを認証するようにダウンストリーム Web プロキシを構成します。

［許可］に設定すると、Web プロキシは **Proxy-Authenticate: Negotiate** ヘッダーを含む 407 ネゴシエートチャレンジで応答します。次に、Web ブラウザーコンテンツリダイレクトは、VDA ユーザーのドメイン資格情報を使用して、Kerberos サービスチケットを取得します。また、Web プロキシへのその後の要求にサービスチケットを含めます。

［禁止］に設定すると、Web ブラウザーコンテンツリダイレクトにより、オーバーレイと Web プロキシ間のすべての TCP トラフィックが干渉することなくプロキシされます。オーバーレイは、基本認証資格情報またはその他の使用可能な資格情報を使用して、Web プロキシへの認証を行います。

デフォルトでは、この設定は禁止されています。

ブラウザーコンテンツリダイレクト **ACL**（アクセス制御リスト）構成ポリシー設定

Web ブラウザーコンテンツリダイレクトを使用できる URL、またはブラウザーコンテンツリダイレクトへのアクセスを拒否する URL のアクセス制御リスト（ACL）を構成するには、この設定を使用します。

承認済み URL は許可リストに登録された URL であり、このリストのコンテンツがクライアントにリダイレクトされます。

ワイルドカード文字「*」は使用可能ですが、この文字は URL のプロトコルおよびドメインアドレスには使用できません。ただし、Citrix Virtual Apps and Desktops 7 2206 以降では、URL のサブドメインアドレス部分でワイルドカード「*」を使用できます。

許可: `http://www.xyz.com/index.html`、`https://www.xyz.com/*`、`http://www.xyz.com/*videos*`、`http://*.xyz.com/`

使用不可: `http://*.*.com/`

URL にパスを指定することにより、より細分化することができます。たとえば、`https://www.xyz.com/sports/index.html`を指定すると、index.html ページのみがリダイレクトされます。

デフォルトでは、この設定は`https://www.youtube.com/*`に設定されています。

詳しくは、Knowledge Center のCTX238236の記事を参照してください。

> 注:
>
> BCR が Web サイトをエンドポイントにリダイレクトできるように、ACL を構成できます。また、構成された URL で使用される認証に Okta や Duo などの ID プロバイダー（IdP）を許可するように、認証サイトを構成できます。

Web ブラウザーコンテンツリダイレクト認証サイト

URL の一覧を構成するには、この設定を使用します。Web ブラウザーコンテンツリダイレクトによりリダイレクトされたサイトは、この一覧を使用してユーザーを認証します。この設定では、許可リストに登録済みの URL から移動するときに、Web ブラウザーコンテンツリダイレクトをアクティブ（リダイレクトあり）のままにする URL を指定します。

一般的なシナリオとしては、ID プロバイダー（IdP）を利用して認証を行う Web サイトが考えられます。たとえば、Web サイト`www.xyz.com`をエンドポイントにする必要があるものの、Okta（`www.xyz.okta.com`）などのサードパーティ IdP が認証を処理しているとします。管理者は、Web ブラウザーコンテンツリダイレクトの ACL 構成ポリシーを使用して、`www.xyz.com`を許可リストに追加します。次に、Web ブラウザーコンテンツリダイレクト認証サイトを使用して、許可リストに`www.xyz.okta.com`を追加します。

詳しくは、Knowledge Center のCTX238236の記事を参照してください。

Web ブラウザーコンテンツリダイレクトの禁止リスト設定

この設定は、Web ブラウザーコンテンツリダイレクトの ACL 構成の設定と連携しています。Web ブラウザーコンテンツリダイレクト ACL 構成の設定と、禁止リスト構成の設定に、URL が存在することを考慮してください。この場合、禁止リストの構成が優先され、URL の Web ブラウザーコンテンツはリダイレクトされません。

承認されていない **URL**： Web ブラウザーコンテンツがクライアントにリダイレクトされずサーバーでレンダリングされる、禁止リストに登録する URL を指定します。

ワイルドカード文字「*」は使用可能ですが、この文字は URL のプロトコルおよびドメインアドレスには使用できません。

使用可能：`http://www.xyz.com/index.html`、`https://www.xyz.com/*`、`http://www.xyz.com/*videos*`

使用不可：`http://*.xyz.com/`

URL にパスを指定することにより、より細分化することができます。たとえば、`https://www.xyz.com/sports/index.html`を指定すると、index.html ページのみが禁止リストに登録されます。

Web ブラウザーコンテンツのリダイレクトのプロキシ設定

この設定は、Web ブラウザーコンテンツリダイレクト用の VDA でのプロキシ設定のオプションです。有効なプロキシアドレスとポート番号、PAC/WPAD URL、または直接/透過型の設定を指定して有効にすると、Citrix Workspace アプリはサーバーフェッチとクライアントレンダリングだけを試行します。

無効にするか構成しないで、デフォルト値を使用すると、Citrix Workspace アプリはクライアントフェッチとクライアントレンダリングを試行します。

デフォルトでは、この設定は禁止されています。

明示的なプロキシで許可されたパターン:

```
http://\<hostname/ip address\>:\<port\>
```

例:

```
http://proxy.example.citrix.com:80
http://10.10.10.10:8080
```

PAC/WPAD ファイルで許可されたパターン:

```
http://<hostname/ip address>:<port>/<path>/<Proxy.pac>
```

例: `http://wpad.myproxy.com:30/configuration/pac/Proxy.pac`

```
https://<hostname/ip address>:<port>/<path>/<wpad.dat>
```

例: `http://10.10.10.10/configuration/pac/wpad.dat`

直接または透過型のプロキシで許可されたパターン:

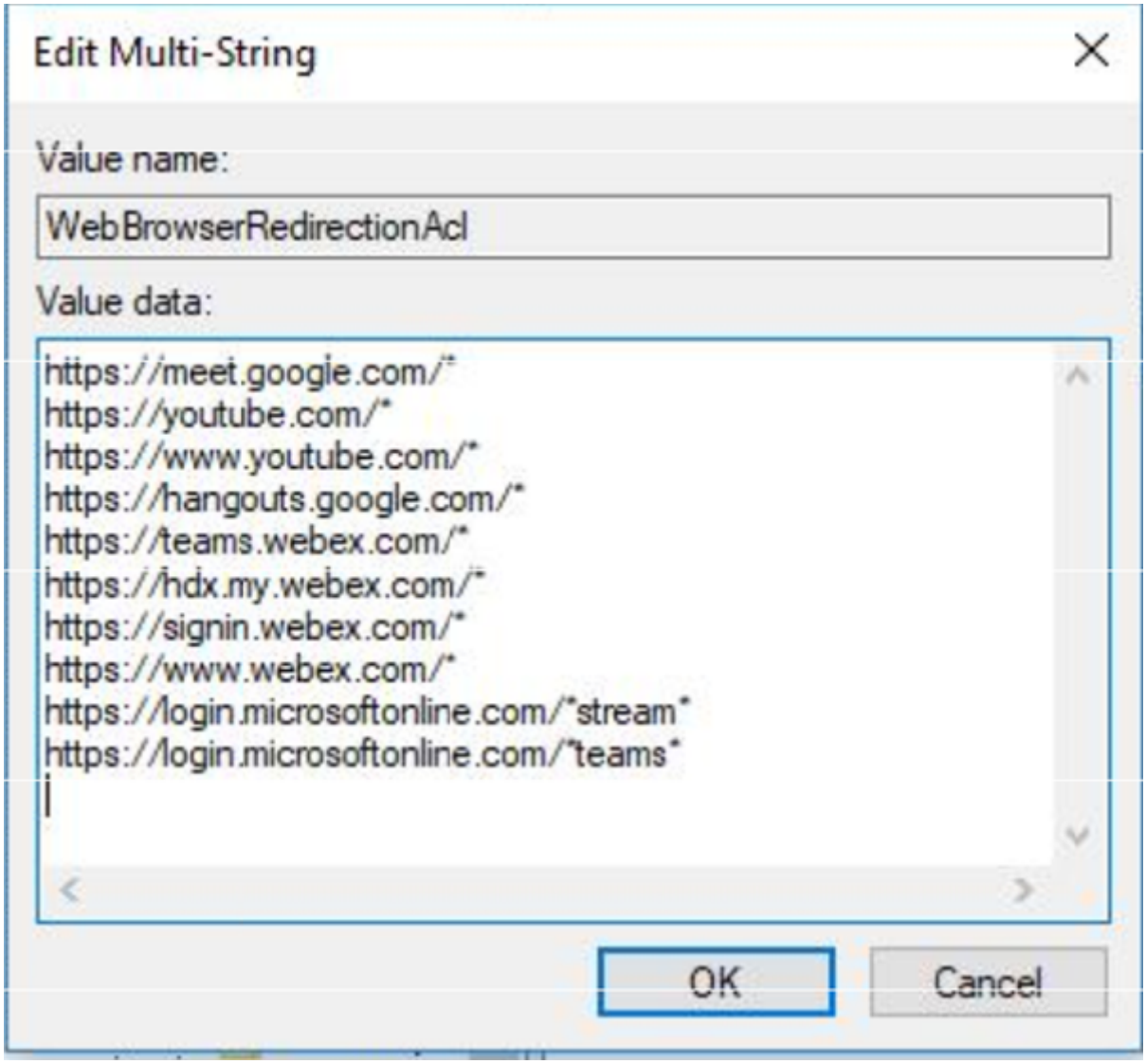
ポリシーテキストボックスに「**DIRECT**」と入力します。

Web ブラウザーコンテンツリダイレクトのレジストリキーの上書き

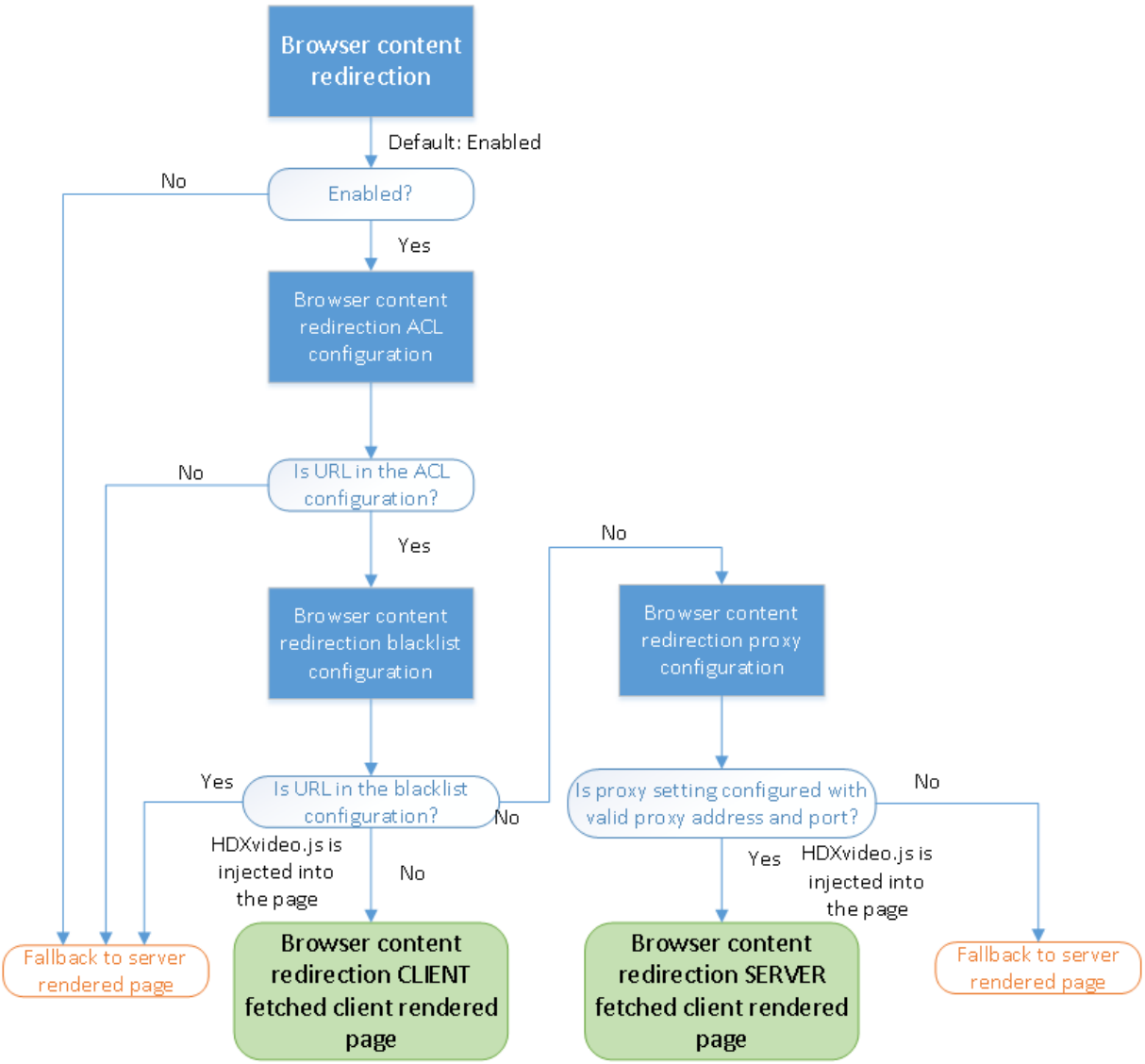
> 警告:
>
> レジストリエディターの使用を誤ると、深刻な問題が発生する可能性があり、オペレーティングシステムの再インストールが必要になる場合もあります。レジストリエディターの誤用による障害に対して、Citrix は一切責任を負いません。レジストリエディターは、お客様の責任と判断の範囲でご使用ください。また、レジストリファイルのバックアップを作成してから、レジストリを編集してください。
>
> ポリシー設定を上書きするレジストリ設定を以下に示します:

`\HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxMediastream`

名前	種類	値
WebBrowserRedirection	DWORD	1= 許可、0= 禁止
WebBrowserRedirectionAcl	REG_MULTI_SZ	
WebBrowserRedirectionAuthenticationMethod	REG_MULTI_SZ	
WebBrowserRedirectionProxyAddress	REG_SZ	`http://myproxy.citrix.com:8080` または `http://10.10.10.10:8888`
WebBrowserRedirectionBlacklist	REG_MULTI_SZ	



Web ブラウザーコンテンツのリダイレクト用の **HDXVideo.js** 挿入



HdxVideo.js は、Chrome の Web ブラウザーコンテンツリダイレクト拡張機能または Internet Explorer Browser Helper Object（BHO）を使用して Web ページに挿入されます。BHO は、Internet Explorer のプラグインモデルです。Web ブラウザー API のフックを提供し、プラグインがナビゲーションを制御するためにページの DOM（Document Object Model）にアクセスできるようにします。

BHO は、特定のページに HdxVideo.js を挿入するかどうかを決定します。この決定は、上記のフローチャートに示した管理ポリシーに基づいています。

JavaScript の挿入とクライアントへの Web ブラウザーコンテンツのリダイレクトが決定されると、VDA 上の Internet Explorer ブラウザーの Web ページが消去されます。**document.body.innerHTML** を空に設定すると、VDA 上では Web ページの本文全体が削除されます。ページがクライアントに送信され、クライアントのオーバーレイ Web ブラウザー（Hdxbrowser.exe）に表示される準備が整います。

クライアントセンサーのポリシー設定

August 17, 2024

［クライアントセンサー］セクションには、ユーザーセッションでのモバイルデバイスのセンサー情報の制御に関するポリシー設定項目があります。

クライアントデバイスの位置情報をアプリケーションで使用する

この設定では、セッション内のアプリケーションをモバイルデバイス上で使用する場合に、そのモバイルデバイスの位置情報をアプリケーションで使用することを許可または禁止します。

デフォルトでは、禁止されます。

位置情報の使用が禁止されている場合、アプリケーションからの位置情報の取得要求に対して「アクセス拒否」が返されます。

位置情報の使用が許可されている場合でも、Citrix Workspace アプリからの位置情報の要求を拒否することで、位置情報の使用をユーザーが拒否できます。Android および iOS デバイスでは、そのセッションで最初に位置情報への要求が発生したときにメッセージが表示されます。

［クライアントデバイスの位置情報をアプリケーションで使用する］設定をサポートするアプリケーションを開発する場合は、以下の点に注意してください。

- 位置情報が常に使用可能であるとは限らないことにご注意ください。これは以下の理由によります:
  - 位置情報の使用をユーザーが拒否する可能性がある。
  - アプリケーションを実行している間に位置情報が提供されない、または位置が変化する可能性がある。
  - 位置情報の提供をサポートしないほかのデバイスからアプリケーションに再接続する可能性がある。
- 位置情報をサポートするアプリケーションの設定として、以下の点を考慮してください。
  - 位置情報の使用をデフォルトで無効にする。
  - アプリケーションの実行時にユーザーが位置情報の使用を許可したり禁止したりできる。
  - アプリケーションがキャッシュした位置情報データをユーザーが消去できる（ただし、Citrix Workspace アプリは位置情報データをキャッシュしません）。
- 位置情報が有効になっているアプリケーションは、位置情報を詳細に管理する必要があります。この管理により、取得したデータがアプリケーションの目的に適していることが確認されます。また、関連するすべての法規制に準拠します。
- 位置情報を使用するときは、保護された接続（TLS や VPN による接続など）が使用されるようにします。Citrix Workspace アプリを信頼できるサーバーに接続してください。
- 位置情報サービスの使用に関して法的なアドバイスを得ることを検討してください。

デスクトップ **UI** のポリシー設定

August 17, 2024

［デスクトップ **UI**］セクションには、デスクトップの壁紙、メニューのアニメーション、およびドラッグ中の画像などの視覚効果を制御するポリシー設定項目があります。これらのポリシー設定項目は、クライアント接続で使用される帯域幅を管理するのに役立ちます。WAN などの狭帯域幅接続で視覚効果を無効にすると、公開アプリケーションのパフォーマンスが向上します。

> 重要：
>
> このリリースでは、従来のグラフィックモードとデスクトップコンポジションリダイレクト（DCR）はサポートしていません。このポリシーは、以下を使用する場合の下位互換性のためにのみ含まれています：
>
> - XenApp 7.15 LTSR
> - XenDesktop 7.15 LTSR
> - Windows 7 および Windows 2008 R2 を使用した過去の VDA リリース。

デスクトップコンポジションリダイレクト

この設定では、ローカルの DirectX グラフィックレンダリングに以下の処理装置を使用して、より滑らかな Windows デスクトップ操作をユーザーに提供するかどうかを指定します：

- ユーザーデバイスのグラフィック処理装置（Graphics processing unit：GPU）
- または、
- ユーザーデバイスの統合グラフィックプロセッサ（Integrated graphics processor：IGP）

［デスクトップコンポジションリダイレクト］を有効にすると、Windows デスクトップの操作レスポンスが向上し、サーバーの高いスケーラビリティが維持されます。

デフォルトでは、［デスクトップコンポジションリダイレクト］は無効になっています。

［デスクトップコンポジションリダイレクト］を無効にしてユーザーセッションに必要な帯域幅を減らすには、この設定項目で ［無効］を選択します。

デスクトップコンポジションリダイレクトの画質

この設定では、デスクトップコンポジションリダイレクトで使用される画質を指定します。

デフォルト値は［高］です。

［高］、［中］、［低］、または［無損失］から選択します。

デスクトップの壁紙

この設定では、ユーザーセッションでの壁紙の表示を許可または禁止します。

デフォルトでは、ユーザーセッションで壁紙を表示できます。

デスクトップの壁紙を非表示にしてユーザーセッションに必要な帯域幅を減らすには、ポリシーにこの設定を追加して ［禁止］をクリックします。

メニューをアニメーション化する

この設定では、ユーザーセッションでのメニューアニメーションを許可または禁止します。

デフォルトでは許可されます。

メニューアニメーションは、アクセスを簡単にするための Microsoft の個人優先設定です。これが有効な場合、スクロールまたはフェードインによってメニューが表示されるのが少し遅れることとなります。矢印アイコンはメニュー下部に表示されます。そのアイコン上にマウスポインターを置くと、メニューの内容が表示されます。

この設定項目が ［許可］に設定されている場合、デスクトップでは［メニューをアニメーション化する］が有効で、かつ、メニューのアニメーション化 Microsoft 個人優先設定が有効です。

> 注:
>
> メニューアニメーション Microsoft 個人優先設定の変更は、デスクトップに影響します。セッションの終了時に変更を破棄するようにデスクトップを設定したとします。この場合、メニューのアニメーション化を有効にしているユーザーは、以降のセッションではメニューのアニメーション化を使用できない可能性があります。メニューのアニメーション化が必要なユーザーについては、デスクトップのメインイメージの Microsoft 設定を有効にするか、またはデスクトップでユーザーの変更を維持する必要があります。

ドラッグ中にウィンドウの内容を表示する

この設定では、ウィンドウをドラッグするときにウィンドウの内容を表示する機能を許可または禁止します。

デフォルトでは許可されます。

［許可］を選択すると、ウィンドウをドラッグするときに内容が表示されたままになります。［禁止］を選択すると、ドロップするまでウィンドウの外枠のみが表示されます。

エンドユーザーモニタリングのポリシー設定

August 17, 2024

［エンドユーザーモニタリング］セクションには、セッショントラフィックの測定に関するポリシー設定項目があります。

ICA 往復測定

この設定では、アクティブな接続に対して ICA 往復測定を実行するかどうかを決定します。

デフォルトでは、ICA 往復測定が実行されます。

デフォルトでは、各 ICA 往復測定の開始は遅延されます。この遅延は、ユーザーの操作を示すトラフィックが発生するまで続きます。このため、ユーザーが操作していないにもかかわらず ICA 往復測定による ICA トラフィックが発生することはありません。

ICA 往復測定間隔

この設定では、ICA 往復測定を実行する頻度を秒単位で指定します。

デフォルトでは、15 秒ごとに測定が実行されます。

アイドル接続の **ICA** 往復測定

この設定では、アイドル状態の接続に対して ICA 往復測定を実行するかどうかを決定します。

デフォルトでは、アイドル接続に対して ICA 往復測定は実行されません。

デフォルトでは、各 ICA 往復測定の開始は遅延されます。この遅延は、ユーザーの操作を示すトラフィックが発生するまで続きます。このため、ユーザーが操作していないにもかかわらず ICA 往復測定による ICA トラフィックが発生することはありません。

デスクトップエクスペリエンス拡張のポリシー設定

August 17, 2024

この設定項目では、サーバーオペレーティングシステム上のセッションに Windows 7 デスクトップテーマを適用するかどうかを構成します。

デフォルトでは、この設定は許可されています。

Windows クラシックテーマが選択されたユーザープロファイルが存在する仮想デスクトップでは、この設定を有効にしてもデスクトップエクスペリエンス拡張が提供されません。Windows 7 テーマのユーザープロファイルを持つユーザーが、Windows Server 2012 を実行している仮想デスクトップにログオンすることを考慮してください。また、このポリシーは構成されていないか、無効になっています。この場合、そのユーザーには、テーマの適用に失敗したことを示すエラーメッセージが表示されます。

これらの問題は、ユーザープロファイルをリセットすることで解決されます。

実行中のユーザーセッションが存在する仮想デスクトップでこの設定項目を無効にすると、Windows 7 テーマおよび Windows クラシックテーマでの表示に問題が発生します。この問題を避けるには、この設定項目の構成を変更した後で仮想デスクトップを再起動してください。次に、仮想デスクトップの移動プロファイルを削除してください。さらに、プロファイル間の一貫性の問題を避けるため、仮想デスクトップのほかのユーザープロファイルもすべて削除することをお勧めします。

ご使用の環境で移動ユーザープロファイルを使用しているとします。この場合、プロファイルを共有するすべての仮想デスクトップでデスクトップエクスペリエンス拡張機能の有効/無効を統一してください。

サーバー OS を実行する仮想デスクトップとクライアント OS を実行する仮想デスクトップで移動プロファイルを共有することは推奨されません。クライアントとサーバーのオペレーティングシステムのプロファイルは異なります。移動プロファイルを共有するとプロファイル内のプロパティの整合性に問題が生じることがあります。

ファイルリダイレクトのポリシー設定

August 17, 2024

［ファイルのリダイレクト］セクションには、クライアント側ドライブのマッピングと最適化に関するポリシー設定が含まれています。

クライアントドライブに自動接続する

この設定では、ログオン時にクライアント側のドライブに自動的にマップすることを許可または禁止します。

デフォルトでは許可されます。

この設定項目をポリシーに追加する場合は、自動接続するドライブの種類別の設定項目についても確認してください。たとえば、クライアント側の CD-ROM ドライブへの自動接続を許可するには、この設定および ［クライアント側光学式ドライブ］設定を許可します。

関連する設定項目は以下のとおりです:

- クライアントドライブリダイレクト
- クライアント側フロッピードライブ
- クライアント側光学式ドライブ
- クライアント側固定ドライブ
- クライアント側ネットワークドライブ
- クライアント側リムーバブルドライブ

クライアントドライブリダイレクト

この設定では、ファイルのクライアント側ドライブへのリダイレクトおよびクライアント側ドライブからのリダイレクトを有効または無効にします。

デフォルトでは有効になっています。

> 注:
>
> [クライアントドライブのリダイレクト] ポリシー設定は、汎用 USB リダイレクトを使用するセッションにマッピングされているドライブには適用されません。

この設定を有効にすると、ユーザーはクライアント側のすべてのドライブにファイルを保存できるようになります。無効にすると、すべてのファイルのリダイレクトが防止されます。この構成は、個々のファイルリダイレクト設定の状態に関係なく適用できます。個々のファイルリダイレクト設定には、クライアントフロッピードライブとクライアントネットワークドライブが含まれます。

関連する設定項目は以下のとおりです:

- クライアント側フロッピードライブ
- クライアント側光学式ドライブ
- クライアント側固定ドライブ
- クライアント側ネットワークドライブ
- クライアント側リムーバブルドライブ

クライアント側固定ドライブ

この設定では、クライアント側の固定ドライブにアクセスしたりファイルを保存したりすることを許可または禁止します。

デフォルトでは、クライアント固定ドライブへのアクセスは許可されています。

この設定をポリシーに追加するときは、[クライアントドライブリダイレクト] 設定で [許可] が選択されていることを確認してください。この設定が無効な場合、クライアント固定ドライブはマップされず、ユーザーが手作業でそれらのドライブにアクセスすることもできなくなります。このとき、[クライアント固定ドライブ] 設定の内容は考慮されません。

ユーザーがログオンしたときに固定ドライブに自動接続できるようにするには、[クライアントドライブに自動接続する] 設定を使用します。

クライアント側フロッピードライブ

この設定では、クライアント側のフロッピードライブにアクセスしたりファイルを保存したりすることを許可または禁止します。

デフォルトでは、クライアントフロッピードライブへのアクセスは許可されています。

この設定をポリシーに追加するときは、［クライアントドライブリダイレクト］設定で［許可］が選択されていることを確認してください。この設定が無効な場合、クライアントフロッピードライブはマップされず、ユーザーが手作業でそれらのドライブにアクセスすることもできなくなります。このとき、［クライアントフロッピードライブ］設定の内容は考慮されません。

ユーザーがログオンしたときにフロッピードライブに自動接続できるようにするには、［クライアントドライブに自動接続する］設定を使用します。

クライアント側ネットワークドライブ

この設定では、クライアント側でマップ済みのネットワークドライブ（リモートドライブ）にアクセスしたりファイルを保存したりすることを許可または禁止します。

デフォルトでは許可されます。

この設定をポリシーに追加するときは、［クライアントドライブリダイレクト］設定で［許可］が選択されていることを確認してください。この設定が無効な場合、クライアントネットワークドライブはマップされず、ユーザーが手作業でそれらのドライブにアクセスすることもできなくなります。この構成では、［クライアントネットワークドライブ］設定の内容は考慮されません。

ユーザーがログオンしたときにネットワークドライブに自動接続できるようにするには、［クライアントドライブに自動接続する］設定を使用します。

クライアント側光学式ドライブ

この設定により、以下にアクセスしたりファイルを保存したりすることを許可または禁止します：

- ユーザーデバイスの CD-ROM
- ユーザーデバイスの DVD-ROM
- ユーザーデバイスの BD-ROM ドライブ。

デフォルトではクライアント光学式ドライブが許可されています。

この設定をポリシーに追加するときは、［クライアントドライブリダイレクト］設定で ［許可］が選択されていることを確認してください。この設定が無効な場合、クライアント光学式ドライブはマップされず、ユーザーが手作業でそれらのドライブにアクセスすることもできなくなります。この構成では、［クライアント光学式ドライブ］設定の内容は考慮されません。

ユーザーがログオンしたときに光学式ドライブに自動接続できるようにするには、［クライアントドライブに自動接続する］設定を使用します。

クライアント側リムーバブルドライブ

この設定により、クライアント側の USB ドライブにアクセスしたりファイルを保存したりすることを許可または禁止します。

デフォルトでは、クライアント側リムーバブルドライブへのアクセスは許可されています。

この設定をポリシーに追加するときは、［クライアントドライブのリダイレクト］設定で［許可］が選択されていることを確認してください。この設定が無効な場合、クライアント側リムーバブルドライブはマップされず、ユーザーが手作業でそれらのドライブにアクセスすることもできなくなります。この構成では、［クライアント側リムーバブルドライブ］設定の内容は考慮されません。

［クライアントドライブに自動接続する］設定を構成し、ユーザーがログオンしたときにリムーバブルドライブに自動接続できるようにします。

ホストからクライアントへのリダイレクト

この設定では、URL や特定のメディアコンテンツをクライアント側で開くためのファイルタイプの関連付けを有効または無効にします。この設定を無効にすると、コンテンツはサーバー上で開きます。

デフォルトでは無効になっています。

この設定を有効にすると、次の種類の URL がクライアント側のアプリケーションで開きます。

- HTTP
- HTTPS
- Real Player および QuickTime（RTSP）
- Real Player および QuickTime（RTSPU）
- 従来の RealPlayer（PNM）
- Microsoft Media Server（MMS）

クライアント側のドライブ文字を保持する

この設定では、クライアント側ドライブをセッション内でマップするときに、元のドライブ文字を保持するかどうかを指定します。

デフォルトでは保持されません。

この設定をポリシーに追加するときは、［クライアントドライブリダイレクト］設定で［許可］が選択されていることを確認してください。

クライアント側ドライブへの読み取り専用アクセス

この設定では、ユーザーおよびアプリケーションが以下を実行することを許可または禁止します：

- マップされたクライアントドライブにファイルを作成する
- マップされたクライアントドライブ上のファイルを変更する
- マップされたクライアントドライブ上のフォルダーを変更する

デフォルトでは許可されます。

［有効］に設定すると、ファイルやフォルダーへの読み取り専用アクセスが許可されます。

この設定をポリシーに追加するときは、［クライアントドライブリダイレクト］設定で［許可］が選択されていることを確認してください。

ユーザーフォルダーのリダイレクト

この設定では、Citrix Workspace アプリや Web Interface を使用するユーザーに対して、セッション内でクライアント側の［ドキュメント］や［デスクトップ］などのローカルフォルダーに簡単にアクセスするための機能を許可または禁止します。

デフォルトでは許可されます。

この設定では、この機能の有効/無効をポリシーの適用条件に基づいて制御できます。この設定が禁止されている場合、ユーザーフォルダーのリダイレクトに関する StoreFront、Web Interface、または Citrix Workspace アプリのすべての設定が無視されます。

ユーザーフォルダーのリダイレクトを許可するユーザーを定義するには、この設定項目で ［許可］を選択し、ポリシーの適用先としてそのユーザーを指定します。この設定は、ユーザーフォルダーのリダイレクトに関するほかの設定よりも優先されます。

クライアント側ハードドライブのファイルへのアクセスや書き込みを禁止すると、ユーザーフォルダーのリダイレクトも禁止されます。この状況は、ユーザーフォルダーのリダイレクトがユーザーデバイスと相互通信する必要があるために発生します。

この設定をポリシーに追加するときは、［クライアント側固定ドライブ］設定で［許可］が選択されていることを確認してください。

ファイル転送のポリシー

デフォルトでは、ファイル転送は有効になっています。Web Studio を使って、［ユーザー設定］**>** ［**ICA**ファイルリダイレクト］にあるこれらのポリシーを変更します。ファイル転送のポリシーを使用する場合は、次の点を検討してください：

- **ChromeOS/HTML5** 向け **Citrix Workspace** アプリのファイル転送 - Citrix Virtual Apps and Desktops セッションとユーザーデバイス間でのユーザーによるファイル転送を許可または拒否します。
- **ChromeOS/HTML5** 向け **Citrix Workspace** アプリのファイルアップロード - ユーザーデバイスから Citrix Virtual Apps and Desktops セッションへのユーザーによるファイルのアップロードを許可または拒否します。

- **ChromeOS/HTML5** 向け **Citrix Workspace** アプリのファイルダウンロード - Citrix Virtual Apps and Desktops セッションからユーザーデバイスへのユーザーによるファイルのダウンロードを許可または拒否します。

> 注:
>
> ファイル転送ポリシーは、HTML5 向け Citrix Workspace アプリと ChromeOS 向け Citrix Workspace アプリにのみ適用されます。

非同期書き込みを使用する

この設定では、クライアント側のディスクへの非同期書き込みを有効または無効にします。

デフォルトでは無効になっています。

非同期書き込みを有効にすると、WAN 接続を介したサーバーからクライアント側へのディスク書き込みおよびファイル転送の遅延が改善されます。ただし、非同期転送時にセッションが切断されたりクライアント側のディスク容量が不足したりしてファイル書き込みが中断された場合に、クライアント側のファイルが破損することがあります。この問題が発生した場合、ポップアップウィンドウが開き、影響を受けたファイルがユーザーに通知されます。ユーザーは問題を解決した後でファイル転送をやり直すことができます。

ディスクへの非同期書き込みを有効にするのは、ファイル転送速度が良好なリモート接続を必要とするユーザーに対してのみ、あるいは接続やディスクに障害が発生した場合に、失われたファイルやデータを簡単に回復できるユーザーに対してのみにすることをお勧めします。

この設定をポリシーに追加するときは、［クライアントドライブのリダイレクト］設定で［許可］が選択されていることを確認してください。この設定が無効の場合、非同期書き込みは行われません。

グラフィックのポリシー設定

August 17, 2024

［グラフィック］セクションには、ユーザーセッションでの画像処理の制御に関するポリシー設定項目があります。

視覚的無損失の圧縮を使用する

この設定により、グラフィックに対して、真の無損失圧縮の代わりに視覚的に無損失の圧縮を使用できるようになります。視覚的無損失では、真の無損失よりもパフォーマンスは向上しますが、見た目にはわからない程度の軽微な損失が発生します。この設定により、［表示品質］設定の値の使用方法が変更されます。

デフォルトでは、無効になっています。

グラフィックス状態インジケーター

この設定では、グラフィックス状態インジケーターがユーザーセッションで実行されるように構成されます。このツールを使用すると、ユーザーはアクティブなグラフィックモードに関する情報を確認できます。この情報には、ビデオコーデック、ハードウェアエンコーディング、画質、およびセッションで使用されているモニターに関する詳細が含まれます。グラフィックス状態インジケーターを使用して、無損失モードを有効または無効にすることもできます。

Citrix Virtual Apps and Desktops 2103 以降のリリースには、ユーザーが画質と対話性の適切なバランスを見つけるのに役立つ画質スライダーが含まれています。

Citrix Virtual Apps and Desktops 2109 以降のリリースには、グラフィックス状態インジケーターを使用して起動されたユーザーインターフェイスを介して仮想ディスプレイレイアウトを構成する機能が含まれています。

グラフィックス状態インジケーターは、以前のバージョンの無損失インジケーターツールに代わるものです。このポリシーにより、Citrix Virtual Apps and Desktops のバージョン 7.16 から 1809 の無損失インジケーターが有効になります。

画面共有

この設定を有効にすると、ユーザーは画面の内容、キーボード、マウスなどのセッションをほかのユーザーと共有できるようになります。

この設定は、デフォルトでは、無効になっています。

VDA は、TCP ポート範囲のポートを使用してデータをやりとりしようとします。最小ポート番号から開始し、後続の接続ごとに番号が大きくなります。ポートは、受信トラフィックと送信トラフィックの両方に使用されます。

デフォルトでは、TCP ポート範囲は 52525～52625 に設定されています。

画面共有に使用するポートをファイアウォールの例外規則の一覧に追加する必要があります。このオプションは、VDA をインストールするときにチェックボックスとして表示されます。デフォルトでは、このオプションはオンになっていません。

表示メモリの制限

この設定では、セッションのビデオバッファーの最大サイズをキロバイト単位で指定します。

デフォルトの表示メモリ制限は、65,536 キロバイトに設定されます。

セッションのビデオバッファーの最大サイズをキロバイト単位で指定します。キロバイト単位の容量指定は、128 から 4,194,303 です。最大値 4,194,303 によって表示メモリが制限されることはありません。デフォルトでは、65,536 キロバイトに設定されます。ウィンドウサイズを大きくしたり、表示色数を多くしたりすると、必要なメモリの量が増えます。従来のグラフィックモードでは、この最大値に達すると、［メモリが不足したときの表示モード］設定に基づいて色数または解像度が低下します。

高い色数および解像度を使用するセッションでは、大きい値を指定します。必要なメモリの量は、次の式で算出できます。

必要とされるメモリ（バイト単位）＝（1 ピクセルあたりのビット数を 8 で割った色数）x（垂直方向のピクセル単位の解像度）x（水平方向のピクセル単位の解像度）

たとえば、ウィンドウの高さが 600、ウィンドウの幅が 800、色数が 32 ビットだとします。この場合、必要なメモリの最大量は（32÷8）x（600）x（800）= 1920000 バイトとなり、1920KB の表示メモリ制限が発生します。

32 ビット以外の色数は、［従来のグラフィックモード］設定が有効な場合のみ使用できます。

HDX では、各セッションで必要な表示メモリ量だけが割り当てられます。このため、デフォルト値よりも多くのメモリが必要なユーザーが一部だけの場合にこの設定項目で表示メモリの制限を増やしても、スケーラビリティは低下しません。

メモリが不足したときの表示モード

> 注:
>
> Virtual Delivery Agent 7.x では、［従来のグラフィックモード］設定が有効な場合のみこの設定項目が適用されます。

この設定では、セッション表示用のメモリが上限に達したときに、色深度と解像度のどちらを下げるかを指定します。

デフォルトでは、最初に色数が低下します。

セッションメモリの上限に達した場合に、表示される画像の品質を下げることができます。色深度と解像度のどちらを最初に下げるかを選択することで、この品質を下げることができます。色数を下げることを選択すると、表示用のメモリが上限に達したときに、まずより少ない色でのイメージ表示に切り替わります。解像度を下げることを選択すると、まず 1 インチあたりのピクセル数が少なくなります。

色数または解像度の低下をユーザーに通知するには、［メモリ不足による表示品質の低下をユーザーに通知する］設定を使用します。

動的ウィンドウプレビュー

この設定では、次のシームレスウィンドウの表示を有効または無効にします:

- フリップ
- フリップ 3D
- タスクバープレビュー
- Windows プレビュー

Windows Aero プレビューオプション	説明
タスクバープレビュー	Windows タスクバー上のアイコン上にマウスポインターを合わせると、そのウィンドウの縮小版がプレビューとして表示されます。
Windows プレビュー	Windows タスクバー上に開いた縮小版上にマウスポインターを合わせると、そのウィンドウがフルサイズで表示されます。
フリップ	Alt+Tab キーを押すと、開いているすべてのウィンドウの縮小版が一覧表示されます。
フリップ 3D	Tab+Windows ロゴキーを押すと、開いているすべてのウィンドウが立体的に重なって一覧表示されます。

デフォルトでは、有効になっています。

イメージキャッシュ

> 注:
>
> Virtual Delivery Agent 7.x では、［従来のグラフィックモード］設定が有効な場合のみこの設定項目が適用されます。

この設定項目では、セッション内のイメージのセクションキャッシュおよび取得を有効または無効にします。セクション内の画像をキャッシュし、必要に応じてこれらのセクションを取得すると、次のようになります:

- ユーザーデバイスでスクロールがスムーズになります
- ユーザーデバイス上のネットワークを介して送信されるデータの量が減ります
- ユーザーデバイス上の必要な処理が減ります

デフォルトでは、イメージのキャッシュ設定は有効になっています。

> 注:
>
> イメージのキャッシュ設定は、イメージがどのようにキャッシュおよび取得されるかを制御します。この設定では、イメージをキャッシュするかどうかは制御されません。従来のグラフィックモード設定が有効な場合は、イメージがキャッシュされます。

従来のグラフィックモード - サポートされていません。後方互換性のためにのみ

> 重要:
>
> このリリースでは、従来のグラフィックモードとデスクトップコンポジションリダイレクト（DCR）はサポートしていません。このポリシーは、Windows 7 および Windows 2008 R2 で XenApp 7.15 LTSR、

> XenDesktop 7.15 LTSR、および以前の VDA リリースを使用している場合の後方互換性のためにのみ含まれています。

この設定では、リッチなグラフィック表示が無効になります。この設定を使用すると、従来のグラフィック表示が取り消され、WAN やモバイル接続での帯域幅の使用量が削減されます。XenApp および XenDesktop 7.13 に導入された帯域幅の削減によって、このモードは廃止されます。

この設定はデフォルトで無効になっており、リッチなグラフィック表示が提供されます。

従来のグラフィックモードは、以下でサポートされています:

- Windows 7
- Windows Server 2008 R2 VDA。

従来グラフィックモードは、以下ではサポートされていません:

- Windows 8.x および 10
- Windows Server 2012、2012 R2、および 2016。

XenApp および XenDesktop 7.6 FP3 以降でのグラフィックモードおよびポリシーの最適化について詳しくは、CTX202687を参照してください。

許可される最大表示色数

> 注:
>
> Virtual Delivery Agent 7.x では、［従来のグラフィックモード］設定が有効な場合のみこの設定項目が適用されます。

この設定では、セッションで許可される最大表示色数を指定します。

デフォルトでは、1 ピクセルあたり 32 ビットまでの色数が許可されます。

この設定は Thinwire ドライバーおよび接続にのみ適用されます。プライマリディスプレイドライバーとして ThinWire 以外のドライバーを使用する VDA には適用されません。ThinWire 以外のドライバーを使用する VDA とは、Windows Display Driver Model（WDDM）ドライバーをプライマリディスプレイドライバーとして使用する VDA のことです。プライマリディスプレイドライバーとして Windows Display Driver Model（WDDM）ドライバーを使用するシングルセッション OS VDA（Windows 8 など）には、この設定は効果がありません。WDDM ドライバーを使用する Windows マルチセッション OS VDA（Windows Server 2019 など）の場合、この設定によりユーザーが VDA に接続できない可能性があります。

高い表示色数をサポートするには、より多くのメモリが必要です。メモリ不足時に自動的に色数を減らすには、［メモリが不足した時の表示モード］設定を使用します。この設定で色数を下げるオプションを選択すると、イメージの表示色数が少なくなります。

メモリ不足による表示品質の低下をユーザーに通知する

> 注:
>
> Virtual Delivery Agent 7.x では、［従来のグラフィックモード］設定が有効な場合のみこの設定項目が適用されます。

この設定では、色数または解像度が低下するときにユーザーに簡単なメッセージを表示するかどうかを指定します。

デフォルトでは、メッセージは表示されません。

3D 画像ワークロードの最適化

この設定では、グラフィックの負荷が過剰なワークロードに合わせて適切なデフォルト設定を構成します。グラフィックワークロードの負荷が大きいアプリケーションのユーザーに対してこの設定を有効にします。このポリシーは、セッションで GPU が利用可能な場合にのみ適用してください。その他の設定がこのポリシーのデフォルト設定を明示的に上書きする場合、そちらが優先されます。

デフォルトでは、3D 画像ワークロードの最適化は無効になっています。

キューイメージの破棄

> 注:
>
> Virtual Delivery Agent 7.x では、［従来のグラフィックモード］設定が有効な場合のみこの設定項目が適用されます。

この設定では、ほかのイメージで置換される中間イメージを破棄するかどうかを指定します。

デフォルトでは、キューイメージの破棄は有効になっています。

有効にすると、グラフィックがユーザーデバイス側に送信されるときのレスポンスが向上します。ただし、中間フレームが脱落するため、アニメーションの動きがスムーズでなくなる場合があります。

圧縮にビデオコーデックを使用する

エンドポイントでビデオのデコードを使用できる場合は、グラフィックの圧縮にビデオコーデックを使用できます。［画面全体］が選択された場合、ビデオコーデックにはすべてのデフォルトコーデックが適用されます。［領域をアクティブに変更］が選択された場合、画面上に変更が定期的にある領域にビデオコーデックが使用され、他のデータでは静止画圧縮およびビットマップのキャッシュが使用されます。エンドポイントでビデオのデコードを使用できない、またはビデオコーデックを使用しないように指定すると、静止画像圧縮とビットマックキャッシュの組み合わせが使用されます。［可能であれば使用］が指定されている場合、選択はさまざまな要素に基づいて行われます。選択方法が拡張されているため、結果はバージョンによって異なる場合があります。

現在のシナリオに最適な設定が自動的に選択されるようにするには、［可能であれば使用］を選択します。

ユーザーエクスペリエンスと帯域幅の改善のために最適化する場合、特にサーバー側でレンダリングするビデオや 3D グラフィックを多用する場合は、［画面全体］を選択します。

ビデオパフォーマンス、特に低帯域幅が改善されるように最適化しつつ、コンテンツが静的かつ徐々に変更されるようにするためにスケーラビリティを維持するには［領域をアクティブに変更］を選択します。この設定は、マルチモニターの展開でサポートされます。

サーバー CPU の負荷を最適化する場合、およびサーバー側でレンダリングするビデオやその他の画像処理に多くのリソースを消費するアプリケーションがほとんどない場合は、［ビデオコーデックを使用しない］を選択します。

デフォルトでは、［可能であれば使用］に設定されています。

ビデオのハードウェアエンコーディングの使用

この設定によりグラフィックハードウェア（搭載している場合）を利用して、画面要素をビデオコーデックで圧縮できます。該当するハードウェアが利用可能でない場合、VDA はソフトウェアビデオコーデックを使用して、CPU ベースのエンコーディングにフォールバックします。

このポリシー設定のデフォルトのオプションは ［有効］です。

複数のモニターがサポートされます。

ビデオデコーディングをサポートする Citrix Workspace アプリはすべて、ハードウェアエンコーディングで使用できます。

NVIDIA

NVIDIA GRID GPU の場合、ハードウェアエンコーディングはマルチセッション OS 対応 VDA およびシングルセッション OS 対応 VDA でサポートされています。

NVIDIA GPU は、NVENC ハードウェアエンコーディングをサポートする必要があります。サポートされている GPU の一覧については、「NVIDIA ビデオコーデック SDK」を参照してください。

NVIDIA GRID には、ドライバーのバージョン 3.1 以上が必要です。NVIDIA Quadro には、ドライバーのバージョン 362.56 以上が必要です。Citrix では NVIDIA リリース R361 ブランチからのドライバーをお勧めします。

無損失テキストは、NVENC ハードウェアエンコーディングと互換性がありません。無損失テキストを有効にした場合、無損失テキストは NVENC ハードウェアエンコーディングよりも優先されます。

［領域をアクティブに変更］に対する H.264 ハードウェアコーデックの選択的使用がサポートされています。

視覚的無損失圧縮（YUV 4:4:4）がサポートされています。視覚的無損失（グラフィックポリシー設定「視覚的無損失の圧縮を使用する」）には、Citrix Workspace アプリ 1808 以降または Citrix Receiver for Windows 4.5 以降が必要です。

Intel

Intel Iris Pro グラフィックプロセッサの場合、ハードウェアエンコーディングはシングルセッション OS 対応 VDA およびマルチセッション OS 対応 VDA でサポートされています。

サポート対象は、Intel Broadwell プロセッサファミリの Intel Iris Pro グラフィックプロセッサ以降です。Intel Remote Displays SDK バージョン 1.0 は必須であり、Intel の Web サイト「Remote Displays SDK」からダウンロードできます。

無損失テキストは、ビデオコーデックポリシーが画面全体に対して設定され、**3D** グラフィック用に最適化されたワークロードポリシーが無効になっている場合にのみサポートされます。

視覚的無損失（YUV 4:4:4）はサポートされていません。

Intel エンコーダーは最大で 8 つのエンコーディングセッションを可能にする優れたユーザーエクスペリエンスを提供します（たとえば、1 人のユーザーが 8 つのモニターを使用したり、8 人のユーザーが各自 1 つのモニターを使用したりするなど）。8 つ以上のエンコーディングセッションが必要な場合は、仮想マシンが接続するモニター数を確認してください。良好なユーザーエクスペリエンスを維持するために、管理者はこのポリシー設定をユーザー単位またはマシン単位に構成できます。

AMD

AMD の場合、ハードウェアエンコーディングはシングルセッション OS 対応 VDA でサポートされています。

AMD GPU が RapidFire SDK をサポートしている必要があります。たとえば、AMD Radeon Pro GPU や FirePro GPU です。

エンコーディングを行うには、最新の AMD ドライバーをインストールします。これらのドライバーはhttps://www.amd.com/en/supportからダウンロードできます。

無損失テキストは、AMD ハードウェアエンコーディングと互換性がありません。無損失テキストを有効にした場合、無損失テキストは AMD ハードウェアエンコーディングよりも優先されます。

［領域をアクティブに変更］に対する H.264 ハードウェアコーデックの選択的使用がサポートされています。

キャッシュのポリシー設定

August 17, 2024

このセクションには、狭帯域幅のクライアント接続でイメージデータをユーザーデバイス上にキャッシュする機能を有効にするための設定項目があります。

固定キャッシュしきい値

注: Virtual Delivery Agent 7.x では、［従来のグラフィックモード］設定が有効な場合のみこの設定項目が適用されます。

この設定では、ユーザーデバイスのハードドライブにビットマップをキャッシュするため、以前のセッションで頻繁に使用されたイメージを再利用できます。

デフォルトのしきい値は、3000000bps です。

帯域幅がこのしきい値を下回る場合、永続キャッシュ機能が有効になります。つまり、デフォルトの設定では、接続帯域幅が 3,000,000bps を下回る場合に、ビットマップがユーザーデバイスのハードドライブ上にキャッシュされます。

Framehawk のポリシー設定

August 17, 2024

> 重要:
>
> Citrix Virtual Apps and Desktops 7 1903 以降、Framehawk はサポートされなくなりました。代わりに、アダプティブトランスポートが有効なThinwireを使用します。

［**Framehawk**］セクションには、サーバーで Framehawk ディスプレイチャネルを有効化し、構成するためのポリシー設定項目があります。

Framehawk ディスプレイチャネル

この機能を有効にすると、サーバーは Framehawk ディスプレイチャネルを使用して、ユーザーのグラフィックスおよび入力リモート処理を試行します。この表示チャネルは、UDP を使用して、高い損失および遅延特性を示すネットワークに、より快適なユーザーエクスペリエンスを提供します。ただし、他のグラフィックモードよりも多くのサーバーリソースと帯域幅を使用する可能性もあります。

デフォルトでは、Framehawk ディスプレイチャネルは無効になっています。

Framehawk 表示チャネルポートの範囲

このポリシー設定項目では、VDA でユーザーデバイスとの Framehawk ディスプレイチャネルデータの送受信に使用される UDP ポート番号の範囲を指定します。ポート番号の形式は、最小ポート番号または最大ポート番号です。VDA は、各ポートの使用を試行します。まず、最小のポート番号から始めて、2 回目以降の試行では 1 つずつ番号を増やしていきます。ポートは、受信トラフィックと送信トラフィックに使用されます。

デフォルトでは、ポートの範囲は 3224、3324 です。

Keep-Alive のポリシー設定

August 17, 2024

［**Keep-Alive**］セクションには、ICA Keep-Alive メッセージの管理に関するポリシー設定があります。

ICA Keep-Alive タイムアウト

この設定では、ICA Keep-Alive メッセージの送信間隔を秒単位で指定します。

デフォルトでは、ICA Keep-Alive メッセージが 60 秒おきに送信されます。

ICA Keep-Alive メッセージの送信間隔として設定可能な範囲は、1〜3600 秒です。ただし、アイドル状態のセッションをネットワーク監視ソフトウェアで自動的に閉じるように設定している環境では、この設定を使用しないでください。

ICA Keep-Alive メッセージ

この設定では、ICA Keep-Alive メッセージを定期的に送信するかどうかを指定します。

デフォルトでは、ICA Keep-Alive メッセージは送信されません。

この設定を有効にすると、ネットワークの問題により切断されたセッションにユーザーが再接続できなくなることを防ぐことができます。また、サーバー側でセッションのアイドル状態が検出されたときに、リモートデスクトップサービス（RDS）によりセッションが切断されることを防ぐことができます。サーバーは、定期的に Keep-Alive メッセージを送信して、セッションがアクティブかどうかを検出します。セッションがアクティブでないことが検出されると、サーバーにより「切断」状態として認識されます。

ICA Keep-Alive は、セッション画面の保持機能を使用する環境では正しく動作しません。セッション画面の保持機能を使用しない環境でのみ、ICA Keep-Alive を有効にしてください。

関連する設定項目：セッション画面の保持。

ローカルアプリケーションアクセスのポリシー設定

August 17, 2024

［ローカルアプリアクセス］セクションには、ユーザーデバイス上にインストールされたローカルアプリケーションと、ホスト上のアプリケーションを管理するポリシー設定項目があります。これらのポリシー設定項目は、ホストされたデスクトップ環境の統合を管理します。

ローカルアプリアクセスを許可する

この設定では、ローカルアプリケーションとホスト上のアプリケーションの統合を許可または禁止します。これらのポリシー設定項目は、ホストされたデスクトップ環境の統合を管理します。

ユーザーがローカルのアプリケーションを起動すると、そのアプリケーションが仮想デスクトップ上で動作しているかのように表示されます。

ポリシーの ［ローカルアプリアクセスを許可する］設定を ［有効］に設定すると、ブラウザーコンテンツのリダイレクトはサポートされず、クライアント側のシステムトレイのバッテリー状態はデスクトップセッションに表示されません。

デフォルトでは、［ローカルアプリアクセスを許可する］は禁止されています。

URL のリダイレクトの禁止リスト

この設定では、ユーザーデバイス上のローカルの Web ブラウザーで開く Web サイトを指定します。これらの Web サイトには、次のものが含まれる場合があります:

- msn.com や newsgoogle.com などのロケール情報を必要とする Web サイト
- ユーザーデバイスでより適切にレンダリングされるリッチメディアコンテンツを含む Web サイト。

デフォルトでは、サイトは指定されていません。

URL のリダイレクトの許可リスト

この設定では、ユーザーデバイス側にリダイレクトしない Web サイトを指定します。

デフォルトでは、サイトは指定されていません。

モバイルデバイスでの動作のポリシー設定

August 17, 2024

［モバイルエクスペリエンス］セクションには、Citrix Mobility Pack の動作を制御するためのポリシー設定項目があります。

キーボードの自動表示

この設定では、モバイルデバイス画面上におけるキーボードの自動表示を有効または無効にします。

デフォルトでは、無効になっています。

タッチパネルでの操作に最適化されたデスクトップ

この設定は無効になっており、Windows 10 または Windows Server 2016 マシンでは使用できません。

この設定により、Citrix Workspace アプリの全体的なインターフェイスの動作が決まります。この設定では、タブレットデバイス用に最適化されたタッチフレンドリーなインターフェイスを許可または禁止します。

デフォルトでは、タッチパネルでの操作に最適化されたデスクトップが起動します。

通常の Windows インターフェイスのデスクトップを起動する場合は、［禁止］を選択します。

コンボボックスをデバイス側で表示する

この設定では、モバイルデバイスでのセッションで表示するコンボボックスの種類を指定します。モバイルデバイス側のコンボボックスコントロールを表示するには、このポリシー設定項目を［許可］に設定します。管理者がこの設定で許可を選択しても、iOS 向け Citrix Workspace アプリのユーザーは、セッション設定で通常の Windows コンボボックスの表示を選択できます。

デフォルトでは、［コンボボックスをデバイス側で表示する］機能は禁止されています。

マルチメディアのポリシー設定

August 17, 2024

［マルチメディア］セクションには、ユーザーセッションでの HTML5 および Windows のオーディオとビデオのストリーム配信の管理に関するポリシー設定項目があります。

> 警告
>
> レジストリエディターの使用を誤ると、深刻な問題が発生する可能性があり、オペレーティングシステムの再インストールが必要になる場合もあります。レジストリエディターの誤用による障害に対して、Citrix は一切責任を負いません。レジストリエディターは、お客様の責任と判断の範囲でご使用ください。また、レジストリファイルのバックアップを作成してから、レジストリを編集してください。

マルチメディアポリシー

デフォルトでは、Delivery Controller で設定されたすべてのマルチメディアポリシーは、次のレジストリに格納されます。

マシンポリシー:

HKEY_LOCAL_MACHINE\Software\Policies\Citrix\MultimediaPolicies

ユーザーポリシー:

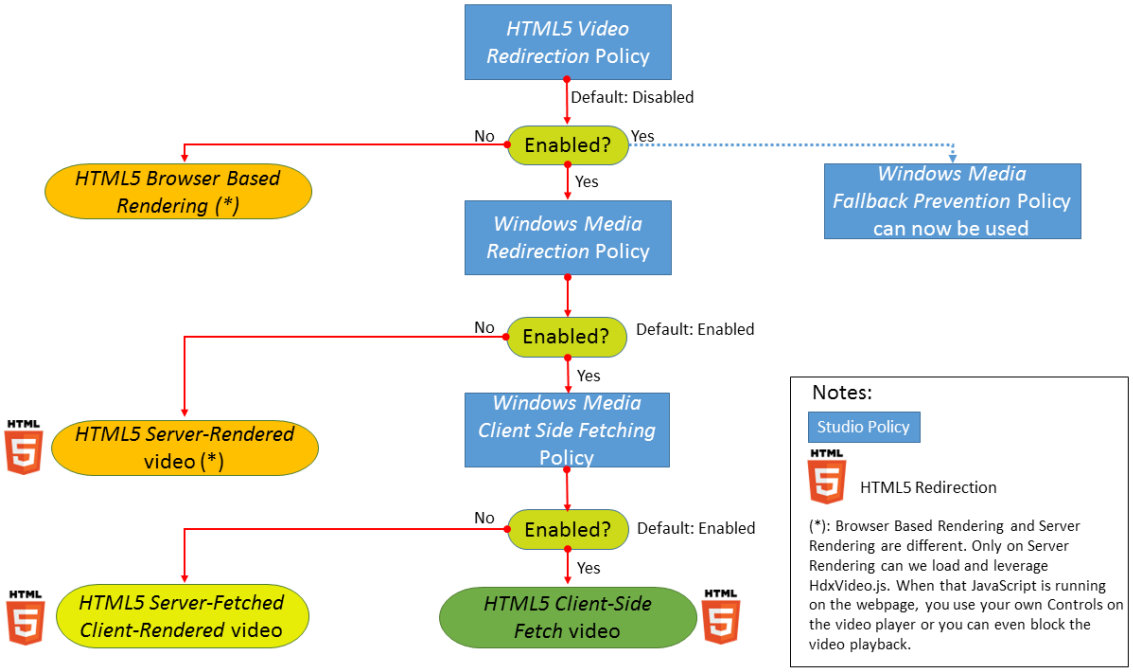
HKEY_LOCAL_MACHINE\Software\Policies\Citrix{ユーザーセッション ID}\User\MultimediaPolicies

現行のユーザーセッション ID を見つけるには、Windows コマンドラインで **qwinsta** コマンドを実行します。

HTML5 ビデオリダイレクト

Citrix Virtual Apps and Desktops サーバーがユーザーに HTML5 マルチメディア Web コンテンツを提供する方法を制御、最適化します。

デフォルトでは、この設定は無効になっています。



このリリースでは、この機能は管理対象 Web ページでのみ利用できます。HTML5 マルチメディアコンテンツが利用できる Web ページ（たとえば、社内研修サイトのビデオ）に JavaScript を追加する必要があります。

HTML5 ビデオリダイレクションを構成するには:

1. **HdxVideo.js** ファイルを、VDA のインストール先の%Program Files%/Citrix/ICA Service/HTML5 Video Redirection から、社内 Web ページの場所にコピーします。
2. 次の行を Web ページに挿入します（Web ページに別のスクリプトが設定されている場合は、**HdxVideo.js** をこのスクリプトの前に追加します）:
   ```
   <script src="HdxVideo.js"type="text/javascript"\></script>
   ```

注: HdxVideo.js が Web ページと同じ場所にない場合は、**src** 属性を使って HdxVideo.js へのフルパスを指定します。

JavaScript が制御された Web ページに追加されておらず、ユーザーが HTML5 ビデオを再生しているとします。この場合、Citrix Virtual Apps and Desktops はデフォルトでサーバー側のレンダリングになります。

Windows Media リダイレクトを許可しないと、HTML5 ビデオリダイレクションは機能しません。このポリシーは、サーバー側フェッチ/クライアント側レンダリングに必須であり、クライアント側フェッチに必要です。次に、クライアント側フェッチでは、［*Windows Media* のクライアント側でのコンテンツ取得］も許可する必要があります。

Microsoft Edge ではこの機能はサポートされていません。

HdxVideo.js により、ブラウザーの HTML5 プレーヤーのコントローラーが独自のものに置き換えられます。特定の Web サイトで HTML5 ビデオリダイレクションが有効であるかどうかを確認するには、プレーヤーのコントローラーを ［**HTML5** ビデオリダイレクション］ポリシーが［禁止］に設定されている場合のシナリオと比較します：

（このポリシーが［許可］に設定されている場合の Citrix のカスタムコントローラー）

（このポリシーが［禁止］に設定されているか未構成の場合のネイティブの Web ページコントローラー）

次のビデオコントロールがサポートされます。

- 再生
- 一時停止
- シーク
- リピート
- オーディオ
- 全画面

HTML5 ビデオリダイレクションのテストページを表示できます。

TLS、**HTML5** ビデオリダイレクト、**Web** ブラウザーコンテンツのリダイレクト

HTML5 ビデオリダイレクトを使用して、次のことができます：

- HTTPS Web サイトからビデオをリダイレクトする
- または
- Web ブラウザーコンテンツリダイレクトで Web サイト全体をリダイレクトする

これらの Web サイトに挿入された JavaScript は、VDA で動作する Citrix HDX HTML5 ビデオリダイレクションサービス（WebSocketService.exe）への TLS 接続を確立する必要があります。VDA の証明書ストアにある Citrix HDX HTML5 ビデオリダイレクトサービスは、次の 2 つを実行するカスタム証明書を生成します：

- ビデオリダイレクトの実現
- Web ページの TLS 整合性の維持

HdxVideo.js は、セキュア WebSocket を使用して VDA で動作する WebSocketService.exe と通信します。このプロセスはローカルシステムアカウントとして動作し、SSL の終了とユーザーセッションマッピングを実行します。

WebSocketService.exe は 127.0.0.1 ポート 9001 でリスンします。

ビデオ品質の制限

この設定は Windows Media にのみ適用され、HTML5 には適用されません。この設定を使用するには、［**WAN** 接続での **Windows Media** マルチメディアリダイレクトの最適化］を有効化する必要があります。

この設定では、HDX 接続で許可される最大ビデオ品質レベルを指定します。最大ビデオ品質を指定すると、マルチメディアコンテンツに対する一定レベルの QoS（Quality of Service）を保証できます。

デフォルトでは、この設定は構成されていません。

許可される最大ビデオ品質レベルを指定するには、次のいずれかのオプションを選択します。

- 1080p/8.5mbps
- 720p/4.0mbps
- 480p/720kbps
- 380p/400kbps
- 240p/200kbps

単一サーバー上で複数のビデオを同時に再生すると多くのリソースが消費され、サーバーのスケーラビリティが低下することがあります。

Microsoft Teams リダイレクト

この設定により、HDX テクノロジに基づいて Microsoft Teams を最適化できます。

このポリシーが有効でサポート対象のバージョンの Citrix Workspace アプリを使用している場合、VDA でこのレジストリキーの値は **1** に設定されます。Microsoft Teams アプリケーションはこのレジストリキーを VDI モードで読み取ってロードします。
レジストリキーを手動で設定する必要はありません。

HKEY_CURRENT_USER\Software\Citrix\HDXMediaStream

値の名前：MSTeamsRedirSupport

値：DWORD（1 - オン、0 -オフ）

> 注：
>
> Web Studio で使用できるポリシーがない古いバージョンの Controller で、バージョン 1906.2 以降の VDA を使用しているとします。古いバージョンのコントローラーの例として、バージョン 7.15 があります。この場

> 合、HDX 最適化は VDA でデフォルトで有効になっています。Workspace アプリのバージョンが 1907 以降の場合、Microsoft Teams は最適化モードで起動します。7.15 LTSR Controller および CR VDA が混在する場合の注意事項については、Knowledge Center の記事CTX205549を参照してください。
>
> この場合、特定のユーザーの機能を無効にするために、レジストリ設定を上書きできます。グループポリシーを使用してレジストリ設定を上書きし、ユーザーの組織単位にログオンスクリプトを適用します。

Microsoft Teams のリダイレクト機能はデフォルトでは有効になっています。

マルチメディア会議

この設定では、ビデオ会議アプリケーションによる最適化された Web カメラリダイレクションテクノロジの使用を許可または禁止します。

デフォルトでは、許可されます。

この設定をポリシーに追加するときは、[**Windows Media** リダイレクト］設定で ［許可］（デフォルト）が選択されていることを確認してください。

［マルチメディア会議］を使用する場合、次の条件を満たしていることを確認してください:

- マルチメディア会議に使用する Web カメラの製造元が提供するドライバーが、クライアントにインストール済みである。
- ビデオ会議セッションの開始前に Web カメラをユーザーデバイスに接続している。サーバーで、複数の Web カメラを同時に使用することはできません。ユーザーデバイス上に複数の Web カメラが装着されている場合、サーバーは最初に検出した Web カメラを使用しようと試みます。この試みは、ビデオ会議セッションが正常に作成されるまで続きます。

このポリシーは、汎用 USB リダイレクトを使用して Web カメラをリダイレクトする場合は必要ありません。その場合は、VDA に Web カメラドライバーをインストールします。

WAN 接続での **Windows Media** マルチメディアリダイレクトの最適化

この設定は Windows Media にのみ適用され、HTML5 には適用されません。この設定により、次のことが可能になります:

- リアルタイムマルチメディアトランスコーディング
- 劣化ネットワークを介したモバイルデバイスへのオーディオおよびビデオメディアストリーム配信の許可
- Windows Media コンテンツの WAN 経由の配信方法を改善することによる、ユーザーエクスペリエンスの向上

デフォルトでは、WAN を介した Windows Media コンテンツの配信が最適化されます。

この設定をポリシーに追加するときは、[**Windows Media** リダイレクト］設定で ［許可］が選択されていることを確認してください。

この設定を有効にすると、メディアのストリーム配信を有効にするリアルタイムマルチメディアトランスコーディングが必要に応じて自動的に適用されます。また、極端なネットワーク条件でもシームレスなユーザーエクスペリエンスを提供します。

WAN 接続での **Windows Media** マルチメディアリダイレクトでの **GPU** の使用

この設定は Windows Media にのみ適用され、Virtual Delivery Agent（VDA）上のグラフィック処理ユニット（GPU）でリアルタイムマルチメディアトランスコード処理を行うことができるようになります。これにより、サーバースケーラビリティが改善されます。GPU でのトランスコード処理は、VDA 側にハードウェアアクセラレーションをサポートする GPU が搭載されている場合にのみ可能になります。適切な GPU がない場合は、CPU がトランスコード処理を行います。

注：GPU でのトランスコード処理は、NVIDIA 社の GPU でのみサポートされます。

デフォルトでは、WAN を介した Windows Media コンテンツ配信を VDA 側の GPU を使用して最適化する機能は禁止されています。

この設定をポリシーに追加するときは、以下の設定が存在し、［許可］に設定されていることを確認してください：

- **Windows Media** リダイレクト
- **WAN** 接続での **Windows Media** マルチメディアリダイレクトの最適化設定

Windows メディアフォールバック防止

この設定は、Web ブラウザーコンテンツのリダイレクト、HTML 5、Windows Media に適用されます。この設定で HTML5 をサポートするには、［**HTML5** ビデオリダイレクション］ポリシーを ［許可］に設定します。

管理者は **Windows** メディアのフォールバック防止ポリシー設定を使って、ユーザーへのストリーム配信コンテンツの配信方法を指定できます。

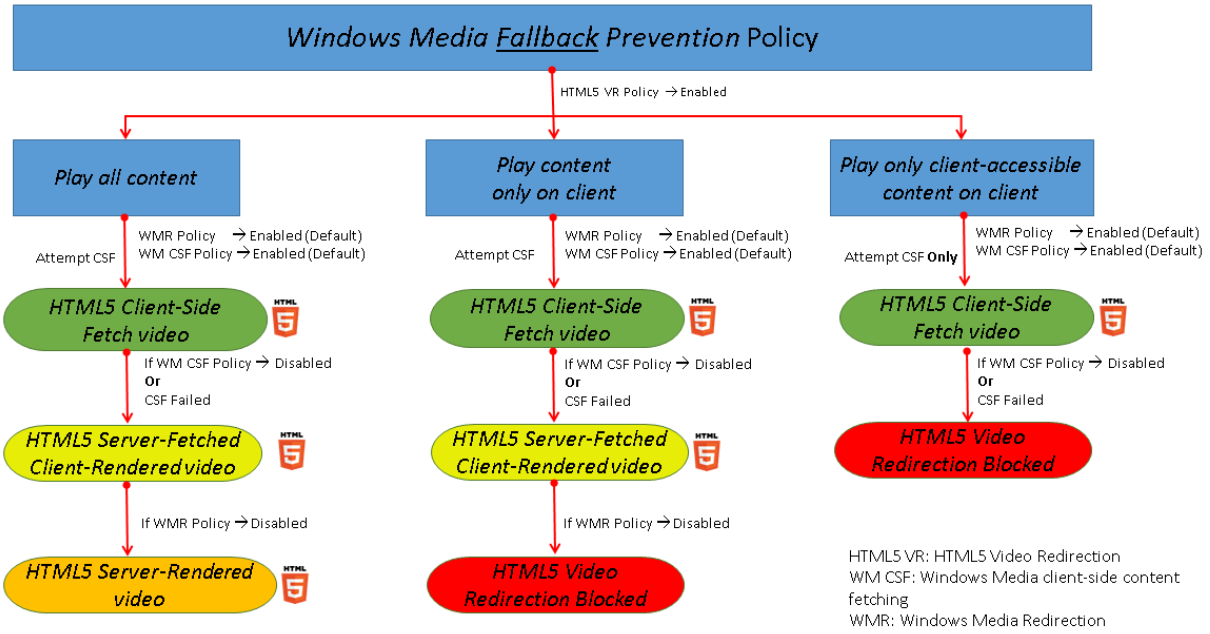
デフォルトでは、この設定は構成されていません。この設定が［未構成］に設定されている場合の動作は、［すべてのコンテンツを再生］のものと同じになります。

この設定を構成するには、次のいずれかのオプションを選択します。

- すべてのコンテンツを再生：クライアント側でのコンテンツ取得、Windows Media リダイレクトの順に試行します。失敗した場合、サーバー上でコンテンツを再生します。
- クライアントにあるすべてのコンテンツのみを再生：クライアント側でのフェッチ、Windows Media リダイレクトの順に試行します。失敗した場合、コンテンツは再生されません。
- クライアント上のクライアントがアクセスできるコンテンツのみを再生：クライアント側でのフェッチのみを試行します。失敗した場合、コンテンツは再生されません。

コンテンツが再生されない場合、次のエラーメッセージがプレーヤーウィンドウに表示されます（デフォルトの経過時間は 5 秒）：


```
"Company has blocked video because of lack of resources"
```



エラーメッセージが表示される期間は、VDA の次のレジストリキーでカスタマイズできます。レジストリにエントリがない場合は、期間はデフォルトで 5 秒間になります。

レジストリパスは、VDA のアーキテクチャによって異なります:

\HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\HdxMediastream

または

\HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxMediastream

レジストリキー:

値の名前:VideoLoadManagementErrDuration

種類:DWORD

範囲:1 から DWORD 制限まで(デフォルト = 5)

単位:秒

Windows Media のクライアント側でのコンテンツ取得

この設定は HTML5 と Windows Media の両方に適用されます。この設定では、インターネットまたはイントラネット上のマルチメディアファイルを、XenApp や XenDesktop のホストサーバーを介さずにソースプロバイダーからユーザーデバイスへ直接ストリーム配信することを許可または禁止します。

デフォルトでは、［許可］に設定されています。この設定を許可すると、ネットワークの使用状況とサーバーのスケーラビリティが向上します。この改善は、メディア上の処理をホストサーバーからユーザーデバイスに移行することで実現されます。また、ユーザーデバイス上に Microsoft DirectShow や Media Foundation などの高度なマルチメディアフレームワークをインストールする必要もなくなります。ユーザーデバイスに必要なのは、URL からファイルを再生する機能だけです

この設定をポリシーに追加するときは、［**Windows Media** リダイレクト］設定で ［許可］が選択されていることを確認してください。［**Windows Media** リダイレクト］設定を無効にすると、Windows Media のクライアント側でのコンテンツ取得機能も無効になります。

Windows Media リダイレクト

この設定は HTML5 と Windows Media の両方に適用され、サーバーでのユーザーへのオーディオとビデオのストリーム配信方法を制御および最適化します。

デフォルトでは、［許可］に設定されています。HTML5 の場合、［**HTML5** ビデオリダイレクション］ポリシーが ［禁止］に設定されているとこの設定は適用されません。

この設定を有効にすると、セッション内で再生されるオーディオおよびビデオの品質が向上して、ユーザーデバイス上のファイルを再生しているときの品質に近くなります。マルチメディアデータはサーバーからユーザーデバイスに、元の圧縮されたままの形で配信され、ユーザーデバイス側でメディアの展開およびレンダリングが行われます。

Windows Media ダイレクトでは、Microsoft 社の DirectShow、DirectX Media Objects（DMO）、および Media Foundation 規格に準拠するコーデックでエンコードされたマルチメディアファイルが最適化されます。ユーザーデバイス側でメディアファイルの展開およびレンダリングを行うため、そのファイルのエンコーディング形式をサポートするコーデックがユーザーデバイス上にインストールされている必要があります。

Citrix Workspace アプリでは、オーディオはデフォルトでは無効になっています。ユーザーが ICA セッション内でマルチメディアアプリケーションを実行できるようにするには、管理者がオーディオのサポートを有効にして、ユーザーが Citrix Workspace アプリのオーディオ機能を有効にする必要があります。

Windows メディアリダイレクトによるメディアの再生品質が、基本的な ICA 圧縮および通常のオーディオ機能での品質よりも悪い場合は、［禁止］を選択します。キーフレームの周波数が低いメディアデータを狭帯域幅接続で再生する場合などで、この機能による問題がまれに生じることがあります。

Windows Media リダイレクトのバッファーサイズ

この設定は古いものであり、HTML5 には適用されません。

この設定では、マルチメディアアクセラレーションのバッファーサイズを 1〜10 秒の間で指定します。

デフォルトのバッファーサイズは 5 秒です。

Windows Media リダイレクトのバッファーサイズ使用

この設定は古いものであり、HTML5 には適用されません。

この設定では、[**Windows Media** リダイレクトバッファーサイズ] 設定で指定したバッファーサイズを有効または無効にします。

デフォルトでは、指定したバッファーサイズが使用されません。

この設定が無効の場合、または **Windows Media** リダイレクトバッファーサイズ設定が構成されていない場合、サーバーではデフォルトのバッファーサイズ値（5 秒）が使用されます。

マルチストリーム接続のポリシー設定

August 17, 2024

[マルチストリーム接続] セクションには、セッションでの複数 ICA 接続の QoS（サービス品質）優先度の管理に関するポリシー設定項目があります。

> 注:
>
> マルチストリーム接続ポリシーが有効になっている場合、MTU Discovery はサポートされません。

UDP を使用したオーディオ

この設定では、サーバーの UDP を使用したオーディオを許可または禁止します。

デフォルトでは許可されます。

この機能を有効にすると、サーバー上の UDP ポートが開き、[UDP でのオーディオリアルタイムトランスポート] 設定が有効なすべての接続でそのポートが使用されます。

オーディオ **UDP** ポートの範囲

この設定は、Virtual Delivery Agent（VDA）が使用するポート番号の範囲（最小ポート番号、最大ポート番号）を指定します。この仕様は、オーディオパケットデータをユーザーデバイスと相互通信するのに役立ちます。VDA では、オーディオデータの送受信に各 UDP ポートペアの使用が試行されます。まず最小のポート番号が使用され、以降の試行では 2 ずつ番号を増やしていきます。各ポートは、受信トラフィックと送信トラフィックの両方に使用されます。

デフォルトでは、「16500,16509」の範囲が設定されています。

マルチポートポリシー

この設定では、ICA トラフィックで使用される TCP ポートおよび各ポートのネットワーク優先度を指定します。

デフォルトでは、プライマリポート（2598）に優先度［高］が設定されています。

ポートには、以下の優先度を設定できます。

- 最高 - Web カメラを使ったビデオ会議など、リアルタイムプロセスに適しています。
- 高 - 画面、キーボード、マウスなど、インタラクティブなトラフィックに適しています。
- 中 - クライアントドライブマッピング機能など、バルクプロセスに適しています。
- 低 - 印刷など、バックグラウンドプロセスに適しています。

各ポートには異なる優先度を設定する必要があります。つまり、CGP ポート 1 と CGP ポート 3 の両方で優先度に［最高］を設定することはできません。

ポートの優先度設定を削除するには、ポート番号として「0」を入力します。プライマリポートの優先度設定を削除したり変更したりすることはできません。

この設定項目をポリシーに追加したら、サーバーを再起動します。この設定は、［マルチストリームコンピューター］設定のポリシー設定が有効な場合のみ適用されます。

マルチストリームコンピューター設定

この設定では、サーバーのマルチストリーム機能を有効または無効にします。

デフォルトでは、無効になっています。コンピューターポリシーのマルチストリームポリシー設定は、Citrix SD-WAN やサードパーティ製のルーターを使用する環境で QoS（サービス品質）優先度を指定するときに使用できます。

マルチストリームが有効になっている場合、アダプティブトランスポートの機能である MTU Discovery はサポートされません。

この設定の変更を反映させるには、サーバーを再起動する必要があります。

> 重要:
>
> この設定項目を、帯域幅を制限するポリシー設定（［セッション全体の最大帯域幅］など）と一緒に使用すると、予期しない動作が発生する可能性があります。ポリシーでこの設定を使用する場合は、帯域幅を制限する設定を構成しないでください。

マルチストリームユーザー設定

この設定では、ユーザーデバイスのマルチストリーム機能を有効または無効にします。

デフォルトでは、すべてのユーザーに対して無効になっています。マルチストリームユーザー設定は、Citrix SD-WAN やサードパーティ製のルーターを使用する環境で QoS（サービス品質）優先度を指定するときに使用できます。

この設定は、［マルチストリームコンピューター］設定のポリシー設定が有効なホストに対してのみ適用されます。

> 重要:
>
> この設定項目を、帯域幅を制限するポリシー設定（[セッション全体の最大帯域幅］など）と一緒に使用すると、予期しない動作が発生する可能性があります。ポリシーでこの設定を使用する場合は、帯域幅を制限する設定を構成しないでください。

マルチストリーム仮想チャネルの割り当て設定

マルチストリーム使用時に仮想チャネルが割り当てられる ICA ストリームを指定します。

これらの設定を構成しない場合、仮想チャネルはデフォルトのストリームに保持されます。仮想チャネルを ICA ストリームに割り当てるには、仮想チャネル名の横の［ストリーム番号］一覧から目的のストリーム番号（0、1、2、3）を選択します。

使用環境にカスタム仮想チャネルがある場合、［追加］をクリックして ［仮想チャネル］の下のテキストボックスに仮想チャネル名を入力し、その隣の ［ストリーム番号］一覧からストリーム番号を選択します。実際の仮想チャネル名を入力し、フレンドリ名は使用しないでください。例：Citrix Browser Acceleration ではなく CTXSBR と入力します。

これらの設定は、マルチストリームコンピューター設定を有効にしたときのみ機能します。

デフォルトの仮想チャネルおよびストリーム割り当ては次のとおりです:

- AppFlow：2
- オーディオ：0
- Web ブラウザーコンテンツリダイレクト：2
- クライアント側 COM ポートのマッピング：3
- クライアントドライブマッピング：2
- クライアント側プリンターのマッピング：3
- クリップボード：2
- CTXDND：1（注：これは、Citrix セッションとローカルエンドポイント間のファイルのドラッグアンドドロップをサポートします。）
- DVC プラグイン（DVC プラグインのフレンドリ名から自動的に生成された、または管理者によって割り当てられた静的 VC 名）：2
- End User Experience Monitoring：1
- ファイル転送（HTML5 Receiver）：2
- 汎用データ転送：2
- ICA コントロール：1
- Input Method Editor：1
- 従来のクライアント側プリンターのマッピング（COM1）：1、3
- 従来のクライアント側プリンターのマッピング（COM1）：2、3
- 従来のクライアント側プリンターのマッピング（LPT1）：1、3
- 従来のクライアント側プリンターのマッピング（LPT2）：2、3

- ライセンス管理：1
- Microsoft Teams/WebRTC リダイレクト：1
- モバイルデバイス上の Receiver：1
- マルチタッチ：1
- ポート転送：2
- リモートオーディオおよびビデオ拡張機能（RAVE）：2
- シームレス（透過型ウィンドウ統合）：1
- センサーおよび位置情報：1
- スマートカード：1
- Thinwire グラフィック：1
- 透過型 UI 統合/ログオン状態：2
- TWAIN リダイレクト：2
- USB：2
- 遅延のないフォントとキーボード：2
- 遅延のないデータチャネル：2

仮想チャネルの割り当てと優先度について詳しくは、Knowledge Center のCTX131001を参照してください。

ポートリダイレクトのポリシー設定

August 17, 2024

［ポートリダイレクト］セクションには、クライアント側の LPT ポートおよび COM ポートのマッピングに関するポリシー設定項目があります。

7.0 より前のバージョンの Virtual Delivery Agent の場合は、次のポリシー設定を使用してポートリダイレクトを構成します。**7.0** から **7.8** のバージョンの VDA の場合は、このような設定はレジストリを使って行います。詳しくは、「レジストリを使った COM ポートおよび LPT ポートリダイレクト設定の構成」を参照してください。VDA バージョン **7.9** の場合は、次のポリシー設定を使用します。

クライアント **COM** ポートを自動接続する

この設定では、ユーザーのログオン時にクライアント側の COM ポートに自動的に接続する機能を有効または無効にします。

デフォルトでは無効になっています。

クライアント **LPT** ポートを自動接続する

この設定では、ユーザーのログオン時にクライアント側の LPT ポートに自動的に接続する機能を有効または無効にします。

デフォルトでは無効になっています。

クライアント **COM** ポートリダイレクト

この設定では、COM ポートのクライアント側へのリダイレクトを許可または禁止します。

デフォルトでは禁止されます。

関連する設定項目は以下のとおりです:

- COM ポートリダイレクトの最大帯域幅 (Kbps)
- COM ポートリダイレクトの最大帯域幅（%）

クライアント **LPT** ポートリダイレクト

この設定では、LPT ポートのクライアント側へのリダイレクトを許可または禁止します。

デフォルトでは禁止されます。

LPT ポートは、印刷ジョブを LPT ポートに送信するレガシーアプリケーションでのみ使用されます。LPT ポートは、ユーザーデバイス上の印刷オブジェクトに印刷ジョブを送信するレガシーアプリケーションでは使用されません。最近のアプリケーションでは、LPT ポートではなくプリンターオブジェクトに印刷ジョブが送信されます。このポリシー設定は、LPT ポートへの出力を行うレガシーアプリケーションをホストするサーバーに対してのみ使用します。

クライアントの COM ポートのリダイレクトは双方向ですが、LPT ポートのリダイレクトは出力のみで ICA セッション内の\\client\LPT1 と\\client\LPT2 に制限されていることに注意してください。

関連する設定項目は以下のとおりです:

- LPT ポートリダイレクトの最大帯域幅（Kbps）
- LPT ポートリダイレクトの最大帯域幅（%）

印刷のポリシー設定

August 17, 2024

印刷セクションには、クライアントからの印刷の管理に関するポリシー設定が含まれています。

クライアントプリンターリダイレクト

この設定項目では、ユーザーのログオン時にクライアントプリンターをサーバーに自動的にマップすることを許可または禁止します。

デフォルトでは許可されます。この設定項目が無効の場合、PDF プリンターはセッションで自動作成されません。

関連する設定項目：クライアントプリンターを自動作成する

デフォルトプリンター

この設定では、セッションのデフォルトのクライアントプリンターとして設定するプリンターを指定します。

デフォルトでは、ユーザーの現在のデフォルトプリンター（通常使うプリンター）がセッションのデフォルトプリンターとして使用されます。

［デフォルトプリンターの設定を変更しない］を選択すると、リモートデスクトップサービスまたは Windows のユーザープロファイルで設定されているデフォルトプリンターが使用されます。この場合、デフォルトプリンターはプロファイルに保存されず、ほかのセッションやクライアント側のプロパティにより変更されなくなります。このオプションでは、セッションで最初に自動作成されたプリンターがセッションのデフォルトプリンターになります。つまり、以下のどちらかのプリンターになります。

- Windows サーバーの ［コントロールパネル］のデバイスとプリンターでローカルに追加された最初のプリンター。
- サーバーにローカルプリンターが追加されていない場合は、最初に自動作成されたプリンター。

プロファイルの設定に基づいてユーザーに最も近いプリンターを提供する（近接プリンター機能を使用する）場合に、このオプションを使用できます。

プリンター割り当て

この設定は、［デフォルトプリンター］設定および［セッションプリンター］設定の代わりに使用します。特定のサイト、大規模グループ、または組織単位用のポリシーを構成する場合は、［デフォルトプリンター］設定および［セッションプリンター］設定を使用します。［プリンター割り当て］設定は、多くのプリンターのグループを複数のユーザーに割り当てる場合に使用します。

この設定では、ユーザーデバイスを一覧に追加して、そのユーザーデバイス上のデフォルトプリンターがセッションでどのように使用されるかを指定します。

デフォルトでは、ユーザーの現在のデフォルトプリンター（通常使うプリンター）がセッションのデフォルトプリンターとして使用されます。

また、各ユーザーデバイスに対してセッションで自動作成するネットワークプリンターを指定します。デフォルトでは、プリンターは指定されていません。

- デフォルトプリンター値は、以下のように設定します。

  ユーザーデバイスの現在のデフォルトプリンターを使用する場合は、［変更しない］を選択します。

  現在のリモートデスクトップサービスまたは Windows のユーザープロファイルで設定されているデフォルトプリンターを使用する場合は、［変更しない］を選択します。この場合、デフォルトプリンターはプロファイルに保存されず、ほかのセッションやクライアント側のプロパティにより変更されなくなります。このオプションでは、セッションで最初に自動作成されたプリンターがセッションのデフォルトプリンターになります。つまり、以下のどちらかのプリンターになります。

  - Windows サーバーの ［コントロールパネル］**>**［デバイスとプリンター］でローカルに追加された最初のプリンター。
  - サーバーにローカルプリンターが追加されていない場合は、最初に自動作成されたプリンター。

- セッションプリンター値を設定するには、自動作成するプリンターの UNC パスを入力します。この一覧の設定は、ユーザーがログオンするたびに適用できます。

プリンター自動作成イベントログの設定

この設定では、プリンターの自動作成処理中にログに記録するイベントを指定します。エラーおよび警告をログに記録しない、エラーのみを記録する、またはエラーおよび警告を記録することを選択できます。

デフォルトでは、エラーおよび警告がログに記録されます。

たとえば、プリンターのネイティブドライバーをインストールできず、代わりにユニバーサルプリンタードライバーがインストールされた場合は、警告がログに記録されます。このような状況でユニバーサルプリンタードライバーを使用できるようにするには、［ユニバーサル印刷の使用］設定で［ユニバーサル印刷のみを使用する］または［要求されたドライバーを使用できない場合にのみユニバーサル印刷を使用する］を選択します。

セッションプリンター

この設定では、セッションで自動作成するネットワークプリンターを指定します。ICA/HDX セッションでは、Citrix Print Manager サービス（CpSvc.exe）によって、セッションプリンターポリシー設定で指定されたネットワークプリンターごとに、セッションログオン時にネットワークプリンター接続が作成されます。プリンターは、セッションのログオフ時に削除されます。デフォルトでは、プリンターは指定されていません。

セッションプリンターポリシー設定では、ネットワークプリンターは Windows プリントサーバーまたは Citrix ユニバーサルプリントサーバー上に存在します。

- **Windows** プリントサーバー： 1 つまたは複数のネットワークプリンターを共有します。ネットワークプリンターを使用するために必要なネイティブのプリンタードライバーも用意されています。
- ユニバーサルプリントサーバー： Citrix ユニバーサルプリントサーバーソフトウェアがインストールされている Windows プリントサーバーです。

Windows プリントサーバーを使用する場合、Citrix Print Manager サービスはネイティブのプリンタードライバーを使用してネットワークプリンターの接続を作成します。Citrix Virtual Apps サーバーには、ネイティブのプリンタードライバーがインストールされている必要があります。

Citrix ユニバーサルプリントサーバーを使用する場合、Citrix Print Manager サービスはネイティブのプリンタードライバー、Citrix ユニバーサルプリンタードライバー、または Citrix Universal XPS プリンタードライバーのいずれかを使用してネットワークプリンターの接続を作成します。使用するドライバーは、ユニバーサルプリントドライバーの使用ポリシー設定によって制御されます。

現在、すべての Windows プリンタードライバーのバージョンは、v3 または v4 のいずれかです。詳しくは、Support for the Microsoft V3 and V4 Printer Driver Architecturesを参照してください。

セッションプリンターを追加してからセッションに表示されるかどうかを確認するには、以下の手順を実行します:

1. Web Studio にサインインし、左側のペインで ［ポリシー］ を選択し、［ポリシー］ タブをクリックします。
2. セッションプリンターポリシーを有効にします。
3. このポリシーに、セッションプリンターを追加します。自動作成するプリンターを追加するには、そのプリンターの UNC パスを入力します。この一覧の設定は、ユーザーがログオンするたびに適用できます。セッションプリンターが一覧に表示されている必要があります。
4. ポリシーの設定後、公開アプリケーションにセッションプリンターが表示されないことがあります。この問題は、Citrix Virtual Apps サーバーのプリンタードライバーがないか、ポリシーが作成されているが有効になっていない場合に発生する可能性があります。

   > 注:
   >
   > セッションプリンターにネイティブプリンタードライバーが必要で、ネイティブプリンタードライバーが VDA にインストールされていない場合、セッションプリンターがセッションで作成されないことがあります。

5. 公開デスクトップを起動して、手動で［デバイスとプリンター］ **>** ［コントロールパネル］ からセッションプリンターを追加します。
6. これが失敗する場合は、Citrix Virtual Apps サーバーとプリントサーバー間の通信を調査します。RDP でのテストの実行を検討してください。

プリンターの自動作成を待機する

Citrix Virtual Desktops でこの機能を有効にするには、Delivery Controller のポリシーを有効にします。

プリンターの自動作成を待機する（サーバーデスクトップ）:

この設定では、クライアントがリダイレクトされたプリンターが自動作成されるまでセッションへの接続を遅延させることができます。

デフォルトでは、プリンターの作成を待機せずに接続します。

プリンターの自動作成を待機する（**Citrix Virtual Apps**）：

次の PowerShell コマンドレットを実行すると、アプリケーションが開く前にクライアントリダイレクトプリンターが自動作成されるように、マルチセッションホスト上で実行されている Virtual Apps への接続を遅延させることができます。

```
Set-BrokerApplication -Name <VirtualAppName> -WaitForPrinterCreation $true
```

デフォルトでは、プリンターの作成を待機せずに接続します。

クライアントプリンターのポリシー設定

August 17, 2024

［クライアントプリンター］セクションには、クライアントプリンターに関するポリシー設定項目があります。これには、クライアントプリンターの自動作成、プリンタープロパティの保存、およびプリントサーバーへの接続のための設定が含まれています。

クライアントプリンターを自動作成する

この設定では、自動作成するクライアントプリンターを指定します。この設定は、デフォルトのクライアントプリンター自動作成設定より優先されます。

デフォルトでは、すべてのクライアントプリンターが自動作成されます。

この設定は、［クライアントプリンターリダイレクト］設定で ［許可］が選択されている場合にのみ適用されます。

この設定では、次のオプションを選択します。

- ［すべてのクライアントプリンターを自動作成する］では、ユーザーデバイス上のすべてのプリンターが自動作成されます。
- ［デフォルトのクライアントプリンターのみを自動作成する］では、ユーザーデバイス上のデフォルトプリンターのみが自動作成されます。
- ［ローカル（ネットワークを介さない）クライアントプリンターのみを自動作成する］では、ユーザーデバイスのローカルポート（LPT ポート、COM ポート、USB ポート、TCP/IP ポートなど）に直接接続されているプリンターのみが自動作成されます。
- ［クライアントプリンターを自動作成しない］では、ユーザーがログオンするときのすべてのクライアントプリンターの自動作成が無効になります。リモートデスクトップサービス（RDS）で設定されているクライアントプリンターの自動作成オプションが適用されるようにするには、このオプションを選択して、そのポリシーの優先度をほかのポリシーよりも高くします。

汎用ユニバーサルプリンターを自動作成する

この設定では、セッションで Citrix ユニバーサルプリンターの汎用印刷オブジェクトを自動作成する機能を有効または無効にします。これらのセッションには、ユニバーサル印刷と互換性のあるユーザーデバイスが使用されているセッションのみが含まれます。

デフォルトでは、汎用ユニバーサルプリンターオブジェクトは自動作成されません。

関連する設定項目は以下のとおりです:

- ユニバーサル印刷の使用
- ユニバーサルドライバーの優先度

PDF ユニバーサルプリンターを自動作成する

この設定では、以下を使用するセッションでの Citrix PDF プリンターの自動作成機能を有効または無効にします:

- Windows 向け Citrix Workspace アプリ（VDA 7.19 以降）
- HTML5 向け Citrix Workspace アプリ
- Chrome 向け Citrix Workspace アプリ

デフォルトでは、Citrix PDF プリンターは自動作成されません。

クライアントプリンター名

この設定では、自動作成されるクライアントプリンターの命名規則を選択します。

デフォルトでは、標準のプリンター名が使用されます。

[標準のプリンター名］を選択すると、「セッション 3 のクライアント名の HP LaserJet 4」などのプリンター名が作成されます。

古いスタイルのクライアントプリンター名を使用し、製品の XenDesktop バージョンに存在する従来のプリンター名との後方互換性を維持するには、［従来のプリンター名］を選択します。このオプションは、製品の最新の Citrix Virtual Apps and Desktops バージョンで使用できます。この場合、「Client/clientname#/HPLaserJet 4」などの名前が使用されます。このオプションは安全性に欠けます。

HTML5 向け Citrix Workspace アプリから起動したセッションで Citrix PDF プリンターを使用する場合は、［クライアントプリンター名］設定をデフォルトとして設定するか、［標準のプリンター名］を選択します。［従来のプリンター名］を選択した場合、HTML5 向け Citrix Workspace アプリは Citrix PDF プリンターオプションをサポートしません。

プリントサーバーへの直接接続

この設定では、クライアントプリンターを使用するときに、クライアントを経由せずに仮想デスクトップやホストサーバーからプリントサーバーに直接接続することを有効または無効にします。ここでは、クライアントプリンターはネットワーク共有上でホストされているものとします。

デフォルトでは有効になっています。

仮想デスクトップやホストサーバーとネットワークプリントサーバーが同一 LAN 上にあり、WAN で隔たれていない場合に直接接続を有効にします。この場合、仮想デスクトップやホストサーバーから LAN を介してプリントサーバーに直接印刷データが転送されるため、処理が高速になります。

仮想デスクトップやホストサーバーとネットワークプリントサーバーが WAN で隔たれていたり、遅延や帯域幅の問題が生じたりする場合は、直接接続を無効にできます。直接接続を無効にすると、印刷ジョブがユーザーデバイスに送信され、そこからネットワークプリントサーバーにリダイレクトされます。ユーザーデバイスに送信されるデータは圧縮されるため、データが WAN を横断するときに消費される帯域幅が少なくなります。

同じ名前を持つネットワークプリンターが 2 つ存在する場合は、ユーザーデバイスと同じネットワーク上のプリンターが使用されます。

プリンタードライバーのマッピングと互換性

この設定では、自動作成されるクライアントプリンターのドライバー置換規則を指定します。

この設定は、自動作成されるクライアントプリンターの一覧から Microsoft OneNote と XPS Document Writer を除外して構成されます。

ドライバー置換規則を定義すると、プリンターの自動作成時に特定のドライバーの使用を許可したり、また、作成されたプリンターがユニバーサルプリンタードライバーのみを使用することを許可できます。ドライバーの置換規則では、サーバーとクライアント間でドライバー名をマップして、ユーザーデバイスから提供されるプリンタードライバーではなくサーバー上のドライバーが使用されるように設定します。これにより、サーバー側のドライバーとクライアント側のドライバーの名前が異なっていても、サーバー上のアプリケーションからクライアントプリンターに出力できるようになります。

以下の操作を実行できます:

- ドライバーマッピングの追加
- 既存のマッピングの編集
- マッピングに対するカスタム設定の上書き
- マッピングの削除
- 一覧のドライバーエントリの順序の変更

マッピングを追加するには、クライアント側プリンタードライバーの名前を入力し、それを置換するサーバー側プリンタードライバーを選択します。

プリンタープロパティの保存

この設定では、プリンターのプロパティを保存するかどうか、どこに保存するかを指定します。

デフォルトでは、システムの判定により、クライアントデバイスに保存できない場合にのみユーザープロファイルにプリンタープロパティが保存されます。

この設定では、次のオプションを選択します。

- ［クライアントデバイスにのみ保存する］は、更新されないユーザープロファイル（固定プロファイルや移動プロファイル）を使用する環境で選択します。
- ［ユーザープロファイルにのみ保存する］は、使用帯域幅とログオン速度に制限があるユーザーデバイス（このオプションではネットワークトラフィックが軽減されます）、または古いプラグインソフトウェアを使用するユーザーのためのオプションです。このオプションでは、サーバー上のユーザープロファイルにプリンタープロパティを保存し、ユーザーデバイス上のプロパティを使用しません。このオプションはリモートデスクトップサービス（RDS）の移動プロファイルにのみ適用されます。
- ［クライアントに保存できない場合にのみユーザープロファイルに保存する］では、システムによりプリンタープロパティの保存先が決定されます。ユーザーデバイスに保存できない場合にのみ、ユーザープロファイルにプリンタープロパティが保存されます。さまざまな環境やクライアントの条件に対応できるオプションですが、システムチェック処理が行われるため、ログオン時に遅延が生じたり使用帯域幅が増えたりすることがあります。
- ［プリンタープロパティを保持しない］を選択した場合、プリンタープロパティは保持されません。

クライアントプリンターの保持と復元

この設定では、ユーザーデバイス上のプリンターをセッション間で保持および再作成する機能を有効または無効にします。デフォルトでは、クライアントプリンターは自動的に保持および復元されます。

「保持されるプリンター」とは、ユーザーが作成し次回セッションの開始時に再作成されるプリンターを指します。保持されるプリンターが Citrix Virtual Apps により再作成されるときは、［クライアントプリンターを自動作成する］設定以外のすべてのポリシー設定が考慮されます。

「復元されるプリンター」とは、管理者がカスタマイズしクライアントポートに永続的に接続された状態で保存されるプリンターを指します。

Citrix PDF ユニバーサルプリンタードライバー

Citrix PDF ユニバーサルプリンタードライバーを使用すると、ホストされているアプリケーション、または Citrix Virtual Apps and Desktops で配信された仮想デスクトップ上で実行中のアプリケーションで開かれているドキュメントを印刷できます。ユーザーが ［**Citrix PDF** プリンター］オプションを選択すると、ドライバーがファイルを PDF に変換して、これをローカルデバイスに転送します。その後、PDF を表示したり、ローカルに接続されたプリンターで印刷したりできます。PDF は、（EMF および XPS に加えて）Citrix ユニバーサル印刷でサポートされている

形式の 1 つです。
Citrix ポリシーを使用して、PDF プリンターを有効化および構成できるほか、デフォルトとして設定できます。[**Citrix PDF** プリンター] オプションは、Windows、Chrome、および HTML5 向けの Citrix Workspace アプリで利用できます。

> 注:
>
> Windows エンドポイントには、PDF ビューアーが必要です。クライアントには、PDF ファイルを開くため、Windows でファイルタイプの関連付けを登録済みのアプリケーションが必要です。

ドライバーのポリシー設定

August 17, 2024

[ドライバー] セクションには、プリンタードライバーに関するポリシー設定項目があります。

付属のプリンタードライバーの自動インストール

> 注
>
> このポリシーは、このリリースの VDA をサポートしていません。

この設定は、プリンタードライバーを以下から自動インストールするのを有効または無効にします:

- Windows に付属するドライバー
- `pnputil.exe /a`によりホスト上にステージングされたドライバーパッケージ

デフォルトでは、自動インストールが有効になっています。

ユニバーサルドライバーの優先度

この設定項目では、ユニバーサルプリンタードライバーの使用優先順位を指定します。一覧の上位にあるドライバーから順に使用されます。

デフォルトの優先順位は以下のとおりです。

- EMF
- XPS
- PCL5c
- PCL4
- PS

この一覧では、ドライバーを追加、編集、または削除したり、優先順位を変更したりできます。

ユニバーサル印刷の使用

この設定では、どのような状況でユニバーサル印刷を使用するかを指定します。

デフォルトでは、要求されたドライバーを使用できない場合にのみユニバーサル印刷を使用します。

ユニバーサル印刷では、プリンター固有の標準ドライバーの代わりに汎用プリンタードライバーが使用されるため、ホストコンピューターでのドライバー管理がシンプルになります。ユニバーサルプリンタードライバーを使用できるかどうかは、ユーザーデバイス、ホスト、およびプリントサーバーソフトウェアにより決定されます。構成によっては、ユニバーサル印刷を使用できない場合があります。

この設定をポリシーに追加する場合、以下の表からいずれかのオプションを選択します:

オプション	説明
プリンター固有のドライバーのみを使用する	サインイン中のクライアントプリンターの自動作成時に、そのプリンター固有の標準プリンタードライバーのみを使用するよう指定します。必要なプリンタードライバーがサーバーにない場合、そのクライアントプリンターは自動作成されません。
ユニバーサル印刷のみを使用する	プリンター固有の標準ドライバーを使用しないことを指定します。ユニバーサルプリンタードライバーのみを使用してプリンターが作成されます。
要求されたドライバーを使用できない場合にのみユニバーサル印刷を使用する	可能な場合はプリンター固有の標準ドライバーを使用します。プリンター固有のドライバーがサーバーにない場合は、最適なユニバーサルドライバーを使用してクライアントプリンターが自動作成されます。
ユニバーサル印刷を使用できない場合にのみプリンター固有のドライバーを使用する	利用可能な場合、ユニバーサルプリンタードライバーを使用します。ユニバーサルプリンタードライバーがサーバーにない場合は、適切なプリンター固有の標準ドライバーを使用してクライアントプリンターが自動作成されます。

ユニバーサルプリントサーバーのポリシー設定

August 17, 2024

［ユニバーサルプリントサーバー］セクションには、ユニバーサルプリントサーバーの動作を制御するためのポリシー設定項目があります。

SSL 暗号の組み合わせ

この設定は、暗号化印刷データストリーム（CGP）でユニバーサルプリントクライアントが使用する SSL/TLS 暗号の組み合わせセットを指定します。

暗号化印刷 Web サービス（HTTPS/SOAP）接続でユニバーサルプリントクライアントが使用する暗号の組み合わせを制御するには、[SCHANNEL] を参照してください。

デフォルト値：ALL

この設定の値は、ALL、COM、または GOV です。

各値に対応する暗号の組み合わせは次のとおりです：

ALL:

TLS_ECDHE_RSA_AES256_GCM_SHA384

TLS_ECDHE_RSA_AES256_CBC_SHA384

TLS_ECDHE_RSA_AES128_CBC_SHA

COM:

TLS_ECDHE_RSA_AES128_CBC_SHA

GOV:

TLS_ECDHE_RSA_AES256_GCM_SHA384

TLS_ECDHE_RSA_AES256_CBC_SHA384

SSL 準拠モード

この設定は、暗号化印刷データストリーム（CGP）でユニバーサルプリントクライアントが使用する NIST Special Publication 800-5 への準拠レベルを指定します。

デフォルト値：なし。

この設定では以下の値を指定できます：

ありません。

暗号化印刷データストリーム（CGP）接続はデフォルトの準拠モードを使用します。

SP800-52。

暗号化印刷データストリーム（CGP）接続は NIST Special Publication 800-52 準拠モードを使用します。

SSL が有効

この設定は、ユニバーサルプリントクライアントが使用する SSL/TLS 暗号の組み合わせセットを、以下について指定します:

- 印刷データストリーム（CGP）接続
- Web サービス（HTTP/SOAP）接続

［ユニバーサルプリントサーバーの有効化］を ［有効。**Windows** のリモート印刷機能にフォールバックする］に設定すると、フォールバック接続は Microsoft Windows ネットワーク印刷プロバイダーによって確立されます。この設定によって、フォールバック接続が影響を受けることはありません。

デフォルト値：無効

この設定では以下の値を指定できます:

有効。

ユニバーサルプリントクライアントはユニバーサルプリントサーバーへの接続に SSL/TLS を使用します。

無効。

ユニバーサルプリントクライアントはユニバーサルプリントサーバーへの接続に SSL/TLS を使用します。

SSL FIPS モード

この設定は、印刷データストリーム（CGP）接続でユニバーサルプリントクライアントが使用する SSL/TLS 暗号モジュールが FIPS モードで実行するかどうか指定します。

デフォルト値：無効

この設定では以下の値を指定できます:

有効。

FIPS モードは有効になっています。

無効。

FIPS モードは無効になっています。

SSL プロトコルバージョン

この設定はユニバーサルプリントクライアントが使用する SSL/TLS プロトコルのバージョンを指定します。

デフォルト値：ALL

この設定では以下の値を指定できます:

ALL。

TLS バージョン 1.0、1.1、または 1.2 を使用します。

TLSv1。

TLS バージョン 1.0 を使用します。

TLSv1.1。

TLS バージョン 1.1 を使用します。

TLSv1.2。

TLS バージョン 1.2 を使用します。

SSL ユニバーサルプリントサーバー暗号化印刷データストリーム（**CGP**）ポート

この設定では、ユニバーサルプリントサーバー暗号化印刷データストリーム（CGP）ポートが使用する TCP ポート番号を指定します。このポートは印刷ジョブのデータを受信します。

デフォルト値：443

SSL ユニバーサルプリントサーバー暗号化 **Web** サービス（**HTTP/SOAP**）ポート

この設定では、ユニバーサルプリントサーバー暗号化 Web サービス（HTTPS/SOAP）ポートが使用する TCP ポート番号を指定します。このポートは印刷コマンドのデータを受信します。

デフォルト値：8443

ユニバーサルプリントサーバーの有効化

このポリシーは、Citrix ユニバーサルプリントサーバー（UPS）の使用を有効または無効にします。このポリシー設定は、仮想デスクトップまたはサーバーホスティングアプリケーションを含んでいる組織単位（OU）に割り当てます。このポリシー設定には、フォールバックオプションが含まれ、Citrix UPS コンポーネントが要求されたプリントサーバーにインストールされていない、または利用できない場合、ネイティブの Windows リモート印刷サービスを使用してプリントサーバーに接続できます。このポリシーへの変更は、VDA の再起動後にのみ適用されます。

デフォルトでは、ユニバーサルプリントサーバーは無効になっています。

この設定では、以下のいずれかのオプションを選択します。

- 有効。**Windows** のリモート印刷機能にフォールバックする：可能な場合は、ユニバーサルプリントサーバーによってネットワークプリンター接続が確立されます。ユニバーサルプリントサーバーを使用できない場合は、Windows の印刷プロバイダーが使用されます。Windows 印刷プロバイダーにより作成されたすべてのプリンターは、引き続き Windows 印刷プロバイダーによって処理されます。

- 有効。**Windows** のリモート印刷機能にフォールバックしない：ユニバーサルプリントサーバーによってネットワークプリンター接続のみ確立されます。ユニバーサルプリントサーバーを使用できない場合は、ネットワークプリンターの接続に失敗します。この設定により、Windows の印刷プロバイダーを使用したネットワーク印刷を禁止できます。Windows 印刷プロバイダーにより作成されたプリンターは、この設定が構成されたポリシーがアクティブな間は作成されなくなります。
- 無効：ユニバーサルプリントサーバー機能は無効になります。UNC 名のネットワークプリンターに接続するときに、ユニバーサルプリントサーバーによる接続は試行されません。リモートプリンターへの接続では、Windows のリモート印刷機能が引き続き使用されます。

ユニバーサルプリントサーバー印刷データストリーム（**CGP**）ポート

この設定では、ユニバーサルプリントサーバー印刷データストリーム CGP（Common Gateway Protocol）リスナーが使用する TCP ポート番号を指定します。このポリシー設定は、プリントサーバーを含んでいる組織単位（OU）に割り当てます。

デフォルトのポート番号は、7229 に設定されています。

ほかのポートを指定する場合は、1 から 65535 の番号を使用してください。

ユニバーサルプリントサーバー入力データストリームの最大帯域幅（**Kbps**）

この設定では、印刷データの転送速度の上限をキロビット/秒単位で指定します。この転送速度は、各印刷ジョブからユニバーサルプリントサーバーに CGP で配信される印刷データに対して計算されます。このポリシー設定は、仮想デスクトップまたはサーバーホスティングアプリケーションを含んでいる組織単位（OU）に割り当てます。

デフォルトでは、上限なし（0）が指定されています。

ユニバーサルプリントサーバー **Web** サービス（**HTTP/SOAP**）ポート

この設定では、ユニバーサルプリントサーバーの Web サービス（HTTP/SOAP）リスナーで使用される TCP ポート番号を指定します。ユニバーサルプリントサーバーはオプションコンポーネントで、ネットワークプリンターでの Citrix ユニバーサルプリントドライバーの使用を有効にします。

ユニバーサルプリントサーバーが使用されると、印刷コマンドが SOAP over HTTP 上の SOAP を経由して、Citrix Virtual Apps and Desktops ホストからユニバーサルプリントサーバーに送信されます。この設定は、ユニバーサルプリントサーバーが HTTP/SOAP 要求を受信するためリスンするデフォルトの TCP ポートを変更します。

ホストおよびプリントサーバーの HTTP ポートの両方を等しく構成する必要があります。ポートを同じように構成しないと、ホストソフトウェアがユニバーサルプリントサーバーに接続されません。この設定を行うと、Citrix Virtual Apps and Desktops 上の VDA が変更されます。また、ユニバーサルプリントサーバーのデフォルトのポートを変更する必要があります。

デフォルトのポート番号は、8080 に設定されています。

ほかのポートを指定する場合は、0 から 65535 の番号を使用してください。

負荷分散のためのユニバーサルプリントサーバー

この設定には、Citrix のほかの印刷ポリシー設定を評価した後、セッション起動時に確立されるプリンター接続の負荷分散に使用するユニバーサルプリントサーバーの一覧が表示されます。プリンターの作成時間を最適化するには、すべてのプリントサーバーに同じ共有プリンターを設定することをお勧めします。負荷分散のために追加できるプリントサーバーの数に上限はありません。

この設定により、プリントサーバーのフェールオーバー検出とプリンター接続復旧も実装できます。プリントサーバーは定期的に可用性を確認されます。サーバー障害が検出されると、そのサーバーは負荷分散スキーマから削除されます。また、そのサーバーのプリンター接続は他の利用可能なプリントサーバーに再分配されます。障害が発生していたプリントサーバーが復旧すると、負荷分散スキーマに戻されます。

各サーバーがプリントサーバーであるかや、サーバーの一覧に重複するサーバー名が含まれていないか、すべてのサーバーに同じ共有プリンターがインストールされていることを確認するには、［サーバーの検証］をクリックします。この操作にはしばらく時間がかかる可能性があります。

ユニバーサルプリントサーバーのサービス停止のしきい値

この設定では、ロードバランサーが、反応しないプリントサーバーの復旧を待機する時間を指定します。タイムアウト後、ロードバランサーはそのサーバーが永続的にオフラインであると判定し、そのロードを他の利用可能なプリントサーバーに再配信します。

デフォルトでは、このしきい値は 180 秒に設定されています。

ユニバーサルプリントサーバー **Web** サービス（**HTTP/SOAP**）の接続タイムアウト

この設定では、ユニバーサルプリントサーバー Web サービスの connect() 操作がタイムアウトするまで、ユニバーサルプリントクライアントが待機する秒数を指定します。この設定では以下の値を指定できます。これらの値はすべて数値で、（時間の）単位は秒です。

- 最小値は 0 です。
- 最大値は 60 です。
- デフォルト値は 10 です。

タイムアウトが 1 ～60（を含む）の場合、ユニバーサルプリントクライアントは操作が完了するまで指定された時間待機します。この操作は、TCP ソケット接続操作です。ソケットは、TCP/IP ネットワーク経由でプロセス間通信を可能にする Windows オペレーティングシステムの機能です。

タイムアウトが 0 の場合、ユニバーサルプリントクライアントは、オペレーティングシステムによって定義されたデフォルトのタイムアウトを使用します。この構成は、この変更前にはユニバーサルプリントクライアントの以前のバージョンで使用可能でした。

ユニバーサルプリントクライアントは、ユニバーサルプリントサーバーと通信する Virtual Delivery Agent（VDA）のコンポーネントです。

> 注:
>
> このポリシー設定は、VDA バージョン 7.35 以降に適用されます。

ユニバーサルプリントサーバー **Web** サービス（**HTTP/SOAP**）の受信タイムアウト

この設定は、ユニバーサルプリントサーバー Web サービスの recv() 操作がタイムアウトするまで、ユニバーサルプリントクライアントが待機する必要がある秒数を指定します。この設定には次の値があり、これらの値はすべて数値で、（時間の）単位は秒です。

- 最小値は 0 です。
- 最大値は 60 です。
- デフォルト値は 10 です。

タイムアウトが 1 ～60（を含む）の場合、ユニバーサルプリントクライアントは操作が完了するまで指定された時間待機します。この操作は、TCP ソケット受信操作です。ソケットは、TCP/IP ネットワーク経由でプロセス間通信を可能にする Windows オペレーティングシステムの機能です。

タイムアウトが 0 の場合、ユニバーサルプリントクライアントは、オペレーティングシステムによって定義されたデフォルトのタイムアウトを使用します。この構成は、この変更前にはユニバーサルプリントクライアントの以前のバージョンで使用可能でした。

ユニバーサルプリントクライアントは、ユニバーサルプリントサーバーと通信する Virtual Delivery Agent（VDA）のコンポーネントです。

> 注:
>
> このポリシー設定は、VDA バージョン 7.35 以降に適用されます。

ユニバーサルプリントサーバー **Web** サービス（**HTTP/SOAP**）の送信タイムアウト

この設定は、ユニバーサルプリントサーバー Web サービスの send() 操作がタイムアウトするまで、ユニバーサルプリントクライアントが待機する必要がある秒数を指定します。この設定では以下の値を指定できます。これらの値はすべて数値で、（時間の）単位は秒です。

- 最小値は 0 です。
- 最大値は 60 です。
- デフォルト値は 10 です。

タイムアウトが 1 ～60（を含む）の場合、ユニバーサルプリントクライアントは操作が完了するまで指定された時間待機します。この操作は、TCP ソケット送信操作です。ソケットは、TCP/IP ネットワーク経由でプロセス間通信を可能にする Windows オペレーティングシステムの機能です。

タイムアウトが 0 の場合、ユニバーサルプリントクライアントは、オペレーティングシステムによって定義されたデフォルトのタイムアウトを使用します。この構成は、この変更前にはユニバーサルプリントクライアントの以前のバージョンで使用可能でした。

ユニバーサルプリントクライアントは、ユニバーサルプリントサーバーと通信する VDA のコンポーネントです。

> 注:
>
> このポリシー設定は、VDA バージョン 7.35 以降に適用されます。

ユニバーサル印刷のポリシー設定

August 17, 2024

［ユニバーサル印刷］セクションには、ユニバーサル印刷の管理に関するポリシー設定項目があります。

ユニバーサル印刷 **EMF** 処理モード

この設定では、Windows ユーザーデバイス上での EMF スプールファイルの処理方法を制御します。

デフォルトでは、EMF スプールファイルがクライアント上のスプールキューに直接挿入されます。

この設定では、次のオプションを選択します。

- ［EMF スプールファイルを再処理する］を有効にすると、EMF スプールファイルが再処理され、ユーザーデバイス上の GDI サブシステム経由で送信されます。通常、EMF 再処理を必要とするドライバーは自動的に検出され、適切な印刷経路が使用されますが、セッションで正しく検出されない場合があります。そのような場合にこのオプションを選択します。
- Citrix ユニバーサルプリンタードライバーで［EMF スプールファイルを直接挿入する］を有効にすると、EMF レコードがホスト上でスプールされ、その EMF スプールファイルがユーザーデバイス側に送信され処理されます。通常、この EMF スプールファイルはクライアント上のスプールキューに直接挿入されます。EMF 形式を処理できるプリンターおよびドライバーでは、この方法により印刷を高速に実行できます。

ユニバーサル印刷イメージ圧縮制限

このコマンドにより、以下が実行されます:

- Citrix ユニバーサルプリンタードライバーでのイメージ印刷で使用できる品質レベルの上限
- Citrix ユニバーサルプリンタードライバーで印刷される画像に使用できる圧縮レベルの下限

デフォルトでは、イメージ品質の上限が［最高品質（無損失圧縮）］に設定されています。

［非圧縮］を選択すると、EMF 印刷では圧縮が無効になります。

この設定では、次のオプションを選択します。

- 非圧縮
- 最高品質（無損失圧縮）
- 高品質
- 標準品質
- 低品質（最大圧縮）

この設定項目を ［ユニバーサル印刷最適化デフォルト］と同じポリシーに追加する場合は、次の点に注意してください：

- ［ユニバーサル印刷イメージ圧縮制限］での圧縮レベルが ［ユニバーサル印刷最適化デフォルト］での設定よりも低い場合は、［ユニバーサル印刷イメージ圧縮制限］の圧縮レベルが適用されます。
- ［ユニバーサル印刷イメージ圧縮制限］で［非圧縮］を選択すると、［ユニバーサル印刷最適化デフォルト］の［必要なイメージ品質］および［ヘビーウェイト圧縮を有効にする］オプションの設定は無視されます。

ユニバーサル印刷最適化デフォルト

この設定では、セッションで作成されるユニバーサルプリンタードライバーのデフォルトの印刷最適化オプションを指定します。

- ［必要なイメージ品質］では、ユニバーサル印刷に適用されるイメージ圧縮レベルの上限を指定します。デフォルトでは［標準品質］が選択されており、ユーザーは標準品質または低品質（最大圧縮）を使ってイメージを印刷できます。
- ［ヘビーウェイト圧縮を有効にする］では、ヘビーウェイト圧縮を有効または無効にします。この機能では、画質を損なわずに［必要なイメージ品質］での圧縮レベルよりも高い帯域幅削減が提供されます。デフォルトでは、ヘビーウェイト圧縮は無効になっています。
- ［イメージおよびフォントのキャッシュ］では、印刷ストリームで使用されているイメージやフォントをキャッシュするかどうかを指定します。この設定により、同一のイメージやフォントがプリンターに複数回送信されることを防ぐことができます。デフォルトでは、埋め込みイメージおよびフォントがキャッシュされます。これらの設定は、ユーザーデバイスでその機能がサポートされている場合にのみ適用されます。
- ［非管理者によるこれらの設定の変更を許可する］では、非管理者ユーザーがセッション内でこれらの最適化設定を変更することを許可または禁止します。デフォルトでは、禁止されています。

注：これらのすべてのオプションは、EMF 印刷に対してのみ適用されます。XPS 印刷では、［必要なイメージ品質］オプションのみがサポートされます。

この設定項目を ［ユニバーサル印刷イメージ圧縮制限］と同じポリシーに追加する場合は、次の点に注意してください：

- ［ユニバーサル印刷イメージ圧縮制限］での圧縮レベルが ［ユニバーサル印刷最適化デフォルト］での設定よりも低い場合は、［ユニバーサル印刷イメージ圧縮制限］の圧縮レベルが適用されます。

- ［ユニバーサル印刷イメージ圧縮制限］で［非圧縮］を選択すると、［ユニバーサル印刷最適化デフォルト］の［必要なイメージ品質］および［ヘビーウェイト圧縮を有効にする］オプションの設定は無視されます。

ユニバーサル印刷プレビューの設定

この設定では、自動作成プリンターまたは汎用ユニバーサルプリンターの印刷プレビュー機能を使用するかどうかを指定します。

デフォルトでは、自動作成プリンターまたは汎用ユニバーサルプリンターの印刷プレビューは使用できません。

この設定では、次のオプションを選択します。

- 自動作成プリンターまたは汎用ユニバーサルプリンターの印刷プレビューを使用しない
- 自動作成プリンターの印刷プレビューのみを使用する
- 汎用ユニバーサル プリンターの印刷プレビューのみを使用する
- 自動作成プリンターおよび汎用ユニバーサル プリンターの印刷プレビューを使用する

ユニバーサル印刷品質制限

この設定では、セッションでの印刷出力で使用できる最大 DPI 値（インチあたりのドット数）を指定します。

デフォルトでは［制限なし］が選択されており、ユーザーは接続しているプリンターで許可されている最高印刷品質を選択できます。

そのほかの値を選択すると、ユーザーが使用できる出力解像度が制限されます。この設定では、印刷品質自体と、ユーザーが接続するプリンターの印刷能力の両方が制限されます。

たとえば、中解像度（600 DPI）を選択した場合、出力印刷は最大品質である 600 DPI でのみ可能です。また、［ユニバーサルプリンター］ダイアログボックスの ［詳細設定］タブの ［印刷品質］設定には、中品質（600 DPI）を超える解像度オプションが表示されなくなります。

この設定では、次のオプションを選択します。

- ドラフト（150dpi）
- 低解像度（300dpi）
- 中解像度（600dpi）
- 高解像度（1200dpi）
- 制限なし

セキュリティのポリシー設定

August 17, 2024

［セキュリティ］セクションには、セッションの暗号化とログオンデータの暗号化の構成に関するポリシー設定が含まれています。

SecureICA の最低暗号化レベル

この設定では、サーバーとユーザーデバイスの間で送信するセッションデータの暗号化に必要な最低限の暗号化レベルを指定します。

重要：Virtual Delivery Agent 7.x の場合、この設定を RC5 128 ビット暗号化によるログオンデータの暗号化を有効にするためだけに使用できます。ほかの暗号化レベルは、以前のバージョンの Citrix Virtual Apps and Desktops との互換性を保持する場合に使用します。

VDA 7.x の場合、セッションデータの暗号化は VDA のデリバリーグループの基本設定を使って設定されます。デリバリーグループに対して［Secure ICA を有効にする］がオンになっている場合、セッションデータは RC5（128 ビット）暗号化で暗号化されます。デリバリーグループに対して［Secure ICA を有効にする］がオフになっている場合、セッションデータは基本レベルの暗号化で暗号化されます。

この設定では、次のオプションを選択します。

- ［基本］では、非 RC5 のアルゴリズムを使ってクライアント接続を暗号化します。この暗号化レベルでは、データストリームが直接読み取られることはありませんが、解読される恐れがあります。デフォルトでは、クライアントとサーバーの間のトラフィックには基本レベルの暗号化が使用されます。
- ［RC5（128 ビット、ログオンのみ）］では、RC5 128 ビット暗号化を使ってログオンデータを暗号化し、基本レベルの暗号化を使ってクライアント接続を暗号化します。
- ［RC5（40 ビット）］では、RC5 40 ビット暗号化を使ってクライアント接続を暗号化します。
- ［RC5（56 ビット）］では、RC5 56 ビット暗号化を使ってクライアント接続を暗号化します。
- ［RC5（128 ビット）］では、RC5 128 ビット暗号化を使ってクライアント接続を暗号化します。

クライアントとサーバー間の実際の通信では、Citrix 製品や Windows オペレーティングシステムでの暗号化設定も考慮されます。サーバーやユーザーデバイスでより高い暗号化レベルが設定されている場合は、その設定が優先されます。

機密データを使用するユーザーなど、特定のユーザーの通信データを保護してメッセージの整合性を保証するために、より高度な暗号化レベルを設定することもできます。ポリシーでより高度な暗号化レベルを指定すると、そのレベルよりも低い暗号化機能を使用する Citrix Receiver は、サーバーに接続できなくなります。

SecureICA では認証の実行またはデータの整合性のチェックはされません。エンドツーエンドの暗号化を提供するには、SecureICA を TLS と共に使用します。

SecureICA では FIPS 準拠のアルゴリズムは使用されません。この設定が問題になる場合は、SecureICA を使用しないようにサーバーと Citrix Receiver を設定します。

SecureICA は、秘密保持のために RFC 2040 で説明されているように RC5 ブロック暗号を使用します。ブロックサイズは、64 ビット（32 ビットワード単位の倍数）です。キーの長さは、128 ビットです。ラウンド数は、12 です。

RC5 ブロック暗号のキーは、セッションの作成時にネゴシエートされます。ネゴシエーションは、Diffie-Hellman アルゴリズムを使用して実行されます。このネゴシエーションでは、Diffie-Hellman パブリックパラメーターが使用されます。これらのパラメーターは、Virtual Delivery Agent のインストール時に Windows レジストリに保存されます。パブリックパラメーターは秘密ではありません。Diffie-Hellman ネゴシエーションの結果は秘密キーであり、その秘密キーから RC5 ブロック暗号のセッションキーが導出されます。個別のセッションキーは、ユーザーログオンおよびデータ転送に使用されます。また、Virtual Delivery Agent 間のトラフィックにも使用されます。したがって、セッションごとに 4 つのセッションキーがあります。秘密キーとセッションキーは保存されません。RC5 ブロック暗号の初期化ベクトルも秘密キーから導出されます。

サーバーの制限のポリシー設定

August 17, 2024

［サーバーの制限］カテゴリには、アイドル状態の接続の制御に関する設定項目が含まれています。

サーバーのアイドルタイマーの間隔

この設定では、アイドル状態のセッション（ユーザーからの入力がない連続セッション）を自動的に切断するまでの時間を指定します。データはミリ秒単位で計算されます。

デフォルトでは、アイドル状態の接続は切断されません。つまり、サーバーのアイドルタイマーの間隔は 0 です。この値を 60000 ミリ秒（60 秒）以上に設定することをお勧めします。

このポリシーを表示するには、［複数のバージョン］を選択してシングルセッション OS バージョンの選択をオフにし、［サーバーの制限］を選択します。

> 注
>
> このポリシー設定が使用される場合、セッションが指定した時間アイドル状態になると、「アイドル タイマーが切れました」ということを示すダイアログボックスがユーザーに表示されることがあります。Citrix ポリシー設定では、この Microsoft のダイアログボックスメッセージは制御されません。詳しくは、http://support.citrix.com/article/CTX118618を参照してください。

セッションの制限のポリシー設定

August 17, 2024

［セッションの制限］セクションには、セッションに接続してから強制的にログオフさせられるまでの時間を制御するためのポリシー設定が含まれています。

切断セッションタイマー

この設定項目では、切断状態でロックされたデスクトップセッションを一定期間後に自動的にログオフする機能を有効または無効にします。

このタイマーが有効な場合、タイマーが期限切れになると、切断されたセッションはログオフします。

デフォルトでは、切断状態のセッションはログオフされません。

リモート **PC** アクセス切断セッションタイマー

この設定は、タイマーの有効期限が切れた後に切断されたユーザーセッションをログオフするタイマーを有効または無効にします。この設定を有効にする場合は、［切断セッションタイマーの間隔］設定を使用して、ユーザーセッションがログオフされるまで、切断されたデスクトップがロックしたままになる時間を分単位で指定します。

デフォルトでは、この設定は無効になっています。

切断セッションタイマーの間隔

この設定項目では、切断状態でロックされたデスクトップセッションを自動的にログオフするまでの時間を分単位で指定します。

デフォルトでは、1,440 分（24 時間）に設定されています。

切断セッションタイマー–マルチセッション

この設定は、タイマーを有効または無効にして、切断された RDS セッションがログオフするまでの時間を決定します。デフォルトでは、このタイマーは無効になっており、切断状態のセッションはログオフしません。

切断セッションタイマーの間隔–マルチセッション

この設定は、セッションがログオフされる前に、切断された RDS セッションがログオフするまでの時間を分単位で決定します。デフォルトでは、1440 分（24 時間）に設定されています。

セッション接続タイマー

この設定項目では、ユーザーデバイスとデスクトップ間の連続セッションを一定期間後に自動的にログオフする機能を有効または無効にします。このタイマーが有効な場合、タイマーが期限切れになると、セッションが切断されるかログオフします。Microsoft の制限時間に達したらセッションを終了する設定によって次のセッションの状態が決定します。

デフォルトでは、無効になっています。

セッション接続タイマーの間隔

この設定項目では、ユーザーデバイスとデスクトップ間の連続セッションを自動的にログオフするまでの時間を分単位で指定します。

デフォルトでは、1,440 分（24 時間）に設定されています。

セッション接続タイマー–マルチセッション

この設定項目では、ユーザーデバイスとターミナルサーバー間の連続セッションを一定期間後に自動的にログオフする機能を有効または無効にします。デフォルトでは、無効になっています。

セッション接続タイマーの間隔–マルチセッション

この設定項目では、ユーザーデバイスと RDS セッション間の連続セッションを自動的にログオフするまでの時間を分単位で指定します。デフォルトでは、1440 分（24 時間）に設定されています。

セッションアイドルタイマー

ユーザーからの入力がない場合、この設定を使用して以下を有効または無効にします:

- ユーザーデバイスとデスクトップ間の連続セッションが維持される期間を指定するタイマー。

タイマーが期限切れになると、セッションは切断状態になり、［切断セッションタイマー］が適用されます。［切断セッションタイマー］が無効になると、セッションはログオフしません。

デフォルトでは、有効になっています。

セッションアイドルタイマーの間隔

ユーザーからの入力がない場合、この設定を使用して以下を有効または無効にします:

- ユーザーデバイスとデスクトップ間の連続セッションが維持される期間（分）。

デフォルトでは、1,440 分（24 時間）に設定されています。

セッションアイドルタイマー–マルチセッション

この設定項目では、ユーザーデバイスとターミナルサーバー間のアイドル接続を一定期間後に自動的にログオフする機能を有効または無効にします。デフォルトでは、無効になっています。

セッションアイドルタイマーの間隔–マルチセッション

この設定項目では、ユーザーデバイスと RDS セッション間のアイドル接続の時間を分単位で指定します。デフォルトでは、1440 分（24 時間）に設定されています。

> 注:
>
> Citrix ポリシーを使用して構成されたマルチセッションマシンのタイマー設定は、Microsoft グループポリシーを使用して構成されたタイマー設定を上書きすることが予想されます。予期しない動作を回避するために、2 つの方法のいずれかを使用してタイマー設定を構成することをお勧めします。

セッション画面の保持のポリシー設定

August 17, 2024

[セッション画面の保持] セクションには、セッション画面の保持の管理に関するポリシー設定が含まれています。

セッション画面の保持

この設定では、セッション画面の保持機能を許可または禁止します。セッション画面の保持機能およびクライアントの自動再接続機能によって、ネットワークの中断からの回復後、ユーザーは Citrix Workspace アプリセッションに自動的に再接続できます。デフォルトでは、セッション画面の保持が許可されます。

Web Studio の設定は、次の場合にクライアントに適用されます:

- Citrix Workspace アプリ 1808 以降
- Citrix Receiver for Windows 4.7 以降。

Web Studio ポリシーはクライアントの Citrix Receiver グループポリシーオブジェクトを上書きします。Web Studio でこれらのポリシーを更新すると、サーバーからクライアントにセッション画面の保持が同期されます。

> 注:
>
> - Citrix Receiver for Windows 4.7 以降、および Windows 向け Citrix Workspace アプリの場合、Web Studio でポリシーを設定します。
> - 4.7 より前の Citrix Receivers for Windows の場合、Web Studio で複数ポリシーを設定します。また、一貫した動作を実現するために、クライアントで Citrix Receiver のグループポリシーオブジェクトテンプレートを設定します。

セッション画面の保持機能は、ICA セッションをアクティブのまま保持し、ネットワークの接続が切断されても、セッションの画面を表示したままにできます。ユーザーは、接続が回復するまでセッション画面を見ることができます。

セッション画面の保持機能を有効にすると、データを損失することなく、サーバー上のセッションがアクティブのまま保持されます。接続が失われると、ユーザーの表示は不透明になります。中断中にユーザーにフリーズしたセッションが表示される場合があります。ネットワーク接続が回復するとアプリケーションでの作業を再開できるようになります。また、セッションに再接続するときに再認証用のログオン画面が表示されないため、ユーザーは即座に作業を再開できます。

セッション画面の保持機能とクライアントの自動再接続機能を一緒に使用する場合は、次のように処理されます。まず、ネットワークが切断されると、セッション画面の保持機能により、セッションがアクティブのままサーバー上に保持されます。[セッション画面の保持のタイムアウト］設定で指定した時間が経過すると、サーバー上のセッションが終了または切断されます。この後でクライアントの自動再接続のポリシー設定により、切断セッションへの再接続が行われます。

デフォルトでは、セッション画面の保持が許可されます。

> 注:
>
> Citrix ADC を使用中の場合は、Citrix StoreFront>[**Citrix Gateway** の管理]>[**Secure Ticket Authority**]で ［セッション画面の保持を有効にする］を選択し、ICA 接続をプロキシ処理する必要があります。

セッション画面の保持のポート番号

この設定では、セッション画面の保持機能で使用される、受信 TCP ポートを指定します。

デフォルトでは、ポート番号は、2598 に設定されます。

セッション画面の保持のタイムアウト

この設定は、時間の長さを秒単位で指定します。ここで指定した時間が経過しても再接続されないセッションは、「切断セッション」として処理されます。

セッションの持続時間を長く設定することもできますが、この機能は利便性が高く、ユーザーに再認証を求めるメッセージを表示することもありません。セッションの持続時間を長くすると、ユーザーがデバイスを置き去りして承認されていないユーザーに利用される可能性が高まります。

デフォルトでは、タイムアウトは 180 秒（3 分）に設定されています。

セッションウォーターマークのポリシー設定

August 17, 2024

[セッション ウォーターマーク］セクションには、この機能を構成するためのポリシー設定が含まれています。
この機能を有効にすると、VDA マシンによるネットワーク帯域幅と CPU の使用率が大幅に上昇します。使用可能な

ハードウェアリソースに基づいて、選択した VDA マシンのセッションウォーターマークを構成することをお勧めします。

> 重要
>
> 他のウォーターマークポリシー設定を有効にするには、セッションウォーターマークを有効にします。ユーザーエクスペリエンスを向上させるためには、ウォーターマークのテキスト項目を 3 つ以上有効にしないようにしてください。

セッション ウォーターマークを有効化

この設定を有効にすると、セッション画面に、セッション固有の情報を示す不透明なテキストウォーターマークが表示されます。他のウォーターマーク設定は、これが有効になっているかどうかで異なります。

デフォルトでは、セッションウォーターマークは無効になっています。

クライアント **IP** アドレスを含む

この設定を有効にすると、セッションで、現在のクライアント IP アドレスがウォーターマークとして表示されます。

デフォルトでは、［クライアント IP アドレスを含む］は無効になっています。

接続時間を含める

この設定を有効にすると、セッションウォーターマークに接続時間が表示されます。形式は、yyyy/mm/dd hh:mm です。表示される時間は、システムクロックとタイムゾーンに基づいています。

デフォルトでは、［接続時間を含める］は無効になっています。

ログオンユーザー名を含む

この設定を有効にすると、セッションで、現在のログオンユーザー名がウォーターマークとして表示されます。表示形式は、USERNAME@DOMAINNAME です。ユーザー名は 20 文字までにすることをお勧めします。ユーザー名が 20 文字を超えている場合は、文字が極端に小さく表示されるか、一部が表示されず、ウォーターマークの効果が低下する可能性があります。

デフォルトでは、［ログオンユーザー名を含む］は有効になっています。

VDA ホスト名を含む

この設定を有効にすると、セッションで、現在の ICA セッションの VDA ホスト名がウォーターマークとして表示されます。

デフォルトでは、［VDA ホスト名を含む］は有効になっています。

VDA の **IP** アドレスを含む

この設定を有効にすると、セッションで、現在の ICA セッションの VDA IP アドレスがウォーターマークとして表示されます。

デフォルトでは、VDA の IP アドレスは無効になっています。

セッションウォーターマークスタイル

この設定は、1 つのウォーターマークテキストラベルを表示するか複数のラベルを表示するかを制御します。［値］ドロップダウンメニューで ［複数］または ［単一］を選択します。

［複数］の場合は、セッションに 5 つのウォーターマークラベルが表示されます。中央に 1 つ、隅に 4 つです。

［単一］の場合は、セッションの中央にウォーターマークラベルが 1 つ表示されます。

デフォルトでは、［セッションウォーターマークスタイル］は［複数］になっています。

ウォーターマークのカスタムテキスト

この設定では、セッションウォーターマークで表示するカスタムテキスト（社名など）を指定できます。空でない文字列を構成すると、ウォーターマークに、新しい行でそのテキストが表示され、有効になっているその他の情報が付け加えられます。ウォーターマークのカスタムテキストの最大値は、25 文字の Unicode です。長い文字列を構成すると、25 文字に切り捨てられます。

デフォルトのテキストはありません。

Citrix Virtual Apps and Desktops 7 2206 以降では、テキスト内のカスタムタグを使用して、さらにカスタマイズを追加できます。その結果、カスタムテキストの最大文字数が 1024 に増えました。

次の表では、ウォーターマーク設定に使用できるタグについて説明します:

タグ	説明	例
`<font=value>`	ウォーターマークテキストのフォントを変更できます。値は、VDA で使用可能なフォント名です。	`<font=Courier New>`

タグ	説明	例
<fontzoom=value>	フォントの拡大/縮小率をパーセンテージで設定できます。ウォーターマークテキストを 200% 拡大する場合、値は 200 です。	<fontzoom=200>
<position=value>	ウォーターマークテキストの位置を変更できます。値はcenter、topleft、topright、bottomleft、およびbottomrightです。このタグは、表示スタイルが single の場合にのみ適用できます。	<position=topright>
<rotation=value>	ウォーターマークテキストを回転できます。値は、度数を-360～360 の範囲で指定できます。	<rotation=45>
<style=value>	表示スタイルを変更できます。このタグは、セッションウォーターマークのスタイルポリシーを上書きします。	<style=single>

次のウォーターマークスタイルを使用できます:

- single スタイル - セッションの中央にウォーターマークラベルが 1 つ表示されます。position タグを使用して場所を変更できます。
- xstyle または multiple - セッションに 5 つのウォーターマークラベル（中央に 1 つ、四隅に 1 つずつ）が表示されます。
- tile - セッションに複数のラベルが表示されます。ウォーターマークテキストは、画面全体に等間隔で配置されます。

次の表では、ウォーターマークテキストを変更するために使用できるタグについて説明します:

タグ	説明
<clientip>	エンドポイントの IP アドレス。
<date>	セッションが確立された日付。
<domain>	ログインしているユーザーアカウントのドメイン名。
<hostname>	VDA のマシン名。
<newline>	追加の行の作成。

タグ	説明
<serverip>	VDA の IP アドレス。
<time>	セッションが確立された時間。
<username>	ユーザーの名前。

> 注:
>
> - ウォーターマークのカスタムテキストポリシーは、セッションウォーターマークを有効化ポリシーが有効になっている場合にのみ有効になります。デフォルト値は ［無効］ です。
> - タグを使用してウォーターマークテキストを変更すると、セッションウォーターマークを ［有効］ にする以外のすべてのセッションウォーターマークポリシーが無視されます。ウォーターマークテキスト設定にタグを使用すると、他のすべてのウォーターマークポリシーを使用できます。

ウォーターマークの透明度

ウォーターマークの不透明度を 0～100 の範囲で指定できます。指定された値が大きいほど、ウォーターマークが不透明になります。

デフォルトでは、値は 17 です。

タイムゾーン制御のポリシー設定

August 17, 2024

［タイムゾーン制御セクション］ には、セッションでのローカルタイムの使用に関するポリシー設定が含まれています。

レガシークライアントのローカルタイムゾーンを検出する

この設定では、クライアント側のローカルタイムゾーンの検出を有効または無効にします。クライアントによっては、正確なタイムゾーン情報がサーバーに送信されない場合があります。

デフォルトでは、必要に応じてクライアント側のタイムゾーンが検出されます。

この設定は、詳しいタイムゾーン情報をサーバーに送信しない、従来の Citrix Receiver または ICA クライアントでの使用を前提にしています。詳しいタイムゾーン情報をサーバーに送信する Citrix Receiver で使用する場合 (Windows でサポートされているバージョンの Citrix Receiver など)、この設定は何の影響も及ぼしません。

セッションの切断時またはログオフ時にデスクトップ **OS** のタイムゾーンを復元する

ユーザーが切断またはログオフした場合は、この設定によって、シングルセッション OS VDA のタイムゾーン設定をコンピューターの元のタイムゾーンに復元するかどうかが決定されます。この設定を有効にした場合、VDA はユーザーが切断またはログオフしたときにマシンのタイムゾーンを元の設定に復元します。この設定を有効にするには、［クライアントのタイム ゾーンを使用する］に ［クライアントのローカル タイム ゾーンを使用する］を設定します。

デフォルトでは、有効になっています。

クライアントのローカルタイムゾーンを使用する

この設定では、ユーザーセッションに適用されるタイムゾーンを指定します。選択できるオプションは、ユーザーセッションのタイムゾーン（サーバータイムゾーン）とユーザーデバイスのタイムゾーン（クライアントタイムゾーン）です。

デフォルトでは、ユーザーセッションのタイムゾーンが適用されます。

この設定を反映するには、グループポリシーエディターで ［タイムゾーンのリダイレクトを許可する］設定を有効にします。この設定は、［ローカルコンピューターポリシー］> ［コンピューターの構成］> ［管理用テンプレート］> [**Windows** コンポーネント］> ［リモートデスクトップサービス］> ［リモートデスクトップセッションホスト］> [デバイスとリソースのリダイレクト］にあります。

サーバー OS を実行しているマシンでシングルセッション VDA（旧称 Workstation VDA）を使用している場合は、ローカルユーザー権限の ［タイムゾーンの変更］を ［全ユーザー］に構成します。このユーザー権限は、［ローカルコンピューターポリシー］> ［コンピューターの構成］> [**Windows** の設定］> ［セキュリティの設定］> ［ローカルポリシー］> ［ユーザー権利の割り当て］にあります。

> 注:
>
> シングルセッション OS の場合は、［ユーザー権利の割り当て］の ［タイムゾーンの変更］で ［**Users**］を追加しますが、マルチセッション OS ではこの設定は行いません。マルチセッション OS では、次のグループポリシーでタイムゾーンを同期します：［コンピューターの構成］> ［管理用テンプレート］> [Windows コンポーネント］> ［リモートデスクトップサービス］> ［リモートデスクトップセッションホスト］> ［デバイスとリソースのリダイレクト］> ［タイムゾーンのリダイレクトを許可する］。このポリシーは、サーバーがマルチセッション OS VDA のリモートデスクトップセッションホストである（インストール時に`/ServerVDI`コマンドを使用している）場合に適用されます。マルチセッション OS では、設計上、デフォルトではユーザーにタイムゾーンを変更できるローカル権限は付与されません。

TWAIN デバイスのポリシー設定

August 17, 2024

［**TWAIN** デバイス］のセクションには、以下に関連するポリシー設定が含まれています：

- デジタルカメラやスキャナーなどのクライアント TWAIN デバイスのマッピング
- サーバーからクライアントへのイメージ転送の最適化

> 注：
>
> Citrix Receiver for Windows 4.5 では、TWAIN 2.0 がサポートされています。

クライアント **TWAIN** デバイスリダイレクト

TWAIN デバイスは、TWAIN プロトコルを使用して、サーバーでホストされている画像処理アプリケーションと通信します。

この設定により、ユーザーデバイス側の TWAIN デバイスにアクセスすることを許可または禁止します。デフォルトでは、TWAIN デバイスリダイレクトは許可されています。

関連する設定項目は以下のとおりです：

- TWAIN 圧縮レベル
- TWAIN デバイスリダイレクトの最大帯域幅（Kbps）
- TWAIN デバイスリダイレクトの最大帯域幅（%）

TWAIN 圧縮レベル

この設定では、クライアントからサーバーに転送される画像の圧縮レベルを指定します。画質を最高にするには［低］を、良好にするには［中］を、低くするには［高］を選択します。デフォルトでは、中レベルの圧縮が選択されています。

USB デバイスのポリシー設定

August 17, 2024

［**USB** デバイス］セクションには、USB デバイスのファイルリダイレクトの管理に関するポリシー設定が含まれています。

クライアント **USB** デバイス最適化規則

クライアント USB デバイス最適化規則をデバイスに適用して最適化を無効にしたり、最適化モードを変更したりできます。

ユーザーが USB 入力デバイスを接続すると、ホストは、そのデバイスが ［**USB** ポリシー］設定で許可されているかどうかをチェックします。デバイスが許可されている場合は、次にホストはデバイスのクライアント **USB** デバイス最適化規則をチェックします。規則が指定されていない場合は、デバイスは最適化されません。キャプチャモード（04）は署名デバイスに対する推奨モードです。遅延が大きいためにパフォーマンスが低下しているその他のデバイスに対して、管理者は対話モード（02）を有効にできます。使用可能なモードの説明については、この記事の表を参照してください。

ヒント

- Wacom 署名パッドおよびタブレットを使用する場合、スクリーンセーバーを無効にすることをお勧めします。スクリーンセーバーを無効にする手順については、このセクションの最後で説明しています。
- Wacom STU 署名パッドおよびタブレット製品シリーズの最適化のサポートは、Citrix Virtual Apps and Desktops ポリシーのインストールで事前構成されています。
- 署名デバイスは Citrix Virtual Apps and Desktops で動作し、署名デバイスとして使用するためのドライバーは必要ありません。Wacom では、デバイスをさらにカスタマイズするためにインストールできる追加のソフトウェアが提供されています。http://www.wacom.com/を参照してください。
- 描画用タブレット。PCI/ACPI バス上の HID デバイスとして表示される特定の描画入力デバイスはサポートされていません。これらのデバイスは、Citrix Virtual Desktops セッション内でリダイレクトするクライアント上の USB ホストコントローラーに接続します。

ポリシー規則は、スペースで区切った tag=value 式の形式にします。以下のタグがサポートされます。

タグ名	説明
モード	最適化モードは、class=**03** の入力デバイスでサポートされます。サポートされているモードは次のとおりです: 最適化なし - 値 **01**。対話モード - 値 **02**。ペンタブレットや 3D Pro マウスなどのデバイスにお勧めします。キャプチャモード - 値 **04**。署名パッドなどのデバイスに推奨します。
VID	デバイス記述子のベンダー ID（4 桁の 16 進数値）
PID	デバイス記述子の製品 ID（4 桁の 16 進数値）
REV	デバイス記述子のリビジョン ID（4 桁の 16 進数値）
クラス	デバイス記述子またはインターフェイス記述子のクラス
SubClass	デバイス記述子またはインターフェイス記述子のサブクラス
Prot	デバイス記述子またはインターフェイス記述子のプロトコル

例

Mode=00000004 VID=067B PID=1230 class=03 # キャプチャモードで動作する入力デバイス

Mode=00000002 VID=067B PID=1230 class=03 # 対話モードで動作する入力デバイス（デフォルト）

Mode=00000001 VID=067B PID=1230 class=03 # 最適化なしで動作する入力デバイス

Mode=00000100 VID=067B PID=1230 # 最適化が無効に設定されているデバイス（デフォルト）

Mode=00000200 VID=067B PID=1230 # 最適化が有効に設定されているデバイス

Wacom 署名パッドデバイスのスクリーンセーバーの無効化

Wacom 署名パッドおよびタブレットを使用する場合、次の手順に従ってスクリーンセーバーを無効にすることをお勧めします。

1. デバイスのリダイレクト後に **Wacom-STU-Driver** をインストールします。
2. **Wacom-STU-Display MSI** をインストールして、署名パッドコントロールパネルへのアクセスを有効にします。
3. ［コントロールパネル］**>** ［**Wacom STU Display**］**>** ［**STU430**］または ［**STU530**］の順に選択し、使用しているモデルのタブを選択します。
4. ［**Change**］を選択し、UAC セキュリティウィンドウがポップアップ表示されたら ［**Yes**］をクリックします。
5. ［**Disable slideshow**］を選択して、［**Apply**］をクリックします。

1 つの署名パッドモデルに対しての設定が完了したら、それがすべてのモデルに適用されます。

クライアント **USB** デバイスリダイレクト

この設定では、USB デバイスのクライアント側へのリダイレクトおよびクライアント側からのリダイレクトを許可または禁止します。

デフォルトでは、USB デバイスはリダイレクトされません。

クライアント **USB** デバイスリダイレクト規則

この設定では、USB デバイスのリダイレクト規則を指定します。

デフォルトでは、規則は指定されていません。

ユーザーが USB デバイスを装着すると、ホストデバイスで一覧の規則が順に検証され、マッチする最初の規則でリダイレクトが許可されているかどうかがチェックされます。最初の一致が Allow 規則の場合、USB デバイスは仮想デスクトップにリモートで接続されます。最初の一致が Deny 規則の場合、その USB デバイスはローカルデスクトップでのみ使用可能になります。一致する規則がない場合、デフォルトの規則が使用されます。

ポリシー規則は、{Allow: | Deny:} の後に、「tag=value」式をスペースで区切って設定します。以下のタグがサポートされます。

タグ名	説明
VID	デバイス記述子のベンダー ID
PID	デバイス記述子の製品 ID
REL	デバイス記述子のリリース ID
クラス	デバイス記述子またはインターフェイス記述子のクラス
SubClass	デバイス記述子またはインターフェイス記述子のサブクラス
Prot	デバイス記述子またはインターフェイス記述子のプロトコル

ポリシー規則を作成する場合、以下の点に注意してください。

- 大文字と小文字は区別されません。
- 規則の末尾に、「#」で始まる任意のコメントを追加できます。
- 空白行およびコメントのみの行は無視されます。
- タグには等号（=）を使用する必要があります（例：VID=067B）。
- 各規則を 1 行ずつ記述するか、同一行に記述する場合はセミコロンで区切られたリスト形式である必要があります。
- 使用可能な USB クラスコードについては、USB Implementers Forum, Inc. の Web サイトを参照してください。

管理者定義の USB ポリシー規則の例

- Allow: VID=067B PID=0007 # 別のメーカーの別のフラッシュドライブ
- DENY: Class=08 subclass=05 # Mass Storage
- すべての USB デバイスを拒否する規則を作成するには、タグを指定せずに「DENY:」を使用します。

クライアント **USB** プラグアンドプレイデバイスリダイレクト

この設定では、カメラや POS（Point-Of-Sale）デバイスなど、プラグアンドプレイデバイスのセッション内での使用を許可または禁止します。

デフォルトでは、許可されます。［許可］を選択すると、特定のユーザーやグループのセッションですべてのプラグアンドプレイデバイスがリダイレクトされます。［禁止］を選択すると、デバイスはリダイレクトされません。

USB デバイスの自動リダイレクトを構成する

USB サポート機能が有効になっており、USB 関連のユーザー設定で USB デバイスに自動接続するように設定されている場合は、USB デバイスが自動的にリダイレクトされます。

> 注:
>
> Citrix Receiver for Windows 4.2 では、デスクトップアプライアンスモードで接続バーが表示されていない場合でも、USB デバイスは自動的にリダイレクトされます。以前のバージョンの Citrix Receiver for Windows では、以下の環境で動作している場合も USB デバイスは自動リダイレクトされます:
>
> - デスクトップアプライアンスモード
> - 仮想マシン（VM）でホストされるアプリケーション

一部の USB デバイスはリダイレクトしない方が良い場合もあります。ユーザーは、USB デバイスリストから、自動的にリダイレクトされないデバイスを明示的にリダイレクトすることができます。USB デバイスのリスト表示とリダイレクトを禁止するには、クライアントエンドポイントまたは Desktop Delivery Controller ポリシーで DeviceRules を適用します。詳しくは、「管理ガイド」を参照してください。

> 注意:
>
> レジストリエディターの使用を誤ると、深刻な問題が発生する可能性があり、オペレーティングシステムの再インストールが必要になる場合もあります。レジストリエディターの誤用による障害に対して、Citrix では一切責任を負いません。レジストリエディターは、お客様の責任と判断の範囲でご使用ください。また、レジストリファイルのバックアップを作成してから、レジストリを編集してください。

USB デバイスの自動リダイレクトのユーザー設定

ポリシー:

1. ローカルグループポリシーエディターを開き、[管理用テンプレート] > [**Citrix** コンポーネント] > [**Citrix Receiver**] > [クライアントデバイスをリモート処理します] > [一般的な **USB** のリモート処理] の順に選択します。
2. [新しい **USB** デバイス] を開いて [有効] を選択し、[**OK**] をクリックします。
3. [既存の **USB** デバイス] を開いて [有効] を選択し、[**OK**] をクリックします。

Citrix Receiver:

1. [**Citrix Receiver** 環境設定] > [接続] の順に選択します。
2. 次のオプションを選択します:
   - セッションの開始時に、デバイスを自動的に接続します
   - セッションの実行中に新しいデバイスが接続されると、自動的にデバイスに接続します
3. [**OK**] をクリックします。

レジストリキーとポリシーに対するすべての変更が、Windows クライアントデバイスに適用されます。

プレーン **USB** プリンターのリダイレクト

プレーン USB プリンターを利用する場合の最適な方法は、専用のユニバーサルプリンタードライバーと仮想チャネルを使用して印刷を行うことです。デフォルトでは、プレーン USB プリンターは自動的にはリダイレクトされません。

プレーンプリンターは、ヒューリスティックスを使用して検出されます。そのため、スキャン機能を備えた高度なプリンターなどを完全に動作させるには、USB サポートを使用してリダイレクトする必要がある場合があります。

プレーンプリンターを自動でリダイレクトするかどうかを構成するには、次のレジストリを使用します:

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB\Devices

値の名前：AutoRedirectPrinters

種類：DWORD

データ：00000000

デフォルト値は 0 です（自動リダイレクトは行われません）。この値を 0 より大きい任意の値にすると、USB サポートが有効になり、プレーン USB プリンターがリダイレクトされるようになります。

Active Directory ポリシーを使用して、次のレジストリキーを展開することもできます。ポリシー以外で値が指定されている場合には、この値が優先されます:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB\Devices

値の名前：AutoRedirectAudio

種類：DWORD

データ：00000000

プレーンオーディオデバイスのリダイレクト

プレーンプリンターと同様に、ICA の専用オーディオ仮想チャネルを使用してプレーンオーディオデバイスから音声データすることで、ユーザーエクスペリエンスを最適化できます。ただし、一部の特殊なデバイスは、USB サポートを使用してリダイレクトする必要のある場合があります。どのデバイスがプレーンオーディオデバイスであるかは、ヒューリスティックスにより判別されます。

プレーンオーディオデバイスを自動でリダイレクトするかどうかを構成するには、クライアントエンドポイントで次のレジストリを使用します:

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB\Devices

値の名前：AutoRedirectAudio

種類：DWORD

データ：00000000

デフォルト設定は 0 です（自動リダイレクトは行われません）。この値を 0 以外に設定すると、USB サポートによりプレーン USB オーディオデバイスがリダイレクトされます。

Active Directory ポリシーを使用して、次のレジストリキーを展開することもできます。ポリシー以外で値が指定されている場合には、この値が優先されます：

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB\Devices

値の名前：AutoRedirectVideo

種類：DWORD

データ：00000000

プレーンストレージデバイス（大容量記憶装置デバイス）のリダイレクト

プレーンストレージデバイスでは、クライアントドライブマッピングなど、最適化も行える専用の仮想チャネルを使用することでユーザーエクスペリエンスを最適化できます。ただし、ファイルの単純な読み取りまたは書き込みだけでなく、CD/DVD の作成や暗号化済みファイルシステムデバイスへのアクセスなどの特殊な操作も行う場合には、汎用 USB サポートによりデバイスをリダイレクトする必要のある場合があります。

どのデバイスがプレーンストレージデバイスであるかは、ヒューリスティックスにより判別されます。プレーンストレージデバイスを自動でリダイレクトするかどうかを構成するには、次のレジストリを使用します：

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB\Devices

値の名前：AutoRedirectStorage

種類：DWORD

データ：00000000

デフォルト設定は 0 です（自動リダイレクトは行われません）。この値を 0 以外に設定すると、汎用 USB サポートによりプレーン USB ストレージデバイスがリダイレクトされます。

Active Directory ポリシーを使用して、次のレジストリキーを展開することもできます。ポリシー以外で値が指定されている場合には、この値が優先されます：

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB\Devices

値の名前：AutoRedirectStorage

種類：DWORD

データ：00000000

> 注：
>
> 汎用 USB サポートを使用する場合、プレーンストレージデバイスへの読み取り専用アクセスを構成することはできませんが、CDM を使用する場合はこのアクセスを構成可能です。

ハードウェア暗号化機能付き **USB** フラッシュドライブのリダイレクト

一般的なハードウェア暗号化機能付き USB フラッシュドライブは、暗号化済みのストレージパーティションと、この暗号化済みパーティションのロック解除用ユーティリティが含まれるユーティリティパーティションで構成されています。USB フラッシュデバイスでは、クライアントドライブマッピング/動的サムドライブマッピングの専用 HDX 仮想チャネルを使用することで、ユーザーエクスペリエンスを最適化できます。このチャネルにより、最適化も行われます。

汎用 USB リダイレクトは、次の場合に必要です:

- Windows 以外のクライアント（Linux クライアントなど）
- 搭載されているローカル機能へのユーザーアクセスを顧客が制限（締め出し）しているクライアント

汎用 USB リダイレクトを使用すると、ハードウェア暗号化のないすべての USB ストレージデバイスを、シングルセッション OS VDA とマルチセッション OS VDA の両方にリダイレクトできます。

バージョン 7 1808 以前の Citrix Virtual Apps and Desktops では、ハードウェア暗号化機能付きの USB フラッシュドライブを、シングルセッション OS VDA セッションおよびマルチセッション OS VDA セッションへ簡単にリダイレクトすることはできませんでした。Citrix Virtual Apps and Desktops 7 1808 で実施された新しい機能強化により、汎用 USB リダイレクトを使用して、シングルセッション OS VDA セッションやマルチセッション OS VDA セッションにハードウェア暗号化機能のある USB フラッシュドライブをリダイレクトできるようになりました。
デバイスがリダイレクトされると、そのドライブはローカルクライアントに表示されません。このため、ドライブのロックを解除する必要がある場合は、セッション内で実行してください。この機能を使用するには、Windows 更新プログラム KB4074590 が必要です。

プレーン静止画デバイス（スキャナーおよびデジタルカメラ）

プレーン静止画デバイスでは、最適化も行える専用の仮想チャネル（TWAIN 仮想チャネルなど）を使用することでユーザーエクスペリエンスを最適化できます。これらのデバイスは、業界標準に準拠している必要があります。デバイスが業界標準に準拠していない場合、または当初の意図と異なる方法で使用されている場合、このデバイスを使用する唯一の方法は汎用 USB リダイレクトです。どのデバイスがプレーン静止画デバイスであるかは、ヒューリスティックスにより判別されます。

プレーン静止画デバイスを自動でリダイレクトするかどうかを構成するには、次のレジストリを使用します:

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB\Devices

値の名前：AutoRedirectImage

種類：DWORD

データ：00000000

デフォルト設定は 0 です（自動リダイレクトは行われません）。この値を 0 以外に設定すると、汎用 USB サポートによりプレーン USB 静止画デバイスがリダイレクトされます。

Active Directory ポリシーを使用して、次のレジストリキーを展開することもできます。ポリシー以外で値が指定されている場合には、この値が優先されます:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB\Devices

値の名前: AutoRedirectImage

種類: DWORD

データ: 00000000

デバイス固有の設定

Citrix で最適化可能なデバイスを選択するためのヒューリスティックスでは、目的と一致しないデバイスが選択されることがあります。最適化可能デバイスとしては、プリンター、オーディオデバイス、ビデオデバイス、ストレージデバイス、および静止画デバイスなどがあります。また、上記に記載のないデバイスについて、自動リダイレクトを制御する必要のある場合もあります。自動リダイレクトの制御は、デバイスごとに行うことができます。

たとえば、DemoTech 2,000 バーコードリーダーを、USB サポートによりリダイレクトする必要がないとします。この製品のベンダー ID は 12AB、製品 ID は 567B です。これらの 16 進数値は、デバイスマネージャーで確認できます。

このバーコードリーダーが自動リダイレクトされないようにするには、デバイス固有のレジストリキーを作成します:

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB\Devices\VID12AB PID5678

値の名前: AutoRedirect

種類: DWORD

データ: 00000000

値が 0 のため、デバイスは自動リダイレクトされません。ゼロ以外の値を指定すると、このデバイスは（ユーザー設定に応じて）自動リダイレクトの対象とみなされます。ベンダー ID と製品 ID の間には、スペース文字を 1 つ挿入します。

Active Directory ポリシーを使用して、この値をレジストリキーに設定することもできます。ポリシー以外により値が設定されている場合は、ポリシーで設定した値が優先されます:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB\Devices\VID12AB PID5678

値の名前: AutoRedirect

種類: DWORD

データ: 00000000

デバイス固有の AutoRedirect 設定は、上述した対象デバイスの幅が広い AutoRedirectXXX の値よりも優先されます。Citrix の最適化対象デバイスを選択するデフォルトのヒューリスティックスでは、デバイスが汎用デバイス

であると誤解される場合があります。このため、自動リダイレクトが行われるようにするには、デバイス固有の AutoRedirect の値を 1 に設定します。

既存の **USB** デバイスの自動接続を許可する

この設定は、リモートセッションへのセッションの開始時に、エンドポイントに接続されている既存の USB デバイスの自動接続を許可または禁止します。

この設定では、以下のいずれかのオプションを選択します。

- 使用可能な USB デバイスをリダイレクトする前に確認する。
- 使用可能な USB デバイスを自動的にリダイレクトしない。
- 使用可能な USB デバイスを自動的にリダイレクトする。

デフォルトでは、[使用可能な **USB** デバイスをリダイレクトする前に確認する] オプションが選択されています。選択されたポリシーに基づいて、クライアントの [基本設定] > [デバイス] セクションで選択されたオプションは上書きできます。

> 注:
>
> 現在、[既存の **USB** デバイスの自動接続を許可する] ポリシーは、Windows 向け Citrix Workspace アプリにのみ適用されます。

新しく受信した **USB** デバイスの自動接続を許可する

この設定は、セッション中にエンドポイントに挿入された USB デバイスのリモートセッションへの自動接続を許可または禁止します。

この設定では、以下のいずれかのオプションを選択します。

- 使用可能な USB デバイスをリダイレクトする前に確認する。
- 使用可能な USB デバイスを自動的にリダイレクトしない。
- 使用可能な USB デバイスを自動的にリダイレクトする。

デフォルトでは、[使用可能な **USB** デバイスをリダイレクトする前に確認する] オプションが選択されています。選択されたポリシーに基づいて、クライアントの [基本設定] > [デバイス] セクションで選択されたオプションは上書きできます。

> 注:
>
> 現在、[新しく受信した **USB** デバイスの自動接続を許可する] ポリシーは、Windows 向け Citrix Workspace アプリにのみ適用されます。

クライアント **USB** デバイスリダイレクト規則（バージョン **2**）

この設定では、USB デバイスをリモートセッションにフィルタリング、分割、および自動接続するための規則を指定します。

この設定が選択されている場合、ホストは、この設定で構成されたデバイス規則で ［クライアント *USB* デバイスリダイレクト規則］設定を上書きします。

詳しくは、「複合 USB デバイスリダイレクトの構成」を参照してください。

仮想チャネルの許可リストポリシー設定

August 17, 2024

仮想チャネルの許可リストポリシー設定により、ICA セッションで開くことを許可する仮想チャネルを指定した許可リストを使用できるようになります。

無効にすると、すべての仮想チャネルが許可されます。

有効にすると、Citrix 仮想チャネルのみが許可されます。

カスタムまたはサードパーティの仮想チャネルを使用するには、仮想チャネルをリストに追加します。仮想チャネルをリストに追加するには以下を行います:

1. 仮想チャネル名のあとにコンマを入力する。
2. その仮想チャネルにアクセスするプロセスへのパスを入力する。

さらに実行可能なパスをリストすることができ、パスはコンマで区切られます。

たとえば、

```
CTXCVC1,C:\VC1\vchost.exe
CTXCVC2,C:\VC2\vchost.exe,C:\Program Files\Third Party\vcaccess.exe
```

Citrix Virtual Apps and Desktops 7 2109 以降、仮想チャネルの許可リストはデフォルトで有効になっています。許可リストへの仮想チャネルの追加について詳しくは、「許可リストへの仮想チャネルの追加」を参照してください

Skype for Business の HDX RealTime Optimization Pack を使用している場合は、仮想チャネルを許可リストに追加します。詳しくは、HDX RealTime Optimization Pack のドキュメントを参照してください。

> 重要:
>
> 設定を有効にするには、VDA マシンを再起動する必要があります。

詳しくは、「ICA 仮想チャネル」を参照してください。

仮想チャネル許可リストのログ

このポリシー設定を使用して、仮想チャネル許可リストのログのレベルを構成できます。

次のオプションが利用可能です:

| オプション | 説明 |
| 無効 | すべてのログイベントを無効にします。 |
| 警告のみをログに記録 | イベントは、開こうとした、許可リストに含まれていないカスタム仮想チャネルについてのみ記録されます。
| すべてのイベントをログに記録 | すべてのイベントがログに記録されます |

仮想チャネルの許可リストのログ調整

このポリシー設定を使用して、アクティブなセッションのイベントをログに記録する頻度を構成できます。

各仮想チャネルのすべてのイベントは、最初に発生したときにログに記録されます。繰り返されるイベントは、セッションがアクティブである間の調整期間中は無効になります。セッションが切断されると、調整期間はリセットされます。

視覚表示のポリシー設定

August 17, 2024

視覚表示セクションには、仮想デスクトップからユーザーデバイスに送信されるイメージの品質を制御するためのポリシー設定が含まれています。

簡素なグラフィックに対する優先的色の解像度

このポリシー設定は VDA バージョン 7.6 FP3 以降で使用できます。8 ビットオプションは VDA バージョン 7.12 以降で使用できます。

この設定により、単純なグラフィックがネットワーク経由で送信される際の色数を低下させることができます。ピクセルあたり 8 ビットまたは 16 ビットに色数を低下させると、低帯域幅接続での応答性を潜在的に向上させることができます。ただし、この操作を実行すると、画質がわずかに低下することがあります。［圧縮にビデオコーデックを使用する］ ポリシーが ［画面全体］ に設定されている場合、8 ビット色数はサポートされません。

デフォルトの優先色数は、ピクセルあたり 24 ビットです。

8 ビット設定が VDA バージョン 7.11 以前に適用されている場合、VDA は 24 ビット（デフォルト）色数にフォールバックします。

ターゲットフレーム数

この設定項目では、仮想デスクトップからユーザーデバイスに送信されるイメージの 1 秒あたりの最大フレーム数（fps）を指定します。

デフォルトの最大フレーム数は、30fps です。

1 秒あたりのフレーム数を高く（30 など）すると、ユーザーエクスペリエンスは向上しますが、より多くの帯域幅が必要になります。1 秒あたりのフレーム数を低く（10 など）すると、ユーザーエクスペリエンスは低下しますが、サーバーのスケーラビリティが向上します。CPU が低速なユーザーデバイスに対しては、小さい値を指定した方がユーザーエクスペリエンスが向上する場合があります。

サポートされている 1 秒あたりの最大フレームレートは 60 です。

表示品質

この設定では、ユーザーデバイス側に表示されるイメージの表示品質を指定します。

この設定のデフォルト値は［中］です。

イメージの表示品質を指定するには、次のいずれかのオプションを選択します。

- 低 - 対話操作性のために表示品質を低下させてもよい、帯域幅が制限されたネットワークに適しています。
- 中 - 一般的に最良のパフォーマンスおよび帯域幅効率が提供されます。
- 高 - 視覚的に無損失なイメージ品質が提供されます。
- ［操作時は低品質］ - 多くのネットワークトラフィックが発生している間は非可逆イメージが送信され、ネットワークトラフィックが減少したときに高品質な無損失イメージが送信されます。この設定により、帯域幅を制限されたネットワーク接続でのパフォーマンスが向上します。
- 常に無損失 - イメージデータの画質を優先する必要がある場合には、［常に無損失］を選択して、非可逆イメージデータがユーザーデバイスに送信されないようにします。たとえば、品質の低下が許容されない X 線画像を表示する場合などに選択します。

動画のポリシー設定

August 17, 2024

［動画］セクションには、動画の圧縮機能を無効にしたり変更したりするためのポリシー設定項目があります。

画質の下限レベル

注：Virtual Delivery Agent 7.x では、［従来のグラフィックモード］設定が有効な場合のみこの設定項目が適用されます。

この設定では、アダプティブ表示の最低レベルの画質を指定します。圧縮率が小さいほど、画質は高くなります。超最高、最高、高、通常、または低から選択します。

デフォルトでは、［通常］に設定されています。

動画圧縮

この設定では、アダプティブ表示を有効または無効にします。アダプティブ表示機能では、ビデオやスライドショーのスライド切り替え時の画質が、使用可能な帯域幅に基づいて自動的に調節します。アダプティブ表示を有効にすると、表示品質を劣化させることなくプレゼンテーションをスムーズに実行できます。

デフォルトでは、アダプティブ表示が有効になっています。

VDA 7.0～7.6 では、［従来のグラフィックモード］が有効な場合のみこの設定が適用されます。VDA Version 7.6 FP1 以降については、従来のグラフィックモードが有効の場合、または従来のグラフィックモードが無効でグラフィックの圧縮にビデオコーデックが使用されていない場合、この設定が適用されます。

従来のグラフィックモードが有効な場合、ポリシーの変更を適用する前にセッションを再起動する必要があります。アダプティブ表示とプログレッシブ表示は相互に排他的です。アダプティブ表示を有効にすると、プログレッシブ表示は無効になり、その逆の場合も同じです。ただし、プログレッシブ表示とアダプティブ表示の両方を同時に無効にすることは可能です。従来からの機能であるプログレッシブ表示は XenApp または XenDesktop にはお勧めしません。プログレッシブしきい値レベルを設定するとアダプティブ表示は無効になります。

プログレッシブ圧縮のレベル

注：Virtual Delivery Agent 7.x では、［従来のグラフィックモード］設定が有効な場合のみこの設定項目が適用されます。

この設定では、最初にダウンロードされるイメージの品質を落として、初期表示のパフォーマンスを向上させる機能を制御します。

デフォルトでは、プログレッシブ圧縮は適用されません。

プログレッシブ圧縮では、初期表示の後で、より詳細なイメージデータがダウンロードされます（そのイメージの圧縮レベルは非可逆圧縮設定で制御されます）。［最高］または［超最高］を選択すると、写真など帯域幅に負荷のかかるグラフィックの表示パフォーマンスが向上します。

プログレッシブ圧縮による効果を得るには、［非可逆圧縮のレベル］よりも高い圧縮レベルを指定する必要があります。

注：プログレッシブ表示の圧縮レベルを高くすると、セッションでの動的イメージの対話操作性が向上します。この機能を有効にすると、3D モデルを回転させる場合など、イメージを動かしている間の表示品質は一時的に低下します。イメージを停止させると、非可逆圧縮のレベルで制御される画質が適用されます。

関連する設定項目は以下のとおりです：

- プログレッシブ圧縮のしきい値
- プログレッシブヘビーウェイト圧縮

プログレッシブ圧縮のしきい値

注：Virtual Delivery Agent 7.x では、［従来のグラフィックモード］設定が有効な場合のみこの設定項目が適用されます。

この設定では、プログレッシブ圧縮を適用する接続の最大帯域幅を、キロビット/秒（Kbps）単位で指定します。この帯域幅に達しないクライアント接続にのみ圧縮が適用されます。

デフォルトのしきい値は、2147483647KB/秒です。

関連する設定項目は以下のとおりです：

- プログレッシブ圧縮のしきい値
- プログレッシブヘビーウェイト圧縮

保持する最低フレーム数

この設定では、低帯域幅接続時に確保される動的イメージの最低フレーム数を、フレーム数/秒（fps）単位で指定します。

デフォルトでは、10fps に設定されています。

VDA 7.0～7.6 では、［従来のグラフィックモード］が有効な場合のみこの設定が適用されます。VDA 7.6 FP1 以降では、［従来のグラフィックモード］が有効であるか無効であるかにかかわらず、この設定が適用されます。

> 注：
>
> 保持する最低フレーム数ポリシーは廃止され、10fps に設定されました。これは、エンドユーザーがグラフィック状態インジケーターの品質スライダーを使用して変更できます。

静止画のポリシー設定

August 17, 2024

［静止画］セクションには、静止画の圧縮機能を無効にしたり変更したりするための設定項目があります。

エクストラ色圧縮

この設定では、狭帯域幅接続でのイメージ配信で使用されるエクストラ色圧縮機能を有効または無効にします。この機能を有効にすると、イメージ品質が低下しますが狭帯域幅接続におけるセッションの応答性が向上します。

デフォルトでは、エクストラ色圧縮は無効になっています。

エクストラ色圧縮を有効にした場合、［エクストラ色圧縮しきい値］の設定値を下回るクライアント接続でのみこの圧縮機能が適用されます。クライアント接続の帯域幅がしきい値を上回る場合、または［エクストラ色圧縮］設定で［無効］が選択されている場合、この圧縮機能は適用されません。

エクストラ色圧縮しきい値

注：Virtual Delivery Agent 7.x では、［従来のグラフィックモード］設定が有効な場合のみこの設定項目が適用されます。

この設定では、エクストラ色圧縮を適用する接続の最大帯域幅を、キロビット/秒（Kbps）単位で指定します。クライアント接続帯域幅がこの値を下回る場合、エクストラ色圧縮が適用されます（［エクストラ色圧縮］設定で［有効］が選択されている場合）。

デフォルトのしきい値は、8192KB/秒です。

ヘビーウェイト圧縮

注：Virtual Delivery Agent 7.x では、［従来のグラフィックモード］設定が有効な場合のみこの設定項目が適用されます。

この設定では、プログレッシブ圧縮よりもさらに消費帯域幅を節約する機能を有効または無効にします。ヘビーウェイト圧縮では、CPU 要求度の高いグラフィックアルゴリズムが使用され、画質を損なわずにイメージデータで使用される帯域幅を抑えることができます。

デフォルトでは、ヘビーウェイト圧縮は無効になっています。

この圧縮機能を有効にすると、すべての非可逆圧縮設定に適用されます。この機能は Citrix Workspace アプリでサポートされていますが、ほかのプラグインソフトウェアでは無視されます。

関連する設定項目は以下のとおりです：

- プログレッシブ圧縮のレベル
- プログレッシブ圧縮のしきい値

非可逆圧縮のレベル

注：Virtual Delivery Agent 7.x では、［従来のグラフィックモード］設定が有効な場合のみこの設定項目が適用されます。

この設定では、狭帯域幅接続でのイメージ配信で使用される非可逆圧縮のレベルを指定します。狭帯域幅接続では、ICA セッション内での非圧縮イメージの表示に時間がかかる場合があります。

デフォルトでは、中レベルの圧縮が選択されています。

イメージ表示のパフォーマンスを改善させるには、高い圧縮レベルを使用します。逆に、X 線写真を表示するなどイメージの画質が優先される場合では、非可逆圧縮を無効にします。

関連する設定項目：非可逆圧縮のしきい値

非可逆圧縮のしきい値

注：Virtual Delivery Agent 7.x では、［従来のグラフィックモード］設定が有効な場合のみこの設定項目が適用されます。

この設定では、非可逆圧縮を適用する接続の最大帯域幅を、キロビット/秒（Kbps）単位で指定します。

デフォルトのしきい値は、2147483647KB/秒です。

非可逆圧縮のしきい値を指定せずに［非可逆圧縮のレベル］設定をポリシーに追加すると、LAN 環境での高精細ビットマップ（写真など）の表示速度が向上する場合があります。

関連する設定項目：非可逆圧縮のレベル

WebSocket のポリシー設定

August 17, 2024

WebSocket セクションには、仮想デスクトップおよびホストアプリケーションへの、HTML5 向け Citrix Workspace アプリを使用したアクセスに関するポリシー設定が含まれています。WebSocket 機能により、Web ブラウザーアプリケーションとサーバーとの間の双方向通信が有効になり、セキュリティが向上して、サーバーのオーバーヘッドが軽減されます。この機能は、複数の HTTP 接続を開くことなく実行できます。

WebSocket 接続

この設定では、WebSocket プロトコルによる接続を許可または禁止します。

デフォルトでは、無効になっています。

WebSocket ポート番号

この設定では、WebSocket 接続の着信ポートの番号を指定します。

デフォルトでは、値は 8008 です。

WebSocket 信頼される接続元サーバー一覧

この設定では、信頼される接続元サーバー（通常 Web 向け Citrix Workspace アプリ）の URL をコンマ区切りの一覧で指定します。この一覧に追加したサーバーからの WebSocket 接続のみが受け入れられます。

デフォルトでは、ワイルドカード文字「*」が設定されています。これにより、Web 向け Citrix Workspace アプリのすべての URL が信頼され、アクセスが許可されます。

この設定では、URL を以下の形式で指定します。

<protocol>://<hostFQDN>:[port]

ここで、<protocol> は HTTP または HTTPS である必要があります。<port> にポート番号を指定しない場合、HTTP では 80、HTTPS では 443 が使用されます。

URL の一部にワイルドカード文字*を使用できますが、IP アドレス（`10.105.*.*`）には使用できません。

WIA デバイスのポリシー設定

August 17, 2024

WIA デバイスセクションには、Windows Image Acquisition（WIA）を使用してスキャナーのリダイレクトを管理するためのポリシー設定が含まれています。

WIA リダイレクト

デジタルカメラやスキャナーなどの WIA デバイスは、WIA フレームワークを使用して、サーバーでホストされている画像処理アプリケーションと通信します。この設定により、ユーザーデバイス側の WIA デバイスにアクセスすることを許可または禁止します。デフォルトでは、WIA リダイレクトは禁止されています。

WIA 準拠デバイスについては、「WIA デバイス」を参照してください。

レジストリで管理される **HDX** 機能

August 17, 2024

> 注:
>
> レジストリエディターの使用を誤ると、深刻な問題が発生する可能性があり、オペレーティングシステムの再インストールが必要になる場合もあります。レジストリエディターの誤用による障害に対して、Citrix では一切責任を負いません。レジストリエディターは、お客様の責任と判断の範囲でご使用ください。また、レジスト

> リファイルのバックアップを作成してから、レジストリを編集してください。

レジストリエディターを開くには、サーバーで`regedit.exe`を実行します。次に、レジストリキーに移動して、設定を追加または編集します。

デバイス

Bloomberg キーボード

Citrix Virtual Apps and Desktops では、Bloomberg モデル 4 およびモデル 3 Starboard キーボードがサポートされています。デフォルトでは、Bloomberg キーボードの拡張サポートは無効になっています。

Bloomberg キーボードのサポートを有効にするには、接続を開始する前にクライアントマシンで次のレジストリ値を設定します:

- キー: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICAClient\GenericUSB`
- 値の名前: `EnableBloombergHID`
- データ型: `DWORD`
- 値のデータ:
  - `0` - 無効
  - `1` - 有効

詳しくは、「Bloomberg キーボード」を参照してください。

マップされたクライアントドライブ

セキュリティ対策として、ユーザーが Citrix Virtual Apps and Desktops にログオンすると、サーバーはデフォルトでユーザーの実行権限なしでクライアントドライブをマップします。ユーザーがマップされたクライアントドライブにある実行可能ファイルを実行できるようにするには、サーバーのレジストリを編集してこのデフォルト設定を上書きします。

アクセスを許可するには、次のレジストリ値を編集します（**CDMSettings** が存在しない場合は作成します）:

- キー: `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\CDMSettings`
- 値の名前: `ExecuteFromMappedDrive`
- データ型: `DWORD`
- 値のデータ:
  - `1` - アクセスを許可
  - `0` - マップされたドライブのアクセスを拒否

この変更は、レジストリの編集後に接続されたセッションに対して有効になります。

Citrix Virtual Apps and Desktops 7 2006 は、このレジストリの場所を含む最初のバージョンです。以前のバージョンの Citrix Virtual Apps and Desktops では、別のレジストリの場所が使用されていました。

詳しくは、「クライアントドライブマッピング」を参照してください。

Microsoft Surface Pro および **Surface Book** のペン

Citrix Virtual Apps and Desktops では、Windows Ink を使用するアプリケーションで標準のペン機能がサポートされています。この機能は、デフォルトで有効になります。

この機能を無効または有効にするには、レジストリ値を次のように設定します:

- キー: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Citrix Virtual Desktop Agent\PenApi`
- 値の名前: `DisablePen`
- データ型: `DWORD`
- 値のデータ:
  - `1` - 無効
  - `0` - 有効

詳しくは、「[Microsoft Surface Pro および Surface Book のペン]」(/en-us/citrix-virtual-apps-desktops/devices/mobile-devices.html#microsoft-surface-pro-and-surface-book-pens) を参照してください。

Windows Image Acquisition アプリケーションの許可リスト

この設定により、VDA 上のどのアプリケーションに Windows Image Acquisition スキャナーのリダイレクトへのアクセスを許可するかを制御できます。

デフォルトでは、Windows Image Acquisition にアクセスできるアプリケーションはありません。

VDA 上のアプリケーションに対して Windows Image Acquisition を調整するには、次のレジストリ設定を作成します:

- キー: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix`
- 値の名前: `WIAAllowedProcesses`

  [**WIAAllowedProcesses**] を選択して右クリックします。[新規] **>** [複数行文字列値] の順に選択して、新しい値の名前を「**AllowProcesses**」に変更します。
- 値のデータ: Windows Image Acquisition にアクセスできる各アプリケーションのフルパスとプロセス名を入力します。各アプリケーションを新しい行に入力します。

この設定への変更は、次に VDA でセッションを起動したときに有効になります。

一般

HDX Reducer

セッションホストで使用する HDX 圧縮アルゴリズム（Reducer）のバージョンを構成できます。

シングルセッション VDA で Reducer V4 を有効にするには、次のレジストリ値を設定します:

キー:HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\GroupPolicy\Defaults\WDSettings

値の名前: ReducerOverrideMask
値の種類: DWORD
値のデータ: 23（10 進数）

マルチセッション VDA で Reducer V4 を有効にするには、次のレジストリ値を設定します:

- キー: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd
- 値の名前: ReducerOverrideMask
- データ型: DWORD
- 値のデータ: 23（10 進数）

EDT タイムアウトを構成する

VDA では、EDT タイムアウトを 5〜25 秒の任意の値に構成できます。デフォルトの EDT タイムアウト値は 25 秒です。

- キー: HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd\Tds\udp\UDPStackParameters
- データ型: DWORD
- 値の名前: edtConnectionTimeout
- 値のデータ: 5〜25 秒の秒単位の時間（10 進数）

Windows 向け Citrix Workspace アプリのタイムアウトを構成することもできます:

- キー: HKLM\SOFTWARE\WOW6432Node\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\EDT
- データ型: String / REG_SZ
- 値の名前: edtConnectionTimeout
- 値のデータ: 5〜25 秒の秒単位の時間（10 進数）

Rendezvous バージョンの構成

使用する Rendezvous バージョンを構成するには、次のレジストリ値を設定します:

- キー: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\VirtualDesktopAgent
- データ型: DWORD
- 値の名前: GctRegistration
- 値のデータ:
  - 1 - V2 を有効にする
  - 0 - V1 を有効にする

VDA への自動ログオンの構成

この設定により、Windows 10 シングルセッション OS およびマルチセッション OS VDA で、Microsoft ポリシーの ［常にパスワードの入力を求める］設定を有効または無効にすることができます。

［常にパスワードの入力を求める］が有効になっている場合、ユーザーはリモートセッションを開始するときに VDA で資格情報を入力する必要があります。この設定が無効になっている場合、ユーザーは VDA で資格情報を入力せずにリモートセッションに自動的に接続します。

デフォルトでは、Microsoft ポリシー設定は無効になっています。［常にパスワードの入力を求める］設定を有効または無効にするには、VDA で次のレジストリ値を設定します:

- キー: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Portica
- 値の名前: AutoLogon
- データ型: DWORD
- 値のデータ:
  - 1 - Microsoft ポリシー設定を無効にして、ユーザーがリモートセッションに自動的にサインインできるようにします。
  - 0 –Microsoft ポリシー設定を有効にし、ユーザーがリモートセッションを起動するときに資格情報を入力するように求めます。

タイムアウト警告を無効にする

デフォルトでは、非アクティブまたはアイドルのセッション状態にあるユーザーは、セッションが自動的に切断される 2 分前に警告メッセージを受け取ります。

この設定により、以下でアイドルセッションタイムアウトの上限に達したユーザーに対して表示される警告メッセージが無効および削除されます:

- Windows Server 2004
- Windows 10 マルチセッション 2004 以降のマルチセッション OS

警告を削除するには、VDA で次のレジストリ値を設定します:

- キー: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Winstations\ICA-CGP
- 値の名前: fEnableTimeoutWarning
- データ型: DWORD
- 値のデータ:
  - 1 - 警告メッセージを無効にする
  - 0 - 警告メッセージを有効にする

警告メッセージを表示するには、レジストリ値を削除するか、0に設定します。

EDT MTU Discovery

MTU Discovery により、セッション確立時に EDT が最大伝送単位（MTU）を自動的に決定できるようにします。これにより、パフォーマンスの低下やセッションの確立失敗となる可能性のある、EDT パケットのフラグメンテーションが防止されます。

この設定項目は、デフォルトで有効になっています。EDT MTU Discovery を無効にするには、以下のレジストリ値を構成して VDA を再起動します。

- キー: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd
- 値の名前: MtuDiscovery
- データ型: DWORD
- 値のデータ: 0

この設定はマシン全体で有効であり、サポートされているクライアントから接続しているすべてのセッションに反映されます。

損失耐性モードを有効にする

Windows 向け Citrix Workspace アプリ、マルチユーザー VDA、およびデスクトップ VDA の双方向オーディオサービスで、損失耐性モードを使用してアダプティブオーディオにアクセスできます。このチェックボックスは、デフォルトでオフになっています。損失耐性モードを有効にするには、使用しているマシンに応じて次のレジストリ値を構成し、それぞれのマシンを再起動します。

Windows クライアント向け Citrix Workspace アプリの場合、

- キー: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ClientAudio
- 値の名前: EdtUnreliableAllowed
- データ型: REG_SZ
- 値のデータ: 1

TS VDA の場合、

- キー: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\Audio
- 値の名前: EdtUnreliableAllowed
- データ型: DWORD
- 値のデータ: 1

WS VDA の場合、

- キー: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Audio
- 値の名前: EdtUnreliableAllowed
- データ型: DWORD
- 値のデータ: 1

一般コンテンツリダイレクト

ホストからクライアントへのリダイレクトの **URL** タイプ一覧の追加

デフォルトでは、次の URL タイプのリダイレクトをサポートしています: HTTP、HTTPS、RTSP、RTSPU、PNM、および MMS。Windows クライアントで、以下のレジストリキーと値を作成することで、一覧に URL タイプを追加できます。

- キー: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Policies\Citrix\ICA Client\SFTA
- 値の名前: ExtraURLProtocols
- データ型: REG_SZ
- 値のデータ: 必要な URL タイプをセミコロンで区切って指定します。URL の権限部分の前にすべてを含めます。例:
  ftp://;mailto:;customtype1://;custometype2://

Windows クライアントに対してのみ URL タイプを追加できます。このレジストリ設定がないクライアントは、Citrix セッションへ戻るリダイレクトを拒否します。クライアントには、指定された URL タイプを処理するようにアプリケーションがインストールおよび構成されている必要があります。

詳しくは、「ホストからクライアントへのリダイレクト」を参照してください。

クライアントフォルダーのリダイレクト

クライアントフォルダーのリダイレクトは、クライアント側のファイルがホスト側のセッションのへアクセスする方法を変更します。管理者がサーバーでクライアントフォルダーのリダイレクトを有効にし、ユーザーがユーザーデバイスでリダイレクトを構成することを検討してください。この場合、ユーザーが指定したローカルボリューム部分がリダイレクトされます。

サーバー側でクライアントフォルダーのリダイレクトを有効にするには、次のレジストリ値を設定します:

- キー: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\Client Folder Redirection
- 値の名前: CFROnlyModeAvailable
- データ型: DWORD
- 値のデータ: 1

詳しくは、「クライアントフォルダーのリダイレクト」を参照してください。

特定の **Web** サイトのセットについてホストからクライアントへリダイレクト

特定の Web サイトのセットについてホストからクライアントへのリダイレクト機能を有効にするには、サーバー VDA で次のレジストリ値を設定します。

- キー: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\SFTA
- 値の名前: ValidSites
- データ型: REG_MULTI_SZ
- 値のデータ: FQDN（完全修飾ドメイン名: Fully-Qualified Domain Name）の組み合わせを指定します。1 つの行に 1 つの FQDN を入力してください。プロトコル（http://または https://）を使用せずに、FQDN のみを含めます。FQDN には、左端にのみワイルドカード文字としてアスタリスク（*）を含めることができます。このワイルドカードは単一レベルのドメインと照合されます。これは RFC 6125 の規則に準拠しています。例:

```
www.example.com
```

```
*.example.com
```

詳しくは、「ホストからクライアントへのリダイレクト」を参照してください。

ログオフおよび切断時のローカルアプリケーションの動作

デフォルトでは、ユーザーが仮想デスクトップからログオフまたは切断しても、ローカルアプリケーションは実行したまま保持されます。仮想デスクトップに再接続すると、そのローカルアプリケーションが再統合されます（仮想デスクトップで使用可能な場合）。ログオフおよび切断時のローカルアプリケーションの動作を構成するには、ホストされるデスクトップで次のレジストリ値を設定します:

- キー: HKEY_LOCAL_MACHINE\SOFTWARE\wow6432node\Citrix\Client Hosted Apps\Policies
- 値の名前: Session State
- データ型: DWORD
- 値のデータ:

  - 1 —ユーザーが仮想デスクトップからログオフまたは切断しても、ローカルアプリケーションは実行したまま保持されます。仮想デスクトップに再接続すると、そのローカルアプリケーションが再統合されます（仮想デスクトップで使用可能な場合）。
  - 3 —ユーザーが仮想デスクトップからログオフまたは切断した場合、ローカルアプリケーションが終了します。

詳しくは、「ローカルアプリアクセスと URL リダイレクト」を参照してください。

ホストからクライアントへのリダイレクトの **URL** タイプ一覧の削除

デフォルトのリダイレクト一覧から URL タイプを削除するには、サーバー VDA で次のレジストリキーと値を作成します。

- キー: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\SFTA`
- 値の名前: `DisableServerFTA`
- データ型: `DWORD`
- 値のデータ: 1
- 値の名前: `NoRedirectClasses`
- データ型: `REG_MULTI_SZ`
- 値のデータ: 値の組み合わせを指定します: `http`、`https`、`rtsp`、`rtspu`、`pnm`、または`mms`。1 つの行に 1 つの値を入力してください。例:

```
http
https
rtsp
```

詳しくは、「ホストからクライアントへのリダイレクト」を参照してください。

サーバー **VDA** のデフォルトの **Web** ブラウザー構成

ホストからクライアントへのリダイレクトを有効にすると、サーバー VDA のデフォルトの Web ブラウザー構成を置き換えることができます。Web URL がリダイレクトされない場合、Citrix Launcher は URL を`command_backup`レジストリキーで構成された Web ブラウザーに渡します。キーはデフォルトで Internet Explorer を指定しますが、これを変更して別の Web ブラウザーへのパスを含めることができます。

- Internet Explorer（デフォルト）
  - キー: `HKEY_CLASSES_ROOT\http\shell\open\command_backup`
  - 値の名前: `Default`

  - データ型: REG_SZ
  - 値のデータ: "c:\program files\internet explorer\iexplore.exe""%1"
  - キー: HKEY_CLASSES_ROOT\https\shell\open\command_backup
  - 値の名前: Default
  - データ型: REG_SZ
  - 値のデータ: "c:\program files\internet explorer\iexplore.exe""%1"

- Google Chrome
  - キー: HKEY_CLASSES_ROOT\http\shell\open\command_backup
  - 値の名前: Default
  - データ型: REG_SZ
  - 値のデータ: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe""%1"
  - キー: HKEY_CLASSES_ROOT\https\shell\open\command_backup
  - 値の名前: Default
  - データ型: REG_SZ
  - 値のデータ: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe""%1"

- Microsoft Edge
  - キー: HKEY_CLASSES_ROOT\http\shell\open\command_backup
  - 値の名前: Default
  - データ型: REG_SZ
  - 値のデータ: "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe""%1"
  - キー: HKEY_CLASSES_ROOT\https\shell\open\command_backup
  - 値の名前: Default
  - データ型: REG_SZ
  - 値のデータ: "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe""%1"

公開アプリケーションのローカルアプリアクセス

ローカルアプリアクセスを有効にすると、ローカルにインストールされている Windows アプリケーションが仮想デスクトップ環境にシームレスに統合されます。公開アプリケーションへのアクセスを許可するには、サーバーで次のレジストリ値を設定します:

- キー: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\DesktopStudio`
- 値の名前: `ClientHostedAppsEnabled`
- データ型: `DWORD`
- 値のデータ:
  - `1` - 有効
  - `0` - 無効

詳しくは、「ローカルアプリアクセスと URL リダイレクト」を参照してください。

グラフィック

CUDA または **OpenCL** アプリケーション用の **GPU** アクセラレーション機能

ユーザーセッションで実行中の CUDA および OpenCL アプリケーションの GPU アクセラレーションは、デフォルトで無効です。

CUDA アクセラレーション POC 機能を有効にするには、次のレジストリを設定します:

- キー: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\CtxHook\AppInit_Dlls\Graphics Helper`
- 値の名前: `CUDA`
- データ型: `DWORD`
- 値のデータ: `00000001`

OpenCL アクセラレーション POC 機能を有効にするには、次のレジストリを設定します:

- キー: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\CtxHook\AppInit_Dlls\Graphics Helper`
- 値の名前: `OpenCL`
- データ型: `DWORD`
- 値のデータ: `00000001`

詳しくは、「Windows マルチセッション OS のための GPU アクセラレーション」を参照してください

プログレッシブモード

プログレッシブモードはデフォルトで無効になっています。プログレッシブモードの状態は、次のレジストリ値を使用して変更できます:

- キー: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics`
- データ型: `REG_DWORD`
- 値の名前: `ProgressiveDisplay`
- 値のデータ:
  - `0` - 常時オフ（プログレッシブモードが無効。この値がデフォルト）
  - `1` - 自動（ネットワーク状態に基づいてオンとオフを切り替える）
  - `2` - 常時オン

詳しくは、「プログレッシブモード」を参照してください。

> 注:
>
> プログレッシブモードは廃止されました。Thinwire は、プログレッシブモードの利点をほぼすべて提供しながら画像配信を最適化し、キャッシュ効率を維持するための代替オプションです。

Windows Presentation Foundation（WPF）のレンダリング

HDX 3D Pro 機能により、Windows マルチセッション OS のセッションで実行しているグラフィック処理アプリケーションで、サーバー上の GPU（Graphics Processing Unit）リソースを使用できるようになります。Windows Presentation Foundation（WPF）の処理をサーバーの GPU に移すことで、グラフィック処理によりサーバーの CPU 速度が低下することを回避できます。

WPF アプリケーションでのレンダリングにサーバーの GPU が使用されるようにするには、Windows マルチセッション OS を実行するサーバー上で次のレジストリキーを設定します:

1. VDA でレジストリエディターを開き、次のキーに移動します:

   `HKLM\Software\Citrix\CtxHook\AppInit_DLLs\Graphics Helper`

2. 次のレジストリ値を作成または編集します:

   - [REG_DWORD] AdapterHandle = 0x00000001
   - [REG_DWORD] DevicePath = 0x00000001
   - [REG_DWORD] Flag = 0x00000412
   - [REG_DWORD] WPF = 0x00000001

3. WPF アプリの実行可能ファイル名でサブキーを作成します。たとえば、アプリケーションの名前が「mywpfapp.exe」の場合は、次のキーを作成します:

   `HKLM\Software\Citrix\CtxHook\AppInit_DLLs\Graphics Helper\mywpfapp.exe`

4. 設定を有効にするには、サーバーを再起動します。

詳しくは、「Windows マルチセッション OS のための GPU アクセラレーション」と、「Getting the best out of WPF apps on Windows multi-session OS」のブログを参照してください。

マルチメディア

マルチメディア会議でのエコーの解消

Citrix Virtual Apps and Desktops は、エコーを最小限に抑えるエコーキャンセルオプションを提供します。この機能はデフォルトで有効になっています。エコーキャンセルを無効にするには、次のレジストリ設定のいずれかを変更します:

- キー:
  - 32 ビット: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ClientAudio`
  - 64-bit: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ClientAudio`
- 値の名前: `EchoCancellation`
- データ型: `String`/`REG_SZ`
- 値のデータ: `False`

詳しくは、「オーディオ機能」を参照してください。

オーディオ制限

クライアントにオーディオデバイスをインストールし、オーディオリダイレクトを有効にして、RDS セッションを開始すると、オーディオファイルがオーディオを再生できないことがあります。回避策として、次のレジストリキーを RDS マシンに追加し、マシンを再起動します:

- キー: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SCMConfig`
- 値の名前: `EnableSvchostMitigationPolicy`
- データ型: `DWORD`
- 値のデータ: `0`

詳しくは、「オーディオ機能」を参照してください。

ブラウザーコンテンツリダイレクトと **DPI**

ユーザーのマシン上でブラウザーコンテンツリダイレクトの DPI（スケール）を 100% を超えて設定して使用すると、リダイレクトされたブラウザーコンテンツ画面が正しく表示されません。この問題を回避するには、ユーザーの

マシン上で次のレジストリ値を設定して、Chrome に対するブラウザーコンテンツリダイレクトの GPU アクセラレーションを無効にします:

- キー: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\HdxMediaStream
- 値の名前: GPU
- データ型: DWORD
- 値のデータ: 0

詳しくは、「ブラウザーコンテンツリダイレクトと DPI」を参照してください。

高品位 **Web** カメラの解像度

メディアの種類のネゴシエーションが失敗した場合、HDX はデフォルトの VGA 解像度（640 x 480 ピクセル）に戻ります。クライアントのレジストリキーを使用して、デフォルトの解像度を設定することができます。以下のレジストリキーを設定する前に、カメラが指定された解像度をサポートしていることを確認してください。

- キー: HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXRealTime
- 幅
  - 値の名前: DefaultWidth
  - データ型: DWORD
  - 値のデータ: 10 進数で必要な幅（1280 など）
- 高さ
  - 値の名前: DefaultHeight
  - データ型: DWORD
  - 値のデータ: 10 進数で必要な高さ（720 など）

Microsoft Teams フォールバックモード

最適化された VDI モードで Microsoft Teams が読み込めない場合（Teams/About/Version で「Citrix HDX 未接続」）、VDA では、Web カメラリダイレクトやクライアントのオーディオとマイクのリダイレクトなどの従来の HDX テクノロジにフォールバックされます。Microsoft Teams の最適化をサポートしていない Workspace アプリのバージョンまたはプラットフォーム OS を使用している場合は、フォールバックレジストリキーが適用されません。

フォールバックメカニズムを制御するには、VDA で次のいずれかのレジストリ値を設定します:

- キー（1 つだけ必要）:
  - コンピューター設定 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Teams
  - ユーザー設定 HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\Teams
- 値の名前: DisableFallback

- データ型: DWORD
- 値のデータ:
  - 1 - フォールバックモードを無効にする
  - 2 - オーディオのみを有効にする

値がない、または 0 に設定されている場合、フォールバックモードが有効になります。この機能を使用するには、Microsoft Teams バージョン 1.3.0.13565 以降が必要です。詳しくは、「Microsoft Teams の最適化」を参照してください。

Citrix App Layering による **Microsoft Teams** の最適化

Citrix App Layering を使用して VDA と Microsoft Teams を異なるレイヤーで管理する場合、コマンドラインからALLUSER=1フラグを使用して Microsoft Teams をインストールする前に Windows で **PortICA** という名前の空のレジストリキーを作成します。名前、種類、およびデータはデフォルト値のままにします。

- 32 ビットバージョンのレジストリエディターのキー: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\PortICA
- 64 ビットバージョンのレジストリエディターのキー: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA

詳しくは、「Microsoft Teams の最適化」を参照してください。

ブラウザーコンテンツリダイレクトの統合 **Windows** 認証によるシングルサインオン

この設定は、VDA と同じドメイン内の統合 Windows 認証（IWA）で構成された Web サーバーへのシングルサインオンを提供します。シングルサインオンを有効にするには、次のレジストリ値を 1 に設定します:

- キー:
  - HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxMediastream

  または
  - HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\HdxMediastream
- 値の名前: WebBrowserRedirectionIwaSupport
- データ型: DWORD
- 値のデータ: 1

詳しくは、「統合 Windows 認証によるシングルサインオン」を参照してください。

user-agent 要求ヘッダー

user-agent ヘッダーは、ブラウザーコンテンツリダイレクトから送信された HTTP 要求を識別するのに役立ちます。この設定は、プロキシ規則とファイアウォール規則を構成するときに役立ちます。たとえば、サーバーがブラウザーコンテンツリダイレクトから送信された要求を禁止する場合、user-agent ヘッダーを含む規則を作成して、特定の要件をバイパスできます。Windows デバイスでのみ、user-agent 要求ヘッダーがサポートされています。

デフォルトでは、user-agent 要求ヘッダー文字列は無効になっています。クライアント側でレンダリングされたコンテンツの user-agent ヘッダーを有効にするには、レジストリエディターを使用します。

Windows 向け Citrix Workspace アプリごとに、次のレジストリ設定のいずれかを設定します:

- キー:
  - 32 ビット: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxMediaStream`
  - 64-bit: `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\HdxMediaStream`
- 値の名前: `EnableCefUserAgentString`
- データ型: `DWORD`
- 値のデータ: 1

レジストリ値を追加すると、user-agent ヘッダーに CitrixBCR/2102.1 というテキストが追加されます。この 2102.1 は、Windows 向け Citrix Workspace アプリのバージョンです。

Web カメラソフトウェア圧縮

Web カメラでハードウェアエンコード機能がサポートされる場合、HDX Web カメラビデオ圧縮ではデフォルトでそのハードウェアエンコードが使用されます。ハードウェアエンコード機能は、ソフトウェアエンコードより多くの帯域幅を消費する場合があります。ソフトウェア圧縮が使用されるようにするには、クライアント側に次の値を追加します:

- キー: `HKEY_CURRENT_USER\SOFTWARE\Citrix\HdxRealTime`
- 値の名前: `DeepCompress_ForceSWEncode`
- データ型: `DWORD`
- 値のデータ: 1

詳しくは、「HDX ビデオ会議と Web カメラビデオ圧縮」を参照してください。

Web カメラビデオ圧縮

HDX Web カメラビデオ圧縮では、仮想セッションで実行されているビデオ会議アプリケーションに H.264 ビデオを直接送信します。VDA リソースを最適化するため、HDX Web カメラ圧縮では Web カメラビデオをエンコード、トランスコード、およびデコードしません。この機能はデフォルトで有効になっています。

サーバーからビデオ会議アプリへの直接ビデオストリーミングを無効にするには、VDA で次のレジストリ値を設定します。

- キー: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxRealTime
- 値の名前: OfferH264ToApp
- データ型: DWORD
- 値のデータ: 0

詳しくは、「HDX ビデオ会議と Web カメラビデオ圧縮」を参照してください。

Web カメラビデオ圧縮フレームレート

最適なビデオフレームレートを調整するには、クライアントで次のレジストリ値を編集します:

- キー: HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXRealTime
- 値の名前: FramesPerSecond
- データ型: DWORD
- 値のデータ: 15

指定したフレームレートを Web カメラがサポートしていない場合、アプリケーションはデフォルトで 15 FPS を使用します。

詳しくは、「HDX ビデオ会議と Web カメラビデオ圧縮」を参照してください。

負荷管理のポリシー設定

August 17, 2024

負荷管理セクションには、Windows マルチセッション OS マシン間の負荷を管理するためのポリシー設定が含まれています。

負荷評価基準インデックスの計算については、CTX202150を参照してください。

同時ログオントレランス

この設定では、サーバーが許容できる同時ログオンの最大数を指定します。

デフォルトでは、この値は「2」に設定されています。

この設定が有効になっているときは、サーバー VDA 上のアクティブな同時ログオン数が指定された数を超えないように負荷分散されます。ただし、上限は厳密に制限されていません。上限を制限する（指定された数値を超える同時ログインを失敗させる）には、次のレジストリキーを作成します。

> HKEY_LOCAL_MACHINE\Software\Citrix\DesktopServer\LogonToleranceIsHardLimit
> 種類：DWORD
> 値：1

CPU 使用率

この設定では、サーバーを「負荷限界」とみなす CPU 使用率をパーセンテージで指定します。この設定を有効にすると、デフォルトで 90% になったときにそのサーバーが負荷限界として認識されます。

デフォルトでは無効になっており、CPU 使用率が負荷計算から除外されます。

CPU 使用率から除外するプロセスの優先順位

> 注:
>
> Workspace Environment Management でマシンを管理するシナリオでは、この設定をCPU 優先度設定と一緒に使用すると、意図しない結果が生じることがあります。CPU 優先度設定を使用する場合は、この設定を無効にすることをお勧めします。

この設定では、特定の優先度レベル以下のプロセスを CPU 使用率の負荷計算から除外できます。

デフォルトでは、この値は ［通常以下］ または ［低］ に設定されています。

ディスク使用率

この設定では、サーバーを「75% の負荷状態」とみなすディスクキューの長さを指定します。この設定を有効にすると、デフォルトでディスクキューの長さが 8 になったときにそのサーバーの負荷が 75% であると認識されます。

デフォルトでは無効になっており、ディスク使用率が負荷計算から除外されます。

最大セッション数

この設定では、サーバーがホストできる最大セッション数を指定します。この設定を有効にすると、デフォルトで最大 250 個のセッションを単一サーバーでホストできます。

デフォルトでは、有効になっています。

メモリ使用率

この設定では、サーバーを「負荷限界」とみなすメモリ使用率をパーセンテージで指定します。この設定を有効にすると、デフォルトで 90% になったときにそのサーバーが負荷限界として認識されます。

デフォルトでは無効になっており、メモリ使用率が負荷計算から除外されます。

基本メモリ使用量

この設定では、基本オペレーティングシステムのメモリ使用量の概算を指定します。また、サーバーの負荷をゼロと見なすメモリ使用量を MB 単位で定義します。

デフォルトでは、この値は「768」MB に設定されています。

Profile Management のポリシー設定

August 17, 2024

このセクションには、Profile Management の有効化および構成に関するポリシー設定が含まれています。

以下のような内容について詳しくは、「Profile Management のポリシー」を参照してください:

- .ini ファイル設定と同じ名前
- ポリシー設定に必要な Profile Management のバージョン

上級設定のポリシー設定

August 17, 2024

ロックされたファイルにアクセスする場合の試行数

ロックされたファイルにアクセスする場合の試行数を設定します。

このポリシーが無効の場合は、デフォルト値の 5 回が使用されます。このポリシーをここで構成しない場合、INI ファイルの値が使用されます。このポリシーをここでまたは INI ファイルで構成しない場合、デフォルト値が使用されます。

ログオフ時にインターネット **Cookie** ファイルを処理

一部の展開環境では、`Index.dat`で参照されない余分なインターネット Cookie がそのまま残ります。ブラウズ実行後にファイルシステムに余分な Cookie が残ると、プロファイルが膨張化することとなります。このポリシーにより、Profile Management で Index.dat の処理を強制実行し余分な Cookie を削除できます。このポリシーは、有効にするとログオフに時間が長くなるため、問題が発生した場合にのみ有効にしてください。

このポリシーをここで構成しない場合、INI ファイルの値が使用されます。このポリシーをここでも INI ファイル内でも構成しない場合、Index.dat の処理は実行されません。

自動構成を無効にする

Profile Management では、あらゆる Citrix Virtual Desktops 環境（Personal vDisk の存在など）が検査され、それに応じてグループポリシーが構成されます。調整されるのは［未構成］状態の Profile Management ポリシーのみなので、ユーザーによるカスタマイズは保持されます。

このポリシーにより、展開を迅速化し最適化を簡易化することができます。このポリシーを構成する必要はありません。ただし、次のいずれかを実行する場合は、自動構成を無効にすることができます:

- 以前のバージョンから設定を保持してアップグレード
- トラブルシューティング

自動構成機能は、ランタイムの環境に応じてデフォルトのポリシー設定を自動的に構成する動的な構成チェッカーのようなものです。これによって、設定を手動で構成する必要がなくなります。ランタイム環境には、以下の要素が含まれます:

- Windows OS
- Windows OS バージョン
- Citrix Virtual Desktops がある
- Personal vDisk がある

環境が変更されると、自動構成により次のポリシーが変更される場合があります:

- アクティブライトバック
- 常時キャッシュ
- ログオフ時にローカルでキャッシュしたプロファイルの削除
- キャッシュしたプロファイルを削除する前の待ち時間
- プロファイルストリーミング

これらのポリシーの OS ごとのデフォルトの状態については、次の表を参照してください:

	マルチセッション OS	シングルセッション OS
アクティブライトバック	有効	無効。Personal vDisk が使用されている場合。それ以外の場合は有効。
常時キャッシュ	無効	無効。Personal vDisk が使用されている場合。それ以外の場合は有効。

	マルチセッション OS	シングルセッション OS
ログオフ時にローカルでキャッシュしたプロファイルの削除	有効	無効（次のいずれかの状況になった場合）：Personal vDisk が使用されている場合、Citrix Virtual Desktops が割り当てられている場合、または Citrix Virtual Desktops がインストールされていない場合。それ以外の場合は有効。
キャッシュしたプロファイルを削除する前の待ち時間	0 秒	ユーザーの変更が永続的でない場合は 60 秒。それ以外の場合は 0 秒。
プロファイルストリーミング	有効	無効。Personal vDisk が使用されている場合。それ以外の場合は有効。

ただし、自動構成機能を無効にすると、上記のすべてのポリシーがデフォルトで無効になります。

> 重要：
>
> Personal vDisk は廃止となっています。詳しくは、「PvD、AppDisk、およびサポートされていないホストの削除」を参照してください。

Profile Management 1909 以降、Windows 10（バージョン 1607 以降）の［スタート］メニューの操作性が向上しました。この機能強化は、次のポリシーの自動構成を通じて行われます：

- ミラーリングするフォルダーに`Appdata\Local\Microsoft\Windows\Caches`と`Appdata\Local\Packages`を追加します。
- 同期するファイルに`Appdata\Local\Microsoft\Windows\UsrClass.Dat*`を追加します。

この設定をここで構成しない場合、INI ファイルの値が使用されます。

この設定をここでも INI ファイル内でも構成しない場合は、自動構成が有効になります。この場合、環境が変わると Profile Management の設定が変更される可能性があります。

問題が発生する場合にユーザーをログオフ

問題が発生した場合に Profile Management によってユーザーをログオフさせるかどうかを指定できます。

このポリシーが無効になっているか構成されていない場合は、問題が発生すると、Profile Management によってユーザーに一時的なプロファイルが提供されます。ユーザーストアは利用できません。

このポリシーが有効な場合は、エラーメッセージが表示されて、ユーザーはログオフされます。この手順により、問題のトラブルシューティングが容易になります。

この設定をここで構成しない場合、INI ファイルの値が使用されます。

この設定をここでも INI ファイル内でも構成しない場合は、一時プロファイルが提供されます。

カスタマーエクスペリエンス向上プログラム

カスタマーエクスペリエンス向上プログラムは、デフォルトで有効になっており、匿名の統計および使用状況データを収集して、Citrix 製品の品質とパフォーマンスを向上させるために役立てます。

この設定をここで構成しない場合、INI ファイルの値が使用されます。

Outlook で検索インデックスの移動を有効にする

Outlook 検索データをユーザープロファイルと一緒に自動的に移動することで、ユーザーベースの Outlook の検索エクスペリエンスを実現します。この機能には、ユーザーストアに Outlook の検索インデックスを保存するための追加の領域が必要です。

このポリシーを有効にするには、ログオフしてから再度ログオンします。

Outlook 検索インデックスデータベース **-** バックアップと復元

［Outlook で検索インデックスの移動を有効にする］ポリシーが有効になっている場合にログオン時に Profile Management で実行される処理を指定できます。

このポリシーが有効になっている場合、Profile Management は、ログオン時にデータベースが正常にマウントされるたびに、検索インデックスデータベースをバックアップします。Profile Management は、バックアップを検索インデックスデータベースの完全な状態に近い正常なコピーとして扱います。データベースが破損したために検索インデックスデータベースのマウントが失敗すると、Profile Management は、検索インデックスデータベースを、前回認識された正常なコピーに自動的に戻します。

> 注:
>
> Profile Management は、新しいバックアップが正常に保存された後に、以前に保存されたバックアップを削除します。バックアップにより、利用可能な VHDX ストレージが消費されます。

Outlook 検索データの移動の同時セッションサポートを有効にする

Profile Management で、ネイティブ Outlook の検索エクスペリエンスを同じユーザーの同時セッションに提供できます。このポリシーは、Outlook ポリシーの検索インデックスの移動で使用します。

このポリシーを有効にすると、同時セッションごとに個別の Outlook OST ファイルが使用されます。

デフォルトでは、Outlook OST ファイルの保存に使用できる VHDX ディスクは 2 つだけです（ディスクごとに 1 つのファイル）。ユーザーがさらにセッションを開始すると、Outlook OST ファイルはローカルユーザープロファイルに保存されます。Outlook OST ファイルを格納する VHDX ディスクの最大数を指定できます。

OneDrive コンテナを有効にする

OneDrive フォルダーをユーザーと一緒に移動できます。

OneDrive コンテナは、VHDX ベースのフォルダー移動ソリューションです。Profile Management は、ファイル共有上のユーザーごとに VHDX ファイルを作成し、ユーザーの OneDrive フォルダーを VHDX ファイルに保存します。VHDX ファイルは、ユーザーがログオンすると接続され、ユーザーがログオフすると解除されます。

UWP アプリのローミング

UWP（ユニバーサル Windows プラットフォーム）アプリがユーザーと一緒にローミングできるようにします。その結果、ユーザーは異なるデバイスから同じ UWP アプリにアクセスできます。

このポリシーを有効にすると、Profile Management は、アプリを別の VHDX ディスクに保存することで、UWP アプリをユーザーと一緒にローミングできるようになります。これらのディスクは、ユーザーのログオン中に接続され、ユーザーのログオフ中は接続解除されます。

構成の優先順位:

この設定をここで構成しない場合、INI ファイルの値が使用されます。
この設定をここで構成しない、または INI ファイルからの設定がない場合、この機能は無効になります。

ログオン時にユーザーのグループポリシーの非同期処理を有効にする

Windows は、ユーザーグループポリシーに同期と非同期の 2 つの処理モードを提供します。Windows はレジストリ値を使用して、次のユーザーログオン時の処理モードを決定します。レジストリ値が存在しない場合は、同期モードが適用されます。レジストリ値はマシンレベルの設定であり、ユーザーと一緒に移動しません。したがって、ユーザーが次の場合、非同期モードは正常に適用されません:

- 別のマシンにログオンする。
- [ログオフ時にローカルでキャッシュしたプロファイルの削除] ポリシーが有効になっている同じマシンにログオンする。

このポリシーを有効にすると、レジストリ値はユーザーとともに移動します。その結果、ユーザーがログオンするたびに処理モードが適用されます。

VHD ディスクの圧縮をトリガーする空き領域率

[VHD ディスクの圧縮を有効にする] がオンになっている場合に適用されます。VHD ディスク圧縮のトリガーとなる空き領域の比率を指定できます。ユーザーのログオフ時に空き領域の比率が指定した値を超えると、ディスクの圧縮がトリガーされます。

空き容量の比率 =（現在の VHD ファイルサイズ–必要最小限の VHD ファイルサイズ *）÷ 現在の VHD ファイルサイズ

* Microsoft Windows オペレーティングシステムの`MSFT_Partition`クラスの GetSupportedSize メソッドを使用して取得します。

VHD ディスクの圧縮をトリガーするログオフの数

［VHD ディスクの圧縮を有効にする］ がオンになっている場合に適用されます。VHD ディスク圧縮のトリガーとなるユーザーログオフ数を指定できます。

最後の圧縮からのログオフ数が指定した値に達すると、ディスク圧縮が再度トリガーされます。

VHD ディスクの圧縮の最適化を無効にする

［VHD ディスクの圧縮を有効にする］ がオンになっている場合に適用されます。VHD ディスク圧縮のファイルのデフラグ（最適化）を無効にするかどうかを指定できます。

VHD ディスク圧縮がオンになっている場合、VHD ディスクファイルは、最初に Windows 組み込みの`defrag`ツールを使用して自動的に最適化され、そのあと圧縮されます。VHD ディスクの最適化により圧縮結果が向上しますが、オフにするとシステムリソースを節約できます。

プロファイルコンテナへのマルチセッションライトバックを有効にする

マルチセッションシナリオで、プロファイルコンテナへのライトバックを有効にします。有効にすると、すべてのセッションでの変更がプロファイルコンテナに書き戻されます。それ以外の場合、最初のセッションのみがプロファイルコンテナで読み取り/書き込みモードになっているため、最初のセッションの変更のみが保存されます。Citrix Profile Management プロファイルコンテナは、Citrix Profile Management 2103 以降でサポートされます。FSLogix プロファイルコンテナは、Citrix Profile Management 2003 以降でサポートされています。

FSLogix プロファイルコンテナにこのポリシーを使用するには、次の前提条件が満たされていることを確認してください:

- FSLogix プロファイルコンテナ機能がインストールされ、有効になっている。
- プロファイルの種類が、読み取り/書き込みプロファイルを試みてから、読み取り専用にフォールバックするように FSLogix で設定されている。

ユーザーストアの複製

ログオンやログオフのたびにリモートユーザープロファイルストアを複数のパスに複製できます。そうすることで、Profile Management はユーザーのログオンでプロファイルの冗長性を提供できます。

ポリシーを有効にすると、システムの入出力が増え、ログオフに時間がかかるようになります。

> 注:
>
> この機能は、ファイルベースとコンテナベースの両方のプロファイルソリューションで利用できます。

ユーザーストアへの資格情報ベースのアクセスを有効にする

デフォルトでは、Citrix Profile Management は現在のユーザーを偽装してユーザーストアにアクセスします。ユーザーストアにアクセスするときに Profile Management に現在のユーザーを偽装させたくない場合は、この機能を有効にします。現在のユーザーがアクセス権限を持たないストレージリポジトリ（Azure Files など）にユーザーストアを配置できます。

Profile Management がユーザーストアにアクセスできるようにするには、プロファイルストレージサーバーの資格情報を Workspace Environment Management（WEM）または Windows 資格情報マネージャーに保存します。Profile Management が実行されている各マシンに同じ資格情報を構成する必要がないように、Workspace Environment Management を使用することをお勧めします。Windows 資格情報マネージャーを使用する場合は、ローカルシステムアカウントを使用して資格情報を安全に保存します。

> 注:
>
> このポリシーは、ファイルベースと VHDX ベースの両方のユーザーストアで使用できます。2212 より前のバージョンの Profile Management では、このポリシーは VHDX ベースのユーザーストアでのみ使用できます。

この設定をここで構成しない場合、INI ファイルの値が使用されます。この設定をここで構成しない、または INI ファイルからの設定がない場合、デフォルトで無効になります。

VHDX ファイルのストレージパスのカスタマイズ

Profile Management は、次の VHDX ベースのポリシーを提供します：プロファイルコンテナ、Outlook の検索インデックスの移動、およびフォルダーのミラーリングの高速化。デフォルトでは、VHDX ファイルはユーザーストアに保存されます。このポリシーでは、個別のパスを指定して VHDX ファイルを保存できます。

VHD コンテナのデフォルト容量

VHD コンテナのデフォルトのストレージ容量（GB 単位）を指定できます。

構成の優先順位:

1. このポリシーをここで構成しない場合、INI ファイルの値が使用されます。
2. このポリシーをここでまたは INI ファイルで構成しない場合、デフォルトは 50（GB）です。

セッションで **VHDX** ディスクを自動的に再接続する

このポリシーを有効にすると、Profile Management により、VHDX ベースのポリシーの高レベルの安定性が確保されます。デフォルトでは、このポリシーは有効になっています。

このポリシーを有効にすると、Profile Management は VHDX ベースのポリシーで使用されている VHDX ディスクを監視します。いずれかのディスクの接続が解除されている場合、Profile Management はディスクを自動的に再接続します。

プロファイルコンテナの自動拡張しきい値

プロファイルコンテナが自動拡張をトリガーするストレージ容量の使用率を指定できます。

構成の優先順位:

- このポリシーをここで構成しない場合、INI ファイルの値が使用されます。
- このポリシーをここでまたは INI ファイルで構成しない場合、デフォルトはストレージ容量の 90（%）です。

プロファイルコンテナの自動拡張の増分

自動拡張がトリガーされたときにプロファイルコンテナが自動的に拡張するストレージ容量（GB 単位）を指定できます。

構成の優先順位:

- このポリシーをここで構成しない場合、INI ファイルの値が使用されます。
- このポリシーをここでまたは INI ファイルで構成しない場合、デフォルトは 10（GB）です。

プロファイルコンテナの自動拡張の制限

自動拡張がトリガーされたときにプロファイルコンテナが自動的に拡張できる最大ストレージ容量（GB 単位）を指定できます。

構成の優先順位:

- このポリシーをここで構成しない場合、INI ファイルの値が使用されます。
- このポリシーをここでまたは INI ファイルで構成しない場合、デフォルトは 80（GB）です。

ユーザーレベルのポリシー設定を有効にする

このポリシーを有効にすると、マシンレベルのポリシー設定がユーザー レベルで機能し、ユーザー レベルの設定がマシンレベルの設定を上書きします。

構成の優先順位:

1. このポリシーをここで構成しない場合、INI ファイルの値が使用されます。
2. このポリシーをここでも INI ファイル内でも構成しない場合、それは無効になります。

ユーザーグループの優先順位を設定する

ユーザーグループの優先順位を指定できます。この順序により、ユーザーが異なるポリシー設定を持つ複数のグループに属している場合に、どのグループが優先されるかが決まります。

ユーザーがポリシー設定が矛盾する複数のグループに属している場合は、次の点を考慮してください:

- ユーザーがこのポリシーで定義された 1 つまたは複数のグループに属している場合は、最も優先順位の高いグループが優先されます。
- ユーザーがこのポリシーで定義されているグループのいずれにも属していない場合は、SID のアルファベット順で最初に表示されているグループが優先されます。

ユーザーストアの選択方法

複数のユーザーストアが使用可能な場合、ユーザーストアの選択方法を指定できます。次のオプションがあります。

- 構成の順序。Profile Management は、最も早く構成されたストアを選択します。
- アクセスパフォーマンス。Profile Management は、最適なアクセスパフォーマンスを示すストアを選択します。

構成の優先順位:

1. この設定をここで構成しない場合、INI ファイルの値が使用されます。
2. この設定をここで、または.ini ファイルで構成しない場合、［構成の順序］が使用されます。

ユーザーストア間でのセッション内プロファイルコンテナのフェールオーバーを有効にする

デフォルトでは、複数のユーザーストアが展開されている場合、プロファイルコンテナのフェールオーバーはユーザーのログオン時にのみ発生します。その結果、プロファイルの冗長性はユーザーのログオン時にのみ利用可能になります。このポリシーを使用すると、フェールオーバーの範囲をセッション全体に拡張し、セッション全体でプロファイルの冗長性を確保できます。このポリシーを有効にすると、セッション中に Profile Management がアクティブなプロファイル コンテナへの接続を失った場合、自動的に別の利用可能なコンテナに切り替わります。

構成の優先順位:

1. このポリシーをここで構成しない場合、INI ファイルの値が使用されます。
2. このポリシーをここでも INI ファイル内でも構成しない場合、この設定は無効になります。

基本設定のポリシー設定

August 17, 2024

このセクションには、Profile Management の基本構成に関するポリシー設定が含まれています。

Profile Management の有効化

デフォルトでは、展開を促進するため、Profile Management はログオンまたはログオフを処理しません。必ずほかのすべてのセットアップタスクを実行し、環境内で Citrix ユーザープロファイルの実行をテストした後で、Profile Management を有効にします。

このポリシーをここで構成しない場合、INI ファイルの値が使用されます。このポリシーをここでまたは INI ファイルで構成しない場合、Profile Management はいかなる方法でも Windows ユーザープロファイルを処理しません。

処理済みグループ

コンピューターのローカルグループとドメイングループ（ローカル、グローバル、およびユニバーサル）の両方を使用できます。ドメイングループは、次の形式で指定する必要があります：ドメイン名\グループ名。

ここでポリシーを構成しない場合は、Profile Management はユーザーグループのメンバーのみを処理します。このポリシーが無効な場合は、Profile Management はすべてのユーザーを処理します。このポリシーをここで構成しない場合、INI ファイルの値が使用されます。このポリシーをここでまたは INI ファイルで構成しない場合、すべてのユーザーグループのメンバーが処理されます。

除外グループ

コンピューターのローカルグループとドメイングループ（ローカル、グローバル、およびユニバーサル）を使用して、特定のユーザープロファイルが処理されないようにすることができます。ドメイングループは、「ドメイン名\グループ名」形式で指定します。

ここでこの設定を構成する場合、これらのユーザーグループのメンバーが除外されます。この設定が無効な場合は、どのユーザーも除外されません。この設定をここで構成しない場合、INI ファイルの値が使用されます。この設定をここでまたは INI ファイルで構成しない場合、どのグループのメンバーも除外されません。

ローカル管理者のログオン処理

BUILTIN\Administrators グループのメンバーのログオンが処理されるかどうかを指定します。Citrix Virtual Apps 環境などのマルチセッションオペレーティングシステムで、このポリシーが無効になっているか、構成されて

いないと考えてください。この場合、Profile Management により、ドメインユーザーのログオンは処理されますが、ローカル管理者のログオンは処理されません。シングルセッション OS（Citrix Virtual Desktops 環境など）では、ローカル管理者のログオンも処理されます。このポリシーにより、ローカル管理者権限を持つドメインユーザー（通常、仮想デスクトップが割り当てられている Citrix Virtual Desktops ユーザー）は、以下を実行できます：

- 処理のバイパス
- ログオン
- Profile Management を使用したデスクトップで発生する問題のトラブルシューティング

注：ドメインユーザーのログオンは、一般的には製品ライセンスに確実に準拠するために、グループのメンバーシップによる制限を受けることがあります。
このポリシーが無効の場合、ローカル管理者によるログオンは Profile Management により処理されません。このポリシーをここで構成しない場合、INI ファイルの値が使用されます。このポリシーをここでまたは INI ファイルで構成しない場合、管理者は処理されません。

ユーザーストアへのパス

ユーザー設定（レジストリ変更および同期済みファイル）が保存されるディレクトリ（ユーザーストア）へのパスを設定します。

以下のパスを設定できます：

- 相対パス。（Active Directory のユーザーの #homeDirectory# 属性として通常構成される）ホームディレクトリに相対する必要があります。
- UNC パス。通常、サーバー共有または DFS 名前空間です。
- 無効または未構成。この場合、#homeDirectory#\Windows の値が使用されます。

次の種類の変数をこのポリシーに使用できます。

- パーセントで囲まれたシステム環境変数（%ProfVer% など）。システム環境変数には通常、追加のセットアップが必要です。
- ハッシュで囲まれた Active Directory ユーザーオブジェクトの属性（#sAMAccountName# など）。
- Profile Management の変数。詳しくは、製品ドキュメントサイトの「Profile Management variables」を参照してください。

ユーザー環境変数は、%username%および%userdomain%以外は、使用できません。またカスタム属性を作成し、場所またはユーザーなどで組織変数を完全に定義することができます。属性では大文字と小文字が区別されます。

例：

- 「\server\share\#sAMAccountName#」と指定した場合、UNC パス\server\share\JohnSmith にユーザー設定が格納されます（現在のユーザーの #sAMAccountName# 属性が JohnSmith である場合）。

- 「\server\profiles$%USERNAME%.%USERDOMAIN%!CTX_OSNAME!!CTX_OSBITNESS!」と指定した場合、「\server\profiles$\JohnSmith.DOMAINCONTROLLER1\Win8x64」に展開する可能性があります。

重要：属性や変数を使用する場合は、NTUSER.DAT があるフォルダーの 1 つ上のフォルダーを指定していることを確認してください。たとえば、このファイルが\server\profiles$\JohnSmith.Finance\Win8x64\UPM_Profile にある場合は、ユーザーストアのパスとして「\server\profiles$\JohnSmith.Finance\Win8x64」を指定します。UPM_Profile サブフォルダーを含める必要はありません。

ユーザーストアへのパスの指定での変数使用について詳しくは、次のトピックを参照してください：

- 複数のファイルサーバー上の Citrix ユーザープロファイルの共有
- 組織単位（OU）内および複数の OU 間でのプロファイルの管理
- Profile Management での高可用性と障害復旧

［ユーザーストアへのパス］が無効の場合は、ユーザー設定はホームディレクトリの Windows サブディレクトリに保存されます。

このポリシーが無効の場合は、ユーザー設定はホームディレクトリの Windows サブディレクトリに保存されます。このポリシーをここで構成しない場合、INI ファイルの値が使用されます。このポリシーをここでまたは INI ファイルで構成しない場合、ホームドライブの Windows ディレクトリが使用されます。

ユーザーストアを移行する

ユーザー設定（レジストリ変更および同期ファイル）が以前に保存されていたフォルダーへのパス（以前に使用したユーザーストアのパス）を指定します。

この設定を構成すると、以前のユーザーストアに保存されたユーザー設定は、［ユーザーストアへのパス］ポリシー設定により指定される現在のユーザーストアに移行されます。

パスは絶対 UNC パスまたはホームディレクトリへの相対パスにすることができます。

いずれの場合でも、次の種類の変数を使用できます：

- パーセント記号で囲まれたシステム環境変数。
- ハッシュ記号で囲まれた Active Directory ユーザーオブジェクトの属性。

例：

- フォルダーWindows\\%ProfileVer%は、ユーザーストアのWindows\W2K3という名称のサブフォルダーにユーザー設定を保存します（W2K3 に解決されるシステム環境変数が%ProfileVer% の場合）。
- \\server\share\\#SAMAccountName#は、UNC パス\\server\share\<JohnSmith>にユーザー設定を保存します（#SAMAccountName#が現在のユーザーの JohnSmith に解決される場合）。

パスには、%username%および%userdomain%以外のユーザー環境変数を使用できます。

この設定が無効な場合、ユーザー設定は現在のユーザーストアに保存されます。

この設定がここで構成されていない場合、INI ファイルの対応する設定が使用されます。

この設定がここまたは INI ファイルで構成されていない場合、ユーザー設定は現在のユーザーストアに保存されます。

アクティブライトバック

変更される（レジストリエントリ以外の）ファイルおよびフォルダーをセッション中にログオフする前にユーザーストアに同期できます。

このポリシーをここで構成しない場合、INI ファイルの値が使用されます。このポリシーをここでまたは INI ファイルで構成しない場合、有効になります。

オフライン プロファイル サポート

このポリシーにより、プロファイルをできるだけ早い段階でユーザーストアと同期できます。これは、ラップトップコンピューターやモバイルデバイスを使ってローミングを実行するユーザーに向けた機能です。ネットワークの切断が発生した場合、再起動や休止状態後もプロファイルはラップトップコンピューターまたはモバイルデバイス上にそのまま保持されます。モバイルユーザーが作業すると、それらのユーザーのプロファイルがローカルで更新されます。また、ネットワーク接続が再確立されると、最終的にユーザーストアと同期されます。

このポリシーをここで構成しない場合、INI ファイルの値が使用されます。このポリシーをここでまたは INI ファイルで構成しない場合、オフラインプロファイルは無効になります。

アクティブライトバックレジストリ

このポリシーを「アクティブライトバック」とともに使用します。変更されるレジストリエントリをセッション中にユーザーストアに同期できます。

この設定をここで構成しない場合、INI ファイルの値が使用されます。

この設定をここで、または INI ファイルで構成しない場合、アクティブライトバックレジストリは無効になります。

セッションのロックおよび切断時にアクティブライトバック

このポリシーと ［アクティブライトバック］ポリシーの両方を有効にすると、プロファイルのファイルとフォルダーは、セッションがロックまたは切断された場合にのみ書き戻し（ライトバック）されます。

このポリシーと、［アクティブライトバック］ポリシーおよび ［アクティブライトバックレジストリ］ポリシーの両方を有効にすると、レジストリエントリは、セッションがロックまたは切断された場合にのみ書き戻されます。

オフライン プロファイル サポート

オフラインプロファイル機能を有効にします。この機能は、一般的にネットワークから削除されるコンピューターを対象としています。たとえば、サーバーやデスクトップではなく、ラップトップやモバイルデバイスです。

この設定をここで構成しない場合、INI ファイルの値が使用されます。

この設定をここまたは INI ファイルで構成しない場合、オフラインプロファイルサポート機能は無効になります。

クロスプラットフォームのポリシー設定

August 17, 2024

このセクションには、**Profile Management** のクロスプラットフォーム機能を構成するためのポリシー設定が表示されます。

クロスプラットフォーム設定の有効化

展開を簡素化するため、デフォルトではクロスプラットフォーム設定は無効になっています。この機能の計画とテストが完了した後後にのみ、このポリシーを有効にしてクロスプラットフォーム設定を有効にします。

このポリシーをここで構成しない場合、INI ファイルの値が使用されます。このポリシーをここでまたは INI ファイルで構成しない場合、クロスプラットフォーム設定は適用されません。

クロスプラットフォーム設定ユーザーグループ

1 つ以上の Windows ユーザーグループを入力します。たとえば、このポリシーを使ってテストユーザーグループのプロファイルのみを処理するとします。このポリシーを構成すると、Profile Management のクロスプラットフォーム設定機能によりこれらのユーザーグループのメンバーのみが処理されます。このポリシーが無効な場合、［処理済みグループ］ポリシーで指定されたすべてのユーザーが処理されます。

このポリシーをここで構成しない場合、INI ファイルの値が使用されます。このポリシーをここまたは INI ファイルで構成しない場合、すべてのユーザーグループが処理されます。

クロスプラットフォーム定義へのパス

ダウンロードパッケージからコピーされた定義ファイルのネットワークの場所です。このパスは、UNC パスである必要があります。ユーザーにはこの場所への読み取りアクセス権限、管理者には書き込みアクセス権限が必要です。この場所は、サーバーメッセージブロック（SMB）または Common Internet File System（CIFS）ファイル共有である必要があります。

このポリシーをここで構成しない場合、INI ファイルの値が使用されます。このポリシーをここでまたは INI ファイルで構成しない場合、クロスプラットフォーム設定は適用されません。

クロスプラットフォーム設定ストアへのパス

クロスプラットフォーム設定ストアへのパスを設定します。このフォルダーには、ユーザーのクロスプラットフォーム設定が保存されています。ユーザーには、このフォルダーに対する書き込みアクセス権限が必要です。パスは絶対 UNC パスまたはホームディレクトリへの相対パスにすることができます。

この領域は、複数のプラットフォームにより共有されるプロファイルデータがあるユーザーストアの共有領域である必要があります。ユーザーには、このフォルダーに対する書き込みアクセス権限が必要です。パスは絶対 UNC パスまたはホームディレクトリへの相対パスにすることができます。［ユーザーストアへのパス］と同じ変数を使用できます。

このポリシーが無効な場合は、パスに Windows\PM_CP が使用されます。このポリシーをここで構成しない場合、INI ファイルの値が使用されます。このポリシーをここでまたは INI ファイルで構成しない場合、デフォルト値が使用されます。

クロスプラットフォーム設定を作成するためのソース

プラットフォームの OU でこのポリシーが有効な場合、基本プラットフォームとしてプラットフォームを指定します。このポリシーは、基本プラットフォームのプロファイルからクロスプラットフォーム設定ストアにデータを移行します。

各プラットフォームのプロファイルのセットは、個別の OU に格納されます。管理者はどのプラットフォームのプロファイルデータを使用してクロスプラットフォーム設定ストアをシードするかを決定する必要があります。このプラットフォームを基本プラットフォームと呼びます。クロスプラットフォーム設定ストアの定義ファイルにデータがない場合、または単一プラットフォームプロファイルのキャッシュデータがそのストアの定義データより新しい場合を考えてください。この場合、このポリシーを無効にしない限り、Profile Management はデータを単一プラットフォームプロファイルからストアに移行します。

> 重要:
>
> このポリシーを複数の OU やユーザー/マシンオブジェクトで有効にすると、最初のユーザーがログオンしたプラットフォームが基本プラットフォームになります。
> デフォルトでは、このポリシーは有効になっています。

ファイルシステムのポリシー設定

August 17, 2024

このセクションには、以下を設定するポリシーが含まれています:

- プロファイルがインストールされているシステムとユーザーストア間で、ユーザープロファイル内のどのファイルが同期されるか
- プロファイルがインストールされているシステムとユーザーストア間で、ユーザープロファイル内のどのディレクトリが同期されるか

除外のポリシー設定

August 17, 2024

このセクションでは、ユーザープロファイル内のファイルやディレクトリを同期処理から除外するためのポリシー設定について説明します。

除外の一覧 - ファイル

同期時に無視されるファイルの一覧。ファイル名は、ユーザープロファイル（%USERPROFILE%）に対する相対パスで指定する必要があります。ワイルドカードはファイル名とフォルダー名でサポートされていますが、再帰的に適用されるのはファイル名のワイルドカードのみです。

例:

- `Desktop\Desktop.ini`は、`Desktop`フォルダー内の`Desktop.ini`ファイルを無視します。
- `%USERPROFILE%\*.tmp`は、プロファイル全体で`.tmp`拡張子を持つすべてのファイルを無視します。
- `AppData\Roaming\MyApp\*.tmp`は、プロファイルの一部で`.tmp`拡張子を持つすべてのファイルを無視します。
- `Downloads\*\a.txt`は、`Downloads`フォルダーのすぐ下にあるサブフォルダーの`a.txt`を無視します。

このポリシーが無効の場合、ファイルは除外されません。このポリシーをここで構成しない場合、INI ファイルの値が使用されます。このポリシーをここでまたは INI ファイルで構成しない場合、ファイルは除外されません。

デフォルトの除外一覧の有効化 - ディレクトリ

同期時に無視されるディレクトリのデフォルトの一覧。このポリシーは、手動で記入しないで GPO 除外ディレクトリを指定するために使用します。

このポリシーを無効にすると、デフォルトで Profile Management は、いかなるディレクトリも除外しません。

このポリシーをここで構成しない場合、Profile Management は INI ファイルの値を使用します。このポリシーを、ここでも INI ファイルでも構成しない場合、デフォルトで Profile Management は、いかなるディレクトリも除外しません。

除外の一覧 - ディレクトリ

同期時に無視されるフォルダーの一覧。フォルダー名は、ユーザープロファイル（%USERPROFILE%）に対する相対パスで指定する必要があります。フォルダー名のワイルドカードはサポートされていますが、再帰的に適用されることはありません。

例:

- `Desktop`は、ユーザープロファイルの`Desktop`フォルダーを無視します。

このポリシーが無効の場合、フォルダーは除外されません。このポリシーをここで構成しない場合、INI ファイルの値が使用されます。このポリシーをここでまたは INI ファイルで構成しない場合、フォルダーは除外されません。

ログオン時の除外チェック

この設定は、ユーザーストアのプロファイルに除外されたファイルまたはフォルダーが含まれる場合に Profile Management がこれをどのように処理するかを構成します。可能なポリシー設定と、それに対応する操作を次の表に示します:

ポリシー設定	アクション
設定が無効になっているか、［ログオン時に除外されたファイルまたはフォルダーを同期］の値がデフォルトに設定されている	Profile Management は、ユーザーのログオン時に、ユーザーストアから除外されたファイルまたはフォルダーをローカルプロファイルと同期します。
設定が［ログオン時に除外されたファイルまたはフォルダーを無視］に設定されている	Profile Management は、ユーザーのログオン時に、ユーザーストアの除外されたファイルまたはフォルダーを無視します。
設定が［ログオン時に除外されたファイルまたはフォルダーを削除］に設定されている	Profile Management は、ユーザーのログオン時に、ユーザーストアの除外されたファイルまたはフォルダーを削除します。
設定が Web Studio で構成されていない	.ini ファイルの値が使用されます。
設定が Web Studio または.ini ファイルで構成されていない	ユーザーのログオン時に、ユーザーストアから除外されたファイルまたはフォルダーがローカルプロファイルと同期されます。

大きなファイルの処理 - シンボリック リンクとして作成されるファイル

より快適にログオンできるようにしたり大きなサイズのファイルを処理したりするために、Profile Management はこの一覧のファイルをコピーするのではなくシンボリックリンクを作成します。

ファイルを参照するポリシーではワイルドカードを使用できます。たとえば`!ctx_localappdata!\Microsoft\Outlook\*.OST`などです。

Microsoft Outlook でオフラインフォルダーファイル（*.ost）を処理するために、**Outlook** フォルダーが Profile Management から除外されていないことを確認してください。

これらのファイルは、複数のセッションで同時にアクセスできないことに注意してください。

同期のポリシー設定

August 17, 2024

「同期」セクションでは、プロファイルがインストールされているシステムとユーザーストアとの間で同期する、ユーザープロファイル内のファイルやフォルダーの指定に関するポリシー設定について説明しています。

同期するディレクトリ

デフォルトでは、Profile Management は、プロファイルがインストールされたシステムとユーザーストアとの間でユーザープロファイルを同期します。同期からフォルダーを除外する場合、このポリシーを使用すると、除外したフォルダーのサブフォルダーを同期に戻すことができます。

この一覧にパスを追加するときは、ユーザープロファイルからの相対パスを入力します。フォルダー名のワイルドカードはサポートされていますが、再帰的に適用されることはありません。

このポリシーをここで構成しない場合、INI ファイルの値が使用されます。このポリシーをここでまたは INI ファイルで構成しない場合、ユーザープロファイル内の非除外フォルダーのみが同期されます。

同期するファイル

デフォルトでは、Profile Management は、プロファイルがインストールされたシステムとユーザーストアとの間でユーザープロファイルを同期します。同期からフォルダーを除外する場合、このポリシーを使用すると、除外したフォルダーの中のファイルを同期に戻すことができます。

この一覧にパスを追加するときは、ユーザープロファイルからの相対パスを入力します。ワイルドカードはファイル名とフォルダー名でサポートされていますが、再帰的に適用されるのはファイル名のワイルドカードのみです。ワイルドカードはネストできません。

例:

- `AppData\Local\Microsoft\Office\Access.qat`は、デフォルト構成で除外されるフォルダーのファイルを指定します。
- `AppData\Local\MyApp\*.cfg`は、プロファイルフォルダー`AppData\Local\MyApp`およびそのサブフォルダー内の`.cfg`拡張子を持つすべてのファイルを指定します。

このポリシーを無効にすると、これを有効にして空の一覧を構成するのと同じ結果になります。

このポリシーをここで構成しない場合、INI ファイルの値が使用されます。このポリシーをここでまたは INI ファイルで構成しない場合、ユーザープロファイル内の非除外ファイルのみが同期されます。

ミラーリングするフォルダー

このポリシーにより、（参照フォルダーとしても知られる）任意のトランザクションフォルダーに関連する問題を解決できます。このフォルダーには、あるファイルがほかのファイルを参照する相互依存ファイルが含まれています。

フォルダーのミラーリングにより、Profile Management がトランザクションフォルダーおよびその内容を単一エンティティとして処理するため、プロファイルの膨張を防ぐことができます。たとえば、**Internet Explorer** の **Cookie** フォルダーをミラーリングして、Index.dat がインデックス対象の Cookie と同期されるように設定できます。このような状況では、最後の書き込みが優先されます。そのため、ミラーリングされたフォルダー内のファイルが複数のセッションで変更された場合、最後の更新によりそのファイルが上書きされ、プロファイルの変更が失われます。

たとえば、以下の表では、ユーザーがインターネットをブラウズする間に Index.dat がどのように Cookie を参照するかを示しています：

シナリオ	Index.dat が Cookie を参照する方法
–	–
1 人のユーザーが 2 つの Internet Explorer セッションを持ち、各セッションが異なるサーバー上にあり、各セッションで異なるサイトにアクセスします。	各サイトからの Cookie が適切なサーバーに追加されます。
ユーザーが、最初のセッションから、またはセッションの途中で、ログオフします（アクティブライトバック機能が構成されている場合）。	2 番目のセッションの Cookie が、最初のセッションの Cookie に置き換わる必要があります。
最初と 2 番目のセッションがマージされ、Index.dat の Cookie への参照が古くなります。	新しいセッションでさらに閲覧すると、マージが繰り返され、Cookie フォルダーが肥大化します。

Cookie フォルダーをミラーリングすると、この問題を解決できます。この場合、ユーザーがログオフするたびに、Cookie は最後のセッションの Cookie で上書きされます。そのため、Index.dat が最新の状態で維持されます。

このポリシーをここで構成しない場合、INI ファイルの値が使用されます。このポリシーをここでまたは INI ファイルで構成しない場合、フォルダーはミラー化されません。

フォルダーのミラーリングを高速化

このポリシーとミラーリングするフォルダーポリシーの両方が有効になっている場合、**Profile Management** はミラーリングされたフォルダーを VHDX ベースの仮想ディスクに保存します。ログオン時に仮想ディスクを接続し、ログオフ時に接続解除します。このポリシーを有効にすると、ユーザーストアとローカルプロファイルの間でフォルダーをコピーする必要がなくなり、フォルダーのミラーリングが高速化されます。

フォルダーリダイレクトのポリシー設定

August 17, 2024

このセクションには、プロファイル内の一般的なフォルダーを共有のネットワークの場所にリダイレクトするためのポリシー設定が含まれています。

管理者アクセスを許可

この設定項目では、リダイレクトされたユーザーのフォルダーに管理者がアクセスすることを有効または無効にします。

> 注:
>
> この設定により、ドメインに完全かつ無制限にアクセスできる管理者に権限が付与されます。

この設定はデフォルトで無効になっており、リダイレクトされたフォルダーの内容に対してユーザーの排他アクセスが付与されています。

ドメイン名を包含

この設定では、UNC パスに環境変数%`userdomain`%を含めることを有効にします。この UNC パスは、リダイレクトされるフォルダーに指定されます。

デフォルトでは、この設定は無効になっています。また、リダイレクトされるフォルダーの UNC パスに環境変数%`userdomain`%は含まれません。

AppData（**Roaming**）のポリシー設定

August 17, 2024

このセクションには、**AppData**（**Roaming**）フォルダーの内容を共有のネットワークの場所にリダイレクトするためのポリシー設定が含まれています。

AppData（**Roaming**）パス

この設定では、**AppData**（**Roaming**）フォルダーのリダイレクト先のネットワークの場所を指定します。

この設定はデフォルトで無効になっており、リダイレクト先は指定されていません。

この設定項目が未構成の場合、このフォルダーは Profile Management によりリダイレクトされません。

AppData(Roaming) のリダイレクト設定

この設定では、**AppData(Roaming)** フォルダーの内容のリダイレクト方法を指定します。

デフォルトでは、UNC パスにリダイレクトされます。詳しくは、「ユーザーストアへのパス」セクションを参照してください。

この設定項目が未構成の場合、このフォルダーは Profile Management によりリダイレクトされません。

アドレス帳のポリシー設定

August 17, 2024

このセクションには、**Contacts** フォルダーの内容を共有のネットワークの場所にリダイレクトするためのポリシー設定が含まれています。

アドレス帳パス

この設定では、**Contacts** フォルダーのリダイレクト先のネットワークの場所を指定します。

この設定はデフォルトで無効になっており、リダイレクト先は指定されていません。

この設定項目が未構成の場合、このフォルダーは Profile Management によりリダイレクトされません。

アドレス帳のリダイレクト設定

この設定では、**Contacts** フォルダーの内容のリダイレクト方法を指定します。

デフォルトでは、UNC パスにリダイレクトされます。

この設定項目が未構成の場合、このフォルダーは Profile Management によりリダイレクトされません。

デスクトップのポリシー設定

August 17, 2024

このセクションには、`Desktop`フォルダーの内容を共有のネットワークの場所にリダイレクトするためのポリシー設定が含まれています。

デスクトップパス

この設定では、**Desktop** フォルダーのリダイレクト先のネットワークの場所を指定します。

この設定はデフォルトで無効になっており、リダイレクト先は指定されていません。

この設定項目が未構成の場合、このフォルダーは Profile Management によりリダイレクトされません。

デスクトップのリダイレクト設定

この設定では、**Desktop** フォルダーの内容のリダイレクト方法を指定します。

デフォルトでは、UNC パスにリダイレクトされます。

この設定項目が未構成の場合、このフォルダーは Profile Management によりリダイレクトされません。

ドキュメントのポリシー設定

August 17, 2024

このセクションには、**Documents** フォルダーの内容を共有のネットワークの場所にリダイレクトするためのポリシー設定が含まれています。

ドキュメントパス

この設定では、**Documents** フォルダーのリダイレクト先のネットワークの場所を指定します。

この設定はデフォルトで無効になっており、リダイレクト先は指定されていません。

この設定項目が未構成の場合、このフォルダーは Profile Management によりリダイレクトされません。

ファイルを **Documents** フォルダーにリダイレクトするだけではなく、**Music**、**Pictures**、**Videos** フォルダーにもリダイレクトするため、［ドキュメントパス］設定を有効にする必要があります。

ドキュメントのリダイレクト設定

この設定では、**Documents** フォルダーの内容のリダイレクト方法を指定します。

デフォルトでは、UNC パスにリダイレクトされます。

Documents フォルダーの内容のリダイレクト方法として、以下のいずれかのオプションを選択します：

- 次の UNC パスにリダイレクト：［ドキュメントパス］ポリシー設定で指定された UNC パスにリダイレクトします。

- ユーザーのホームディレクトリにリダイレクト：ユーザーのホームディレクトリ（通常 Active Directory でユーザーの #homeDirectory# 属性として構成される）にリダイレクトします。

この設定項目が未構成の場合、このフォルダーは Profile Management によりリダイレクトされません。

ダウンロードのポリシー設定

August 17, 2024

このセクションには、**Downloads** フォルダーの内容を共有のネットワークの場所にリダイレクトするためのポリシー設定が含まれています。

ダウンロードパス

この設定では、**Downloads** フォルダーのリダイレクト先のネットワークの場所を指定します。

この設定はデフォルトで無効になっており、リダイレクト先は指定されていません。

この設定項目が未構成の場合、このフォルダーは Profile Management によりリダイレクトされません。

ダウンロードのリダイレクト設定

この設定では、**Downloads** フォルダーの内容のリダイレクト方法を指定します。

デフォルトでは、UNC パスにリダイレクトされます。

この設定項目が未構成の場合、このフォルダーは Profile Management によりリダイレクトされません。

お気に入りのポリシー設定

August 17, 2024

このセクションには、**Favorites** フォルダーの内容を共有のネットワークの場所にリダイレクトするためのポリシー設定が含まれています。

お気に入りパス

この設定では、**Favorites** フォルダーのリダイレクト先のネットワークの場所を指定します。

この設定はデフォルトで無効になっており、リダイレクト先は指定されていません。

この設定項目が未構成の場合、このフォルダーは Profile Management によりリダイレクトされません。

お気に入りのリダイレクト設定

この設定では、**Favorites** フォルダーの内容のリダイレクト方法を指定します。

デフォルトでは、UNC パスにリダイレクトされます。

この設定項目が未構成の場合、このフォルダーは Profile Management によりリダイレクトされません。

リンクのポリシー設定

August 17, 2024

このセクションには、**Links** フォルダーの内容を共有のネットワークの場所にリダイレクトするためのポリシー設定が含まれています。

リンクパス

この設定では、**Links** フォルダーのリダイレクト先のネットワークの場所を指定します。

この設定はデフォルトで無効になっており、リダイレクト先は指定されていません。

この設定項目が未構成の場合、このフォルダーは Profile Management によりリダイレクトされません。

リンクのリダイレクト設定

この設定では、**Links** フォルダーの内容のリダイレクト方法を指定します。

デフォルトでは、UNC パスにリダイレクトされます。

この設定項目が未構成の場合、このフォルダーは Profile Management によりリダイレクトされません。

ミュージックのポリシー設定

August 17, 2024

このセクションには、**Music** フォルダーの内容を共有のネットワークの場所にリダイレクトするためのポリシー設定が含まれています。

ミュージックパス

この設定では、**Music** フォルダーのリダイレクト先のネットワークの場所を指定します。

この設定はデフォルトで無効になっており、リダイレクト先は指定されていません。

この設定項目が未構成の場合、このフォルダーは Profile Management によりリダイレクトされません。

ミュージックのリダイレクト設定

この設定では、**Music** フォルダーの内容のリダイレクト方法を指定します。

デフォルトでは、UNC パスにリダイレクトされます。

Music フォルダーの内容のリダイレクト方法として、以下のいずれかのオプションを選択します:

- 次の UNC パスにリダイレクト:［ミュージックパス］設定で指定された UNC パスにリダイレクトします。
- Documents フォルダーに相対的リダイレクト: Documents フォルダーのリダイレクト先と相対的に同じ場所にあるフォルダーにリダイレクトします。

コンテンツを **Documents** フォルダーに相対するフォルダーにリダイレクトするには、［ドキュメントパス］設定を有効にする必要があります。

この設定項目が未構成の場合、このフォルダーは Profile Management によりリダイレクトされません。

ピクチャのポリシー設定

August 17, 2024

このセクションには、**Pictures** フォルダーの内容を共有のネットワークの場所にリダイレクトするためのポリシー設定が含まれています。

ピクチャパス

この設定では、**Pictures** フォルダーのリダイレクト先のネットワークの場所を指定します。

この設定はデフォルトで無効になっており、リダイレクト先は指定されていません。

この設定項目が未構成の場合、このフォルダーは Profile Management によりリダイレクトされません。

ピクチャのリダイレクト設定

この設定では、**Pictures** フォルダーの内容のリダイレクト方法を指定します。

デフォルトでは、UNC パスにリダイレクトされます。

Pictures フォルダーの内容のリダイレクト方法として、以下のいずれかのオプションを選択します:

- 次の UNC パスにリダイレクト:［ピクチャパス］設定で指定された UNC パスにリダイレクトします。
- Documents フォルダーに相対的リダイレクト: Documents フォルダーのリダイレクト先と相対的に同じ場所にあるフォルダーにリダイレクトします。

コンテンツを **Documents** フォルダーに相対するフォルダーにリダイレクトするには、［ドキュメントパス］設定を有効にする必要があります。

この設定項目が未構成の場合、このフォルダーは Profile Management によりリダイレクトされません。

保存したゲームのポリシー設定

August 17, 2024

このセクションには、**Saved Games** フォルダーの内容を共有のネットワークの場所にリダイレクトするためのポリシー設定が含まれています。

保存したゲームのリダイレクト設定

この設定では、**Saved Games** フォルダーの内容のリダイレクト方法を指定します。

デフォルトでは、UNC パスにリダイレクトされます。

この設定項目が未構成の場合、このフォルダーは Profile Management によりリダイレクトされません。

保存したゲームパス

この設定では、**Saved Games** フォルダーのリダイレクト先のネットワークの場所を指定します。

この設定はデフォルトで無効になっており、リダイレクト先は指定されていません。

この設定項目が未構成の場合、このフォルダーは Profile Management によりリダイレクトされません。

スタートメニューのポリシー設定

August 17, 2024

このセクションには、**Start Menu** フォルダーの内容を共有のネットワークの場所にリダイレクトするためのポリシー設定が含まれています。

スタートメニューのリダイレクト設定

この設定では、**Start Menu** フォルダーの内容のリダイレクト方法を指定します。

デフォルトでは、UNC パスにリダイレクトされます。

この設定項目が未構成の場合、このフォルダーは Profile Management によりリダイレクトされません。

スタートメニューパス

この設定では、**Start Menu** フォルダーのリダイレクト先のネットワークの場所を指定します。

この設定はデフォルトで無効になっており、リダイレクト先は指定されていません。

この設定項目が未構成の場合、このフォルダーは Profile Management によりリダイレクトされません。

検索のポリシー設定

August 17, 2024

このセクションには、**Searches** フォルダーの内容を共有のネットワークの場所にリダイレクトするためのポリシー設定が含まれています。

検索のリダイレクト設定

この設定では、**Searches** フォルダーの内容のリダイレクト方法を指定します。

デフォルトでは、UNC パスにリダイレクトされます。

この設定項目が未構成の場合、このフォルダーは Profile Management によりリダイレクトされません。

検索パス

この設定では、**Searches** フォルダーのリダイレクト先のネットワークの場所を指定します。

この設定はデフォルトで無効になっており、リダイレクト先は指定されていません。

この設定項目が未構成の場合、このフォルダーは Profile Management によりリダイレクトされません。

ビデオのポリシー設定

August 17, 2024

このセクションには、**Video** フォルダーの内容を共有のネットワークの場所にリダイレクトするためのポリシー設定が含まれています。

ビデオのリダイレクト設定

この設定では、**Video** フォルダーの内容のリダイレクト方法を指定します。

デフォルトでは、UNC パスにリダイレクトされます。

Video フォルダーのリダイレクト方法として、以下のいずれかのオプションを選択します:

- 次の UNC パスにリダイレクト:［ビデオパス］ポリシー設定で指定された UNC パスにリダイレクトします。
- Documents フォルダーに相対的リダイレクト: Documents フォルダーのリダイレクト先と相対的に同じ場所にあるフォルダーにリダイレクトします。

コンテンツを **Documents** フォルダーに相対するフォルダーにリダイレクトするには、［ドキュメントパス］設定を有効にする必要があります。

この設定項目が未構成の場合、このフォルダーは Profile Management によりリダイレクトされません。

ビデオパス

この設定では、**Video** フォルダーのリダイレクト先のネットワークの場所を指定します。

この設定はデフォルトで無効になっており、リダイレクト先は指定されていません。

この設定項目が未構成の場合、このフォルダーは Profile Management によりリダイレクトされません。

ログのポリシー設定

August 17, 2024

このセクションには、Profile Management のログ機能の構成に関するポリシー設定が含まれています。

Active Directory 操作

この設定では、Active Directory で実行された操作についての詳細なログ機能を有効または無効にします。

デフォルトでは、この設定は無効になっています。

この設定を有効にするときは、［ログの有効化］設定で［有効］が選択されていることを確認してください。

この設定を Web Studio で構成しない場合、INI ファイルの値が使用されます。

この設定が Web Studio または INI ファイルで構成されていない場合、以下がログに記録されます:

- エラー
- 全般的な情報

一般的な情報

この設定では、一般的な情報についての詳細なログ機能を有効または無効にします。

デフォルトでは、この設定は無効になっています。

この設定を有効にするときは、［ログの有効化］設定で［有効］が選択されていることを確認してください。

この設定をここで構成しない場合、INI ファイルの値が使用されます。

この設定が Web Studio または INI ファイルで構成されていない場合、以下がログに記録されます:

- エラー
- 全般的な情報

一般的な警告

この設定では、一般的な警告についての詳細なログ機能を有効または無効にします。

デフォルトでは、この設定は無効になっています。

この設定を有効にするときは、［ログの有効化］設定で［有効］が選択されていることを確認してください。

この設定をここで構成しない場合、INI ファイルの値が使用されます。

この設定が Web Studio または INI ファイルで構成されていない場合、以下がログに記録されます:

- エラー
- 全般的な情報

ログの有効化

この設定では、Profile Management のデバッグモード（詳細ログモード）のログ機能を有効または無効にします。デバッグモードでは、詳細な状態情報が%SystemRoot%\System32\Logfiles\UserProfileManager フォルダーのログファイルに記録されます。

この設定はデフォルトで無効になっており、エラーのみがログに記録されます。

この設定は、Profile Management のトラブルシューティング時にのみ有効にすることをお勧めします。

この設定をここで構成しない場合、INI ファイルの値が使用されます。

この設定をここまたは INI ファイルで構成しない場合、エラーのみが記録されます。

ファイルシステム操作

この設定項目では、ファイルシステムで実行された操作についての詳細なログ機能を有効または無効にします。

デフォルトでは、この設定は無効になっています。

この設定を有効にするときは、［ログの有効化］設定で［有効］が選択されていることを確認してください。

この設定をここで構成しない場合、INI ファイルの値が使用されます。

この設定が Web Studio または INI ファイルで構成されていない場合、以下がログに記録されます：

- エラー
- 全般的な情報

ファイルシステム通知

この設定では、ファイルシステムで発生した通知についての詳細なログ機能を有効または無効にします。

デフォルトでは、この設定は無効になっています。

この設定を有効にするときは、［ログの有効化］設定で［有効］が選択されていることを確認してください。

この設定をここで構成しない場合、INI ファイルの値が使用されます。

この設定が Web Studio または INI ファイルで構成されていない場合、以下がログに記録されます：

- エラー
- 全般的な情報

ログオフ

この設定では、ユーザーのログオフについての詳細なログ機能を有効または無効にします。

デフォルトでは、この設定は無効になっています。

この設定を有効にするときは、［ログの有効化］設定で［有効］が選択されていることを確認してください。

この設定をここで構成しない場合、INI ファイルの値が使用されます。

この設定が Web Studio または INI ファイルで構成されていない場合、以下がログに記録されます:

- エラー
- 全般的な情報

ログオン

この設定では、ユーザーのログオンについての詳細なログ機能を有効または無効にします。

デフォルトでは、この設定は無効になっています。

この設定を有効にするときは、［ログの有効化］設定で［有効］が選択されていることを確認してください。

この設定をここで構成しない場合、INI ファイルの値が使用されます。

この設定が Web Studio または INI ファイルで構成されていない場合、以下がログに記録されます:

- エラー
- 全般的な情報

ログファイルの最大サイズ

この設定では、Profile Management で生成されるログファイルの最大サイズをバイト単位で指定します。

デフォルトでは、この値は「1048576」バイト（1MB）に設定されています。

ディスクに十分な空き領域がある場合は、5MB 以上を指定することをお勧めします。ログファイルが最大サイズを超えた場合:

- ファイル（.bak）の既存のバックアップが削除されます
- ログファイルの名前が.bak に変更されます
- 新しいログファイルが作成されます

ログファイルは、%SystemRoot%\System32\Logfiles\UserProfileManager フォルダーに生成されます。

この設定をここで構成しない場合、INI ファイルの値が使用されます。

この設定および INI ファイルをここで構成しない場合、デフォルト値が使用されます。

ログファイルへのパス

この設定項目では、Profile Management のログファイルの保存フォルダーを指定します。

この設定項目はデフォルトで無効になっており、デフォルトのフォルダー(%SystemRoot%\System32\Logfiles\UserProfileMa
にログファイルが生成されます。

保存フォルダーのパスとして、ローカルドライブ、リモートドライブ、またはネットワークドライブ（UNC パス）を指定できます。リモートパスは、大規模な分散環境では役立ちますが、大量のネットワークトラフィックが発生し、ログファイルに対して適切でなくなる可能性があります。プロビジョニングした仮想マシンに永続的なハードドライブがある場合は、そのドライブ上のローカルパスを指定します。この設定では、仮想マシンを再起動してもログファイルが保持されます。固定ハードドライブがない仮想マシンの場合、UNC パスを指定するとログファイルを保持できます。ただし、この仮想マシンのシステムアカウントにはその UNC 共有に対する書き込みアクセス権が必要です。オフラインプロファイル機能で管理するラップトップコンピューターの場合は、ローカルパスを使用します。

ログファイルを UNC パス上のフォルダーに保存する場合は、そのフォルダーに適切なアクセス制御リストを適用することを Citrix ではお勧めします。この設定により、許可されたユーザーまたはコンピューターアカウントだけが、格納されたファイルにアクセスできるようになります。

この設定をここで構成しない場合、INI ファイルの値が使用されます。

この設定をここまたは INI ファイルで構成しない場合、デフォルトの場所である%SystemRoot%\System32\Logfiles\UserProfi
が使用されます。

個人用ユーザー情報

この設定では、個人用ユーザー情報についての詳細なログ機能を有効または無効にします。

デフォルトでは、この設定は無効になっています。

この設定を有効にするときは、［ログの有効化］設定で［有効］が選択されていることを確認してください。

この設定をここで構成しない場合、INI ファイルの値が使用されます。

この設定が Web Studio または INI ファイルで構成されていない場合、以下がログに記録されます：

- エラー
- 全般的な情報

ログオンおよびログオフ時のポリシー値

この設定では、ユーザーのログオン時およびログオフ時のポリシー設定値についての詳細なログ機能を有効または無効にします。

デフォルトでは、この設定は無効になっています。

この設定を有効にするときは、［ログの有効化］設定で［有効］が選択されていることを確認してください。

この設定をここで構成しない場合、INI ファイルの値が使用されます。

この設定が Web Studio または INI ファイルで構成されていない場合、以下がログに記録されます:

- エラー
- 全般的な情報

レジストリ操作

この設定では、レジストリで実行された操作についての詳細なログ機能を有効または無効にします。

デフォルトでは、この設定は無効になっています。

この設定を有効にするときは、［ログの有効化］設定で［有効］が選択されていることを確認してください。

この設定をここで構成しない場合、INI ファイルの値が使用されます。

この設定が Web Studio または INI ファイルで構成されていない場合、以下がログに記録されます:

- エラー
- 全般的な情報

ログオフ時のレジストリ差分

この設定では、ユーザーのログオフ時のレジストリ設定の相違についての詳細なログ機能を有効または無効にします。

デフォルトでは、この設定は無効になっています。

この設定を有効にするときは、［ログの有効化］設定で［有効］が選択されていることを確認してください。

この設定をここで構成しない場合、INI ファイルの値が使用されます。

この設定が Web Studio または INI ファイルで構成されていない場合、以下がログに記録されます:

- エラー
- 全般的な情報

プロファイル制御のポリシー設定

August 17, 2024

このセクションには、Profile Management でのユーザープロファイルの管理方法を指定するポリシー設定が含まれています。

キャッシュしたプロファイルを削除する前の待ち時間

この設定では、ローカルにキャッシュされたプロファイルをそのユーザーのログオフ後に Profile Management が削除するまでの待機時間を指定します。

0 を指定すると、ログオフ処理が完了した後でプロファイルが直ちに削除されます。Profile Management では、1 分ごとにログオフの状態がチェックされます。結果として、値が 60 なら、ユーザーのログオフ後 1〜2 分の間にプロファイルが削除されます。この動作は、最後のチェックがいつ行われたかによって異なります。ログオフ時にファイルやレジストリハイブにアクセスするプロセスがある場合は、ここで待機時間を延長できます。また、プロファイルのサイズが大きい場合、待機時間を延長することでこのプロセスが短縮されることがあります。

デフォルトでは値は 0 に指定されており、ローカルにキャッシュされたプロファイルがログオフ後に直ちに削除されます。

この設定を有効にするときは、［ログオフ時にローカルでキャッシュしたプロファイルの削除］設定で［有効］が選択されていることを確認してください。

この設定をここで構成しない場合、INI ファイルの値が使用されます。

この設定をここまたは INI ファイルで構成しない場合、プロファイルは直ちに削除されます。

ログオフ時にローカルでキャッシュしたプロファイルの削除

この設定では、ユーザーのログオフ後にローカルにキャッシュされたプロファイルを削除するかどうかを指定します。

この設定を有効にすると、ユーザーのローカルプロファイルキャッシュがログオフ後に削除されます。ターミナルサーバーではこの設定を有効にすることをお勧めします。

この設定はデフォルトで無効になっており、ローカルプロファイルはユーザーのログオフ後も保持されます。

この設定をここで構成しない場合、INI ファイルの値が使用されます。

この設定をここまたは INI ファイルで構成しない場合、キャッシュされたプロファイルは削除されません。

ローカルプロファイル競合の制御

この設定は、ユーザープロファイルが以下の両方に存在する場合の Profile Management の動作を構成します:

- ユーザーストア
- ローカルの Windows ユーザープロファイル（Citrix ユーザープロファイルではありません）

デフォルトでは、Profile Management はローカルの Windows プロファイルを使用しますが、そのプロファイルを変更することはありません。

Profile Management の動作を制御するには、次のいずれかのオプションを選択します。

- [ローカルプロファイルを使用]。Profile Management はローカルのプロファイルを使用し、そのプロファイルを変更することはありません。
- [ローカルプロファイルを削除]。Profile Management は、ローカルの Windows ユーザープロファイルを削除して、ユーザーストアから Citrix ユーザープロファイルをインポートします。
- [ローカルプロファイル名を変更]。Profile Management は、ローカルの Windows ユーザープロファイルの名前を変更してバックアップ用に保持し、ユーザーストアから Citrix ユーザープロファイルをインポートします。

この設定をここで構成しない場合、INI ファイルの値が使用されます。

この設定をここまたは INI ファイルで構成しない場合、既存のローカルプロファイルが使用されます。

既存のプロファイルの移行

この設定では、ログオンしたユーザーのプロファイルがユーザーストアに存在しない場合に、どのプロファイルをユーザーストアに移行するかを指定します。

Profile Management では、ユーザーストアにプロファイルが存在しないユーザーがログオンしたときに、既存のプロファイルが自動的にユーザーストアに移行されます。その後、ユーザーストアプロファイルは、Profile Management によって、以下の両方で使用されます:

- 現在のセッション
- 同じユーザーストアへのパスで構成された他のセッション

デフォルトでは、ローカルプロファイルおよび移動プロファイルがログオン時にユーザーストアに移行されます。

ログオン時にユーザーストアに移行されるプロファイルの種類を指定するには、以下のいずれかのオプションを選択します:

- ローカルおよび移動
- ローカル
- ローミング
- なし（無効）

[なし] を選択すると、通常の Windows の動作（つまり Profile Management がインストールされていない場合の動作）に基づいて、プロファイルが作成されます。

この設定をここで構成しない場合、INI ファイルの値が使用されます。

この設定をここまたは INI ファイルで構成しない場合、既存のローカルおよび移動プロファイルが移行されます。

既存のアプリケーションプロファイルの自動移行

この設定は、異なるオペレーティングシステム間での既存のアプリケーションプロファイルの自動移行を有効または無効にします。アプリケーションプロファイルには、`AppData`フォルダー内のアプリケーションデータ

とHKEY_CURRENT_USER\SOFTWAREのレジストリエントリの両方が含まれます。この設定は、アプリケーションプロファイルを異なるオペレーティングシステム間で移行する場合に役立ちます。

たとえば、オペレーティングシステム（OS）を Windows 10 バージョン 1803 から Windows 10 バージョン 1809 にアップグレードするとします。この設定を有効にすると、Profile Management は、各ユーザーの初回ログオン時に、既存のアプリケーション設定を Windows 10 バージョン 1809 に自動的に移行します。その結果、AppDataフォルダー内のアプリケーションデータと HKEY_CURRENT_USER\SOFTWARE のレジストリエントリが移行されます。

既存のアプリケーションプロファイルが複数ある場合、Profile Management は、次の優先度に従って移行を実行します:

1. 同じ種類の OS のプロファイルから移行します（シングルセッション OS からシングルセッション OS またはマルチセッション OS からマルチセッション OS）。
2. 同じ Windows OS ファミリの OS のプロファイルから移行します（Windows 10 から Windows 10、Windows Server 2016 から Windows Server 2016 など）。
3. 以前の OS のプロファイルから移行します（Windows 7 から Windows 10、Windows Server 2012 から Windows Server 2016 など）。
4. 最も近い OS のプロファイルから移行します。

注：ユーザーストアパスに変数「!CTX_OSNAME!」を含めてオペレーティングシステムの短い名前を指定する必要があります。これによって、Profile Management が既存のアプリケーションプロファイルを見つけることができます。

この設定をここで構成しない場合、INI ファイルの設定が使用されます。

この設定をここで構成しない、または.ini ファイルからの設定がない場合、デフォルトで無効になります。

テンプレートプロファイルへのパス

この設定では、Profile Management でユーザープロファイルを作成するときにテンプレートとして使用するプロファイルのパスを指定します。

このパスは、NTUSER.DAT レジストリファイルや、テンプレートプロファイルに必要なそのほかのフォルダーやファイルを格納しているフォルダーのものである必要があります。

注:パスに「NTUSER.DAT」を含めないでください。たとえば、「\\myservername\myprofiles\template\ntuser.dat」ではなく「\\myservername\myprofiles\template」を指定します。

UNC パスやローカルマシン上のパスなどの絶対パスを使用します。たとえば、Citrix Provisioning Services イメージ上のテンプレートプロファイルを永続的に指定するにはローカルマシン上のパスを指定します。相対パスは使用できません。

注：Active Directory 属性の拡張、システム環境変数、および%USERNAME%や%USERDOMAIN%変数を使用することはできません。

この設定はデフォルトで無効になっており、最初にログオンしたデバイス上のデフォルトのユーザープロファイルを基にそのユーザーのプロファイルが作成されます。

この設定をここで構成しない場合、INI ファイルの値が使用されます。

この設定をここまたは INI ファイルで構成しない場合、テンプレートは使用されません。

テンプレートプロファイルがローカル プロファイルを上書きする

この設定では、ユーザープロファイルの作成時にローカルプロファイルよりもテンプレートプロファイルを優先する機能を有効または無効にします。

ユーザーには、Citrix ユーザープロファイルがなく、ローカルの Windows ユーザープロファイルがあると考えてください。この場合、この値が有効になっていると、デフォルトでローカルプロファイルが使用され、ユーザーストアに移行されます。このポリシー設定を有効にすると、ユーザープロファイルの作成時にローカルプロファイルではなくテンプレートプロファイルが使用されます。

この設定をここで構成しない場合、INI ファイルの値が使用されます。

この設定をここまたは INI ファイルで構成しない場合、テンプレートは使用されません。

テンプレートプロファイルが移動プロファイルを上書きする

この設定では、ユーザープロファイルの作成時に移動プロファイルよりもテンプレートプロファイルを優先する機能を有効または無効にします。

ユーザーには、Citrix ユーザープロファイルがなく、ローミングの Windows ユーザープロファイルがあると考えてください。この場合、この値が有効になっていると、デフォルトでローミングプロファイルが使用され、ユーザーストアに移行されます。このポリシー設定を有効にすると、ユーザープロファイルの作成時に移動プロファイルではなくテンプレートプロファイルが使用されます。

この設定をここで構成しない場合、INI ファイルの値が使用されます。

この設定をここまたは INI ファイルで構成しない場合、テンプレートは使用されません。

すべてのログオンで **Citrix** 固定プロファイルとして使用されるテンプレートプロファイル

この設定では、Profile Management でユーザープロファイルを作成するときに、テンプレートプロファイルをデフォルトのプロファイルとして使用するかどうかを指定します。

この設定はデフォルトで無効になっており、最初にログオンしたデバイス上のデフォルトのユーザープロファイルを基にそのユーザーのプロファイルが作成されます。

この設定をここで構成しない場合、INI ファイルの値が使用されます。

この設定をここまたは INI ファイルで構成しない場合、テンプレートは使用されません。

レジストリのポリシー設定

August 17, 2024

このセクションには、特定のレジストリキーを Profile Management の処理対象として指定したり除外したりするためのポリシー設定が含まれています。

除外の一覧

ログオフ時に無視される HKEY_CURRENT_USER ハイブのレジストリキーの一覧です。

例：Software\Policies

このポリシーが無効の場合、レジストリキーは除外されません。このポリシーをここで構成しない場合、INI ファイルの値が使用されます。このポリシーをここでまたは INI ファイルで構成しない場合、レジストリキーは除外されません。

包含の一覧

ログオフ時に処理される HKEY_CURRENT_USER ハイブのレジストリキーの一覧です。

例：Software\Adobe

このポリシーが有効な場合、この一覧のキーのみが処理されます。このポリシーが無効な場合、すべての HKEY_CURRENT_USER ハイブが処理されます。このポリシーをここで構成しない場合、INI ファイルの値が使用されます。このポリシーをここでまたは INI ファイルで構成しない場合、すべての HKEY_CURRENT_USER ハイブが処理されます。

デフォルトの除外の一覧の有効化 **- Profile Management 5.5**

ユーザーのプロファイルに同期しない HKCU ハイブのレジストリキーのデフォルトの一覧。このポリシーは、手動で記入しないで GPO 除外ファイルを指定するために使用します。

このポリシーを無効にすると、デフォルトで Profile Management は、いかなるレジストリキーも除外しません。このポリシーをここで構成しない場合、Profile Management は INI ファイルの値を使用します。このポリシーを、ここでも INI ファイルでも構成しない場合、デフォルトで Profile Management は、いかなるレジストリキーも除外しません。

NTUSER.DAT のバックアップ

破損時に、健全とわかっている最新の NTUSER.DAT のコピーのバックアップを有効化し、ロールバックします。

このポリシーをここで構成しない場合、Profile Management は INI ファイルの値を使用します。このポリシーを、ここでも INI ファイルでも構成しない場合、Profile Management は NTUSER.DAT をバックアップしません。

ストリーム配信ユーザープロファイルのポリシー設定

August 17, 2024

このセクションには、Profile Management でのストリーム配信ユーザープロファイルの管理方法を指定するポリシーが含まれています。

常時キャッシュ

この設定では、ユーザーのログオン後にストリーム配信されたファイルをキャッシュするかを指定します。ファイルをキャッシュするとネットワークの帯域幅消費が減少し、ユーザーエクスペリエンスが向上します。

この設定項目は、［プロファイルストリーム配信］設定と一緒に使用します。

この設定はデフォルトで無効になっており、ユーザーのログオン後にストリーム配信されたファイルはキャッシュされません。

この設定をここで構成しない場合、INI ファイルの値が使用されます。

この設定をここで構成しない、または INI ファイルからの設定がない場合、無効になります。

常時キャッシュサイズ

この設定では、ストリーム配信されるファイルの最小サイズをメガバイト（MB）単位で指定します。Profile Management では、ここで指定した値以上のサイズのファイルがユーザーのログオン後にキャッシュされます。

デフォルトでは、値に 0 が指定されており、プロファイル全体がキャッシュされます。この場合、ユーザーのログオン後、バックグラウンドタスクとしてユーザーストアのプロファイルの内容すべてが Profile Management によりキャッシュされます。

この設定をここで構成しない場合、INI ファイルの値が使用されます。

この設定をここで構成しない、または INI ファイルからの設定がない場合、無効になります。

プロファイルストリーミング

この設定では、Profile Management によるユーザープロファイルのストリーム配信機能を有効または無効にします。有効にすると、ユーザーがログオン後にアクセスした場合にのみ、プロファイルファイルとフォルダーがユーザ

ーストアからローカルコンピューターに取得されます。待機領域内のレジストリエントリやファイルは、直ちに取得されます。

デフォルトでは、無効になっています。

この設定をここで構成しない場合、INI ファイルの値が使用されます。

この設定をここで構成しない、または INI ファイルからの設定がない場合、無効になります。

ストリーム配信ユーザープロファイルグループ

この設定では、ストリーム配信する組織単位のユーザープロファイルを Windows ユーザーグループで指定します。

この設定を有効にすると、指定したユーザーグループのユーザープロファイルのみがストリーム配信されます。ほかのユーザープロファイルは、通常どおりに処理されます。

この設定はデフォルトで無効になっており、組織単位のすべてのユーザープロファイルが通常どおりに処理されます。

この設定をここで構成しない場合、INI ファイルの値が使用されます。

この設定をここで構成しない、または INI ファイルからの設定がない場合、すべてのユーザープロファイルが処理されます。

プロファイルストリーム配信の除外機能を有効にする

プロファイルストリーミングの除外機能を有効にする場合:

- Profile Management は、除外リスト内のフォルダーをストリーミングしません
- ユーザーがログオンするとすぐに、そのすべてのフォルダーがユーザーストアからローカルコンピューターにフェッチされます

詳しくは、「ユーザープロファイルのストリーム配信」を参照してください。

待機領域のロックファイルのタイムアウト

この設定項目では、ストレージサーバーが応答不能になってユーザーストアのロックが解除されない場合に、待機領域のファイルをユーザーストアに同期するまでの日数を指定します。この動作により、待機領域が膨張することを防いで、ユーザーストアに常に最新のファイルが同期されるようになります。

デフォルトでは、これは 1 日に設定されています。

この設定をここで構成しない場合、INI ファイルの値が使用されます。

この設定をここで構成しない、または INI ファイルからの設定がない場合、デフォルト値が使用されます。

待機領域のプロファイルストリーミングを有効にする

待機領域内のファイルおよびフォルダーに対して、プロファイルストリーミング機能を有効にできます。

待機領域は、プロファイルストリーミングが有効になっている間、プロファイルの整合性を確保するために使用されます。同時セッションで変更されたプロファイルファイルとフォルダーを一時的に保存します。

デフォルトでは、このポリシーは無効になっており、待機領域のすべてのファイルとフォルダーはログオン時にローカルプロファイルに取得されます。このポリシーを有効にすると、待機領域のファイルは、要求された場合にのみローカルプロファイルに取得されます。プロファイルストリーミングポリシーとともにこのポリシーを使用して、同時セッションシナリオで最適なログオンエクスペリエンスを確保します。

このポリシーは、［フォルダーのプロファイルストリーミングを有効にする］ポリシーが有効になっている場合に、待機領域のフォルダーに適用されます。

ユーザー個人設定レイヤーポリシーの設定

August 17, 2024

Virtual Delivery Agent 内のユーザーレイヤーのマウントを有効にするには、構成パラメーターを使用して以下を指定します:

- ユーザーレイヤーにアクセスするネットワーク上の場所。
- 新しいユーザーレイヤーのディスクが拡大できるサイズ。

このために、次の 2 つのポリシーが利用可能なポリシーの一覧に表示されます:

- ユーザーレイヤーリポジトリパス - 「値」フィールドに「server name or address\folder name」の形式でパスを入力します。
- ユーザーレイヤーサイズ GB - デフォルトのユーザーレイヤーサイズは 10GB で、Citrix が推奨する最小サイズです。ユーザーレイヤーは、領域が使用されると設定したサイズまで拡張するシンプロビジョニングされたディスクです。ユーザーレイヤーのサイズが小さくなることはありません。

> 注:
>
> ユーザーレイヤーサイズを大きくすると、新しいユーザーレイヤーに影響し、既存のユーザーレイヤーが拡張されます。レイヤーサイズを小さくすると、新しいユーザーレイヤーにのみ影響します。既存のユーザーレイヤーのサイズが小さくなることはありません。

詳しくは、「ユーザー個人設定レイヤー」を参照してください。

Virtual Delivery Agent のポリシー設定

August 17, 2024

[Virtual Delivery Agent 設定］カテゴリには、Virtual Delivery Agent（VDA）と Controller 間の通信を制御するための設定項目が含まれています。

重要：重要：VDA を Delivery Controller に登録するときに、これらの設定項目で提供される情報が必要になります（自動更新機能を使用しない場合）。これらの情報は登録に必要であるため、グループポリシーエディターを使って以下の設定項目を構成する必要があります（VDA のインストール時にこれらの情報を指定する場合を除く）。

- コントローラー登録の IPv6 ネットマスク
- コントローラー登録ポート
- コントローラー SID
- Controller
- IPv6 コントローラー登録のみを使用する
- サイト GUID

コントローラー登録の IPv6 ネットマスク

このポリシー設定では、VDA で使用されるサブネットを指定できます。この場合、グローバル IP は使用されません。これにより、指定した IPv6 アドレスおよびネットワークでのみ VDA が登録されます。VDA は、指定されたネットマスクに最初にマッチしたアドレスでのみ登録されます。この設定は、［IPv6 Controller 登録のみを使用する］ポリシー設定が有効な場合にのみ有効です。

デフォルトでは、空白になっています。

コントローラー登録ポート

この設定を使用する場合は、［コントローラーの自動更新を有効にする］設定が無効になっていることを確認してください。

この設定項目では、VDA の Controller 登録をレジストリで行うときに使用される TCP/IP ポート番号を指定します。

デフォルトのポート番号は、80 に設定されています。

コントローラー SID

この設定を使用する場合は、［コントローラーの自動更新を有効にする］設定が無効になっていることを確認してください。

この設定項目では、VDA の Controller 登録をレジストリで行うときに使用される Controller のセキュリティ識別子（SID）をスペース区切りの一覧で指定します。この設定はオプションの設定項目で、［**Controller**］設定と一緒に使用して、登録に使用される Controller の一覧を制限できます。

デフォルトでは、空白になっています。

Controller

この設定を使用する場合は、［コントローラーの自動更新を有効にする］設定が無効になっていることを確認してください。

この設定項目では、VDA の Controller 登録をレジストリで行うときに使用される Controller の完全修飾ドメイン名（FQDN）をスペース区切りの一覧で指定します。この設定はオプションの設定項目で、［コントローラー **SID**］設定と一緒に使用することもできます。

デフォルトでは、空白になっています。

コントローラーの自動更新を有効にする

この設定項目では、インストール後の VDA を Controller に自動的に登録する機能を許可または禁止します。

VDA を Controller に登録すると、登録先の Controller により環境内の Controller の FQDN および SID の一覧が VDA に送信されます。この一覧の内容は、VDA により永続的なストレージに書き込まれます。また、各 Controller も Controller 情報について 90 分ごとにサイトのデータベースをチェックします。次のいずれかが発生した場合、Controller は更新されたリストを登録済みの VDA に送信します:

- 前回のチェック以降、Controller が追加または削除された
- ポリシーが変更された

VDA は、受信した最新のリストに基づいてすべての Controller からの接続を受け入れます。

デフォルトでは、有効になっています。

IPv6 コントローラー登録のみを使用する

この設定項目では、Controller への登録時に VDA で使用されるアドレスの形式を指定します。

- この設定項目を有効にすると、そのマシンの IPv6 アドレスを使用して VDA が Controller と登録および通信を行います。VDA が Controller と通信するときに、グローバル IP アドレス、ユニークローカルアドレス（ULA）、リンクローカルアドレス（ほかの IPv6 アドレスを使用できない場合のみ）の順で IPv6 アドレスが選択されます。
- この設定が無効な場合、そのマシンの IPv4 アドレスを使用して VDA が Controller と登録および通信を行います。

デフォルトでは、この設定は無効になっています。

サイト **GUID**

この設定を使用する場合は、［コントローラーの自動更新を有効にする］設定が無効になっていることを確認してください。

この設定項目では、VDA の Controller 登録を Active Directory ベースで行うときに使用される、サイトのグローバル一意識別子（GUID）を指定します。

デフォルトでは、空白になっています。

HDX 3D Pro のポリシー設定

August 17, 2024

HDX 3D Pro セクションには、ユーザーの画質構成ツールを有効にして構成するための設定項目が含まれています。このツールを使用すると、ユーザーは使用可能な帯域幅の使用を最適化できます。この最適化に向けて、画質と応答性のバランスがリアルタイムで調整されます。

無損失を有効にする

この設定では、ユーザーが画質構成ツールで無損失圧縮を有効にしたり無効にしたりすることを許可するかどうかを指定します。デフォルトでは、ユーザーは無損失圧縮を有効にできません。

ユーザーが無損失圧縮を有効にしたと考えてください。この場合、自動的に画質構成ツールで設定可能な最高画質に設定されます。デフォルトでは、ユーザーデバイスとホストコンピューターの能力に応じて、GPU または CPU ベースの圧縮が使用されます。

HDX 3D Pro 品質レベル

この設定では、ユーザーが画質構成ツールで設定できる最小値および最大値を指定します。これらの値を使用して、ユーザーは画質構成ツールで画質調整範囲を定義できます。

画質は 0～100 の値で指定します。最大値には、最小値を超える値を設定する必要があります。

監視のポリシー設定

August 17, 2024

監視セクションには、プロセスとリソースの監視、およびアプリケーション障害の監視に関するポリシー設定が含まれています。

これらのポリシーのスコープは、以下に基づいて定義できます:

- サイト
- デリバリーグループ
- デリバリーグループの種類
- 組織単位
- タグ

プロセスおよびリソース監視のポリシー

CPU、メモリ、およびプロセスの各データポイントは VDA から収集され、監視データベースに格納されます。VDA からデータポイントを送信するとネットワーク帯域幅が消費され、これを保存すると監視データベースで大幅に容量が消費されます。特定のスコープのリソースデータまたはプロセスデータ、あるいはその両方を監視したくない場合を考えてください。たとえば、特定のデリバリーグループまたは組織単位です。この場合、ポリシーを無効にすることをお勧めします。

プロセスの監視を有効にします

この設定を有効にすると、VDA がインストールされているマシンでのプロセスの監視が許可されます。CPU やメモリ使用量などの統計が監視サービスに送信されます。統計は、Director でのリアルタイム通知および履歴レポートに使用されます。

デフォルトでは、この設定は無効になっています。

リソースの監視を有効にします

この設定を有効にすると、VDA がインストールされているマシンでのクリティカルパフォーマンスカウンターの監視が許可されます。統計（CPU やメモリ使用量、IOPS、ディスク遅延などのデータ）が監視サービスに送信されます。統計は、Director でのリアルタイム通知および履歴レポートに使用されます。

デフォルトでは、この設定は有効になっています。

スケーラビリティ

CPU とメモリのデータは、5 分間隔で各 VDA からデータベースにプッシュされます。プロセスデータ（有効な場合）は、10 分間隔でデータベースにプッシュされます。IOPS およびディスク遅延データは、データベースに 1 時間間隔で適用されます。

CPU とメモリデータ

CPU とメモリデータは、デフォルトで ［有効］に設定されています。データ保持の値は次のとおりです（Platinum ライセンス）。

データの粒度	日数
5 分データ	1 日
10 分データ	7 日間
時間単位のデータ	30 日間
日単位のデータ	90 日間

IOPS およびディスク遅延データ

IOPS およびディスク遅延データは、デフォルトで ［有効］に設定されています。データ保持の値は次のとおりです（Platinum ライセンス）。

データの粒度	日数
時間単位のデータ	3 日
日単位のデータ	90 日間

データ保持設定では、1 つの VDA の以下のデータを 1 年間格納するのに約 276KB の容量が必要です：

- CPU
- メモリ
- IOPS
- ディスク遅延データ

マシン数	必要なストレージ
1	276KB
1K	270MB
40K	10.6GB

プロセスデータ

デフォルトでは、プロセスデータは ［無効］になっています。プロセスデータは、必要に応じてマシンのサブセットで有効にすることをお勧めします。プロセスデータのデフォルトのデータ保持設定は次のとおりです:

データの粒度	日数
10 分のデータ	1 日
時間単位のデータ	7 日間

プロセスデータがデフォルトの保持設定で有効な場合、プロセスデータは 1 年間で VDA あたり約 1.5MB、ターミナルサービス VDA（TS VDA）あたり約 3MB を消費します。

マシン数	必要なストレージ（VDA）	必要なストレージ（TS VDA）
1	1.5MB	3MB
1K	1.5GB	3GB

> 注:
>
> 前述の数値には、インデックス領域は含まれません。この計算はすべて概算であり、展開によって異なります。

オプションの構成

デフォルトの保持設定をニーズに合わせて変更できます。ただし、この構成はストレージを余分に消費します。以下の設定を有効にすると、プロセス使用データがより正確になります。有効にできる構成は次のとおりです。

EnableMinuteLevelGranularityProcessUtilization

EnableDayLevelGranularityProcessUtilization

これらの構成は、監視 PowerShell コマンドレット：Set-MonitorConfigurationで有効にできます。

アプリケーション障害の監視ポリシー

デフォルトでは、［アプリケーション障害］タブは、マルチセッション OS VDA からのアプリケーション障害のみが表示されます。アプリケーション障害の監視の設定は、以下の監視ポリシーによって変更できます。

アプリケーション障害の監視を有効にする

アプリケーション障害の監視を、アプリケーションのエラーまたは障害（クラッシュと未処理例外）のいずれか、または両方を監視するように構成するには、以下の設定を行ってください。
［値］を ［なし］に設定して、アプリケーション障害の監視を無効にしてください。
デフォルトでは、この設定はアプリケーション障害のみになっています。

シングルセッション **OS VDA** でアプリケーション障害の監視を有効にする

デフォルトでは、マルチセッション OS の VDA でホストされたアプリケーションの障害のみが監視されています。シングルセッション OS VDA を監視するには、このポリシーを ［許可］に設定します。
デフォルトでは、この設定は ［禁止］になっています。

障害の監視から除外するアプリケーション一覧

障害を監視しないアプリケーションの一覧を指定します。
デフォルトでは、この一覧は空です。

分析のためのデータ収集ポリシー

分析のための **VDA** データ収集

ポリシーを使用して、パフォーマンス分析およびセキュリティ分析のために VDA のパフォーマンスおよびセキュリティ関連メトリックを Monitor サービスが収集することを有効または無効にします。デフォルトでは、ポリシーは［許可］に設定されています。ポリシーを ［禁止］に設定して、VDA からのデータの収集を停止します。

セキュリティ監視のためにクリップボードの場所メタデータを収集

このポリシーを使用して、セキュリティの監視、監査、およびコンプライアンスのためにブローカーサービスによるクリップボードの場所メタデータの収集を有効または無効にします。デフォルトでは、このポリシーは ［有効］になっています。ポリシーを ［無効］に設定すると、VDA からのデータの収集を停止します。

パフォーマンス監視のための診断データ収集

このポリシーは、監視サービスがセッション情報、UPM/EUEM サービス状態、Microsoft Teams の最適化、接続プロトコルなどの診断データを収集できるようにします。デフォルトでは、このポリシーは ［有効］になっています。ポリシーを ［無効］に設定すると、VDA からのデータの収集を停止します。

ストレージ計画のヒント

グループポリシーリソースデータやプロセスデータを監視しない場合は、グループポリシーを使ってどちらかまたは両方をオフにできます。詳しくは、「ポリシーの作成」の「グループポリシー」セクションを参照してください。

データのグルーミングデフォルトのデータ保持設定を変更して、データを早くグルーミングし、ストレージ領域を開放できます。グルーミングの設定について詳しくは、「API を使ったデータアクセス」の「データの粒度と保持」を参照してください。

仮想 IP のポリシー設定

August 17, 2024

> 重要:
>
> - Windows 10 Enterprise マルチセッションでは、リモートデスクトップ IP 仮想化（仮想 IP）がサポートされていないため、Windows 10 Enterprise マルチセッションでは、リモートデスクトップ IP 仮想化も仮想ループバックもサポートしていません。
> - リモートデスクトップ IP 仮想化（仮想 IP）は、クラウドでホストされているマシンではサポートされていません。詳しくは、Microsoftのドキュメントを参照してください。

仮想 **IP** セクションには、セッションの仮想ループバックアドレスの使用を制御するための設定項目が含まれています。

仮想 IP ループバックサポート

この設定項目では、各セッション固有の仮想ループバックアドレスの使用を有効にするかどうかを指定します。無効にすると、セッション固有の仮想ループバックアドレスは使用されません。

デフォルトでは、この設定は無効になっています。

仮想 IP ループバックプログラム一覧

この設定項目では、仮想ループバックアドレスを使用できるアプリケーション実行可能ファイルを指定します。リストにプログラムを追加するときは、実行可能ファイルの名前のみを指定します。パス全体を入力する必要はありません。

デフォルトでは、実行可能ファイルは指定されていません。

仮想 **IP** ループバックポートの除外

アプリケーションがこの設定で指定された任意のポート上のループバックアドレスを呼び出す場合、仮想ループバックは呼び出しをセッション固有のループバックアドレスに変更しません

レジストリを使った **COM** ポートおよび **LPT** ポートリダイレクト設定の構成

August 17, 2024

VDA バージョン 7.0〜7.8 では、**COM** ポートおよび **LPT** ポートの設定はレジストリを使用した場合にのみ構成できます。7.0 より前のバージョンの VDA、および VDA バージョン 7.9 以降では、これらの設定は Web Studio で構成できます。詳しくは、「ポートリダイレクトのポリシー設定」および「帯域幅のポリシー設定」を参照してください。

COM ポートおよび LPT ポートのリダイレクト設定は、VDA イメージまたはマシンのレジストリ HKEY_LOCAL_MACHINE\Software\Citrix\GroupPolicy\Defaults\Deprecated で構成します。

COM ポートおよび LPT ポートリダイレクトを有効にするには、以下のレジストリキーを追加して REG_DWORD 値を設定します。

注意：レジストリエディターの使用を誤ると、深刻な問題が発生する可能性があり、OS の再インストールが必要になる場合もあります。レジストリエディターの誤用による障害に対して、Citrix では一切責任を負いません。レジストリエディターは、お客様の責任と判断の範囲でご使用ください。また、レジストリファイルのバックアップを作成してから、レジストリを編集してください。

レジストリキー	説明	値
AllowComPortRedirection	COM ポートリダイレクトを許可または禁止する	1（許可）または 0（禁止）
LimitComBw	COM ポートリダイレクトチャネルの最大帯域幅	数値
LimitComBWPercent	COM ポートのリダイレクトチャネルで使用可能な帯域幅のセッション全体に対する割合	0〜100 の数値
AutoConnectClientComPorts	ユーザーデバイス側の COM ポートへの自動接続	1（許可）または 0（禁止）
AllowLptPortRedirection	LPT ポートリダイレクトを許可または禁止する	1（許可）または 0（禁止）
LimitLptBw	LPT ポートリダイレクトチャネルの最大帯域幅	数値

レジストリキー	説明	値
LimitLptBwPercent	LPT ポートのリダイレクトチャネルで使用可能な帯域幅のセッション全体に対する割合	0～100 の数値
AutoConnectClientLptPorts	ユーザーデバイス側の LPT ポートへの自動接続	1（許可）または 0（禁止）

これらのレジストリを設定したら、そのマスターイメージまたは物理マシンが使用されるようにマシンカタログを変更します。ユーザーのデスクトップは、ログオフ時に新しい設定で更新されます。

Connector for Configuration Manager 2012 のポリシー設定

August 17, 2024

[Connector for Configuration Manager 2012] カテゴリには、Citrix Connector 7.5 エージェントを構成するための設定項目が含まれています。

> 重要:
>
> 警告、ログオフ、および再起動メッセージに関する設定項目は、手動管理または Provisioning Services で管理するマルチセッション OS マシンカタログにのみ適用されます。これらのマシンカタログでは、保留中のアプリケーションのインストールまたはソフトウェアのアップデートがある場合、Connector サービスによりユーザーに警告が表示されます。

MCS で管理するカタログでは、Web Studio でユーザーに通知してください。手動管理のシングルセッション OS カタログでは、Configuration Manager でユーザーに通知してください。Provisioning Services で管理するシングルセッション OS カタログでは、Provisioning Services でユーザーに通知してください。

警告表示間隔

この設定項目では、警告メッセージを表示する間隔を定義します。

間隔は、ddd.hh:mm:ss 形式で設定します。

- ddd はオプションのパラメーターで、日数を 0～999 で指定します。
- hh は、時間を 0～23 で指定します。
- mm は、分を 0～59 で指定します。
- ss は、秒を 0～59 で指定します。

デフォルトでは、01:00:00（1 時間）が設定されています。

警告メッセージボックスの本文テキスト

この設定項目では、予定されているソフトウェア更新、またはログオフが必要となるメンテナンスをユーザーに通知するためのメッセージを入力します。

デフォルトでは、「{TIMESTAMP} Save your work. The server goes offline for maintenance in {TIMELEFT}」というメッセージが設定されています。

警告メッセージボックスのタイトル

この設定項目では、警告メッセージのタイトルバーに表示されるテキストを入力します。

デフォルトでは、「Upcoming Maintenance」というタイトルが設定されています。

警告表示期間

この設定項目では、ソフトウェアの更新またはメンテナンスについての警告メッセージを表示する期間を定義します。

期間は、ddd.hh:mm:ss 形式で設定します。

- ddd はオプションのパラメーターで、日数を 0～999 で指定します。
- hh は、時間を 0～23 で指定します。
- mm は、分を 0～59 で指定します。
- ss は、秒を 0～59 で指定します。

デフォルトでは、16:00:00（16 時間）が設定されています。これにより、メンテナンスの約 16 時間前に最初の警告メッセージが表示されます。

最終的な強制ログオフ メッセージの内容

この設定項目では、強制ログオフ処理が開始されたことをユーザーに通知するためのメッセージを入力します。

デフォルトでは、「The server is currently going offline for maintenance」というメッセージが設定されています。

最終的な強制ログオフ メッセージのタイトル

この設定項目では、最終的な強制ログオフメッセージのタイトルバーに表示される文字列を入力します。

デフォルトでは、「Notification From IT Staff」というタイトルが設定されています。

強制ログオフの猶予期間

この設定項目では、ソフトウェアの更新またはメンテナンスのために、ユーザーにログオフを警告してから実際に強制ログオフ処理を開始するまでの待機期間を定義します。

期間は、ddd.hh:mm:ss 形式で設定します。

- ddd はオプションのパラメーターで、日数を 0～999 で指定します。
- hh は、時間を 0～23 で指定します。
- mm は、分を 0～59 で指定します。
- ss は、秒を 0～59 で指定します。

デフォルトでは、00:05:00（5 分）が設定されています。

強制ログオフ メッセージの内容

この設定項目では、強制ログオフが開始される前に作業を保存してログオフするようにユーザーに通知するためのメッセージを入力します。

デフォルトでは、「{TIMESTAMP} Save your work and log off. The server goes offline for maintenance in {TIMELEFT}」というメッセージが設定されています。

強制ログオフ メッセージのタイトル

この設定項目では、強制ログオフメッセージのタイトルバーに表示される文字列を入力します。

デフォルトでは、「Notification From IT Staff」というタイトルが設定されています。

Image Provider 統合の有効化

Connector エージェントでは、Provisioning Services または MCS で管理されるマシンのクローン上で動作しているかどうかが自動的に検出されます。これらのイメージ管理されたクローン上では、Configuration Manager によるアップデートが Connector エージェントによってブロックされ、カタログのマスターイメージ上にアップデートが自動的にインストールされます。

マスターイメージのアップデートが完了したら、Web Studio で MCS カタログクローンの再起動をオーケストレーションします。Connector エージェントは、Configuration Manager のメンテナンスウィンドウで PVS カタログクローンの再起動を自動的にオーケストレーションします。この動作を無効にして、Configuration Manager によってソフトウェアがカタログクローンにインストールされるように設定するには、イメージ管理モードを［無効］に変更します。

再起動メッセージの内容

この設定項目では、サーバーの再起動をユーザーに通知するためのメッセージを入力します。

デフォルトでは、「The server is currently going offline for maintenance」というメッセージが設定されています。

定期的なエージェント タスクの実行間隔

この設定項目では、Citrix Connector エージェントタスクの実行間隔を指定します。

期間は、ddd.hh:mm:ss 形式で設定します。

- ddd はオプションのパラメーターで、日数を 0～999 で指定します。
- hh は、時間を 0～23 で指定します。
- mm は、分を 0～59 で指定します。
- ss は、秒を 0～59 で指定します。

デフォルトでは、00:05:00（5 分）が設定されています。

ポリシーの変更

August 17, 2024

次の表に、Citrix Virtual Apps and Desktops 7 2407 のポリシードキュメントに対する重要な変更点を示します。

ポリシーの変更されたコンテンツの表:

ポリシー設定	変更	日付
Profile Management > 詳細設定 > ユーザーストア間でセッション内ポリシーコンテナのフェールオーバーを有効にする	ユーザーストア間でのセッション内プロファイルコンテナのフェールオーバーに関する新しいポリシー。詳細情報。	31 Jul 2024
Profile Management > レジストリ > 包含の一覧	レジストリの除外と包含のサポートがコンテナベースのプロファイルソリューションに拡張されました。詳細情報。	31 Jul 2024
Profile Management > レジストリ > 除外リスト		31 Jul 2024
Profile Management > フォルダーのリダイレクト	フォルダーのリダイレクトポリシーの機能強化。詳細情報。	31 Jul 2024

ポリシー設定	変更	日付
セッションメトリックの収集	詳しくは、「ICA のポリシー設定」を参照してください。	31 Jul 2024

ポリシーで廃止予定コンテンツの表:

ポリシー設定	廃止済み	日付
Citrix Virtual Apps and Desktops 7 2407 のリリース。	なし	31 Jul 2024

管理

August 17, 2024

Citrix Virtual Apps and Desktops サイトの管理では、さまざまなアイテムとタスクを管理します。

ライセンス

サイトを作成するときには、Citrix ライセンスサーバーへの有効な接続が必要です。その後、Studio から、ライセンスの追加、ライセンスの種類やモデルの変更、ライセンス管理者の管理などのライセンス管理タスクを行うことができます。また、Studio からライセンス管理コンソールにアクセスすることもできます。

アプリケーション

アプリケーションは、デリバリーグループ、および必要に応じてアプリケーショングループで管理します。

ゾーン

地理的に分散した展開では、ゾーンを使用して、エンドユーザーにより近いところにアプリケーションやデスクトップを配置し、パフォーマンスを向上させることができます。サイトをインストールおよび構成するときには、Controller、マシンカタログ、ホスト接続はすべて、1 つのプライマリゾーンにあります。その後、Studio を使って、これらのアイテムを含むサテライトゾーンを作成します。サイトに複数のゾーンを作成すると、新しく作成するマシンカタログ、ホスト接続、追加の Controller をどのゾーンに配置するか、指定できるようになります。また、ゾーン間でのアイテムの移動も可能です。

接続とリソース

ユーザーにアプリケーションやデスクトップを配信するマシンのホストに、ハイパーバイザーやその他のサービスを使用している場合、サイトを作成したときに、そのハイパーバイザーやその他のサービスへの最初の接続を作成します。接続のストレージとネットワークの詳細が、その接続のリソースになります。後でその接続やリソースを変更したり、追加の接続を作成したりできます。また、構成された接続を使用するマシンの管理も可能です。

ローカルホストキャッシュ

ローカルホストキャッシュを使用すると、Delivery Controller とサイトデータベースの間の接続が失敗しても、サイト内の接続仲介操作を続行できます。

仮想 IP と仮想ループバック

Microsoft 社の仮想 IP アドレス機能により、セッションごとに動的に割り当てられる固有の IP アドレスを公開アプリケーションで使用できます。Citrix の仮想ループバック機能を使用すると、ローカルホストの範囲内で固有の仮想ループバックアドレスが使用されるように、ローカルホストとの通信に依存するアプリケーションを構成できます。

Delivery Controller

この記事では、Controller をサイトに追加およびサイトから削除する場合の考慮事項と手順を説明します。また、Controller を別のゾーンやサイトに移動する方法、および VDA を別のサイトに移動する方法についても説明します。

Delivery Controller による VDA 登録

VDA でアプリケーションやデスクトップの配信を支援できるようにするには、まず、Controller に登録（接続を確立）する必要があります。Controller のアドレスを指定するいくつかの方法については、この記事で説明します。Controller をサイトに追加、移動、または削除すると同時に、VDA が最新情報を受け取ることが重要です。

セッション

最高のユーザーエクスペリエンスを提供するためには、日々のセッションアクティビティを保守することが重要です。中には、セッションの信頼性を最適化し、不便さやダウンタイム、生産性の損失を軽減できる機能もあります。

- セッション画面の保持
- クライアントの自動再接続
- ICA Keep-Alive
- ワークスペースコントロール
- セッションローミング

Studio での検索の使用

Studio で、マシン、セッション、マシンカタログ、アプリケーション、またはデリバリーグループに関する情報を表示するには、柔軟な検索機能を使用します。

タグ

タグは、マシン、アプリケーション、グループ、ポリシーなどの項目を識別するために使用します。タグを使用すると、特定の操作が指定したタグの項目のみに適用されるように調整できます。

IPv4/IPv6

Citrix Virtual Apps and Desktops では、IPv4 のみまたは IPv6 のみ（ピュア IPv4 またはピュア IPv6）の環境、および重複する IPv4 と IPv6 のネットワークを使用したデュアルスタック環境がサポートされます。ここでは、これらの展開について説明します。また、IPv4 または IPv6 の使用を制御する Citrix ポリシー設定についても説明します。

ユーザープロファイル

デフォルトでは、VDA をインストールすると、Citrix Profile Management も自動的にインストールされます。このプロファイルソリューションを使用する場合は、この記事で一般的な情報を確認してください。詳しくは、Profile Managementのドキュメントを参照してください。

Citrix Diagnostic Facility（CDF）トレースを収集する

CDFControl ユーティリティはイベントトレースコントローラー、つまりコンシューマーであり、各種 Citrix トレースプロバイダーに表示される Citrix Diagnostic Facility（CDF）トレースメッセージを記録します。このユーティリティは、Citrix に関連する複雑な問題のトラブルシューティング、フィルターサポートの解析、パフォーマンスデータの収集を行うためのものです。

Citrix Insight Services

Citrix Insight Services（CIS）は、計測を行って利用統計情報を収集し、ビジネス洞察を得るための、Citrix が提供するプラットフォームです。

Citrix Scout

Citrix Scout は診断情報を収集し、ヘルスチェックを実行します。結果は、Citrix Virtual Apps and Desktops 展開環境での予防的な保守に使用できます。Citrix では、Citrix Insight Services を通じて、収集した診断データの包括的な自動分析機能を提供しています。Scout を使用して、お客様単独で、または Citrix サポートの支援を受けながら問題のトラブルシューティングを行うこともできます。

アプリケーション

August 20, 2024

> 注:
>
> Web Studio（Web ベース）と Citrix Studio（Windows ベース）の 2 つの管理コンソールを使用して、Citrix Virtual Apps and Desktops の展開を管理できます。この記事では Web Studio のみを扱います。Citrix Studio について詳しくは、Citrix Virtual Apps and Desktops 7 2212 以前の同様の記事を参照してください。

はじめに

デリバリーグループのみを使用する（アプリケーショングループは使用しない）環境の場合は、デリバリーグループにアプリケーションを追加します。アプリケーショングループもある場合は、通常、アプリケーショングループにアプリケーションを追加します。このガイダンスでは、管理を簡単にする方法について説明します。アプリケーションは、常に少なくとも 1 つのデリバリーグループまたはアプリケーショングループに属する必要があります。

［アプリケーションの追加］ウィザードでは、デリバリーグループを 1 つまたは複数か、アプリケーショングループを 1 つまたは複数を選択できますが、両方は選択できません。アプリケーションのグループ関連付け（アプリケーショングループからデリバリーグループにアプリケーションを移動するなど）は後で変更できますが、余計な複雑さを回避するのがベストプラクティスです。アプリケーションは、どちらかの種類のグループのみに含めます。

アプリケーションを複数のグループに関連付ける場合、そのすべてのグループのアプリケーションを見ることができる十分な権限を有していなければ、表示上の問題が発生する可能性があります。そのような問題が発生した場合は、より上位の権限を持つ管理者に相談するか、またはアプリケーションが関連付けられているグループをすべて含むように自分の権限を拡張してください。

（おそらく異なるグループの）同じ名前の 2 つのアプリケーションを同じユーザーに公開する場合は、Web Studio の`Application name (for user)`プロパティを変更します。これを行わないと、Citrix Workspace アプリで同じ名前が 2 つ表示されます。

アプリケーションのプロパティ（設定）は、追加時、または後で変更できます。アプリケーションの追加時、またはその後で、アプリケーションを配置するアプリケーションフォルダーを変更することもできます。

詳しくは、次のページを参照してください：

- デリバリーグループの作成
- アプリケーショングループの作成
- タグ

アプリケーションの追加

デリバリーグループまたはアプリケーショングループを作成するとき、アプリケーションを追加できます。これらの手順については、「デリバリーグループの作成」および「アプリケーショングループの作成」で詳しく説明しています。次の手順で、グループ作成後にアプリケーションを追加する方法について説明します。

ヒント：

- リモート PC アクセスのデリバリーグループにアプリケーションを追加することはできません。
- デリバリーグループまたはアプリケーショングループからアプリケーションを削除するために、［アプリケーションの追加］ウィザードを使用することはできません。これは、別の処理になります。

1 つまたは複数のアプリケーションを追加するには、以下の手順に従います。

1. 左側のペインで ［アプリケーション］を選択し、操作バーで ［アプリケーションの追加］を選択します。
2. ［アプリケーショングループの追加］ウィザードが起動され、［はじめに］ページが表示されます。このページは、今後このウィザードが起動されたときに開かないように設定できます。
3. ウィザードの指示に従って、［グループ］ページ、［アプリケーション］ページ、および ［概要］ページの操作を行います。各ページの操作を終えたら、［概要］ページに到達するまで ［次へ］をクリックします。

手順 1 の代わりに、アプリケーションを単一のデリバリーグループまたはアプリケーショングループに追加する場合は、以下の手順に従います：

- **1** つのデリバリーグループのみにアプリケーションを追加するには：手順 1 において Web Studio の左側のペインで ［デリバリーグループ］を選択してから、中央ペインでデリバリーグループを 1 つ選択し、操作バーで ［アプリケーションの追加］を選択します。ウィザードに ［グループ］ページは表示されません。
- **1** つのアプリケーショングループのみにアプリケーションを追加するには：手順 1 において Web Studio の左側のペインで ［アプリケーション］を選択してから、中央ペインでアプリケーショングループを 1 つ選択し、操作バーで、選択したアプリケーショングループ名の下にある ［アプリケーションの追加］を選択します。ウィザードに ［グループ］ページは表示されません。

グループページ

このページには、サイトのすべてのデリバリーグループが一覧表示されます。アプリケーショングループも作成してある場合は、このページにアプリケーショングループとデリバリーグループが一覧表示されます。どちらかのグループを選択できますが、両方のグループは選択できません。言い換えると、アプリケーションを同時にアプリケーショングループとデリバリーグループに追加することはできません。通常は、アプリケーショングループを使用している場合は、デリバリーグループではなくアプリケーショングループにアプリケーションを追加します。

アプリケーションを追加するとき、少なくとも 1 つはデリバリーグループ（または、使用できる場合はアプリケーショングループ）の横にあるチェックボックスをオンにします。すべてのアプリケーションは、常に少なくとも 1 つのグループに関連付けられている必要があります。

アプリケーションページ

［追加］をクリックして、アプリケーションのソースを表示します。

- ［スタート］メニューから：選択したデリバリーグループのマシンで検出されたアプリケーション。このソースを選択すると、新たなページが開き、検出されたアプリケーションが一覧表示されます。追加するアプリケーションのチェックボックスをオンにし、［**OK**］をクリックします。

  このソースは、（1）デリバリーグループが関連付けられていないアプリケーショングループを選択した、（2）マシンを含まないデリバリーグループが関連付けられているアプリケーショングループを選択した、（3）マシンを含まないデリバリーグループを選択した、のいずれかの場合には選択できません。

- 手動：デリバリーグループまたはネットワーク内の別の場所にある VDA 上のアプリケーション。このソースを選択すると、次の方法により、追加するアプリケーションを指定する新しいページが開きます：

  - 実行可能ファイルのパス、作業ディレクトリ、コマンドライン引数（オプション）、管理者およびユーザー用の表示名を入力します。
  - デリバリーグループ内の VDA からアプリケーションを選択します。これを行うには、［参照］をクリックして、VDA にアクセスするための資格情報を入力し、VDA に接続されたあと、VDA からアプリケーションを選択します。選択したアプリケーションのプロパティが、ページ内のフィールドに自動的に入力されます。

- 既存：以前サイトに追加したアプリケーション。このソースを選択すると、新たなページが開き、検出されたアプリケーションが一覧表示されます。追加するアプリケーションのチェックボックスをオンにし、［**OK**］をクリックします。

  このソースは、サイトにアプリケーションが含まれていない場合は選択できません。

- **App-V**： App-V パッケージのアプリケーション。このソースを選択すると、新たなページが開くので、そのページで App-V サーバーまたはアプリケーションライブラリを選択します。結果表示で、追加するアプリケーションのチェックボックスをオンにし、［**OK**］をクリックします。詳しくは、「App-V アプリケーションの展開および配信」を参照してください。

  このソースは、サイトで App-V を構成していない場合は選択できません。

- アプリケーショングループ：アプリケーショングループ。このソースを選択すると、新しいページが開き、アプリケーショングループが一覧表示されます。（各グループのアプリケーションの一覧も表示されますが、グループのみを選択できます。個別のアプリケーションは選択できません。）選択したグループの現在または将来のすべてのアプリケーションが追加されます。追加するアプリケーショングループのチェックボックスをオンにし、［**OK**］をクリックします。

  このソースは、（1）アプリケーショングループがない場合、または（2）選択したデリバリーグループがアプリケーショングループをサポートしない場合（マシンが静的に割り当てられているデリバリーグループなど）は、選択できません。

表で説明したように、［追加］リストの一部のソースは、そのタイプの有効なソースがない場合は選択できません。互換性のないソースはリストに含まれません（たとえば、アプリケーショングループにアプリケーショングループを追加することはできません）。選択したグループに既に追加済みのアプリケーションは選択できません。

アプリケーションのプロパティ（設定）は、このページから、または後で変更できます。

アプリケーションをデリバリーグループに追加すると、デフォルトで`Applications`という名前のフォルダー内に表示されます。アプリケーションは、このページから、または後で変更できます。アプリケーションの追加時に、同じフォルダー内に同じ名前のアプリケーションが存在する場合、追加するアプリケーションの名前を変更するよう指示するメッセージが表示されます。提案された新しい名前を受け入れるか、または拒否してアプリケーションの名前を変更するか別のフォルダーを選択できます。たとえば、**Applications** フォルダーに既に「`app`」が存在する場合に、このフォルダーに「`app`」という名前の別のアプリケーションを追加しようとすると、新しい名前「`app_1`」が提案されます。

概要ページ

追加するアプリケーションが 10 個以下の場合、［追加するアプリケーション］のリストにそれらの名前が表示されます。追加するアプリケーションが 10 個より多い場合は、合計数が示されます。

概要の情報を確認し、［完了］をクリックします。

アプリケーションのグループ関連付けの変更

アプリケーションの追加後、アプリケーションを関連付けるデリバリーグループやアプリケーショングループを変更できます。

アプリケーションを追加のグループにドラッグできます。ドラッグアンドドロップする代わりに、操作バーのコマンドを使用することもできます。

アプリケーションを複数のデリバリーグループまたはアプリケーショングループに関連付けた場合、グループの優先度を使用して、アプリケーションを検索するときに複数のグループを確認する順序を指定できます。デフォルトでは、すべてのグループの優先度は 0（最高）です。同じ優先度のグループは負荷分散されます。

アプリケーションは、アプリケーションを配信できる共有（プライベートではない）マシンを含むデリバリーグループに関連付けることができます。また、(1) デリバリーグループに共有マシンが含まれていてこのグループがバージョン 7.9 以前の XenDesktop 7.x で作成されており、かつ (2) [Edit delivery group] 権限が付与されている場合は、デスクトップのみを配信可能な共有マシンが含まれるデリバリーグループを選択することもできます。［プロパティ］ダイアログボックスをコミットすると、デリバリーグループの種類が自動的に「desktops and applications」に変換されます。

1. Web Studio にサインインし、左側のペインで ［アプリケーション］をクリックしてからアプリケーションを選択します。
2. 操作バーで ［プロパティ］を選択します。
3. ［グループ］ページを選択します。
    - グループを追加する場合は、［追加］をクリックし、［アプリケーショングループ］または ［デリバリーグループ］を選択します。（アプリケーショングループを作成していない場合は、［デリバリーグループ］のみが表示されます。）次に、1 つまたは複数の追加可能なグループを選択します。アプリケーションと互換性のないグループや、既にそのアプリケーションが関連付けられているグループは選択できません。
    - グループを削除する場合は、グループを 1 つまたは複数選択して ［削除］をクリックします。グループの関連付けを削除した結果、アプリケーションがグループのいずれにも関連付けられなくなる場合は、アプリケーションが削除されることが通知されます。
    - グループの優先度を変更する場合は、グループを選択して ［優先度の編集］をクリックします。優先度の値を選択し、［**OK**］をクリックします。
4. 作業が完了したら、変更を適用してウィンドウを開いたままにする場合は ［適用］を、変更を適用してウィンドウを閉じる場合は ［**OK**］をクリックします。

アプリケーションの複製、有効化または無効化、名前変更、および削除

実行できるアクションは次のとおりです：

- 複製：アプリケーションを複製して、パラメーターまたはプロパティが異なる別のバージョンを作成することができます。アプリケーションを複製すると、一意のサフィックスを使用してアプリケーション名が自動的に

変更され、元のアプリケーションの隣に配置されます。アプリケーションを複製して、別のグループに追加することもできます。(複製後、アプリケーションを移動する最も簡単な方法は、アプリケーションをドラッグすることです。)

- 有効化または無効化：アプリケーションの有効化と無効化は、デリバリーグループやアプリケーショングループの有効化と無効化とは異なる操作です。
- 名前変更：同時に名前を変更できるアプリケーションは 1 つのみです。アプリケーションの名前を変更しようとしたときに、同じフォルダーまたはグループ内に同じ名前のアプリケーションが存在する場合、別の名前を指定するよう指示するメッセージが表示されます。
- 削除：アプリケーションを削除すると、そのアプリケーションが関連付けられているデリバリーグループおよびアプリケーショングループからは削除されますが、元々アプリケーションを追加するときに使用したソースからは削除されません。アプリケーションの削除は、デリバリーグループまたはアプリケーショングループからアプリケーションを削除する操作とは異なる操作です。

アプリケーションを複製、有効化、無効化、名前変更、または削除するには：

1. 左側のペインで ［アプリケーション］を選択します。
2. 中央ペインで 1 つまたは複数のアプリケーションを選択し、操作バーで目的のタスクを選択します。
3. 確認のメッセージが表示されたら、［はい］をクリックします。

デリバリーグループからのアプリケーションの削除

アプリケーションは、少なくとも 1 つのデリバリーグループまたはアプリケーショングループに関連付けられる（属する）必要があります。アプリケーションをデリバリーグループから削除することでデリバリーグループまたはアプリケーショングループへのアプリケーションの関連付けが削除される場合、続行すればアプリケーションが削除されるという通知が表示されます。この場合、そのアプリケーションを配信する必要がある場合は、有効なソースからもう一度追加する必要があります。

1. 左側のペインで ［デリバリーグループ］を選択します。
2. デリバリーグループを選択します。下部中央のペインで ［アプリケーション］タブを選択し、削除するアプリケーションを選択します。
3. 操作バーの ［アプリケーションの削除］を選択します。
4. 削除を確認します。

アプリケーショングループからのアプリケーションの削除

アプリケーションは、少なくとも 1 つのデリバリーグループまたはアプリケーショングループに属する必要があります。アプリケーションをアプリケーショングループから削除することでグループへのアプリケーションの関連付けが削除される場合、続行すればアプリケーションが削除されるという通知が表示されます。この場合、そのアプリケーションを配信する必要がある場合は、有効なソースからもう一度追加する必要があります。

1. 左側のペインで ［アプリケーション］を選択します。

2. 中央ペインでアプリケーショングループを選択し、1 つまたは複数のアプリケーションを選択します。
3. 操作バーの ［アプリケーショングループから削除します］を選択します。
4. 削除を確認します。

アプリケーションプロパティの変更

同時にプロパティを変更できるアプリケーションは 1 つのみです。

アプリケーションのプロパティを変更するには、次の手順に従います。

1. 左側のペインで ［アプリケーション］を選択します。
2. アプリケーションを選択し、操作バーで ［アプリケーションプロパティの編集］を選択します。
3. 変更するプロパティを含むページを選択します。
4. 作業が完了したら、行った変更を適用してウィンドウを開いたままにするには ［適用］を、変更を適用してウィンドウを閉じるには ［**OK**］をクリックします。

以下の一覧では、ページはカッコ内に示しています。

プロパティ	ページ
Citrix Workspace アプリでアプリケーションを表示するカテゴリ/フォルダー	配信
コマンドライン引数（「公開アプリケーションにパラメーターを渡す」を参照）	場所
アプリケーションを使用できるデリバリーグループおよびアプリケーショングループ	グループ
説明	識別
ファイル拡張子とファイルタイプの関連付け：アプリケーションが自動的に開く拡張子	ファイルタイプの関連付け
アイコン	配信
StoreFront 用のキーワード	識別
制限（「アプリケーション制限の構成」を参照）	配信
名前：ユーザーと管理者に表示される名前	識別
実行可能ファイルのパス（「公開アプリケーションにパラメーターを渡す」を参照）	場所
ユーザーのデスクトップにショートカットを表示するかどうか：有効化または無効化	配信

プロパティ	ページ
表示できるユーザー：Citrix Workspace アプリでアプリケーションを表示できるユーザーを制限します。制限しても非表示のアプリケーションを起動できます。非表示にして起動できないようにするには、別のグループに追加します。	表示の制限
作業ディレクトリ	場所

使用中のアプリケーションに変更内容を反映させるには、ユーザーがそのセッションからログオフする必要があります。

アプリケーション制限の設定

アプリケーションの使用を管理するため、アプリケーション制限を設定します。たとえば、アプリケーション制限を使用して、アプリケーションに同時にアクセスするユーザーの数を管理することができます。同様に、アプリケーション制限を使用して、リソースの消費量が大きいアプリケーションの同時インスタンスの数を管理することもできます。この制限により、サーバーパフォーマンスを維持し、サービスの質の低下を防ぐことができます。

この機能により、（Citrix Workspace アプリや StoreFront などからの）Controller を介したアプリケーション起動数が制限されます。これ以外の方法で起動される実行中のアプリケーションの数は制限されません。すなわち、アプリケーション制限は、同時使用を管理する管理者をサポートし、あらゆるシナリオに適用されるわけではありません。たとえば、Controller が停止状態モードである場合は、アプリケーション制限を適用できません。

デフォルトでは、同時に実行できるアプリケーションインスタンスの数に制限はありません。アプリケーション制限の設定はいくつかあります。それらのいずれかまたはすべてを構成できます。

- デリバリーグループのすべてのユーザーが実行できるアプリケーションの最大同時インスタンス数。
- デリバリーグループのユーザーごとに 1 つのアプリケーションインスタンス。
- マシンごとの最大同時実行アプリケーションインスタンス数（PowerShell のみ）

制限が設定されている場合、設定された制限を超過するアプリケーションインスタンスをユーザーが起動しようとすると、エラーメッセージが生成されます。複数の制限が構成されている場合、最初の制限に達するとエラーが報告されます。

アプリケーション制限の使用例

- 最大同時インスタンス数を制限する：デリバリーグループで、アプリケーション`Alpha`の同時インスタンスの最大数を 15 に設定しました。その後、このデリバリーグループのユーザーたちが、このアプリケーションの 15 インスタンスを同時に実行しています。このデリバリーグループのユーザーが`Alpha`を起動しようとすると、エラーメッセージが生成され、`Alpha`は起動しません。起動すると、先ほど設定した、アプリケーションの同時インスタンス数の制限値（15）を超過することになるためです。

- ユーザーごとにアプリケーションインスタンスを **1** つのみに制限する：別のデリバリーグループで、1 ユーザーにつき 1 インスタンスのオプションをアプリケーションBetaに対して有効にしました。ユーザー Tony が、アプリケーションBetaを正常に起動しました。当日のその後、このアプリケーションは Tony のセッションで引き続き実行中でしたが、Tony はBetaの別のインスタンスを起動しようとしました。しかし、起動すると 1 ユーザーにつき 1 インスタンスの制限を超過することになるため、エラーメッセージが生成され、Betaは起動しません。
- 最大同時インスタンス数を制限し、ユーザーごとにアプリケーションインスタンスを **1** つのみに制限する：別のデリバリーグループで、同時インスタンスの最大数を 10 に設定し、1 ユーザーにつき 1 インスタンスのオプションをアプリケーションDeltaに対して有効にしました。その後、このデリバリーグループの 10 人のユーザーがそれぞれDeltaのインスタンスを実行している場合、このデリバリーグループの別のユーザーがDeltaを起動しようとすると、エラーメッセージが生成され、Deltaは起動しません。現在の 10 人のDeltaユーザーの誰かがこのアプリケーションの 2 つ目のインスタンスを起動しようとしても、エラーメッセージが表示され、2 つ目のインスタンスは起動しません。
- マシンごとの最大同時インスタンス数の制限とタグによる制限を組み合わせる：アプリケーションCharlieには、特定のサーバーで同時に実行可能なインスタンス数に関するライセンスとパフォーマンス上の要件があります。これらの要件は、サイト内のすべてのサーバーで同時に実行できるインスタンスの数も決定します。

  マシンごとのアプリケーションインスタンス数に関する制限は、（指定したデリバリーグループ内のマシンだけでなく）サイト内のすべてのサーバーに影響します。たとえば、サイトに 3 つのサーバーがあるとします。アプリケーションCharlieの場合、マシンごとのアプリケーションインスタンス数の上限を 2 に設定します。このようにすると、サイト全体で起動できるアプリケーションCharlieのインスタンスは、6 個以下に制限されます（3 つのサーバーそれぞれでは、Charlie のインスタンスは 2 個までに制限されます）。

  アプリケーションの使用をデリバリーグループ内の特定のマシンのみに制限する（また、サイト全体のすべてのマシンのインスタンスを制限する）には：

  - それらのマシンのタグ付け機能を使用します。
  - そのアプリケーションのマシンごとのインスタンス最大数を構成します。

アプリケーションが Controller を介さない方法（Controller が停止状態モードの場合など）で起動し、構成した制限を超過している場合、アプリケーションを使用中のユーザーがインスタンスを終了して実行中のインスタンス数が制限を超過しなくなるまで、追加のインスタンスを起動することはできません。制限を超えたインスタンスは強制的にはシャットダウンされません。ユーザーが閉じるまで続行できます。

セッションローミングを無効にする場合、1 ユーザーにつき 1 インスタンスのアプリケーション制限も無効にしてください。1 ユーザーにつき 1 インスタンスのアプリケーション制限を有効にする場合、新規デバイスでの新規セッションを許可する 2 つの値は、どちらも設定しないでください。ローミングについては、「セッション」を参照してください。

デリバリーグループごとの最大インスタンス数制限と、1 ユーザーにつき 1 インスタンス制限を構成するには：

1. 左側のペインで ［アプリケーション］を選択してから、アプリケーションを 1 つ選択します。
2. 操作バーで ［アプリケーションプロパティの編集］を選択します。

3. ［配信］ページで、次のいずれかのオプションを選択します。

    - アプリケーションの無制限使用を許可します。インスタンスの同時実行数に制限はありません。これがデフォルトの設定です。
    - アプリケーションの制限を設定します。以下の 2 種類の制限があります。いずれかまたは両方を指定します。
        - マシン 1 台あたりが同時に実行できるインスタンスの最大数の指定
        - 1 ユーザーにつき 1 アプリケーションインスタンスの制限

4. 変更を適用してダイアログボックスを閉じる場合は ［**OK**］をクリックし、変更を適用してダイアログボックスを開いたままにするには ［適用］をクリックします。

マシンごとの最大インスタンス数制限（PowerShell のみ）を構成するには:

- PowerShell（Citrix Cloud 環境の場合はリモート PowerShell SDK、オンプレミス環境の場合は PowerShell SDK）で、`MaxPerMachineInstances`パラメーターを使用して適切な`BrokerApplication`コマンドレットを入力します。
- 詳しくは、`Get-Help`コマンドレットを使用してください。例:

```
Get-Help Set-BrokerApplication -Parameter MaxPerMachineInstances
```

公開アプリケーションにパラメーターを渡す

アプリケーションのプロパティの ［場所］ページで、コマンドラインを入力し、公開アプリケーションにパラメーターを渡します。

公開アプリケーションをファイルタイプに関連付けると、その公開アプリケーションのコマンドライン（実行可能ファイルのパス）の末尾に`"%*"`（二重引用符で囲んだパーセント記号とアスタリスク記号）が追加されます。これらの記号は、ユーザーデバイス側に渡されるパラメーターのプレースホルダーとして機能します。

ファイルタイプに関連付けられている公開アプリケーションが起動しない場合は、記号が正しくコマンドラインに含まれていることを確認してください。`"%*"`記号が追加されている場合、デフォルトでは、ユーザーデバイスから渡されるパラメーターが検証されます。特殊なパラメーターを必要とする公開アプリケーションでは、コマンドラインに`"%**"`（二重引用符で囲んだパーセント記号と 2 個のアスタリスク記号）が追加されています。これによりコマンドライン検証が無効になります。コマンドラインにこれらの記号が含まれていない場合は、手作業で追加できます。

実行可能ファイルのパスに、「`"C:\Program Files"`」のようなスペースを使ったフォルダー名が含まれている場合は、アプリケーションのコマンドラインを二重引用符で囲み、このスペースがコマンドラインに属していることを示します。それには、パスの前後に二重引用符を追加し、%*記号の前後にもう 1 組の二重引用符を追加します。このとき、パスの末尾の二重引用符と、%*記号の前の二重引用符の間に、必ずスペースを 1 つ入力してください。

たとえば、公開アプリケーション Windows Media Player のコマンドラインは次のようになります:

```
"C:\Program Files\Windows Media Player\mplayer1.exe""%*"
```


> 注:
>
> 公開アプリケーションを起動するためのコマンドラインの最大文字数は、引数を含めて 203 文字です。

公開アプリケーションでのセッションサインアウトの問題のトラブルシューティング

アプリケーションを公開する場合、公開アプリケーションのメインの実行可能ファイルのみが指定されます。ただし、一部のアプリケーションでは、バックグラウンドで実行され、公開されているメインのアプリケーションが閉じられても、対応するメインの実行可能ファイルによって閉じられない追加の（子）プロセスが生成される場合があります。実行されたスクリプトや、RunやRunOnceKeyなどの特定のレジストリキーから、追加のプロセスが作成される場合もあります。これらのアプリケーションは正常なサインアウトを妨げ、セッションが残留したりハングしたりすることになり、セッションが終了せずユーザーがサインアウトされる可能性があります。

この場合、Citrix Director を使用してこれらのセッションをリセットまたは終了する必要があります。

適切にサインアウトされていないセッションを特定してトラブルシューティングするために、Citrix は 3 つのレジストリエントリを用意しています。これらの問題によりセッションが適切にログオフされない場合の特定とトラブルシューティングは、次の 3 つの手順で行います:

1. 公開アプリケーションが正常なサインアウトを妨げているセッションを特定する
2. 公開アプリケーションが追加の（子）プロセスを生成するかどうかを特定する
3. これらのプロセスを指定されたレジストリエントリに追加して、サインアウトが滞らないようにする

手順 **2**: 公開アプリケーションが追加の（子）プロセスを生成するかどうかを特定する

公開アプリケーションが正常なサインアウトを遅らせていることが特定された場合、次の手順は、このアプリケーションの実行時に追加のプロセスが生成されるかどうかを判断することです。

HKCU\Software\CitrixVolatile\Seamless\Sessions\[ID]\LogoffCheckerBlockingProce
を読み取ることで、公開アプリケーションが閉じられたときに正常なサインアウトをブロックしているプロセスがあるかどうかを判断できます。

次の例では、キーLogoffCheckerBlockingProcessに次のエントリが含まれています:

```
PhoneExperienceHost.exe
SkypeApp.exe
SkypeBackgroundHost.exe
```

これらのプロセスにより、正常なサインアウトが滞っています。

> 注:
>
> [ID] には、確認するセッションの正しいセッション ID を入力します。

手順 **3**：これらのプロセスを指定されたレジストリエントリに追加して、サインアウトが滞らないようにする

これらのプロセスを次のレジストリ キーに追加すると、以降のセッションでサインアウトが妨げられるのを防ぐことができます：

```
Add the process file name to the following registry key:
Caution! Refer to the Disclaimer at the end of this article before
   using the Registry Editor.
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWI
Value Name:LogoffCheckSysModules
Type:REG_SZ
String:MyAppName.exe
```

`LogoffCheckSysModules`について詳しくは、「Graceful logoff from a published application renders the session in an active state」を参照してください。

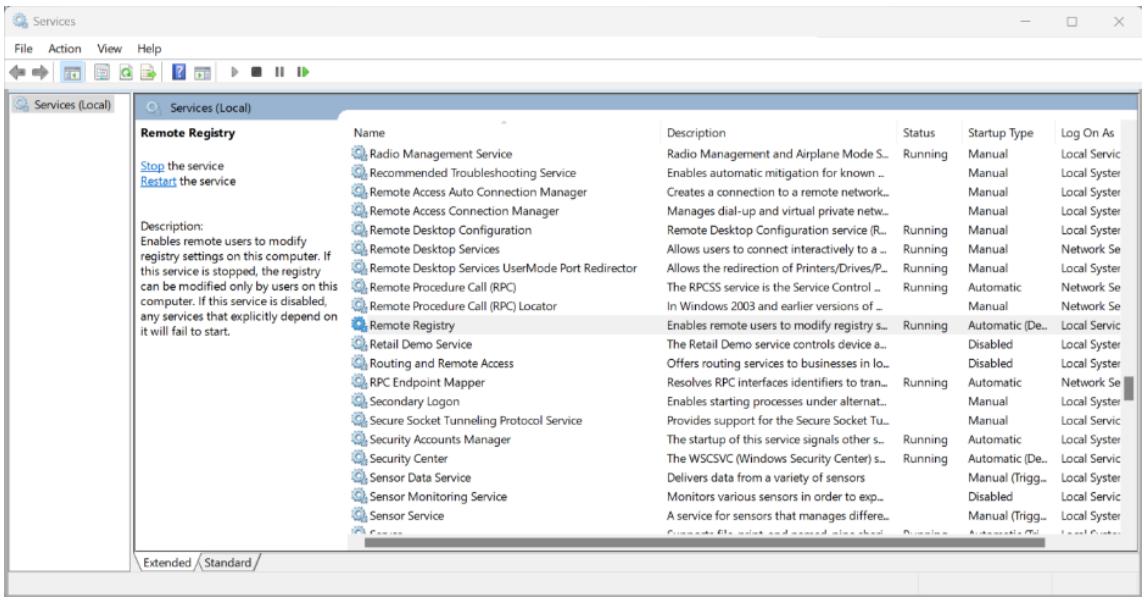
詳細な手順のトラブルシューティングガイド

1. テスト対象の VDA でリモートレジストリサービスを開始します：

   a)［コントロールパネル］で管理ツール、サービスの順に選択します。

   b)［**Remote Registry Service**］を右クリックし、［プロパティ］を選択します。

   c)［スタートアップの種類］で、ドロップダウンメニューから ［自動］を選択します。



2. テスト対象の VDA で Windows ファイアウォールをオフにするか、受信ファイアウォール規則を作成してポート 455 を有効にします：

   a)［コントロールパネル］で ［**Windows Defender** ファイアウォール］**>**［詳細設定］を選択します。

b) ［受信の規則］を右クリックして ［新しい規則］を選択します。

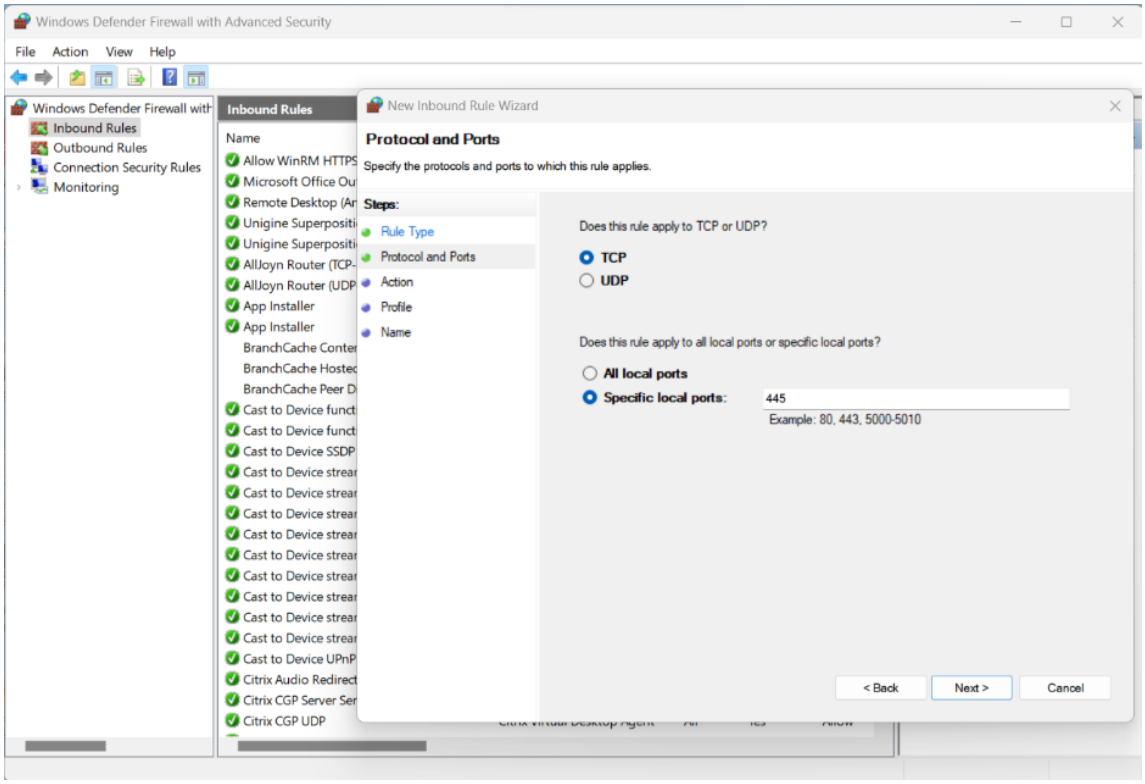
c) 新しい受信の規則ウィザードで、［ポート］を選択します。

d) ［プロトコルおよびポート］ページで、**TCP** と特定のローカルポートを選択します。ローカルポートとして445を入力します。

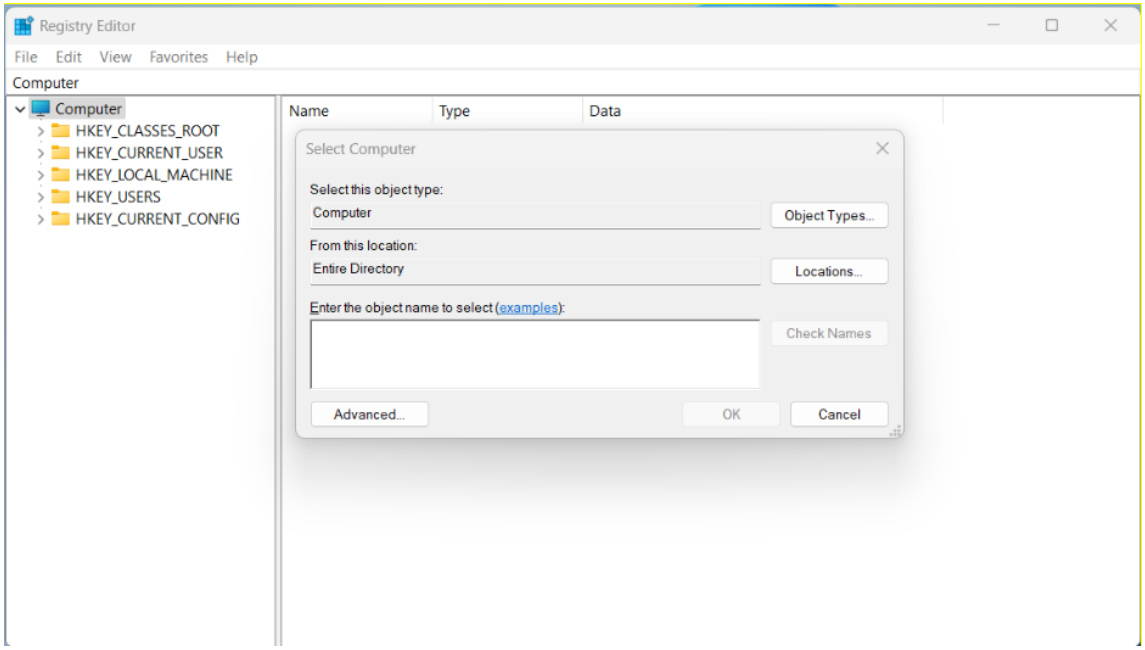
e) ［操作］ページで ［接続を許可する］を選択します。

f) 新しい受信規則を適用するファイアウォールプロファイルを選択します。

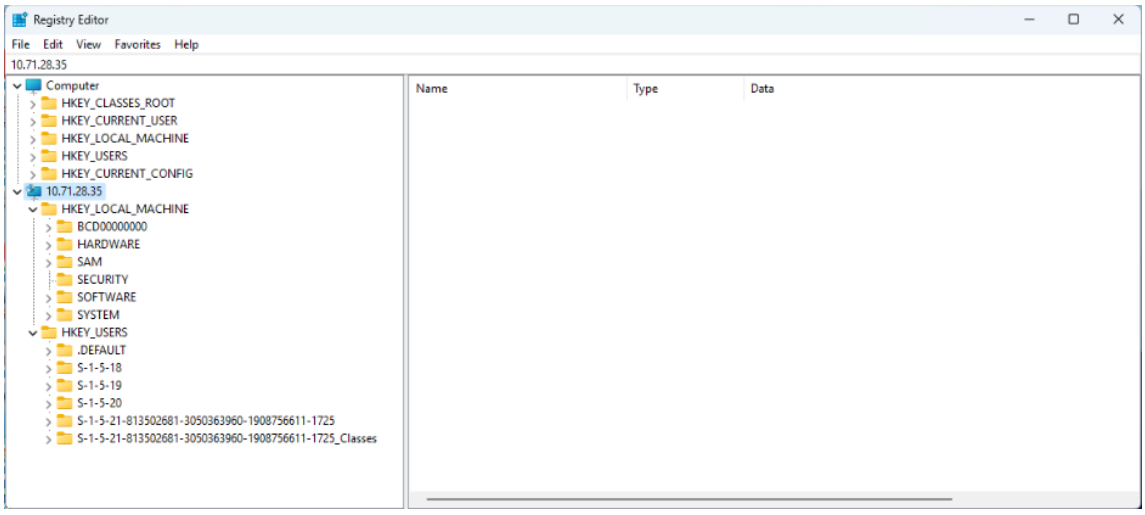
g) ファイアウォール規則に名前を付け、［完了］を選択して、新しい受信規則ウィザードを終了します。



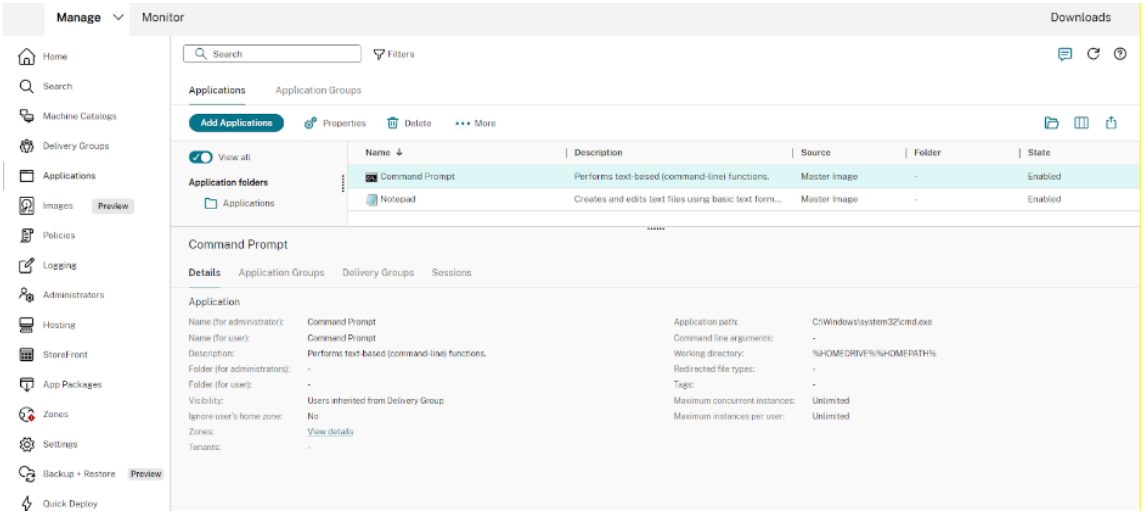
3. 同じドメイン上の別の仮想マシン（DC、DDC、または別の VDA など）から`Regedit`を実行し、リモートレジストリに接続します。



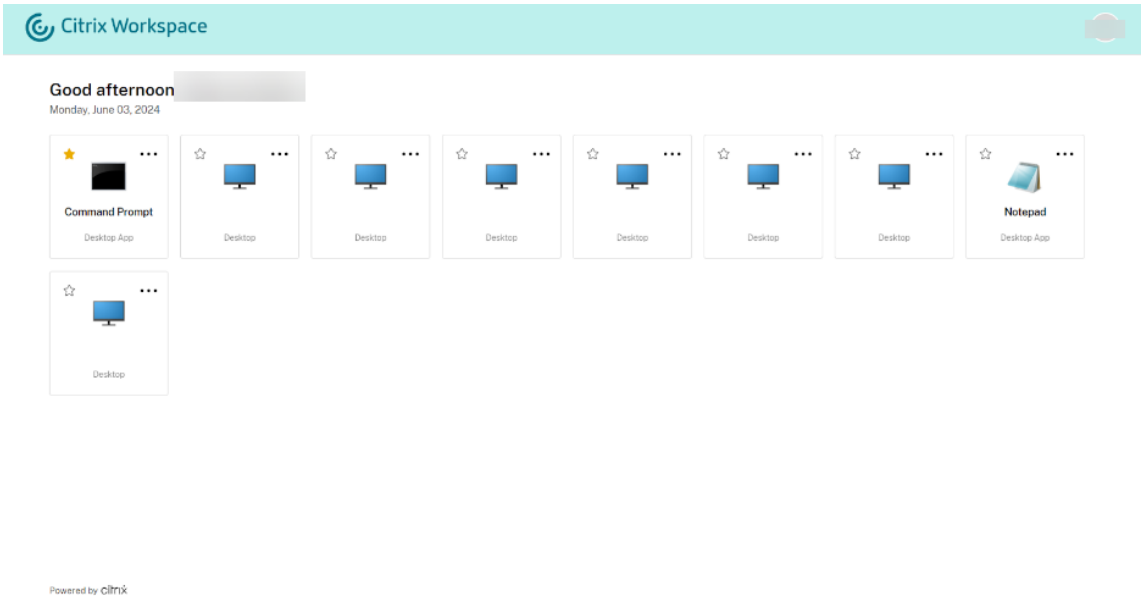
4. テスト対象の VDA の IP アドレスを入力し、[**OK**] をクリックします。`regedit`ツリーには、テスト対象の VDA のブランチが表示される必要があります。



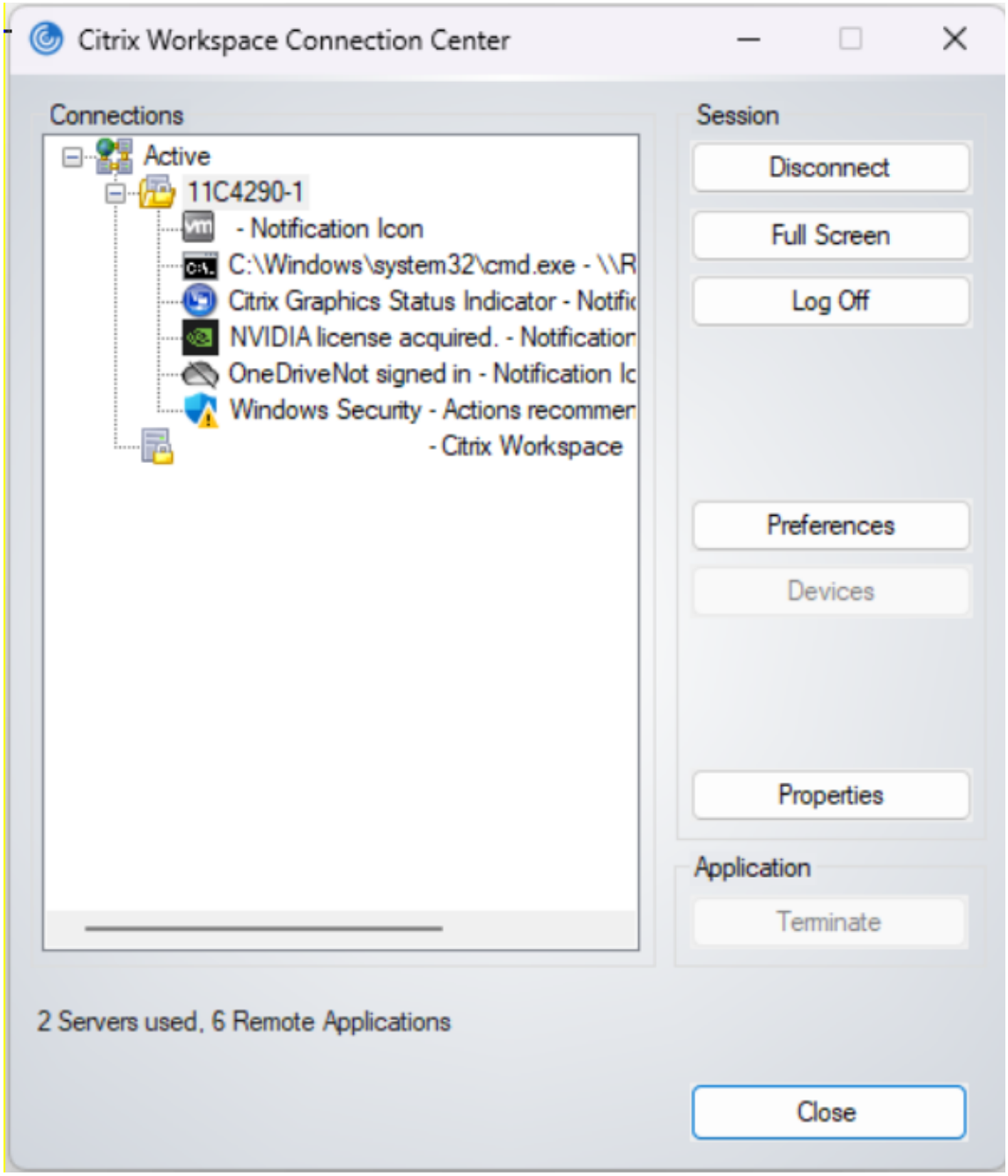
5. コマンドプロンプト公開アプリケーションを開きます。



コマンドプロンプトアプリが Citrix Workspace に表示されます。



6. クライアントで コネクションセンターを開きます。これは、開いているシームレスアプリを閉じた後にセッションがサインアウトされた場合、監視するために使用されます。次の画像では、コマンド プロンプトプロセス`c:\Windows\system32\cmd.exe`がリモート VDI でアクティブになっていることがわかります。



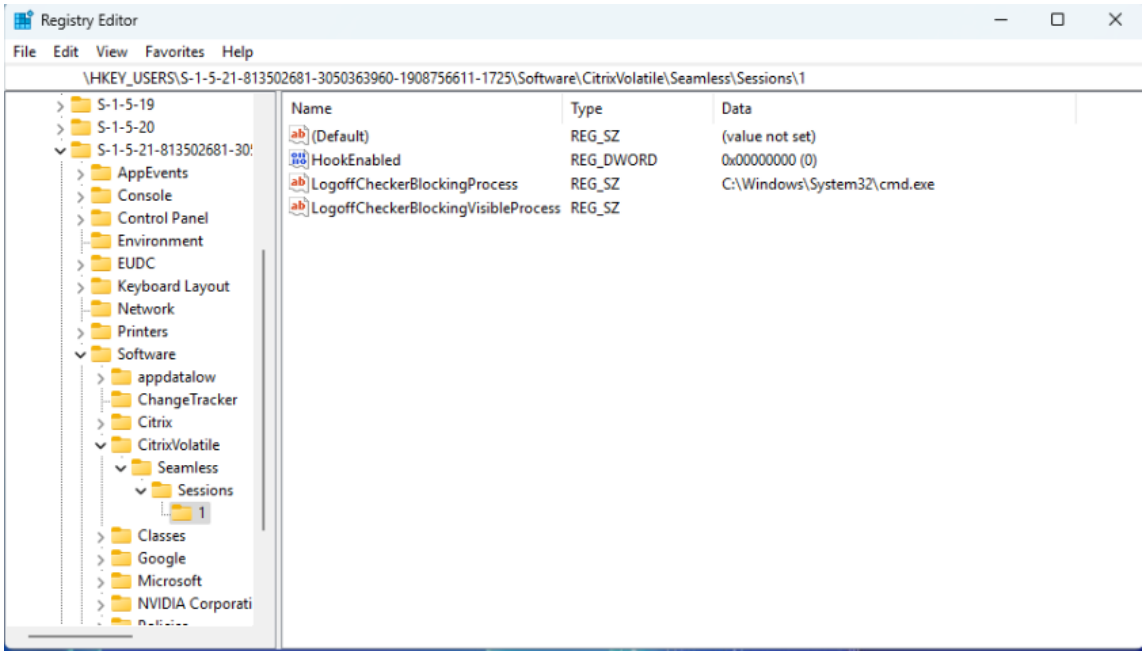
7. **regedit** が実行されている VDA から、次のリモート IP の場所に移動します：
   `HKEY_USERS\S-1-X-XX-XXXXXXXX-XXXXXXXXXX-XXXXXXXXXX-XXXX\SOFTWARE\CitrixVolatile\Seamless\Sessions\X\`

   > **Note:**
   >
   > This path changes every time you open a new session.

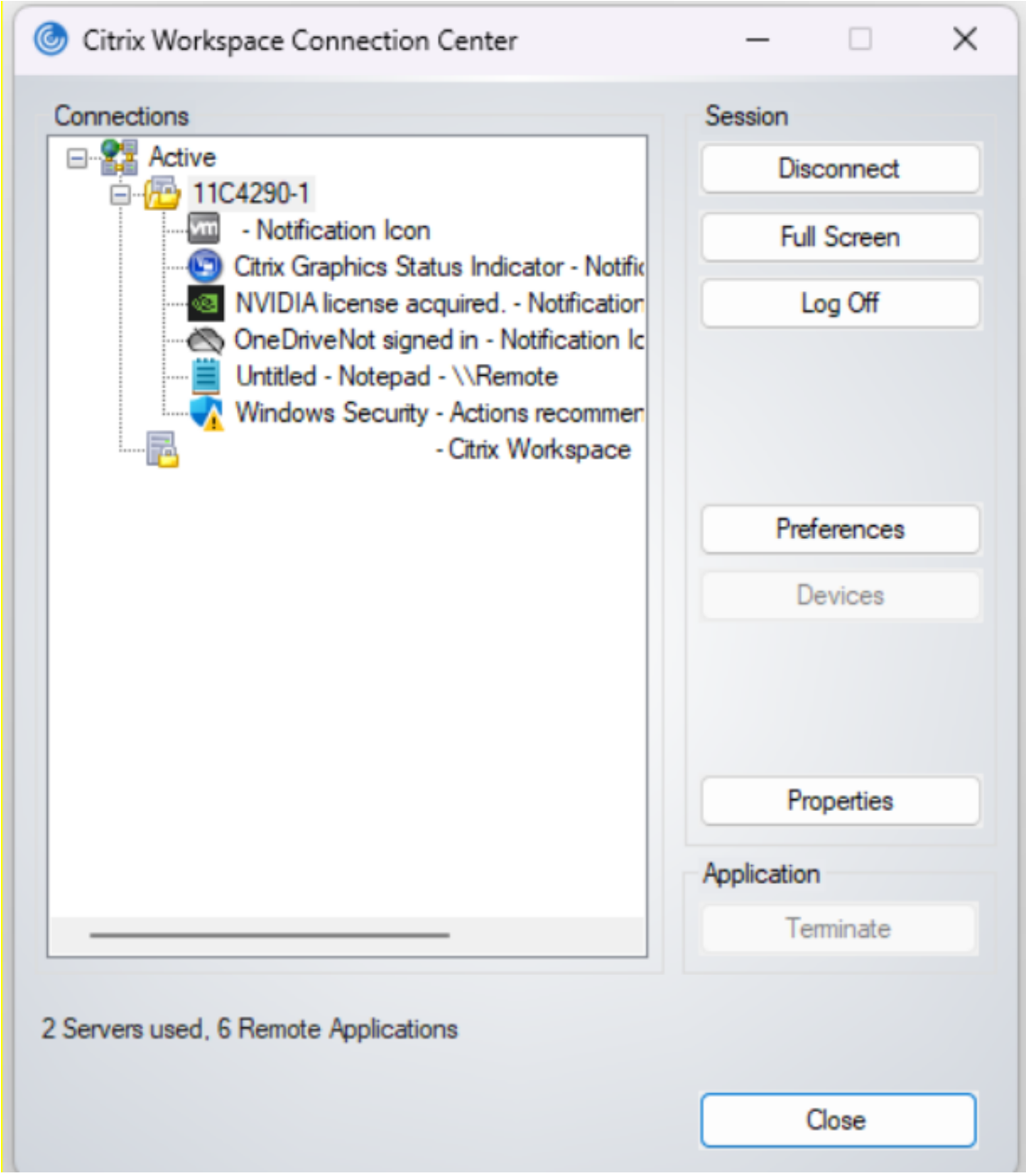
8. ここに読み取る 2 つのキーがあります（これらをここで変更しないでください）：**LogoffCheckBlockingProcess** および **LogoffCheckerBlockingVisibleProcess**。これらのキーは、サインアウトをブロック

しているプログラムを表示します。最初のキーでは開いていてまだ閉じられていない、`C:\Windows\System32\cmd.exe`が表示される必要があります。

> 注:
>
> **LogoffCheckBlockingProcess** および **LogoffCheckerBlockingVisibleProcess** は手動で編集しないでください。これらのレジストリ値を手動で編集すると、セッションが不安定になる可能性があります。

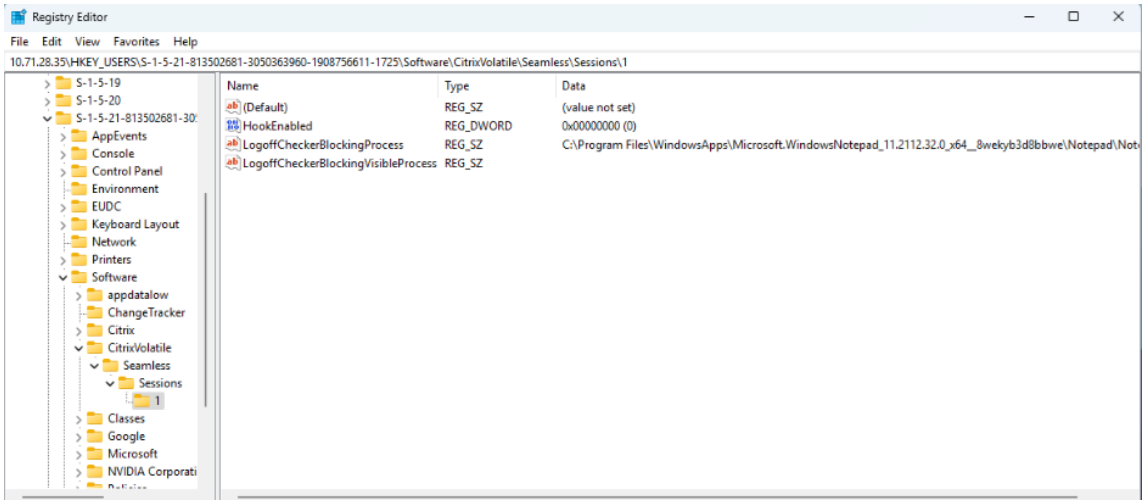


9. **Seamless CMD** を終了するには、右上隅の ［**X**］をクリックします。
10. コネクションセンターをチェックして、セッションが終了しているかどうかを確認します。終了までに最大 30 秒かかる場合があります。終了すると、正常なサインアウトを妨げるアプリケーションやプロセスは存在しなくなります。



11. セッションが終了しなかった場合は、F5 キーを押して **regedit** の出力を更新します。
12. **LogoffCheckBlockingProcess** と **LogoffCheckerBlockingVisibleProcess** の内容を再度確認します。CMD はもう存在していない一方で、別のプロセスが表示されているはずです。現在セッションのサインアウトをブロックしているプロセスがここに表示されます。

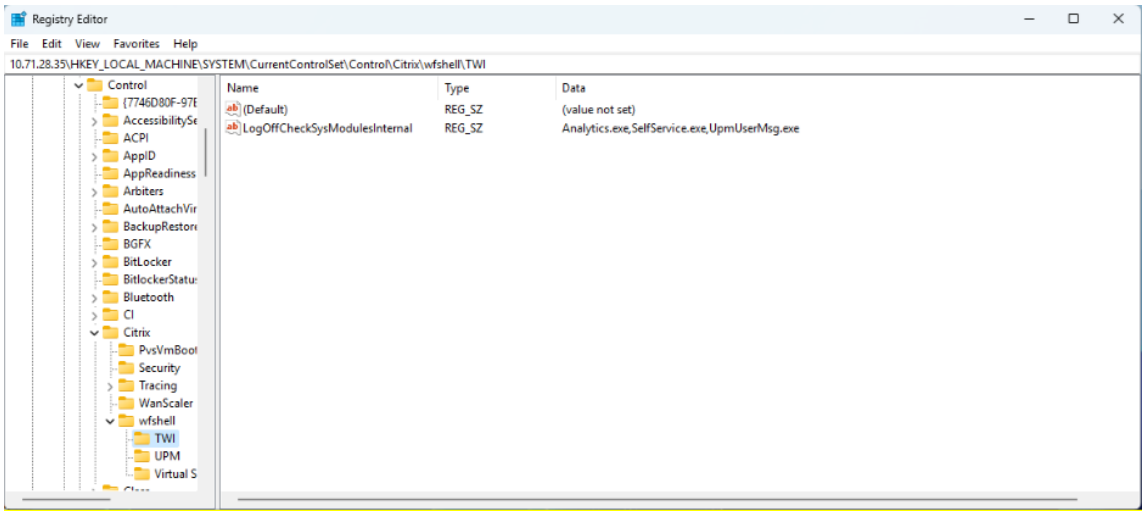
    この場合、コマンドプロンプトが閉じられる前に、公開されたコマンドプロンプトから **Notepad.exe** が開かれており、このリモートメモ帳プロセスが正常なサインアウトを妨げています。



13. この実行可能ファイルへのパスと、それがどのキーに出現したかをメモし、それをリモートツリーの下の次のレジストリキーに入力します:

    - **LogoffCheckBlockingProcess** に表示される場合:HKLM\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWILogoffCheckSysModulesInternal
    - **LogoffCheckerBlockingVisibleProcess** に表示される場合:HKLM\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWILogoffCheckVisibleSysModules

    > 注:
    >
    > キーに既に 1 つ以上のエントリがある場合は、最後にコンマを追加し、コンマの後に新しいエントリを配置します。



14. クライアントのコネクションセンターでセッションからサインアウトし、リモートアプリケーションを再度開きます。
15. リモートアプリケーションを閉じてから 30 秒以内にセッションが自動的にサインアウトされるまで、手順 9～16 を繰り返します。

> 注:
>
> トラブルシューティングが完了したら、一時的なファイアウォールの変更を元に戻し、必要に応じてリモートレジストリアクセスを許可できるようにします。

公開アプリケーションを開いたときに **Windows** の免責事項メッセージをフルサイズで表示するように **LogonUI** を変更する方法

認証パススルーが発生しないシナリオで、**LogonUI** ウィンドウのスケーリングが向上しました。**LogonUI** ウィンドウは、使用されているモニターの解像度と DPI 設定に基づいて拡大縮小され、クリッピングされることなく **LogonUI** ウィンドウ全体が表示されます。

ウィンドウサイズ（ピクセル単位）は、レジストリで手動で設定することもできます。

1. [ファイル名を指定して実行] コマンドで`regedit`を使用してレジストリエディターを起動します。
2. `HKEY_LOCAL_MACHINE\Software\Citrix\CtxHook\AppInit_DLLS\Seamless Hook\`に移動します。
3. 2 つの新しい DWORD キーを作成します：**LogonUIWidth** と **LogonUIHeight**。
4. キーの値を、**LogonUI** ウィンドウに必要な幅と高さ（ピクセル単位）に設定します。

   LogonUI ウィンドウのサイズを手動で設定すると、自動スケーリングは無効になります。

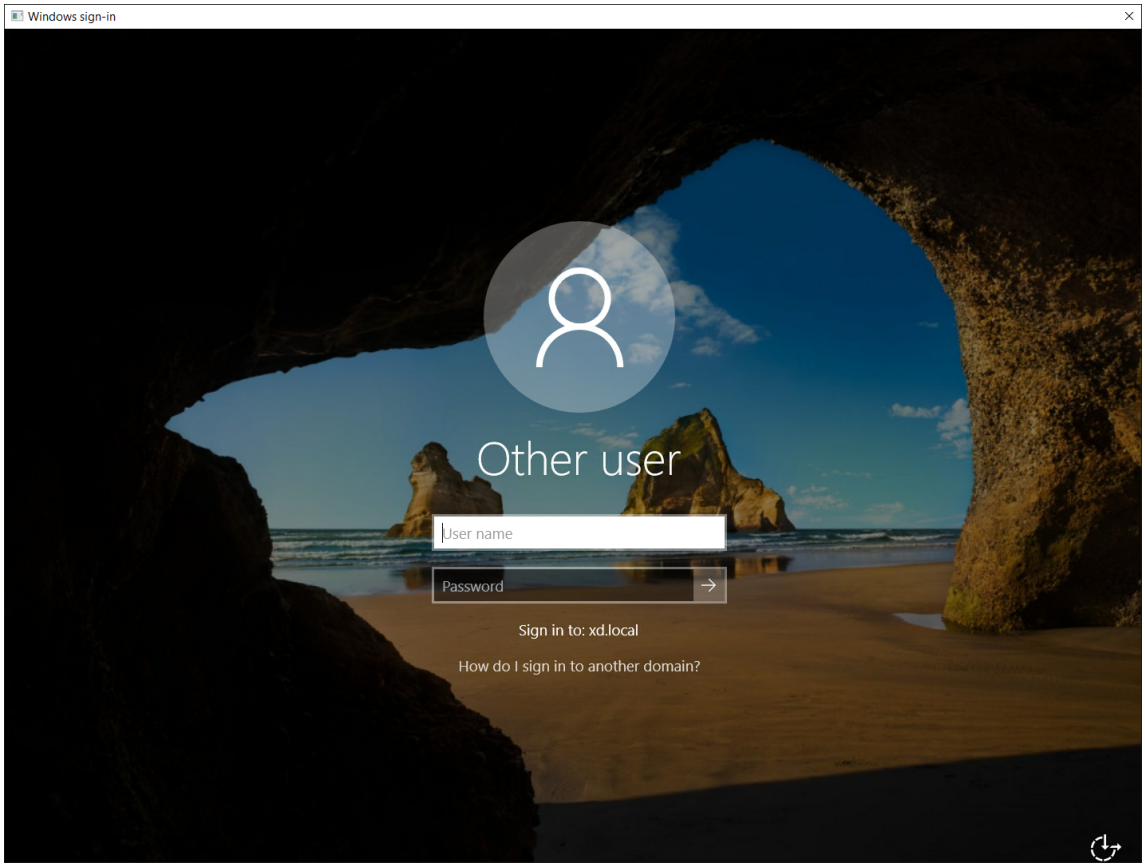
> 注:
>
> これらのレジストリパスは 2407 以降から変更されています。古いレジストリ値は無視され、非推奨となります。

デフォルトでは、**LogonUI** ウィンドウには閉じるボタン付きのタイトルバーが含まれており、エンドユーザーは必要に応じてセッションから切断できます。

タイトルバーを無効にする

次のレジストリキーを使用して、**LogonUI** ウィンドウのタイトルバーを無効にすることができます:

1. [ファイル名を指定して実行] コマンドで`regedit`を使用してレジストリエディターを起動します。
2. `HKEY_LOCAL_MACHINE\Software\Citrix\CtxHook\AppInit_DLLS\Seamless Hook\`に移動します。
3. 新しい DWORD キー **LogonUICaption** を作成し、キーの値を`0`に設定します。



アプリケーションフォルダーの管理

デリバリーグループに追加した新しいアプリケーションは、デフォルトで **Applications** という名前のフォルダーに配置されます。デリバリーグループの作成時、アプリケーションの追加時、またはその後で、別のフォルダーを指定することもできます。

ヒント:

- 「アプリケーション」フォルダーの名前を変更したり、「アプリケーション」フォルダーを削除したりすることはできません。ただし、「アプリケーション」フォルダー内のすべてのアプリケーションを、作成済みの別のフォルダーに移動することは可能です。
- フォルダー名は、1～64 文字とすることができます。スペースを使用できます。
- フォルダーは 5 レベルまで入れ子にできます。
- フォルダーにアプリケーションを含める必要はありません。空のフォルダーは許可されます。
- フォルダーは、移動したり作成時に別の場所を指定したりしない限り、Web Studio でアルファベット順に表示されます。
- 親フォルダーが異なる限り、同じ名前の子フォルダーを作成できます。同様に、保存先フォルダーが異なる限り、同じ名前のアプリケーションを作成できます。
- フォルダー内のアプリケーションを表示するには、[`View Applications`] 権限が必要です。また、ア

プリケーションを含むフォルダーを移動、名前変更、または削除するには、フォルダーに含まれるすべてのアプリケーションに対する［Edit Application Properties］権限が必要です。

- 以下の手順の大半で、Web Studio の操作バーを使用した操作が求められます。また、右クリックメニューやドラッグも使用できます。たとえば、意図しない場所にフォルダーを作成または移動した場合は、正しい場所にドラッグアンドドロップできます。

アプリケーションのフォルダーを管理するには、左側のペインで ［アプリケーション］を選択します。次の一覧を参考にしてください。

- すべてのフォルダー（サブフォルダーを除く）を表示するには：フォルダー一覧の上にある ［すべて表示］をクリックします。
- フォルダーを最上位レベルに作成する（サブフォルダーにしない）には：アプリケーションフォルダーを選択します。**Applications**（アプリケーション）フォルダー以外の既存のフォルダー内にフォルダーを配置するには、その既存のフォルダーを選択します。次に、操作バーで ［フォルダーの作成］を選択します。名前を入力してください。
- フォルダーを移動するには：目的のフォルダーを選択し、操作バーで ［フォルダーの移動］を選択します。サブフォルダーを持つフォルダーを除き、一度に複数のフォルダーを移動することはできません。（フォルダーを移動する最も簡単な方法は、フォルダーをドラッグすることです。）
- フォルダー名を変更するには：目的のフォルダーを選択し、操作バー ［フォルダー名の変更］を選択します。名前を入力してください。
- フォルダーを削除するには：目的のフォルダーを選択し、操作バーで ［フォルダーの削除］を選択します。アプリケーションやサブフォルダーを含んでいるフォルダーを削除すると、それらのアプリケーションやサブフォルダーも削除されます。アプリケーションを削除すると、そのアプリケーションの割り当てがデリバリーグループから削除されます。マシンからは削除されません。
- アプリケーションをフォルダーに移動するには：アプリケーションを 1 つまたは複数選択します。次に、操作バーで ［アプリケーションの移動］を選択します。移動先のフォルダーを選択します

また、デリバリーグループまたはアプリケーショングループを作成するとき、［アプリケーション］ページで、追加するアプリケーションをフォルダーに配置することもできます。追加したアプリケーションは、デフォルトでは **Applications** フォルダー内に配置されます。［変更］をクリックして、フォルダーを選択または作成します。

公開デスクトップ上のアプリケーションのローカル起動を制御する

ユーザーが公開デスクトップで公開アプリケーションを起動する場合、そのデスクトップセッションでアプリケーションを起動するのか、公開アプリケーションとして起動するのかを制御できます。Citrix Workspace アプリは、VDA の Windows レジストリでアプリケーションのインストールパスを検索し、存在する場合はアプリケーションのローカルインスタンスを起動します。それ以外の場合は、アプリケーションのホストされたインスタンスを起動します。VDA にインストールされていないアプリケーションを起動すると、ホストされているアプリケーションが起動します。詳しくは、「vPrefer 起動」を参照してください。

この操作は、PowerShell（Citrix Cloud 環境の場合はリモート PowerShell SDK、オンプレミス環境の場合は PowerShell SDK）で変更できます。

`New-Broker`アプリケーションまたは`Set-BrokerApplication`コマンドレットで、`LocalLaunchDisabled`オプションを使用します。例:

```
Set-BrokerApplication -LocalLaunchDisabled <Boolean>
```

デフォルトでは、このオプションの値は false（`-LocalLaunchDisabled $false`）です。公開デスクトップ内で公開アプリケーションを起動すると、そのデスクトップセッションでアプリケーションが起動されます。

オプションの値を true（`-LocalLaunchDisabled $true`）に設定すると、公開アプリケーションが起動します。この場合、公開されたデスクトップ（Windows 向け Citrix Workspace アプリを使用）で、公開アプリケーションとの別の追加セッションが作成されます。

要件および制限:

- アプリケーションの`ApplicationType`値は`HostedOnDesktop`である必要があります。
- このオプションは、適切な PowerShell SDK でのみ使用できます。Web Studio のグラフィカルユーザーインターフェイスでは現在使用できません。
- このオプションを使用するには、最低でも StoreFront 3.14、Citrix Receiver for Windows 4.11、および Delivery Controller 7.17 が必要です。

アプリパッケージ

August 17, 2024

> 注:
>
> Web Studio（Web ベース）と Citrix Studio（Windows ベース）の 2 つの管理コンソールを使用して、Citrix Virtual Apps and Desktops の展開を管理できます。この記事では Web Studio のみを扱います。Citrix Studio について詳しくは、Citrix Virtual Apps and Desktops 7 2212 以前の同様の記事を参照してください。

Microsoft は、アプリケーションを配信するために、次の 3 つのパッケージ化テクノロジを提供しています: App-V、MSIX、および MSIX アプリのアタッチ。ここでは、**Web Studio >** ［アプリパッケージ］を使用してこれらのパッケージアプリケーションを展開および配信する方法について説明します:

- App-V アプリケーションの展開および配信
- MSIX および MSIX アプリのアタッチアプリケーションの展開と配信

App-V アプリケーションの展開および配信

このセクションでは、次の情報について説明します:

- 概要。App-V パッケージを配布および管理するための管理方法について説明します。
- 手順。これらのパッケージを展開および配信する手順を提供します。

概要

このセクションでは、App-V パッケージを配布および管理するための管理方法について説明します。App-V パッケージアプリケーションの配信時に対話するコンポーネントと概念について詳しくは、Microsoft のドキュメントを参照してください：https://docs.microsoft.com/en-us/windows/application-management/app-v/appv-for-windows。

次の方法を使用して、App-V パッケージを配布および管理できます：

- デュアル管理。アプリケーションパッケージは、App-V サーバーで構成および管理されます。Citrix Virtual Apps and Desktops と App-V サーバーは連携して、パッケージを配信および管理します。

  この方法では、Citrix Virtual Apps and Desktops が、App-V サーバーの状態を示すスナップショットビューを定期的に更新する必要があります。これにより、ハードウェア、インフラストラクチャ、および管理にオーバーヘッドが生じます。Citrix Virtual Apps and Desktops と App-V サーバーは、特にユーザーの権限においては、同期されたままである必要があります。

  デュアル管理は、App-V と利用環境が緊密に連携している環境で最適に機能します：

  - **App-V** 管理サーバー。App-V パッケージと動的構成ファイルのライフサイクルを公開および管理します。
  - VDA マシンにインストールされた **Citrix Personalization** コンポーネント。アプリケーションの起動に必要な、適切な App-V 公開サーバーの登録を管理します。

  この方式によって、App-V 公開サーバーは適切なタイミングでユーザーに対して同期されます。公開サーバーは、ログオングループや接続グループの更新など、パッケージのライフサイクルにおけるさまざまな面を維持します。

- シングル管理。アプリケーションパッケージはネットワーク共有に保存されます。Citrix Virtual Apps and Desktops は、パッケージを個別に配信および管理します。

  この方式では、環境に App-V サーバーとデータベースインフラストラクチャが必要ないため、オーバーヘッドが削減されます。

  この方式では、App-V パッケージをネットワーク共有に保存し、そのメタデータをその場所から利用環境にアップロードします。VDA マシンにインストールされた Citrix Personalization コンポーネントは、次のようにアプリケーションを管理および配信します：

  - アプリケーションの起動時に、展開の構成ファイルとユーザー構成ファイルを処理します。
  - ホストマシン上のパッケージのライフサイクルに関するすべての面を管理します。

両方の管理方式を同時に使用することもできます。つまり、アプリケーションをデリバリーグループに追加する場合、App-V サーバーまたはネットワーク共有にある App-V パッケージからアプリケーションを追加できます。

> 注:
>
> 両方の管理方式を同時に使用しており、App-V パッケージで両方の場所に動的構成ファイルがある場合は、App-V サーバーのファイル（デュアル管理）が使用されます。

手順

App-V アプリケーションの配信をサポートするには、VDA マシンに Citrix Personalization コンポーネントをインストールする必要があります。詳しくは、「VDA マシンへの Citrix Personalization コンポーネントのインストール」を参照してください。

App-V パッケージアプリケーションをユーザーに配信するには、次の手順に従います:

1. アプリケーションパッケージをネットワーク共有に保存する。
2. アプリケーションパッケージを環境にアップロードする。
3. デリバリーグループにアプリケーションを追加する。
4. 相互依存する App-V パッケージの自動配信を有効にするには、分離グループを作成します。

Citrix Virtual Apps and Desktops がシングル管理方式で App-V 動的構成ファイルを認識し、適用できるようにするには、こちらのCitrix ブログを参照してください。

MSIX および MSIX アプリのアタッチアプリケーションの展開と配信

このセクションでは、次の情報について説明します:

- 概要。MSIX および MSIX アプリのアタッチパッケージを、配信および管理する方法について説明します。
- 手順。これらのパッケージを展開および配信する手順を提供します。

概要

Citrix Virtual Apps and Desktops は、VDA マシンにインストールされた Citrix Personalization コンポーネントを介して、MSIX および MSIX アプリのアタッチアプリケーションをユーザーに提供します。このコンポーネントは、ホストマシン上のパッケージのライフサイクルに関するすべての面を管理します。

MSIX および MSIX アプリのアタッチについて詳しくは、Microsoft のドキュメント（それぞれhttps://docs.microsoft.com/en-us/windows/msix/およびhttps://docs.microsoft.com/en-us/azure/virtual-desktop/what-is-app-attach）を参照してください。

手順

MSIX および MSIX アプリのアタッチパッケージの配信をサポートするには、VDA マシンに Citrix Personalization コンポーネントをインストールする必要があります。詳しくは、「VDA マシンへの Citrix Personalization コンポー

ネントのインストール」を参照してください。

MSIX および MSIX アプリのアタッチパッケージアプリケーションをユーザーに配信するには、次の手順に従います:

1. アプリケーションパッケージをネットワーク共有に保存する。
2. アプリケーションパッケージを環境にアップロードする。
3. デリバリーグループにアプリケーションを追加する。

VDA マシンへの Citrix Personalization コンポーネントのインストール

Citrix Personalization コンポーネントは、App-V、MSIX、および MSIX アプリのアタッチ形式のアプリケーションパッケージの公開プロセスを管理します。VDA をインストールする場合、このコンポーネントはデフォルトではインストールされません。VDA のインストール中またはインストール後にコンポーネントをインストールできます。

VDA のインストール中にコンポーネントをインストールするには、次のいずれかの方法を使用します:

- インストールウィザードで、[追加コンポーネント] ページに移動してから、[**Citrix Personalization for App-V - VDA**] チェックボックスをオンにします。
- コマンドラインインターフェイスの場合は、「**/includeadditional** "**Citrix Personalization for App-V –VDA**"」オプションを使用します。

VDA のインストール後にコンポーネントをインストールするには、次の手順に従います:

1. VDA マシンで、[コントロールパネル] **>** [プログラム] **>** [プログラムと機能] に移動し、[**Citrix Virtual Delivery Agent**] を右クリックして [変更] を選択します。
2. ウィザードが表示されたら、[追加コンポーネント] ページに移動し、[**Citrix Personalization for App-V - VDA**] チェックボックスをオンにします。

> 注:
>
> Microsoft App-V デスクトップクライアントは、ユーザーデバイス上の App-V パッケージから仮想アプリケーションを実行するコンポーネントです。Windows 10 (1607 以降)、および Windows Server 2019 には、この App-V クライアントソフトウェアが既に組み込まれています。VDA マシンでオンにするだけで使用できます。詳しくは、こちらの Microsoft 社のドキュメントを参照してください: https://docs.microsoft.com/en-us/windows/application-management/app-v/appv-enable-the-app-v-desktop-client。

アプリケーションパッケージをネットワーク共有に保存する

インフラストラクチャをセットアップした後、アプリケーションパッケージを生成し、それらを UNC または SMB ネットワーク共有などのネットワークの場所、または Azure ファイル共有に保存します。

詳細な手順は次のとおりです:

1. アプリケーションパッケージを生成します。詳しくは、Microsoft 社のドキュメントを参照してください。
2. アプリケーションパッケージをネットワークの場所に保存します:
   - **App-V** のシングル管理の場合: パッケージとそれに対応する動的構成ファイル（App-V）を UNC または SMB ネットワーク共有、または Azure ファイル共有に保存します。
   - **App-V** のデュアル管理の場合: UNC パスから App-V 管理サーバーにパッケージを公開します。(HTTP URL からの公開はサポートされていません。)
   - **MSIX** または **MSIX** アプリのアタッチの場合: パッケージを UNC または SMB ネットワーク共有、または Azure ファイル共有に保存します。
3. VDA にパッケージストレージパスの読み取り権限があることを確認してください:
   - AD ドメインの UNC または SMB ネットワーク共有にパッケージを保存する場合は、VDA マシンにストレージパスへの読み取り権限を付与します。これを行うには、マシンの AD アカウントに共有への読み取り権限を明示的に付与するか、その権限を持つ AD グループにアカウントを含めることができます。
   - パッケージを Azure ファイル共有に保存する場合は、最初にユーザーアカウントに Azure のストレージパスへの読み取り権限を付与します。次に、そのユーザーアカウントを使用してパッケージストレージパスにアクセスするように VDA マシンで実行される`ctxAppVService`を構成します。手順について詳しくは、以降のセクションを参照してください。

ユーザーログオンアカウントの変更

VDA は`ctxAppVService`を呼び出して、パッケージストレージパスにアクセスします。デフォルトでは、`ctxAppVService`はマシンのローカルシステムアカウントを使用してパッケージストレージパスにアクセスします。この種類のマシン認証は、AD ドメインで機能します。ただし、ユーザーアカウントベースの認証が必要となる AD と Azure AD との統合シナリオでは機能しません。

パッケージを Azure ファイル共有に保存する場合は、`ctxAppVService`のログオンアカウントをパッケージストレージパスへの読み取り権限があるユーザーアカウントに変更します。詳細な手順は次のとおりです:

1. [サービス] を起動し、**ctxAppVService** を右クリックして、[プロパティ] を選択します。
2. [ログオン] タブで、[このアカウント] を選択し、パッケージストレージパスへの読み取り権限があるユーザーアカウントを入力してから、ユーザーのパスワードを 2 回入力します。
3. [**OK**] をクリックします。

アプリケーションパッケージを環境にアップロードする

必要に応じてアプリケーションパッケージをネットワークの場所に保存したら、それらを環境にアップロードして配信します。必要に応じて、次のいずれかの方法を使用します:

- 一括アップロード
- 1 つずつアップロード

準備

Citrix Virtual Apps and Desktops は、VDA マシンを使用して、パッケージ検出用のネットワークの場所への接続をセットアップします。したがって、事前にデリバリーグループを作成し、グループ内の 1 つ以上の VDA が次の要件を満たしていることを確認してください:

- VDA バージョン:
  - App-V パッケージを検出する場合:2203 以降
  - MSIX および MSIX アプリのアタッチパッケージを検出する場合:2209 以降
- Citrix Personalization for App-V コンポーネント:インストール済み
- パッケージの場所での権限:読み取り(手順 2 のアプリケーションパッケージをネットワーク共有に保存するを参照してください。)
- 電源:オン
- 状態:登録済み

アプリケーションパッケージの一括アップロード

ネットワークの場所にあるパッケージを環境にアップロードします。アップロードする前に、次のアイテムの準備ができていることを確認してください:

- 「準備」に記載されている要件を満たすデリバリーグループ
- ネットワークの場所のパス

パッケージを一括でアップロードするには、次の手順に従います:

1. 左側のペインで、[アプリパッケージ]を選択します。
2. [ソース]タブで、[追加]ボタンをクリックします。[ソースの追加]ページが表示されます。
3. [名前]フィールドに、わかりやすいパッケージソースの名前を入力します。
4. [デリバリーグループ]フィールドで、[デリバリーグループの選択]をクリックします。次に、「準備」に記載されている要件を満たすデリバリーグループを選択し、[**OK**]をクリックします。
5. [場所の種類]フィールドで、パッケージの保存場所に基づいて [**Microsoft App-V** サーバー]または [ネットワーク共有]を選択し、それに対応する設定を構成します:
   - [**Microsoft App-V** サーバー]を選択した場合は、次の情報を入力します:
     - 管理サーバーの URL。例:`http://appv-server.example.com`
     - 管理サーバー管理者のログイン資格情報。

- 公開サーバーの URL とポート番号。例: `http://appv-server.example.com:3330`

- ［ネットワーク共有］を選択した場合は、次の情報を指定します:
  - ネットワーク共有の UNC パスを入力します。例: `\\Package-Server\apps\`
  - アップロードするパッケージの種類を選択します。オプションには、App-V、MSIX、MSIX アプリのアタッチがあります。
  - サブフォルダーでパッケージを検索するかどうかを指定します。

6. ［ソースの追加］をクリックします。

   ［ソースの追加］ページが閉じ、新しく追加されたソースがソース一覧に表示されます。Citrix Virtual Apps and Desktops は、デリバリーグループの VDA を使用してパッケージを環境にアップロードします。アップロードが完了すると、［ステータス］フィールドに「インポート成功」と表示されます。対応するパッケージが［パッケージ］タブに表示されます。

   > 注:
   >
   > ソースの場所でパッケージの更新を確認して環境にインポートするには、ソース一覧で場所を選択し、［パッケージの更新の確認］をクリックします。

アプリケーションパッケージを **1** つずつアップロード

ネットワーク共有から環境にアプリケーションパッケージをアップロードします。アップロードする前に、次のアイテムの準備ができていることを確認してください:

- 「準備」に記載されている要件を満たすデリバリーグループ
- ネットワークの場所のパス。

パッケージを環境にアップロードするには、次の手順に従います:

1. 左側のペインで、［アプリパッケージ］を選択します。
2. ［パッケージ］タブで、［パッケージの追加］ボタンをクリックします。［パッケージの追加］ページが開きます。
3. ［デリバリーグループ］フィールドで、［デリバリーグループの選択］をクリックします。次に、「準備」に記載されている要件を満たすデリバリーグループを選択し、［**OK**］をクリックします。
4. ［パッケージの完全パス］フィールドに、必要に応じてパスを入力します:

   - 一度に複数のパッケージをアップロードするには、セミコロン（`;`）で区切って完全パスを入力します。例: `\\Package-Server\apps\office365.appv;\\Package-Server\apps\skype.msix;\\Package-Server\apps\slack.vhd`
   - ネットワーク共有にあるすべてのパッケージをアップロードするには、ストレージパスを入力します。例: \package-Server\apps\

5. ［パッケージの追加］をクリックします。

   アプリケーションパッケージが ［パッケージ］タブに表示されます。

デリバリーグループへのアプリケーションの追加

アプリケーションパッケージが完全にアップロードされたら、必要に応じてそのアプリケーションを 1 つまたは複数のデリバリーグループに追加します。これらのデリバリーグループに関連付けられているユーザーは、アプリケーションにアクセスできるようになります。

パッケージ内の 1 つまたは複数のアプリケーションを複数のデリバリーグループに追加するには、次の手順に従います:

1. 左側のペインで、[アプリパッケージ] を選択します。
2. [パッケージ] タブで、必要に応じてパッケージを選択します。
3. 操作バーで、[デリバリーグループの追加] をクリックします。[デリバリーグループの追加] ページが開きます。
4. 必要に応じてパッケージ内の 1 つまたは複数のアプリケーションを選択し、[次へ] をクリックします。
5. デリバリーグループ一覧で、アプリケーションを割り当てるグループを選択し、[次へ] をクリックします。
   注: MSIX または MSIX アプリのアタッチパッケージを選択した場合、機能レベルが 2106 以降のデリバリーグループのみが一覧に表示されます。
6. [完了] をクリックします。

以下を実行する際に、パッケージアプリケーションをデリバリーグループに追加することもできます:

- デリバリーグループを作成する。詳しくは、「デリバリーグループの作成」を参照してください。
- 既存のデリバリーグループまたはアプリケーショングループを編集する。詳しくは、「アプリケーションの追加」を参照してください。

(オプション) **App-V** パッケージの分離グループの作成

分離グループを作成し、相互依存する App-V パッケージの自動配信を有効にできます。

> 注:
>
> 分離グループは、App-V のシングル管理方式でサポートされています。App-V のデュアル管理方式を使用している場合は、Microsoft App-V インフラストラクチャで接続グループを作成することで同じ目的を達成できます。詳しくは、こちらの Microsoft 社のドキュメントを参照してください: https://docs.microsoft.com/en-us/windows/application-management/app-v/appv-connection-group-file。

分離グループについて

分離グループは、仮想環境を作成するために同じ Windows サンドボックスで実行する必要がある相互依存するアプリケーションパッケージのコレクションです。Citrix App-V 分離グループは、App-V 接続グループと似ていますが同じではありません。分離グループには、次の 2 種類のパッケージが含まれます:

- **Explicit**（明示的な）アプリケーションパッケージ。特定のライセンス要件があるアプリケーション。これらのアプリケーションをデリバリーグループに追加することで、これらのアプリケーションを特定の範囲のユーザーに制限できます。
- **Automatic**（自動）アプリケーションパッケージ。デリバリーグループに追加されているかどうかに関係なく、すべてのユーザーが常に使用できるアプリケーション。

たとえば、アプリケーションapp-aを実行するには JRE 1.7 が必要です。app-a（「*Explicit*」とマークされている）と JRE 1.7（「*Automatic*」とマークされている）を含む分離グループを作成できます。次に、app-aの App-V パッケージを 1 つまたは複数のデリバリーグループに追加します。ユーザーが app-a を実行すると、JRE 1.7 が自動的に app-a で展開されます。

ユーザーが分離グループで *Explicit* とマークされた App-V アプリケーションを起動すると、Citrix Virtual Apps and Desktops はデリバリーグループ内のアプリケーションへのユーザーのアクセス権限を確認します。ユーザーがそのアプリケーションにアクセスする権限を持っている場合、ユーザーは同じ分離グループ内のすべての *Automatic* アプリケーションパッケージを使用できます。

Automatic パッケージをデリバリーグループに追加する必要はありません。分離グループに別の *Explicit* アプリケーションパッケージがある場合、そのパッケージは、同じデリバリーグループにある場合にのみユーザーが使用できます。

分離されたグループについて詳しくは、こちらのCitrix ブログを参照してください。

App-V 分離グループの作成　分離グループを作成し、相互依存するアプリケーションパッケージを追加します。詳細な手順は次のとおりです：

1. ［分離グループ］タブで、［分離グループの追加］をクリックします。
2. 分離グループの名前と説明を入力します。環境内のすべてのアプリケーションパッケージが ［使用可能なパッケージ］一覧に表示されます。
3. ［使用可能なパッケージ］一覧から、必要に応じたアプリケーションを選択し、右矢印をクリックします。選択したアプリケーションが ［分離グループ内のパッケージ］一覧に表示されます。
4. ［展開］フィールドで、そのアプリケーションに対して **Explicit**（明示的）または **Automatic**（自動）を選択します。
5. 手順 2～3 を繰り返して、さらにパッケージを追加します。
6. 一覧のパッケージの順序を変更するには、上矢印または下矢印をクリックします。
7. ［保存］をクリックします。

> 注：
>
> 分離グループの構成により、VDA 上に App-V 接続グループが作成されます。展開シナリオは複雑になる可能性があり、App-V クライアントは、1 つのアクティブな接続グループに同時に存在するパッケージをサポートします。同じデリバリーグループに追加された 2 つの異なる分離グループに、同じパッケージを追加しないことをお勧めします。

パッケージアプリケーションをシングルセッション **VDA** または共有デスクトップ **VDA** で公開

App-V、MSIX、および MSIX アプリアタッチのパッケージを、デリバリーグループを通じてシングルセッションまたは共有デスクトップ VDA セッションに直接配信できるようになりました。アプリケーションに設定されているアクセス権限に基づいて、サインイン時にデスクトップ VDA 上のパッケージアプリケーションにアクセスできます。

メリット

- アプリケーションはサインイン時に VDA で利用可能ですが、Workspace または StoreFront 経由でオンデマンドでステージングされることはありません。
- パッケージアプリケーションにアクセスするときの起動時間が短縮されました。
- VDA の基本イメージから分離され、パッケージアプリケーションの個別のメンテナンスを容易にします。

注意事項

- このオプションは、適切な PowerShell SDK によってシングルセッション VDA でのみ使用できます。現在、Web Studio ワークフローでは使用できません。共有デスクトップへの公開は、PowerShell SDK を使用して行うことも、Web Studio ワークフローを使用した既存の方法で行うこともできます。既存の手順について詳しくは、「デリバリーグループへのアプリケーションの追加」を参照してください。
- アプリケーションはデリバリーグループの一部である必要があります。

はじめに

- パッケージアプリケーションが署名済みで、ファイル共有で、または UNC の場所で利用できることを確認します。詳しくは、「アプリケーションパッケージをネットワーク共有に保存する」を参照してください。
- VDA マシンに Citrix Personalization コンポーネントをインストールします。

手順

パッケージアプリケーションをデスクトップ VDA に配信するには、次の手順を実行します:

1. アプリケーションパッケージを Web Studio にインポートする。
2. パッケージ化された BrokerApplication を公開する。
3. Web Studio でのアプリケーションの表示を制限する。

アプリケーションパッケージを **Web Studio** にインポートする

1. Web ブラウザーを開きます。「`https://<address of the server hosting Web Studio>/Citrix/Studio`」を入力します。

2. デリバリーグループを作成します。詳しくは、「デリバリーグループの作成」を参照してください。
3. アプリケーションパッケージを Web Studio にインポートします。詳しくは、「アプリケーションパッケージの一括アップロード」を参照してください。

パッケージ化された **BrokerApplication** を公開する

マルチセッション（共有）VDA またはシングルセッションのアプリケーション VDA に公開する場合、公開手順は変わりません。詳しくは、「デリバリーグループへのアプリケーションの追加」を参照してください。
シングルセッションのデスクトップ VDA に公開している場合は、次の手順を実行します:

Delivery Controller で、以下の PowerShell コマンドを実行します:

1. パッケージに存在するコマンドを取得するには:

   ```
   Import-Module "D:\Support\Tools\Scripts\Citrix.Cloud.AppLibrary.Admin.v1.psm1"
   ```

   > 注:
   >
   > この機能をサポートするApp-V **package** discovery moduleのバージョンは、上記のパスの Citrix Virtual Apps and Desktops ISO（2311 以降のバージョン）にあります。

2. 関連するデリバリーグループ ID とパッケージアプリケーション ID を取得するには、次の手順を実行します:

   ```
   Get-BrokerDesktopGroup | Format-Table Uid, Name
   Get-AppLibAppVApplication | Format-Table Uid, Name
   ```

3. パッケージを公開し、適切な BrokerMachineConfigurations を作成するには、次の手順を実行します:

   ```
   Publish-PackagedApplication -AppLibararyApplicationUid <AppLibararyApplica
   .Uid > -DesktopGroupUid <DesktopGroup.Uid>
   ```

4. 後で VDA 上の Broker Agent に送信される Broker 構成を同期するには、次の手順を実行します:

   ```
   Update-DesktopGroupMachineConfigurations -DesktopGroupUid <
   DesktopGroup.Uid>
   ```

   > 注:
   >
   > パッケージアプリケーションを VDA から公開または削除した後は、必ず PowerShell コマンドUpdate-DesktopGroupMachineConfigurationsを実行してください。

Web Studio でのアプリケーションの表示を制限する

デフォルトでは、ユーザーは、デスクトップセッションで利用可能な VDA を提供するデリバリーグループに割り当てられた、すべてのパッケージアプリケーションを利用できます。Web Studio でアプリケーションの表示を特定のユ

ーザーまたはグループに設定することで、デスクトップ VDA 上のパッケージアプリケーションの表示を制御できます。パッケージアプリケーションの表示を管理するには、「アプリケーションプロパティの変更」を参照してください。

ユニバーサル **Windows** プラットフォームアプリ

August 17, 2024

ユニバーサル Windows プラットフォーム（UWP）アプリについて詳しくは、以下の Microsoft 社のドキュメントを参照してください。

- ユニバーサル Windows プラットフォーム（UWP）アプリとは
- Windows パッケージマネージャー

要件および制限事項

Citrix Virtual Apps and Desktops は、次の Windows マシンで VDA での UWP アプリの使用をサポートしています:

- Windows 10 以降のバージョン
- Windows Server 2016 以降のバージョン

VDA のバージョンは 7.11 以上である必要があります。

以下の Citrix Virtual Apps and Desktops 機能は、UWP アプリの使用時にはサポートされないか、または制限されます:

- ファイルタイプの関連付けはサポートされません。
- ローカルアプリケーションアクセスはサポートされません。
- 動的プレビュー：セッションで実行中のアプリが重複している場合、プレビューにはデフォルトのアイコンが表示されます。動的プレビューに使用される Win32 API は、UWP アプリではサポートされません。
- アクションセンターリモート：UWP アプリでは、アクションセンターを使用して、セッションでメッセージを表示することができます。これらのメッセージは現在、エンドポイントにリダイレクトされてユーザーに表示されることはありません。

同じサーバーからの UWP アプリと非 UWP アプリの起動は、サポートされません。代わりに、UWP アプリと非 UWP アプリは別のデリバリーグループまたはアプリケーショングループに配置する必要があります。

マシンにインストールされる UWP アプリはすべて列挙されるため、Windows ストアへのユーザーアクセスを無効にすることをお勧めします。これにより、1 人のユーザーによってインストールされた UWP アプリが他のユーザーによってアクセスされるのを防ぐことができます。

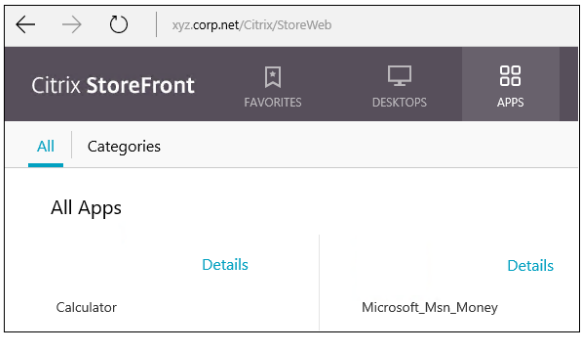
サイドローディングの実行中に、UWP アプリはマシンにインストールされ、他のユーザーが使用できるようになります。別のユーザーがアプリを起動すると、アプリがインストールされ、OS はその AppX データベースを更新して、そのユーザーによって「インストール済み」であることを示します。

固定ウィンドウまたはシームレスウィンドウで起動された公開 UWP アプリから正常にログオフすると、VDA セッションが終了せず、ユーザーが強制的にログオフされる場合があります。この問題が発生すると、VDA セッションに残っているいくつかのプロセスにより、セッションが適切に終了できなくなります。これを解決するには、CTX891671のガイダンスに従って、VDA セッションの終了を阻止しているプロセスを特定し、そのプロセスを「LogoffCheckSysModules」レジストリキーの値に追加します。

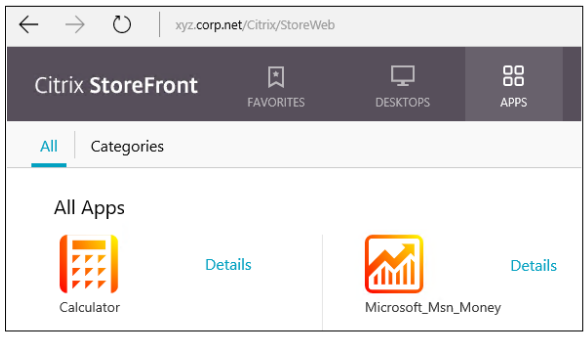
UWP アプリのアプリケーション表示名や説明の名前が正しくないことがあります。アプリケーションをデリバリーグループに追加するときに、これらのプロパティを編集および修正してください。

その他の問題については、「既知の問題」を参照してください。

現時点では、複数の UWP アプリに透過性が有効になった白いアイコンがありますが、これによって StoreFront のディスプレイの白い背景でアイコンが見えなくなるという問題があります。これを回避するために、背景の色を変更できます。たとえば、StoreFront マシンで、ファイル`C:\inetpub\wwwroot\Citrix\StoreWeb\custom\style.css`を編集します。このファイルの末尾に、「`.storeapp-icon { background-image: radial-gradient( circle at top right, yellow, red ); }`」を追加します。以下の図は、この例の編集前と編集後を示しています。



Before



After

Windows Server 2016 以降のバージョンでは、UWP アプリを起動するとサーバーマネージャーも起動されることがあるという問題がありました。この問題の発生を回避するには、`HKLM\Software\Microsoft\ServerManager\DoNotOpenServerManagerAtLogon`レジストリキーを使用して、ログオン時のサーバーマネージャーの自動起動を無効にします。詳しくは、https://blogs.technet.microsoft.com/rmilne/2014/05/30/how-to-hide-server-manager-at-logon/を参照してください。

UWP アプリのインストールと公開

UWP アプリのサポートは、デフォルトで有効になっています。

1 つまたは複数の UWP アプリを VDA（またはマスターイメージ）にインストールするには、以下のいずれかの方法を使用します:

- ビジネス向け Windows ストアからのオフラインインストールの完了、Deployment Image Servicing and Management（DISM）などのツールを使用した、アプリのデスクトップイメージへの展開。詳しくは、「Windows パッケージマネージャー」を参照してください。
- アプリのサイドロード。詳しくは、「Windows クライアントデバイスでの基幹業務（LOB）アプリのサイドロード」を参照してください。
- ビジネス向け Windows ストアから、目的のユーザーごとに UWP アプリを直接インストールします。

Citrix Virtual Apps または Citrix Virtual Desktops に UWP アプリを 1 つまたは複数追加（公開）するには、次の手順を実行します:

1. UWP アプリがマシンにインストールされたら、UWP アプリをデリバリーグループまたはアプリケーショングループに追加します。この処理は、グループの作成時、またはその後に行うことができます。[アプリケーション］ページの ［追加］メニューで、[［スタート］メニューから］を選択します。
2. アプリケーションの一覧が表示されたら、公開する UWP アプリを選択します。
3. ウィザードを先に進めるか、編集ダイアログを閉じます。

VDA でユニバーサルアプリを使用できないようにするには、`HKLM\Software\Citrix\VirtualDesktopAgent\FeatureToggle`に **EnableUWASeamlessSupport** レジストリ設定を追加して、**0** に設定します。

UWP アプリのアンインストール

UWP アプリを`Remove-AppXPackage`などのコマンドでアンインストールする場合、アイテムは管理者に対してのみアンインストールされます。アプリを起動して使用した可能性のあるユーザーのマシンからアプリを削除するには、各マシンで削除コマンドを実行します。すべてのユーザーのマシンから 1 つのコマンドで AppX パッケージをアンインストールすることはできません。

Autoscale

August 17, 2024

> 注:
>
> Web Studio（Web ベース）と Citrix Studio（Windows ベース）の 2 つの管理コンソールを使用して、Citrix Virtual Apps and Desktops の展開を管理できます。この機能は Web Studio でのみ使用できます。

Autoscale は、プロアクティブにマシンの電源を管理するための、一貫した、高性能なソリューションです。その目的は、コストとユーザーエクスペリエンスのバランスを取ることです。

Autoscale によって、デリバリーグループに登録されているすべてのシングルセッションおよびマルチセッション OS マシンの電源をプロアクティブに管理できます。

Autoscale 機能には、次が含まれます:

- スケジュールベースおよび負荷ベースの設定
- 動的セッションタイムアウト
- タグ付きマシンのオートスケール（クラウドバースト）
- ユーザーログオフ通知

サポートされる **VDA** ホストプラットフォーム

Autoscale は、Citrix Virtual Apps and Desktops がサポートするすべてのプラットフォームをサポートします。これには XenServer、Amazon Web Services、Google Cloud Platform、Microsoft Azure Resource Manager、VMware vSphere など、さまざまなインフラストラクチャプラットフォームが含まれます。サポート対象のプラットフォームの一覧については、Citrix Virtual Apps and Desktops の「システム要件」を参照してください。

> 注:
>
> パブリッククラウドホスト接続を展開環境に追加する場合は、ハイブリッド権利ライセンスが必要です。ハイブリッド権利ライセンスについては、「移行とトレードアップ（TTU）とハイブリッド権利」を参照してください。ライセンスの追加については、「サイトの作成」を参照してください。

サポートされるワークロード

Autoscale は、マルチセッション OS とシングルセッション OS の両方のデリバリーグループをサポートしています。考慮するユーザーインターフェイスは 3 種類です:

- マルチセッション OS のデリバリーグループ（旧 RDS デリバリーグループ）の Autoscale ユーザーインターフェイス
- シングルセッション OS のランダム（プールされた）デリバリーグループ（旧プールされた VDI デリバリーグループ）の Autoscale ユーザーインターフェイス
- シングルセッション OS の静的デリバリーグループ（旧静的 VDI デリバリーグループ）の Autoscale ユーザーインターフェイス

さまざまなデリバリーグループのユーザーインターフェイスについて詳しくは、「Autoscale ユーザーインターフェイス」を参照してください。

メリット

Autoscale 機能には次の長所があります:

- デリバリーグループ内のマシンの電源を管理するための、単一の一貫したメカニズムを提供します。
- 負荷ベース、スケジュールベース、またはその両方を組み合わせた電源管理によって、可用性とコストの管理を可能にします。
- コスト削減や処理能力の利用状況などのメトリックを監視し、通知を有効にするには、［Director］ を使用します。

ビデオツアー（2 分間）

次のビデオでは、Autoscale を簡単に紹介するクイックツアーを提供しています。

これは埋め込みビデオです。リンクをクリックしてビデオを見る

Autoscale の利用を開始する

August 17, 2024

Autoscale はデリバリーグループレベルで機能します。設定したスケジュールに基づいて、デリバリーグループ内のマシンの電源をプロアクティブに管理します。

Autoscale はすべての種類のデリバリーグループに適用されます：

- シングルセッションの静的 OS
- シングルセッションランダム OS
- マルチセッションランダム OS

この記事では、Autoscale 関連の基本的な概念について説明し、デリバリーグループの Autoscale を有効にして構成する方法について説明します。

基本的な概念

始める前に、以下の Autoscale の基本的な概念について説明します：

- スケジュール
- 処理能力バッファ
- 負荷インデックス

スケジュール

Autoscale は、設定したスケジュールに基づいて、デリバリーグループのマシンの電源をオンまたはオフにします。

スケジュールには、ピーク時とオフピーク時の動作が定義された、時間枠ごとのアクティブなマシンの数などの情報が含まれます。

スケジュール設定は、デリバリーグループの種類によって異なります。詳しくは、次のトピックを参照してください:

- マルチセッション OS のデリバリーグループ
- シングルセッション OS のランダムデリバリーグループ
- シングルセッション OS の静的デリバリーグループ

処理能力バッファ

処理能力バッファは、動的な負荷の増加を考慮し、現在の需要に応じて予備の処理能力を追加するために使用されます。次の 2 つのシナリオに注意する必要があります:

- マルチセッション OS のデリバリーグループの場合、処理能力バッファは、負荷インデックスを基準としたデリバリーグループの合計処理能力のパーセンテージで定義されます。
- シングルセッション OS のデリバリーグループの場合、処理能力バッファは、デリバリーグループ内のマシンの総数に対するパーセンテージで定義されます。

負荷インデックス

> 重要:
>
> 負荷インデックスは、マルチセッションのデリバリーグループにのみ適用されます。

負荷インデックスのメトリックで、マシンがユーザーのログオン要求を受け入れる可能性を判断します。負荷インデックスの値は、同時ログオン、セッション、CPU、ディスク、メモリの使用が構成された **Citrix** 負荷管理ポリシー設定で算出されます。

負荷インデックスの範囲は、0〜10,000 です。デフォルトでは、マシンは 250 のセッションをホストしている時に負荷限界であると見なされます:

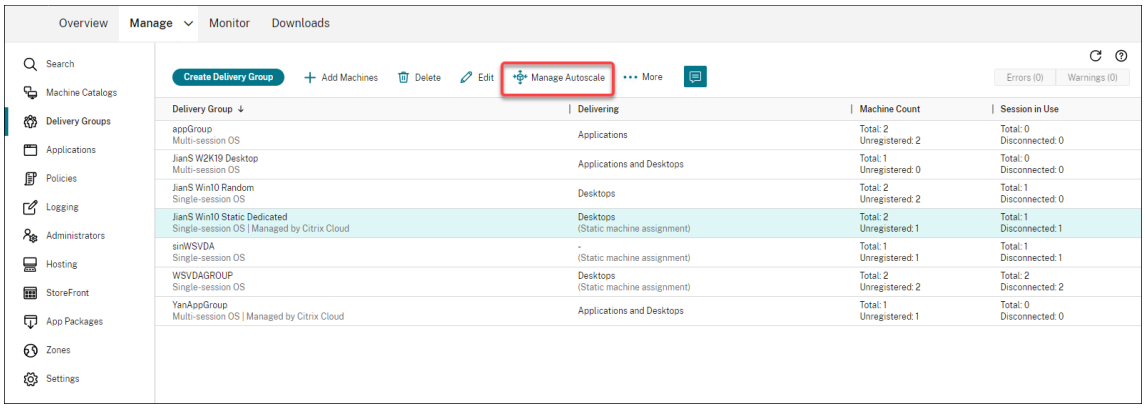
- 値が「0」であれば、マシンは負荷から解放されています。負荷インデックス値が「0」のマシンは基準の負荷状態です。
- 値が「10,000」であれば、これ以上セッションを実行できない、負荷が最大状態のマシンです。

デリバリーグループの **Autoscale** の有効化

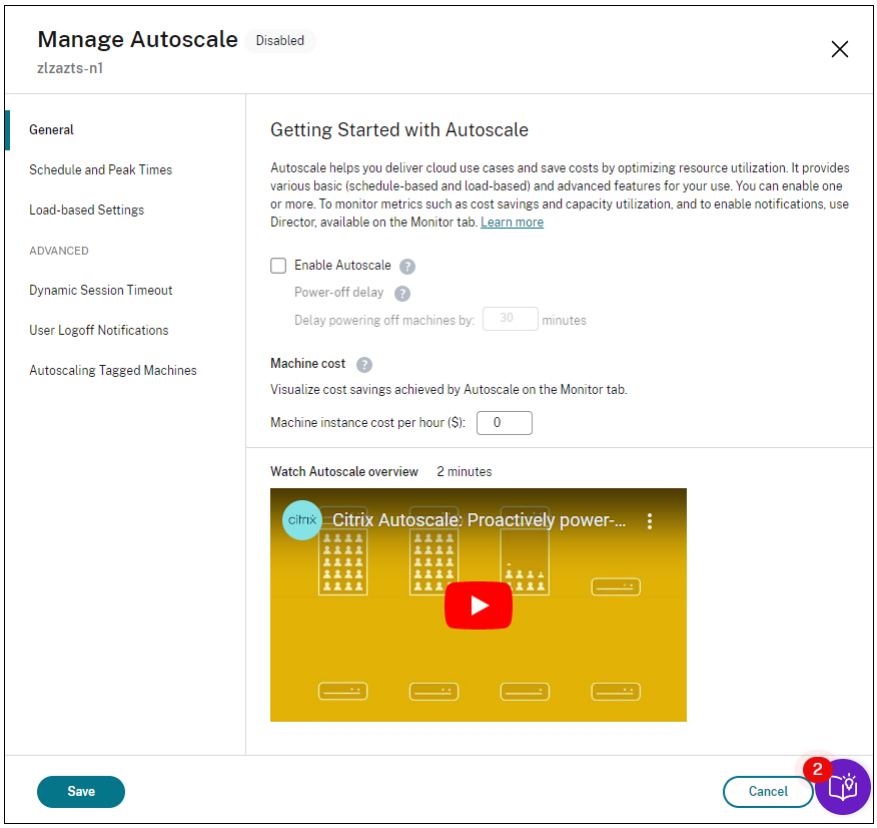
デリバリーグループを作成すると、デフォルトでは Autoscale が無効になります。Web Studio を使用してデリバリーグループの Autoscale を有効にして構成するには、次の手順に従います:

PowerShell コマンドを使用して、デリバリーグループの Autoscale を有効にして構成することもできます。詳しくは、「Broker PowerShell SDK コマンド」を参照してください。

1. 左側のペインで ［デリバリーグループ］を選択します。
2. 管理するデリバリーグループを選択し、［**Autoscale** の管理］をクリックします。



3. ［**Autoscale** の管理］ページで ［**Autoscale** を有効にする］チェックボックスをオンにして Autoscale を有効にします。Autoscale を有効にすると、ページ上のオプションが有効になります。



4. 組織のニーズに合わせてデフォルト設定を変更するには、次のように設定します:
   - スケジュールの設定
   - より効率的に非アクティブなマシンの電源をオフにするには、動的セッションタイムアウトとユーザーログオフ通知を使用します。

- デリバリーグループ内のマシンのサブセットの電源管理を行う場合は、タグ付けされたマシンのAutoscaleを使用します。

Autoscale を無効にするには、[**Autoscale**] チェックボックスをオフにします。ページのオプションが灰色表示になり、選択したデリバリーグループに対して Autoscale が無効になっていることを示します。

> 重要:
>
> - Autoscale を無効にすると、Autoscale によって管理されているすべてのマシンは、無効になった時点の状態のままになります。
> - Autoscale を無効にした後、ドレイン状態にあるマシンはドレイン状態が解除されます。ドレイン状態について詳しくは、「ドレイン状態」を参照してください。

メトリックの監視

デリバリーグループの Autoscale を有効にすると、Director で Autoscale 管理対象マシンの以下のメトリックを監視できます。

- マシンの使用量
- 見積もり削減額
- マシンとセッションのアラート通知
- マシンの状態
- 負荷評価傾向

> 注:
>
> 最初にデリバリーグループの Autoscale を有効にすると、そのデリバリーグループの監視データを表示するのに数分かかることがあります。
> デリバリーグループの Autoscale が有効から無効になっても、監視データは引き続き利用できます。Autoscale は、5 分間隔で監視データを収集します。

メトリックについて詳しくは、「Autoscale 管理対象マシンの監視」を参照してください。

ヒント

Autoscale はデリバリーグループレベルで機能します。そのため、デリバリーグループごとに構成され、選択したデリバリーグループ内のマシンのみを電源管理します。

処理能力とマシン登録

Autoscale では、容量（処理能力）の決定時に、サイトに登録されているマシンのみを扱います。電源がオンになった未登録のマシンは、セッション要求を受け入れることができません。結果として、これらのマシンはデリバリーグループの総合的な処理能力に含まれません。

複数のマシンカタログにわたるスケーリング

一部のサイトでは、複数のマシンカタログが単一のデリバリーグループに関連付けられている場合があります。Autoscale は、スケジュールまたはセッション需要の要件を満たすために、各カタログからランダムにマシンの電源をオンにします。

たとえば、デリバリーグループに 2 つのマシンカタログがあるとします。カタログ A には電源がオンになった 3 台のマシンがあり、カタログ B には電源がオンになった 1 台のマシンがあります。Autoscale が追加のマシンの電源をオンにする必要がある場合は、カタログ A またはカタログ B のいずれかからマシンの電源をオンにします。

マシンのプロビジョニングとセッション需要

デリバリーグループに関連付けられているマシンカタログには、需要の増減に応じて電源をオンまたはオフするために十分な数のマシンが必要です。セッション需要がデリバリーグループ内の登録済みマシンの総数を超えても、Autoscale はすべての登録済みマシンの電源がオンになっていることを確認します。しかし、**Autoscale** が追加のマシンをプロビジョニングすることはありません。

インスタンスサイズの考慮事項

パブリッククラウドでインスタンスのサイズを適切に設定することで、コストを最適化できます。ワークロードのパフォーマンスと処理能力に関する要件を満たす限り、小さいインスタンスをプロビジョニングすることをお勧めします。

小さいインスタンスは、大きいインスタンスよりも少ないユーザーセッションをホストします。そのため、最後のユーザーセッションがログオフされるまでの時間が短いので、Autoscale はマシンをいち早くドレイン状態にします。つまり、Autoscale は小さいインスタンスの電源をすぐにオフにするので、コストを削減できます。

ドレイン状態

Autoscale は、デリバリーグループ内の電源がオンになっているマシンの数を、構成されたプールサイズおよび処理能力バッファにまでスケールダウンしようとします。

この目標を達成するために、Autoscale は、セッションの数が最も少ない余分なマシンを「ドレイン状態」にし、すべてのセッションがログオフしたときにそれらの電源をオフにします。この動作は、セッション需要が減少し、スケジュールに必要なマシンの数が電源オンになったマシンよりも少なくなる場合に発生します。

Autoscale は、余分なマシンを 1 台ずつ「ドレイン状態」にします:

- 2 台以上のマシンに同数のアクティブなセッションがある場合、Autoscale は指定された電源オフの遅延期間中電源がオンになっているマシンをドレイン状態にします。

  これによって、最近電源がオンになった、セッション数が少ない可能性が高いマシンをドレイン状態にすることを回避します。

- 指定された電源オフの遅延期間中複数のマシンの電源がオンになっている場合、Autoscale はそれらのマシンを 1 台ずつランダムにドレイン状態にします。

ドレイン状態のマシンは、新しいセッションの開始をホストしなくなり、既存のセッションがログオフされるまで待機します。すべてのセッションがログオフされた場合にのみ、マシンはシャットダウンの候補になります。ただし、セッション起動時にすぐに使用できるマシンがない場合、Autoscale は、新しくマシンの電源をオンにするのではなく、ドレイン状態のマシンでセッションを起動することを優先します。

次のいずれかの条件が満たされると、マシンの状態がドレイン状態以外に変更されます:

- マシンの電源がオフになる。
- マシンが属するデリバリーグループの Autoscale が無効化される。
- Autoscale により、必要なスケジュールまたは負荷の需要の要件を満たすためにマシンが使用される。これは、スケジュール（スケジュールベースのスケール）または現在の需要（負荷ベースのスケール）で、この時点で電源がオンになっているマシンより多くのマシンが必要な場合に発生します。

> 重要:
>
> セッション起動用にすぐに使用できるマシンがない場合、Autoscale は、新しくマシンの電源をオンにするのではなく、ドレイン状態のマシンでセッションを起動することを優先します。セッション起動をホストするドレイン状態のマシンは、ドレイン状態を維持します。

どのマシンがドレイン状態にあるかを調べるには、PowerShell コマンドの`Get-BrokerMachine`を使用します。例: `Get-BrokerMachine -DrainingUntilShutdown $true`。または、［管理］コンソールを使用できます。「ドレイン状態のマシンの表示」を参照してください。

ドレイン状態のマシンの表示

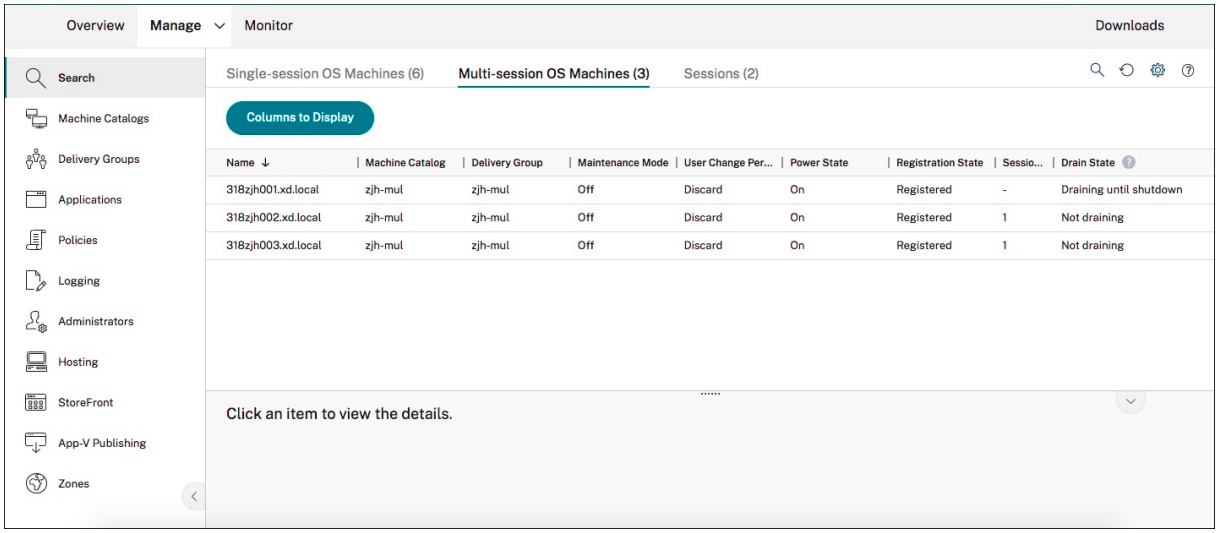
> 注:
>
> この機能は、マルチセッションマシンのみに適用されます。

Web Studio では、ドレイン状態のマシンを表示して、間もなくシャットダウンされるマシンを確認できます。次の手順を実行します:

1. ［検索］ノードに移動し、［表示する列］をクリックします。
2. ［表示する列］ウィンドウで、［ドレイン状態］の横にあるチェックボックスをオンにします。
3. ［保存］をクリックして、［表示する列］ウィンドウを閉じます。

［ドレイン状態］列には、次の情報を表示できます：

- シャットダウンまでドレインを実行中。マシンがシャットダウンされるまでドレイン状態のときに表示されます。
- ドレインは実行されていません。マシンがまだドレイン状態でないときに表示されます。



追加情報

Autoscale について詳しくは、Tech Zone の「Citrix Autoscale」を参照してください。

スケジュールベースおよび負荷ベースの設定

August 17, 2024

Autoscale によるマシンの電源管理方法

Autoscale は、選択したスケジュールに基づいてマシンの電源をオンまたはオフにします。Autoscale では、特定の曜日を含む複数のスケジュールを設定し、その期間中利用可能なマシンの数を調整できます。特定の日の特定の時間に特定のユーザーグループがマシンリソースを消費すると予想される場合は、その間のエクスペリエンスを最適化できます。それらのマシンで実行中のセッションがあるかどうかにかかわらず、スケジュール中にマシンの電源がオンになることに注意してください。

> 注：
>
> Autoscale は、すべての電力管理マシンをサポートします。

これはデリバリーグループのタイムゾーンに基づいたスケジュールです。タイムゾーンを変更するには、デリバリーグループのユーザー設定を変更します。詳しくは、「デリバリーグループの管理」を参照してください。

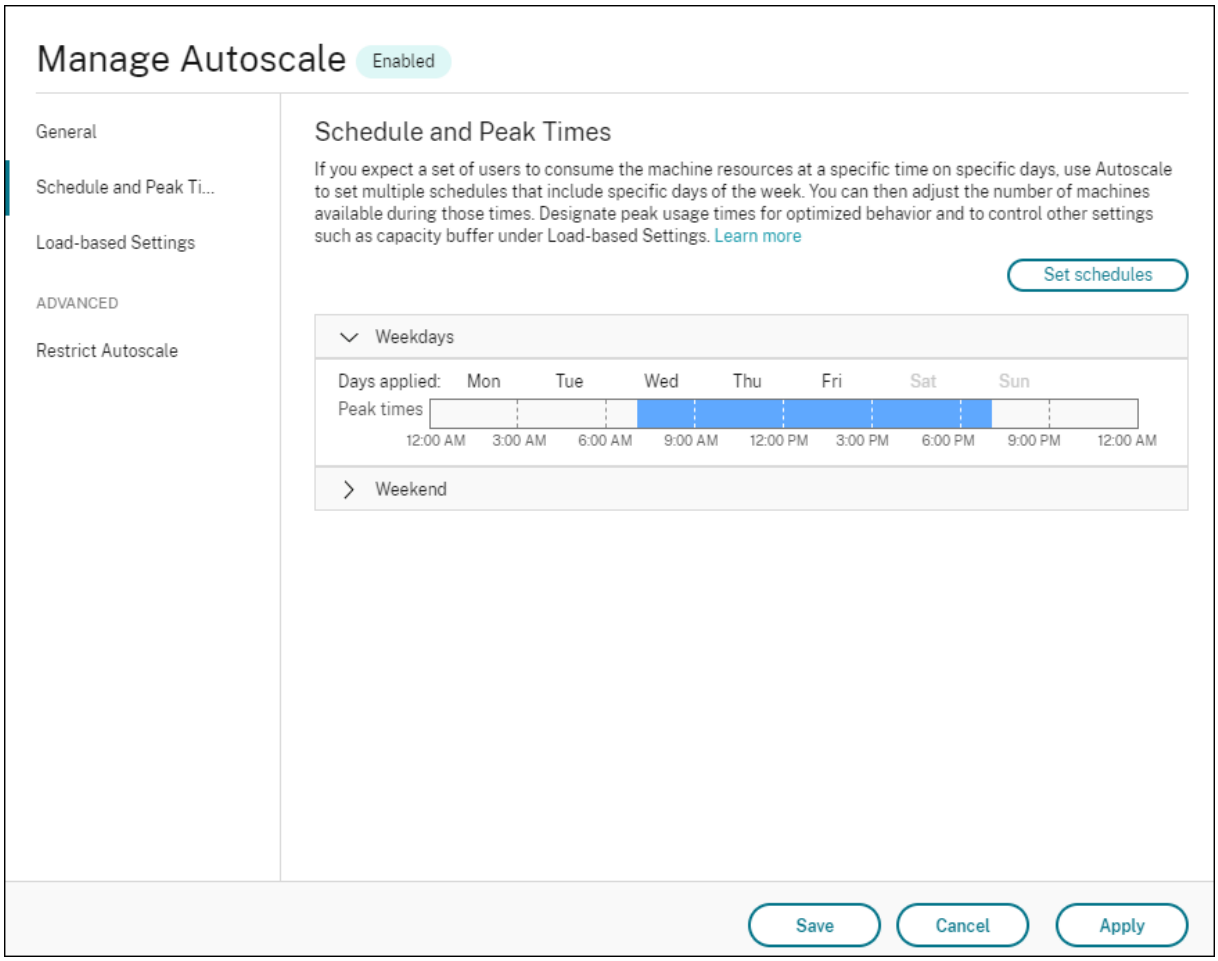
Autoscale には次の 2 種類のデフォルトのスケジュールがあります：平日（月曜日から金曜日まで）と週末（土曜日と日曜日）。デフォルトでは、平日のスケジュールでは、ピーク時の午前 7 時から午後 6 時 30 分までの間、1 台のマシンの電源が投入され、オフピーク時には稼働しません。デフォルトの処理能力バッファは、ピーク時とオフピーク時には 10% に設定されます。デフォルトでは、週末のスケジュールでは、マシンの電源はオンになりません。

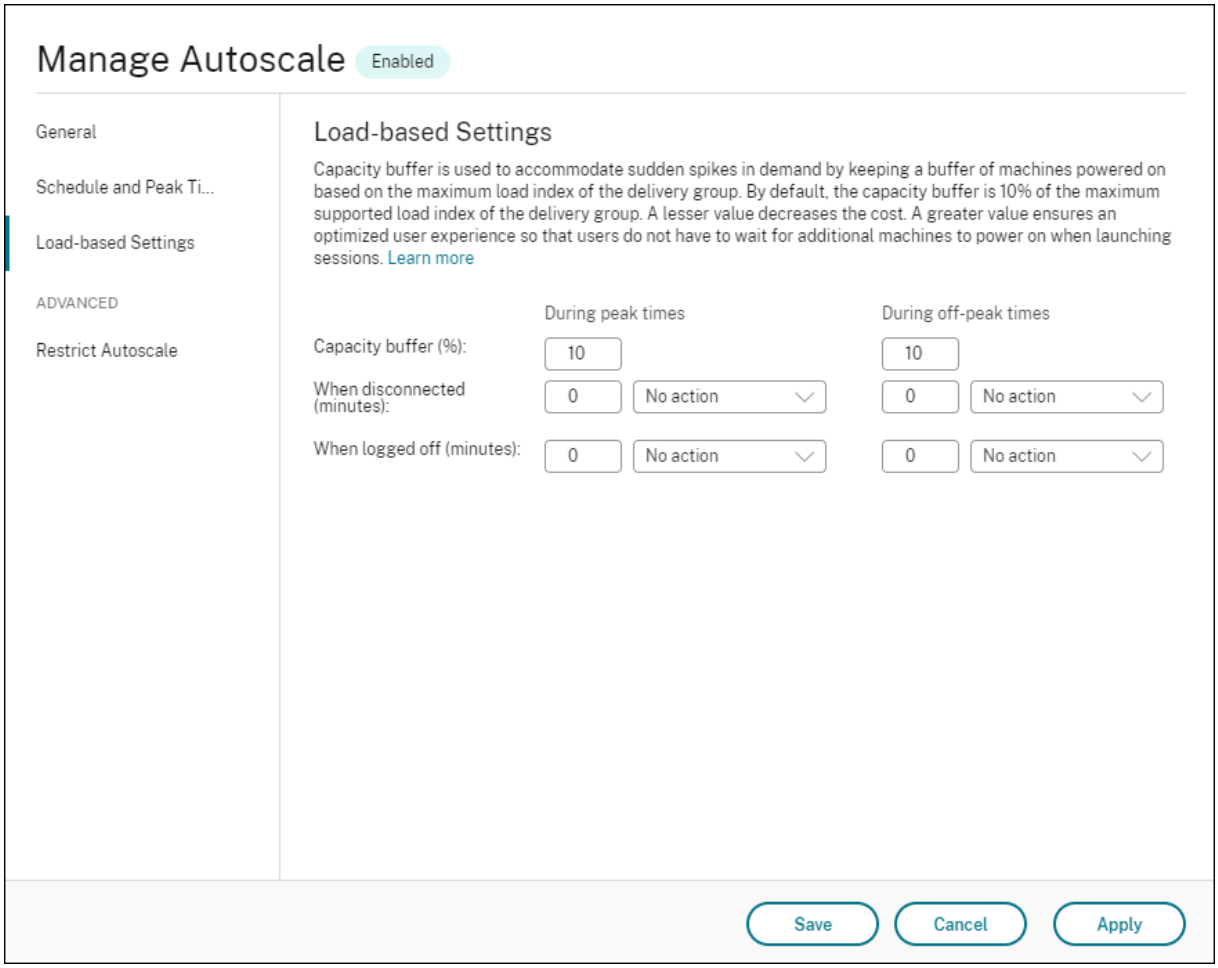
> 注：
>
> Autoscale は、サイトに登録されているマシンのみを、使用可能な処理能力の一部として計算します。「登録されている」とは、そのマシンが使用可能であるか、既に使用中であることを意味します。これによって、ユーザーセッションを実行できるマシンのみがデリバリーグループの処理能力として見なされるようになります。

ユーザーインターフェイス

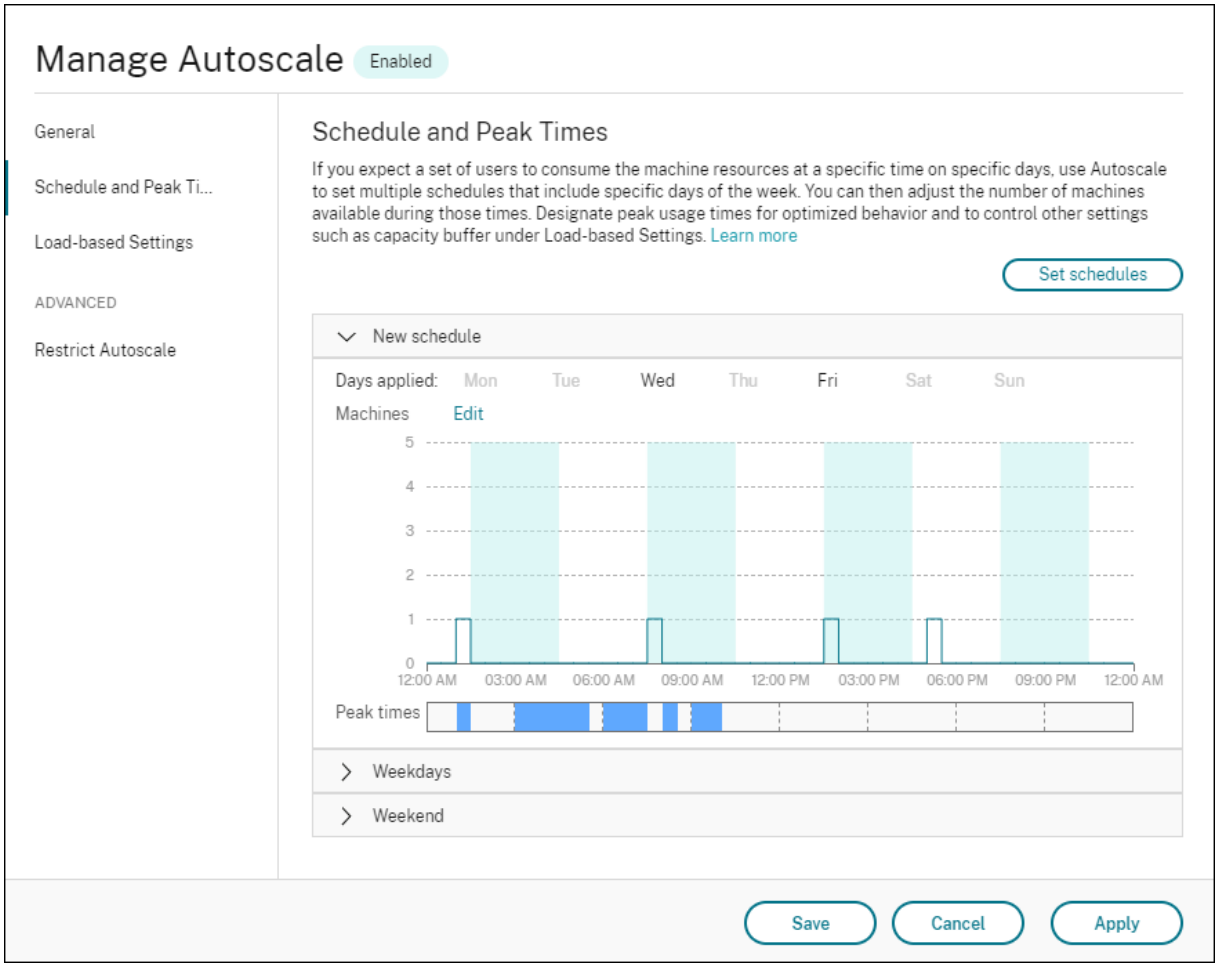
考慮するユーザーインターフェイスは 3 種類です。

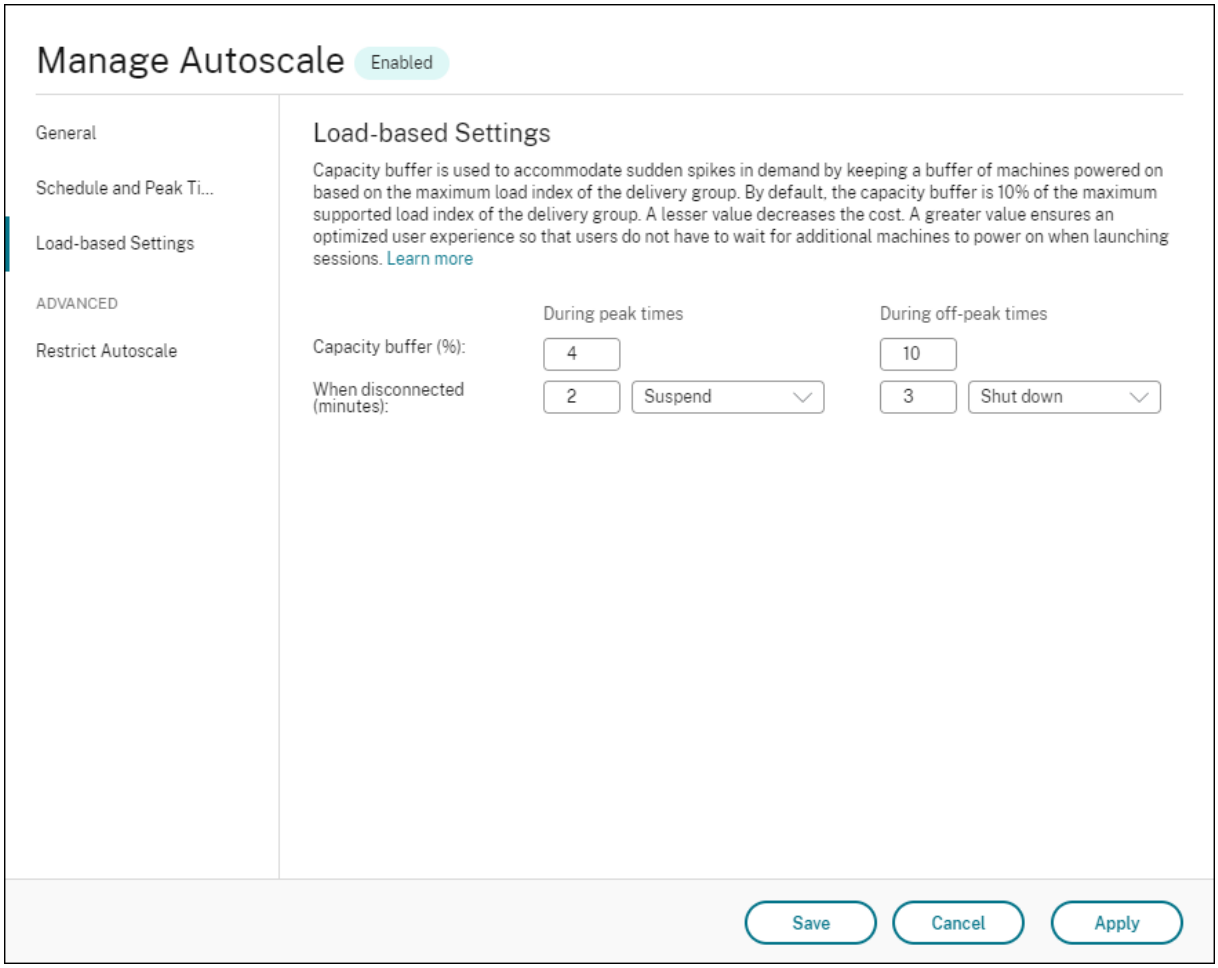
シングルセッション *OS* の静的デリバリーグループのユーザーインターフェイス：



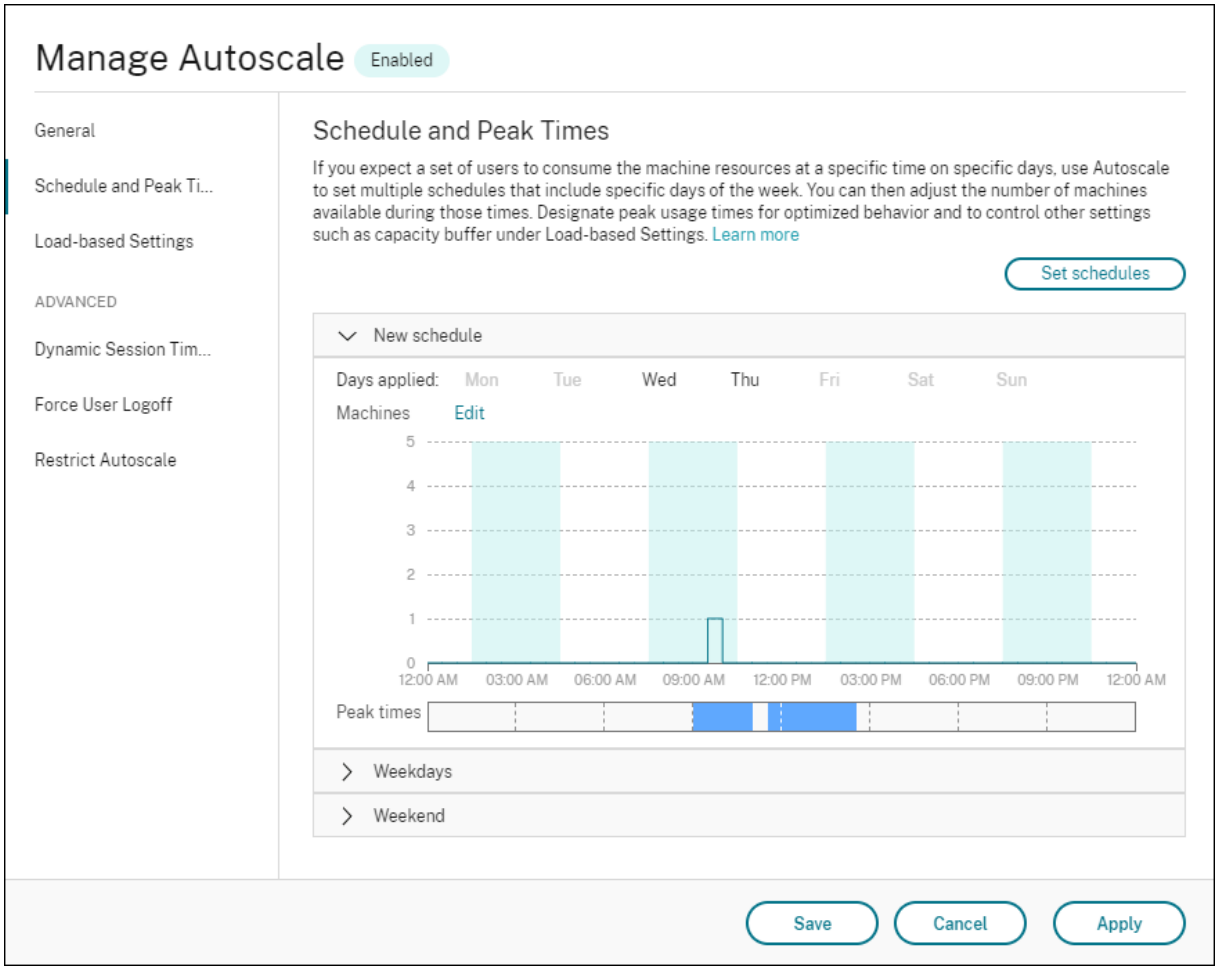


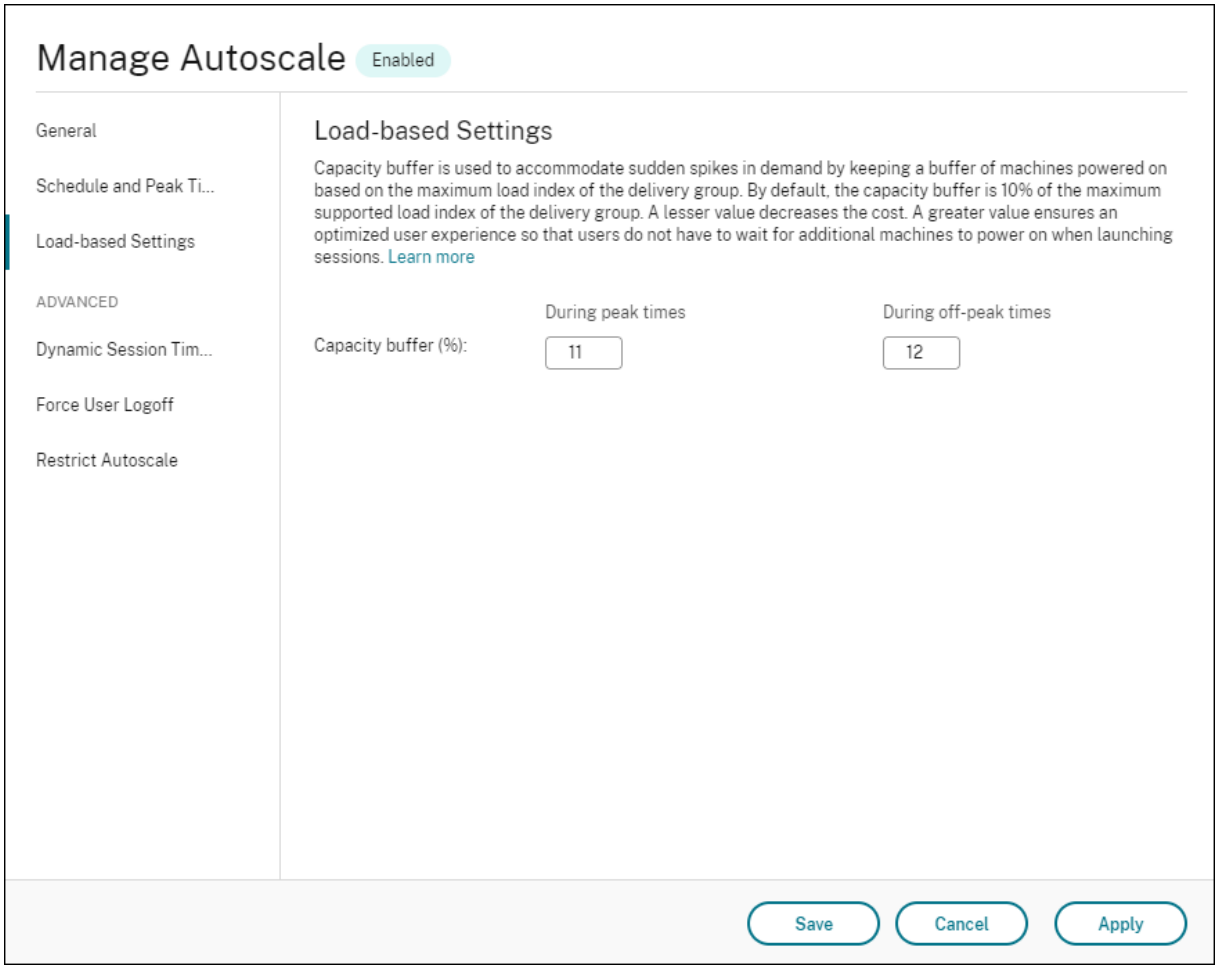
シングルセッション *OS* のランダムデリバリーグループの Autoscale ユーザーインターフェイス:





マルチセッション *OS* デリバリーグループの Autoscale ユーザーインターフェイス:





スケジュールベースの設定

Autoscale スケジュール。スケジュールを追加、編集、選択、削除できます。

適用する曜日。選択したスケジュールに適用した曜日を強調表示します。残りの曜日は灰色表示されます。

編集。1 時間ごとまたは 30 分ごとにマシンを割り当てることができます。数字またはパーセンテージでマシンを割り当てることができます。

> 注:
>
> - このオプションは、マルチセッション OS およびシングルセッション OS のランダムデリバリーグループの Autoscale ユーザーインターフェイスでのみ使用可能です。
> - ［編集］の横のヒストグラムは、異なる時間枠で実行中のマシンの数またはパーセンテージを表示します。
> - ［ピーク時］の上の ［編集］をクリックすると、時間枠ごとにマシンを割り当てることができます。［起動するマシン］ウィンドウのメニューで選択したオプションによって、マシンを数字またはパーセンテージで割り当てることができます。
> - マルチセッション OS のデリバリーグループの場合、実行するマシンの最小数を 1 日あたり 30 分単位で

> 個別に設定できます。シングルセッション OS のランダムデリバリーグループの場合、実行するマシンの最小数を 1 日あたり 60 分単位で個別に設定できます。

独自にスケジュールを定義するには、以下の手順を実行します:

1. [**Autoscale** の管理] ウィンドウの [スケジュールとピーク時] ページで、[スケジュールの設定] をクリックします。
2. [**Autoscale** スケジュールの編集] ウィンドウで、各スケジュールに適用する日付を選択します。必要に応じてスケジュールを削除することもできます。
3. [完了] をクリックしてスケジュールを保存し、[スケジュールとピーク時] ページに戻ります。
4. 該当するスケジュールを選択し、必要に応じて構成します。
5. [適用] をクリックして [**Autoscale** の管理] ウィンドウを終了するか、他のページで設定を構成します。

> 重要:
>
> - Autoscale では、同じ日を異なるスケジュールで上書きすることはできません。たとえば、schedule1 で月曜日を選択した後に schedule2 で月曜日を選択すると、schedule1 で自動的に月曜日が消去されます。
> - スケジュール名では大文字と小文字が区別されません。
> - スケジュール名は空白にしたり、スペースだけを含めたりすることはできません。
> - Autoscale では、文字間にスペースを入れることができます。
> - スケジュール名に次の文字は使用できません: \ / ; : # . * ? = < > | [ ] ( ) { } “ “。
> - Autoscale では、重複したスケジュール名は使用できません。スケジュールごとに異なる名前を入力してください。
> - Autoscale では、空のスケジュールはサポートしていません。つまり、選択した日のないスケジュールは保存されません。
>
> 注:
>
> 選択したスケジュールに含まれている日が強調表示され、含まれていない日は灰色表示になります。

負荷ベースの設定

ピーク時。選択したスケジュールに適用した曜日のピーク時間を定義できます。このためには、横棒グラフを右クリックします。ピーク時間を定義すると、残りの未定義の時間はデフォルトでオフピーク時間に設定されます。デフォルトでは、午前 7 時から午後 7 時の時間枠が選択したスケジュールの曜日のピーク時間として定義されます。

> 重要:
>
> - マルチセッション OS のデリバリーグループの場合、ピーク時の棒グラフが処理能力バッファに使用されます。
> - シングルセッション OS のデリバリーグループの場合、ピーク時の棒グラフが処理能力バッファに使用さ

> れ、ログオフや切断後にトリガーされるアクションを制御します。
> - マルチセッション OS とシングルセッション OS のデリバリーグループの両方について、スケジュールに含まれる日のピーク時間を 30 分の詳細レベルで定義できます。または、代わりに`New-BrokerPowerTimeScheme PowerShell`コマンドを使用できます。詳しくは、「Broker PowerShell SDK コマンド」を参照してください。

処理能力バッファ。電源がオンになっているマシンのバッファを維持できます。値が小さいほどコストが低くなります。値を大きくするとユーザーエクスペリエンスが確実に最適化されるため、セッションを起動する時に追加のマシンの電源がオンになるまで待機する必要がありません。デフォルトでは、処理能力バッファはピーク時およびオフピーク時の 10% です。処理能力バッファを 0（ゼロ）に設定した場合、セッションを起動する時に追加のマシンの電源がオンになるまで待機が必要な場合もあります。Autoscale では、ピーク時とオフピーク時で個別に処理能力バッファを指定できます。

その他の設定

> ヒント：
>
> - Broker PowerShell SDK を使用して、その他の設定を構成することを選択できます。詳しくは、「Broker PowerShell SDK コマンド」を参照してください。
> - 切断時およびログオフ時の設定に関連する SDK コマンドを理解するには、https://citrix.github.io/delivery-controller-sdk/Broker/about_Broker_PowerManagement/#power-policyを参照してください。

切断時。セッションが切断されてから一時停止またはシャットダウンされるまで、切断されロックされたマシンの電源をオンにしておく時間を指定できます。指定した切断時間が経過すると、構成したアクションに応じて、マシンは一時停止またはシャットダウンします。デフォルトでは、切断されたマシンにアクションは割り当てられていません。ピーク時とオフピーク時で個別にアクションを定義できます。このためには、下向き矢印をクリックして、メニューから次のいずれかのオプションを選択します：

- 何もしない。これを選択すると、セッション切断後のマシンの電源はオンのままになります。Autoscale は何もしません。
- 一時停止。これを選択すると、指定された切断時間が経過したときに Autoscale がマシンをシャットダウンせずに一時停止します。［一時停止］を選択すると、以下のオプションが使用できます。
  - 再接続がない場合（分）。一時停止したマシンは、切断されたユーザーが再接続すると引き続き使用できますが、新しいユーザーは使用できません。マシンを再び使用可能にしてすべてのワークロードを処理できるようにするには、マシンをシャットダウンします。Autoscale がマシンをシャットダウンするまでのタイムアウト時間を分単位で指定します。
- シャットダウン。これを選択すると、指定された切断時間が経過したときに Autoscale がマシンをシャットダウンします。

> 注:
>
> このオプションは、シングルセッション OS のランダムおよび静的デリバリーグループの Autoscale ユーザーインターフェイスでのみ使用可能です。

ログオフ時。セッションのログオフから一時停止またはシャットダウンされるまで、マシンの電源をオンにしておく時間を指定できます。指定したログオフ時間が経過すると、構成したアクションに応じて、マシンは一時停止またはシャットダウンします。デフォルトでは、ログオフしたマシンにアクションは割り当てられていません。ピーク時とオフピーク時で個別にアクションを定義できます。このためには、下向き矢印をクリックして、メニューから次のいずれかのオプションを選択します:

- 何もしない。これを選択すると、セッションログオフ後のマシンの電源はオンのままになります。Autoscale は何もしません。
- 一時停止。これを選択すると、指定されたログオフ時間が経過したときに Autoscale がマシンをシャットダウンせずに一時停止します。
- シャットダウン。これを選択すると、指定されたログオフ時間が経過したときに Autoscale がマシンをシャットダウンします。

> 注:
>
> このオプションは、シングルセッション OS の静的デリバリーグループの Autoscale ユーザーインターフェイスでのみ使用可能です。

セッションが切断された状態で異なる期間に移行するシングルセッション **OS** マシンの電源管理

> 重要:
>
> - この拡張機能は、セッションが切断されたシングルセッション OS マシンにのみ適用されます。ログオフされたセッションがあるシングルセッション OS マシンには適用されません。
> - この機能拡張を有効にするには、該当するデリバリーグループの Autoscale を有効にする必要があります。それ以外の場合、電源ポリシーの切断操作は、期間の移行時にトリガーされません。

以前のリリースでは、アクション（切断アクション =「一時停止」または「シャットダウン」）が必要な期間に移行するシングルセッション OS マシンの電源がオンのままになっていました。このシナリオは、操作（切断アクション =「何もしない」）が不要な期間（ピーク時またはオフピーク時）にマシンが切断された場合に発生しました。

このリリース以降では、指定した切断時間が経過すると、Autoscale はマシンを一時停止または電源をオフにします。これは、その期間に対して構成された切断アクションによって異なります。

たとえば、シングルセッション OS デリバリーグループに対して次の電源ポリシーを構成するとします:

- `PeakDisconnectAction`を「何もしない」に設定
- `OffPeakDisconnectAction`を「シャットダウン」に設定
- 「OffPeakDisconnectTimeout」を「10」に設定

> 注:
>
> 切断アクション電源ポリシーについて詳しくは、「https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/about_Broker_PowerManagement/#power-policy」および「https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/Get-BrokerDesktopGroup/」を参照してください。

以前のリリースでは、ピーク時にセッションが切断されたシングルセッション OS マシンは、ピークからオフピークに移行しても電源がオンのままでした。このリリース以降、`OffPeakDisconnectAction`および`OffPeakDisconnectTimeout`ポリシーのアクションは、期間移行時にシングルセッション OS マシンに適用されます。その結果、オフピークに移行してから 10 分後にマシンの電源がオフになります。

以前の動作に戻す（つまり、セッションが切断された状態でピークからオフピークまたはオフピークからピークに移行するマシンでは何も実行しない）場合は、次のいずれかの操作を行います:

- 「LegacyPeakTransitionDisconnectedBehaviour」レジストリ値を 1 に設定します（true: 以前の動作を有効にします）。デフォルトでは、値は 0 です（false、期間の移行時に電源ポリシーの切断アクションがトリガーされます）。
  - パス: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\DesktopServer
  - 値の名前: LegacyPeakTransitionDisconnectedBehaviour
  - 種類: REG_DWORD
  - 値のデータ: 0x00000001（1）
- `Set-BrokerServiceConfigurationData` PowerShell コマンドを使用して設定を構成します。例:
  - `PS C:\> Set-BrokerServiceConfigurationData HostingManagement.LegacyPeakTransitionDisconnectedBehaviour -SettingValue $true`

期間移行時に電源ポリシーアクションを適用するには、マシンが次の条件を満たす必要があります:

- 切断されたセッションがある。
- 保留中の電源操作がない。
- 異なる期間に移行するシングルセッション OS のデリバリーグループに属している。
- 特定の期間（ピーク時またはオフピーク時）に切断し、電源操作が割り当てられている期間に移行するセッションがある。

処理能力バッファについて

処理能力バッファは、動的な負荷の増加を考慮し、現在の需要に応じて予備の処理能力を追加するために使用されます。次の 2 つのシナリオに注意する必要があります:

- マルチセッション OS のデリバリーグループの場合、処理能力バッファは、負荷インデックスを基準としたデリバリーグループの合計処理能力のパーセンテージで定義されます。負荷インデックスについて詳しくは、「負荷インデックス」を参照してください。
- シングルセッション OS のデリバリーグループの場合、処理能力バッファは、コンピューターの数を基準としたデリバリーグループの合計処理能力のパーセンテージで定義されます。

> 注:
>
> Autoscale をタグ付きマシンに制限するシナリオでは、処理能力バッファは、負荷インデックスを基準としたデリバリーグループ内のタグ付きマシンの合計処理能力のパーセンテージとして定義されます。

Autoscale では、ピーク時とオフピーク時で個別に処理能力バッファを指定できます。処理能力バッファフィールドの値を小さくすると、Autoscale がオンにする予備の処理能力が少なくなるため、コストが削減されます。値を大きくするとユーザーエクスペリエンスが確実に最適化されるため、セッションを起動する時に追加のマシンの電源がオンになるまで待機する必要がありません。デフォルトでは、処理能力バッファは 10% です。

> 重要:
>
> 処理能力バッファにより、予備の合計処理能力がデリバリーグループの合計処理能力の「X」パーセントを下回るレベルに低下すると、マシンの電源がオンになります。これによって、必要なパーセンテージの予備の処理能力が確保されます。

マルチセッション **OS** のデリバリーグループ

マシンの電源がオンになる状況

> 重要:
>
> スケジュールが選択されている場合、Autoscale はスケジュールで電源をオンにするよう構成されている、すべてのマシンの電源をオンにします。負荷に関係なく、このスケジュール中、指定された台数のマシンの電源をオンにしたままにします。

デリバリーグループ内の電源がオンになっているマシンの数が負荷インデックス基準で処理能力を確保するためのバッファに一致しなくなると、Autoscale は追加のマシンの電源をオンにします。たとえば、デリバリーグループに 20 台のマシンがあり、スケジュールベースのスケール、20% の処理能力バッファで 3 台のマシンの電源がオンになる予定とします。この場合、負荷がなくなると、最終的に 4 台のマシンの電源がオンになります。これは、バッファとして 4x10,000 の負荷インデックスが必要であり、少なくとも 4 台のマシンの電源をオンにする必要があるためです。こうした事態は、ピーク時、マシンの負荷が増加したとき、新しいセッションの起動時、新しいマシンをデリバリーグループに追加したときに発生する可能性があります。Autoscale は、次の基準を満たすマシンの電源のみをオンにします:

- マシンがメンテナンスモードではない。
- マシンが稼働しているハイパーバイザーがメンテナンスモードになっていない。

- 現在マシンの電源がオフになっている。
- マシンに保留中の電源操作がない。

マシンの電源がオフになる状況

> 重要:
>
> - スケジュールが選択されている場合、Autoscale はスケジュールに従ってマシンの電源をオフにします。
> - このスケジュール中、電源がオンになるよう構成されているマシンの電源はオフにしません。

デリバリーグループの電源がオンになっているマシンの数（処理能力バッファを含める）をサポートするのに十分な数のマシンがある場合、Autoscale は追加のマシンの電源をオフにします。こうした事態は、オフピーク時、マシンの負荷が減少したとき、セッションのログオフ時、そしてマシンをデリバリーグループから削除した時に発生する可能性があります。Autoscale は、次の基準を満たすマシンの電源のみをオフにします:

- マシンとそのマシンが稼働しているハイパーバイザーがメンテナンスモードになっていない。
- 現在マシンの電源がオンになっている。
- マシンが利用可能として登録されている、または起動後、登録を待機している。
- マシンにアクティブなセッションがない。
- マシンに保留中の電源操作がない。
- マシンが指定された電源オフの遅延条件を満たしている。これは、少なくとも「X」分間マシンの電源がオンになっていたことを意味します。「X」は対象のデリバリーグループで指定された電源オフの遅延です。

サンプルシナリオ

次のようなシナリオを想定します:

- デリバリーグループの構成。Autoscale が電源管理するデリバリーグループには 10 台のマシンが含まれています（M1～M10）。
- **Autoscale** の構成
  - 処理能力バッファは 10% に設定します。
  - 選択したスケジュールにマシンが含まれていません。

このシナリオは以下の順序で実行されます:

1. ユーザーはログオンしていません。
2. ユーザーセッションが増加します。
3. 追加のユーザーセッションが開始されます。

4. セッションの終了により、ユーザーセッションの負荷が減少します。
5. ユーザーセッションの負荷は、オンプレミスリソースによってのみ処理されるようになるまで減少し続けます。

上記のシナリオで Autoscale がどのように機能するかについては、以下を参照してください。

- ユーザー負荷なし（初期の状態）
  - 1 台のマシン（例：M1）の電源がオンになっています。マシンの電源がオンになっているのは、処理能力バッファが構成されているためです。この場合、10（マシン数）×10,000（負荷インデックス）×10%（構成された処理能力バッファ）=10,000 です。したがって、1 台のマシンの電源がオンになります。
  - 電源がオンになっているマシン（M1）の負荷インデックス値は基準の負荷（負荷インデックス = 0）です。
- 最初のユーザーがログオンする
  - セッションは、マシン M1 でホストされます。
  - 電源がオンになっているマシン M1 の負荷インデックスが増大し、M1 は基準の負荷を超えます。
  - 処理能力バッファが構成されているため、需要の増大に応じて Autoscale が追加のマシン（M2）の電源をオンにします。
  - マシン M2 の負荷インデックス値は基準の負荷になっています。
- ユーザーが負荷を増やす
  - マシン M1 と M2 の間でセッションの負荷が分散されます。その結果、電源がオンになっているマシン（M1 と M2）の負荷インデックスが増加します。
  - 予備の合計処理能力は、まだ負荷インデックス基準で 10,000 を超えています。
  - マシン M2 の負荷インデックス値は基準の負荷ではなくなります。
- 追加のユーザーセッションが開始される
  - マシン間（マシン M1 と M2）でセッションの負荷が分散されます。その結果、電源がオンになっているマシン（M1 と M2）の負荷インデックスがさらに増加します。
  - 予備の合計処理能力が負荷インデックス基準で 10,000 未満に低下すると、処理能力バッファが構成されているため、需要の増大に応じて Autoscale が追加のマシン（M3）の電源をオンにします。
  - マシン M3 の負荷インデックス値は基準の負荷になっています。
- さらに追加のユーザーセッションが開始される
  - マシン間（マシン M1 から M3 まで）でセッションの負荷が分散されます。その結果、電源がオンになっているマシン（M1 から M3 まで）の負荷インデックスが増加します。
  - 予備の合計処理能力は、負荷インデックス基準で 10,000 を超えています。
  - マシン M3 の負荷インデックス値は基準の負荷ではなくなります。
- セッションの終了によりユーザーセッションの負荷が減少する

  - ユーザーがセッションからログオフした後、またはアイドル状態のセッションがタイムアウトした後、マシン M1 から M3 までの解放された処理能力は、他のユーザーが開始したセッションのホストで再利用されます。
  - 予備の合計処理能力が負荷インデックス基準で 10,000 を超えるレベルに増加すると、Autoscale はいずれかのマシン（例：M3）をドレイン状態にします。その結果、他のユーザーによって開始されたセッションは、新しい変更がない限りはそのマシンに送信されなくなります。たとえば、エンドユーザーの負荷が再び増加したり、他のマシンの負荷が最小になったりした場合です。

- ユーザーセッションの負荷が減少し続ける
  - マシン M3 上のすべてのセッションが終了し、指定された電源オフの遅延でタイムアウトになると、Autoscale はマシン M3 の電源をオフにします。
  - さらにユーザーがセッションからログオフすると、電源がオンになったマシン（M1 と M2）の解放された処理能力は他のユーザーが開始したセッションのホストで再利用されます。
  - 予備の合計処理能力が負荷インデックス基準で 10,000 を超えるレベルに増加すると、Autoscale はいずれかのマシン（例：M2）をドレイン状態にします。その結果、他のユーザーによって開始されたセッションは、そのマシンに送信されなくなります。

- セッションがすべて終了するまで、ユーザーセッションの負荷は減少し続けます。
  - マシン M2 上のすべてのセッションが終了し、指定された電源オフの遅延でタイムアウトになると、Autoscale はマシン M2 の電源をオフにします。
  - 電源がオンになっているマシン（M1）の負荷インデックス値は基準の負荷になっています。処理能力バッファが構成されているため、Autoscale はマシン M1 をドレイン状態にしません。

> 注:
>
> マルチセッション OS のデリバリーグループの場合、ユーザーのセッションログオフ時にデスクトップへの変更はすべて失われます。ただし、ユーザー固有の設定が構成されている場合、ユーザープロファイル設定とともにローミングされます。

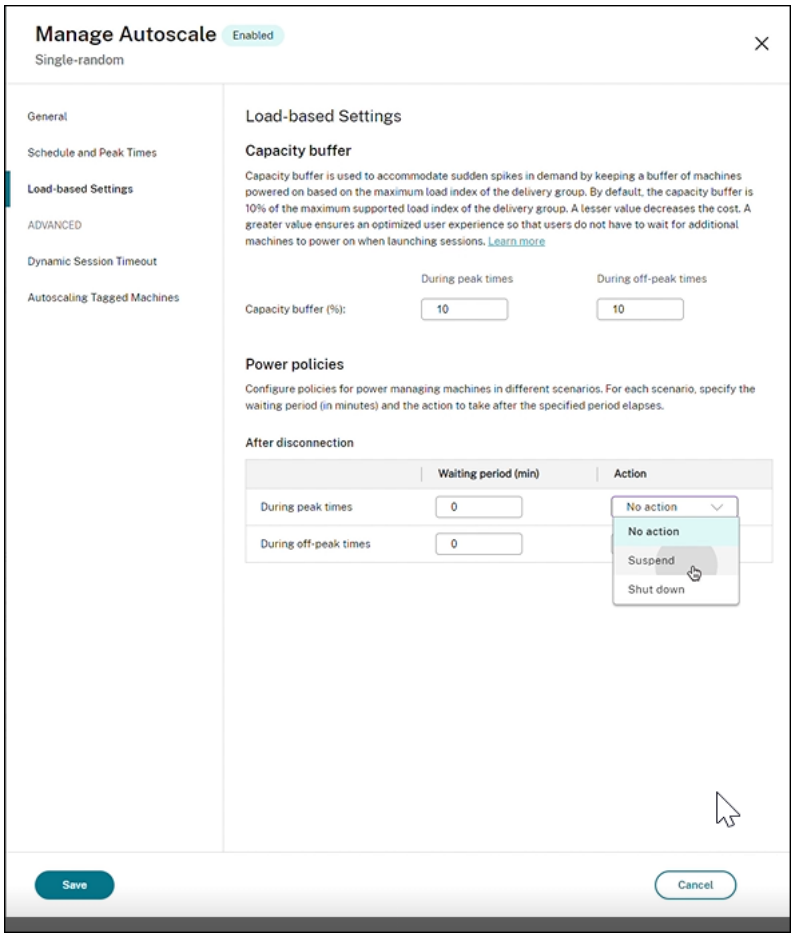
シングルセッション **OS** のランダムデリバリーグループ

処理能力バッファを使用すると、デリバリーグループ内のマシンの総数を基にして電源がオンになっているマシンのバッファを確保することで、需要の急増に対応できます。デフォルトでは、処理能力バッファは、デリバリーグループ内にあるマシンの総数の 10% です。

マシン数（処理能力バッファを含む）が現在電源がオンになっているマシンの総数を上回っている場合、需要に対応して追加のマシンの電源がオンになります。マシン数（処理能力バッファを含む）が現在電源がオンになっているマシンの総数を下回っている場合、構成されたアクションに従って余分なマシンはシャットダウンするか一時停止します。

電源ポリシー

さまざまなシナリオに合わせてマシンの電源管理ポリシーを構成します。シナリオごとに、待機時間（分単位）と、指定した時間の経過後に実行するアクションを指定できます。電源ポリシーは、シングルセッション OS のランダムデリバリーグループとシングルセッション OS の静的デリバリーグループに適用されます。

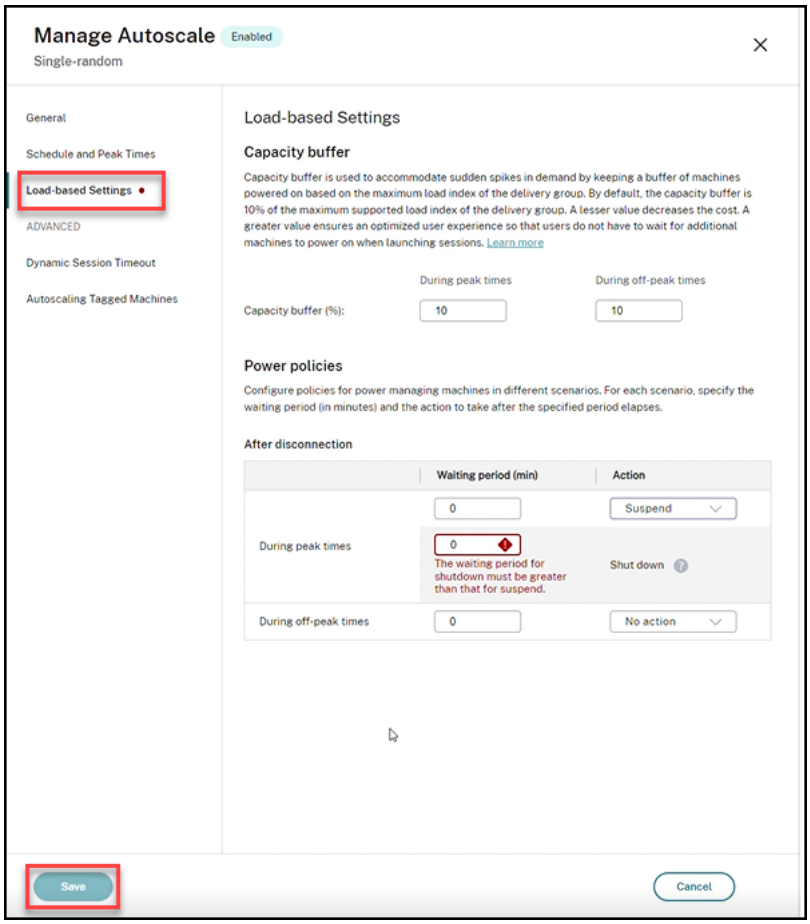


切断後は、ピーク時とオフピーク時の両方で次の設定を適用できます:

- 待機時間を分単位で設定したり、ドロップダウンから、何もしない、一時停止、シャットダウンなどのアクションを設定できます。
- 一時停止アクションを選択した場合は、マシンをシャットダウンするまでの追加の待機時間を構成します。

> 注:
>
> - ピーク時およびオフピーク時においては、シャットダウンアクションの待機時間をサスペンドの待機時間より長くする必要があります。
> - 一時停止されたマシンには、切断されたユーザーのみが再接続することによりアクセスできます。一時停止されたマシンを新しいユーザーが使用できるようにするには、マシンをシャットダウンします。
> - 一時停止フィールドおよびシャットダウンフィールドの時間設定が正しく構成されていない場合、[保存]

> オプションは無効になり、ナビゲーション項目の横に設定エラーを示す赤い点も表示されます。



例

- 待機時間を 12 分に設定し、最初のアクションとして何もしないを選択した場合は、12 分が経過した後もマシンは引き続きパワーオンの状態になります。
- 待機時間を 15 分に設定して最初のアクションとして一時停止を選択し、2 番目の待機時間を 20 分に選択した場合、15 分が経過するとマシンは一時停止されます。2 番目の待機時間が終了すると、マシンはシャットダウンされます。
- 待機時間を 18 分に設定し、シャットダウンする最初のアクションを選択した場合、18 分が経過するとマシンがシャットダウンされます。

サンプルシナリオ

次のようなシナリオを想定します:

- デリバリーグループの構成。Autoscale が電源管理するデリバリーグループには 10 台のマシンが含まれています（M1～M10）。
- **Autoscale** の構成

  - 処理能力バッファは 10% に設定します。
  - 選択したスケジュールにマシンが含まれていません。

このシナリオは以下の順序で実行されます：

1. ユーザーはログオンしていません。
2. ユーザーセッションが増加します。
3. 追加のユーザーセッションが開始されます。
4. セッションの終了により、ユーザーセッションの負荷が減少します。
5. ユーザーセッションの負荷は、オンプレミスリソースによってのみ処理されるようになるまで減少し続けます。

上記のシナリオで Autoscale がどのように機能するかについては、以下を参照してください。

- ユーザー負荷なし（初期の状態）
  - 1 台のマシン（M1）の電源がオンになっています。マシンの電源がオンになっているのは、処理能力バッファが構成されているためです。この場合、10（マシン数）×10%（構成された処理能力バッファ）=1 です。したがって、1 台のマシンの電源がオンになります。
- 最初のユーザーがログオンする
  - デスクトップを使用するためにユーザーが初めてログオンしたときに、電源がオンになったマシンでホストされたデスクトッププールからデスクトップが割り当てられます。この場合、ユーザーにはマシン M1 からデスクトップが割り当てられます。
  - 処理能力バッファが構成されているため、需要の増大に応じて Autoscale が追加のマシン（M2）の電源をオンにします。
- 2 人目のユーザーがログオンする
  - ユーザーにはマシン M2 からデスクトップが割り当てられます。
  - 処理能力バッファが構成されているため、需要の増大に応じて Autoscale が追加のマシン（M3）の電源をオンにします。
- 3 人目のユーザーがログオンする
  - ユーザーにはマシン M3 からデスクトップが割り当てられます。
  - 処理能力バッファが構成されているため、需要の増大に応じて Autoscale が追加のマシン（M4）の電源をオンにします。
- ユーザーのログオフ
  - ユーザーがログオフした後、またはユーザーのデスクトップがタイムアウトした後、解放された処理能力（M3 など）をバッファとして利用できます。その結果、処理能力バッファが 10% で構成されているため Autoscale はマシン M4 の電源をオフにします。
- ユーザーがいなくなるまで、ユーザーのログオフは続きます。

  - さらにユーザーがログオフすると、Autoscale はマシンの電源（M2 または M3 など）をオフにします。
  - ユーザーが残っていなくても、Autoscale は予備の処理能力用に確保された最後の 1 台のマシン（M1 など）の電源はオフにしません。

> 注:
>
> シングルセッション OS のランダムデリバリーグループの場合、ユーザーのセッションログオフ時にデスクトップへの変更はすべて失われます。ただし、ユーザー固有の設定が構成されている場合、ユーザープロファイル設定とともにローミングされます。

シングルセッション **OS** の静的デリバリーグループ

処理能力バッファを使用すると、デリバリーグループ内の未割り当てのマシンの総数を基に電源がオンになっている未割り当てのマシンのバッファを確保することで、需要の急増に対応できます。デフォルトでは、処理能力バッファは、デリバリーグループ内にある未割り当てのマシンの総数の 10% です。

> 重要:
>
> デリバリーグループ内のすべてのマシンが割り当てられた後は、処理能力バッファがマシンの電源のオンオフに関与することはなくなります。

マシン数（処理能力バッファを含む）が現在電源がオンになっているマシンの総数を上回っている場合、需要に対応して未割り当てのマシンの電源が追加でオンになります。マシン数（処理能力バッファを含む）が現在電源がオンになっているマシンの総数を下回っている場合、構成されたアクションに従って余分なマシンは電源がオフになるか一時停止します。

シングルセッション OS の静的デリバリーグループの Autoscale:

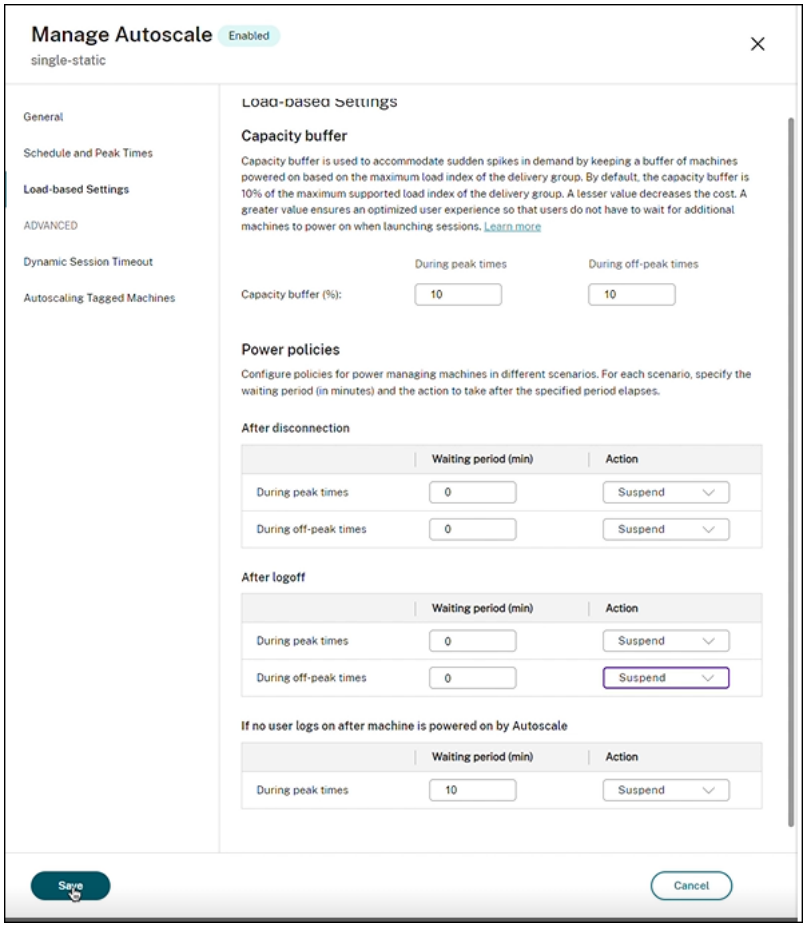
- 該当するシングルセッション OS のデリバリーグループの`AutomaticPowerOnForAssigned`プロパティが true に設定されているときにのみ、割り当てられたマシンの電源をピーク時にオンにし、オフピーク時にオフにします。
- `AutomaticPowerOnForAssignedDuringPeak`プロパティが true に設定されているデリバリーグループに所属するマシンの電源がピーク時にオフになっている場合、自動的にオンにします。

割り当てられたマシンで処理能力バッファがどのように機能するかを理解するには、次のことを考慮してください:

- 処理能力バッファは、デリバリーグループに未割り当てのマシンが 1 つまたは複数ある場合にのみ機能します。
- デリバリーグループ内に未割り当てのマシンがない（すべてのマシンが割り当てられている）場合、処理能力バッファがマシンの電源のオンオフに関与することはなくなります。
- `AutomaticPowerOnForAssignedDuringPeak`プロパティは割り当てられたマシンの電源がピーク時にオンになるかを決定します。true に設定されている場合、Autoscale はピーク時にマシンの電源をオンのままにします。Autoscale は、電源がオフの場合でも電源をオンにします。

電源ポリシー

さまざまなシナリオに合わせてマシンの電源管理ポリシーを構成します。シナリオごとに、待機時間（分単位）と、指定した時間の経過後に実行するアクションを指定できます。電源ポリシーは、シングルセッション OS のランダムデリバリーグループとシングルセッション OS の静的デリバリーグループに適用されます。



切断後およびログオフ後は、以下の設定がピーク時とオフピーク時の両方に適用されます。待ち時間を分単位で設定し、ドロップダウンから何もしない、一時停止、シャットダウンなどのアクションを設定できます。

Autoscale によってマシンの電源がオンになった後、ユーザーがログオンしていない場合、以下の設定がピーク時に適用されます。待ち時間を分単位で設定し、ドロップダウンから何もしない、一時停止、シャットダウンなどのピーク時のアクションを設定できます。

サンプルシナリオ

次のようなシナリオを想定します：

- デリバリーグループの構成。Autoscale が電源管理するデリバリーグループには 10 台のマシンが含まれています（M1～M10）。
- **Autoscale** の構成

  - マシン M1 から M3 までが割り当てられ、マシン M4 から M10 までは未割り当てです。
  - 処理能力バッファはピーク時およびオフピーク時の 10% に設定します。
  - 選択されたスケジュールに従って、Autoscale は午前 9:00 から午後 6:00 までマシンの電源を管理します。

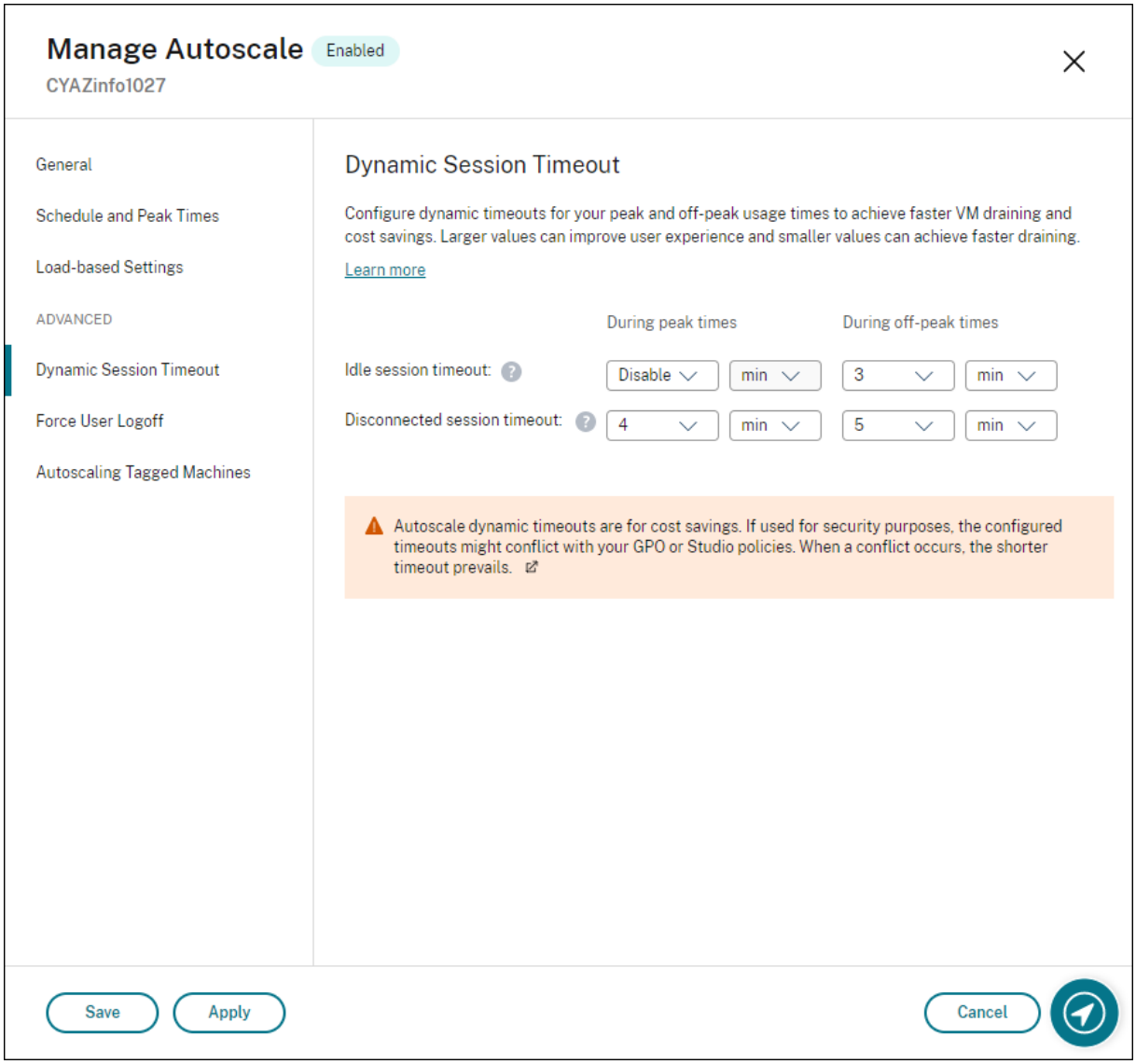
上記のシナリオで Autoscale がどのように機能するかについては、以下を参照してください。

- スケジュールの開始 - 午前 09:00
  - Autoscale は、マシン M1 から M3 までの電源をオンにします。
  - 処理能力バッファが構成されているため、Autoscale が追加のマシン（例：M4）の電源をオンにします。マシン M4 は未割り当てです。
- 最初のユーザーがログオンする
  - デスクトップを使用するためにユーザーが初めてログオンしたときに、電源がオンになった未割り当てのマシンでホストされたデスクトッププールからデスクトップが割り当てられます。この場合、ユーザーにはマシン M4 からデスクトップが割り当てられます。そのユーザーによる以降のログオンでは、最初の使用時に割り当てられたデスクトップに接続します。
  - 処理能力バッファが構成されているため、需要の増大に応じて Autoscale が追加のマシン（例：M5）の電源をオンにします。
- 2 人目のユーザーがログオンする
  - ユーザーには電源がオンになっている未割り当てのマシンからデスクトップが割り当てられます。この場合、ユーザーにはマシン M5 からデスクトップが割り当てられます。そのユーザーによる以降のログオンでは、最初の使用時に割り当てられたデスクトップに接続します。
  - 処理能力バッファが構成されているため、需要の増大に応じて Autoscale が追加のマシン（例：M6）の電源をオンにします。
- ユーザーのログオフ
  - ユーザーがデスクトップからログオフしたり、デスクトップがタイムアウトになると、Autoscale は午前 09:00 から午後 06:00 までマシン M1 から M5 までの電源をオンにしたままにします。これらのユーザーが次回ログオンすると、最初の使用時に割り当てられたものと同じデスクトップに接続されます。
  - 未割り当てのマシン M6 は、未割り当ての新規ユーザーにデスクトップを提供するため待機します。
- スケジュールの終了 - 午後 06:00
  - Autoscale は午後 06:00 にマシン M1 から M5 までの電源をオフにします。
  - 処理能力バッファが構成されているため、Autoscale は未割り当てのマシン M6 の電源をオンにしたままにします。このマシンは、未割り当ての新規ユーザーにデスクトップを提供するため待機しています。
  - このデリバリーグループ内では、マシン M6 から M10 までは未割り当てのマシンです。

動的セッションタイムアウト

August 17, 2024

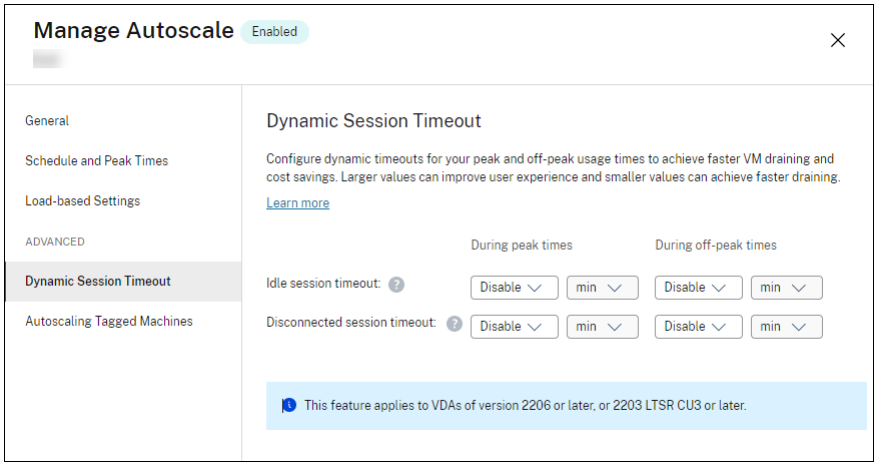
この機能を使用すると、ピーク時とオフピーク時に切断されるセッションとアイドル状態になるセッションのタイムアウトを構成して、マシンのドレインを高速化し、コストを削減できます。この機能は、シングルセッションおよびマルチセッションの OS マシンに適用されます。VDA は、10 分を超えてアイドル状態になっているセッションのアイドル時間を報告するため、動的セッションタイムアウトは、アイドル状態から 10 分以内はアイドル状態のセッションを切断できません。値が小さいほど、残留セッションが早く削除されるため、コストが削減されます。



注:

- この機能は、マルチセッション OS のデリバリーグループでサポートされています。

- シングルセッション OS デリバリーグループの場合、この機能は VDA のバージョン 2206 CR 以降、または 2203 LTSR CU3 以降に適用されます。これらの VDA が Citrix Cloud に最低 1 回は登録されていることを確認してください。使用できない場合、次のユーザーインターフェイスが表示されます:



- Autoscale の動的タイムアウトは、コスト削減のためのオプションです。セキュリティ上の目的で使用すると、構成されたタイムアウトが GPO または［管理］コンソールのポリシーと競合することがあります。競合が発生すると、短いタイムアウトが優先されます。

アイドル状態セッションタイムアウト。ユーザーからの入力がない場合に、中断のないユーザー接続をどのくらい長く維持するのかを指定するタイマーを有効または無効にします。タイマーが時間切れになると、セッションは切断状態になり、［切断されたセッションタイムアウト］が適用されます。［切断されたセッションタイムアウト］が無効な場合、セッションはログオフしません。

重要:

- 10 分（600 秒）以下の値を指定すると、Autoscale は、関連するセッションが 10 分間アイドル状態になった後、それらのセッションを切断します。これは、VDA が報告するセッションアイドル時間に Autoscale が依存しているためです。VDA は、10 分を超えてアイドル状態になっているセッションについてのみアイドル時間を報告します。
- アイドルセッションがタイムアウトに達してから最後の 5 分以内にユーザーがそのセッションと通信した場合、アイドルセッションは切断状態のままになります。

切断されたセッションタイムアウト。切断されたデスクトップをロックしたままセッションがログオフするまでの時間を指定するタイマーを有効または無効にします。有効な場合、タイマーが時間切れになると、切断されたセッションはログオフします。

タグ付けされたマシンの **Autoscale**（クラウドバースト）

August 17, 2024

> 注:
>
> この機能は、以前は Autoscale の制限と呼ばれていました。

はじめに

Autoscale には、デリバリーグループ内のマシンのサブセットのみを電源管理できる柔軟性があります。この場合、1 つまたは複数のマシンにタグを適用し、タグ付きマシンのみを電源管理するように Autoscale を構成します。

この機能はクラウドの処理が増大した場合に有用であり、クラウドベースのリソースで追加の需要（バーストワークロード）が発生する前にオンプレミスのリソース（またはパブリッククラウドのリザーブドインスタンス）を使用してワークロードを処理できます。最初にオンプレミスのマシン（またはリザーブドインスタンス）をワークロードに対応させるには、タグ制限とゾーン優先度を使用する必要があります。

タグ制限は、Autoscale で電源管理されるマシンを指定します。ゾーン優先度では、ユーザーの起動要求を処理する優先ゾーンのマシンを指定します。詳しくは、「タグ」および「ゾーン優先度」を参照してください。

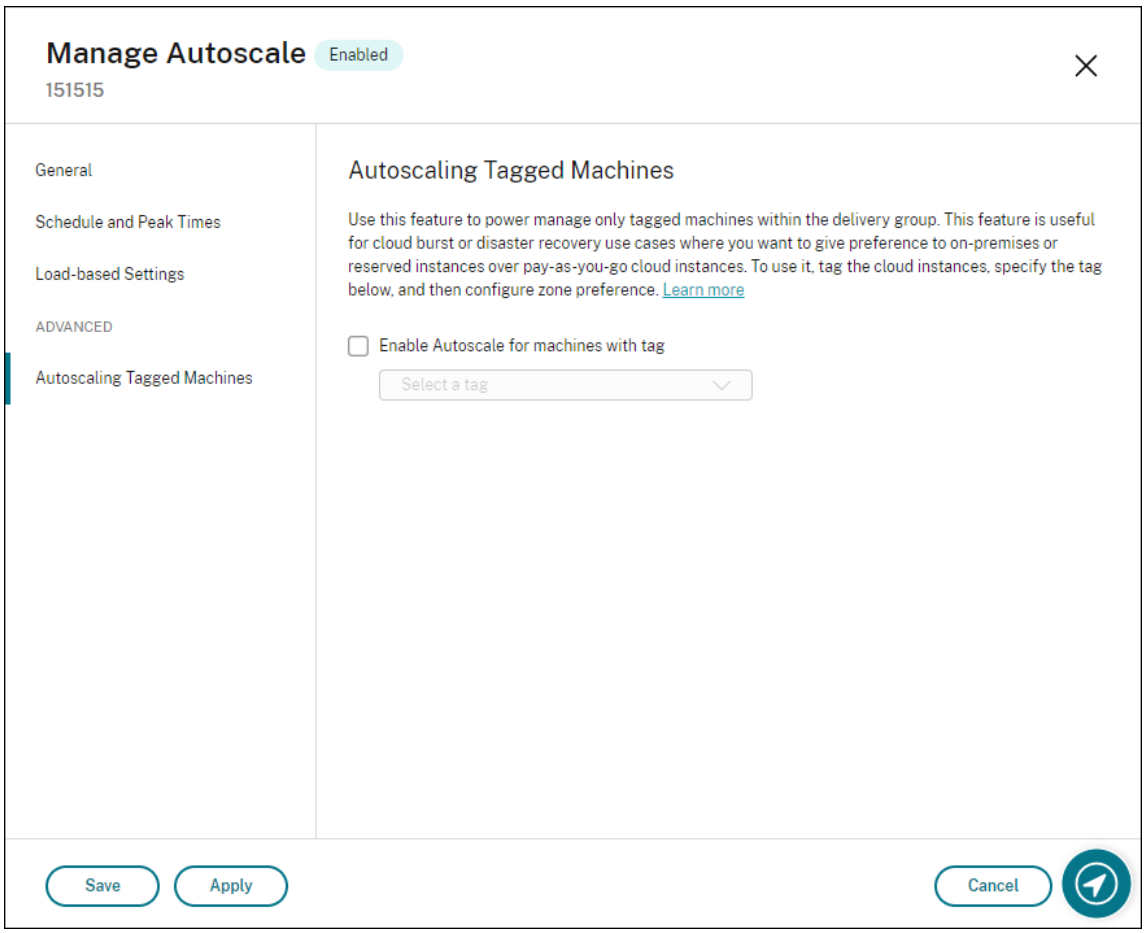
特定のタグ付きマシンをオートスケールするために、［管理］コンソールまたは PowerShell を使用できます。

［管理］コンソールを使用して特定のタグ付きマシンに **Autoscale** を使用する

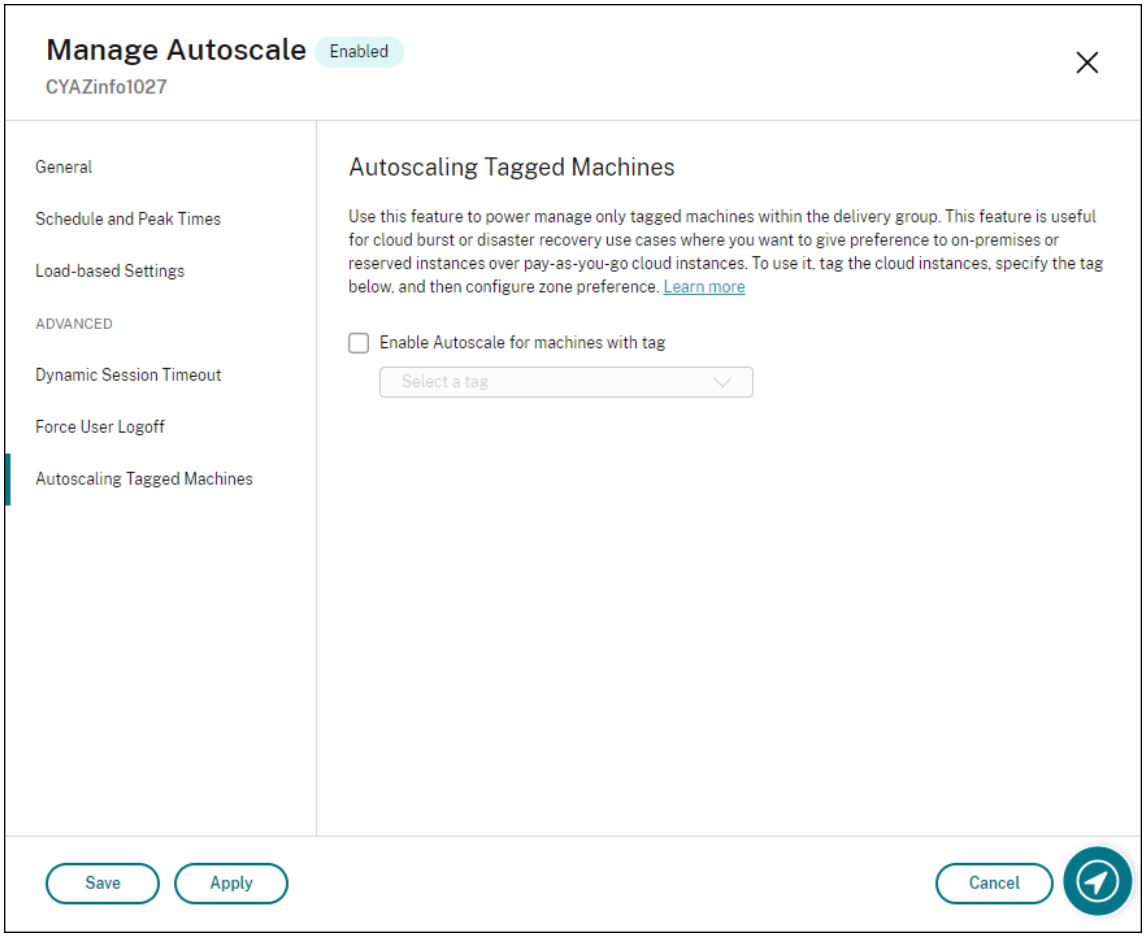
特定のタグ付きマシンに Autoscale を使用には、次の手順を実行します:

1. タグを作成し、そのタグをデリバリーグループ内の該当するマシンに適用します。詳しくは、「タグとタグ制約の管理」を参照してください。
2. デリバリーグループを選択し、**Autoscale** の管理ウィザードを開きます。
3. ［タグ付けされたマシンの **Autoscale**］ページで ［タグ付けされたマシンの **Autoscale** を有効にする］を選択し、一覧からタグを選択します。次に ［適用］をクリックして変更を保存します。

   シングルセッション OS の静的およびランダムのデリバリーグループのユーザーインターフェイス:



マルチセッション *OS* デリバリーグループのユーザーインターフェイス:



警告:

- 特定のタグを持つマシンの Autoscale では、ヒストグラムが自動的に更新され、タグごとのマシンの数に反映される場合があります。［スケジュールとピーク時間］ページで、必要であれば手動で時間枠ごとにマシンを割り当てることができます。
- タグ付きマシンで使用されているタグを削除することはできません。タグを削除するには、最初にタグ制限を削除する必要があります。

タグ制限を適用し、あとからデリバリーグループから削除することができます。これを行うには、［**Autoscale** の管理］**>**［タグ付けされたマシンの **Autoscale**］ページに移動してから、［タグ付けされたマシンの **Autoscale** を有効にする］をオフにします。

警告:

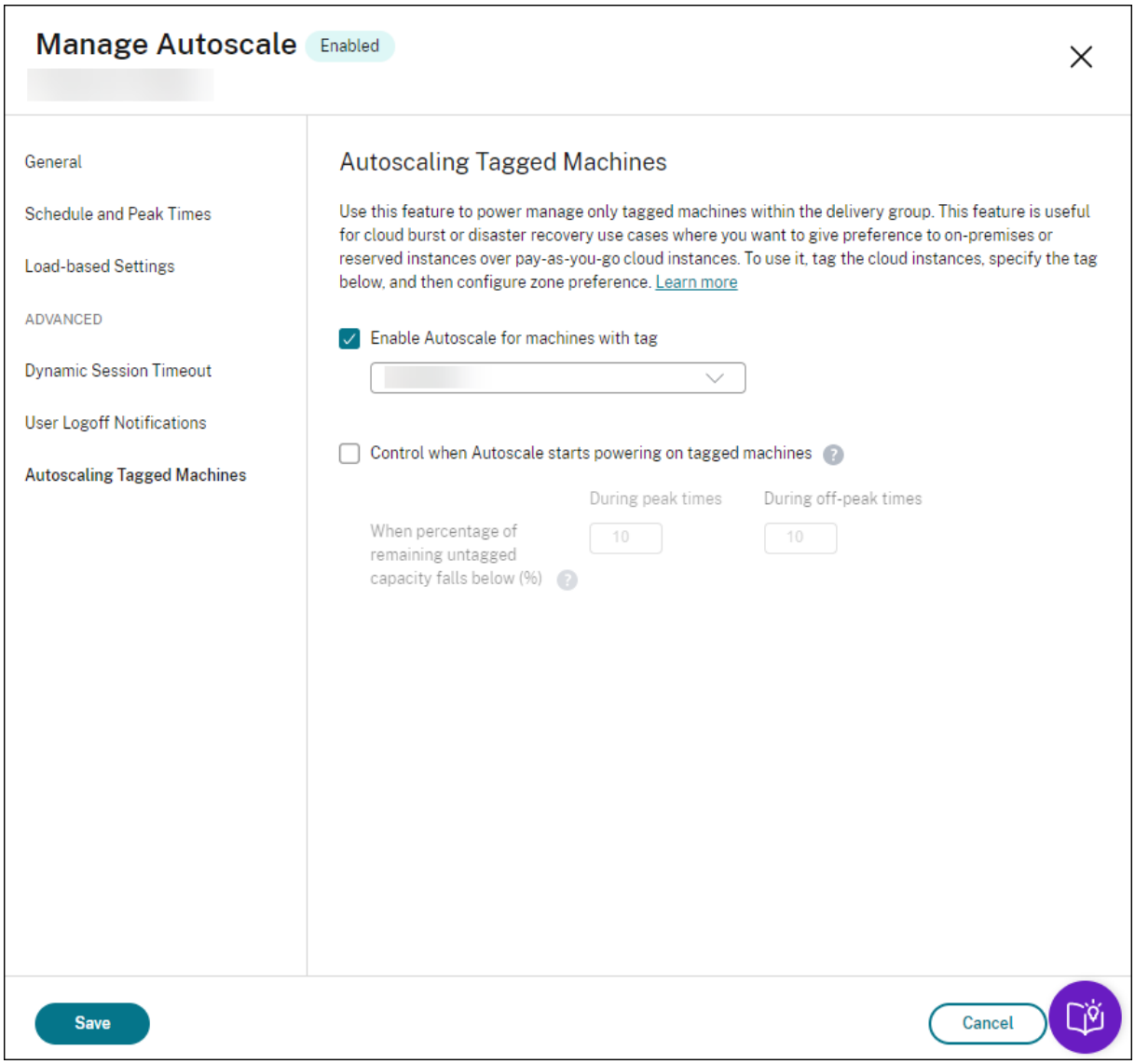
- ［タグ付きマシンの **Autoscale** を有効にする］をオフにしないで該当マシンからタグを削除し、［**Autoscale** の管理］ウィザードを開くと、警告を受け取ることがあります。マシンからタグを削除すると Autoscale で指定したタグが無効になるため、Autoscale が管理するマシンがなくなる可能性があります。警告を解決するには、［タグ付けされたマシンの **Autoscale**］ページで無効なタグを削除し、［適用］をクリックして変更を保存します。

Autoscale がリソースを電源オンするタイミングを制御する

Autoscale は、タグ付けされていないマシンの使用状況に基づいて、タグ付けされたマシンの電源投入を開始するタイミングを制御することもできます。これにより、タグ付きまたはパブリッククラウドのワークロードの消費をさらに最適化できます。

このためには、次の手順を実行します:

1. ［タグ付けされたマシンの **Autoscale**］ページで、［**Autoscale** がタグ付けされたマシンの電源投入を開始するタイミングを制御する］を選択します。
2. ピーク時およびオフピーク時のタグなしマシン使用量のパーセンテージを入力し、［適用］をクリックします。使用できる値：0～100。



> ヒント：
>
> このパーセンテージは、Autoscale によるタグ付けされたマシンの電源投入を開始するタイミングを制御します。パーセンテージがしきい値を下回った場合（デフォルトは 10%）、Autoscale がタグ付けされたマシンの電源投入を開始します。パーセンテージがしきい値を超えると、Autoscale は電源オフモードになります。パーセンテージを入力するときは、次の 2 つのシナリオを考慮してください。
>
> - シングルセッション OS デリバリーグループの場合：この値は、アイドル状態にあるタグなしマシンの総数のパーセンテージで定義されます。例：タグなしのシングルセッション OS マシンが 10 台あるとします。セッションのないマシンが 1 台だけ残っている場合、Autoscale はタグ付けされたマシンの電源を投入し始めます。
> - マルチセッション OS のデリバリーグループの場合：この値は、負荷インデックスを基準とした使用可能なタグなしマシンの合計処理能力のパーセンテージで定義されます。例：タグなしのマルチセッション OS マシンが 10 台あるとします。負荷が 90% になると、Autoscale はタグ付けされたマシンの電源を投入し始めます。

PowerShell を使用して特定のタグ付きマシンを **Autoscale** する

PowerShell SDK を直接使用するには、次の手順を実行します：

1. タグを作成します。New-Brokertag PowerShell コマンドを使用してタグを作成します。
   - 例：`$managed = New-BrokerTag Managed`。この場合、タグの名前は「Managed」です。New-Brokertag PowerShell コマンドについて詳しくは、https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/New-BrokerTag/を参照してください。
2. タグをマシンに適用します。Get-Brokermachine PowerShell コマンドを使用して、Autoscale で電源管理するカタログのマシンにタグを適用します。
   - 例：`Get-BrokerMachine -CatalogName "cloud"| Add-BrokerTag $managed.Name`。この場合、カタログの名前は「cloud」です。
   - Get-Brokermachine PowerShell コマンドについて詳しくは、https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/Get-BrokerMachine/を参照してください。

   > 注：
   >
   > タグの適用後、新しいマシンをカタログに追加できます。タグはこれらの新しいマシンに自動的に適用されません。

3. **Autoscale** で電源管理するデリバリーグループにタグ付きのマシンを追加します。Get-BrokerDesktopGroup PowerShell コマンドを使用して、対象のマシンが含まれるデリバリーグループにタグ制限を追加します（つまり、「X タグでマシンの起動を制限します」）。

- 例: `Get-BrokerDesktopGroup -Uid 1 | Set-BrokerDesktopGroup -RestrictAutoscaleTagUid $managed.Uid`。この場合、デリバリーグループの UID は 1 です。
- Get-BrokerDesktopGroup PowerShell コマンドについて詳しくは、https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/Get-BrokerDesktopGroup/を参照してください。

タグ制限を適用し、あとからデリバリーグループから削除することができます。この場合、Get-BrokerDesktopGroup PowerShell コマンドを使用します。

例:`Get-BrokerDesktopGroup -Uid 1 | Set-BrokerDesktopGroup -RestrictAutoscaleTagU $null`。この場合、デリバリーグループの UID は 1 です。

> 注:
>
> タグなしのマシンは、ユーザーが電源をオフにすると自動的に再起動します。この動作により、ワークロードをより迅速に処理できるようになります。この動作は、`Set-BrokerDesktopGroup` の`AutomaticRestartForUntaggedMachines`プロパティを使用して、デスクトップごとのグループで有効または無効にできます。詳しくは、https://citrix.github.io/delivery-controller-sdk/Broker/Set-BrokerDesktopGroup/を参照してください。

サンプルシナリオ

次のようなシナリオを想定します:

- マシンカタログの構成。2 つのマシンカタログ（C1 と C2）があります。
  - カタログ C1 には、オンプレミス展開でローカルにある 5 台のマシン（M1 から M5）が含まれています。
  - カタログ C2 には、クラウド展開でリモートにある 5 台のマシン（M6 から M10）が含まれています。
- タグ制限。「Cloud」という名前のタグが作成され、カタログ C2 のマシン M6 から M10 に適用されます。
- ゾーン構成。2 つのゾーン（Z1 および Z2）が作成されます。
  - カタログ C1 を含むゾーン Z1 は、オンプレミス展開に対応しています。
  - カタログ C2 を含むゾーン Z2 は、クラウド展開に対応しています。
- デリバリーグループの構成
  - このデリバリーグループには、10 台のマシン（M1 から M10）、カタログ C1 からの 5 台のマシン（M1 から M5）、およびカタログ C2 からの 5 台のマシン（M6 から M10）が含まれます。
  - マシン M1 から M5 は手動で電源をオンにされ、スケジュール全体を通してオンのままになります。
- **Autoscale** の構成
  - 処理能力バッファは 10% に設定します。

  - Autoscale はタグ「Cloud」が付いたマシンのみ電源を管理します。この場合、Autoscale はクラウドマシン M6 から M10 の電源を管理します。

- 公開アプリケーションまたはデスクトップの構成。ゾーン優先度が、たとえば公開デスクトップ用に構成されると、ユーザーの起動要求でゾーン Z1 がゾーン Z2 より優先されます。

  - ゾーン Z1 は、公開デスクトップの優先ゾーン（ホームゾーン）として構成されます。

このシナリオは以下の順序で実行されます：

1. ユーザーはログオンしていません。
2. ユーザーセッションが増加します。
3. ユーザーセッションは、すべてのオンプレミスマシンが消費されるまで増加します。
4. 追加のユーザーセッションが開始されます。
5. セッションの終了により、ユーザーセッションが減少します。
6. ユーザーセッションは、セッションの負荷がオンプレミスマシンによってのみ処理されるようになるまで減少し続けます。

上記のシナリオで Autoscale がどのように機能するかについては、以下を参照してください。

- ユーザー負荷なし（初期の状態）

  - オンプレミスマシン M1 から M5 まですべての電源がオンになっています。
  - クラウド内の 1 台のマシン（たとえば M6）の電源がオンになります。マシンの電源がオンになっているのは、処理能力バッファが構成されているためです。この場合、10（マシン数）×10,000（負荷インデックス）×10%（構成された処理能力バッファ）=10,000 です。したがって、1 台のマシンの電源がオンになります。
  - 電源がオンになっているすべてのマシン（M1 から M6）の負荷インデックス値は基準の負荷（負荷インデックス =0）になっています。

- ユーザーのログオン

  - セッションは構成されたゾーン優先度によってマシン M1 〰 M5 でホストされ、これらのオンプレミスマシン全体で負荷が分散されます。
  - 電源がオンになっているマシン（M1 から M5 まで）の負荷インデックスが増加します。
  - 電源がオンになっているマシン M6 の負荷インデックス値は基準の負荷になっています。

- ユーザーが負荷を増やし、すべてのオンプレミスのリソースを消費

  - セッションは構成されたゾーン優先度によってマシン M1 〰 M5 でホストされ、これらのオンプレミスマシン全体で負荷が分散されます。
  - 電源がオンになっているすべてのマシン（M1 から M5 まで）の負荷インデックスが 10,000 に達します。
  - 電源がオンになっているマシン M6 の負荷インデックス値は基準の負荷のままです。

- さらに 1 人のユーザーがログオン

  - ゾーン優先度がオーバーフローし、セッションはクラウドマシン M6 でホストされます。
  - 電源がオンになっているすべてのマシン（M1 から M5 まで）の負荷インデックスが 10,000 に達します。
  - 電源がオンになっているマシン M6 の負荷インデックス値が上昇し、基準の負荷を超えます。予備の合計処理能力が負荷インデックス基準で 10,000 未満に低下すると、処理能力バッファが構成されているため、需要の増大に応じて Autoscale が追加のマシン（M7）の電源をオンにします。マシン M7 の電源をオンにするまで時間がかかり、準備が整うまで遅延が生じる場合があります。

- さらにユーザーがログオン

  - セッションは、マシン M6 でホストされます。
  - 電源がオンになっているすべてのマシン（M1 から M5 まで）の負荷インデックスが 10,000 に達します。
  - 電源がオンになったマシン M6 の負荷インデックス値がさらに上昇しますが、予備の合計処理能力は、負荷インデックス基準で 10,000 を超えています。
  - 電源がオンになっているマシン M7 の負荷インデックス値は基準の負荷のままです。

- さらに多くのユーザーがログオン

  - マシン M7 の準備が整うと、セッションはマシン M6 および M7 でホストされるようになり、これらのマシン間で負荷が分散されます。
  - 電源がオンになっているすべてのマシン（M1 から M5 まで）の負荷インデックスが 10,000 に達します。
  - マシン M7 の負荷インデックス値は基準の負荷ではなくなります。
  - 電源がオンになっているマシン（M6 と M7）の負荷インデックスが増加します。
  - 予備の合計処理能力は、まだ負荷インデックス基準で 10,000 を超えています。

- セッションの終了によりユーザーセッションの負荷が減少する

  - ユーザーがセッションからログオフした後、またはアイドルセッションがタイムアウトした後、マシン M1 から M7 までの解放された処理能力は他のユーザーが開始したセッションのホストで再利用されます。
  - 予備の合計処理能力が負荷インデックス基準で 10,000 を超えるレベルに増加すると、Autoscale はいずれかのマシン（例：M6 〰 M7）をドレイン状態にします。その結果、他のユーザーによって開始されたセッションは、（ユーザー負荷が再度増大する、または他のクラウドマシンの負荷が最小になるなど）新しい変更が行われない限り、そのマシン（M7 など）に送信されなくなります。

- 1 つまたは複数のクラウドマシンが不要になるまで、ユーザーセッションの負荷はさらに減少します。

  - マシン M7 上のすべてのセッションが終了し、指定された電源オフの遅延でタイムアウトになると、Autoscale はマシン M7 の電源をオフにします。
  - 電源がオンになっているマシン（M1 から M5 まで）の負荷インデックスが 10,000 を下回るレベルに下降します。
  - 電源がオンになっているマシン（M6）の負荷インデックスが減少します。

- クラウドマシンが不要になるまで、ユーザーセッションの負荷はさらに減少します。
  - マシン M6 にユーザーセッションがない場合でも、Autoscale は予備の処理能力用に確保しているため電源をオフにしません。
  - 処理能力バッファが構成されているため、Autoscale は残されたクラウドマシン M6 の電源をオンにしたままにします。このマシンは、新規ユーザーにデスクトップを提供するため待機しています。
  - セッションは、オンプレミスマシンに利用できる処理能力がある限り、マシン M6 でホストされません。

ユーザーログオフ通知（旧称ユーザー強制ログオフ）

August 17, 2024

> 重要:
>
> この機能は、デリバリーグループベースのマルチセッションアプリ用の Autoscale ユーザーインターフェイスでのみ使用可能です。

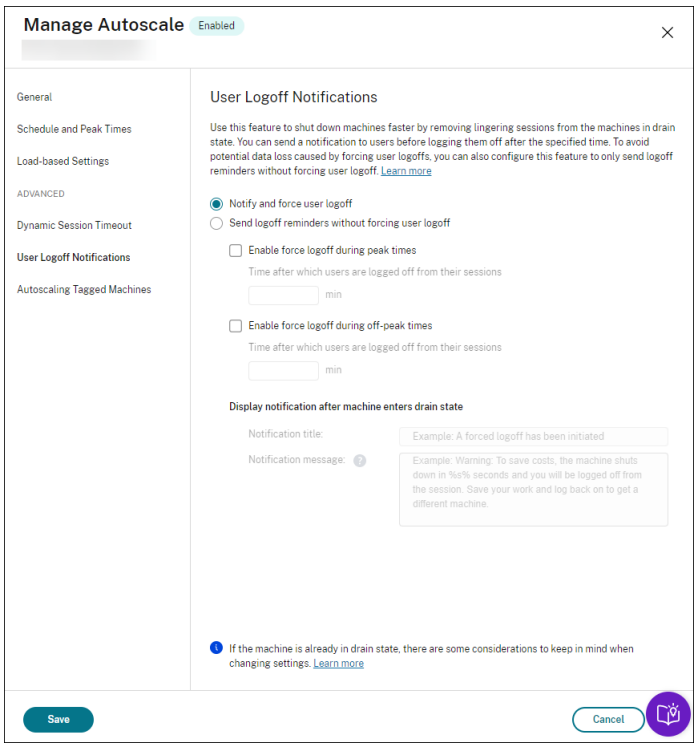
適切なコスト削減のために、Autoscale では、管理者が残留セッションからのログオフを強制することができます。この場合、管理者がカスタム通知をユーザーに送信でき、セッションが強制的にログオフされた後の猶予期間を設定できます。これは、ドレイン状態のマシンに対してのみ実行され、電源がオンになっているマシンすべてに対しては実行されません。ユーザーを強制ログオフすることで生じるデータ損失の可能性を避けるため、代わりに、ユーザーを強制ログオフせずにログオフリマインダーを送信するだけにすることもできます。

次の 2 つのオプションが使用できます:

- ユーザーに通知して強制ログオフする
- ユーザーを強制的にログオフせずにログオフリマインダーを送信する

ユーザーに通知して強制ログオフする

これを選択した場合、下記で指定する時間が経過すると、Autoscale はユーザーをセッションからログオフします。



ピーク時の強制ログオフを有効にする。これを選択した場合、ピーク時に指定された時間が経過すると、Autoscale はユーザーをセッションからログオフします。

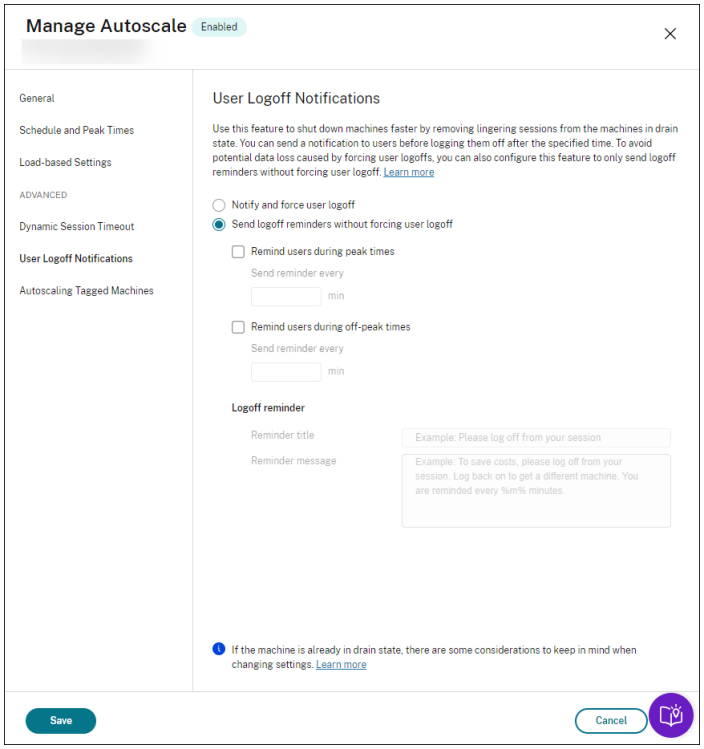
オフピーク時の強制ログオフを有効にする。これを選択した場合、オフピーク時に指定された時間が経過すると、Autoscale はユーザーをセッションからログオフします。

マシンがドレイン状態になった後に通知を表示する。ユーザーのマシンがドレイン状態になった後、ユーザーに通知を送信できます。

- 通知タイトル。ユーザーに送信する通知のタイトルを指定できます。例: `A forced logoff has been initiated.`
- 通知メッセージ。ユーザーに送信する通知の内容を指定できます。%s% または%m% を変数として使用して、メッセージで指定された時間を示すことができます。時間を秒単位で表すには、%s% を使用します。時間を分単位で表すには、%m% を使用します。例: `Warning: To save costs, the machine shuts down in %s% seconds and you will be logged off from the session. Save your work and log back on to get a different machine.`

ユーザーを強制的にログオフせずにログオフリマインダーを送信する

これを選択した場合、ユーザーは、マシンがドレイン状態になった後にマシンからログオフされる旨のリマインダーを受け取ります。このリマインダーは、下記で指定する間隔で送信されるように構成できます。



ピーク時にユーザーにリマインダーを送付する。これを選択した場合、ユーザーは、ピーク時にセッションからログオフされる旨のリマインダーを X 分ごとに受け取ります（X は指定した時間）。

オフピーク時にユーザーにリマインダーを送付する。これを選択した場合、ユーザーは、オフピーク時にセッションからログオフされる旨のリマインダーを X 分ごとに受け取ります（X は指定した時間）。

ログオフリマインダー。ユーザーのマシンがドレイン状態になった後、ユーザーにリマインダーを送信するように構成できます。

- リマインダーの件名。ユーザーに送信するリマインダーのタイトルを指定できます。例：`Please log off from your session`。
- リマインダーメッセージ。ユーザーに送信するメッセージを指定できます。例：`Please log off from your session and log back on to save costs`。

注意事項

マシンが既にドレイン状態にある場合は、設定を変更するときに次の点を考慮してください：

- ［ユーザーを強制的にログオフせずにログオフリマインダーを送信する］を ［ユーザーに通知して強制ログオフする］に変更すると、この新しい設定がすぐに有効になります。
- ［ユーザーに通知して強制ログオフする］を ［ユーザーを強制的にログオフせずにログオフリマインダーを送信する］に変更した場合、この新しい設定は、次にマシンがドレイン状態になるまで有効になりません。引き続き、ユーザーは強制的にログオフされます。

Broker PowerShell SDK コマンド

August 17, 2024

Broker PowerShell SDK を使用してデリバリーグループの Autoscale を構成できます。PowerShell コマンドを使用して Autoscale を構成するには、PowerShell SDK バージョン 7.21.0.12 以降を使用する必要があります。PowerShell SDK について詳しくは、「SDK および API」を参照してください。

Set-BrokerDesktopGroup

既存の BrokerDesktopGroup の有効化と無効化を切り替えるか、またはグループの設定を変更します。このコマンドレットについて詳しくは、https://citrix.github.io/delivery-controller-sdk/Broker/Set-BrokerDesktopGroup/を参照してください。

例

PowerShell コマンドレットの使用方法について詳しくは、以下の例を参照してください:

Autoscale の有効化

- 「MyDesktop」という名前のデリバリーグループに対して Autoscale を有効にする場合、PowerShell コマンドSet-BrokerDesktopGroupを使用します。例:

```
- PS C:\> Set-BrokerDesktopGroup "MyDesktop"-AutoscalingEnabled
  $true
```

ピーク時とオフピーク時で個別に処理能力バッファを構成する

- 「MyDesktop」という名前のデリバリーグループに対して、ピーク時には処理能力バッファを 20% に、オフピーク時には 10% に設定する場合、PowerShell コマンドSet-BrokerDesktopGroupを使用します。例:

```
- PS C:\> Set-BrokerDesktopGroup "MyDesktop"-PeakBufferSizePercent
  20 -OffPeakBufferSizePercent 10
```

切断時のタイムアウト設定の構成

- 「MyDesktop」という名前のデリバリーグループに対して切断時のタイムアウトの値を、ピーク時には 60 分に、オフピーク時には 30 分に設定する場合、PowerShell コマンドSet-BrokerDesktopGroupを使用します。例:

```
- PS C:\> Set-BrokerDesktopGroup "MyDesktop"-PeakDisconnectTimeout
  60 -OffPeakDisconnectTimeout 30
```


ログオフ時のタイムアウト設定の構成

- 「MyDesktop」という名前のデリバリーグループに対してログオフ時のタイムアウトの値を、ピーク時には 60 分に、オフピーク時には 30 分に設定する場合、PowerShell コマンドSet-BrokerDesktopGroupを使用します。例:

  - ```
    PS C:\> Set-BrokerDesktopGroup "MyDesktop"-PeakLogOffTimeout
    60 -OffPeakLogOffTimeout 30
    ```

電源オフの遅延設定の構成

- 「MyDesktop」という名前のデリバリーグループに対して、電源オフの遅延を 15 分に設定する場合、PowerShell コマンドSet-BrokerDesktopGroupを使用します。例:

  - ```
    PS C:\> Set-BrokerDesktopGroup "MyDesktop"-PowerOffDelay 15
    ```

電源オフの遅延が有効にならない期間の構成

- 「MyDesktop」という名前のデリバリーグループに対して、電源オフの遅延を 30 分が経過してから有効に設定する場合、PowerShell コマンドSet-BrokerDesktopGroupを使用します。例:

  - ```
    C:\PS> Set-BrokerDesktopGroup "MyDesktop"-SettlementPeriodBeforeAutoSh
    30。
    ```

マシンインスタンスコスト設定の構成

- 「MyDesktop」という名前のデリバリーグループに対して、1 時間あたりのマシンインスタンスコストを 0.2 ドルに設定する場合、PowerShell コマンドSet-BrokerDesktopGroupを使用します。例:

  - ```
    PS C:\> Set-BrokerDesktopGroup "MyDesktop"-MachineCost 0.2
    ```

New-BrokerPowerTimeScheme

デリバリーグループ用に BrokerPowerTimeScheme を作成します。詳しくは、https://citrix.github.io/delivery-controller-sdk/Broker/New-BrokerPowerTimeScheme/を参照してください。

例

UID 値が 3 のデリバリーグループに対して、電源時間スキームを作成する場合、新しいスキームで週末、月曜日、火曜日を指定します。これらの曜日で、午前 8:00 から午後 6:30 の時間枠をピーク時間として定義します。ピーク時のプールサイズ（電源をオンにしたままにするマシンの数）は 20 で、オフピーク時は 5 です。PowerShell コマンドのSet-BrokerDesktopGroupを使用できます。例:

- ```
  PS C:\> $ps48=(0..47 | %{ if ($_ -lt 16 -or $_ -gt 37){ 5 } else
  { 20 } } )
  ```


  ```

- `PS C:\> $pt48=(0..47 | %{ if ($_ -lt 16 -or $_ -gt 37){ $false } else { $true } } )`
- `PS C:\> New-BrokerPowerTimeScheme -Name 'First Half Week'-DaysOfWeek Weekend,Monday,Tuesday -DesktopGroupUid 3 -PeakHalfHours $pt48 -PoolSize $ps48`

動的セッションタイムアウトのパラメーター

次の Broker PowerShell SDK コマンドレットは、動的セッションタイムアウト用に拡張され、複数の新しいパラメーターをサポートします:

- Get-BrokerDesktopGroup
- New-BrokerDesktopGroup
- Set-BrokerDesktopGroup

これらのパラメーターには次が含まれます:

- **DisconnectPeakIdleSessionAfterSeconds** - ピーク時にアイドル状態のセッションが切断されるまでの時間を秒単位で表します。このプロパティのデフォルト値は 0 です。これは、関連する動作がピーク時に無効になっていることを示します。0 より大きい値は、ピーク時のデリバリーグループの動作のみを有効にします。
- **DisconnectOffPeakIdleSessionAfterSeconds** - オフピーク時にアイドル状態のセッションが切断されるまでの時間を秒単位で表します。このプロパティのデフォルト値は 0 です。これは、関連する動作がオフピーク時に無効になっていることを示します。0 より大きい値は、オフピーク時のデリバリーグループの関連する動作のみを有効にします。
- **LogoffPeakDisconnectedSessionAfterSeconds** - ピーク時に切断されたセッションが終了するまでの時間を秒単位で表します。このプロパティのデフォルト値は 0 です。これは、関連する動作がピーク時に無効になっていることを示します。0 より大きい値は、ピーク時のデリバリーグループの関連する動作のみを有効にします。
- **LogoffOffPeakDisconnectedSessionAfterSeconds** - オフピーク時に切断されたセッションが終了するまでの時間を秒単位で表します。このプロパティのデフォルト値は 0 です。これは、関連する動作がオフピーク時に無効になっていることを示します。0 より大きい値は、オフピーク時のデリバリーグループの関連する動作のみを有効にします。

例

「MyDesktop」という名前のデリバリーグループについて、ピーク時のアイドル状態セッションタイムアウトを 3,600 秒に設定するとします。PowerShell コマンド`Set-BrokerDesktopGroup`を使用します。例:

- `C:\PS> Set-BrokerDesktopGroup "MyDesktop"-DisconnectOffPeakIdleSessionAfte`
  `3600`

これにより、「MyDesktop」という名前のデスクトップグループで、オフピーク時に 1 時間を超えてアイドル状態になっているセッションが切断されます。

## Citrix Insight Services

August 17, 2024

Citrix Insight Services（CIS）は、計測を行って利用統計情報を収集し、ビジネス洞察を得るための、Citrix が提供するプラットフォームです。この計測機能と利用統計情報機能を使用することで、技術ユーザー（顧客、パートナー、エンジニア）は自己診断を行い、問題を解決し、環境を最適化することができます。CIS の詳細、最新情報、および機能について詳しくは、https://cis.citrix.comを参照してください（Citrix アカウントの資格情報が必要です）。

Citrix にアップロードされた情報はすべて、トラブルシューティングや診断、および以下の対象となる製品の品質、信頼性、パフォーマンス向上を目的として使用されます。

- Citrix Insight Services ポリシー：https://cis.citrix.com/legal
- Citrix のプライバシーポリシー：https://www.cloud.com/privacy-policy

Citrix Virtual Apps and Desktops のリリースでは、以下の技術がサポートされます。

- Citrix Virtual Apps and Desktops のインストールとアップグレードの分析機能
- Citrix カスタマーエクスペリエンス向上プログラム（CEIP）
- Citrix Call Home
- Citrix Scout

CIS および Citrix Analytics に追加（および別途）：Studio をインストール（またはアップグレード）すると、Google Analytics が自動的に収集され（後でアップロードされ）ます。Studio をインストールした後、レジストリキー HKEY_LOCAL_MACHINE\Software\Citrix\DesktopStudio\GAEnabled でこの設定を変更できます。値 1 で収集とアップロードを有効にし、0 で収集とアップロードを無効にします。

### インストールとアップグレード分析

全製品インストーラーを使用して Citrix Virtual Apps and Desktops コンポーネントを展開またはアップグレードする場合、インストールプロセスに関する匿名の情報が、コンポーネントをインストール/アップグレードするマシンで収集および保存されます。このデータは、インストールに関する Citrix カスタマーエクスペリエンス向上のために使用されます。

この情報は、ローカルの%ProgramData%\Citrix\CTQs に保存されます。

このデータの自動アップロードは、全製品インストーラーのグラフィックおよびコマンドラインインターフェイスの両方で、デフォルトで有効です。

- デフォルト値はレジストリ設定で変更できます。インストール/アップグレードの前にレジストリ設定を変更すると、全製品インストーラーの使用時にその値が使用されます。
- コマンドラインインターフェイスを使用して、コマンドにオプションを指定してインストール/アップグレードする場合、デフォルト設定をオーバーライドできます。

自動アップロードの制御:

- インストール/アップグレード分析の自動アップロードを制御するレジストリ設定（デフォルト = 1）:
  - 場所: HKEY_LOCAL_MACHINE\Software\Citrix\MetaInstall
  - 値の名前: SendExperienceMetrics
  - 値: 0 = 無効、1 = 有効
- PowerShell を使用する場合、次のコマンドレットはインストール/アップグレード分析機能の自動アップロードを無効にします。

```
New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\MetaInstall -Name
    SendExperienceMetrics -PropertyType DWORD -Value 0
```

- XenDesktopServerSetup.exe または XenDesktopVDASetup.exe コマンドで自動アップロードを無効にするには、/disableexperiencemetricsオプションを含めます。

  XenDesktopServerSetup.exe または XenDesktopVDASetup.exe コマンドで自動アップロードを有効にするには、/sendexperiencemetricsオプションを含めます。

Citrix カスタマーエクスペリエンス向上プログラム

Citrix カスタマーエクスペリエンス向上プログラム（CEIP）に参加すると、匿名の統計および使用状況情報が、Citrix 製品の品質およびパフォーマンスを向上させる目的で送信されます。詳しくは、https://more.citrix.com/XD-CEIPを参照してください。

サイトの作成中またはアップグレード中の登録

CEIP には、サイトの作成時に自動で登録されます（最初の Delivery Controller のインストール後）。サイトの作成からおよそ 7 日後に、初回データアップロードが行われます。

登録は、サイトの作成後にいつでも取り消すことができます。Web Studio の左側のペイン（[設定] ノードを選択し、**Citrix** カスタマーエクスペリエンス向上プログラムの設定をオフにします。

Citrix Virtual Apps and Desktops 環境をアップグレードする場合:

- CEIP をサポートしないバージョンからアップグレードする場合、参加するかどうかを確認するメッセージが表示されます。

- CEIP をサポートするバージョンからアップグレードし、参加が有効になっていた場合、CEIP はアップグレードしたサイトで有効になります。
- CEIP をサポートするバージョンからアップグレードし、参加が無効になっていた場合、CEIP はアップグレードしたサイトで無効になります。
- CEIP をサポートするバージョンからアップグレードし、参加が不明な場合、参加するかどうかを確認するメッセージが表示されます。

収集された情報は匿名になるため、Citrix Insight Services へのアップグレード後は表示されません。

VDA のインストール時の登録

デフォルトでは、ユーザーは Windows VDA のインストール時に CEIP に自動登録されます。このデフォルトはレジストリ設定で変更できます。VDA インストールの前にレジストリ設定を変更すると、その値が使用されます。

CEIP への自動登録を制御するレジストリ設定（デフォルト = 1）:

場所：HKEY_LOCAL_MACHINE\Software\Citrix\Telemetry\CEIP
値の名前：Enabled
値：0 = 無効、1 = 有効

デフォルトでは、レジストリに`Enabled`プロパティは表示されません。未指定のままの場合、自動アップロード機能は有効です。

PowerShell を使用する場合、次のコマンドレットは CEIP への登録を無効にします。

```
New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\Telemetry\CEIP -Name
    Enabled -PropertyType DWORD -Value 0
```

収集されたランタイムデータポイントは、定期的に出力フォルダ（デフォルトは%programdata%/Citrix/VdaCeip）にファイルとして書き込まれます。

VDA のインストールからおよそ 7 日後に、初回データアップロードが行われます。

他の製品およびコンポーネントのインストール時の登録

CEIP へは、関連する Citrix 製品、コンポーネント、テクノロジ（Citrix Provisioning、AppDNA、Citrix ライセンスサーバー、Windows 向け Citrix Workspace アプリ、ユニバーサルプリントサーバー、Session Recording）のインストール時にも参加できます。インストールと参加のデフォルト値について詳しくは、該当のドキュメントを参照してください。

Citrix Call Home

Citrix Virtual Apps and Desktops で特定のコンポーネントおよび機能をインストールする場合、Citrix Call Home に参加するかどうかを選択できるページが表示されます。Call Home は診断データを収集し、その後その

データを含む利用統計情報パッケージを、分析およびトラブルシューティングの目的で定期的に Citrix Insight Services に直接アップロードします（デフォルトポート 443 上の HTTPS 経由）。

Citrix Virtual Apps and Desktops では、Call Home は Citrix Telemetry Service という名前のバックグラウンドサービスとして実行されます。詳しくは、https://more.citrix.com/XD-CALLHOMEを参照してください。

Citrix Scout では、Call Home のスケジュール機能も使用できます。詳しくは、「Citrix Scout」を参照してください。

収集される項目

Citrix Diagnostic Facility（CDF）トレースは、トラブルシューティングに役立つ情報を記録します。Call Home は、一般的な障害（VDA の登録やアプリケーション/デスクトップの起動など）のトラブルシューティングに役立つ CDF トレースのサブセットを収集します。このテクノロジは、常時トレース（AOT）と呼ばれます。AOT ログは C:\Users\CitrixTelemetryService\Appdata\Local\CitrixAOT に保存されます。

Call Home ではその他の Event Tracing for Windows（ETW）情報が収集されることはなく、収集されるように設定することもできません。

また、Call Home では以下の情報も収集されます：

- Citrix Virtual Apps and Desktops によって`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix`に作成されたレジストリ
- Citrix 名前空間の Windows Management Instrumentation（WMI）情報。
- 実行中のプロセス一覧
- %PROGRAM DATA%\Citrix\CDF に保存されている Citrix プロセスのクラッシュダンプ
- インストールとアップグレードの情報これには、製品全体の Metainstaller ログ、失敗した MSI ログ、MSI ログアナライザーからの出力、StoreFront ログ、ライセンスの互換性チェックログ、サイトの事前アップグレードテストの結果が含まれます。

トレース情報は収集時に圧縮されます。Citrix Telemetry Service は、最長 8 日間、圧縮されたトレース情報を最大 10MB 保持します。

- データを圧縮することで、Call Home の VDA 上の占有領域を小さくできます。
- プロビジョニングされたマシンでの IOP を避けるため、トレースはメモリで保持されます。
- トレースバッファーでは、循環メカニズムを使用してトレースがメモリで保持されます。

Call Home は、「Call Home のキーデータポイント」に記載されているキーデータポイントを収集します。

サマリーの構成と管理

全製品インストールウィザードの使用時、またはそれ以降に、PowerShell コマンドレットを使用して、Call Home に登録することができます。登録すると、デフォルトで、ローカルタイムの毎日曜日午前 3 時頃に診断情報が収集さ

れ、Citrix にアップロードされます。アップロードは、指定された時間の前後 2 時間以内に行われます。つまり、デフォルトのスケジュールの場合、アップロードは午前 3 時から午前 5 時の間に行われます。

診断情報をスケジュールベースでアップロードしない場合（またはスケジュールを変更する場合）は、PowerShell コマンドレットを使用して診断情報を手動で収集し、アップロードするかローカルに保存してください。

Call Home のスケジュールによるアップロード登録する場合、および診断情報を手動で Citrix にアップロードする場合は、Citrix のアカウントまたは Citrix Cloud の資格情報を入力します。Citrix は、アカウント資格情報を、顧客の識別とデータのアップロードに使用されるアップロードトークンに交換します。アカウント資格情報は保存されません。

アップロードが実行されると、Citrix アカウントに関連付けられたアドレスに通知メールが送信されます。

コンポーネントのインストール時に Call Home を有効にした場合、後で無効にできます。

前提条件

- PowerShell 3.0 またはそれ以降が実行されている必要があります。
- Citrix Telemetry Service が実行されている必要があります。
- システム変数`PSModulePath`は、C:\Program Files\Citrix\Telemetry Service\などの、Telemetry のインストールパスに設定する必要があります。

コンポーネントインストール時の **Call Home** の有効化

VDA のインストールまたはアップグレード時：全製品インストーラーのグラフィカルインターフェイスを使用して Virtual Delivery Agent をインストールまたはアップグレードする場合には、Call Home に参加するかどうかを確認するメッセージが表示されます。2 つのオプションがあります：

- Call Home に参加します。
- Call Home に参加しません。

VDA をアップグレードしていて、Call Home に以前参加していた場合には、そのウィザードページは表示されません。

Controller のインストールまたはアップグレード時：グラフィカルインターフェイスを使用して Delivery Controller をインストールまたはアップグレードする場合には、Call Home に参加するかどうかを確認するメッセージが表示されます。3 つのオプションがあります。

Controller をインストールする場合、そのサーバーがポリシー設定「サービスとしてログオン」が適用される Active Directory GPO を持っていると、インストールウィザードで Call Home ページ上の情報を構成できません。詳しくは、CTX218094を参照してください。

Controller をアップグレードしていて、Call Home に以前登録していた場合、参加確認のメッセージは表示されません。

PowerShell コマンドレット

各コマンドレットの説明や、上記の一般的なユースケースでは使用されないパラメーターを含む包括的な構文は、PowerShell ヘルプに記載されています。

プロキシサーバーを使用してアップグレードする方法については、「プロキシサーバーの構成」を参照してください。

- スケジュールによるアップロードの有効化：収集された診断情報は、Citrix に自動的にアップロードされます。カスタムスケジュール用の追加のコマンドレットを入力しない場合、デフォルトのスケジュールが使用されます。

  ```
  $cred = Get-Credential
  Enable-CitrixCallHome -Credential $cred
  ```

  スケジュールによるアップロードが有効になっていることを確認するには、「`Get-CitrixCallHomeGet-CitrixCallHome`」と入力します。有効な場合は、「`IsEnabled=True`」および「`IsMasterImage=False`」が返されます。

- マスターイメージから作成されたマシンでのスケジュールによるアップロードの有効化：マスターイメージでのスケジュールによるアップロードを有効にすると、マシンカタログで作成された各マシンを構成する必要がなくなります。

  ```
  Enable-CitrixCallHome -Credential $cred -MasterImage
  ```

  スケジュールによるアップロードが有効になっていることを確認するには「**Get-CitrixCallHome**」と入力します。有効な場合は、「`IsEnabled=True`」および「`IsMasterImage=True`」が返されます。

- カスタムスケジュールの作成：診断情報の収集およびアップロードのスケジュールを、日次または週次で作成できます。

  ```
  $timespan = New-TimeSpan -Hours hours -Minutes minutes
  Set-CitrixCallHomeSchedule -TimeOfDay $timespan -DayOfWeek day
     -UploadFrequency {
  Daily|Weekly }
  ```

例：

次のコマンドレットでは、毎日午後 10 時 20 分にデータを収集してアップロードするスケジュールが作成されます。Hours パラメーターには、24 時間形式を使用します。`UploadFrequency`パラメーターの値が Daily の場合、`DayOfWeek`パラメーターは無視されます（指定されている場合）。

```
$timespan - New-TimeSpan -Hours 22 -Minutes 20
Set-CitrixCallHomeSchedule -TimeOfDay $timespan -UploadFrequency Daily
```

スケジュールを確認するには、「`Get-CitrixCallHomeSchedule`」と入力します。上記の例では、「`StartTime=22:20:00, DayOfWeek=Sunday (ignored), Upload Frequency=Daily`」が返される必要があります。

以下のコマンドレットでは、毎週水曜日の午後 10 時 20 分にデータを収集してアップロードするスケジュールが作成されます。

```
$timespan - New-TimeSpan -Hours 22 -Minutes 20
Set-CitrixCallHomeSchedule -TimeOfDay $timespan -DayOfWeek Wed -
    UploadFrequency Weekly
```

スケジュールを確認するには、「Get-CitrixCallHomeSchedule」と入力します。上記の例では、「StartTime=22:20:00, DayOfWeek=Wednesday, Upload Frequency=Weekly」が返される必要があります。

Call Home の無効化

Call Home を無効にするには、PowerShell コマンドレットか Citrix Scout を使用します。

AOT ログは、Call Home のスケジュールによるアップロードが無効な場合でも収集されディスクに保存されます。(スケジュールによるアップロードが無効な場合、AOT ログは自動的に Citrix にアップロードされません。) AOT ログの収集およびローカル保存は無効化できます。

PowerShell で Call Home を無効にする　以下のコマンドレットを実行すると、診断データは自動的に Citrix にアップロードされません。(キャンセル後も、Citrix Scout または Telemetry の PowerShell コマンドレットを使用した診断データのアップロードは実行できます)。

```
Disable-CitrixCallHome
```

Call Home が無効になったことを確認するには、Get-CitrixCallHomeを入力します。無効な場合は、「IsEnabled=False」および「IsMasterImage=False」が返されます。

Citrix Scout を使用して収集スケジュールを無効にする　Citrix Scout を使用して診断収集スケジュールを無効にするには、「収集スケジュールの設定」のガイドに従います。手順 3 で、[**Off**] をクリックして選択したマシンのスケジュールをキャンセルします。

AOT ログの収集を無効にする　以下のコマンドレットを実行すると (Enabledフィールドを**false**に設定)、AOT ログは収集されません。

```
Enable-CitrixTrace -Listen'{ "trace":{ "enabled":false,"persistDirectory
":"C:\Users\Public","maxSizeBytes":1000000, "sliceDurationSeconds
":300 } } '
```

Listenパラメーターには JSON 形式の引数が含まれます。

Call Home のアップロードのためにプロキシサーバーを構成

Call Home が有効に設定されたマシンで、以下のタスクを実行します。以下の手順のサンプル図では、サーバーアドレスおよびポートは 10.158.139.37:3128 となっています。お客様の情報はこれとは異なります。

1. Web ブラウザーにプロキシサーバー情報を追加します。Internet Explorer で、［インターネットオプション］**>**［接続］**>**［**LAN** の設定］の順に選択します。［**LAN** にプロキシサーバーを使用する］をオンにして、プロキシサーバーのアドレスとポート番号を入力します。
2. PowerShell で「`netsh winhttp import proxy source=ie`」を実行します。

```
PS C:\Users\administrator.JLGXH> netsh winhttp import proxy source=ie

Current WinHTTP proxy settings:

    Proxy Server(s) :  10.108.124.245:8080
    Bypass List     :  (none)
```

3. テキストエディターを使用して、TelemetryService.exe 構成ファイルを編集します。このファイルは、C:\Program Files\Citrix\Telemetry Service にあります。以下の赤い枠内の情報を追加します。

```
TelemetryService.exe - Notepad
File  Edit  Format  View  Help
<?xml version="1.0" encoding="utf-8"?>
<configuration>
    <startup>
                <supportedRuntime version="v4.0" sku=".NETFramework,Version=v4.5.1" />
    </startup>
    <runtime>
      <assemblyBinding xmlns="urn:schemas-microsoft-com:asm.v1">
        <dependentAssembly>
          <assemblyIdentity name="Newtonsoft.Json" culture="neutral" publicKeyToken="30ad4fe6b2a6aeed" />
          <bindingRedirect oldVersion="0.0.0.0-9.0.0.0" newVersion="9.0.0.0" />
        </dependentAssembly>
        <probing privatePath="TelemetryModule" />
      </assemblyBinding>
    </runtime>
<system.net>
<defaultProxy>
<proxy bypassonlocal="false" usesystemdefault="true" proxyaddress="http://10.108.124.245:8080" />
</defaultProxy>
</system.net>

</configuration>
```

4. Telemetry Service を再起動します。

PowerShell で Call Home コマンドレットを実行します。

手動による診断情報の収集およびアップロード

CIS Web サイトを使用して、診断情報のバンドルを CIS にアップロードすることができます。PowerShell コマンドレットを使って、診断情報を収集して CIS にアップロードすることもできます。

CIS Web サイトを使用してバンドルをアップロードするには、以下の手順に従います。

1. Citrix のアカウント資格情報を使用して Citrix Insight Services にログオンします。
2. [**My Workspace**] を選択します。
3. [**Healthcheck**] を選択し、次にデータの場所に移動します。

CIS では、データのアップロードを管理する複数の PowerShell コマンドレットがサポートされます。このドキュメントでは、2 つの一般的なケースにおけるコマンドレットについて説明します。

- `Start-CitrixCallHomeUpload`コマンドレットを使用して、診断情報のパッケージを手動で収集して CIS にアップロードします。(パッケージはローカルには保存されません)。
- `Start-CitrixCallHomeUpload`コマンドレットを使用して、手動でデータを収集し、診断情報のパッケージをローカルに保存します。これにより、データをプレビューできるようになります。その後、`Send-CitrixCallHomeBundle`コマンドレットを使用して、パッケージのコピーを手動で CIS にアップロードします。(最初に保存したデータはローカルに残ります)。

各コマンドレットの説明や、上記の一般的なユースケースでは使用されないパラメーターを含む包括的な構文は、PowerShell ヘルプに記載されています。

CIS にデータをアップロードするコマンドレットを入力すると、アップロードを確認するメッセージが表示されます。アップロードの完了前にコマンドレットがタイムアウトした場合は、システムイベントログでアップロードのステータスをチェックしてください。サービスが既にアップロードを実行している場合は、アップロード要求が拒否されることがあります。

データを収集して **CIS** へパッケージをアップロードする:

```
Start-CitrixCallHomeUpload [-Credential] PSCredential [-InputPath
    string] [-Description string] [-IncidentTime string] [-SRNumber
    string] [-Name string] [-UploadHeader string] [-AppendHeaders string
    ] [-Collect string] [<CommonParameters>]
```

データを収集してローカルに保存する:

```
Start-CitrixCallHomeUpload -OutputPath <String> [-InputPath string] [-
    Description string] [-IncidentTime string] [-SRNumber string] [-Name
     string] [-UploaderHeader string] [-AppendHeaders string] [-Collect
    strings] [<CommonParameters>]
```

使用できるパラメーターは次のとおりです。

- **Credential**: アップロード先を CIS に設定します。
- **InputPath**: パッケージに含める zip ファイルの場所。これは、Citrix サポートから要求される追加ファイルである可能性があります。拡張子.zip を含めてください。
- **OutputPath**: 診断情報を保存する場所。このパラメーターは、Call Home データをローカルに保存するときに必要です。
- **Description** および **Incident Time**: アップロードに関する自由形式の情報。
- **SRNumber**: Citrix テクニカルサポートのインシデント番号。

- **Name**: パッケージの識別名。
- **UploadHeader**: CIS にアップロードするアップロードヘッダーを指定する、JSON 形式の文字列。
- **AppendHeaders**: CIS にアップロードする追加ヘッダーを指定する、JSON 形式の文字列。
- **Collect**:「{ 'collector' :{ 'enabled' :Boolean}}」の形で、どのデータを修正または省略するかを指定する JSON 形式の文字列。ここで、Boolean は true または false です。
  有効な collector の値は以下のとおりです。
  - 'wmi'
  - 'process'
  - 'registry'
  - 'crashreport'
  - 'trace'
  - 'file'
  - 'msi'
  - 'localdata'
  - 'sitedata'
  - 'sfb'

  デフォルトでは、'sfb' 以外のすべての collector が有効です。

  'sfb' collector は、Skype for Business の問題を診断するためにオンデマンドで使用するよう設計されています。'sfb' collector は、'enabled' パラメーターに加えて、ターゲットユーザーを指定する 'account' パラメーターと 'accounts' パラメーターをサポートします。以下のいずれかの形式を使用します。
  - "-Collect "{ 'sfb' :{ 'account' :' domain\\user1' }}"
  - "-Collect "{ 'sfb' :{ 'accounts' :['domain\\\user1' , 'domain\\\user2']}}"
- 一般的なパラメーター: PowerShell のヘルプを参照してください。

ローカルに保存されているデータをアップロードする:

```
Send-CitrixCallHomeBundle -Credential <PSCredentia\> -Path string [<
CommonParameters>]
```

Pathパラメーターにより、以前保存されたパッケージの場所を指定します。

例:

以下のコマンドレットでは、(WMI コレクターからのデータを除く) Call Home データの CIS へのアップロードが要求されます。このデータは、午後 2 時 30 分に Citrix サポートケース 123456 で記録された、Citrix Provisioning VDA の登録エラーに関連するものです。アップロードされるパッケージには、Call Home データに加えてファイル「c:\Diagnostics\ExtraData.zip」が含まれます。


```
C:\PS>Start-CitrixCallHomeUpload -InputPath "c:\Diagnostics\ExtraData.
    zip" -Description "Registration failures with Citrix Provisioning
    VDAs" -IncidentTime "14:30" -SRNumber 123456 -Name "
    RegistrationFailure-021812016" -Collect "{
 'wmi':{
 'enabled':false }
  }
 " -UploadHeader "{
 'key1':'value1' }
 " -AppendHeaders "{
 'key2':'value2' }
 "
```

以下のコマンドレットでは、午前 8 時 15 分に記録された Citrix サポートケース 223344 に関連する Call Home データが保存されます。このデータは、ネットワーク共有上の mydata.zip ファイルに保存されます。保存されるパッケージには、Call Home データに加えてファイル「c:\Diagnostics\ExtraData.zip」が含まれます。

```
C:\PS>Start-CitrixCallHomeUpload -OutputPath \mynetwork\myshare\mydata.
    zip -InputPath "c:\Diagnostics\ExtraData.zip" -Description "
    Diagnostics for incident number 223344" -IncidentTime "8:15" -
    SRNumber 223344
```

以下のコマンドレットでは、以前保存したデータパッケージがアップロードされます。

```
$cred=Get-Credential
C:\PS>Send-CitrixCallHomeBundle  - Credential $cred -Path \mynetwork\
    myshare\mydata.zip
```

Citrix Scout

August 17, 2024

はじめに

Citrix Scout は診断情報を収集し、ヘルスチェックを実行します。結果は、Citrix Virtual Apps and Desktops 展開の保守に使用できます。Citrix では、Citrix Insight Services を通じて、収集した診断データの包括的な自動分析機能を提供しています。Scout を使用して、お客様単独で、または Citrix サポートの支援を受けながら問題のトラブルシューティングを行うこともできます。

収集ファイルを Citrix にアップロードすると、Citrix Support による分析と支援を受けることができます。または、収集ファイルをローカルに保存してお客様自身でレビューを行い、その後 Citrix にアップロードして分析を受けることもできます。

Scout では以下の機能が利用できます:

- 収集：サイト内の選択したマシン上で一度だけ診断情報収集を実行します。その後、ユーザーはファイルを Citrix にアップロードするか、ローカルに保存できます。
- トレースおよび再現：選択したマシン上で手動でトレースを開始します。次に、そのマシン上で問題を再現します。問題を再現すると、トレースは停止します。Scout はその他の診断情報を収集し、ファイルを Citrix にアップロードするか、ローカルに保存します。
- スケジュール：選択したマシン上で、日次または週次の指定時刻に診断情報を収集するようスケジュールを設定します。ファイルは自動で Citrix にアップロードされます。
- ヘルスチェック：サイトとそのコンポーネントの正常性および可用性を測定するチェックを実行します。Delivery Controller、Virtual Delivery Agent（VDA）、StoreFront サーバー、および Citrix ライセンスサーバーのヘルスチェックを実行できます。チェック中に問題が見つかった場合は、Scout で詳細レポートが提供されます。Scout は起動時に必ず最新のヘルスチェックスクリプトがあるかを確認します。新しいバージョンがある場合は自動的に Scout がダウンロードし、次回のヘルスチェックで使用します。

> 注：
>
> トレースと再現、スケジュール、ヘルスチェックは現在 Linux VDA で利用できません。

この記事で説明するグラフィカルインターフェイスは、Scout を使用する初歩的な手段です。代わりに PowerShell を使用して、診断情報の収集とアップロードを一度だけまたは定期的に実行するように構成することもできます。「Call Home」を参照してください。

Scout は次の場所で実行します：

- オンプレミスの展開環境では、Delivery Controller から Scout を実行して診断情報を収集するか、1 つまたは複数の Virtual Delivery Agent（VDA）、Delivery Controller、StoreFront サーバー、ライセンスサーバーでチェックを実行します。VDA から Scout を実行してローカルの診断情報を収集することもできます。
- Citrix DaaS（旧称 Citrix Virtual Apps and Desktops サービス）を使用する Citrix Cloud 環境では、Scout を VDA から実行してローカルの診断情報を収集します。

Scout アプリケーションのログは、`C:\ProgramData\Citrix\TelemetryService\ScoutUI.log`に保存されます。このファイルはトラブルシューティングに使用できます。

収集される項目

Scout により収集される診断情報には、Citrix Diagnostic Facility（CDF）のトレースログファイルが含まれます。常時トレース（AOT）と呼ばれる CDF トレースファイルのサブセットも対象となります。AOT の情報は、VDA の登録やアプリケーションまたはデスクトップの起動など、よくある問題の解決に役立ちます。その他の Event Tracing for Windows（ETW）情報が収集されることはありません。

収集には以下が含まれます：

- Citrix Virtual Apps and Desktops によって`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix`に作成されたレジストリエントリ。

- **Citrix** 名前空間の Windows Management Instrumentation（WMI）情報。
- 実行中のプロセス。
- %PROGRAMDATA%\Citrix\CDF に保存されている Citrix プロセスのクラッシュダンプ。
- CSV 形式の Citrix ポリシー情報
- インストールとアップグレードの情報収集には、製品全体の Metainstaller ログ、失敗した MSI ログ、MSI ログアナライザーからの出力、StoreFront ログ、ライセンスの互換性チェックログ、サイトの事前アップグレードテストの結果が含まれます。

トレース情報の概要を以下に示します。

- マシン上の占有領域を抑えるため、トレース情報は収集時に圧縮されます。
- Citrix Telemetry Service は、最長 8 日間、圧縮されたトレース情報を各マシン上に保持します。
- Citrix Virtual Apps and Desktops 7 1808 より、AOT のトレース情報はデフォルトでローカルディスク上に保存されるようになりました。（以前のバージョンでは、トレースはメモリに保持されていました。）デフォルトパス = `C:\Users\CitrixTelemetryService\AppData\Local\CitrixAOT`。
- Citrix Virtual Apps and Desktops 7 1811 より、ネットワーク共有に保存された AOT トレースは、他の診断と一緒に収集されます。
- 最大サイズ（デフォルト値は 10MB）とスライス時間は、`Enable-CitrixTrace`コマンドレットを使用するか、または`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Telemetry DefaultListen`レジストリ文字列を指定することで変更できます。
- トレース情報は、ファイルサイズが`MaxSize`の 10% になるまでファイルに追加されます。

Scout で収集されるデータポイントの一覧については、「Call Home のキーデータポイント」を参照してください。

Scout の構成

Scout は、Linux VDA で機能するように構成できます。Linux VDA とテレメトリについて詳しくは、「Citrix Telemetry Service との統合」を参照してください。

Linux VDA では、自動的に`ctxtelemetry`ソケットポートや Telemetry Service のポートが変更される場合があります。その場合は、手動でポートを構成する必要があります。

1. C:\Program Files\Citrix\Telemetry Service に移動します。
2. ScoutUI.exe.config ファイルを開きます。
3. LinuxVDATelemetryServicePort または LinuxVDATelemetryWakeupPort の値を Linux VDA で構成された値に変更します：

- `<add key="LinuxVDATelemetryServicePort"value="7502"/>`
- `<add key="LinuxVDATelemetryWakeupPort"value="7503"/>`

1. 変更を保存してファイルを閉じます。
2. Scout を再度開いて、最新の構成が読み込まれているのを確認します。

ヘルスチェックについて

ヘルスチェックデータは`C:\ProgramData\Citrix\TelemetryService\`の下のフォルダーに保存されます。

サイトのヘルスチェック

サイトのヘルスチェックは、FlexCast Management Architecture（FMA）サービスを総合的に評価する Environment Test Service の機能の 1 つです。このチェックではサービスの可用性を確認するだけでなく、正常性を示す他の指標（データベース接続など）も確認します。

サイトのヘルスチェックは Delivery Controller で実行されます。サイトの規模によっては、チェックが完了するまでに最大 1 時間程度かかることがあります。

Delivery Controller 構成チェック　サイトヘルスチェックの一部として行います。Delivery Controller 構成チェックでは、Virtual Apps and Desktops サイトに関する Citrix の推奨事項に基づいて、次の問題が存在するかどうかを確認します:

- 1 つ以上の Delivery Controller でエラーが発生している。
- サイトに Delivery Controller が 1 つしかない。
- Delivery Controller のバージョンが異なる。

ヘルスチェックで権限と要件を満たすことに加え、Delivery Controller 構成チェックでは以下が必要とされます:

- 1 つ以上の Controller の電源がオンになっている。
- Broker Service が Controller で実行されている。
- Controller からサイトデータベースへの有効な接続がある。

VDA のヘルスチェック

VDA のヘルスチェックは、VDA 登録、セッションの起動、タイムゾーンリダイレクトの問題を引き起こす原因となるものを見つけ出します。

VDA への登録について、Scout は以下をチェックします:

- VDA ソフトウェアのインストール状況
- VDA マシンドメインへの参加状況
- VDA の通信ポートの可用性
- VDA サービスの状態
- Windows ファイアウォールの構成
- Controller との通信

- Controller との時刻同期
- VDA の登録の状態

VDA でのセッション起動について、Scout は以下をチェックします:

- セッション開始時の通信ポートの可用性
- セッション起動サービスの状態
- セッション開始時の Windows ファイアウォールの構成
- VDA リモートデスクトップサービスのクライアントアクセスライセンス
- VDA のアプリケーション起動パス
- セッションの起動レジストリ設定

VDA でのタイムゾーンリダイレクトについて、Scout は以下をチェックします:

- Windows の Hotfix のインストール状況
- Citrix の Hotfix のインストール状況
- Microsoft のグループポリシー設定
- Citrix のグループポリシー設定

VDA の Profile Management では、Scout は以下をチェックします:

- ハイパーバイザーの検出
- プロビジョニングの検出
- Citrix Virtual Apps and Desktops
- Personal vDisk の構成
- ユーザーストア
- Profile Management サービスの状態検出
- Winlogon.exe のフックテスト

Profile Management でチェックを実行するには、VDA に Profile Management をインストールして有効にする必要があります。Profile Management の構成チェックについて詳しくは、Knowledge Center のCTX132805を参照してください。

StoreFront ヘルスチェック

StoreFront チェックでは以下が確認されます:

- Citrix デフォルトドメインサービスが実行されている
- Citrix Credential Wallet サービスが実行されている
- StoreFront サーバーから Active Directory ポート 88 への接続
- StoreFront サーバーから Active Directory ポート 389 への接続
- ベース URL の FQDN が有効である
- ベース URL からの正しい IP アドレスを取得できる

- IIS アプリケーションプールで.NET 4.0 を使用している
- 証明書がホスト URL の SSL ポートにバインドされているかどうか
- 証明書チェーンが完全かどうか
- 証明書の有効期限が切れているかどうか
- 証明書の有効期限切れが近いかどうか（30 日以内）

ライセンスサーバーチェック

ライセンスサーバーチェックでは以下が確認されます:

- Delivery Controller からのライセンスサーバー接続
- ライセンスサーバーファイアウォールのリモートアクセスのステータス
- Citrix ライセンスサーバーサービスのステータス
- ライセンスサーバーの猶予期間の状態
- ライセンスサーバーのポート接続
- Citrix ベンダーデーモン（CITRIX）が実行されているかどうか
- システムクロックが同期されているかどうか
- Citrix ライセンスサービスがローカルサービスアカウントで実行されていません
- `CITRIX.opt` ファイルの存在
- カスタマーサクセスサービスの有効期限
- Citrix ライセンスサーバーの更新
- ライセンスサーバー証明書が Delivery Controller の信頼されたルートストアにあるかどうか

ヘルスチェックの権限と要件を満たすことに加え、ライセンスサーバーがドメインに参加している必要があります。参加していないと、ライセンスサーバーは検出されません。

ヘルスチェックを実行

ヘルスチェックはマシンの選択、チェックの開始、結果レポートの確認の各手順から構成されます。

1. Scout の起動。マシンの［スタート］メニューで［**Citrix**］**>**［**Citrix Scout**］の順に選択します。開始ページで［ヘルスチェック］をクリックします。
2. マシンの選択。［マシンの検索］クリックして、マシンを検出します。［マシンの選択］ページには、サイト内にあるすべての VDA、Delivery Controller、ライセンスサーバーが一覧表示されます。表示される項目をマシン名で絞り込むことができます。診断情報を収集する各マシンの隣にあるチェックボックスをオンにして、［続行］をクリックします。

   他のタイプのコンポーネント（StoreFront サーバー、VDA マシンなど）を追加するには、「手動でのマシンの追加 」および「VDA マシンのインポート」を参照してください。Citrix Provisioning サーバーやライセンスサーバーを手動で追加することはできません。

選択した各マシン上で確認テストが自動で開始され、各マシンが「確認テスト」に記載されている基準を満たしているか確認されます。確認テストで不合格になると、［状態］列にメッセージが表示され、該当するマシンのチェックボックスがオフになります。次のどちらかの手順を行います：

- 問題を解決して該当するマシンのチェックボックスを再びオンにします。このようにすると、確認テストが再び行われます。
- 該当するマシンを収集対象から除外します（チェックボックスをオフのままにします）。そのマシンのヘルスチェックは実行されません。

確認テストが完了したら、［続行］をクリックします。

3. 選択したマシンのヘルスチェックを実行します。概要に、ヘルスチェックが実行されるマシン（選択し、確認テストに合格したマシン）が一覧表示されます。［チェックの開始］をクリックします。

   確認中および確認後の状態：

   - ［状態］列には、マシンの現在のチェック状態が表示されます。
   - 進行中のチェックをすべて停止するには、ページの右下隅にある ［チェックの停止］をクリックします。（ヘルスチェックの取り消しはチェック対象のマシン全台に適用されます。マシン単体を選んで取り消すことはできません。チェックが完了したマシンからの情報は保持されます。
   - すべての選択したマシンでチェックが完了すると、右下隅にある ［チェックの停止］が ［完了］に変わります。
   - チェックが失敗した場合は、［操作］列の ［再試行］をクリックできます。
   - チェックが完了しても問題が見つからなかった場合は、［操作］列には何も表示されません。
   - チェックで問題が見つかった場合は、［詳細の表示］で結果を確認できます。
   - すべてのマシンでチェックが完了した後に、［戻る］をクリックしないでください。（クリックすると、チェック結果は失われます）

4. チェックが終了したら、［完了］をクリックして Scout の開始ページに戻ります。

ヘルスチェックの結果

Citrix がチェックするレポート生成には、次の情報が含まれます：

- 結果レポートが生成された日時
- チェックが行われたマシン
- チェック対象のマシンで検索する条件

権限と要件

権限：

- 診断情報を収集するには、以下の条件を満たしている必要があります：

  - 診断情報の収集元になる各マシンのローカル管理者およびドメインユーザーである必要があります。
  - 各マシン上の LocalAppData ディレクトリに書き込む権限がある必要があります。

- ヘルスチェックを実行するには、以下の条件を満たしている必要があります:

  - ドメインユーザーグループのメンバーである必要があります。
  - すべての権限を持つ管理者であるか、対象サイトに対する読み取り専用の権限と ［環境テストの実行］権限があるカスタムロールを付与されている必要があります。
  - スクリプトを実行するには、スクリプトの実行ポリシーを`RemoteSigned`またはそれ以上に設定する必要があります。例: `Set-ExecutionPolicy RemoteSigned`。注: 他のスクリプト実行権限も同様に機能します。

- Scout の起動時には ［管理者として実行］を使用してください。

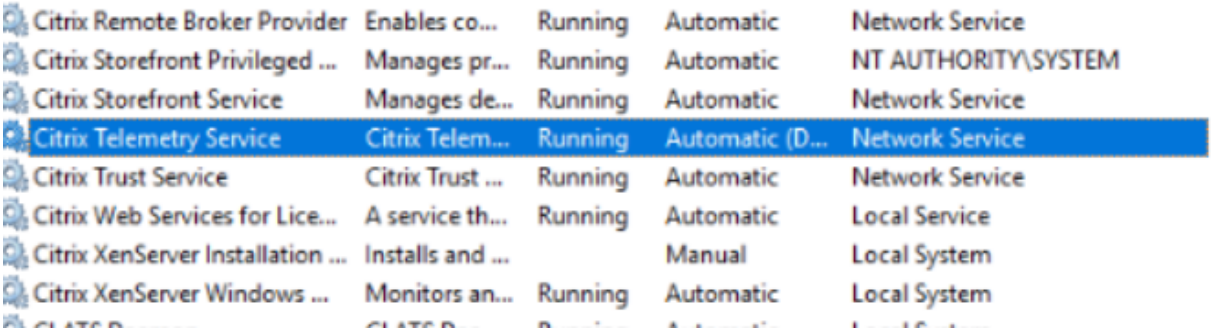
診断情報の収集元またはヘルスチェックの実行元になる各マシンは、次の条件を満たしている必要があります:

- Scout は当該マシンと通信できる必要があります。
- ファイルとプリンターの共有は設定されている必要があります。
- PSRemoting と WinRM は有効になっている必要があります。PowerShell 3.0 以降が実行されている必要もあります。
- Citrix Telemetry Service が実行されている必要があります。
- Windows Management Infrastructure（WMI）へのアクセスが有効になっている必要があります。
- 診断収集のスケジュールを設定するには、マシンで互換性のある Scout バージョンが実行されている必要があります。

パス名で指定するユーザー名にドル記号（$）を使用しないでください。この記号があると、診断情報を収集できません。

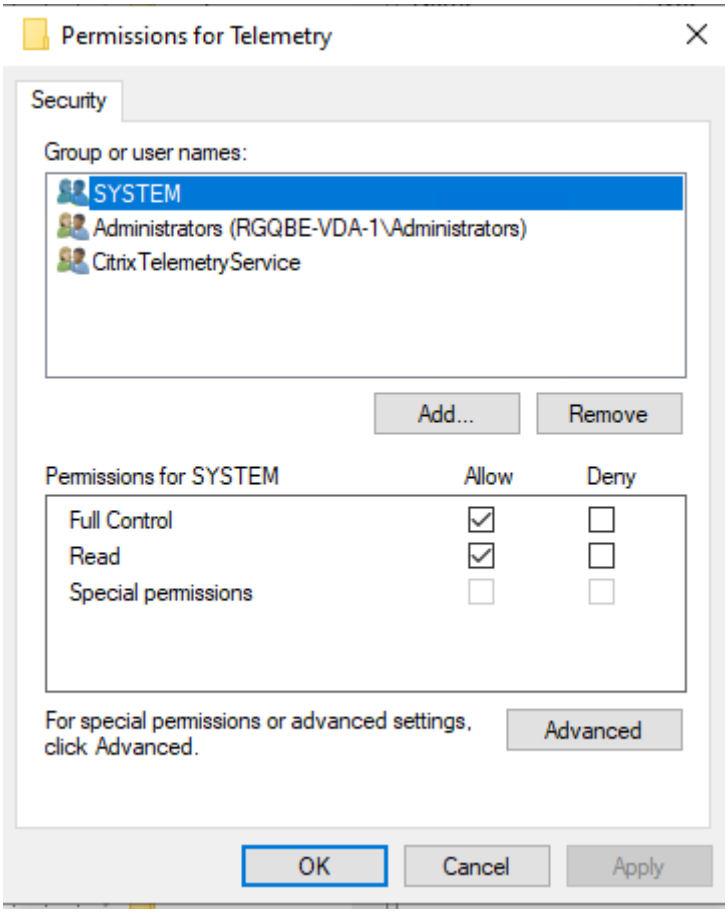
Scout により、指定したマシン上で確認テストが実行され、これらの要件が満たされているか確認されます。

Windows 用の Telemetry Service は Network Service で実行されます。

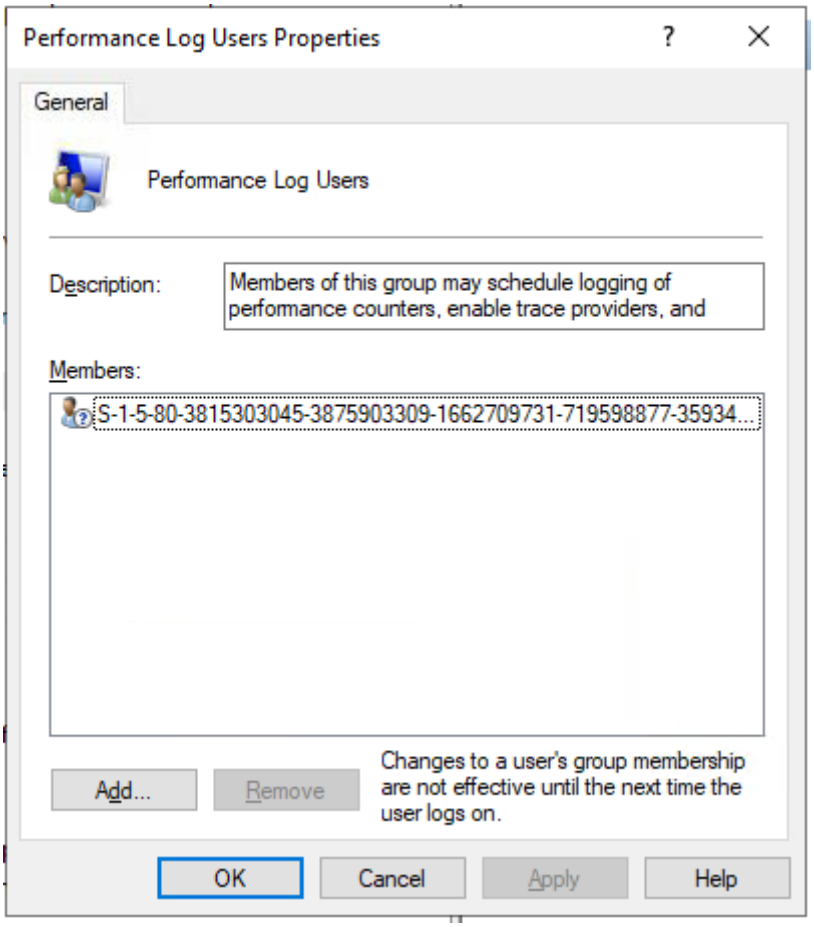


AOT トレースフォルダーは「`C:\ProgramData\Citrix\TelemetryService\CitrixAOT`」に保存されています。

Administrator グループ、System、および Telemetry Service SID のユーザーのみが、「`HKEYLOCALMACHINE:SOFTWARE\Citrix\Telemetry`」レジストリにアクセスする権限を持っています。



Telemetry Service SID は、Telemetry Service をアンインストールしたあとも Performance Log Users グループに残りますが、手動で削除できます。



確認テスト

診断情報の収集またはヘルスチェックの開始前に、指定した各マシンについて自動で確認テストが実行されます。これらのテストで、要件が満たされているか確認されます。あるマシンでテストが失敗した場合、Scout には修正アクション案を含むメッセージが表示されます。

- **Scout** はこのマシンに接続できません：次のことを確認してください：
  - マシンの電源が入れられていること。
  - ネットワーク接続が正しく動作していること（これにはファイアウォールが正しく構成されていることを含みます。）
  - ファイルおよびプリンターの共有が設定されていること。手順については、Microsoft 社のドキュメントを参照してください。
- **PSRemoting** および **WinRM** を有効にする：PowerShell リモート処理と Windows リモート管理は同時に有効にできます。`Enable-PSRemoting`コマンドレットを、［管理者として実行］で実行します。詳しくは、Microsoft のコマンドレットのヘルプを参照してください。

- **Scout** には **PowerShell 3.0** 以降が必要です：マシンに PowerShell 3.0 以降をインストールして、PowerShell リモート処理を有効にします。
- このマシンの **LocalAppData** ディレクトリにアクセスできません：マシン上の LocalAppData ディレクトリに書き込む権限がアカウントにあることを確認してください。
- **Citrix Telemetry Service** が見つかりません：Citrix Telemetry Service がマシンにインストールされ、開始していることを確認してください。
- スケジュールを取得できません：マシンを XenApp および XenDesktop 7.14 以上にアップグレードしてください。
- **WMI** がマシン上で実行されていません：Windows Management Instrumentation（WMI）アクセスが有効になっていることを確認してください。
- **WMI** 接続がブロックされました：Windows ファイアウォールサービスで WMI を有効にします。
- **Citrix Telemetry Service** の新しいバージョンが必要です：バージョンの確認は［収集］と［トレースおよび再現］の処理でのみ行われます。対象のマシンで Telemetry Service のバージョンをアップグレードしてください（「インストールとアップグレード」を参照してください）。サービスをアップグレードしていないマシンは、［収集］または ［トレースと再現］の対象になりません。
- **Scout** はこのマシンの **systemd** ソケットに接続できません：次を確認します：
  - ポート 7503 が開いている。`systemd ctxtelemetry.socket`がマシンのポート 7503 でリスンしていることを確認します。`ctxtelemetry.socket`のポートが変更された場合、異なるポートの可能性があります。ポートの調整については、「Scout の構成 」を参照してください。
  - ネットワーク接続が正しく動作していること（ファイアウォールが正しく構成されていることの確認も含まれる場合があります）。
- このマシンでは、**Linux VDA Telemetry Service** が開始されていません：次を確認します：
  - ポート 7502 が開いている。Linux VDA Telemetry Service がマシンにインストールされ、開始されていることを確認します。Telemetry Service のポートが変更された場合、異なるポートの可能性があります。ポートの調整については、「Scout の構成 」を参照してください。
  - ネットワーク接続が正しく動作していること（ファイアウォールが正しく構成されていることの確認も含まれる場合があります）。

バージョンの互換性

本バージョンの Scout（3.x）は、Citrix Virtual Apps and Desktops（または XenApp および XenDesktop 7.14 以降）の Controller と VDA 上での実行を想定しています。

旧バージョンの Scout は、バージョン 7.14 より前の XenApp および XenDesktop で提供されています。旧バージョンについて詳しくは、CTX130147を参照してください。

バージョン 7.14 より前の Controller または VDA をバージョン 7.14（以降のサポートするバージョン）にアップグレードすると、旧バージョンの Scout が最新バージョンに置き換えられます。

機能	Scout 2.23	Scout 3.0
Citrix Virtual Apps and Desktops（と XenApp および XenDesktop 7.14～7.18）のサポート	はい	はい
XenDesktop 5.x、7.1～7.13 のサポート	はい	いいえ
XenApp 6.x、7.5～7.13 のサポート	はい	いいえ
製品への同梱	7.1～7.13	7.14 以降
CTX 記事からのダウンロード	はい	いいえ
CDF トレースのキャプチャ	はい	はい
常時トレース（AOT）のキャプチャ	いいえ	はい
診断データの収集対象	一度に 10 台のマシンまで（デフォルト）	無制限（リソースの可用性に依存）
Citrix への診断データの送信	はい	はい
診断データのローカルへの保存	はい	はい
Citrix Cloud 資格情報のサポート	いいえ	はい
Citrix の資格情報のサポート	はい	はい
アップロード用プロキシサーバーのサポート	はい	はい
スケジュールの調整	-	はい
スクリプトのサポート	コマンドライン（ローカルの Controller のみ）	Call Home コマンドレットを使用した PowerShell（Telemetry Service をインストール済みのすべてのマシン）
ヘルスチェック	いいえ	はい
データマスキング	いいえ	3.17 以降

インストールとアップグレード

デフォルトでは、Scout は VDA または Controller のインストールまたはアップグレード時に Citrix Telemetry Service の一部として自動でインストールまたはアップグレードされます。

VDA のインストール時に Citrix Telemetry Service を除外した場合、またはこのサービスを後で削除した場合には、Citrix Virtual Apps and Desktops のインストールメディアに含まれる`x64\Virtual Desktop Components`フォルダーまたは`x86\Virtual Desktop Components`フォルダーにある`TelemetryServiceInstaller_xx.msi`を実行します。

マシンが実行する Citrix Telemetry Service のバージョンが古い場合には、［収集］または ［トレースおよび再現］アクションを選択したときに、その旨を知らせるメッセージが表示されます。Citrix ではサポートされている最新バージョンを使用することをお勧めします。Telemetry Service をアップグレードしていないマシンは、［収集］または ［トレースおよび再現］の対象になりません。Telemetry Service をアップグレードするには、インストールと同じ手順を実行します。

アップロードの認証

収集した診断情報を Citrix にアップロードする場合、Citrix または Citrix Cloud のアカウントが必要になります。（これらのアカウントは、Citrix ダウンロードまたは Citrix Cloud Control Center へのアクセス時に使用する資格情報です）。アカウントの資格情報の検証後、トークンが発行されます。

Citrix アカウントまたは Citrix Cloud アカウントを使用して認証を行う場合はリンクをクリックし、HTTPS を使用してデフォルトのブラウザーで Citrix Cloud にアクセスします。Citrix Cloud 資格情報を入力すると、トークンが表示されます。このトークンをコピーして Scout に貼り付けます。Scout ウィザードの手順を進めることができるようになります。

トークンは、Scout が実行されているマシンにローカルに保存されます。このトークンを次回の ［収集］または ［トレースおよび再現］でも使用するには、［トークンを保存して次回以降この手順を省略する］チェックボックスをオンにします。

Scout の開始ページで ［スケジュール］を選択するたびに再度認証を行う必要があります。スケジュールの作成時または変更時には、保存したトークンは使用できません。

アップロードでのプロキシの使用

プロキシサーバーを使用して Citrix へ収集情報をアップロードするには、お使いのブラウザーのインターネットプロパティで構成済みのプロキシ設定を使用するように Scout を構成します。または、プロキシサーバーの IP アドレスとポート番号を指定できます。

マシンの検索

［収集］、［トレースおよび再現］、および ［スケジュール］の手順では、Scout は自動的に検出した Controller と VDA を一覧表示します。

Delivery Controller から Scout ヘルスチェックを実行するときは、［マシンの検索］をクリックして、Delivery Controller、VDA、ライセンスサーバー、StoreFront サーバーなどのマシンを検出します。

Delivery Controller ではないドメイン参加済みマシンから Scout ヘルスチェックを実行すると、Scout は自動的にマシンを検出できません。マシンを手動で追加するか、VDA マシンをインポートする必要があります。

手動でのマシンの追加

Scout が検出した Controller と VDA の一覧が表示されたら、StoreFront サーバー、ライセンスサーバー、Citrix Provisioning サーバーなどの展開にある他のマシンを手動で追加できます。

ヘルスチェックの実行時には、以下のようになります:

- ドメイン内の Citrix ライセンスサーバーは自動検出されます。ライセンスサーバーを手動で追加することはできません。
- ヘルスチェックは現在、Citrix Provisioning サーバーをサポートしていません。

検出されたマシンの一覧が表示されている Scout のページで、［**+** マシンの追加］をクリックします。追加するマシンの完全修飾ドメイン名を入力し、［続行］をクリックします。必要に応じて、他のマシンの追加を繰り返します。(FQDN の代わりに DNS エイリアスを入力しても有効に見える場合がありますが、ヘルスチェックは失敗する可能性があります)

手動で追加したマシンは、常に、マシンの一覧の上部、検出されたマシンの上に表示されます。

手動で追加したマシンを簡単に識別する方法は、行の右端にある赤い削除ボタンです。手動で追加したマシンにだけこのボタンがあります。検出されたマシンにはありません。

手動で追加したマシンを削除するには、行の右端にある赤いボタンをクリックします。削除を確認します。手動で追加した他のマシンの削除を繰り返します。

Scout は、削除されるまで、手動で追加されたマシンを覚えています。Scout を閉じてから再び開くと、手動で追加したマシンはそのまま一覧の一番上に表示されています。

StoreFront サーバーでトレースおよび再現を使用しているときは、CDF トレースは収集されません。ただし、他のすべてのトレース情報は収集されます。

VDA マシンのインポート

ヘルスチェックを実行するとき、VDA マシンを環境にインポートできます。

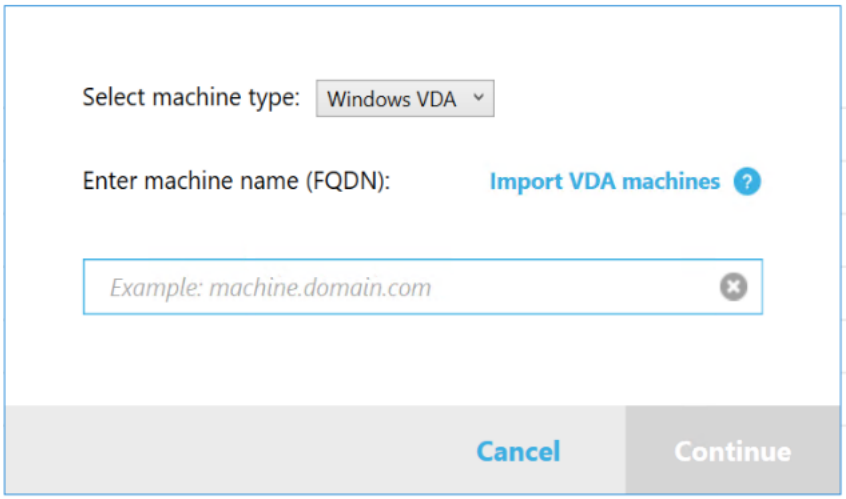
1. Delivery Controller または Connector で、PowerShell コマンドを使用してマシンリストファイルを生成します。Connector では、Citrix 資格情報を入力し、ポップアップダイアログで顧客を選択する必要があります。

   ```
   Get-BrokerMachine| foreach { $_.DnsName } | out-file C:\machineList
   .txt
   ```

2. machineList.txt ファイルを、Scout ヘルスチェックを起動するドメイン参加済みマシンにコピーします。

3. ［Scout ヘルスチェック］ページで、［マシンの追加］をクリックします。
4. マシンの種類で ［**Windows VDA**］を選択します。
5. ［**VDA** マシンのインポート］をクリックします。
6. machineList.txt ファイルを選択します。
7. ［開く］をクリックします。

インポートされた VDA マシンは、［Scout ヘルスチェック］ページに一覧表示されます。



診断の収集

収集の手順では、マシンを選択し、診断情報の収集を開始してから、収集結果のファイルを Citrix にアップロードするかローカルに保存します。

1. Scout の起動。マシンの ［スタート］メニューで ［**Citrix**］**>** ［**Citrix Scout**］の順に選択します。開始ページで ［収集］をクリックします。
2. マシンの選択。

   - ［マシンの選択］ページに、サイト内にあるすべての VDA と Controller が一覧表示されます。表示される項目をマシン名で絞り込むことができます。StoreFront や Citrix Provisioning サーバーなどの他のマシンを手動で追加するには、「手動でのマシンの追加」を参照してください。
   - 他のコンポーネント（VDA サーバーなど）では、［マシンの選択］ページにローカルマシンのみが一覧表示されます。マシンの手動追加はサポートされていません。

   診断情報を収集する各マシンの隣にあるチェックボックスをオンにして、［続行］をクリックします。

   選択した各マシン上で確認テストが自動で開始され、各マシンが「確認テスト」に記載されている基準を満たしているか確認されます。確認テストで不合格になると、［状態］列にメッセージが表示され該当するマシンのチェックボックスがオフになります。次のどちらかの手順を行います：

- 問題を解決して該当するマシンのチェックボックスを再びオンにします。このようにすると、確認テストが再び行われます。
- 該当するマシンを収集対象から除外します（チェックボックスをオフのままにします）。このマシンの診断情報は収集されません。

確認テストが完了したら、［続行］をクリックします。

3. 診断情報を収集します。概要に、診断情報の収集元になるマシン（選択し、確認テストに合格したマシン）がすべて一覧表示されます。［収集の開始］をクリックします。

   収集は以下のように進行します。

   - ［状態］列には、マシンの現在の収集状態が表示されます。
   - 1 台のマシンで進行中の収集を停止するには、そのマシンの ［操作］列の ［キャンセル］をクリックします。
   - 進行中の収集をすべて停止するには、ページの右下隅にある ［収集の停止］をクリックします。収集が完了したマシンの診断情報は保持されます。収集を再開するには、各マシンの ［操作］列で ［再試行］をクリックします。
   - すべての選択したマシンで収集が完了すると、右下隅にある ［収集の停止］が ［続行］に変わります。
   - 診断情報を再度収集するには、そのマシンの ［アクション］列で ［再度収集する］をクリックします。新しい収集情報によって過去の収集情報が上書きされます。
   - 収集が失敗した場合は、［操作］列の ［再試行］をクリックできます。アップロードまたは保存されるのは収集に成功した情報だけです。
   - 選択したすべてのマシンで収集が完了した後に、［戻る］をクリックしないでください。クリックすると、収集した情報は失われます。

   収集が完了したら、［続行］をクリックします。

4. 収集情報の保存またはアップロード。ファイルを Citrix にアップロードするか、ローカルのマシンに保存するかを選択します。

   このファイルをすぐにアップロードすることを選択した場合は、手順 5 に進んでください。

   このファイルをローカルに保存することを選択した場合は、次の操作を行います。

   - Windows の ［保存］ダイアログボックスが開きます。保存場所を指定します。
   - ローカルへの保存が完了すると、保存したファイルのパス名のリンクが表示されます。このファイルを確認できます。ファイルは後で Citrix にアップロードできます。CTX136396を参照してください。

   ［完了］をクリックして Scout の開始ページに戻ります。この操作では、以下の手順を行う必要はありません。

5. アップロードの認証を行い、任意でプロキシを指定します。詳しくは、「アップロードの認証」を参照してください。

   - Scout で認証を行っていない場合、以下の手順を実行します。

- Scout で認証を行っている場合は、デフォルトで保存済みの認証トークンが使用されます。それでよい場合には、このオプションを選択して ［続行］をクリックします。今回の収集では資格情報は求められません。手順 6 に進んでください。
- 以前に認証を行っているものの、再度認証を行って新しいトークンを取得する場合は、［変更/再認証］をクリックして以下の手順を実行します。

アップロードの認証に Citrix 資格情報と Citrix Cloud 資格情報のどちらを使用するかを選択します。［続行］をクリックします。保存済みのトークンを使用しない場合のみ、［資格情報］ページが表示されます。

［資格情報］ページで次の操作を行います。

- ファイルのアップロードにプロキシサーバーを使用する場合は、［プロキシの構成］をクリックします。お使いのブラウザーのインターネットプロパティで構成済みのプロキシ設定を使用するように Scout を構成するか、プロキシサーバーの IP アドレスとポート番号を指定します。プロキシのダイアログボックスを閉じます。
- Citrix Cloud アカウントの場合は、［トークンの生成］をクリックします。デフォルトのブラウザーで Citrix Cloud のページが開き、トークンが表示されます。このトークンをコピーして Scout のページに貼り付けます。
- Citrix アカウントの場合はお使いの資格情報を入力します。

入力が完了したら、［続行］をクリックします。

6. アップロードの情報を入力します。

   - ［名前］フィールドには、収集した診断情報のファイルのデフォルト名が入力されています。ほとんどの収集ではこの名前で十分ですが、名前を変えることもできます（デフォルト名を削除して［名前］フィールドを空のままにした場合、デフォルト名が使用されます）。
   - オプションとして、8 桁の Citrix Support ケース番号を指定します。
   - 該当する場合、オプションの ［説明］フィールドに問題の詳細と発生時期を入力します。

   完了したら、［アップロードの開始］をクリックします。

   アップロード中、ページの左下にアップロードのおよそ何% が完了したかが表示されます。進行中のアップロードをキャンセルするには、［アップロードの停止］をクリックします。

   アップロードが完了すると、アップロード先の URL リンクが表示されます。この Citrix のアップロード先へのリンクをクリックしてアップロードした情報の分析結果を確認するか、リンクをコピーします。

   ［完了］をクリックして Scout の開始ページに戻ります。

トレースと再現

トレースと再現の手順では、マシンを選択し、トレースを開始し、問題を再現し、診断情報の収集を完了してから、ファイルを Citrix にアップロードするかローカルに保存します。

この手順は、標準の収集手順と同様です。ただし、マシン上でトレースを開始し、問題を再現することができます。すべての診断情報には AOT トレース情報が含まれています。この手順ではトラブルシューティングに役立つ CDF トレースも追加されます。

1. Scout の起動。マシンの［スタート］メニューで［**Citrix**］**>**［**Citrix Scout**］の順に選択します。開始ページで、［トレースと再現］をクリックします。
2. マシンの選択。［マシンの選択］ページに、サイト内にあるすべての VDA と Controller が一覧表示されます。表示される項目をマシン名で絞り込むことができます。トレースと診断情報を収集する各マシンの隣にあるチェックボックスをオンにします。次に、［続行］をクリックします。

   StoreFront や Citrix Provisioning サーバーなどの他のマシンを手動で追加するには、「手動でのマシンの追加」を参照してください。

   選択した各マシン上で確認テストが自動で開始され、各マシンが「確認テスト」に記載されている基準を満たしているか確認されます。マシンが確認テストで不合格になると、［状態］列にメッセージが表示され、該当するマシンのチェックボックスがオフになります。次のどちらかの手順を行います:

   - 問題を解決して該当するマシンのチェックボックスを再びオンにします。このようにすると、確認テストが再び行われます。
   - 該当するマシンを収集対象から除外します（チェックボックスをオフのままにします）。このマシンの診断情報とトレースは収集されません。

   確認テストが完了したら、［続行］をクリックします。
3. トレースを開始します。概要に、トレースの収集対象になるすべてのマシンが一覧表示されます。［トレースの開始］をクリックします。

   選択した 1 台または複数台のマシンで、経験した問題を再現します。この間もトレースの収集は継続されています。問題の再現が完了したら、Scout で ［続行］をクリックします。これによりトレースが停止されます。

   トレースの停止後、このトレース中に問題を再現したかどうかを指定します。
4. マシンの診断データの収集。［収集の開始］をクリックします。収集は以下のように進行します。

   - ［状態］列には、マシンの現在の収集状態が表示されます。
   - 1 台のマシンで進行中の収集を停止するには、そのマシンの ［操作］列の ［キャンセル］をクリックします。
   - 進行中の収集をすべて停止するには、ページの右下隅にある ［収集の停止］をクリックします。収集が完了したマシンの診断情報は保持されます。収集を再開するには、各マシンの ［操作］列で ［再試行］をクリックします。
   - すべての選択したマシンで収集が完了すると、右下隅にある ［収集の停止］が ［続行］に変わります。
   - マシンから診断情報を再度収集するには、そのマシンの ［アクション］列で ［再度収集する］をクリックします。新しい収集情報によって過去の収集情報が上書きされます。
   - 収集が失敗した場合は、［操作］列の ［再試行］をクリックできます。アップロードまたは保存されるのは収集に成功した情報だけです。

- 選択したすべてのマシンで収集が完了した後に、［戻る］をクリックしないでください。クリックすると、収集した情報は失われます。

収集が完了したら、［続行］をクリックします。

5. 収集情報の保存またはアップロード。ファイルを Citrix にアップロードするか、ローカルに保存するかを選択します。

   このファイルをすぐにアップロードすることを選択した場合は、手順 6 に進んでください。

   このファイルをローカルに保存することを選択した場合は、次の操作を行います。

   - Windows の［保存］ダイアログボックスが開きます。保存先を選択します。
   - ローカルへの保存が完了すると、保存したファイルのパス名のリンクが表示されます。このファイルを確認できます。注：ファイルは後で Citrix からアップロードできます。Citrix Insight Services の場合はCTX136396を参照してください。

   ［完了］をクリックして Scout の開始ページに戻ります。この操作では、以下の手順を行う必要はありません。

6. アップロードの認証を行い、任意でプロキシを指定します。このプロセスについて詳しくは、「アップロードの認証」を参照してください。

   - Scout で認証を行っていない場合、以下の手順を実行します。
   - Scout で認証を行っている場合は、デフォルトで保存済みの認証トークンが使用されます。それでよい場合には、このオプションを選択して ［続行］をクリックします。今回の収集では資格情報は求められません。手順 7 に進んでください。
   - 以前に認証を行っているものの、再度認証を行って新しいトークンを取得する場合は、［変更/再認証］をクリックして以下の手順を実行します。

   アップロードの認証に Citrix 資格情報と Citrix Cloud 資格情報のどちらを使用するかを選択します。［続行］をクリックします。保存済みのトークンを使用しない場合のみ、［資格情報］ページが表示されます。

   ［資格情報］ページで次の操作を行います。

   - ファイルのアップロードにプロキシサーバーを使用する場合は、［プロキシの構成］をクリックします。お使いのブラウザーのインターネットプロパティで構成済みのプロキシ設定を使用するように Scout を構成するか、プロキシサーバーの IP アドレスとポート番号を指定します。プロキシのダイアログボックスを閉じます。
   - Citrix Cloud アカウントの場合は、［トークンの生成］をクリックします。デフォルトの Web ブラウザーで Citrix Cloud のページが開き、トークンが表示されます。このトークンをコピーして Scout のページに貼り付けます。
   - Citrix アカウントの場合はお使いの資格情報を入力します。

   入力が完了したら、［続行］をクリックします。

7. アップロードに関する情報の指定。

   アップロードの詳細を入力します。

- ［名前］フィールドには、収集した診断情報のファイルのデフォルト名が入力されています。ほとんどの収集ではこの名前で十分ですが、名前を変えることもできます（デフォルト名を削除して［名前］フィールドを空のままにした場合、デフォルト名が使用されます）。
- オプションとして、8 桁の Citrix Support ケース番号を指定します。
- 該当する場合、オプションの［説明］フィールドに問題の詳細と発生時期を入力します。

完了したら、［アップロードの開始］をクリックします。

アップロード中、ページの左下にアップロードのおおよそ何% が完了したかが表示されます。進行中のアップロードをキャンセルするには、［アップロードの停止］をクリックします。

アップロードが完了すると、アップロード先の URL リンクが表示されます。この Citrix のアップロード先へのリンクをクリックしてアップロードした情報の分析結果を確認するか、リンクをコピーします。

［完了］をクリックして Scout の開始ページに戻ります。

追加のログ収集を有効にする

追加のログ収集 機能を有効にすると、perfmon、Netsh、DebugView、Wireshark などのより多くのツールでトレースおよび再現機能を使用できます。

2407 リリース以降、別のログ収集を有効にすると、Scout はマシンにインストールされている CDC 関連ツールを自動的に検出し、CDC ツール関連のトレースログを zip パッケージに自動収集します。これらの zip ファイルをカスタマイズして Scout に添付することができます。この自動化により、Citrix Scout をより効果的に使用できるようになり、問題を迅速に診断できるようになります。

> 注:
>
> これはローカルマシンにのみ適用されます。

追加のログ収集を設定するには:

1. Citrix Scout を起動します。
2. 設定用の歯車をクリックします。
3. ［**Enable additional log collection with more tools**］をクリックします。
4. ［保存］をクリックします。

追加のログを収集するには:

1. Scout のホームページで、［トレースと再現］をクリックします。
2. ［マシンの選択］ページで、ローカルマシンの右側にある歯車をクリックします。
3. ［Trace and Reproduce］ の手順に従います。
4. 完了後、zip ファイルのログを確認します。ログは *CDCLogs* フォルダーに圧縮されています。

> 注:
>
> トレースに Procmon Tool が選択されている場合、プロセスモニターログは急速に大きくなる可能性があります。必要なツールのみを選択するようにしてください。*%temp%\Scout-CDC-Log* にあるログのサイズを監視することもできます。

収集スケジュールの設定

> 注:
>
> 収集機能についてはスケジュールを指定して実行することができますが、現時点ではヘルスチェックでスケジュールを指定することはできません。

スケジュール設定手順では、マシンを選択し、スケジュールを設定またはキャンセルします。スケジュールで収集された診断情報は、Citrix に自動的にアップロードされます（PowerShell インターフェイスを使用すると、スケジュールにより収集されたデータをローカルに保存できます。「Citrix Call Home」を参照してください。）

1. Scout の起動。マシンの［スタート］メニューで［**Citrix**］**>**［**Citrix Scout**］の順に選択します。開始ページで［スケジュール］をクリックします。
2. マシンの選択。サイト内のすべての VDA とコントローラーが一覧表示されます。表示される項目をマシン名で絞り込むことができます。

   グラフィカルインターフェイスを使用して VDA およびコントローラーをインストールした場合、Call Home スケジュールを設定すると（「Citrix Call Home」を参照）、Scout ではデフォルトでこれらの設定が表示されます。このバージョンの Scout では、スケジュール済みの収集を初めて開始するか、構成済みのスケジュールを変更できます。

   コンポーネントのインストール時に Call Home をマシンごとに有効化または無効化しても、Scout で設定されたスケジュールは選択したすべてのマシンに影響します。

   診断情報を収集する各マシンの隣にあるチェックボックスをオンにして、［続行］をクリックします。

   StoreFront や Citrix Provisioning サーバーなどの他のマシンを手動で追加するには、「手動でのマシンの追加」を参照してください。

   選択した各マシン上で確認テストが自動で開始され、各マシンが「確認テスト」に記載されている基準を満たしているか確認されます。マシンが確認テストで不合格になると、［状態］列にメッセージが表示され、該当するマシンのチェックボックスがオフになります。次のどちらかの手順を行います:

   - 問題を解決して該当するマシンのチェックボックスを再びオンにします。このようにすると、確認テストが再び行われます。
   - 該当するマシンを収集対象から除外します（チェックボックスをオフのままにします）。このマシンの診断情報（またはトレース）は収集されません。

   確認テストが完了したら、［続行］をクリックします。

［概要］ページに、スケジュールが適用されるマシンが一覧表示されます。［続行］をクリックします。

3. スケジュールを設定します。診断情報を収集するタイミングを指定します。注：スケジュールは選択したマシンすべてに影響します。

   - 選択したマシンについて週次のスケジュールを構成するには、［毎週］をクリックします。曜日を選択します。収集を開始する時刻（24 時間形式）を入力します。
   - 選択したマシンについて日次のスケジュールを構成するには、［毎日］をクリックします。収集を開始する時刻（24 時間形式）を入力します。
   - （別のスケジュールに置き換えずに）選択したマシンの既存のスケジュールをキャンセルするには、［オフ］をクリックします。選択したマシンで構成済みのスケジュールがすべてキャンセルされます。

   ［続行］をクリックします。

4. アップロードの認証を行い、任意でプロキシを指定します。このプロセスについて詳しくは、「アップロードの認証」を参照してください。注：Scout のスケジュールを使用する場合、保存済みのトークンを使用して認証を行うことはできません。

   アップロードの認証に Citrix 資格情報と Citrix Cloud 資格情報のどちらを使用するかを選択します。［続行］をクリックします。

   ［資格情報］ページで次の操作を行います。

   - ファイルのアップロードにプロキシサーバーを使用する場合は、［プロキシの構成］をクリックします。お使いのブラウザーのインターネットプロパティで構成済みのプロキシ設定を使用するように Scout を構成するか、プロキシサーバーの IP アドレスとポート番号を指定します。プロキシのダイアログボックスを閉じます。
   - Citrix Cloud アカウントの場合は、［トークンの生成］をクリックします。デフォルトのブラウザーで Citrix Cloud のページが開き、トークンが表示されます。このトークンをコピーして Scout のページに貼り付けます。
   - Citrix アカウントの場合はお使いの資格情報を入力します。

   入力が完了したら、［続行］をクリックします。

   構成済みのスケジュールを確認します。［完了］をクリックして Scout の開始ページに戻ります。

   収集中、選択した各マシンの Windows アプリケーションログに収集とアップロードの情報が書き込まれます。

データマスキング

Citrix Scout を使用して収集した診断情報は、セキュリティ上の機密情報が含まれている場合があります。Citrix Scout のデータマスキング機能を使用すると、Citrix にアップロードする前に診断ファイル内の機密データをマスキングすることができます。

Scout のデータマスキングは、IP アドレス、マシン名、ドメイン名、ユーザー名、ハイパーバイザー名、デリバリーグループ名、カタログ名、アプリケーション名、SID をマスキングするように構成されます。

> 注:
>
> CDF トレースは暗号化されており、マスキングすることはできません。
>
> Linux VDA ログは`.tar.gz2`形式で圧縮されており、マスキングすることはできません。

新しい診断情報の収集およびデータマスキングの実行

Citrix Scout のデータマスキング機能を使用するには、コマンドラインで Scout を起動します。

1. Windows で、管理者としてコマンドプロンプトを開きます。
2. Scout がインストールされているディレクトリに移動します: `cd C:\Program Files\Citrix\Telemetry Service`。
3. Scout を起動します: `ScoutUI.exe datamasking`。
4. [収集] または [トレースと再現] をクリックして診断情報を収集します。
5. 収集の完了後、[データマスキングを有効にする] を選択します。このオプションは、デフォルトで有効になっています。
6. データマスキングを構成します。デフォルトの規則を使用するか、規則をカスタマイズできます。
7. 収集した診断情報をアップロードするか保存するかを選択します。
   - [収集した診断情報を **Citrix** にアップロードする] を選択した場合、マスキングされた診断情報ファイルが Citrix にアップロードされます。
   - [収集した診断情報をローカルマシンに保存する] を選択した場合、元の診断情報とマスキングされた診断情報の両方が指定された場所に保存されます。

既存の診断情報でデータマスキングを実行

1. Windows で、管理者としてコマンドプロンプトを開きます。
2. Scout がインストールされているディレクトリに移動します: `cd C:\Program Files\Citrix\Telemetry Service`。
3. データマスキングモードで Scout を直接起動します: `ScoutUI.exe datamasking filePath`。
4. [データマスキングを有効にする] を選択して続行します。このオプションは、デフォルトで有効になっています。
5. データマスキングを構成します。デフォルトの規則で、または規則をカスタマイズしてデータマスキングを実行できます。
6. 収集した診断情報をアップロードするか保存するかを選択します。
   - [収集した診断情報を **Citrix** にアップロードする] を選択した場合、マスキングされた診断情報ファイルが Citrix にアップロードされます。

- ［収集した診断情報をローカルマシンに保存する］を選択した場合、元の診断情報とマスキングされた診断情報の両方が指定された場所に保存されます。

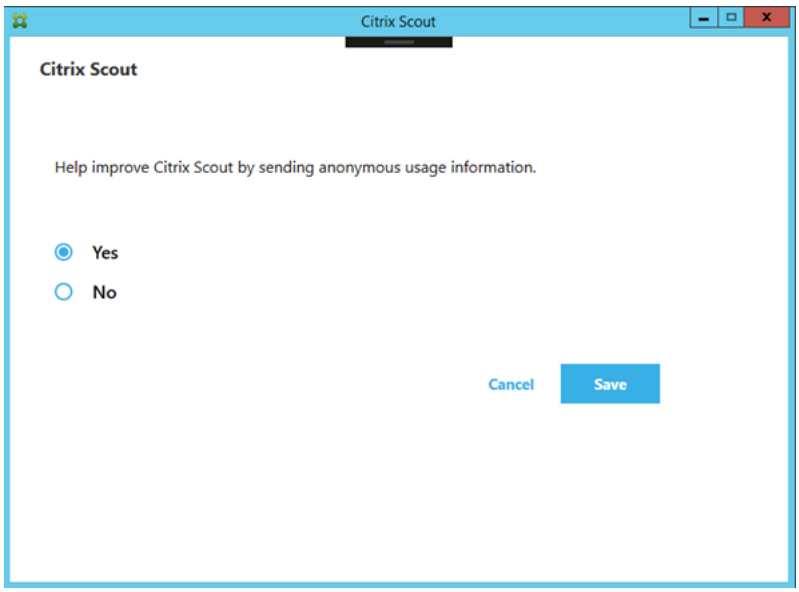
マスキングされたデータファイルとマッピングファイルの場所

診断情報をアップロードまたは保存したあと、リンクをクリックして元の診断情報やマスキングされた診断情報を開いたり、マッピング情報ファイルを開いたりできます。

使用状況データ収集

Scout を使用する場合、Citrix は Google Analytics を使用して匿名の使用状況データを収集し、将来の製品機能や改善に役立てます。データ収集は、デフォルトで有効に設定されています。

使用状況データの収集とアップロードを変更するには、Scout UI の ［設定］歯車をクリックします。次に、［はい］か ［いいえ］を選択して情報を送信するかどうかを選択できます。選択したら ［保存］をクリックします。



システム起動時に **Citrix Diagnostic Facility**（**CDF**）トレースを収集する

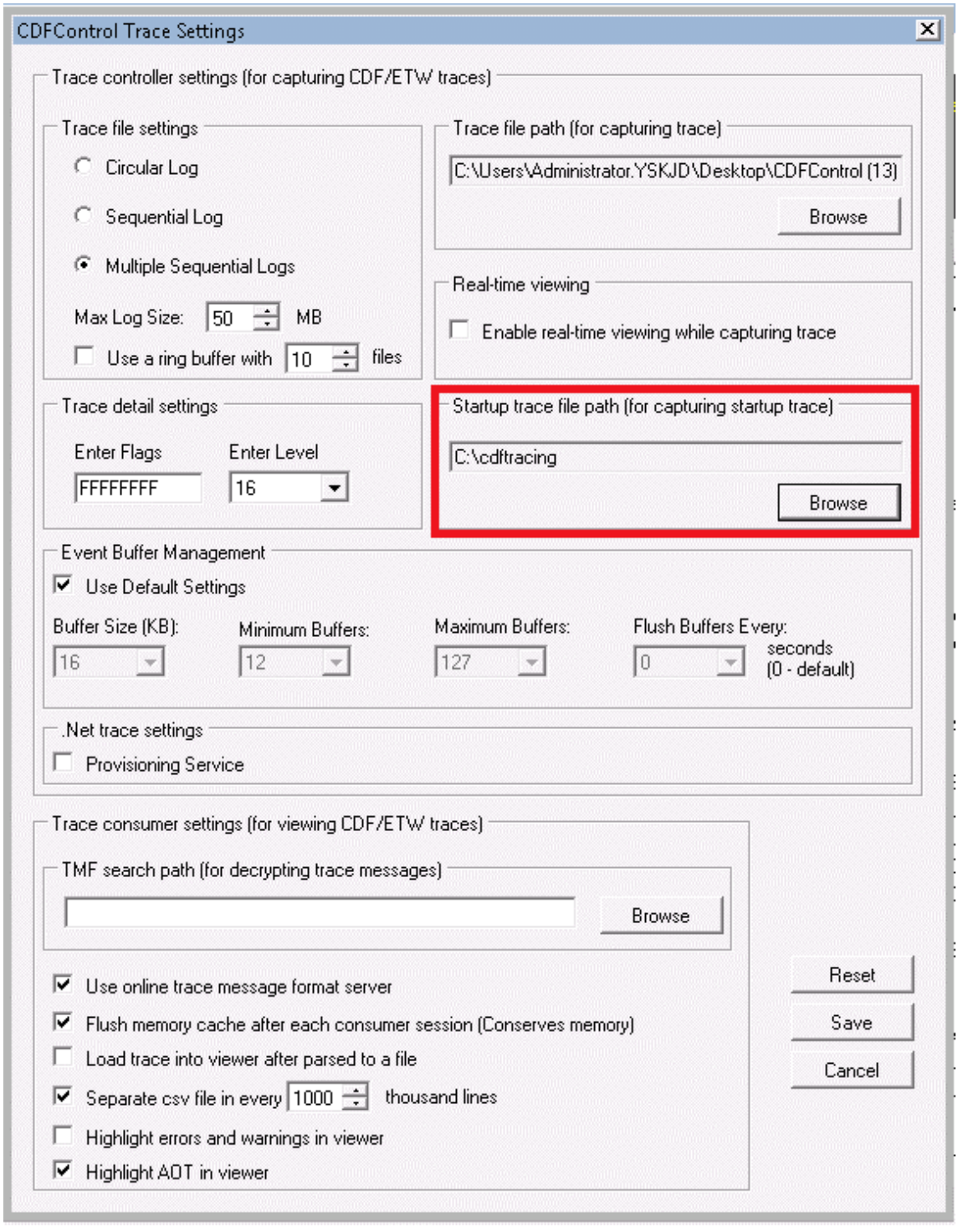
August 17, 2024

CDFControl ユーティリティはイベントトレースコントローラー、つまりコンシューマーであり、各種 Citrix トレースプロバイダーに表示される Citrix Diagnostic Facility（CDF）トレースメッセージを記録します。このユーティリティは、Citrix に関連する複雑な問題のトラブルシューティング、フィルターサポートの解析、パフォーマンスデータの収集を行うためのものです。CDFControl ユーティリティのダウンロード方法については、CTX111961を参照してください。

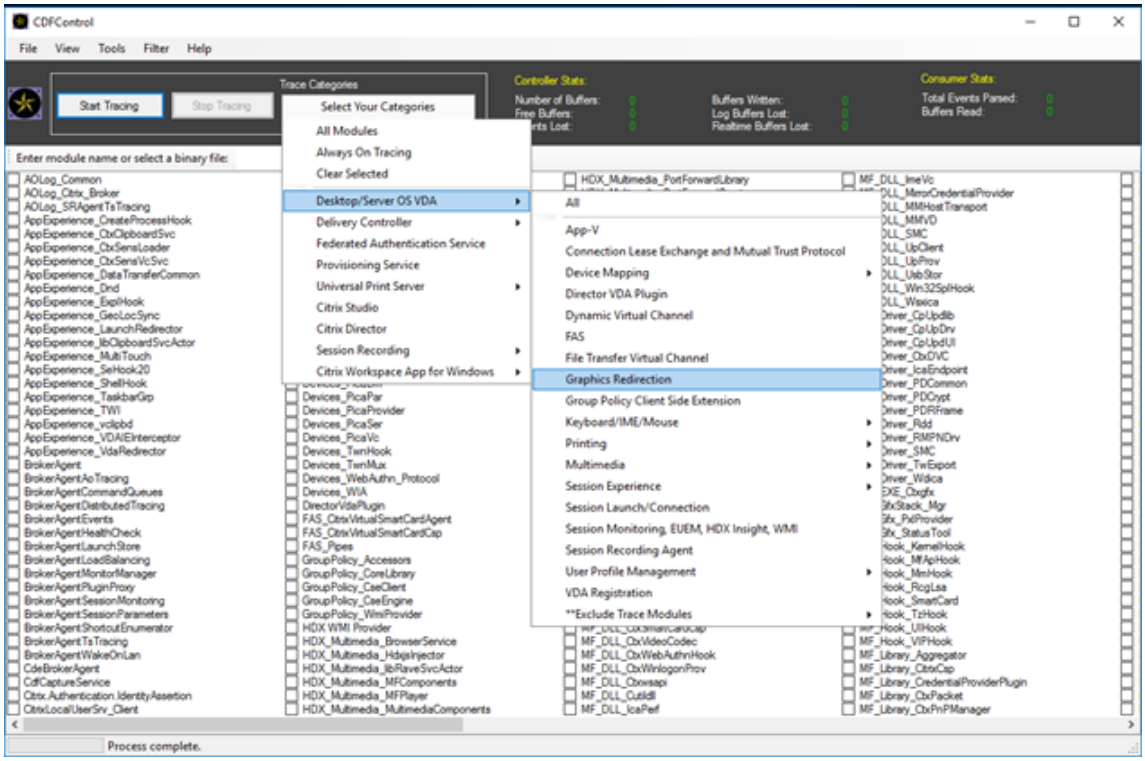
システムの起動時にトレースを収集する

システムの起動時に CDF トレースを収集するには、次の手順を実行します。管理者特権が必要です。

1. **CDFControl** を起動し、［**Tools**］メニューで ［**Options**］を選択します。
2. ［**Startup trace file path for capturing startup trace**］セクションで、トレースファイルのパスを指定します。次に、［**Save**］をクリックします。



3. Citrix サポートから推奨された [**Trace Categories**] を選択します。(次の例では、[**Graphics Redirection**] が選択されています。この選択はほんの一例です。トラブルシューティングでは、特定の問題に関するプロバイダーを有効にすることをお勧めします。)



4. [**Startup Tracing**] を選択し、[**Tools**] メニューから [**Enable**] を選択します。

   [**Enable**] をクリックすると、バーのスクロール表示が始まります。このアクティビティは手順には影響しません。次の手順に進みます。

5. [**Startup Tracing**] が有効になったら、**CDFControl utility** を閉じて、システムを再起動します。
6. **CDFControl** ユーティリティを起動します。システムの再起動後にエラーが表示された場合は、[**Tools**] メニューから [**Startup Tracing** を選択して [**Disable**] をクリックし、起動トレースを無効にします。
7. 手順 2 で指定したトレースファイルのパスへ移動し、分析用のトレースログファイル（.etl）を収集します。

委任管理

August 17, 2024

> 注:
>
> Web Studio（Web ベース）と Citrix Studio（Windows ベース）の 2 つの管理コンソールを使用して、Citrix Virtual Apps and Desktops の展開を管理できます。この記事では Web Studio のみを扱います。Citrix Studio について詳しくは、Citrix Virtual Apps and Desktops 7 2212 以前の同様の記事を参照してください。

委任管理モデルにより、役割やオブジェクトベースの制御により、組織の管理業務の分担に基づいて柔軟に管理権限を委任することができます。あらゆる規模のサイトで委任管理機能を使用でき、展開環境が複雑化するにつれてより詳細な権限の分担を構成できます。管理権限の委任機能では、管理者、役割、およびスコープという 3 つの概念が使用されます。

- 管理者：管理者は、Active Directory アカウントにより識別される、管理権限を持つ個人またはそのグループを示します。各管理者には、1 つまたは複数の役割とスコープのペアが割り当てられます。
- 役割：役割は管理ジョブの機能を表し、それぞれ定義された権限が割り当てられています。たとえば、［デリバリーグループ管理者］の役割には、「デリバリーグループの作成」および「デリバリーグループからのデスクトップの削除」などの権限があります。管理者は、サイトに対して複数の役割を有することができ、1 人の管理者がデリバリーグループ管理者とマシンカタログ管理者を兼ねることができます。役割には、組み込みの役割とカスタムの役割があります。

  組み込みの役割は、次のとおりです。

役割	アクセス許可
完全な管理者	すべてのタスクおよび操作を実行できます。［すべての管理権限を実行できる管理者］の役割は、常に［すべて］のスコープとペアになります。
読み取り専用管理者	全体的な情報に加えて、指定されたスコープのすべてのオブジェクトを表示できますが、変更はできません。たとえば、「大阪」というスコープを作成して読み取り専用管理者に割り当てると、構成ログなどのグローバルオブジェクトと、大阪支社用のデリバリーグループなど、［大阪］スコープのオブジェクトを表示できます。ただし、この管理者は「ニューヨーク」スコープのオブジェクトを表示できません。
ヘルプデスク管理者	デリバリー グループを表示して、そのセッションやマシンを管理できます。監視対象のデリバリーグループについて、マシンカタログとホスト情報を表示できます。また、それらのデリバリーグループ内のマシンのセッションや電源を管理できます。
マシンカタログ管理者	マシンカタログを作成および管理したり、マシンカタログにマシンをプロビジョニングしたりできます。仮想化インフラストラクチャ、Provisioning Services、および物理マシンを使用してマシンカタログを作成できます。この役割では、基本イメージを管理したりソフトウェアをインストールしたりできますが、アプリケーションやデスクトップをユーザーに割り当てることはできません。

役割	アクセス許可
デリバリーグループ管理者	アプリケーション、デスクトップ、およびマシンを配信し、関連するセッションの管理もできます。ポリシーや電源管理設定など、アプリケーションおよびデスクトップの構成を管理することもできます。
ホスト管理者	ホスト接続およびその関連リソース設定を管理できます。マシン、アプリケーション、またはデスクトップをユーザーに配信することはできません。

この製品の一部のエディションでは、必要に応じてカスタムの役割を作成して、より詳細な権限を委任することができます。カスタムの役割では、コンソールにおける操作またはタスク単位で権限を割り当てることができます。

- スコープ：接続、マシンカタログ、デリバリーグループなど、その管理者が管理できるオブジェクトをグループ化したものです。スコープでは、組織の要件に基づいてオブジェクトをグループ化します（営業チームで使用されるデリバリーグループのセットなど）。オブジェクトを複数のスコープに含めることができます。つまり、1 つまたは複数のスコープでオブジェクトをラベル付けすることができます。組み込みのスコープである「すべて」には、すべてのオブジェクトが含まれています。［すべての管理権限を実行できる管理者］の役割は、常にこのスコープとペアになります。

例

XYZ 社は自社の部署（経理、営業、倉庫）およびそのデスクトップオペレーティングシステム（Windows 7 または Windows 8）に基づいてアプリケーションとデスクトップを管理することにしました。管理者は 5 つのスコープを作成し、各デリバリーグループに 2 つのスコープ（部署を表すスコープと使用するオペレーティングシステムを表すスコープ）を割り当てました。

次の管理者を作成しました。

管理者	役割	スコープ
ドメイン/fred	完全な管理者	すべて（［すべての管理権限を実行できる管理者］の役割は、常に［すべて］スコープとペアになります）
ドメイン/rob	読み取り専用管理者	すべて
ドメイン/heidi	読み取り専用管理者、ヘルプデスク管理者	すべての営業担当者
ドメイン/warehouseadmin	ヘルプデスク管理者	倉庫

管理者	役割	スコープ
ドメイン/peter	デリバリーグループ管理者、マシンカタログ管理者	Win7

- Fred は「すべての管理権限を実行できる管理者」で、システム内のすべてのオブジェクトを表示、編集、および削除できます。
- Rob はサイト内のすべてのオブジェクトを表示できますが、それらを編集または削除することはできません。
- Heidi はすべてのオブジェクトを表示でき、［営業］スコープのデリバリーグループでヘルプデスクタスクを実行できます。これにより、［営業］スコープのデリバリーグループに割り当てられているセッションとマシンを管理できます。ただし、これらのデリバリーグループに（マシンの追加や削除などの）変更を加えることはできません。
- Active Directory セキュリティグループ warehouseadmin のすべてのメンバーは、［倉庫］スコープのマシンに対するヘルプデスクタスクを表示および実行できます。
- Peter は Windows 7 の専門家で、すべての Windows 7 マシンカタログを管理でき、所属している部署のスコープに関係なく Windows 7 アプリケーション、デスクトップ、およびマシンを配信できます。当初、管理者は Peter を［Win7］スコープの「すべての管理権限を実行できる管理者」にしようとしました。しかし、管理者はこれを考え直しました。これは、「すべての管理権限を実行できる管理者」には、そのスコープに含まれていないオブジェクト（「サイト」や「管理者」など）に対する全権限が付与されるためです。

委任管理の使用方法

一般的に、管理者数およびその権限の細分性は展開のサイズおよびその複雑度に応じて異なります。

- 小規模または検証用の展開サイトでは、1 人または少数の管理者ですべてを管理します。委任管理はありません。この場合、組み込みの［すべての管理権限を実行できる管理者］役割（および［すべて］スコープ）の管理者を作成します。
- より多くのマシン、アプリケーション、およびデスクトップがあるサイトでは、委任管理者の配置が必要になります。何人かの管理者に、より専門的な管理責任（役割）を付与できます。たとえば、2 人の「すべての管理権限を実行できる管理者」を設定して、残りをヘルプデスク管理者にします。さらに、マシンカタログなど、特定グループ（スコープ）のオブジェクトの管理を 1 人の管理者に委任することもできます。この場合、新しいスコープを作成して、組み込みの役割とそのスコープをペアにした管理者を作成します。
- 大規模サイトにおいても、より多くの（またはより詳細な）スコープと、特殊な役割を持つさまざまな管理者が必要になることがあります。この場合は、追加のスコープを作成または編集して、カスタムの役割を作成し、組み込みまたはカスタムの役割と既存または新しいスコープを持つ各管理者を作成します。

スコープは、管理者を作成するときに作成できます。また、マシンカタログやホスト接続を作成または編集するときにスコープを指定することもできます。

管理者の作成と管理

ローカルの管理者アカウントを使用してサイトを作成するときは、すべてのオブジェクトに対する完全な管理権限を持つ管理者としてそのアカウントが設定されます。ただし、サイトを作成した後では、ローカル管理者には特別な特権は与えられません。

すべての管理タスクの実行権限を持つ管理者には、常に［すべて］のスコープが割り当てられます。これを変更することはできません。

デフォルトでは、管理者は有効になります。管理者を作成するときに、その管理者が実際に作業を始めるまで管理者を無効にしておく必要が生じる場合があります。また、オブジェクトやスコープを再構成するときに、既存の管理者を一時的に無効にすることもできます。完全な管理権限を持つ管理者が 1 人しかいない環境では、その管理者を無効にすることはできません。管理者の有効/無効は、管理者を作成、コピー、または編集するときの［管理者を有効にする］チェックボックスで設定できます。

管理者を編集したりコピーしたりするときのダイアログボックスでスコープ/役割ペアを削除すると、その管理者とスコープ/役割ペアとの関連付けが削除され、個々のスコープや役割は削除されません。役割やスコープは削除されません。また、同じスコープ/役割ペアが割り当てられている管理者がいる場合でも、その関連付けは削除されません。

管理者を作成および管理するには、次の手順に従います:

1. Web Studio にサインインして、左側のペインで ［管理者］をクリックし、［管理者］タブをクリックします。
2. 完了するタスク用の手順を実行します:

    - 管理者を作成する：操作バーの ［管理者の作成］をクリックします。ユーザーアカウント名を入力するか参照し、スコープを選択または作成して、役割を選択します。新しい管理者はデフォルトで有効になりますが、無効にすることもできます。
    - 管理者をコピーする：管理者を選択し、操作バーで ［管理者のコピー］をクリックします。ユーザーアカウント名を入力するか参照します。必要に応じて、スコープ/役割ペアを編集または削除したり、新しいペアを追加したりできます。新しい管理者はデフォルトで有効になりますが、無効にすることもできます。
    - 管理者を編集する：管理者を選択し、操作バーで ［管理者の編集］をクリックします。必要に応じて、スコープ/役割ペアを編集または削除したり、新しいペアを追加したりできます。
    - 管理者を削除する：管理者を選択し、操作バーで ［管理者の削除］をクリックします。完全な管理権限を持つ管理者が 1 人しかいない環境では、その管理者を削除することはできません。

上ペインに、作成した管理者が表示されます。管理者を選択すると、その詳細が下ペインに表示されます。［警告］列に、管理者に割り当てられた役割とスコープのペアに、使用できない役割またはスコープが含まれているかどうかが示されます。割り当てられた役割とスコープのペアに使用できない役割またはスコープが含まれている場合、次の警告メッセージが表示されます:

- 割り当てられている役割またはスコープが使用できません

> 重要:
>
> 警告メッセージは、割り当てられた役割とスコープのペアに使用できない役割またはスコープ（もしくはその両方）が含まれている場合にのみ表示されます。

管理者から役割とスコープのペアを削除するには、次のいずれかの手順を実行します:

- 役割とスコープのペアを削除する。
  1. 操作バーで、［管理者の編集］をクリックします。
  2. ［管理者名および詳細］ウィンドウで、役割とスコープのペアを選択し、［削除］をクリックします。
  3. ［保存］をクリックして終了します。
- 管理者を削除する。
  1. 操作バーで、［管理者の削除］をクリックします。
  2. 確認のウィンドウで ［削除］をクリックします。

役割の作成と管理

管理者が役割を作成または編集する場合、自身が持っている権限のみを有効にできます。これにより、管理者は現在よりも多くの権限を持つ役割を作成して自身に割り当てる（または既に割り当てられた役割を編集する）ことができなくなります。

役割には、64 文字までの Unicode 文字で名前を付けることができます。ただし、バックスラッシュ、スラッシュ、セミコロン、コロン、番号記号、コンマ、アスタリスク、疑問符、等号、小なり記号、大なり記号、パイプ、角かっこ、丸かっこ、二重引用符、およびアポストロフィは使用できません。説明には、256 文字までの Unicode 文字を入力できます。

組み込みの役割を編集または削除することはできません。いずれかの管理者が使用しているカスタムの役割は削除できません。

> 注:
>
> カスタムの役割を作成するには、特定の製品エディションが必要です。カスタムの役割をサポートするエディションのみで、操作バーに関連エントリが表示されます。

役割を作成および管理するには、次の手順に従います:

1. Web Studio にサインインして、左側のペインで ［管理者］をクリックし、［役割］タブをクリックします。
2. 完了するタスク用の手順を実行します:
   - 役割の詳細を表示する：その役割を選択します。下ペインに、その役割のオブジェクトの種類および許可される権限が一覧表示されます。ここで ［管理者］タブをクリックすると、その役割が割り当てられている管理者が表示されます。

- カスタム役割を作成する：操作バーの ［役割の作成］をクリックします。名前と説明を入力します。この役割に割り当てるオブジェクトの種類と権限を選択します。
- 役割をコピーする：役割を選択し、操作バーの ［役割のコピー］をクリックします。必要に応じて、役割の名前、説明、および権限を変更します。
- カスタム役割を編集する：役割を選択し、操作バーの ［役割の編集］をクリックします。必要に応じて、役割の名前、説明、および権限を変更します。
- カスタム役割を削除する：役割を選択し、操作バーの ［役割の削除］をクリックします。確認のメッセージが表示されたら、［削除］をクリックします。

スコープの作成と管理

サイトを作成すると、［すべて］のスコープのみが使用可能になります。このスコープは削除できません。

スコープを作成するには、次の手順を使用します。管理者を作成するときにスコープを作成することもできます。すべての管理者は、少なくとも 1 つの役割とスコープのペアが割り当てられている必要があります。デスクトップ、マシンカタログ、アプリケーション、またはホストを作成したり編集したりするときに、それらを既存のスコープに追加できます。ただし、特定のスコープに追加しない場合でも、自動的に［すべて］のスコープに追加されます。

サイトの作成および委任管理オブジェクト（スコープおよび役割）をスコープに含めることはできません。ただし、スコープに含めることができないオブジェクトも［すべて］のスコープには含まれています。すべての管理タスクの実行権限を持つ管理者には、常に［すべて］のスコープが割り当てられます。マシン、電源操作、デスクトップ、およびセッションはスコープに含まれません。これらのオブジェクトに関する権限は、マシンカタログまたはデリバリーグループで管理者に割り当てることができます。

スコープの作成と管理のルール：

- スコープには、Unicode 文字で 64 文字以下の名前を付けることができます。スコープ名には、次の文字は使用できません：バックスラッシュ、スラッシュ、セミコロン、コロン、番号記号、コンマ、アスタリスク、疑問符、等号、小なり記号、大なり記号、パイプ、角かっこ、丸かっこ、二重引用符、アポストロフィ。
- スコープの説明には、256 文字までの Unicode 文字を入力できます。
- スコープをコピーまたは編集するときにオブジェクトをスコープから削除すると、管理者がそのオブジェクトにアクセスできなくなる可能性があることに注意してください。編集するスコープにいくつかの役割が関連付けられている場合は、編集により役割/スコープのペアが使用できなくならないかどうかを確認してください。

スコープを作成および管理するには、次の手順に従います：

1. Web Studio にサインインして、左側のペインで［管理者］をクリックし、［スコープ］タブをクリックします。
2. 完了するタスク用の手順を実行します：

    - スコープを作成する：操作バーの ［**Create new Scope**］をクリックします。名前と説明を入力します。オブジェクトの種類（［デリバリーグループ］チェックボックスなど）を選択すると、その種類のすべてのオブジェクトがスコープに追加されます。特定のオブジェクトを追加するには、オブジェクトの

種類を開き、個々のオブジェクトを選択します（営業部で使用される特定のデリバリーグループを選択する場合など）。

- スコープのコピー：スコープを選択し、操作バーの ［スコープのコピー］をクリックします。名前と説明を入力します。必要に応じて、オブジェクトの種類とオブジェクトを変更します。
- スコープの編集：スコープを選択し、操作バーの ［スコープの編集］をクリックします。必要に応じて、名前、説明、オブジェクトの種類、およびオブジェクトを変更します。
- スコープの削除：スコープを選択し、操作バーの ［スコープの削除］をクリックします。確認のメッセージが表示されたら、［削除］をクリックします。

テナント管理の設定

テナント管理を設定して、単一の Citrix Virtual Apps and Desktops サイト内に管理パーティションを作成します。各テナントには、マシンカタログやデリバリーグループなどの分離されたリソースと構成があります。特定のテナントへのアクセス権を持つ管理者は、そのテナントに関連付けられたリソースと構成のみを管理できます。使用例には次のようなものがあります：

- 単一のサイトにさまざまなビジネスサイロ（独立した部門または個別の IT 管理チーム）がある。
- 単一サイトで複数の顧客向けの展開をセットアップおよび管理する Citrix サービスプロバイダー。

大まかに言えば、テナント管理を設定するためのワークフローには次のものが含まれます：

1. テナントを作成する
2. テナントの管理者を追加する

テナントを作成する

テナントスコープを作成してテナントを作成します。詳細な手順は次のとおりです：

1. Web Studio にサインインして、左側のペインで［管理者］をクリックし、［スコープ］タブをクリックします。
2. *［スコープの作成］** をクリックして、テナントの作成を開始します。
3. テナントのスコープの次の詳細を入力します：

    a) スコープのわかりやすい名前を入力します。この名前はテナントの識別子としても機能します。
    b)（オプション）簡単な説明を入力します。
    c)［テナントのスコープ］を選択します。
    d) 必要に応じて、テナントに関連付けられているオブジェクトを選択します。オブジェクトを作成または管理するときに、テナントのスコープにオブジェクトを追加することもできます。
    e)［**OK**］をクリックして作成を完了します。

完了すると、次の内容が表示されます：

- 新しいテナントスコープのレコードがスコープ一覧に表示され、［種類］列でテナントとして識別されます。

- スコープ名は、Web Studio の右上隅にある ［すべてのテナント］ドロップダウンリストに表示されます。

テナントのスコープを使用する場合は、次の点に注意してください:

- テナントプロパティは、次の階層の順序で割り当てられます: ホスト > マシンカタログ > デリバリーグループ > アプリケーション。下位レベルのオブジェクトは、上位レベルのオブジェクトからテナントプロパティを継承します。たとえば、テナントのスコープでデリバリーグループを選択するときは、関連するホストとマシンカタログも選択する必要があります。選択しないと、デリバリーグループはテナントプロパティを継承できません。
- テナントスコープを作成した後、オブジェクトを変更してテナントの割り当てを編集できます。テナントの割り当てが変更された場合でも、同じテナントまたはそれらのテナントのサブセットに割り当てる必要があるという制約があります。ただし、テナントの割り当てが変更されても、下位レベルのオブジェクトは再評価されません。テナントの割り当てを変更するときは、オブジェクトが適切に制限されていることを確認してください。たとえば、TenantAとTenantBのマシンカタログが使用できる場合、TenantAのデリバリーグループとTenantBのデリバリーグループを作成できます（TenantAとTenantBは両方ともそのマシンカタログに関連付けられています）。次に、TenantAのみに関連付けられるようにマシンカタログを変更できます。その結果、TenantBに関連付けられているデリバリーグループは無効になります。

テナントの管理者を追加する

ユーザーアカウントに管理者の役割とテナントを割り当てて、テナントの管理者を追加します。

テナントの管理者を追加するには、次の手順を実行します:

1. Web Studio にサインインして、左側のペインで ［管理者］をクリックし、［管理者］タブをクリックします。
2. ［管理者の追加］をクリックし、次の手順に従って完了します:
   a) ユーザーアカウント名を入力するか、参照してから ［次へ］をクリックします。
   b) ［カスタムアクセス］を選択し、必要に応じて 1 つまたは複数の役割（マシンカタログ管理者など）を選択します。
   c) 各役割の横にある ［スコープの編集］をクリックし、スコープを ［すべて］から目的のテナントスコープに変更して、［保存］をクリックします。
3. ［次へ］をクリックします。
4. ［**Review and confirm**］ページで ［**Send invitation**］をクリックします。

レポートの作成

次の 2 種類の委任管理レポートを作成できます:

- 管理者に関連付けられているスコープ/役割ペアと各種類のオブジェクト（デリバリーグループおよびマシンカタログなど）に対する個々の権限の一覧についての HTML レポート。Web Studio で生成できます。

  このレポートを作成するには、以下の手順に従います:

1. Web Studio にサインインして、左側のペインで ［管理者］をクリックします。
2. 管理者を選択し、操作バーで ［レポートの作成］をクリックします。

このレポートは、管理者の作成、コピー、および編集時に作成することもできます。

- 組み込みおよびカスタムの役割とそれらに関連付けられた権限を一覧表示する HTML または CSV レポート。このレポートは、PowerShell スクリプト OutputPermissionMapping.ps1 を実行して生成します。

  このスクリプトを実行するには、すべての管理権限を実行できる管理者、読み取り専用管理者、または役割の読み取り権限を持つ管理者である必要があります。このスクリプトは、Program Files\Citrix\DelegatedAdmin\SnapIn\Citrix.DelegatedAdmin.Admin.V1\Scripts\ にあります。

  構文:

  ```
  OutputPermissionMapping.ps1 [-Help] [-Csv] [-Path string] [-AdminAddress string] [-Show] [CommonParameters]
  ```

パラメーター	説明
-Help	スクリプトのヘルプを表示します。
-Csv	CSV レポートを作成します。デフォルト値：HTML
-Path string	出力先を指定します。デフォルト値：stdout
-AdminAddress string	接続先の Delivery Controller の IP アドレスまたはホスト名を指定します。デフォルト値：localhost
-Show	（-Pathパラメーターを指定した場合のみ有効）ファイルに出力する場合に-Show を指定すると、-Showによりレポートが適切なアプリケーションプログラム（Web ブラウザーなど）で表示されます。
CommonParameters	Verbose、Debug、ErrorAction、ErrorVariable、WarningAction、WarningVariable、OutBuffer、OutVariable。詳しくは、Microsoft 社のドキュメントを参照してください。

次の例では、Roles.html という名前のファイルに HTML テーブルが出力され、Web ブラウザーで表示されます。

```
& "$env:ProgramFiles\Citrix\DelegatedAdmin\SnapIn\
Citrix.DelegatedAdmin.Admin.V1\Scripts\OutputPermissionMapping.ps1"
-Path Roles.html  - Show
```

次の例では、Roles.csv という名前のファイルに CSV テーブルが出力されます。このテーブルは自動的には表示されません。


```
& "$env:ProgramFiles\Citrix\DelegatedAdmin\SnapIn\
Citrix.DelegatedAdmin.Admin.V1\Scripts\OutputPermissionMapping.ps1"
 - CSV -Path Roles.csv
```

上の例を Windows コマンドプロンプトから実行する場合は、次のコマンドを実行します:

```
powershell -command "& '%ProgramFiles%\Citrix\DelegatedAdmin\SnapIn\
Citrix.DelegatedAdmin.Admin.V1\Scripts\OutputPermissionMapping.ps1'
-CSV -Path Roles.csv"
```

Delivery Controller

August 17, 2024

> 注:
>
> Web Studio (Web ベース) と Citrix Studio (Windows ベース) の 2 つの管理コンソールを使用して、Citrix Virtual Apps and Desktops の展開を管理できます。この記事では Web Studio のみを扱います。Citrix Studio について詳しくは、Citrix Virtual Apps and Desktops 7 2212 以前の同様の記事を参照してください。

Delivery Controller は、ユーザーアクセスの管理や接続の仲介と最適化を行うためのサーバー側のコンポーネントです。また、Controller は、デスクトップおよびサーバーイメージを作成する Machine Creation Service も提供します。

サイトには、1 つ以上の Controller が必要です。1 つめの Controller のインストール後、サイトを作成するとき、または後日、さらに Controller を追加できます。サイトに複数の Controller があると、以下の 2 つの利点がもたらされます。

- 冗長性: ベストプラクティスとしては、実稼働サイトでは、常に 2 つ以上の Controller をそれぞれ異なる物理サーバー上に配置してください。一方の Controller に障害が発生しても、他方の Controller で接続を管理し、サイトを制御できます。
- スケーラビリティ: サイトのアクティビティが増えるにつれ、Controller 上の CPU 使用率およびデータベースアクティビティも増加します。Controller を追加すると、より多くのユーザーやより多くのアプリケーションとデスクトップ要求を処理できるようになり、制御処理全体を向上させることができます。

各 Controller は、サイトデータベースと直接通信します。複数のゾーンを持つサイトでは、各ゾーンに存在する Controller が、プライマリゾーンにあるサイトデータベースと通信します。

> 重要:
>
> サイトを構成した後は、コンピューター名や Controller のドメインメンバーシップを変更しないでください。

Controller への **VDA** の登録方法

VDA を使用するには、そのサイトの Delivery Controller に登録（接続を確立）する必要があります。VDA の登録について詳しくは、「Delivery Controller への VDA の登録」を参照してください。

Controller の追加、削除、または移動

Controller の追加、削除、移動を行うには、データベースの記事に記載されているサーバーの役割とデータベースの役割の権限が必要です。

SQL クラスター化または SQL ミラー化インストールにおける、ノード上への Controller のインストールはサポートされていません。

Delivery Controller をサイトに追加する際には、そのマシンのログオン資格情報を、高可用性のために使用するレプリカ SQL Server に追加してください。

展開環境でデータベースのミラーリングを使用している場合は、以下の点について注意してください。

- Controller を追加、削除、または移動する前に、プライマリデータベースとミラーデータベースの両方が実行中であることを確認してください。また、SQL Server Management Studio でスクリプトを使用している場合は、スクリプト実行前に SQLCMD モードを有効にしてください。
- Controller の追加、削除、または移動後にミラーリングを確認するには、PowerShell コマンドレットの`Get-configdbconnection`を実行します。このコマンドレットにより、ミラーに対する接続文字列でフェールオーバーパートナーが設定されているかどうかを確認できます。

Controller の追加、削除、または移動後の作業

- 自動更新が有効な場合、VDA は 90 分以内に最新の Controller 一覧を受信します。
- 自動更新が無効な場合は、すべての VDA について Controller ポリシー設定または ListOfDDCs レジストリキーが更新されていることを確認してください。Controller をほかのサイトに移動した後は、両方のサイトでポリシー設定またはレジストリキーを更新する必要があります。

Controller の追加

Controller は、サイトの作成時、または後日、追加できます。このソフトウェアの以前のバージョンでインストールされた Controller を、このバージョンで作成されたサイトに追加することはできません。

1. サポートされているオペレーティングシステムが稼動しているサーバーでインストーラーを実行します。Delivery Controller コンポーネントと、必要なコアコンポーネントをすべてインストールします。インストールウィザードを完了します。
2. サイトをまだ作成していない場合は、この Controller でCitrix Site Managerを実行してサイトを作成します。この Controller の IP アドレスは、新しいサイトに自動的に追加されます。

データベースの初期化スクリプトを生成する場合は、そのスクリプトを生成する前に Controller を追加してください。

3. 既にサイトを作成している場合は、次の手順に従います:

   a) この Controller でCitrix Site Managerを実行し、［**Join an existing site**］をクリックして、参加するサイトの Controller のアドレスを入力します。
   b) Studio 構成ツールを使用して、Controller を Web Studio に追加します。

Controller の削除

サイトから Controller を削除しても、Citrix ソフトウェアやその他のコンポーネントはアンインストールされません。このアクションにより、Controller がデータベースから削除され、接続の仲介や他のタスクの実行に使用できなくなります。削除した Controller を、後で元のサイトや別のサイトに追加することができます。サイトには最低 1 つの Controller が必要なため、Web Studio の一覧に表示される最後の Controller を削除することはできません。

サイトから Controller 削除しても、データベースサーバーへの Controller ログオンは削除されません。これは、同じマシン上のほかの製品のサービスで使用されるログオンが削除されるのを防ぐためです。ログオンが不要になった場合は、手動で削除する必要があります。ログオンを削除するには、`securityadmin`サーバーの役割のアクセス権限が必要です。

Controller の削除後の作業:

- 自動更新を使用する VDA は、他の使用可能な Controller に再登録します。この再登録は、自動更新メカニズムが有効になっていて、VDA が（削除された Controller と同じセカンダリゾーン内、またはオンプレミス展開のプライマリゾーン内の）他の Controller に到達できる場合にのみ発生します。
- Citrix StoreFront の Controller 情報を更新します。詳しくは、「Controller の管理」を参照してください。
- Citrix StoreFront で、Citrix Gateway を介したリモートアクセスのために Secure Ticket Authority（STA）の URL を更新します。詳しくは、「Secure Ticket Authority の管理」を参照してください。
- Citrix Gateway で、仮想サーバーの STA の URL を更新します。詳しくは、「Ctirix Gateway」を参照してください。

> 重要:
>
> サイトから Controller を削除するまでは、Active Directory からその Controller を削除しないでください。

1. Controller が動作しており、1 時間以内にその Controller が Web Studio にロードされることを確認してください。削除する Controller を Web Studio がロードしたら、Controller 上のすべてのサービスが実行中であり、Controller の電源がオフになっていることを確認します。
2. Web Studio にサインインし、左側のペインで ［設定］を選択します。
3. ［**Delivery Controller**］タイルを見つけて、［編集］をクリックします。
4. ［**Delivery Controller** の管理］ページで、削除する Controller を選択します。

5. ［コントローラーの削除］を選択します。適切なデータベースロールや権限がない場合は、Controller を削除するためのスクリプトを生成できます。そのスクリプトの実行をデータベース管理者に依頼してください。

   Web Studio は、Controller を削除する前に事前チェックを実行します。Controller の電源がオフで、次のサービス状態でない場合は、Controller を安全に取り外すことができます。

   - 不明
   - データベース保留中エラー
   - 古いバージョン
   - 新しいバージョン
   - バージョンの変更中
   - 必須機能がありません

   Controller の電源がオフになっておらず、前述のサービス状態のいずれかである場合、Web Studio は Controller の電源をオフにするように求めます。

6. データベースサーバーから Controller のマシンアカウントを削除する必要があります。削除前に、ほかのサービスがそのアカウントを使用していないことを確認してください。

Web Studio を使って Controller を削除した後、実行中のタスクを適切に完了させるためにその Controller へのトラフィックがしばらく残ることがあります。Controller を即座に削除するには、Controller がインストールされているサーバーをシャットダウンするか、Active Directory からそのサーバーを削除することを Citrix ではお勧めします。その後で、サイト内のほかの Controller を再起動します。これにより、削除された Controller との通信が行われなくなります。

Controller の別のゾーンへの移動

サイトに複数のゾーンが含まれている場合、Controller を別のゾーンに移動できます。VDA 登録やほかの操作に対するこの操作の影響については、「ゾーン」を参照してください。

1. 左側のペインで ［ゾーン］を選択します。
2. 中央ペインでゾーンを選択し、Controller を選択します。
3. 操作バーで ［アイテムの移動］を選択します。
4. 表示された ［アイテムの移動］ページで、Controller を移動するゾーンを選択します。
5. ［保存］をクリックします。

VDA から別のサイトへの移動

VDA が Citrix Provisioning を使ってプロビジョニングされた場合、または既存のイメージの場合は、アップグレード時、またはテストサイトで作成された VDA イメージを実稼働サイトに移動させる場合に、VDA をほかのサイトに（サイト 1 からサイト 2 へ）移動できます。Machine Creation Services（MCS）を使用してプロビジョニングされた VDA は、あるサイトから別のサイトに移動することはできません。MCS では、Controller に登録するため

に VDA がチェックする ListOfDDC の変更をサポートしていません。MCS を使用してプロビジョニングされた VDA は、それらが作成されたサイトに関連付けられた ListOfDDC を常にチェックします。

VDA をほかのサイトに移動するにはインストーラーを使用するか、Citrix ポリシーを使用します。

インストーラー　インストーラーを実行し、サイト 2 の Controller の完全修飾ドメイン名（DNS エントリ）を指定して、Controller を追加します。

Controller のポリシー設定を使用しない場合にのみ、インストーラーで Controller を指定してください。

グループポリシーエディター　次の例では、複数の VDA をほかのサイトに移動します。

1. サイト 1 でポリシーを作成して以下のように設定し、そのポリシーを VDA 移行を行うデリバリーグループに割り当てます。
    - Controller：サイト 2 の 1 つまたは複数の Controller の完全修飾ドメイン名（DNS エントリ）を指定します。
    - Controller の自動更新を有効にする：［無効］に設定します。
2. デリバリーグループの各 VDA は、新しいポリシーの適用後 90 分以内にアラートを受信します。VDA は、受信した Controller の一覧を無視して（自動更新が無効なため）、ポリシーで指定されている、サイト 2 のいずれかの Controller を選択します。
3. VDA がサイト 2 の Controller への登録に成功すると、サイト 2 の ListOfDDCs およびポリシー情報を受け取り、これによりデフォルトで自動更新が有効になります。サイト 1 での VDA 登録先の Controller は、サイト 2 の Controller によって送信された一覧にはありません。そのため、サイト 2 の一覧の Controller のいずれかに VDA が再登録されます。これにより、VDA はサイト 2 からの情報に基づいて自動的に更新されます。

グループポリシーエディターの使用方法については、「Citrix ポリシー」のドキュメントを参照してください。

IPv4/IPv6 サポート

August 17, 2024

このリリースでは、IPv4 のみまたは IPv6 のみ（ピュア IPv4 またはピュア IPv6）の環境がサポートされ、重複する IPv4 と IPv6 のネットワークを使用した「デュアルスタック」環境がサポートされます。

次のコンポーネントは IPv4 のみをサポートします。その他はすべて IPv4 と IPv6 をサポートしています。

- XenServer
- ［**IPv6 Controller** 登録のみを使用する］ポリシー設定が設定されていない Virtual Delivery Agent（VDA）

IPv6 通信は、VDA 接続関連の 2 つの Citrix ポリシー設定で制御されます。

- **IPv6** を強制的に使用するプライマリ設定： IPv6 Controller 登録のみを使用する。

  このポリシー設定では、Delivery Controller への登録時に VDA で使用されるアドレスの形式を指定します。

  有効にすると、VDA が Controller に対して登録および通信を行うときに、グローバル IP アドレス、ユニークローカルアドレス（ULA）、リンクローカルアドレス（ほかの IPv6 アドレスを使用できない場合のみ）の順で単一の IPv6 アドレスが選択されます。

  この設定が無効な場合、そのマシンの IPv4 アドレスを使用して VDA が Controller と登録および通信を行います。これがデフォルト値です。

  チームが IPv6 ネットワークを頻繁に使用する場合は、[**IPv6 Controller** 登録のみを使用する] ポリシー設定が有効になっているイメージまたは組織単位（OU）に基づいて、それらのユーザーのデスクトップとアプリケーションを公開します。

  チームが IPv4 ネットワークを頻繁に使用する場合は、[**IPv6 Controller** 登録のみを使用する] ポリシー設定が無効になっているイメージまたは OU に基づいて、それらのユーザーのデスクトップとアプリケーションを公開します。

- **IPv6** ネットマスクを定義する従属設定：コントローラー登録の IPv6 ネットマスク。

  各マシンに複数の IPv6 アドレスを設定できます。このポリシー設定では、VDA で使用されるサブネットを指定できます。この場合、グローバル IP は使用されません。この設定では、VDA が登録されるネットワークを指定します。VDA は、指定されたネットマスクに最初にマッチしたアドレスでのみ登録されます。

  この設定を使用する場合は、[**IPv6 Controller** 登録のみを使用する] ポリシー設定を有効にする必要があります。デフォルトでは空文字が設定されています。

展開に関する考慮事項

環境内に IPv4 と IPv6 の両方のネットワークがある場合、IPv4 のみのクライアントと IPv6 ネットワークにアクセスできるクライアントに対して、別個のデリバリーグループ構成を作成します。ユーザーを区別するために、名前付け、手動 Active Directory グループ割り当て、または SmartAccess フィルターの使用を検討してください。
IPv6 ネットワークで接続されたセッションに IPv4 アクセスのみのクライアントから再接続する場合、再接続に失敗することがあります。

注 - これらの考慮事項は、DNS 解決が有効になっている場合には適用されません。

Web Studio を使用した **Citrix Virtual Apps and Desktops** のライセンス

August 17, 2024

> 注:
>
> Web Studio（Web ベース）と Citrix Studio（Windows ベース）の 2 つの管理コンソールを使用して、Citrix Virtual Apps and Desktops の展開を管理できます。この記事では Web Studio のみを扱います。Citrix Studio について詳しくは、Citrix Virtual Apps and Desktops 7 2212 以前の同様の記事を参照してください。

管理者は、Web Studio を使用してライセンスを管理したり監視したりできます（ライセンスサーバーが Web Studio と同じドメインまたは信頼されたドメインで動作する場合）。ライセンス関連のタスクについては、ライセンスのドキュメントおよび「マルチタイプのライセンス」を参照してください。

以下の表に、サポートされるエディションとライセンスモデルを示します。

製品	エディション	ライセンスモデル
Citrix Virtual Apps	Premium、Advanced、Standard	同時使用
Citrix Virtual Desktops	Premium、Advanced、Standard	ユーザー/デバイスおよび同時使用

詳しくは、「同時使用ライセンス」および「ユーザー/デバイスライセンス」を参照してください。

サポートされる最新リリース（**CR**）および長期サービスリリース（**LTSR**）のバージョン

以下の表に、Citrix Virtual Apps and Desktops、XenApp および XenDesktop でサポートされる **LS** の最小互換バージョンを示します。Citrix 製品のライフサイクル日程について詳しくは、「製品マトリクス」を参照してください。

> 重要:
>
> 次の表の情報は、製品の互換性を示すためにのみ提供されています。改善された機能またはセキュリティのメリットを得るために、常に最新バージョンの Citrix ライセンスサーバーを使用することを強くお勧めします。
>
> 注:
>
> ライセンスサーバー VPX はサービス終了しており、今後、メンテナンスやセキュリティ修正サービスの提供を受けることはできません。11.16.6 以前のバージョンのライセンスサーバー VPX を使用しているお客様は、できるだけ早く最新バージョンの Windows 用ライセンスサーバーに移行することをお勧めします。

最新リリース	LS の最小互換バージョン
2305	11.17.2.0 ビルド 35000
2303	11.17.2.0 ビルド 35000

最新リリース	LS の最小互換バージョン
2212	11.17.2.0 ビルド 35000
2209	11.17.2.0 ビルド 35000
2206	11.17.2.0 ビルド 35000
2203	11.17.2.0 ビルド 35000
2112	11.17.2.0 ビルド 35000
2109	11.17.2.0 ビルド 35000
2106	11.17.2.0 ビルド 35000
2103	11.16.3.0 ビルド 28000

長期サービスリリース	LS の最小互換バージョン
2203 LTSR	11.17.2.0 ビルド 35000
1912 LTSR	11.16.3.0 ビルド 28000
7.15 LTSR	11.15.0.0 ビルド 24100
7.6 LTSR	11.14.0.1 ビルド 21103

従来の製品と製品バージョンの情報については、「レガシー製品マトリクス」を参照してください。

次のタスクを完了するには、すべての管理作業を実行できるライセンス管理者である必要があります。Web Studio でライセンス情報を表示するには、［ライセンスの表示］以上の委任管理権限が必要です。この権限は、組み込みのすべての管理作業を実行できる管理者と読み取り専用管理者の役割に含まれています。

Web Studio を使用したライセンスのダウンロードとインストール

1. Web Studio にサインインし、左側のペインで ［ライセンス］をクリックします。
2. 操作バーで ［ライセンスの割り当て］を選択します。
3. ライセンスアクセスコードを入力します。ライセンスの購入後または更新後に、Citrix からメールが届きます。
4. 製品を選択して、［ライセンスの割り当て］を選択します。その製品に使用できるライセンスが割り当てられダウンロードされます。ライセンスアクセスコードを入力してすべてのライセンスを割り当ておよびダウンロードすると、そのライセンスアクセスコードは再使用できなくなります。同じコードで他のライセンス処理が必要な場合は、My Account にログオンしてください。

ローカルコンピューターまたはネットワークに保存されているライセンスの追加

1. Web Studio にサインインし、左側のペインで ［ライセンス］をクリックします。
2. 操作バーで ［ライセンスの割り当て］を選択します。
3. ライセンスファイルを参照して、ライセンスサーバーに追加します。

ライセンスサーバーの変更

1. Web Studio にサインインし、左側のペインで ［ライセンス］をクリックします。
2. 操作バーで ［ライセンスサーバーの変更］を選択します。
3. ライセンスサーバーのアドレスを 「*name:port*」形式で入力します。name はライセンスサーバーの DNS、NetBIOS、または IP アドレスです。ポート番号（<port>）を指定しない場合、デフォルトのポート（27000）が使用されます。

使用するライセンスの種類の選択

- サイトを構成するときに、ライセンスサーバーを指定した後で、使用するライセンスの種類を選択します。サーバーにライセンスがない場合は、30 日間製品を試用できるオプションが自動的に選択されます。
- サーバーに複数のライセンスがある場合はその詳細が表示されます。いずれかのライセンスを選択します。または、サーバーにライセンスファイルを追加してそれを選択します。

製品エディションおよびライセンスモデルの変更

1. Web Studio にサインインし、左側のペインで ［ライセンス］をクリックします。
2. 操作バーで ［製品エディションの編集］を選択します。
3. 適切なオプションを更新します。

ライセンス管理コンソールにアクセスするには、操作バーで ［ライセンス管理コンソール］を選択します。ライセンス管理コンソールが自動的に開くか、パスワードによる保護が構成済みの場合は資格情報を入力するための画面が開きます。コンソールの使い方について詳しくは、ライセンスのドキュメントを参照してください。

> 注:
>
> Web Studio でライセンスを切り替えた場合、その変更が Citrix Director に表示されるまでに最大 5 分かかります。たとえば、Advanced と Premium を切り替える場合、またはその逆の場合です。

ライセンス管理者の追加

1. Web Studio にサインインし、左側のペインで ［ライセンス］をクリックします。
2. ［ライセンス管理者］タブを選択します。

3. 操作バーで ［ライセンス管理者の追加］を選択します。
4. 管理者として追加するユーザーを参照して、権限を選択します。

ライセンス管理者の権限の変更またはライセンス管理者の削除

1. Web Studio にサインインし、左側のペインで ［ライセンス］をクリックします。
2. ［ライセンス管理者］タブを選択し、目的の管理者を選択します。
3. 操作バーで ［ライセンス管理者の編集］または ［ライセンス管理者の削除］を選択します。

ライセンス管理者グループの追加

1. Web Studio にサインインし、左側のペインで ［ライセンス］をクリックします。
2. ［ライセンス管理者］タブを選択します。
3. 操作バーで ［ライセンス管理者グループの追加］を選択します。
4. ライセンス管理者として追加するグループを参照して、権限を選択します。Active Directory グループを追加すると、ライセンス管理者権限がそのグループのすべてのユーザーに設定されます。

ライセンス管理者グループの権限の変更またはライセンス管理者グループの削除

1. Web Studio にサインインし、左側のペインで ［ライセンス］をクリックします。
2. ［ライセンス管理者］タブを選択し、目的の管理者グループを選択します。
3. 操作バーで、［ライセンス管理者グループの編集］または ［ライセンス管理者グループの削除］を選択します。

ライセンス情報の表示

Web Studio にサインインし、左側のペインで ［ライセンス］をクリックします。指定したライセンスサーバーにインストールされているすべてのライセンスの一覧と、それらのライセンスの使用状況およびサイトのライセンス設定の概要が表示されます。

製品の種類、ライセンスのエディション、ライセンスモデルなどのサイトのライセンス設定と、設定済みのライセンスサーバーが使用しているライセンスが一致するようにしてください。一致していない場合は既存のライセンスをダウンロードするか、または割り当てるかしてサイトのライセンス設定に合わせなければならない場合があります。

ライセンスの有効期限通知の表示

Web Studio は、Citrix ライセンスサーバーに照会してライセンスファイルの有効期限情報を取得します。ライセンスファイルの有効期限が近づいているか、既に有効期限が切れている場合、Web Studio で管理者に通知を表示されます。

関連項目

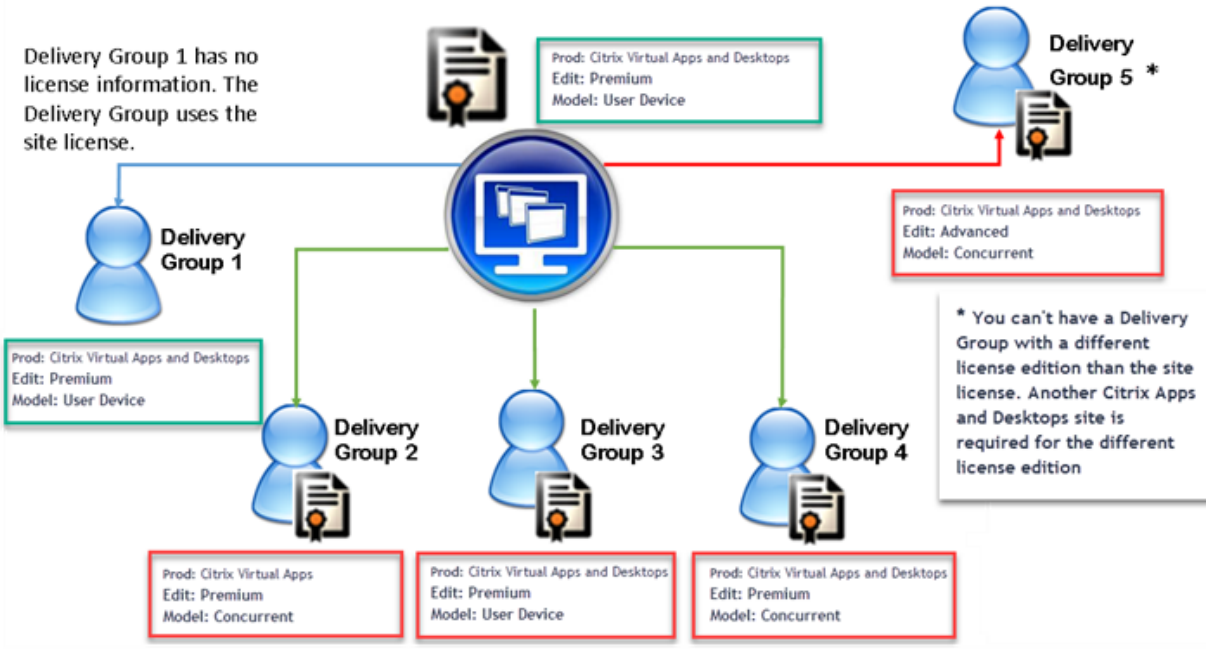
- 「年間および期間ベースの製品版ライセンスの Citrix オンプレミスサブスクリプション」を参照してください。
- 「移行とトレードアップ（TTU）とハイブリッド権利」を参照してください。

マルチタイプのライセンス

August 17, 2024

マルチタイプのライセンスでは、単一の Citrix Virtual Apps and Desktops サイト上にある複数のデリバリーグループでそれぞれ異なる種類のライセンスを使用できます。種類とは、製品 ID（XDT または MPS）とモデル（ユーザーデバイスまたは同時使用）の組み合わせのことです。デリバリーグループは、サイトレベルでの構成と同じ製品エディション（PLT/Premium または ENT/Advanced）を使用する必要があります。Citrix Virtual Apps and Desktops 展開のマルチタイプライセンスを構成する場合は、この記事の最後の「特殊考慮事項」に注意してください。

マルチタイプのライセンスが構成されていない場合は、個別のサイト上で構成されるときのみ異なる種類のライセンスを使用できます。デリバリーグループではサイトのライセンスが使用されます。マルチタイプのライセンス構成時の重要な通知制限については、「特殊考慮事項」を参照してください。



各種類のライセンスを使用するデリバリーグループを指定するには、次の Broker PowerShell コマンドレットを使用します:

- New-BrokerDesktopGroup
- Set-BrokerDesktopGroup
- Get-BrokerDesktopGroup

ライセンスをインストールするには次を使用します。

- Citrix Studio
- Citrix Licensing Manager
- citrix.com

カスタマーサクセスサービスの有効期間は、各ライセンスファイルおよび各製品とモデルに固有です。デリバリーグループ間のカスタマーサクセスサービス有効期間は異なる場合があります。

特殊考慮事項

マルチタイプのライセンスの機能は、通常の Citrix Virtual Apps and Desktops のライセンスとは異なります。

サイト構成と異なる種類を使用するように構成されたデリバリーグループには、Director または Studio からのアラートおよび通知はありません。

- ライセンスの上限に近づいた場合、もしくは追加猶予期間のトリガーまたは有効期限に近づいた場合でも情報は提供されません。
- 特定のグループに問題が発生しても、通知はされません。

マルチタイプのライセンス用に構成されたデリバリーグループは、そのライセンスの種類のみを消費し、完全に消費したあとはサイト構成にフォールバックしません。

Citrix Virtual Apps Standard および Citrix Virtual Desktops Standard のライセンスエディション名は、どちらも Standard であることを示していますが、同じエディションではありません。マルチタイプのライセンスは、Citrix Virtual Apps Standard および Citrix Virtual Desktop Standard のライセンスとともに使用することはできません。

ライセンスの互換性マトリックス

この表は、古い製品名、新しい製品名、および関連する機能名を示しています。互換性の 4 つの列では、マルチタイプライセンスに互換性がある製品とライセンスモデルの組み合わせを指定します。CCU と CCS は同時ライセンスであり、UD はユーザー/デバイスライセンスです。

Old Name	New Name	Feature	Multi-type licensing compatibility			
			STD	ADV	ENT	PLT
Citrix XenApp Standard	Citrix XenApp Standard	MPS_STD_CCU	X			
Citrix XenApp Advanced	Citrix Virtual Apps Standard	MPS_ADV_CCU		X		
Citrix XenApp Enterprise	Citrix Virtual Apps Advanced	MPS_ENT_CCU			X	
Citrix XenApp Platinum	Citrix Virtual Apps Premium	MPS_PLT_CCU				X
Citrix XenDesktop VDI Edition (XDT-U)	Citrix Virtual Desktops Standard- Per User/Device	XDT_STD_UD	X			
Citrix XenDesktop VDI Edition (XDT-C)	Citrix Virtual Desktops Standard - Concurrent	XDT_STD_CCS	X			
Citrix XenDesktop Enterprise Edition (XDT-C)	Citrix Virtual Apps and Desktops Advanced - Concurrent	XDT_ENT_CCS			X	
Citrix XenDesktop Enterprise Edition (XDT-U)	Citrix Virtual Apps and Desktops Advanced - Per User/Device	XDT_ENT_UD			X	
Citrix XenDesktop Platinum Edition (XDT-C)	Citrix Virtual Apps and Desktops Premium - Concurrent	XDT_PLT_CCS				X
Citrix XenDesktop Platinum Edition (XDT-U)	Citrix Virtual Apps and Desktops Premium - Per User/Device	XDT_PLT_UD				X

Broker PowerShell SDK

DesktopGroup オブジェクトには次の 2 つのプロパティがあり、関連する New-BrokerDesktopGroup コマンドレットおよび Set-BrokerDesktopGroup コマンドレットを使用して操作することができます。

名前	値	制限事項
LicenseModel	グループのライセンスモデルを指定するパラメーター（同時使用またはユーザーデバイス）です。何も指定されていない場合、サイト全体のライセンスモデルが使用されます。	機能トグルが無効な場合、プロパティを設定しようとしても失敗します。
ProductCode	グループのライセンス製品 ID を指定する XDT（Citrix Virtual Desktops の場合）または MPS（Citrix Virtual Apps の場合）のテキスト文字列です。何も指定されていない場合、サイト全体の製品コードが使用されます。	機能トグルが無効な場合、プロパティを設定しようとしても失敗します。

LicenseModel および ProductCode について詳しくは、「about_Broker_Licensing」を参照してください。

New-BrokerDesktopGroup

デスクトップのグループの仲介を管理するデスクトップグループを作成します。このコマンドレットについて詳しくは、https://citrix.github.io/delivery-controller-sdk/Broker/New-BrokerDesktopGroup/を参照してください。

Set-BrokerDesktopGroup

既存のブローカーデスクトップグループの有効化と無効化を切り替えるか、またはグループの設定を変更します。このコマンドレットについて詳しくは、https://citrix.github.io/delivery-controller-sdk/Broker/Set-BrokerDesktopGroup/を参照してください。

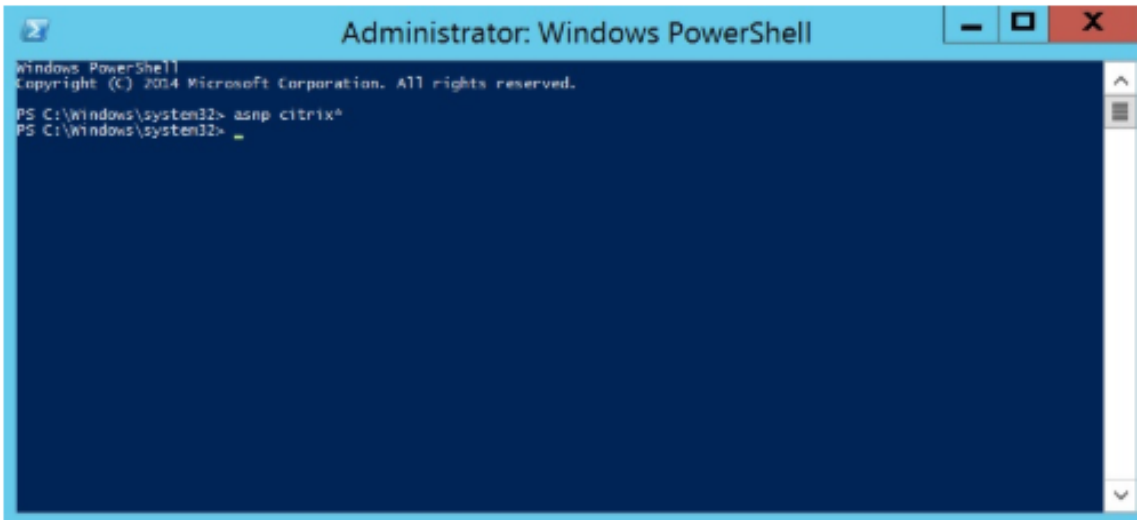
Get-BrokerDesktopGroup

指定した条件に一致するデスクトップグループを取得します。Get-BrokerDesktopGroup コマンドレットの出力には、グループの **ProductCode** プロパティと **LicenseModel** プロパティが含まれます。これらのプロパティが New- BrokerDesktopGroup または Set-BrokerDesktopGroup により設定されていない場合、null 値が返されます。null の場合、サイト全体のライセンスモデルと製品コードが使用されます。このコマンドレットについて詳しくは、https://citrix.github.io/delivery-controller-sdk/Broker/Get-BrokerDesktopGroup/を参照してください。

デリバリーグループごとに異なるライセンス製品とモデルを構成する

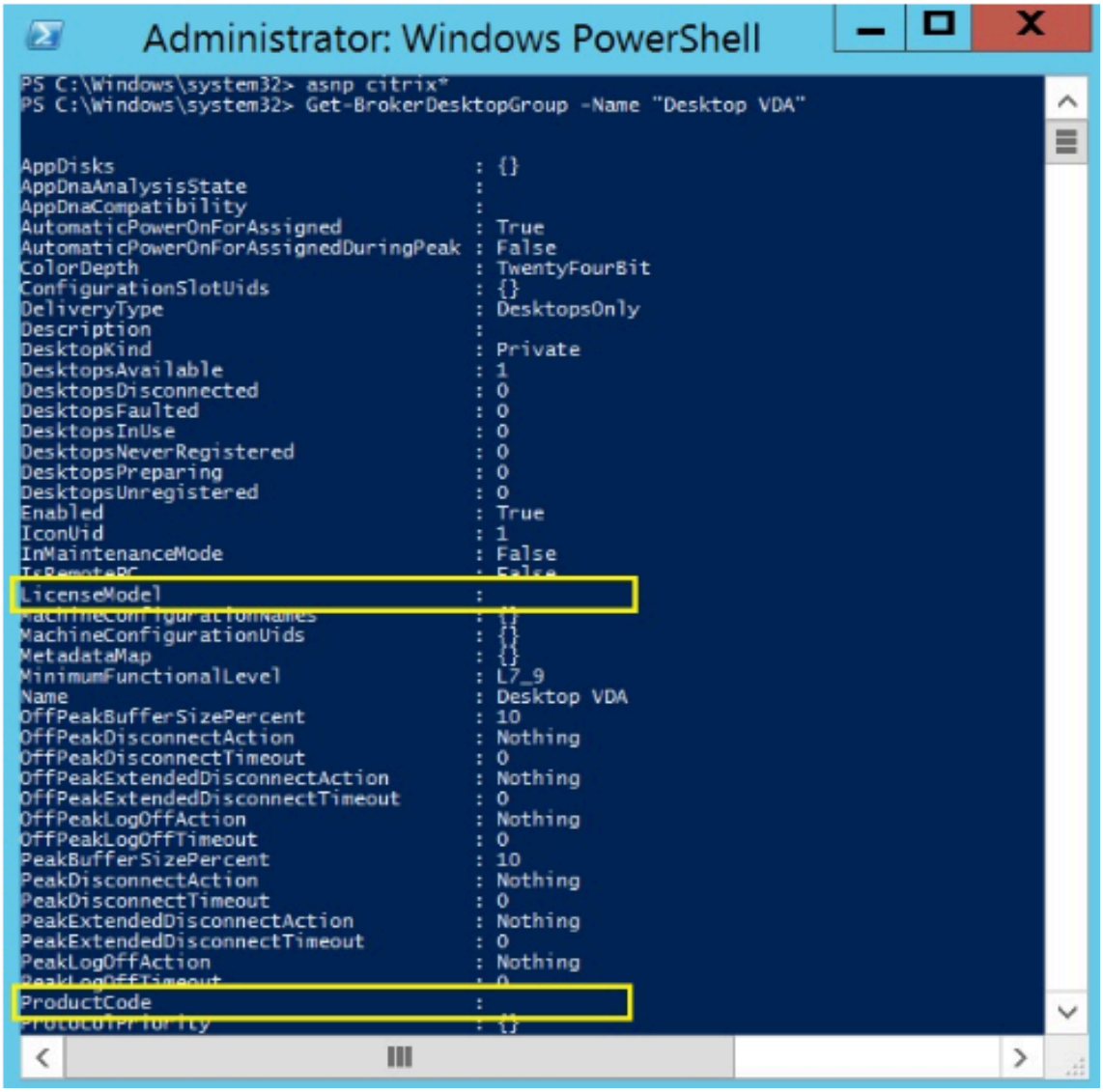
> 注:
>
> 1 つのデリバリーグループで 2 つ以上の異なる種類の製品、エディション、またはライセンスモデルを構成することはできません。異なる種類の製品、エディション、またはライセンスモデルがある場合は、それらを別々のデリバリーグループで構成します。

1. 管理者権限で PowerShell を開き、Citrix スナップインを追加します。

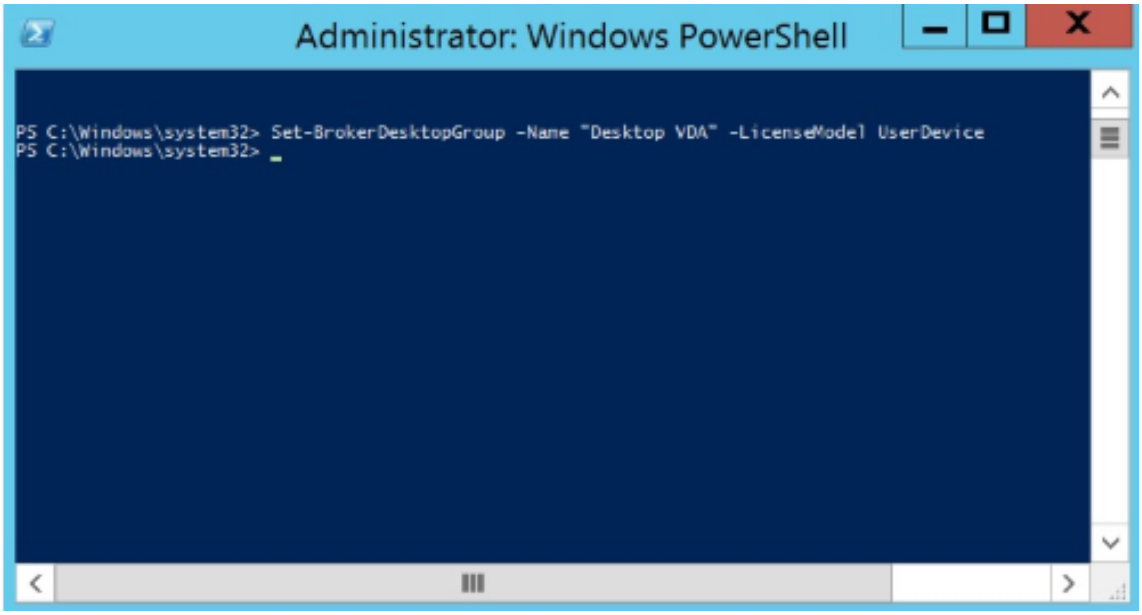


2. コマンド **Get-BrokerDesktopGroup** -**Name** “**DeliveryGroupName**” を実行して最新のライセンス構成を表示します。パラメーター **LicenseModel** および **ProductCode** を参照します。これらのパラメーターを以前に構成してない場合、空白の可能性があります。

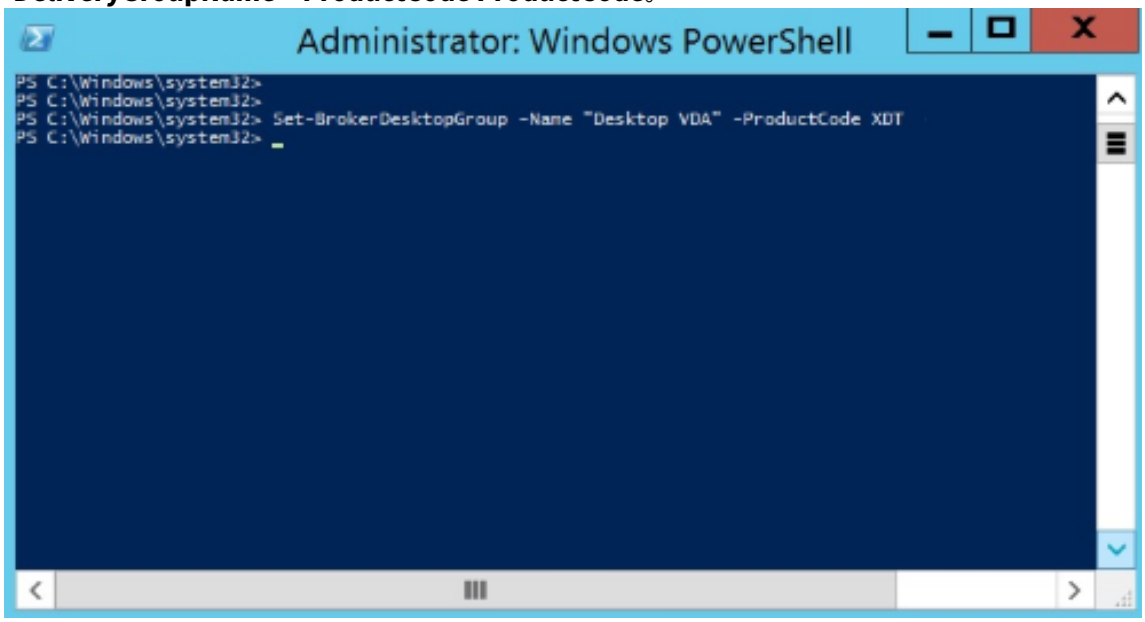
> 注:
>
> デリバリーグループにライセンス情報が設定されていない場合、デフォルトの **Site level Site license** が適用されます。



3. 次のコマンドを実行してライセンスモデルを変更します: **Set-BrokerDesktopGroup -Name "DeliveryGroupName" -LicenseModel LicenseModel**。

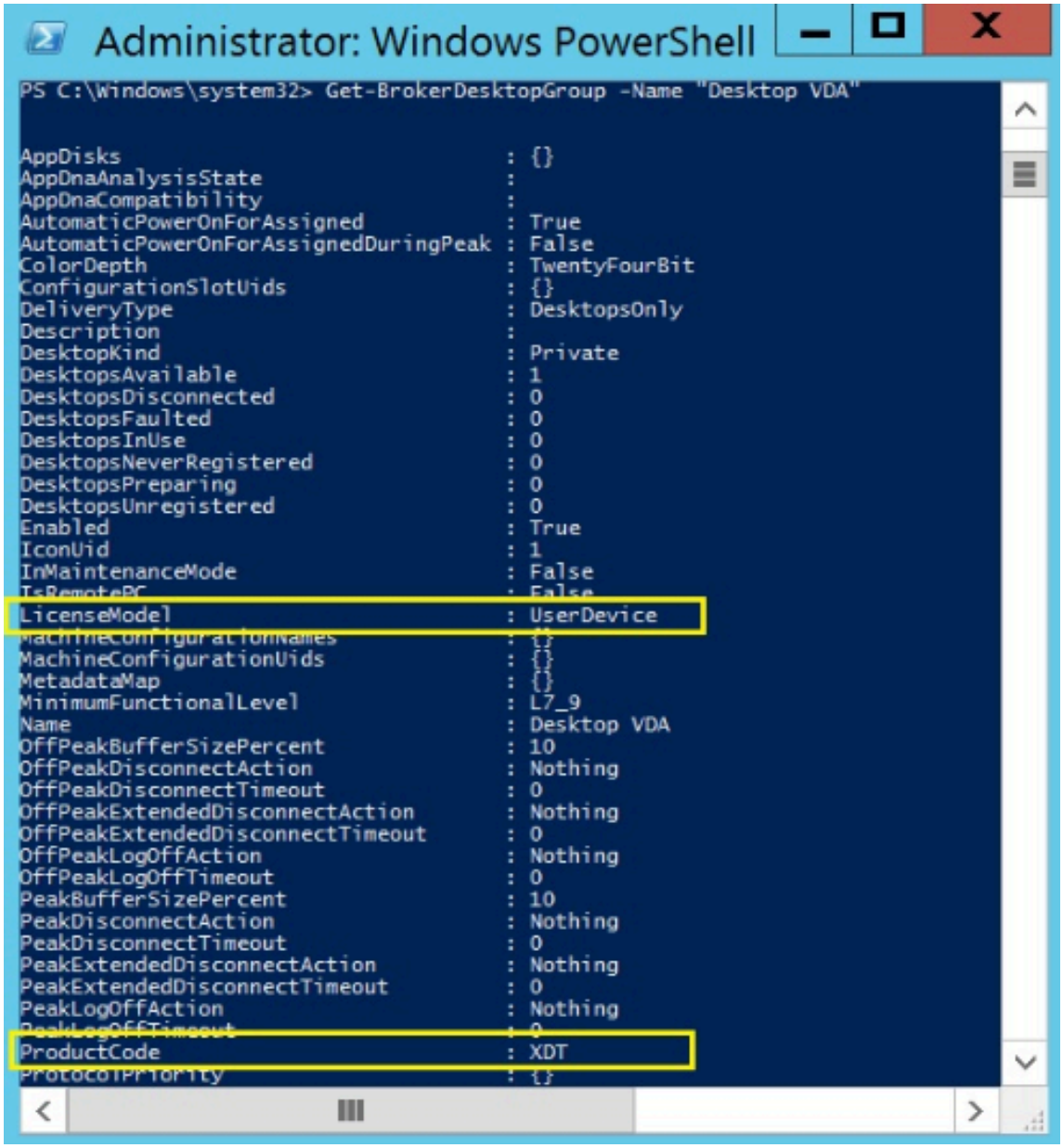


4. 次のコマンドを実行してライセンスモデルを変更します: **Set-BrokerDesktopGroup** –**Name** “**DeliveryGroupName**”–**ProductCode ProductCode**。



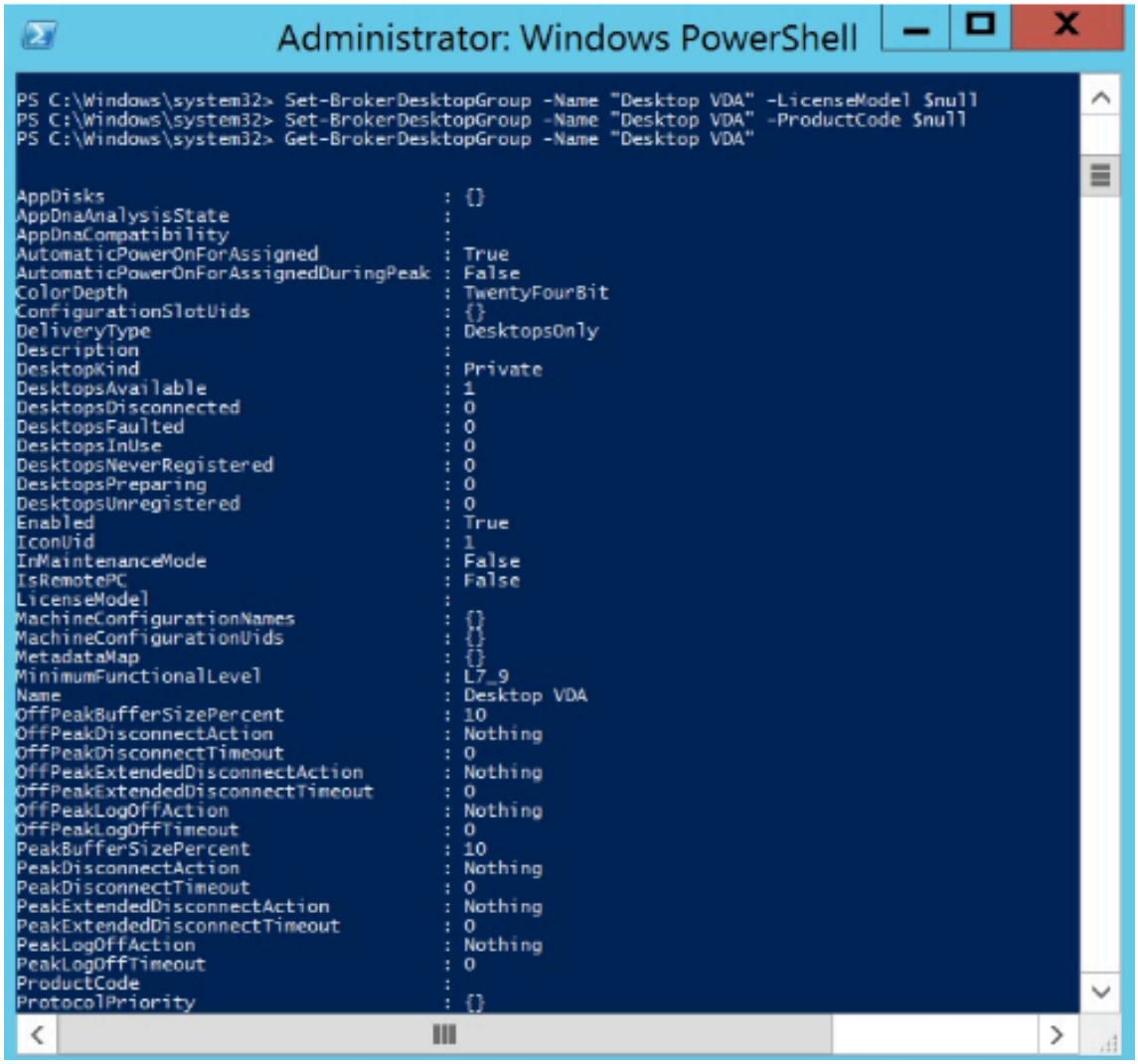
5. コマンド **Get-BrokerDesktopGroup** –**Name** “**DeliveryGroupName**” を入力して変更を確認します。

> 注:
>
> 同じサイトでエディションを混在させて一致させることはできません。たとえば、Premium ライセンスと Advanced ライセンスなどの場合です。異なるエディションのライセンスがある場合は、複数のサイトが必要です。



6. ライセンス構成を削除するには、前述と同じ **Set-BrokerDesktopGroup** コマンドを実行して、値を **$null** に設定します。

> 注:
>
> Studio はデリバリーグループごとにライセンス構成を表示しません。PowerShell を使用して最新の構成を表示します。



例

次の PowerShell コマンドレットの例では、2 つの既存のデリバリーグループに対してマルチタイプのライセンスを設定し、3 番目のデリバリーグループを設定する方法について説明します。

デリバリーグループに関連付けられているライセンス製品とライセンスモデルを確認するには、PowerShell コマンドレット **Get-BrokerDesktopGroup** を使用します。

1. 1 番目のデリバリーグループを XenApp および Concurrent に設定します。

   Set-BrokerDesktopGroup -Name “Delivery group for Citrix Virtual Apps Premium Concurrent” -ProductCode MPS -LicenseModel Concurrent

2. 2 番目のデリバリーグループを XenDesktop および Concurrent に設定します。

   Set-BrokerDesktopGroup -Name “Delivery group for Citrix Virtual Desktops Premium Concurrent” -ProductCode XDT -LicenseModel Concurrent

3. 3 番目のデリバリーグループを作成し、XenDesktop および UserDevice に設定します。

   New-BrokerDesktopGroup -Name “Delivery group for Citrix Virtual Desktops Premium UserDevice” -PublishedName “MyDesktop” -DesktopKind Private -ProductCode XDT -LicenseModel UserDevice

ライセンスについてよく寄せられる質問

August 17, 2024

> 注:
>
> - 新型コロナウイルス（COVID-19）感染拡大に対応したビジネス継続性に関する情報については、CTX27055を参照してください。
> - ビジネス継続性の維持に関する一般的な情報については、「Business continuity —on demand」を参照してください。
> - 最新の Citrix ライセンスサーバーについて詳しくは、「ライセンス」を参照してください。

Citrix ライセンスサーバー

ライセンスファイルを取得するにはどうすればよいですか

ライセンスアクセスコードをメールでお送りします。ライセンスアクセスコードを使用してライセンスファイルを生成するには、次の 3 つの方法があります:

- citrix.comの［マイアカウント］ページにある ［ライセンスの管理］詳しくは、「Citrix.com でのライセンスの管理」を参照してください。
- Web Studio における購入の割り当てと Citrix ライセンスサーバーへのライセンスファイルの自動インストール
- Citrix ライセンスサーバー内の Citrix Licensing Manager における購入の割り当てとライセンスファイルのインストール詳しくは、「ライセンスのインストール」を参照してください。

マイアカウントにライセンスを割り当てる方法

「ライセンスの割り当て」を参照してください。

割り当てられたライセンスをライセンスサーバーに追加する方法

「ライセンスの変更」を参照してください。

Citrix ライセンスサーバーはどの **TCP** ポートが使用されますか

- ライセンスサーバー：27000
- ベンダーデーモン：7279
- 管理コンソール Web ポート：8082
- Web Services for Licensing ポート：8083

Citrix ライセンスサーバーとは何ですか

Citrix ライセンスサーバーは、ネットワークを介したライセンスの共有を可能にするシステムです。詳しくは、「ライセンス処理の概要」を参照してください。

Citrix ライセンスサーバーを仮想化またはクラスター化できますか

はい。Citrix ライセンスサーバーは仮想化することも、クラスター化することもできます。詳しくは、「ライセンスサーバーのクラスター化」を参照してください。

Citrix ライセンスサーバーを仮想化すると、どのようなメリットがありますか

Citrix ライセンスサーバーを仮想化すると、冗長なソリューションが提供されます。このソリューションにより、ダウンタイムなしで複数の物理サーバーを切り替えることが可能になります。

Citrix ライセンスサーバーを仮想化する場合に考慮する必要がある制限はありますか

いいえ。

Citrix ライセンスサーバーでは、**Citrix Virtual Apps and Desktops** 環境のライセンスがすべて管理されますか

Citrix ライセンスサーバーは、Citrix Gateway で使用される Premium Edition のライセンスを除き、Citrix Virtual Apps and Desktops で受け取るすべてのライセンスを管理します。これらの Premium Edition のライセンスは、セキュリティ指向のネットワークデバイスで必要とされるネットワークアプライアンスに組み込まれたライセンスサーバーによって管理されます。

Citrix Licensing Manager とは何ですか

Citrix Licensing Manager がインストールされているライセンスサーバーからライセンスファイルをダウンロードし、割り当てることができます。Citrix Licensing Manager はライセンスサーバーの推奨管理手段であり、以下を実行できます：

- 短いコードを使用してライセンスサーバーを Citrix Cloud に登録でき、登録解除も簡単です。
- ユーザーアカウントとグループアカウントを構成します。
- ダッシュボードを使用して、インストールされたライセンス、使用中のライセンス、期限切れのライセンス、使用可能なライセンス、カスタマーサクセスサービス日を表示します。
- レポートで使用するため、ライセンス使用データをエクスポートします。
- 使用履歴データの保持期間を構成。デフォルトのデータ保有期間は 180 日です。
- ライセンスアクセスコードまたはダウンロードしたファイルを使用して、ライセンスファイルをライセンスサーバーに簡単にインストールできます。
- 追加猶予期間を有効または無効にする。
- カスタマーエクスペリエンス向上プログラム（CEIP）と Call Home を構成します。
- カスタマーサクセスサービス更新ライセンスを自動または手動で確認し、ライセンスが見つかると通知またはインストール。
- 次のライセンスサーバーの状態を通知 - 起動ライセンスの不足、時間の問題、アップローダの失敗。
- 以下のポートの変更:
  - ライセンスサーバー（デフォルトは 27000）
  - ベンダーデーモン（デフォルトは 7279）
  - Web Services For Licensing（デフォルトは 8083）

詳しくは、「Citrix Licensing Manager」を参照してください。

Citrix ライセンス管理コンソールはどこにありますか**?**

ライセンス管理コンソールは、サポートが終了し、ライセンスサーバーバージョン 11.16.6 から削除されました。Citrix Licensing Manager を使用することをお勧めします。

ライセンスサーバーが Studio と同じドメインまたは信頼済みドメインにある場合、Studio を使用してライセンスを管理および追跡できます。

詳しくは、「Citrix Licensing Manager」を参照してください。

ライセンス割り当て期間とは何ですか

ライセンス割り当て期間は、Citrix Virtual Apps and Desktops ライセンスがユーザーまたはデバイスに割り当てられる期間です。デフォルトのライセンス割り当て期間は 90 日です。

組織が購入したライセンスの数を確認するにはどうすればよいですか

https://www.citrix.comの ［マイアカウント］ページにある安全な ［ライセンスの管理］ツールボックスで、購入したすべてのライセンスを 24 時間 365 日いつでもレビューでき、またそれらにアクセスできます。

特定の時点で使用されているライセンスの数を確認するにはどうすればよいですか

Citrix Licensing Manager と Studio では、ライセンスの使用に関する詳細がリアルタイムで提供されます。

ライセンスサーバーの障害回復とメンテナンス

ライセンスサーバーの障害回復とメンテナンスについては、Citrix ライセンスサーバードキュメントの「障害回復とメンテナンス」を参照してください。

Citrix Virtual Apps and Desktops ライセンス

Citrix Virtual Apps and Desktops のライセンスはどのように割り当てられますか

Citrix Virtual Apps and Desktops のライセンスでは、ユーザー/デバイスモデルと同時使用ライセンスモデルが提供されています。

ユーザー/デバイス:

柔軟性の高いユーザー/デバイスモデルは、以下に適しています:

- エンタープライズ規模でのデスクトップの使用。
- 基盤となる Microsoft デスクトップ仮想化ライセンス。
- ユーザーが仮想デスクトップと仮想アプリにアクセスする頻度が低い顧客向けの同時使用ライセンス。

ユーザー/デバイスライセンスでは、ユーザーが仮想デスクトップと仮想アプリにアクセスできるデバイスの数に制限がありません。デバイスライセンスでは、1 台のデバイスから仮想デスクトップとアプリにアクセスできるユーザーの数に制限がありません。このアプローチは柔軟性を最大化し、Microsoft デスクトップ仮想化ライセンスに適しています。

> 重要:
>
> ユーザーまたはデバイスにライセンスを手動で割り当てることはできません。ライセンスサーバーまたはクラウドサービスによってライセンスが割り当てられます。ユーザー/デバイスライセンスでは、一度割り当てられたライセンスは 90 日間非アクティブになるまで別のユーザーに割り当てることができません。

同時使用:

同時使用ライセンスでは、ユーザーおよびデバイスに対し、数に制限のない仮想アプリおよびデスクトップへの接続が 1 つ許可されます。ライセンスは、アクティブなセッション中にのみ使用されます。セッションが切断または終了している間、ライセンスはプールにチェックインされます。

ユーザー/デバイスライセンスについて詳しくは「ユーザー/デバイスライセンス」、同時使用ライセンスについて詳しくは「同時使用ライセンス」を参照してください。

ライセンスを購入する前に **Citrix Virtual Apps and Desktops** を試用できますか

はい。Citrix Virtual Apps and Desktops ソフトウェアをダウンロードして、試用モードで実行できます。試用モードでは、Citrix Virtual Apps and Desktops オンプレミスをライセンスなしで 30 日間、10 接続まで使用できます。詳しくは、「評価版ライセンス」を参照してください。

Citrix Cloud 用の Citrix DaaS（旧称 Citrix Virtual Apps and Desktops サービス）は、承認に基づいて試用サービスを利用できます。詳しくは、Citrix の担当者にお問い合わせください。

Citrix では、**Citrix Virtual Apps and Desktops** の同時使用をどのように定義していますか

Citrix Virtual Apps and Desktops の同時使用モデルでは、ユーザーおよびデバイスに対し、数に制限のない仮想アプリおよびデスクトップへの接続が 1 つ許可されます。ライセンスは、アクティブなセッション中にのみ使用されます。セッションが切断または終了している間、ライセンスは再発行に備えてプールにチェックインされます。詳しくは、「同時使用ライセンス」を参照してください。

1 つのライセンスサーバーに、複数のエディションの **Citrix Virtual Apps and Desktops** ライセンスを展開できますか

はい。ライセンスサーバーは、両方の Citrix Virtual Apps and Desktops のライセンスを同時に管理できます。最新バージョンのライセンスサーバーをインストールすることをお勧めします。ライセンスサーバーのバージョンが適正かどうかわからない場合は、Citrix のダウンロードサイトにあるバージョン番号を参照して調べることができます。

1 つのサイトで **Citrix Virtual Apps** と **Citrix Virtual Apps and Desktops** の両方のライセンスを使用できますか

バージョンによっては、1 つの Citrix Virtual Apps または Citrix Virtual Apps and Desktops サイトでユーザー/デバイスと同時接続の両方のライセンスモデルに対応できます。1 つの Citrix Virtual Apps または Citrix Virtual Apps and Desktops サイトで対応できるエディションは、1 つのみです。詳しくは、「マルチタイプのライセンス」を参照してください。

複数のタイプのライセンスに対応するのは、XenApp および XenDesktop 7.15 長期サービスリリース（LTSR）および Citrix Virtual Apps and Desktops 7 1808 以上のバージョンです。

ライセンスサーバーに **Citrix Virtual Apps and Desktops** のユーザー/デバイスライセンスまたは **Citrix Virtual Apps and Desktops** の同時使用ライセンスがインストールされている場合、製品モデルとして **Citrix Virtual Apps** 同時使用を選択できますか

Citrix Virtual Apps and Desktops Advanced Edition または Premium Edition の機能として Citrix Virtual Apps を使用する場合、Citrix Virtual Apps のライセンスモデルは Citrix Virtual Apps and Desktops の Ad-

vanced Edition または Premium Edition と同じになります。Citrix Virtual Apps and Desktops を購入した場合は、Citrix Virtual Apps の機能のみを使用する予定であっても、ライセンスを Citrix Virtual Apps and Desktops として構成します。Citrix Virtual Apps 同時使用スタンドアロンライセンスがライセンスサーバーにインストールされている場合にのみ、Citrix Virtual Apps を製品モデルとして選択します。

Citrix Virtual Apps と **Citrix Virtual Apps and Desktops** の各エディションにはどの製品コンポーネントが含まれていますか

エディションごとの詳細な機能マトリックスについては、「Citrix Virtual Apps and Desktops の機能」を参照してください。

Citrix Virtual Apps and Desktops のライセンス契約書に準拠して **Citrix Virtual Desktops** 環境のライセンスを取得するにはどうすればよいですか

Citrix Virtual Apps and Desktops のライセンス契約書に準拠し、ユーザー/デバイスライセンスモデルまたは同時使用ライセンスモデルで Citrix Virtual Apps and Desktops を展開するには、ライセンスファイルをライセンスサーバーに適用します。ライセンスサーバーによって、ライセンスのコンプライアンスが制御および監視されます。購入内容に基づいて製品を構成することをお勧めします。たとえば、Citrix Virtual Apps and Desktops Premium を購入するものの、Citrix Virtual Apps の機能のみを使用する場合は、コンプライアンスのため製品を Citrix Virtual Apps and Desktops に構成します。詳しくは、「製品ライセンスコンプライアンスセンター」を参照してください。

Citrix Virtual Apps and Desktops のライセンス契約書に準拠して **Citrix Virtual Apps** 環境のライセンスを取得するにはどうすればよいですか

Citrix Virtual Apps のライセンス契約書に準拠し、同時使用ライセンスモデルで Citrix Virtual Apps を展開するには、ライセンスファイルをライセンスサーバーに適用します。ライセンスサーバーによって、ライセンスのコンプライアンスが制御および監視されます。

Citrix Virtual Apps and Desktops のサービスオプションである長期サービスリリース（**LTSR**）または最新リリース（**CR**）に関するライセンス要件はありますか

長期サービスリリースなどの Citrix Virtual Apps and Desktops のサービスオプションは、カスタマーサクセスサービスプログラムの特典です。LTSR の特典を受けるには、カスタマーサクセスサービスがアクティブである必要があります。詳しくは、「[Citrix Virtual Apps、Citrix Virtual Apps and Desktops、XenServer のサービスオプション」を参照してください。

Remote Browser Isolation（**RBI**）サービスのプール時間のしくみ

購入したサービスユーザーの数が 25 以上である場合、5,000 時間のサービス使用権が付与され、すべてのユーザーによって共有されます。後でユーザーの権利を追加購入しても、プール時間は追加で付与されません。サービス使用権の時間を増やすには、アドオンパックを購入する必要があります。

CCU ライセンスをリモート **PC** アクセスで使用することはできますか

はい。

リモート PC アクセスについて詳しくは、「リモート PC アクセス」を参照してください。

Citrix 環境のソフトウェアメンテナンスが期限切れになるとどうなりますか**?**

セッションの開始後に Citrix Virtual Apps and Desktops がサポートされていないことを示す警告メッセージがユーザーに届きます。この時点では、顧客はいかなるサポートも受ける権利がありません。ライセンスを更新するには、Citrix の営業担当者またはパートナーにお問い合わせください。

Citrix Virtual Apps and Desktops の警告:

```
Your corporate Citrix environment is currently unsupported. Please
contact your IT department to resolve any support related issues.
```

ユーザーライセンスまたはデバイスライセンス

Citrix は、ユーザー**/**デバイスライセンスモデルでユーザーにどのようにライセンスを割り当てますか

ユーザー/デバイスライセンスモデルでは、ライセンスサーバーによってライセンスが一意のユーザー ID に割り当てられます。1 人のユーザーに対するデバイスと接続の数に関する制限はありません。デスクトップまたはデバイスに接続するユーザーには、仮想デスクトップまたはアプリケーションにアクセスするために 1 つのライセンスが割り当てられている必要があります。ライセンスサーバーまたはクラウドサービスによってライセンスが割り当てられます。これらのライセンスを手動で割り当てることはできません。ライセンスは共有デバイスではなくユーザーに割り当てられます。一度割り当てられたライセンスは、90 日間の非アクティブ状態が経過するまで別のユーザーに割り当てることができません。詳しくは、「ユーザー/デバイスライセンス」を参照してください。

Citrix では、ユーザー**/**デバイスライセンスモデルでライセンスが割り当てられたデバイスをどのように定義していますか

ライセンスが割り当てられたデバイスでは、一意のエンドポイントデバイス ID が必要です。ユーザー/デバイスモデルでは、デバイスとは Citrix Virtual Apps and Desktops のインスタンスにアクセスするために個人が使用を許可された機器を指します。共有デバイスの場合、1 つの Citrix Virtual Apps and Desktops ユーザー/デバイスライセ

ンスが、デバイスを共有する複数のユーザーに適用されます。たとえば、共有デバイスにはクラスルームワークステーションや病院の臨床ワークステーションが含まれます。

Citrix Virtual Desktops Standard Edition の同時使用ライセンスをユーザー**/**デバイスモデルに変換できますか

Citrix Virtual Desktops Standard Edition の同時使用ライセンスを Citrix Virtual Desktops Standard Edition のユーザー/デバイスライセンスに変換することはできません。同様に、Citrix Virtual Desktops Standard Edition のユーザー/デバイスモデルを Citrix Virtual Desktops Standard Edition の同時使用ライセンスに変換することもできません。

Citrix Virtual Desktops Standard Edition の同時使用ライセンスを所有しており、ユーザー/デバイスライセンスモデルを希望する場合は、Citrix Virtual Apps and Desktops Advanced Edition または Premium Edition にアップグレードします。

アップグレード元	Standard の同時接続	Standard のユーザー/デバイス	Advanced のユーザー/デバイス	Premium のユーザー/デバイス
Citrix Virtual Desktops Standard Edition の同時使用ライセンス	-	同時使用からユーザー/デバイスへの変換は不可	ライセンスモデルは変換できませんが、Citrix Virtual Apps and Desktops Advanced Edition または Premium Edition にアップグレードできます。	ライセンスモデルは変換できませんが、Citrix Virtual Apps and Desktops Advanced Edition または Premium Edition にアップグレードできます。
Citrix Virtual Desktops Standard Edition のユーザー/デバイスライセンス	ユーザー/デバイスから同時使用への変換は不可	-	-	-

同時使用ライセンスとユーザー**/**デバイスライセンスはどこが違いますか

同時使用ライセンスは、同時デバイス接続に基づいています。同時使用ライセンスは、デバイスでアクティブ接続が確立されている間にのみ使用されます。接続が終了すると、同時使用ライセンスはライセンスプールに戻ります。戻ったライセンスはすぐに使用できます。ライセンスの使用頻度が高くない場合は、このライセンスモデルをお勧めします。ユーザー/デバイスライセンスは一定期間リースされ、リースの期限が切れるまで他のユーザーは使用できません。

ユーザー/デバイスモデルで、同じ企業内のユーザーとデバイスの両方にライセンスを割り当てることはできますか

はい。1 つの企業内で 2 つのタイプを併用できます。ライセンスサーバーは、使用状況に基づいてライセンスをユーザーまたはデバイスに最適に割り当てます。これらのライセンスを手動で割り当てることはできません。

ライセンスを割り当てるユーザーやデバイスの数はどのようにして決定しますか

ユースケースの要件を評価し、適切なライセンス数を決定します。ユーザー/デバイスライセンスでは、仮想デスクトップと仮想アプリの数にも、それらにアクセスできるデバイスの数にも制限がなく、無制限でアクセスできます。同時使用ライセンスでは、仮想デスクトップと仮想アプリの数に制限がなく、無制限でアクセスできます。アクセスできるデバイスは 1 つだけですが、デバイスを使用できるユーザーの数に制限はありません。下の式を考慮してください:

```
(Number of total users) - (number of users that only access
   exclusively
 with shared devices) + (number shared devices) = total number
 of licenses to buy.

For example, there are 1000 total users at the hospital. If 700 of them
    access only
Citrix Virtual Desktops from 300 shared devices in the hospital, the
   number of
licenses to purchase is 1000 - 700 + 300 = 600 licenses.
```

ユーザー/デバイスモデルでは、ライセンスが割り当てられたユーザーによる環境への接続に最大いくつのデバイスを使用できますか

ライセンスが割り当てられた各ユーザーが使用できる接続デバイスまたはオフラインデバイスの数に、制限はありません。

ユーザー/デバイスモデルでは、ライセンスが割り当てられたデバイスに最大何人のユーザーがアクセスできますか

ライセンスが割り当てられた各デバイスを使用できる組織内のユーザー数に制限はありません。

ユーザー/デバイスモデルでは、ライセンスが割り当てられたユーザーが最大いくつの仮想デスクトップまたは **RBI Web** アプリケーションを同時に使用できますか

ライセンスが割り当てられた各ユーザーが接続できる仮想デスクトップや Web アプリケーションの数に、制限はありません。

Citrix Virtual Apps and Desktops のライセンスを購入して、既存の **Citrix Virtual Apps and Desktops** 環境でより多くのユーザー/デバイスにライセンスを割り当てることができますか

はい。Citrix Virtual Apps and Desktops のライセンスを購入することで、既存の Citrix Virtual Apps and Desktops 環境でライセンスを割り当てるユーザー/デバイスの数を増やすことができます。

付与されたユーザー/デバイスライセンスを解放するにはどうすればよいですか

付与されたユーザー/デバイスライセンスを解放するには、ライセンス契約書に従って`udadmin`ユーティリティを使用します。それにより、ライセンスサーバーによって該当する次のユーザー/デバイスにライセンスが割り当てられます。詳しくは、「ユーザーライセンスまたはデバイスライセンスの表示と解放」を参照してください。

購入したユーザー/デバイスライセンスの数を超えた場合はどうなりますか

ユーザー/デバイスライセンスでは、ライセンスが生成されるときに 10%の超過使用保護ライセンスも含まれます。超過使用保護ライセンスはインストール済みライセンス数に含まれます。使用の急増によって超過使用保護を含めたインストール数を超過した場合、これ以上のユーザーアクセスは拒否されます。追加のユーザーがアクセスできるようにするには、新しいライセンスを購入して展開してください。

すべてのライセンス（超過使用保護分も含む）が使用されると、追加猶予期間で無制限のアクセスが許可されます。追加猶予期間中に、ユーザーの作業を中断させることなく最大ライセンス数を超過した原因を調査し、さらにライセンスを購入するかを検討することができます。追加猶予期間は、15 日経過するまで、または他の製品版ライセンスを追加するまで継続します。どちらか一方が発生した時点で終了します。詳しくは、「追加猶予期間」を参照してください。

Director は、猶予期間の状態を表示します。詳しくは、「Director のダッシュボードのパネル」を参照してください。

ライセンスが割り当てられたユーザーは、最大でいくつの仮想アプリケーションを同時に使用できますか

ライセンスが割り当てられた各ユーザーが接続できる仮想アプリケーションの数に、制限はありません。

ライセンスが割り当てられたユーザーが組織を離れるとどうなりますか

ライセンスが割り当てられた既存ユーザーが組織を離れた場合、Citrix に通知せずにそのユーザーのライセンスを解放できます。ライセンスの解放には、`udadmin`ユーティリティを使用します。ライセンスを解放しない場合、非アクティブの状態が 90 日続くと、ライセンスサーバーによってライセンスが自動的に解放されます。この情報は、EULA で指定された条件に準拠します。

ライセンスが割り当てられたユーザーが長期間不在にするとどうなりますか

ライセンスが割り当てられた既存ユーザーが長期間不在にする場合、Citrix に通知せずにライセンスを解放して再割り当てできます。ライセンスの解放には、udadminユーティリティを使用します。

組織内でライセンスを割り当てたデバイスを交換するとどうなりますか

ライセンスが割り当てられた既存デバイスを交換する場合、Citrix に通知せずにライセンスを解放して再割り当てできます。ライセンスの解放には、udadminユーティリティを使用します。

ライセンスを割り当てたデバイスが長期間使用できなくなった場合はどうなりますか

ライセンスが割り当てられた既存デバイスが長期間使用できなくなった場合、Citrix に通知せずにライセンスを解放して再割り当てできます。ライセンスの解放には、udadminユーティリティを使用します。ライセンスを解放しない場合、非アクティブの状態が 90 日続くと、ライセンスサーバーによってライセンスが自動的に解放されます。この情報は、EULA で指定された条件に準拠します。

デバイスまたはユーザーにライセンスを割り当てた後、ユーザーライセンスとデバイスライセンスを切り替えることはできますか

はい。この変更は自動的に行われます。ライセンスサーバーは、使用パターンに基づいてライセンスをユーザーまたはデバイスに割り当てます。使用パターンが変化した場合、新しい使用状況に基づき、ライセンスサーバーによって割り当てが切り替えられることがあります。ライセンスサーバーは、常に顧客にとっての経済性を最優先にしてライセンスを割り当てます。また、ライセンスサーバーはライセンスを監視し、90 日の割り当て期間後に未使用ライセンスを特定します。90 日の割り当て期間後に未使用として特定されたライセンスは、他のユーザーまたはデバイスに再割り当てできます。

同時使用ライセンス

同時使用モデルでは、**Citrix Virtual Apps and Desktops** のライセンスが割り当てられたユーザーが最大いくつの仮想デスクトップを同時に使用できますか

エンドポイントは多数のユーザーに対応でき、無制限の接続が可能です。

1 つのライセンスサーバーに、旧バージョンの **Citrix Virtual Apps and Desktops** の同時使用ライセンスと、新しいユーザー/デバイスライセンスまたは同時接続ライセンスを展開できますか

はい。引き続き同じライセンスサーバーを使用して、ユーザー/デバイスライセンスまたは同時使用ライセンスの環境に対応できます。

1 つのライセンスサーバーに、同時使用ライセンスとユーザー**/**デバイスライセンスまたは同時接続ライセンスを展開できますか**?**

はい。引き続き同じライセンスサーバーを使用して、同時使用ライセンスとユーザー/デバイスライセンスまたは同時使用ライセンスの環境に対応できます。

Citrix Virtual Apps and Desktops Advanced Edition および **Premium Edition** には、**Citrix Virtual Apps** の同時使用ライセンスが含まれていますか

Citrix Virtual Apps and Desktops Advanced Edition および Premium Edition のユーザー/デバイスライセンスには、互換性のみを目的として Citrix Virtual Apps の同時使用ライセンスが含まれています。これらの同時使用ライセンスは、ユーザー/デバイスライセンスとの互換性がない旧製品バージョンにのみ使用できます。ユーザー/デバイスライセンスに含まれる同時使用互換ライセンスの使用は、6.5 より前の XenApp バージョンと 5.0 Service Pack 1 より前の XenDesktop バージョンのみで許可されます。

購入した同時使用ライセンス数を超えた場合はどうなりますか

すべてのライセンスが使用されると、追加猶予期間で無制限のアクセスが許可されます。追加猶予期間中に、ユーザーの作業を中断させることなく最大ライセンス数を超過した原因を調査し、さらにライセンスを購入するかを検討することができます。追加猶予期間は、15 日経過するまで、または他の製品版ライセンスを追加するまで継続します。どちらか一方が発生した時点で終了します。詳しくは、「追加猶予期間」を参照してください。

Director は、猶予期間の状態を表示します。詳しくは、「Director のダッシュボードのパネル」を参照してください。

超過使用保護ライセンス

超過使用保護ライセンスを取得するにはどうすればよいですか**?**

ユーザー/デバイス、ユーザー、またはデバイスのライセンスモデルをサポートする製品（Citrix Cloud を除く）には、アクセス拒否を防止するために制限された数の追加ライセンスを使用できるライセンスの超過使用保護機能が含まれています。超過使用保護機能は、ライセンス使用権には関係なく便宜上提供されています。同時使用ライセンスおよびサーバーライセンスには、超過使用保護は含まれません。使用する超過使用保護ライセンスは、最初の使用から 30 日以内に購入する必要がありますが、使用は 30 日に限定されません。Citrix は、本製品の新規リリースで超過使用保護機能を削除する権利を留保します。詳しくは、「ライセンスの超過使用保護」を参照してください。

ライセンスの超過使用はどのようにして特定できますか**?**

Citrix Licensing Manager で、超過使用のライセンス数を含む使用状況の情報を表示できます。Studio にも、超過使用情報が含まれています。

超過使用保護ライセンスが使用されるとどうなりますか?

ライセンスはインストールされたライセンスから割り当てられ、Citrix Virtual Apps and Desktops 環境へのアクセスが許可されます。この超過使用保護ライセンスでは、他のライセンスと同様のアクセス権と機能が提供されます。

超過使用保護ライセンスが使用された場合に、通知を受け取ることはできますか?

現時点では、超過使用保護ライセンスが使用されても特定の通知は送信されません。

超過使用保護ライセンスは何日間使用できますか?

超過使用保護ライセンスは、最初の使用から 30 日以内に購入してください。

その他の製品固有のライセンス情報

- Citrix ADC
- Citrix Cloud
- Citrix Endpoint Management
- Citrix Gateway
- XenServer
- Citrix ライセンスサーバー

マシンの負荷分散

August 17, 2024

> 注:
>
> Web Studio（Web ベース）と Citrix Studio（Windows ベース）の 2 つの管理コンソールを使用して、Citrix Virtual Apps and Desktops の展開を管理できます。この機能は Web Studio でのみ使用できます。
>
> この機能は、すべてのカタログ（シングルセッション OS カタログまたはマルチセッション OS カタログ）に適用されます。垂直負荷分散は、マルチセッション OS マシンにのみ適用されます。

負荷分散はサイトレベルとデリバリーグループレベルで構成できます。垂直と水平の 2 つのオプションがあります。デフォルトでは、水平負荷分散が有効になっています。

サイトレベルでの負荷分散設定

- 垂直負荷分散。最大負荷に達していない最も負荷の高いマシンに受信のユーザーセッションを割り当てます。これにより、既存のマシンが飽和状態になった後、新しいマシンに移ります。ユーザーが既存のマシンから切断すると、マシンの容量が解放されます。次に、受信の負荷がこれらのマシンに割り当てられます。垂直負荷分散により、ユーザーエクスペリエンスは低下しますが、コストを削減できます（セッションが電源オンのマシンの処理能力を最大化）。

  例：それぞれ 10 セッション用に構成された 2 つのマシンがあります。最初のマシンは、最初の 10 個の同時セッションを処理します。2 つ目のマシンは、11 番目のセッションを処理します。

  > ヒント：
  >
  > マシンがホストできるセッションの最大数を指定するには、最大セッション数ポリシー設定を使用します。

  または、PowerShell を使用して、サイト全体で垂直負荷分散を有効または無効にすることができます。`Set-BrokerSite`コマンドレットの`UseVerticalScalingForRdsLaunches`設定を使用します。`Get-BrokerSite`を使用して、`UseVerticalScalingForRdsLaunches`設定の値を表示します。詳しくは、コマンドレットのヘルプを参照してください。

- 水平負荷分散。受信ユーザーセッションを、最も負荷が少なく電源がオンになっている使用可能なマシンに割り当てます。水平負荷分散によりユーザーエクスペリエンスは向上しますが、コストが増加します（より多くのマシンで電源オンの状態が保持されるため）。デフォルトでは、水平負荷分散が有効になっています。

  例：それぞれ 10 セッション用に構成された 2 つのマシンがあります。最初のマシンは 5 つの同時セッションを処理します。2 つ目のマシンも 5 つのセッションを処理します。

この機能を構成するには、［管理］**>**［完全な構成］の左側ペインで ［設定］を選択します。［マルチセッションカタログの負荷分散］でオプションを選択します。

デリバリーグループレベルでの負荷分散設定

デリバリーグループレベルで負荷分散を構成すると、サイトレベルから継承した負荷分散設定を上書きできます。デリバリーグループレベルで垂直負荷分散を選択すると、各マシンの使用率を最大化できます。これはパブリッククラウドのコスト削減に役立ちます。この構成は、新しいデリバリーグループの作成時または既存のデリバリーグループの編集時に実行できます。

水平負荷分散。セッションは、電源がオンになっているマシン間で分散されます。たとえば、2 台のマシンがそれぞれ 10 セッション用に構成されている場合、1 台目のマシンが 5 つ、2 台目のマシンが 5 つの同時セッションを処理します。

垂直負荷分散。セッションは電源オンのマシンの容量を最大化し、マシンコストを節約します。たとえば、2 台のマシンがそれぞれ 10 セッション用に構成されている場合、最初のマシンが最初の 10 個の同時セッションを処理します。2 つ目のマシンは、11 番目のセッションを処理します。

ローカルホストキャッシュ

August 17, 2024

Citrix Virtual Apps and Desktops サイトデータベースを常に使用可能状態にするために、Microsoft 社の高可用性ベストプラクティスに従って、耐障害性の高い SQL Server 展開から開始することをお勧めします（SQL Server のサポートされる高可用性機能については、「データベース」を参照してください）。ただし、ネットワークの問題および中断によって、ユーザーがアプリケーションやデスクトップに接続できなくなる場合があります。

ローカルホストキャッシュ機能を使用すると、停止状態が発生しても、サイトの接続仲介操作を続行できます。オンプレミスの Citrix 環境で Delivery Controller とサイトデータベースとの間の接続が失敗すると、停止状態が発生します。ローカルホストキャッシュは、サイトデータベースに 90 秒間アクセスできない場合に使用されます。

XenApp および XenDesktop 7.16 より、接続リース機能（以前のリリースでの高可用性機能）は削除され、使用できなくなりました。

データコンテンツ

ローカルホストキャッシュには、メインデータベースの情報の一部として次の情報が格納されます:

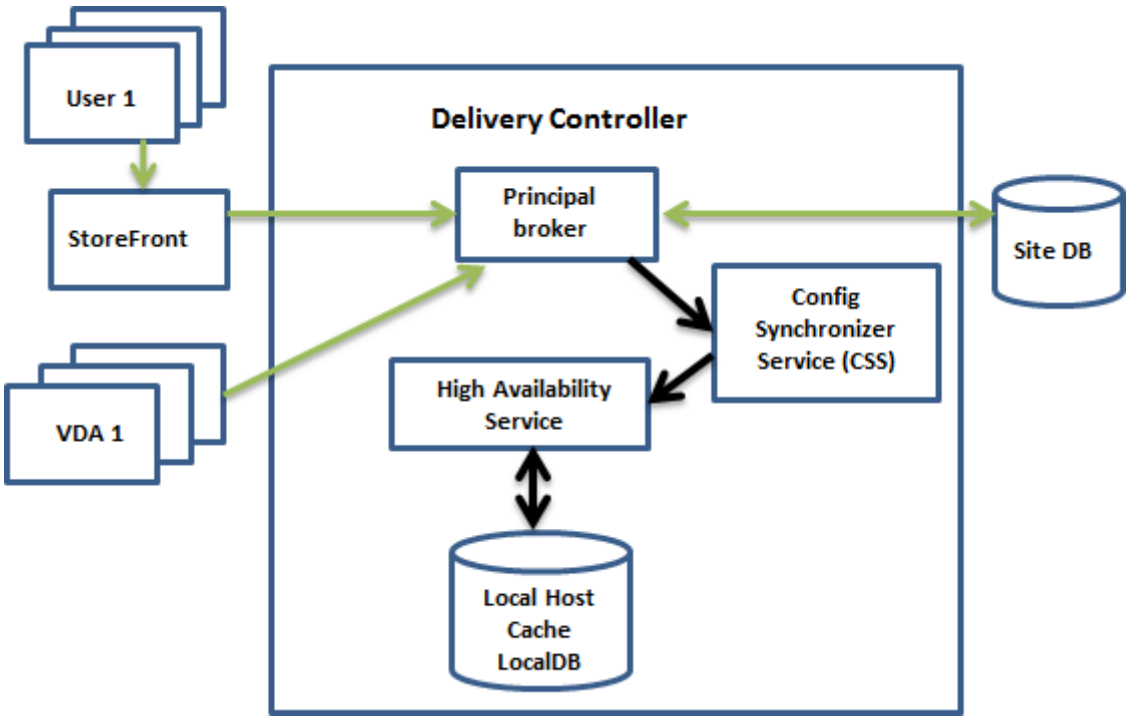
- サイトから公開されたリソースに対する権限が割り当てられているユーザーおよびグループの ID。
- サイトの公開リソースを現在使用しているか、最近使用したユーザーの ID。
- サイトで構成されている VDA マシン（リモート PC アクセスマシンを含む）の ID。
- 公開リソースへの接続で頻繁に使用されている Citrix Receiver クライアントマシンの ID（名前と IP アドレス）

また、メインデータベースが利用できなくなったときに確立され、現在アクティブな接続に関する情報も格納されています:

- Citrix Receiver で実行されたクライアントマシンのエンドポイント分析の結果
- サイトに関連するインフラストラクチャマシン（NetScaler Gateway や StoreFront サーバーなど）の ID
- ユーザーによる最近のアクティビティの日時とタイプ

機能

次の図は、通常の操作中のローカルホストキャッシュコンポーネントと通信経路を示しています。



通常の操作中

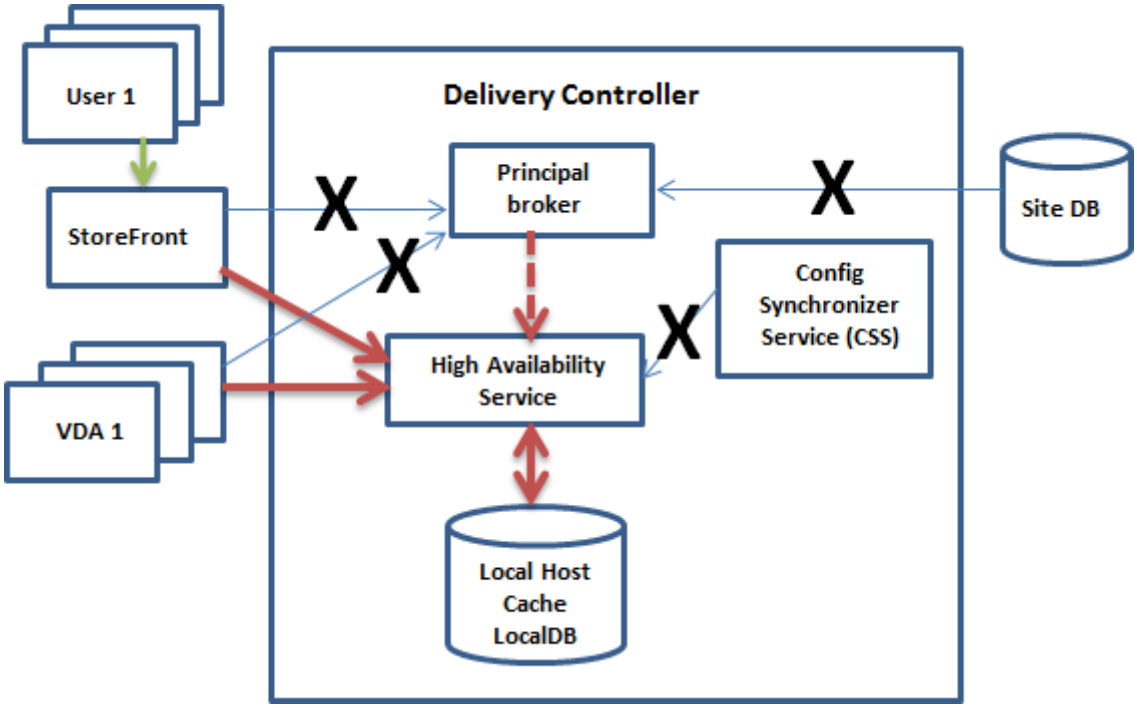
- Controller 上のプリンシパルブローカー（Citrix Broker Service）は、StoreFront からの接続要求を受け取ります。このブローカーはサイトデータベースと通信して、Controller に登録されている VDA にユーザーを接続します。
- Citrix Config Synchronizer Service（CSS）は、ブローカーを 5 分ごとにチェックして、構成に変更がないか確認します。こうした変更には、管理者によるもの（デリバリーグループのプロパティの変更など）とシステム操作（マシン割り当てなど）があります。
- 前回のチェック以降に構成が変更された場合、CSS は、Controller のセカンダリブローカーに情報を同期（コピー）します。（セカンダリブローカーは、High Availability Service とも呼ばれます）。

  前回のチェック以降に変更された項目だけでなく、すべての構成データがコピーされます。CSS は、Controller 上の Microsoft SQL Server Express LocalDB データベースに構成データをインポートします。このデータベースはローカルホストキャッシュデータベースとして参照されます。CSS は、ローカルホストキャッシュデータベースの情報がサイトデータベースの情報と一致することを確認します。ローカルホストキャッシュデータベースは、同期が発生するたびに再作成されます。

  Controller をインストールする場合、（ローカルホストキャッシュデータベースで使用するために）Microsoft SQL Server Express LocalDB が自動的にインストールされます（Controller をコマンドラインからインストールする場合は、インストールされるのを回避できます）。ローカルホストキャッシュデータベースは、Controller 間で共有できません。ローカルホストキャッシュデータベースのバックアップを作成する必要はありません。構成の変更が検出されるたびに再作成されます。

- 最後のチェック以降に変更が発生しなかった場合、データはコピーされません。

次の図に、プリンシパルブローカーがサイトデータベースとの接続を失った（停止状態が開始された）場合の通信径路の変化を示します。



停止状態中

停止が開始された場合：

- セカンダリブローカーは、接続要求のリッスンと処理を開始します。
- 停止状態の開始時には、セカンダリブローカーに最新の VDA 登録データはありませんが、VDA との通信が始まると登録処理がトリガーされます。その処理中、セカンダリブローカーは、その VDA に関する現在のセッション情報も取得します。
- セカンダリブローカーが接続を処理する間も、プリンシパルブローカーは引き続き接続を監視します。接続が回復すると、プリンシパルブローカーはセカンダリブローカーに接続情報のリスニングを停止するように指示して、仲介操作を再開します。VDA がプリンシパルブローカーと次に通信するときに、登録処理がトリガーされます。セカンダリブローカーは、前回の停止状態以降に残っている VDA 登録をすべて削除します。CSS は、展開内で構成が変更されたことを検出すると、情報の同期を再開します。

同期中に停止状態が開始されるという可能性の低い事象では、その時点のインポートは破棄され、最新の既知の構成が使用されます。

イベントログには、同期および停止に関する情報が含まれます。

停止モードでの操作に時間制限は適用されませんが、

通常モードと停止モードとの間の移行は、既存のセッションには影響しません。新しいセッションの起動にのみ影響します。

意図的に停止を引き起こすこともできます。これを行う理由と方法について詳しくは、「停止状態の強制」を参照してください。

複数の **Controller** があるサイト

CSS は、他のタスク同様、ゾーン内のすべての Controller に関する情報を日常作業としてセカンダリブローカーに提供します（展開に複数のゾーンがない場合、この操作はサイト内のすべての Controller に影響します）。その情報により、各セカンダリブローカーは、ゾーン内のその他の Controller で実行される同じ立場にあるすべてのセカンダリブローカーを認識します。

セカンダリブローカーは独立したチャネルで相互に通信します。これらのセカンダリブローカーは、実行しているマシンの完全修飾ドメイン名のアルファベット順の一覧を使用して、停止状態が発生したときにどのセカンダリブローカーがゾーン内の仲介操作を担当するかを決定（選出）します。停止状態中、すべての VDA が、選出されたセカンダリブローカーに登録されます。選出されていないゾーン内のセカンダリブローカーは、受信接続と VDA 登録要求を能動的に拒否します。

停止状態中に、選出されたセカンダリブローカーに障害が発生した場合、別のセカンダリブローカーが選出されて処理を引き継ぎ、VDA は新しく選出されたセカンダリブローカーに登録されます。

停止状態中に Controller を再起動した場合：

- この Controller が選出されたブローカーでない場合は、再起動しても影響はありません。
- この Controller が選出されたブローカーである場合、別の Controller が選出され、VDA はそちらに登録されます。再起動した Controller の電源がオンになると、この Controller が自動的にブローカーを引き継ぐため、VDA は再度登録されます。このシナリオでは、登録中にパフォーマンスに影響が生じることがあります。

ブローカーに選出した Controller を、通常の操作中に電源を切ってから停止状態中に電源を入れると、ローカルホストキャッシュをこの Controller 上で使用することはできません。

イベントログには、選出に関する情報が含まれます。

停止状態中にできなくなること、およびその他の相違点

停止モードでの操作に時間制限は適用されませんが、ただし、接続をできるだけ早く復元することをお勧めします。

停止状態中：

- Studio は使用できません。
- PowerShell SDK へのアクセスが制限されます。
  - 次のことを最初に行う必要があります：

    * レジストリキーEnableCssTestModeを値 1 で追加します: `New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer\LHC -Name EnableCssTestMode -PropertyType DWORD -Value 1`
    * ポート 89 を使用します: `Get-BrokerMachine -AdminAddress localhost:89 | Select MachineName, ControllerDNSName, DesktopGroupName, RegistrationState`
  - これらのコマンドを実行すると、次のものを使用できるようになります:
    * すべてのGet-Broker*コマンドレット。

- ハイパーバイザー資格情報をホストサービスから取得できません。すべてのマシンの電力状態が不明で、電源操作を発行できません。ただし、電源が入っているホスト上の VM を接続要求のために使用することができます。
- 割り当てられたマシンは、通常の操作中に割り当てが発生した場合のみ使用できます。停止状態中は新しい割り当てはできません。
- リモート PC アクセスマシンの自動登録と構成はできません。ただし、通常の操作中に登録、構成されたマシンは使用できます。
- サーバーでホストされるアプリケーションとデスクトップのユーザーは、リソースが異なるゾーンにある場合、構成されている最大セッション数よりも多くのセッションを使用できる場合があります。
- ユーザーは、現在アクティブな、または選出されているセカンダリブローカーを含むゾーン内の登録済み VDA からのみ、アプリケーションとデスクトップを起動できます。停止中は、ゾーン間での起動（あるゾーンのセカンダリブローカーから別のゾーンの VDA へ）はサポートされません。
- デリバリーグループ内の VDA に対してスケジュールされた再起動が開始される前にサイトデータベースの停止が発生した場合、停止が終了すると再起動が開始されます。これは意図しない結果につながる可能性があります。詳しくは、「データベースの停止によるスケジュールされた再起動の遅延」を参照してください。
- ［ゾーン優先度］を構成できません。構成されていても、環境設定はセッション起動では考慮されません。
- タグを使用してゾーンを指定するタグ制限機能は、セッション起動ではサポートされていません。このタグ制限が構成されていて、StoreFront ストアの ［詳細なヘルスチェック］ オプションが有効になっている場合、セッションが断続的に起動に失敗することがあります。

アプリケーションとデスクトップのサポート

LHC は次の種類の VDA と配信モデルをサポートしています:

VDA の種類	配信モデル	LHC イベント中の VDA の可用性
マルチセッション OS	アプリケーションとデスクトップ	常に利用できます。

VDA の種類	配信モデル	LHC イベント中の VDA の可用性
シングルセッション OS 静的（割り当て済み）	デスクトップ	常に利用できます。
電源管理されたシングルセッション OS ランダム（プール）	デスクトップ	デフォルトでは利用できません。プールされたデリバリーグループ内の電源管理された VDA に対する、すべてのセッション起動の試みは、デフォルトで失敗します。

> 注:
>
> プールされたデリバリーグループ内の電源管理されたデスクトップ VDA へのアクセスを有効にしても、通常の操作中に構成された`ShutdownDesktopsAfterUse`プロパティの機能結果には影響しません。LHC 中にこれらのデスクトップへのアクセスが有効になっている場合、LHC イベントの完了後、VDA は自動的に再起動しません。プールされたデリバリーグループ内の電源管理されたデスクトップ VDA は、再起動するまで以前のセッションのデータを保持できます。VDA の再起動は、ユーザーが LHC 以外の操作中に VDA からログオフしたとき、または管理者が VDA を再起動したときに発生することがあります。

ーザーセッションからのデータと変更が後続のセッションに残る可能性があります。

完全な構成を使用し、電源管理されたシングルセッション **OS** のプールされた **VDA** に対して **LHC** を有効にします

完全な構成を使用すると、デリバリーグループごとに、これらのマシンを LHC イベント中に新しい接続で利用できるようにすることができます:

- デリバリーグループの作成中にこの機能を有効にするには、「デリバリーグループの作成」を参照してください。
- 既存のデリバリーグループでこの機能を有効にするには、「デリバリーグループの管理」を参照してください。

> 注:
>
> この設定は、電源管理された VDA を配信するプールされたデスクトップデリバリーグループに対する、完全な構成でのみ使用できます。

PowerShell を使用し、電源管理されたシングルセッション **OS** のプールされた **VDA** に対して **LHC** を有効にします

特定のデリバリーグループ内の VDA に対して LHC を有効にするには、次の手順を実行します:

1. 次のコマンドを実行して、サイトレベルでこの機能を有効にします:

   ```
   Set-BrokerSite -ReuseMachinesWithoutShutdownInOutageAllowed $true
   ```

2. デリバリーグループ名を指定してこのコマンドを実行し、デリバリーグループの LHC を有効にします:


```
Set-BrokerDesktopGroup -Name "name"-ReuseMachinesWithoutShutdownInOutage
 $true
```

電源管理された VDA を含む新しく作成されたプールされたデリバリーグループで、デフォルトの LHC の可用性を変更するには、次のコマンドを実行します:

```
Set-BrokerSite -DefaultReuseMachinesWithoutShutdownInOutage $true
```

RAM サイズの考慮事項

LocalDB サービスは、約 1.2GB の RAM（データベースキャッシュ用に最大 1GB、SQL Server Express LocalDB の実行用にさらに 200MB）を使用できます。セカンダリブローカーは、停止状態が長時間続き、多数のログオンが発生した場合（たとえば 12 時間でユーザー数 1 万人）、最大 1GB の RAM を使用できます。これらのメモリ要件は Controller の通常の RAM 要件とは別なので、RAM の総容量を増やす必要がある場合があります。

サイトデータベースに SQL Server Express インストールを使用する場合、サーバーに 2 つの sqlserver.exe プロセスを持つ点に注意してください。

CPU コアとソケットの構成に関する考慮事項

Controller の CPU 構成、特に SQL Server Express LocalDB が利用できるコア数は、メモリ割り当て以上に、ローカルホストキャッシュのパフォーマンスに直接影響を及ぼします。この CPU オーバーヘッドが発生するのは、データベースとの接続が失われ、セカンダリブローカーがアクティブである停止状態の間だけです。

LocalDB は複数のコア（最大 4 つ）を使用できますが、単一のソケットだけに制限されます。ソケットを追加しても（たとえば、4 つのソケットにそれぞれ 1 つのコア）、パフォーマンスは向上しません。それよりも複数のコアを持つ複数のソケットの使用を Citrix ではお勧めします。Citrix のテストでは、2x3（2 つのソケット、3 つのコア）の構成が、4x1 および 6x1 の構成より良好なパフォーマンスを示しました。

ストレージの考慮事項

ユーザーが停止状態の間にリソースにアクセスすると、LocalDB は増大します。たとえば、1 秒に 10 回ログオンするログオン/ログオフテスト実行では、データベースは 2〜3 分に 1MB 増大しました。通常の操作が再開すると、ローカルデータベースが再作成され、容量は元に戻ります。ただし、停止状態の間のデータベース増大を考慮に入れ、LocalDB がインストールされるドライブ上に、十分な空き領域がある必要があります。ローカルホストキャッシュを使用すると、停止状態中に追加の I/O が生じます（数十万の読み取りで、1 秒あたり約 3MB の書き込み）。

パフォーマンスについての考慮事項

停止状態中は 1 つのセカンダリブローカーがすべての接続を処理するため、通常の操作時に複数の Controller に負荷を分散するサイト（あるいは、ゾーン）では、停止状態中に、選出されたセカンダリブローカーが普通よりはるか

に多くの要求を処理する必要があることがあります。このため、CPU への要求が高くなります。停止状態中に選出されたセカンダリブローカーが変更される可能性があるため、サイト（ゾーン）内のすべてのセカンダリブローカーが、ローカルホストキャッシュデータベースと影響を受けるすべての VDA によって課される追加の負荷を処理できる必要があります。

VDI の制限事項:

- 単一ゾーンに VDI を展開する場合、停止状態時には最大 10,000 の VDA を効果的に処理できます。
- 複数ゾーンに VDI を展開する場合、停止状態時には各ゾーンで最大 10,000 の VDA、サイト全体では最大 40,000 の VDA を効果的に処理できます。たとえば次のそれぞれのサイトが、停止状態時に効果的に処理されます。
  - 4 つのゾーンそれぞれに 10,000 の VDA が含まれるサイト。
  - 1 つのゾーンには 10,000 の VDA が含まれ、残り 6 つのゾーンにはそれぞれ 5,000 の VDA が含まれる、合計 7 つのゾーンからなるサイト。

停止状態中に、サイト内の負荷管理が影響を受ける可能性があります。負荷評価基準（特にセッション数規則）を超過する可能性があります。

すべての VDA がセカンダリブローカーに登録する間、そのサービスは現在のセッションの一部を把握できなくなる場合があります。このため、その間の接続要求により、既存のセッションへの再接続が可能であっても、新しいセッションが起動される可能性があります。こうした時間（「新しい」セカンダリブローカーが再登録時にすべての VDA からセッション情報を取得する時間）が発生するのは避けられません。停止状態の開始時に接続していたセッションは移行期間に影響を受けることはありませんが、新しいセッションおよびセッション再接続は影響を受ける可能性があります。

この期間は、VDA の登録が必要なときには必ず発生します:

- 停止状態の開始：プリンシパルブローカーからセカンダリブローカーに移行するとき。
- 停止状態中にセカンダリブローカーに障害が発生した場合：障害が発生したセカンダリブローカーから新しく選出されたセカンダリブローカーに移行するとき
- 停止からの回復：通常の操作が再開し、プリンシパルブローカーが制御を再開したとき。

Citrix Broker Protocol の`HeartbeatPeriodMs`レジストリ値（デフォルト = 600000ms（10 分））を小さくすることによって期間を短縮できます。このハートビート値は、VDA が ping に使用する間隔の 2 倍であるため、デフォルト値では 5 分ごとに ping が発生します。

たとえば、ハートビートを 5 分（300000ms）に変更するには、次のコマンドを実行します。このようにすると、ping は 2.5 分ごとに発生します:

```
New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer -Name
HeartbeatPeriodMs -PropertyType DWORD -Value 300000
```

ハートビート値を変更するときは注意が必要です。頻度を増やすと、通常モードと停止モードのどちらの間でも、Controller の負荷が増加します。

VDA の登録をどんなに早くしても、間隔を完全になくすことはできません。

セカンダリブローカー間の同期にかかる時間は、オブジェクト（VDA、アプリケーション、グループなど）の数により増加します。たとえば、5,000 個の VDA を同期する場合には、10 分以上かかる可能性があります。

XenApp 6.x リリースとの相違点

このローカルホストキャッシュ実装は、XenApp 6.x 以前の XenApp リリースのローカルホストキャッシュ機能の名前を共有しますが、大幅に改善されています。この実装は、破損に対してより頑強で耐性もあります。定期的に`dsmaint`コマンドを実行する必要がないなど、メンテナンス要件が最小になります。このローカルホストキャッシュは技術的にはまったく異なる実装です。

ローカルホストキャッシュの管理

ローカルホストキャッシュを正常に動作させるには、各 Controller 上の PowerShell 実行ポリシーを、RemoteSigned、Unrestricted、または Bypass に設定する必要があります。

SQL Server Express LocalDB

ローカルホストキャッシュが使用する Microsoft SQL Server Express LocalDB ソフトウェアは、Controller をインストールするか、Controller を 7.9 以前のバージョンからアップグレードするときに、自動的にインストールされます。セカンダリブローカーだけがこのデータベースと通信します。PowerShell コマンドレットを使用して、このデータベースに関する変更を行うことはできません。LocalDB は、Controller 間で共有できません。

SQL Server Express LocalDB データベースソフトウェアは、ローカルホストキャッシュが有効かどうかに関係なくインストールされます。

このインストールを防止するには、Controller のインストールまたはアップグレード時に、`XenDesktopServerSetup.exe`コマンドで`/exclude "Local Host Cache Storage (LocalDB)"`オプションを使用します。ただし、ローカルホストキャッシュ機能はデータベースがないと機能しないことと、セカンダリブローカーでは異なるデータベースを使用できないことに注意してください。

この LocalDB データベースのインストールは、サイトデータベースとして使うために SQL Server Express をインストールするかどうかには影響しません。

以前のバージョンの SQL Server Express LocalDB を新しいバージョンに置き換える方法について詳しくは、「SQL Server Express LocalDB の置き換え」を参照してください。

製品のインストールとアップグレード後のデフォルト設定

Citrix Virtual Apps and Desktops（バージョン 7.16 以降）の新規インストール時に、ローカルホストキャッシュが有効になります。

アップグレード（バージョン 7.16 以降へ）後は、展開全体に 10,000 個未満の VDA が存在する場合に、ローカルホストキャッシュが有効になります。

ローカルホストキャッシュの有効化と無効化

- ローカルホストキャッシュを有効化するには、次のように入力します:

  ```
  Set-BrokerSite -LocalHostCacheEnabled $true
  ```

  ローカルホストキャッシュが有効かどうかを判断するには、`Get-BrokerSite`を入力します。`LocalHostCacheEnabled`プロパティが`True`であることを確認します。

- ローカルホストキャッシュを無効にするには、次のように入力します。

  ```
  Set-BrokerSite -LocalHostCacheEnabled $false
  ```

注意：XenApp および XenDesktop 7.16 より、接続リース機能（バージョン 7.6 以降に提供されていた、ローカルホストキャッシュに先行する機能）は削除され、使用できなくなりました。

ローカルホストキャッシュが動作していることを確認する

ローカルホストキャッシュが適切に設定され動作していることを確認するには:

- 同期のインポートが正常に完了していることを確認します。イベントログをチェックします。
- SQL Server Express LocalDB データベースが Delivery Controller ごとに作成されたことを確認します。これにより、必要に応じてセカンダリブローカーが処理を引き継げるようになります。
  - Delivery Controller サーバーで、`C:\Windows\ServiceProfiles\NetworkService`に移動します。
  - `HaDatabaseName.mdf`および`HaDatabaseName_log.ldf`が作成されたことを確認します。
- Delivery Controller に停止状態を強制します。ローカルホストキャッシュが動作することを確認したら、すべての Controller を通常モードに戻します。これには約 15 分かかります。

イベントログ

イベントログに、同期および停止状態が発生した時刻が示されます。イベントビューアーのログでは、停止状態モードは *HA* モードと見なされます。

Config Synchronizer Service:

通常の操作中、ローカルホストキャッシュブローカーを使用して CSS が構成データをローカルホストキャッシュデータベースにインポートすると次のイベントが発生することがあります。

- 503：Citrix Config Sync Service が更新された構成を受信しました。このイベントは、同期プロセスが開始されたことを表します。
- 504：Citrix Config Sync Service が更新された構成をインポートしました。構成のインポートが正常に完了しました。
- 505：Citrix Config Sync Service がインポートに失敗しました。構成のインポートが正常に完了しませんでした。過去に正常にインポートされた構成がある場合、停止状態の発生時にはその構成が使用されます。ただし、この構成は現在の構成よりも古いものです。使用可能な過去の構成がない場合、停止状態中、サービスはセッション仲介に参加できません。この場合は、「トラブルシューティング」セクションを確認の上、Citrix サポートにお問い合わせください。
- 507：システムが停止状態であり、ローカルホストキャッシュブローカーが使用中であるため、Citrix Config Sync Service によりインポートが中止されました。サービスは新しい構成を受け取りましたが、停止状態が発生したためインポートは中止されました。これは正常な動作です。
- 510：プライマリ構成サービスから構成サービス構成データを受信していません。
- 517：プライマリブローカーとの通信に問題がありました。
- 518：セカンダリブローカー（High Availability Service）が実行されていないため、Config Sync スクリプトが中止されました。

High Availability Service:

このサービスは、ローカルホストキャッシュブローカーとも呼ばれます。

- 3502：停止状態が発生しローカルホストキャッシュブローカーが仲介操作を実行しています。
- 3503：停止状態が解消され、通常の操作が再開しました。
- 3504：どのローカルホストキャッシュブローカーが選出されたかと、選出に関わった他のローカルホストキャッシュブローカーを示します。
- 3507：ローカルホストキャッシュの更新された状態情報を 2 分ごとに提供します。この情報は、選択されたブローカーでローカルホストキャッシュモードがアクティブであることを示すものです。停止時間、VDA 登録、セッション情報など、停止の概要も含まれます。
- 3508：選択されたブローカー上でローカルホストキャッシュがアクティブではなくなり、通常の操作が復元されたことを通知します。停止時間、ローカルホストキャッシュ（LHC）イベント中に登録されたマシンの数、LHC イベント中に成功した起動の数など、停止の概要も含まれます。
- 3509：選択されていないブローカー上でローカルホストキャッシュがアクティブであることを通知します。2 分ごとの停止時間と選択されているブローカーも通知します。
- 3510：選択されていないブローカー上でローカルホストキャッシュがアクティブでなくなったことを通知します。停止時間と選択されているブローカーも通知します。

停止状態の強制

停止状態は意図的に発生させることもできます。

- ネットワークが稼動と停止を繰り返している場合。ネットワークの問題が解決するまで強制的に停止状態にす

ることにより、通常モードと停止状態モードの移行が繰り返され、VDA 登録ストームが頻繁に発生するのを防げます。

- 障害回復プランをテストするには:
- ローカルホストキャッシュが正常に動作することを確認する場合。
- サイトデータベースサーバーの交換または修理中。

停止状態を強制するには、Delivery Controller を含む各サーバーのレジストリを編集します。HKLM\Software\Citrix\DesktopServer\LHCでOutageModeForcedを作成し、REG_DWORDを1に設定します。この設定により、ローカルホストキャッシュブローカーはデータベースの状態に関係なく停止状態モードに入るよう指示されます。値を0に設定すると、ローカルホストキャッシュブローカーの停止状態モードは終了します。

イベントを確認するには、C:\ProgramData\Citrix\WorkspaceCloud\Logs\Plugins\HighAvailabilityServiceのCurrent_HighAvailabilityServiceログファイルを監視します。

トラブルシューティング

ローカルホストキャッシュデータベースへの同期インポートが失敗し 505 イベントがポストされた場合には、次のトラブルシューティングツールが役立ちます。

CDF トレーシング: ConfigSyncServerモジュールおよびBrokerLHCモジュール向けのオプションが用意されています。それらのオプションと他のブローカーモジュールの組み合わせで問題を識別できるはずです。

レポート: 同期インポートが失敗した場合は、レポートを生成できます。このレポートの最後に、エラーの原因となったオブジェクトが記載されています。このレポート機能は同期速度に影響するため、Citrix では使用しないときは無効にしておくことをお勧めします。

CSS トレースレポートを有効化および作成するには、次のコマンドを入力します:

```
New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer\LHC -Name EnableCssTraceMode -PropertyType DWORD -Value 1
```

HTML レポートはC:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\CitrixBrokerConfigSyncReport.htmlに格納されます。

レポートが生成されたら、次のコマンドを入力してレポート機能を無効にします:

```
Set-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer\LHC -Name EnableCssTraceMode -Value 0
```

ブローカー構成のエクスポート: デバッグのために正確な構成を提供します。

```
Export-BrokerConfiguration | Out-File <file-pathname>
```

例: `Export-BrokerConfiguration | Out-File C:\\BrokerConfig.xml`。

ローカルホストキャッシュ用の **PowerShell** コマンド

PowerShell コマンドを使用して、Delivery Controller 上のローカルホストキャッシュ (LHC) を管理できます。

PowerShell モジュールは、Delivery Controller 上の次の場所にあります。

```
C:\Program Files\Citrix\Broker\Service\ControlScripts
```

> 重要:
>
> このモジュールは Delivery Controller 上でのみ実行してください。

PowerShell モジュールのインポート　PowerShell モジュールをインポートするには、Delivery Controller で次のコマンドを実行します。

```
cd C:\Program Files\Citrix\Broker\Service\ControlScripts Import-Module .\HighAvailabilityServiceControl.psm1
```

LHC を管理するための **PowerShell** コマンド　以下のコマンドは、Delivery Controller で LHC モードをアクティブ化して管理するのに役立ちます。

コマンドレット	機能
`Enable-LhcForcedOutageMode`	ブローカーを LHC モードにします。`Enable-LhcForcedOutageMode`が正しく機能するには、LHC データベースファイルが ConfigSync Service によって正常に作成されている必要があります。このコマンドレットは、LHC が実行されていた Delivery Controller でのみ、LHC を強制的にアクティブ化します。LHC をアクティブ化するには、ゾーン内のすべての Delivery Controller でこのコマンドを実行する必要があります。
`Disable-LhcForcedOutageMode`	ブローカーの LHC モードを解除します。このコマンドレットは、LHC が実行されていた Delivery Controller の LHC モードのみを無効にします。`Disable-LhcForcedOutageMode`は、ゾーン内のすべての Delivery Controller で実行する必要があります。

コマンドレット	機能
`Set-LhcConfigSyncIntervalOverride`	Citrix Config Synchronizer Service（CSS）がサイト内に構成変更がないかをチェックする間隔を設定します。時間間隔の範囲は 60 秒（1 分）～3600 秒（1 時間）です。この設定は、LHC が実行されていた Delivery Controller にのみ適用されます。Delivery Controller 間の一貫性を確保するには、すべての Delivery Controller でこのコマンドレットを実行してください。たとえば、次のようになります: `Set-LhcConfigSyncIntervalOverride -Seconds 1200`
`Clear-LhcConfigSyncIntervalOverride`	Citrix Config Synchronizer Service（CSS）がサイト内に構成変更がないかをチェックする間隔をデフォルト値の 300 秒（5 分）に設定します。この設定は、LHC が実行されていた Delivery Controller にのみ適用されます。Delivery Controller 間の一貫性を確保するには、すべての Delivery Controller でこのコマンドレットを実行してください。
`Enable-LhcHighAvailabilitySDK`	LHC が実行されていた Delivery Controller 内で、すべての`Get-Broker*`コマンドレットへのアクセスを有効にします。
`Disable-LhcHighAvailabilitySDK`	LHC が実行されていた Delivery Controller 内で、ブローカーコマンドレットへのアクセスを無効にします。

> 注:
>
> - Delivery Controller で`Get-Broker*`コマンドレットを実行する場合は、ポート 89 を使用します。例:
>
>   ```
>   - Get-BrokerMachine -AdminAddress localhost:89
>   ```
>
> - LHC モードではない Delivery Controller の LHC ブローカーは、構成情報のみを保持しています。
> - LHC モード中、選択された Delivery Controller の LHC ブローカーは次の情報を保持しています。
>   - リソースの状態
>   - セッションの詳細
>   - VDA 登録
>   - 構成情報

検索を使用してマシンとセッションを監視および管理

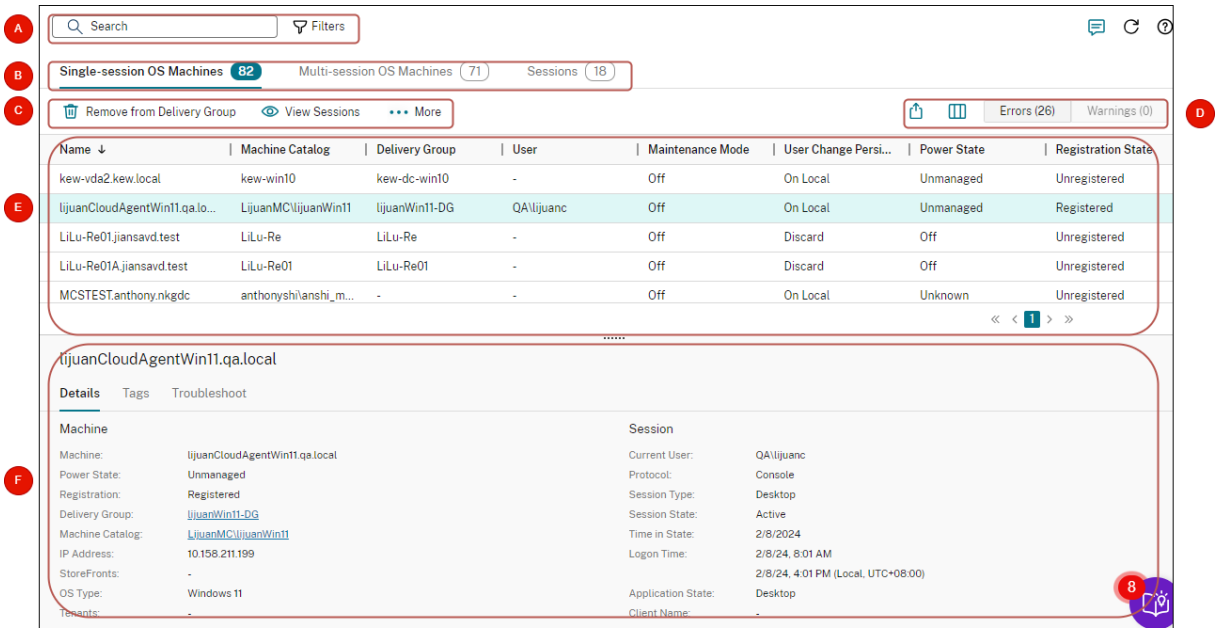
August 17, 2024

> 注:
>
> Web Studio（Web ベース）と Citrix Studio（Windows ベース）の 2 つの管理コンソールを使用して、Citrix Virtual Apps and Desktops の展開を管理できます。この記事では Web Studio のみを扱います。Citrix Studio について詳しくは、Citrix Virtual Apps and Desktops 7 2212 以前の同様の記事を参照してください。

この記事では、［完全な構成］**>**［検索］を使用してマシンとセッションを監視および管理する方法について説明します。

このノードについて

検索ノードは、マシンとユーザーセッションをまとめて監視および管理するための場所を提供します。



ラベル	エリア	説明
A	検索バー	クイック検索と、複雑な検索条件を定義できるフィルターベースの検索を提供します。詳しくは、「インスタンスの検索」を参照してください。

ラベル	エリア	説明
B	種類のタブ	マシンを種類別に一覧表示するか、すべてのセッションを表示するタブを表示します。インスタンス数はタブ名に表示されます。
C	インスタンスレベルの操作	選択したインスタンス（マシンまたはセッション）で実行できる操作が表示されます。詳しくは、マシンの操作および セッションの操作を参照してください。
D	一覧レベルの操作	現在の一覧に対して実行できる操作を表示します エクスポートアイコン：メイン ビューに表示されているインスタンスの一覧を CSV ファイルにエクスポートします。
E	メインビュー	表示する列のアイコン：一覧のメインビューをカスタマイズします。 エラーラベル：このラベルを有効にすると、エラーのある未登録のマシンのみがメインビューに表示されます。 警告ラベル：このラベルを有効にすると、警告のある未登録のマシンのみがメインビューに表示されます。
F	詳細ペイン	インスタンスとそのプロパティを表示します。表示する列アイコンを選択して、メインビューをカスタマイズできます。使用可能な列について詳しくは、マシンの列およびセッションの列を参照してください。 ［詳細］ペインの［トラブルシューティング］タブに移動します。 次の詳細を表示します： 選択したインスタンス（マシンまたはセッション）の詳細 選択したマシンに適用されるタグ 選択したマシンのエラーまたは警告の詳細（問題、考えられる原因、推奨される解決策など） 問題の詳細を表示するには、［詳細］ペインの［トラブルシューティング］タブに移動します。

インスタンスの検索

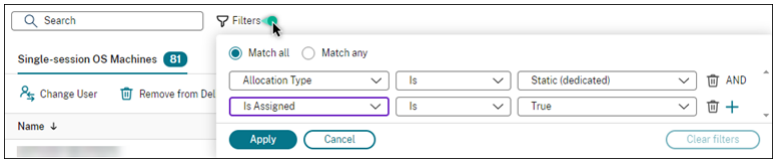
検索機能を使用して、特定のマシンカタログを見つけます：

- フィルターを使用して検索する
- クイック検索のために現在のフィルターセットを保存する
- 検索バーにフィルターフィールドを固定する
- クイック検索ボックスを使用して検索する
- 高度な検索を行うためのヒント

フィルターを使用して検索する

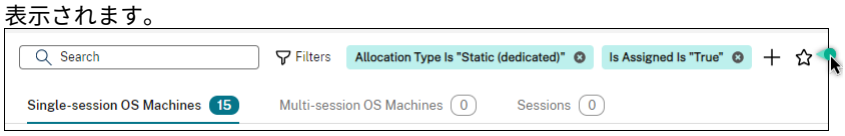
たとえば、静的でユーザーに割り当てられているすべてのシングルセッション OS マシンを見つけるには、次の手順を実行します:

1. [シングルセッション **OS** マシン] タブで、フィルターアイコンをクリックします。フィルターパネルが表示されます。
2. 必要なフィルター基準を追加します。



3. すべてのフィルター基準に一致する結果が検索で返されるようにする場合は、[すべて一致] (AND 演算子) を選択します。いずれかのフィルター基準に一致する結果が検索で返されるようにする場合は、[一部が一致] (OR 演算子) を選択します。
4. [適用] をクリックします。

   フィルター後の一覧には、静的かつユーザーに割り当てられているすべてのシングルセッション OS マシンが表示されます。

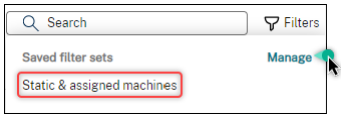


クイック検索のために現在のフィルターセットを保存する

たとえば、静的でユーザーに割り当てられているシングルセッション OS マシンのフィルターセットを以降の検索のために保存するには、次の手順を実行します:

1. フィルターベースの検索を実行した後、上の図に示された検索バーの星のアイコンをクリックします。
2. 表示されたページで、このフィルターセットの名前を入力します (例: 静的で割り当てられたマシン)。
3. [保存] をクリックします。

   保存されたフィルターセットは、検索ボックスをクリックすると検索履歴一覧に表示されます。

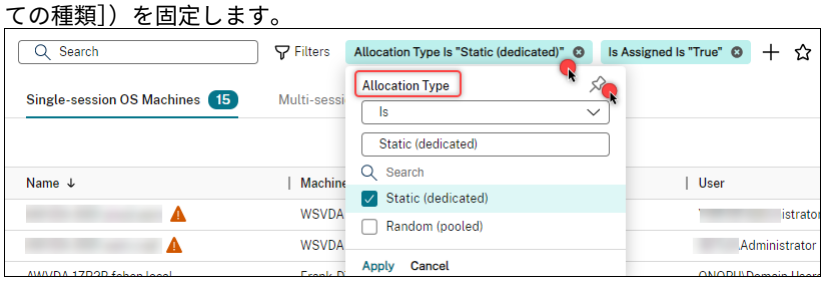


> 注:
>
> フィルターセットはユーザーアカウントごとに保存されます。保存済みのフィルターセットを管理するには、[管理] を選択します。

検索バーにフィルターフィールドを固定する

頻繁に使用するフィルターフィールドを検索バーに固定して、簡単にアクセスできるようにします。たとえば、フィルターベースの検索を実行した後、検索バーに［割り当ての種類］を固定するとします。以下の手順を実行します：

1. 検索バーで「フィルターの設定」** をクリックします。
2. 表示されたパネルで、固定アイコンをクリックして、検索バーのフィルターフィールド（この例では ［割り当ての種類］）を固定します。



クイック検索ボックスを使用して検索する

クイック検索ボックスは、名前関連のプロパティまたは保存されたフィルターセットに基づいてインスタンスを検索する便利な方法を提供します。詳細な手順は次のとおりです：

1. 検索ボックスをクリックします。最近の検索と保存されたフィルターセットがドロップダウンリストに表示されます。以前の検索またはフィルターセットをクリックすると、簡単に検索できます。
2. 新しい検索を開始するには、次のオプションから名前の全部または一部を入力します：

   - マシン名または DNS 名
   - マシンカタログ名
   - デリバリーグループ名
   - セッションユーザー名
   - セッションのクライアント名
   - ハイパーバイザーによって使用される、セッションをホストする仮想マシンのフレンドリ名
   - ホストサーバー名

高度な検索を行うためのヒント

検索機能を使用するときは、次のヒントを考慮してください：

- ［検索］ノードで、任意の列を選択してアイテムを並べ替えます。
- 検索と並べ替えができる画面に追加の特性を表示するには、［表示する列］を選択するか、任意の列をクリックして ［表示する列］を選択します。［表示する列］ウィンドウで、表示するアイテムの横にあるチェックボックスをオンにし、［保存］を選択して終了します。

> 注:
>
> パフォーマンスを低下させる列には、［パフォーマンスの低下］ラベルが付きます。

- マシンに接続しているユーザーデバイスを検索するには、［クライアント（**IP**）］および ［次のもの］を指定してデバイスの IP アドレスを入力します。
- アクティブなセッションを検索するには、［セッション状態］、［次のもの］、［接続済み］を指定します。
- デリバリーグループ内のすべてのマシンを一覧表示するには、左側ペインで ［デリバリーグループ］を選択します。グループを選択し、操作バーまたはコンテキストメニューから ［マシンの表示］を選択します。

並べ替え操作を実行するときは、次の考慮事項に留意してください:

- アイテムの数が 5,000 を超えない限り、任意の列をクリックしてその中のアイテムを並べ替えることができます。数が 5,000 を超える場合は、（現在のタブに応じて）名前または現在のユーザーでのみ並べ替えることができます。並べ替えを有効にするには、フィルターを使用してアイテムの数を 5,000 以下に減らします。
- アイテム数が 500 を超え 5,000 を超えない場合:
  - 並べ替えのパフォーマンスを向上させるために、すべてのデータをローカルにキャッシュします。［シングル セッション **OS** マシン］タブと ［マルチセッション **OS** マシン］タブでは、列（［名前］列を除く任意の列）を最初にクリックして並べ替えたときにデータがキャッシュされます。［セッション］タブでは、列（［現在のユーザー］列を除く任意の列）を最初にクリックして並べ替えたときにデータがキャッシュされます。その結果、並べ替えの完了に時間がかかります。パフォーマンスを向上させるには、名前または現在のユーザーで並べ替えるか、フィルターを使用してアイテムの数を減らします。
  - 表の下にある次のメッセージは、データがキャッシュされていることを示しています。最終更新: <the time when you refreshed the table>。この場合、並べ替え操作は以前に読み込まれたアイテムに基づいて行われます。これらのアイテムは最新ではない可能性があります。最新にするには、更新アイコンをクリックします。

表示する列のカスタマイズ

パーソナライズされたメイン ビューを作成して、日常の操作に重要なプロパティとステータスを表示します。詳細な手順は次のとおりです:

1. 検索ノードで、必要に応じて ［マルチセッション **OS** マシン］、［シングルセッション **OS** マシン］、または［セッション］タブを選択します。
2. 操作バーの 表示する列アイコンをクリックし、列を選択します。

   使用可能な列とその説明について詳しくは、「マシン列」および「セッション列」を参照してください。

列の選択中、［パフォーマンスの低下］ラベルの付いた列が表示されることがあります。これらの列を選択すると、コンソールのパフォーマンスが低下する可能性があります。次の考慮事項に留意してください:

- カスタマイズの完了後、テーブルが更新され、選択した列が表示されます。このような列が存在すると、テーブルを更新するときに遅延が発生する可能性があります。
- ブラウザーを更新するか、コンソールからサインアウトしてサインインすると、これらの列を保持するかどうかを尋ねるメッセージが表示されます。それらを保持することを選択した場合、コンソールのパフォーマンスを最適化するために、テーブルの更新間隔が 1 分以下にならないように制限されます。より頻繁に更新するには、パフォーマンスを低下させる列を削除します。

マシンとセッションの管理

検索ノードの操作を使用して、マシンやセッションの問題のトラブルシューティングを行ったり、ユーザー要求を処理したりできます。

ヒント

さまざまなレベルでマシンを管理できます:

- 個別のマシンレベルの場合。検索ノードを使用してターゲットマシンを見つけ、操作を実行します。
- マシンカタログレベルの場合。カタログのマスターイメージの変更、カタログからのマシンの削除、カタログへのマシンの追加など。詳しくは、「マシンカタログの管理」を参照してください。
- デリバリーグループレベルの場合。グループ内のマシンのメンテナンスモードのオンまたはオフなど。詳しくは、「デリバリーグループの管理」を参照してください。

個別のセッションレベルに加えて、デリバリーグループのセッションの事前起動や残留の構成など、デリバリーグループレベルでセッションを管理することもできます。詳しくは、「デリバリーグループの管理」を参照してください。

マシンまたはセッション上で操作を実行する

個別のインスタンスレベルでマシンまたはセッションを管理するには、次の手順を実行します:

1. 検索ノードで、[マルチセッション **OS** マシン]、[シングルセッション **OS** マシン]、または [セッション] タブを選択します。
2. 必要に応じて 1 つまたは複数のインスタンスを選択します。
3. 操作バーまたは右クリックメニューから、インスタンスまたはユーザー要求で発生した問題に基づいて操作を選択します。

   使用可能な操作とその説明について詳しくは、「マシンの操作」および「セッションの操作」を参照してください。

> 注:
>
> 2 つ以上のインスタンスを選択した場合、それらすべてに適用される操作のみが使用可能になります。

マシンまたはセッションのデータを **CSV** ファイルにエクスポート

タブに表示されているインスタンス（マシンまたはセッション）の一覧（最大 30,000 項目）を CSV ファイルにエクスポートします。詳細な手順は次のとおりです:

1. 検索ノードで、必要に応じて［マルチセッション **OS** マシン］、［シングルセッション **OS** マシン］、または［セッション］タブを選択します。
2. 右上隅にあるエクスポートアイコンをクリックします。
3. ダイアログボックスが表示されたら、［続行］をクリックします。

   エクスポートが完了するまでに数分かかる場合があります。このファイルは、ブラウザーのデフォルトのダウンロードフォルダーにあります。

> 注:
>
> 検索ノードの各タブでは、エクスポートの進行中に別のエクスポートを実行することはできません。

マシンの操作と列

August 17, 2024

この記事では、参照用にマシンの操作と列を記載します。

操作

マシン上で実行できる操作とその説明を表示します。

アクション	説明	適用先
デリバリー グループから削除	デリバリーグループからのマシンを削除します。	シングルセッションとマルチセッション
デリバリーグループに追加	マシンをデリバリーグループに追加します。	シングルセッションとマルチセッション
セッションの表示	マシン上で実行中のセッションを表示します	シングルセッションとマルチセッション

アクション	説明	適用先
タグの管理	マシンのタグを追加および管理します。タグの一般的な使用例について詳しくは、「タグ」を参照してください。	シングルセッションとマルチセッション
メンテナンスモードをオンにする	パッチを適用する前、またはトラブルシューティングの際には、マシンをメンテナンスモードにします。このモードでは、そのマシンに新たに接続できなくなります。ユーザーはそのマシンの既存のセッションに接続できますが、そのマシンの新しいセッションを開始することはできなくなります。	シングルセッションとマルチセッション
メンテナンスモードをオフにする	マシンのメンテナンスモードをオフにします。	シングルセッションとマルチセッション
VDA のアップグレード	マシンの VDA をアップグレードします。	特定の要件を満たすシングルセッションまたはマルチセッション OS マシン：詳細情報。
ログオフ	マシンを強制的にログオフします	シングルセッションとマルチセッション
削除	VM をハイパーバイザーまたはクラウドサービス上にそのまま残して、マシンカタログから VM を削除します。	シングルセッションとマルチセッション
ユーザーの変更	マシンを特定のユーザーに割り当てます。	シングルセッションの静的マシン。
開始	マシンを起動します。	シングルセッションとマルチセッション
シャットダウン	マシンをシャットダウンします。	シングルセッションとマルチセッション
再起動	マシンを再起動します	シングルセッションとマルチセッション
一時停止	マシンを休止状態または一時停止状態にします。マシンを一時停止すると、Delivery Controller ストアはマシンのメモリ内容をファイルに保存し、マシンをシャットダウンします。	シングルセッション OS マシン

アクション	説明	適用先
再開	一時停止したマシンを再開します。一時停止したマシンを再開すると、Delivery Controller はマシンを起動し、以前の状態に復元します。	シングルセッション OS マシン
強制再起動	マシンを強制的に再起動します。	シングルセッション OS マシン
強制シャットダウン	マシンを強制的にシャットダウンします。	シングルセッション OS マシン

列

すべてのマシン列とその説明を種類別に表示します:

- マシン
- マシンの詳細
- アプリケーション
- ホスト
- 接続
- 登録
- セッションの詳細
- セッション

マシン

マシン カテゴリの列。

列	説明	適用先
名前	マシンの DNS ホスト名です。	シングルセッションとマルチセッション
マシンカタログ	マシンが属するカタログの名前。	シングルセッションとマルチセッション
デリバリーグループ	マシンが属するデリバリーグループの名前。	シングルセッションとマルチセッション

列	説明	適用先
ユーザー表示名	マシンに関連付けられているユーザーのフルネーム（通常は `Firstname Lastname`の形式）。関連付けられたユーザーは、共有マシンの現在のユーザーと、専用マシンの割り当てられたユーザーです。	シングルセッションとマルチセッション
ユーザー	マシンに関連付けられているユーザーのユーザー名（「ドメイン\ユーザー」の形式）。関連付けられたユーザーは、共有マシンの現在のユーザーと、専用マシンの割り当てられたユーザーです。	シングルセッションとマルチセッション
ユーザープリンシパル名	マシンに関連付けられているユーザーのユーザープリンシパル名（「ユーザー @ ドメイン」の形式）。関連付けられたユーザーは、共有マシンの現在のユーザーと、専用マシンの割り当てられたユーザーです。	シングルセッションとマルチセッション
デスクトップの表示名	セッションの起動に最初に使用されたマシンの公開名。これは、Citrix Workspace アプリまたは StoreFront に表示される名前です。注：デスクトップの表示を変更するには、［マシンの更新］の権限が必要です。表示名の変更にはマシンプロパティの更新が含まれるためです。	シングルセッションのみ
デスクトップ状態	マシンの未処理のデスクトップ状態の一覧。設定可能な値：不明、CPU、ICA 遅延、および UPM ログオン時間。	シングルセッションとマルチセッション
割り当ての種類	マシンの割り当ての種類：無期限。ユーザーに無期限で割り当てられる場合。ランダム。ランダムに割り当てられる場合。	シングルセッションとマルチセッション
メンテナンスモード	マシンがメンテナンス モードであるかどうかを示します。	シングルセッションとマルチセッション

列	説明	適用先
Windows 接続設定	Windows によって報告されたログオンモード。 設定可能な値：ログオン有効、ドレイン中、再起動するまでドレイン中、およびログオン無効。	マルチセッションのみ
割り当て済み	専用デスクトップがユーザーまたはクライアントに割り当てられているかどうかを示します（名前/アドレス）。ユーザーは明示的に割り当てることも、初回使用時割り当てで割り当てることができます。	シングルセッションとマルチセッション
物理的	マシンが物理的かどうかを示します。`True`はマシンが物理的であることを示し、Delivery Controller によって電源管理されていないことを意味します。`False`はそうでないことを示します。	シングルセッションとマルチセッション
プロビジョニングの種類	マシンがプロビジョニングされた方法。設定可能な値： 手動：PVS または MCS を使用してプロビジョニングされていません。 PVS：PVS を使用したプロビジョニング（物理マシン、ブレード、仮想マシン） MCS：MCS を使用したプロビジョニング（VM のみ）	シングルセッションとマルチセッション
スケジュールされた再起動	マシンのスケジュールされた再起動操作の状態。設定可能な値： なし：再起動はスケジュールされていません。 保留中：再起動を待機中ですが、使用できます。 ドレイン中：再起動を待機しているため、新しいセッションには使用できませんが配置されて既存の接続の再接続は引き続き許可されます。 進行中：関連付けられた再起動が進行中です。	シングルセッションとマルチセッション
ゾーン	マシンが配置されているゾーンの名前。	シングルセッションとマルチセッション
状態	マシンの全体的な状態。セッション状態、登録状態、電源状態、再起動が進行中など特定の状態は再起動を待機していると想定できる状態：オフ、未登録、使用可能、切断、使用中、および準備中。	シングルセッションとマルチセッション

列	説明	適用先
タグ	マシンに関連付けられたタグの一覧。	シングルセッションとマルチセッション
VDA のアップグレード	VDA パッケージのアップグレード操作のマシンの状態。 設定可能な値：MissingUpgradeType、UpgradeScheduled、UpgradeAvailable、UpToDate、および Unknown。	シングルセッションとマルチセッション
一時停止が可能	マシンが電源操作（一時停止および再開）をサポートしているかどうかを示します。	シングルセッションとマルチセッション
負荷インデックス	現在の負荷インデックス。詳しくは、詳細情報を参照してください。	マルチセッションのみ
ドレイン状態	マシンがドレイン中であり、マシン上のすべてのセッションが終了した後にシャットダウンするかどうかを示します。True は、電源管理されたマルチセッションマシンの場合にのみ表示されます。 注：マシンがメンテナンスモードの場合、マシンはシャットダウンしません。メンテナンスモードをオフにした後にのみシャットダウンします。	マルチセッションのみ

マシンの詳細

マシンの詳細カテゴリの列。

列	説明	適用先
エージェントのバージョン	マシン上にインストールされた Virtual Desktop Agent（VDA）のバージョンです。	シングルセッションとマルチセッション
IP アドレス	マシンの IP アドレス。	シングルセッションとマルチセッション

列	説明	適用先
割り当て済み	専用デスクトップがユーザーまたはクライアントに割り当てられているかどうかを示します（名前/アドレス）。ユーザーは明示的に割り当てることも、初回使用時割り当てで割り当てることができます。	シングルセッションとマルチセッション
OS の種類	マシンで実行されているオペレーティングシステムの種類です。	シングルセッションのみ

アプリケーション

アプリケーションカテゴリの列。

列	説明	適用先
使用中のアプリケーション	マシン上で使用中のアプリケーションの一覧（ブラウザー名として表示）。	シングルセッションとマルチセッション
公開アプリケーション	マシンで公開されたアプリケーションの一覧（ブラウザー名として表示）。	シングルセッションとマルチセッション

接続

接続カテゴリの列。

列	説明	適用先
クライアント（IP）	マシンに接続されているクライアントの IP アドレス。	シングルセッションのみ
クライアント	マシンに接続されているクライアントのホスト名。	シングルセッションのみ
プラグインのバージョン	接続されたクライアント上の Citrix Workspace アプリのバージョン。	シングルセッションのみ
接続経由	受信接続のホスト名（通常はゲートウェイ、ルーター、またはクライアント）。	シングルセッションのみ

列	説明	適用先
接続経由（IP アドレス）	受信接続の IP アドレス（通常はゲートウェイ、ルーター、またはクライアント）。	シングルセッションのみ
接続の種類	セッションに使用されるプロトコル。設定可能な値：HDX、RDP、およびコンソール。注：XenDesktop 5 VDA 上のコンソールセッションの場合、フィールドは空白のままです。	シングルセッションのみ
前回の接続時間（UTC）	最後に検出された接続試行が失敗または成功した時間。	シングルセッションとマルチセッション
直前の接続ユーザー	最後にマシンへの接続を試みたユーザーの SAM 名（「ドメイン\ユーザー」の形式）。SAM 名が使用できない場合は、SID が使用されます。	シングルセッションとマルチセッション
SecureICA アクティブ	SecureICA が現在のセッションでアクティブであるかどうかを示します。マルチセッションマシンの場合は常に null。	シングルセッションとマルチセッション

ホスト

ホストカテゴリの列。

列	説明	適用先
VM	これは、ハイパーバイザーによって使用されセッションを実行する、ホストされているマシンのフレンドリ名です。マシンの DNS 名や AD 名と必ずしも一致するとは限りません。	シングルセッションとマルチセッション
ホストサーバー名	管理対象のマシンをホストするハイパーバイザーの DNS 名です。	シングルセッションとマルチセッション
接続	セッションをホストするマシンに割り当てられたホスト接続の名前。	シングルセッションとマルチセッション
更新保留中	ホストされているマシンの VM イメージが古いため、マシンの次回の再起動時に新しいイメージに更新される予定であるかどうかを示します。	シングルセッションとマルチセッション

列	説明	適用先
ユーザー変更の保持	ユーザーの変更がどのように処理されるか、変更が永続的であるかどうかを示します： ローカル上：永続的。ユーザーによる変更は、ローカル保存先で永続的です。 破棄：非永続的。ユーザーによる変更は破棄されます。	シングルセッションとマルチセッション
保留中の電源操作	マシンに対して保留中の電源操作があるかどうかを示します。	シングルセッションとマルチセッション
電源状態	マシンの電源状態。設定可能な値：非管理、不明、使用不可、オフ、オン、一時停止、投入中、シャットダウン中、一時停止中、および再開中。	シングルセッションとマルチセッション
使用後にシャットダウン	電源管理されたシングルセッションのマシンにのみ適用されます。マシンが不良状態であり、マシン上のすべてのセッションが終了した後にシャットダウンするかどうかを示します。 注：マシンがメンテナンスモードの場合、シャットダウンされません。メンテナンスモードを解除した後にのみシャットダウンします。	シングルセッションのみ

登録

登録カテゴリの列。

列	説明	適用先
前回の登録エラー	マシンがブローカーで最後に登録解除された理由。	シングルセッションとマルチセッション

列	説明	適用先
	設定可能な値は次のとおりです：エージェントのシャットダウン、エージェント一時停止、エージェント要求、非互換バージョン、エージェント アドレス解決の失敗、エージェントとの通信不可、エージェントの Active Directory OU が正しくない、登録要求が空、登録機能がない、エージェントバージョンがない、登録機能に整合性がない、機能のライセンスがない、サポートされていない資格情報セキュリティ バージョン、無効な登録要求、シングル/マルチ セッションの不一致、カタログに対して機能レベルが低すぎる、デスクトップ グループに対して機能レベルが低すぎる、電源オフ、デスクトップが再起動した、デスクトップが削除された、デスクトップが削除された、送信設定エラー、セッション監査エラー、セッション準備エラー、接続の損失、設定作成エラー、不明なエラー、および ブローカー登録制限に到達した。	
前回の登録エラー時刻（UTC）	マシンが最後に登録解除された時間。	シングルセッションとマルチセッション
登録状態	マシンの登録状態。設定可能な値：未登録、初期化中、登録済み、および エージェントエラー。	シングルセッションとマルチセッション
障害の状態	マシンの現在の障害の状態に関する概要。設定可能な値： なし：障害はありません。マシンは正常です。 起動に失敗：マシンの最後の電源投入操作が失敗しました。 起動時にスタック：マシンの電源を入れた後、起動に失敗しました。 未登録。マシンが予想期間内に登録できなかったか、登録が拒否されました。 最大容量：マシンは最大容量時に報告します。	シングルセッションとマルチセッション

セッションの詳細

セッションの詳細カテゴリの列。

列	説明	適用先
起動経由	現在のブローカーセッションの起動に使用される StoreFront サーバーのホスト名。マルチセッションマシンの場合は常に null。	シングルセッションとマルチセッション
起動経由（IP アドレス）	現在のブローカーセッションの起動に使用される StoreFront サーバーの IP アドレス。マルチセッションマシンの場合は常に null。	シングルセッションとマルチセッション
セッション変更時間（UTC）	現在のセッションの状態が最後に変更された時間。	シングルセッションのみ
SmartAccess フィルター	現在のセッションの Smart Access タグ。マルチセッションマシンの場合は常に null。	シングルセッションとマルチセッション

セッション

セッションのカテゴリの列。

列	説明	適用先
セッション状態	現在のセッションの状態。設定可能な値：そのほか、セッション準備中、接続済み、アクティブ、切断済み、再接続中、非仲介セッション、および不明。	シングルセッションのみ
現在のユーザー	現在のセッションのユーザーの名前(「ドメイン\ユーザー」の形式)。	シングルセッションのみ
開始日時（UTC）	現在のセッションの開始時間。	シングルセッションのみ
セッション数	マシン上のセッションの数。	マルチセッションのみ

セッションの操作と列

August 17, 2024

この記事では、参照用にマシンの操作と列を記載します。

操作

セッションで実行できる操作とその説明を表示します。

アクション	説明	次のセッションに適用
ログオフ	ユーザーをセッションからログオフします。	シングルセッション OS マシンまたはマルチセッション OS マシン
メッセージの送信	セッションのユーザーにメッセージを送信します。	シングルセッション OS マシンまたはマルチセッション OS マシン
マシンの表示	セッションのホストマシンを表示します。	シングルセッション OS マシンまたはマルチセッション OS マシン
切断	セッションを切断します。セッションが切断状態になると、セッションおよびアプリケーションは終了しませんが、Delivery Controller とユーザーデバイス間の通信が切断されます。	シングルセッション OS マシンまたはマルチセッション OS マシン
マシンをシャットダウンします	セッションに関連付けられたマシンをシャットダウンします。	シングルセッション OS マシン
マシンを再起動します	セッションに関連付けられたマシンを再起動します。	シングルセッション OS マシン

列

セッション列とその説明を表示します。

列	説明
現在のユーザー	ユーザーの名前。ユーザーのユーザープリンシパル名 (UPN)。
名前	セッションをホストしているマシンの DNS ホスト名。

列	説明
デリバリーグループ	セッションのホストマシンを含むデリバリーグループの名前。
マシンカタログ	セッションのホストマシンを含むマシンカタログの名前。
エージェントのバージョン	セッションをホストしているマシン上にインストールされた Virtual Desktop Agent（VDA）のバージョン。
使用中のアプリケーション	セッションで使用されているアプリケーションの一覧。管理名で識別されます。
自律的仲介	これが仲介なしに直接接続によって確立された HDX セッションであるかどうか。
仲介時間（UTC）	セッションが仲介された時間。
仲介ユーザー名	仲介ユーザーの名前。
クライアント（IP）	セッションに接続されているクライアントの IP アドレス。
クライアント	セッションに接続されているクライアントのホスト名。
プラグインのバージョン	セッションに接続されたクライアントで実行されている Citrix Workspace アプリのバージョン。
接続経由	受信接続のホスト名（通常はゲートウェイ、ルーター、またはクライアント）。
接続経由（IP アドレス）	受信接続の IP アドレス（通常はゲートウェイ、ルーター、またはクライアント）。
割り当ての種類	セッションが共有か専用か。
非表示	セッションをユーザーに対して非表示にして、再接続されないようにするかどうか。
VM	ハイパーバイザーによって使用される、セッションをホストする仮想マシンのフレンドリ名です。マシンの DNS 名や AD 名と必ずしも一致するとは限りません。
ホストサーバー名	セッションの管理対象のマシンをホストするハイパーバイザーの DNS 名。
接続	セッションをホストするマシンに割り当てられたホスト接続の名前。
更新保留中	ホストされているマシンの VM イメージが古く、マシンの次回の再起動時に新しいイメージに更新される予定であるかどうか。
メンテナンスモード	セッションをホストしているマシンがメンテナンスモードであるかどうか。
IP アドレス	セッションをホストしているマシンの IP アドレス。

列	説明
物理的	セッションをホストしているマシンが物理かどうか。`True`はマシンが物理であることを示し、Delivery Controller によって電源管理されていないことを意味します。`False`はそれ以外を示します。
起動経由	セッションの起動に使用される StoreFront サーバーのホスト名。セッションがワークスペース経由で起動された場合は空白です。
起動経由（IP アドレス）	セッションの起動に使用される StoreFront サーバーの IP アドレス。セッションがワークスペース経由で起動された場合は空白です。
OS の種類	セッションをホストしているオペレーティングシステムの ID 文字列。
ユーザー変更の保持	ユーザーの変更がどのように処理されるか、変更が永続的であるかどうかを示します： ローカル上：永続的。ユーザーによる変更はローカルに保存されます。 破棄：非永続的。ユーザーによる変更は破棄されます。
接続の種類	HDX、RDP、コンソールなど、セッションに使用されるプロトコル。 注： XenDesktop 5 VDA 上のコンソールセッションの場合、フィールドは空白です。
プロビジョニングの種類	セッションをホストしているマシンがプロビジョニングされた方法： 手動：PVS または MCS を使用してプロビジョニングされていません。 PVS：PVS によるプロビジョニング（物理マシン、ブレード、仮想マシン）。 MCS：MCS によるプロビジョニング（VM のみ）。
SecureICA アクティブ	SecureICA がセッションでアクティブであるかどうか。
セッション状態	セッションの状態。設定可能な値：接続済み、アクティブ、または切断済み。L7 より前の機能レベルのマシン上のセッションでは、セッション準備中、再接続中、非仲介セッション、そのほか、不明など、他の状態が発生する可能性があります。
セッション変更時間	セッションが最新の状態に変更された時間。
アプリケーションの状態	セッション内のアプリケーションの状態。設定可能な値：ログオン前、事前起動、アクティブ、デスクトップ、残留、および NoApps。
セッションサポート	セッションをホストしているマシンが複数のセッションをサポートするか、単一のセッションをサポートするか。

列	説明
ゾーン	セッションをホストしているマシンが配置されているゾーンの名前。
SmartAccess フィルター	セッションの Smart Access タグ。
開始日時（UTC）	セッションが開始された日時。
状態	マシンの状態の概要。設定可能な値：未登録、切断済み、または使用中。
この状態での経過時間（UTC）	セッションが現在の状態になってからの時間。
Delivery Controller	セッションのホストマシンが登録しているコントローラーの DNS ホスト名。
ユーザー表示名	ユーザーのフルネーム。
デスクトップの表示名	セッションの起動に最初に使用されたマシンの公開名。これは、Citrix Workspace アプリまたは StoreFront に表示される名前です。アプリケーションセッションの場合、アプリケーションがその後終了した場合でも、セッション内で最初に起動されたアプリケーションの名前になります。後でリソースの名前が変更または削除されても、名前は変更されません。

セキュリティキーの管理

August 17, 2024

> 重要:
>
> - この機能は、StoreFront 1912 LTSR CU2 以降とともに使用する必要があります。
> - Secure XML 機能は、Citrix ADC および Citrix Gateway リリース 12.1 以降でのみサポートされます。
>
> 注:
>
> Web Studio（Web ベース）と Citrix Studio（Windows ベース）の 2 つの管理コンソールを使用して、Citrix Virtual Apps and Desktops の展開を管理できます。この記事では Web Studio のみを扱います。Citrix Studio について詳しくは、Citrix Virtual Apps and Desktops 7 2212 以前の同様の記事を参照してください。

この機能を使用すると、承認された StoreFront マシンおよび Citrix Gateway マシンのみが Delivery Controller と通信できるようになります。この機能を有効にすると、キーが含まれていないすべての要求がブロックされます。

この機能を使用して、内部ネットワークの攻撃から保護するセキュリティ層を追加します。

この機能を使用するための一般的なワークフローは次のとおりです:

1. Web Studio を有効にして機能設定を表示します。
2. サイトの設定を構成します。
3. StoreFront の設定を構成します
4. Citrix ADC の設定を構成します。

Web Studio を有効にして機能設定を表示する

デフォルトでは、セキュリティキーの設定は Web Studio から非表示になっています。Web Studio でそれらを表示できるようにするには、以下の手順で PowerShell SDK を使用します:

1. Citrix Virtual Apps and Desktops PowerShell SDK を実行します。
2. コマンドウィンドウで、次のコマンドを実行します:
    - `Add-PSSnapIn Citrix*`。このコマンドは、Citrix スナップインを追加します。
    - `Set-ConfigSiteMetadata -Name "Citrix_DesktopStudio_SecurityKeyManageme "-Value "True"`

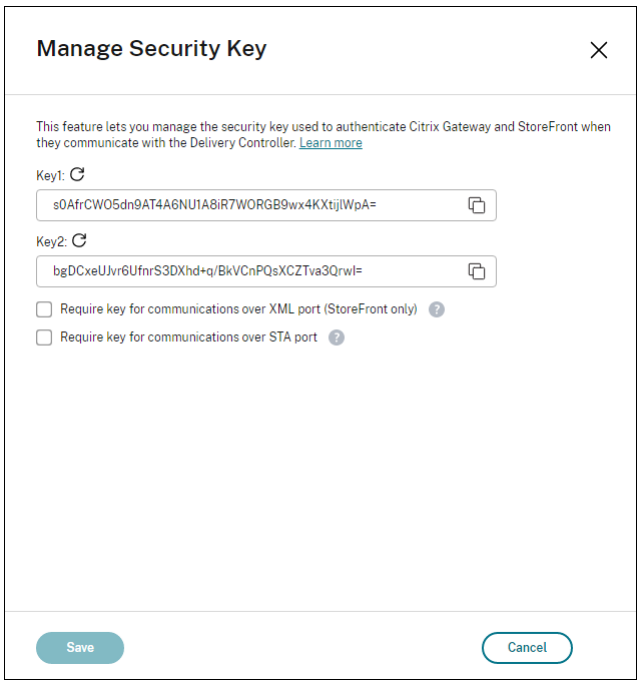
PowerShell SDK について詳しくは、「SDK および API」を参照してください。

サイトの設定を構成する

Web Studio または PowerShell を使用して、サイトのセキュリティキー設定を構成できます。

Web Studio を使用する

1. Web Studio にサインインし、左側のペインで ［設定］を選択します。
2. ［セキュリティキーの管理］タイルを見つけて、［編集］をクリックします。［セキュリティキーの管理］ページが開きます。



3. 更新アイコンをクリックしてキーを生成します。

> 重要:
>
> - 2 つのキーを使用できます。XML ポートと STA ポートを介した通信に、同じキーまたは異なるキーを使用できます。一度に 1 つのキーのみを使用することをお勧めします。未使用のキーは、キーの交換にのみ使用されます。
> - 既に使用中のキーを更新するために更新アイコンをクリックしないでください。クリックした場合、サービスが中断されます。

4. 通信にキーが必要な場合を選択します:

   - **XML** ポート経由の通信にキーが必須とする (**StoreFront** のみ)。選択されている場合、XML ポート経由での通信を認証するためにキーを必要とするかを示します。StoreFront は、このポートを介して Citrix Cloud と通信します。XML ポートの変更について詳しくは、Knowledge Center のCTX127945を参照してください。
   - **STA** ポート経由の通信にキーが必須とする。選択されている場合、STA ポート経由での通信を認証するためにキーを必要とするかを示します。Citrix Gateway および StoreFront は、このポートを介して Citrix Cloud と通信します。STA ポートの変更について詳しくは、Knowledge Center のCTX101988を参照してください。

5. [保存] をクリックして、変更を適用してウィンドウを閉じます。

PowerShell の使用

以下は、Web Studio の操作に相当する PowerShell の手順です。

1. Citrix Virtual Apps and Desktops Remote PowerShell SDK を実行します。
2. コマンドウィンドウで、次のコマンドを実行します:
   - `Add-PSSnapIn Citrix*`
3. 次のコマンドを実行してキーを生成し、Key1 を設定します:
   - `New-BrokerXmlServiceKey`
   - `Set-BrokerSite -XmlServiceKey1 <the key you generated>`
4. 次のコマンドを実行してキーを生成し、Key2 を設定します:
   - `New-BrokerXmlServiceKey`
   - `Set-BrokerSite -XmlServiceKey2 <the key you generated>`
5. 次のコマンドのいずれかまたは両方を実行して、通信の認証でキーを使用できるようにします:
   - XML ポート経由での通信を認証するには、次を実行します:
     - `Set-BrokerSite -RequireXmlServiceKeyForNFuse $true`
   - STA ポート経由での通信を認証するには、次を実行します:
     - `Set-BrokerSite -RequireXmlServiceKeyForSta $true`

ガイダンスと構文について詳しくは、PowerShell コマンドのヘルプを参照してください。

StoreFront の設定を構成する

サイトでの構成が完了したら、PowerShell を使って StoreFront で関連する設定を構成する必要があります。

StoreFront サーバーで、次の PowerShell コマンドを実行します:

XML ポート経由での通信のキーを構成するには、次のコマンドを使用します。[Set-STFStoreFarm	https://developer-docs.citrix.com/en-us/storefront-powershell-sdk/current-release/Set-STFStoreFarm.html]。例:

```
$store = Get-STFStoreService -VirtualPath [Path to store]
$farm = Get-STFStoreFarm -StoreService $store -FarmName [Resource feed name]
Set-STFStoreFarm -Farm $farm -XMLValidationEnabled $true -XMLValidationSecret [secret]
```

次のパラメーターの適切な値を入力します:

- `Path to store`
- `Resource feed name`

- secret

STA ポート経由での通信のキーを設定するには、New-STFSecureTicketAuthorityおよびSet-STFRoamingGatewayコマンドを使用します。例:

```
$gateway = Get-STFRoamingGateway -Name [Gateway name]
$sta1 = New-STFSecureTicketAuthority -StaUrl [STA1 URL] -
    StaValidationEnabled $true -StaValidationSecret [secret]
$sta2 = New-STFSecureTicketAuthority -StaUrl [STA2 URL] -
    StaValidationEnabled $true -StaValidationSecret [secret]
Set-STFRoamingGateway -Gateway $gateway -SecureTicketAuthorityObjs
    $sta1,$sta2
```

次のパラメーターの適切な値を入力します:

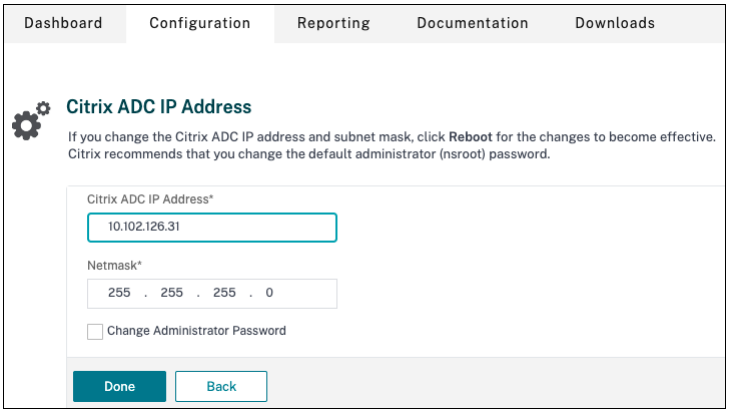
- Gateway name
- STA URL
- Secret

ガイダンスと構文について詳しくは、PowerShell コマンドのヘルプを参照してください。

Citrix ADC の設定を構成する

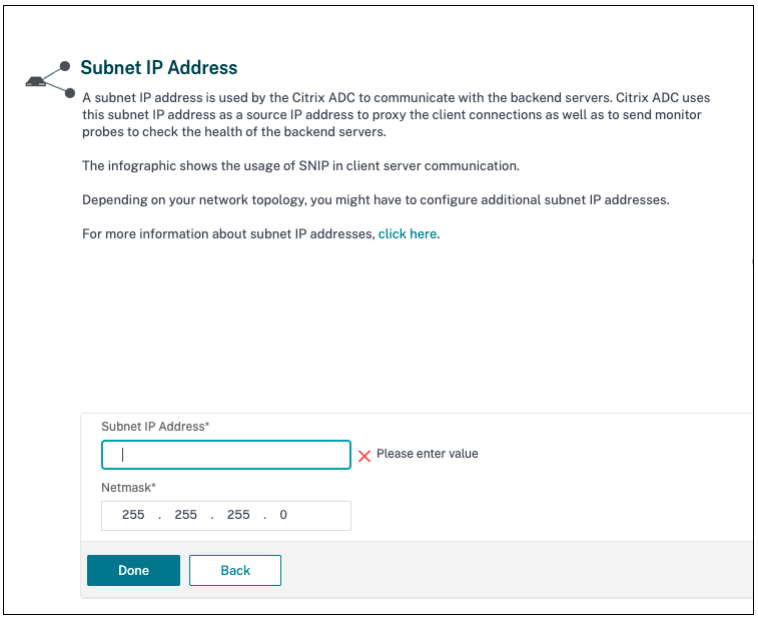
> 注:
>
> ゲートウェイとして Citrix ADC を使用しない限り、Citrix ADC のこの機能を構成する必要はありません。Citrix ADC を使用する場合は、以下の手順に従ってください:

1. 以下の前提条件の構成が既に設定されていることを確認してください:
    - 以下の Citrix ADC 関連の IP アドレスが構成されている。
        - Citrix ADC コンソールにアクセスするための Citrix ADC 管理 IP（NSIP）アドレス。詳しくは、「NSIP アドレスの構成」を参照してください。

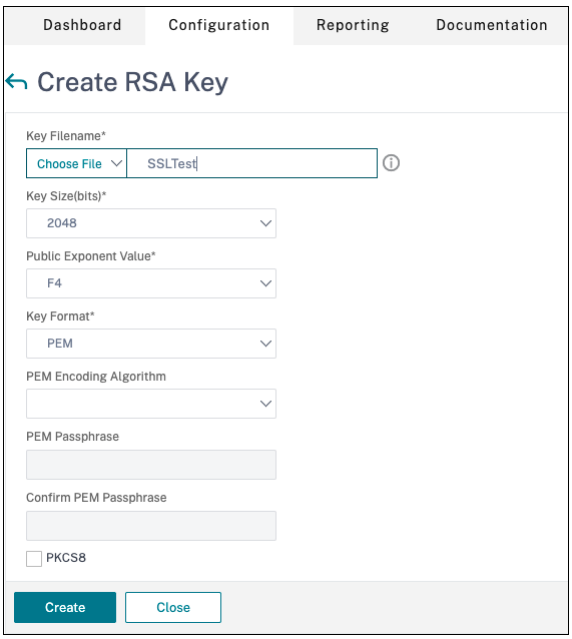


        - Citrix ADC アプライアンスとバックエンドサーバー間の通信を有効にするためのサブネット IP（SNIP）アドレス。詳しくは、「サブネット IP アドレスの構成」を参照してください。

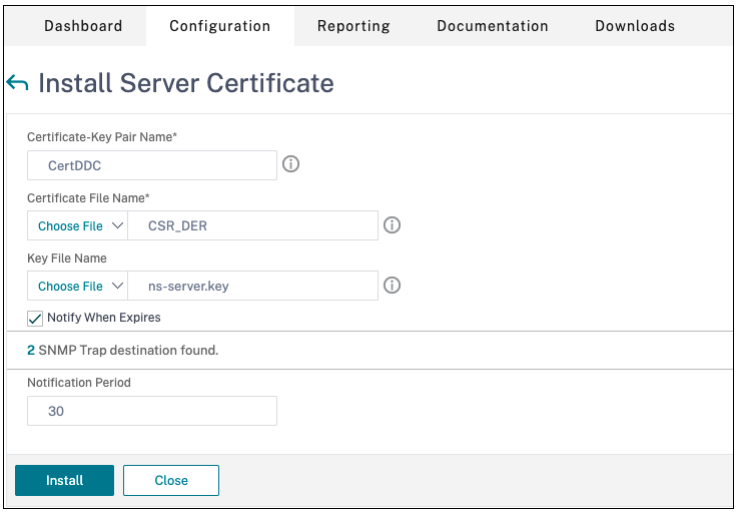
  - ADC アプライアンスにログインしてセッションを起動するための Citrix Gateway 仮想 IP アドレスとロードバランサー仮想 IP アドレス。詳しくは、「仮想サーバーの作成」を参照してください。

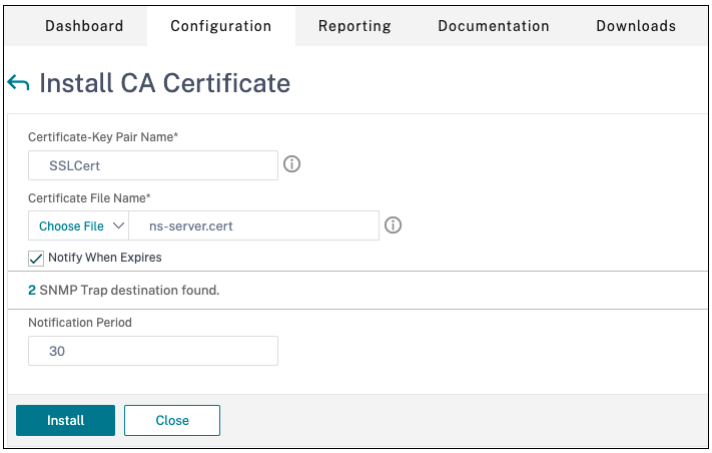


- Citrix ADC アプライアンスで必要なモードと機能が有効である。
  - モードを有効にするには、Citrix ADC GUI で［**System**］>［**Settings**］>［**Configure Mode**］の順に移動します。
  - 機能を有効にするには、Citrix ADC GUI で ［**System**］>［**Settings**］>［**Configure Basic Features**］の順に移動します。
- 証明書関連の構成が完了している。
  - 証明書署名要求（CSR：Certificate Signing Request）が作成されていること。詳しくは、「証明書の作成」を参照してください。

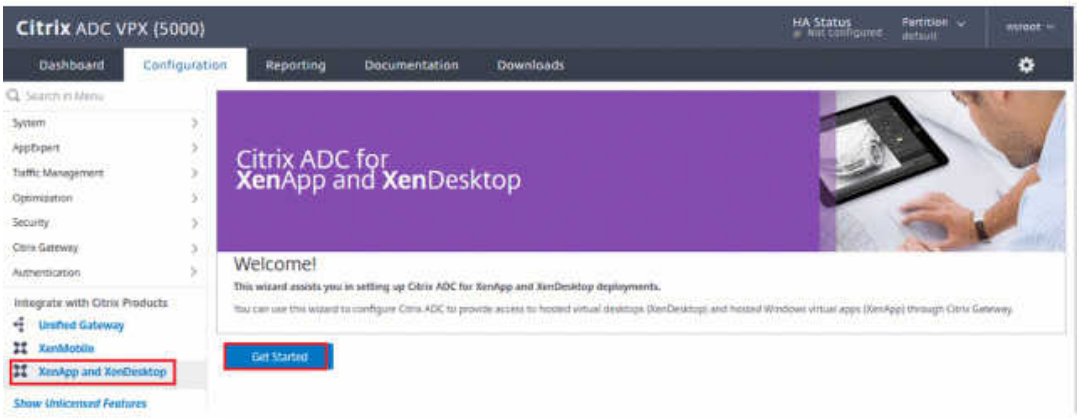


- サーバー証明書と CA 証明書およびルート証明書がインストールされていること。詳しくは、「インストール、リンク、および更新」を参照してください。





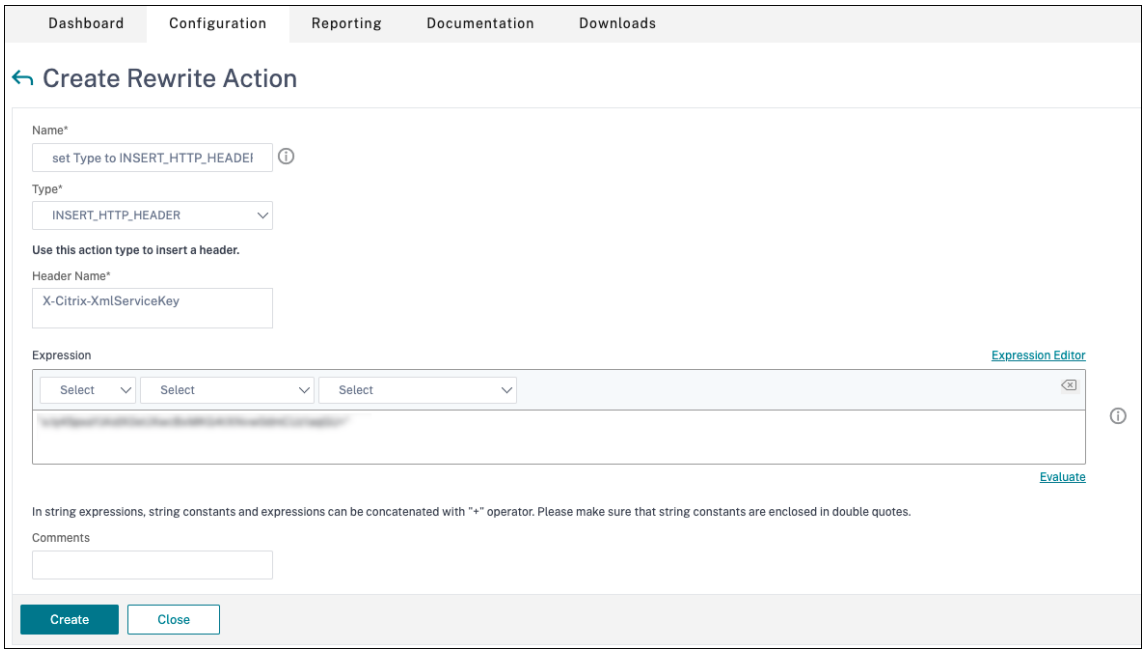
– Citrix Virtual Desktops 用に Citrix Gateway が作成されていること。[**Test STA Connectivity**] ボタンをクリックして接続をテストし、仮想サーバーがオンラインであることを確認します。詳しくは、「Citrix Virtual Apps and Desktops 用の Citrix ADC のセットアップ」を参照してください。



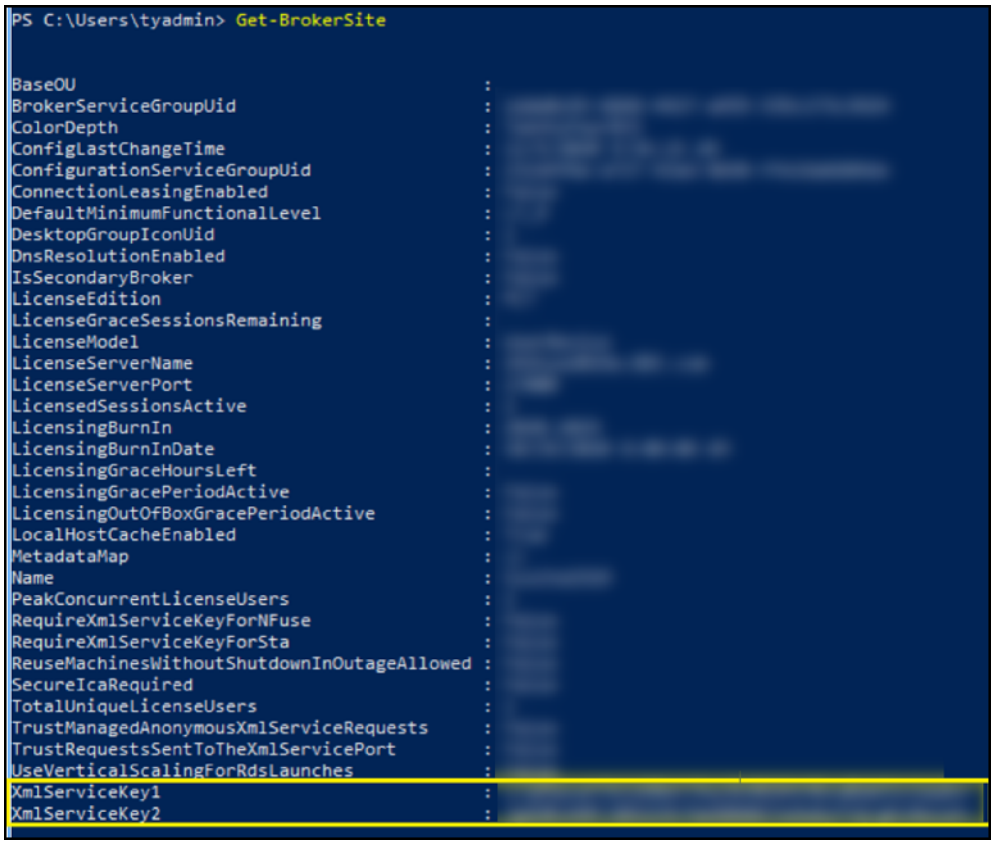
2. 書き換えアクションを追加します。詳しくは、「書き換えアクションの構成」を参照してください。

   a) [**AppExpert**] > [**Rewrite**] > [**Actions**] の順に移動します。

   b) [**Add**] をクリックして、新しい書き換えアクションを追加します。アクションに「set Type to INSERT_HTTP_HEADER」という名前を付けることができます。

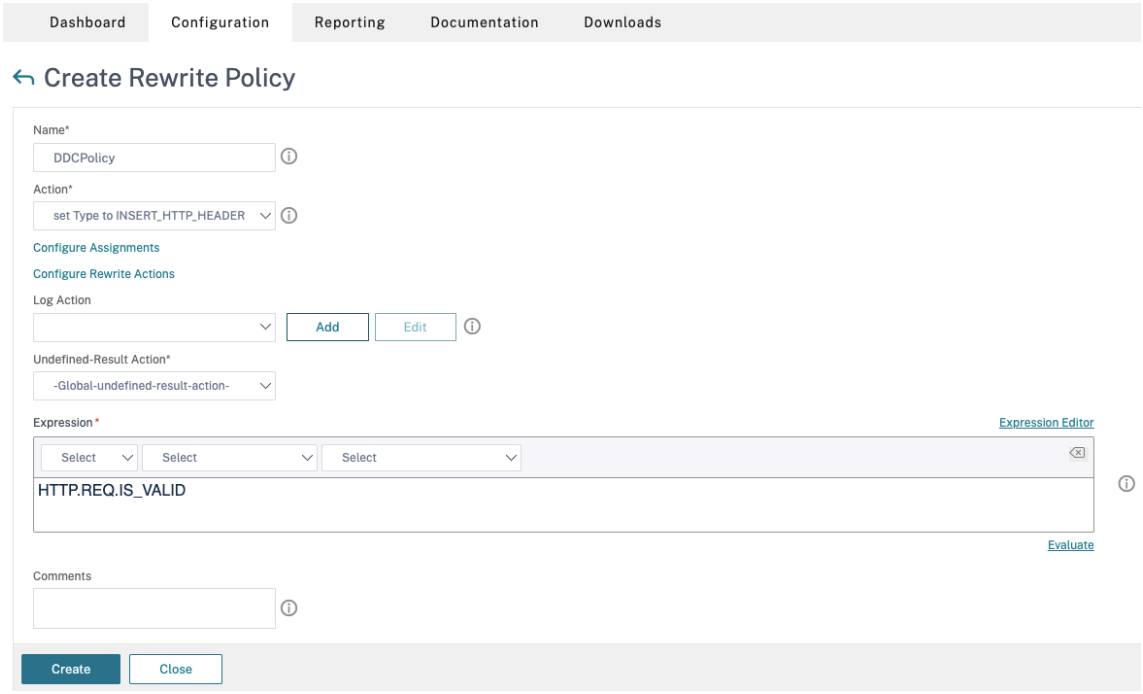


a) [**Type**] で、[**INSERT_HTTP_HEADER**] を選択します。
b) [**Header Name**] に「X-Citrix-XmlServiceKey」と入力します。
c) [**Expression**]に、引用符付きで「<XmlServiceKey1 value>」を追加します。XmlServiceKey1 の値は、Desktop Delivery Controller の構成からコピーできます。



3. 書き換えポリシーを追加します。詳しくは、「書き換えポリシーの構成」を参照してください。

a) [**AppExpert**] > [**Rewrite**] > [**Policies**] の順に移動します。
b) [**Add**] をクリックして、新しいポリシーを追加します。



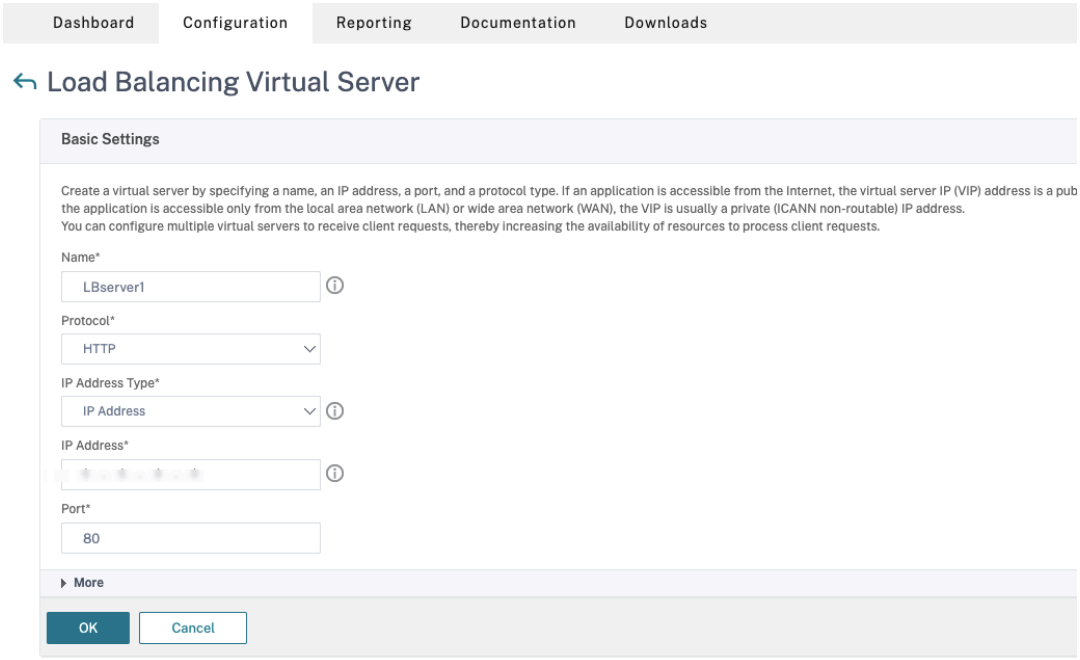
a) [**Action**] で、前の手順で作成したアクションを選択します。
b) [**Expression**] に、「HTTP.REQ.IS_VALID」を追加します。
c) [**OK**] をクリックします。

4. 負荷分散を設定します。STA サーバーごとに 1 つの負荷分散仮想サーバーを構成する必要があります。そうしない場合、セッションの起動が失敗します。

   詳しくは、「基本的な負荷分散の設定」を参照してください。

   a) 負荷分散仮想サーバーを作成します。

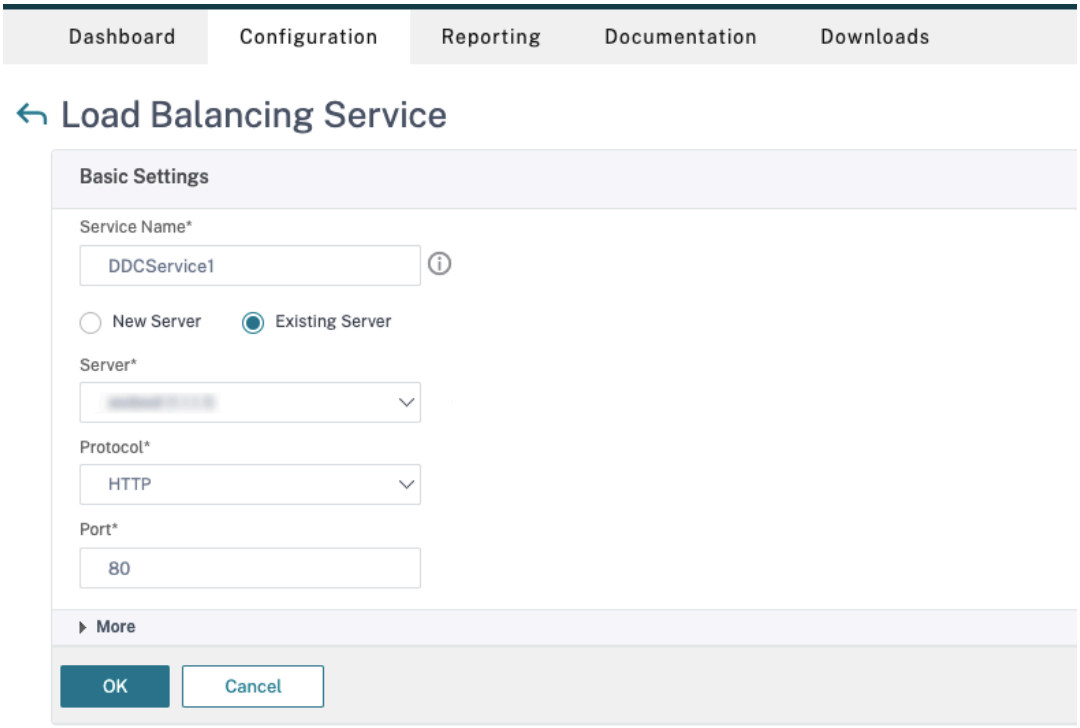
      - [**Traffic Management**] > [**Load Balancing**] > [**Servers**] の順に移動します。
      - [**Virtual Servers**] ページで [**Add**] をクリックします。



- [**Protocol**] で、[**HTTP**] を選択します。
- 負荷分散仮想 IP アドレスを追加し、[**Port**] で [**80**] を選択します。
- [**OK**] をクリックします。

b) 負荷分散サービスを作成します。

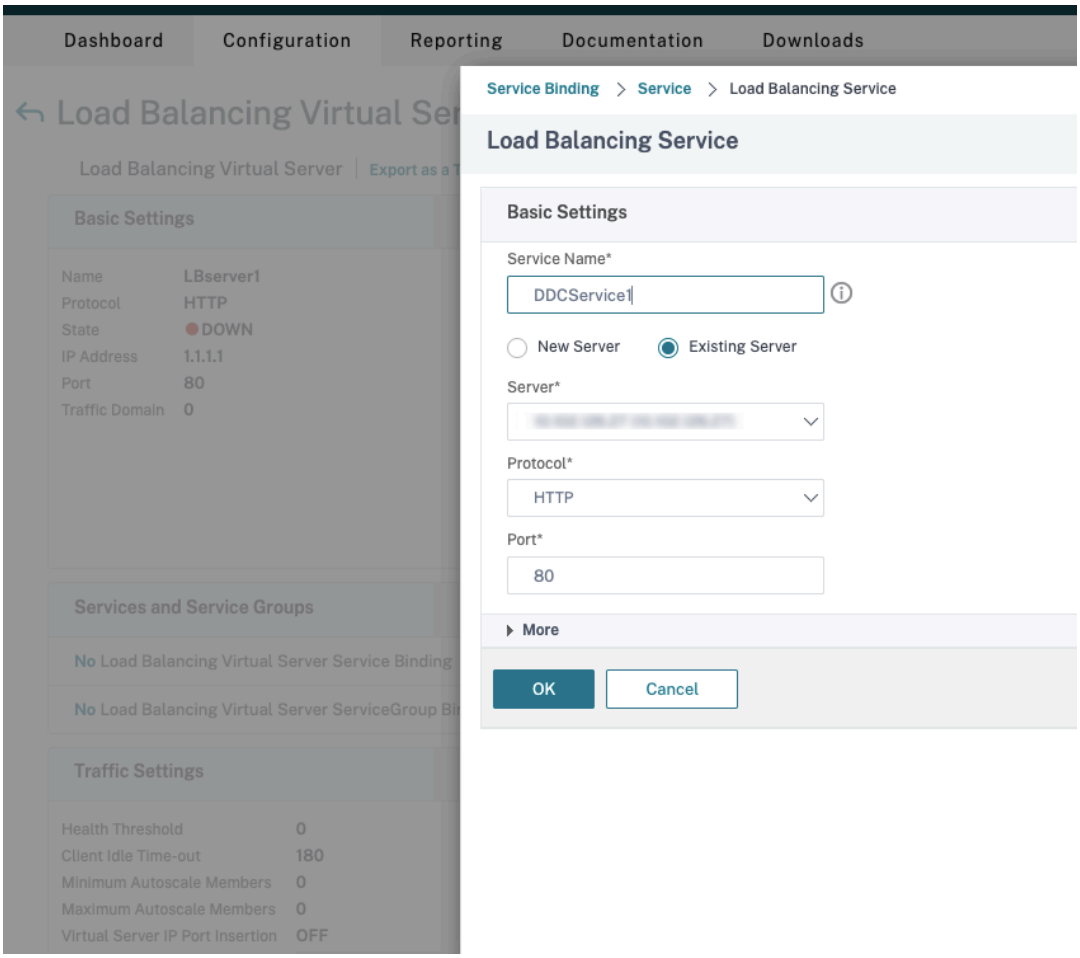
- [**Traffic Management**] > [**Load Balancing**] > [**Servers**] の順に移動します。



- [**Existing Server**] で、前の手順で作成した仮想サーバーを選択します。
- [**Protocol**] で [**HTTP**] を選択し、[**Port**] で [**80**] を選択します。
- [**OK**] をクリックし、[**Done**] をクリックします。

c) サービスを仮想サーバーにバインドします。

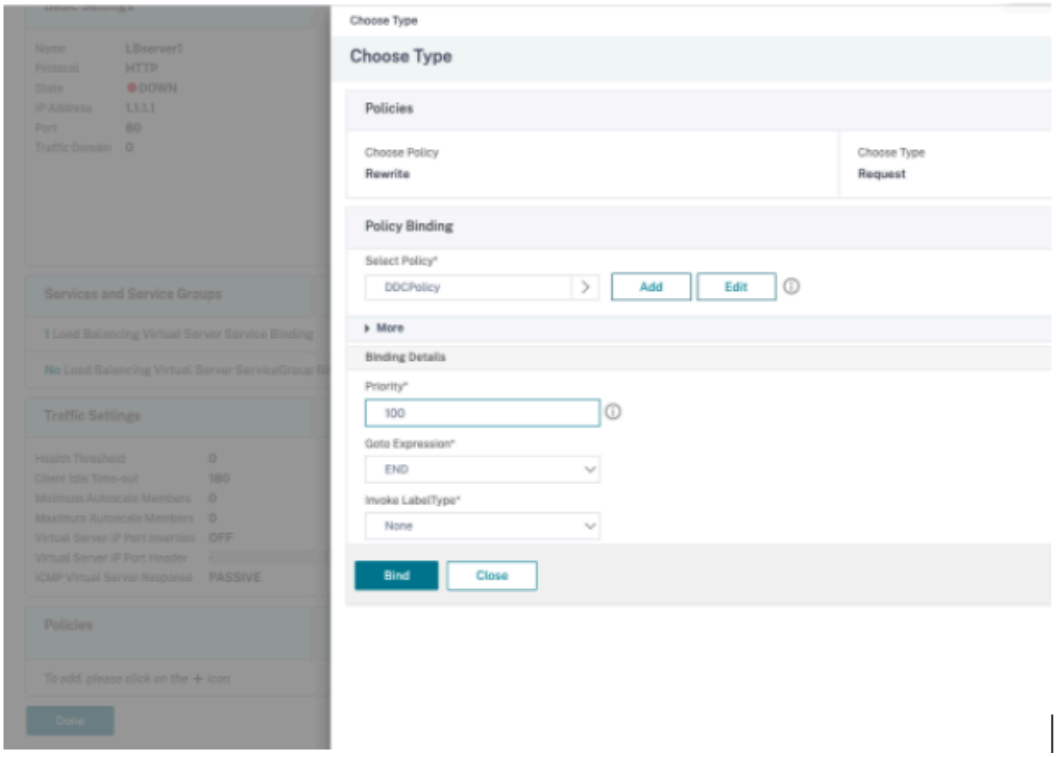
- 以前に作成した仮想サーバーを選択し、[**Edit**] をクリックします。
- [**Services and Service Groups**] の [**No Load Balancing Virtual Server Service Binding**] をクリックします。



- [**Service Binding**] で、前に作成したサービスを選択します。
- [**Bind**] をクリックします。

d) 以前に作成した書き換えポリシーを仮想サーバーにバインドします。

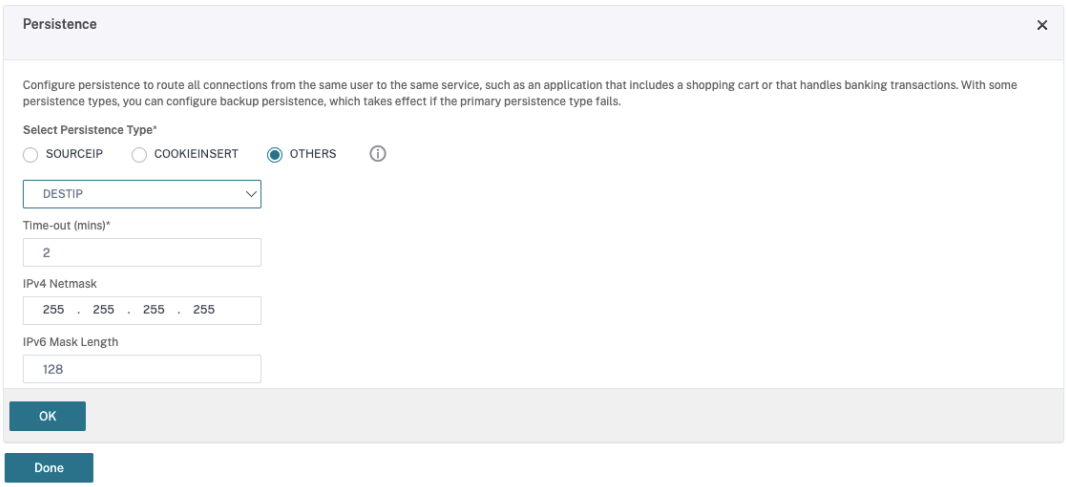
- 以前に作成した仮想サーバーを選択し、[**Edit**] をクリックします。
- [**Advanced Settings**] で [**Policies**] をクリックし、[**Policies**] セクションで [**+**] をクリックします。



- [**Choose Policy**] で [**Rewrite**] を選択し、[**Choose Type**] で [**Request**] を選択します。
- [続行] をクリックします。
- [**Select Policy**] で、前に作成した書き換えポリシーを選択します。
- [**Bind**] をクリックします。
- [完了] をクリックします。

e) 必要に応じて、仮想サーバーの永続性を設定します。

- 以前に作成した仮想サーバーを選択し、[**Edit**] をクリックします。
- [**Advanced Settings**] で、[**Persistence**] をクリックします。



- 永続性タイプを [**Others**] にします。

- 仮想サーバーによって選択されたサービスの IP アドレス（宛先 IP アドレス）に基づいて、永続セッションを作成するには、[**DESTIP**] を選択します。
- [**IPv4 Netmask**] で、DDC と同じネットワークマスクを追加します。
- [**OK**] をクリックします。

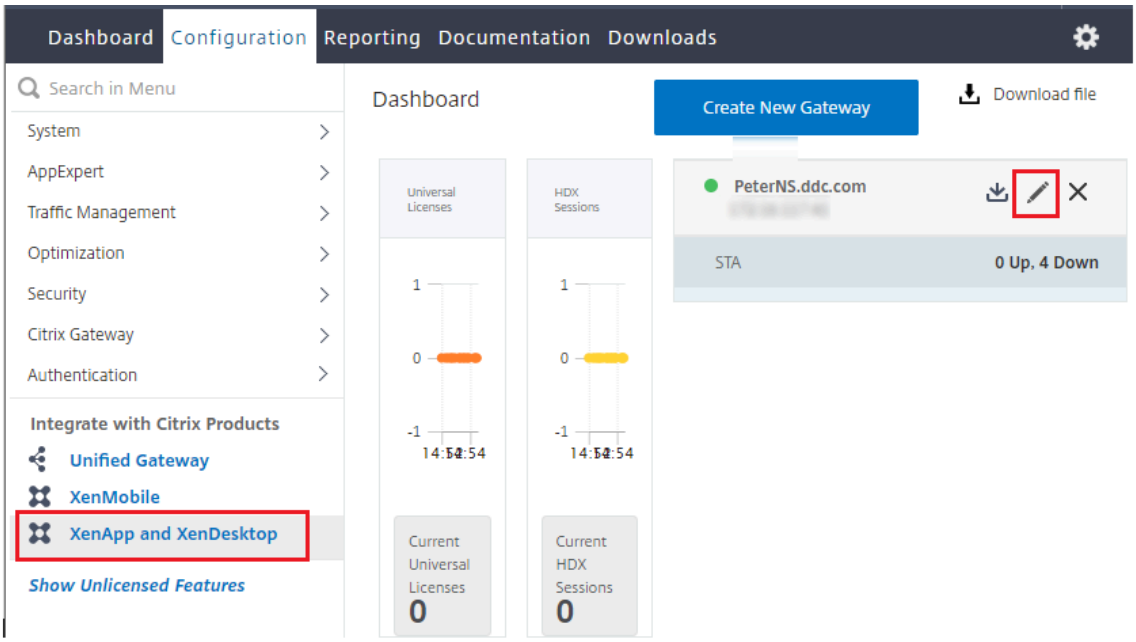
f) 他の仮想サーバーについても、これらの手順を繰り返します。

Citrix ADC アプライアンスが既に **Citrix Virtual Desktops** により構成されている場合の構成の変更

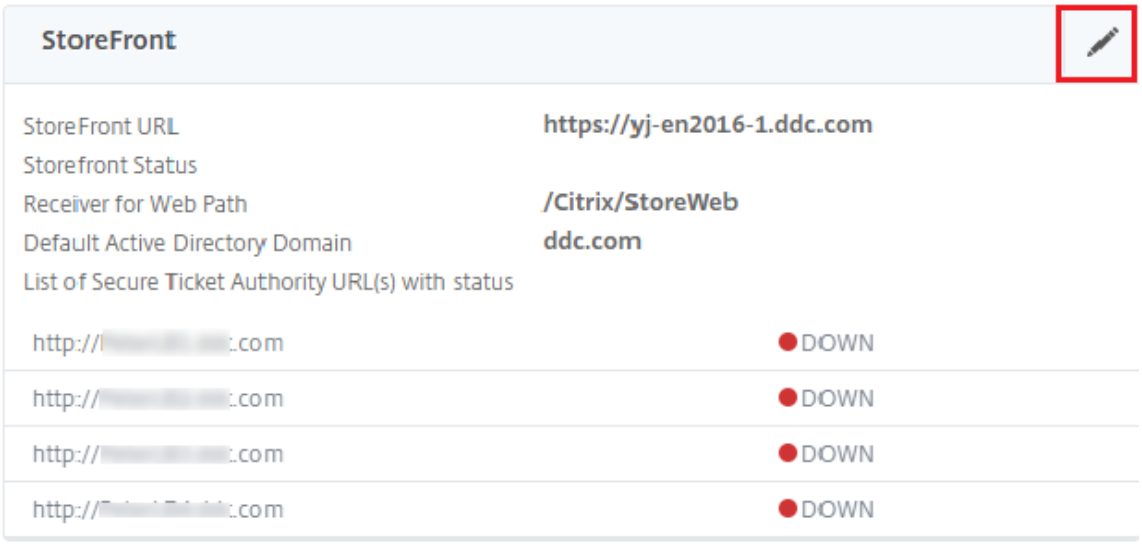
Citrix Virtual Desktops を使用して Citrix ADC アプライアンスを既に構成している場合、Secure XML 機能を使用するには、次の構成変更を行う必要があります。

- セッションを起動する前に、ゲートウェイの **Security Ticket Authority URL** を変更して、負荷分散仮想サーバーの FQDN（完全修飾ドメイン名）を使用します。
- `TrustRequestsSentToTheXmlServicePort`パラメーターが False に設定されていることを確認してください。デフォルトでは、`TrustRequestsSentToTheXmlServicePort`パラメーターは False に設定されています。ただし、顧客が Citrix Virtual Desktops 用に Citrix ADC を既に構成している場合は、`TrustRequestsSentToTheXmlServicePort`が True に設定されています。

1. Citrix ADC GUI で、[**Configuration**] > [**Integrate with Citrix Products**] の順に移動し、[**XenApp and XenDesktop**] をクリックします。
2. ゲートウェイインスタンスを選択し、編集アイコンをクリックします。

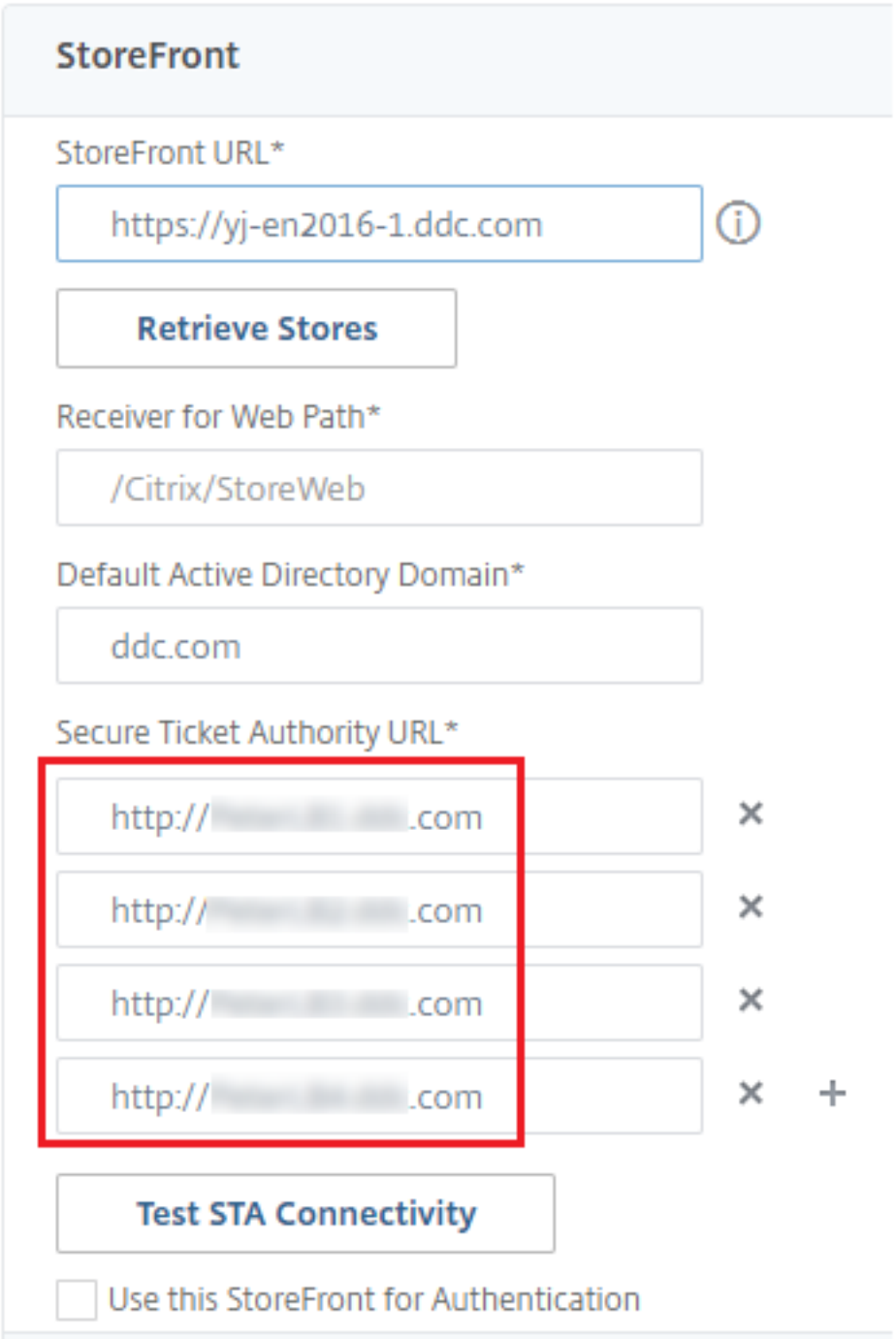


3. StoreFront ペインで、編集アイコンをクリックします。



4. [**Secure Ticket Authority URL**] を追加します。

   - Secure XML 機能が有効になっている場合、STA URL は負荷分散サービスの URL である必要があります。
   - Secure XML 機能が無効になっている場合、STA URL は STA の URL（DDC のアドレス）である必要があり、DDC の`TrustRequestsSentToTheXmlServicePort`パラメーターは True に設定されている必要があります。



セッションの復元性設定

August 17, 2024

最高のユーザーエクスペリエンスを提供するためには、日々のセッションアクティビティを保守することが重要です。

ネットワークの信頼性が低い、通信速度が一定していない、ワイヤレスデバイスの伝送距離が制限されているなどの理由でネットワーク接続が失われると、ユーザーの労働意欲が損なわれます。デバイス間をすばやく移動し、ログオンするたびに同じアプリケーションにアクセスできることは、医療従事者などの多くのモバイルワーカーにとって優先事項です。

この記事で説明する機能では、セッションの信頼性が最適化され、利便性が向上し、ダウンタイムの増加や生産性の低下を防ぐことができます。また、モバイルユーザーがデバイス間をすばやく移動できるようになります。

セッション画面の保持

セッション画面の保持機能は、ICA セッションをアクティブのまま保持し、ネットワークの接続が切断されても、セッションの画面を表示したままにできます。ユーザーは、接続が回復するまでセッション画面を見ることができます。

この機能は、ワイヤレス接続を使用するモバイルユーザーにとって特に有用です。たとえば、ワイヤレス接続でのセッション中にトンネルや障害物などの影響で接続に障害が生じた場合、通常はセッションが切断され、セッションの画面が表示されなくなります。この場合、切断セッションに再接続されるまで、そのセッションでは何もできません。セッション画面の保持機能を有効にすると、データを損失することなくセッションがアクティブのまま保持されます。ネットワークが中断されると、セッション画面が停止し、反対側で接続が再開するまでカーソルの形が砂時計に変わるため、ユーザーにもネットワークが切断されていることがわかります。このとき、セッションウィンドウが閉じたりエラーメッセージが表示されたりする代わりに画面表示が保持され、バックグラウンドで再接続が試行されます。ネットワーク接続が回復すると、自動的にセッションでの作業を再開できるようになります。また、セッションに再接続するときに再認証用のログオン画面が表示されないため、ユーザーは即座に作業を再開できます。

Citrix Workspace アプリのユーザーは、Controller 側の設定を上書きできません。

セッション画面の保持機能と共に、TLS（Transport Layer Security）を使用できます。TLS は、ユーザーデバイスと Citrix Gateway 間で送信されるデータのみを暗号化します。

セッション画面の保持機能は、以下のポリシー設定で構成します。

- ［セッション画面の保持］ポリシー設定により、セッション画面の保持を許可または禁止します。
- ［セッション画面の保持のタイムアウト］ポリシー設定には、デフォルトで 180 秒（3 分）が設定されています。この時間を長く設定することもできますが、この機能の本来の目的はユーザーの利便性にあります。したがって、ユーザーに再認証を求めるプロンプトは表示されません。必要以上に長い時間を設定すると、接続の再開を待ちきれないユーザーが席を離れる可能性が高くなります。その間に不正なユーザーがセッションにアクセスしてしまう危険性があります。
- セッション画面の保持機能が有効な受信接続ではポート 2598 が使用されます。このポート番号はポリシーの［セッション画面の保持のポート番号］設定で変更できます。
- 切断したセッションに再接続するユーザーを再認証する場合は、クライアントの自動再接続機能を使用します。［クライアントの自動再接続時の認証］ポリシー設定を構成して、中断されたセッションにユーザーが再接続するときに再認証を要求することができます。

セッション画面の保持機能とクライアントの自動再接続機能を一緒に使用する場合は、次のように処理されます。まず、ネットワークが切断されると、セッション画面の保持機能により、セッションがアクティブのままサーバー上に

保持されます。［セッション画面の保持のタイムアウト］設定で指定した時間が経過すると、サーバー上のセッションが終了または切断されます。この後で［クライアントの自動再接続］の各ポリシー設定が有効になり、切断セッションへの再接続が行われます。

クライアントの自動再接続

クライアント自動再接続機能では、ネットワークの問題などによって切断されたセッションを Citrix Workspace アプリが検出して、そのセッションに自動的に再接続します。この機能がサーバーで有効になっていると、ユーザーは作業を続けるために手動で再接続する必要がありません。

アプリケーションセッションでは、Citrix Workspace アプリは、接続に成功するかユーザーがキャンセルするまで再接続を繰り返し試行します。

デスクトップセッションでは、Citrix Workspace アプリは、指定された時間の間に、再接続に成功するかユーザーが再接続キャンセルするまで再接続を繰り返し試みます。デフォルトでは、この時間は 5 分です。この時間を変更するには、ユーザーデバイスで次のレジストリ設定を編集します（`seconds`は、セッションの再接続が試行されなくなるまでの秒数です）。

```
HKLM\Software\Citrix\ICA Client\TransportReconnectRetryMaxTimeSeconds
; DWORD;<seconds>
```

クライアント自動再接続機能は、以下のポリシー設定で構成します。

- クライアントの自動再接続：接続が中断した場合の Citrix Workspace アプリによる自動再接続を有効または無効にします。
- クライアントの自動再接続時の認証：自動再接続時にユーザーの認証を要求するかどうかを指定します。
- クライアントの自動再接続のログ：再接続イベントのイベントログへの記録を有効または無効にします。ログ機能は、デフォルトで無効になっています。この機能を有効にすると、サーバーのシステムログに自動再接続の成功および失敗イベントが記録されます。各サーバーは自身のシステムログに、再接続イベントに関する情報を記録します。サイトは、すべてのサーバーの再接続イベントを記録した統合ログを提供しません。

> 注:
>
> 再認証なしのクライアントの自動再接続は、パスワード認証の場合にのみサポートされます。フェデレーション認証サービスまたはスマートカード認証を使用する場合、再認証なしのクライアントの自動再接続はサポートされません。このような場合、ユーザーはログイン画面にリダイレクトされます。

クライアントの自動再接続機能には、暗号化されたユーザー資格情報に基づく再認証メカニズムが使用されています。ユーザーが最初にログオンするとき、サーバーはユーザーの資格情報を暗号化してメモリに保存します。また、サーバーは、その暗号キーを含んだ Cookie を作成して Citrix Workspace アプリに送信します。Citrix Workspace アプリは、再接続時にこのキーをサーバーへ送信します。サーバーは復号化した資格情報を Windows のログオンプロセスに送信して認証を求めます。Cookie の有効期限が切れた場合、ユーザーは資格情報を再入力する必要があります。

［クライアントの自動再接続時の認証］設定を有効にした場合、Cookie は使用されません。その代わりに、Citrix Workspace アプリの切断セッションへの自動再接続時に、ユーザーの資格情報を入力するためのダイアログボックスが開きます。

ユーザーの資格情報とセッションを最大限にセキュリティ保護するために、クライアントとサイトの間のすべての通信で暗号化機能を使用してください。

Windows 向け Citrix Workspace アプリで自動再接続機能を無効にするには、icaclient.adm ファイルを編集します。詳しくは、該当するバージョンの Windows 向け Citrix Workspace アプリのドキュメントを参照してください。

接続の設定も、クライアントの自動再接続機能に影響します。

- 前述のように、クライアントの自動再接続は、ポリシー設定によりデフォルトでサイト全体で有効になっています。ユーザーの再認証も不要です。ただし、サーバーで ICA TCP 接続が切断されたときにセッションをリセットするように設定すると、自動再接続は実行されません。クライアントの自動再接続は、エラーの発生またはタイムアウトによりサーバーがセッションを切断した場合にのみ実行されます。ここでの ICA TCP 接続とは、実際のネットワーク接続ではなく、TCP/IP ネットワーク上のセッションで使用されるサーバーの仮想ポートを指します。
- サーバー上の ICA TCP 接続では、デフォルトでエラーやタイムアウトが発生した接続のセッションを切断するように設定されています。切断されたセッションはそのままシステムメモリに残るので、ユーザーは同じサーバーに自動的に再接続して、そのセッションでの作業を続行できます。
- エラーが生じたりタイムアウトしたりした接続のセッションについてはリセット、つまりログオフされるように構成できます。セッションがリセットされた場合、再接続しようとすると、新しいセッションが開始されます。切断前の作業状態からセッションが復元されるのではなく、アプリケーションが再起動されます。
- セッションがリセットされるようにサーバーが構成されている場合、クライアントの自動再接続により新しいセッションが開始されます。この場合、ユーザーが自分の資格情報を入力して、サーバーにログオンし直す必要があります。
- 外部からの侵入などによって Citrix Workspace アプリまたはプラグインから正しくない認証情報が提供された場合、またはセッションの切断が検出されてから自動再接続までの時間が長すぎた場合は、自動再接続に失敗することがあります。

ICA Keep-Alive

ICA Keep-Alive 機能を有効にすると、ネットワークの問題により切断されたセッションにユーザーが再接続できなくなることを防ぐことができます。また、この機能を有効にすると、サーバー側でセッションのアイドル状態が検出されたときに、リモートデスクトップサービスによりセッションが切断されるのを防ぐことができます。セッションのアイドル状態の例として、時計が進んでいない、マウスが動かされていない、画面が更新されていないなどがあります。サーバーは、定期的に Keep-Alive パケットを送信して、セッションがアクティブかどうかを検出します。セッションがアクティブでないことが検出されると、サーバーにより「切断」状態として認識されます。

> 重要:
>
> ICA Keep-Alive は、セッション画面の保持機能を使用しない環境でのみ正しく動作します。セッション画面の保持機能では、ICA Keep-Alive とは異なるメカニズムで切断セッションが管理されます。セッション画面の保持機能を使用しない環境でのみ、ICA Keep-Alive を有効にしてください。

ここでの ICA Keep-Alive 機能の設定は、Windows のグループポリシーによる同様の設定よりも優先されます。

ICA Keep-Alive 機能は、以下のポリシー設定で構成します。

- **ICA Keep-Alive** タイムアウト: ICA Keep-Alive メッセージの送信間隔を 1〜3600 秒の範囲で指定します。ただし、ネットワークの問題によるセッションの切断が少なく、アイドル状態のセッションをネットワーク監視ソフトウェアで自動的に閉じるように設定している環境では、このオプションを構成しないでください。

  デフォルト値は 60 秒で、サーバーからユーザーデバイスに ICA Keep-Alive パケットが 60 秒おきに送信されます。クライアントが 60 秒以内に応答しない場合、そのセッションは「切断」状態（タイムアウト）と認識されます。
- **ICA Keep-Alive**: ICA Keep-Alive メッセージを送信するかどうかを指定します。

ワークスペースコントロール

ワークスペースコントロール機能を有効にすると、ユーザーがセッションの途中でデバイスを切り替えても、新しいデバイス上でそのデスクトップやアプリケーションでの作業を継続できます。これにより、ユーザーは自分のデスクトップや作業中のアプリケーションにどこからでもシームレスにアクセスできるようになります。たとえば、病院内の複数のワークステーション間を移動しながら、常に同じアプリケーションセットにアクセスしなければならない医療従事者をサポートするために、この機能を利用できます。ワークスペースコントロールを構成すると、ユーザーは複数のアプリケーションを一度に切断して、その後で別のクライアントデバイスからそれらのアプリケーションに再接続できます。

ワークスペースコントロールを有効にすると、ユーザーの操作は以下のようになります。

- ログオン：デフォルトでは、ユーザーが移動先でログオンすると、実行されていたすべてのデスクトップおよびアプリケーションに自動的に再接続されます。デスクトップやアプリケーションを手作業で起動する必要はありません。ワークスペースコントロールにより、ユーザーは切断されたデスクトップまたはアプリケーションを開くことができ、別のクライアントデバイス上でデスクトップまたはアプリケーションがアクティブな場合でも開くことができます。ユーザーがデスクトップやアプリケーションとの接続を切断しても、サーバー上のセッションは終了しません。管理者は、ユーザーが切断したものだけが再接続されるように構成することもできます。これにより、移動先のクライアントデバイスを使ってユーザーが再ログオンしたときに、前のクライアントデバイスでアクティブなデスクトップやアプリケーションには再接続されず、切断されているものだけが再接続されます。
- 再接続：サーバーに再ログオンしたユーザーは、［再接続］をクリックすることで自分のデスクトップやアプリケーションに一度に再接続できます。デフォルトでは、切断されているデスクトップやアプリケーションと、

ほかのクライアントデバイスでアクティブなデスクトップやアプリケーションが再接続されます。管理者は、切断されているデスクトップやアプリケーションだけが再接続されるように構成することもできます。

- ログオフ：ユーザーが StoreFront 経由でデスクトップやアプリケーションにアクセスする場合に、［ログオフ］コマンドにより StoreFront およびすべてのアクティブセッションからログオフするのか、StoreFront だけからログオフするのかを管理者が構成できます。
- 切断：ユーザーは、実行中のすべてのデスクトップやアプリケーションを一度に切断できます。個々に切断する必要はありません。

ワークスペースコントロールは、Citrix Workspace アプリユーザーが Citrix StoreFront 経由でデスクトップやアプリケーションにアクセスする場合にのみ使用できます。デフォルトでは、仮想デスクトップセッションではワークスペースコントロールが無効になり、ホストされたアプリケーションセッションでは有効になります。公開デスクトップ上で公開アプリケーションを実行する場合、デフォルトではこれらのセッションは共有されません。

ユーザーが別のクライアントデバイスに移動すると、ポリシー、クライアント側ドライブのマッピング、およびプリンターの設定が適切に変更されます。ポリシーとクライアントドライブマッピングは、ユーザーがセッションにログオンするクライアントデバイスの条件に基づいて適用されます。たとえば、医療従事者が救急処置室のユーザーデバイスからログオフし、レントゲン室のワークステーションにログオンするとします。レントゲン室でのセッションに適したポリシー、クライアント側プリンターのマッピング、およびクライアントドライブマッピング設定が、セッション開始時に有効になります。

管理者は、ユーザーが場所を移動したときに使用可能になるプリンターをカスタマイズできます。また、ローカルプリンターでの印刷の可否やリモート接続時に使用される帯域幅などの印刷環境を制御することもできます。

ワークスペースコントロール機能を有効にして構成する方法については、StoreFront のドキュメントを参照してください。

セッションローミング

> 注:
>
> 次の情報は、PowerShell を使用したセッションローミングの構成について説明されたものです。代わりに Web Studio を使用できます。詳しくは、「デリバリーグループの管理」を参照してください。

デフォルトでは、ユーザーのクライアントデバイス間でセッションローミングが行われます。ユーザーがセッションを開始した後に別のデバイスに移動した場合、同じセッションが使用され、両方のデバイスでアプリケーションを使用することができます。デバイスや、現在のセッションが存在するかどうかに関係なく、アプリケーションが引き継がれます。たいていの場合、アプリケーションに割り当てられたプリンターやそのほかのリソースも引き継がれます。

このデフォルト動作には多数のメリットがありますが、すべてのケースで理想的であるわけではありません。PowerShell SDK を使用して、セッションローミングを無効にすることができます。

例 1：医療専門家が、2 つのデバイスを使用しています。デスクトップ PC では保険用紙に入力し、タブレットでは患者情報を確認します。

- セッションローミングが有効な場合、両方のアプリケーションが両方のデバイスに表示されます（どちらかのデバイスで起動されたアプリケーションが、使用しているすべてのデバイスに表示されます）。これが、セキュリティ要件に準拠しない場合があります。
- セッションローミングを無効にすると、患者レコードはデスクトップ PC には表示されず、保険用紙はタブレットには表示されません。

例 2：生産管理者が、自分のオフィスにある PC でアプリケーションを起動します。デバイスの名前と場所に基づいて、このセッションで使用できるプリンターやそのほかのリソースが決定されます。その日のうちに、生産管理者は隣の建物のオフィスに移動し、プリンターを使用する必要があるミーティングに出席します。

- セッションローミングが有効な場合、生産管理者は会議室の近くにあるプリンターを使用できない可能性があります。ミーティングより前に自分のオフィス内でアプリケーションを起動したため、オフィスの近くにあるプリンターやそのほかのリソースへの割り当てが行われているためです。
- セッションローミングが無効な場合、（同じ資格情報を使用して）別のマシンにログオンすると、新たなセッションが開始され、近くにあるプリンターやリソースを使用できるようになります。

セッションローミングを構成する

セッションローミングを構成するには、「SessionReconnection」プロパティを含む以下の資格ポリシー規則コマンドレットを使用します。オプションで、「LeasingBehavior」プロパティを指定することもできます。

デスクトップセッションの場合：

```
Set-BrokerEntitlementPolicyRule <Delivery-Group-name> -SessionReconnection
 <value> -LeasingBehavior Allowed|Disallowed
```

アプリケーションセッションの場合：

```
Set-BrokerAppEntitlementPolicyRule <Delivery-Group-name> -SessionReconnection
 <value> -LeasingBehavior Allowed|Disallowed
```

ここでは、`value`には次のいずれかを指定できます：

- **Always**：クライアントデバイスに関係なく、セッションが接続中でも、切断中でも、セッションローミングが常に実行されます。これがデフォルト値です。
- **DisconnectedOnly**：既に切断されているセッションのみに再接続します。それ以外のセッションについては、新規セッションを開始します（最初に切断するか、ワークスペースコントロールを使用して明示的にローミングすることによって、クライアントデバイス間のセッションローミングを実行することができます）。別のクライアントデバイスからのアクティブな接続済みセッションは、使用されません。代わりに、新規セッションが開始されます。
- **SameEndpointOnly**：ユーザーが使用する各クライアントデバイスに対し、一意のセッションが割り当てられます。ローミングは、完全に無効になります。ユーザーは、セッションで過去に使用されたものと同じデバイスのみに再接続できます。

「LeasingBehavior」プロパティについては、後述の説明を参照してください。

ほかの設定の影響:

セッションローミングの無効化は、デリバリーグループにおけるアプリケーションのプロパティのアプリケーション制限「**1** ユーザーあたり **1** インスタンスのみ許可する」の影響を受けます。

- セッションローミングを無効にする場合、このアプリケーション制限も無効にします。
- このアプリケーション制限を有効にする場合、新規デバイスでの新規セッションを許可する 2 つの値は、どちらも設定しないでください。

ログオン間隔

デスクトップ VDA がインストールされている仮想マシンが、ログオンプロセスが完了する前に終了する場合は、プロセスにより多くの時間を割り当てることができます。7.6 以降のバージョンのデフォルトは 180 秒です（7.0〜7.5 は 90 秒です）。

マシン上（またはマシンカタログで使用されるマスターイメージ上）で、以下のレジストリキーを設定します:

キー: `HKLM\SOFTWARE\Citrix\PortICA`

- 値: `AutoLogonTimeout`
- 種類: `DWORD`
- 十進法時間（秒）を 0〜3600 の範囲で指定します。

マスターイメージを変更する場合は、カタログを更新してください。

この設定は、デスクトップ VDA を搭載した VM にのみ適用されます。サーバー VDA を搭載したマシンのログオンタイムアウトは、Microsoft 社により制御されます。

設定

August 17, 2024

> 注:
>
> Web Studio（Web ベース）と Citrix Studio（Windows ベース）の 2 つの管理コンソールを使用して、Citrix Virtual Apps and Desktops の展開を管理できます。この記事では Web Studio のみを扱います。Citrix Studio について詳しくは、Citrix Virtual Apps and Desktops 7 2212 以前の同様の記事を参照してください。

Web Studio を使用して、これらの設定を管理できます:

- 認証を管理する

- Citrix カスタマーエクスペリエンス向上プログラム
- Delivery Controller の削除
- ログデータベースの変更
- 日付と時刻の設定
- サイトの一元管理
- リモート PC アクセスの複数ユーザーの自動割り当てを有効にする
- DNS 解決を有効にする
- XML 信頼を有効にする
- セキュリティキーの管理
- Studio コンソールで非アクティブタイムアウトを設定する

認証を管理する

デフォルトでは、ユーザーはドメインユーザー名とパスワードを使用して Web Studio にログオンします。スマートカード認証や統合 Windows 認証など、ユーザーに対して別の認証方法を選択することもできます。

ユーザーの認証方法を選択するには、次の手順を実行します:

1. Web Studio にサインインし、左側のペインで［設定］を選択します。
2. 認証タイルを見つけて、［編集］をクリックし、オプションを選択します:
    - ドメイン資格情報
    - ドメイン資格情報または統合 Windows 認証

      統合 Windows 認証を有効にすると、ユーザーは Windows 資格情報（Kerberos/NTLM）またはクライアント証明書で Web Studio にアクセスできます。

      Web Studio と Delivery Controller が異なるマシンにインストールされている場合、統合 Windows 認証を機能させるには、［クロスオリジンアクセスを許可する］を有効にし、Web Studio サーバーの URL を許可リストに追加します。

      > 重要
      >
      > Web Studio が Delivery Controller のプロキシとして構成されている場合、統合 Windows 認証は機能しません。

    - スマートカード認証。
    - ドメイン資格情報またはスマートカード認証

      スマートカード認証を有効にするには、追加の構成が必要です。詳しくは、「Web Studio のスマートカード認証の設定」を参照してください。

統合 **Windows** 認証オプションを有効にすると、ユーザーは次回ログオンするときに自動的にサインインされます。ユーザーとして自動的にサインインできない場合は、次の手順に従って統合 Windows 認証を許可するように Web ブラウザーを構成します。

Google Chrome の場合:

1. ［コントロール］パネルで［インターネットオプション］を起動します。
2. ［詳細設定］タブを選択します。
3. ［統合 **Windows** 認証を使用する］を選択します。
4. ［セキュリティ］タブを選択します。
5. ［ローカルイントラネット］**>**［サイト］**>** ［詳細設定］を選択します。
6. ［この **Web** サイトをゾーンに追加する］ボックスで、以下を実行します:
    - Web Studio と Delivery Controller が同じサーバー上に存在する場合は、Web Studio を実行しているホストの URL を入力します。
    - そうでない場合は、ワイルドカードドメインを入力します。例: Delivery Controller が`ddc.domain.com`にある場合は、`*.domain.com`と入力します。
7. ［追加］**>**［閉じる］をクリックします。

Mozilla Firefox の場合:

1. ブラウザーから、URL ボックスに`about:config`を入力します。
2. 検索ボックスに「`network negotiate`」と入力します。
3. **network.negotiate-auth.trusted-uris** を右クリックし、［変更］を選択します。
4. ［文字列を入力してください］ボックスで、以下を実行します:
    - Web Studio と Delivery Controller が同じサーバー上に存在する場合は、Web Studio をホストしているサーバー名を参照する URL および/またはエイリアスの、コンマ区切りの一覧を追加します。
    - または、次の方法で URL を追加します。例: Delivery Controller が`ddc.domain.com`にある場合は、`*.domain.com`と入力します。

ブラウザーを構成した後、サインインページで ［**Windows** 統合サインイン］をクリックして再試行できます。

Web Studio と Delivery Controller が異なるマシンにインストールされている場合、統合 Windows 認証が機能するには、［クロスオリジンアクセスを許可する］を有効にする必要があります。

次の手順に従って、［クロスオリジンアクセスを許可する］を有効にします:

1. ［クロスオリジンアクセスを許可する］チェックボックスを選択します。
2. Web Studio サーバーの URL を許可リストに追加します。
3. ［**URL** を入力］フィールドに URL を入力します。必要に応じて、［追加］をクリックしてさらに追加します。

> 注
>
> - URL は次の正しい形式で指定する必要があります：<scheme>://<hostname>。パスや末尾のスラッシュが含まれていないことを確認してください。
> - IP アドレスと完全修飾ドメイン名がサポートされています。URL を追加するときは、Web Studio へのアクセス方法に対応していることを確認してください。たとえば、IP アドレスを使用して Web Studio にアクセスする場合は、IP アドレスベースの URL をリストに追加します。
> - デフォルト以外のポートを使用する場合は、必ずポート番号を含めてください。

4. 必要に応じて、［追加］をクリックしてさらに追加します。
5. 完了したら ［完了］をクリックし、保存して終了します。

タイムゾーンを設定する

好みに合わせて日付と時刻の形式をカスタマイズするには、次の手順に従います：

1. Web Studio にサインインし、左側のペインで ［設定］を選択します。
2. ［日時］タイルを見つけて ［編集］をクリックして、次のオプションを構成します：
   - 時間形式：
     - 12 時間制（例：09:00 PM）または 24 時間制（例：21:00）で時刻を表示することを選択します。
   - 日付の形式：
     - 環境設定に合わせて日付形式を構成します。例：yyyy/MM/dd。
   - タイムゾーン：
     - **UTC**：ユーザーインターフェイス全体で、日付と時刻を UTC で表示します。日付と時刻の上にマウスを置くと、その情報がローカルタイムゾーンで表示されます。
     - ローカルタイムゾーン：ユーザーインターフェイス全体で、日付と時刻をローカルタイムゾーンで表示します。日付と時刻の上にマウスを置くと、その情報が UTC で表示されます。

> 注：
>
> これらの設定は各ユーザー アカウントに固有です。

DNS 解決を有効にする

ICA ファイルで IP アドレスの代わりに DNS 名を表示するには、次の手順に従います：

1. Web Studio にサインインし、左側のペインで ［設定］を選択します。
2. ［**DNS** 解決を有効にする］設定を有効にします。

Studio コンソールで非アクティブタイムアウトを設定する

管理者が Studio コンソールから自動的にサインアウトするまでの非アクティブ期間を設定できます。

1. Web Studio にサインインし、左側のペインで ［設定］を選択します。
2. 10 分から 24 時間の範囲で期間を入力します。
3. この設定を適用するには、ページを更新するか、サインアウトしてから再度サインインします。

サイトの一元管理

この機能を使用すると、1 つの Web Studio コンソールを使用して複数の Citrix Virtual Apps and Desktops サイトを管理できます。詳しくは、「複数のサイト管理を有効にする」を参照してください。

タグ

August 17, 2024

> 注:
>
> Web Studio（Web ベース）と Citrix Studio（Windows ベース）の 2 つの管理コンソールを使用して、Citrix Virtual Apps and Desktops の展開を管理できます。この記事では Web Studio のみを扱います。Citrix Studio について詳しくは、Citrix Virtual Apps and Desktops 7 2212 以前の同様の記事を参照してください。

はじめに

タグは、マシン、アプリケーション、デスクトップ、デリバリーグループ、アプリケーショングループ、ポリシーなどのアイテムを識別する文字列です。タグを作成してアイテムに追加すると、以下のように、特定の操作を指定されたタグのあるアイテムのみに適用するように調整できます。

- Web Studio での検索結果の表示を調整する。

  たとえば、テスターに最適化されているアプリケーションのみを表示するには、「テスト」という名前のタグを作成し、それらのアプリケーションに追加（適用）します。これで、Web Studio の検索結果を「テスト」タグでフィルタリングできます。

- 選択したデリバリーグループ内のマシンのサブセットだけを対象にして、アプリケーショングループまたは特定のデスクトップからアプリケーションを公開する。この機能は、タグによる制限と呼ばれます。

  タグによる制限で、複数の公開タスクに既存のマシンを使用できるので、追加のマシンを展開、管理するコストを節約できます。タグ制限は、デリバリーグループのマシンをさらに分割（またはパーティション化）する

ものと考えることができます。その機能は、7.x より前のリリースの XenApp ワーカーグループに類似していますが、同一ではありません。

タグによる制限のあるアプリケーショングループやデスクトップを使用すると、デリバリーグループ内のマシンのサブセットを分離してトラブルシューティングするときに便利です。

- デリバリーグループ内のマシンのサブセットの定期再起動をスケジューリングする。

  マシンでタグによる制限を使用すると、新しい PowerShell コマンドレットを使用して、デリバリーグループ内のマシンのサブセットに対して複数の再起動スケジュールを構成できます。例と詳細については、「デリバリーグループの管理」を参照してください。

- デリバリーグループのマシンのサブセット、デリバリーグループの種類、指定されたタグを持つ（または持たない）OU への Citrix ポリシーの適用（割り当て）を調整する。

  たとえば、より強力なワークステーションにのみ Citrix ポリシーを適用するには、それらのマシンに「ハイパワー」という名前のタグを追加します。その後、ポリシーの作成ウィザードの ［ポリシーの割り当て］ページでこのタグを選択し、［有効化］チェックボックスをオンにします。デリバリーグループにタグを追加し、そのデリバリーグループに Citrix ポリシーを適用することもできます。詳しくは、「ポリシーの作成」を参照してください。

タグは次のものに適用できます：

- マシン
- アプリケーション
- マシンカタログ（PowerShell のみ、「マシンカタログのタグ」を参照）
- デリバリーグループ
- アプリケーショングループ

タグによる制限は、Web Studio で次のものを作成または編集するときに構成できます：

- 共有デリバリーグループのデスクトップ
- アプリケーショングループ

デスクトップまたはアプリケーショングループのタグによる制限

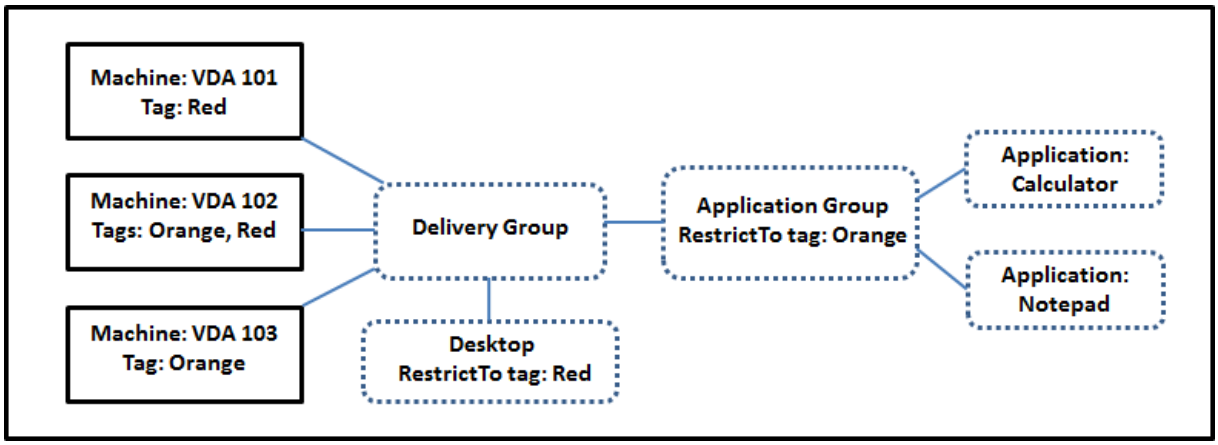
タグによる制限には、いくつかの手順があります：

- タグを作成し、マシンに追加（適用）します。
- タグによる制限を持つグループを作成または編集します（言い換えると、タグ x を持つマシンに起動を制限します）。

タグによる制限は、ブローカーのマシン選択プロセスを拡張します。ブローカーは、関連するデリバリーグループから、アクセスポリシー、構成されたユーザーの一覧、ゾーン優先度、起動対応度、およびタグによる制限（存在する場合）に従うマシンを選択します。アプリケーションの場合、ブローカーは優先度順に他のデリバリーグループにフォールバックし、関係する各デリバリーグループに同じマシン選択規則を適用します。

例 **1**：単純なレイアウト

この例では、あるデスクトップおよびアプリケーションの起動に関係するマシンを、タグを使用して制限する、単純なレイアウトを紹介します。サイトには、1 つの共有デリバリーグループ、1 つの公開デスクトップ、および 2 つのアプリケーションで構成された 1 つのアプリケーショングループがあります。



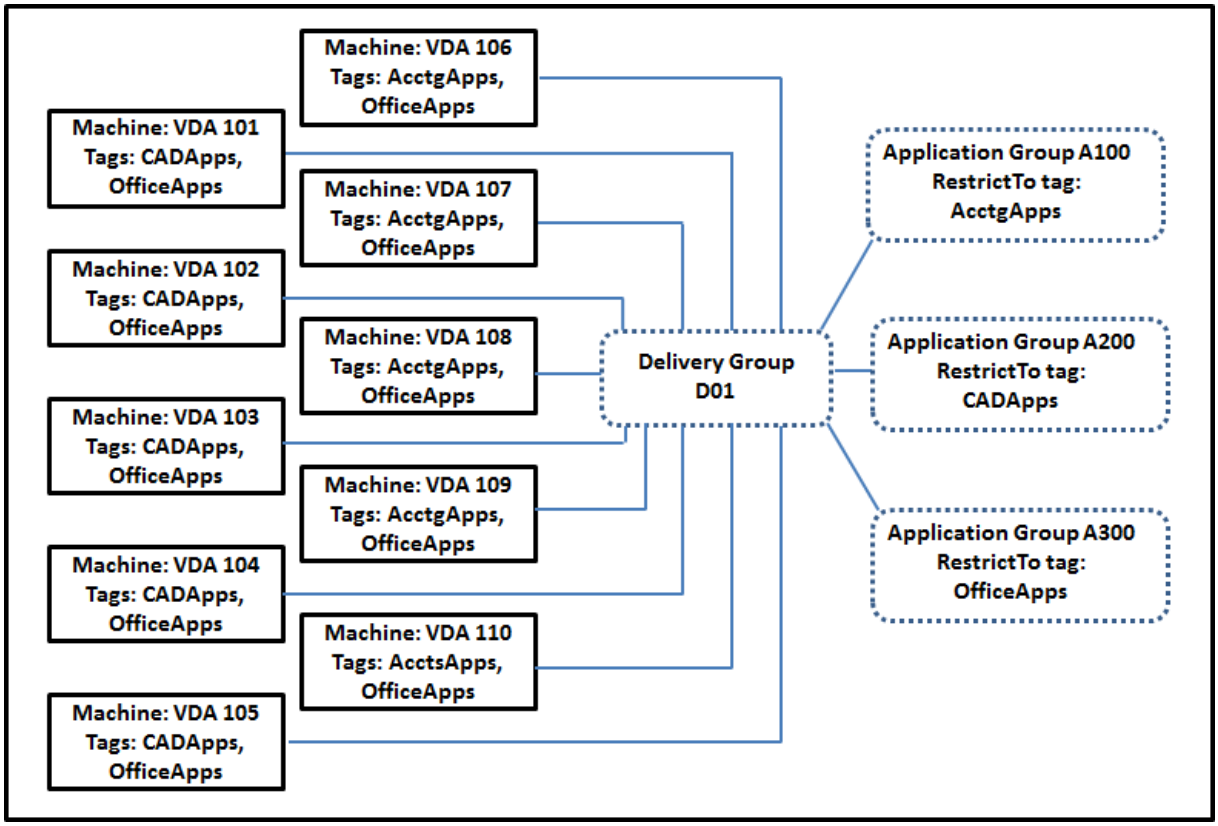
- 3 台のマシン（VDA 101～103）それぞれにタグが追加されています。
- 共有デリバリーグループのデスクトップは、「赤」という名前のタグによる制限を使用して作成されました。デスクトップは、タグ「赤」を持つそのデリバリーグループ内のマシン（VDA 101 および 102）でのみ起動できます。
- アプリケーショングループは「Orange」のタグ制限で作成されているので、各アプリケーション（電卓とメモ帳）は、デリバリーグループの、タグが「Orange」のマシン VDA 102 および 103 上でのみ起動できます。

マシン VDA 102 は両方のタグ（Red および Orange）を持っており、したがってアプリケーションとデスクトップの起動に関与できます。

例 **2**：複雑なレイアウト

この例には、タグによる制限を使用して作成された複数のアプリケーショングループが含まれます。これにより、デリバリーグループのみを使用する場合に必要な数より少ないマシンでより多くのアプリケーションを提供できます

タグを作成、適用し、この例のタグによる制限を構成するための手順については、「例 2 を構成する方法」に示しています。



この例では、10 台のマシン（VDA 101～110）、1 つのデリバリーグループ（D01）、および 3 つのアプリケーショングループ（A100、A200、A300）を使用します。各アプリケーショングループの作成時に、各マシンにタグを適用し、タグによる制限を指定することにより、以下のことが可能です：

- グループ内の会計ユーザーは、5 台のマシン（VDA 101～105）上で、必要なアプリにアクセスできます。
- グループ内の CAD デザイナーは、5 台のマシン（VDA 106～110）上で、必要なアプリにアクセスできます。
- Office アプリケーションを必要とするグループのユーザーは、10 台のマシン（VDA 101～110）上で、Office アプリにアクセスできます。

使用されるマシンは 10 台のみで、デリバリーグループは 1 つだけです。1 台のマシンは 1 つのデリバリーグループにのみ属することができるので、デリバリーグループのみを使用する場合は（アプリケーショングループ不使用時）、2 倍のマシンが必要になります。

タグとタグによる制限の管理

タグの作成、追加（適用）、編集、適用済みのアイテムからの削除は、Web Studio の ［タグの管理］操作を使用して行います

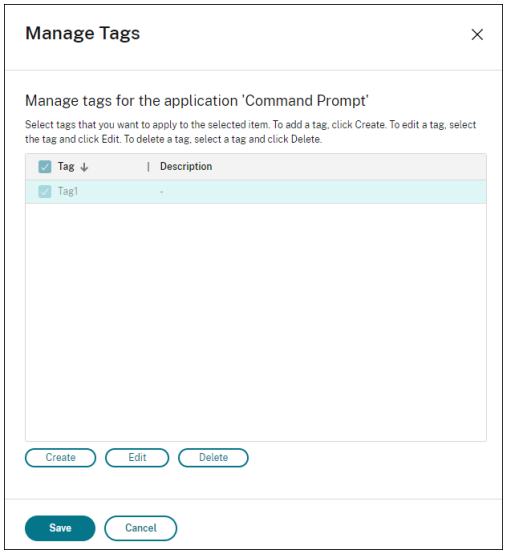
（例外：ポリシー割り当てに使用するタグは、Web Studio の ［タグの管理］操作を使用して作成、編集、削除します。ただし、タグが適用される（割り当てられる）のはポリシーの作成時です。詳しくは、「ポリシーの作成」を参照してください）。

タグによる制限は、デリバリーグループでデスクトップを作成または編集するとき、およびアプリケーショングループを作成および編集するときに構成されます。

Web Studio での［タグの管理］ダイアログの使用

Web Studio で、タグの適用先となる項目（1 つまたは複数のマシン、アプリケーション、デスクトップ、デリバリーグループ、アプリケーショングループ）を選び、操作バーで ［タグの管理］を選択します。［タグの管理］ダイアログボックスには、選択した項目のタグだけでなく、サイトで作成されたすべてのタグが表示されます。

- チェックマークが付いているチェックボックスは、選択したアイテムにタグが既に追加されていることを表します（下の画面キャプチャで、選択されたマシンには「Tag1」という名前のタグが適用されています）。
- 複数の項目を選択した場合、ハイフンを含むチェックボックスは、一部の項目（すべての項目ではない）にそのタグが追加されていることを表します。



［タグの管理］ダイアログボックスでは、以下の操作を実行できます。「タグを使用する場合の注意事項」を必ず確認してください。

- タグを作成するには：

  ［作成］をクリックします。名前と説明を入力します。タグの名前は一意でなければならず、大文字と小文字は区別されません。［**OK**］をクリックします。（タグを作成しても、選択しているアイテムに自動的に適用されることはありません。チェックボックスを使用してタグを適用します。）

- **1** つまたは複数のタグを追加（適用）するには：

  タグ名の隣にあるチェックボックスをオンにします。複数のアイテムを選択し、タグの隣のチェックボックスにハイフンが付いている場合（選択されたアイテムの一部（すべてではない）に、タグが既に適用されていることを示す）、このチェックボックスをオンにすると、選択されているすべてのマシンに影響が及びます。

1 つまたは複数のマシンにタグを追加しようとしていて、そのタグが現在アプリケーショングループの制限として使用されている場合、その操作により、それらのマシンが起動対象になることがあるという警告が表示されます。それが意図どおりであれば続行します。

- **1** つまたは複数のタグを削除するには:

  タグ名の隣にあるチェックボックスをオフにします。複数のアイテムを選択し、タグの隣のチェックボックスにハイフンが付いている場合（選択されたアイテムの一部（すべてではない）に、タグが既に適用されていることを示す）、そのチェックボックスをオフにすると、選択されているすべてのマシンからタグが削除されます。

  タグを制限として使用しているマシンからそのタグを削除しようとすると、この操作により起動対象となるマシンに影響が及ぶ可能性があるという警告メッセージが表示されます。それが意図どおりであれば続行します。

- タグを編集するには:

  タグを選択し、［編集］をクリックします。新しい名前、説明、またはその両方を入力します。同時に編集できるタグは 1 つのみです。

- **1** つまたは複数のタグを削除するには:

  タグを選択し、［削除］をクリックします。［タグの削除］ダイアログボックスに、選択したタグを現在使用しているアイテムの数が表示されます（「2 台のマシン」など）。アイテムをクリックすると、詳細が表示されます。たとえば、［2 台のマシン］というアイテムをクリックすると、そのタグを適用されている 2 台のマシンの名前が表示されます。タグを削除するかどうかを確認します。

  Web Studio を使用して、制限として使用されているタグを削除することはできません。最初にアプリケーショングループを編集してから、タグによる制限を削除するか、異なるタグを選択します。

［タグの管理］ダイアログボックスでの操作が完了したら、［保存］をクリックします。

マシンにタグが適用されているかを確認するには、左側ペインで ［デリバリーグループ］を選択します。中央ペインでデリバリーグループを選択して、操作バーで ［マシンの表示］を選択します。中央のペインでマシンを選択し、［詳細］ペインで ［タグ］タブを選択します。

タグによる制限の管理

タグによる制限の構成は複数の手順があるプロセスです。まずタグを作成し、それをマシンに追加/適用します。次に、アプリケーショングループまたはデスクトップに制限を追加します。

- タグの作成と適用:

  前述の ［タグの管理］操作を使用して、タグを作成してマシンに追加（適用）します。タグを追加したマシンには、タグによる制限の影響が生じます。

- アプリケーショングループにタグによる制限を追加するには:

  アプリケーショングループを作成または編集します。［デリバリーグループ］ページで、［タグでマシンの起動を制限します］をオンにし、一覧からタグを選択します。

- アプリケーショングループのタグによる制限を変更または削除するには:

  グループを編集します。[デリバリーグループ] ページで、異なるタグを一覧から選択するか、[タグでマシンの起動を制限します] をオフにしてタグによる制限を完全に削除します。

- デスクトップにタグによる制限を追加するには:

  デリバリーグループを作成または編集します。[デスクトップ] ページで [追加] または [編集] をクリックします。[デスクトップの追加] ダイアログボックスで、[タグでマシンの起動を制限します] をオンにし、ドロップダウンからタグを選択します。

- デリバリーグループのタグによる制限を変更または削除するには:

  グループを編集します。[デスクトップ] ページで、[編集] をクリックします。ダイアログボックスで、異なるタグを一覧から選択するか、[タグでマシンの起動を制限します] をオフにしてタグによる制限を完全に削除します。

タグを使用する場合の注意事項

項目に適用されるタグはさまざまな目的に使用できるため、タグの追加や削除が意図しない結果になる可能性があることに注意してください。タグを使用して Web Studio 検索フィールドのマシン表示を並べ替えることができます。アプリケーショングループまたはデスクトップを構成するときに、制限として同じタグを使用できます。このタグにより、タグが付いている指定されたデリバリーグループのマシンだけに起動対象が制限されます。

デスクトップまたはアプリケーショングループのタグによる制限としてタグを構成した後でマシンにタグを追加しようとすると、警告が表示されます。このタグを追加すると、そのマシンを使用して、追加のアプリケーションまたはデスクトップを起動できるようなる可能性があります。それが意図どおりであれば続行します。そうでない場合は、操作を取り消すこともできます。

たとえば、「Red」というタグによる制限を持つアプリケーショングループを作成するとします。後から、そのアプリケーショングループによって使用される同じデリバリーグループに、他のマシンをいくつか追加します。それらのマシンに「Red」というタグを追加しようとすると、次のようなメッセージが表示されます:「タグ「Red」は、次のアプリケーショングループ上の制限として使用されています。このタグを追加すると、選択されたマシンからこのアプリケーショングループのアプリケーションが起動可能になる可能性があります。」次に、それらの追加マシンへのそのタグの追加を確認またはキャンセルできます。

同様に、アプリケーショングループで起動を制限するためにタグが使用されている場合、グループを編集してタグによる制限を削除するまで、そのタグを削除できないという警告が表示されます（アプリケーショングループの制限として使用されているタグの削除を許可されている場合、アプリケーショングループに関連付けられたデリバリーグループ内のすべてのマシンでアプリケーションの起動を許可することになる可能性があります）。デスクトップ起動の制限としてタグが使用されている場合も、タグの削除は同様に不可能です。アプリケーショングループまたはデリバリーグループ内のデスクトップを編集してタグによる制限を削除すれば、タグを削除できます。

すべてのマシンが同一セットのアプリケーションを持つとは限りません。1 人のユーザーが、それぞれ異なるタグによる制限を持ち、デリバリーグループのマシン構成が異なるか重なり合っている複数のアプリケーショングループに属する場合があります。次の表に、対象マシンがどのように決まるかを示します。

アプリケーションの追加先	選択したデリバリーグループ内で起動対象となるマシン
タグによる制限を持たない 1 つのアプリケーショングループ	すべてのマシン。
タグによる制限 A を持つ 1 つのアプリケーショングループ	タグ A が適用されているマシン。
2 つのアプリケーショングループ。タグによる制限 A を持つグループとタグによる制限 B を持つグループ	タグ A とタグ B を持っているマシン。存在しない場合、タグ A またはタグ B を持っているマシン。
2 つのアプリケーショングループ。タグによる制限 A を持つグループとタグによる制限を持たないグループ	タグ A を持つマシン。存在しない場合、すべてのマシン。

マシン再起動スケジュールでタグによる制限を使用している場合、タグ適用またはタグによる制限に影響する変更はすべて、次回のマシン再起動サイクルに影響を与えます。変更の実行中に進行している再起動サイクルには影響しません

例 **2** を構成する方法

次の手順は、タグを作成、適用し、2 番目の例で示したアプリケーショングループのためにタグによる制限を構成する方法を示しています。

VDA とアプリケーションはマシンに既にインストール済み、デリバリーグループは作成済みです。

マシンにタグを作成し、適用します:

1. Web Studio でデリバリーグループ D01 を選択して、操作バーで ［マシンの表示］を選択します。
2. マシン VDA 101～105 を選択して、操作バーで ［タグの管理］を選択します。
3. ［タグの管理］ダイアログボックスで［作成］をクリックし、CADAppsという名前のタグを作成します。[**OK**] をクリックします。
4. ［作成］を再度クリックして、OfficeApps という名前のタグを作成します。[**OK**] をクリックします。
5. ［タグの管理］ダイアログボックスで、各タグ名（CADAppsおよびOfficeApps）の隣にあるチェックボックスをオンにして、新しく作成したタグを選択したマシンに追加（適用）します。完了したら、ダイアログボックスを閉じます。
6. デリバリーグループ D01 を選択して、操作バーで ［マシンの表示］を選択します。
7. マシン VDA 106～110 を選択して、操作バーで ［タグの管理］を選択します。
8. ［タグの管理］ダイアログボックスで ［作成］をクリックします。「AcctgApps」という名前のタグを作成します。[**OK**] をクリックします。
9. 各タグ名の隣にあるチェックボックスをオンにして、選択したマシンに新しく作成したAcctgAppsタグとOfficeAppsタグを適用し、ダイアログボックスを閉じます。

タグによる制限を持つアプリケーショングループを作成します。

1. Web Studio の左側のペインで［アプリケーション］を選択し、次に［アプリケーショングループ］タブを選択し、操作バーで［アプリケーショングループの作成］を選択します。アプリケーショングループの作成ウィザードが起動します。
2. ウィザードの［デリバリーグループ］ページで、デリバリーグループ D01 を選択します。［タグでマシンの起動を制限します］をオンにし、一覧から`AcctgApps`タグを選択します。
3. 会計ユーザーと会計アプリケーションを指定して、ウィザードを完了します（アプリケーションを追加するときに［[スタート］メニューから］を選択すると、`AcctgApps`タグが適用されているマシン上にあるアプリケーションが検索されます）。［概要］ページで、グループに`A100`という名前を付けます。
4. 前の手順を繰り返してアプリケーショングループ`A200`を作成し、`CADApps`タグを持っているマシンと、適切なユーザーおよびアプリケーションを指定します。
5. 手順を繰り返してアプリケーショングループ`A300`を作成し、`OfficeApps`タグを持っているマシンと、適切なユーザーおよびアプリケーションを指定します。

マシンカタログのタグ

マシンカタログでタグを使用できます。タグを作成してカタログに適用する全体的な手順は、前述のとおりです。ただし、カタログへのタグの適用は、PowerShell インターフェイスを介してのみサポートされます。Web Studio を使用して、タグをカタログに適用したり、カタログからタグを削除したりすることはできません。Web Studio のカタログ表示では、タグが適用されているかどうかは示されません。

概要：Web Studio または PowerShell を使用して、カタログで使用するタグを作成または削除できます。タグをカタログに適用するには、PowerShell を使用します。

カタログでタグを使用する例を次に示します：

- デリバリーグループには複数のカタログのマシンがありますが、操作（再起動スケジュールなど）を特定のカタログ内のマシンのみに適用する必要があります。該当するカタログにタグを適用することで、それが実現します。
- アプリケーショングループで、アプリケーションセッションを特定のカタログ内のマシンに制限する必要があります。該当するカタログにタグを適用することで、それが実現します。

影響を受ける PowerShell コマンドレット：

- `Add-BrokerTag`や`Remove-BrokerTag`などのコマンドレットにカタログオブジェクトを渡すことができます。
- `Get-BrokerTagUsage`で、タグを含むカタログの数が表示されます。
- `Get-BrokerCatalog`には`Tags`というプロパティがあります。

たとえば、次のコマンドレットにより、`fy2018`という名前のタグが`acctg`という名前のカタログに追加されます：`Get-BrokerCatalog -Name acctg | Add-BrokerTag fy2018`（タグは以前に Web Studio または PowerShell を使用して作成されました。）

ガイダンスと構文について詳しくは、PowerShell コマンドレットのヘルプを参照してください。

自動タグ（プレビュー）

自動タグ付けにより、管理者はカスタムルールに基づいて、さまざまな Citrix Virtual Apps and Desktops オブジェクトのタグを自動的に設定したり削除したりできます。この機能拡張により、環境の最適化のために定期的に実行されるさまざまなスクリプトを保持する必要がなくなります。

使用例

自動タグ付けを使用すると、コストの削減、インフラストラクチャの最適化、消費の促進など、ビジネスの推進要因に関連する規則を実装できます。以下にユースケースの一部を示します。

- 未使用の **VDI** を解放する - 使用されていない期間が事前に構成された日数を超えている専用ワークロードを、使用可能なプールにリリースします。
- 余分なアプリを削除する - 使用されていない期間が事前に構成された日数を超えているアプリケーションを特定して、余分なアプリケーションを削減します。
- **X** 未満の機能レベルを持つ **DG** - 特定の機能レベル未満のデリバリーグループを見つけます。
- 非アクティブなユーザー - ログオンしていない期間が事前に構成された日数を超えているユーザーのリソースを解放します。

PowerShell コマンド

PowerShell コマンドを使用して自動タグを作成できます。自動タグの規則が作成されると、600 秒の頻度で評価されます。詳しくは、「New-BrokerAutoTagRule」を参照してください。

例　`New-BrokerAutoTagRule`は、`Get-BrokerMachine`コマンドレットと同じオブジェクトタイプとフィルターパラメーターを使用します。詳しくは、「GetBrokerMachine」を参照してください。

1. 30 日以上使用されていない専用 VDI に ID 123 のタグを付けます。

    a) 未使用の VDI にタグ付けするためのタグ（例：**unused-VDI**）を定義します。

    - タグ名：unused-VDI
    - タグ ID： 123

    b) 未使用のマシンにタグを付ける自動タグ付け規則を作成します。規則のパラメーターを定義します。

    - 名前：規則の汎用名。
    - オブジェクトの種類：マシン。
    - 規則テキスト：静的な割り当て済みのマシンで、最終接続時から 30 日を超えているか、その値がない。
    - タグ UID： 関連付けようとするタグ ID、123。


```
New-BrokerAutoTagRule -Name 'UnusedVdi' -ObjectType 'Machine
' -RuleText "-AllocationType Static -IsAssigned $true -
Filter { SummaryState -ne `"InUse`" -and ( LastConnectionTime
 -lt '-30' -or LastConnectionTime -eq `$null )} " -TagUid
123
```

c) **unused-VDI** タグが付いているマシンを確認し、リリースします。

2. X 未満の機能レベルでデリバリーグループにタグを付ける場合（**L7_20** をしきい値機能レベルとして使用）:

```
New-BrokerAutoTagRule -Name 'LowFL'-ObjectType 'DesktopGroup'-RuleText
 "-Filter { MinimumFunctionalLevel -lt 'L7_20' } "-TagUid 123
```

1. フォルダーを使用せずに公開された、ユーザーに表示されるアプリにタグを付ける場合:

```
New-BrokerAutoTagRule -Name 'NoFolder'-ObjectType 'Application'-
RuleText "-Enabled $true -Filter { ClientFolder -eq $null )} "-TagUid
 123
```

追加情報

ブログ記事: How to Assign Desktops to Specific Servers。

ユーザープロファイル

August 17, 2024

デフォルトでは、マスターイメージ上に Virtual Delivery Agent をインストールするときに Citrix Profile Management が自動的にインストールされます。ただし、プロファイル管理ツールとして Profile Management を常に使用しなければならないということではありません。

ユーザーのニーズに応じて Citrix Virtual Apps and Desktops ポリシーを構成して、各デリバリーグループ内のマシンに異なるプロファイル処理を適用できます。たとえば、あるデリバリーグループではネットワーク上の特定の場所にテンプレートが格納される Citrix 固定プロファイルを使用して、別のデリバリーグループではいくつかのリダイレクトフォルダーと共に別の場所に格納される Citrix 移動プロファイルを使用するポリシーを構成できます。

- 組織内のほかの管理者が Citrix Virtual Apps and Desktops ポリシーを管理する場合は、すべてのデリバリーグループにプロファイル関連のポリシーが正しく適用されるように共同で作業する必要があります。
- Profile Management ポリシーは、グループポリシーや Profile Management の INI ファイルで設定したり、各仮想マシン上でローカルに設定したりできます。これらの設定は、以下の順に読み取られます。

  1. グループポリシー（ADM または ADMX ファイル）

2.［ポリシー］ノードにある Citrix Virtual Apps and Desktops ポリシー
3. ユーザーが接続する仮想マシン上のローカルポリシー
4. Profile Management の INI ファイル

たとえば、グループポリシーと［ポリシー］ノードの両方で同じポリシーを構成する場合、グループポリシーのポリシー設定が適用され、Citrix Virtual Apps and Desktops ポリシー設定は無視されます。

いずれのプロフィル処理でも、Director 管理者はユーザープロファイルの診断情報にアクセスしたりトラブルシューティングを行ったりできます。詳しくは、Directorのドキュメントを参照してください。

自動構成

デスクトップの種類は、インストールされている Virtual Delivery Agent に基づいて自動的に検出され、それに応じて Studio での構成オプションや Profile Management のデフォルトの動作が設定されます。

Profile Management で設定されるポリシーは、以下の表のとおりです。ポリシーの非デフォルトの設定は保持され、この機能で上書きされることはありません。各ポリシーについて詳しくは、Profile Management のドキュメントを参照してください。プロファイルを作成するマシンの種類により、調整されるポリシーが異なります。最初の要因は、マシンの種類が固定なのかプロビジョニングなのかという点です。次の要因は、それが複数のユーザーによって共有されるのか特定のユーザーに専用のものなのかという点です。

固定システムにはある種のローカルストレージが備わっていて、システムの電源がオフになってもシステムの内容を維持することができます。固定システムでは、ローカルディスクとして SAN のようなストレージテクノロジを使用できます。これと対照的に、プロビジョニングシステムは基本ディスクとある種の ID ディスクから「オンザフライ」で作成されます。通常、RAM ディスクまたはネットワークディスクがローカルストレージとして使用され、ネットワークディスクはしばしば高速リンクの SAN によって提供されます。プロビジョニングテクノロジとは、一般的に Citrix Provisioning または Machine Creation Services（またはサードパーティの同等物）を指します。場合により、プロビジョニングされたシステムが固定ローカルストレージを伴うことがあります。この場合は固定システムとして分類されます。

これらの 2 つの要因により、以下の種類のマシンが定義されます:

- 固定かつ専用。静的に割り当てられ固定ローカルストレージを持つ Machine Creation Services で作成されるシングルセッション OS マシン、物理的ワークステーション、およびノートブックコンピューターなど。
- 固定かつ共有。Machine Creation Services で作成されるマルチセッション OS マシン、Citrix Virtual Apps サーバーなど。
- プロビジョニングかつ専用。静的に割り当てられるが固定ストレージを持たない、（Citrix Virtual Desktops の）Citrix Provisioning Services で作成されるシングルセッション OS マシンなど。
- プロビジョニングかつ共有。ランダムに割り当てられる、（Citrix Virtual Desktops の）Citrix Provisioning Services で作成されるシングルセッション OS マシン、Citrix Virtual Apps サーバーなど。

次の表は、各種類のマシンに適した Profile Management ポリシー設定を示しています。通常、これらの設定は効果的ですが、必要に応じて変更した方がよい場合もあります。

> 重要:
>
> ［ログオフ時にローカルでキャッシュしたプロファイルの削除］、［プロファイルストリーム配信］、および ［常時キャッシュ］は自動構成機能により設定されます。ほかのポリシー設定は、必要に応じて手作業で変更してください。

固定マシン

ポリシー	固定かつ専用	固定かつ共有
ログオフ時にローカルでキャッシュしたプロファイルの削除	無効	有効
プロファイルストリーミング	無効	有効
常時キャッシュ	有効（注 1）	無効（注 2）
アクティブライトバック	無効	無効（注 3）
ローカル管理者のログオン処理	有効	無効（注 4）

プロビジョニングされたマシン

ポリシー	プロビジョニングかつ専用	プロビジョニングかつ共有
ログオフ時にローカルでキャッシュしたプロファイルの削除	無効（注 5）	有効
プロファイルストリーミング	有効	有効
常時キャッシュ	無効（注 6）	無効
アクティブライトバック	有効	有効
ローカル管理者のログオン処理	有効	有効（注 7）

1. このマシンの種類では ［プロファイルストリーム配信］が無効なため、［常時キャッシュ］設定は常に無視されます。
2. ［常時キャッシュ］は無効にします。ただし、このポリシー設定を有効にして制限サイズ（MB）を指定すると、ログオン後すぐにサイズの大きなファイルがプロファイルにロードされるようになります。制限サイズ以上のすべてのファイルは、すぐにローカルにキャッシュされます。
3. ［アクティブライトバック］は無効にします。ただし、Citrix Virtual Apps サーバー間を移動するユーザーのプロファイルの変更を保存する場合は、このポリシー設定を有効にします。
4. ［ローカル管理者のログオン処理］は無効にします。ただし、ホスト共有デスクトップの場合は、このポリシー設定を有効にします。

5. ［ログオフ時にローカルでキャッシュしたプロファイルの削除］は無効にします。この設定により、ローカルにキャッシュされたプロファイルが保持されます。各マシンが個々のユーザーに割り当てられているため、ログオフ時にマシンがリセットされても、プロファイルのキャッシュによりすばやくログオンできるようになります。
6. ［常時キャッシュ］は無効にします。ただし、このポリシー設定を有効にして制限サイズ（MB）を指定すると、ログオン後すぐにサイズの大きなファイルがプロファイルにロードされるようになります。制限サイズ以上のすべてのファイルは、すぐにローカルにキャッシュされます。
7. ［ローカル管理者のログオン処理］は有効にします。ただし、Citrix Virtual Apps and Desktops サーバー間を移動するユーザーのプロファイルに対しては、このポリシー設定を無効にします。

フォルダーのリダイレクト

フォルダーリダイレクトを有効にすると、ユーザーデータをユーザープロファイルとは異なるネットワーク共有上に格納できます。これにより、プロファイルのサイズが小さくなるため短時間でロードされるようになりますが、ネットワーク帯域幅が消費されます。フォルダーリダイレクト機能では、Citrix ユーザープロファイルを使用する必要はありません。管理者は独自にユーザーのプロファイルを管理して、フォルダーをリダイレクトできます。

フォルダーリダイレクトを構成するには、Studio で Citrix ポリシーを使用します。

- フォルダーのリダイレクト先のネットワーク共有が使用可能であり、適切なアクセス権が設定されていることを確認します。リダイレクト先のプロパティは自動的に検証されます。
- リダイレクト先のネットワーク共有をセットアップすると、ユーザーの次回ログオン時にプロファイルがリダイレクトされます。

フォルダーリダイレクト機能は、Citrix ポリシーまたは Active Directory グループポリシーオブジェクトのいずれか一方のみを使用して構成してください。両方のポリシーエンジンを使用すると、予期しない問題が発生することがあります。

詳細なフォルダーリダイレクト

複数のオペレーティングシステムが混在する展開環境では、ユーザープロファイルの一部がすべてのオペレーティングシステムで共有されるように構成できます。プロファイルの残りの部分は共有されず、単一のオペレーティングシステムでのみ使用されます。異なるオペレーティングシステム上で一貫したユーザーエクスペリエンスを提供するには、オペレーティングシステムごとに異なる構成（詳細なフォルダーリダイレクト）が必要です。たとえば、2 つのオペレーティングシステム上で使用される異なるバージョンのアプリケーションで共通のファイルがロードされるようにするには、そのファイルをネットワーク上の単一の場所にリダイレクトします。また、［スタートメニュー］フォルダーの構造が 2 つのオペレーティングシステムで異なる場合は、どちらか一方のオペレーティングシステムのフォルダーのみがリダイレクトされるように設定できます。これにより、各オペレーティングシステムで ［スタートメニュー］フォルダーおよびその内容が分離され、ユーザーに一貫したエクスペリエンスを提供できます。

詳細なフォルダーリダイレクトを使用する場合は、ユーザープロファイル内のデータ構造を理解して、どの部分をオペレーティングシステム間で共有できるかを確認する必要があります。フォルダーリダイレクトを正しく使用しないと、予期しない問題が発生する可能性があります。

詳細なフォルダーリダイレクトを使用するには、以下のタスクを行います。

- 各オペレーティングシステムで異なるデリバリーグループを使用します。
- 配信する仮想アプリケーション（仮想デスクトップ上のものを含む）がユーザーのデータや設定をどこに格納するか、およびそのデータ構造を確認します。
- 移動可能な共有プロファイルデータ（異なるオペレーティングシステムでも構造が同じデータ）を含んでいるフォルダーを、各デリバリーグループでリダイレクトされるように設定します。
- 共有できないプロファイルデータについては、1 つのデリバリーグループでのみリダイレクトされるように設定します。通常、使用頻度の高いオペレーティングシステムやより実用的なデータのデリバリーグループでリダイレクトを設定します。または、共有できないプロファイルデータを含んでいるフォルダーを、オペレーティングシステムごとに異なるネットワーク共有にリダイレクトすることもできます。

高度なフォルダーリダイレクトの例

この例では、Windows 10 と Windows Server 2019 で異なるバージョンの Microsoft Outlook と Internet Explorer がインストールされている場合について説明します。これら 2 つのオペレーティングシステム用に 2 つのデリバリーグループをセットアップします。ユーザーがこれらのアプリケーションで共通の「連絡先」と「お気に入り」にアクセスできるようにするには、詳細なフォルダーリダイレクトを以下のように構成します。

重要：ここで説明する内容は、上記のオペレーティングシステムおよび配信環境での例であり、実際の環境ではさまざまな要因によりフォルダー構造が異なる場合があります。

- これらのデリバリーグループに適用するポリシーで、以下のフォルダーをリダイレクトします。

フォルダー	Windows 10 でリダイレクト?	Windows Server 2019 でリダイレクト?
マイドキュメント	はい	はい
アプリケーションデータ	いいえ	いいえ
連絡先	はい	はい
デスクトップ	はい	いいえ
ダウンロード	いいえ	いいえ
お気に入り	はい	はい
リンク	はい	いいえ
マイミュージック	はい	はい
マイピクチャ	はい	はい

フォルダー	Windows 10 でリダイレクト?	Windows Server 2019 でリダイレクト?
マイビデオ	はい	はい
検索	はい	いいえ
保存したゲーム	いいえ	いいえ
［スタート］メニュー	はい	いいえ

- オペレーティングシステム間で共有されるフォルダーをリダイレクトする場合、以下の点に注意してください。
  - 「連絡先」フォルダーと「お気に入り」フォルダーのリダイレクトを設定する前に、異なるバージョンの Outlook と Internet Explorer でユーザーデータのフォルダー構造を確認してください。
  - 「マイドキュメント」、「マイミュージック」、「マイピクチャ」、および「マイビデオ」の各フォルダーの構造はこれらのオペレーティングシステムで共通です。そのため、両方のデリバリーグループで同じネットワーク共有にリダイレクトできます。
- オペレーティングシステム間で共有できないフォルダーをリダイレクトする場合、以下の点に注意してください。
  - 「デスクトップ」、「リンク」、「検索」、および「スタートメニュー」の各フォルダーの構造はこれらのオペレーティングシステムで異なるため、Windows Server 2008 用のデリバリーグループではリダイレクトされないように設定します。これにより、これらのデータは共有されなくなります。
  - 予期せぬ問題の発生を避けるため、これらのフォルダーは Windows 10 用のデリバリーグループでのみリダイレクトします。Windows 10 は、日々の作業でユーザーがより頻繁に使用します。ユーザーが Windows Server によって提供されるアプリケーションにアクセスすることは、あまり多くありません。また、これらのデータは、アプリケーション環境よりもデスクトップ環境のものの方が実用的です。たとえば、デスクトップ上のショートカットは「デスクトップ」フォルダーに格納されるため、Windows Server マシンよりも Windows 10 マシンのデスクトップショートカットをリダイレクトした方が便利です。
- 以下のフォルダーは、オペレーティングシステム間での共有に向いていません。
  - ユーザーがダウンロードしたファイルがサーバー上にコピーされるのを防ぐため、「ダウンロード」フォルダーはリダイレクトしません。
  - 個々のアプリケーションのデータにより互換性やパフォーマンス上の問題が生じることがあるので、「アプリケーションデータ」フォルダーはリダイレクトしません。

フォルダーリダイレクトについて詳しくは「フォルダーリダイレクト、オフラインファイル、および移動ユーザープロファイルの概要」を参照してください。

フォルダーリダイレクトと除外設定

Studio ではなく Citrix Profile Management を使用する場合は、一部のユーザープロファイルフォルダーに対して除外規則を設定して、パフォーマンスを向上できます。この機能を使用する場合は、リダイレクトされるフォルダーに対して除外規則を設定しないでください。フォルダーのリダイレクト機能と除外機能は連携して機能します。リダイレクトされるフォルダーが Profile Management の処理から除外されないようにしてください。これにより、後でリダイレクト機能を無効にしてもユーザープロファイルフォルダー構造の整合性が保持されます。除外について詳しくは、「項目の包含および除外」を参照してください。

VDA 登録

August 17, 2024

はじめに

> 注:
>
> オンプレミス環境で VDA を Delivery Controller に登録します。Citrix Cloud サービス環境で VDA を Cloud Connector に登録します。ハイブリッド環境では、一部の VDA が Delivery Controller に登録し、それ以外は Cloud Connector に登録する場合があります。

VDA を使用するには、そのサイトの 1 つまたは複数の Controller または Cloud Connector に登録（接続を確立）する必要があります。VDA は`ListofDDCs`と呼ばれる一覧をチェックして Controller または Connector を見つけます。VDA の`ListOfDDCs`には、その VDA をサイトの Controller または Cloud Connector にポイントする DNS エントリが含まれています。負荷分散のため、VDA は一覧のすべての Controller または Cloud Connector で接続を自動的に分散させます。

VDA 登録が重要な理由

- セキュリティの観点から、登録は慎重に行う必要があります。Controller または Cloud Connector と VDA 間の接続を確立することになるからです。このように注意が必要な操作では、不完全なものが 1 つでもあればその接続を拒否する必要があります。実際には、2 つの個別の通信チャネル（VDA から Controller または Cloud Connector、Controller または Cloud Connector から VDA）を確立することになります。接続では Kerberos が使用されるため、時刻の同期およびドメインへの参加に関する問題は見過ごせないものになります。Kerberos ではサービスプリンシパル名（SPN）が使用されるため、負荷分散された IP やホスト名は使用できません。
- Controller または Cloud Connector の追加および削除は、VDA に正確かつ最新の Controller（または Cloud Connector）の情報が設定されていないと、未登録の Controller または Cloud Connector により仲介されたセッションの起動が VDA により拒否される場合があります。また、無効なエントリにより、仮想

デスクトップシステムソフトウェアの起動に遅延が生じることがあります。VDA では、信頼されていない不明な Controller または Cloud Connector からの接続は受け入れられません。

ListofDDCsに加えて、ListOfSIDs（セキュリティ ID）により、ListofDDCsに記載されているどのマシンを信頼するかが指定されます。ListofSIDsは、Active Directory での負荷を軽減したり、改ざんされた DNS サーバーからのセキュリティ上の脅威を防いだりするために使用できます。詳しくは、「ListOfSIDs」を参照してください。

ListofDDCsに複数の Controller または Cloud Connector が指定されている場合、VDA はランダムな順序で接続を試行します。オンプレミスの展開では、ListofDDCsには Controller のグループを含めることもできます。VDA は、これらのグループ内の各 Controller への接続を試行し、その後ListofDDCsのほかのエントリを試行します。

Citrix Virtual Apps and Desktops では、VDA のインストール中に構成済みの Controller または Cloud Connector に対する接続が自動でテストされます。Controller または Cloud Connector に接続できない場合は、エラーが表示されます。Controller または Cloud Connector に接続できないことを示す警告を無視した場合（または VDA のインストール中に Controller または Cloud Connector のアドレスを指定しなかった場合）は、メッセージが表示されます。

Controller または **Cloud Connector** のアドレスの構成方法

VDA の初めての登録時（初回登録と呼びます）に、管理者は使用する構成方法を選択します。初回登録中に、VDA 上に永続キャッシュが作成されます。以降の登録では、構成の変更が検出されない限り、VDA はこのローカルキャッシュから Controller または Cloud Connector のリストを取得します。

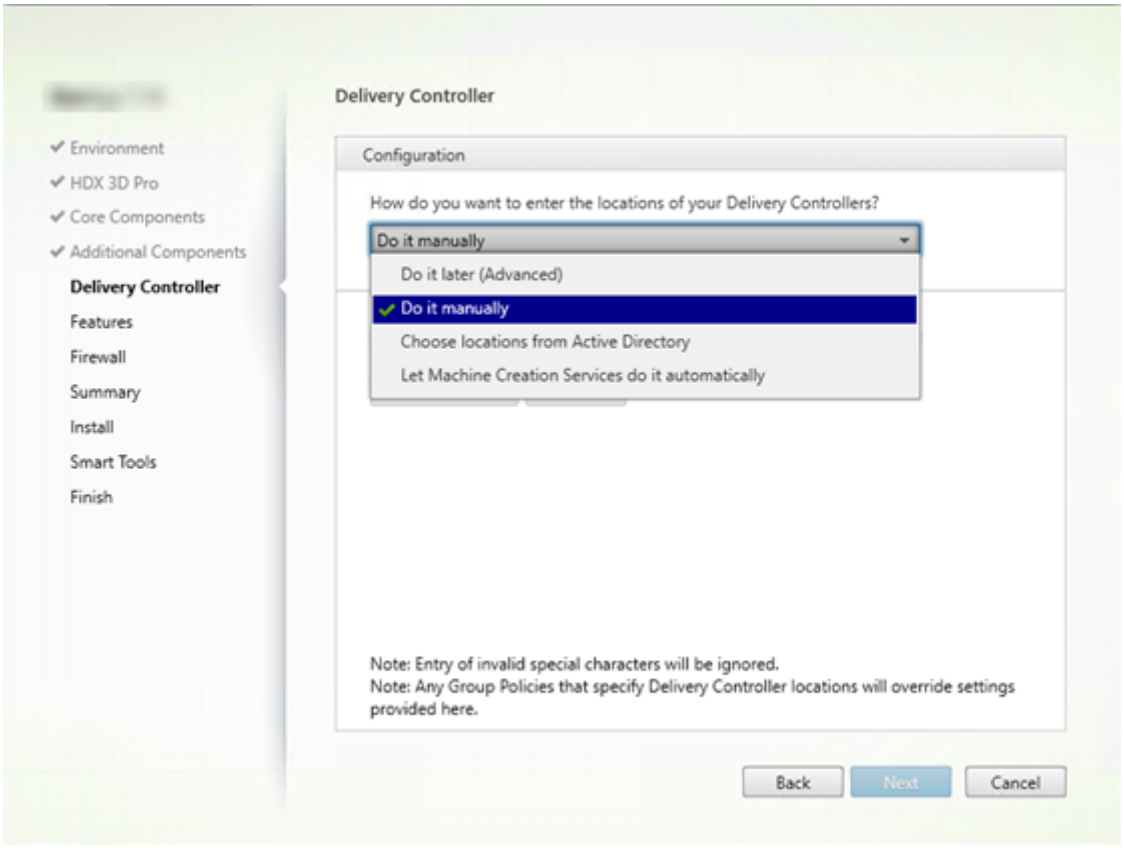
以降の登録時にこのリストを取得する一番簡単な方法は、自動更新機能を使用することです。自動更新はデフォルトで有効になっています。詳しくは、「自動更新」を参照してください。

VDA で Controller または Cloud Connector のアドレスを構成する方法は複数存在します。

- ポリシーベース（LGPO または GPO）
- レジストリベース（手動、グループポリシーの基本設定（GPP）、VDA のインストール中に指定）
- Active Directory の OU ベース（旧 OU 検出）
- MCS ベース（personality.ini）

VDA をインストールするときに初回登録の方法を指定します（自動更新を無効にすると、初回以降の登録で VDA のインストール時に選択した方法が使用されます）。

次の画像に、VDA インストールウィザードの ［**Delivery Controller**］ページを示します。



ポリシーベース（**LGPO** または **GPO**）

VDA の初回登録では GPO を使用することを Citrix ではお勧めします。この方法が最優先です（リスト上では自動更新が最優先となっていますが、自動更新は初回登録後にのみ使用します）。ポリシーベースの登録には、構成にグループポリシーを使用できるという集中化のメリットがあります。

この方法を指定するには、次の手順の両方を実行します。

- VDA インストールウィザードの［**Delivery Controller**］ページで、［あとで実行（上級）］を選択します。VDA のインストール中に Controller のアドレスの指定は行いませんが、ウィザードからこれらのアドレスを指定するように複数回促されます（VDA の登録が非常に重要なためです）。
- `Virtual Delivery Agent Settings > Controllers`設定で、Citrix ポリシーを使用してポリシーベースの VDA 登録を有効化または無効化します（セキュリティが最優先の場合、`Virtual Delivery Agent Settings > Controller SIDs`設定を使用します）。

この設定は`HKLM\Software\Policies\Citrix\VirtualDesktopAgent (ListOfDDCs)`に格納されています。

レジストリ ベース

この方法を指定するには、次の手順のいずれかを実行します。

- VDA インストールウィザードの ［**Delivery Controller**］ページで、［手動で指定する］を選択します。次に、インストール済みの Controller の完全修飾ドメイン名を入力し、［追加］をクリックします。追加の Controller をインストールした場合は、アドレスも追加します。
- コマンドラインでの VDA のインストールの場合は、/controllers オプションを使用してインストール済みの Controller または Cloud Connector の FQDN を指定します。

この情報は、レジストリキー`HKLM\Software\Citrix\VirtualDesktopAgent`または`HKLM\Software\Wow6432Node\Citrix\VirtualDesktopAgent`のレジストリ値`ListOfDDCs`に格納されています。

また、このレジストリキーを手動で構成するか、グループポリシーの基本設定（GPP）を使用することもできます。この方法は、Controller または Cloud Connector 別に条件付きの処理を行う（例: コンピューター名が XDW-001-から始まる場合は XDC-001 を使用する）場合などは、ポリシーベースの方法よりも適しています。

サイトのすべての Controller または Cloud Connector の完全修飾ドメイン名の一覧が設定されている、`ListOfDDCs`レジストリキーを更新します。（このキーは Active Directory サイトの組織単位に相当します）。

`HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent\ListOfDDCs` （`REG_SZ`）

レジストリ`HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent`に`ListOfDDCs`と`FarmGUID`のキーが両方ある場合、`ListOfDDCs`が Controller または Cloud Connector の検出に使用されます。`FarmGUID`は、VDA のインストール時にサイト組織単位を指定した場合に作成されます（このキーは古い展開環境で使用する場合があります）。

オプションで、`ListOfSIDs`レジストリキーを更新します（詳しくは「ListOfSID」を参照してください）:

`HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent\ListOfSIDs` （`REG_SZ`）

注: Citrix ポリシーによりポリシーベースの VDA 登録も有効化している場合は、ポリシーベースの方法の方が優先度が高いため、VDA のインストール時に指定した設定がポリシーベースの設定で上書きされます。

Active Directory の **OU** ベース（旧）

この方法は主として後方互換性のためにサポートされているものであり、推奨されていません。現在もこの方法を使用している場合は、別の方法に変えることを Citrix ではお勧めします。

この方法を指定するには、次の手順の両方を実行します。

- VDA インストールウィザードの ［**Delivery Controller**］ページで、［**Active Directory** から場所を選択する］を選択します。

- Set-ADControllerDiscovery.ps1スクリプトを使用します（各 Controller 上にあります）。また、各 VDA 上のFarmGuidレジストリを、適切な組織単位を指すように構成します。この設定はグループポリシーを使用して行うことができます。

MCS ベース

VM のプロビジョニングに MCS を使用する場合は、MCS は Controller または Cloud Connector の一覧を設定します。この機能は自動更新と連携します。マシンカタログの作成時、MCS は初回プロビジョニングで Controller または Cloud Connector の一覧をPersonality.iniファイルに書き込みます。自動更新により、この一覧が最新状態に保たれます。

この方法を使用する場合は、VDA インストールウィザードの ［**Delivery Controller**］ページで、［**Machine Creation Services** で指定する］を選択します。

レビューと推奨事項

ベストプラクティス：

- 初回登録にはグループポリシーによる登録方法を使用します。
- 自動更新（デフォルトで有効化されています）を使用して Controller のリストを最新に保ちます。
- マルチゾーン展開（Controller または Cloud Connector が 2 つ以上）では、初回構成にグループポリシーを使用します。各ゾーンにローカルの Controller または Cloud Connector に対して VDA をポイントします。自動更新を使用して、VDA を最新の状態に保ちます。自動更新により、サテライトゾーンにある VDA のListofDDCsが自動で最適化されます。
- Controller が利用不能な場合に登録の問題が発生しないようにするため、ListOfDDCsレジストリキーで複数の Controller をスペースで区切って指定します。例：

```
DDC7x.xd.local DDC7xHA.xd.local

32-bit: HKEY_LOCAL_MACHINE \Software\Citrix\VirtualDesktopAgent\
    ListOfDDCs

HKEY_LOCAL_MACHINE \Software\Citrix\VirtualDesktopAgent\
    ListOfDDCs (REG_SZ)
```

- 起動時に登録がすみやかに行われるようにするため、ListofDDCsに指定する値はすべて有効な完全修飾ドメイン名と対応させてください。

自動更新

自動更新（XenApp および XenDesktop 7.6 で導入）は、デフォルトで有効化されています。これは、VDA 登録を最新の状態に保つ最も効率的な方法です。初回登録では自動更新は使用しませんが、自動更新ソフトウェアにより、

初回登録を行うときにListofDDCsがダウンロードされ、永続キャッシュに格納されます。このプロセスは、VDA ごとに実行されます。このキャッシュには、マシンポリシーの情報も格納されます。これにより、再起動後もポリシー設定が保持されます。

MCS または Citrix Provisioning を使用してマシンをプロビジョニングする場合、自動更新がサポートされます。Citrix Provisioning サーバーのキャッシュは除外されます。これは、自動更新キャッシュ用の永続的なストレージがないためです。

この方法を指定するには次の手順を実行します。

- Virtual Delivery Agent Settings > Enable auto update of Controllers 設定が含まれる Citrix ポリシーで自動更新を有効または無効にします。この設定項目は、デフォルトで有効になっています。

自動更新の仕組みは次のとおりです。

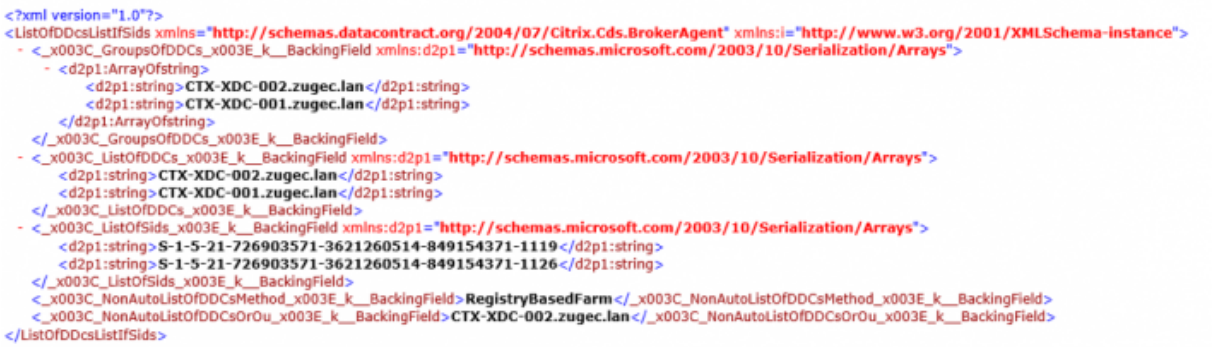
- VDA の再登録の度（マシンの再起動後など）にキャッシュが更新されます。また、各 Controller または Cloud Connector も 90 分ごとにサイトのデータベースをチェックします。最後のチェック以降に Controller または Cloud Connector が追加または削除されていた場合、または VDA 登録に影響するポリシー変更が行われていた場合、Controller または Cloud Connector から Controller または Cloud Connector に登録済みの VDA に最新のリストが送信され、キャッシュが更新されます。VDA は、最近キャッシュ化されたリストに含まれているすべての Controller または Cloud Connector からの接続を受け入れます。
- VDA が受信したリストに登録先の Controller または Cloud Connector が含まれていない場合（つまり、その Controller または Cloud Connector がサイトから削除された場合）、ListofDDCsのいずれかの Controller または Cloud Connector に VDA が再登録されます。

例：

- 環境内に 3 つの Controller A、B、C があります。VDA は（VDA のインストール時に指定した）Controller B に登録されています。
- その後、サイトに 2 つの Controller（D および E）を追加します。90 分以内に、更新されたリストが VDA に送信されます。これにより、VDA は Controller A、B、C、D、E からの接続を受け入れるようになります（VDA を再起動するまでは、すべての Controller 間で負荷分散は行われません）。
- さらにそのあとで、Controller B を別のサイトに移動します。前回のチェック以降にサイトの Controller に変更があったため、元のサイトの VDA は 90 分以内に更新済みのリストを受信します。初めに Controller B（リストから削除されています）に登録されていた VDA は、現在のリストに含まれる Controller（A、C、D、E）のいずれかに再登録されます。

マルチゾーン展開のサテライトゾーンでは、まず自動更新によりすべてのローカル Controller がキャッシュ化されます。プライマリゾーンの Controller はすべて、バックアップグループにキャッシュ化されます。サテライトゾーンのローカル Controller を利用できない場合、プライマリゾーンの Controller への登録が試みられます。

以下の例に示すように、キャッシュファイルにはホスト名およびセキュリティ ID のリスト（ListofSIDs）が含まれています。VDA は SID を照会しないため、Active Directory の負荷が抑えられます。



このキャッシュファイルは、WMI 呼び出しを使用することで取得できます。ただし、このファイルは SYSTEM アカウントのみが読み取り可能な場所に格納されています。

> 重要:
>
> この情報は説明のみを目的として紹介しています。このファイルは変更しないでください。このファイルまたはフォルダーを変更すると、構成はサポート対象外となります。

```
Get-WmiObject -Namespace "Root\Citrix\DesktopInformation"-Class "
Citrix_VirtualDesktopInfo"-Property "PersistentDataLocation"
```

セキュリティ上の理由で（Active Directory の負荷の抑制とは異なる理由で）`ListofSIDs`を手動で構成する必要がある場合、自動更新は使用できません。詳しくは、「ListOfSIDs」を参照してください。

自動更新の優先度の例外

通常、自動更新はすべての VDA 登録方法の中で最も優先度が高くなっており、ほかの方法の設定を上書きしますが、例外も存在します。キャッシュの`NonAutoListOfDDCs`要素により、初回の VDA 構成方法が指定されます。自動更新ではこの情報を監視しています。初回登録の方法が変更されると、登録プロセスでは自動更新が省略され、優先度が次に高く構成されている方法が使用されます。このプロセスは、（障害復旧時など）VDA を別のサイトに移動する場合に役立ちます。

構成に関する考慮事項

一般的な VDA 登録の構成をご覧ください。

これは埋め込みビデオです。リンクをクリックしてビデオを見る

VDA 登録の手順をご覧ください。

これは埋め込みビデオです。リンクをクリックしてビデオを見る

VDA 登録に影響を与える可能性のある設定を構成するときは、次の点を考慮してください。

Controller または **Cloud Connector** のアドレス

Controller または Cloud Connector の指定に使用する方法にかかわらず、Citrix では FQDN アドレスを使用することをお勧めします。IP アドレスは DNS レコードよりも侵害されやすいため、信頼性の高い構成とは言えません。`ListofSIDs`を手動で入力する場合は、`ListofDDCs`の IP を使用できます。ただし、この場合でも FQDN が推奨されています。

負荷分散

前述のとおり、VDA は`ListofDDCs`に含まれるすべての Controller または Cloud Connector で接続を自動的に分散させます。フェールオーバーおよび負荷分散機能は、Citrix Brokering Protocol（CBP）に組み込まれています。構成内で複数の Controller または Cloud Connector を指定する場合、登録では必要に応じてこれらの Controller または Cloud Connector 間で自動的にフェールオーバーが行われます。自動更新を使用すると、すべての VDA で自動フェールオーバーが自動的に行われます。

セキュリティ上の理由から、Citrix ADC などのネットワークロードバランサーは使用できません。VDA 登録では Kerberos 相互認証を使用しており、クライアント（VDA）はその身元をサービス（Controller）に対して証明する必要があります。また、Controller または Cloud Connector はその身元を VDA に対して証明する必要があります。つまり、VDA と Controller または Cloud Connector は、サーバーであるのと同時にクライアントとしても動作するということです。本記事の初めに述べたように、通信チャネルには、VDA から Controller/Cloud Connector と Controller/Cloud Connector から VDA の 2 つが存在します。

このプロセスのコンポーネントはサービスプリンシパル名（SPN）と呼ばれ、Active Directory コンピューターオブジェクトにプロパティとして格納されます。VDA は、Controller または Cloud Connector に接続する場合、通信相手を指定する必要があります。このアドレスが SPN です。負荷分散 IP を使用する場合、Kerberos 相互認証では、この IP が目的の Controller または Cloud Connector に属していないことが適切に認識されます。

詳しくは、次のトピックを参照してください:

- Kerberos の概要
- Kerberos を使用した相互認証

CNAME から自動更新への移行

自動更新機能は、バージョン 7.x 以前の XenApp および XenDesktop の CNAME（DNS エイリアス）機能に代わるものです。XenApp および XenDesktop 7 以降では、CNAME 機能は無効になっています。CNAME の代わりに自動更新を使用してください（CNAME を使用する必要がある場合は、CTX137960を参照してください。DNS エイリアスの動作の一貫性を保つため、自動更新と CNAME の両方を同時に使用しないでください）。

Controller/Cloud Connector グループ

特定のシナリオでは、優先グループと、すべての Controller/Cloud Connector で障害が発生した場合のフェールオーバーに使用する別のグループを用意して、Controller または Cloud Connector をグループで処理できます。Controller または Cloud Connector はリストからランダムに選択されるものであるため、グループ化すると優先的な使用を指定しやすくなります。

これらのグループは、単一のサイト内（複数のサイトではなく）での使用を目的としています。

Controller または Cloud Connector のグループを指定するにはかっこを使用します。たとえば Controller が 4 つ（主に使用するものが 2 つとバックアップ用が 2 つ）ある場合、次のようにグループ化します。

```
(XDC-001.cdz.lan XDC-002.cdz.lan)(XDC-003.cdz.lan XDC-004.cdz.lan)
```

この例では、最初のグループの Controller（001 と 002）が初めに処理されます。両方で障害が発生した場合、2 番目のグループの Controller（003 と 004）が処理されます。

XenDesktop 7.0 以降では、登録グループ機能を使用する場合、追加の手順を実施する必要があります。Studio で、［**Controller** の自動更新を有効にする］ポリシーを禁止にしてください。

ListOfSIDs

登録時に VDA が通信可能な Controller をまとめたものが`ListofDDCs`です。VDA はどの Controller が信頼可能であるかも把握する必要があります。VDA は、`ListofDDCs`に含まれている Controller を自動的に信頼するわけではありません。`ListofSIDs`（セキュリティ ID）により、信頼可能な Controller が指定されます。VDA が登録を試みるのは、信頼されている Controller だけです。

ほとんどの環境では、`ListofSIDs`は`ListofDDCs`から自動で作成されます。CDF トレースを使用して`ListofSIDs`を読み取ることができます。

一般には、`ListofSIDs`を手動で変更する必要はありません。ただし、いくつかの例外があります。最初の 2 つの例外は、新しいテクノロジが使用可能になったため有効ではなくなりました。

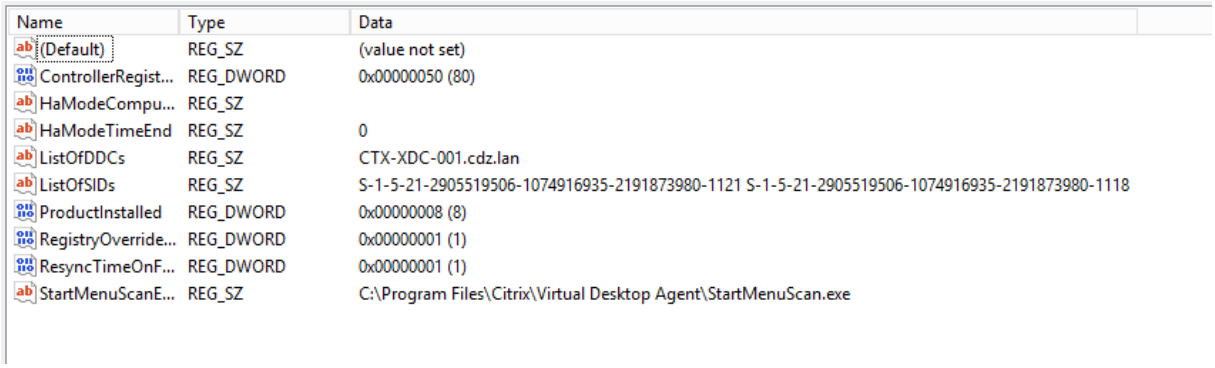
- **Controller** の役割の分離: XenApp および XenDesktop 7.7 でゾーンが導入される前は、登録に Controller のサブセットのみを使用する場合`ListofSIDs`を手動で構成していました。たとえば、XDC-001 と XDC-002 を XML ブローカーとして使用し、XDC-003 と XDC-004 を VDA 登録に使用する場合、`ListofSIDs`にはすべての Controller を指定し、`ListofDDCs`には XDC-003 と XDC-004 を指定していました。これは典型的な構成や推奨される構成ではありません。最新の環境では使用しないでください。代わりにゾーンが使用されています。
- **Active Directory** の負荷の削減： XenApp および XenDesktop 7.6 で自動更新機能が導入される前は、ドメインコントローラーに対する負荷を抑えるために`ListofSIDs`を使用していました。`ListofSIDs`を事前に指定しておくことで、DNS 名から SID への解決を省略できます。しかし、自動更新機能では永続キャッシュに SID が含まれるようになったため、この作業を行う必要はなくなりました。自動更新機能は有効にしておくことを Citrix ではお勧めします。

- セキュリティ：高度なセキュリティで保護された環境では、侵害された DNS サーバーからのセキュリティ上の脅威を防ぐために、信頼されている Controller の SID を手動で構成していました。ただし、この構成を行うには、自動更新機能を無効にする必要があります。無効にしない場合、永続キャッシュの構成が使用されます。

このため、特別な理由がない限り`ListofSIDs`は変更しないでください。

`ListofSIDs`を変更する必要がある場合、`HKLM\Software\Citrix\VirtualDesktopAgent`に`ListOfSIDs` (`REG_SZ`)という名前のレジストリキーを作成します。値には、信頼できる SID の一覧を指定します。SID が複数ある場合はスペースで区切って指定します。

次の例では、1 つの Controller を VDA の登録に使用しますが（`ListofDDCs`）、2 つの Controller は仲介に使用します（ListOfSIDs）。



Name	Type	Data
(Default)	REG_SZ	(value not set)
ControllerRegist...	REG_DWORD	0x00000050 (80)
HaModeCompu...	REG_SZ	
HaModeTimeEnd	REG_SZ	0
ListOfDDCs	REG_SZ	CTX-XDC-001.cdz.lan
ListOfSIDs	REG_SZ	S-1-5-21-2905519506-1074916935-2191873980-1121 S-1-5-21-2905519506-1074916935-2191873980-1118
ProductInstalled	REG_DWORD	0x00000008 (8)
RegistryOverride...	REG_DWORD	0x00000001 (1)
ResyncTimeOnF...	REG_DWORD	0x00000001 (1)
StartMenuScanE...	REG_SZ	C:\Program Files\Citrix\Virtual Desktop Agent\StartMenuScan.exe

VDA 登録中の Controller の検索

VDA が登録しようとすると、Broker Agent は最初にローカルドメインで DNS ルックアップを実行し、指定された Controller に到達できるようにします。

最初のルックアップで Controller が見つからない場合、Broker Agent は AD でフォールバックトップダウンクエリを開始することがあります。このクエリは、すべてのドメインを検索し、頻繁に繰り返します。Controller のアドレスが無効である場合（たとえば、管理者が VDA のインストール時に誤った FQDN を入力した場合）、そのクエリのアクティビティにより、ドメインコントローラーで分散サービス拒否（DDoS）状態が発生する可能性があります。

次のレジストリキーは、Broker Agent が最初の検索時に Controller を検出できない場合に、フォールバックトップダウンクエリを使用するかどうかを制御します。

`HKEY_LOCAL_MACHINE\Software\Policies\Citrix\VirtualDesktopAgent`

- 値の名前：`DisableDdcWildcardNameLookup`
- 種類：`DWORD`
- 値：1（デフォルト）または`0`

`1`に設定すると、フォールバック検索は無効になります。Controller の初回検索が失敗すると、Broker Agent は検索を停止します。これがデフォルトの設定です。

0に設定すると、フォールバック検索が有効になります。Controller の初回検索が失敗した場合、フォールバックトップダウン検索が開始されます。

読み取り専用ドメインコントローラーを使用した **VDA** 登録時の **LDAP** バインドシーケンス

VDA が読み取り専用ドメインコントローラー（RODC）に登録されると、Broker Agent は無視するライトウェイトディレクトリアクセスプロトコル（LDAP）バインドを選択する必要があります。Broker Agent がこの選択を行うには、Broker Agent に適切なレジストリキーが必要です。

レジストリキーが指定されていない場合、またはレジストリキーフィールドが空の場合、元の LDAP バインドシーケンスを実行する必要があるため、RODC への VDA の登録に時間がかかります。

LDAP バインドシーケンスを変更するために、レジストリキー`ListofIgnoredBindings`が`HKEY_LOCAL_MACHINE\Software\Policies\Citrix\VirtualDesktopAgent`に追加されました。`ListofIgnoredBindings`を使用すると、必要に応じて LDAP バインドシーケンスを変更できるため、RODC への VDA 登録を高速化できます。

- 値の名前：`ListofIgnoredBindings`
- 種類：`REG_SZ`
- 値：`DefaultPath`, `DomainPath`, `PDCPath`

値は、コンマで区切られたバインドパスオプションのリストです。レジストリキーは、有効と認識しなかった値を無視します。

VDA 登録の問題のトラブルシューティング

先に述べたように、仲介セッションを起動する場合、対象の Delivery Controller または Cloud Connector に VDA が登録されている必要があります。VDA が登録されていないと、登録されていれば使用されるはずの資源が使用されない場合があります。VDA が登録されない理由はさまざまですが、その多くは管理者がトラブルシューティングできます。Studio では、カタログ作成ウィザード内で、およびカタログをデリバリーグループに登録した後に、トラブルシューティング情報が提供されます。

- マシンカタログの作成時に問題を特定する：カタログ作成ウィザードで、既存のマシンを追加すると、コンピューターアカウント名の一覧に、各マシンがカタログに追加するのに適しているかどうかが示されます。各マシンの横にあるアイコンにマウスを合わせると、そのマシンに関する情報メッセージが表示されます。

  メッセージで問題のあるマシンが示された場合は、該当のマシンを（[削除] ボタンを使って）削除することも、そのマシンを追加することもできます。たとえば、（登録されたことがないなどの理由により）マシンに関する情報が取得されていないことを示すメッセージが表示された場合は、そのマシンを追加する可能性があります。

  カタログの機能レベルにより、どの製品機能がカタログにあるマシンで利用可能かが制御されます。新しい製品バージョンで導入された機能を使用するには、新しい VDA が必要な場合があります。機能レベルを設定すると、そのバージョン（機能レベルが変更されない場合はそのバージョン以降）で導入されたすべての機能が

カタログで利用できるようになります。ただし、以前の VDA バージョンのカタログにあるマシンは登録できません。

- デリバリーグループの作成後に問題を特定する：デリバリーグループを作成すると、そのグループと関連付けられているマシンの詳細が Studio に表示されます。

  デリバリーグループの［詳細］ペインに、登録の必要があるのに登録されていないマシンの数が表示されます。つまり、電源が入っており保守モードではないのに、Controller に現在登録されていないマシンが 1 台または複数台存在することが考えられます。「未登録だが登録する必要がある」のマシンが表示された場合は、［詳細］ペインの ［トラブルシューティング］タブで、考えられる原因と推奨される修正アクションを確認します。

VDA 登録のトラブルシューティングの詳細

- 機能レベルについて詳しくは、「VDA バージョンと機能レベル」を参照してください。
- VDA 登録のトラブルシューティングについて詳しくは、CTX136668を参照してください。
- Citrix Scout のヘルスチェックを使用して、VDA 登録とセッションの開始に関するトラブルシューティングを行うことも可能です。詳しくは、「ヘルスチェックについて」を参照してください。

仮想 **IP** と仮想ループバック

August 17, 2024

> 重要：
>
> - Windows 10 Enterprise マルチセッションでは、リモートデスクトップ IP 仮想化（仮想 IP）がサポートされていないため、Windows 10 Enterprise マルチセッションでは、リモートデスクトップ IP 仮想化も仮想ループバックもサポートしていません。
> - リモートデスクトップ IP 仮想化（仮想 IP）は、クラウドでホストされているマシンではサポートされていません。
>
> 詳しくは、Microsoftのドキュメントを参照してください。

リモートデスクトップ IP 仮想化および仮想ループバック機能は、Windows Server 2016、Windows Server 2019、および Windows Server 2022 マシンでサポートされています。これらの機能は、Windows デスクトップ OS マシンでは使用できません。

Microsoft 社のリモートデスクトップ IP 仮想化アドレス機能により、セッションごとに動的に割り当てられる固有の IP アドレスを公開アプリケーションで使用できます。Citrix の仮想ループバック機能を使用すると、ローカルホスト（デフォルトで 127.0.0.1）と通信するアプリケーションで、ローカルホストの範囲内（127.*）で固有の仮想ループバックアドレスが使用されるように構成できます。

CRM（Customer Relationship Management）や CTI（Computer Telephony Integration）などの特定のアプリケーションでは、アドレス割り当て、ライセンス付与、識別、またはそのほかの目的で IP アドレスが使用されるため、固有の IP アドレスまたはループバックアドレスが必要です。また、一部のアプリケーションでは静的なポートにバインドされるため、マルチユーザー環境でそのアプリケーションの追加インスタンスを起動しようとすると、そのポートが使用中なので起動に失敗します。これらのアプリケーションが Citrix Virtual Apps 環境で正しく動作するためには、クライアントデバイスごとに異なる IP アドレスが使用される必要があります。

リモートデスクトップ IP 仮想化と仮想ループバックは、互いに独立した機能です。これらの機能のいずれかまたは両方を使用できます。

使用する機能に応じて、管理者は以下の操作を行います:

- Microsoft リモートデスクトップ IP 仮想化を使用するには、Windows サーバー上でこれを有効にして構成します。（Citrix ポリシーの設定は必要ありません。）
- Citrix の仮想ループバック機能を使用するには、Citrix ポリシーで 2 つの設定項目を構成します。

リモートデスクトップ **IP** 仮想化（仮想 **IP**）

Windows サーバー上でリモートデスクトップ IP 仮想化機能を有効にすると、セッション内で動作する各アプリケーションで固有のアドレスが使用されるように構成できます。ユーザーは、Citrix Virtual Apps 上にあるこれらのアプリケーションを、ほかの公開アプリケーションと同じように使用することができます。以下のいずれかの動作をするプロセスでは、リモートデスクトップ IP 仮想化を設定します:

- ハードコードされた（固定された）TCP ポート番号を使用する
- Windows ソケットを使用し、固有の IP アドレスまたは固定された TCP ポート番号を使用する

アプリケーションでリモートデスクトップ IP 仮想化が必要かどうかを判断するには、次の手順に従います:

1. Microsoft の Web サイトから、**TCPView** ツールを入手します。このツールを使用すると、特定の IP アドレスおよびポートを使用しているすべてのアプリケーションを一覧表示できます。TCPView について詳しくは、Microsoftのドキュメントを参照してください。
2. [**Resolve IP Addresses**] を無効にします。これにより、一覧にホスト名ではなくアドレスが表示されるようになります。
3. 対象となるアプリケーションを起動して、使用されている IP アドレスとポート、およびそれらのポートを開いているプロセスの名前を **TCPView** で確認します。
4. サーバーの IP アドレス 0.0.0.0 または 127.0.0.1 を使用するプロセスを構成します。
5. そのアプリケーションの別のインスタンスを起動して、別のポート上で同じ IP アドレスが使用されないことを確認します。

Microsoft リモートデスクトップ（**RD**）の **IP** 仮想化のしくみ

- 仮想 IP アドレスを使用するには、Windows サーバー上でこの機能を有効にする必要があります。

たとえば、Windows Server 2016 環境でサーバーマネージャーを使用し、［リモートデスクトップサービス］**>**［**RD** セッションホストの構成］の順に展開して RD IP 仮想化機能を有効にします。次に、IP アドレスを DHCP（Dynamic Host Configuration Protocol：動的ホスト構成プロトコル）サーバーによりセッションごとまたはプログラムごとに動的に割り当てるように設定を行います。リモートデスクトップ IP 仮想化の構成について詳しくは、Microsoft のドキュメントを参照してください。

- この機能を有効にすると、セッション起動時にサーバーは、DHCP サーバーから動的に割り当てられた IP アドレスを要求します。
- **RD IP** 仮想化機能によって、セッションごとまたはプログラムごとに、リモートデスクトップ接続に IP アドレスが割り当てられます。複数のプログラムに IP アドレスを割り当てる場合、これらのプログラム間でセッションごとの IP アドレスが共有されます。
- アドレスがセッションに割り当てられた後、以下の呼び出しが行われるたびに、セッションはシステムのプライマリ IP アドレスではなく仮想アドレスを使用します：`bind`、`closesocket`、`connect`、`WSAConnect`、`WSAAccept`、`getpeername`、`getsockname`、`sendto`、`WSASendTo`、`WSASocketW`、`gethostbyaddr`、`getnameinfo`、`getaddrinfo`。

リモートデスクトップセッションのホスト環境で Microsoft の IP 仮想化機能を使用すると、アプリケーションと Winsock コールとの間に「フィルター」コンポーネントを挿入することで、アプリケーションと特定の IP アドレスがバインドされます。IP アドレスがバインドされると、アプリケーションはそのアドレスだけで要求を待ち受けるようになります。アプリケーションの TCP リスナーまたは UDP リスナーは自動的に仮想 IP アドレス（または仮想ループバックアドレス）にバインドされます。アプリケーションからの接続はその仮想アドレスから開かれます。

Windows ポリシーにより制御される`GetAddrInfo()`など、アドレスを返す関数でローカルホスト IP アドレスが要求されると、返された IP アドレスがそのセッションのリモートデスクトップ IP 仮想化アドレスに変換されます。このような関数でローカルサーバーの IP アドレスを取得しようとするアプリケーションには、セッション固有のリモートデスクトップ IP 仮想化アドレスだけが渡されます。このようにしてアプリケーションに渡された IP アドレスは、以降のソケットコール（bind や connect など）で使用されます。Windows ポリシーについて詳しくは、RDS IP Virtualization in Windows Serverを参照してください。

アプリケーションでは、アドレス 0.0.0.0 で、リスナー用のポートのバインドが必要になる場合があります。このようなアプリケーションで静的なポート番号が使用されると、競合が発生するため、複数のインスタンスを起動できなくなります。リモートデスクトップ IP 仮想化アドレス機能では、0.0.0.0 への関数呼び出しが特定の仮想 IP アドレスに変換されます。これにより、セッションごとに異なるアドレス上のポートが使用されるため、同じポート番号を使用する複数のアプリケーションを実行できるようになります。このファンクションコールは、リモートデスクトップ IP 仮想化アドレス機能が有効な ICA セッションでのみ変換されます。たとえば、すべてのインターフェイス（0.0.0.0）と特定のポート（9000 など）にバインドするアプリケーションの 2 つのインスタンスが、それぞれ異なるセッションで実行される場合、VIPAddress1:9000 と VIPAddress2:9000 にバインドされるため、競合が起きません。

仮想ループバック

Citrix ポリシーでリモートデスクトップ **IP** 仮想化ループバック機能を有効にすると、各セッションで通信に独自のループバックアドレスが使用されるようになります。アプリケーションが Winsock 呼び出しでローカルホストのアドレス（デフォルトで 127.0.0.1）を使用する場合、仮想ループバック機能により、127.0.0.1 が 127.X.X.X（X.X.X はセッション ID に 1 を足したものです）に置き換えられます。たとえば、セッション ID が 7 の場合は 127.0.0.8 になります。セッション ID が 4 オクテットを超える場合（つまり 255 を超える場合）は、127.0.1.0 のように次のオクテットに繰り上げられます。また、最大値は 127.255.255.255 です。

以下のいずれかの動作をするプロセスでは、仮想ループバックを設定します。

- Windows ソケットのループバック（localhost）アドレス 127.0.0.1 を使用する。
- ハードコードされた（固定された）TCP ポート番号を使用する

プロセス間通信でループバックアドレスを使用するアプリケーションでは、仮想ループバックアドレスポリシー設定を使用します。追加の構成は必要ありません。仮想ループバックは仮想 IP に依存しないため、Windows サーバーの構成は不要です。

- 仮想 IP ループバックサポートこのポリシー設定を有効にすると、各セッション固有の仮想ループバックアドレスが使用されるようになります。このチェックボックスは、デフォルトでオフになっています。この機能は、［仮想 IP ループバックプログラム一覧］ポリシー設定で指定したアプリケーションにのみ適用されます。
- 仮想 IP ループバックプログラム一覧このポリシー設定では、仮想 IP ループバック機能を使用するアプリケーションを指定します。この設定は、［仮想 IP ループバックサポート］ポリシー設定が有効になっている場合のみ適用されます。
- 仮想 IP ループバックポートの除外。アプリケーションがこの設定で指定されたポート上のループバックアドレスを呼び出す場合、仮想ループバックは呼び出しをセッション固有のループバックアドレスに変更しません。

関連機能

次のレジストリ設定により、仮想ループバックが仮想 IP よりも優先されるようになります。この機能は、優先ループバックと呼ばれます。ただし、以下の点に注意してください。

- 仮想 IP アドレスと仮想ループバックの両方の機能を有効にする場合にのみ、優先ループバック機能を使用してください。そうしないと、意図しない結果が生じることがあります。
- レジストリエディターの使用を誤ると、深刻な問題が発生する可能性があり、オペレーティングシステムの再インストールが必要になる場合もあります。レジストリエディターの誤用による障害に対して、Citrix は一切責任を負いません。レジストリエディターは、お客様の責任と判断の範囲でご使用ください。また、レジストリファイルのバックアップを作成してから、レジストリを編集してください。

アプリケーションのホストサーバー上で、regedit を実行します。

- HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\VIP
- 値の名前：PreferLoopback、種類：REG_DWORD、値のデータ：1

- 値の名前：PreferLoopbackProcesses、種類：REG_MULTI_SZ、データ：< プロセスの一覧 > プロセスの一覧 >

ゾーン

August 17, 2024

> 注：
>
> Web Studio（Web ベース）と Citrix Studio（Windows ベース）の 2 つの管理コンソールを使用して、Citrix Virtual Apps and Desktops の展開を管理できます。この記事では Web Studio のみを扱います。Citrix Studio について詳しくは、Citrix Virtual Apps and Desktops 7 2212 以前の同様の記事を参照してください。

展開が WAN で接続された広範な場所に分散している場合、ネットワークの遅延と信頼性に関する問題が発生することがあります。このような問題の影響を軽減するには、次の 2 つの方法があります：

- それぞれに独自の SQL Server サイトデータベースを持つ複数のサイトの展開

  このオプションは、大規模な環境で推奨されます。複数サイトは個別に管理され、各サイトに独自の SQL Server サイトデータベースが必要です。各サイトが個別の Citrix Virtual Apps 展開です。

- 単一サイト内に複数のゾーンを構成します。

  ゾーンを構成することにより、リモートのユーザーが、WAN の大規模セグメントを経由する接続を必ずしも必要とせず、リソースに接続できるようにサポートできます。ゾーンを使用することにより、単一の Web Studio コンソール、Citrix Director、およびサイトデータベースからの効果的なサイト管理が実現します。これにより、リモートの場所への追加サイト（個別のデータベースを含む）の展開、それに要する人員の配置、ライセンス取得、および運用のコストが削減されます。

  ゾーンは、あらゆる規模の展開で有用です。ゾーンを使用して、アプリケーションおよびデスクトップとエンドユーザーの距離を縮めることにより、パフォーマンスを改善することができます。1 つのゾーンにおいて、1 つまたは複数の Controller をローカルでインストールして冗長性と回復性を確保することができますが、これは必須ではありません。

  サイトで多数の Controller を構成すると、サイト自体への Controller の新規追加など一部の操作のパフォーマンスが低下することがあります。こうした事態を回避するため、Citrix Virtual Apps サイトまたは Citrix Virtual Desktops サイトのゾーンの数は、50 以下に制限することをお勧めします。

  ゾーンのネットワーク遅延が 250 ミリ秒（RTT）を超える場合は、ゾーンではなくサイトを複数展開することをお勧めします。

このアーティクルを通じ、「ローカル」という用語は、対象となるゾーンを指しています。たとえば、「VDA はローカル Controller に登録されます」という場合、VDA が存在するゾーンの Controller に登録されることを意味します。

このリリースでのゾーンは、XenApp Version 6.5 以前と大きな違いはありませんが、同一ではありません。たとえば、このゾーン実装では、データコレクターが存在しません。サイトのすべての Controller が、プライマリゾーンの 1 つのサイトデータベースと通信します。また、このリリースではフェールオーバーおよび優先ゾーンの機能が異なります。

ゾーンの種類

1 つのサイトには、必ず 1 つのプライマリゾーンがあります。また、サイトにはオプションで 1 つまたは複数のサテライトゾーンを含めることもできます。サテライトゾーンは、障害回復、地理的に離れたデータセンター、ブランチオフィス、クラウド、またはクラウドのアベイラビリティゾーンに使用できます。

プライマリゾーン:

プライマリゾーンのデフォルト名は「Primary」です。このゾーンには、SQL Server サイトデータベース（および使用している場合は高可用性 SQL Server）、Web Studio、Director、Citrix StoreFront、Citrix ライセンスサーバー、および Citrix Gateway が含まれます。サイトデータベースは、常にプライマリゾーンにあるようにします。

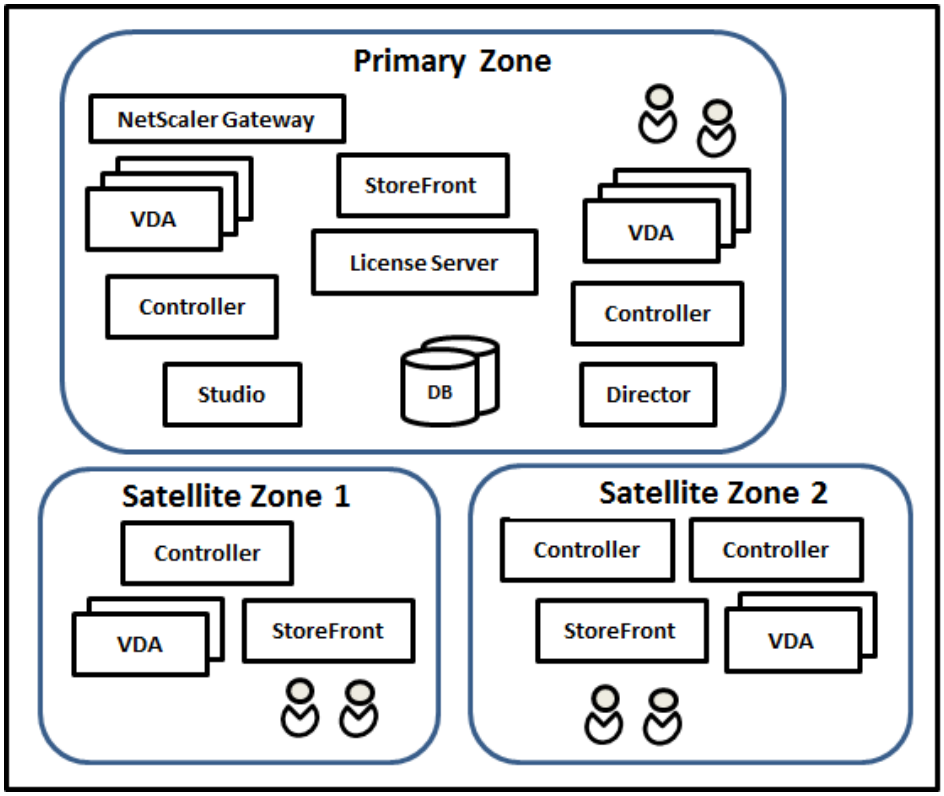
プライマリゾーンには、冗長性のために少なくとも 2 つの Controller が必要です。また、プライマリゾーンにはデータベースおよびインフラストラクチャと密結合されたアプリケーションを含む VDA が含まれることがあります。

サテライトゾーン:

サテライトゾーンには、1 つまたは複数の VDA と、Controller、StoreFront サーバー、および Citrix Gateway サーバーが含まれます。通常時には、サテライトゾーンの Controller はプライマリゾーンのデータベースと直接通信します。

特に大きなサテライトゾーンには、そのゾーンのマシンのプロビジョニングと保存に使用されるハイパーバイザーも含まれることがあります。サテライトゾーンの構成時には、ハイパーバイザーまたはその他のサービスの接続をサテライトゾーンに関連付けることができます（この接続を使用するカタログが同じゾーンに含まれていることを確認してください）。

ニーズと環境に応じて、1 つのサイトに異なる構成のサテライトゾーンを含めることができます。次の図は、1 つのプライマリゾーンと、複数のサテライトゾーンの例を示しています。



この図の内容は次のとおりです:

- プライマリゾーン: Controller が 2 つ、Web Studio、Director、StoreFront、ライセンスサーバー、サイトデータベース（および高可用性 SQL Server 展開）が含まれています。また、プライマリゾーンには複数の VDA および Citrix Gateway も含まれています。
- サテライトゾーン **1**（**VDA** と **Controller**）: サテライトゾーン 1 には、1 つの Controller、複数の VDA、1 つの StoreFront サーバーが含まれています。このサテライトゾーンの VDA は、ローカル Controller に登録されます。ローカル Controller は、プライマリゾーンのサイトデータベースおよびライセンスサーバーと通信します。

  ローカルホストキャッシュ機能を使用すると、WAN で障害が発生した場合に、サテライトゾーン内の Controller がそのゾーン内の VDA への接続を引き続き仲介できるようになります。このような展開は、作業者がローカル StoreFront サイトおよびローカル Controller を使用してローカルリソースにアクセスするオフィスで効果的です。
- サテライトゾーン **2**（**VDA** と冗長性用 **Controller**）: サテライトゾーン 2 には、2 つの Controller、複数の VDA、1 つの StoreFront サーバーが含まれています。この種類のゾーンは回復性が最も高く、WAN とローカル Controller の 1 つで同時に障害が発生しても、それに耐えることができます。

VDA の登録と **Controller** のフェールオーバー

プライマリゾーンとサテライトゾーンを含み、VDA のバージョンが 7.7 以降のサイトでは、以下のルールが適用されます:

- プライマリゾーンの VDA は、プライマリゾーンの Controller に登録されます。プライマリゾーンの VDA では、サテライトゾーンの Controller への登録は試行されません。
- サテライトゾーンの VDA は、可能な場合はローカル Controller に登録されます（これが優先 Controller になります）。ローカル Controller を利用できない場合（ローカル Controller で追加の VDA 登録を受け入れられない場合や、ローカル Controller で障害が発生している場合など）、VDA ではプライマリゾーンの Controller への登録が試行されます。この場合、サテライトゾーンの Controller が再び利用可能になっても、VDA はプライマリゾーンで登録されたままになります。サテライトゾーンの VDA では、別のサテライトゾーンの Controller への登録が試行されることはありません。
- Controller の VDA 検出で自動更新が有効になっており、VDA のインストール時に Controller アドレスの一覧を指定した場合、初回登録では、（Controller が含まれるゾーンに関係なく）その一覧からランダムに Controller が選択されます。その VDA が含まれるマシンが再起動された後、そのローカルゾーン内の Controller が VDA 登録の優先 Controller になります。
- サテライトゾーンの Controller で障害が発生した場合、可能であれば別のローカル Controller へのフェールオーバーが実行されます。ローカル Controller を利用できない場合は、プライマリゾーンの Controller へのフェールオーバーが実行されます。
- Controller をゾーン内またはゾーン外に移動し、自動更新が有効である場合、両方のゾーンの VDA に対し、ローカルの Controller とプライマリゾーンの Controller を示す更新された一覧が送信されます。これにより、登録および接続の受け入れが可能な Controller が VDA で認識されます。
- カタログを別のゾーンに移動すると、そのカタログの VDA が、カタログを移動したゾーンの Controller に再登録されます（カタログを別のゾーンに移動するときは、このゾーンと、関連付けられたホスト接続のあるゾーンとが正しく接続されていることを確認します。帯域幅が制限されているか遅延が長い場合は、ホスト接続を、関連付けられたマシンカタログを含む同じゾーンに移動します。

プライマリゾーンですべての Controller が失敗すると、以下の状態になります。

- Web Studio がサイトに接続できない。
- プライマリゾーンで VDA に接続できない。
- プライマリゾーンの Controller が使用できるようになるまで、サイトのパフォーマンスが低下する。

Version 7.7 よりも前の VDA バージョンが含まれるサイトでは、以下のルールが適用されます:

- サテライトゾーンの VDA では、そのローカルゾーンおよびプライマリゾーンの Controller からの要求が受け入れられます（Version 7.7 以降の VDA では、ほかのセカンダリゾーンからの Controller 要求を受け入れることができます）。
- サテライトゾーンの VDA は、プライマリゾーンまたはローカルゾーンの Controller にランダムに登録されます（Version 7.7 以降の VDA では、ローカルゾーンが優先されます）。

ゾーン優先度

ゾーン優先度機能を使用するには、StoreFront 3.7 以上および Citrix Gateway 11.0-65.x 以上を使用している必要があります。

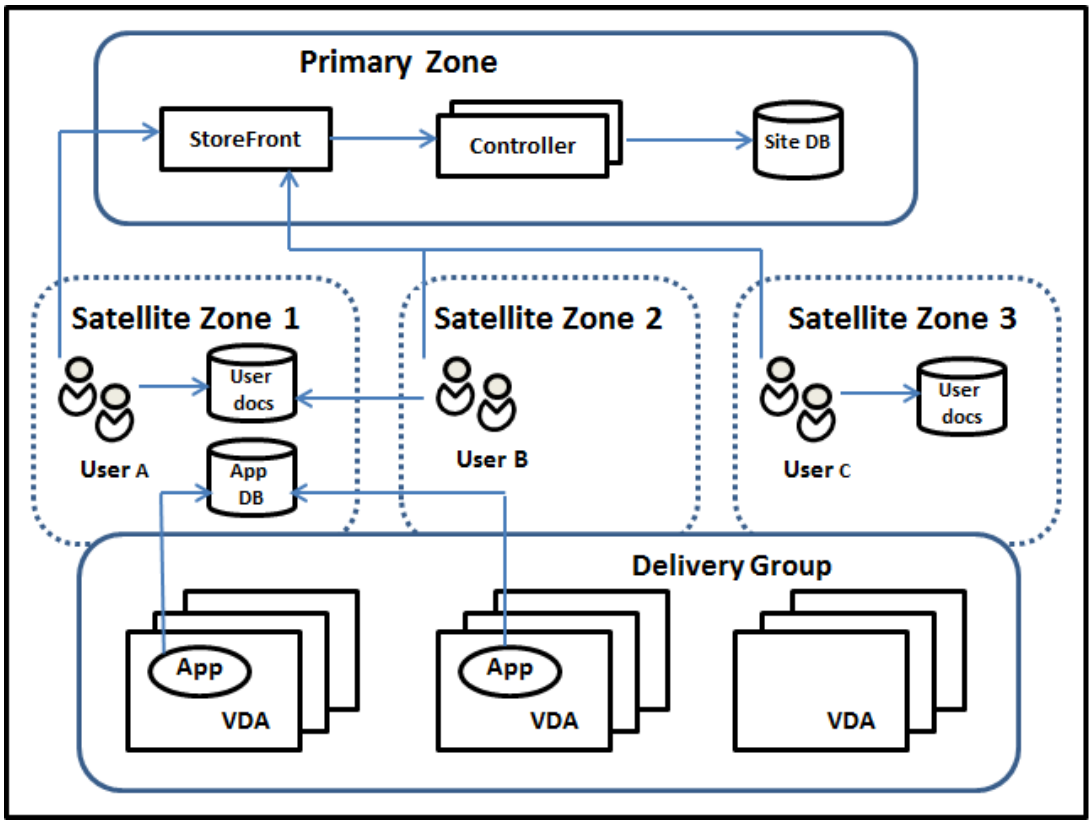
複数のゾーンがあるサイトでは、管理者は、アプリケーションやデスクトップの起動にどの VDA が使用されるかを、ゾーンの優先度機能によってより柔軟に制御できます。

ゾーンの優先度のしくみ

ゾーンの優先度には以下の 3 つの形式があります。以下によっては、特定のゾーンに VDA を使用するのが好ましい場合があります。

- アプリケーションのデータの保存先。これを「アプリケーションホーム」と呼びます。
- プロファイルやホームシェアなどの、ユーザーのホームデータの場所。これを「ユーザーホーム」と呼びます。
- （Citrix Workspace アプリが実行されている）ユーザーの現在位置。これを「ユーザーの場所」と呼びます。

次の図は、マルチゾーン構成の例を示しています。



この例では、VDA は 3 つのサテライトゾーンにまたがっていますが、同じデリバリーグループに属しています。そのため、ブローカーはユーザーの起動依頼にどの VDA を使用するかを選択できる場合があります。この例は、ユーザーが Citrix Workspace アプリのエンドポイントを実行できるいくつかの場所があることを示しています：

- ユーザー A は、サテライトゾーン 1 の Citrix Workspace アプリでデバイスを使用しています。
- ユーザー B は、サテライトゾーン 2 のデバイスを使用しています。
- ユーザーのドキュメントも異なる場所に保管できます。
  - ユーザー A と B は、サテライトゾーン 1 を本拠とした共有を使用します。
  - ユーザー C は、サテライトゾーン C からの共有を使用します。
  - 公開アプリケーションのいずれかによって、サテライトゾーン 1 にあるデータベースが使用されます。

ユーザーまたはアプリケーションにホームゾーンを構成して、ユーザーまたはアプリケーションをゾーンと関連付けることができます。すると、Delivery Controller のブローカーがこれらの関連付けを使用して、セッションが開始されるゾーンを選択します（リソースが利用可能な場合）。次の操作を実行できます：

- ユーザーをゾーンに追加して、ユーザーのホームゾーンを構成します。
- アプリケーションプロパティを編集して、アプリケーションのホームゾーンを構成します。

ユーザーまたはアプリケーションに構成できるホームゾーンは 1 回あたり 1 つのみです（ユーザーについては、複数のゾーンメンバーシップがある場合は例外となることがあります。「そのほかの考慮事項」セクションを参照してください。ただし、その場合においても、ブローカーが使うホームゾーンは 1 つのみです）。

ユーザーおよびアプリケーションのゾーン優先度を構成できますが、ブローカーは起動する優先ゾーンを 1 つだけ選択します。優先ゾーンの選択におけるデフォルトの優先順位は、アプリケーションホーム、ユーザーホーム、ユーザーの場所の順になります。この順序は調整可能です。「ゾーン優先度の調整」を参照してください。ユーザーがアプリケーションを起動すると、優先ゾーンは次のように選択されます：

- アプリケーションに構成済みのゾーンの関連付け（アプリケーションホーム）がある場合、優先ゾーンはそのアプリケーションのホームゾーンとなります。
- アプリケーションには構成済みのゾーンの関連付けがなく、ユーザーには構成されたゾーンの関連付け（ユーザーホーム）がある場合、優先ゾーンはそのユーザーのホームゾーンとなります。
- アプリケーションにもユーザーにもゾーンの関連付けが構成されていない場合、優先ゾーンはユーザーが Citrix Workspace アプリインスタンスを実行しているゾーン（ユーザーの場所）となります。このゾーンが定義されていない場合は、VDA およびゾーンのランダム選択が使用されます。負荷分散は、優先ゾーン内のすべての VDA に適用されます。優先ゾーンがない場合、負荷分散はデリバリーグループ内のすべての VDA に適用されます。

ゾーン優先度の調整

ユーザーまたはアプリケーションのホームゾーンを構成（または削除）することで、ゾーン優先度を使用する方法をさらに制限することもできます。

- ユーザーのホームゾーンの使用必須：デリバリーグループで、セッションをユーザーのホームゾーンで開始し（構成されている場合）、ホームゾーンに利用可能なリソースがない場合には別のゾーンにフェールオーバーしないように指定できます。この制限は、大きなプロファイルやデータファイルがゾーン間でコピーされないよ

うにする必要がある場合に有用です。つまり、他のゾーンでセッションを開始するのではなく、他のゾーンではセッションが開始されないようにします。

- アプリケーションのホームゾーンの使用必須：同様に、アプリケーションのホームゾーンを構成する際に、アプリケーションをそのゾーンでのみ起動し、アプリケーションのホームゾーンでリソースが利用可能でない場合には他のゾーンにフェールオーバーしないように指定できます。
- アプリケーションのホームゾーンなし、構成済みのユーザーホームゾーンは無視：アプリケーションのホームゾーンを指定しない場合は、アプリケーションを起動するときに構成済みのユーザーゾーンを考慮しないように指定することもできます。たとえば、ユーザーの場所ゾーン優先度を使用して、ユーザーに他のホームゾーンがある場合でも、ユーザーのデバイスの近くにある VDA でアプリケーションが実行されるようにできます。

優先ゾーンによるセッション使用への影響

ユーザーがアプリケーションやデスクトップを起動すると、ブローカーは既存のセッションよりも優先ゾーンを使用しようとします。

アプリケーションまたはデスクトップを起動しているユーザーに、起動中のリソースに最適なセッション（アプリケーションのセッション共有を使用できるセッション、または起動中のリソースを既に実行しているセッションなど）があるにもかかわらず、セッションがユーザーまたはアプリケーションの優先ゾーン以外のゾーンの VDA で実行されている場合、新しいセッションが作成されることがあります。これにより、セッションは、ユーザーのセッション要件に対して優先度の低いゾーンに再接続される前に、正しいゾーンで開始されます（そのゾーンに使用可能な容量がある場合）。

操作できなくなる孤立セッションが発生しないようにするため、優先ではないゾーンにあっても、再接続は既存の切断されたセッションにのみ許可されます。

セッション開始の望ましさの順は、以下のとおりです。

1. 優先ゾーンにある既存セッションに再接続する。
2. 優先ゾーン以外のゾーンにある既存の切断されたセッションに再接続する。
3. 優先ゾーンで新しいセッションを開始する。
4. 優先ゾーン以外のゾーンにある接続中の既存セッションに再接続する。
5. 優先ゾーン以外のゾーンで新しいセッションを開始する。

ゾーン優先度に関するそのほかの考慮事項

- ユーザーグループ（セキュリティグループなど）のホームゾーンを構成する場合、（直接または間接メンバーシップによる）そのグループのユーザーは、指定されたゾーンに関連付けられます。ただし、ユーザーは複数のセキュリティグループのメンバーになることができるため、別のグループのメンバーシップで他のホームゾーンが構成されている可能性があります。そのような場合は、そのユーザーのホームゾーンの特定があいまいになる可能性があります。

ユーザーに、グループメンバーシップで取得されなかった構成済みのホームゾーンがある場合、そのゾーンがゾーン優先度に使用されます。グループメンバーシップで取得されたゾーンの関連付けはすべて無視されます。

ユーザーに、グループメンバーシップのみで取得された複数の異なるゾーンの関連付けがある場合、ブローカーはそれらのゾーンの中からランダムに選択します。ブローカーがゾーンを選択すると、そのゾーンはユーザーのグループメンバーシップが変更されるまで、後続のセッションの開始に使用されます。

- ユーザーの場所ゾーン優先度には、デバイス接続で経由されている Citrix Gateway により、エンドポイントデバイス上の Citrix Workspace アプリが検出される必要があります。Citrix Gateway は、IP アドレスの範囲を特定のゾーンに関連付けるように構成する必要があり、検出されたゾーンの ID は、StoreFront から Controller に渡される必要があります。

ゾーン優先度について詳しくは、「Zone Preference Internals」を参照してください。

考慮事項、要件、およびベストプラクティス

- ゾーンには、Controller、マシンカタログ、ホスト接続、ユーザー、およびアプリケーションを配置することができます。カタログでホスト接続が使用される場合、そのカタログと接続が同じゾーンに含まれていることを確認します。（ただし、遅延が少ない高帯域幅接続を利用可能な場合は、異なるゾーンに存在できます。）
- サテライトゾーンにアイテムを配置すると、これらのアイテムおよびこれらに関連する他のオブジェクトとサイトとの通信方法に影響します。
  - Controller がサテライトゾーンに配置されている場合、これらのマシンは同一のゾーンにあるハイパーバイザーおよび VDA と良好に（ローカルに）接続できるものとみなされます。そのため、サテライトゾーンにあるハイパーバイザーや VDA マシンを処理する場合、プライマリゾーンの Controller ではなく同じサテライトゾーンにある Controller が使用されます。
  - ハイパーバイザー接続がサテライトゾーンに配置されている場合、このハイパーバイザー接続で管理されているすべてのハイパーバイザーも同じサテライトゾーン内に存在するものとみなされます。そのため、サテライトゾーンにあるハイパーバイザー接続を使用して通信する場合、プライマリゾーンの Controller ではなく同じサテライトゾーンにある Controller が使用されます。
  - マシンカタログがサテライトゾーンに配置されている場合、このカタログ内のすべての VDA マシンも同じサテライトゾーンにあるとみなされます。このため、各 VDA の初回登録後に Controller リストの自動更新メカニズムが有効になると、サイトへの登録時にはプライマリゾーンの Controller ではなくローカルの Controller が使用されます。
  - Citrix Gateway インスタンスもゾーンに関連付けることができます。この関連付けはこの記事で説明する他の要素と同様に、サイト構成ではなく StoreFront の最適な HDX ルーティング構成の一環として行います。ゾーンに関連付けられた Citrix Gateway は、そのゾーンにある VDA マシンへの HDX 接続で優先して使用されます。
- 実稼働サイトを作成してから、最初のカタログおよびデリバリーグループを作成した場合、すべてのアイテムがプライマリゾーンに含まれます。初期セットアップを完了するまで、サテライトゾーンは作成できません

（空のサイトを作成した場合、初期段階ではプライマリゾーンにはコントローラのみが含まれます。カタログとデリバリーグループグループの作成前または作成後に、サテライトゾーンを作成することができます）。

- 1 つまたは複数のアイテムが含まれる最初のサテライトゾーンを作成する場合、サイトのそのほかすべてのアイテムはプライマリゾーンに残ります。
- プライマリゾーンのデフォルト名は「プライマリ」です。この名前は変更できます。Web Studio 表示ではどのゾーンがプライマリゾーンかが示されますが、プライマリゾーンには容易に特定できる名前を使用するのがベストプラクティスです。プライマリゾーンは再割り当てする（すなわち、別のゾーンをプライマリゾーンにする）ことができます。ただし、プライマリゾーンには必ずサイトデータベースと高可用性サーバーが含まれている必要があります。
- サイトデータベースは、常にプライマリゾーンにあるようにします。
- ゾーンを作成した後、アイテムをゾーン間で移動できます。この柔軟性により、近くに配置することによって最適に機能する複数のアイテムを別々のゾーンに配置してしまう可能性があります。たとえば、カタログを、カタログ内のマシンを作成する接続（ホスト）とは異なるゾーンに移動すると、パフォーマンスに影響する可能性があります。アイテムをゾーン間で移動する前に、意図しない影響が出る可能性を考慮してください。カタログとホスト接続（同じゾーンまたは適切に接続されているゾーン（遅延が少なく高帯域幅のネットワーク経由など）でカタログが使用するもの）を維持します。
- パフォーマンスを最適化するため、Web Studio と Director はプライマリゾーンのみにインストールします。Web Studio および Director は Web アプリケーションであるため、サテライトゾーンからアクセスできます（Controller が含まれるサテライトゾーンが、プライマリゾーンにアクセスできなくなった場合のフェールオーバーとして使用されている場合など）。
- サテライトゾーンの Citrix Gateway はゾーン内の接続に使用できますが、ほかのゾーンまたは外部からそのゾーンへのユーザー接続に使用するのが理想的です。
- 注意：ゾーン優先度機能を使用するには、StoreFront 3.7 以上および Citrix Gateway 11.0-65.x 以上を使用している必要があります。

接続の質の制限

サテライトゾーンの Controller は、サイトデータベースに対して SQL 操作を直接実行します。このため、サテライトゾーンと、サイトデータベースが含まれるプライマリゾーンとのリンクの質はある程度制限されます。一部の制限は、サテライトゾーンに展開されている VDA の数とこれらの VDA 上のユーザーセッションの数に関係します。このため、VDA とセッションの数が少ないサテライトゾーンでは、VDA とセッションの数が多いサテライトゾーンよりもデータベースへの接続の質が低下します。

詳しくは、「遅延および SQL ブロッキングクエリの向上」を参照してください。

仲介のパフォーマンスに対する遅延時間の影響

ゾーンではリンクの遅延時間が大きくなりますが、ローカルブローカーが存在する場合、エンドユーザーのエクスペリエンスではさらに遅延が生じることになります。こうしたユーザーが行う作業のほとんどで、サテライトゾーンの Controller とサイトデータベースとの間で往復時間による遅れが生じます。

アプリケーションを起動する場合、セッションの仲介プロセスでセッション開始の要求を送信するのに適した VDA が見つかるまで、さらに遅れが生じます。

ゾーンの作成と管理

すべての管理権限を実行できる管理者は、ゾーンの作成および管理に関するすべてのタスクを実行できます。ただし、ゾーンを作成、編集、または削除できるカスタムの役割を作成することもできます。アイテムをゾーン間で移動するために、ゾーン関連の権限（ゾーン読み取り権限を除く）は必要ありません。ただし、移動するアイテムの編集権限は必要になります。たとえば、カタログをゾーン間で移動するには、そのカタログの編集権限が必要です。詳しくは、「管理者権限の委任」を参照してください。

Citrix Provisioning を使用する場合：Citrix Provisioning コンソールではゾーンが認識されないため、サテライトゾーンにカタログを作成する場合は、Web Studio を使用することをお勧めします。Web Studio でカタログを作成し、適切なサテライトゾーンを指定します。その後、Citrix Provisioning コンソールを使用して、そのカタログのマシンをプロビジョニングします（Citrix Provisioning ウィザードを使用してカタログを作成する場合、カタログはプライマリゾーンに配置されます。後で Web Studio を使用してサテライトゾーンに移動する必要があります）。

ゾーンの作成

1. Web Studio にサインインします。
2. 左側のペインで ［ゾーン］を選択します。
3. 操作バーの ［ゾーンの作成］を選択します。
4. ゾーンの名前と説明（オプション）を入力します。名前はサイト内で一意にする必要があります。
5. 新しいゾーンに配置するアイテムを選択します。選択できるアイテムの一覧では、フィルターまたは検索を実行できます。また、アイテムを選択せずに空のゾーンを作成することもできます。
6. ［保存］をクリックします。

この方法とは別に、Web Studio でアイテムを 1 つ以上選択してから、操作バー ［ゾーンの作成］を選択することもできます。

ゾーンの名前または説明の変更

1. Web Studio にサインインします。
2. 左側のペインで ［ゾーン］を選択します。
3. 中央ペインでゾーンを選択し、操作バーで ［ゾーンの編集］を選択します。

4. ゾーンの名前または説明（もしくはその両方）を変更します。プライマリゾーンの名前を変更する場合、そのゾーンをプライマリゾーンとして容易に特定できるようにしてください。
5. ［保存］または ［適用］をクリックします。

アイテムのゾーン間移動

1. Web Studio にサインインします。
2. 左側のペインで ［ゾーン］を選択します。
3. 中央ペインでゾーンを選択し、1 つまたは複数のアイテムを選択します。
4. アイテムを移動先ゾーンにドラッグするか、または操作バーで ［アイテムを移動］を選択してから移動先ゾーンを指定します。

選択したアイテムが確認メッセージで一覧にされ、それらすべてのアイテムを移動するかどうかが確認されます。

注意：カタログでハイパーバイザーまたはその他のサービスへのホスト接続を使用している場合、そのカタログと接続は同じゾーンに配置する必要があります。同じゾーンに含まれていない場合、パフォーマンスが低下する可能性があります。どちらかのアイテムを移動したら、もう 1 つのアイテムも移動してください。

ゾーンの削除

ゾーンは、削除する前に空にする必要があります。プライマリゾーンは削除できません。

1. Web Studio にサインインします。
2. 左側のペインで ［ゾーン］を選択します。
3. 中央ペインでゾーンを選択します。
4. 操作バーで ［ゾーンの削除］を選択します。ゾーンが空ではない（アイテムが含まれている）場合、それらのアイテムの移動先ゾーンを選択するよう指示するメッセージが表示されます。
5. 削除を確認します。

ユーザーのホームゾーンの追加

ユーザーにホームゾーンを構成することは、ゾーンへのユーザーの追加とも言います。

1. Web Studio にサインインします。
2. 左側のペインで ［ゾーン］を選択してから、中央ペインでゾーンを選択します。
3. 操作バーで ［ゾーンにユーザーを追加します］を選択します。
4. ［ゾーンへのユーザーの追加］ダイアログボックスで、［追加］をクリックしてからゾーンに追加するユーザーおよびユーザーグループを選択します。既にホームゾーンがあるユーザーを指定すると、2 つの選択肢を提供するメッセージが表示されます。［はい］を選択すると、指定したユーザーのうち、ホームゾーンのないユーザーのみが追加されます。［いいえ］を選択すると、ユーザー選択ダイアログに戻ります。
5. ［**OK**］をクリックします。

構成済みのホームゾーンがあるユーザーについては、ユーザーのホームゾーンからのセッション開始のみ要求できます。

1. デリバリーグループを作成または編集します。
2. ［ユーザー］ページで、［セッションはユーザーのホームゾーンで開始（構成済みの場合）］チェックボックスを選択します。

そのデリバリーグループ内のユーザーによって開始されたすべてのセッションは、そのユーザーのホームゾーンから開始される必要があります。そのデリバリーグループ内のユーザーに構成済みのホームゾーンがない場合、この設定は有効になりません。

ユーザーのホームゾーンの削除

この手順は、ゾーンからのユーザーの削除とも言います。

1. Web Studio にサインインします。
2. 左側のペインで ［ゾーン］を選択してから、中央ペインでゾーンを選択します。
3. 操作バーで ［ゾーンからユーザーを削除します］を選択します。
4. ［ゾーンへのユーザーの追加］ダイアログボックスで、［削除］をクリックして、ゾーンから削除するユーザーおよびグループを選択します。このアクションにより、ユーザーがゾーンからのみ削除されます。これらのユーザーは、属しているデリバリーグループおよびアプリケーショングループには残ったままとなります。
5. 確認のメッセージが表示されたら、削除を確定します。

アプリケーションのホームゾーンの管理

アプリケーションにホームゾーンを構成することは、ゾーンへのアプリケーションの追加とも言います。デフォルトで、マルチゾーン環境では、アプリケーションにはホームゾーンがありません。

アプリケーションのホームゾーンは、アプリケーションのプロパティで指定されます。アプリケーションのプロパティは、アプリケーションをグループに追加するとき、またはその後に構成できます。

- デリバリーグループを作成するとき、アプリケーショングループを作成するとき、またはアプリケーションを既存のグループに追加するときに、ウィザードの［アプリケーション］ページで［プロパティ］を選択します。
- アプリケーションの追加後にアプリケーションのプロパティを変更するには、左側のペインで ［アプリケーション］を選択します。アプリケーションを選択し、操作バーで ［アプリケーションプロパティの編集］を選択します。

アプリケーションのプロパティまたは設定の ［ゾーン］ページで以下の操作を行います：

- アプリケーションにホームゾーンを追加する場合は、
  - ［選択したゾーンを決定に使用］をクリックしてから、ゾーンを選択します。

  - アプリケーションを選択したゾーンからのみ起動する（他のゾーンからは起動しないようにする）には、ゾーン選択の下にあるチェックボックスを選択します。

- アプリケーションにホームゾーンを設定しない場合は、
  - ［ホームゾーンを構成しない］ラジオボタンを選択します。
  - このアプリケーションを起動するときに、ブローカーによって構成済みのユーザーのゾーンが考慮されないようにするには、ラジオボタンの下にあるチェックボックスを選択します。この場合、アプリケーションのホームゾーンやユーザーのホームゾーンが、このアプリケーションを起動する場所の決定に使用されることはありません。

ゾーンの指定が含まれるそのほかの操作

サテライトゾーンを 1 つ以上作成したあと、ホスト接続を追加するとき、またはカタログを作成するときにゾーンを指定できます。

通常、プライマリゾーンがデフォルトで指定されます。Machine Creation Services を使用してカタログを作成する場合、ホスト接続に対して構成されたゾーンが自動的に選択されます。

サイトにサテライトゾーンが含まれていない場合は、プライマリゾーンとして処理され、ゾーン選択ボックスは表示されません。

監視

August 17, 2024

管理者およびヘルプデスク担当者は、さまざまな機能やツールを使用して、Citrix Virtual Apps and Desktops のサイトをモニターできます。これらのツールを使って、モニターできるものは以下のとおりです:

- ユーザーセッションおよびセッションの利用状況
- ログオン処理のパフォーマンス
- 接続とマシン（エラーを含む）
- 負荷評価
- 履歴傾向
- インフラストラクチャ

Citrix Director

リアルタイム Web ツールである Director を使用して、セッションの監視、トラブルシューティングなど、エンドユーザーに対するサポートタスクを実行できます。

詳しくは、「Director」の記事を参照してください。

構成ログ

構成ログでは、サイトで管理者が行った変更内容が記録されます。構成を変更した後で問題が発生した場合は、構成ログを確認して問題の内容を診断し、トラブルシューティングを施します。また、変更管理、構成の記録、および管理アクティビティのレポート生成が可能です。

ログに記録した情報に関するレポートは、Studio から表示および生成できます。ログの内容は、Director の［傾向］ビューで確認し、構成変更についての通知を提供することもできます。これは、Studio へのアクセス権限を持たない管理者には便利な機能です。

［傾向］ビューでは、特定の期間に行われた構成変更の履歴データを表示できます。これにより、どのような変更がいつ、だれによって行われたかを確認して、問題の原因究明に役立てることができます。このビューには、構成情報が以下の 3 つのカテゴリに分けて表示されます:

- 接続エラー
- 障害が発生したシングルセッションマシン
- 障害が発生したマルチセッションマシン

構成ログ機能の有効化と構成方法について詳しくは、「構成ログ機能」を参照してください。「Director」には、このツールを使って、ログ情報を表示する方法を記載した記事があります。

イベントログ

Citrix Virtual Apps and Desktops 内のサービスは、発生するイベントを記録します。イベントログは、操作を監視およびトラブルシューティングするために使用します。

詳しくは、「イベントログ」を参照してください。個別の機能に関する記事には、イベント情報も含まれることがあります。

構成ログ

August 17, 2024

構成ログは、管理者によるサイト構成の変更やそのほかの管理操作をデータベースに記録する機能です。この機能はデフォルトで有効にされています。このログは、以下の目的で使用できます:

- 構成変更の履歴を確認して問題の診断およびトラブルシューティングを行う。ログではブレッドクラムが示されます。
- 変更管理の補助および構成の追跡を行う。
- 管理アクティビティのレポートを生成する。

Citrix Studio では、構成ログの基本設定を変更したり、構成ログを表示したり、HTML および CSV 形式のレポートを生成したりできます。日範囲および全文検索の結果により構成ログ表示をフィルターできます。必須ログ機能を有効にすると、ログが記録可能になるまで管理者による構成の変更が禁止されます。適切な権限を持つ管理者は、構成ログのエントリを削除できます。構成ログ機能では、ログの内容を編集することはできません。

構成ログでは、PowerShell SDK と Configuration Logging Service が使用されます。構成ログサービスは、サイト内のすべての Controller で実行されます。任意の Controller に障害が発生しても、ほかの Controller が自動的にログ要求を処理します。

デフォルトでは、構成ログ機能は有効で、サイト作成時に作成されたデータベース（サイト構成データベース）が使用されます。データベースには別の場所を指定できます。構成ログデータベースでは、サイト構成データベースと同じ高可用性機能がサポートされます。

構成ログへのアクセスは、［ログ基本設定を編集］権限および［構成ログを表示］権限による委任管理で制御されます。

構成ログの言語には、作成時のロケールが適用されます。たとえば、英語で作成されたログは、管理者側のロケールには関係なく英語で表示されます。

ログの内容

構成ログには、Studio、Director、および PowerShell スクリプトから開始された構成の変更および管理アクティビティのログが記録されます。以下の項目に対する作成、編集、削除などの操作が構成ログに記録されます。

- マシンカタログ
- デリバリーグループ（電源管理設定の変更を含む）
- 管理者の役割とスコープ
- ホストのリソースおよび接続
- Studio で構成する Citrix ポリシー

ログが記録される管理変更の例には次のものがあります:

- 仮想マシンまたはユーザーのデスクトップの電源管理
- Studio または Director からユーザーへのメッセージ送信

次の操作はログに記録されません。

- 仮想マシンのプール管理電源オンなどの自動操作。
- グループポリシー管理コンソール（GPMC）でのポリシー操作。これらの操作のログは Microsoft のツールを使って表示できます。
- レジストリによる変更、データベースの直接的な変更、および Studio、Director、PowerShell 以外での変更。
- 展開の初期化後、最初の Configuration Logging Service インスタンスが Configuration Service に登録されたときに構成ログが有効になります。このため、構成の初期のアクティビティが記録されない場合があります（ハイパーバイザーの初期化時にデータベーススキーマが取得および適用される場合など）。

構成ログの管理

デフォルトでは、サイトの作成時に作成されたデータベース（サイト構成データベース）に構成ログが記録されます。Citrix では、以下の理由により、構成ログデータベース（および監視データベース）には別の場所を使用することを推奨しています：

- 構成ログデータベースのバックアップ方針が、サイト構成データベースのバックアップ方針と異なる場合があります。
- 構成ログ（および Monitoring Service）で収集されるデータの量によっては、サイト構成データベース用の領域が不足する場合があります。
- データベースを分散させると、単一ポイント障害の問題が解消されます。

構成ログをサポートしない製品エディションでは、Studio に［ログ］ノードが表示されません。

構成ログと必須ログの有効化および無効化

デフォルトでは、構成ログ機能は有効になっており、必須ログ機能は無効になっています。

1. Web Studio にサインインし、左側のペインで ［ログ］を選択します。
2. 操作バーの ［基本設定］を選択します。［ログ設定］ダイアログボックスが開き、データベースに関する情報と、構成ログおよび必須ログ機能の有効/無効が表示されます。
3. 望ましい操作を選択します：

   構成ログを有効にするには、［有効］をクリックします。これがデフォルトの設定です。データベースに書き込みができない場合、ログ情報は破棄されますが構成内容は正しく反映されます。

   構成ログを無効にするには、［無効］をクリックします。それまでに記録されたログの内容は、PowerShell SDK で読み取ることができます。

   必須ログ機能を有効にするには、［データベースが切断されている場合の構成変更を禁止する］をクリックします。通常、ログに記録される構成の変更や管理作業は、構成ログデータベースへの書き込みが可能になるまで許可されません。必須ログ機能は、構成ログが有効な場合（［有効］が選択されている場合）にのみ有効にできます。Configuration Logging Service に障害が発生して、しかも高可用性が無効な場合、必須ログが有効になります。このような場合、構成ログデータベースに記録されるようなタスクは実行できなくなります。

   必須ログ機能を無効にするには、［データベースが切断されていても構成変更を許可する］をクリックします。構成ログデータベースにアクセスできない場合でも、管理者は構成の変更やそのほかの管理タスクを実行できます（管理タスクが優先されます）。これがデフォルトの設定です。

構成ログデータベースの場所の変更

必須ログ機能が有効になっている場合、データベースの場所を変更することはできません。データベースの変更時に短時間データベースから切断されるためです。

1. サポートされるバージョンの SQL Server を使用してデータベースサーバーを作成します。
2. Web Studio にサインインし、左側のペインで ［ログ］を選択します。
3. 操作バーの ［基本設定］を選択します。
4. ［ログ設定］ダイアログボックスで ［ログデータベースの変更］をクリックします。
5. ［ログデータベースの変更］ダイアログボックスで、新しいデータベースサーバーが入っているサーバーの場所を指定します。有効な形式については、「データベースのアドレス形式」を参照してください。
6. Studio で自動的にデータベースを作成する場合は、［**OK**］をクリックします。確認のメッセージが表示され、［**OK**］をクリックするとデータベースが自動的に作成されます。現在の Studio ユーザーの資格情報を使ってデータベースへのアクセスが試行されます。それが失敗すると、データベースユーザーの資格情報の入力を求められます。アクセスに成功すると、Studio によりデータベーススキーマがデータベースにアップロードされます（資格情報はデータベース作成時のみ保持されます）。
7. データベースを手動で作成する場合は、［データベーススクリプトの生成］をクリックします。生成されるスクリプトにはデータベースを手動で作成するためのコマンドが記述されます。スキーマをアップロードする前に、データベースが空であること、および 1 人以上のユーザーがそのデータベースにアクセスでき、変更できることを確認してください。

変更前のデータベース内の構成ログデータは変更後のデータベースにインポートされません。構成ログデータベースの場所を変更する場合、変更前のデータベースの内容は集約されなくなります。変更後の構成ログデータベースの最初にデータベースの変更を示すログが記録されますが、変更前のデータベースの場所は記録されません。

構成ログの内容を表示

管理者が構成の変更などの管理作業を開始すると、Studio や Director によって作成された高レベル操作が Studio の中央ペインの上部に表示されます。高レベル操作により 1 つまたは複数のサービスおよび SDK の呼び出しが実行されます。これは、低レベル操作です。ペインの上部で高レベル操作を選択すると、ペインの下部に低レベル操作が表示されます。

操作が完了する前に失敗すると、データベースでログ操作が完結しない場合があります。たとえば、開始レコードに対応する停止レコードがないなどです。このような場合、情報不足であることがログに示されます。時間の範囲を指定してログを表示する場合、未完結のログが表示される場合があります。たとえば、直近 5 日間のログを表示するときにその 5 日間に開始時間のみが含まれ、終了時間が含まれていない場合も、その操作のログが表示されます。

PowerShell コマンドレットを呼び出すスクリプトを使う場合、親の高レベル操作を指定せずに低レベル操作を作成すると、構成ログにより代わりの高レベル操作が作成されます。

構成ログの内容を表示するには、Studio のナビゲーションペインで ［ログ］ノードを選択します。デフォルトでは、中央ペインにログコンテンツが時系列順に（最新のエントリが最初に）表示されます。次の操作を実行できます:

- 列の見出しで表示を並べ替える。
- 日間隔を指定したり、［検索］ボックスにテキストを入力したりして、表示をフィルタリングする。検索を使用した後で通常のログ表示に戻すには、［検索］ボックスの文字列をクリアします。

- 表の右上隅にある 表示する列アイコンを選択して、画面に表示する列を選択します。たとえば、管理者が Web Studio にアクセスするために使用する IP アドレスを表示するには、アイコンをクリックしてクライアント **IP** 列を追加します。

レポートの生成

構成ログデータを CSV および HTML 形式のレポートとして書き出すことができます。

- CSV 形式のレポートには、指定した期間のすべてのログデータが書き込まれます。データベースの階層データが単一の CSV テーブルとして出力されます。データの特定の要素に基づいて並べ替えられたものではありません。書式も適用されず、読み取りやすさについても考慮されていません。レポートファイル（MyReport）には、汎用的な書式でデータが書き出されます。CSV ファイルはデータのアーカイブ化や、レポート機能または Microsoft Excel などデータ操作ツールのデータソースとして使用されます。
- HTML 形式のレポートには、指定した期間のログデータが判読可能な形式で書き込まれます。変更内容の確認が容易な、構造的でナビゲーション可能なレポートです。HTML レポートでは、概要（Summary）および詳細（Details）の 2 つのファイルが生成されます。概要レポートには、各操作の実行日時、操作主、および操作結果など、より高レベルな情報が一覧で表示されます。各操作項目の横にある ［詳細］リンクをクリックすると詳細ファイルが開き、より低いレベルの操作に関する情報を参照できます。

構成ログレポートを生成するには、Studio のナビゲーションペインで ［ログ］を選択し、操作バーの ［カスタムレポートの作成］を選択します。

- レポートの日付の範囲を選択します。
- レポート形式として、[CSV ファイル]、[HTML]、または［両方］を選択します。
- レポートを保存する場所を参照します。

構成ログの内容の削除

構成ログを削除するには、特定の委任管理権限および SQL Server データベース権限が必要です。

- 委任管理：展開構成を読み取ることができる委任管理の役割が必要です。すべての管理権限を実行できる管理者には、この権限があります。カスタムの役割では、［そのほかの権限］カテゴリで［読み取り専用］または［管理］権限を選択する必要があります。

  構成ログデータを削除する前にバックアップを作成するには、[ログ］カテゴリで［読み取り専用］または［管理］権限を選択する必要もあります。

- **SQL Server** データベース：データベースからレコードを削除するための権限を持つ SQL Server のログインアカウントが必要です。次のいずれかの方法を使用します：

  - データベースに対するすべての権限を持つ sysadmin サーバーロールを持つ SQL Server データベースログインを使用します。また、`serveradmin`または`setupadmin`サーバーの役割でも削除操作を実行できます。

- 高度なセキュリティが必要な環境では、データベースからレコードを削除する権限を持つデータベースユーザーにマップされた非 sysadmin データベースログインを使用します。

  1. SQL Server Management Studio で、sysadmin 以外のサーバーロールを持つ SQL Server ログインを作成します。
  2. 作成したログインをデータベースのユーザーにマップします。SQL Server により、ログインと同じ名前のユーザーがデータベースに作成されます。
  3. データベースの役割のメンバーシップとして、このデータベースユーザーに`ConfigurationLoggingSch`または`dbowner`の役割を指定します。

  詳しくは、SQL Server Management Studio のドキュメントを参照してください。

構成ログを削除するには、以下の手順に従います:

1. Web Studio にサインインし、左側のペインで ［ログ］を選択します。
2. 操作バーの ［ログの削除］を選択します。
3. 削除する前にログのバックアップを作成するかどうかを確認するメッセージが表示されます。バックアップを作成する場合は、バックアップを保存する場所を参照します。バックアップは CSV ファイルとして作成されます。

構成ログを削除すると、その削除操作が最初のエントリとしてログに記録されます。このエントリには、いつだれがログを削除したのかが記述されます。

API と PowerShell のログを表示する

現在のセッション中に行われた API 要求を監視するには、［**API**］タブをクリックします。Web Studio からサインアウトすると、API ログはクリアされます。

その日に実行した UI 操作に対応する PowerShell コマンドを表示するには、**PowerShell** タブをクリックします。

メタデータを構成ログに関連付ける

`MetadataMap`という`name-value`ペアをログレコードに関連付けることにより、構成ログにメタデータを添付できます。

> 注:
>
> - メタデータは高レベルの操作オブジェクトにのみ添付できます。
> - メタデータは、実行時に既存のレコードに関連付けられます。

メタデータを設定する

PowerShell コマンドSet-LogHighLevelOperationMetadataを実行して、ログレコードをMetadataMapに関連付けます。
Set-LogHighLevelOperationMetadataは次のパラメーターを使用します:

- **Id**: 高レベルの操作の ID。
- **InputObject**: メタデータを追加する高レベルの操作。これは、Idパラメーターの代わりの方法で、高レベルの操作オブジェクトまたはオブジェクトのリストが PowerShell コマンドに渡されます。

Name: 追加されるメタデータのプロパティ名。プロパ　[]” ‘。
ティは、指定された高レベルの操作に対して一意である
必要があります。プロパティには次の文字を含めること
はできません: ()/;:#.*?=<>

-
- **Value**: プロパティの値。
- **Map**: プロパティの（名前、値）ペアのディクショナリ。これは、-Nameおよび-Valueパラメーターを使用してメタデータを設定する代わりの方法です。

たとえば、ID 40 のすべての高レベルのログレコードにメタデータを添付するには、次の PowerShell コマンドを実行します:

```
Get-LogHighLevelOperation - Id 40 | Set-LogHighLevelOperationMetadata
 -Name A -Value B
```

ユーザーabc@example.comの高レベルのレコードにメタデータを添付するには、次の PowerShell コマンドを実行します:

```
Get-LogHighLevelOperation - User `abc@example.com` | Set-LogHighLevelOperationM
 -Name C -Value D
```

メタデータを使用して取得する

次の PowerShell コマンドを実行して、関連するメタデータを使用してログレコードを取得します:

- キーと値で検索:

  ```
  Get-LogHighLevelOperation -Metadata "Key:Value"
  ```

- 値と任意のキーで検索:

  ```
  Get-LogHighLevelOperation -Metadata "*:Value"
  ```


- キーと任意の値で検索:

```
Get-LogHighLevelOperation -Metadata "Key:*"
```

メタデータを削除する

PowerShell コマンド`Remove-LogHighLevelOperationMetadata`を実行して、関連するメタデータを削除します。
`Remove-LogHighLevelOperationMetadata`は次のパラメーターを使用します:

- **Id**: 高レベルの操作の ID。
- **InputObject**: メタデータを追加する高レベルの操作。これは、`Id`'パラメーターの代わりの方法で、高レベルの操作オブジェクトまたはオブジェクトのリストが PowerShell コマンドに渡されます。
- **Name**: 削除するメタデータのプロパティ名。指定したオブジェクトのすべてのメタデータを削除するには、$null に設定します。
- **Map**: プロパティの（名前、値）ペアのディクショナリ。これは、ハッシュテーブル（@{ “name1” = “val1”; “name2” = “val2” } で作成）または文字列ディクショナリ（new-object “System.Collections.Generic.Dictionary[String, String]” で作成）のいずれかです。名前がマップ内のキーと一致するプロパティは削除されます。

イベントログ

August 17, 2024

次の記事には、Citrix Virtual Apps and Desktops に含まれる各種サービスで記録できるイベントの一覧と説明が記載されています。

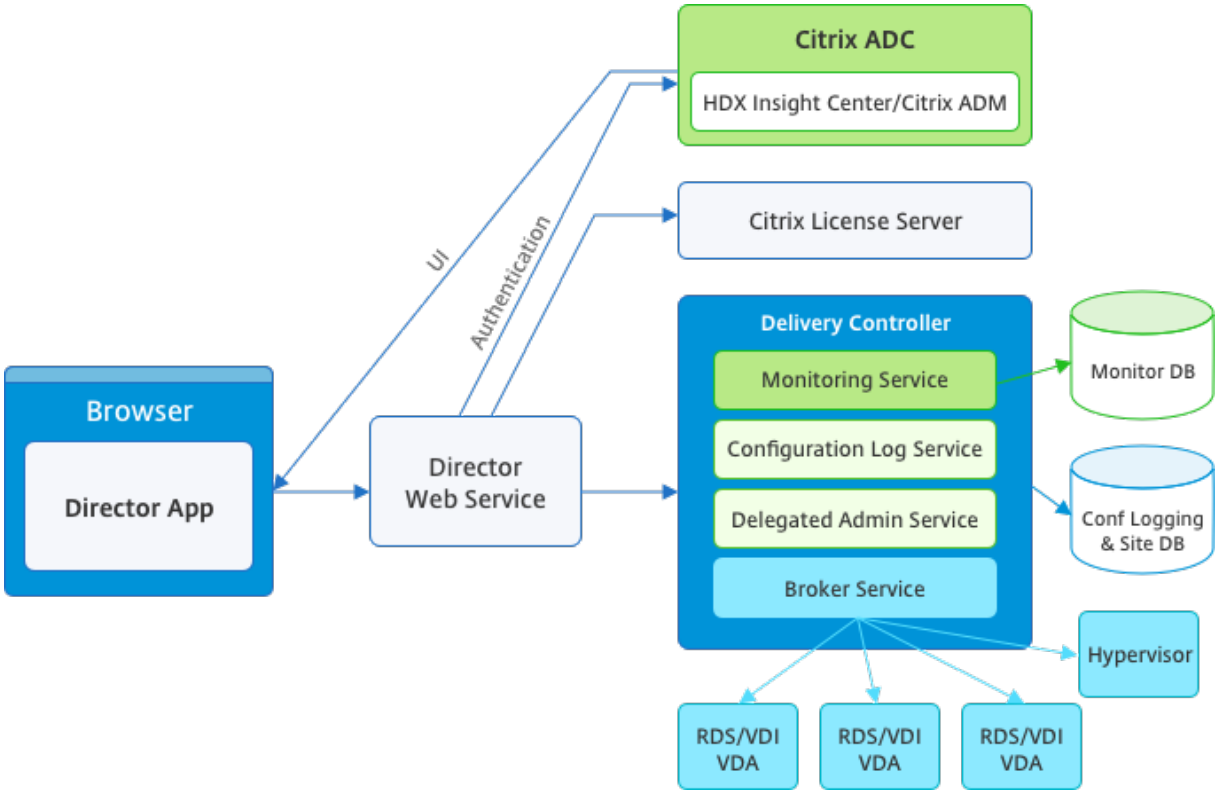
この情報は包括的ではありません。個別の特集記事で、追加のイベント情報を確認してください。

- Citrix Broker Service イベント
- Citrix FMA Service SDK イベント
- Citrix Configuration Service イベント
- Citrix Delegated Administration Service イベント

Director

August 17, 2024

Director は、Citrix Virtual Apps and Desktops の監視およびトラブルシューティングのためのコンソールです。



Director では、以下の情報にアクセスできます。

- Broker Agent からのリアルタイムデータ。Analytics、Performance Manager、および Network Inspector の機能が統合されたコンソールを使用します。Citrix ADM に搭載された以下の分析機能により、Citrix Virtual Apps または Desktops 環境のネットワークに起因するボトルネックを特定します:
  - 健全性と容量保証のためのパフォーマンス管理
  - 履歴傾向とネットワークの分析
- 監視データベースに格納される履歴データ。構成ログデータベースへのアクセスで使用されます。
- Citrix ADM を使用した Citrix Gateway からの ICA データ。
  - Citrix Virtual Apps または Desktops 環境の仮想アプリケーションやデスクトップを使用するエンドユーザーのユーザーエクスペリエンスを視覚化できます。
  - ネットワークデータをアプリケーションデータやリアルタイム測定値に関連付けて効率的にトラブルシューティングを施せます。
  - Citrix Virtual Desktop 7 Director の監視ツールに統合されています。

Director では、Citrix Virtual Apps または Desktops サイトのリアルタイムおよび履歴ヘルス監視を提供するトラブルシューティングダッシュボードが使用されます。この機能により、リアルタイムで問題を確認して、エンドユーザーがどのような問題に直面しているのかを判断できるようになります。

Delivery Controller（DC）、VDA、その他の依存するコンポーネントについての Director の機能の互換性について詳しくは、「機能互換性マトリックス」を参照してください。

> 注:
>
> Meltdown および Spectre の投機的実行のサイドチャネルの脆弱性に関する発表を受けて、Citrix では、問題を軽減する適切なパッチをインストールすることをお勧めしています。これらのパッチは SQL Server のパフォーマンスに影響することがあります。詳しくは、Microsoft のサポート記事「スペクターおよびメルトダウンのサイドチャネルの脆弱性に対する攻撃から SQL Server を保護する」を参照してください。実稼働環境でパッチを展開する前にスケールをテストし、ワークロードを計画することをお勧めします。

Director は、Delivery Controller 上の Web サイトとしてデフォルトでインストールされます。必須要件などについて詳しくは、このリリースのドキュメントの「システム要件」を参照してください。Director のインストールと設定の詳細については、「Director のインストールと設定」を参照してください。

Director へのログオン

Director にログオンするには、Web ブラウザーで https または`http://<Server FQDN>/Director`にアクセスします。

複数サイト環境でいずれかのサイトがダウンしている場合、ログオンに時間がかかる場合があります。これは、ダウンしているサイトへの接続が試行されるためです。

Director での PIV スマートカード認証の使用

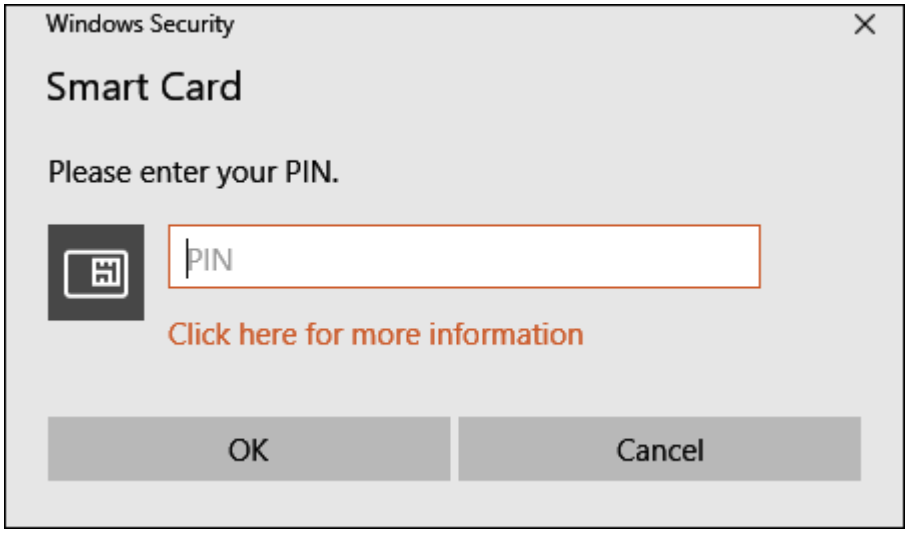
Director で、ログオンのために Personal Identity Verification（PIV）ベースのスマートカード認証がサポートされるようになりました。この機能は、アクセス制御にスマートカードベースの認証を使用する組織や政府機関に役立ちます。
スマートカード認証には、Director サーバーと Active Directory での特定の構成が必要となります。構成手順について詳しくは、「PIV スマートカード認証の構成」を参照してください。

> 注:
>
> スマートカード認証は、同じ Active Directory ドメインからのユーザーに対してのみサポートされています。

必要な構成を実行した後は、スマートカードを使用して Director にログオンできます。

1. スマートカードをスマートカードリーダーに挿入します。
2. Web ブラウザーを開き、Director の URL（`https://<directorfqdn>/Director`）に移動します。
3. 表示された一覧から有効なユーザー証明書を選択します。

4. スマートカードトークンを入力します。



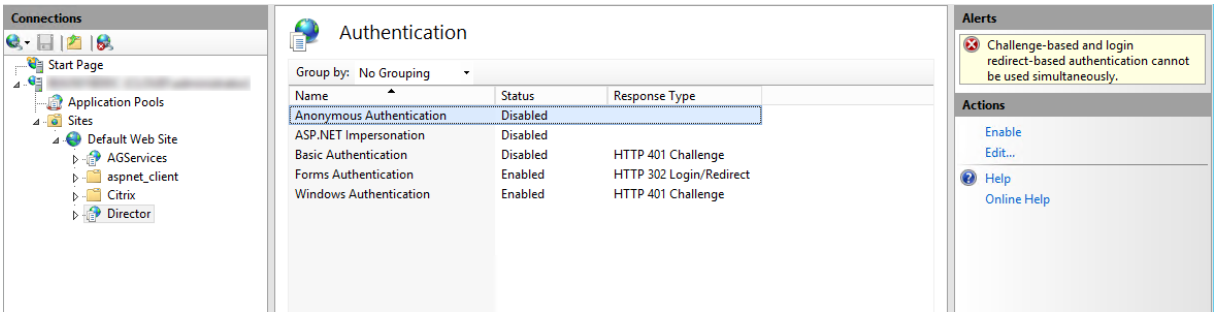
5. 認証されると、Director ログオンページで追加の資格情報を入力せずに Director にアクセスできます。

Director での統合 **Windows** 認証の使用

統合 Windows 認証（IWA）を使うと、ドメイン参加のユーザーは、Director のログオンページに資格情報を再度入力しなくても、Director に直接アクセスできます。Director での統合 Windows 認証の使用には、以下の前提条件があります:

- Director をホストしている IIS Web サイトで統合 Windows 認証を有効化します。Director をインストールするときには、匿名認証とフォーム認証が有効化されています。Director で統合 Windows 認証を使用するには、匿名認証を無効化し、Windows 認証を有効化します。フォーム認証は、非ドメインユーザーを認証するために、有効化したままにしておく必要があります。

  1. IIS マネージャーを起動します。
  2. ［サイト］>［既定の **Web** サイトのホーム］>［**Director**］に移動します。
  3. ［認証］を選択します。
  4. ［**Anonymous Authentication**］を右クリックし、［無効化］を選択します。
  5. ［**Windows** 認証］を右クリックし、［有効化］を選択します。



- Director マシンの Active Directory 委任アクセス許可を構成します。構成は、Director と Delivery Controller が異なるマシンにインストールされている場合のみ必要です。

  1. Active Directory マシンで、Active Directory 管理コンソールを開きます。
  2. Active Directory 管理コンソールで、［ドメイン名］>［コンピューター］の順に移動します。Director マシンを選択します。
  3. 右クリックし、［プロパティ］を選択します。
  4. ［プロパティ］で ［委任］タブを選択します。
  5. ［**Trust this computer for delegation to any service (Kerberos only)**］オプションを選択します。

- Director へのアクセスに使用するブラウザーは、統合 Windows 認証をサポートしている必要があります。Firefox と Chrome では、さらに構成作業が必要になる場合があります。詳しくは、ブラウザーのドキュメントを参照してください。
- Monitoring Service では、Director のシステム要件に記載されている Microsoft.NET Framework 4.5.1 以降のバージョンが実行されている必要があります。詳しくは、「システム要件」を参照してください。

ユーザーが Director をログオフするか、セッションがタイムアウトすると、ログオンページが表示されます。ログオンページで認証の種類を ［自動ログオン］または ［ユーザー資格情報］に設定できます。

インターフェイスのビュー

Director では、管理者ごとに異なるインターフェイス（ビュー）が表示されます。Citrix 管理者の権限により、表示される内容と実行できるコマンドが異なります。

たとえば、ヘルプデスク管理者にはヘルプデスクタスク用のインターフェイスが表示されます。ヘルプデスク管理者は、問題を報告しているユーザーを Director で検索し、そのユーザーに関するアクティビティを表示できます。たとえば、ユーザーのアプリケーションとプロセスの状態です。ヘルプデスク管理者は応答しないアプリケーションやプロセスを終了したり、ユーザーのマシン上の操作をシャドウしたり、マシンを再起動したり、ユーザープロファイルを再設定したりして問題を解決できます。

これに対して、すべての管理タスクの実行権限を持つ管理者はサイト全体を表示および管理でき、複数のユーザーやマシンに対してコマンドを実行できます。Dashboard には、セッションの状態、ユーザーのログオン、およびサイトインフラストラクチャなど、展開の主な要素に関する概要が表示されます。情報は 1 分ごとに更新されます。問題が発生すると、発生した問題の数や種類に関する詳細が自動的に表示されます。

Director でのさまざまな役割とその権限について詳しくは、「管理権限の委任と Director」を参照してください

Pendo による使用状況データ収集

Director がインストールされると、Director サービスは Pendo を使った利用状況データの収集を開始します。［傾向］ページと OData API 呼び出し分析の使用状況に関する統計が収集されます。Analytics のコレクションは、

Citrix プライバシーポリシーに準拠しています。Director をインストールすると、データ収集はデフォルトで有効になります。

Pendo のデータ収集をオプトアウトするには、Director がインストールされているマシンでレジストリキーを編集します。レジストリキーが存在していない場合は、作成して目的の値に設定します。レジストリキー値を変更した後、Director インスタンスを更新します。

注意：レジストリエディターを誤って使用すると深刻な問題が発生する可能性があり、オペレーティングシステムの再インストールが必要になることがあります。レジストリエディターの誤用による障害に対して、Citrix では一切責任を負いません。レジストリエディターは、お客様の責任と判断の範囲でご使用ください。変更前に Windows レジストリのバックアップを作成してください。

場所：HKEY_LOCAL_MACHINE\Software\Citrix\Director

値の名前：DisableGoogleAnalytics

> 注：
>
> 以前は、Director サービスは Google Analytics を使用してデータを収集していました。同じレジストリ キーが Pendo でも使用されるようになりました。

値：0 = 有効（デフォルト）、1 = 無効

次の PowerShell コマンドレットを使用して、Pendo によるデータ収集を無効にすることができます：

```
New-Item HKLM:\SOFTWARE\Citrix -Name Director

New-ItemProperty HKLM:\SOFTWARE\Citrix\Director -Name
    DisableGoogleAnalytics -PropertyType DWORD -Value 1
```

新機能ガイド

Director には、最新バージョンでリリースされた新機能に関する情報を提供するためにPendoを使用した製品内ガイドがあります。このガイドは、簡単な概要と適切な製品内メッセージを組み合わせているため、製品の新機能を理解するのに役立ちます。

この機能をオプトアウトするには、Director がインストールされているマシンで以下のようにレジストリキーを編集します。レジストリキーが存在していない場合は、作成して目的の値に設定します。レジストリキー値を変更した後、Director インスタンスを更新します。

> 注意：
>
> レジストリエディターの使用を誤ると、深刻な問題が発生する可能性があり、オペレーティングシステムの再インストールが必要になる場合もあります。レジストリエディターの誤用による障害に対して、Citrix では一切責任を負いません。レジストリエディターは、お客様の責任と判断の範囲でご使用ください。変更前に Windows レジストリのバックアップを作成してください。

場所：HKEY_LOCAL_MACHINE\Software\Citrix\Director

値の名前：DisableGuidedHelp

値：0 = 有効（デフォルト）、1 = 無効

次の PowerShell コマンドレットを使用して、製品内ガイドを無効にできます：

```
New-Item HKLM:\SOFTWARE\Citrix -Name Director

New-ItemProperty HKLM:\SOFTWARE\Citrix\Director -Name DisableGuidedHelp
    -PropertyType DWORD -Value 1
```

参考記事

- Reduce MTTR from Citrix Director
- Citrix Director - Manage and configure alerts and notifications with PowerShell
- Citrix Virtual Apps and Desktops の開発者ドキュメント

関連製品の新着情報

- Citrix DaaS
- StoreFront
- Secure Private Access
- Citrix Enterprise Browser
- Citrix Workspace
- Provisioning

インストールと構成

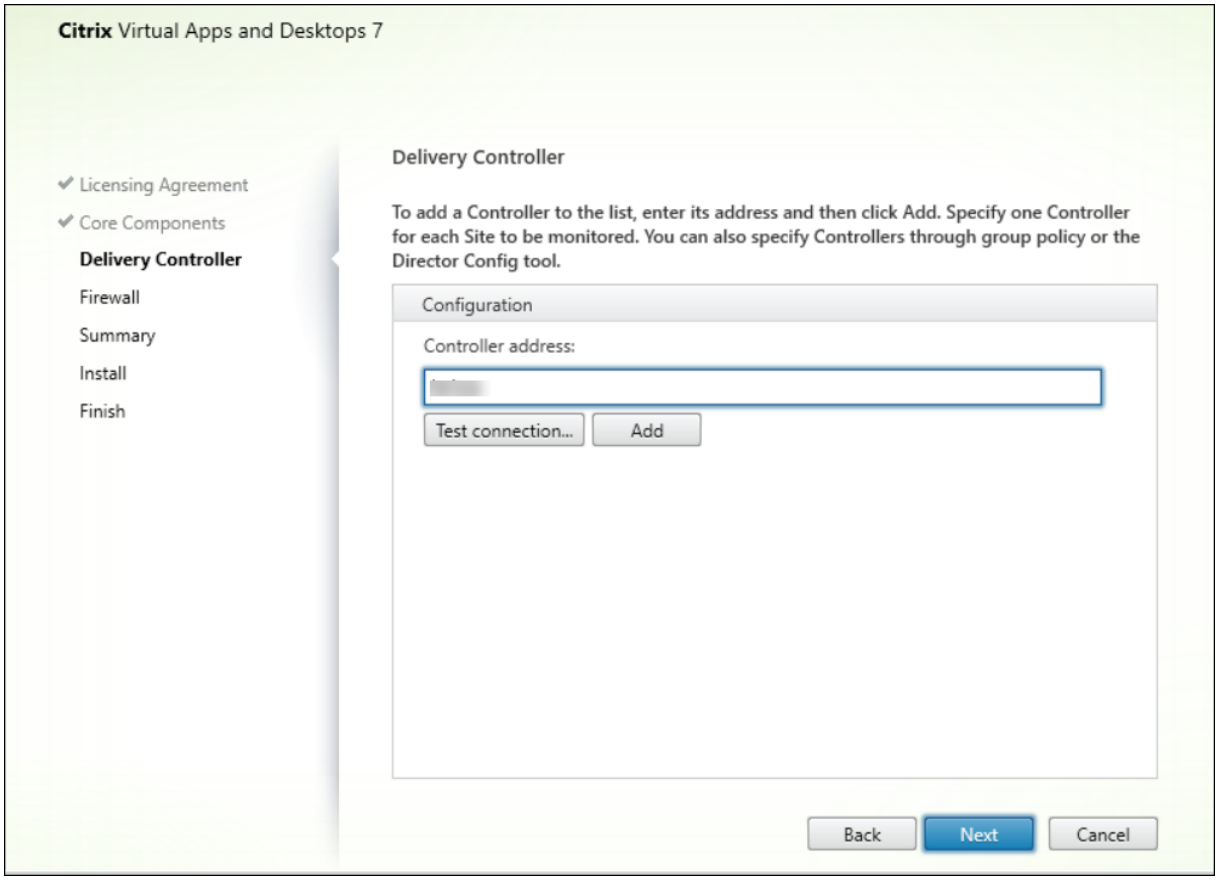
August 17, 2024

Director のインストール

Director のインストールは、Citrix Virtual Apps and Desktops 用の全製品 ISO インストーラーを使って行います。このインストーラーは、前提条件をチェックして不足しているコンポーネントをすべてインストールし、Director の Web サイトをセットアップして、基本的な構成を行います。必須要件などについて詳しくは、このリリースのドキュメントの「システム要件」を参照してください。このリリースの Director には、Virtual Apps 6.5 以前の環境または Virtual Desktops 7 以前の環境との互換性はありません。
ISO インストーラーによるデフォルトの構成のままでも、一般的な展開を管理できます。インストール時に Director

を含めなかった場合は、ISO インストーラーを再度実行して Director をインストールします。追加のコンポーネントをインストールするには、ISO インストーラーを再度実行して必要なコンポーネントを選択します。ISO インストーラーの使用について詳しくは、インストールに関するドキュメントで「コアコンポーネントのインストール」を参照してください。個々の MSI ファイルではなく、全製品 ISO インストーラーを実行して各コンポーネントをインストールすることをお勧めします。

Controller 上に Director をインストールすると、Director は localhost をサーバーアドレスとして自動的に構成され、デフォルトでローカルの Controller と通信します。Controller とは別の専用サーバー上に Director をインストールする場合は、Controller の完全修飾ドメイン名（FQDN）または IP アドレスを指定する必要があります。



> 注:
>
> 監視対象の Controller を追加するには、［追加］をクリックします。

Director は、ここで指定したアドレスの Controller と通信します。監視する各サイトに Controller のアドレスを 1 つのみ指定します。Director で同じサイト内の他のすべての Controller が自動検出され、指定した Controller にエラーが発生した場合はそれらの他の Controller にフォールバックされます。

> 注:
>
> Director は、Controller 間で負荷分散を行いません。

Web ブラウザーと Web サーバー間の通信を保護するため、Director をホストする IIS Web サイトで TLS を実装

することをお勧めします。手順については、Microsoft 社の IIS ドキュメントを参照してください。Director 側では、TLS を有効にするために何らかの構成を行う必要はありません。

Director の展開と構成

複数のサイトがある環境で Director を使用している場合、Controller、Director、およびその他のコアコンポーネントがインストールされているすべてのサーバーのシステムクロックを同期させる必要があります。システムクロックが同期していない場合、Director にサイトの情報が正しく表示されないことがあります。

> 重要:
>
> ユーザー名とパスワードがプレーンテキストで送信されないように、Director 接続では HTTP ではなく HTTPS での接続のみを許可します。特定のツールを使用すると、HTTP（非暗号化）ネットワークパケット内のプレーンテキストのユーザー名やパスワードを読み取ることができるため、ユーザーにとってセキュリティ上のリスクとなる場合があります。

権限を構成する

Director にログオンする管理者は、Active Directory ドメインユーザーで、以下の権限を持っている必要があります:

- 検索するすべての Active Directory フォレストを読み取る権限（「詳細構成」を参照）
- 構成済みの委任管理者の役割（「管理権限の委任と Director」を参照）。
- ユーザーをシャドウするには、Windows リモートアシスタンスの Microsoft グループポリシーを使って管理者を構成する必要があります。また、次のように指定します:
  - VDA をインストールするすべてのユーザーデバイス上で、Windows リモートアシスタンス機能が有効である必要があります。この機能は、デフォルトで有効になっています。
  - Director をインストールするサーバーに、Windows リモートアシスタンス機能がインストールされている必要があります。この機能は、デフォルトでインストールされています。ただし、デフォルトでは無効になっています。Director を使ってエンドユーザーを支援する場合、この機能を有効にする必要はありません。セキュリティ上の理由から、この機能を無効にしておくことをお勧めします。
  - 管理者が Windows リモートアシスタンスを開始できるようにするには、適切な Microsoft グループポリシー設定を使用して管理者に必要な権限を付与します。詳しくは、CTX127388: How to Enable Remote Assistance for Desktop Directorを参照してください。

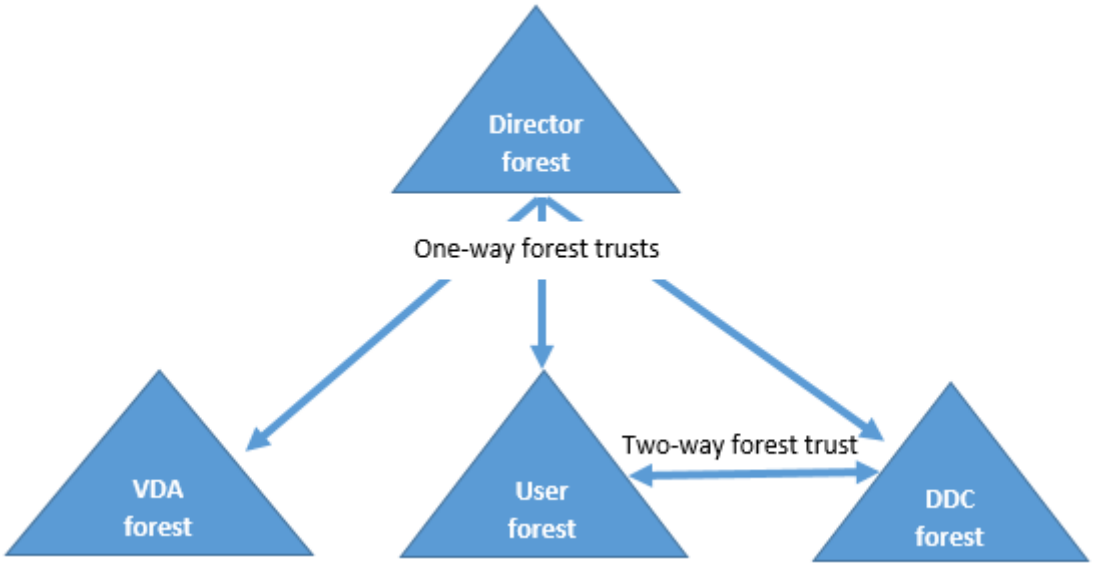
詳細な構成

August 17, 2024

Director は、ユーザー、Delivery Controller（DC）、VDA、および Director が異なるフォレストに存在するフォレスト構成に広がるマルチフォレスト環境をサポートできます。このためには、フォレストと構成設定の間の信頼関係を適切にセットアップする必要があります。

マルチフォレスト環境での推奨構成

推奨構成では、全ドメイン認証を使用してフォレスト間の送受信フォレスト信頼関係を作成する必要があります。



Director からの信頼関係があると、管理者は異なるフォレストに存在するユーザーセッション、VDA、および Delivery Controller の問題をトラブルシューティングできます。

Director による複数のフォレストのサポートに必要な詳細構成は、インターネットインフォメーションサービス（IIS）マネージャーの設定を介して制御します。

> 重要:
>
> IIS の設定を変更すると、Director サービスが自動的に再起動してユーザーをログオフします。

IIS を使って詳細設定を構成するには、次の手順に従います。

1. インターネットインフォメーションサービス（IIS）マネージャーコンソールを開きます。
2. ［Default Web Site］ノードを開き、［Director］Web サイトを選択します。
3. ［アプリケーションの設定］をダブルクリックします。
4. 編集する設定をダブルクリックします。
5. 新しい設定を追加するには ［追加］をクリックします。

Director は Active Directory を使ってユーザーを検索し、ユーザーおよびマシンの追加情報を照会します。Director のデフォルトでは、以下のドメインまたはフォレストが検索されます。

- 管理者のアカウント属しているドメインやフォレスト。

- Director の Web サーバーが属しているドメインやフォレスト（管理者が属しているものと異なる場合）。

Director では、Active Directory グローバルカタログによるフォレストレベルでの検索が試行されます。管理者にフォレストレベルで検索する権限がない場合、ドメインのみが検索されます。

ほかの Active Directory ドメインまたはフォレストからのデータを検索または照会するには、対象のドメインまたはフォレストを明示的に設定する必要があります。次のアプリケーション設定を IIS マネージャーの Director Web サイトに構成します：

```
Connector.ActiveDirectory.Domains = (user),(server)
```

値属性 user および server は、それぞれ Director ユーザー（つまり管理者）のドメインおよび Director サーバーのドメインを表しています。

ほかのドメインまたはフォレストからのデータを検索するには、次のようにドメイン名をリストに追加します：

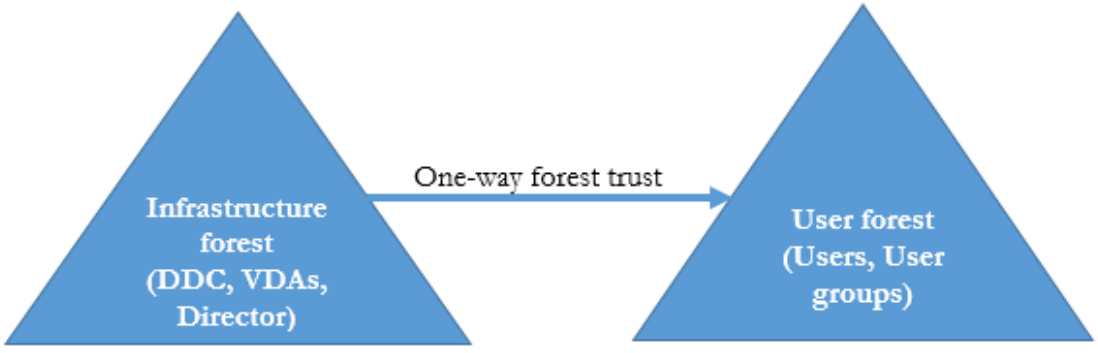
```
Connector.ActiveDirectory.Domains = (user),(server),\<domain1\>,\<
    domain2\>
```

リストに追加した各ドメインについて、Director によりフォレストレベルの検索が試行されます。管理者にフォレストレベルで検索する権限がない場合、ドメインのみが検索されます。

ドメインローカルグループの設定

ほとんどの Citrix Service Provider（CSP）は、Infrastructure フォレストに、VDA、DC、および Director で構成される同様の環境設定を備えています。ユーザーまたはユーザーグループのレコードは、Customer フォレストに属します。Infrastructure フォレストから Customer フォレストへの一方向の送信の信頼が存在します。

CSP 管理者は、通常、Infrastructure フォレスト内にドメインローカルグループを作成し、Customer フォレスト内のユーザーまたはユーザーグループをこのドメインローカルグループに追加します。



Director は、このようなマルチフォレストの設定をサポートし、ドメインローカルグループを使用して構成されたユーザーのセッションを監視できます。

1. 次のアプリケーション設定を IIS マネージャーの Director Web サイトに追加します：


```
Connector.ActiveDirectory.DomainLocalGroupSearch= true

DomainLocalGroupSearchDomains= \<domain1\>,\<domain2\>
```

<domain1><domain2> は、ドメインローカルグループが存在するフォレストの名前です。

2. Web Studio でドメインローカルグループをデリバリーグループに割り当てます。
3. 変更を有効にするには、IIS を再起動して Director に再度ログオンします。これで、Director でこれらのユーザーのセッションを監視して表示できます。

Director へのサイトの追加

Director がインストール済みの場合は、複数のサイトを監視できるように構成できます。構成するには、各 Director サーバー上で IIS マネージャーコンソールを使って［アプリケーションの設定］のサーバーアドレスの一覧を更新します。

各サイトの Controller のアドレスを次の設定に追加します:

```
Service.AutoDiscoveryAddresses = SiteAController,SiteBController
```

SiteAController と SiteBController は、2 つの異なるサイトの Delivery Controller のアドレスです。

アクティビティマネージャーで実行中のアプリケーションを非表示にする

Director のアクティビティマネージャーのデフォルトでは、そのユーザーのセッションで実行されているすべてのアプリケーションが一覧表示されます。この情報を表示するには、Director のアクティビティマネージャー機能へのアクセス権限が必要です。この権限を持つ管理者の役割は、すべての管理権限を実行できる管理者、デリバリーグループ管理者、およびヘルプデスク管理者です。

ユーザーのプライバシーと、ユーザーが使用しているアプリケーションを保護するために、［アプリケーション］タブでアプリケーションの一覧を非表示にできます。

> 警告:
>
> レジストリエディターの使用を誤ると、深刻な問題が発生する可能性があり、オペレーティングシステムの再インストールが必要になる場合もあります。レジストリエディターの誤用による障害に対して、Citrix では一切責任を負いません。レジストリエディターは、お客様の責任と判断の範囲でご使用ください。また、レジストリファイルのバックアップを作成してから、レジストリを編集してください。

1. VDA で、レジストリキー HKEY_LOCAL_MACHINE\Software\Citrix\Director\TaskManagerDataDisplayed を変更します。デフォルトでは 1 に設定されています。値を 0 に変更すると、VDA から情報が収集されなくなるため、アクティビティマネージャーに情報が表示されなくなります。
2. Director がインストールされたサーバー上で、実行中のアプリケーションの表示を制御する設定を変更します。デフォルトの値は「true」で、これにより［アプリケーション］タブに実行中のアプリケーションの一覧

が表示されます。値を「false」に変更すると、アプリケーションの一覧が表示されなくなります。このオプションは、VDA ではなく Director のアクティビティマネージャーにのみ適用されます。
次の設定で値を変更します:
UI.TaskManager.EnableApplications = false

> 重要:
>
> 実行中のアプリケーションの表示を無効にするには、これらの両方の値を変更して、アクティビティマネージャーにデータが表示されなくなるようにしてください。

PIV スマートカード認証の構成

August 17, 2024

この記事では、スマートカード認証機能を有効にするために Director サーバーと Active Directory で必要な構成について説明します。

> 注:
>
> スマートカード認証は、同じ Active Directory ドメインからのユーザーに対してのみサポートされています。

Director サーバー構成

Director サーバーで、次の構成手順を実行します。

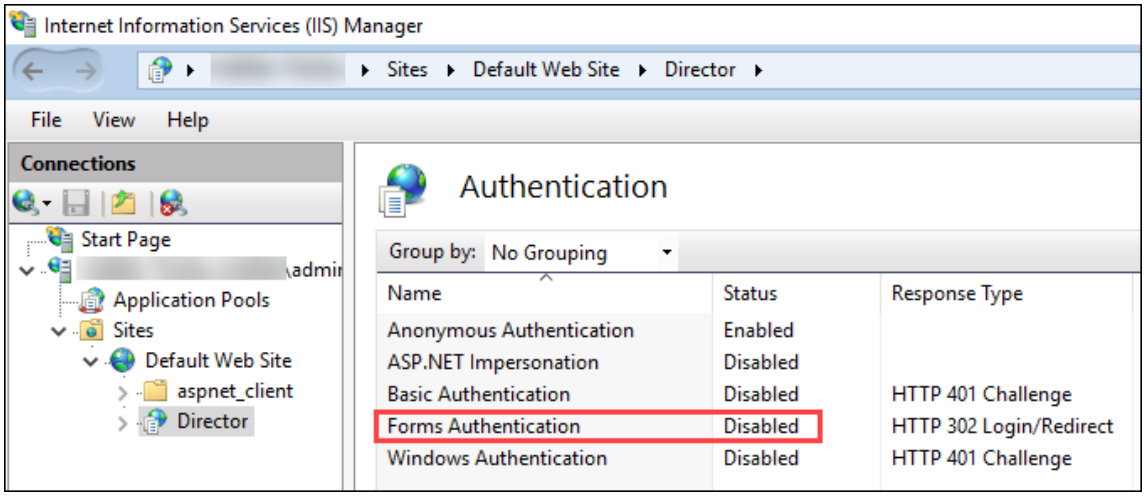
1. クライアント証明書マッピング認証をインストールして有効にします。Microsoft のドキュメント「Client Certificate Mapping Authentication」の「**Client Certificate Mapping authentication using Active Directory**」の説明に従います。
2. Director サイトでフォーム認証を無効にします。

   IIS マネージャーを起動します。

   [サイト] > [既定の **Web** サイトのホーム] > [**Director**] に移動します。

   [認証] を選択します。

   [フォーム認証] を右クリックし、[無効化] を選択します。



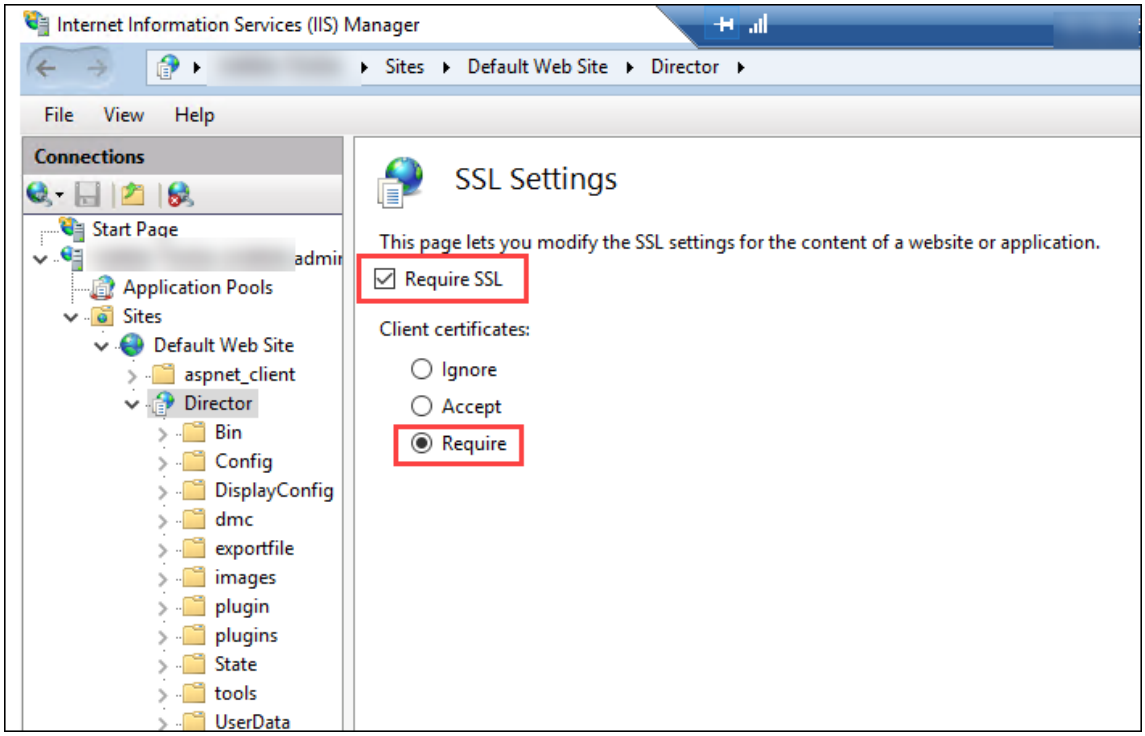
3. クライアント証明書認証として、Director URL に、より安全な https プロトコル（HTTP ではなく）を構成します。

   a) IIS マネージャーを起動します。

   b) ［サイト］> ［既定の **Web** サイトのホーム］> ［**Director**］に移動します。

   c) ［**SSL** 設定］を選択します。

   d) ［**SSL** を必須にする］および ［クライアント証明書］> ［必須］を選択します。



4. web.config を更新します。テキストエディターを使用して web.config ファイル(c:\inetpub\wwwroot\Director にある）を開きます。

<system.webServer>親要素の下で、最初の子要素として次のスニペットを追加します:

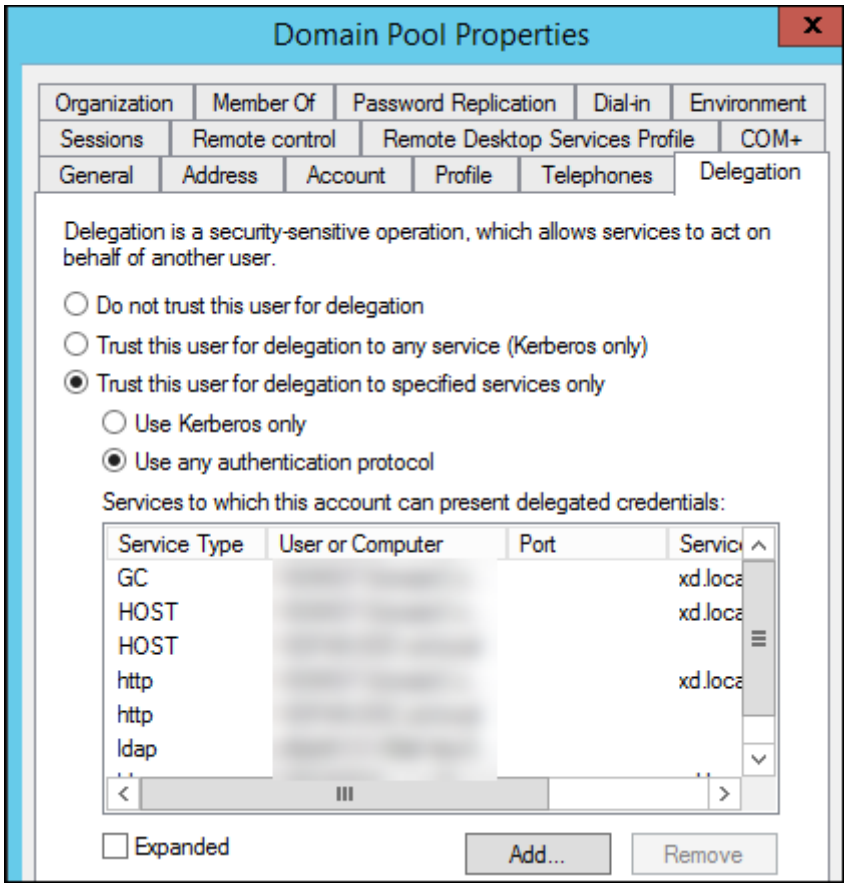
```
<defaultDocument>
   <files>
       <add value="LogOn.aspx"/>
   </files>
</defaultDocument>
```

Active Directory 構成

デフォルトでは、Director アプリケーションは、アプリケーションプール ID プロパティを使用して実行されます。スマートカード認証には委任が必要であり、この委任には、Director アプリケーション ID にサービスホスト上の TCB（Trusted Computing Base）特権が必要となります。

アプリケーションプール ID 用に別個のサービスアカウントを作成することを Citrix ではお勧めします。Microsoft の MSDN の記事「Protocol Transition with Constrained Delegation Technical Supplement」内の説明に従って、サービスアカウントを作成し、TCB 特権を割り当てます。

新しく作成したサービスアカウントを Director アプリケーションプールに割り当てます。次の図は、サンプルサービスアカウント Domain Pool のプロパティダイアログです。

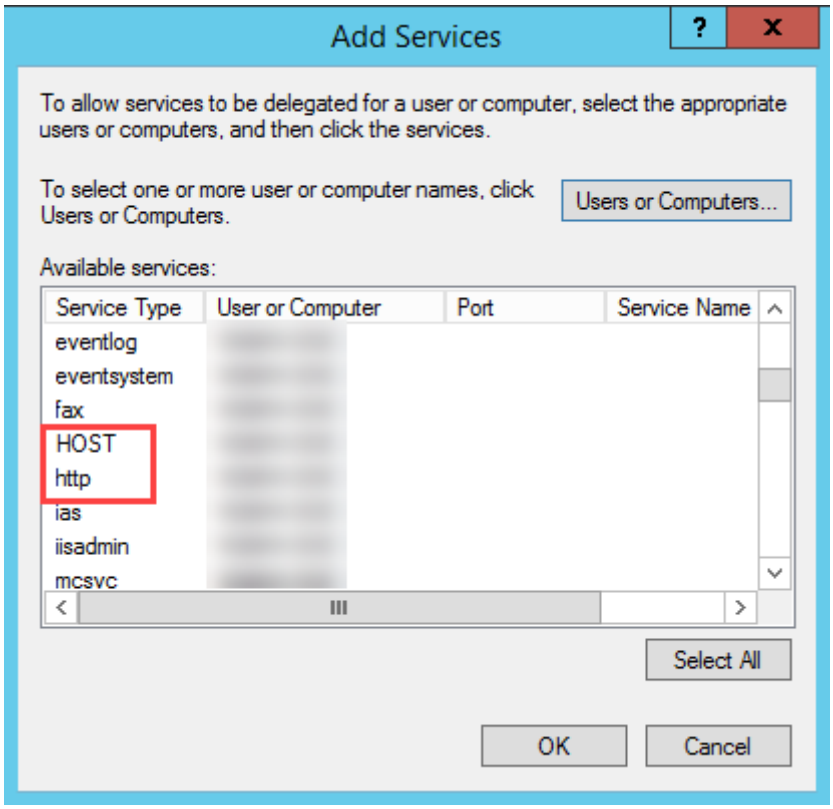


このアカウント用に以下のサービスを構成します:

- Delivery Controller：HOST、HTTP
- Director：HOST、HTTP
- Active Directory：GC、LDAP

構成するには、

1. ユーザーアカウントのプロパティダイアログで、［追加］をクリックします。
2. ［サービスの追加］ダイアログで、［ユーザーまたはコンピューター］をクリックします。
3. Delivery Controller ホスト名を選択します。
4. ［使用可能なサービス］一覧から、［HOST］および［HTTP］サービスタイプを選択します。



同様に、**Director** および **Active Directory** のホストのサービスタイプを追加します。

サービスプリンシパル名レコードの作成

各 Director サーバーのサービスアカウントと、Director サーバーのプールへのアクセスに使用される負荷分散された仮想 IP（VIP）を作成する必要があります。新しく作成したサービスアカウントへの委任を構成するには、サービスプリンシパル名（SPN）レコードを作成する必要があります。

- 次のコマンドを使用して、Director サーバーの SPN レコードを作成します：

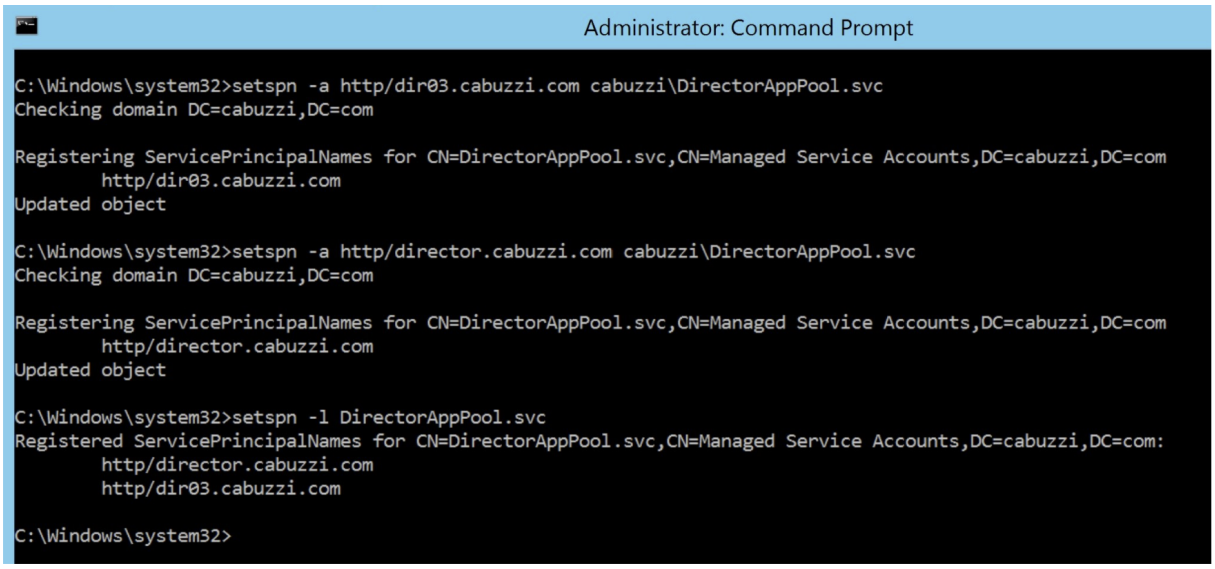

```
setspn -a http/<directorServer>.<domain_fqdn> <domain><
    DirectorAppPoolServiceAcct>
```

- Use the following command to create an SPN record for a load-balanced VIP:

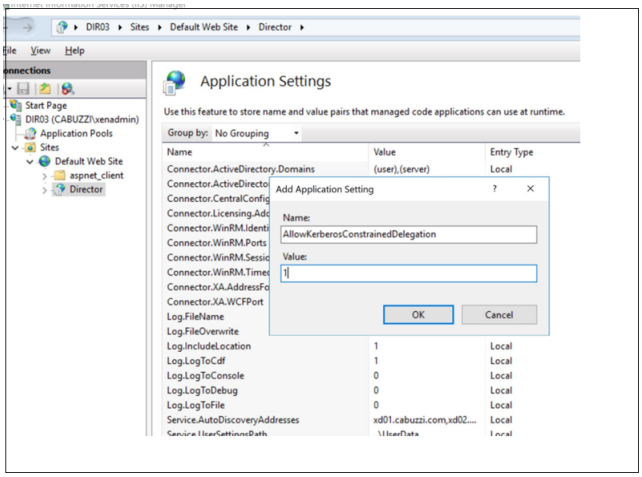
```
setspn -S http/<DirectorFQDN> <domain>\<
    DirectorAppPoolServiceAcct>
```

- 作成された SPN を表示またはテストするには、次のコマンドを使用します:

```
setspn  -l <DirectorAppPoolServiceAcct>
```



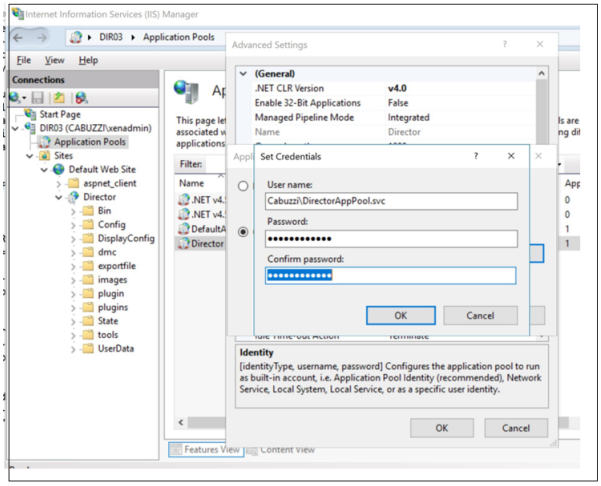
- Select the Director virtual directory in the left pane and double click **Application Settings**. Inside the Application Settings window, click **Add** and ensure **AllowKerberosConstrainedDelegation** is set to 1.



- Select **Application Pools** in the left-hand pane, then right-click the Director application pool

and select **Advanced Settings**.

- Select **Identity**, click the ellipses (“…”) to enter the service account domain\logon and password credentials. Close the IIS console.

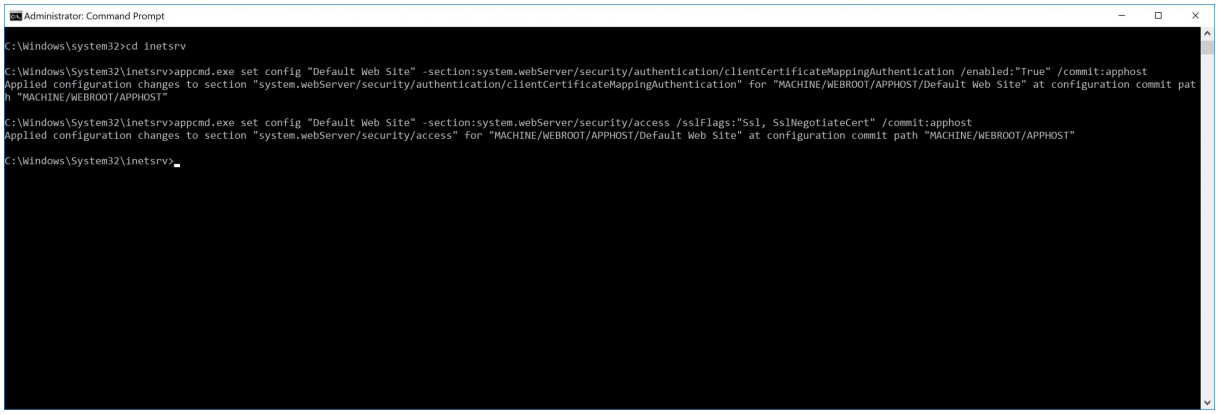


- From an elevated command prompt, change the directory to C:\Windows\System32\inetsrv and enter the following commands:

```
1    appcmd.exe set config “Default Web Site” -section:system.webServer
       /security/authentication/clientCertificateMappingAuthentication /
       enabled:” True” /commit:apphost
```

“‘

```
1  appcmd.exe set config “Default Web Site” -section:system.webServer/
     security/access /sslFlags:” Ssl, SslNegotiateCert” /commit:apphost
     \`\`\`
```



Firefox ブラウザー構成

Firefox ブラウザーを使用するには、OpenSC 0.17.0で使用可能な PIV ドライバーをインストールします。インストールと構成の手順については、「Installing OpenSC PKCS#11 Module in Firefox, Step by Step」を参照してください。
Director でスマートカード認証機能を使用する方法については、Director の記事で「Director での PIV スマートカード認証の使用」のセクションを参照してください。

ネットワーク分析機能の構成

August 17, 2024

> 注:
> この機能は、組織のライセンスおよび管理者権限によっては使用できない場合があります。

Director は、Citrix ADM との統合により、次のようなネットワーク分析機能とパフォーマンス管理機能を提供します:

- ネットワーク分析機能では、Citrix ADM の HDX Insight を使用して、ネットワークのアプリケーションおよびデスクトップのコンテキストビューを提供します。この機能を使用すると、Director で ICA トラフィックを高度に分析できます。
- パフォーマンス管理機能により、履歴保持および傾向に関するレポートを生成できます。データの履歴保持とリアルタイム評価により、管理者はサーバーのキャパシティとヘルスに関する傾向レポートを作成できます。

Director でこの機能を有効にすると、HDX Insight レポートにより以下の追加情報が Director に提供されます。

- [傾向] ページの [ネットワーク] タブには、展開環境全体におけるアプリケーション、デスクトップ、ユーザーに対する遅延と帯域幅の影響が表示されます。
- [ユーザーの詳細] ページには、特定のユーザーセッションに特化した遅延と帯域幅情報が表示されます。

制限事項:

- [傾向] ビューでは、XenDesktop 7 よりも前のバージョンの VDA については HDX 接続のログオンデータが収集されません。以前のバージョンの VDA については、グラフのデータが 0 として表示されます。

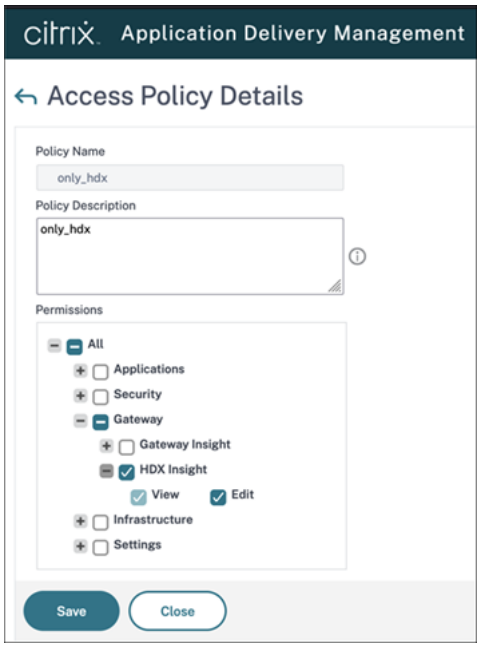
ネットワーク分析機能を有効にするには、Director に Citrix ADM をインストールし、構成する必要があります。Director には、Citrix ADM Version 11.1 Build 49.16 以降が必要です。NetScaler MAS は、XenServer で実行される仮想アプライアンスです。Director では、ネットワーク分析により、環境のトラフィック情報を収集します。

詳しくは、Citrix ADMのドキュメントを参照してください。

> 注:
>
> Citrix NetScaler Insight Center のメンテナンスは、2018 年 5 月 15 日時点で終了しました。「Citrix の製品マトリクス」を参照してください。ネットワーク分析機能を利用するには、Director を Citrix ADM と統合してください。NetScaler Insight Center から Citrix ADM への移行方法については、「NetScaler Insight Center から Citrix ADM への移行」を参照してください。

1. Director がインストールされているサーバー上のコマンドラインプロンプトで、C:\inetpub\wwwroot\Director\tools にある DirectorConfig コマンドに/configNetscaler パラメーターを指定して実行します。
2. 画面上の指示に従って、Citrix ADM マシン名（完全修飾ドメイン名または IP アドレス）、ユーザー名、パスワード、および接続の種類として HTTPS（HTTP よりも望ましい）を入力して、Citrix ADM との統合を選択します。
3. 変更を確認するには、いったんログオフして再ログオンします。

> 注:
>
> セキュリティ上の理由から、HDX Insight のみにアクセスするために必要な権限を持つ ADM の Director への統合用のカスタムロールを作成することをお勧めします。



詳しくは、「アクセスポリシーの構成」を参照してください。

委任管理と **Director**

August 17, 2024

管理権限の委任機能では、管理者、役割、およびスコープという 3 つの概念が使用されます。管理者の権限は、その管理者の役割とそのスコープに基づいて定義されます。たとえば、管理者にヘルプデスク管理者の役割を割り当てて、その役割のスコープとして特定のサイトのエンドユーザーを指定できます。

委任管理者の作成について詳しくは、「委任管理」を参照してください。

付与されている管理権限により、その管理者に表示される Director のインターフェイスと実行可能なタスクが決定されます。権限により、次の内容が決定されます。

- その管理者がアクセスできる Director の表示内容。これを「ビュー」と呼びます。
- その管理者が表示したり操作したりできるデスクトップ、マシン、およびセッション。
- ユーザーセッションのシャドウやメンテナンスモードの有効化など、その管理者が実行できるコマンド。

組み込みの役割および権限によっても、管理者が Director で実行できるタスクが決定されます。

管理者の役割	Director での権限
完全な管理者	すべてのビューに制限なくアクセスして、ユーザーセッションのシャドウ、メンテナンスモードの有効化、傾向データのエクスポートなどすべてのコマンドを実行できます。
デリバリーグループ管理者	すべてのビューに制限なくアクセスして、ユーザーセッションのシャドウ、電源管理とセッション管理、メンテナンスモードの有効化、傾向データのエクスポートなどすべてのコマンドを実行できます。
読み取り専用管理者	すべてのビューに制限なくアクセスして、指定されているスコープのすべてのオブジェクトと一般的な情報を表示できます。HDX チャネルからレポートをダウンロードして、[傾向] ビューのエクスポートオプションを使って傾向データをエクスポートできます。そのほかのコマンドは実行できず、ビューで設定を変更することはできません。
ヘルプデスク管理者	[ヘルプデスク] および [ユーザーの詳細] ビューにのみアクセスでき、委任されたオブジェクトのみを表示できます。ユーザーセッションをシャドウしたり、そのユーザーに対してコマンドを実行したりできます。メンテナンスモードを有効にしたり解除したりできます。シングルセッションOS マシンの電源制御オプションを使用できます。[ダッシュボード] ビュー、[傾向] ビュー、[アラート] ビュー、および [フィルター] ビューにはアクセスできません。マルチセッション OS マシンの電源制御オプションは使用できません。

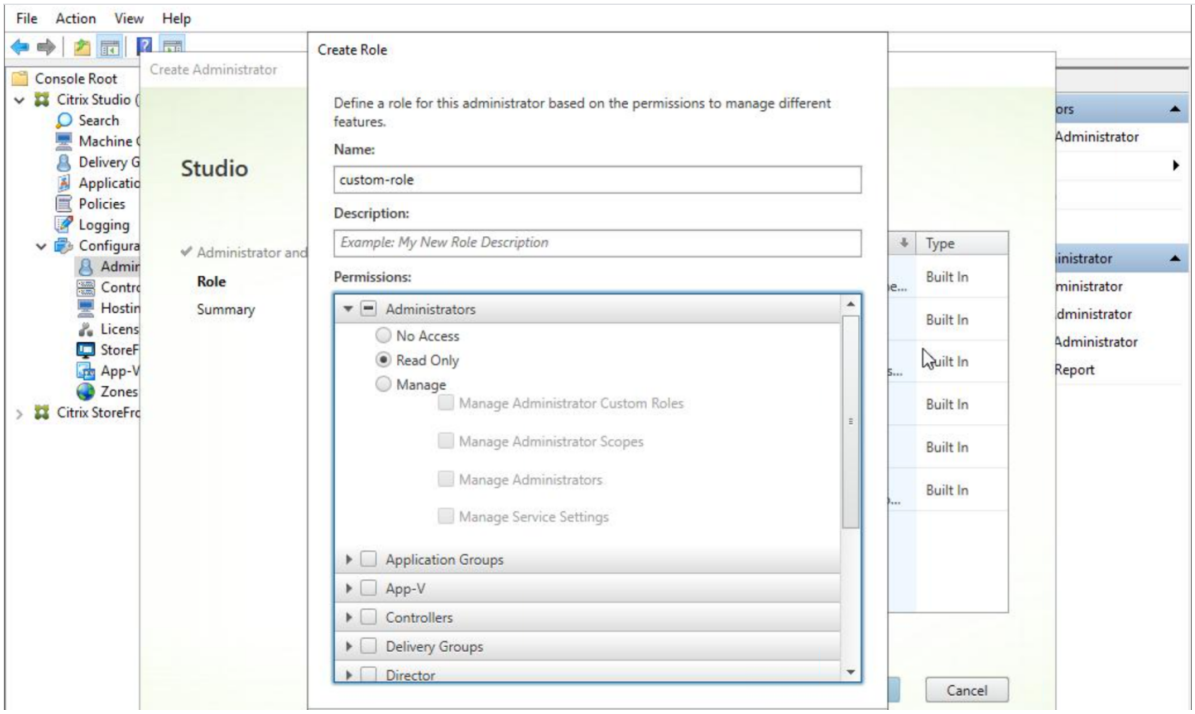
管理者の役割	Director での権限
マシンカタログ管理者	［マシン詳細］ページ（マシンベースの検索）にのみアクセスできます。
ホスト管理者	アクセスなし。この管理者は、Director を使用したりデータを表示したりできません。

Director 管理者のカスタム役割を構成する

Studio では、組織の要件に応じて Director 用のカスタムの役割を構成して、管理権限を柔軟に委任できます。たとえば、組み込みのヘルプデスク管理者の役割を制限して、この管理者がユーザーのセッションをログオフすることを禁止できます。

Director 用のカスタムの役割を作成する場合は、その役割に以下の一般的な権限も付与する必要があります:

- Director にログオンするための Delivery Controller 権限 - 少なくとも管理者ノードでの読み取り専用アクセス
- デリバリーグループのデータを Director で閲覧するための権限 - 少なくとも読み取り専用アクセス

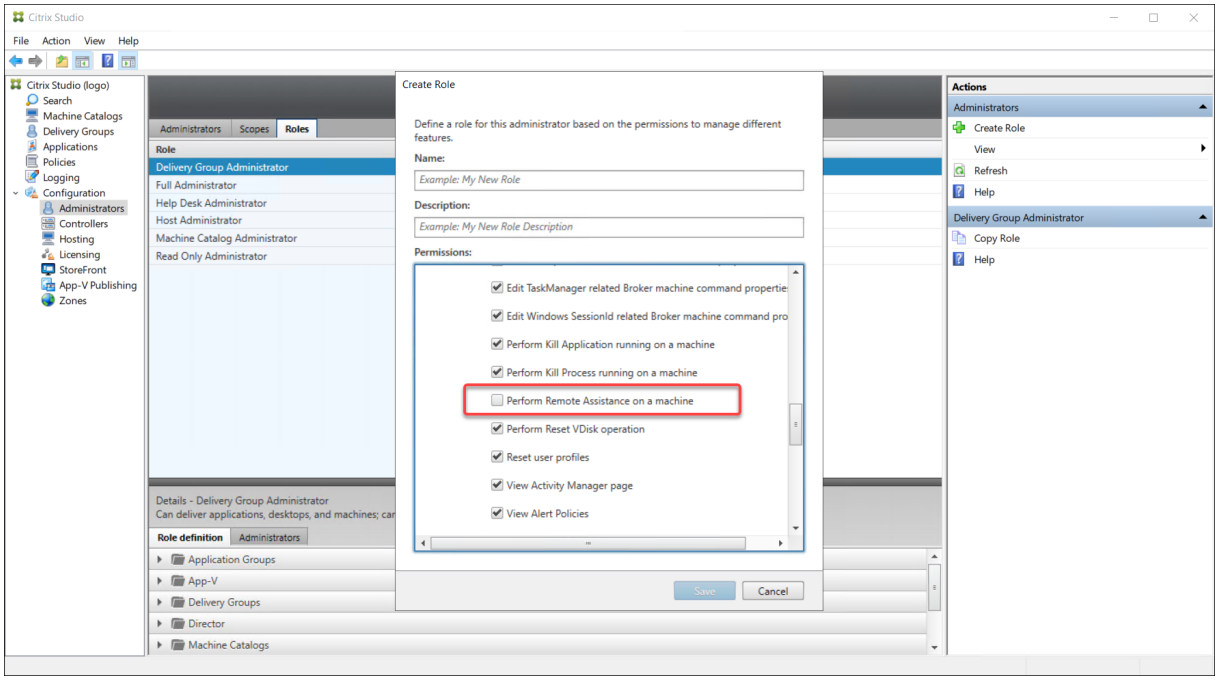


または、既存の役割をコピーしてカスタムの役割を作成し、異なるビューのための権限を追加することができます。たとえば、ヘルプデスクの役割をコピーして、［ダッシュボード］ページや［フィルター］ページを表示するための権限を追加できます。

以下の Director 用の権限を追加します。

- マシンで実行中のアプリケーションの強制終了
- マシンで実行中のプロセスの強制終了
- マシン上でのリモート アシスタンス
- ユーザー プロファイルのリセット
- クライアント詳細ページの表示
- ダッシュボード ページの表示
- フィルターページの表示
- マシン詳細ページの表示
- 傾向ページの表示
- ユーザー詳細ページの表示

この例では、シャドウ機能（マシン上でのリモートアシスタンス）が無効になっています。



権限は、UI で使えるようにするために、他の権限への依存関係を持つ場合があります。たとえば、マシンで実行中のアプリケーションの強制終了権限を選択すると、その役割のために権限を持つこれらのパネルのみで、［アプリケーションの終了］の機能が有効になります。以下のパネルの権限を選択することができます：

- フィルターページの表示
- ユーザー詳細ページの表示
- マシン詳細ページの表示
- クライアント詳細ページの表示

さらに、他のコンポーネントの権限の一覧から、次のデリバリーグループ権限の追加を検討します：

- デリバリーグループメンバーシップによるマシンのメンテナンスモードの有効/無効。
- デリバリーグループメンバーシップによる Windows デスクトップマシンの電源操作。

- デリバリーグループメンバーシップによるマシンのセッション管理。

Director 展開環境の保護

August 17, 2024

この記事では、Director の展開および構成時に使用すべき、システムのセキュリティを保護するための機能について説明します。

Microsoft インターネットインフォメーションサービス（IIS）の構成

制限された IIS 構成で Director を構成できます。

アプリケーションプールのリサイクル制限

次のアプリケーションプールのリサイクル制限を設定できます。

- 仮想メモリの制限：4,294,967,295
- プライベートメモリの制限：StoreFront サーバーの物理メモリのサイズ
- 要求の制限：4,000,000,000

ファイル名拡張子

一覧にないファイル拡張子を禁止することができます。

Director は要求のフィルタリングに、次のファイル拡張子が必要です。

- .aspx
- .css
- .html
- .js
- .png
- .svc
- .png
- .json
- .woff
- .woff2
- .ttf

Director は要求のフィルタリングに、次の HTTP 動詞が必要です。次の一覧にない動詞を禁止できます。

- GET
- POST
- HEAD

Director は次を必要としません。

- ISAPI フィルター
- ISAPI 拡張
- CGI プログラム
- FastCGI プログラム

> 重要:
>
> - Director には完全な信頼が必要です。グローバル.NET 信頼レベルを［High］またはそれ以下に設定しないでください。
> - Director は個別のアプリケーションプールを保持します。Director の設定を変更するには、Director サイトを選択し変更します。

ユーザー権利の構成

Director をインストールすると、そのアプリケーションプールには次の権限が付与されます:

- ［サービスとしてログオン］のログオン権限
- ［プロセスのメモリクォータの増加］、［セキュリティ監査の生成］、［プロセスレベルトークンの置き換え］の特権

上記の権限や特権は、アプリケーションプールが作成されたときの通常のインストール動作です。

通常、これらのユーザー権利を変更する必要はありません。これらの権限は Director では使用されず自動的に無効になります。

Director の通信

実稼働環境では、Director とサーバーの間で通信されるデータを保護するために、インターネットプロトコルセキュリティ（IPsec）または HTTPS プロトコルを使用します。

IPsec は、インターネットプロトコルの標準機能拡張のセットです。インターネットプロトコルは、データ整合性と再生の保護により通信の認証と暗号化の機能を提供します。IPsec はネットワーク層のプロトコルセットであるため、上位レベルのプロトコルでそのまま IPSec を使用できます。HTTPS は、TLS（Transport Layer Security）プロトコルを使用して強力なデータ暗号化機能を提供します。

> 注:
>
> - イントラネットネットワーク内の Director コンソールへのアクセスを制限することを強くお勧めします。
> - 実稼働環境では、Director へのすべての接続が保護されるようにしてください。
> - Director からの通信を保護するには、個別に各接続を構成する必要があります。
> - SSL プロトコルは、推奨されていません。代わりにより安全な TLS プロトコルを使用します。
> - IPsec ではなく TLS を使用して、Citrix ADC との通信を保護します。

Director と Citrix Virtual Apps and Desktops サーバー間の（監視機能およびレポート機能のための）通信を保護する方法について詳しくは、「Data Access Security」を参照してください。

Director と Citrix ADC の（Citrix Insight のための）通信を保護する方法について詳しくは、「ネットワーク分析機能の構成」を参照してください。

Director とライセンスサーバーの通信を保護する方法について詳しくは、「ライセンス管理コンソールの保護」を参照してください。

Director のセキュリティ境界による分離

Director と同じ Web ドメイン（ドメイン名とポート）に任意の Web アプリケーションを展開できます。ただし、これらの Web アプリケーションにセキュリティリスクがあれば、Director 環境のセキュリティが低下する可能性があります。セキュリティ境界を分離してセキュリティを強化するため、Web アプリケーションと異なる Web ドメインに Director を展開することをお勧めします。

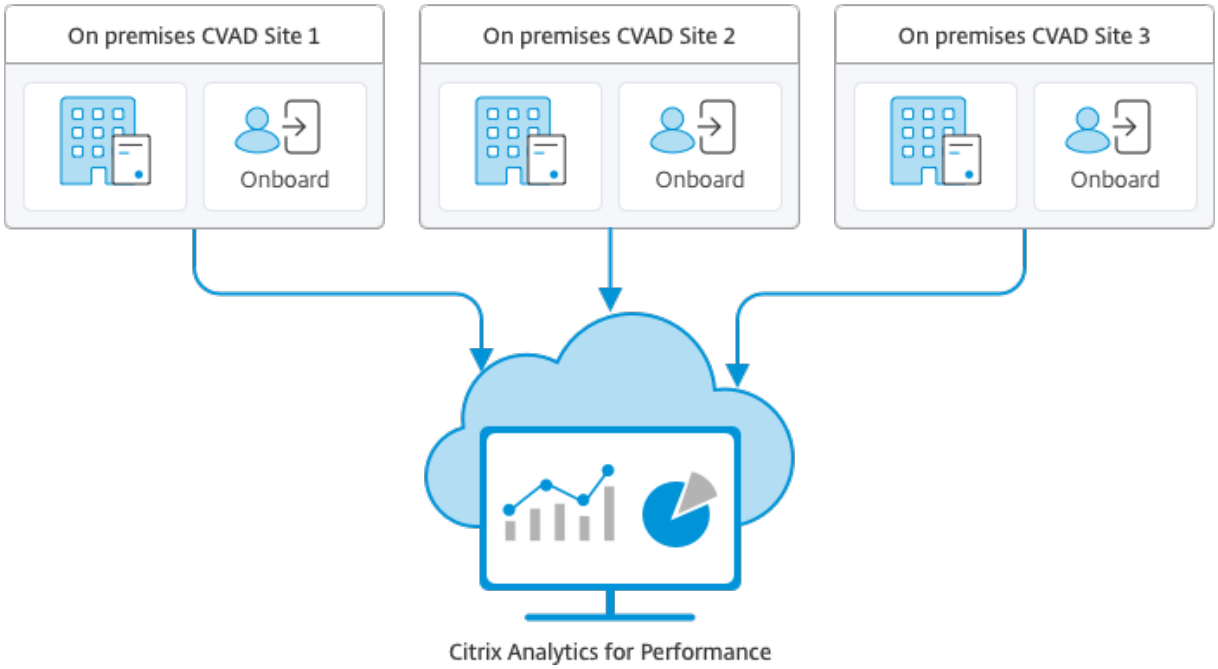
Citrix Analytics for Performance を使用したオンプレミスサイトの構成

August 17, 2024

Citrix Analytics for Performance（パフォーマンス分析）は、Citrix Analytics クラウドサービスの包括的なパフォーマンス監視ソリューションです。パフォーマンス分析は、パフォーマンスメトリックに基づいて構築された高度な洞察と分析を提供します。パフォーマンス分析は、組織内の 1 つまたは複数の Citrix Virtual Apps and Desktops サイトの使用状況とパフォーマンスメトリックを監視および表示するのに役立ちます。

パフォーマンス分析について詳しくは、パフォーマンス分析の記事を参照してください。

パフォーマンスデータをサイトから Citrix Cloud 上の Citrix Analytics for Performance に送信して、高度なパフォーマンス分析機能を活用できます。パフォーマンス分析を表示して使用するには、まず **Director** の［**Analytics**］タブから、Citrix Analytics for Performance でオンプレミスサイトを構成する必要があります。



パフォーマンス分析は安全な方法でデータにアクセスし、Citrix Cloud からオンプレミス環境にデータが転送されることはありません。

前提条件

Director から Citrix Analytics for Performance を構成するには、新しいコンポーネントをインストールする必要はありません。次の要件が満たされていることを確認します:

- Delivery Controller と Director のバージョンは 1912 CU2 以降を使用しています。詳しくは、「機能の互換性マトリックス」を参照してください。

> 注:
>
> - Delivery Controller が 4.8 より前のバージョンの Microsoft .NET Framework を実行している場合、Director からの Citrix Analytics for Performance を使用したオンプレミスサイトの構成が失敗する可能性があります。この問題を回避するには、Delivery Controller の.NET Framework をバージョン 4.8 にアップグレードします。LCM-9255。
> - Director から Citrix Analytics for Performance を使用して、Citrix Virtual Apps and Desktops バージョン 2012 を実行しているオンプレミスサイトを構成すると、数時間後、または Delivery Controller で Citrix Monitor Service を再起動した後に構成が失敗する場合があります。この場合、Analytics タブには未接続ステータスが表示されます。回避策として、Delivery Controller のレジストリに次の暗号化フォルダーを作成します。場所: HKEY_LOCAL_MACHINE\Software\Citrix\XDservices\Monitor フォルダー名: 暗号化 Citrix Monitor アカウントが暗号化フォルダーへのフルコントロールのアクセス権を持っていることを確認してください。Citrix Monitor Service を再起動します。DIR-14324。

- この構成を実行するための ［**Analytics**］タブには、完全な管理者のみがアクセスできます。

- パフォーマンス分析でパフォーマンスメトリックにアクセスする場合、アウトバウンドインターネットアクセスは、すべての Delivery Controller、および Director がインストールされているマシンで利用できます。具体的には、次の URL にアクセスできるようにしてください。
  - Citrix キーの登録: `https://*.citrixnetworkapi.net/`
  - Citrix Cloud: `https://*.citrixworkspacesapi.net/`
  - Citrix Analytics: `https://*.cloud.com/`
  - Microsoft Azure: `https://*.windows.net/`

    Delivery Controller と Director マシンがイントラネット内にあり、送信用のインターネットアクセスがプロキシサーバーを経由している場合、以下を確認してください:
- プロキシサーバーは、前述の URL 一覧を許可する必要があります。
- Director の web.config ファイルと citrix.monitor.exe.config ファイルに次の構成を追加します。[構成] タグ内でこの構成を追加してください:

```
<system.net>
    <defaultProxy>
        <proxy  usesystemdefault = "false"  proxyaddress = "http
            ://<your_proxyserver_address>:80" bypassonlocal = "
            true"  />
    </defaultProxy>
</system.net>
```

  - Director web.config は、Director がインストールされているマシンの`C:\inetpub\wwwroot\Director\web.config`にあります。
  - citrix.monitor.exe.config は、Delivery Controller がインストールされているマシンの`C:\Program Files\Citrix\Monitor\Service\Citrix.Monitor.exe.Config`にあります。

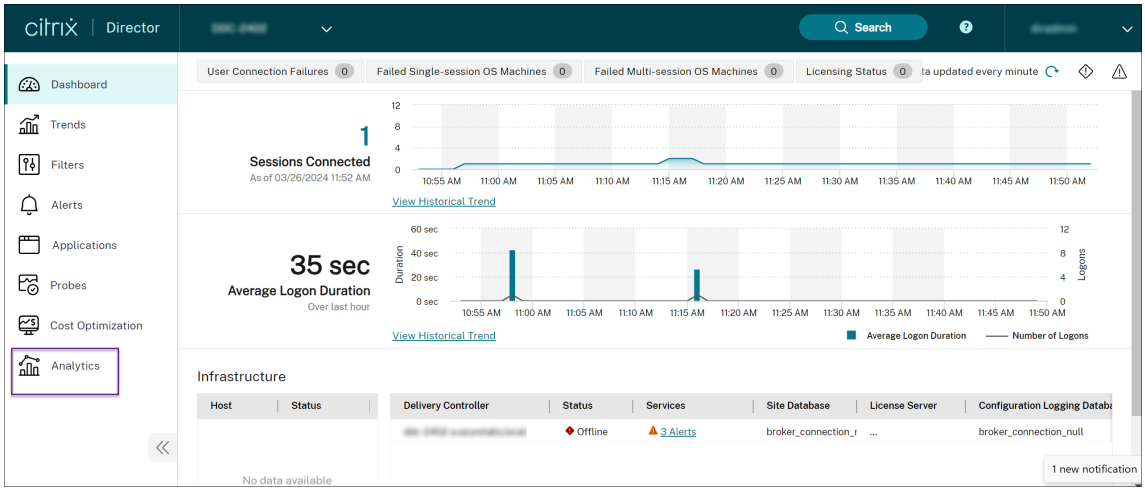
  この設定は Microsoft によって IIS で提供されます。詳しくは、`https://docs.microsoft.com/en-us/dotnet/framework/network-programming/proxy-configuration`を参照してください。

  構成ファイルの **defaultproxy** フィールドは、Director および Monitor サービスの送信アクセスを制御します。パフォーマンス分析の構成および通信で、**defaultproxy** フィールドを **true** に設定する必要があります。適用されるポリシーでこのフィールドを false に設定することもできます。この場合、フィールドを手動で true に設定する必要があります。変更を加える前に、構成ファイルのバックアップを取ってください。変更を有効にするには、Delivery Controller の Monitoring Service を再起動します。
- Citrix Analytics for Performance を使用するアクティブな Citrix Cloud 使用権があります。
- Citrix Cloud アカウントは、製品登録操作の権限を持つ管理者アカウントです。管理者権限について詳しくは、「管理者権限を変更する」を参照してください。

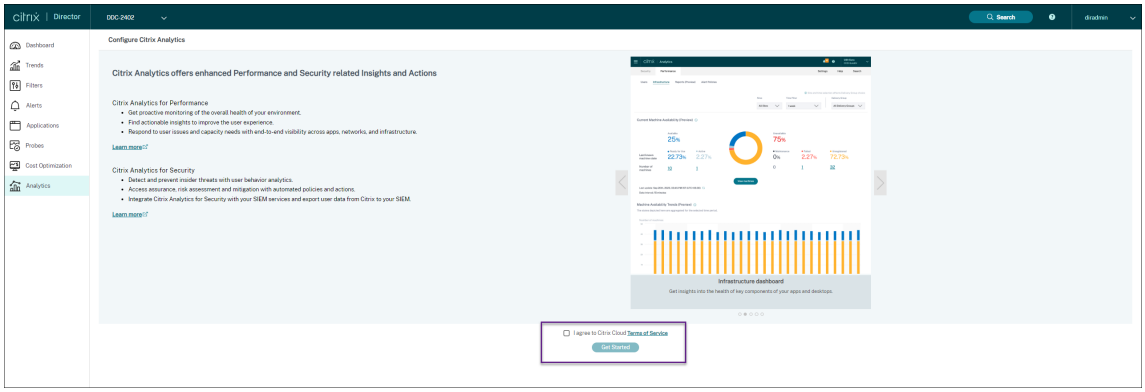
構成の手順

前提条件を確認したら、次の操作を行います:

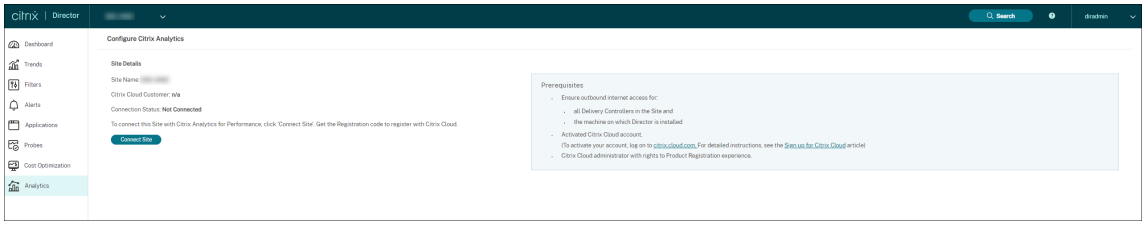
1. 完全な管理者として Director にサインインし、パフォーマンス分析で構成するサイトを選択します。Director のダッシュボードページが表示されます。



2. [**Analytics**] タブをクリックします。[**Citrix Analytics** の構成] ページが表示されます。

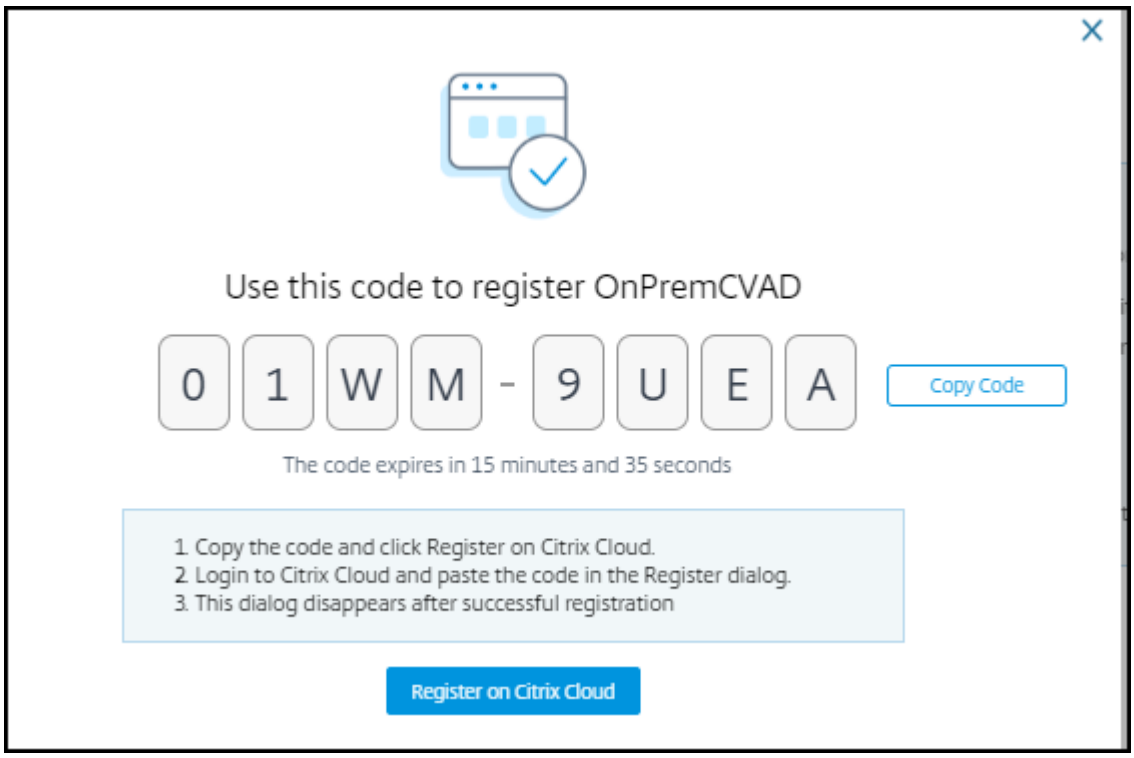


3. 手順を確認し、サービス利用規約を選択し、[開始] をクリックします。[サイトの詳細] のページが開きます。

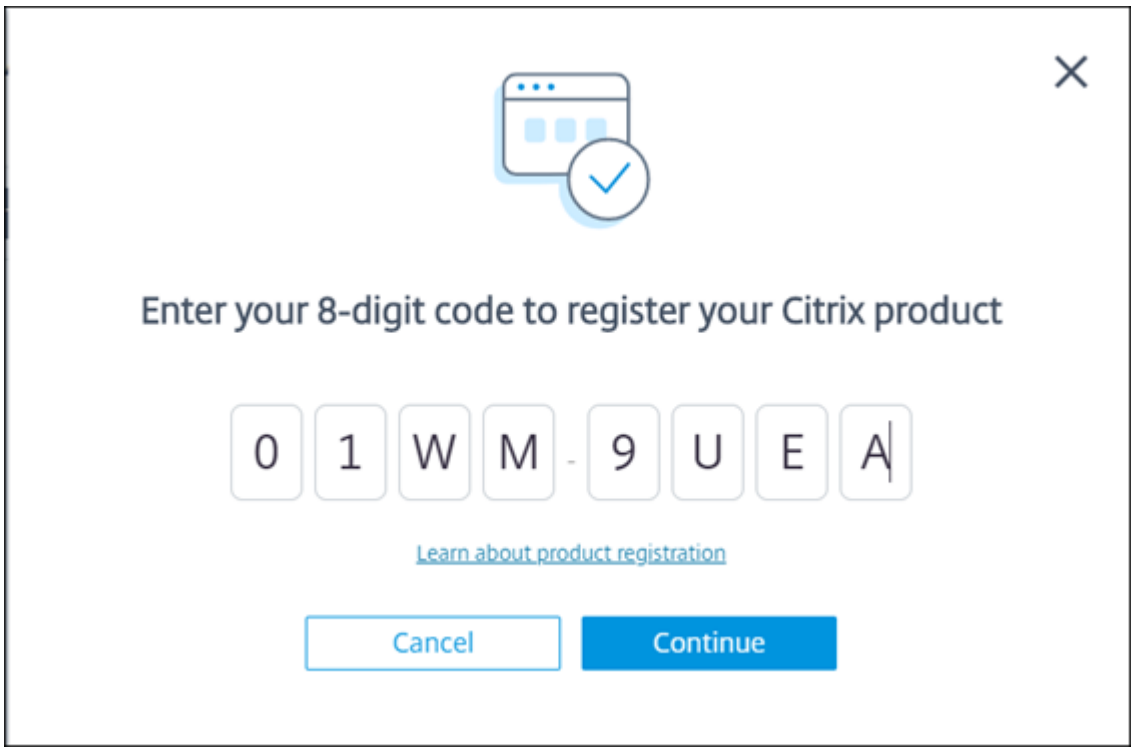


4. 前提条件を確認し、それらが満たされていることを確認します。サイトの詳細を確認します。
5. [サイトを接続する] をクリックして、構成プロセスを開始します。

   このサイトを Citrix Cloud に登録するために使用する一意の 8 桁の登録コードが生成されます。

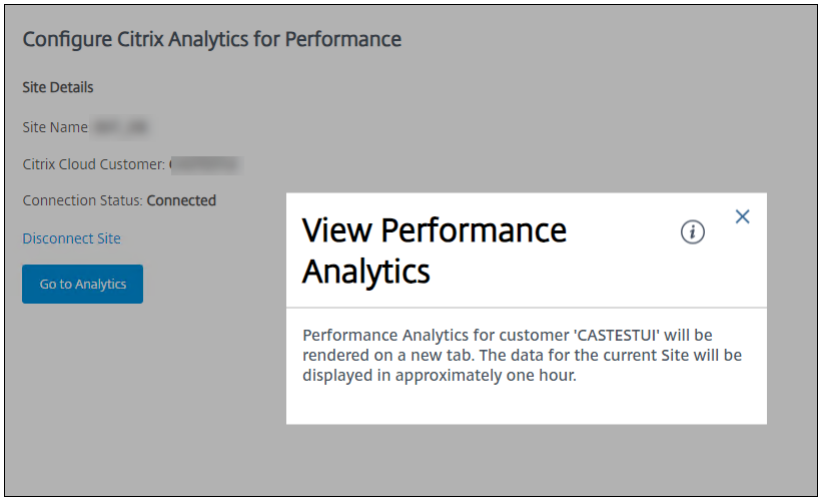


6. ［コードのコピー］をクリックしてコードをコピーし、［**Citrix Cloud** に登録］をクリックします。Citrix Cloud の登録 URL にリダイレクトされます。
7. Citrix Cloud の資格情報でサインインし、顧客を選択します。
8. コピーした登録コードを Citrix Cloud の［製品の登録］ページに貼り付けます。［続行］をクリックして登録します。登録の詳細を確認してから、［登録］をクリックします。

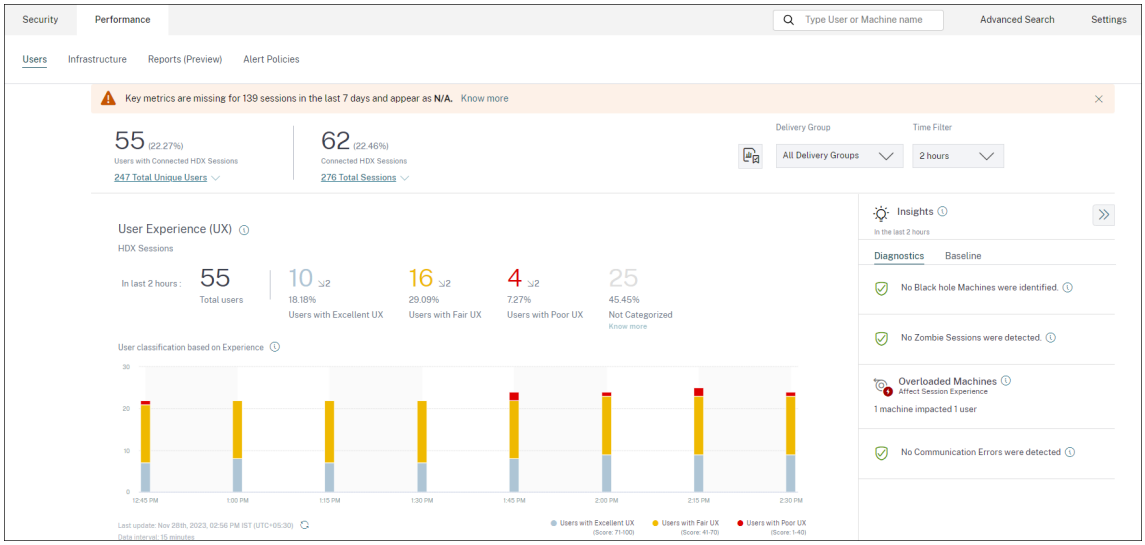


オンプレミスサイトが Citrix Cloud に登録されます。

9. **Director** から ［**Analytics**］タブで ［**Analytics** に移動］をクリックします。



パフォーマンス分析は、Web ブラウザーの新しいタブで開きます。



Citrix Cloud セッションの有効期限が切れている場合、Citrix.com または My Citrix アカウントのログオンページにリダイレクトされることがあります。

10. 複数のサイトをパフォーマンス分析に登録するには、Director のサイトごとに前述の構成手順を繰り返します。すべての構成済みサイトのメトリックは、パフォーマンス分析ダッシュボードに表示されます。

    サイトごとに複数の Director インスタンスが実行されている場合は、任意の Director インスタンスから構成します。サイトに接続されている他のすべての Director インスタンスは、構成プロセス後の次回の更新時に更新されます。

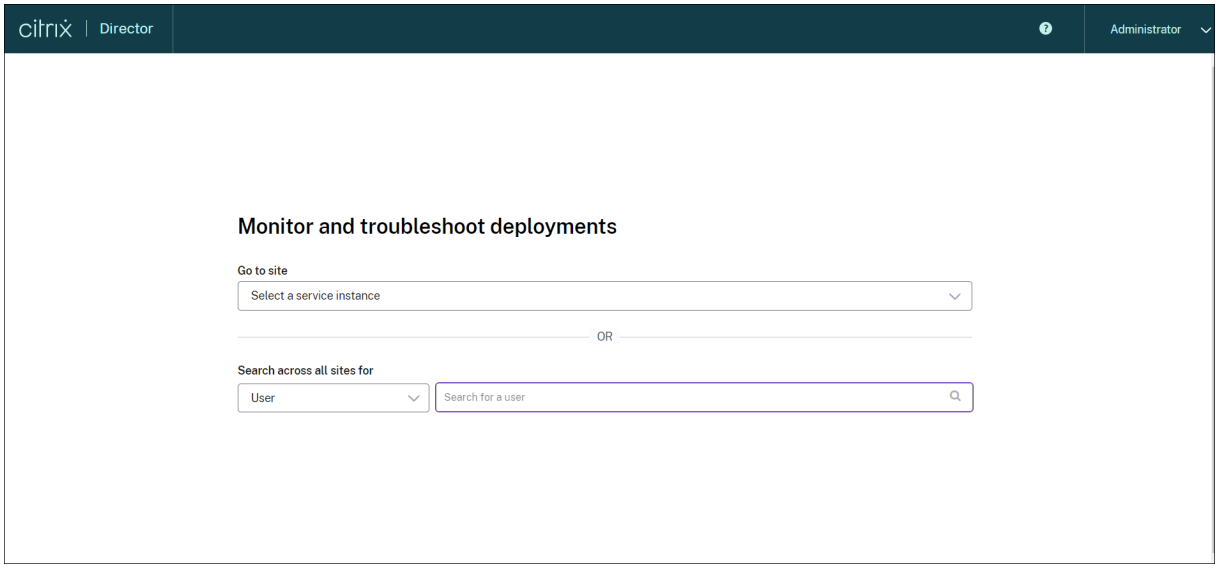
11. Citrix Cloud からサイトを切断するには、［サイトを切断する］をクリックします。このオプションは、既存の構成を削除します。

    > 注:
    >
    > サイトを初めて構成するときに、サイトからのイベントの処理に多少の時間（約 1 時間）がかかる場合があります。このため、パフォーマンス分析ダッシュボードでのメトリックの表示に遅延が生じます。その後、イベントは定期的に更新されます。
    >
    > 切断すると、新しいアカウントからのイベントが転送されるまで、古いアカウントからのデータ送信がしばらく継続されます。データ送信が停止してから約 1 時間、古いアカウントに関連する分析が パフォーマンス分析ダッシュボードに表示されたままになります。
    >
    > Citrix Analytics サービスの使用権の有効期限が切れると、パフォーマンス分析へのサイトメトリックの送信を停止するまでに 1 日ほどかかります。

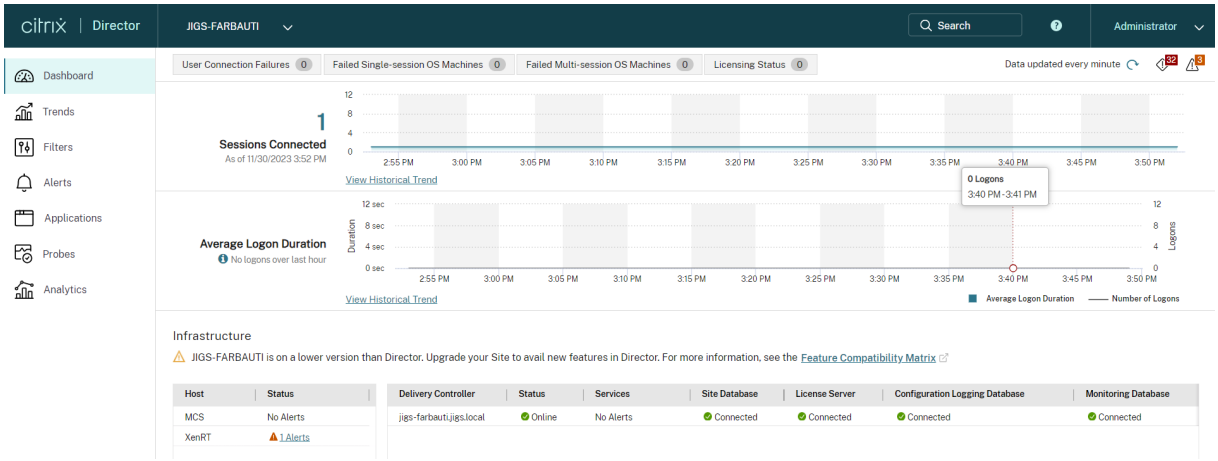
サイト分析

August 17, 2024

Director を使用すると、展開の正常性を監視できます。オンボーディング中のすべてのサイトでユーザー、エンドポイント、またはマシンを検索することで、パフォーマンスの問題をトラブルシューティングできます。



すべての管理権限を実行できる管理者として Director を起動すると、ダッシュボードでサイトの正常性や使用状況を一元的にモニターできます。



現在エラーがなく、かつ直近の 60 分間にエラーが発生していない場合、パネルは閉じたままになります。エラーが発生している場合はそのエラーを示すパネルが自動的に開きます。

> 注:
>
> 組織のライセンスおよび管理者権限によって、表示されるオプションや機能は異なります。

Director のダッシュボードのパネル

ユーザー接続エラー

過去 60 分間の接続エラーが表示されます。エラー総数の横にあるカテゴリをクリックして、各種のエラーのメトリックを確認します。隣接する表には、発生したエラー数がデリバリーグループごとに表示されます。接続エラーには、アプリケーション制限に達したことによって発生したエラーも含まれます。アプリケーション制限について詳しくは、「アプリケーション」を参照してください。

失敗したシングルセッション**OS** マシンまたは失敗したマルチセッション **OS** マシン

過去 60 分間の総エラー数がデリバリーグループごとに表示されます。エラーの種類として、起動の失敗、起動時のスタック、および未登録があります。マルチセッション OS マシンの場合は、最大負荷に達しているマシンも含まれます。

ライセンスの状態

ライセンスサーバーアラートには、ライセンスサーバーから送信されたアラートメッセージとそのアラートを解決するための操作が表示されます。ライセンスサーバー 11.12.1 以降が必要です。Delivery Controller アラートには、Controller から送信されたライセンス状態の詳細が表示されます。XenApp 7.6 または XenDesktop 7.6 以降の Controller が必要です。アラートのしきい値は、Studio で設定できます。［**Delivery Controller**］ > ［詳細］ > ［製品エディション］ > ［**PLT**］の画面に表示されるライセンスステータスは ［**Premium**］です（［**Platinum**］ではありません）。

猶予期間の状態

Director は、次のいずれかの猶予期間の状態を表示します。この情報は、Delivery Controller から取得します。

1. 非アクティブ：どの種類の猶予期間にも該当しません。通常のライセンス制限が適用されます。
2. 緊急猶予期間：ライセンスサーバーに到達できない場合、または接続の仲介中ライセンス情報が取得できない場合に有効になります。ユーザーは影響を受けません。ライセンスサーバーに到達できるようになるまで、Director で表示されたエラーは破棄できません。
3. 猶予期間の期限切れ：緊急猶予期間が期限切れになりました。

詳しくは、「ライセンスの超過使用保護」および「追加猶予期間」を参照してください。

接続セッション

すべてのデリバリーグループでの過去 60 分間の接続セッションが表示されます。

平均ログオン時間

過去 60 分間のログオン処理に関するデータが表示されます。左側にある大きなサイズの数値は、全体的な平均ログオン処理時間を示します。この平均には、XenDesktop 7.0 より前のバージョンの VDA へのログオンデータは含まれません。詳しくは、「ユーザーログオンの問題の診断」を参照してください。

インフラストラクチャ

サイトのインフラストラクチャ一覧 - ホストおよびコントローラー。XenServer または VMware のインフラストラクチャで、パフォーマンスアラートを表示できます。たとえば、XenCenter では、サーバーまたは仮想サーバーの CPU、ネットワーク I/O、またはディスク I/O の使用量が特定のしきい値を超えた場合にパフォーマンスアラートが発せられるように構成できます。アラートの送信間隔はデフォルトで 60 分ですが、必要に応じて変更できます。詳しくは、XenServer 製品ドキュメントの XenCenter のパフォーマンスアラートに関するセクションを参照してください。

> 注:
>
> ホスト上でサポートされてない種類のメトリックのアイコンは表示されません。たとえば、System Center Virtual Machine Manager（SCVMM）ホスト、AWS および CloudStack のヘルス情報は表示されません。

次のオプション（次のセクションで説明）を使用して、問題のトラブルシューティングを続けます:

- ユーザーマシンの電源の制御
- マシンへの接続の無効化

セッションの監視

セッションが切断状態になると、セッションおよびアプリケーションは終了しませんが、サーバーとユーザーデバイス間の通信が切断されます。

アクション	説明
ユーザーが接続しているマシンまたはセッションを表示する	[アクティビティマネージャー] および [ユーザーの詳細] ビューで、ユーザーが接続しているマシンまたはセッションと、そのユーザーがアクセスしているすべてマシンおよびセッションの一覧を表示します。セッションの一覧にアクセスするには、そのユーザーのビューのタイトルバーにあるセッション切り替え用のアイコンをクリックします。詳しくは、「セッションの復元」を参照してください。

アクション	説明
すべてのデリバリーグループで接続されたセッションの総数を表示する	ダッシュボードの ［接続セッション］ペインには、すべてのデリバリーグループで過去 60 分間に接続されたセッションの合計数が表示されます。その合計数をクリックすると、［フィルター］ビューが開きます。ここでは、デリバリーグループごとのセッションデータや、すべてのデリバリーグループでの特定期間での使用量を視覚的に確認できます。
アイドル状態のセッションを終了する	［セッションフィルター］ビューにすべてのアクティブなセッションの関連データが表示されます。セッションに関連付けられているユーザー、デリバリーグループ、セッション状態、しきい値の時間を超えたアイドル時間に基づいてフィルターします。フィルターされた一覧で、ログオフまたは切断するセッションを選択します。詳しくは、「アプリケーションのトラブルシューティング」を参照してください。
長期間のデータを表示する	［傾向］ビューで ［セッション］タブを選択し、接続されたセッションと切断されたセッションの長期間（つまり、過去 60 分より前のセッションの合計）のより具体的な利用状況データにドリルダウンします。この情報を表示するには、［履歴傾向の表示］をクリックします。

> 注:
>
> Virtual Delivery Agent 7 より前のバージョンの VDA、または Linux VDA を実行する場合、セッションに関する一部の情報が Director に表示されません。代わりに、利用できる情報がないというメッセージが表示されます。

デスクトップ割り当て規則の制限:
Web Studio では、さまざまなユーザーまたはユーザーグループの複数のデスクトップ割り当て規則（DAR）をデリバリーグループ内の 1 つの VDA に割り当てることができます。StoreFront は、ログインしたユーザーの DAR に従って、割り当てられたデスクトップを対応する表示名で表示します。ただし、Director では DAR はサポートされておらず、ログインしているユーザーに関係なく、デリバリーグループ名を使用して割り当て済みのデスクトップが表示されます。このため、Director で特定のデスクトップをマシンにマッピングすることはできません。
StoreFront に表示されている割り当て済みデスクトップを、Director に表示されているデリバリーグループ名にマッピングするには、次の PowerShell コマンドを使用します:

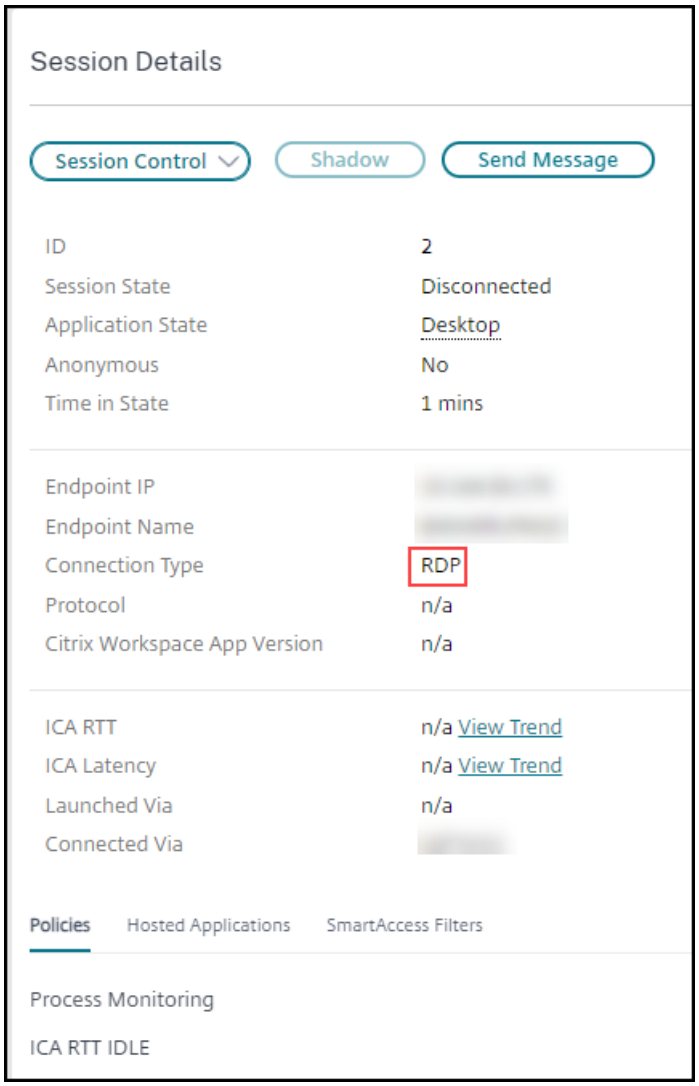
```
Get-BrokerDesktopGroup | Where-Object {
  \$\_.Uid -eq \(Get-BrokerAssignmentPolicyRule | Where-Object {
  \$\_.PublishedName -eq \"\<Name on StoreFront\>\"  }
 ).DesktopGroupUid  }
```



```
5    | Select-Object -Property Name, Uid
```

セッショントランスポートプロトコル

［セッション詳細］パネルで、現在のセッションの HDX 接続タイプに使用されているトランスポートプロトコルを表示します。この情報はバージョン 7.13 以降の VDA で起動するセッションで利用できます。



- **HDX** 接続の種類の場合、
  - EDT が HDX 接続に使用されている場合、プロトコルは **UDP** と表示されます。
  - TCP が HDX 接続に使用されている場合、プロトコルは **TCP** と表示されます。
- **RDP** 接続の種類の場合、プロトコルは「該当なし」と表示されます。

アダプティブトランスポートが構成されている場合、セッショントランスポートプロトコルは、ネットワーク条件に応じて、EDT（UDP 上）と TCP を動的に切り替えます。HDX セッションを EDT で確立できない場合は、TCP プロ

トコルにフォールバックします。

アダプティブトランスポート構成について詳しくは、「アダプティブトランスポート」を参照してください。

レポートのエクスポート

傾向データをエクスポートして、通常使用レポートおよび能力管理レポートを生成できます。エクスポートでは、PDF、Excel、および CSV レポート形式がサポートされます。PDF と Excel 形式のレポートには、傾向がグラフとテーブルとして表示されます。CSV 形式のレポートには、処理してビューを生成したり、アーカイブしたりできる表形式のデータが含まれます。

レポートをエクスポートするには、次の手順に従います。

1. [傾向] タブに移動します。
2. フィルターの基準と期間を設定し、[適用] をクリックします。傾向グラフとテーブルにデータが入力されます。
3. [エクスポート] をクリックして、レポートの名前と形式を入力します。

Director は、選択したフィルター基準に基づいてレポートを生成します。フィルター基準を変更した場合は、[適用] をクリックしてから [エクスポート] をクリックします。

> 注:
>
> 大量のデータをエクスポートすると、Director サーバー、Delivery Controller および SQL サーバーのメモリと CPU の消費が著しく増加します。サポートされる同時エクスポート処理の数とエクスポートできるデータの量は、エクスポートのパフォーマンスを最適にするため、デフォルトの上限に設定されています。

サポートされるエクスポート上限

エクスポートされる PDF と Excel のレポートは、選択されたフィルター基準によるグラフィカルなチャートが含まれています。ただし、すべてのレポート形式の表形式のデータは、行の数またはテーブルのレコード数のデフォルト値を超えた値は切り捨てられています。サポートされるデフォルトのレコード数は、レポート形式に基づいて定義されます。

Director アプリケーションの設定をインターネットインフォメーションサービス（IIS）で構成して、デフォルトの上限を変更できます。

VHD 形式	サポートされるデフォルトのレコード数	**Director** アプリケーションの設定におけるフィールド	サポートされる最大レコード数
PDF	500	UI.ExportPdfDrilldownLimit	5000
Excel	100,000	UI.ExportExcelDrilldownLimit	1000,000

VHD 形式	サポートされるデフォルトのレコード数	**Director** アプリケーションの設定におけるフィールド	サポートされる最大レコード数
CSV	100,000（[セッション] タブで 10,000,000）	UI.ExportCsvDrilldownLimit	100,000

エクスポートできるレコード数の上限を変更するには、次の手順に従います。

1. IIS マネージャーコンソールを開きます。
2. [Default Web Site] ノードを開き、[Director] Web サイトを選択します。
3. [アプリケーションの設定] をダブルクリックします。
4. 必要に応じて、UI.ExportPdfDrilldownLimit、UI.ExportExcelDrilldownLimit、または UI.ExportCsvDrilldownLimit フィールドの設定を編集または追加します。

[アプリケーションの設定] でこれらのフィールドの値を追加すると、デフォルト値が上書きされます。

> 警告:
>
> サポートされる最大レコード数より大きい値にフィールド値を設定すると、エクスポートのパフォーマンスが影響を受ける可能性があり、サポートもされません。

Error Handling

このセクションでは、エクスポート処理中に発生しうるエラーに対処するための情報を提供します。

- **Director** のタイムアウト

このエラーは、Director サーバーでの、または Monitor Service による、ネットワーク問題や高いリソース使用率によって発生することがあります。

デフォルトのタイムアウト時間は 100 秒間です。Director サービスのタイムアウト時間を増やすには、インターネットインフォメーションサービス（IIS）の Director アプリケーションの設定で **Connector.DataServiceContext.Timeout** フィールド の値を設定します:

1. IIS マネージャーコンソールを開きます。
2. [Default Web Site] ノードを開き、[Director] Web サイトを選択します。
3. [アプリケーションの設定] をダブルクリックします。
4. 値 **Connector.DataServiceContext.Timeout** を編集します。

- モニターのタイムアウト

このエラーは、Monitor Service による、または SQL サーバーでの、ネットワーク問題や高いリソース使用率によって発生することがあります。

Monitor Service のタイムアウト時間を増やすには、Delivery Controller で以下の PowerShell コマンドを実行します:

```
asnp Citrix.*
Get-MonitorConfiguration
Set-MonitorConfiguration -MonitorQueryTimeoutSeconds <timeout value>
```

- 同時エクスポートまたはプレビュー処理上限

Director では、エクスポートまたはプレビューの 1 つのインスタンスがサポートされます。同時エクスポートまたはプレビュー処理上限エラーが発生した場合は、次のエクスポート処理を後で実行してください。

同時エクスポートまたはプレビュー処理の数を増やすことはできますが、Director のパフォーマンスに影響する可能性があり、サポートもされません:

1. IIS マネージャーコンソールを開きます。
2. [Default Web Site] ノードを開き、[Director] Web サイトを選択します。
3. [アプリケーションの設定] をダブルクリックします。
4. 値 **UI.ConcurrentExportLimit** を編集します。

- **Director** のディスク領域不足

各エクスポート処理には、Windows Temp フォルダーに最大 2GB のハードディスク容量が必要です。容量をクリアするか、Director サーバーにハードディスク容量を追加してからエクスポートを再試行してください。

Hotfix の監視

特定のマシンの VDA（物理または仮想）にインストールされている Hotfix を確認するには、[マシンの詳細] ビューを選択します。

ユーザーマシンの電源状態の制御

Director で選択したマシンの電源の状態を制御するには、[電源制御] オプションを使用します。これらのオプションはシングルセッションOS マシンに対して実行できますが、マルチセッション OS マシンに対しては使用できないことがあります。

> 注:
>
> この機能は、物理マシンまたはリモート PC アクセスを使用しているマシンに対しては使用できません。

コマンド	機能
再起動	仮想マシン上のすべてのプロセスを停止して、通常の再起動処理（ソフト再起動）を実行します。たとえば、Director に起動に失敗したことが表示されたマシンを再起動するときにこのコマンドを使用します。
強制再起動	通常のシャットダウン処理を行わずに強制的に仮想マシンを再起動します。これは、物理サーバーの電源プラグを抜いてから電源を入れるのと同等の操作です。
シャットダウン	仮想マシンの正常な（ソフト）シャットダウンを実行します。実行中のプロセスはすべて個別に停止されます。
強制シャットダウン	通常のシャットダウン処理を行わずに強制的に仮想マシンをシャットダウンします。物理サーバーの電源プラグを抜くのと同等の操作です。実行中のプロセスを正しく停止できない場合があるため、この方法で仮想マシンをシャットダウンするとデータが失われる可能性があります。
一時停止	仮想マシンを一時停止して、そのときの状態をデフォルトのストレージリポジトリ上にファイルとして保存します。この方法で仮想マシンを一時停止してからそのホストサーバーをシャットダウンし、ホストサーバーを再起動してから仮想マシンを元の実行状態に戻すことができます。
再開	一時停止状態の仮想マシンを再開して、元の実行状態に戻します。
開始	シャットダウン状態の仮想マシンを起動します（「コールドスタート」とも呼ばれます）。

電源制御操作に失敗した場合、アラート上にマウスポインターを置くと問題の詳細情報がポップアップメッセージとして表示されます。

マシンへの接続の無効化

メンテナンスモードでは、管理者がイメージの保守作業を行っている間、一時的にユーザーが接続できなくなります。

マシンをメンテナンスモードにすると、メンテナンスモードを解除するまでそのマシンへの接続が禁止されます。そのマシンにユーザーがログオンしている場合は、すべてのユーザーがログオフした後でメンテナンスモードに切り替わります。ユーザーのログオフを促すには、マシンのシャットダウンを通知するメッセージをユーザーに送信したり、電源制御機能を使って強制的にマシンをシャットダウンしたりできます。

1. ［ユーザーの詳細］ビューなどからマシンを選択するか、［フィルター］ビューでマシンのグループを選択します。
2. ［メンテナンスモード］を選択し、オプションをオンにします。

メンテナンスモードの割り当て済みデスクトップにユーザーが接続を試みると、デスクトップを使用できないことを示すメッセージが表示されます。管理者がメンテナンスモードを解除するまで、新しい接続は許可されません。

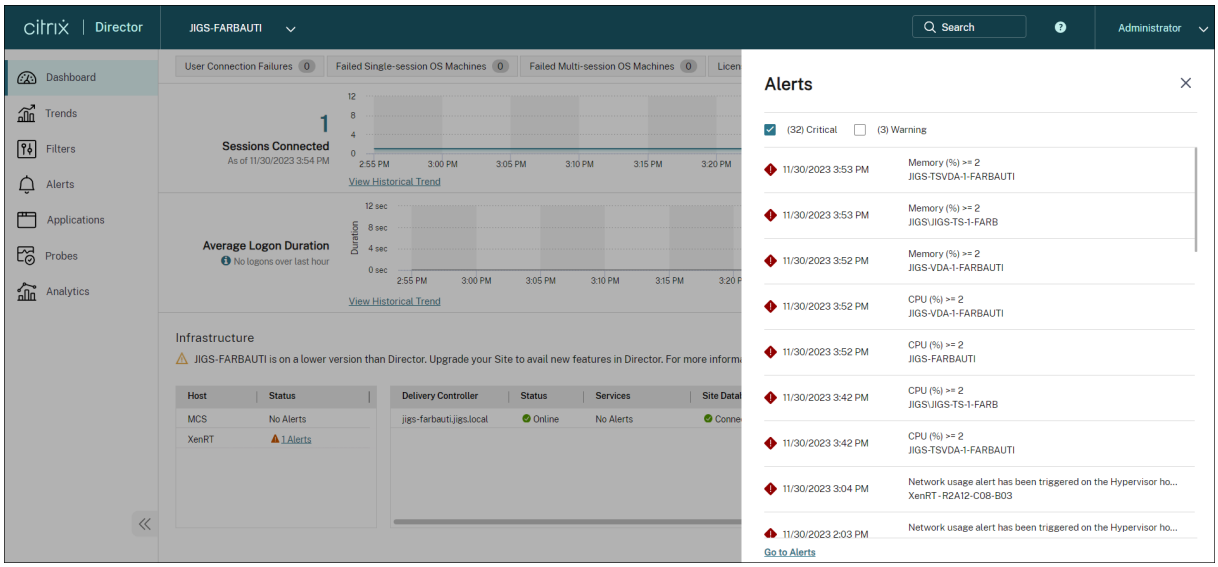
アプリケーション分析

［アプリケーション］タブには、アプリケーションのパフォーマンスを効率的に分析および管理するのに役立つアプリケーションごとの分析結果が、単一の統合ビューで表示されます。サイトに公開されているすべてのアプリケーションの正常性および使用状況に関する情報について貴重な分析情報を得ることができます。プローブの結果、アプリケーションごとのインスタンス数、公開アプリケーションに関連する障害およびエラーなどのメトリックが表示されます。詳しくは、「アプリケーションのトラブルシューティング」の「アプリケーションの分析」セクションを参照してください。

アラートおよび通知

August 20, 2024

アラートは、Director のダッシュボードおよびそのほかの概要ビューに、警告および重大アラートシンボルと共に表示されます。アラートは、**Premium** ライセンスを持つユーザーが使用できます。アラートは、1 分ごとに自動的に更新されます。オンデマンドで更新することもできます。

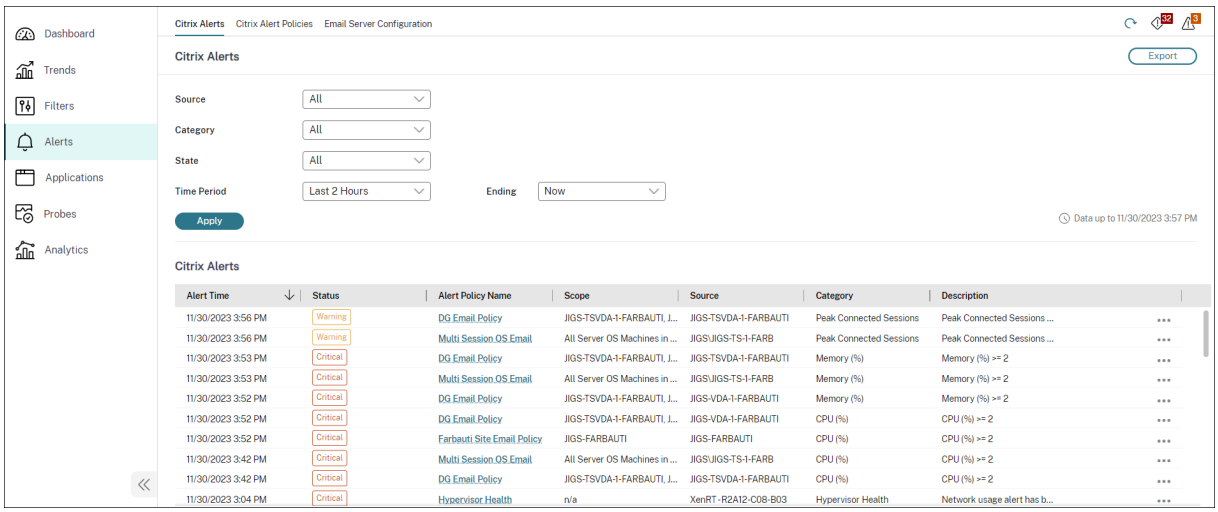


警告アラート（黄色の三角形）は、条件の警告しきい値以上になっていることを示します。

重大アラート（赤の円）は、条件の重大しきい値以上になっていることを示します。

サイドバーでアラートを選択して下部にある ［アラートに移動］リンクをクリックするか、［Director］ページの上部にある ［アラート］を選択すると、アラートに関するさらに詳細な情報を表示できます。

［アラート］ビューで、アラートをフィルターおよびエクスポートできます。たとえば、先月特定のデリバリーグループで失敗したマルチセッション OS マシンや、特定のユーザーに対するすべてのアラートを特定することができます。詳しくは、「レポートのエクスポート」を参照してください。



Citrix アラート

Citrix アラートは、Citrix コンポーネントで発生し、Director で監視されるアラートです。Citrix アラートは、Director 内で［アラート］>［**Citrix** アラートポリシー］の順に選択して構成できます。この構成では、設定したしきい値を超過した場合のアラートに関して、ユーザーおよびグループにメール送信する通知を設定できます。Citrix アラートのセットアップについて詳しくは、「アラートポリシーの作成」を参照してください。

> 注:
>
> ファイアウォール、プロキシ、または Microsoft Exchange Server がメール通知をブロックしないようにしてください。

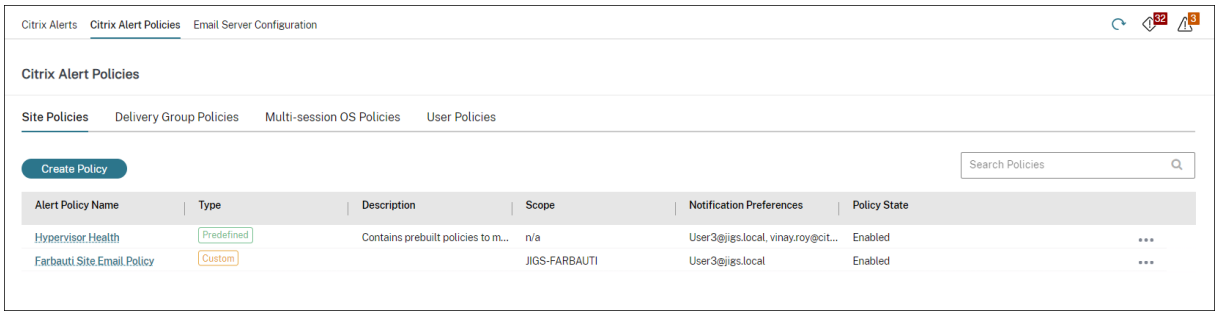
スマートアラートポリシー

定義済みのしきい値を持つ組み込みアラートポリシーのセットは、デリバリーグループおよびマルチセッション OS VDA スコープで使用できます。この機能には、Delivery Controller バージョン 7.18 以降が必要です。［アラート］>［**Citrix** アラートポリシー］で、組み込みアラートポリシーのしきい値パラメーターを変更できます。
これらのポリシーは、少なくとも 1 つのアラートターゲット（サイト内に定義されているデリバリーグループまたはマルチセッション OS VDA）が存在する場合に作成されます。さらに、これらの組み込みアラートは、新しいデリバリーグループまたはマルチセッション OS VDA に自動的に追加されます。

Director とサイトをアップグレードする場合、以前の Director インスタンスのアラートポリシーが引き継がれます。対応するアラートルールが監視データベースに存在しない場合にのみ、組み込みアラートポリシーが作成されま

す。

組み込みアラートポリシーのしきい値については、「アラートポリシーの条件」を参照してください。



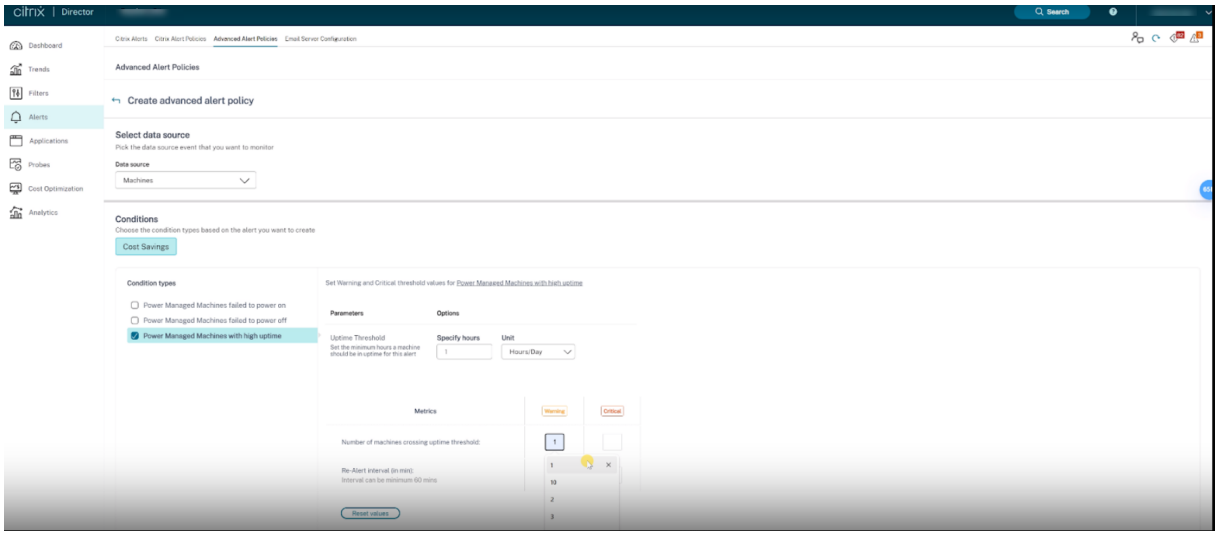
高度なアラートポリシー

Director の積極的な通知およびアラート機能が強化され、高度なアラートポリシーという新しいアラートフレームワークが追加されました。この機能を使用すると、各要素または条件の詳細を含めてアラートを作成できるため、アラートのスコープをより細かく制御できます。現在、これらのポリシーにはコスト削減とインフラストラクチャに関するアラートが含まれています。

データソース主導のアラートである高度なアラートポリシーの導入により、複数条件のスコープによるフィルタリングを使用できるようになりました。

この機能を使用すると、重要な問題に対処する際の応答性や有効性の低下につながる可能性のある、過剰なアラートを削減できます。このポリシーは、アラートポリシーの有効性と管理者の関与を測定するのに役立ちます。

［アラート］>［高度なアラートポリシー］>［ポリシーの作成］セクションから、高度なアラートポリシーを作成できます。



カテゴリとして、電源管理されたマシンの電源をオンにできませんでした、電源管理されたマシンの電源をオフにできませんでした、稼働率の高い電源管理されたマシンを選択し、ポリシーに必要な条件を選択できます。ポリシーの

作成方法について詳しくは「アラートポリシーの作成」を参照してください。ポリシーを作成した後、[Citrix アラート] ページでポリシーを編集、削除、または無効にできます。

上記の各条件に対して、特定のパラメーターと対応するオプションを選択できます。

稼働率の高い電源管理されたマシンのカテゴリでは、次のメトリックが確認されます:

- 稼働時間のしきい値を超えたマシンの数
- 再アラート間隔（分）は最小 60 分にできます

電源管理されたマシンの電源をオンにできませんでしたと電源管理されたマシンの電源をオフにできませんでしたカテゴリでは、次のメトリックが確認されます:

- 稼働時間のしきい値を超えたマシンの数
- サンプリング間隔（分）の間隔は、30 分の倍数にできます
- 再アラート間隔（分）の再アラートは、60 分の倍数にできます

必要に応じて、前述のカテゴリの重大度を設定できます。これらのアラートの再アラート間隔をスケジュールすることもできます。

ポリシーのスコープを定義する

アラートのスコープを定義し、例外を追加できます。アラートは選択したスコープに対してのみ生成され、例外の追加を使用して除外されたサブスコープはアラートの生成に含まれません。この機能は、詳細なレベルでアラートを作成するのに役立ちます。

メールまたは webhook URL を通じて通知を作成できます。アラートを受信する際の優先言語を選択することもできます。アラートパラメーターをメールの.CSV 添付ファイルで受信するか、または webhook URL を介して JSON ペイロードで受信するオプションを選択することもできます。添付ファイルには必要なパラメーターの詳細が含まれています。詳しくは、「アラートコンテンツの機能強化」を参照してください。

次のデータは、メールまたは **Citrix** アラートページでアラートとして受信されます:

フィールド	説明
カスタマー ID	サイトのカスタマー ID。
アラートレベル	この値は、各アラート条件に対して設定された定義済みの値です。可能な値は、Critical と Warning です。
条件	この値は、ポリシーの作成時に設定される条件です。たとえば、未登録のマシンの数が 20 以上です。
ターゲット	アラートがトリガーされるデリバリーグループまたはサイトの名前。
サイト	サイトの名前。

フィールド	説明
スコープ	ポリシーのスコープ。この値にはサブスコープも含まれます。
ポリシー	ポリシーの名前。
説明	アラートがトリガーされる問題の説明。

PowerShell スクリプトを使用して高度なアラートポリシーを作成する方法

アラートポリシーを作成する PowerShell スクリプト:

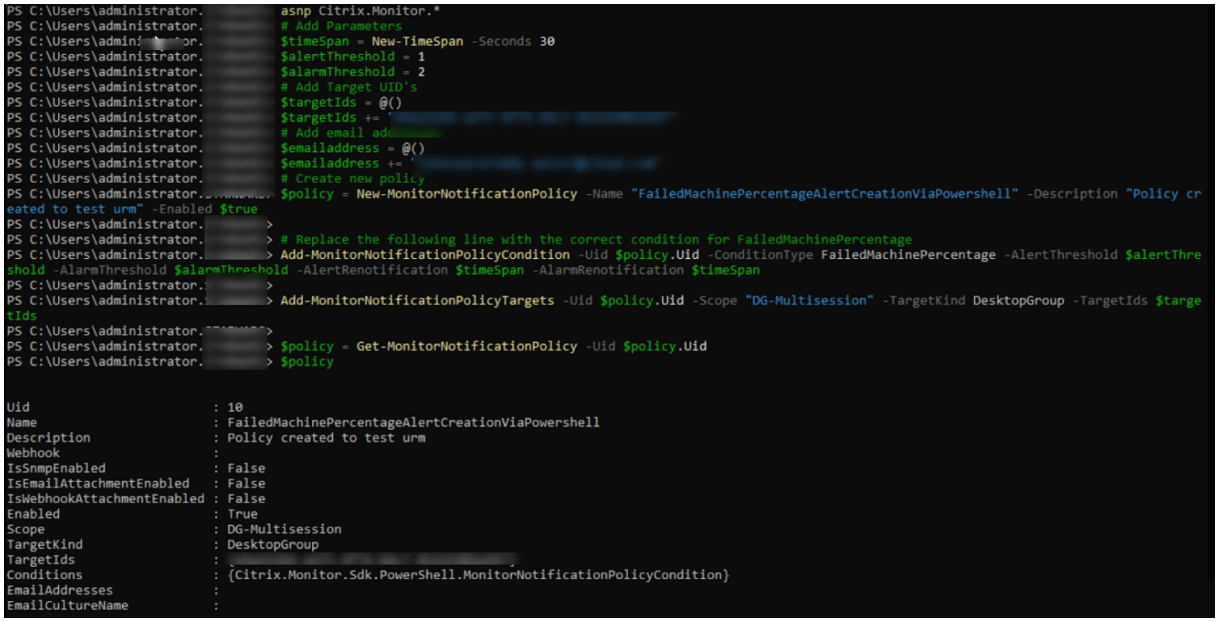
```
asnp Citrix.Monitor.*
# Add Parameters
$timeSpan = New-TimeSpan -Seconds 30
$alertThreshold = 1
$alarmThreshold = 2
# Add Target UID's
$targetIds = @()
$targetIds += "e9a211b4-a1f3-4f74-b6c7-85225902e997"
# Add email addresses
$emailaddress = @()
$emailaddress += "loki@abc.com"
# Create new policy
$policy = New-MonitorNotificationPolicy -Name "
    FailedMachinePercentageAlertCreationViaPowershell" -Description "
    Policy created to test urm" -Enabled $true
```

次の行を **FailedMachinePercentage** の正しい条件に置き換えます

```
Add-MonitorNotificationPolicyCondition -Uid $policy.Uid -ConditionType
    FailedMachinePercentage -AlertThreshold $alertThreshold -
    AlarmThreshold $alarmThreshold -AlertRenotification $timeSpan -
    AlarmRenotification $timeSpan

Add-MonitorNotificationPolicyTargets -Uid $policy.Uid -Scope "DG-
    Multisession" -TargetKind DesktopGroup -TargetIds $targetIds

$policy = Get-MonitorNotificationPolicy -Uid $policy.Uid
$policy
```

上の画像から、ポリシーが作成され、Uid が 10 であることがわかります。

構成にメールを追加するには

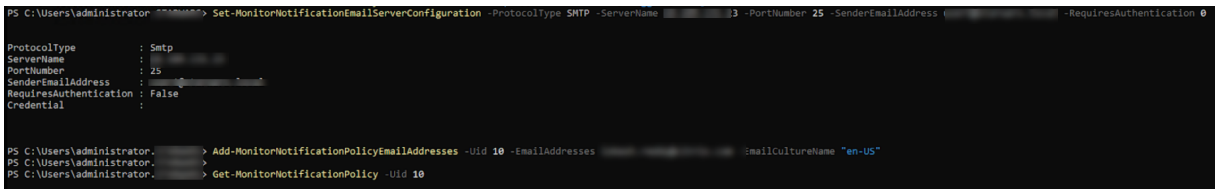
```
Set-MonitorNotificationEmailServerConfiguration -ProtocolType SMTP -
    ServerName NameOfTheSMTPServerOrIPAddress -PortNumber 80 -
    SenderEmailAddress loki@abc.com -RequiresAuthentication 0
```

ポリシーにメールを追加するには

```
Add-MonitorNotificationPolicyEmailAddresses -Uid $policy.Uid -
    EmailAddresses $emailaddress -EmailCultureName "en-US"
```

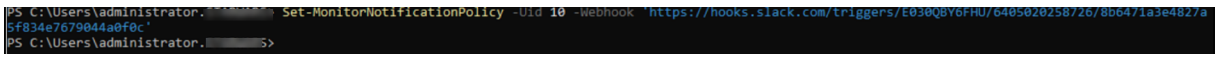
メールを追加するためのサンプルスクリプト:

```
Add-MonitorNotificationPolicyEmailAddresses -Uid 10 -EmailAddresses
    $emailaddress -EmailCultureName "en-US"
```



ポリシーに **webhook URL** を追加するには

```
Set-MonitorNotificationPolicy  - Uid $polcy.Uid  - Webhook 'URL'
```

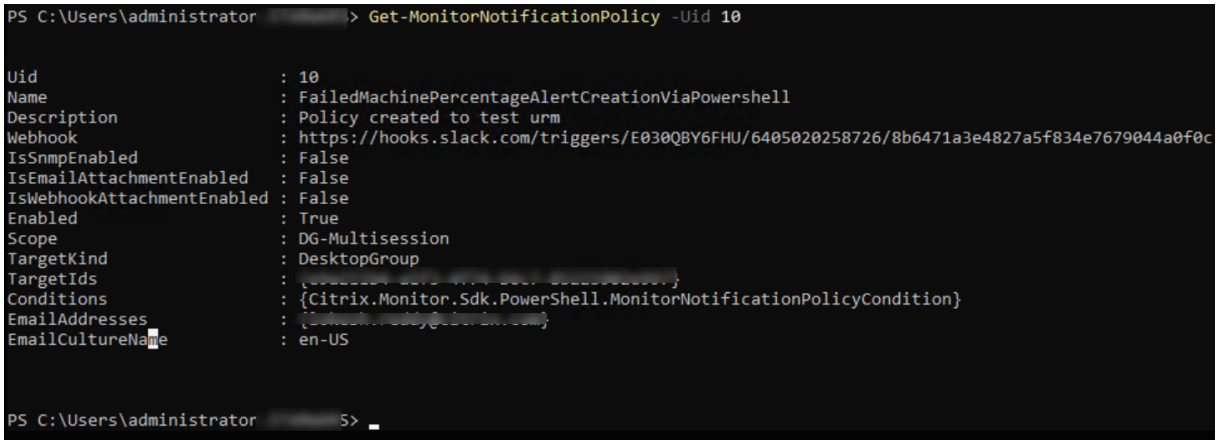


webhook URL を追加するためのサンプルスクリプト:


```
Set-MonitorNotificationPolicy -Uid 10 -Webhook 'https://hooks.slack
    .com/triggers/E030QBY6FHU/6405020258726/8
    b6471a3e4827a5f834e7679022a1f1c'
```

作成されたポリシーの詳細を取得する

```
Get-MonitorNotificationPolicy -Uid 10
```



インフラストラクチャポリシー（**Technical Preview**）

これらのポリシーは、サポートされている Citrix Virtual Apps and Desktops コンポーネントの正常性に関連するアラートを作成するために導入されています。

インフラストラクチャ監視のセットアップが完了したら、Director で利用可能な正常性データを使用して、必要なコンポーネントのアラートを構成できます。管理者は、条件、範囲、通知媒体を設定して、重要なアラートを電子メールまたは Webhook 経由の JSON ペイロードで受信できます。発生したアラートは、**Citrix** アラートセクションで分析および管理することもできます。

新しく導入されたインフラストラクチャ ポリシーの一部として、アラート条件は次の 4 つのセクションに分類されます:

- 到達可能性
- 依存サービス
- 影響
- リソース使用率

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

［アラート］>［**Citrix** アラートポリシー］セクションからインフラストラクチャポリシーを作成できます。必要なカテゴリを選択し、ポリシーに必要な条件を選択できます。ポリシーの作成方法について詳しくは「アラートポリシーの作成」を参照してください。ポリシーを作成した後、［Citrix アラート］ページでポリシーを編集、削除、または無効にできます。

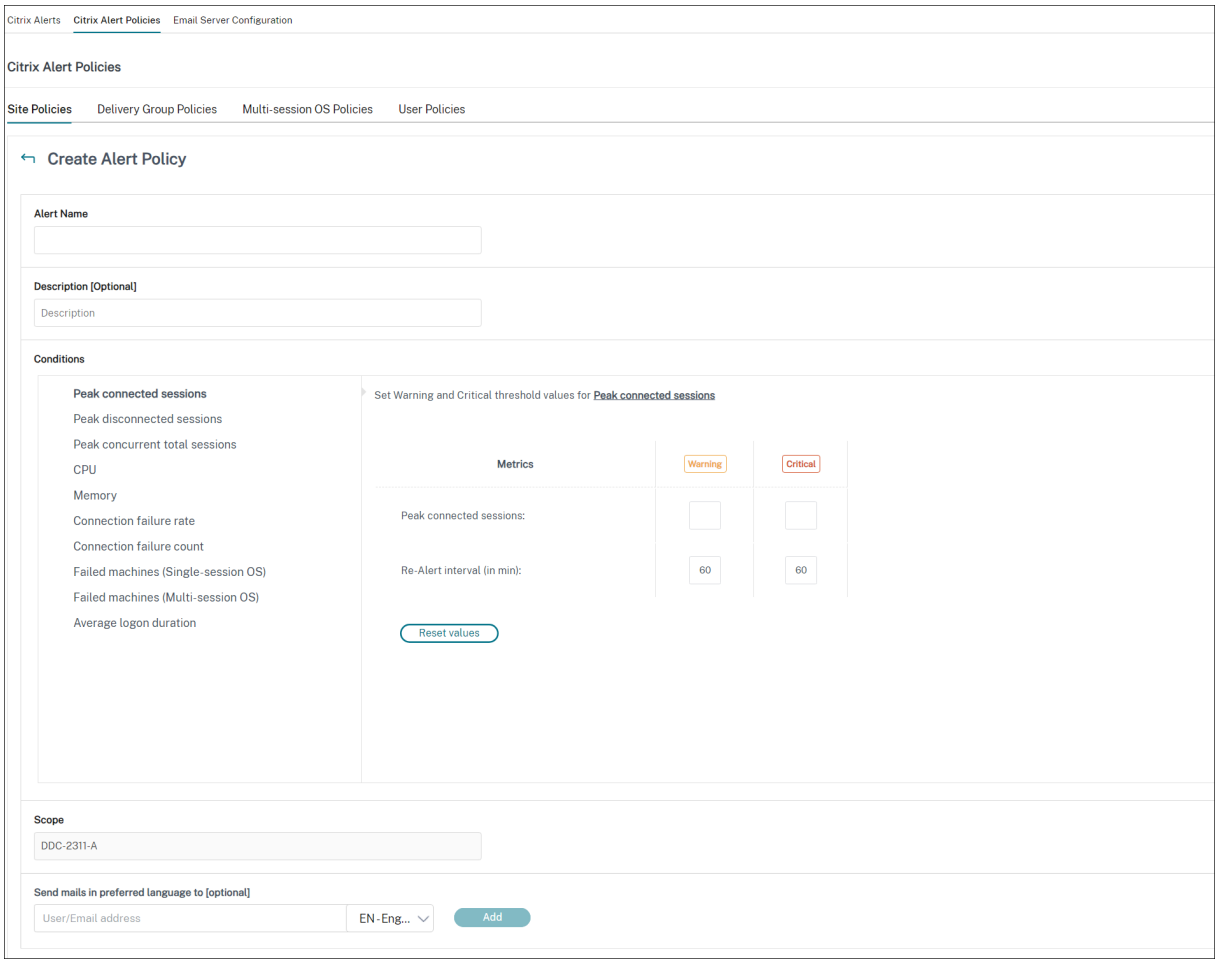
各カテゴリおよびコンポーネントでサポートされている条件の詳細については、以下を参照してください:

- PVS の正常性メトリック
- StoreFront の正常性メトリック

次のデータは、メールまたは Citrix アラートページでアラートとして受信されます:

フィールド	説明
カスタマー ID	サイトのカスタマー ID。
アラートレベル	可能な値は、Critical と Warning です。
ターゲット	アラートがトリガーされるマシンの名前。
時間	アラートがトリガーされた時刻。
スコープ	ポリシーのスコープ。
ポリシー	ポリシーの名前。
説明	アラートがトリガーされる問題の説明。

アラートポリシーの作成



特定のセッション数基準のセットを満たした場合にアラートを生成するなどの目的で、新しいアラートポリシーを作成するには、以下の手順に従います:

1. [アラート] > [**Citrix** アラートポリシー] の順に選択し、[マルチセッション OS ポリシー] などを選択します。
2. [作成] をクリックします。
3. ポリシーの名前と説明を入力し、アラートをトリガーするために満たす必要がある条件を設定します。たとえば、最大接続セッション数、最大切断セッション数、および最大同時セッション数に対して、警告とする数および重大とする数を指定します。警告値を重大値よりも大きくすることはできません。詳しくは、「アラートポリシーの条件」を参照してください。
4. 再アラート間隔を設定します。アラートの条件が引き続き満たされている場合、アラートはこの間隔で再トリガーされます。アラートポリシーで設定されている場合は、メール通知が生成されます。クリアされたアラートの場合、再アラート間隔でメール通知が生成されることはありません。
5. スコープを設定します。たとえば、特定のデリバリーグループに対して設定します。
6. お知らせ設定で、アラートがトリガーされたときのメール通知の送信先を指定します。アラートポリシーでメ

ールお知らせ設定を行うには、［メールサーバーの構成］タブでメールサーバーを指定する必要があります。

a) アラートコンテンツを、.CSV 添付ファイルまたは json ペイロード経由で受信することもできます。このためには、次のチェックボックスを選択します：

- **webhook** に添付ファイルとして **JSON** ペイロードを含める
- メールに **csv** ファイルを添付する

> 注：
>
> CSV 添付ファイルおよび json ペイロードのオプション経由でアラートコンテンツを受信するオプションは、現在、一部のアラートでのみ使用できます。詳しくは、「アラートコンテンツの機能強化」を参照してください

7. ［保存］をクリックします。

スコープに 20 件以上のデリバリーグループが定義されているポリシーを作成すると、構成が完了するまでにおよそ 30 秒かかる場合があります。完了するまで、スピナーアイコンが表示されます。

最大 20 の一意のデリバリーグループに対して、50 以上のポリシー（合計で 1000 デリバリーグループターゲット）を作成すると、応答時間が遅くなることがあります（5 秒以上）。

アクティブなセッションがあるマシンをデリバリーグループから別のデリバリーグループに移動すると、マシンパラメーターで定義されたデリバリーグループアラートが誤って発信されることがあります。

> 注：
>
> アラートポリシーを削除した後、ポリシーによって生成されたアラート通知が停止するまでに最大 30 分かかる場合があります。

アラートコンテンツの機能強化

Director のアラート機能が強化され、CSV 添付ファイルと JSON ペイロードが含まれるようになりました。この機能強化により、アラートの詳細をメールの CSV 添付ファイルで取得したり、webhook がある場合は JSON ペイロードとして取得したりできるようになります。この CSV 添付ファイルまたは JSON ペイロードを使用すると、詳細なレベルで充実したコンテンツを受け取ることができ、問題を迅速に特定して解決するのに役立ちます。

現在、この機能強化は次のアラートでのみ利用可能です：

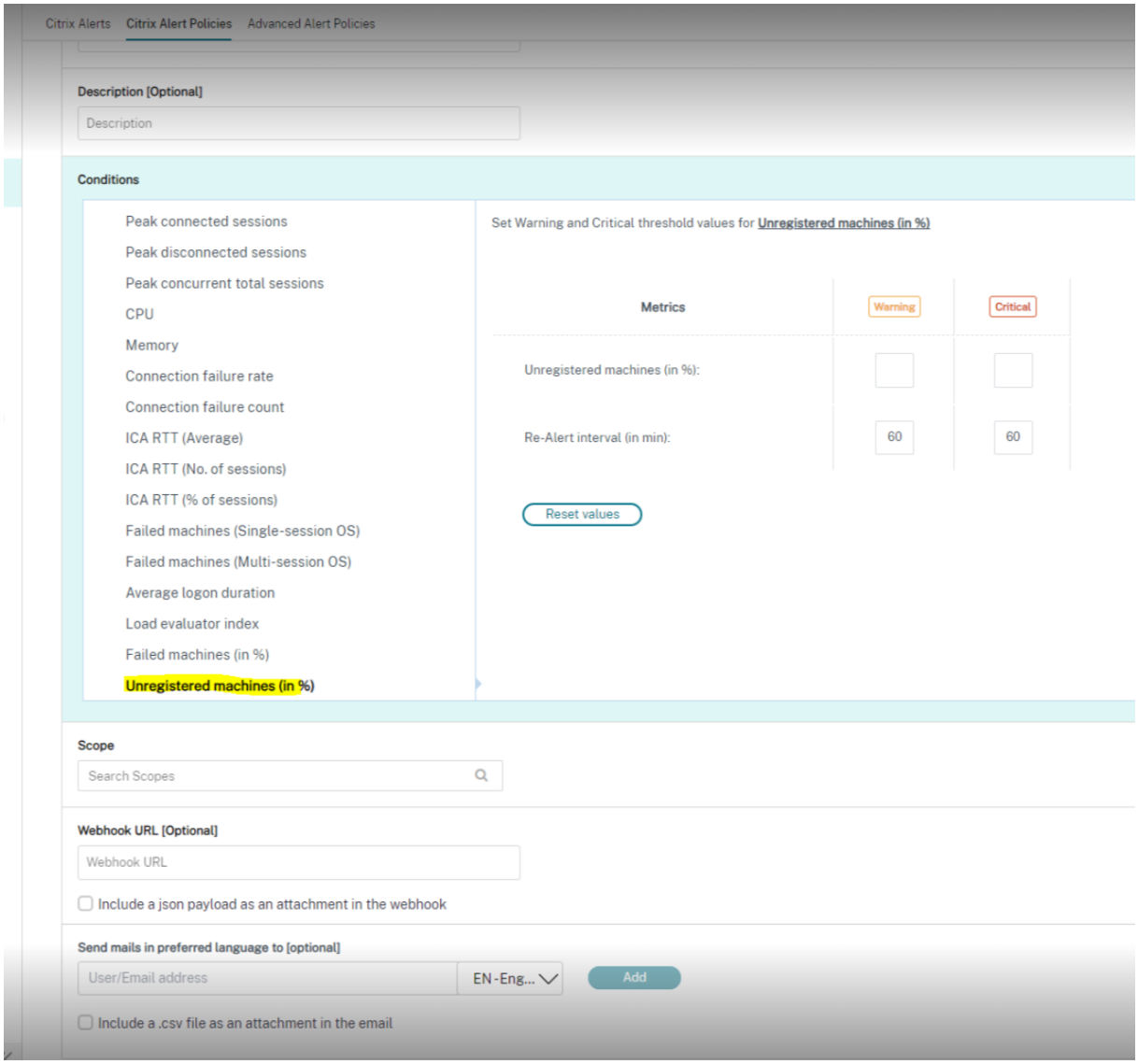
- マシンの稼働時間
- 電源オン操作の失敗
- 電源オフ操作の失敗
- 未登録のマシン（%）

この機能を使用するには、アラートに移動して次のチェックボックスを選択します：

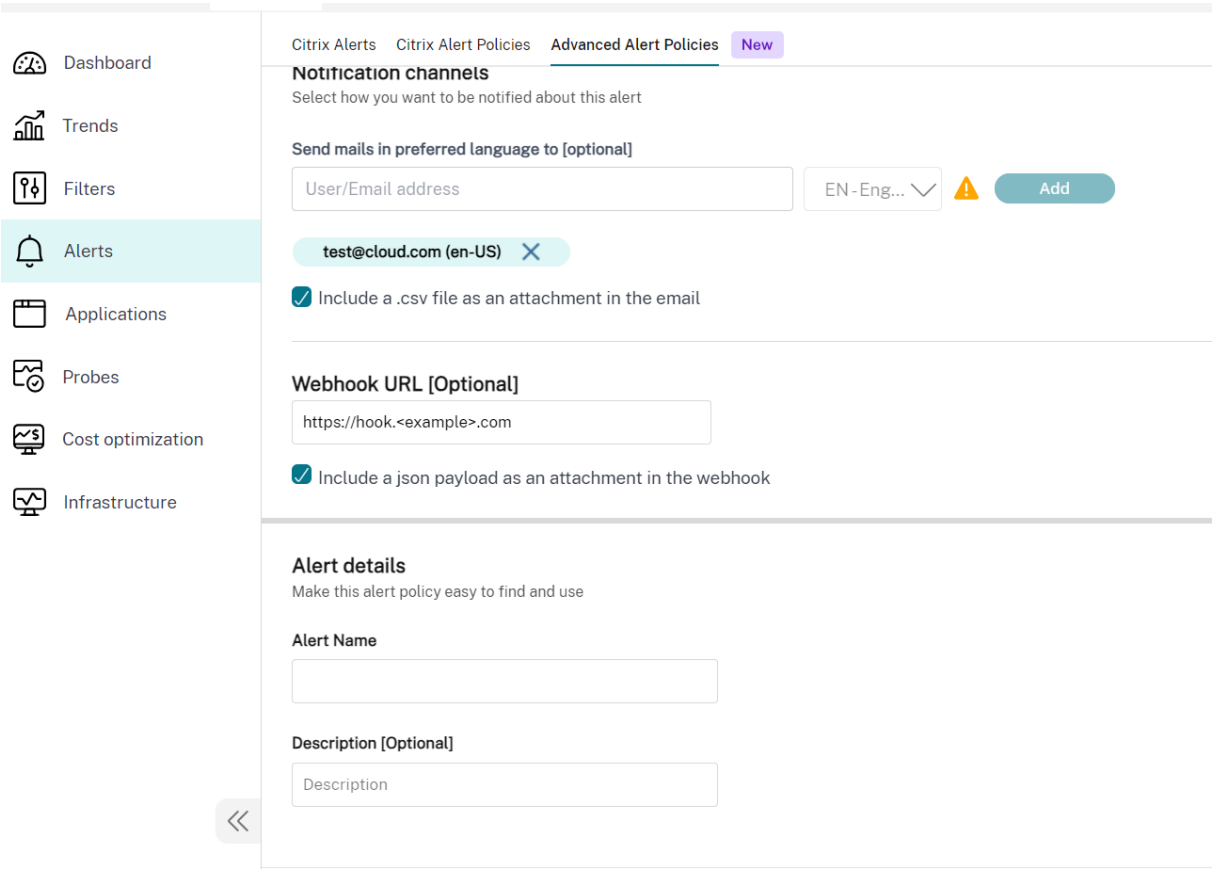
- **webhook** に添付ファイルとして **JSON** ペイロードを含める

- メールに **csv** ファイルを添付する

以下は、［**Citrix** アラートポリシー］セクションのスクリーンショットです：



以下は、［高度なアラートポリシー］セクションのスクリーンショットです：



CSV 添付ファイル　次の表は、サポートされているすべてのアラートの.CSV 添付ファイルの列を示しています：

列	該当するアラート
マシン名、IP アドレス、デリバリーグループ名	マシンの稼働時間、電源オフ操作の失敗、電源オン操作の失敗、および未登録マシン（%）
現在の登録状態、エラーの日付、エラーの状態、ライフサイクルの状態	未登録マシン（%）
最後の電源操作失敗の理由、最後の電源操作のトリガー元、最後の電源操作の種類、最後の電源操作の完了日	電源オフ操作の失敗と電源オン操作の失敗
電源状態、電源オンの日付、合計稼働時間（分）	マシンの稼働時間

webhook ペイロード

未登録マシンの割合アラート

```
Webhook Payload
{

    "Address": "<Webhook URL>",
```



```
    "NotificationId": "<NotificationGUID>",
    "NotificationState": "NotificationActive",
    "Priority": "<Critical/Warning>",
    "Target": "<DeliveryGroupName>",
    "Condition": "Unregistered machines (in %)",
    "Value": "<Value Set as Threshold>",
    "Timestamp": "<Timestamp string Eg: April 25, 2024 9:33 PM (UTC +5)
       >",
    "PolicyName": "<Alert Policy Name>",
    "Description": "<Alert Policy Description>",
    "Scope": "DeliveryGroup",
    "Site": "<Name of the Site>",
    "AttachmentData": [{

                                        "Machine Name": "<Name of the
                                           Machine>",
                                        "IP Address":  “<IP Address>” ,
                                        "Delivery Group Name": "<Name of
                                           the DeliveryGroup>",
                                        "Current Registration State": "
                                           Unregistered",
                                        "Failure Date":  “<Date of
                                           Failure>” ,
                                        "Fault State": "<Fault State of
                                           the Machine>",
                                        "Lifecycle State": "<Lifecycle
                                           state of the Machine>"
                                    }
,
                                   {

                                        "Machine Name": "<Name of the
                                           Machine>",
                                        "IP Address":  “<IP Address>” ,
                                        "Delivery Group Name": "<Name of
                                           the DeliveryGroup>",
                                        "Current Registration State": "
                                           Unregistered",
                                        "Failure Date":  “<Date of
                                           Failure>” ,
                                        "Fault State": "<Fault State of
                                           the Machine>",
                                        "Lifecycle State": "<Lifecycle
                                           state of the Machine>"
                                    }
]
}
```

電源オン操作の失敗アラート

```
Webhook Payload Body
{

    "Address": "<Webhook URL>",
```



```
5       "NotificationId": "<NotificationGUID>",
6       "NotificationState": "NotificationActive",
7       "Priority": "<Critical/Warning>",
8       "Target": "<DeliveryGroupName>",
9       "Condition": "Failure To PowerOn Action",
10      "Value": "<Value Set as Threshold>",
11      "Timestamp": "<Timestamp string Eg: April 25, 2024 9:33 PM (UTC +5)
           >",
12      "PolicyName": "<Alert Policy Name>",
13      "Description": "<Alert Policy Description>",
14      "Scope": "DeliveryGroup",
15      "Site": "<Name of the Site>",
16      "AttachmentData": [{
17
18                                          "Machine Name": "<Name of the
                                               Machine>",
19                                          "IP Address":  “<IP Address>” ,
20                                          "Delivery Group Name": "<Name of
                                               the DeliveryGroup>",
21                                        "Last Power Action Failure Reason"
                                               : "<HypervisorReportedFailure,
                                               HypervisorRateLimitExceeded,
                                               UnknownError,Power Action Type>
                                               ",
22                                          "Last Power Action Triggered By":
                                                "<End-User,Administrator,Auto
                                               -Scale,Schedule>",
23                                          "Last Power Action Type":  “<
                                               PowerOn/PowerOff>” ,
24                                          "Last Power Action Completed Date
                                               ": "<Time string Eg:
                                               2024-05-15T15:04:27.723>",
25                                    {
26
27                                          "Machine Name": "<Name of the
                                               Machine>",
28                                          "IP Address":  “<IP Address>” ,
29                                          "Delivery Group Name": "<Name of
                                               the DeliveryGroup>",
30                                          "Last Power Action Failure Reason
                                               ": "<HypervisorReportedFailure
                                               ,HypervisorRateLimitExceeded,
                                               UnknownError,Power Action Type
                                               >",
31                                          "Last Power Action Triggered By":
                                                "<End-User,Administrator,Auto
                                               -Scale,Schedule>",
32                                          "Last Power Action Type":  “<
                                               PowerOn/PowerOff>” ,
33                                          "Last Power Action Completed Date
                                               ": "<Time string Eg:
                                               2024-05-15T15:04:27.723>"
34                                      }
```



```
]
}
```

電源オフ操作の失敗アラート

```
{

    "Address": "<Webhook URL>",
    "NotificationId": "<NotificationGUID>",
    "NotificationState": "NotificationActive",
    "Priority": "<Critical/Warning>",
    "Target": "<DeliveryGroupName>",
    "Condition": "Failure To PowerOff Action",
    "Value": "<Value Set as Threshold>",
    "Timestamp": "<Timestamp string Eg: April 25, 2024 9:33 PM (UTC +5)
       >",
    "PolicyName": "<Alert Policy Name>",
    "Description": "<Alert Policy Description>",
    "Scope": "DeliveryGroup",
    "Site": "<Name of the Site>",
    "AttachmentData": [{

                                        "Machine Name": "<Name of the
                                           Machine>",
                                        "IP Address":  “<IP Address>” ,
                                        "Delivery Group Name": "<Name of
                                           the DeliveryGroup>",
                                        "IP Address": "<IPV4 Address of
                                           the Machine>",
                                        "Last Power Action Failure Reason
                                           ": "<HypervisorReportedFailure
                                           ,HypervisorRateLimitExceeded,
                                           UnknownError,Power Action Type
                                           >",
                                        "Last Power Action Triggered By":
                                            "<End-User,Administrator,Auto
                                           -Scale,Schedule>",
                                        "Last Power Action Type":  “<
                                           PowerOn/PowerOff>” ,
                                        "Last Power Action Completed Date
                                           ": "<Time string Eg:
                                           2024-05-15T15:04:27.723>"
                                    }
 ,
                                   {

                                        "Machine Name": "<Name of the
                                           Machine>",
                                        "IP Address":  “<IP Address>” ,
                                        "Delivery Group Name": "<Name of
                                           the DeliveryGroup>",
                                        "IP Address": "<IPV4 Address of
                                           the Machine>",
                                      "Last Power Action Failure Reason"
```



```
                                                    : "<HypervisorReportedFailure,
                                                    HypervisorRateLimitExceeded,
                                                    UnknownError,Power Action Type>
                                                    ",
34                                                "Last Power Action Triggered By":
                                                     "<End-User,Administrator,Auto
                                                    -Scale,Schedule>",
35                                                "Last Power Action Type":  “<
                                                    PowerOn/PowerOff>” ,
36                                                "Last Power Action Completed Date
                                                    ": "<Time string Eg:
                                                    2024-05-15T15:04:27.723>"
37                                            }
38   ]
39   }
```

マシン稼働時間のアラート

```
1   {
2
3       "Address": "<Webhook URL>",
4       "NotificationId": "<NotificationGUID>",
5       "NotificationState": "NotificationActive",
6       "Priority": "<Critical/Warning>",
7       "Target": "<DeliveryGroupName>",
8       "Condition": "Machine Uptime Alert",
9       "Value": "<Value Set as Threshold>",
10      "Timestamp": "<Timestamp string Eg: April 25, 2024 9:33 PM (UTC +5)
           >",
11      "PolicyName": "<Alert Policy Name>",
12      "Description": "<Alert Policy Description>",
13      "Scope": "DeliveryGroup",
14      "Site": "<Name of the Site>",
15      "AttachmentData": [{
16
17                                            "Machine Name": "<Name of the
                                                 Machine>",
18                                            "IP Address":  “<IP Address>” ,
19                                            "Delivery Group Name": "<Name of
                                                 the DeliveryGroup>",
20                                            "IP Address": "<IPV4 Address of
                                                 the Machine>",
21                                            "Power State": "<On/Off>",
22                                            "Powered On Date": "Time sting Eg
                                                 : 2024-05-15T15:04:27.723",
23                                            "Total Uptime In Minutes": 180
24                                        }
25   ,
26                                       {
27
28                                            "Machine Name": "<Name of the
                                                 Machine>",
29                                            "IP Address":  “<IP Address>” ,
30                                            "Delivery Group Name": "<Name of
```



```
                                                    the DeliveryGroup>",
31                                                "IP Address": "<IPV4 Address of
                                                    the Machine>",
32                                                "Power State": "<ON/OFF>",
33                                                "Powered On Date": "<Time string
                                                    Eg: 2024-05-15T15:04:27.723>",
34                                                "Total Uptime In Minutes": <
                                                    Uptime Duration>
35                                            }
36    ]
37    }
```

アラートポリシーの条件

アラートカテゴリ、アラートを緩和するための推奨アクション、および定義されている場合は組み込みポリシーの条件を以下に示します。組み込みアラートポリシーは、60 分のアラートおよび再アラートの間隔で定義されています。

最大接続セッション数

- Director セッションの傾向ビューで、最大接続セッション数をチェックします。
- セッションの負荷に対応するのに十分な処理能力があることを確認します。
- 必要に応じ、マシンを追加します。

最大切断セッション数

- Director セッションの傾向ビューで、最大切断セッション数をチェックします。
- セッションの負荷に対応するのに十分な処理能力があることを確認します。
- 必要に応じ、マシンを追加します。
- 必要に応じ、切断されたセッションからログオフします。

合計最大同時セッション数

- Director セッションの傾向ビューで、最大同時セッション数をチェックします。
- セッションの負荷に対応するのに十分な処理能力があることを確認します。
- 必要に応じ、マシンを追加します。
- 必要に応じ、切断されたセッションからログオフします。

CPU

CPU 使用率は、プロセスも含めた VDA の全体的な CPU の消費を示します。関連 VDA の ［マシンの詳細］ページで個別のプロセスによる CPU 使用率に関する情報を表示できます。

- ［マシンの詳細］**>**［履歴使用率の表示］**>**［上位 **10** 位のプロセス］に移動して、CPU を消費しているプロセスを確認します。プロセス監視ポリシーが有効になっていることを確認して、プロセスレベルのリソース使用統計の収集を開始します。
- 必要に応じてプロセスを終了します。
- プロセスを終了すると、保存されていないデータは失われます。
- すべてが想定どおりに機能している場合は、将来的に CPU リソースを追加します。

  > 注:
  >
  > ポリシー設定 ［リソースの監視を有効にします］はデフォルトで有効で、VDA がインストールされているマシンの CPU とメモリパフォーマンスカウンターを監視できます。このポリシー設定が無効にされると、CPU とメモリの条件に関するアラートはトリガーされません。詳しくは、「監視のポリシー設定」を参照してください。

  スマートポリシーの条件:

  - スコープ: デリバリーグループ、マルチセッション OS スコープ
  - しきい値: 警告 - 80%、重大 - 90%

メモリ

メモリ使用率は、プロセスも含めた VDA の全体的なメモリの消費を示します。関連 VDA の ［マシンの詳細］ページで個別のプロセスによるメモリ使用率に関する情報を表示できます。

- ［マシンの詳細］**>**［履歴使用率の表示］**>**［上位 **10** 位のプロセス］に移動して、メモリを消費しているプロセスを確認します。プロセス監視ポリシーが有効になっていることを確認して、プロセスレベルのリソース使用統計の収集を開始します。
- 必要に応じてプロセスを終了します。
- プロセスを終了すると、保存されていないデータは失われます。
- すべてが想定どおりに機能している場合は、将来的にメモリを追加します。

  > 注:
  >
  > ポリシー設定 ［リソースの監視を有効にします］はデフォルトで有効で、VDA がインストールされているマシンの CPU とメモリパフォーマンスカウンターを監視できます。このポリシー設定が無効にされ

> ると、CPU とメモリの条件に関するアラートはトリガーされません。詳しくは、「監視のポリシー設定」を参照してください。

スマートポリシーの条件：

- スコープ：デリバリーグループ、マルチセッション OS スコープ
- しきい値：警告 - 80%、重大 - 90%

接続エラー率

過去 1 時間の接続エラーの率。

- 接続の合計試行回数に対する合計エラー数の割合に基づいて計算されます。
- Director 接続エラーの傾向ビューで、構成ログから記録されたイベントをチェックします。
- アプリケーションまたはデスクトップにアクセスできるかどうかを確認します。

接続エラー数

過去 1 時間の接続エラー数。

- Director 接続エラーの傾向ビューで、構成ログから記録されたイベントをチェックします。
- アプリケーションまたはデスクトップにアクセスできるかどうかを確認します。

ICA 往復時間（平均）

平均 ICA 往復時間

- Citrix ADM で ICA RTT のブレークダウンをチェックして、原因を特定します。詳しくは、Citrix ADMのドキュメントを参照してください。
- Citrix ADM が利用可能でない場合は、Director の［ユーザーの詳細］ビューで ICA RTT および遅延をチェックして、これがネットワークの問題か、それともアプリケーションやデスクトップの問題かを特定します。

ICA 往復時間（セッション数）

ICA 往復時間を超過しているセッションの数。

- Citrix ADM で、ICA RTT が高いセッションの数をチェックします。詳しくは、Citrix ADMのドキュメントを参照してください。
- Citrix ADM が利用可能でない場合は、ネットワークチームと協力して原因を特定してください。

  スマートポリシーの条件：

  - スコープ：デリバリーグループ、マルチセッション OS スコープ
  - しきい値：警告 - 5 つ以上のセッションで 300ms、重大 - 10 以上のセッションで 400ms

ICA 往復時間（セッションの**%**）

平均 ICA 往復時間を超過しているセッションの割合。

- Citrix ADM で、ICA RTT が高いセッションの数をチェックします。詳しくは、Citrix ADMのドキュメントを参照してください。
- Citrix ADM が利用可能でない場合は、ネットワークチームと協力して原因を特定してください。

ICA RTT（ユーザー）

特定のユーザーによって開始されたセッションに適用された ICA 往復時間。1 つ以上のセッションで ICA RTT がしきい値よりも高い場合は、アラートがトリガーされます。

障害が発生したマシン（シングルセッション **OS**）

障害が発生したシングルセッションOS マシンの数。Director の［ダッシュボード］ビューおよび［フィルター］ビューに表示されるように、失敗はさまざまな理由で発生することがあります。

- Citrix Scout 診断を実行して、原因を特定します。

  スマートポリシーの条件：

  - スコープ：デリバリーグループ、マルチセッション OS スコープ
  - しきい値：警告 - 1、重大 - 2

障害が発生したマシン（マルチセッション **OS**）

失敗したマルチセッション OS マシンの数。Director の［ダッシュボード］ビューおよび［フィルター］ビューに表示されるように、失敗はさまざまな理由で発生することがあります。

- Citrix Scout 診断を実行して、原因を特定します。

  スマートポリシーの条件：

  - スコープ：デリバリーグループ、マルチセッション OS スコープ
  - しきい値：警告 - 1、重大 - 2

障害が発生したマシン（**%**）

障害が発生したマシンの数に基づいて計算された、デリバリーグループ内の障害が発生したシングルセッションおよびマルチセッション OS マシンの割合。アラートの条件を設定する際、アラートのしきい値をデリバリーグループ内の障害が発生したマシンの割合で構成できます。この条件は 30 秒ごとに計算されます。
Director の［ダッシュボード］ビューおよび［フィルター］ビューに表示されるように、失敗はさまざまな理由で発生することがあります。Citrix Scout 診断を実行して、原因を特定します。詳しくは、「ユーザーの問題のトラブルシューティング」を参照してください。

電源オフ操作の失敗と電源オン操作の失敗

電源オンまたはオフに失敗した電源管理されたマシンの数に基づいて計算された、デリバリーグループ内の失敗した電源オン操作の数と失敗した電源オフ操作の数。このアラート条件を使用すると、デリバリーグループ内で電源のオン/オフに失敗した電源管理されたマシンの数としてアラートしきい値を構成でき、このしきい値は 30 分ごとに計算されます。

管理者は、高度なアラートポリシーでこれらのアラートの次のパラメーターを設定できます：

- トリガー元：電源操作をトリガーしたもの
- エラーの理由:：操作が失敗した理由
- しきい値：ポリシーをトリガーする、電源操作に失敗したマシンのしきい値数
- サンプリング間隔：失敗した電源操作をチェックする間隔
- 再アラート間隔：アラートを再送信するまでの期間

Director の［ダッシュボード］ビューおよび［フィルター］ビューに表示されるように、失敗はさまざまな理由で発生することがあります。Citrix Scout 診断を実行して、原因を特定します。詳しくは、「ユーザーの問題のトラブルシューティング」を参照してください。

未登録マシン（**%**）

再起動によりマシンが不安定になった場合、または Delivery Controller と仮想マシンの間に通信の問題が発生した場合、マシンは未登録とみなされます。未登録マシン（**%**）デリバリーグループ内の未登録のシングルセッションおよびマルチセッション OS マシンの割合で、未登録マシンの数に基づいて計算されます。このアラート条件を使用すると、警告および重大のしきい値を、デリバリーグループ内の未登録マシンの割合で構成できます。再アラートの間隔を設定できます。未登録マシン（**%**）の条件が満たされたときに通知を受け取るメールアドレスを追加することもできます。重大または警告のしきい値を超えると、アラートとメールが生成されます。**Citrix** アラートでアラートを表示できます。未登録マシン（**%**）カテゴリで必要な状態および時間に関してフィルタリングできます。

アラートの詳細は、メールの場合は CSV 添付ファイルで、webhook の場合は JSON ペイロードで受け取ることもできます。

> 注:
>
> 重大値は警告値より大きくなければなりません。

ポリシー条件:

- スコープ: シングルセッション OS、およびマルチセッション OS デリバリーグループ
- しきい値: 警告および重大

マシン稼働時間のアラート

デリバリーグループ内のマシンの稼働時間は、デリバリーグループ内でオンになっているマシンの 1 日あたりの時間数、1 週間あたりの時間数、または 1 か月あたりの時間数に基づいて計算されます。このアラート条件を使用すると、アラートのしきい値を、デリバリーグループ内でオンになっているマシンの時間数で構成できます。マシン稼働時間のアラートは、次の場合に機能します:

- 1 日あたりの時間 - 1 日にマシンがオンになっている時間数を指定できます。これは 30 分ごとに計算されます。1 日あたりに設定できる最大時間数は 24 時間です。
- 1 週間あたりの時間 - 1 週間にマシンがオンになっている時間数を指定できます。これは 6 時間ごとに計算されます。1 週間あたりに設定できる最大時間数は 168 時間です。
- 1 か月あたりの時間 - 1 か月にマシンがオンになっている時間数を指定できます。これは 1 日 1 回計算されます。1 か月あたりの最大時間は 720 時間です。
  設定できる最小の再アラート間隔値は 60 分です。警告および重大なアラートのセクションで、マシンの稼働時間のしきい値を超えるマシンの数を入力できます。任意のマシンに対して例外を追加することもできます。

たとえば、このアラートに 5 つのデリバリーグループが追加されていて、最初のデリバリーグループと 4 番目のデリバリーグループマシンの数が警告または重大なしきい値を超えた場合、最初のデリバリーグループと 4 番目のデリバリーグループに対してアラートが個別にトリガーされます。

このアラートは、管理者がマシンの稼働時間を分析するのに役立ち、この分析に基づいて管理者はコストの最適化を実行できます。アラートの詳細は、メールの場合は CSV 添付ファイルで、webhook の場合は JSON ペイロードで受け取ることもできます。

平均ログオン時間

過去 1 時間に行われたログオンの平均ログオン処理時間。

- Director のダッシュボードをチェックし、ログオン処理時間に関する最新の測定基準を取得します。短時間のうちに多数のユーザーがログインするとログオン処理時間が長引くことがあります。
- 原因を絞り込むため、ログオンのベースラインおよび内訳をチェックします。詳しくは、「ユーザーログオンの問題の診断」を参照してください

  スマートポリシーの条件:

  - スコープ：デリバリーグループ、マルチセッション OS スコープ
  - しきい値：警告 - 45 秒、重大 - 60 秒

ログオン処理時間（ユーザー）

過去 1 時間に行われた指定されたユーザーのログオンに関するログオン処理時間。

負荷評価基準インデックス

過去 5 分間の負荷評価基準インデックスの値。

- Director で、ピーク負荷（最大負荷）に達している可能性があるマルチセッション OS マシンをチェックします。ダッシュボード（失敗）および負荷評価基準インデックス傾向レポートを表示します。

  スマートポリシーの条件：

  - スコープ：デリバリーグループ、マルチセッション OS スコープ
  - しきい値：警告 - 80%、重大 - 90%

webhook によるアラートポリシーの構成

メール通知以外に、webhook でアラートポリシーを構成できます。

注：この機能の使用には、Delivery Controller バージョン 7.11 以降が必要です。

PowerShell コマンドレットを使用して、HTTP コールバックまたは HTTP POST でアラートポリシーを構成できます。webhooks のサポートのために拡張されます。

新しい Octoblu ワークフローの作成および対応する webhook URL の取得について詳しくは、『Octoblu Developer Hub』を参照してください。

新しいアラートポリシーや既存のポリシーに対して webhook URL を構成するには、次の PowerShell コマンドレットを使用します。

webhook URL で新しいアラートポリシーを作成する場合：

```
$policy = New-MonitorNotificationPolicy -Name <Policy name> -
    Description <Policy description> -Enabled $true -Webhook <Webhook
    URL>
```

既存のアラートポリシーに webhook URL を追加する場合：

```
Set-MonitorNotificationPolicy - Uid <Policy id> -Webhook <Webhook URL>
```

PowerShell コマンドのヘルプについては、たとえば次のように PowerShell ヘルプを使用します：

```
Get-Help  <Set-MonitorNotificationPolicy>
```


アラートポリシーから生成された通知によって、webhook URL への POST コールで webhook がトリガーされます。POST メッセージには通知の情報が JSON 形式で含まれます:

```
{
 "NotificationId" : \<Notification Id\>,

"Target" : <Notification Target Id>,

"Condition" : <Condition that was violated>,

"Value" : <Threshold value for the Condition>,

"Timestamp": <Time in UTC when notification was generated>,

"PolicyName": <Name of the Alert policy>,

"Description": <Description of the Alert policy>,

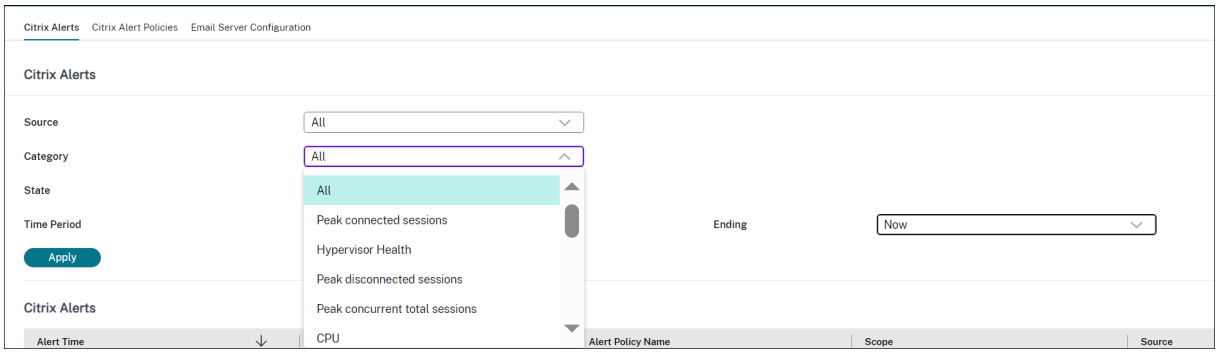
"Scope" : <Scope of the Alert policy>,

"NotificationState": <Notification state critical, warning, healthy or
   dismissed>,

"Site" : \<Site name\> }
```

ハイパーバイザーアラートの監視

Director では、ハイパーバイザーの正常性を監視するアラートが表示されます。XenServer と VMware vSphere のアラートは、ハイパーバイザーのパラメーターと状態を監視するのに役立ちます。ハイパーバイザーへの接続状態も監視され、クラスターまたはホストのプールが再起動された場合、または使用できなくなった場合にアラートが出されます。

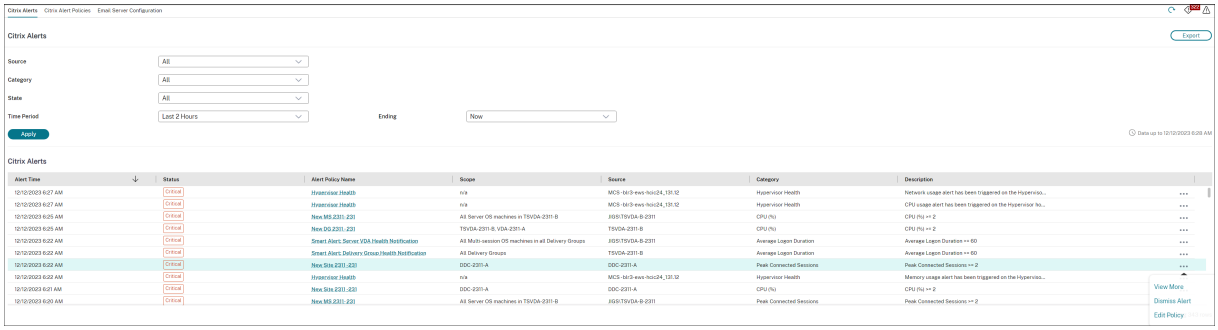


ハイパーバイザーアラートを受信するには、Web Studio でホスト接続が作成されている必要があります。詳しくは、「接続およびリソース」を参照してください。ハイパーバイザーアラートではこれらの接続のみが監視されます。

これらのアラートは、しきい値に達するか超過すると表示されます。ハイパーバイザーのアラートには次のものがあります:

- 重大—ハイパーバイザーアラームポリシーの重大しきい値に達したか超過した

- 警告—ハイパーバイザーアラームポリシーの警告しきい値に達したか超過した
- 解除—アラートはアクティブなアラートとして表示されなくなる



この機能の使用には、Delivery Controller バージョン 7 1811 以降が必要です。サイトの 7 1811 以降で古いバージョンの Director を使用している場合は、ハイパーバイザーアラート数のみが表示されます。アラートを表示するには、Director をアップグレードする必要があります。

次の表に、ハイパーバイザーアラートのさまざまなパラメーターと状態を示します。

アラート	サポートされるハイパーバイザー	トリガー元	条件	構成
CPU 使用率	XenServer、VMware vSphere	Hypervisor	CPU 使用率アラートしきい値に達しているか、超過している	アラートしきい値は、ハイパーバイザーで設定する必要があります。
メモリ使用率	XenServer、VMware vSphere	Hypervisor	メモリ使用率アラートしきい値に達しているか、超過している	アラートしきい値は、ハイパーバイザーで設定する必要があります。
ネットワーク使用状況	XenServer、VMware vSphere	Hypervisor	ネットワーク使用率アラートしきい値に達しているか、超過している	アラートしきい値は、ハイパーバイザーで設定する必要があります。
ディスク使用率	VMware vSphere	Hypervisor	ディスク使用率アラートしきい値に達しているか、超過している	アラートしきい値は、ハイパーバイザーで設定する必要があります。
ホスト接続や電源の状態	VMware vSphere	Hypervisor	ハイパーバイザーホストが再起動されたか、または利用できない	アラートは VMware vSphere にあらかじめ組み込まれています。追加の構成は必要ありません。

アラート	サポートされるハイパーバイザー	トリガー元	条件	構成
使用不可のハイパーバイザー接続	XenServer、VMware vSphere	Delivery Controller	ハイパーバイザー（プールまたはクラスター）への接続が失われるか、電源がオフになるか、再起動されます。このアラートは、接続が利用できない間、1 時間ごとに生成されます。	アラートは Delivery Controller にあらかじめ組み込まれています。追加の構成は必要ありません。

> 注:
>
> アラートの構成について詳しくは、「Citrix XenCenter アラート」を参照するか、VMware vCenter アラートのドキュメントを確認してください。

メール通知設定は、［**Citrix** アラートポリシー］**>**［サイトポリシー］**>**［ハイパーバイザーの正常性］から設定できます。Hypervisor のアラートポリシーのしきい値条件は、Director からではなくハイパーバイザーからのみ設定、編集、無効化、または削除できます。ただし、メール設定の変更とアラートの解除は Director で行うことができます。役割にインフラストラクチャの監視が含まれていない場合は、アラートを無効にすることができます。

> 重要:
>
> - アラートは Hypervisor により取得され、Director に表示されます。ただし、Hypervisor のアラートのライフサイクルや状態に対する変更は、Director には反映されません。
> - 正常状態のアラートや Hypervisor コンソールで破棄または無効化したアラートであっても、Director には表示され続けるため、Director で明示的に破棄する必要があります。
> - アラートを Director で破棄しても、Hypervisor コンソールで自動的に破棄されることはありません。

トラブルシューティングのためのデータのフィルター処理

August 17, 2024

［ダッシュボード］で数値をクリックしたり［フィルター］メニューから事前定義のフィルターを選択したりすると、［フィルター］ビューが開きます。ここには、選択したマシンまたはエラーの種類に関するデータが表示されます。

事前定義のフィルターはそのままでは編集できませんが、それをカスタムフィルターとして保存してから編集することができます。また、すべてのデリバリーグループでのマシン、接続、セッション、アプリケーションインスタンスのカスタムフィルタービューを作成できます。

1. 以下のビューを選択します。

    - マシン。シングルセッションOS マシンまたはマルチセッション OS マシンを選択します。これらのタブには構成されたマシンの数が表示されます。また、［マルチセッション OS マシン］タブには負荷評価基準インデックスが表示され、その測定値上にマウスポインターを置くと各パフォーマンスカウンターの測定値やセッション数がツールチップとして表示されます。
    - セッション。直近の 60 分、24 時間、7 日間、またはカスタムの期間などのさまざまな期間でセッションをフィルタリングできます。［セッション］ビューでセッション数を表示することもできます。アイドル時間の測定値から、しきい値時間を超えてアイドル状態にあるセッションを特定できます。［関連ユーザー］をクリックすると、ユーザーのアクティビティマネージャーが開きます。エンドポイントの名前をクリックすると、エンドポイントのアクティビティマネージャーが開きます。各場合に［詳細の表示］をクリックすると、［ユーザーの詳細］ページまたは ［エンドポイント詳細］ページが開きます。詳しくは、 ［ユーザーの詳細］を参照してください。
    - 接続。直近の 60 分、24 時間、7 日間、またはカスタムの期間などのさまざまな期間で接続をフィルタリングできます。
    - アプリケーションインスタンス。直近の 60 分、24 時間、7 日間、またはカスタムの期間などのさまざまな期間でアプリケーションインスタンスをフィルタリングできます。このビューは、サーバーおよびシングルセッション OS VDA 上におけるすべてのアプリケーションインスタンスのプロパティを表示します。セッションのアイドル時間測定機能は、マルチセッション OS 対応 VDA のアプリケーションインスタンスに利用できます。

    > 注:
    >
    > Windows 10 1809 コンピューターにインストールされた VDA でデスクトップセッションを起動した場合、実際にはバックグラウンドで実行されている Microsoft Edge と Office が、Director のアクティビティマネージャー上ではアクティブ状態のアプリケーションとして表示されることがあります。

2. ［フィルター基準］で、フィルター条件を選択します。
3. 必要に応じて、各ビューで追加のタブを使用してフィルターを実行します。
4. 必要に応じて追加の列を選択して、より詳細な情報を表示します。
5. フィルターに名前を付けて保存します。
6. 複数の Director サーバーからフィルターにアクセスするには、これらのサーバーからアクセス可能な共有フォルダーにフィルターを保存します:

    - 共有フォルダーには、Director サーバーのアカウントを変更する権限が必要です。
    - Director サーバーは、共有フォルダーにアクセスするよう構成されている必要があります。構成するには、**IIS** マネージャーを実行します。［サイト］**>**［既定の **Web** サイト］**>**［**Director**］**\>**［アプリケー

ションの設定］の順に移動し、**Service.UserSettingsPath** の設定が共有フォルダーの UNC パスを反映するように変更します。

7. 後でフィルターを開くには、［フィルター］メニューでフィルターの種類（マシン、セッション、接続、またはアプリケーションインスタンス）を選択し、保存済みのフィルターを選択します。
8. データを CSV 形式のファイルにエクスポートするには、［エクスポート］をクリックします。最大 100,000 レコードのデータをエクスポートできます。この機能は、Delivery Controller バージョン 1808 以降で使用できます。
9. ［マシン］ビューまたは ［接続］ビューでは、必要に応じ一覧でマシンを選択して電源制御操作を実行できます。［セッション］ビューでは、セッション制御を実行したりメッセージを送信したりできます。
10. ［マシン］ビューおよび ［接続］ビューで障害が発生したマシンまたは接続の ［エラーの理由］をクリックすると、障害の詳細な説明と、障害をトラブルシューティングするために推奨される操作が表示されます。マシンおよび接続でエラーが発生した場合のエラーの理由と推奨される解決手順は、「Citrix Director の失敗の原因とトラブルシューティング」に記載されています。
11. ［マシン］ビューでマシン名のリンクをクリックすると、対応する ［マシンの詳細］ページが開きます。マシンの詳細を表示するこのページでは、電源制御が提供され、CPU、メモリ、ディスクの監視、および GPU の監視グラフが表示されます。また、［履歴使用率の表示］をクリックすると、マシンのリソース使用傾向が表示されます。詳しくは、「マシンのトラブルシューティング」を参照してください。
12. ［アプリケーションインスタンス］ビューでは、しきい値時間を超えた ［アイドル時間］に基づいてソートまたはフィルターできます。終了させるアイドル状態のアプリケーションインスタンスを選択します。ログオフまたはアプリケーションインスタンスを切断すると同一セッション内のすべてのアクティブなアプリケーションインスタンスが終了します。詳しくは、「アプリケーションのトラブルシューティング」を参照してください。アプリケーションインスタンスのフィルターページと、セッションのフィルターページにあるアイドル時間の測定値は、Citrix Director、Delivery Controller、および VDA の各バージョンが 7.13 以降である場合に使用可能です。

> 注:
> Web Studio では、さまざまなユーザーまたはユーザーグループの複数のデスクトップ割り当て規則（DAR）を、デリバリーグループ内の 1 つの VDA に割り当てることができます。StoreFront は、ログインしたユーザーの DAR に従って、割り当てられたデスクトップを対応する表示名で表示します。ただし、Director では DAR はサポートされておらず、ログインしているユーザーに関係なく、デリバリーグループ名を使用して割り当て済みのデスクトップが表示されます。このため、Director で特定のデスクトップをマシンにマッピングすることはできません。StoreFront に表示されている割り当て済みデスクトップを Director に表示されているデリバリーグループ名にマッピングするには、次の PowerShell コマンドを使用します:

```
Get-BrokerDesktopGroup | Where-Object {
  $_.Uid -eq (Get-BrokerAssignmentPolicyRule | Where-Object {
  $_.PublishedName -eq "<Name on StoreFront>"  }
 ).DesktopGroupUid  }
  | Select-Object -Property Name, Uid
```


サイト全体の履歴傾向の監視

August 17, 2024

［傾向］ビューでは、次のパラメーターについて各サイトの履歴傾向情報が表示されます：

- セッション
- 接続エラー
- マシンエラー
- ログオン処理のパフォーマンス
- 負荷評価
- 容量管理
- マシンの使用量
- リソース使用
- 各サイトのネットワーク分析。

この情報を表示するには、［傾向］メニューをクリックします。

ズームインドリルダウン機能により、（グラフ内のデータポイントをクリックして）ある期間について着目し、その傾向に関連する詳細情報を表示させて、傾向チャートを参照できます。この機能を使用すれば、誰がまたは何が影響を受けているかについての詳細を把握できます。

各グラフのデフォルトの表示範囲を変更するには、［期間］フィルターを変更して適用します。

履歴傾向情報を必要とする期間を選択します。使用可能な期間は、Director 環境に応じて次のように異なります：

- Premium Edition ユーザーは、前年（365 日）までの傾向レポートを利用できます。
- Advanced Edition ユーザーは、前月（31 日）までの傾向レポートを利用できます。
- Premium Edition および Advanced Edition 以外のユーザーは、過去 7 日間の傾向レポートを利用できます。

> 注：
>
> - すべての Director 展開環境で、セッション、障害、ログオンパフォーマンスの傾向情報をグラフやテーブルとして表示できるのは、期間を ［先月（現時点まで）］以下に設定した場合です。期間に、終了日が設定可能な［先月］、または［昨年］を選択すると、傾向情報はグラフとして表示できますが、テーブルとしては表示できません。
> - Monitor Service の保持値をグルーミングすることで、傾向データの可用性を制御できます。デフォルト値は、「データの粒度と保持」に記載されています。Premium Edition では、クリーンアップ保持を必要な保持日数に変更できます。
> - IIS マネージャーの次のパラメーターは、選択可能なカスタム終了日の範囲を制御します。ただし、選択した日付のデータ可用性は、測定されている特定のメトリックのグルーミング保持設定によって異なります。

パラメーター	デフォルト値
UI.TrendsLast2HoursRange	3
UI.TrendsLast24HoursRange	32
UI.TrendsLast7DaysRange	32
UI.TrendsLastMonthRange	365

利用できる傾向

セッションの傾向の表示：［セッション］タブから、同時接続セッション数に関するより詳細な情報を表示するデリバリーグループと期間を選択します。

［セッションの自動再接続］列はセッション内で自動的に再接続を行う回数を表します。自動再接続は、［セッション画面の保持］ポリシーまたは［クライアントの自動再接続］ポリシーが有効な場合に有効になります。エンドポイントでネットワークの接続が中断された場合は、次のポリシーが有効になります：

- セッション画面の保持ポリシーが有効になり、デフォルトで 3 分間の持続時間に Citrix Receiver または Citrix Workspace アプリが VDA への接続を試みます。
- クライアントの自動再接続ポリシーが有効になり、3〜5 分間の持続時間にクライアントが VDA への接続を試みます。

どちらの場合も再接続の情報は記録され、ユーザーが確認できるようになっています。この情報が Director UI に表示されるまでには、再接続が施行されてから最大 5 分ほどかかることがあります。

自動再接続の情報は中断が発生したネットワーク接続の確認やトラブルシューティングに役立ちます。また、シームレスなネットワークの分析にも活用できます。再接続数はデリバリーグループを指定したり、フィルターで特定の期間に絞り込んだりしたうえで表示することができます。ドリルダウンではセッション画面の保持やクライアントの自動再接続、タイムスタンプ、エンドポイントの IP、Workspace アプリがインストールされているマシンのエンドポイント名などの詳しい情報を確認できます。

デフォルトでは、ログはイベントが起きたタイムスタンプに従って降順で並び替えられます。この機能は、Windows 向け Citrix Workspace アプリ、Mac 向け Citrix Workspace アプリ、Citrix Receiver for Windows、および Citrix Receiver for Mac で使用できます。使用するには Delivery Controller バージョン 7 1906 以降および VDA のバージョン 1906 以降が必要です。

セッションの再接続について詳しくは、「セッション」を参照してください。

ポリシーについて詳しくは、「クライアントの自動再接続のポリシー設定」および「セッション画面の保持のポリシー設定」を参照してください。

次の理由により、自動再接続データが Director に表示されない場合があります：

- Workspace アプリから VDA に自動再接続データが送信されていない。

- VDA から監視サービスにデータが送信されていない。
- 対応するセッションがない可能性があるため、Delivery Controller が VDA ペイロードを破棄する。

> 注:
>
> 特定の Citrix Gateway ポリシーが設定されていると、クライアント IP アドレスが正しく取得できないことがあります。

接続エラーの傾向の表示:［エラー］タブで、サイト全体のユーザー接続エラーの詳細情報を含むグラフを表示する接続、マシンの種類、エラーの種類、デリバリーグループ、および期間を選択します。

マシン障害の傾向の表示:［失敗したシングルセッション**OS** マシン］タブまたは［失敗したマルチセッション OS マシン］タブで、サイト全体のマシンエラーの詳細情報を含むグラフを表示するエラーの種類、デリバリーグループ、および期間を選択します。

ログオンパフォーマンスの傾向の表示:［ログオンパフォーマンス］タブで、サイト全体のログオン処理時間と、ログオン数がパフォーマンスに影響しているかについての詳細情報を含むグラフを表示するデリバリーグループと期間を選択します。このビューには、仲介処理時間や仮想マシンの起動時間などのログオンフェーズにおける平均時間も表示されます。
このデータはユーザーのログオンに関するものであり、切断セッションへの再接続は含まれません。
グラフの下のテーブルに、ユーザーセッションごとのログオン時間が表示されます。表示する列を選択し、いずれかの列を基準にレポートを並べ替えることができます。これらのレポートを.CSV ファイルにエクスポートすることもできます。
詳しくは、「ユーザーログオンの問題の診断」を参照してください

負荷評価の傾向の表示:［負荷評価基準インデックス］タブで、マルチセッション OS マシン間で分散された負荷に関する情報を表示します。このグラフでは、対象のデリバリーグループ、マルチセッション OS マシン、および期間を指定できます（マルチセッション OS マシンは、デリバリーグループのマルチセッション OS マシンが選択されている場合のみ指定可能）。

ホストされたアプリケーションの使用量の表示:この機能は、組織のライセンスによっては使用できない場合があります。
［容量管理］タブから ［ホストされたアプリケーションの使用量］タブを選択します。特定のデリバリーグループおよび期間を選択すると、最大同時使用量を示すグラフとアプリケーションごとの使用量を示す表が表示されます。［アプリケーションごとの使用量］の表では、特定のアプリケーションについての詳細や、そのアプリケーションを使用しているユーザー、および使用していたユーザーの情報を表示できます。

シングルセッション **OS** およびマルチセッション **OS** の使用状況の表示:［傾向］ビューでは、サイト別およびデリバリーグループ別のシングルセッション OS の使用状況が表示されます。［サイト］を選択すると、デリバリーグループごとの使用状況が表示されます。デリバリーグループを選択すると、ユーザーごとの使用状況が表示されます。
［傾向］ビューでは、サイト別、デリバリーグループ別、およびマシン別のマルチセッション OS の使用状況も表示されます。［サイト］を選択すると、デリバリーグループごとの使用状況が表示されます。デリバリーグループを選択すると、マシンごとおよびユーザーごとの使用状況が表示されます。マシンを選択すると、ユーザーごとの使用状況が表示されます。

仮想マシン使用量の確認：［マシン使用量］タブで ［シングルセッション **OS** マシン］または［マルチセッション **OS** マシン］を選択して、仮想マシンの使用状況をリアルタイムで表示し、サイトのキャパシティニーズにすばやく対処することができます。
シングルセッション OS の可用性 - シングルセッション OS マシン（VDI）の現在の状態をサイト全体または特定のデリバリーグループについて可用性に基づいて表示します。
マルチセッション OS の可用性 - マルチセッション OS マシンの現在の状態をサイト全体または特定のデリバリーグループについて可用性に基づいて表示します。

> 注：
> 使用可能カウンターに表示されるマシンの数には、保守モードのマシンが含まれます。

リソース使用の表示：［リソース使用］タブで ［シングルセッション **OS** マシン］または［マルチセッション **OS** マシン］を選択して、各 VDI マシンの CPU とメモリ使用量、および IOPS とディスク遅延に関する履歴傾向を取得し、容量の計画に役立てることができます。
この機能の使用には、Delivery Controller および VDA のバージョン **7.11** 以降が必要です。
平均 CPU、平均メモリ、平均 IOPS、ディスク遅延、および最大同時セッション数を表示するグラフです。マシンにドリルダウンして、CPU を消費している上位 10 のプロセスに関するデータとチャートを表示できます。

デリバリーグループ別および期間別でフィルターできます。過去 2 時間、24 時間、7 日間、月、年の CPU、メモリ使用量、最大同時セッション数のグラフを入手できます。平均 IOPS とディスク遅延は、過去 24 時間、月、年のグラフが入手可能です。

> 注：
>
> - データを収集して［マシン使用率の履歴］ページの［上位 10 位のプロセス］表に表示するには、監視ポリシーの ［プロセスの監視を有効にします］設定を ［許可］に設定する必要があります。このポリシーはデフォルトでは禁止されています。デフォルトではすべてのリソース使用率データが収集されます。これは、ポリシーの［リソース監視の有効化］設定で無効にできます。グラフの下のテーブルは、マシンごとのリソース使用率データを示しています。詳しくは、「監視のポリシー設定」を参照してください。
> - 平均 IOPS は、1 日の平均値を示します。最大 IOPS は、選択した期間の IOPS の平均において最も高い IOPS が算出されます。（IOPS の平均は、選択した期間に VDA で収集された IOPS の 1 時間当たりの平均です）。
> - マシンのドリルダウンで、平均 CPU または平均メモリ使用率が 1% を超えるプロセスが一覧表示されます（一覧に含まれるプロセスが 10 個未満になることがあります）。

ネットワーク分析データの表示：この機能は、組織のライセンスおよび管理者権限によっては使用できない場合があります。この機能には、Delivery Controller バージョン **7.11** 以降が必要です。

［ネットワーク］タブで、ネットワークのユーザー、アプリケーション、およびデスクトップコンテキストビューを表示してネットワーク分析をモニターします。この機能により、Director は Citrix ADM の HDX Insight レポートを使用して ICA トラフィックを詳細に分析できます。詳しくは、「ネットワーク分析機能の構成」を参照してください。

アプリケーション障害の表示：［アプリケーション障害］タブで、VDA 上の公開アプリケーションに関連した障害が表示されます。

この機能の使用には、Delivery Controller および VDA のバージョン **7.15** 以降が必要です。Windows Vista 以降が動作するシングルセッション OS VDA、および Windows Server 2008 以降が動作するマルチセッション OS VDA がサポートされます。
詳しくは、「アプリケーション障害履歴の監視」を参照してください。

デフォルトでは、マルチセッション OS VDA からのアプリケーション障害のみが表示されます。監視ポリシーを使って、アプリケーション障害の監視の設定ができます。詳しくは、「監視のポリシー設定」を参照してください。

プローブの結果を表示する：［プローブの結果］タブには、［構成］ページでプロービングが設定されているアプリケーションおよびデスクトップのプローブの結果が表示されます。そこには、失敗した起動の段階が記録されています。

詳しくは、「アプリケーションプロービングおよびデスクトッププロービング」を参照してください。

カスタム レポートの作成：［カスタムレポート］タブには、監視データベースのリアルタイムデータおよび履歴データを含むカスタムレポートを表形式で生成するためのユーザーインターフェイスがあります。

この機能には、Delivery Controller バージョン **7.12** 以降が必要です。

以前に保存されたカスタムレポートクエリの一覧で、［実行してダウンロード］をクリックするとそのレポートを CSV 形式でエクスポートでき、［**OData** のコピー］をクリックすると該当する OData クエリをコピーして共有でき、［編集］をクリックするとクエリを編集できます。
マシン、接続、セッション、またはアプリケーションインスタンスに基づいて、カスタムレポートクエリを作成できます。フィールド（たとえばマシン、デリバリーグループ、または期間）に基づいてフィルター条件を指定します。カスタムレポートに必要な追加の列を指定します。プレビューには、レポートデータのサンプルが表示されます。カスタムレポートクエリを保存すると、保存済みクエリのリストに追加されます。

コピーした OData クエリに基づいて、カスタムレポートクエリを作成できます。それには、OData Query オプションを選択し、コピーした OData クエリを貼り付けます。結果として得られたクエリを、後で実行するために保存できます。

> 注：
> OData クエリを使用して生成したレポートのプレビューとエクスポートでは、列名はローカライズされず、英語で表示されます。

また、重要なイベントやアクションの発生は、フラグアイコンで示されます。フラグをクリックすると、発生したイベントまたはアクションが表示されます。

> 注：
>
> - バージョン 7 より前の VDA に対しては、HDX 接続のログオンデータは収集されません。以前のバージョンの VDA については、グラフのデータが 0 として表示されます。
> - Citrix Studio で削除されたデリバリーグループは、関連データがクリーンアップされるまで Director の［傾向］フィルターで選択できます。削除されたデリバリーグループを選択すると、保存まで使用可能なデータのグラフが表示されます。ただし、テーブルにはデータは表示されません。
> - デリバリーグループ間でアクティブなセッションがあるマシンを移動すると、移動後のデリバリーグループの ［リソース使用率］および［負荷評価基準インデックス］テーブルで両方のデリバリーグループの統

> 合された測定値が表示されます。

Autoscale 管理対象マシンの監視

August 17, 2024

Autoscale は、デリバリーグループに登録されているすべてのマルチセッションおよびシングルセッションOS マシンの電源をプロアクティブに管理できる電源管理機能です。Autoscale は、Web Studio で選択したデリバリーグループで構成できます。詳しくは、「Autoscale」を参照してください。
Director を使用して Autoscale 対応マシンの主要メトリックを監視できます。

マシンの使用量

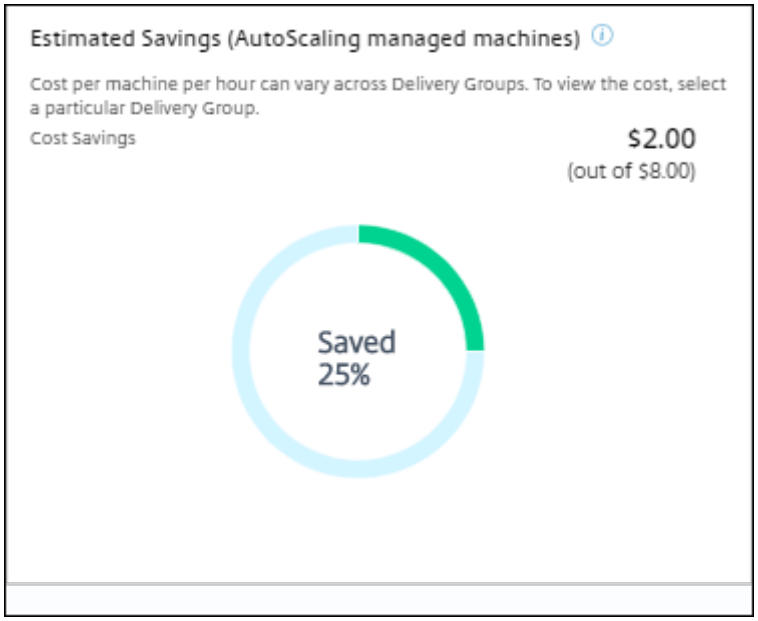
［マシンの使用量］ページでは、選択したデリバリーグループおよび期間に電源がオンになっている、Autoscale 対応マルチセッションおよびシングルセッション OS マシンの総数を表示します。このメトリックは、デリバリーグループ内のマシンの実際の使用量を示します。
［シングルセッション **OS** マシン］または ［マルチセッション **OS** マシン］タブで、デリバリーグループと期間を選択します。

このチャートは、以下のメトリックを表示しています:

- 有効になっているマシン - 電源がオンになっている Autoscale 対応マシンの数
- 登録されたマシン - 登録されたマルチセッションまたはシングルセッション OS マシンの数
- メンテナンス中のマシン - メンテナンスモードがオンになっているマルチセッションまたはシングルセッションOS マシンの数

見積もり削減額

［マシン使用量］ページでは、選択したデリバリーグループで Autoscale を有効にすることによって達成された推定コスト削減額についても表示します。



見積もり削減額は、［デリバリーグループの編集］>［**Autoscale**］で構成された 1 時間あたりのマシンごとの削減額（米ドル）をパーセンテージで算出します。マシンごとの削減額の構成について詳しくは、「Autoscale」を参照してください。

すべてのデリバリーグループを選択すると、すべてのデリバリーグループに関する見積もり削減額の平均値が表示されます。

見積もり削減額は、管理者が既存のインフラストラクチャを統合し、削減額と使用率を最大化するための処理能力を計画する時に役立ちます。

マシンとセッションのアラート通知

Director ダッシュボードには、ドリルダウン可能なアラート通知が表示されます。アラートの詳細は ［アラート］ページに表示されます。

- デリバリーグループでアラートポリシーを作成するには、［アラート］>［**Citrix** アラートポリシー］>［デリバリーグループポリシー］に移動します。
- ここでは、以下の警告および限界しきい値を設定できます:
  - 障害が発生したマシン数（シングルセッション OS）および障害が発生したマシン数（マルチセッション OS）、
  - デリバリーグループでの最大接続セッション数、最大切断セッション数、合計最大同時セッション数。
- デリバリーグループ内の対応するメトリックがしきい値に達すると、アラートが生成されます。

アラートポリシーの条件と新しいアラートポリシーの作成について詳しくは、「アラートおよび通知」を参照してください。

マシンの状態

- ［フィルター］>［マシン］では、すべてのマシンの電源状態を表形式で表示します。特定のデリバリーグループで絞り込むことができます。
- ［フィルター］>［セッション］はマシン名ごとにフィルターを表示し、関連付けられたセッションおよびリアルタイムの状態を確認できます。
- ［傾向］>［セッション］でデリバリーグループと期間を選択して、セッションの傾向と関連するメトリックを表示します。

詳しくは、「トラブルシューティングのためのデータのフィルター処理」を参照してください。

負荷評価傾向

［傾向］>［負荷評価基準インデックス］ページで、マルチセッション OS マシン間で分散された負荷に関する詳細な情報をグラフに表示します。このグラフでは、対象のデリバリーグループ、デリバリーグループのマルチセッション OS マシン、マルチセッション OS マシン、および期間を指定できます（マルチセッション OS マシンは、デリバリーグループのマルチセッション OS マシンが選択されている場合のみ指定可能）。負荷評価基準インデックスは、合計 CPU、メモリ、ディスク、またはセッションのパーセンテージとして表示され、最後の間隔での接続ユーザー数と比較されます。

展開のトラブルシューティング

August 17, 2024

ヘルプデスク管理者は、問題を報告したユーザーを検索して、そのユーザーに関連付けられているセッションまたはアプリケーションの詳細を確認できます。同様に、問題が報告されたマシンやエンドポイントを検索します。関連するメトリックを監視し、適切な対処法を実行することで、問題を迅速に解決します。

使用可能な操作は次のとおりです：

- 応答しないアプリケーションまたはプロセスの終了
- ユーザーのマシンでの操作のシャドウ
- 応答しないセッションのログオフ
- マシンの再起動
- マシンをメンテナンスモードにすること
- ユーザープロファイルのリセット

アプリケーションのトラブルシューティング

August 17, 2024

アプリケーション分析

［アプリケーション］ビューには、アプリケーションのパフォーマンスを効率的に分析および管理するのに役立つ、単一の統合ビューにアプリケーションベースの分析が表示されます。サイトに公開されているすべてのアプリケーションの正常性および使用状況に関する情報について貴重な分析情報を得ることができます。デフォルトのビューは、よく実行されているアプリケーションを識別するのに役立ちます。
この機能を使用するには、Delivery Controllers バージョン 7.16 以降、および VDA バージョン 7.15 以降が必要です。

［プローブの結果］列には、過去 24 時間に実行されたアプリケーションプロービングの結果が表示されます。［傾向］>［アプリケーション プローブの結果］ページで詳細を表示するには、プローブの結果のリンクをクリックします。アプリケーションプローブを構成する方法について詳しくは、「アプリケーションおよびデスクトッププロービング」を参照してください。

［インスタンス］列には、アプリケーションの使用状況が表示されます。現在実行中のアプリケーションインスタンス（接続インスタンスと切断インスタンスの両方）の数を示します。詳細なトラブルシューティングを行うには、［インスタンス］フィールドをクリックして、対応する ［アプリケーションインスタンス］フィルターページを表示します。ここでは、ログオフまたは切断するアプリケーションインスタンスを選択できます。

> 注:
>
> カスタムスコープ管理者の場合、Director はアプリケーショングループに作成されたアプリケーションインスタンスを表示しません。すべてのアプリケーションインスタンスを表示するには、すべての管理権限を実行できる管理者である必要があります。詳しくは、Knowledge Center のCTX256001を参照してください。

［アプリケーション障害］列と ［アプリケーションエラー］列を使用して、サイト内の公開アプリケーションの正常性をモニターします。これらの列には、過去 1 時間以内に対応するアプリケーションを起動している間に発生した障害とエラーの合計数が表示されます。［アプリケーション障害］または ［アプリケーションエラー］フィールドをクリックすると、選択したアプリケーションに対応する ［傾向］ > ［アプリケーション障害］ページに障害の詳細が表示されます。

アプリケーション障害ポリシーの設定では、障害やエラーの可用性と表示を管理します。ポリシーとその変更方法について詳しくは、「監視のポリシー」設定の「アプリケーション障害の監視ポリシー」を参照してください。

リアルタイムアプリケーション監視

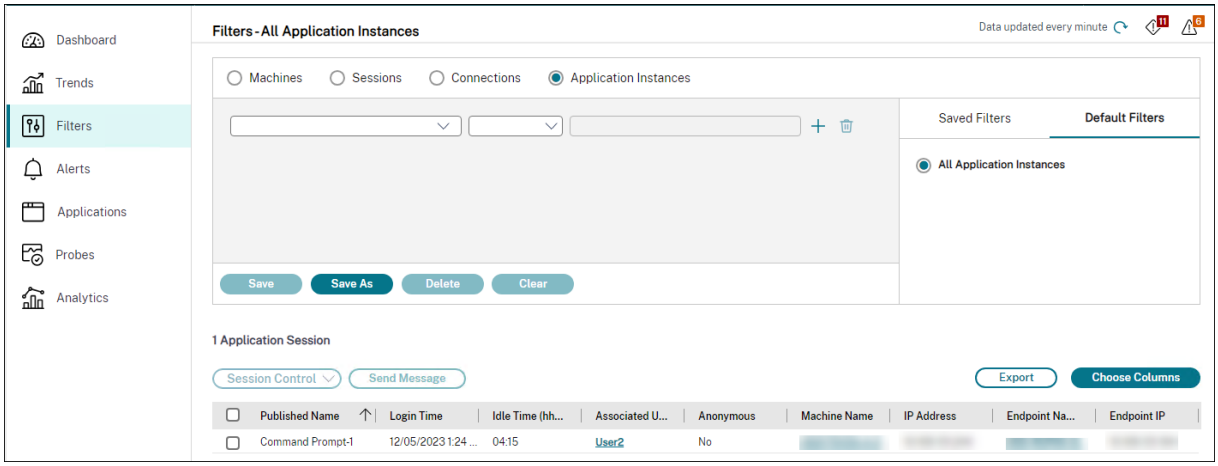
アイドル状態の時間の指標を使用して、特定の時間制限を超えてアイドル状態であるインスタンスを識別することで、アプリケーションとセッションをトラブルシューティングできます。

アプリケーションベースのトラブルシューティングの一般的な用途は、ヘルスケアのセクターです。このセクターでは、従業員間でアプリケーションライセンスが共有されています。このため、Citrix Virtual Apps and Desktops の環境の削除、パフォーマンスの低いサーバーの再構成、アプリケーションの保守およびアップグレードを行うには、アイドル状態のセッションとアプリケーションインスタンスを終了する必要があります。

［アプリケーションインスタンス］フィルターページには、サーバー上とシングルセッション OS 上にある VDA のすべてのアプリケーションインスタンスが表示されます。関連付けられたアイドル時間の測定値は、10 分間以上アイドル状態になっているマルチセッション OS 対応 VDA のアプリケーションインスタンスについて表示されます。

> 注:
> アプリケーションインスタンスの測定値は、すべてのライセンスエディションのサイトで確認できます。

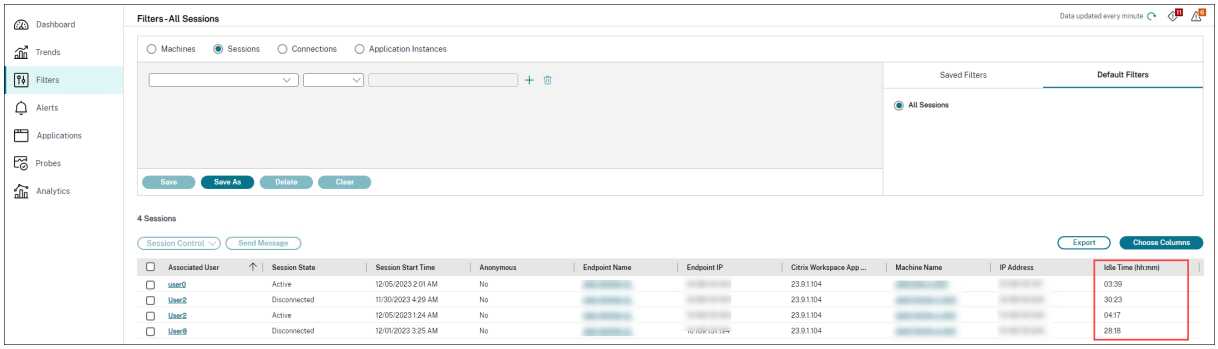
一定時間以上アイドル状態になっているアプリケーションインスタンスを識別して、必要に応じてログオフするか接続を切断するためにこの情報を使用します。これを行うには、［フィルター］**>**［アプリケーション インスタンス］の順に選択し、保存済みのフィルターを選択するか ［すべてのアプリケーションインスタンス］を選択し、独自のフィルターを作成します。



フィルターの例は次のようになります。［フィルター基準］条件として ［公開名］（アプリケーションの公開名）と［アイドル時間］を選択します。次に ［アイドル時間］に ［次のもの以上］を設定して特定の時間制限を指定、再利用のためのフィルターを保存します。フィルター後の一覧から、アプリケーションインスタンスを選択します。メッセージを送信するオプションを選択するか、［セッション制御］ドロップダウンリストから ［ログオフ］または ［切断］を選択してインスタンスを終了します。

> 注:
> ログオフするか 1 つのアプリケーションインスタンスを切断すると、現在のセッションがログオフされるか切断されるため、同じセッションに属するすべてのアプリケーションインスタンスが終了します。

［セッション］フィルターページでセッション状態とセッションのアイドル時間の指標を使用してアイドル状態のセッションを識別できます。［アイドル時間］列で並べ替えるか、特定の時間制限を超えてアイドル状態であるセッションを識別するフィルターを定義します。アイドル時間は、10 分間以上アイドル状態であるマルチセッション OS 対応 VDA 上のセッションに対して表示されます。



セッションまたはアプリケーションインスタンスが次のいずれかの場合、［アイドル時間］には ［なし］と表示されます。

- アイドル状態の時間が 10 分未満の場合
- シングルセッション OS の VDA 上で起動されている場合
- バージョン 7.12 以前を実行する VDA 上で起動されている場合

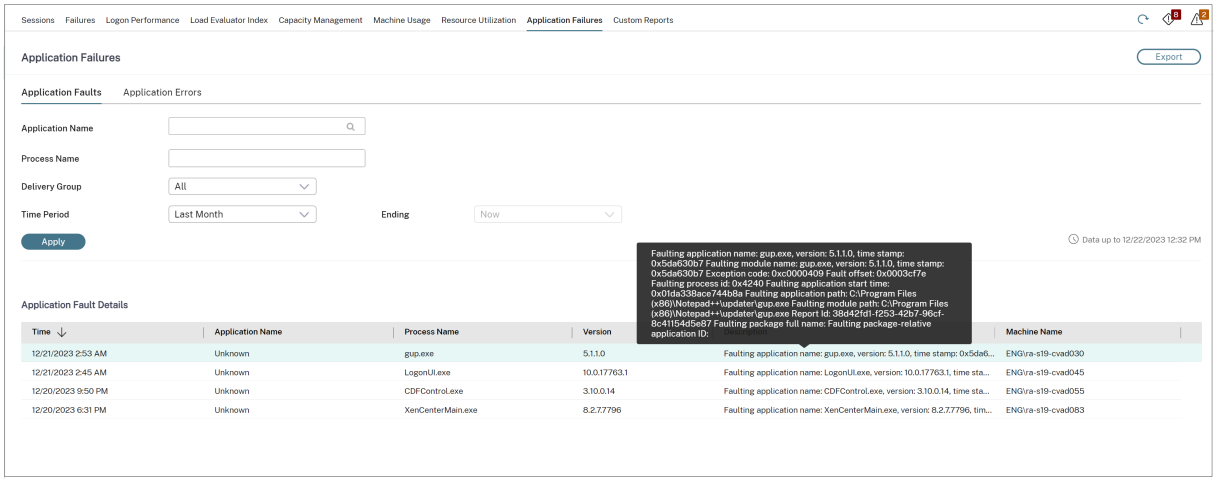
アプリケーション障害履歴の監視

［傾向］>［アプリケーション障害］タブに、VDA 上の公開アプリケーションに関連する障害が表示されます。

アプリケーション障害の傾向は、Premium および Advanced Edition では、過去 2 時間、24 時間、7 日間、および 1 か月間で提供されます。他のライセンスの種類では、過去 2 時間、24 時間、および 7 日間で使用できます。ソースに「アプリケーションエラー」がある場合は、イベントビューアーに記録されているアプリケーション障害が監視されます。［エクスポート］をクリックすると、CSV、Excel、または PDF フォーマットのレポートが生成されます。

アプリケーション障害監視のクリーンアップ保持設定は、Premium Edition も Premium Edition 以外も、GroomApplicationErrorsRetentionDays および GroomApplicationFaultsRetentionDays がデフォルトで 1 日に設定されています。この設定は、PowerShell コマンドを使用して変更できます:

```
PowerShell command Set-MonitorConfiguration -\<setting name\> \<value
\>
```

障害はその重要度によって［アプリケーション障害］または［アプリケーションエラー］として表示されます。［アプリケーション障害］タブには、機能またはデータの損失に関連した障害が表示されます。［アプリケーションエラー］には、即座に関連しない問題が示されます。これは、将来問題が発生する可能性がある状況を意味しています。

障害は、公開アプリケーション名、プロセス名またはデリバリーグループ、および期間によってフィルターできます。表には、障害またはエラーコードと簡単な説明が表示されます。詳細な障害の説明はツールチップとして表示されます。

> 注:
> 対応するアプリケーション名を派生できない場合、公開アプリケーション名は「不明」として表示されます。これは、通常、アプリケーションの起動がデスクトップセッションで失敗した場合、または依存している実行ファイルが原因で処理できない例外により失敗した場合に発生します。

デフォルトでは、マルチセッション OS VDA でホストされたアプリケーションの障害のみが監視されています。監視グループポリシーでは次のような監視設定が変更できます：アプリケーション障害の監視の有効化、シングルセッション OS VDA 上のアプリケーション障害の監視の有効化、および障害の監視から除外されるアプリケーションの一覧の設定。詳しくは、「監視のポリシー設定」の「アプリケーション障害の監視ポリシー」を参照してください。

［傾向］ > ［アプリケーションプローブの結果］ページには、そのサイトで過去 24 時間および過去 7 日間に実行されたアプリケーションプロービングの結果が表示されます。アプリケーションプローブを構成する方法について詳しくは、「アプリケーションプロービング」を参照してください。

マシンのトラブルシューティング

August 17, 2024

> 注:
>
> **Citrix Health Assistant** は、未登録の VDA の構成に関する問題をトラブルシューティングするためのツ

> ールです。このツールは、いくつかのヘルスチェックを自動化して、セッションの起動やタイムゾーンリダイレクトの構成における VDA 登録の失敗と問題の根本原因を特定します。Knowledge Center の記事「Citrix Health Assistant - VDA の登録とセッションの起動のトラブルシューティング」には、**Citrix Health Assistant** ツールのダウンロード方法と使用方法が記載されています。

Director コンソールの ［フィルター］ **>** ［マシン］ビューには、そのサイトに構成されているマシンが表示されます。また、［マルチセッション OS マシン］タブには負荷評価基準インデックスが表示され、その測定値上にマウスポインターを置くと各パフォーマンスカウンターの測定値やセッション数がツールチップとして表示されます。

登録に失敗したマシンの ［失敗の理由］列をクリックすると、失敗の詳細な説明とその失敗をトラブルシューティングするための推奨手順が表示されます。マシンおよび接続でエラーが発生した場合のエラーの理由と推奨される解決手順は、「Citrix Director の失敗の原因とトラブルシューティング」に記載されています。

マシン名のリンクをクリックし、［マシンの詳細］ページに移動します。

［マシンの詳細］ページには、マシンの詳細、インフラストラクチャの詳細、およびマシンに適用済みの HotFix の詳細の一覧が表示されます。

マシンごとのリアルタイムのリソース使用率

［マシン稼働］パネルには、CPU とメモリのリアルタイムの使用状況を示すグラフが表示されます。Delivery Controller および VDA のバージョン **7.14** 以降がインストールされているサイトでは、ディスクと GPU の監視グラフも表示されます。

重要なパフォーマンス測定値としてディスク監視グラフ、平均 IOPS、ディスク遅延があり、VDA ディスク関連の問題をモニターし解決する上で役立ちます。［平均 IOPS］グラフには、ディスクの読み取りおよび書き込みの平均回数が表示されます。［ディスク遅延］を選択すると、データが要求されてディスクから返されるまでの時間をミリ秒単位で示すグラフが表示されます。

GPU 使用率

［**GPU** 使用率］を選択すると GPU、GPU メモリ、およびエンコーダーとデコーダーの使用率がパーセント値として表示され、マルチセッションおよびシングルセッション OS の VDA での GPU に関連した問題を解決できます。

サポートされる **GPU** バージョン:

- ディスプレイ ドライバー バージョン 369.17 以降を実行する NVIDIA Tesla M60 GPU。詳しくは、NVIDIA vGPU Softwareを参照してください。
- AMD Radeon Instinct MI25 GPU および AMD EPYC 7V12（Rome）CPU。詳しくは、AMD ドライバーとサポートを参照してください。

ドライバー:

適切なドライバーまたは拡張機能が VDA にインストールされている必要があります。

- NVIDIA GPU の場合、GRID ドライバーを手動で、または拡張機能によってインストールします。詳しくは、NVIDIA vGPU Softwareを参照してください。
  - NVIDIA の場合、GRID ドライバーのみがサポートされています。CUDA ドライバーは NVadsA10 v5 シリーズでは動作せず、サポートされていません。
  - Azure ベースのマシンに拡張機能によって NVIDIA Grid GPU ドライバーをインストールするプロセスのサンプルについては、「NVIDIA GRID ドライバー」を参照してください。NVIDIA GPU ドライバー拡張機能 - Azure Windows 仮想マシン - Azure 仮想マシン。
  - NVIDIA Grid GPU ドライバーを手動でインストールするプロセスのサンプルについては、「Windows を実行している N シリーズ VM に NVIDIA GPU ドライバーをインストールする」を参照してください。
- AMD GPU の場合、AMD グラフィックドライバーを手動で、または拡張機能によってインストールします。詳しくは、AMD ドライバーとサポートを参照してください。
  - Azure ベースのマシンに拡張機能によって AMD GPU ドライバーをインストールするプロセスのサンプルについては、「Windows 用の AMD GPU ドライバー拡張機能」を参照してください。
  - Azure マシンに AMD GPU ドライバーを手動でインストールするプロセスのサンプルについては、「Windows を実行している N シリーズ VM に AMD GPU ドライバーをインストールする」を参照してください。

使用上の注意:

- GPU 使用率グラフは、64 ビット Windows を実行している VDA でのみ使用できます。
- VDA で GPU アクセラレーションを使用するには、HDX 3D Pro を有効にする必要があります。詳しくは、「Windows シングルセッション OS のための GPU アクセラレーション」および「Windows マルチセッション OS のための GPU アクセラレーション」を参照してください。
- VDA が 1 つ以上の GPU にアクセスしている場合、［GPU 使用率］グラフには個々の GPU から収集された GPU 測定値の平均が表示されます。GPU 測定値は、個々のプロセスではなく VDA 全体について収集されます。
- AMD の場合、エンコーダーとデコーダーの使用は個別にはサポートされていません。GPU を使用するエンコーディング/デコーディングのワークロードは、GPU 使用率で一般的な 3D 負荷として報告されます。
- インストール中に NVIDIA WMI をインストールするようにしてください。このウィンドウは、手動インストール中にのみ使用できます。
- ドライバーがインストールされているが、Director が GPU を検出しない場合

  - タスクマネージャーを確認してください。ドライバーが正しくインストールされていれば、GPU がタスク マネージャーに表示されます。
  - マシンが登録されていることを確認してください。マシンがオンラインとして検出されるまでに時間がかかる場合があります。

- Director で GPU の使用率にアクティビティが表示されない場合は、実行中のワークロードが GPU を使用していることを確認してください。グラフィックワークロードは、［Settings］>［System］>［Display］>［Graphics Settings］で基本設定を設定するアプリを選択して、有効にできます。必ず高パフォーマンスを有効にしてください。場合によっては、他の設定に基づいて Windows がシステムのデフォルトまたは省電力に設定されている場合、デフォルト設定でグラフィックワークロードに CPU を使用することがあります。
- データは毎分更新され、**GPU** 使用率を選択してから 1 分以内にデータの視覚化が開始されます。

マシンごとの過去のリソース使用率

［マシン稼働］パネルの ［履歴使用率の表示］をクリックすると、選択したマシンでのリソースの使用履歴を確認できます。
使用率グラフには、CPU、メモリ、最大同時セッション数、平均 IOPS、ディスク遅延などの重要なパフォーマンス測定が表示されます。

> 注:
>
> データを収集して［マシン使用率の履歴］ページの［上位 10 位のプロセス］表に表示するには、監視ポリシーの ［プロセスの監視を有効にします］設定を［許可］に設定する必要があります。この設定はデフォルトでは［禁止］に設定されています。

デフォルトでは、CPU とメモリの使用率、平均 IOPS、ディスク遅延に関するデータが収集されます。この収集は、［リソースの監視を有効にします］ポリシー設定で無効にできます。

1. ［マシンの詳細］ビューの ［マシン稼働］パネルから、［履歴使用率の表示］を選択します。

2. ［マシン使用率の履歴］ページで、［期間］で、使用率を表示する期間を過去 2 時間、過去 24 時間、過去 7 日間、過去 30 日間、または過去 1 年から選択します。

   > 注:
   >
   > 現在、平均 IOPS とディスク遅延のデータについては、過去 24 時間、過去 30 日間、過去 1 年についてのみ表示できます。カスタムの終了時刻は使用できません。

3. ［適用］をクリックして、目的のグラフを選択します。
4. グラフの他のセクションにマウスを合わせると、選択した期間の詳細が表示されます。

たとえば、［過去 **2** 時間］を選択すると、基準の期間は選択した時間範囲の 2 時間前になります。過去 2 時間と基準期間の CPU、メモリ、およびセッションの傾向を表示します。［過去 **1** か月］を選択すると、基準期間は過去 1 か月間になります。これを選択すると、先月から基準日時までの平均 IOPS およびディスク遅延が表示されます。

1. 選択した期間のリソース使用率データをエクスポートするには、［エクスポート］をクリックします。詳しくは、「展開環境の監視」の「レポートのエクスポート」セクションを参照してください。
2. グラフの下には、CPU とメモリの使用率が上位 10 位のプロセスを示すテーブルが表示されます。選択した時間範囲のアプリケーション名、ユーザー名、セッション ID、平均 CPU、ピーク時の CPU、平均メモリ、ピーク時のメモリが表示される列から任意の列を選択してソートできます。［平均 IOPS］列と［ディスク遅延］列は並び替えできません。

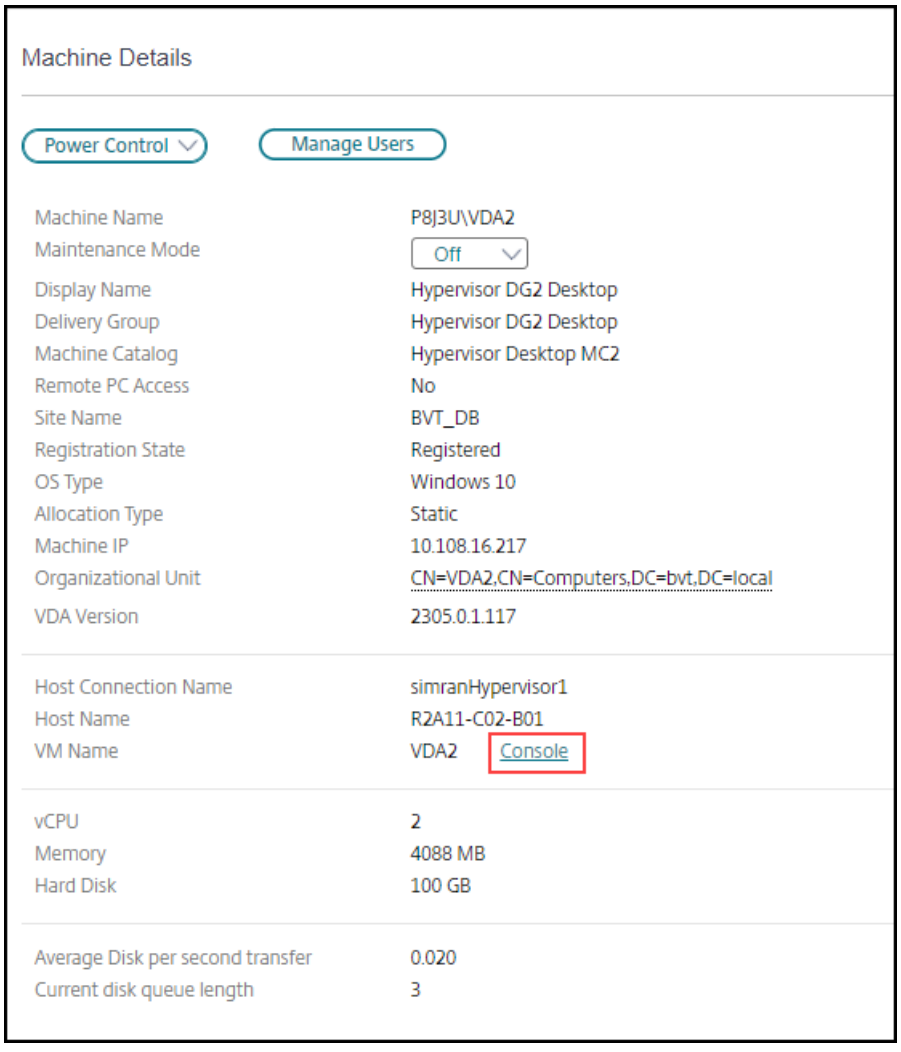
   > 注:
   >
   > システムプロセスのセッション ID は「0000」と表示されます。

3. 特定プロセスのリソース消費に関する履歴傾向を表示するには、上位 10 位のプロセスから任意のプロセスを選択してドリルダウンします。

マシンコンソールへのアクセス

XenServer Version 7.3 以降でホストされているシングルセッションOS マシンおよびマルチセッション OS マシンのコンソールに、Director から直接アクセスできます。このため、XenServer がホストする VDA での問題を解決するために XenCenter を使用する必要はありません。この機能を利用できるようにするには:

- バージョン 7.16 以降の Delivery Controller が必要です。
- マシンをホストする XenServer は、バージョン 7.3 以降である必要があり、Director UI からアクセスできる必要があります。



マシンのトラブルシューティングを行うには、対応する［マシンの詳細］パネルで ［コンソール］リンクをクリックします。提供したホスト資格情報が認証されると、Web ベースの VNC クライアントである noVNC を使用して、別のタブでマシンコンソールが開きます。これで、キーボードとマウスでコンソールにアクセスできるようになりました。

> 注:
>
> - この機能は、Internet Explorer 11 ではサポートされていません。
> - マシンコンソール上のマウスポインターの位置がずれている場合は、CTX230727で、問題を解決する手順を参照してください。
> - Director は、新しいタブでコンソールアクセスを起動し、Web ブラウザー設定でポップアップが許可されていることを確認します。
> - セキュリティ上の理由から、Web ブラウザーに SSL 証明書をインストールすることを Citrix ではお勧めします。

最近電源操作を行ったマシンを検査する

成功した電源操作と失敗した電源操作のステータスを使用してマシンを検査できるようになりました。この機能は、次の分析に役立ちます:

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

> 注:
>
> データは電源管理されたマシンでのみ使用できます。この機能がサポートされる前に実行された電源操作のデータは利用できません。

次の方法を使用して、マシンの電源操作状態を表示できます:

［フィルター］ -> ［マシン］タブ。この場合、デフォルトでは、電源動作時間列と電源操作の結果列が表示されます。表示する列を選択することもできます。

［コストの最適化］タブ。この場合、デフォルトのフィルターは、［電源操作のトリガー］が ［*Autoscale*］に設定され、［電源操作の結果］が ［失敗］に設定されます。

この機能を使用すると、電源操作のコントロールの詳細を表示できます。たとえば、誰が操作をトリガーしたか、どの操作が電源状態を変更したか、失敗の理由、操作が完了した時刻を表示できます。これらの詳細をエクスポートすることもできます。

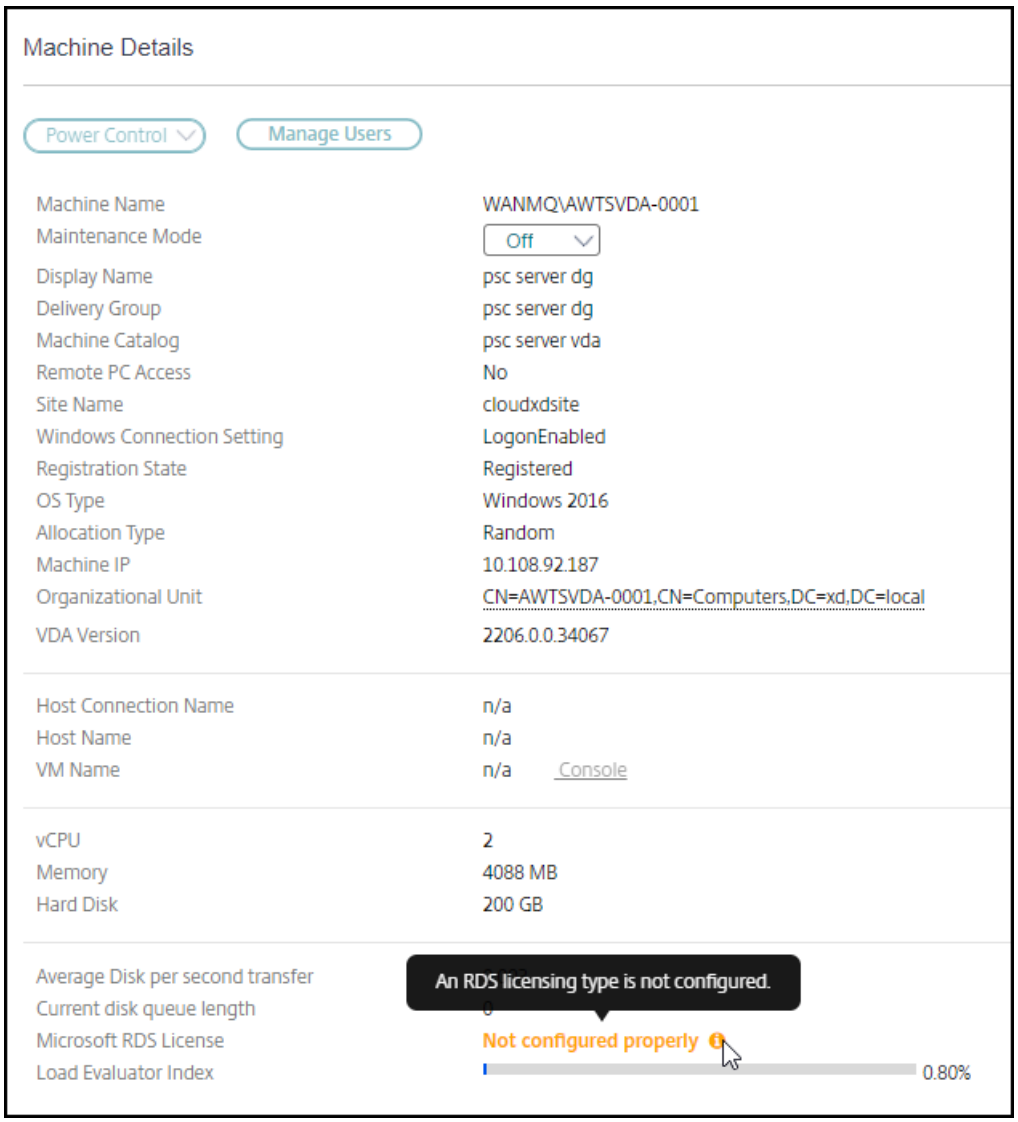
電源操作状態を表示するために、次のフィルターが追加されています:

フィルター	説明
電源操作の結果	電源操作の結果を表示します。使用可能なフィルター値は成功と失敗です。
電源操作のトリガー	誰が、または何が電源操作をトリガーしたかを表示します。使用可能なフィルター値は次のとおりです

フィルター	説明
	• Autoscale - この値は、以下によって電源操作がトリガーされたときに表示されます • 管理者が仮想マシンをシャットダウンして、仮想マシンの OS ディスクを初期状態に戻すとき • 設定されたポリシーに基づいて仮想マシンがシャットダウンまたは一時停止されたとき • プールサイズまたはバッファサイズの構成に基づいて仮想マシンが使用可能になったとき • 管理者 - この値は、電源操作が管理者によってトリガーされたときに表示されます。考えられる例としては、管理者が VM の電源オフ、電源オン、一時停止、再開、または再起動を要求した場合です。 • ユーザー - この値は、ユーザーによって電源操作がトリガーされたときに表示されます。例としては、ユーザーが仮想マシンをリセット、オンにしたとき、または仮想マシン上での作業を再開する場合があります。 • そのほか - この値は、電源操作がスケジュールされた、または不明な理由によってトリガーされた場合に表示されます。
最後の電源操作	電源オン、電源オフ、シャットダウン、再起動、リセット、再開など、マシンで発生した電源操作を正確に表示します
電源動作時間	電源操作が完了した時刻。可能なフィルター値は、過去 1 分間、過去 5 分間、過去 30 分間、過去 1 時間、今日、過去 24 時間、および昨日です。
電源操作の失敗の理由	失敗した理由が表示されます。可能なフィルター値は、ハイパーバイザーがエラーを報告した、ハイパーバイザーのレート制限を超えました、不明なエラー、およびなし、です。成功した操作がある場合は、「なし」と表示されます。

Microsoft RDS ライセンスの正常性

マルチセッション OS マシンの ［マシンの詳細］ページと ［ユーザーの詳細］ページの ［マシンの詳細］パネルに、Microsoft RDS（Remote Desktop Services）のライセンスの状態を表示できます。



次のいずれかのメッセージが表示されます：

- ライセンスを使用できます
- 正しく構成されていません（警告）
- ライセンスエラー（エラー）
- 非互換 VDA バージョン（エラー）

> 注：
>
> 有効なライセンスのある猶予期間中のマシンの Microsoft RDS ライセンス正常性の状態には、［ライセンスを使用できます］のメッセージが緑色で表示されます。有効期限が切れる前にライセンスを更新してください。

警告メッセージとエラーメッセージの場合、情報アイコンの上にカーソルを置くと、次の表に示す詳細情報が表示されます。

メッセージの種類	Director でのメッセージ
エラー	VDA バージョン 7.16 以降で使用可能
エラー	新しい RDS 接続は許可されていません。
エラー	Microsoft RDS ライセンスの猶予期間が終わりました。
エラー	ライセンスサーバーが、クライアントアクセスライセンス（接続デバイス数）の種類で必要な OS レベル用に構成されていません。
エラー	構成されたライセンスサーバーは、クライアントアクセスライセンス（接続デバイス数）の RDS ホスト OS レベルと互換性がありません。
警告	パーソナルターミナルサーバーは Citrix Virtual Apps and Desktops 展開で有効な RDS ライセンスの種類ではありません。
警告	管理用リモートデスクトップは Citrix Virtual Apps and Desktops 展開で有効な RDS ライセンスの種類ではありません。
警告	RDS ライセンスの種類は構成されていません。
警告	RDS クライアントアクセスライセンス（接続ユーザー数）の種類では、ドメインコントローラーまたはライセンスサーバーに接続できません。
警告	ライセンスの種類がクライアントアクセス（接続デバイス数）の場合、必要な OS レベルのライセンスサーバーに接続できないため、クライアントデバイスライセンスを確認できません。

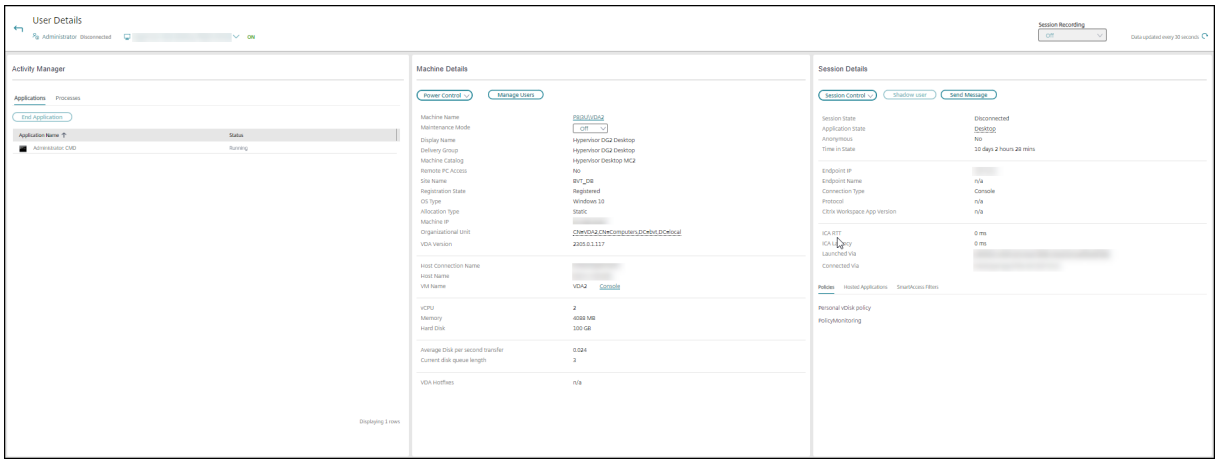
> 注:
>
> この機能は、Microsoft RDS CAL（クライアントアクセスライセンス）にのみ適用されます。

ユーザーの問題のトラブルシューティング

August 17, 2024

Director の［アクティビティマネージャー］ページにある［ヘルプデスク］ビューを使って、ユーザーまたはセッションに関する情報を確認します:

ユーザーのアクティビティマネージャーから［詳細を表示］をクリックすると、［ユーザーの詳細］ページが開きます。エンドポイントのアクティビティマネージャーから ［詳細を表示］をクリックすると、［エンドポイントの詳細］ページが開きます。



セッションセレクタ

ユーザーが複数のセッションを開始した場合、セッションセレクタはセッションの選択に役立ちます。

詳細を表示したいセッションを選択します。

- セッション、ユーザーのサインインエクスペリエンス、セッションの開始、接続、およびアプリケーションに関する詳細を確認できます。
- ユーザーのマシンをシャドウすることができます。
- ICA セッションを記録する。

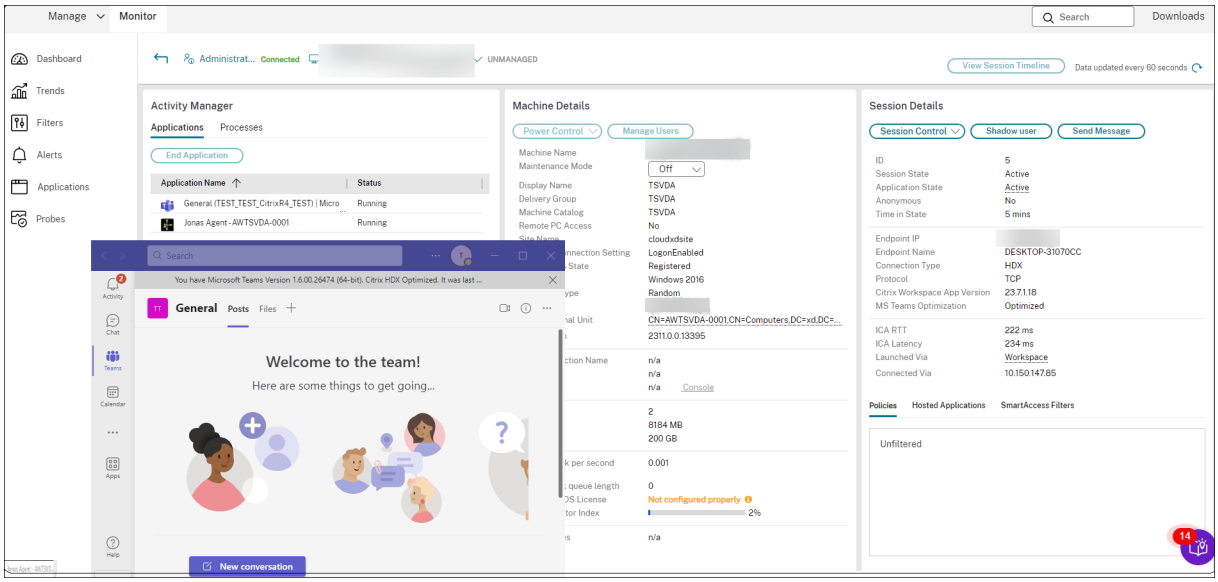
Microsoft Teams の最適化の状態

Director は、［ユーザーの詳細］ページ >［セッションの詳細］>［**MS Teams** の最適化］フィールドで、HDX セッションの Microsoft Teams の最適化の状態を表示します。Microsoft Teams の最適化は、クリアな音声やビデオなどのユーザーエクスペリエンスを向上させるために重要です。Microsoft Teams の最適化の状態を可視化することは、チケットの解決に必要な時間を短縮するのに役立ち、管理者がトラブルシューティング中に重要なメトリックを特定するのに役立ちます。

> 注:
>
> Citrix Director は、Microsoft Teams バージョン 2.1 以前をサポートします。

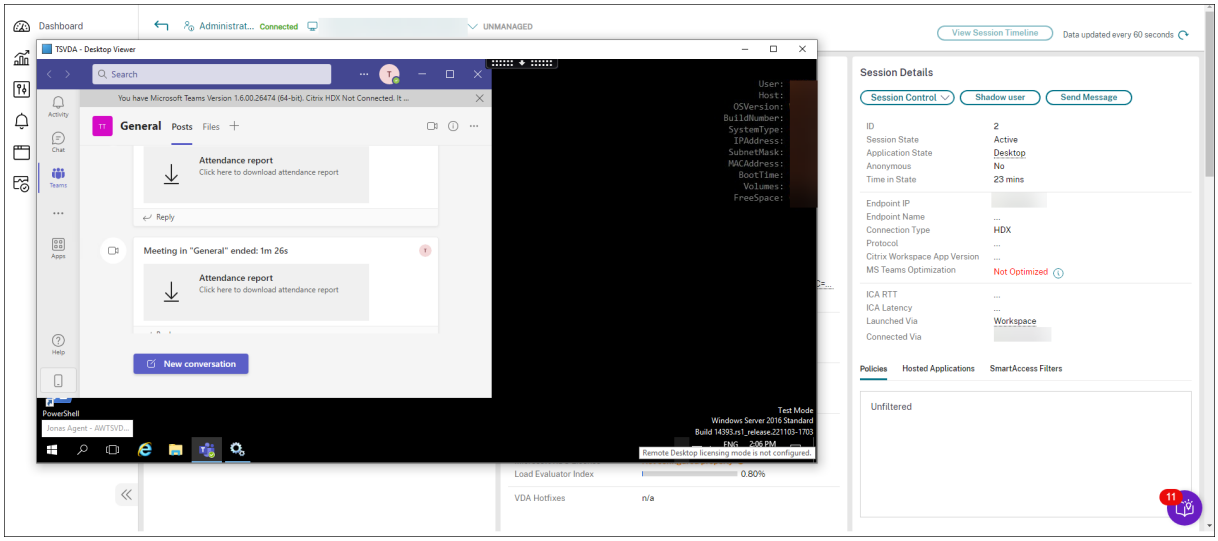
前提条件:

- VDA はバージョン 2311 以降を実行しています。
- サポートされている Citrix Workspace アプリのバージョンは、「Microsoft Teams の最適化」に記載されています。
- Microsoft Teams は、公開アプリとして、または公開デスクトップ内で実行されます。
- Citrix HDX HTML5 ビデオリダイレクトサービスなどの重要なサービスが実行されています。



Microsoft Teams が最適化されていない場合、ヒントには、Microsoft Teams を最適化するためのヒントを含む HDX の外部トラブルシューティングライブ記事へのリンクが表示されます。「HDX 最適化のトラブルシューティン

グ」。



トラブルシューティングのヒント

次の表に示す方法で問題のトラブルシューティングを行い、必要な場合は問題を担当の管理者に報告する。

ユーザーの問題	提案
ログオンに時間がかかる。断続的もしくは繰り返し失敗する	ユーザーログオンの問題の診断
セッションの開始に時間がかかる。断続的もしくは繰り返し失敗する	セッション起動の問題の診断
セッションの応答が遅い、または応答しない	セッションのパフォーマンスの問題を診断する
アプリケーションが遅いか、応答しない	アプリケーション障害の解決
接続に失敗した	デスクトップ接続の復元
セッションが遅いまたは応答しない	セッションの復元
セッションの録画	セッションの録画
ビデオが遅いまたは画質が悪い	HDX チャネルシステムレポートの実行

> 注:
> [ユーザーの詳細] ビューの [マシンの詳細] パネルで、マシンがメンテナンスモードになっていないことを確認してください。

セッションログオン

［ユーザーの詳細］ビュー >［セッションログオン］タブには、セッションログオンプロセスの包括的なビューが表示されます。このタブには、さまざまなログオンフェーズがプロットされたログオン期間フェーズグラフが含まれています。このデータを使用して、ユーザーログオンの問題をトラブルシューティングします。詳しくは、「ユーザーログオンの問題の診断」を参照してください。

セッションパフォーマンス

［セッションパフォーマンス］タブでは、ユーザーセッション内の問題を特定する際にリアルタイムで指標を相関させる機能をはじめ、トラブルシューティングのワークフローが強化されています。［セッションのトポロジ］パネルは、接続された HDX セッションのセッション内パスを視覚的に表現します。［パフォーマンスメトリック］パネルは、ICARTT、ICA 遅延、フレーム数/秒、利用可能な出力帯域幅、消費された出力帯域幅などのセッションメトリックの傾向を提供し、これらの指標が時間の経過とともにどのように実行されたかを把握するのに役立てることができます。詳しくは、「セッションパフォーマンスの問題を診断する」を参照してください。

検索のヒント

Director の［検索］フィールドにユーザー名を入力すると、Director のサポートが構成されたすべてのサイトで Active Directory ユーザーが検索されます。

［検索］フィールドにマルチユーザーマシンの名前を入力すると、Director でそのマシンの［マシンの詳細］ページが開きます。

［検索］フィールドにエンドポイントの名前を入力すると、Director はそのエンドポイントに接続している認証が不要なユーザー（匿名ユーザー）セッションおよび認証が必要なセッションを使用します。この検索により、匿名ユーザーセッションのトラブルシューティングを行うことができます。匿名ユーザーセッションのトラブルシューティングを行うには、エンドポイント名が重複していないことが重要です。

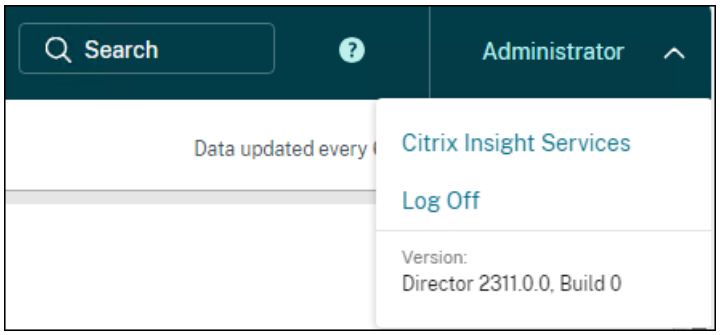
検索結果には、現在マシンを使用していないユーザーや、マシンに割り当てられていないユーザーも含まれます。

- 検索では大文字と小文字は区別されません。
- 検索語の一部を入力すると、一致する候補が一覧で表示されます。
- 2 つの部分で構成された名前の何文字かをスペースで区切って入力すると、両方の文字列と一致する項目が検索されます。2 つの部分で構成された名前の例には、ユーザー名、姓と名、または表示名があります。たとえば、「jo rob」と入力すると、「John Robertson」や「Robert, Jones」などが検索されます。

ホームページに戻るには、**Director** のロゴをクリックします。

Citrix Insight Services にアクセスする

Director の ［ユーザー］ドロップダウンリストからCitrix Insight Services（CIS）にアクセスすることで、診断からさらに情報を得ることができます。CIS で提供されるデータは、Call Home や Citrix Scout などのソースから取得されます。



Citrix テクニカルサポートにトラブルシューティング情報をアップロードする

単一の Delivery Controller または Virtual Delivery Agent から Citrix Scout を実行し、選択したコンピューターのトラブルシューティングに必要なデータ要素や Citrix Diagnostics Facility（CDF）トレースをキャプチャします。Scout は、CIS プラットフォームにデータを安全にアップロードする機能を提供し、Citrix のテクニカルサポートのトラブルシューティングを支援します。Citrix のテクニカルサポートは CIS プラットフォームを使用して、カスタマーから報告された問題解決する時間を短縮します。

Scout は、Citrix Virtual Apps and Desktops のコンポーネントと一緒にインストールされます。Windows のバージョンによっては、Citrix Virtual Apps and Desktops をインストールするかこれにアップグレードすると、Scout が **Windows** のスタートメニューまたはスタート画面に表示されるようになります。

スタートメニューやスタート画面から Scout を起動するには、［**Citrix**］**>**［**Citrix Scout**］を選択します。

Scout の使用と構成、およびよくある質問について詳しくは、CTX130147を参照してください。

セッション起動の問題の診断

August 17, 2024

Director には「ユーザーログオンの問題の診断」セクションに記載されているログオンプロセスのフェーズだけでなく、セッション開始時の実行時間も表示されます。これは ［ユーザーの詳細］ページの［セッション開始時の Workspace アプリの実行時間］と、［マシンの詳細］ページの［セッション開始時の VDA の実行時間］に分かれます。この 2 つの時間にはフェーズの情報も含まれていて、各フェーズの実行時間も確認できます。このデータはセッションの開始時間が長い場合に問題を把握し、トラブルシューティングを行うのに役立ちます。また、セッションの開始プロセスを構成する各フェーズの実行時間の情報は、それぞれのフェーズに関連する問題のトラブルシューティ

ングに有効です。たとえばドライブマッピングの時間が長い場合は、有効なすべてのドライブが GPO に正しくマップされているかを確認するか、スクリプトを確認するという対処ができます。この機能は、Delivery Controller バージョン 7 1906 以降および VDA 1903 以降で使用できます。

前提条件

セッションの開始時間を表示するには、以下の条件を満たしている必要があります:

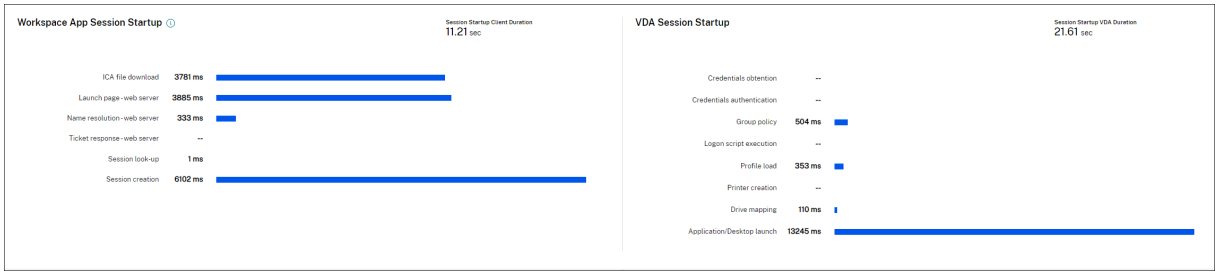
- Delivery Controller のバージョン 7 1906 以降。
- VDA のバージョン 1903 以降。
- EUEM（End User Experience Monitoring：エンドユーザー状況監視）サービスが VDA で実行されている。

制限事項

Director でセッションの開始時間を表示する場合は、以下の制限が適用されます。

- セッションの開始時間は HDX セッションでのみ確認できます。
- iOS および Android OS から開始したセッションについては、セッション開始時の VDA の実行時間のみ確認できます。
- ICA ファイルのダウンロード実行時間（IFDCD）は、Web ブラウザーからの起動時に Workspace アプリが検出された場合にのみ使用できます。
- Mac OS から開始したセッションで IFDCD を使用するには、Workspace アプリのバージョン 1902 以降が必要です。
- Windows OS から開始したセッションで IFDCD を使用するには、Workspace アプリのバージョン 1902 以降が必要です。それ以前のバージョンで IFDCD を表示するには、Workspace アプリが検出された状態で Web ブラウザーからアプリを起動する必要があります。

> 注:
>
> - 条件が整っているにもかかわらずセッションの開始時間を表示するのに問題がある場合は、CTX130320の記事を参考にして Director サーバーのログと VDA のログを確認してください。
>   共有セッション（複数のアプリケーションが同一セッションで起動された状態）では、Workspace アプリの開始メトリックには最新の接続または最新のアプリケーション起動についての情報が表示されます。
> - VDA セッションの開始では、再接続時には適用されないメトリックがあります。その場合はメッセージが表示されます。



Workspace アプリでのセッションの開始フェーズ

セッション開始時のクライアントの実行時間（**SSCD**）

このメトリックの値が高い場合は、開始時間が長くなる要因がクライアント側にあることを示しています。問題の根本的な原因を特定するには、後に続くメトリックを調査します。SSCD は、リクエストの時間（マウスクリック）にできるだけ近い状態で開始されます。クライアントデバイスと VDA との間の ICA 接続が確立されると終了します。共有セッションの場合は、サーバーとの接続を新たに確立するときのセットアップコストがそれほど生じないため、この時間は大幅に短くなります。次のレベルでは、いくつかの詳しいメトリックを利用できます。

ICA ファイルのダウンロード実行時間

これはクライアントがサーバーから ICA ファイルをダウンロードするのにかかった時間を表します。このプロセスの全容は、以下のとおりです：

1. ユーザーが Workspace アプリでリソース（アプリケーションまたはデスクトップ）をクリックします。
2. Citrix Gateway が構成されている場合は、それを介してユーザーの要求が StoreFront に送信されます。要求は StoreFront から Delivery Controller に送信されます。
3. Delivery Controller は要求を処理できるマシンを探し、そのマシンの情報などの詳細を StoreFront に送信します。また、StoreFront は Secure Ticket Authority にワンタイムチケットを要求し、これを受信します。
4. StoreFront は ICA ファイルを生成し、Citrix Gateway（構成されている場合）を介してユーザーに送信します。

IFDCD はこのプロセス（手順 1～4）が完了するまでにかかる時間を表します。クライアントが ICA ファイルを受信すると、IFDCD のカウントが停止します。

LPWD は、このプロセスにおける StoreFront のコンポーネントです。

IFDCD の値が高い（ただし LPWD の値は普通である）場合、サーバー側の開始処理は正常ですが、クライアントデバイスと StoreFront との間の通信に問題があったことを示しています。これは 2 台のマシンをつなぐネットワーク上の問題によるものです。これがわかれば、最初にネットワークの潜在的な問題に対処することができます。

ページ開始時の **Web** サーバーの実行時間（**LPWD**）

これは StoreFront の起動ページ（launch.aspx）の処理にかかる時間を表します。LPWD の値が高い場合、StoreFront にボトルネックがある可能性があります。

考えられる原因は次のとおりです：

- StoreFront の高負荷 Internet Information Services（IIS：インターネットインフォメーションサービス）のログ、監視ツール、タスクマネージャー、パフォーマンスモニターなどを確認して、速度低下の原因を特定します。
- StoreFront で Delivery Controller などの他のコンポーネントとの通信に問題が生じています。StoreFront と Delivery Controller との間のネットワーク接続が遅くなっていないか、または停止や過負荷の状態になっている Delivery Controller がないかを確認してください。

名前解決時の **Web** サーバーの実行時間（**NRWD**）

これは Delivery Controller が公開アプリケーションまたは公開デスクトップの名前を VDA マシンの IP アドレスに解決するのにかかる時間を表します。

このメトリックの値が高い場合、Delivery Controller が公開アプリケーションの名前を IP アドレスに解決するのに時間がかかっていることを示しています。

この原因としては、クライアントの問題、Delivery Controller の問題（過負荷など）、クライアントと Delivery Controller をつなぐネットワークリンクの問題などが考えられます。

チケット応答時の **Web** サーバーの実行時間（**TRWD**）

これはチケットが必要な場合に、Secure Ticket Authority（STA）サーバーまたは Delivery Controller からチケットを取得するのにかかる時間を表します。この時間が長い場合は、STA サーバーまたは Delivery Controller が過負荷になっていることを示しています。

セッション検索時のクライアントの実行時間（**SLCD**）

これは要求された公開アプリケーションをホストするためにすべてのセッションを照会するのにかかる時間を表します。この照会処理は既存のセッションでアプリケーションの起動要求を処理できるかどうかを判断するために、クライアント上で実行されます。新規セッションか共有セッションかによって異なる手法が使用されます。

セッション作成時のクライアントの実行時間（**SCCD**）

これはセッションの作成にかかった時間です。具体的には wfica32.exe ファイルが実行されてから接続が確立されるまでの時間を表しています。

VDA セッションの開始フェーズ

セッション開始時の **VDA** の実行時間（**SSVD**）

この時間は VDA が開始処理の全体を実行するのに要する時間を含めた、サーバー側の接続開始時の高レベルメトリックを表します。このメトリックの値が高い場合は、セッション開始までの時間が長くなる要因が VDA 側にあることを示しています。VDA が開始処理全体の実行にかかった時間は、この値に含まれます。

アカウント情報取得時の **VDA** の実行時間（**COVD**）

VDA がユーザーの資格情報を取得するのにかかった時間を表します。

ユーザーが適時に資格情報を提供できなかった場合、この時間は人為的に長くなることがあります。そのため、VDA 開始時間には含まれません。この時間が意味を持つと考えられるのは、ログイン操作が必要かつサーバー側で資格情報の入力を求めるダイアログボックスが表示される場合（またはログイン前に法律上の注意点が表示される場合）に限られます。

アカウント情報認証時の **VDA** の実行時間（**CAVD**）

これは、VDA が認証プロバイダーに対してユーザーの資格情報を認証するのにかかる時間です。認証プロバイダーは、Kerberos、Active Directory、または Security Support Provider Interface（SSPI）のいずれかになります。

グループポリシーの **VDA** の実行時間（**GPVD**）

これはログオン中にグループポリシーオブジェクトを適用するのにかかる時間を表します。

ログインスクリプト実行時の **VDA** の実行時間（**LSVD**）

これは VDA がユーザーのログインスクリプトを実行するのにかかる時間を表します。

ユーザーまたはグループのログインスクリプトの実行を非同期にすることを検討してください。アプリケーション互換性スクリプトを最適化するか、代わりに環境変数を使用することを検討してください。

プロファイルロード時の **VDA** の実行時間（**PLVD**）

これは VDA がユーザーのプロファイルを読み込むのにかかる時間を表します。

この時間が長い場合は、ユーザープロファイルの設定を見直してください。移動プロファイルのサイズと保存場所によってはセッションの開始が遅くなります。ユーザーがターミナルサービスの移動プロファイルとホームフォルダーが有効になっているセッションにログオンすると、移動プロファイルの内容とホームフォルダーへのアクセスがログ

オン時にマップされます。その分だけリソースが必要になります。場合によっては CPU 使用率が著しく高くなることもあります。この問題による影響を軽減するには、ターミナルサービスのホームフォルダーと、リダイレクトされた個人用フォルダーの使用を検討してください。通常、Citrix 環境でユーザープロファイルを管理する場合は、Citrix Profile Management を使用することを検討してください。Citrix Profile Management を使用していてログオン時間が遅くなる場合は、アンチウイルスプログラムが Citrix Profile Management ツールをブロックしていないかを確認してください。

プリンター作成時の **VDA** の実行時間（**PCVD**）

これは VDA がユーザーのクライアントプリンターを同期的にマップするのにかかる時間を表します。プリンターの作成を非同期で実行するように構成している場合は、セッションの開始処理の完了に影響しないため、PCVD の値は記録されません。

プリンターのマッピングの時間が長くなるのは、多くの場合プリンターの自動作成ポリシーの設定に原因があります。ユーザーのクライアントデバイスにローカルで追加されたプリンターの台数と印刷設定は、セッションの開始時間に直接影響を及ぼす可能性があります。Citrix Virtual Apps and Desktops はセッションが開始されると、ローカルにマップされたすべてのプリンターをクライアントデバイス上に作成する必要があります。特にユーザーの設定で多数のローカルプリンターが存在する場合は、印刷ポリシーを設定しなおして、作成するプリンターの台数を減らすことを検討してください。これを行うには、Delivery Controller と Citrix Virtual Apps and Desktops でプリンターの自動作成ポリシーを編集します。

ドライブマッピング時の **VDA** の実行時間（**DMVD**）

これは VDA がユーザーのクライアントドライブ、デバイス、ポートをマップするのにかかる時間です。

基本ポリシーに、未使用の仮想チャネルを無効にする設定が含まれていることを確認します。たとえば、ICA プロトコルを最適化し、全体的なセッションパフォーマンスを改善するための、オーディオまたは COM ポートマッピングなどです。

アプリケーション/デスクトップ起動時の **VDA** の実行時間（**ALVD**/**DLVD**）

このフェーズは Userinit と Shell の実行時間を合わせたものです。ユーザーが Windows マシンにログオンすると、winlogon は userinit.exe を実行します。userinit.exe はログオンスクリプトを実行し、ネットワーク接続を再確立して、Explorer.exe を起動します。Userinit は、userinit.exe の開始から、仮想デスクトップまたはアプリケーションのユーザーインターフェイスの起動までの時間に相当します。Shell の実行時間は、ユーザーインターフェイスの初期化から、ユーザーにキーボードとマウスの制御が渡されるまでの時間に相当します。

セッション作成時の **VDA** の実行時間（**SCVD**）

この時間には VDA でのセッション作成時における各種の遅延時間が含まれます。

ユーザーログオンの問題の診断

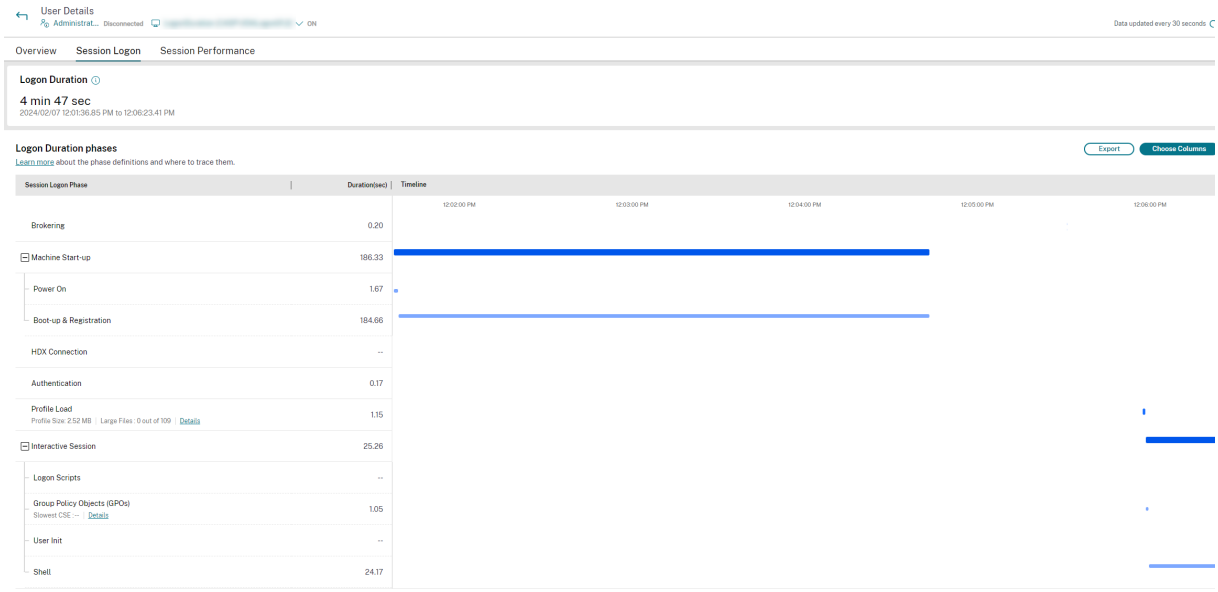
August 17, 2024

［ユーザーの詳細］ビュー >［セッションログオン］タブには、セッションログオンプロセスの包括的なビューが表示されます。このデータを使用して、ユーザーログオンの問題をトラブルシューティングします。

ログオン処理時間は、HDX を使用するデスクトップまたはアプリに初めて接続する場合のみ測定されます。このデータには、リモートデスクトッププロトコルを使用して接続しようとするユーザーや、切断されたセッションから再接続するユーザーは含まれません。具体的には、ユーザーが最初に HDX 以外のプロトコルを使用して接続してから、HDX を使用して再接続するときは、ログオン処理時間は測定されません。

ユーザーが Citrix Virtual Apps and Desktops にログオンすると、Monitor Service はログオンプロセスのフェーズを追跡します。ログオンプロセスのフェーズは、ユーザーが Citrix Workspace アプリを使用して接続した時点から始まり、アプリまたはデスクトップを使用する準備ができた時点までになります。

［セッションログオン］タブには、さまざまなログオンフェーズがプロットされたログオン期間フェーズグラフが含まれています。ログオン期間は、接続の確立および Delivery Controller からのアプリまたはデスクトップの取得にかかった時間と、仮想アプリまたはデスクトップの認証とログオンにかかった時間を表示します。処理時間の情報は秒単位（または秒の小数単位）まで表示されます。



ログオン期間フェーズグラフには、さまざまなログオンフェーズとその開始時間および終了時間が明確に表示されます。このグラフには、個別のログオンフェーズの重複が表示されます。合計ログオン時間は、個別のログオンフェーズ期間の合計ではない場合があります。これは、個々のフェーズが重複する可能性があり、すべてのログオンフェーズがこの表示に含まれるわけではないためです。また、特定のフェーズは、ユーザーが仮想アプリまたはデスクトップの操作を開始した後でも延長される可能性があり、この期間はログオン期間全体の一部として測定されません。

このビューを使用して、セッション起動の遅延を引き起こしている特定のログオンフェーズを識別します。各ログオ

ンフェーズの定義と、情報を追跡できるイベントソースは、さらにトラブルシューティングをする場合に役立ちます。グラフ上にマウスを移動すると、現在のセッションのフェーズ期間、ユーザーの 7 日間の平均、デリバリーグループの 7 日間の平均を含むヒントが表示されます。この情報は、現在のセッションのログオン期間を 7 日間の平均値と比較するのに役立ちます。GPO およびプロファイルの詳細の場合は、サブフェーズの測定値をさらにドリルダウンできます。この視覚化は、ログオン時間に関連する問題を容易に理解してトラブルシューティングするのに役立ちます。

前提条件

ログオン期間データとドリルダウンが表示されるようにするには、次の前提条件を満たす必要があります:

1. VDA に **Citrix User Profile Manager** と **Citrix User Profile Manager WMI Plugin** をインストールする。
2. Citrix Profile Management Service が実行されている。
3. XenApp および XenDesktop サイト 7.15 以前の場合、GPO 設定 ［従来の実行リストを処理しない］を無効にします。
4. 対話型セッションのドリルダウンでは、監査プロセスの追跡を有効にする必要があります。
5. GPO ドリルダウンの場合は、グループポリシーの操作ログのサイズを大きくします。

> 注:
>
> - ログオン処理時間は、デフォルトの Windows シェル（explorer.exe）でのみサポートされ、カスタムシェルではサポートされません。
> - リモート PC アクセスのログオン処理時間データは、リモート PC インストール中に **Citrix User Profile Manager** および **Citrix User Profile Manager WMI Plugin** が追加のコンポーネントとしてインストールされている場合のみ利用できます。詳しくは、「リモート PC アクセスの構成と順序の考慮事項」の手順 4 を参照してください。

ユーザーログオンの問題のトラブルシューティング手順

1. ［ユーザーの詳細］ビュー > ［セッションログオン］タブから、ログオン期間グラフを使用してログオン状態のトラブルシューティングを行います。
   - ユーザーがログオン中の場合は、ここにログオンのプロセスが表示されます。
   - ユーザーがログオン済みの場合、ユーザーがそのセッションにログオンするときにかかった時間が［ログオン処理時間］パネルに表示されます。
2. ログオンプロセスの各フェーズを調査します。

ログオンプロセスのフェーズ

仲介

ユーザーに割り当てるデスクトップを決定するのに要した時間です。

マシンのスタートアップ

マシンの起動を必要とするセッションの場合、これは仮想マシンの起動にかかった時間です。次のサブセクションでは、さまざまなフェーズで仮想マシンを起動するのにかかる時間の内訳を示します:

- 電源投入 - 仮想マシンの電源オンにかかる時間を表示します
- 起動と登録 - 仮想マシンの起動と登録にかかる時間を表示します

折りたたみ可能ボタンを使用して、[マシンのスタートアップ] の下のオプションを折りたたんだり展開したりできます。

HDX 接続

クライアントから仮想マシンへの HDX 接続の設定で必要な手順を実行するためにかかった時間です。

認証

リモートセッションへの認証を実行するのにかかった時間です。

GPO

仮想マシン上でグループポリシー設定が有効になっている場合に、ログオン中にグループポリシーオブジェクトの適用にかかった時間です。GPO バーにマウスカーソルを重ねると、CSE（クライアント側拡張機能）ごとに各ポリシーの適用にかかった時間の詳細がヒントとして表示されます。

［詳細］をクリックすると、ポリシーの状態と対応する GPO 名を示すテーブルが表示されます。ドリルダウンの期間は CSE 処理時間のみを表し、合計 GPO 時間には加算されません。ドリルダウンテーブルは、詳細なトラブルシューティングやレポートで使用するためにコピーできます。各ポリシーの GPO 時間は、イベントビューアーのログから取得されます。操作ログに割り当てられているメモリ（デフォルトサイズは 4MB）によっては、このログは上書きされる可能性があります。操作ログのログサイズを増やす方法について詳しくは、Microsoft の記事「Configuring the Event Logs」を参照してください。

ログオンスクリプト

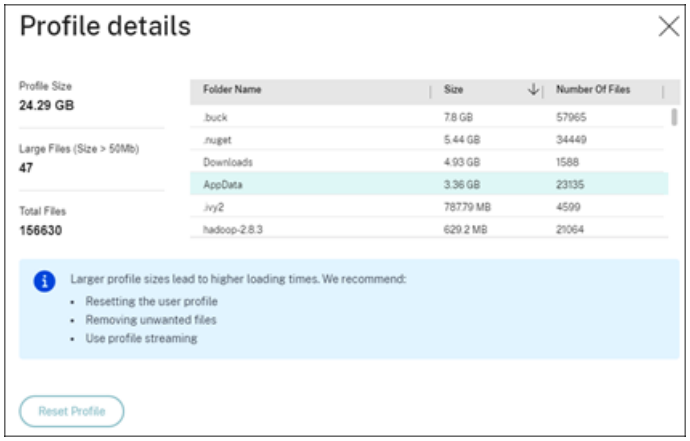
セッションでログオンスクリプトが構成されている場合、これはログオンスクリプトの実行にかかった時間です。

プロファイルのロード

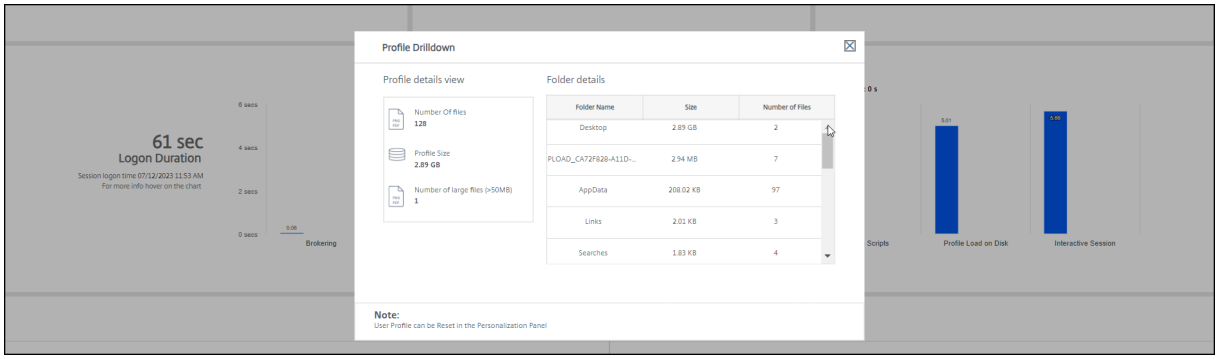
ユーザーまたは仮想マシンに対してプロファイル設定が構成されている場合、これはプロファイルのロードにかかった時間です。

Citrix Profile Management および FSLogix が構成されている場合、［プロファイルのロード］バーに表示されるのは Citrix Profile Management および FSLogix がユーザープロファイルの処理に要する時間です。この情報は、管理者が処理に時間がかかる問題をトラブルシューティングするために役立ちます。Profile Management および FSLogix が構成されている場合、［プロファイルロード］バーには長くなった処理時間が表示されます。この処理時間の増加は機能を拡張した結果であり、パフォーマンスが低下したわけではありません。この機能強化は、VDA バージョン 2407 以降で利用できます。

［プロファイルのロード］バーの上にカーソルを置くと、現在のセッションのユーザープロファイルの詳細を示すツールチップが表示されます。



［詳細］をクリックすると、プロファイルのルートフォルダー（C:/Users/username など）内の個別のフォルダー、そのサイズとファイル数（サブフォルダー内のファイルを含む）へと、さらにドリルダウンできます。



プロファイルのドリルダウンは、Delivery Controller バージョン 7 1811 以降および VDA 1811 以降で使用できます。プロファイルドリルダウン情報を使用すると、長いプロファイルロード時間に関連する問題を解決できます。次の操作を実行できます:

- ユーザープロファイルをリセットする
- 大きな不要ファイルを削除してプロファイルを最適化する
- ファイル数を減らしてネットワーク負荷を軽減する
- プロファイルストリーム配信を使用する

デフォルトでは、プロファイルのルートフォルダー内にあるすべてのフォルダーがドリルダウンに表示されます。フォルダーを非表示にするには、VDA マシンの以下のレジストリ値を編集します:

> 警告:
>
> レジストリの追加や編集を誤ると、深刻な問題が発生する可能性があり、オペレーティングシステムの再インストールが必要になる場合もあります。レジストリエディターの誤用による障害に対して、Citrix では一切責任を負いません。レジストリエディターは、お客様の責任と判断の範囲でご使用ください。また、レジストリファイルのバックアップを作成してから、レジストリを編集してください。

1. VDA で、HKEY_LOCAL_MACHINE\Software\Citrix\Director に新しいレジストリ値 **ProfileFolderNameHidden** を追加します。\
2. 値を 1 に設定します。この値は、DWORD（32 ビット）値である必要があります。フォルダ名の表示が無効になりました。
3. フォルダ名を再度表示するには、値を 0 に設定します。

> 注:
>
> GPO または PowerShell コマンドを使用して、複数のマシンでレジストリ値の変更を適用できます。GPO を使用してレジストリの変更を展開する方法について詳しくは、ブログを参照してください。

追加情報

- プロファイルのドリルダウンでは、リダイレクトされたフォルダーは考慮されません。
- ルートフォルダー内の NTUser.dat ファイルは、エンドユーザーに表示されないことがあります。ただし、これらはプロファイルのドリルダウンに含まれ、ルートフォルダー内のファイルのリストに表示されます。

- AppData フォルダーの一部の隠しファイルは、プロファイルドリルダウンに含まれません。
- ファイル数およびプロファイルサイズに関するデータは、Windows の制限事項が原因で［個人設定］パネルのデータと一致しないことがあります。

対話型セッション

対話型セッションは、ユーザープロファイルを読み込んだ後、キーボードやマウスの制御をユーザーに「渡す」までにかかった時間です。通常、ログオンプロセスのすべてのフェーズで最も長い時間であり、次のように計算されます：対話型セッションの処理時間 **=** デスクトップ準備完了イベントのタイムスタンプ（**VDA** の **EventId 1000**）**-** ユーザープロファイルロード完了イベントのタイムスタンプ（**VDA** の **EventId 2**）。対話型セッションには、userinit 実行前、userinit、Shell の 3 つのサブフェーズがあります。対話型セッションにカーソルを合わせると、次のツールチップが表示されます：

- サブフェーズ
- 各サブフェーズの所要時間
- これらのサブフェーズ間の合計累積遅延時間

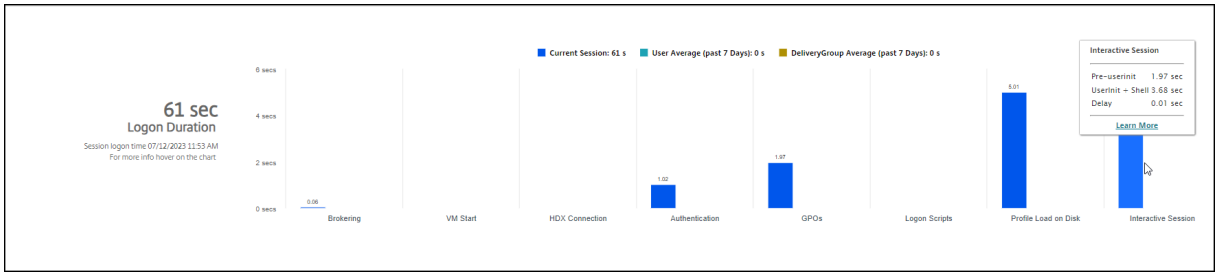
折りたたみ可能ボタンを使用して、［対話型セッション］の下のオプションを折りたたんだり展開したりできます。

> 注：
>
> この機能は VDA バージョン 1811 以降で使用できます。7.18 より前のバージョンのサイトでセッションを開始してから 7.18 以降にアップグレードした場合、「サーバーエラーのためドリルダウンを使用できません。」というメッセージが表示されます。アップグレード後にセッションを起動した場合は、エラーメッセージは表示されません。

各サブフェーズの期間を表示するには、仮想マシン（VDA ）でプロセス追跡の監査を有効にします。プロセス追跡の監査が無効（デフォルト）の場合、表示されるのは userinit 実行前の時間と、Userinit と Shell の合計時間になります。以下の手順により、グループポリシーオブジェクト（GPO）を使用してプロセス追跡の監査を有効化できます：

1. GPO を作成し、GPO エディターで編集します。
2. ［コンピューターの構成］**>** ［**Windows** の設定］**>** ［セキュリティの設定］**>** ［ローカルポリシー］**>** ［監査ポリシー］の順に移動します。
3. 右側のペインで、［プロセス追跡の監査］をダブルクリックします。
4. ［成功］チェックボックスをオンにして、［OK］をクリックします。
5. この GPO を目的の VDA やグループに適用します。

プロセス追跡の監査の詳細とこの機能の有効化および無効化の切り替え方法については、Microsoft のドキュメント「Audit process tracking」を参照してください。



［ユーザーの詳細］ビューの［ログオン処理時間］パネル。

- 対話型セッション-**userinit** 実行前：対話型セッションの所要時間のうち、グループポリシーオブジェクトおよびスクリプトの適用にかかった時間です。このサブフェーズは、GPO とスクリプトを最適化することで短縮できます。
- 対話型セッション-**userinit**： Windows マシンにユーザーがログオンすると、Winlogon により userinit.exe が実行されます。Userinit.exe はログオンスクリプトを実行し、ネットワーク接続を再確立して、Windows ユーザーインターフェイスである Explorer.exe を起動します。この対話型セッションのサブフェーズは、userinit.exe の開始から、仮想デスクトップまたはアプリケーションのユーザーインターフェイスの起動までの時間に相当します。
- 対話型セッション-**Shell**：前のサブフェーズで、userinit により Windows ユーザーインターフェイスの初期化が開始されます。Shell サブフェーズは、ユーザーインターフェイスの初期化から、ユーザーにキーボードとマウスの制御が渡されるまでの時間に相当します。
- 遅延： **userinit** 実行前および **userinit** と **userinit** および **Shell** の各サブフェーズ間の累積遅延時間です。

総ログオン時間は、これらの各フェーズを厳密に合計したものではありません。たとえば、一部のフェーズは並行して発生するほか、フェーズによっては追加処理が発生してログオン処理時間が合計値よりも大きくなることがあります。総ログオン処理時間には、ICA ファイルのダウンロードとアプリケーションでの ICA ファイルの起動までの時間に相当する、ICA アイドル時間は含まれません。
アプリケーション起動時に ICA ファイルを自動的に開くようにするは、ICA ファイルをダウンロード時に自動で開くようにお使いの Web ブラウザーを構成します。詳しくは、CTX804493を参照してください。

> 注：
>
> ［ログオン処理時間］グラフには、ログオンフェーズが秒単位で表示されます。1 秒未満の時間値はすべて、秒未満の値として表示されます。1 秒を超える値は、0.5 秒単位に丸められます。グラフは、Y 軸の最高値を 200 秒として表示するように設計されています。200 秒を超える値はすべて、実際の値を棒グラフの上に添えて表示されます。

データのエクスポート

デフォルトのログオン期間の段階テーブルオプション（セッションログオン段階と期間）に加えて、セッションログオンページで次の列を選択することもできます：

- 開始時間
- 終了時間

- デリバリーグループ - 7 日間の平均（秒）
- ユーザー - 7 日間の平均（秒）

上記のデータを.CSV ファイルにエクスポートすることもできます。

トラブルシューティングのヒント

グラフで異常な値または予期しない値を識別するには、現在のセッションの各フェーズで要した時間と、このユーザーの最近 7 日間の平均処理時間、およびこのデリバリーグループのすべてのユーザーの最近 7 日間の平均処理時間を比較します。

必要に応じて、担当管理者に報告します。たとえば、マシンのスタートアップに時間がかかり、ハイパーバイザーが問題の原因である可能性がある場合は、ハイパーバイザー管理者に問題を報告します。

以下の問題について調査します：

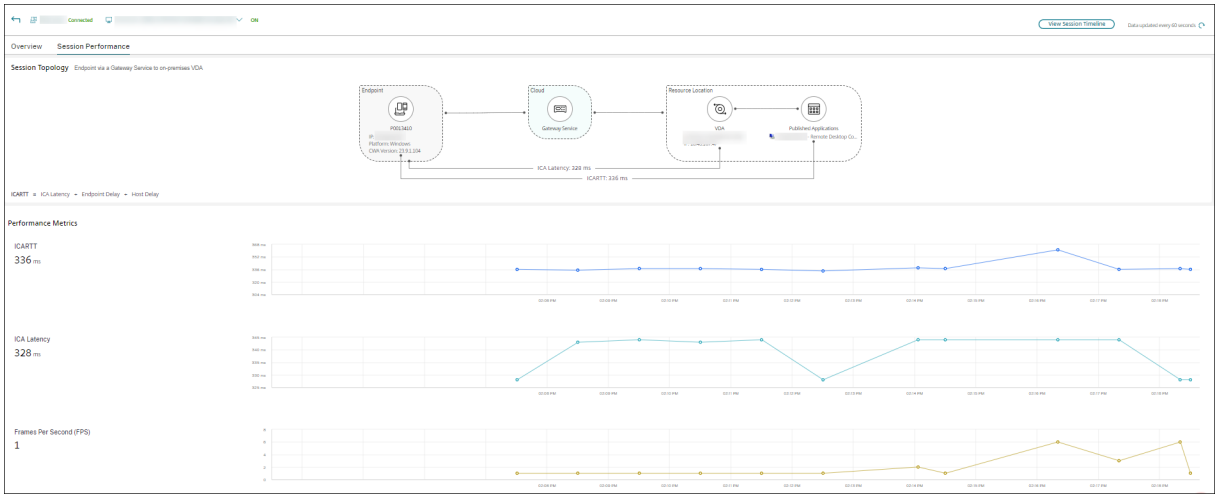
- （現在の）ログオンを示すバーが表示されていない。
- 現在のログオン処理時間とこのユーザーの平均処理時間が大きく食い違う。次の原因が考えられます：
  - 新しいアプリケーションがインストールされた。
  - オペレーティングシステムが更新された。
  - 構成が変更された。
  - ユーザーのプロファイルサイズが大きい。この場合、プロファイルロード時間が長くなります。
- ユーザーのログオン処理時間（現在値および平均値）とデリバリーグループの平均値が大きく食い違う。

必要な場合は、［再起動］をクリックしてユーザーに再ログオンしてもらい、マシンのスタートアップや仲介時に問題が発生するかどうかを確認します。

セッションのパフォーマンスの問題を診断する

August 17, 2024

［ユーザーの詳細］ページの ［セッションパフォーマンス］タブでは、HDX ユーザーセッション内の問題の特定に役立つトラブルシューティングワークフローが強化されました。［セッションのトポロジ］と［パフォーマンスメトリック］パネルは、単一のビューでコンポーネントビューとセッションの複数のパフォーマンス指標を関連付けることに役立ち、セッションエクスペリエンスの問題の解決にかかる平均時間を短縮します。



エンドツーエンドのネットワークホップビュー

エンドツーエンドのネットワークホップビューは、トラブルシューティングワークフローを強化するための次のステップです。[ユーザーの詳細] > [セッションパフォーマンス] > [セッションのトポロジ] セクションでは、接続された HDX セッションのエンドツーエンドのネットワークホップビューを視覚的に表現します。

接続されたセッションのセッショントポロジには、セッションパスに含まれるコンポーネントとそのメタデータ、コンポーネント間のリンク、および VDA で公開されたアプリケーションが表示されます。
さらに、セッションに関する次のセッションパフォーマンスメトリックが表示されます:

- ICA 遅延 - ICA 遅延は基本的にネットワーク遅延です。このパラメーターは、ネットワークの速度が遅いかどうかを示します。
- ICA 往復時間 - ICA 往復時間は、ユーザーの操作と画面に表示されるグラフィックによる応答の間の時間間隔です。この測定には、ICA 遅延、エンドポイント遅延、およびホスト遅延が含まれます。

このビューを使用すると、セッションデータのフローでコンポーネントを理解し、パフォーマンスの問題を引き起こしている可能性のある特定のホップを識別できます。

[セッションのトポロジ] ビューのパフォーマンスメトリックは、接続状態の HDX セッションでのみ使用できます。

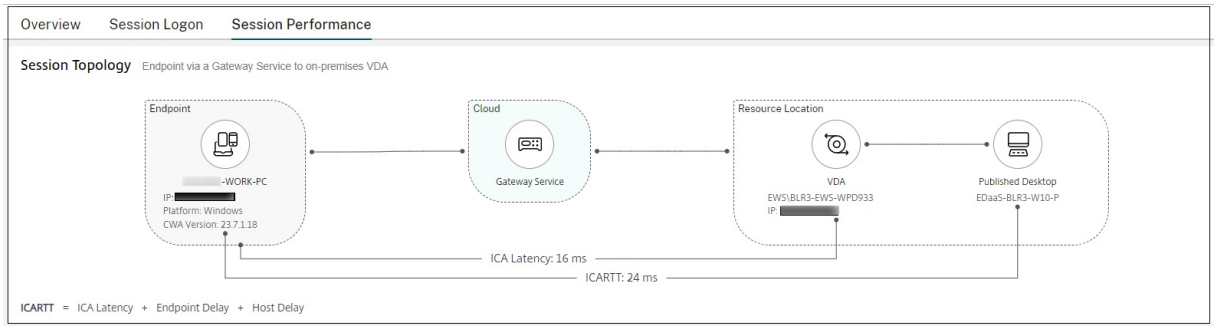
セッショントポロジのシナリオ

サイトの展開シナリオに応じて、セッションに関係するコンポーネントは次のすべてまたはいずれかになります:

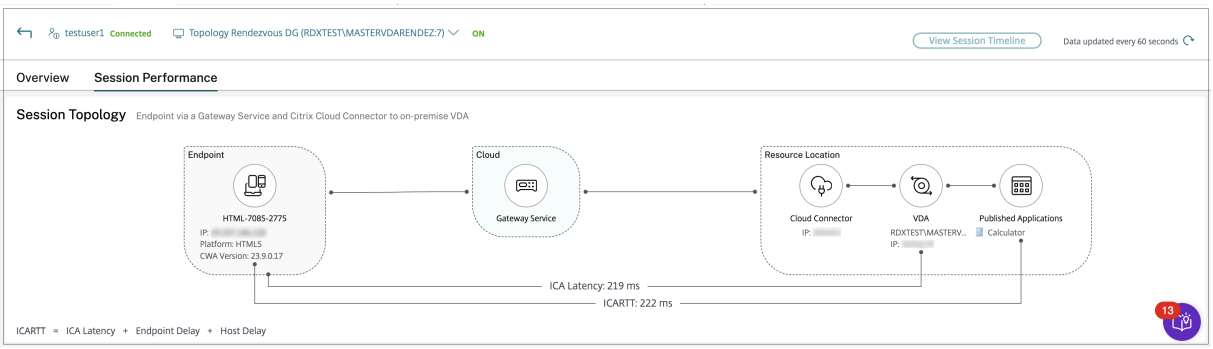
- エンドポイント上の Citrix Workspace アプリ
- Gateway サービス/オンプレミス Gateway
- Cloud Connector –ハイブリッド接続の場合、Gateway は Cloud Connector 経由で DaaS に接続されます。
- VDA

したがって、想定されるネットワークトポロジは次のとおりです:

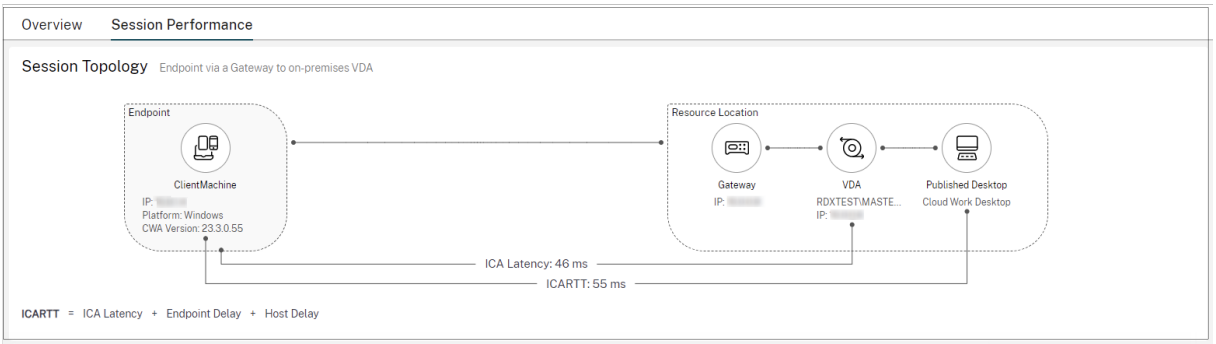
- エンドポイント上の Citrix Workspace アプリは、Citrix Workspace および Gateway サービスを介してオンプレミスの VDA に接続します。VDA への接続に Cloud Connector は使用されません。



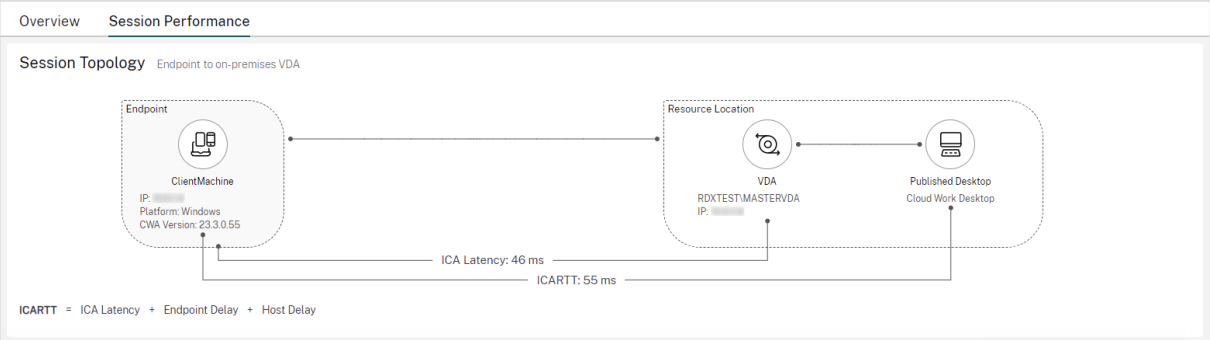
- エンドポイント上の Citrix Workspace アプリは、Citrix Workspace および Gateway サービス経由で、Cloud Connector を介したオンプレミスの VDA に接続します。



- エンドポイント上の Citrix Workspace アプリは、StoreFront およびオンプレミス Gateway を介してオンプレミスの VDA に接続します。



- エンドポイント上の Citrix Workspace アプリは、StoreFront を介してオンプレミスの VDA に接続します。



パフォーマンスメトリック

[パフォーマンスメトリック] パネルでは、ユーザーセッション内の問題を特定する際にリアルタイムの指標を関連付けることができます。セッションメトリックの傾向は、これらの指標が時間の経過とともにどのように実行されたかを示すのに役立ちます。[セッションのパフォーマンス] タブをクリックすると、リアルタイムデータとともに、過去 15 分間と 24 時間のデータを表示できます。ここでは、複数のコンポーネントのパフォーマンス メトリックを 1 つのビューで相関させるのに役立ちます。

> 注:
>
> - メトリックは 15 分間継続するため、セッションが接続および切断されている期間のグラフが描画されます。切断されたセッションのメトリックは値 0 で表示されます。
> - 過去 24 時間のメトリックのサポートにより、ICA 往復時間および ICA 遅延のプロットが履歴データメトリックで更新されます。

ICARTT と ICA 遅延のほかに、次のメトリックでリアルタイムおよび過去 15 分間のメトリックを取得できます:

- フレーム数/秒 - フレーム数/秒は、セッションの応答性を示す重要な指標です。
  利用可能な出力帯域幅 - 利用可能な出力帯域幅は、VDA からエンドポイントにデータを送信するために利用できる合計帯域幅の基準です。

- 消費された出力帯域幅 - 消費された出力帯域幅は、ユーザーにセッションを表示するために VDA からエンドポイントに送信された実際のデータ量を示します。

利用可能な出力帯域幅と消費された出力帯域幅を分析すると、セッションの処理に十分な帯域幅が利用可能かどうかを確認し、セッションが帯域幅不足の影響を受けているかどうかを検出するのに役立ちます。

ICA 往復時間またはセッションのログオン期間のデータの入力に失敗した場合のトラブルシューティング

以前は、EUEM サービスまたは Profile Management サービスの実行に失敗した場合、ICA 往復時間またはセッションのログオン期間に関連するデータの取得に失敗した理由は表示されませんでした。この新機能を使用すると、失敗の理由と、その失敗に対応する解決策を取得できます。「詳細情報」リンクには、次の表に示すように、ICA 往復時間およびセッションのログオン期間エラー、失敗の理由、および解決策が表示されます:

エラーの種類	エラー	エラーメッセージ	解決策
ICA 往復時間エラー	ICA 往復時間値が表示されません。	**Citrix End User Experience Monitoring** が実行されていません。	1. サービスコンソールを開きます。このコンソールを開くには、[スタート] をクリックし、「**Services**」と入力します。 2. Citrix EUEM が実行されていることを確認してください。 3. デスクトップセッションを再度開いて試してください。ICA 往復時間値が表示されている必要があります。 4. 問題が解決しない場合は、Citrix 管理者に問い合わせてください。
ICA 往復時間エラー	ICA 往復時間値が表示されません。	**Citrix End User Experience Monitoring** がインストールされていません。	1. VDA を再インストールします。 2. サービスコンソールを開きます。このコンソールを開くには、[スタート] をクリックし、「Services」と入力します

エラーの種類	エラー	エラーメッセージ	解決策
			3. Citrix EUEM が実行されていることを確認してください。 4. デスクトップセッションを再度開いて試してください。すぐに ICA 往復時間値が表示される必要があります。 5. 問題が解決しない場合は、Citrix 管理者に問い合わせてください。
ICA 往復時間エラー	ICA 往復時間値が表示されません。	データの取得中にエラーが発生しました。	1. サービスコンソールを開きます。このコンソールを開くには、［スタート］をクリックし、「Services」と入力します。 2. **Windows Management Instrumentation Service** が実行されていることを確認します。 3. また、Wf-Shell.exe/PicaShell.exe プロセスは ［アクティビティマネージャー］>［プロセス］タブで実行されていることを確認します。実行されていない場合は、デスクトップセッションを再度開きます。

エラーの種類	エラー	エラーメッセージ	解決策
			4.前の手順が機能しない場合は、次のコマンドを実行して、Citrix_Euem_RoundTrip インスタンスが存在することを確認します: `Get-CimInstance -Namespace 'ROOT\Citrix\Euem'-Query "select * from Citrix_Euem_RoundTrip"` 5. Citrix_Euem_RoundTrip インスタンスが存在する場合は、デスクトップセッションを再度開きます。 6.問題が解決しない場合は、Citrix 管理者に問い合わせてください。
セッションログオン期間エラー	グラフが読み込まれていません。	**Citrix Profile Management** が実行されていません	1.サービスコンソールを開きます。このコンソールを開くには、[スタート] をクリックし、「Services」と入力します。 2.**Citrix Profile Management Service** が実行されていることを確認します。 3.デスクトップセッションを再度開いて試してください。グラフが表示されている必要があります。

エラーの種類	エラー	エラーメッセージ	解決策
			4. 問題が解決しない場合は、Citrix 管理者に問い合わせてください。
セッションログオン期間エラー	グラフが読み込まれていません。	**Citrix Profile Management** がインストールされていません。	1. Citrix Profile Management サービスインストールします。 2. サービスコンソールを開きます。このコンソールを開くには、［スタート］をクリックし、「Services」と入力します。 3. **Citrix Profile Management Service** が実行されていることを確認します。 4. デスクトップセッションを再度開いて試してください。グラフが表示されている必要があります。 5. 問題が解決しない場合は、Citrix 管理者に問い合わせてください。
セッションログオン期間エラー	グラフが読み込まれていません。	データの取得中にエラーが発生しました。	1. サービス コンソールを開きます。このコンソールを開くには、［スタート］をクリックし、「Services」と入力します。 2. **Windows Management Instrumentation Service** が実行されていることを確認します。

エラーの種類	エラー	エラーメッセージ	解決策
			3.前述のサービスがすでに実行されている場合は、次のコマンドを実行して、`LogonTimings instance is present`であることを確認します: `Get-CimInstance -Namespace 'ROOT\Citrix\Profile\Metrics' -Query "select * from LogonTimings"` 4.問題が解決しない場合は、Citrix 管理者に問い合わせてください。

ユーザーのシャドウ

August 17, 2024

Director のユーザーのシャドウ機能を使用すると、ユーザーの仮想マシンまたはセッションを直接表示したり操作したりできます。Windows と Linux VDA の両方をシャドウできます。この機能を使用するには、そのマシンにユーザーが接続している必要があります。ユーザーが接続している場合、ユーザーのタイトルバーにそのマシン名が表示されます。

Director は新しいタブでシャドウを開始し、Director URL からのポップアップを許可するように Web ブラウザーの設定を更新します。

[ユーザーの詳細] ビューからシャドウ機能にアクセスします。ユーザーセッションを選択し、[アクティビティマネージャー] ビューまたは [セッション詳細] パネルで、[シャドウ] をクリックします。

Linux VDA のシャドウ

シャドウは、RHEL7.3 または Ubuntu バージョン 16.04 Linux ディストリビューションを実行する Linux VDA バージョン 7.16 以降で使用できます。

> 注:
>
> - シャドウが機能するには、Director UI から VDA にアクセスできる必要があります。したがって、シャドウは Director クライアントと同じイントラネット内の Linux VDA に対してのみ実行できます。
> - Director は完全修飾ドメイン名を使用してターゲットの Linux VDA に接続します。Director クライアントが Linux VDA の完全修飾ドメイン名を解決できるようにしてください。
> - VDA には、python websockify パッケージと x11vnc パッケージがインストールされている必要があります。
> - VDA への noVNC 接続は、WebSocket プロトコルを使用します。デフォルトでは、**ws://** WebSocket プロトコルが使用されます。セキュリティ上の理由からセキュリティ保護された **wss://** プロトコルを使用することをお勧めします。各 Director クライアントおよび Linux VDA に SSL 証明書をインストールします。

VDA をシャドウ用に設定するには、「セッションのシャドウ」の手順に従います。

1. [シャドウ] をクリックすると、シャドウ接続が初期化され、確認プロンプトがユーザーデバイスに表示されます。
2. ユーザーが [はい] をクリックすると、マシンまたはセッションの共有が開始されます。
3. 管理者は、シャドウセッションのみを表示できます。

Windows VDA のシャドウ

Windows VDA セッションは、Windows リモートアシスタンスを使用してシャドウされます。VDA のインストール中にユーザーの **Windows** リモートアシスタンス機能を有効にします。詳しくは、「機能を有効または無効にする」セクションを参照してください。

1. [シャドウ] をクリックするとシャドウ接続が初期化されます。これにより、.msrc インシデントファイルを開くか保存するかを確認するダイアログボックスが開きます。
2. デフォルトで選択されていない場合は、Remote Assistance Viewer でファイルを開きます。ユーザーデバイス側には、確認のメッセージが表示されます。
3. ユーザーが [はい] をクリックすると、マシンまたはセッションの共有が開始されます。
4. ユーザーがマウスやキーボードの制御を許可すると、管理者がシャドウセッションを制御できるようになります。

シャドウのための **Microsoft Internet Explorer** ブラウザーの構成

Microsoft Internet Explorer ブラウザーでダウンロードした Microsoft リモートアシスタンスファイル（.msra）がリモートアシスタンスクライアントで自動的に開くように構成します。

これを行うには、グループポリシーエディターで [ファイルのダウンロード時に自動的にダイアログを表示] を有効にする必要があります。

［コンピューターの構成］>［管理用テンプレート］>［Windows コンポーネント］>［Internet Explorer］>［インターネットコントロールパネル］>［セキュリティページ］>［インターネットゾーン］>［ファイルのダウンロード時に自動的にダイアログを表示］

デフォルトでは、ローカルイントラネットゾーンのサイトに対してこのオプションが有効になっています。Director サイトがローカルイントラネットゾーンにない場合は、ローカルイントラネットゾーンに追加することを検討してください。

ユーザーへのメッセージの送信

August 17, 2024

Director では、マシンに接続しているユーザーにメッセージを送信できます。突発的にデスクトップの保守、ログオフ、再起動、プロファイルのリセットなどが必要になった場合に、ユーザーに緊急のメッセージを送信できます。

1. ［アクティビティマネージャー］ビューでユーザーを選択して、［詳細］をクリックします。
2. ［ユーザーの詳細］ビューの［セッション詳細］パネルで、［メッセージの送信］をクリックします。
3. 送信するメッセージの［件名］および［メッセージ］を入力して、［送信］をクリックします。

メッセージが正しく送信されると、Director に確認メッセージが表示されます。メッセージがユーザーのマシンに表示されます。

メッセージの送信に問題が発生すると、Director にエラーメッセージが表示されます。そのエラーメッセージに従って問題を解決してください。問題を解決したら、件名およびメッセージテキストを入力して再度 ［試行］をクリックします。

アプリケーション障害の解決

August 17, 2024

［アクティビティマネージャー］ビューで［アプリケーション］タブをクリックします。ここでは、このユーザーがアクセス権限をもつすべてのマシン上のすべてのアプリケーションとその状態を確認できます。これには、接続しているマシンのローカルアプリケーションおよびホストされるアプリケーションが含まれます。

> 注:
>
> ［アプリケーション］タブが灰色表示になっている場合は、このタブを有効にする権限を持つ管理者に問い合わせてください。

一覧には、セッション内で起動されたアプリケーションのみが表示されます。

マルチセッション OS マシンおよびシングルセッションOS マシンでは、アプリケーションが切断セッションごとに一覧で表示されます。ユーザーが接続していない場合、アプリケーションは表示されません。

アクション	説明
応答していないアプリケーションを終了する	応答していないアプリケーションを選択し、［アプリケーションの終了］をクリックします。アプリケーションが終了したら、ユーザーに再度起動するように通知します。
応答していないプロセスを終了する	必要な権限がある場合は、［プロセス］タブをクリックします。アプリケーションに関連するプロセス、または CPU リソースやメモリを過度に消費しているプロセスを選択し、［プロセスの終了］をクリックします。プロセスを終了するための権限がない場合、プロセスを終了することはできません。
ユーザーのマシンを再起動する	シングルセッションOS マシンでは、選択したセッションで［再起動］をクリックします。または、［マシンの詳細］ビューで電源制御を使ってマシンを再起動またはシャットダウンします。アプリケーションの状態を再確認するには、ユーザーに再度ログオンするように通知します。マルチセッション OS マシンでは、［再起動］オプションを使用できません。代わりに、ユーザーをログオフして、再度ログオンさせます。
マシンをメンテナンスモードにする	パッチまたはそのほかの更新などによりマシンのイメージをメンテナンスする必要がある場合は、マシンをメンテナンスモードにします。［マシンの詳細］ビューで［詳細］をクリックして、メンテナンスモードのオプションをオンにします。担当の管理者に報告します。

デスクトップ接続の復元

August 17, 2024

Director ビューでは、タイトルバーにそのユーザーの接続状態が表示されます。

デスクトップ接続に問題が発生するとその原因が表示されるため、トラブルシューティング方法を判別することができます。

アクション	説明
マシンがメンテナンスモードでないことを確認する	[ユーザーの詳細］ページで、メンテナンスモードがオフであることを確認します。
ユーザーのマシンを再起動する	マシンを選択して ［再起動］をクリックします。このオプションは、ユーザーのマシンが応答しない場合や接続できない場合に使用します。たとえば、マシンが異常に大量の CPU リソースを使用している場合、CPU が使用できなくなることがあります。

セッションの復元

August 17, 2024

セッションが切断状態になると、セッションおよびアプリケーションは終了しませんが、サーバーとユーザーデバイス間の通信が切断されます。

[ユーザーの詳細］ビューの ［セッション詳細］パネルで、セッション障害のトラブルシューティングを行います。現在のセッションがセッション ID で示され、詳細を確認できます。

アクション	説明
応答していないアプリケーションまたはプロセスを終了する	［アプリケーション］タブをクリックします。応答していないアプリケーションを選択し、［アプリケーションの終了］をクリックします。同様に、応答していないプロセスを選択し、［プロセスの終了］をクリックします。また、メモリや CPU リソースを過度に消費しているプロセスを終了します。
Windows セッションを切断する	［セッション制御］をクリックし、［切断］を選択します。このオプションは、仲介されたマルチセッション OS マシンに対してのみ使用できます。仲介されていないセッションでは無効です。
ユーザーのセッションからログオフする	［セッション制御］をクリックし、［ログオフ］を選択します。

セッション障害が解決されたことを確認するために、ユーザーに再度ログオンさせます。また、ユーザーをシャドウしてセッションをより詳しく監視することもできます。

HDX チャネルシステムレポートの実行

August 17, 2024

ユーザーのマシン上の HDX チャネルの状態を確認するには、［ユーザーの詳細］ビューの［**HDX**］パネルを使用します。このパネルは、HDX を使ってユーザーマシンに接続している場合にのみ操作できます。

情報を使用できないことを示すメッセージが表示された場合は、ページが更新されるまで 1 分待つか、［更新］ボタンをクリックしてください。HDX データはほかのデータより更新に時間がかかることがあります。

エラーまたは警告のアイコンをクリックすると、詳細が表示されます。

> ヒント：
>
> このダイアログボックスでは、タイトルバーの左隅にある矢印をクリックしてほかのチャネルの情報を表示することもできます。

HDX チャネルシステムレポートは、主に Citrix サポートチームによるトラブルシューティング時に使用されます。

1. ［HDX］パネルで、［システムレポートのダウンロード］をクリックします。
2. 生成された XML 形式のレポートファイルを表示したり保存したりできます。
    - XML ファイルを表示するには、［開く］をクリックします。Director に XML ファイルの内容が表示されます。
    - XML ファイルを保存するには、［保存］をクリックします。［名前を付けて保存］ダイアログボックスで、ファイルの保存場所として Director が動作するマシン上のフォルダーを指定します。

ユーザープロファイルのリセット

August 17, 2024

> 注意：
>
> プロファイルをリセットすると、ユーザーのフォルダーやファイルが保存され、新しいプロファイルにコピーされます。ただし、ほとんどのユーザープロファイルデータがありません（たとえば、レジストリがリセットされ、アプリケーション設定が削除されることがあります）。

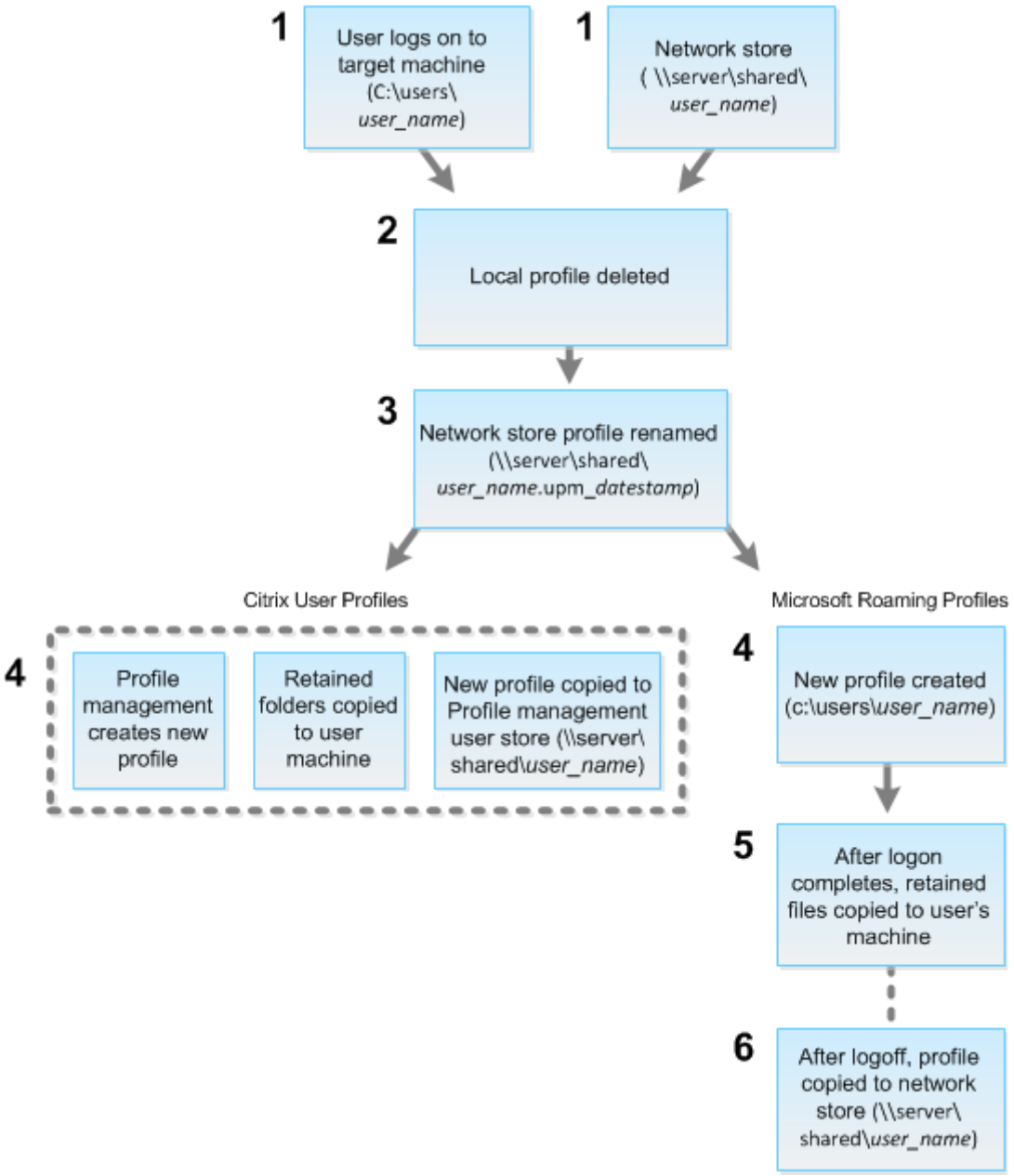
リセット機能は、ファイルベースとコンテナベースの両方のプロファイル ソリューションに適用されます。

リセットされたプロファイルはどのように処理されるか

いずれの Citrix ユーザープロファイルまたは Microsoft 移動プロファイルもリセットできます。ユーザーがログオフした後に管理者が Director または PowerShell SDK でリセットコマンドを選択すると、使用されているユ

ーザープロファイルが識別され、Director により適切なリセットコマンドが発行されます。Director は Profile Management を介してプロファイルのサイズ、種類、およびログオン時間などに関する情報を取得します。

これは、ユーザーログオン後の、ユーザープロファイルがリセットされた場合の処理を説明した図です。



Director からのリセットコマンドにより、プロファイルの種類が指定されます。次に、Profile Management サービスによりその種類のプロファイルのリセットが試行され、適切なネットワーク共有（ユーザーストア）が検出されます。Profile Management により処理されたユーザーのプロファイルに対して移動プロファイル用のコマンドが発行された場合は拒否されます（逆の場合も同様）。

1. ローカルプロファイルがある場合は削除されます。
2. ネットワークプロファイルの名前が変更されます。

3. 次の処理は、リセットされるプロファイルが Citrix ユーザープロファイルか Microsoft 移動プロファイルかにより異なります。

   Citrix ユーザープロファイルの場合、Profile Management インポート規則を使用して新しいプロファイルが作成されます。フォルダーはネットワークプロファイルにコピーされ、ユーザーは通常どおりログオンできます。リセットに移動プロファイルが使用される場合は、移動プロファイル内のすべてのレジストリ設定がリセットプロファイル内に保持されます。必要な場合は、テンプレートプロファイルが移動プロファイルよりも優先されるように Profile Management を構成することもできます。

   Microsoft 移動プロファイルの場合、Windows によってプロファイルが作成され、ユーザーがログオンするとフォルダーがユーザーデバイスにコピーされます。ユーザーが再度ログオフすると、新しいプロファイルがネットワークストアにコピーされます。

Director でユーザープロファイルをリセットするには

Citrix Virtual Desktops（デスクトップ VDA）を使用している場合は、次の手順を実行します：

1. **Director** で、プロファイルをリセットするユーザーを検索してから、このユーザーのセッションを選択します。
2. ［プロファイルのリセット］をクリックします。
3. ユーザーに、すべてのセッションからログオフするように指示します。
4. ユーザーに再度ログオンするように指示します。
   ユーザープロファイルから保存されたフォルダーやファイルが新しいプロファイルにコピーされます。

Citrix Virtual Desktops（サーバー VDA）を使用している場合は、プロファイルのリセットを実行するためにログオンする必要があります。ユーザーはいったんログオフしてから再度ログオンし、プロファイルのリセットを完了させる必要があります。

> 重要：
>
> 複数のプラットフォーム上（Windows 8 と Windows 7 など）にユーザーのプロファイルが存在する場合は、問題が発生したデスクトップまたはアプリケーションに最初にログオンするよう指示します。このログオン操作により、正しいプロファイルがリセットされます。Citrix ユーザープロファイルの場合、ユーザーのデスクトップが表示された時点でリセットされています。Microsoft の移動プロファイルの場合、フォルダーの復元処理に時間がかかる場合があります。この復元処理が完了するまで、ユーザーはログオンしていなければなりません。

プロファイルが正しくリセットされない場合（ユーザーがそのマシンに再ログオンできなかったり一部のファイルが見つからなかったりする場合など）、管理者が手作業で元のプロファイルを復元する必要があります。

以下の点に注意してください：

- ユーザープロファイルソリューションとしてユーザーストアが有効になっている場合、新しいプロファイルには、元のユーザープロファイルの次の個人用フォルダーが含まれます：

  - デスクトップ
  - Cookies
  - お気に入り
  - ドキュメント
  - ピクチャ
  - ミュージック
  - ビデオ

- Citrix Management プロファイルコンテナがユーザープロファイルソリューション全体として有効になっている場合、新しいプロファイルには前述の個人用フォルダーが含まれません。
- Windows 8 以降では、プロファイルのリセット時に Cookies フォルダーが新しいプロファイルにコピーされません。

リセットに失敗したプロファイルを手動で復元するには

1. ユーザーに、すべてのセッションからログオフするように指示します。
2. ローカルプロファイルが存在する場合は削除します。
3. ネットワーク共有上のアーカイブフォルダーを検索します。アーカイブフォルダーには、名前に日時と upm_datestamp 拡張子が含まれます。
4. 現在のプロファイル名を削除します。つまり、upm_datestamp 拡張子のないものです。
5. 元のプロファイル名を使用して、アーカイブされたフォルダーの名前を変更します。つまり、日時の拡張子を削除します。プロファイルがリセット前の状態に戻りました。

PowerShell SDK を使用してプロファイルをリセットするには

Broker PowerShell SDK を使用してプロファイルをリセットできます。

New-BrokerMachineCommand

特定のユーザー、セッション、またはマシンに配信するためのキューに登録されたコマンドを作成します。このコマンドレットについて詳しくは、https://citrix.github.io/delivery-controller-sdk/Broker/New-BrokerMachineCommand/を参照してください。

例

PowerShell コマンドレットを使用してプロファイルをリセットする方法の詳細については、以下の例を参照してください:

Profile Management プロファイルのリセット

- user1 のプロファイルをリセットしたいとします。PowerShell コマンドの New-BrokerMachineCommand を使用します。例:

  ```
  New-BrokerMachineCommand -Category UserProfileManager -CommandName "ResetUpmProfile"-DesktopGroups 1 -CommandData $byteArray -SendTrigger logon -user domain1\user1
  ```

> 重要:
>
> `CommandData $byteArray`を使用する際は、`<SID>[,<backup path>]`の形式にする必要があります: バックアップパスを指定しない場合、Profile Management により現在の日付と時刻で名前が付けられたバックアップフォルダが生成されます。

Windows 移動プロファイルのリセット

- user1 の移動プロファイルをリセットしたいとします。PowerShell コマンドの New-BrokerMachineCommand を使用します。例:

  ```
  New-BrokerMachineCommand -Category UserProfileManager -CommandName "ResetRoamingProfile"-DesktopGroups 1 -CommandData $byteArray -SendTrigger logon -user domain1\user1
  ```

セッションの録画

August 17, 2024

Director の［ユーザーの詳細］と［マシンの詳細］画面から、Session Recording 制御を使って、ICA セッションを録画することができます。この機能は **Platinum** ライセンスを持つユーザーが使用できます。

動的なセッション録画

［ユーザーの詳細］画面から、Session Recording 制御を使って、現在アクティブなセッションを録画することができます。動的なセッション録画について詳しくは、「Session Recording サービス」の記事を参照してください。

ポリシーベースのセッション録画

DirectorConfig ツールを使って Director でポリシーベースの Session Recording を構成するには、「Session Recording ポリシーの構成」の「**Director** を構成して **Session Recording** サーバーを使用する」を参照してください。
ログインユーザーに Session Recording ポリシーを変更する権限がある場合のみ、Director の Session Recording

制御を使用できます。この権限は、「ユーザーの承認」で説明されているように、Session Recording 承認コンソールで設定できます。

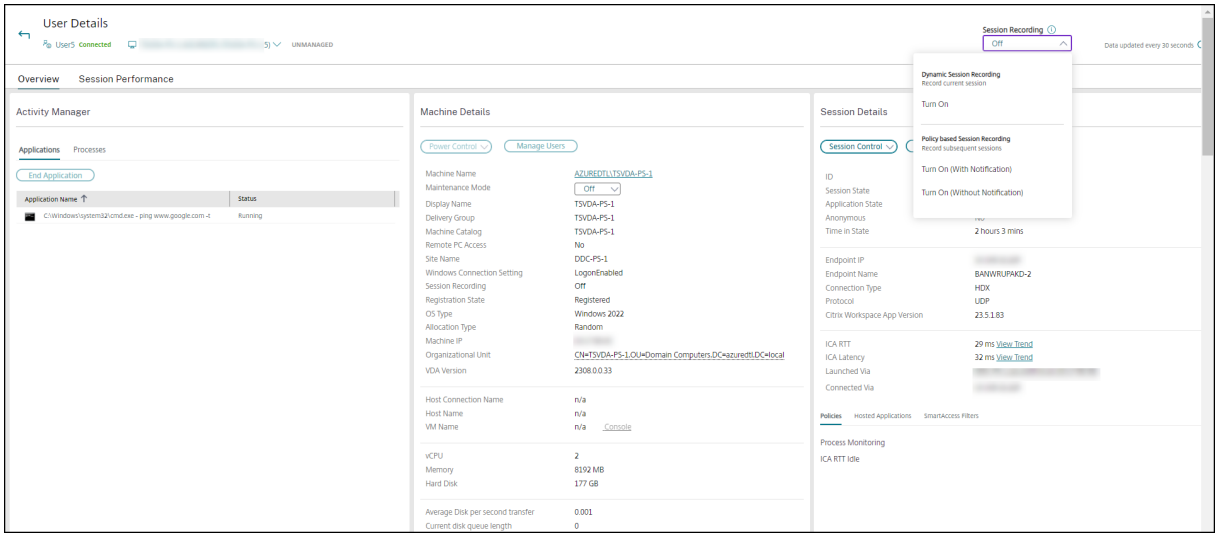
> 注:
> Director または Session Recording ポリシーコンソールによる Session Recording の設定の変更は、次の ICA セッションの起動時から有効になります。

Director での Session Recording 制御

［ユーザーの詳細］>［**Session Recording**］の次の操作で、現在のまたは以降のセッションを録画できます。

- 動的なセッション録画をオンにする - 現在のセッションが録画されます。
- オンにする（通知あり）- 以降のセッションが録画され、ICA セッションへのログオン時にセッションが録画されていることがユーザーに通知されます。
- オンにする（通知なし）- 以降のセッションが録画され、セッションは、ユーザーに通知されることなく録画されます。
- オフにする - ユーザーのセッションの録画を無効にします。

［ポリシー］パネルには、アクティブな Session Recording ポリシーの名前が表示されます。



［マシンの詳細］パネルには、そのマシンの Session Recording ポリシーの状態が表示されます。

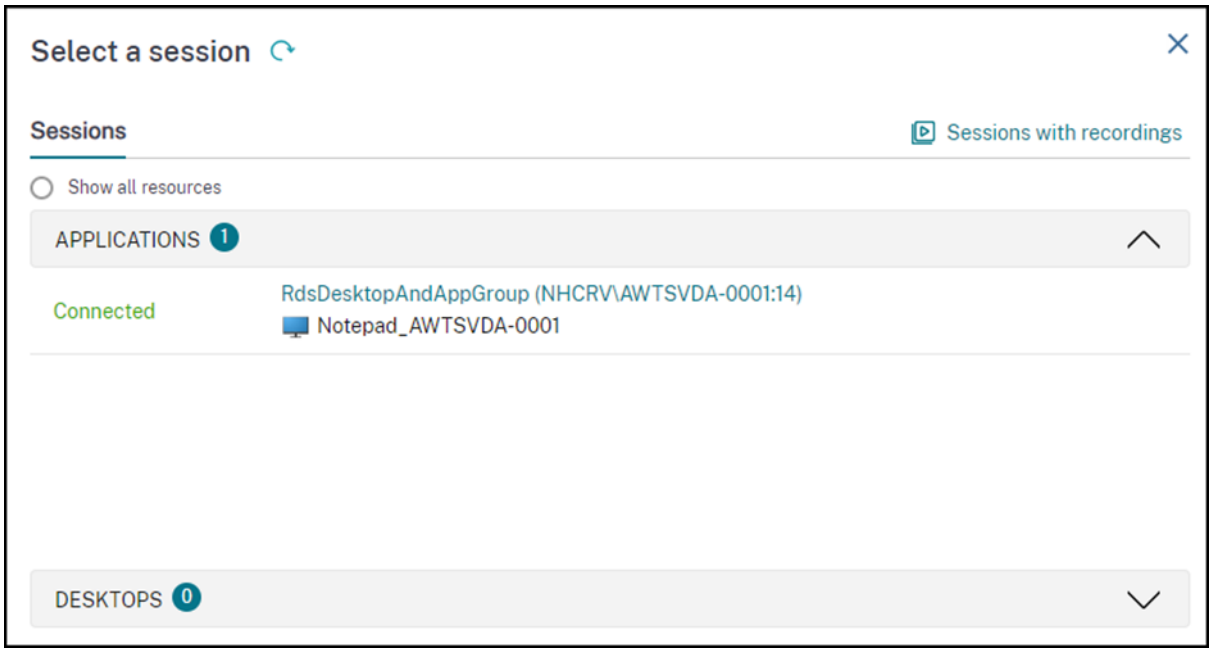
ライブセッションと録画されたセッションを再生する

録画されたユーザーセッションやライブのユーザーセッションを再生することで、ユーザーが遭遇した問題を確認できます。Director コンソール内で録画およびセッション関連のメトリックに簡単にアクセスできるため、複数のセッション録画サーバー間で録画を検索したり、録画を表示するためのサードパーティアプリを探したりする必要がなくなります。これは、録画で検出された問題をパフォーマンスメトリックと関連付けるのに役立ちます。

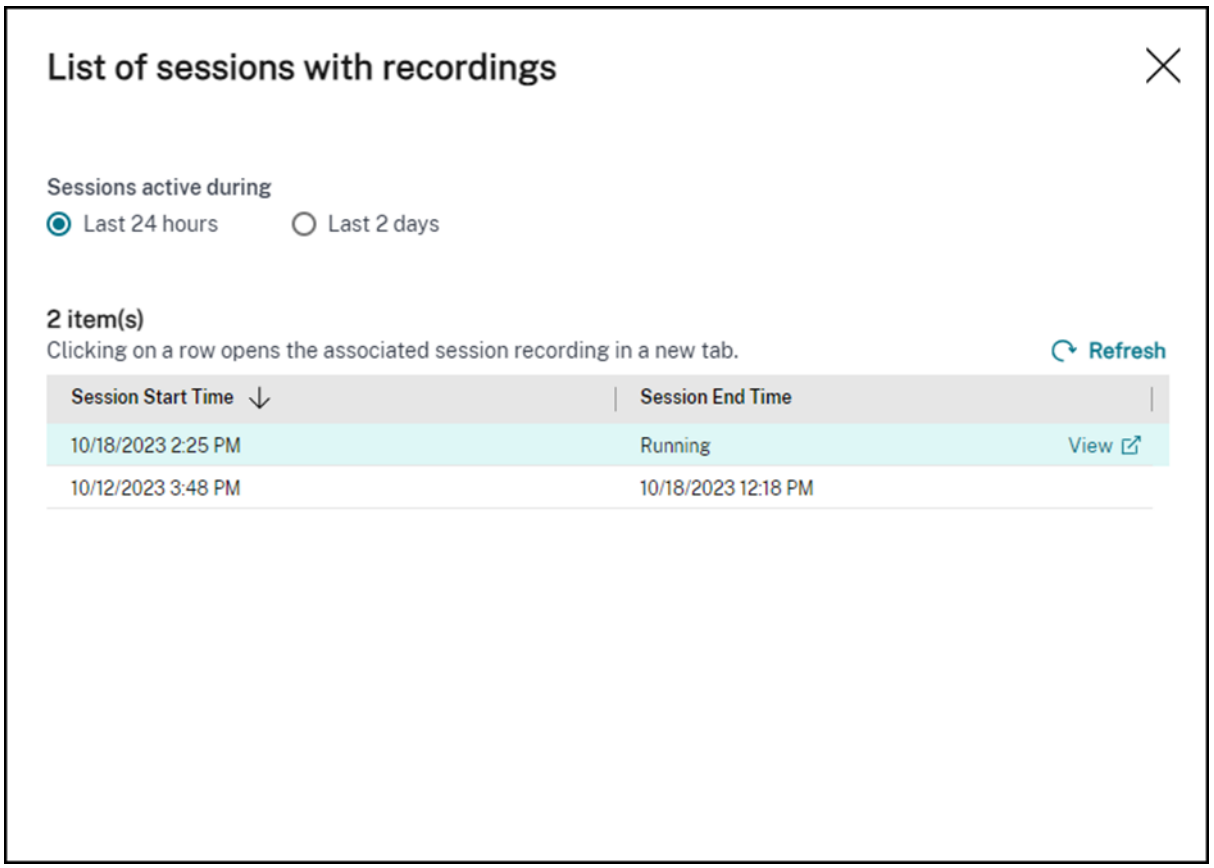
この機能には、以下が必要です:

- VDA および Session Recording サーバーがバージョン 2308 以降である。
- Delivery Controller と Director がバージョン 2311 以降である。

Director は、セッションの録画を集中リポジトリに保存します。セッションのセレクタモーダル > ［録画のあるセッション］リンクをクリックすると、そのユーザーに属する録画の一覧が表示されます。



過去 24 時間または過去 2 日間にアクティブだったセッションの録画を表示することを選択できます。現在アクティブなセッションのライブ録画には、［セッション終了時間］が ［実行中］としてマークされます。



［表示］リンクをクリックし、Citrix Session Recording 再生サーバーを使用して新しいタブで録画を再生します。

機能の互換性マトリックス

August 17, 2024

Citrix Director 7 2203 は以下の製品と互換性があります:

- Citrix Virtual Apps and Desktops 7 2112 以降
- Citrix Virtual Apps and Desktops 7 1912 LTSR

各サイトでは、Delivery Controller の以前のバージョンとともに Director を使用できますが、Director の最新バージョンの機能の一部が使用できない場合があります。Citrix では Director、Delivery Controller、VDA は同じバージョンを使用されることをお勧めします。

> 注:
>
> Delivery Controller のアップグレード後に Studio を開くと、サイトのアップグレードを要求するメッセー

> ジが表示されます。詳しくは、「アップグレードの順序」（「環境のアップグレード」セクション）を参照してください。

Director のアップグレード後に初めてログオンすると、設定されたサイトでバージョンチェックが実行されます。いずれかのサイトで Director のバージョンよりも前のバージョンの Controller が実行されている場合は、Director のコンソールにメッセージが表示され、サイトのアップグレードが推奨されます。また、サイトのバージョンが Director のバージョンより古い場合は、この不一致を示す通知が Director のダッシュボードに表示されたままになります。

> 注:
>
> 以前のバージョンの Citrix Director では、最新バージョンの VDA で実行中のユーザーセッションに適用されるポリシーが表示されません。Citrix Director 1912 以前のバージョンでは、VDA バージョン 2003 以降で実行中のユーザーセッションに適用されるポリシーが表示されません。これらのポリシーを表示するには、Citrix Director バージョン 2003 以降を使用してください。

Director の特定の機能と、Delivery Controller（DC）、VDA、およびライセンスエディションとともに必要なその他の従属コンポーネントの最小バージョンを次に示します。

Director のバージョン	機能	依存関係 - 必要な最小バージョン	エディション
2311	ライブセッションと録画されたセッションを再生する	VDA 2308 および Desktop Delivery Controller 2311	すべて
2311	セッションのトポロジ	なし	すべて
2311	最適な画面解像度	なし	すべて
2311	MS Teams の最適化	VDA 2311 および Desktop Delivery Controller の最新バージョン	すべて
2311	プローブの概要の機能強化	なし	すべて
2311	刷新されたセッションのログオン期間ビュー	なし	すべて
2308	プローブの概要とドリルダウン	なし	すべて
2308	Citrix Gateway の多要素認証に対する Citrix Probe Agent のサポート	Citrix Gateway	すべて

Director のバージョン	機能	依存関係 - 必要な最小バージョン	エディション
2308	ハイパーバイザー通知の無効化	なし	すべて
2308	セッションエクスペリエンス指標の傾向	なし	すべて
2305	Citrix Gateway 経由の認証をサポート	なし	すべて
2305	Director での Autoscale 管理	なし	すべて
2303	障害が発生したマシンアラート	DC 7 2303	Premium
2203	TLS 1.3 のサポート	-	すべて
2212	AMD GPU で利用可能なリアルタイム GPU 使用率	DC 7.14 および VDA 7.14。64 ビット Windows を実行し、HDX 3D Pro が有効になっている	すべて
2212	高度なプローブスケジュール設定	DC 7 1906 および Citrix Probe Agent 2209	Premium
1909	Citrix Analytics for Performance を使用したオンプレミスサイトの構成	DC 7 1906 および VDA 1906	すべて
1906	セッションの自動再接続	DC 7 1906 および VDA 1906	すべて
1906	セッションの開始時間	DC 7 1906 および VDA 1903	すべて
1906	デスクトッププロービング	DC 7 1906 および Citrix Probe Agent 1903	Premium
7.9 以降	Citrix Profile Management のプロファイルのロード時間	VDA 1903	すべて
1811	プロファイルのドリルダウン	DC 7 1811 および VDA 1811	すべて
1811	ハイパーバイザーアラートの監視	DC 7 1811	Premium

Director のバージョン	機能	依存関係 - 必要な最小バージョン	エディション
1811	アプリケーションプロービング	DC 7 1811 および Citrix Application Probe Agent 1811	Premium
1811	Microsoft RDS ライセンスの正常性	DC 7 1811 および VDA 7.16	すべて
1811	RTOP の主要データの表示	DC 7 1811 および VDA 1808	Premium
1808	フィルターデータのエクスポート	DC 7 1808	すべて
1808	対話型セッションのドリルダウン	DC 7 1808 および VDA 1808	すべて
1808	GPO のドリルダウン	DC 7 1808 および VDA 1808	すべて
1808	OData API を使用したマシン履歴データの取得	DC 7 1808	すべて
7.18	アプリケーションプロービング	DC 7.18	Premium（旧称 Platinum）
7.18	スマートアラートポリシー	DC 7.18	Premium（旧称 Platinum）
7.18	Health Assistant リンク	なし	すべて
7.18	対話型セッションのドリルダウン	なし	すべて
7.17	PIV スマートカード認証	なし	すべて
7.16	アプリケーション分析	DC 7.16 および VDA 7.15	すべて
7.16	OData API V.4	DC 7.16	すべて
7.16	Linux VDA ユーザーのシャドウ	VDA 7.16	すべて
7.16	ドメインローカルグループのサポート	なし	すべて
7.16	マシンコンソールへのアクセス	DC 7.16	すべて
7.15	アプリケーション障害の監視	DC 7.15 および VDA 7.15	すべて

Director のバージョン	機能	依存関係 - 必要な最小バージョン	エディション
7.14	アプリケーションを中心としたトラブルシューティング	DC 7.13 および VDA 7.13	すべて
7.14	ディスクの監視	DC 7.14 および VDA 7.14	すべて
7.14	GPU の監視	DC 7.14 および VDA 7.14	すべて
7.13	［セッション詳細］パネル上のトランスポート プロトコル	DC 7.x および VDA 7.13	すべて
7.12	ユーザーフレンドリな接続およびマシンの障害の説明	DC 7.12 および VDA 7.x	すべて
7.12	Enterprise Edition での履歴データ提供期間の延長	DC 7.12 および VDA 7.x	Enterprise
7.12	カスタムレポート	DC 7.12 および VDA 7.x	Premium（旧称 Platinum）
7.11	リソース使用レポート	DC 7.11 および VDA 7.11	すべて
7.11	CPU、メモリ、ICA RTT 条件に対応するアラート拡張	DC 7.11 および VDA 7.11	Premium（旧称 Platinum）
7.11	エクスポートレポートの改善	DC 7.11 および VDA 7.x	すべて
7.11	Citrix ADM との統合	DC 7.11、VDA 7.x、および MAS バージョン 11.1 ビルド 49.16	Premium（旧称 Platinum）
7.9	ログオン処理時間の内訳	DC 7.9 および VDA 7.x	すべて
7.7	予見的な監視およびアラート	DC 7.7 および VDA 7.x	Premium（旧称 Platinum）
7.7	Windows 認証の統合	DC 7.x および VDA 7.x	すべて
7.7	シングルセッション OS およびマルチセッション OS の使用	DC 7.7 および VDA 7.x	Premium（旧称 Platinum）
7.6.300	Framehawk 仮想チャネルのサポート	DC 7.6 および VDA 7.6	すべて
7.6.200	セッション記録の統合	DC 7.6 および VDA 7.x	Premium（旧称 Platinum）

Director のバージョン	機能	依存関係 - 必要な最小バージョン	エディション
7	HDX Insight 統合	DC 7.6、VDA 7.x、および Citrix ADM	Premium（旧称 Platinum）

データの粒度と保持

August 17, 2024

データ値の集計

Monitor Service は、ユーザーセッション使用状況、ユーザーログオンの処理性能の詳細、セッションの負荷分散の詳細、および接続とマシンのエラー情報を含む、さまざまなデータを収集します。データはカテゴリにより異なる方法で集計されます。OData Method API を使って示されたデータ値の集計を理解することは、データの解釈に不可欠です。例:

- 接続セッション（Connected Session）やマシンエラー（Machine Failure）は一定の期間の状態を示すため、その期間内の最大値として公開されます。
- ログオン期間（LogOn Duration）は時間の長さを示す指標であるため、期間内の平均として公開されます。
- ログオン数（LogOn Count）および接続障害（Connection Failure）は一定の期間に発生した数を示し、期間内の合計値として公開されます。

同時データ評価

重複しているセッションは同時発生していると考える必要があります。ただし、時間間隔が 1 分の場合、その 1 分内のすべてのセッションが（重複していても重複していなくても）同時と見なされます。この間隔のサイズは非常に小さいため、精度の計算に関連するパフォーマンス上のオーバーヘッドを考慮する必要はありません。2 つのセッションがその 1 時間内の別々の 1 分間に発生する場合、それらは重複しているとはみなされません。

サマリー表と生データの相関

データモデルでは、以下の 2 つの方法でメトリックが示されます:

- サマリーテーブルでは、分単位、時間単位、および日単位のメトリックを集計したものが示されます。
- 生データは、セッション、接続、アプリケーション、およびそのほかのオブジェクト内で記録された個々のイベントまたは現在の状態を示します。

データを API コール間またはそのデータモデル内で関連付けるときは、以下の概念および制限事項を考慮してください。

- 未完の間隔にはサマリーデータがありません。メトリックサマリーは長時間での履歴傾向を示すためのものであり、完結した間隔のサマリーテーブルに集計されます。データ収集の開始時（利用可能な最も古いデータ）や終了時の未完の間隔のサマリーデータはありません。これは、1 日（間隔 =1440）の集計値の場合、最初と最後の未完の 1 日にはデータがないことを意味します。これらの未完の間隔に生データが存在しても、そのデータが集計されることはありません。各データ粒度の最初と最後の集計間隔は、各サマリーテーブルから最小と最大の SummaryDate を取得することで決定できます。SummaryDate 列は、間隔の開始時を示します。Granularity 列はその集計データの間隔の長さを示します。
- 時間による関連付け。前のセクションで説明したように、メトリックスは完結した間隔のサマリーテーブルに集計されます。これらの値は履歴傾向を知る目的で使用できますが、生イベントの方が集計された値よりも傾向分析に適切な状態を示している場合があります。要約データと生データの時間ベースの比較では、発生する可能性のある部分区間、または期間の開始と終了の要約データがないことを考慮する必要があります。
- 欠落イベントまたは潜在イベント集計期間で欠落または潜在しているイベントがあると、サマリーテーブルに集計されたメトリックが正確でない場合があります。Monitor Service では現在の状態の正確な維持が試行されますが、過去にさかのぼって欠落イベントや潜在イベントをサマリーテーブルに再集計することはありません。
- 接続の高可用性。接続の高可用性により、現在の接続のサマリーデータ数に差異が生じることがありますが、セッションインスタンスは生データ内で実行されています。
- データの保持期間。サマリーテーブルのデータは、生イベントデータとは異なるグルーミングスケジュールで保持されます。このため、サマリーテーブルまたは生テーブルのクリーンアップにより、データが消去されている場合があります。データの保有期間は、サマリーデータの粒度によっても異なる場合があります。低い粒度（分単位）のデータは、高い粒度（日単位）のデータよりも早くクリーンアップされます。特定の粒度のデータが消去されていても、より高い粒度のデータが存在している場合があります。API コールでは指定した粒度のデータのみが返されるため、データを取得できない場合でもその期間内のより高い粒度では取得できることがあります。
- タイムゾーン。格納されるメトリックのタイムスタンプでは UTC が使用されます。サマリーテーブルは 1 時間区切りのタイムゾーンごとに集計されます。1 時間区切りのタイムゾーンに属さない場合は、データの集計先に不整合が生じることがあります。

データの粒度と保持

Director で取得される集計データの粒度は、要求された時間（T）の関数です。以下の規則があります。

- 0 < T <= 1 時間 - 分単位の粒度
- 0 < T <= 30 日 - 時間単位の粒度
- T > 31 日 - 日単位の粒度

集計データから取得されないデータを要求すると、生のセッション（Session）および接続（Connection）情報から取得されます。このデータの量はすぐに大きくなるため、専用のスケジュールでクリーンアップされます。クリーン

アップにより、意味のあるデータのみが長期間保持されます。また、レポートに必要な粒度を維持しながら良好なパフォーマンスが提供されます。Premium Edition では、クリーンアップ保持を必要な保持日数に変更できます。変更しない場合にはデフォルト値が使用されます。サイト構成データベースとの接続が切れた場合、Monitor Service は、以下の表に指定されている Premium 資格のデフォルトの保持日数を使用します:

設定にアクセスするには、Delivery Controller で以下の PowerShell コマンドを実行します:

```
asnp Citrix.*
 Get-MonitorConfiguration
 Set-MonitorConfiguration -<setting name> <value>
```

	設定名	対象データ	Premium の保持日数	Advanced の保持日数
1	GroomSessionsRetentionDays	セッションの終了から 7 日後のセッションレコードと接続レコードの保有	90	31
2	GroomFailuresRetentionDays	MachineFailureLog レコードおよび ConnectionFailureLog レコード	90	31
3	GroomLoadIndexesRetentionDays	LoadIndex レコード	90	31

	設定名	対象データ	Premium の保持日数	Advanced の保持日数
4	GroomDeletedRetentionDays	LifecycleState が「Deleted」である Machine エンティティ、Catalog エンティティ、DesktopGroup エンティティ、および Hypervisor エンティティ。この設定により、関連する Session レコード、SessionDetail レコード、Summary レコード、Failure レコード、または LoadIndex レコードも削除されます。	90	31
5	GroomSummariesRetentionDays	DesktopGroupSummary レコード、FailureLogSummary レコード、および LoadIndexSummary レコード。集計データ（日単位）	365	31
6	GroomMachineHotfixLogRetentionDays	VDA および Controller マシンに適用された Hotfix	90	31

	設定名	対象データ	Premium の保持日数	Advanced の保持日数
7	GroomMinuteRetentionDays	集計データ（分単位）	3	3
8	GroomHourlyRetentionDays	集計データ（時間単位）	32	31
9	GroomApplicationInstanceRetentionDays	アプリケーションインスタンスの履歴	90	該当なし
10	GroomNotificationLogRetentionDays	通知ログ	90	該当なし
11	GroomResourceUsageRawDataRetentionDays	Usage 機能の生データ（生データ）	3	3
12	GroomResourceUsageMinuteDataRetentionDays	Usage 機能のサマリーデータ（分単位）	7	7
13	GroomResourceUsageHourDataRetentionDays	Usage 機能の概要データ（時間単位）	30	30
14	GroomResourceUsageDayDataRetentionDays	Usage 機能の概要データ（日単位）	365	31
15	GroomProcessUsageRawDataRetentionDays	アプリ使用状況の生データ（生データ）	1	1
16	GroomProcessUsageMinuteDataRetentionDays	アプリ使用状況のデータ（分単位）	3	3
17	GroomProcessUsageHourDataRetentionDays	アプリ使用状況のデータ（時間単位）	7	7
18	GroomProcessUsageDayDataRetentionDays	アプリ使用状況のデータ（日単位）	30	30
19	GroomSessionMetricsDataRetentionDays	セッションのメトリックデータ	1	1
20	GroomMachineMetricDataRetentionDays	マシンのメトリクデータ	3	3
21	GroomMachineMetricDaySummaryDataRetentionDays	マシンのメトリクサマリーデータ	365	31

	設定名	対象データ	Premium の保持日数	Advanced の保持日数
22	GroomApplicationErrorsRetentionDays	アプリケーションエラーデータ	1	1
23	GroomApplicationFaultsRetentionDays	アプリケーション障害データ	1	1

> 注意:
>
> Monitor Service データベースの値を変更した後でその値を適用するには、このサービスを再起動する必要があります。Monitor Service データベースの値の変更は、Citrix サポート担当者からの指示があった場合のみ行ってください。

GroomProcessUsageRawDataRetentionDays、GroomResourceUsageRawDataRetentionDays、および GroomSessionMetricsDataRetentionDays の設定はデフォルト値の 1 に制限されていますが、GroomProcessUsageMinuteDataRetentionDays はデフォルト値の 3 に制限されています。プロセス使用データが急速に増加する傾向があるため、これらの値を設定する PowerShell コマンドは無効になっています。
また、以下はライセンスごとのその他の保持設定です:

- **Premium** ライセンスがあるサイト - すべての設定のクリーンアップ保持が 1000 日間に制限されます (Citrix では 365 日を推奨)。
- **Advanced** ライセンスがあるサイト - すべての設定のクリーンアップ保持が 31 日間に制限されます。
- その他すべてのサイト - すべての設定のクリーンアップ保持が 7 日間に制限されます。

例外:

- GroomApplicationInstanceRetentionDays は、Premium ライセンスがあるサイトにのみ設定できます。
- GroomApplicationErrorsRetentionDays および GroomApplicationFaultsRetentionDays は、Premium ライセンスがあるサイトでは 31 日間の制限があります。

データを長期間保持すると、テーブルのサイズについて以下の影響が発生します:

- 時間単位のデータ。時間単位のデータを 2 年などの長期間保持すると、1000 個のデリバリーグループがあるサイトではデータベースが以下の数式に基づいて増大します:

  「1000 個のデリバリーグループ ×24 時間/日 ×365 日/年 ×2 年＝ 17,520,000 行のデータ」集計テーブルのデータ量が多いため、パフォーマンスに大きな影響を及ぼします。ダッシュボードのデータがこのテーブルから取得されると、データベースサーバーに対する要求が高くなることがあります。データ量が過度に多いと、パフォーマンスが大きく低下することがあります。

- セッションとイベントのデータ。各セッションの開始時および接続/再接続時に収集されるデータです。大規模サイト（100,000 ユーザーなど）では、このデータの量が急速に増加します。たとえば、これらのテーブルでは 2 年間で 1TB 以上のデータが保持され、高性能なエンタープライズレベルのデータベースが必要になります。

Citrix Director の失敗の原因とトラブルシューティング

August 17, 2024

次の表に、さまざまな失敗のカテゴリ、理由、および問題を解決するために必要なアクションを示します。詳しくは、「列挙型、エラーコード、および説明」を参照してください。

接続失敗エラー

カテゴリ	理由	問題	アクション
-	[0] Unknown. このエラーコードはマッピングされていません。	Monitoring Service は、Broker Service によって共有された情報からは、報告された起動または接続エラーの理由を判別できません。	コントローラーで CDF ログを収集し、Citrix サポートに連絡してください。
[0] None	[1] None	なし	-
[2] MachineFailure	[2] SessionPreparation	Delivery Controller から VDA へのセッション準備要求が失敗しました。考えられる原因: Delivery Controller と VDA 間の通信の問題、準備要求の作成中に Broker Service で発生した問題、または VDA が要求を受け入れない結果となるネットワークの問題。	コントローラーと VDA 間の通信の問題を引き起こす一般的な問題については、Knowledge Center の記事「Citrix Virtual Apps and Desktops における Deliver Controller を使用した Virtual Delivery Agent 登録のトラブルシューティング」に記載されているトラブルシューティング手順を参照してください。

カテゴリ	理由	問題	アクション
[2] MachineFailure	[3] RegistrationTimeout	VDA の電源は入っていますが、Delivery Controller を使用した登録を試行中にタイムアウトしました。	Citrix Broker Service が Delivery Controller 上で実行されており、Desktop Service が VDA 上で実行されていることを確認します。停止している場合は、起動してください。
[1] ClientConnection-Failure	[4] ConnectionTimeout	VDA がセッションの起動のために準備された後、クライアントがその VDA に接続しませんでした。セッションは正常に仲介されましたが、クライアントが VDA に接続するのを待っている間にタイムアウトが発生しました。考えられる原因：ファイアウォール設定、ネットワークの中断、またはリモート接続を妨げる設定。	Director コンソールをチェックして、クライアントに現在アクティブな接続があるかどうかを確認します。これは、ユーザーに影響がないことを確認するためです。セッションが存在しない場合は、クライアントと VDA のイベントログでエラーを確認します。クライアントと VDA 間のネットワーク接続の問題を解決します。
[4] NoLicensesAvailable	[5] Licensing	ライセンス要求に失敗しました。考えられる原因：ライセンスの数が不足しているか、ライセンスサーバーが 30 日以上ダウンしています。	ライセンスサーバーがオンラインかつ到達可能な状態であることを確認します。ライセンスサーバーへのネットワーク接続の問題を解決するか、ライセンスサーバーが誤動作していると思われる場合はライセンスサーバーを再起動します。環境に必要な数のライセンスがあり、必要であれば割り当てが可能なことを確認します。

カテゴリ	理由	問題	アクション
[1] ClientConnection-Failure	[6] Ticketing	チケット作成中にエラーが発生しました。VDA へのクライアント接続が仲介した要求に一致しません。起動要求チケットは Broker によって準備され、ICA ファイルで配信されます。ユーザーがセッションを起動しようとすると、VDA が Broker を使用して ICA ファイル内の起動チケットを検証します。考えられる原因：ICA ファイルが破損しているか、ユーザーが不正な接続を試みています。	デリバリーグループで定義されたユーザーグループに基づいて、ユーザーがアプリケーションまたはデスクトップにアクセスできることを確認します。これが 1 回限りの問題であるかどうかを判断するために、アプリケーションまたはデスクトップを再起動するようにユーザーに指示します。問題が再度発生する場合は、クライアントデバイスのイベントログでエラーを確認します。ユーザーが接続しようとしている VDA が登録済みであることを確認します。登録されていない場合は、VDA のイベントログを確認し、登録の問題を解決します。
[1] ClientConnection-Failure	[7] Other	クライアントが最初に VDA に接続を試行してから接続シーケンスが完了する前に、VDA でセッションが終了したことが報告されました。	起動前にユーザーがセッションを終了していないことを確認します。セッションを再起動してください。問題が解決しない場合は、CDF ログを収集して Citrix サポートに連絡してください。
[1] ClientConnection-Failure	[8] GeneralFail	セッションを起動できませんでした。考えられる原因：ブローカーの起動中または初期化中に、仲介される起動が要求されたか、起動の仲介フェーズ中に内部エラーが発生しました。	Citrix Broker Service が実行されていることを確認して、セッションの起動を再試行します。

カテゴリ	理由	問題	アクション
[5] Configuration	[9] MaintenanceMode	VDA、または VDA が属するデリバリーグループはメンテナンスモードに設定されています。	メンテナンスモードが必要かどうかを判断します。必要がなければ、対象のデリバリーグループまたはマシンでメンテナンスモードを無効にして、再接続するようユーザーに指示します。
[5] Configuration	[10] ApplicationDisabled	アプリケーションが管理者によって無効にされているため、エンドユーザーがアプリケーションにアクセスできません。	アプリケーションが実稼働で使用するよう設定されている場合は、アプリケーションを有効にして再接続するようユーザーに指示します。
[4] NoLicensesAvailable	[11] LicenseFeature Refused	使用中の機能が既存のライセンスでカバーされていません。	Citrix の営業担当者に連絡して、Citrix Virtual Apps and Desktops の既存のライセンスエディションおよびライセンス種類でカバーされている機能を確認してください。
[3] NoCapacityAvailable	[13] SessionLimitReached	すべての VDA が使用中であるため、追加のセッションをホストする容量はありません。考えられる原因: すべての VDA が使用中である（シングルセッション OS VDA の場合）、またはすべての VDA が設定した最大同時セッション数に達しています（マルチセッション OS VDA の場合）。	メンテナンスモードの VDA があるかどうかを確認します。さらに容量を解放する必要がない場合は、メンテナンスモードを無効にします。Citrix ポリシー設定で ［セッションの上限数］の値を増やすと、サーバーの VDA ごとにさらにセッションを追加できます。マルチセッション OS VDA を追加できます。シングルセッション OS VDA を追加できます。

カテゴリ	理由	問題	アクション
[5] Configuration	[14] DisallowedProtocol	ICA および RDP プロトコルは許可されていません。	Delivery Controller で PowerShell コマンドの「**Get-BrokerAccessPolicyRule**」を実行し、[**AllowedProtocols**] の値にすべての必要なプロトコルがあることを確認します。この問題は、構成に誤りがある場合にのみ発生します。
[5] Configuration	[15] ResourceUnavailable	ユーザーが接続しようとしているアプリケーションまたはデスクトップが利用できません。このアプリケーションまたはデスクトップが存在しないか、実行できる VDA がない可能性があります。考えられる原因: アプリケーションまたはデスクトップが公開されていないか、アプリケーションまたはデスクトップをホストしている VDA が負荷上限に達しているか、アプリケーションまたはデスクトップがメンテナンスモードに設定されています。	アプリケーションまたはデスクトップが公開されていることと、VDA がメンテナンスモードになっていないことを確認します。マルチセッション OS VDA が負荷限界に達しているかどうかを確認します。達している場合は、追加でマルチセッション OS VDA をプロビジョニングします。接続に使用できるシングルセッション OS VDA があることを確認します。必要に応じて、追加でシングルセッション OS VDA をプロビジョニングします。
[5] Configuration	[16] ActiveSessionReconnectDisabled	ICA セッションがアクティブであり、別のエンドポイントに接続されています。ただし、[アクティブセッションの再接続] が無効になっているため、クライアントがアクティブセッションに接続できません。	Delivery Controller で、[アクティブセッションの再接続] が有効になっていることを確認します。**HKEY_LOCAL_MACHINE\Software** で、レジストリの **DisableActiveSessionReconnect** の値が 0 に設定されていることを確認します。

カテゴリ	理由	問題	アクション
[2] MachineFailure	[17] NoSessionToReconnect	クライアントが特定のセッションに再接続しようとしましたが、セッションが終了しています。	ワークスペースコントロールの再接続を再試行します。
[2] MachineFailure	[18] SpinUpFailed	セッション起動のためにVDA の電源をオンにしようとしてもオンにならない。これはハイパーバイザーで報告された問題です。	まだマシンの電源がオフになっている場合は、Citrix Studio からマシンを起動してみます。起動に失敗した場合は、ハイパーバイザーの接続とアクセス権限を確認してください。VDA が PVS でプロビジョニングされたマシンである場合は、PVS コンソールでマシンが実行されていることを確認します。そうでない場合は、マシンに Personal vDisk が割り当てられていることを確認し、ハイパーバイザーにログインして VM をリセットします。
[2] MachineFailure	[19] Refused	Delivery Controller がエンドユーザーからの接続を準備するための要求をVDA に送信しますが、VDA はアクティブにこの要求を拒否します。	ping を使用して、Delivery Controller と VDA が正常に通信できることを確認します。正常に通信できていない場合は、ファイアウォールまたはネットワークルーティングの問題を解決します。

カテゴリ	理由	問題	アクション
[2] MachineFailure	[20] ConfigurationSet Failure	Delivery Controller が、セッション起動中の VDA にポリシー設定やセッション情報などの必要な構成データを送信しませんでした。考えられる原因: Delivery Controller と VDA 間の通信の問題と VDA 間の通信の問題、構成セット要求の作成中に Broker Service で発生した問題、または VDA が要求を受け入れない結果となるネットワークの問題。	-
[3] NoCapacityAvailable	[21] MaxTotalInstance-sExceeded	アプリケーションのインスタンス数上限に達しました。アプリケーションの追加のインスタンスを VDA で開くことができません。この問題は、アプリケーションの上限機能に関連しています。	ライセンスで可能な限り、アプリケーション設定の［同時に実行されるインスタンスの上限数］をより高い値に設定できます。
[3] NoCapacityAvailable	[22] MaxPerUserIn-stancesExceeded	ユーザーがアプリケーションで複数のインスタンスを開こうとしていますが、アプリケーションがユーザーごとに 1 つのインスタンスのみを許可するよう構成されています。この問題は、アプリケーションの上限機能に関連しています。	デフォルトでは、アプリケーションのインスタンスはユーザーごとに 1 つだけ許可されます。ユーザーごとに複数のインスタンスが必要な場合は、アプリケーション設定の ［ユーザーごとに **1** つのインスタンスに制限します］をオフにします。

カテゴリ	理由	問題	アクション
[1] ClientConnection-Failure	[23] Communication error	Delivery Controller が、接続を準備する要求などの情報を VDA に送信しようとしていますが、通信の試行中にエラーが発生しました。これは、ネットワークの中断によって発生した可能性があります。	既に開始されている場合は、VDA でデスクトップサービスを再起動して登録プロセスを再開し、VDA が正常に登録されることを確認します。アプリケーションイベントログの詳細を確認し、VDA 用に構成された Delivery Controller が正確であることを確認します。
[3] NoCapacityAvailable	[100] NoMachineAvailable Monitoring service converts [12] NoDesktopAvailable to this error code.	セッションの起動に割り当てられた VDA は、無効な状態か使用することができません。考えられる原因: VDA の電源状態が不明または使用できない、最後のユーザーのセッション以降 VDA が再起動しなかった、現在のセッションで有効にする必要があるセッション共有が無効になっている、または VDA が配信グループまたはサイトから削除された。	VDA がデリバリーグループにあることを確認します。ない場合は、適切なデリバリーグループに追加します。十分な数の VDA がデリバリーグループに存在し、ユーザーの要求により公開済みの共有デスクトップまたはアプリケーションを起動する準備ができた状態であることを確認します。VDA をホストしているハイパーバイザーがメンテナンスモードになっていないことを確認します。

カテゴリ	理由	問題	アクション
[2] MachineFailure	[101] MachineNotFunctional. Monitoring Service が「[12] NoDesktopAvailable」をこのエラーコードに変換します。	VDA は動作していません。考えられる原因：VDA がデリバリーグループから削除された、VDA が登録されていない、VDA の電源の状態が使用不可になっている、または VDA で内部の問題が発生しています。	VDA がデリバリーグループにあることを確認します。ない場合は、適切なデリバリーグループに追加します。Citrix Studio で VDA が電源オンとして表示されていることを確認します。複数のマシンの電源の状態が不明な場合は、ハイパーバイザーへの接続の問題またはホストの障害を解決します。VDA をホストしているハイパーバイザーがメンテナンスモードになっていないことを確認します。これらの問題が解決されたら、VDA を再起動します。

マシンエラーの種類

エラーコード	エラーコード ID	問題	アクション
不明	-	-	-
未登録	3	-	-
MaxCapacity（Director で［最大負荷］として表示されます）	4	マシンは最大容量（最大負荷のインデックス）で報告します。	すべてのハイパーバイザーの電源が入っていることを確認してください。ハイパーバイザーの容量を追加するか、ハイパーバイザーを追加することにより、影響を受けるデリバリーグループにマシンを追加します。

エラーコード	エラーコード ID	問題	アクション
起動時にスタック	2	仮想マシンの起動シーケンスが完了しませんでした。ハイパーバイザーと通信していません。	VM がハイパーバイザーで正常に起動したことを確認します。OS の問題など、仮想マシン上の他のメッセージを確認します。ハイパーバイザーツールが仮想マシンにインストールされていることを確認してください。VDA が仮想マシンにインストールされていることを確認してください。
起動に失敗	1	ハイパーバイザーで仮想マシンの起動中に問題が発生しました。	ハイパーバイザーログをチェックします。
なし	0	-	-

マシンの登録解除の理由（エラーの種類が **Unregistered** または **Unknown** の場合に適用されます）

エラーコード	エラーコード ID	問題	アクション
AgentShutdown	0	VDA は、正常にシャットダウンされました。	既存の電源管理ポリシーに基づいて、VDA のオフ状態を予期していない場合は VDA の電源をオンにします。イベントログでエラーを確認します。
AgentSuspended	1	VDA は休止状態またはスリープモードです。	VDA の休止状態モードを解除します。Citrix Virtual Apps and Desktops VDA の電源設定で、休止状態を無効にすることができます。
IncompatibleVersion	100	Citrix のプロトコルバージョンが一致しないため、VDA が Delivery Controller と通信できません。	VDA と Delivery Controller のバージョンを揃えます。

エラーコード	エラーコード ID	問題	アクション
AgentAddressResolutionFailed	101	Delivery Controller が、VDA の IP アドレスを解決できませんでした。	Active Directory（AD）に VDA マシンアカウントが存在することを確認します。存在しない場合は、作成します。DNS の VDA の名前と IP アドレスが正確であることを確認します。正確でない場合は、修正します。広範囲に及ぶ場合は、Delivery Controller の DNS 設定を検証します。`nslookup`コマンドを実行して、Delivery Controller から DNS 解決を確認します。
	101	Delivery Controller が、VDA の IP アドレスを解決できませんでした。	Active Directory（AD）に VDA マシンアカウントが存在することを確認します。存在しない場合は、作成します。DNS の VDA の名前と IP アドレスが正確であることを確認します。正確でない場合は、修正します。

エラーコード	エラーコード ID	問題	アクション
AgentNotContactable	102	Delivery Controller と VDA の間で通信の問題が発生しました。	ping を使用して、Delivery Controller と VDA が正常に通信できていることを確認します。通信できていない場合は、ファイアウォールまたはネットワークの問題を解決します。コントローラーと VDA 間の通信の問題を引き起こす一般的な問題については、Knowledge Center の記事「Citrix Virtual Apps and Desktops における Deliver Controller を使用した Virtual Delivery Agent 登録のトラブルシューティング（CTX136668）」に記載されているトラブルシューティング手順を参照してください。
	102	Delivery Controller と VDA の間で通信の問題が発生しました。	コントローラーと VDA 間の通信の問題を引き起こす一般的な問題については、Knowledge Center の記事「Citrix Virtual Apps and Desktops における Deliver Controller を使用した Virtual Delivery Agent 登録のトラブルシューティング（CTX136668）」に記載されているトラブルシューティング手順を参照してください。Citrix サポートに連絡してください。

エラーコード	エラーコード ID	問題	アクション
AgentWrongActiveDirectoryOU	103	Active Directory 検出の構成ミスが発生しました。VDA レジストリで構成済みのサイト固有の OU（サイトコントローラー情報が AD に格納されている場所）は、別のサイト用です。	Active Directory の構成が正しいことを確認します。またはレジストリ設定を確認します。
EmptyRegistrationRequest	104	VDA から Delivery Controller に送信された登録要求が空でした。これは、VDA ソフトウェアのインストールが破損していることが原因である可能性があります。	VDA でデスクトップサービスを再起動して、登録プロセスを再起動し、アプリケーションのイベントログで VDA が正しく登録されていることを確認します。
MissingRegistrationCapabilities	105	このバージョンの VDA は Delivery Controller と互換性がありません。	VDA をアップグレードするか、VDA を削除してから再インストールします。
MissingAgentVersion	106	このバージョンの VDA は Delivery Controller と互換性がありません。	問題がすべてのマシンに影響を与えている場合は、VDA ソフトウェアを再インストールします。
InconsistentRegistrationCapabilities	107	VDA が、その機能をブローカーに伝達できません。これは、VDA のバージョンと Delivery Controller のバージョンに互換性がないことが原因である可能性があります。登録機能は、各バージョンで異なり、登録要求と一致しない形式で表現されています。	VDA と Delivery Controller のバージョンを揃えます。
NotLicensedForFeature	108	使用を試みている機能のライセンスがありません。	Citrix のライセンスエディションを確認します。または、VDA を削除してから再インストールします。
	108	使用を試みている機能のライセンスがありません。	Citrix サポートに連絡してください。

エラーコード	エラーコード ID	問題	アクション
UnsupportedCredentialSecurityversion	109	VDA と Delivery Controller が、同じ暗号化メカニズムを使用していません。	VDA と Delivery Controller のバージョンを揃えます。
InvalidRegistrationRequest	110	VDA がブローカーに登録要求を行いましたが、登録要求の内容が破損しているか無効です。	コントローラーと VDA 間の通信の問題を引き起こす一般的な問題については、Knowledge Center の記事「Citrix Virtual Apps and Desktops における Deliver Controller を使用した Virtual Delivery Agent 登録のトラブルシューティング（CTX136668）」に記載されているトラブルシューティング手順を参照してください。
SingleMultiSessionMismatch	111	VDA のオペレーティングシステムの種類が、マシンカタログまたはデリバリーグループと互換性がありません。	正しいマシンカタログの種類に、または同じオペレーティングシステムのマシンを含むデリバリーグループに、VDA を追加します。
FunctionalLevelTooLowForCatalog	112	マシンカタログが、インストールされている VDA のバージョンよりも高い VDA の機能レベルに設定されています。	VDA のマシンカタログの機能レベルが、VDA の機能レベルと一致していることを確認します。マシンカタログをアップグレードまたはダウングレードして、VDA の機能レベルと一致させます。

エラーコード	エラーコード ID	問題	アクション
FunctionalLevelTooLowForDesktopGroup	199	デリバリーグループが、インストールされている VDA のバージョンよりも高い VDA の機能レベルに設定されています。	VDA のデリバリーグループの機能レベルが、VDA の機能レベルと一致していることを確認します。マシンカタログをアップグレードまたはダウングレードして、VDA の機能レベルと一致させます。
PowerOff	200	VDA が正常にシャットダウンされませんでした。	VDA の電源がオンになっているはずである場合は、Citrix Studio から VDA を起動して、起動と登録が正しく実行されることを確認してください。起動または登録の問題をトラブルシューティングします。シャットダウンの根本的な原因を特定するために VDA のイベントログをバックアップ後に確認します。
AgentRejectedSettingsUpdate	208	Citrix ポリシーなどの設定が変更または更新されましたが、VDA への更新の送信中にエラーが発生しました。これは、更新がインストールされている VDA のバージョンと互換性がない場合に発生することがあります。	必要な場合は、VDA をアップグレードします。適用された更新が VDA バージョンでサポートされているかどうかを確認します。
SessionPrepareFailure	206	ブローカーが、VDA で実行されているセッションの監査を完了しませんでした。	広範囲にわたる問題の場合は、Delivery Controller の Citrix Broker Service を再起動します。
	206	ブローカーが、VDA で実行されているセッションの監査を完了しませんでした。	Citrix サポートに連絡してください。

エラーコード	エラーコード ID	問題	アクション
ContactLost	207	Delivery Controller と VDA との接続が切断されました。これは、ネットワークの切断が原因である可能性があります。	Citrix Broker Service が Delivery Controller 上で実行されており、Desktop Service が VDA 上で実行されていることを確認します。停止している場合は、起動してください。既に開始されている場合は、VDA でデスクトップサービスを再起動して登録プロセスを再開し、VDA が正常に登録されることを確認します。アプリケーションイベントログの詳細を確認し、VDA 用に構成された Delivery Controller が正確であることを確認します。ping を使用して、Delivery Controller と VDA が正常に通信できていることを確認します。通信できていない場合は、ファイアウォールまたはネットワークの問題を解決します。
	207	Delivery Controller と VDA との接続が切断されました。これは、ネットワークの切断が原因である可能性があります。	デスクトップサービスが VDA で実行されていることを確認します。停止していた場合は、開始します。

エラーコード	エラーコード ID	問題	アクション
BrokerRegistrationLimitReached	201	Delivery Controller が、構成済みの同時に登録できる VDA 数の上限に達しました。デフォルトでは、Delivery Controller は同時に 10,000 個の VDA の登録を許可します。	Delivery Controller をサイトに追加するか、新しいサイトを作成することができます。**HKEY_LOCAL_MACHINE\Software** レジストリキーを使用して、Delivery Controller に同時に登録できる VDA の数を増やすことができます。詳しくは、Knowledge Center の記事「Citrix Virtual Apps and Desktops で使用されるレジストリキーエントリ（CTX117446）」を参照してください。この数を増やすと、Delivery Controller 用により多くの CPU とメモリーリソースが必要になる場合があります。
SettingsCreationFailure	208	ブローカーが、VDA に送信するための一連の設定と構成を構築しませんでした。ブローカーがデータを収集できない場合、登録は失敗し、VDA は未登録になります。	Delivery Controller のイベントログでエラーを確認してください。ログで特定の問題が明らかにならない場合は、Broker Service を再起動します。Broker Service を再起動したら、影響を受ける VDA で Desktop Service を再起動し、VDA が正常に登録されたことを確認します。

エラーコード	エラーコード ID	問題	アクション
	208	ブローカーが、VDA に送信するための一連の設定と構成を構築しませんでした。ブローカーがデータを収集できない場合、登録は失敗し、VDA は未登録になります。	影響を受ける VDA で Desktop Service を再起動し、VDA が正常に登録されたことを確認します。Citrix サポートに連絡してください。
SendSettingsFailure	204	ブローカーが、設定と構成のデータを VDA に送信しませんでした。ブローカーでデータを収集できるが送信はできないという場合、登録が失敗します。	単一の VDA に限定される場合、VDA の Desktop Service を再起動して再登録を強制し、アプリケーションイベントログで VDA が正常に登録されたことを確認します。表示されたエラーのトラブルシューティングを行います。コントローラーと VDA 間の通信の問題を引き起こす一般的な問題については、Knowledge Center の記事「Citrix Virtual Apps and Desktops における Deliver Controller を使用した Virtual Delivery Agent 登録のトラブルシューティング（CTX136668）」に記載されているトラブルシューティング手順を参照してください。
AgentRequested	2	不明なエラーが発生しました。	Citrix サポートに連絡してください。
DesktopRestart	201	不明なエラーが発生しました。	Citrix サポートに連絡してください。
DesktopRemoved	202	不明なエラーが発生しました。	Citrix サポートに連絡してください。
SessionAuditFailure	205	不明なエラーが発生しました。	Citrix サポートに連絡してください。

エラーコード	エラーコード ID	問題	アクション
UnknownError	300	不明なエラーが発生しました。	Citrix サポートに連絡してください。
RegistrationStateMismatch	302	不明なエラーが発生しました。	Citrix サポートに連絡してください。
不明	-	不明なエラーが発生しました。	Citrix サポートに連絡してください。

サードパーティ製品についての通知

August 17, 2024

Citrix Virtual Apps and Desktops のこのリリースには、次のドキュメントで規定された条件の元でライセンス提供されているサードパーティのソフトウェアが含まれている可能性があります:

- Citrix Virtual Apps and Desktops サードパーティ製品についての通知（PDF ダウンロード）
- Non-Commercial Software Disclosures For FlexNet Publisher 2017 (11.15.0.0)（PDF のダウンロード）（英語）
- FLEXnet Publisher Documentation Supplement Third Party および FlexNet Publisher 11.15.0 で使用されるオープンソースソフトウェア（PDF のダウンロード）（英語）

SDK および API

August 17, 2024

このリリースでは、複数の SDK および API を使用できます。SDK と API にアクセスするには、「Build anything with Citrix」に移動します。そこから、［**Citrix Workspace**］を選択して、Citrix Virtual Apps and Desktops とその関連コンポーネントのプログラミング情報にアクセスします。

> 注:
>
> Citrix Virtual Apps and Desktops SDK および Citrix グループポリシー SDK は、モジュールまたはスナップインとしてインストールできます。いくつかのコンポーネント SDK（Citrix Licensing、Citrix Provisioning、StoreFront など）は、スナップインのみを使用してインストールします。

この製品は、PowerShell のバージョン 3 から 5 までをサポートします。

Citrix Virtual Apps and Desktops SDK

この SDK は、Delivery Controller または Studio をインストールすると PowerShell モジュールとして自動的にインストールされます。これにより、スナップインを追加しなくても、この SDK のコマンドレットを使用できるようになります。（この SDK をスナップインとしてインストールする場合の手順は後で説明します。）

アクセス許可

シェルまたはスクリプトは、Citrix 管理者の権限を持つ ID を使用して実行する必要があります。Controller のローカル管理者グループのメンバーには、Citrix Virtual Apps または Citrix Virtual Desktops のインストールに必要な完全な管理権限が自動的に付与されますが、ローカル管理者アカウントを使うのではなく、適切な権限を持つ Citrix 管理者を作成することをお勧めします。

コマンドレットのアクセスと実行

1. PowerShell のシェルを開きます。Studio を開き、［**PowerShell**］タブを選択して ［**PowerShell** の起動］をクリックします。
2. スクリプト内で SDK コマンドレットを使用するには、PowerShell 実行ポリシーを設定する必要があります。PowerShell 実行ポリシーについては、Microsoft 社のドキュメントを参照してください。
3. （モジュールではなく）スナップインを使用する場合は、`Add-PSSnapin`（または`asnp`）コマンドレットを使用してスナップインを追加します。

   V1 と V2 は、スナップインのバージョンを示します。XenDesktop 5 スナップインはバージョン 1 です。Citrix Virtual Apps and Desktops、およびそれ以前の XenDesktop 7 バージョンのスナップインはバージョン 2 です。たとえば、Citrix Virtual Apps and Desktops スナップインをインストールするには、「`Add-PSSnapin Citrix.ADIdentity.Admin.V2`」と入力します。すべてのコマンドレットをインポートするには、次のように入力します: `Add-PSSnapin Citrix.*.Admin.V*`

これで、コマンドレットとヘルプファイルを使用できます。

- この SDK のヘルプファイルにアクセスするには、［カテゴリ］ ボックスの一覧で製品またはコンポーネントを選択してから、［**Citrix Virtual Apps and Desktops SDK**］を選択します。
- PowerShell のガイダンスについては、「Windows PowerShell Integrated Scripting Environment (ISE)」を参照してください。

グループポリシー **SDK**

Citrix グループポリシー SDK により、グループポリシーの設定およびフィルターを表示して構成できます。この SDK は、PowerShell プロバイダーを使用して、マシン、ユーザー設定、およびフィルターに対応する仮想ドライブを作成します。このプロバイダーは、`New-PSDrive`に対する拡張として表示されます。

Group Policy SDK を使用するには、Studio または Citrix Virtual Apps and Desktops SDK のいずれかをインストールする必要があります。

Citrix グループポリシーの PowerShell プロバイダーは、モジュールまたはスナップインとして利用できます。

- このモジュールを使用するために追加で作業が必要になることはありません。
- このスナップインを追加するには、「`Add-PSSnapin citrix.common.grouppolicy`」と入力します。

ヘルプにアクセスするには、「`help New-PSDrive -path localgpo:/`」と入力します。

仮想ドライブを作成して設定を読み込むには、「`New-PSDrive <Standard Parameters> [-PSProvider] CitrixGroupPolicy -Controller <string>`」と入力します。ここで、<string> は接続して設定を読み込むサイトの Controller の完全修飾ドメイン名です。

Citrix Virtual Apps and Desktops REST API

Citrix Virtual Apps and Desktops の REST API で、Citrix Virtual Apps and Desktops 展開のリソースの管理を自動化できます。

Citrix Virtual Apps and Desktops REST API はhttps://developer.cloud.com/citrixworkspace/citrix-daas-rest-apis/docs/citrix-virtual-apps-and-desktops-apisで入手できます。Citrix Virtual Apps and Desktops に適用できない API は、マークが付けられます。そのガイダンスに従って、API サービスへのアクセスを構成し、API を使用してリソースを管理および最適化します。

Monitor Service OData

Monitor API を使用すると、OData API のバージョン 3 または 4 を使用して Monitor Service データにアクセスできます。Monitor Service データからクエリされたデータに基づいて、カスタマイズした監視ダッシュボードおよびレポートダッシュボードを作成できます。OData V.4 は、ASP.NET Web APIに基づいており、アグリゲーションクエリをサポートしています。

詳しくは、「Monitor Service OData API」を参照してください。