シトリックス バーチャル アプリケーションズ アンド デスクトップ™ 7 2402 LTSR

> **重要:**
>
> Current Releases (CR) および Long Term Service Releases (LTSR) の製品ライフサイクル戦略については、ライフサイクルマイルストーンに記載されています。

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

Citrix Virtual Apps and DesktopsのLong Term Service Release (LTSR) プログラムは、Citrix Virtual Apps and Desktopsリリースに安定性と長期サポートを提供します。

Cumulative Update 2 (CU2) は、2402 LTSRの最新のアップデートです。LTSRは、Citrix Virtual Apps and Desktops 1912および2203でも利用可能です。

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

以前のリリース

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

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

Citrix Cloud™におけるシトリックス バーチャル アプリケーションズ アンド デスクトップ

Citrix Cloud Virtual Apps and Desktopsの提供はCitrix DaaSです。詳細については、Citrix DaaSを参照してください。

役立つリンク

- シトリックス サポービリティ パック
- LTSR FAQ
- Citrix Virtual Apps and Desktops サービスオプション
- 製品ライフサイクル日付
- Citrix Workspaceアプリ向けLTSRプログラム

新機能

累積更新プログラム 4 (CU4)

リリース日: May 08, 2026

このリリースについて

Citrix Virtual Apps and Desktops 7 2402 LTSR 累積更新プログラム 4 (CU4) は、2402 LTSR の初回リリース以降に報告された30を超える問題を修正します。

2402 LTSR (一般情報)

2402 LTSR (機能とアップグレード情報)

このリリースの新機能

Citrix Virtual Apps and Desktops 7 2402 LTSR (初回リリース) で修正された問題

このリリースの既知の問題

非推奨と削除

Citrix 製品サブスクリプションアドバンテージの対象期間

ダウンロード

シトリックス バーチャル アプリケーションズ アンド デスクトップス 7 2402 LTSR CU4

新規展開

CU4 をゼロから展開するにはどうすればよいですか?

CU4 メタインストーラーを使用して、CU4 に基づく新しい Citrix Virtual Apps and Desktops 環境をセットアップできます。その前に、製品についてよく理解しておくことをお勧めします。

展開を計画する前に、Citrix Virtual Apps and Desktops 7 2402 LTSR (初期リリース)セクションを熟読し、技術概要、インストールと構成、およびセキュリティの各セクションに特に注意してください。セットアップがすべてのコンポーネントのシステム要件を満たしていることを確認してください。

既存の展開

何を更新しますか?

CU4は、2402 LTSRの15のベースラインコンポーネントの更新を提供します。注意：Citrixは、展開のすべてのLTSRコンポーネントをCU4に更新することを推奨します。例：Citrix ProvisioningがLTSR展開の一部である場合、Citrix Provisioningコンポーネントを CU4に更新します。Citrix Provisioningが展開の一部でない場合、インストールまたは更新する必要はありません。

2402 LTSR CU4ベースラインコンポーネント

2402 CU4ベースラインコンポーネント	プログラムと機能に表示されるバージョン	ドキュメント
シングルセッションVDA	2402.0.4100.4597	シングルセッションVDA
マルチセッションVDA	2402.0.4100.4597	マルチセッションVDA
デリバリーコントローラー	2402.0.4100.4597	デリバリーコントローラー
シトリックス スタジオ	7.41.4100.46	シトリックス スタジオ
シトリックス ディレクター	7.41.4100.33	シトリックス ディレクター
Citrixグループポリシー管理	7.41.4100.40	Citrixグループポリシー管理
Citrixグループポリシー クライアント側拡張	7.41.4100.40	
シトリックス ストアフロント	2402.0.4100.21	Citrix ストアフロント
ユニバーサル プリント サーバー	7.41.4100.77	「ユニバーサルプリントサーバー」(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/printing/printing-provision-printers.html)
セッション録画	24.2.3100	「セッションレコーディング」(/ja-jp/session-recording.html)
リナックス VDA	24.02.1100.21	Linux 仮想配信エージェント(/ja-jp/linux-virtual-delivery-agent.html)

2402 CU4ベースラインコンポーネント	プログラムと機能に表示されるバージョン	ドキュメント
プロファイル管理	24.2.4100.23	「プロファイル管理」(/ja-jp/profile-management.html)
Citrix フェデレーション認証サービス	10.17.4100.21	Citrix フェデレーション認証サービス (FAS)(/ja-jp/federated-authentication-service/2402-ltsr.html)
ブラウザコンテンツリダイレクション	15.48.4100.78	「ブラウザコンテンツリダイレクション」(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/multimedia/browser-content-redirection.html)
Citrix プロブエージェント 2206	7.41.4100.20	ダウンロード

2402 LTSR CU4 互換コンポーネント

以下のコンポーネントは、記載されているバージョンでLTSR環境と互換性があります。これらはLTSRのメリット（延長されたライフサイクルと修正のみの累積更新プログラム）の対象ではありません。Citrix®は、2402環境内でこれらのコンポーネントを新しいバージョンにアップグレードするよう求める場合があります。

互換性のあるコンポーネントと機能	プログラムと機能に表示されるバージョン	ドキュメント
アプリレイヤリング	2206.0.0	Citrix アプリレイヤリング
HDX リアルタイム最適化パック	2.9.400.2702	HDX リアルタイム最適化パック
ライセンスサーバー	11.17.2.0_BUILD_55100	ライセンスサーバー(/ja-jp/licensing/11-17-2-48000/)
ユーザーパーソナライゼーションレイヤー	25.11.2	ユーザーパーソナライゼーションレイヤー(/ja-jp/citrix-virtual-apps-desktops/2402-

互換性のあるコンポーネントと機能	プログラムと機能に表示されるバージョン	ドキュメント
		ltsr/install-configure/user-personalization-layer.html)
セッションレコーディングウェブプレーヤー	24.2.4100.13	セッションレコーディングWebプレーヤー(/ja-jp/session-recording/2402-ltsr/view-recordings/session-recording-web-player.html)
Microsoft Teamsの最適化	15.32.1000.9	Microsoft Teamsの最適化(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/multimedia/opt-ms-teams.html)
ワークスペース環境管理	2507.1.110.1	ワークスペース環境管理
XenApp & XenDesktop 7.15 LTSR VDA (最新リリース)*	最新の累積更新プログラムのみ	ドキュメント
CVAD 2402 CUx Delivery Controller を使用して Windows Server 2025 にインストールされた VDA 2411 以降	2411.x.x.x	ドキュメント

2402 LTSR CU4 の主な除外事項

以下の機能、コンポーネント、およびプラットフォームは、2402 ライフサイクルマイルストーンおよび特典の対象外です。具体的には、累積更新プログラムと拡張ライフサイクル特典は除外されます。除外された機能およびコンポーネントの更新は、通常の最新リリースを通じて利用できます。

除外されるコンポーネントと機能
AppDisks™
AppDNA®
Citrix SCOM 管理パック

除外されるコンポーネントと機能
フレームホーク
パーソナル vDisk
StoreFront Citrix オンライン統合

除外される WINDOWS プラットフォーム *
Windows 2008 32ビット (ユニバーサル プリント サーバー用)

* Citrix は、サードパーティベンダーのライフサイクルマイルストーンに基づいてプラットフォームサポートを更新する権利を留保します。

新機能

以下の新機能と機能強化がCitrix Virtual Apps and Desktops™ 7 2402 LTSR Cumulative Update 4 (CU4)で利用可能です。

2203 LTSR CU7 をご利用の場合は、以下のいずれかのアップグレードパスに従うことをお勧めします。

- 2402 LTSR CU3 以降の累積更新プログラムにアップグレードします。
- 2507 以降のリリースにアップグレードします。
- 一般的に、将来のリリースにアップグレードすることをお勧めします。

HDX ダイレクト

マルチセッションホストの HDX Direct タイムアウトを延長して、60 秒を超えるログオンに対応できるようになりました。詳細については、HDX Direct の考慮事項を参照してください。

常時オンのトレース (AOT)

Always On Tracing (AOT) は、Citrix Virtual Apps and Desktops (CVAD) 2402 LTSR CU4 およびそれ以降の累積更新プログラムでサポートされるようになりました。

AOT は、サポートされている Citrix コンポーネントからログを継続的に収集し、管理者とサポートチームが手動でのログ収集や問題の再現を必要とせずに問題をトラブルシューティングできるようにします。ログは自動的に一元化された AOT ログサーバーに転送され、Citrix Director やその他のサポートされているツールを介して分析にすぐに利用できるようになります。

このリリースにより、2402 LTSR CU4 を実行しているお客様は AOT を展開し、サポートされているコンポーネントからテレメトリの収集を開始できます。これにより、トラブルシューティング時間の短縮と問題診断の改善に役立ちます。 展開の前提条件、サポートされている展開トポロジ、コンポーネントの互換性、インストール手順、および構成ガイダンスについては、最新リリースの Always On Tracing ドキュメントを参照してください。

> **注：**
>
> Always On Tracing の展開および構成プロセスは、Citrix Cloud 環境で VDA を実行しているお客様を含め、サポートされているすべての CVAD リリースで共通です。最新のガイダンスとサポートされているシナリオについては、最新の AOT ドキュメントを参照してください。

> 詳細については、Always On Tracing ドキュメントを参照してください。

修正された問題

Citrix Virtual Apps and Desktops™ 7 2402 LTSR CU3以降、以下の問題が修正されました。

全般

- ダブルホップシナリオでWindows Mediaリダイレクトを使用すると、最初のホップでWindows Media Playerがハングしたり、CPU使用率が高くなったりする場合があります。
- Microsoft Edge Web Storeからブラウザコンテンツリダイレクト拡張機能を使用すると、ブラウザコンテンツリダイレクトが失敗する場合があります。
- Citrixオーディオリダイレクトが断続的に動作を停止し、サービスを再起動する必要がある場合があります。

Citrix Director (シトリックス ディレクター)

- Directorからセッションレコーディングを再生すると、一部のリンクがHTTPSではなくHTTPで開かれる場合があります。
- ホスト数が10を超えると、Directorダッシュボードのインフラストラクチャセクションでホストステータスの更新が正しく行われない場合があります。
- 最近のMicrosoft OSセキュリティパッチを適用した後、Citrixシャドウイングを使用できなくなる場合があります。

Citrixポリシー

- Virtual Delivery Agent (VDA) がMicrosoft Entra IDユーザーアカウントを使用すると、ポリシーが適用されない場合があり、その結果、セッション間でポリシーの動作が一貫しなくなる可能性があります。
- CitrixグループポリシーがWindows 365 VDAマシンに適用されない場合があります。

シトリックス スタジオ

- PVSカタログを作成すると、vDiskのリスト中にタスクが失敗し、メッセージサイズクォータを超過したことを示す場合があります。
- CSVファイルからActive Directoryユーザーまたはマシンマッピングをインポートすると、「ユーザー名が見つかりません」というエラーでインポートが失敗する場合があります。
- FQDNに正規表現として解釈可能な文字が含まれている場合、Web Studioに管理者としてサインインできない場合があります。
- Desktop Delivery Controllerが特定のIPアドレスにSSLバインディングを設定しており、Citrix Orchestrationサービスが誤ってlocalhost IPアドレスを使用している場合、Web Studioでタグの管理などのアクションを実行できない場合があります。

デリバリーコントローラー

- 既存のActive DirectoryアカウントをIDプールに追加すると、必要なコンピューターアカウントが作成されない場合があり、その結果、WebSocket接続に影響を与える可能性があります。
- Broker ServiceがFMA Trust Serviceに接続すると、徐々にメモリ使用量が増加する場合があります。
- サインインすると、Citrix App-Vランチャーでエラーが表示されることがあります。特に英語以外のシステムで発生します。
- Web Studioで新しいアプリパッケージをデリバリーグループに割り当てると、アプリの検出に失敗し、アプリがWeb Studioに表示されず、デリバリーグループに割り当てられないことがあります。
- 複数のライセンスエンタイトルメントがある環境では、セッション起動時にエンドユーザーにライセンス有効期限切れの警告が表示されたり、ライセンスサーバー上のいずれかのエンタイトルメントが期限切れまたは期限切れ間近の場合に管理者にCitrix Studioで警告が表示されたりすることがあります。この問題は、現在の製品に対して有効でアクティブなエンタイトルメントが存在する場合でも発生します。
- ライセンス状態の移行中に競合状態が発生すると、ライセンスキャッシュモード期間の計算が誤って行われる可能性があります。これにより、セッションの起動が妨げられます。

- 重要なライセンス変更なしに構成同期が発生した場合、高可用性サービスが不必要にライセンスアクティベーションサービス (LAS) リクエストをトリガーする可能性があります。
- アプリケーションまたはデスクトップの列挙中にBrokerサービスがクラッシュし、サービスの可用性に影響を与える可能性があります。
- XenDesktopVDASetup.exeの削除中にVDAアップグレードエージェント (VUA) とインストーラーの間でタイミングの競合が発生すると、VUAがすでにアップグレードを完了しているVDAでアップグレードを再開する可能性があります。
- VDAハートビートスレッドが予期せず停止すると、Delivery Controller™がVDAとの接続を失い、VDAが未登録状態になる可能性があります。登録を復元するには、VDAを手動で再起動するか、RDPセッションを開始する必要があります。
- デバイスがアプリケーションの起動を開始してもセッション共有をサポートしていない場合、アプリケーションの起動を妨げるTokenNotFoundExceptionが発生する可能性があります。

マシン作成サービス

- Machine Creation Services (MCS) で作成されたWindows 11 VMでは、バックグラウンドエージェントサービスが停止し、システムの安定性に影響を与える可能性があります。
- VDAを1つだけ含むマシンカタログを作成する場合、MCSは常にVDAを最初のストレージ場所に配置します。
- Web Studioで、管理者ドメインとは異なるIDプール ドメインを持つActive Directory参加済みマシン用のカタログを作成または更新すると、マシンの作成に失敗する可能性があります。

グラフィック

メタインストーラー

ユニバーサル プリント サーバー

印刷

- 大容量ファイルをPDFに印刷すると失敗する可能性があります
- 拡張メタファイル (EMF) 印刷を使用するPDFで、アイコンの色が入れ替わることがあります。

シングルセッションOS用VDA

セッション/接続

- セッションとクライアント間でクリップボードのリダイレクトが断続的に停止することがあります。

- 新しいセッションを開始する際に、マシンがウェルカム画面でハングアップするなど、断続的な問題が発生することがあります。
- IPv6を使用している場合、「接続元」フィールドに、予期されるネットワークアドレスではなくローカルループバックアドレスが表示されることがあります。
- 複数のモニターで再接続した後、Windows 11のアプリウィンドウが非表示になることがあります。
- セッションに再接続した後、保存した仮想ディスプレイレイアウトが適用されないことがあります。
- クライアントからコピーしたファイル名を貼り付けると、ビープ音が鳴ることがあります。
- Citrix StoreFrontからアプリケーションを起動すると、起動に失敗し、「Cannot Start App: {app name}」というエラーメッセージが表示されることがあります。
- Windows 11マルチセッションVDAでCitrixセッションを切断して再接続すると、タイムゾーン設定に関わらずタイムゾーンがリセットされることがあります。

システム例外

- 再接続後にICAセッションパフォーマンスカウンターインスタンスが見つからなくなり、問題が発生することがあります。
- 最大化されたウィンドウをモニター間で移動すると、フリーズしたり黒くなったりすることがあります。
- 作業中またはホバー中に、公開アプリケーションがフリーズしたり応答しなくなったりすることがあります。
- USBドライバーエラーにより、Citrix Provisioningでプロビジョニングされたデスクトップを再起動するとブルースクリーンが表示されることがあります。
- サインイン画面がクラッシュし、デスクトップが応答しなくなることがあります。
- 公開されたChromeアプリのブラウザコンテンツリダイレクトが、拡張子のないURLをリダイレクトしないことがあります。
- FIDO2 は、デフォルトでは edgewebview2 で動作しません。
- VDA をインストールすると、Windows の設定が変更され、Outlook がクラッシュする場合があります。
- メモリアクセスエラーやシステムサービスエラーなどのブルースクリーンエラーが発生する場合があります。
- FIDO2 認証はブラウザセッションでのみ機能し、Office 365 アプリでは失敗します。

- バッテリーステータスインジケーターが表示されないため、セッション内からデバイスの残り電力を確認する際に問題が発生する場合があります。
- シームレスモードでサイズ変更すると、Excel のフィルタードロップダウンが消える場合があります。
- 「クライアントのローカル時間を使用」を「クライアントのタイムゾーンを使用」に設定した後、ウォーターマークのタイムゾーンが同期されない場合があります。
- 公開された Internet Explorer が起動時にすぐに閉じる場合があります。
- UDP オーディオの問題により、送信オーディオの途切れやビープ音が発生する場合があります。
- シングルモニターの場合、HDX 3D Pro が無効になっているときに、誤った HDX 3D Pro 全画面警告が表示される場合があります。
- セッション内で USB ヘッドセットが誤って識別され、Citrix HDX Audio として表示される場合があります。
- VDA をアンインストールして再起動した後、マシンにログインできない場合があります。
- ドメインに参加していないマシン上の英語以外の Windows オペレーティングシステムに Citrix VDA をインストールすると、インストーラーが VDA サービスにローカライズされたサービスアカウント名を使用する可能性があります。その結果、CitrixVDACeipService および CitrixTelemetryService サービスが起動に失敗する場合があります。

マルチセッションOS用VDA

クリップボード

セッション/接続

- 匿名セッションを起動すると、予期せずセッションが閉じずにアクティブなままになる場合があります。
- picadm.sys モジュールの問題により、PAGE_FAULT_IN_NONPAGED_AREA (0x50) というコードのブルースクリーンエラーが断続的に発生する場合があります。
- 断続的なデスクトップサービスの再登録や再接続の失敗が発生する可能性があります。
- キオスクデバイスでは、ユーザーセッション間でセッションが最大化されたままにならない場合があります。
- Windows Server 2016またはWindows Server 2022上のリモートアプリケーションへの再接続にわずかな遅延が発生する可能性があります。

- マルチユーザーデスクトップでアイドル状態になった後、クリップボードのリダイレクトが機能しなくなることがあります。
- 複数のモニターで再接続した後、Windows 11アプリのウィンドウが非表示になることがあります。
- セッションに再接続した後、保存された仮想ディスプレイレイアウトが適用されない場合があります。
- VDAが異なる解像度の2つのモニターに接続され、ディスプレイが垂直に配置されているデュアルモニター設定で、シームレスアプリケーションでマウスカーソルを下から上に移動させると、プライマリモニターからセカンダリモニターにジャンプする可能性があります。
- ユーザーログオンに予想よりも時間がかかった場合、VDA 2402 LTSRおよびVDA 2507 LTSR CU2以降のセッションでHDX Directがアクティブ化に失敗する可能性があります。

スマートカード

システム例外

- ディスプレイドライバーがクラッシュし、デスクトップセッションが中断される状況が発生する可能性があります。
- HDX MediaStreamサービスが断続的に停止すると、音声が失われる可能性があります。
- Citrix Audio Redirectionサービスの問題により、サインインできなくなり、プロセスが停止する可能性があります。
- オーディオサービスの問題により、Microsoft Searchが応答しなくなることがあります。
- ウィンドウ表示の公開アプリケーションが全画面表示にリサイズされない状況が発生する可能性があります。
- システムドライバーの問題により、時々ブルースクリーンエラーが発生する可能性があります。
- FIDO2 は、デフォルトでは edgewebview2 で動作しません。
- メモリアクセスエラーやシステムサービスエラーなどのブルースクリーンエラーが発生する可能性があります。
- VDA をインストールすると、Windows の設定が変更され、Outlook がクラッシュする原因となる場合があります。
- FIDO2 認証はブラウザセッションでのみ機能し、Office 365 アプリでは失敗します。
- バッテリーステータスインジケーターが表示されないため、セッション内からデバイスの残り電力を確認する際に問題が発生する可能性があります。

- マルチユーザーデスクトップでアイドル状態になった後、クリップボードのリダイレクトが機能しなくなります。
- シームレスモードでサイズ変更すると、Excel のフィルタードロップダウンが消えることがあります。
- 公開された Internet Explorer が起動時にすぐに閉じる場合があります。
- AMD Turin ベースのホストで VDA 2203 CU5 を使用すると、picaser.sys でブルースクリーンが発生する可能性があります。
- FIDO2 リダイレクトが有効な場合、最近の Windows 11 アップデートをインストールした後、Microsoft Edge が予期せず終了する可能性があります。

リナックス ブイディーエー

修正された問題については、個別のドキュメントにある修正された問題の記事を参照してください。

プロファイル管理

修正された問題については、個別のドキュメントにある修正された問題の記事を参照してください。

セッション録画

修正された問題については、個別のドキュメントにある修正された問題の記事を参照してください。

StoreFront™

修正された問題については、個別のドキュメントにある修正された問題の記事を参照してください。

累積更新プログラム 3 (CU3)

リリース日: August 26, 2025

このリリースについて

Citrix Virtual Apps and Desktops 7 2402 LTSR 累積更新プログラム 3 (CU3) は、2402 LTSR の初回リリース以降に報告された 30 を超える問題を修正します。

2402 LTSR (一般情報)

2402 LTSR (機能とアップグレード情報)

このリリースの新機能

Citrix Virtual Apps and Desktops 7 2402 LTSR (初回リリース) で修正された問題

このリリースの既知の問題

非推奨と削除

Citrix 製品の Subscription Advantage 資格日

ダウンロード

シトリックス バーチャル アプリケーションズ アンド デスクトップ 7 2402 LTSR CU3(https://www.citrix.com/downloads/citrix-virtual-apps-and-desktops/product-software/citrix-virtual-apps-and-desktops-2402ltsr-cu3-all-editions.html)

新規展開

CU3 をゼロから展開するにはどうすればよいですか?

CU3 メタインストーラーを使用して、CU3 に基づく新しい Citrix Virtual Apps and Desktops 環境をセットアップできます。その前に、製品についてよく理解しておくことをお勧めします。

展開の計画を開始する前に、Citrix Virtual Apps and Desktops 7 2402 LTSR (initial release)セクションを確認し、Technical Overview、Install and Configure、およびSecurityの各セクションに特に注意してください。セットアップがすべてのコンポーネントのシステム要件を満たしていることを確認してください。

既存の展開

何を更新しますか?

CU3は、2402 LTSRの15のベースラインコンポーネントの更新を提供します。Citrixは、展開のすべてのLTSRコンポーネントをCU3に更新することを推奨しています。例：Citrix ProvisioningがLTSR展開の一部である場合、Citrix Provisioningコンポーネントを CU3に更新してください。Citrix Provisioningが展開の一部でない場合、インストールまたは更新する必要はありません。

2402 LTSR CU3ベースラインコンポーネント

2402 CU3ベースラインコンポーネント	プログラムと機能に表示されるバージョン	ドキュメント
シングルセッションVDA	2402.0.3100.3651	シングルセッションVDA

2402 CU3ベースラインコンポーネント	プログラムと機能に表示されるバージョン	ドキュメント
マルチセッションVDA	2402.0.3100.3651	マルチセッションVDA
デリバリーコントローラー	2402.0.3100.3651	デリバリーコントローラー
シトリックス スタジオ	7.41.3100.56	シトリックス スタジオ
シトリックス ディレクター	7.41.3100.32	シトリックス ディレクター
Citrix グループポリシー管理	7.41.3100.55	Citrix グループポリシー管理
Citrix グループポリシー クライアント側拡張	7.41.3100.55	
シトリックス ストアフロント	2402.0.3100.14	シトリックス ストアフロント(/ja-jp/storefront/2402-ltsr)
ユニバーサル プリント サーバー	7.41.3100.89	ユニバーサルプリントサーバー(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/printing/printing-provision-printers.html)
セッション録画	24.2.3100	セッションレコーディング(/ja-jp/session-recording.html)
リナックス VDA	24.02.1100.21	Linux 仮想デリバリーエージェント(/ja-jp/linux-virtual-delivery-agent.html)
プロファイル管理	24.2.3100.31	プロファイル管理(/ja-jp/profile-management.html)
Citrix フェデレーション認証サービス	10.17.3100.24	Citrix フェデレーション認証サービス (FAS)
ブラウザコンテンツリダイレクト	15.48.3100.106	ブラウザコンテンツリダイレクト
シトリックス プローブ エージェント 2206	7.41.3100.23	ダウンロード

2402 LTSR CU3 互換コンポーネント

以下のコンポーネントは、記載されているバージョンでLTSR環境と互換性があります。これらはLTSRのメリット（延長されたライフサイクルと修正のみの累積更新プログラム）の対象ではありません。Citrix®は、2402環境内でこれらのコンポーネントを新しいバージョンにアップグレードするよう求める場合があります。

互換性のあるコンポーネントと機能	プログラムと機能に表示されるバージョン	ドキュメント
アプリケーションレイヤリング	2206.0.0	Citrix アプリケーションレイヤリング
HDX リアルタイム オプティマイゼーション パック	2.9.400.2702	HDX リアルタイム最適化パック
ライセンスサーバー	11.17.2.0_BUILD_53100	「ライセンスサーバー」(/ja-jp/licensing/11-17-2-48000/)
ユーザーパーソナライゼーションレイヤー	25.3.3	「ユーザーパーソナライゼーションレイヤー」(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/install-configure/user-personalization-layer.html)
セッションレコーディング Webプレーヤー	24.2.3100.12	「セッションレコーディング Webプレーヤー」(/ja-jp/session-recording/2402-ltsr/view-recordings/session-recording-web-player.html)
Microsoft Teamsの最適化	15.32.1000.9	「Microsoft Teamsの最適化」(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/multimedia/opt-ms-teams.html)
ワークスペース環境管理	2402.1.100.1	ワークスペース環境管理
XenApp & XenDesktop 7.15 LTSR VDA (最新リリース)*	最新の累積更新プログラムのみ	ドキュメント

互換性のあるコンポーネントと機能	プログラムと機能に表示されるバージョン	ドキュメント
CVAD 2402 CUx Delivery Controller を使用して Windows Server 2025 にインストールされた VDA 2411 以降	2411.x.x.x	ドキュメント

2402 LTSR CU3 の主な除外事項

以下の機能、コンポーネント、およびプラットフォームは、2402 ライフサイクルマイルストーンおよび特典の対象外です。具体的には、累積更新プログラムおよび拡張ライフサイクル特典は除外されます。除外された機能およびコンポーネントの更新プログラムは、通常の現行リリースを通じて利用できます。

除外されるコンポーネントと機能
AppDisks™
AppDNA®
Citrix SCOM 管理パック
フレームホーク
パーソナル vDisk
ストアフロント シトリックス オンライン 統合

除外される WINDOWS プラットフォーム *
Windows 2008 32ビット版 (Universal Print Server 向け)

* Citrix は、サードパーティベンダーのライフサイクルマイルストーンに基づいてプラットフォームサポートを更新する権利を留保します。

新機能

Citrix Virtual Apps and Desktops™ 7 2402 LTSR Cumulative Update 3 (CU3) で利用可能な新機能と機能強化は次のとおりです。

2203 LTSR CU7 をご利用の場合は、以下のいずれかのアップグレードパスに従うことをお勧めします。

- 2402 LTSR CU3 以降の累積更新プログラムにアップグレードします。
- 2507 以降のリリースにアップグレードします。
- 一般的に、将来のリリースにアップグレードすることをお勧めします。

ファイルベースのライセンスシステムのEOL通知

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

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

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

セキュアHDX™

Secure HDXが一般提供されるようになりました。これは、トラフィックパス内のネットワーク要素がHDXトラフィックを検査するのを防ぐアプリケーションレベル暗号化 (ALE) ソリューションです。詳しくは、Secure HDXを参照してください。

ウェブスタジオ

ドメイン選択の強化

UIの新しいオプションにより、ドメイン選択が必要な場所でドメイン名を正確に一致させるために指定できるようになりました。この機能強化には、以下の利点があります。

- 検索の高速化: 大規模なディレクトリを閲覧する手間を省き、結果を直接かつ即座に取得できます。
- 時間の節約: ディレクトリ全体の読み込みをなくし、ワークフローを高速化します。
- エクスペリエンスの向上: 特に大規模なディレクトリを持つ環境において、管理者による管理効率を向上させます。

Web Studio を使用した Azure および VMware 環境での Citrix Provisioning™ Hybrid Azure AD 参加済みカタログの作成のサポート

Web Studio を使用すると、Azure および VMware 環境で Citrix Provisioning Hybrid Azure AD 参加済みカタログを作成できるようになりました。以前は、Citrix Virtual Apps and Desktops オンプレミス環境で Hybrid Azure AD 参加済みカタログを作成するには PowerShell を使用するしかありませんでした。詳細については、「Hybrid Azure AD 参加済みカタログの作成」を参照してください。

デリバリーコントローラー™

Citrix Virtual Apps and Desktops™ サイトとのライセンスサーバーのバージョン互換性

Citrix Virtual Apps and Desktops サイトの作成およびアップグレードでは、ライセンスサーバーがバージョン 11.17.2 ビルド 53100 以降を実行していることを確認してください。

修正された問題

Citrix Virtual Apps and Desktops™ 7 2402 LTSR CU2 以降、以下の問題が修正されました。

Citrix Director (シトリックス ディレクター)

- Director 2402 LTSR では、パスワードが50文字を超えると、GUIでSMTPサーバーを設定できません。
- Directorバージョン2407以降では、ブラウザの言語をfr-CAまたはfr-FRに設定しても、コンソールがフランス語で表示されません。
- Citrix Director 2402の「セッションの選択」ビューで「すべてのリソースを表示」ボタンをクリックすると、切断されたセッションや非アクティブなセッションの代わりに「表示するレコードがありません」と表示されることがあります。
- Citrix Directorで、管理者がマシンまたはセッションフィルターにアクセスする際に断続的なエラーが発生することがあります。この問題は、`AtomValueUtils.ConvertStringToPrimitive`メソッドの失敗が原因です。

Citrixポリシー

- グループポリシー管理コンソール (GPMC) を使用してグループポリシーを管理する場合、バージョン2411以前のCitrixGroupPolicyManagement_x64.msiをインストールした後でも、「VDAアップグレードプロキシ構成」設定が編集できない場合があります。
- 休止状態から復帰した後、VDAがドメイン構成のGPOを適用せず、再初期化時にポリシーの不整合が発生する場合があります。
- Web StudioでレガシーPowerShellプロバイダーを使用して生成されたポリシーを読み込む際に問題が発生する可能性があります。

シトリックス スタジオ

- 冗長構成で1つのDelivery Controller™がシャットダウンされると、残りのコントローラーからWeb Studioにサインインできなくなることがあります。この問題はバージョン2402 LTSRで発生し、「サインインできません。後でもう一度お試しください。」というメッセージが表示されます。
- Web Studio経由でマシンカタログを作成する際に、例外が発生する可能性があります。この問題はMMC Studioでは発生しません。
- Studio for Webで、ユーザーやマシンの追加など、AD関連のアクションを実行する際にActive Directoryの資格情報が失敗します。同じアクションは、完全なStudioアプリケーションでは正しく機能します。

デリバリーコントローラー

- タスク定義内の無効な変数名が原因で、Monitor Serviceのグルーミングが失敗する場合があります。この問題は`GroomResourceUtilization`タスクに影響を与え、他のグルーミングタスクにも影響を及ぼす可能性があります。
- アップグレード期間中にVDA CUアップグレードエージェントが応答しなくなります。その結果、すべてのVDAが「アップグレード可能」と表示されず、一部はスケジュールされた期間内にインストールできません。
- DDCを2402 CU1にアップグレードした後、リモートPCセッションが機能しなくなることがあります。この問題はリモートPC VDAのみに影響します。
- Delivery Groups AdministratorおよびDelivery GroupsカスタムスコープでWeb Studioにログインすると、「タグの管理」を選択してシングルセッションOSマシンまたはマルチセッションマシンからタグを削除しようとしたときにエラーが発生する場合があります。

マシン作成サービス

- マシンパスワードの更新に失敗した場合、MCS Linux VDA は一定期間後に登録解除される可能性があります。
- Google Cloud Platform (GCP) では、2402 CU2 の Daisy 仮想マシン用のイメージが非推奨になったため、イメージのエクスポートが失敗します。
- Web Studio で新しいハイブリッド参加済み Windows 11 カタログを作成しようとすると、エラーが発生する場合があります。このプロセスは、マシンアカウント作成フェーズで「Set-AcctADAccountUserCert: Object reference not set to an instance of an object.」というエラーで失敗します。
- Citrix Studio での自動サイトアップグレード中に、Delivery Controller を 2203 CU5 から 2402 CU1 にアップグレードすると失敗する場合があります。Delivery Controller のアップグレードは完了しますが、サイトの更新は正常に終了しません。

グラフィック

- デュアルモニター設定を使用し、ポップアウトされたブラウザウィンドウを共有すると、視聴者には親ブラウザが背景に表示されます。

メタインストーラー

- 2203 CU3 から CU5 への VDA アップグレードでは、`HKLM\SYSTEM\CurrentControlSet\Services\picadm` の下のすべてのレジストリ設定がリセットされ、`DisableFullStreamWrite` エントリの削除も含まれます。これらの設定を保持したい場合は、アップグレード後に再適用する必要がある場合があります。
- Citrix Virtual Apps and Desktops (CVAD) 2203 CU5 または 2402 にアップグレードした後、WMI インスタンス `Citrix_Client_Enum` へのアクセスが「Provider Load Failure」エラーで失敗する場合があります。

ユニバーサル プリント サーバー

印刷

- Universal Print Server (UPS) から 2203 LTSR CU5 にアップグレードした後、プリンターを選択する際に長い遅延が発生する場合があります。プリンターが「プリンターに接続中」の状態のままで、使用可能になるまでに 1 分以上かかることがあります。

シングルセッションOS用VDA

セッション/接続

- Windows 11 24H2 を使用すると、セッションがハングし、起動中に黒い画面が表示されます。
- picadm.sys モジュールの問題により、コード PAGE_FAULT_IN_NONPAGED_AREA (0x50) のブルースクリーンエラーが断続的に発生する場合があります。
- ドラッグアンドドロップが有効な公開デスクトップに接続し、その後切断して再接続するか、ドラッグアンドドロップが無効な別のクライアントから接続した場合、ログオフして新しいセッションを開始するまでドラッグアンドドロップは有効なままになります。
- Windows 10 セッションからログオフする際に、「ログオフ中」画面で遅延が発生する場合があります。
- 公開アプリケーションを起動すると、アプリケーションの横に黒いボックスが表示され、セッションをログオフするまで表示されたままになります。

システム例外

- 以前のバージョンでは、picadm.sys の新しい問題により、デバイスでブルースクリーンエラーが表示されることがありました。
- VDI 1.0 では、受信ビデオの表示、セルフプレビューの使用、または画面共有ができない場合があります。
- Citrix Workspace for HTML5 を使用している場合、Excel で大量のデータをコピー＆ペーストすると、Wfshell.exe がクラッシュすることがあります。この問題は、ローカルにインストールされた Citrix Workspace アプリを使用している場合には発生しません。
- VDA 2402 にアップグレードした後、共有環境での公開アプリケーションセッション中に CPU 使用率が急上昇します。
- Windows アップデートをインストールした後、シングルセッション VDA でマウスカーソルが予測不能に動き、ランダムにジャンプすることがあります。

マルチセッションOS用VDA

クリップボード

- Excel でコンテンツをコピー＆ペーストした後、Citrix WinFrame Shell (WFshell.exe) がクラッシュし、セッションが中断され、新しいアプリを起動したり、公開アプリと対話したりできなくなることがあります。この問題は Citrix Workspace for HTML を使用している場合にのみ発生し、Citrix Workspace App には影響しません。

セッション/接続

- VDA セッションのクラッシュとそれに続くマシンの再起動が発生する場合があります。
- VDA 2402 LTSR では、セッションが予期せず切断された後、「アクセスが拒否されました」というエラーがランダムに表示されることがあります。この場合、セッションは警告なしに消滅し、再接続の試行も同じエラーで失敗します。
- VDA が登録解除され、完全に応答しなくなることがあります。影響を受ける仮想マシンは、手動で再起動するまで再接続できません。
- picadm.sys モジュールの問題により、PAGE_FAULT_IN_NONPAGED_AREA (0x50) というコードのブルースクリーンエラーが断続的に発生する場合があります。
- ドラッグ＆ドロップが有効な公開デスクトップに接続し、その後切断して再接続するか、ドラッグ＆ドロップが無効な別のクライアントから接続した場合、ログオフして新しいセッションを開始するまでドラッグ＆ドロップは有効のままになります。
- 公開アプリケーションを起動すると、アプリケーションの横に黒いボックスが表示され、セッションをログオフするまで表示されたままになります。
- Citrix Workspace™ App for Linux からセッションを起動すると、セッションは開いたように見えますが、エラーを表示することなくすぐに閉じます。

スマートカード

- Citrix Virtual Apps and Desktops (CVAD) 2402 CU1 にアップグレードした後、`CertPropSvc` プロセスでクラッシュが時々発生することがあります。これにより、スマートカードアクセスに問題が生じる可能性があります。

システム例外

- 以前のバージョンのVDAでは、ストップコード `SYSTEM_THREAD_EXCEPTION_NOT_HANDLED (0x7E)` でランダムなクラッシュが発生する可能性があります。
- LVDA 2402CU1にアップグレードした後、ユーザーセッションが「不明」と表示され、再接続に失敗する場合があります。
- 以前のバージョンでは、セカンダリモニターがない場合、ラップトップ画面でマウスを使用してSAPウィンドウを水平方向に拡大することはできません。
- CVADの以前のバージョンでは、picadm.sysの新しい問題により、デバイスにブルースクリーンエラーが表示されることがあります。
- Citrix Workspace for HTML5を使用している場合、Excelで大量のデータをコピー＆ペーストすると、Wfshell.exeがクラッシュすることがあります。この問題は、ローカルにインストールされたCitrix Workspaceアプリを使用している場合には発生しません。

- マルチセッションシナリオでは、約2,493文字を超える文字をコピーすると、コピー＆ペースト機能が動作しなくなることがあります。
- Clipboard DLLの問題により、クリップボード操作中にCtxSvcHost.exeがクラッシュすることがあります。
- 複数のLDAPサーバーに到達できない場合、Delivery ControllerへのVDA登録が失敗したり、LDAP検索で問題が発生したりすることがあります。
- VDAマスターイメージでTLSを有効にすると、`Enable-VDASSL.ps1` スクリプトが期待どおりに動作しない場合があります。
- クライアントの地理位置情報がTSVDAのVDIにリダイレクトされない場合があり、特定のアプリケーションやセキュリティ機能に影響を与える可能性があります。
- Citrixポリシーが完全に適用される前にアプリケーションを起動すると、一部の公開アプリケーションがローカルクライアント時間ではなくVDAシステム時間を使用する場合があります。
- VDAが10〜15分間使用されていない場合、画面が応答しなくなり、問題を解決するにはVDAを再接続/リセットする必要があります。
- 以前のバージョンでは、シームレスなApp-Vアプリケーションを移動およびドラッグできない場合があります。
- ホストからクライアントへのURLリダイレクトは、大文字と小文字を区別するURLパラメータを大文字から小文字に変換するため、特定の文字の大文字/小文字を必要とするアプリケーションへのアクセス時に障害が発生する可能性があります。
- ブラウザコンテンツリダイレクトは実際のリダイレクトされたページを読み込まず、BCRの背景ページ（「ページがリダイレクトされました」）が表示されます。ページを再読み込みしても問題は解決しません。
- Windowsアップデートをインストールした後、マウスカーソルが予測不能に動き、シングルセッションVDAでランダムにジャンプすることがあります。

リナックス ブイディーエー

修正された問題については、個別のドキュメントにある修正された問題の記事を参照してください。

プロファイル管理

修正された問題については、個別のドキュメントにある修正された問題の記事を参照してください。

セッション録画

修正された問題については、個別のドキュメントにある修正された問題の記事を参照してください。

StoreFront™

修正された問題については、個別のドキュメントにある修正された問題の記事を参照してください。

累積更新プログラム 2 (CU2)

リリース日: February 06, 2025

> **注：**

> CTX692777 で報告された問題は、CU2 リリースの最新バージョンで対処されています。

> お客様はこの新しいバージョンにアップグレードできます。既存のCU2展開は引き続き機能します。

このリリースについて

Citrix Virtual Apps and Desktops™ 7 2402 LTSR 累積更新プログラム 2 (CU2) は、2402 LTSR の初回リリース以降に報告された30を超える問題を修正します。

2402 LTSR (一般情報)

2402 LTSR (機能とアップグレード情報)

このリリースの新機能

Citrix Virtual Apps and Desktops 7 2402 LTSR で修正された問題 (初回リリース)

このリリースの既知の問題

非推奨と削除

Citrix製品のサブスクリプション特典の対象日

ダウンロード

シトリックス バーチャルアプリ＆デスクトップ 7 2402 LTSR CU2

新しい展開

CU2 をゼロから展開するにはどうすればよいですか?

CU2 メタインストーラーを使用して、CU2 に基づく新しい Citrix Virtual Apps and Desktops 環境をセットアップできます。その前に、製品についてよく理解しておくことをお勧めします。

展開計画を開始する前に、Citrix Virtual Apps and Desktops 7 2402 LTSR (初期リリース) セクションを熟読し、技術概要、インストールと構成、および セキュリティ の各セクションに特に注意してください。セットアップがすべてのコンポーネントのシステム要件を満たしていることを確認してください。

既存の展開

何を更新しますか?

CU2 は、2402 LTSR の 15 のベースラインコンポーネントの更新を提供します。注意: Citrix は、展開のすべての LTSR コンポーネントを CU2 に更新することを推奨しています。例: Citrix Provisioning が LTSR 展開の一部である場合、Citrix Provisioning コンポーネントを CU2 に更新します。Citrix Provisioning が展開の一部でない場合、インストールまたは更新する必要はありません。

2402 LTSR CU2 ベースラインコンポーネント

2402 CU2 ベースラインコンポーネント	プログラムと機能に表示されるバージョン	ドキュメント
シングルセッション VDA	2402.0.2150.2566	シングルセッション VDA
マルチセッション VDA	2402.0.2150.2566	マルチセッション VDA
デリバリーコントローラー	2402.0.2150.2566	デリバリーコントローラー
Citrixスタジオ	7.41.2150.32	Citrixスタジオ
シトリックス ディレクター	7.41.2150.21	シトリックス ディレクター
Citrixグループポリシー管理	7.41.2150.32	Citrixグループポリシー管理

2402 CU2 ベースラインコンポーネント	プログラムと機能に表示されるバージョン	ドキュメント
Citrixグループポリシー クライアント側拡張	7.41.2150.32	
シトリックス ストアフロント	2402.0.2100.11	シトリックス ストアフロント
ユニバーサル プリント サーバー	7.41.2100.52	ユニバーサルプリントサーバー
セッション録画	24.2.2100	セッションレコーディング
リナックス VDA	24.02.1100.21	Linux仮想デリバリーエージェント
プロファイル管理	24.2.2100.17	プロファイル管理
Citrixフェデレーテッド認証サービス	10.17.2150.16	Citrixフェデレーテッド認証サービス (FAS)
ブラウザーコンテンツリダイレクト	15.48.2100.49	ブラウザコンテンツリダイレクト
Citrix プローブエージェント 2206	7.41.2150.16	ダウンロード

2402 LTSR CU2互換コンポーネント

以下のバージョンで示されているコンポーネントは、LTSR環境と互換性があります。これらはLTSRのメリット（拡張されたライフサイクルと修正のみの累積更新プログラム）の対象ではありません。Citrixは、2402環境内でこれらのコンポーネントを新しいバージョンにアップグレードするよう求める場合があります。

互換性のあるコンポーネントと機能	プログラムと機能に表示されるバージョン	ドキュメント
アプリケーション レイヤリング	2206.0.0	Citrix アプリケーション レイヤリング
HDX リアルタイム最適化パック	2.9.400.2702	HDX リアルタイム最適化パック

互換性のあるコンポーネントと機能	プログラムと機能に表示されるバージョン	ドキュメント
ライセンスサーバー	11.17.2.0_Build 51000	ライセンスサーバー
ユーザーパーソナライゼーションレイヤー	24.9.0	ユーザーパーソナライゼーションレイヤー
セッション録画Webプレーヤー	24.2.2100.7	セッション録画Webプレーヤー
Microsoft Teamsの最適化	15.32.1000.9	Microsoft Teamsの最適化
ワークスペース環境管理	2402.1.100.1	ワークスペース環境管理
XenApp & XenDesktop 7.15 LTSR VDA (最新リリース)*	最新の累積更新プログラムのみ	ドキュメント
Windows Server 2025 にインストールされた VDA 2411 以降と、CVAD 2402 CUx Delivery Controller	2411.x.x.x	ドキュメント

2402 LTSR CU2 の主な除外事項

以下の機能、コンポーネント、およびプラットフォームは、2402 ライフサイクルマイルストーンおよび特典の対象外です。具体的には、累積更新プログラムと拡張ライフサイクル特典は除外されます。除外された機能およびコンポーネントの更新は、通常の現行リリースを通じて利用できます。

除外されるコンポーネントと機能
AppDisks™
AppDNA®
シトリックス SCOM マネジメントパック
フレームホーク
パーソナル vディスク
StoreFront シトリックス オンライン統合

除外される WINDOWS プラットフォーム *
Windows 2008 32ビット (ユニバーサルプリントサーバー用)

* Citrix は、サードパーティベンダーのライフサイクルマイルストーンに基づいて、プラットフォームサポートを更新する権利を留保します。

新機能

以下の新機能と機能強化が、Citrix Virtual Apps and Desktops™ 7 2402 LTSR Cumulative Update 2 (CU2) で利用可能です。

Web Studio を使用した VMware 環境での Citrix Provisioning™ カタログ作成のサポート

Web Studio を使用して、VMware 環境で Citrix Provisioning カタログを作成できるようになりました。以前は、管理者はカタログのプロビジョニングと管理のために異なるコンソールを切り替える必要がありました。この機能により、コンソールを切り替える必要が減り、Web Studio 内で直接プロビジョニングと電源管理を処理できるようになります。詳細については、「Studio を使用した VMware 環境での Citrix Provisioning カタログの作成」を参照してください。

マシンカタログのサブネットマッピングの変更

以前は、マシンカタログのサブネットマッピングを変更するには、カタログを削除し、新しいサブネットマッピングでカタログを作成する必要がありました。この機能により、カタログのサブネットマッピングを変更することで、同じ機能を実現できるようになりました。これにより、このカタログの下で作成される新しい仮想マシンが新しいサブネットマッピング上に配置されることが保証されます。この機能強化により、カタログの削除とその関連作業のオーバーヘッドが削減されます。詳細については、「カタログの編集」を参照してください。

Pendo の統合

バージョン 2402 LTSR CU2 以降、Web Studio は Pendo と統合されており、デフォルトで有効になっています。Pendo は、Citrix プライバシーポリシーに従って使用状況データを収集します。使用状況データを共有したくない場合は、Studio 構成ツールを使用して Pendo を無効にできます。詳細については、「Pendo の有効化または無効化」を参照してください。

LTSR 展開向け Director の独立リリース

LTSR 展開向け Director の独立リリースにより、互換性のある LTSR 環境で Citrix® 環境におけるトラブルシューティングと監視を強化するための最新の Director 機能にアクセスするオプションが提供されるようになりました。この機能により、お客様は 2402 LTSR 展開で最新の Director

バージョンを使用できます。また、LTSR の発表後にリリースされた機能にも、アプリケーション配信インフラストラクチャに影響を与えることなくアクセスできます。

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

> **注:**
>
> SQL Server 2016 は、Director または Monitor サービスの現在のリリースと互換性がありません。

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

- シトリックス バーチャルアプリ アンド デスクトップ 2407 リリース
- シトリックス バーチャルアプリ アンド デスクトップ 2411 リリース

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

主な考慮事項

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

詳しくは、「LTSR展開向けDirectorの独立リリース」を参照してください。

イメージ管理が一般提供開始

イメージ管理機能は、Citrix Virtual Apps and Desktops 2402 LTSR CU2から、AzureおよびVMware仮想化環境で一般提供されています。詳しくは、「イメージ管理」を参照してください。

StoreFront™

最新のエクスペリエンス - 一般提供

新しい最新のエクスペリエンスが、オンプレミスストアで一般提供されるようになりました。このUIは、以前はクラウドストアでのみ利用可能でしたが、クラウドストアとオンプレミスストア全体で一貫したルックアンドフィールを保証します。 新しいユーザーインターフェイスは、Citrixアプリとデスクトップにアクセスするエンドユーザーエクスペリエンスを向上させ、簡素化するように設計されています。視覚的な複雑さを軽減し、重要な機能への簡単なアクセスを提供し、StoreFrontアプリのエクスペリエンスを洗練させます。仮想アプリとデスクトップリソースの効果的な管理を容易にするアクティビティマネージャーなどの新機能をサポートします。 詳しくは、「StoreFront 2402 LTSR CU2の新機能」を参照してください。

修正された問題

Citrix Virtual Apps and Desktops™ 7 2402 LTSR CU1以降、以下の問題が修正されました。

Citrix Director (シトリックス ディレクター)

- UI.TaskManager.EnableApplicationsオプションがUIで無視され、アプリケーションリストがDirectorに表示されたままになることがあります。
- UserProfileの詳細をクリックしてテキストを選択しようとすると、UserProfileBoxが消えてデータコピーが妨げられるという問題が発生する可能性があります。
- HDX™接続がSecure ICAを使用して確立されたかどうかがDirectorに表示されなくなったことに気づくかもしれません。
- 2203 CU4から2402にアップグレードした後、負荷分散されたDirectorでSSONが時々失敗する可能性があります。
- マルチサイトDirector 2402環境では、「サイトへ移動」ページで15分間操作がないと、ユーザーがコンソールから自動的にサインアウトされることがあります。
- CU1では、Directorのフィルターページにあるマシンページへのリンクが壊れています。マシンを手動で検索する必要があります。
- Director CU1では、ソート後に誤った行が選択されたり、マシンやセッションを選択する際に余分なレコードが追加されたりすることがあります。
- Citrix Director 2402 CU1では、アクティビティマネージャーがユーザー名を表示せず、代わりにユーザー表示名を表示することがあります。

Citrixポリシー

- CseEngine.exeプロセスによるメモリ使用量が高くなり、マシンの登録問題を引き起こす可能性があります。
- 以前のバージョンから2402にアップグレードした後、ポリシーを編集または作成できない場合があります。この問題は新規インストールサイトでは発生しません。
- Delivery Controller (DDC) とデータベースを1912から2402にアップグレードした後、Citrix Studioのポリシー優先度が変更され、すべてのサイトに影響します。
- Windows 11マルチセッションマシンにStudioをインストールし、グループポリシー管理コンソールを開くと、Citrixグループポリシーモジュールを読み込む際に以下のエラーメッセージが表示されます。 `ERROR_CODE: (NTSTATUS) 0xc0000005 - The instruction at 0x%p referenced memory at 0x%p`

シトリックス スタジオ

- On-Prem Web Studio 2402では、マシンカタログの作成または更新中に更新ボタンを使用できません。
- ドメインに1文字のトップレベルドメイン (TLD) がある場合、「無効なトークン」エラーが発生し、WebStudioにログインできないことがあります。
- CVAD Studio 2402 CU1で、セッションタブからデリバリーグループ列を削除した後、セッション詳細の代わりにエラーが表示されることがあります。
- ブローカーアプリケーションの「名前」と「公開名」の両方が変更された場合、App-Vアプリケーションの詳細で「配信元」フィールドが空白になることがあります。
- Web Studio 2402 CU1は、Virtual Delivery Agent (VDA) からデータを取得する際に、登録メトリックのDelivery Controller™情報を表示しない場合があります。

デリバリーコントローラー

- 一意でないデバイスIDが報告された場合、セッションの再接続が失敗し、セッションの動作やアプリ制限のバイパスに関する問題が発生する可能性があります。
- 数ヶ月分のデータを保持する大規模なMonitorDBで、高いCPU使用率が発生する場合があります。インデックスを追加することで、CPU使用率を約10〜15%削減できます。
- オンプレミスのCitrix Virtual Apps and Desktops 2402では、Citrix Broker Serviceが高いメモリ使用量を示し、メモリリークが原因である可能性があり、3〜4時間ごとにDelivery Controllerの再起動が必要になります。
- 複数のDelivery Controller (DDC) インスタンスを持つサイトを2203 CU6から2402にアップグレードする際、最初のDelivery Controllerをアップグレードするときに「データベースと通信で

きません。データベースが実行されていることを確認してください」というエラーで失敗する場合があります。

マシン作成サービス

- Citrix 2402のMachine Creation Services™ (MCS) で、既存のカタログに追加しようとしたマシンの半分しか成功しないという断続的な問題が発生する場合があります。マシンはActive Directoryに表示されますが、Studioには成功したマシンのみが表示され、失敗したマシンはActive Directoryから手動でインポートされるまでNutanixハイパーバイザーに表示されません。
- Google Cloud Platform (GCP) では、2402でDaisy仮想マシン用のイメージが非推奨になったため、イメージのエクスポートが失敗します。

メタインストーラー

- VDAから2402にアップグレードする際、インストールが「MSI製品 'MultimediaVideoTs_x64.msi' の削除がコード 'UnknownProduct' (1605) で失敗しました」というエラーで失敗する場合があります。
- 診断情報収集機能が有効な状態でVDA 2402のインストール中にCall Homeに参加する際、「入力した資格情報は無効です」というエラーが発生する場合があります。
- 一部のVDAでVDAアップグレードの失敗が発生する場合があります。特にWorkspaceアプリがVDAと一緒に既にインストールされている場合、Workspaceアプリのインストール中に問題が発生します。

ユニバーサル プリント サーバー

印刷

- Citrix Print Management Serviceが断続的に終了し、リダイレクトされたプリンターが機能しなくなることがあります。
- セッションを再接続する前にスプーラーサービスが再起動された場合、再接続後にクライアントマップされたプリンターが消えることがあります。

シングルセッションOS用VDA

クリップボード

- 「テキストと画像にコピー」オプションを使用してコンテンツをコピーしたり、書式設定されたコンテンツをコピーしたりすると、失敗する可能性があります。

セッション/接続

- 2203 CU4にアップグレードした後、セッションからログオフしたり、公開アプリケーションウィンドウを終了したりする際に、VDAからクリアされるまでに2〜3分かかる問題が発生する可能性があります。
- セッションを再接続する前にスプーラーサービスが再起動された場合、再接続後にクライアントマップされたプリンターが消えることがあります。
- 「Windows + Print Screen」ショートカットを使用すると、Virtual Delivery Agent (VDA) で「explorer.exe」プロセスがクラッシュする可能性があります。
- ウォーターマークポリシーが有効になっている場合、ICA®セッションで継続的な画面のちらつきが発生する可能性があります。

システム例外

- CVAD 2203にアップグレードした後、デスクトップを開く際に約10秒の遅延が発生する可能性があります。
- エンドポイントから公開アプリケーションおよびデスクトップへのドラッグアンドドロップを使用すると、断続的な障害が発生する可能性があります。
- Citrix Cloudを使用している場合、Windows 2019以降およびWindows 10以降でドラッグアンドドロップが安定して動作しないことがあります。
- VDA内の大きな画像やExcelグラフの場合、セッションクリップボードのリダイレクトが失敗し、これらのアイテムをクライアント側にコピー＆ペーストできなくなる問題が発生する可能性があります。
- 公開デスクトップを起動した後、画面の左上部分が応答しなくなり、アイコンは表示されるがクリックできない状態になることがあります。この領域をアクティブにするには、他のアイコンを同時に選択する必要があります。この問題は、ドラッグアンドドロップが有効になっている場合に発生します。
- MS Teamsのようなオーディオアプリケーションを使用中にCtxAudioサービスがランダムにクラッシュするため、通話中にオーディオが機能しないことに気づくかもしれません。
- クライアントユーザーに対してランダムなUSBリダイレクトの失敗が発生し、Pinpad、TCR、プリンターなどのUSBデバイスがセッション中に消えることがあります。
- VDIセッションへの接続または再接続中に、USBヘッドセットのスピーカーとマイクのレベルが0（ミュート）に設定される問題が発生する可能性があります。この問題は断続的に発生し、レベルは手動で調整できます。
- VDA 2402 LTSRでは、公開アプリケーション内でウィンドウのドラッグが機能しないことがあります。

マルチセッションOS用VDA

クリップボード

- 「テキストと画像にコピー」オプションを使用してコンテンツをコピーしたり、書式設定されたコンテンツをコピーしたりすると、失敗する場合があります。

セッション/接続

- VDA 2402にアップグレードした後、再起動後の最初のICAセッションでグレースクリーンが表示される場合があります。これは、切断して再接続するか、最初にアプリケーションセッションを起動することで解決します。
- 2203 CU4にアップグレードした後、セッションからログオフしたり、公開アプリケーションウィンドウを終了したりすると、VDAからクリアされるまでに2〜3分かかるという問題が発生する場合があります。
- ICAセッションではバッテリーアイコンが1つしか表示されないにもかかわらず、その他のシステムトレイアイコンのリストにCitrix WinFrame Shell項目が増加していることに気づく場合があります。この蓄積は、システム設定の「個人用設定」>「タスクバー」>「その他のシステムトレイアイコン」で発生します。
- セッションを再接続する前にスプーラーサービスが再起動された場合、再接続後にクライアントマップされたプリンターが消えることがあります。
- VDAがランダムに応答しなくなり、未登録状態になることで、ユーザーがICAセッションから強制的に切断されるという問題が発生する場合があります。
- Citrixでは、ICAセッション接続時にクライアントの地理位置情報がTSVDAのVDIにリダイレクトされず、特定のアプリケーションやセキュリティ機能にとって重要です。ICAセッションを上書きするには、`GeoLocSync.exe`で`Refresh`を手動でクリックする必要がある場合があります。
- ウォーターマークポリシーが有効になっている場合、ICAセッションで画面のちらつきが継続的に発生する場合があります。

システム例外

- VDAがバッテリーステータスを受信しているにもかかわらず、Windows 11マルチセッションVDAでバッテリーステータスが表示されないという問題が発生する場合があります。
- エンドポイントから公開アプリケーションやデスクトップへのドラッグアンドドロップを使用する際に、断続的な失敗が発生する場合があります。
- Citrix Cloudを使用している場合、Windows 2019以降およびWindows 10以降でドラッグアンドドロップが常に機能しないという問題が発生する場合があります。

- 自動クライアント再接続 (ACR) が無効になっている場合、再接続するたびにイベント「MetaFrame 9006」がログに記録され、不要なエラーメッセージが多数生成されることに気づく場合があります。
- VDAで大きな画像やExcelグラフのセッションクリップボードリダイレクトが失敗し、これらの項目をクライアント側にコピー＆ペーストできないという問題が発生する場合があります。
- 公開デスクトップを起動した後、画面の左上部分が応答せず、アイコンは表示されているもののクリックできない状態になることがあります。この領域をアクティブにするには、同時に他のアイコンを選択する必要があります。この問題は、ドラッグアンドドロップが有効になっている場合に発生します。
- ローミング中にオーディオアプリケーションでクラッシュが発生する場合があります。これは、icaendpoint.dllモジュールでのハングが原因です。
- 公開されたNew Teamsアプリのシステムトレイアイコンが、VDA 2402またはVDA 2402 CU1を搭載したWindows 2022 OS上でシームレスアプリケーションとして実行されている場合、左クリックに反応しない問題が発生する可能性があります。これはアプリが最小化されている場合にのみ発生し、フルデスクトップセッションでは正常に動作します。
- クライアントユーザーでランダムなUSBリダイレクトの失敗が発生し、セッション中にPinpad、TCR、プリンターなどのUSBデバイスが消えることがあります。
- 2203 CU5ではレジストリのLastPingTimeが更新されず、切断される可能性があります。
- VDA 2402 LTSRでは、公開アプリケーション内でウィンドウのドラッグが機能しない場合があります。
- ライセンス状態の読み取り中に、wdica32.exeでバグチェック0x50が発生する場合があります。

フェデレーション認証サービス

- FASサーバー内でユーザー証明書を生成する際に、パフォーマンスの問題が発生する可能性があります。

  パフォーマンス改善を有効にするには、FASサーバーで以下のレジストリキーを設定します。

  HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\Authentication\UserCredentialService

  名前: SignerCaching

  種類: REG_SZ

  値: on

リナックス ブイディーエー

修正された問題については、個別のドキュメントにある修正された問題の記事を参照してください。

プロファイル管理

修正された問題については、個別のドキュメントにある修正された問題の記事を参照してください。

セッション録画

修正された問題については、個別のドキュメントにある修正された問題の記事を参照してください。

StoreFront™

修正された問題については、個別のドキュメントにある修正された問題の記事を参照してください。

累積更新プログラム 1 (CU1)

リリース日: August 20, 2024

このリリースについて

Citrix Virtual Apps and Desktops™ 7 2402 LTSR 累積更新プログラム 1 (CU1) は、2402 LTSR の初回リリース以降に報告された30を超える問題を修正します。

2402 LTSR (一般情報)

2402 LTSR (機能とアップグレード情報)

このリリースの新機能

Citrix Virtual Apps and Desktops 7 2402 LTSR (初回リリース) で修正された問題

このリリースの既知の問題

非推奨と削除

Citrix製品のSubscription Advantage資格日

ダウンロード

シトリックス バーチャル アプリケーションズ アンド デスクトップ 7 2402 LTSR CU1

新規展開

CU1をゼロから展開するにはどうすればよいですか?

CU1メタインストーラーを使用して、CU1に基づいた新しいCitrix Virtual Apps and Desktops環境をセットアップできます。その前に、製品についてよく理解しておくことをお勧めします。

デプロイメントの計画を開始する前に、Citrix Virtual Apps and Desktops 7 2402 LTSR (初期リリース)セクションを熟読し、技術概要、インストールと構成、およびセキュリティの各セクションに細心の注意を払ってください。セットアップがすべてのコンポーネントのシステム要件を満たしていることを確認してください。

既存の展開

何を更新しますか?

CU1は、2402 LTSRの15のベースラインコンポーネントに更新を提供します。注意：Citrixは、展開のすべてのLTSRコンポーネントをCU1に更新することを推奨しています。例：Citrix Provisioning™がLTSR展開の一部である場合、Citrix Provisioningコンポーネントを CU1に更新します。Citrix Provisioningが展開の一部でない場合、インストールまたは更新する必要はありません。

2402 LTSR CU1ベースラインコンポーネント

2402 CU1ベースラインコンポーネント	プログラムと機能に表示されるバージョン	ドキュメント
シングルセッションVDA	2402.0.1100.1256	シングルセッションVDA
マルチセッションVDA	2402.0.1100.1256	マルチセッションVDA
デリバリーコントローラー	2402.0.1100.1256	デリバリーコントローラー
シトリックス スタジオ	7.41.1100.48	シトリックス スタジオ
シトリックス ディレクター	7.41.1100.33	シトリックス ディレクター
シトリックス グループポリシー管理	7.41.1100.34	シトリックス グループポリシー管理
シトリックス グループポリシー クライアント側拡張	7.41.1100.34	

2402 CU1ベースラインコンポーネント	プログラムと機能に表示されるバージョン	ドキュメント
シトリックス ストアフロント	2402.0.1100.8	シトリックス ストアフロント
ユニバーサル プリント サーバー	7.41.1100.58	ユニバーサルプリントサーバー
セッション録画	24.2.1100	セッションレコーディング
リナックス VDA	24.02.1100.21	Linux仮想デリバリーエージェント
プロファイル管理	24.2.1100.23	プロファイル管理
Citrix フェデレーション認証サービス	10.17.1100.16	Citrix フェデレーション認証サービス (FAS)
ブラウザーコンテンツリダイレクト	15.48.1100.65	ブラウザーコンテンツリダイレクト
Citrix プローブ エージェント 2206	7.41.1100.15	ダウンロード

2402 LTSR CU1 対応コンポーネント

以下のコンポーネント（下記バージョン）は、LTSR環境と互換性があります。これらはLTSRのメリット（延長されたライフサイクルと修正のみの累積更新プログラム）の対象ではありません。Citrixは、2402環境内でこれらのコンポーネントを新しいバージョンにアップグレードするよう求める場合があります。

対応コンポーネントと機能	プログラムと機能に表示されるバージョン	ドキュメント
アプリケーションレイヤリング	2206.0.0	Citrix アプリケーションレイヤリング
HDX RealTime オプティマイゼーションパック	2.9.400.2702	HDX RealTime オプティマイゼーションパック
ライセンスサーバー	11.17.2.0_BUILD_48000	ライセンスサーバー(/ja-jp/licensing/11-17-2-48000/)

対応コンポーネントと機能	プログラムと機能に表示されるバージョン	ドキュメント
ユーザーパーソナライゼーションレイヤー	24.3.2	ユーザーパーソナライゼーションレイヤー(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/install-configure/user-personalization-layer.html)
セッションレコーディング Webプレーヤー	24.2.1100.16	セッションレコーディング Webプレーヤー
Microsoft Teamsの最適化	15.32.1000.9	Microsoft Teamsの最適化(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/multimedia/opt-ms-teams.html)
ワークスペース環境管理	2402.1.100.1	ワークスペース環境管理
XenApp & XenDesktop 7.15 LTSR VDA (最新リリース)*	最新の累積更新プログラムのみ	ドキュメント
CVAD 2402 CUx Delivery Controller を使用する Windows Server 2025 にインストールされた VDA 2411 以降	2411.x.x.x	ドキュメント

2402 LTSR CU1 の主な除外事項

以下の機能、コンポーネント、およびプラットフォームは、2402 ライフサイクルマイルストーンおよび特典の対象外です。具体的には、累積更新プログラムと拡張ライフサイクル特典は除外されます。除外された機能およびコンポーネントの更新は、通常の最新リリースを通じて利用できます。

除外されるコンポーネントと機能
AppDisks™
AppDNA®
Citrix SCOM 管理パック

除外されるコンポーネントと機能
フレームホーク
パーソナル vDisk
StoreFront Citrix オンライン統合

除外される WINDOWS プラットフォーム *
Windows 2008 32ビット (ユニバーサルプリントサーバー用)

* Citrix は、サードパーティベンダーのライフサイクルマイルストーンに基づいてプラットフォームサポートを更新する権利を留保します。

新機能

以下の新機能と機能強化がCitrix Virtual Apps and Desktops™ 7 2402 LTSR Cumulative Update 1 (CU1) で利用可能です。

スマートカード認証のサポート

Web Studio はスマートカード認証をサポートするようになり、管理者は PIV および CAC カードを使用して Web Studio にアクセスできるようになりました。詳細については、「Web Studio のスマートカード認証をセットアップする」を参照してください。

使用状況テレメトリレポートの機能強化

ライセンス使用状況テレメトリ機能の強化により、Citrix 管理環境に展開されている Citrix 製品、コンポーネント、および機能のライセンス利用状況データが収集および処理されます。この実装はライセンスコンプライアンスを確認するためのものであり、データは Citrix License Server を介して管理されます。ライセンスサーバーを最新バージョンに更新し、Citrix Cloud™ アカウントを持っている必要があります。詳細については、以下を参照してください。

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

ライセンステレメトリデータ要素のリストについては、「Citrix ライセンステレメトリデータ要素」を参照してください。

修正された問題

Citrix Virtual Apps and Desktops™ 7 2402 LTSR (初回リリース) 以降、以下の問題が修正されました。

Citrix Director (シトリックス ディレクター)

- 「フィルター - すべてのマシン」ページで、画面に表示されているすべてのマシンを選択し、リストを下にスクロールしようとすると、更新後にオブジェクトの選択が正しく機能しません。
- テーブルのレイアウトが画面の小さな部分に限定されて表示されます。
- Directorのフィルターマシンページで、「マルチセッション」タブを選択して別のページに移動した後、マシンページに戻ると、デフォルトの「シングルセッションデスクトップマシン」タブが選択されます。
- UserProfileの詳細をクリックし、テキストを選択しようとするとUserProfileBoxが消え、データのコピーが妨げられる問題が発生する可能性があります。
- UIでUI.TaskManager.EnableApplicationsオプションが無視され、アプリケーションリストがDirectorに表示されたままになることがあります。
- 2203 CU4から2402にアップグレードした後、負荷分散されたDirectorでSSONの失敗が時折発生する可能性があります。
- Secure ICAを使用してHDX™接続が確立された場合、Directorに表示されなくなることがあります。

Citrixポリシー

- GpfxSettings.dllを変更せずにGpoScannerを2404に移植できます。
- CseEngine.exeプロセスによる高いメモリ使用率が発生し、マシン登録の問題を引き起こす可能性があります。
- 以前のバージョンから2402にアップグレードした後、ポリシーを編集または作成できない場合があります。この問題は、新規インストールサイトでは発生しません。
- Citrix Virtual Apps and Desktops 2402 LTSRにアップグレードした後、双方向コンテンツリダイレクトが失敗する問題が発生する可能性があります。

シトリックス スタジオ

- Studioを公開アプリケーションとして使用する場合、またはICA®セッション下の公開VDAで使用する場合、Studioコンソールがフリーズすることがあります。

デリバリーコントローラー™

- Desktop Delivery Controller (DDC) バージョンLTSR 2203 CU5をアンインストールするか、「Citrix.Analytics」サービスを停止すると、「Citrix.Analytics」サービスが失敗します。

マシン作成サービス

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

グラフィック

- 作業中に約10秒間続く断続的な画面のブラックアウトが発生し、その間にCitrixソフトウェアグラフィックプロセス (Ctxgfx.exe) がリセットされることがあります。twencodeスレッドでアクセス違反例外が発生し、ctxExceptionHandlerがミニダンプを記録してこの問題を引き起こします。ctxExceptionHandlerは、調査のために完全なダンプを生成するように設定されています。
- デスクトップを起動する際、ctxgfxの障害により黒い画面が表示されることがあります。

メタインストーラー

- VDAWorkstationSetup_2402.exe、VDAServerSetup_2402.exe、またはVDAWorkstationCoreSetup_2402.exeを使用してCitrix Rendezvous V2をインストールすると、これらのパッケージにCitrix.Diagnostics.Tracing.dllファイルがないため、インストールが失敗する可能性があります。
- コマンドラインからCitrix Virtual Apps and Desktops 2402をインストールしようとすると、`Exclude "Local Host Cache Storage (LocalDB)"`コマンドが期待どおりに動作しません。
- Citrix Virtual Apps and Desktops 2402以降、デリバリーコントローラーで`/exclude "Local Host Cache Storage (LocalDB)"`コマンドを使用すると、LocalDBなしでインストールを続行する代わりに、SQL Server Express LocalDBデータベースソフトウェアのインストールが停止します。

ユニバーサル プリント サーバー

印刷

- cpmon.dllが原因でVDA上のWindows Print Spoolerサービスがクラッシュし、プリンターが失われたり、印刷ジョブを送信した後に印刷できなくなったりする可能性があります。

シングルセッションOS用VDA

クリップボード

- VDA 2203 LTSR CU4を使用している場合、WebP形式のコンテンツをコピー＆ペーストすると、`WfShell`が動作を停止します。

セッション/接続

- OpenTEXT ETXアプリケーションは、次のモジュールでのアクセス違反のため開くことができません。 C:\Program Files\Citrix\HDX\bin\CtxMFPlugin64.dll
- アクティブなセッションがない状態で、停止期間への移行時または停止期間からの移行時に、シングルセッションのランダムなマシンの電源オフが発生する可能性があります。

スマートカード

- サーバーVDAインスタンスでCitrixスマートカードサービスにメモリリークの問題が発生し、メモリ消費量が最大100%に達する可能性があります。

マルチセッションOS用VDA

クリップボード

- VDA 2203 LTSR CU4を使用している場合、WebP形式のコンテンツをコピー＆ペーストすると、`WfShell`が動作を停止します。

セッション/接続

- OpenTEXT ETXアプリケーションは、次のモジュールでのアクセス違反のため開くことができません。 C:\Program Files\Citrix\HDX\bin\CtxMFPlugin64.dll
- Citrix VDAでTermServiceのクラッシュが発生する可能性があります。
- VDAが断続的に応答しなくなることがあります。
- クラウドブローカーデータがVDAと同期していないというエラーが発生し、その結果、VDA上のアクティブなセッションがDirectorでログオフ状態として表示されることがあります。

スマートカード

- サーバーVDAインスタンス上のCitrixスマートカードサービスでメモリリークの問題が発生し、メモリ使用量が100%に達する可能性があります。

リナックス ブイディーエー

修正された問題については、個別のドキュメントにある修正された問題の記事を参照してください。

プロファイル管理

修正された問題については、個別のドキュメントにある修正された問題の記事を参照してください。

セッション録画

修正された問題については、個別のドキュメントにある修正された問題の記事を参照してください。

StoreFront™

修正された問題については、個別のドキュメントにある修正された問題の記事を参照してください。

2402 LTSR (初回リリース)

リリースについて

Citrix Virtual Apps and Desktops™ 向け Long Term Service Release (LTSR) プログラムは、Citrix Virtual Apps and Desktops のリリースに対して安定性と長期サポートを提供します。

LTSR は、Citrix Virtual Apps and Desktops 2203 および 1912 でも利用可能です。

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

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

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

インストールとアップグレードの手順については、以下を参照してください。

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

2402 LTSR 初回リリース ベースラインコンポーネント

2402 ベースラインコンポーネント	プログラムと機能に表示されるバージョン	ドキュメント
シングルセッションVDA	2402.0.4000.4310	シングルセッションVDA
マルチセッションVDA	2402.0.4000.4310	マルチセッションVDA
デリバリーコントローラー	7.41.100.229	デリバリーコントローラー
シトリックス スタジオ	7.41.100.251	シトリックス スタジオ
Citrix Director (シトリックス ディレクター)	7.33.4000.26	シトリックス ディレクター
Citrixグループポリシー管理	7.41.100.115	Citrixグループポリシー管理
Citrixグループポリシー クライアント側拡張	7.41.100.115	
シトリックス ストアフロント	2402.0.100.64	Citrix ストアフロント
シトリックス プロビジョニング	7.41.100	Citrix プロビジョニング
ユニバーサル プリント サーバー	7.33.4000.11	「ユニバーサルプリントサーバー」(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/printing/printing-provision-printers.html)
セッション録画	24.2.100.35	セッションレコーディング
リナックス ブイディーエー	24.02.0.93	Linux 仮想配信エージェント(/ja-jp/linux-virtual-delivery-agent.html)
プロファイル管理	24.2.100.52	プロファイル管理
Citrix フェデレーション認証サービス	10.17.100.90	Citrix フェデレーション認証サービス (FAS)(/ja-jp/federated-authentication-service/current-release.html)

2402 ベースラインコンポーネント	プログラムと機能に表示されるバージョン	ドキュメント
ブラウザコンテンツリダイレクション	15.32.4000.12	「ブラウザコンテンツリダイレクション」(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/multimedia/browser-content-redirection.html)
シトリックス プローブ エージェント 2402	7.41.100.78	ダウンロード

2402 LTSR 初期リリース互換コンポーネント

以下のバージョンで示されているコンポーネントは、LTSR環境と互換性があります。これらはLTSRのメリット（延長されたライフサイクルと修正のみの累積更新プログラム）の対象ではありません。Citrixは、2402環境内でこれらのコンポーネントを新しいバージョンにアップグレードするよう求める場合があります。

互換性のあるコンポーネントと機能	プログラムと機能に表示されるバージョン	ドキュメント
HDX リアルタイム最適化パック	2.9.600	HDX RealTime Optimization Pack (HDX RealTime最適化パック)
ライセンスサーバー	11.17.2.0_BUILD_47000	ライセンスサーバー(/ja-jp/licensing/current-release.html)
ユーザーパーソナライゼーションレイヤー	23.9.1	ユーザーパーソナライゼーションレイヤー(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/install-configure/user-personalization-layer.html)
セッションレコーディングウェブプレーヤー	22.3.4000.4	セッションレコーディングWebプレーヤー(/ja-jp/session-recording/view-recordings/session-recording-web-player.html)

互換性のあるコンポーネントと機能	プログラムと機能に表示されるバージョン	ドキュメント
Microsoft Teamsの最適化	15.32.3000.9	Microsoft Teamsの最適化(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/multimedia/opt-ms-teams.html)
ワークスペース環境管理	2402.1.100.1	ワークスペース環境管理

2402 LTSR 初期リリース 主な除外事項

以下の機能、コンポーネント、およびプラットフォームは、2402ライフサイクルマイルストーンおよび特典の対象外です。具体的には、累積更新プログラムと拡張ライフサイクル特典は除外されます。除外された機能およびコンポーネントの更新プログラムは、通常の現在のリリースを通じて利用できます。

除外されるコンポーネントと機能
AppDisks™
AppDNA®
Citrix SCOM 管理パック
フレームホーク
パーソナル vDisk
StoreFront Citrix オンライン統合

除外される WINDOWS プラットフォーム *
Windows 2008 32ビット (ユニバーサル プリント サーバー用)

* Citrix は、サードパーティベンダーのライフサイクルマイルストーンに基づいてプラットフォームサポートを更新する権利を留保します。

新機能

この記事では、Citrix Virtual Apps and Desktops™ 7 2402 LTSR の新機能と強化された機能について説明します。更新はコンポーネントごとに整理されています。

HDX

Secure HDX (プレビュー)

Secure HDX を使用できるようになりました。これは、トラフィックパス内のネットワーク要素が HDX トラフィックを検査できないようにするアプリケーションレベル暗号化 (ALE) ソリューションです。詳しくは、「Secure HDX」を参照してください。

新しい HDX Graphics ポリシー - Windows 画面ロックを許可

HDX Graphics の新しい **Windows 画面ロックを許可** ポリシーを使用すると、要件に応じてワークステーション OS 上の Citrix Virtual Desktop セッションで Windows ディスプレイのタイムアウトを変更するオプションが利用できるようになりました。 詳しくは、「Windows 画面ロックを許可」を参照してください。

オーディオポリシーの新しい損失許容モード

オーディオの損失許容モードが利用可能になり、損失許容モードポリシーを通じてオーディオ配信が可能になりました。 詳しくは、「オーディオの損失許容モード」を参照してください。

署名済みサードパーティバイナリ

Citrix が配布するバイナリは署名されるようになりました。署名済みバイナリは、Citrix が生成した証明書または信頼できるサードパーティの証明書によって検証されていることを示します。詳しくは、「VDA のインストール」を参照してください。

ブラウザコンテンツリダイレクトのシステムログの強化

システムログの強化により、ブラウザコンテンツリダイレクトで管理者が機能ステータスを監視できるようになりました。詳しくは、「ブラウザコンテンツリダイレクトのトラブルシューティング方法」を参照してください。

双方向コンテンツリダイレクト構成の強化

以前は、双方向コンテンツリダイレクトの構成には、「双方向コンテンツリダイレクトを許可」、「URL の VDA へのリダイレクトを許可」、および「URL のクライアントへのリダイレクトを許可」という 3 つの異なるポリシーの管理が必要でした。これらのポリシーには、サーバー側とクライアント側の両方での構成 (グループポリシーを通じて構成) が必要でした。このリリースから、これら 3 つのポリシーすべてを単一の統合ポリシーに統合しました。これにより、構成プロセスが簡素化および強化されるだけでなく、クライアント側の構成の要件もなくなります。詳しくは、「双方向コンテンツリダイレクト構成」を参照してください。

HDX リデューサー

セッションホストで使用するHDX圧縮アルゴリズム、またはReducerのバージョンを設定できるようになりました。 詳細については、HDX Reducerを参照してください。

EDTタイムアウトを設定するための新しいHDXレジストリ設定

レジストリを設定することで、EDTタイムアウトを構成するオプションが利用できるようになりました。詳細については、「EDTタイムアウトの構成」を参照してください。

Microsoft Teamsの最適化 - 許可リストに登録されたレジストリエントリ

Citrix Virtual Apps and Desktops 2402以降、`msedgewebview2.exe`レジストリエントリはデフォルトで許可リストに登録されているため、手動で構成する必要がなくなりました。

詳細については、Microsoftドキュメントを参照してください。

環境変数に対する仮想チャネル許可リストのサポート

信頼されたプロセスのパスでシステム環境変数を使用できるようになりました。詳細については、「システム環境変数の使用」を参照してください。

SCVMM 2025のサポート

Citrix Virtual Apps and Desktopsは、MicrosoftのSystem Center Virtual Machine Manager (SCVMM) 2025をサポートするようになりました。SCVMM 2025でサポートされる新機能の詳細については、System Center Virtual Machine Managerの新機能を参照してください。

オンプレミス向けCitrix Secure Private Access™

オンプレミス向けSecure Private AccessとZTNAおよびその他の機能強化のサポート

Citrix Secure Private Accessオンプレミスソリューションは、StoreFront™オンプレミス ポータルをWebおよびSaaSアプリへの統合アクセス ポータルとして使用し、ブラウザベースのアプリ（内部WebおよびSaaSアプリ）へのゼロトラストアクセスを容易に提供する機能により、組織全体のセキュリティとコンプライアンス体制を強化します。これは、Citrix Workspaceの統合された一部として仮想アプリおよびデスクトップとともに提供されます。Citrix Secure Private Accessオンプレミスは、顧客が管理するZero Trust Network Access (ZTNA) ソリューションであり、VPNなしで内部WebおよびSaaSアプリケーションへのアクセスを提供し、以下のシームレスなエンドユーザーエクスペリエンスを実現します。

- 最小特権の原則
- シングルサインオン (SSO)
- 多要素認証
- デバイスのポスチャ評価
- アプリケーションレベルのセキュリティ制御
- アプリ保護機能

詳しくは、「Citrix Secure Private Access for on-premises – General Availability」を参照してください。

Virtual Delivery エージェント (VDA) 2402 LTSR

VDAのインストール、アップグレード、またはアンインストール中にCitrix Workspaceアプリをインストール、アップグレード、またはアンインストールするオプション

この機能を使用すると、次のシナリオでVDAのインストール、アップグレード、またはアンインストール中にCitrix Workspaceアプリをインストール、アップグレード、またはアンインストールするかどうかを選択できます。

- VDAのインストール中に、Citrix Workspaceアプリをインストールすることを選択できます。デフォルトでは、VDAのインストール中にCitrix Workspaceアプリはインストールされません。
- VDAのアップグレード中に、Citrix WorkspaceアプリがVDAにまだインストールされていない場合、Citrix Workspaceアプリをインストールすることを選択できます。
- VDAのアップグレード中に、Citrix Workspaceアプリのバージョンをアップグレードできる場合、Citrix Workspaceアプリをアップグレードするオプションが表示されます。
- VDAのアンインストール中に、Citrix Workspaceアプリをアンインストールしないことを選択できます。デフォルトでは、VDAのアンインストール中にCitrix Workspaceアプリはアンインストールされます。詳しくは、「インストールするコンポーネントとインストール場所の選択」および「VDAをインストールするためのコマンドラインオプション」を参照してください。

VDAのWebSocketサポート

Citrix Virtual Apps and Desktopsでは、Citrix Brokering Protocol（CBP）を介してWebSocketテクノロジーを使用し、VDAとDelivery Controller間の通信を容易にできるようになりました。この機能では、VDAからDelivery Controllerへの通信にTLSポート443のみが必要です。

詳しくは、「VDAとDelivery Controller間のWebSocket通信」を参照してください。

VDAがアクセスできるローカルファイル共有からのVDA更新のサポート（プレビュー）

ローカルファイル共有からのVDAアップデートをサポートし、PowerShellコマンドを通じてVDAインストーラーの場所を指定できるようになりました。詳細については、「ローカルファイル共有からのVDAアップデートのサポート」を参照してください。

ウェブスタジオ

マシンプロファイルを使用したVMware VMのプロビジョニングのサポート

Machine Creation Service (MCS) を使用してVMware VMをプロビジョニングする際、既存のテンプレートをマシンプロファイルとして選択できるようになりました。これにより、カタログ内のVMは選択したテンプレートから設定を継承できます。

継承される設定には以下が含まれます。

- テンプレートに配置されたタグ
- カスタム属性
- vSANストレージポリシー
- 仮想ハードウェアバージョン
- vSphere仮想TPM (vTPM)
- CPU数とソケットあたりのコア数
- NIC数

詳細については、「マシンカタログの作成」を参照してください。

イメージノードを使用した準備済みイメージの管理

Web Studioで**イメージ**ノードが利用可能になり、単一のソースイメージからMCSイメージ（準備済みイメージ）を準備し、さまざまなMCSマシンカタログに展開できるようになりました。このノードは、イメージ定義、バージョン、およびカタログの作成を可能にすることで、完全なイメージライフサイクル管理を容易にします。

このノードを使用して準備されたイメージは、AzureおよびVMware環境でのみ使用できます。イメージ管理の詳細については、「イメージ管理（プレビュー）」を参照してください。

または、**Machine Catalogs**ノードを使用して、準備済みイメージを含むカタログを作成することもできます。詳細については、「マシンカタログの作成」を参照してください。

ポリシー関連

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

非推奨の機能

Web Studioでは、以下の機能と設定が非推奨になりました。

- Azure 環境:

  異なるリージョンのマスターイメージを使用して VM をプロビジョニングする機能は非推奨になりました。VM が作成されるリージョンにマスターイメージをレプリケートするには、Azure Compute Gallery を使用することをお勧めします。

- AWS 環境:

  マシンカタログのセットアップ > マシンテンプレートページにあるオプション「**マシンテンプレートのプロパティを仮想マシンに適用**」は非推奨になりました。代わりに、マシンプロファイルを使用して VM のマシンプロパティを指定することをお勧めします。

- すべてのハイパーバイザーおよびクラウドサービス環境:

  ディスクキャッシュのみでメモリキャッシュなしでライトバックキャッシュを構成する機能は非推奨になりました。メモリキャッシュサイズをゼロより大きい値に設定することをお勧めします。

シトリックス ディレクター

DirectorとのSecure Private Access統合（プレビュー）

DirectorとのSecure Private Access統合により、ヘルプデスク管理者またはフル管理者は、Directorですべてのセッションを監視およびトラブルシューティングできます。この機能をサポートするには、Director、Secure Private Access、Citrix Workspaceアプリ、およびVDAのバージョン2402以降を使用する必要があります。

利用可能なアクションには、以下の詳細の表示が含まれます。

- **セッションの選択**ポップアップ > **セッション**タブ > **WebアプリとSaaSアプリ**の下にあるユーザーのSecure Private Accessアクティブセッション
- **セッションの選択**ポップアップ > **アクセス拒否**タブの下にあるSecure Private Accessの失敗またはブロックされた列挙と失敗したアプリ起動
- アクティブおよび失敗したアプリ起動のセッションとアプリケーションの詳細ビュー
- 失敗およびブロックされた列挙のセッションとアプリケーションの詳細ビュー

詳細については、「Director との Secure Private Access 統合 (プレビュー)」ページを参照してください。

強化されたパフォーマンスメトリックパネル

パフォーマンスメトリックパネルには、リアルタイムメトリックの強化された視覚化機能があります。**セッションパフォーマンス**タブをクリックすると、リアルタイムデータとともに、ページ読み込み時間を待つことなく過去15分間のデータを表示できます。この機能強化により、管理者が複数のコンポーネントのパフォーマンスメトリックを単一のビューで関連付けられるようになるため、解決までの平均時間を短縮できます。詳細については、「パフォーマンスメトリック」セクションを参照してください。

新しいバージョンのMicrosoft Teamsのサポート

Citrix Directorは、Microsoft Teamsバージョン2.1以前をサポートするようになりました。

マシンクリエーションサービス™ (MCS)

イメージ管理 (プレビュー)

イメージ管理機能により、MCSはマスタリングフェーズをプロビジョニングワークフロー全体から分離します。

単一のソースイメージからMCSイメージ (準備済みイメージ) を準備し、複数の異なるMCSマシンカタログでそれを使用できます。この実装により、ストレージと時間のコストが大幅に削減され、VMの展開とイメージの更新プロセスが簡素化されます。

このイメージ管理機能を使用する利点は次のとおりです。

- カタログを作成せずに、準備済みイメージを事前に生成します。
- カタログの作成や更新など、複数のシナリオで準備済みイメージを再利用します。
- カタログの作成または更新時間を大幅に短縮します。

イメージ管理の詳細については、「イメージ管理 (プレビュー)」を参照してください。

VMware で複数の NIC を確認する

VMware 環境では、ホスティングユニットとマシンプロファイルテンプレートに複数のネットワークがあり、`-NetworkMapping` パラメーターが `New-ProvScheme` および `Set-ProvScheme` コマンドで使用されている場合に、さまざまな事前チェックを導入しました。複数の NIC の事前チェックリストの詳細については、「複数の NIC の確認」を参照してください。

GCP での Windows 11 VM 作成のサポート

GCP で Windows 11 VM を作成できるようになりました。マスターイメージに Windows 11 をインストールする場合は、マスターイメージ作成プロセス中に vTPM を有効にする必要がありま

す。また、マシンプロファイルソース (VM またはインスタンステンプレート) で vTPM を有効にする必要があります。

この機能は以下に適用されます。

- 永続的および非永続的 MCS マシンカタログ
- ソールテナントノードグループのみ

シングルテナントノード上に Windows 11 VM を作成する方法については、シングルテナントノード上に Windows 11 VM を作成するを参照してください。

VMware で MCS PowerShell コマンドを使用した Citrix Provisioning™ カタログ作成のサポート

VMware で MCS PowerShell コマンドを使用して Citrix Provisioning カタログを作成できるようになりました。

この実装により、次の利点が得られます。

- MCSとCitrix Provisioningカタログの両方を管理するための単一の統合API。
- ID管理ソリューション、オンデマンドプロビジョニングなど、Citrix Provisioning カタログの新機能を利用できます。

詳細については、「Citrix Studio で Citrix Provisioning カタログを作成する」を参照してください。

プロファイル管理

新機能については、別のドキュメントの「新機能」を参照してください。

リナックス VDA

新機能については、別のドキュメントの「新機能」を参照してください。

セッション録画

新機能については、別のドキュメントの「新機能」を参照してください。

ワークスペース環境管理™

新機能については、別のドキュメントの「新機能」を参照してください。

シトリックス プロビジョニング

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

フェデレーション認証サービス

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

修正された問題

Citrix Virtual Apps and Desktops™ 7 2311以降、以下の問題が修正されました。

全般

- オーディオデバイス名が200文字を超えると、デバイスが仮想セッションにリダイレクトされない場合があります。
- Webカメラのリダイレクトの場合、セカンドホップへのRDPクライアントはサポートされていません。
- 以下に説明するように環境が構成されているデスクトップセッションで画像をスキャンすると、画像がスキャンされない場合があります。この問題は断続的に発生します。
  - スキャナードライバーとイメージングアプリケーションのインストール。
  - DDCでUSBリダイレクトポリシーが有効になっている。
  - 環境設定:
    - DDCにおける Win2k19 + 7.33CU4
    - VDA: Win2k19/Win2k16+ 7.40.0.191
    - クライアント: Win10x64 22H2 + CWA 24.1.0.597
- SSLが有効でセッションの信頼性がオフの場合、2番目のシームレスアプリの起動に失敗します。シームレスアプリが起動された場合、同じサーバーへの別のシームレスアプリのその後の起動は、既存のセッション（セッション共有）で起動される必要がありますが、クライアントはアプリを新しいセッションで起動する傾向があり、ブローカーに予期しない検証要求が送信されます。。
- ステレオオーディオストリームにモノラルオーディオを使用している場合、両耳で両方のチャンネルを受信する代わりに、片方のイヤホンで1つのオーディオチャンネルしか聞こえない場合があります。

デリバリーコントローラー™

- 監視データベースの`MonitorData.ResourceUtilization`テーブルの更新が遅延します。
- Windows 10でVDAバージョン2203 CU3を使用している場合、Rendezvous Proxyが構成されていると、VDAインストーラーはカスタムWCFポートをホストしません。

ディレクター

- **Multi Forest Site**でマルチセッションまたはシングルセッションデスクトップVDAを使用すると、ユーザー中心の検索機能が動作しません。

グラフィック

- Windows 11バージョン22H2で、セッション内でWindows Media Playerウィンドウを移動すると、ビデオの下半分のみが表示されます。回避策として、 > > > > を選択します。
- Citrix Virtual Apps and Desktops 2203を使用している場合、切断されたセッションに再接続する際に黒い画面が表示されることがあります。

ポリシー

- Citrix Virtual Apps and DesktopsをバージョンCU3からCU4またはCU5にアップグレードした後、VDAがDelivery Controllerに登録されず、未登録のままになることがあります。
- VDA上で、`CSEngine.exe` が予想よりも多くのメモリを消費しています。

スタジオ

- 「すべて」のスコープを持たないカスタム管理者は、デフォルトのポリシーセットからポリシーを編集または削除できません。回避策として、カスタム管理者がアクセスできるスコープをデフォルトポリシーに追加します。
- 展開で*Citrix Studio*と*Web Studio*の両方を使用している場合、*Citrix Studio*でアプリケーションフォルダーを作成しても、そこにアプリケーションを追加しないと、その空のフォルダーが*Web Studio*に表示されないという問題が発生する可能性があります。
- Web Studioを使用してAzureへのホスティング接続を作成する際に、**接続の詳細**ページで**サービスプリンシパルの作成**をクリックし、**次へ**をクリックすると、エラーが発生する場合があります。この問題を解決するには、ブラウザでサードパーティCookieを許可してください。
- Citrix Studioを介してStoreFront™サーバーアドレスを追加し、それをデリバリーグループに割り当てると、ストアはデフォルトでオフに設定されます。

ユニバーサル プリント サーバー

印刷

- VDAバージョン1912 CU5およびOSバージョン2012 R2を使用している場合、本番環境のCitrix UPSプリントサーバーからのさまざまな印刷ジョブが、次のエラーメッセージとともに失敗します。 `CCgpStream::Open: WaitForMultipleObjects time out.` `InternalUpcRemoteOpenStream: Failed to Open Stream. Abort Job.`

- Citrix Virtual Apps and Desktopsバージョン2212または2305でUPSバージョン2212または2305をWindows 10 VDAとともに使用すると、CUPSを使用するプリンターに次のメッセージが表示されます。 `Access Denied, cannot connect message`

シングルセッションOS用VDA

- Windows VDAを使用しているときに、日本語キーボードから韓国語キーボードに切り替えると、キーボードマッピングエラーが発生する場合があります。
- `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\GroupPolicy` レジストリキーの下にある `SaveRsopToFile`、`SaveRsopToMemory`、および `SaveRsopToRegistry` の値が復元されない場合があります。
- VDAをバージョン2203にアップグレードした後、Skype for Businessアプリがスプラッシュ画面で応答しなくなることがあります。
- VDA上で、`CSEngine.exe` が予想よりも多くのメモリを消費しています。
- Broker Agentでのデッドロックにより、DNS IPアドレスの変更時にマシンが再登録されなくなります。
- この修正により、コアコンポーネントのインストールまたはアップグレード時に、マシン上の以前のWindowsインストールからの保留中の再起動のチェックを防ぐコマンドラインオプション `/no_pending_reboot_check` が導入されます。
- VDAの再起動後、`WebSocketService.exe` プロセスが起動に失敗します。
- VDAバージョンLTSR 2203 CU 4.1を使用すると、セッションの開始時またはセッション中に、VDAが次のメッセージとともにバグチェックを実行する場合があります。

  `Error "StopCode: SYSTEM THREAD EXCEPTION NOT HANDLED": Tdica.sys`

- マシンを使用すると、ユーザーセッションの起動が断続的に失敗します。
- ICA®セッションの再接続中に、サードパーティ製メッセージングアプリケーションのチャットウィンドウが自動的に前面に表示されることがあります。
- ローカルワークステーションからVDA LTSR 2203のCitrixセッションにファイルをコピーして貼り付けると、`Wfshell.exe` プロセスがクラッシュする可能性があります。
- Windows 10 VDAバージョン2308を使用すると、`ctxappvservice.exe` プロセスがクラッシュする可能性があります。
- 公開されたMicrosoft Visioまたはデスクトップ上のVisioアプリからユーザーデバイス上のアプリにコンテンツをコピーすると、失敗する場合があります。
- WebSocketService (HTML5 Video Redirection WebSocker Service) がクラッシュする可能性があります。

- Virtual Apps and Desktops 2203 LTSR、Citrix Workspace™ app 2203 LTSR CU3 (2303または2205)、およびWindows 11 22h2を搭載したVDA 2203 LTSRを使用している場合、再接続後に左モニターの左半分に設定されたアプリケーションが画面の中央に誤って表示されます。

マルチセッションOS用VDA

- VDA上で `WebSocketService.exe` プロセスが予想よりも多くのメモリを消費する可能性があります。
- VDA上で `CSEngine.exe` が予想よりも多くのメモリを消費しています。
- Broker Agentのデッドロックにより、DNS IPの変更時にマシンが再登録できなくなります。
- VDAの再起動後、 `WebSocketService.exe` プロセスが起動に失敗します。
- VDAバージョンLTSR 2203 CU 4.1を使用すると、セッションの開始時またはセッション中に、VDAが次のメッセージとともにバグチェックを実行する場合があります。 `Error "StopCode: SYSTEM THREAD EXCEPTION NOT HANDLED": Tdica.sys`
- 公開アプリケーションセッションで実行されている場合、Citrix Workspaceアプリの一部のプロセスが予期したとおりに閉じない場合があります。
- Server 2019 VDAバージョンLTSR 2203 CU3では、 `WmiPrvSE.exe` がクラッシュします。
- VDA LTSR 2203のCitrixセッションにローカルワークステーションからファイルをコピーアンドペーストすると、 `Wfshell.exe` プロセスがクラッシュする場合があります。
- ACR再接続後、ターミナルサービスプロセスがクラッシュする場合があります。
- Windows Server 2022では、アプリまたはOSによってマウスが特定の場所に移動された場合、アプリまたはOSによってマウスが別の場所に移動されるまで、その位置にマウスを再度移動できません。
- **Session Idle**の制限時間が有効になっているにもかかわらず、2022 OS VDAのICAセッションに**Warning Idle Time Expired Message**ダイアログボックスが表示されません。
- デスクトップ上の公開されたMicrosoft VisioまたはVisioアプリからユーザーデバイス上のアプリにコンテンツをコピーすると、失敗する場合があります。

プロファイル管理

修正された問題については、個別のドキュメントにある修正された問題の記事を参照してください。

リナックス ブイディーエー

修正された問題については、個別のドキュメントにある修正された問題の記事を参照してください。

セッション録画

修正された問題については、個別のドキュメントにある修正された問題の記事を参照してください。

ワークスペース環境管理™

修正された問題については、個別のドキュメントにある修正された問題の記事を参照してください。

シトリックス プロビジョニング™

修正された問題については、個別のドキュメントにある修正された問題の記事を参照してください。

フェデレーション認証サービス

修正された問題については、個別のドキュメントにある修正された問題の記事を参照してください。

既知の問題

注

- 本記事の2402初期リリースおよびCU1セクションに記載されている既知の問題は、修正済み問題のリストに含まれていない限り、CU2にも引き続き存在します。
- 既知の問題に回避策がある場合は、問題の説明の後に記載されています。
- レジストリエントリの変更を推奨する回避策には、以下の警告が適用されます。

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

2402 CU4の既知の問題

- DDCがLicensing Activation Service (LAS)用に構成されている状態で、MMCベースのStudioでライセンスを更新すると、V6ライセンスファイルの詳細は一時的に誤って表示されます。これにより、MMC Studio内でのライセンス情報の正確な表示が一時的に影響を受けます。回避するには、MMC Studioを閉じて再度開きます。

2402 CU3の既知の問題

- CVAD 2402 LTSR CU3から2411へのアップグレードが失敗する可能性があります。回避策として、2503以降の新しいバージョンにアップグレードできます。
- 2402 CU3 VDAにアップグレードすると、Secure HDX™ポリシーは以前のデフォルトの無効状態から許可に更新されます。
- 複数のタブでブラウザコンテンツリダイレクトを全画面で使用している場合、タブをゆっくりドラッグアウトしているときに、ブラウザのビューポートが飛び出すことがあります。ドラッグが停止すると、ブラウザのビューポートはブラウザ画面に調整されます。
- HTML5ビデオのリダイレクトを使用している場合、自動再生されないビデオでは、利用可能な場合でもビデオコントロールが表示されないことがあります。

2402 CU2の既知の問題

- Outlookアプリケーションを起動してログオンした後の最初のログオン時に、Outlookのシステムトレイメニューが表示される場合がありますが、右クリックしてもアクションメニューはポップアップしません。回避策として、セッションからログオフして再度ログオンすると、メニューにアクセスできます。
- シームレスアプリケーションを起動した後、設定ウィンドウで、閉じる（'X'）ボタンがウィンドウから分離して初期位置に残るという問題が発生する可能性があります。
- シングルサインオン (SSO) に拡張ドメインパススルーを使用している場合、ユーザーが最初に接続したとき、セッション内のアプリケーションへのSSOは期待どおりに機能します。しかし、ユーザーが切断し、後で同じセッションに再接続すると、セッション内のSSOが機能しなくなる可能性があります。これは、2025年3月および4月にリリースされたWindowsアップデートで導入されたリグレッションが原因です。この問題が発生しているお客様は、Microsoftにサポートケースを開き、追跡ID 2410230030007977を参照することをお勧めします。

2402 CU1 の既知の問題

- Virtual Channel Dynamin Plugin Manager 機能は UI に表示されますが、現在のバージョンではサポートされていません。

- Delivery Groups Administrator および Delivery Groups カスタムスコープで Web Studio にログインすると、 を選択してシングルセッション OS マシンまたはマルチセッションマシンからタグを削除しようとしたときにエラーが発生する場合があります。
- StoreFront 2402 を 2402 CU1 にアップグレードした後、ドイツ語デバイスのユーザーは、ブラウザーで Citrix Workspace アプリおよび Citrix Workspace Web クライアントにサインインできない場合があります。サインインページが読み込まれても結果が表示されないことがあります。詳しくは、CTX691873 を参照してください。

2402 初期リリースの既知の問題

- レジストリエントリの変更を推奨する回避策には、次の警告が適用されます。

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

全般

- VDA をアップグレードする前に Citrix Files for Windows および/または Citrix Files for Office がインストールされている場合、これらのコンポーネントはアップグレードプロセス中にアンインストールされます。これを解決するには、VDA のアップグレードが完了した後、コンポーネントを再インストールしてください。
- アプリバーを起動してから、Windows 向け Citrix Workspace™ アプリで接続センターメニューを開くと、アプリバーがホストサーバーの下に表示されません。
- Windows 向け Citrix Workspace アプリを使用し、アプリバーを垂直位置で起動すると、バーがスタートメニューまたはシステムクロックトレイを覆います。
- ユーザーがホスト上で既にフォーカスされているコンボボックスを選択すると、コンボボックスが正しく表示されない場合があります。回避策として、別の UI 要素を選択してからコンボボックスを選択してください。
- Windows 10 から Windows 11 へのインプレース OS アップグレードを実行した後、Citrix Desktop Service が起動に失敗する場合があります。この問題を解決するには、マシンを再起動してください。

- マルチセッション VDA の **セッション制限** 設定は、Windows Server 2022、Windows 10 Enterprise マルチセッション、および Windows 11 Enterprise マルチセッションを実行しているセッションホストでは拒否されます。 回避策として、GPO を介して **RDS セッション時間制限** を構成できます。
- 管理者権限でアプリケーションを実行している場合、FIDO2 に関連付けられた Windows セキュリティダイアログボックスは ICA® セッションウィンドウの前面に表示されません。昇格されたプロセスとして実行されている場合、Windows セキュリティダイアログボックスが ICA セッションウィンドウの背後に隠れるのは、オペレーティングシステムの設計によるものです。
- クライアントから ICA セッションへの 100MB を超えるデータのクリップボードコピーアンドペーストが失敗する場合があります。大きなバッファーのコピーはサポートされていません。
- Windows 10またはWindows 11マルチセッションOSはWindowsシステムの復元をサポートしていません。そのため、UIで復元ポイントを作成するオプションは利用できません。コマンドラインオプション`/EnableRestore`または`/EnableRestoreCleanup`は無視され、「**システムの復元は現在Windows 10/11マルチセッションOSではサポートされていません**」というメッセージがログに記録されます。
- Citrixは、Citrixが生成したバイナリとサードパーティのバイナリの両方に署名します。これは、バイナリがCitrixによって認証されることを意味します。サードパーティのバイナリのバージョンは、サードパーティから調達されたものと同じままです。バイナリがすでにインストールされている場合、バージョンが一致するため、VDAのアップグレードではバイナリはインストールされません。この制限を回避するには：

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

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

- 一部のシナリオでは、クライアントIPポリシーフィルターを使用すると、ポリシーの評価に使用されるIPアドレスが正しくありません。
- シングルサインオンに拡張ドメインパススルーを使用している場合、クライアントデバイスまたはセッションホストがWindows 11を実行していると、セッションへのSSOが失敗する可能性があります。
- ポリシー設定の更新とサイトサービスでのBLOBの生成との間に5分の遅延があります。その結果、ポリシーが更新され、セッションに反映されるまでに時間がかかる場合があります。

- CVAD 2311で追加された新しいApp-V関連機能により、App-V機能はWeb Studioでのみ完全にサポートされるようになりました。App-VにMMC Studioを使用すると問題が発生する可能性があります。

  a. 既存のApp-Vアプリケーションが動作しなくなる可能性があります

  Delivery Controller (DDC) を2402 LTSR CU3またはそれ以前の2402 LTSRバージョン、あるいは2507 RTMにアップグレードした後、 以前MMC Studioを使用して作成されたApp-Vアプリケーションが期待どおりに機能しなくなる可能性があります。回避策として： 2402 LTSR CU3またはそれ以前の2402 LTSRバージョンの場合、siteDBでSQLを実行します：

```
-- Convert Broker Apps which are Packaged Apps to be explicitly
labeled as such.

-- this is detected by the presence of ctxAppVLauncher.exe on the
command line

-- The application record in the Applibrary and the related Package
and Library denote which packaging technology was used.



    update chb_Config.Applications

    set ApplicationType = 4, --$ATPackagedApplication

        --NB: The AppLibrary's LibaryUid and the Broker's
PackagedApplicationType have the same value

        PackagedApplicationType = case

                                    when
TRY_CONVERT(uniqueidentifier, A.CommandLineArguments) is null then 2
--Dual Admin

                                    else 1 -- Single Admin.

                                            -- This is a bug with
legacy MMC Studio not understanding the new Broker App format. But
only App-V apps can be affected

                                end,
```

```
        PackagedApplicationId = case

                                    when
TRY_CONVERT(uniqueidentifier, A.CommandLineArguments) is null then
REPLACE(A.CommandLineArguments, N'"','')

                                    else CONVERT(char(36),
CONVERT(uniqueIdentifier,  A.CommandLineArguments))

                                end

    from chb_Config.Applications A

        inner join chb_Config.ApplicationsMetadata AMD on A.Uid =
AMD.ApplicationUid

    where A.CommandLineExecutable like N'%ctxAppVLauncher.exe'

        and A.ApplicationType = 0 --$ATHostedOnDesktop

        and AMD.Name = 'Citrix_DesktopStudio_SequenceLocation'

        and right(AMD.Value, 5) = '.appv'
```

b. MMC Studioで新しいApp-Vアプリケーションを作成する

2402 LTSRおよび2507 LTSRでは、MMC Studioを介して新しいApp-Vアプリケーションを作成すると、正しく機能しない場合があります。新しいApp-Vアプリケーションを作成するには、Web Studioを使用することをお勧めします。

ポリシー

- Citrix Virtual Apps and Desktopsの以前のバージョンから2311または2402 LTSRにアップグレードする場合、ポリシー設定に無効なデータ値が存在すると、ポリシーデータが失われる可能性があります。この問題と関連する回避策の詳細については、CTX666304を参照してください。

グラフィック

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

- Skype for desktopアプリで、リモートデスクトップに接続されている余分なWebカメラに気づく場合があります。これらの余分なWebカメラのプレビューはセキュリティ上の理由からブロックされ、黒い画面が表示されることがあります。余分なWebカメラは無視して、エンドポイントのWebカメラを使い続けることができます。
- IntelおよびNVIDIA GPUでのH265 444は、セッションでアーティファクトが表示される原因となる可能性があります。Intel GPUに関連する問題については、セッションのサイズを変更するか、フルスクリーンモードを切り替える一時的な回避策があります。

マシン作成サービス™

- AWSでホストされているVMware環境では、マスターイメージでvTPMが有効になっている場合、MCSマシンカタログの作成が失敗します。この問題は、すべてのCitrix Virtual Apps and Desktopsバージョンに影響し、VMware環境の問題が原因です。サポートについては、VMwareサポートにお問い合わせください。
- 一部の2402 LTSR以前のバージョン（バージョン2302、2305、2308、2311を含む）から2402 LTSRにMulti-Delivery Controllerサイトをアップグレードする際、サイトが部分的にしかアップグレードされていない場合、VMでの電源操作が失敗する可能性があります。詳細については、CTX666299を参照してください。

印刷

- 仮想デスクトップで選択されたUniversal Print Serverプリンターは、コントロールパネルの**デバイスとプリンター**ウィンドウに表示されません。ただし、ユーザーがアプリケーションで作業しているときは、それらのプリンターを使用できます。この問題はWindows 10でのみ発生します。詳細については、CTX213540を参照してください。
- 印刷ダイアログウィンドウでデフォルトプリンターが正しくマークされない場合があります。この問題は、デフォルトプリンターに送信される印刷ジョブには影響しません。
- Universal Print ServerへのSSL接続が有効になっている場合、ロードバランスされたネットワークプリンターからの印刷ジョブの一部が失敗することがあります。これは、印刷ジョブが次々と高速に実行された場合に発生します。
- **Citrix VDAが既にインストールされているマシンでインプレースWindowsアップグレード後に印刷が失敗する可能性がある** インプレースWindowsアップグレード後、Citrix印刷プロバイダーが呼び出されなくなり、印刷の失敗につながる可能性があります。この問題は、Windowsアップグレードプロセスが印刷プロバイダーの実行順序をリセットし、Citrix登録済みプロバイダーを保持しないために発生します。Microsoftは、これがWindowsの動作であり、アップグレード中に実行順序のプロバイダー登録を現在保持しないことを確認しています。

回避策は、印刷プロバイダーを適切なレジストリの場所に戻すことです。

```
1.  Open the Registry Editor.

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

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

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

1.  Reboot the VDA.
```

FIDO2

- 仮想アプリまたはデスクトップセッション内でChromiumベースのブラウザーを使用している場合、ブラウザーがChromiumバージョン147以降を実行していると、FIDO2キーの登録が機能しません。

VDAバージョン2503以降にアップグレードすると、この問題は解決されます。

または、回避策として、FIDO2リダイレクトを無効にし、USBリダイレクトを利用してFIDO2キーをセッションにリダイレクトできます。詳細については、USBリダイレクトを参照してください。

サードパーティの問題

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

プロファイル管理

- 既知の問題については、既知の問題の記事を参照してください。

リナックス VDA

- 既知の問題については、既知の問題の記事を参照してください。

セッション録画

- 既知の問題については、既知の問題の記事を参照してください。

ワークスペース環境管理™

- 既知の問題については、既知の問題の記事を参照してください。

シトリックス プロビジョニング™

- 既知の問題については、既知の問題の記事を参照してください。

フェデレーション認証サービス

- 既知の問題については、既知の問題の記事を参照してください。

廃止予定と削除

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

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

非推奨事項

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

項目	非推奨が発表されたバージョン	代替
サードパーティ製 HPE Moonshot Machine Manager プラグイン	2402	(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/install-configure/install-prepare/hpe-moonshot.html#install-the-citrix-managed-hpe-moonshot-plug-in)を使用してください。
ファイルベースライセンス	2507	License Activation Service (LAS) は、Citrix製品スイート全体で製品のアクティベーションを行うための次世代テクノロジーです。ファイルベースのライセンスを使用しているお客様は、互換性のあるリリースにアップグレードし、April 15, 2026までにこのテクノロジー移行を実行する必要があります。April 15, 2026以降、LASはCitrixオンプレミスコンポーネントをアクティベートおよびライセンス供与する唯一の方法となります。
ランデブー V1	2402	Rendezvous V2を使用してください。
セキュア ICA®	2402	Secure HDXを使用してください。

項目	非推奨が発表されたバージョン	代替
Windows Server 2016でのVDAサポート	2402	最新のWindows Serverバージョンにアップグレードしてください。
Windows Server 2016でのDelivery Controller™、Web Studio、Citrix Director、Citrix License Server、Citrix StoreFront、シングルセッションOS用Server VDI、マルチセッションOS用VDA、Active Directoryフォレストおよびドメイン、Universal Print Serverのサポート	2402	Windows Server の最新バージョンにアップグレードしてください。
サイト構成、構成ログ、および監視データベースに対するMicrosoft SQL Server バージョン 2016 および 2017 のサポート	2402	Microsoft SQL Server の最新バージョンにアップグレードしてください。
ディスクキャッシュのみを含み、メモリキャッシュを含まないライトバックキャッシュを構成するためのサポート	2402	メモリキャッシュサイズの構成オプションを使用し、ゼロ以外のサイズを割り当ててください。
オンデマンドプロビジョニング機能より前に作成されたAzureカタログ	2402	Azure レガシーカタログVMを再作成します。カタログはオンデマンドでプロビ

項目	非推奨が発表されたバージョン	代替
（「レガシー」カタログ）のサポート		ジョニングされるため、ストレージコストを節約できます。
ターゲット最小フレームレートポリシー	2311	**グラフィックステータスインジケーター**を使用して、ターゲット最小フレームレートを変更します。
System Center Configuration Manager に対応する Citrix Connector 3.1 のサポート	2311	イメージまたはアプリケーションの更新を手動で行います。
カタログが作成されたリージョンとは異なるリージョンでのマスターイメージの使用のサポート	2311	Azure Compute Gallery を使用して、マスターイメージを目的のリージョンにレプリケートします。
HDX™ グラフィック表示メモリ制限設定	2311	クライアントの表示レイアウトが完全に収まるように、必要な最小メモリ量が割り当てられます。
HDX Graphicsでのプログレッシブモードのサポート	2311	Thinwireを使用してください。プログレッシブモードを参照してください。
Internet Explorer 11 でのブラウザーコンテンツリダイレクトのサポート	2311	Google Chromeベースのブラウザーコンテンツリダイレクトを使用してください。

項目	非推奨が発表されたバージョン	代替
AWSボリュームワーカーのサポートを削除しました	2311	ディスクの直接アップロードとダウンロードを使用します。ディスクの直接アップロードとダウンロードを参照してください。
BrokerでのSQL Server 2016のサポート	2308	最新バージョンを使用してください。詳しくは、システム要件を参照してください。
DirectorでのXenApp 5.xのサポート	2308	---
DirectorでのXenApp 6.xのサポート	2308	---
Director のアラート用 SCOM パック	2308	---
Director のプラグインのサポート	2308	---
WebRTC SDP 形式 (プラン B) のサポート	2308	Citrix Workspace™ アプリをサポートされているバージョンにアップグレードしてください。
Microsoft Teams 最適化におけるシングルウィンドウモードのサポート	2308	Citrix Workspace アプリをマルチウィンドウモードをサポートするバージョンにアップグレードしてください。詳細については、「機能マトリックスとバージョ

項目	非推奨が発表されたバージョン	代替
		ンサポート」を参照してください。
AWS環境で使用される `AwsCaptureInstanceProperties` のサポート	2308	マシンプロファイルを使用します。マシンプロファイルを使用してカタログを作成するを参照してください。
`Schedule-ProvVMUpdate` PowerShellコマンド	2305	`Set-ProvVMUpdateTimeWindow` を使用します。
`Request-ProvVMUpdate` PowerShellコマンド	2305	`-StartsNow` および `-DurationInMinutes -1` パラメーターとともに `Set-ProvVMUpdateTimeWindow` を使用します。
`Cancel-ProvVMUpdate` PowerShellコマンド	2305	`Clear-ProvVMUpdateTimeWindow` を使用します。
`New-ProvScheme` コマンドで使用される `DedicatedTenancy` パラメーター	2303	`TenancyType` パラメーターを使用します。
ライセンスサーバーVPX	2206	---

項目	非推奨が発表されたバージョン	代替
ホストからクライアントへの (URL) リダイレクト	2203	双方向コンテンツリダイレクト。
クラウドおよびオンプレミス環境で使用される、AWS 固有の 4 つのコマンド (`Revoke-HypSecurityGroupIngress`、`Revoke-HypSecurityGroupEgress`、`Grant-HypSecuritygroupegress`、`Grant-HypSecurityGroupIngress`) のサポート。	2203	---
VDA メタインストーラーからの Citrix Files for Windows および Citrix Files for Outlook。	2203	スタンドアロンインストーラー を使用します。
VDA メタインストーラーからの WEM Agent コンポーネント。	2203	---
Remote PC Access 用の SCCM 統合 Wake on LAN オプション。	2012	スタンドアロンの Wake on LAN 機能 を使用します。
Citrix Studio での PVS インポートウィザードのサポート	1912 LTSR	Citrix Provisioning マシンをプロビジョニングするには、次

項目	非推奨が発表されたバージョン	代替	
		のいずれかの方法を使用します • Citrix Provisioning コンソールを使用してマシンをプロビジョニングし、Citrix Provisioning デバイスエクスポートウィザードを使用して Citrix Virtual Apps and Desktops にエクスポートします。詳細については、「デバイスエクスポートウィザード」を参照してください。	
XenApp および XenDesktop、Provisioning Services、StoreFront 用の Citrix SCOM Management Pack。監視できる製品バージョンについては、「Citrix SCOM Management Pack	1912	展開の監視と管理には Director を使用します。SCOM の EOL と代替の詳細については、https://support.citrix.com/article/CTX266943 を参照してください。	

項目	非推奨が発表されたバージョン	代替
のドキュメント」を参照してください。		
モビリティ SDK / モバイル SDK (旧 Citrix Labs 製)	7.16	モバイルエクスペリエンスポリシー設定、およびホストされたデスクトップ/アプリのネイティブエクスペリエンスに置き換えられました。

削除された機能

削除された項目は、Citrix Virtual Apps and Desktops で削除されたか、サポートされなくなりました。

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

項目	廃止が発表されたバージョン	削除されたバージョン	代替
NVIDIA GPUハードウェアエンコード (NVENC) (vGPU 11以前、およびドライバーバージョン 466.77以前)。	2305	2305	現在サポートされているNVIDIAドライバーを使用してください: vGPU 13以降、バージョン 471.41以降。
VDAメタインストーラーからのCitrix Supportability Tools (SupportabilityTool_x64 .msi)。	---	2212	---
Citrix License Administration Console (Windows License Server 11.16.3 build 30000 に最後に含まれ、Windows License Server v11.16.6 build 31000 で削除されました)。	2003	2006	Citrix Licensing Manager を使用します。
Windows 10 バージョン 1709 以前での Citrix Indirect Display Driver (IDD) グラフィックアダプターのサポート。	2003	2003	Citrix Virtual Apps and Desktops 7 1912 LTSR VDA を使用します。
GRID 9 以前のディスプレイドライバーを使用した NVIDIA GPU (NVENC) によるハードウェアエンコード。	2003	2003	Citrix Virtual Apps and Desktops 7 2003 以降の VDA で GRID 10 ディスプレイドライバーを使用するか、Citrix Virtual Apps and Desktops 7 1912 LTSR VDA を使用します。

項目	廃止が発表されたバージョン	削除されたバージョン	代替
セルフサービスパスワードリセット (SSPR) 機能。	2003	2006	---
VDAおよびコアサーバーコンポーネント向けのMicrosoft .NET Frameworkバージョン4.8より前のバージョンに対するサポート。Delivery Controller、Studio、Directorが含まれます。	1912	2003	.NET Framework バージョン4.8にアップグレードします。
Windows Server 2012 R2 上で動作するVDA。	1912	2003	サポートされているオペレーティングシステムにVDAをインストールします。
Citrix Virtual Apps and Desktops PremiumエディションのAppDNA®アプリケーション移行コンポーネント。	1909	2003	---
32ビット（x86）マシンへのStudioのインストール。	1909	2003	サポートされているx64オペレーティングシステムにインストールします。
シームレスアプリケーションにおけるExcelフックのサポート。これは、Microsoft Excel 2010の各ワークブックに対して個別のタスク	1909	1909	---

項目	廃止が発表されたバージョン	削除されたバージョン	代替
バーアイコンを作成するために使用されていました。			
Windows Server 2012 R2（サービスパックを含む）上のコアサーバーコンポーネント。以下が含まれます：Delivery Controller、Studio、Director。	1906	2003	より新しいサポート対象のオペレーティングシステムにインストールしてください。
Microsoft SQL Serverバージョン 2008 R2、2012、2014（すべてのサービスパックおよびエディションを含む）上のサイト構成、構成ログ、および監視データベースのサポート。	1906	2003	サポートされているMicrosoft SQL Serverバージョンにデータベースをインストールします。
x86プラットフォーム上のWindows 10におけるVDAのサポート。	1906	1909*	サポートされているx64オペレーティングシステムにVDAをインストールします。 *この機能は、Citrix Virtual Apps and Desktops 7 1912 LTSRで引き続きサポートされています。
Citrix Virtual Apps and Desktopsインストールメディアからのインストール時のCitrix Smart Tools Agentの削除。	1903	1906	---

項目	廃止が発表されたバージョン	削除されたバージョン	代替
StoreFront内の以下のサポート終了製品（VDI-in-a-Box、およびXenMobile（9.0以前））に対するDelivery Controllerオプションの削除。	1903	1903	---
Red Hat Enterprise Linux/CentOS 7.5でのLinux VDAのサポート。	1903	1903	Red Hat Enterprise Linux の新しいバージョンに Linux VDA をインストールしてください。
Citrix Virtual Apps and Desktops（旧XenAppおよびXenDesktop）とCitrix Receiver、およびWorkspace Hub間のTLS 1.0およびTLS 1.1プロトコルに対するStoreFrontのサポート。	7.17	2203	Citrix Receiverを、TLS 1.2プロトコルをサポートするCitrix Workspaceアプリにアップグレードします。Citrix Workspaceアプリの詳細については、https://docs.citrix.com/ja-jp/citrix-workspace-app を参照してください。
ポリシー設定「インボックスプリンタードライバーの自動インストール」に対するVDAのサポート。	7.16	2311	なし。ポリシー設定は、以前のOS（Windows 7、Windows Server 2012 R2以前）のVDAでのみサポートされます。
デスクトップアプライアンスサイト上のデスクトップにユーザーがアクセスする	1811	1912	ドメインに参加していないユースケースには、(/ja-jp/citrix-workspace-app-for-windows/workspace-

項目	廃止が発表されたバージョン	削除されたバージョン	代替
ためのStoreFrontサポート			windows-desktop-lock.html)を使用します。
Framehawkディスプレイリモートテクノロジーのサポート	1811	1903	(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/hdx-transport/adaptive-transport.html)を有効にして、(/ja-jp/xenapp-and-xendesktop/current-release/graphics/thinwire.html)を使用します。
すべてのCitrix Virtual Apps and Desktops（およびXenApp and XenDesktop）バージョンにおけるCitrix Smart Scaleのサポート。この機能は31 May 2019にサポート終了となります。	1808	1906	電源管理機能の改善のために、Citrix Cloud上の(/ja-jp/citrix-daas.html)の使用を検討してください。
Citrix StoreFront、Citrix VDA、Citrix Studio、Citrix Director、およびCitrix Delivery ControllerによるMicrosoft .NET Frameworkバージョン4.5.1、4.5.2、4.6、4.6.1、4.6.2、および4.7のサポート。	7.18	1808	.NET Framework バージョン 4.7.1 以降にアップグレードしてください。(インストーラーは、まだインストールされていない場合、.NET Framework 4.7.1 を自動的にインストールします。)

項目	廃止が発表されたバージョン	削除されたバージョン	代替
Red Hat Enterprise Linux 7.3 上の Linux VDA のサポート。	7.18	1808	Red Hat Enterprise Linux の新しいバージョンに Linux VDA をインストールしてください。
SUSE Linux Enterprise Server 11 Service Pack 4 上で動作する Linux VDA のサポート。	7.16	7.16	サポートされている SUSEバージョンに Linux VDAをインストールしてください。
VDA 上の Citrix WDDM ドライバーのサポート	7.16	7.16	Citrix WDDM ドライバーは、VDA とともにインストールされなくなりました。
Windows 10 バージョン 1511 (Threshold 2) およびそれ以前の Windows シングルセッション OS リリース (Windows 8.x および Windows 7 を含む) 上の VDA (<https://www.citrix.com/blogs/2018/01/08/the-citrix-strategy-for-windows-7-virtual-desktop-users/> を参照)。	7.15 LTSR (および 7.12)	7.16	Windows 10 最小バージョン 1607 (Redstone 1) 以降の半期チャネルにシングルセッション OS VDA をインストールします。1607 LTSB を使用している場合は、7.15 VDA をお勧めします。CTX224843 を参照してください。
Windows Server 2008 R2 および Windows Server 2012 (サービスパックを含む) 上の VDA	7.15 LTSR (および 7.12)	7.16	サポートされているオペレーティングシステムにVDAをインストールします。

項目	廃止が発表されたバージョン	削除されたバージョン	代替
デスクトップコンポジションリダイレクト (以前は DirectX Command Remoting と呼ばれていました) (DCR)	7.15 LTSR	7.16	Thinwire を使用します。
Citrix Receiver for Web のクラシックエクスペリエンス (「緑の吹き出し」ユーザーインターフェイス)	7.15 LTSR (および StoreFront 3.12)	1903	Citrix Receiver for Web の統合エクスペリエンス。
Windows Server 2012 および Windows Server 2008 R2 (Service Pack を含む) 上のコアコンポーネント。含まれるもの: Delivery Controller、Studio、Director、StoreFront、License Server、Universal Print Server。	7.15 LTSR	7.18	サポートされているオペレーティングシステムにコンポーネントをインストールします。
Windows Server 2012 および Windows Server 2008 R2 (Service Pack を含む) 上のセルフサービスパスワードリセット (SSPR) 機能	7.15 LTSR	7.18	より新しいサポート対象のオペレーティングシステムにインストールしてください。
Windows 7、Windows 8、および Windows 8.1	7.15 LTSR	7.18	サポートされているオペレーティングシステムに Studio をインストールします。

項目	廃止が発表されたバージョン	削除されたバージョン	代替
(Service Pack を含む) 上の Studio			
Flashリダイレクト	7.15 LTSR	1912	HTML5ビデオとしてビデオコンテンツを作成します。管理対象コンテンツにはHTML5ビデオリダイレクトを、公開Webサイトにはブラウザコンテンツリダイレクトを使用します。詳細については、Flashリダイレクトのサポート終了の注記を参照してください。
StoreFrontとのCitrix Online統合（Goto製品）	7.14（およびStoreFront 3.11）	StoreFront 3.12	---
VDAのインストール中に作成され、VDAマシンのローカル管理者グループに追加されていたユーザーアカウントCtxAppVCOMAdminは、作成されなくなりました。基盤となる「COM」メカニズムも削除されました。	7.14	7.14	WindowsサービスCtxAppVServiceは同じ機能を実行します。これは自動的にインストールおよび構成され、ユーザーによる操作は不要です。
Windows Server 2008 32ビットでのUniversal Print Server UpsServerコ	7.14	7.14	より新しいサポート対象のオペレーティングシステムにインストールしてください。

項目	廃止が発表されたバージョン	削除されたバージョン	代替
ンポーネントのサポート			
Internet Explorer 8 での ストアフロントおよび レシーバー・フォー・ウェブ	7.13	7.13	---
Citrix App-Vコンポーネントのインストールを防止するためのVDAコマンドラインインストールオプション /no_appv	7.13	7.13	コマンドラインインストールオプション /exclude "Citrix Personalization for App-V – VDA" を使用します。
フルプロダクトインストーラーは、新規インストール時にCitrix.Common.Commandsスナップインをインストールしなくなり、既存のインストールをアップグレードする際に自動的に削除します。	7.13	7.13	Citrix.Common.Commandsスナップインによって提供されていた一部のPowerShellコマンドは、XenApp 6.5 SDKで引き続き利用可能です。
*-CtxIconコマンドレットによって提供されていた、アイコンデータを操作する部分的な機能。	7.13	7.13	現在はBroker Serviceの*-BrokerIconコマンドレットによって提供されています。
レガシーThinwireモード	7.12	7.16	Thinwireを使用します。Windows Server 2008 R2でレガシーThinwireモードを使用している場合は、Windows Server 2012 R2またはWindows Server 2016に移行し、

項目	廃止が発表されたバージョン	削除されたバージョン	代替
			Thinwireを使用してください。
StoreFront 2.0、2.1、2.5、および2.5.2からのインプレースアップグレード	7.13	7.16	これらのバージョンのいずれかから、より新しいサポート対象バージョンにアップグレードし、その後XenAppおよびXenDesktop 7.16にアップグレードします。
XenDesktop 5.6または5.6 FP1からのインプレースアップグレード	7.12	7.16	XenDesktop 5.6または5.6 FP1の展開を現在のXenDesktopバージョンに移行します。これを行うには、まずXenDesktop 7.6 LTSR（最新のCUを含む）にアップグレードし、次に最新のCitrix Virtual Desktops（旧XenDesktop）リリースまたはLTSRバージョンにアップグレードします。
32ビット（x86）マシンへのDelivery Controller、Director、StoreFront、またはLicense Serverのインストール。	7.12	7.16	サポートされているx64オペレーティングシステムにインストールします。
コネクションリース	7.12	7.16	ローカルホストキャッシュを使用します。

項目	廃止が発表されたバージョン	削除されたバージョン	代替
Windows XPで使用されるXenDesktop 5.6。Windows XPへのVDAインストールはサポートされていません。	7.12	7.16	サポートされているオペレーティングシステムにVDAをインストールします。
CloudPlatform接続のサポート	7.12	2003	別のサポートされているハイパーバイザーまたはクラウドサービスを使用します。
Azure Classic（Azure Service Managementとも呼ばれる）接続のサポート	7.12	2003	Citrix Cloud上のVirtual Apps and Desktops Serviceの使用を検討してください。
AppDisks機能（およびそれをサポートするStudioへのAppDNA統合）	7.13	2003	Citrix App Layeringを使用してください。
パーソナル vDisk 機能	7.15	2006†	Citrix App Layering ユーザーレイヤーまたはユーザーパーソナライゼーションレイヤーテクノロジーを使用してください。

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

システム要件

はじめに

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

インストールを開始する前に、インストールの準備を確認してください。

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

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

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

ハードウェア要件

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

次の表に、コアコンポーネントの最小要件を示します。

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

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

デスクトップとアプリケーションを提供するVMのサイジング

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

詳細については、以下を参照してください。

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

マイクロソフト ビジュアル C++

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

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

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

デリバリーコントローラー

サポートされているオペレーティングシステム:

- ウィンドウズ サーバー コア 2022
- ウィンドウズ サーバー 2022
- Windows Server 2019、StandardおよびDatacenter Edition、およびServer Coreオプション付き
- Windows Server 2016、StandardおよびDatacenterエディション、Server Coreオプション付き

要件:

- Microsoft .NET Framework 4.8（またはそれ以降のバージョン）がまだインストールされていない場合、自動的にインストールされます。
- Windows PowerShell 3.0、4.0、または5.0。
- Microsoft Visual C++ 2015–2019 再頒布可能パッケージ。
- Citrix Virtual Apps and Desktopsバージョン2407から2411以降にアップグレードする場合、またはバージョン2411以降を新規インストールする場合は、最初のステップとしてライセンスサーバーを最新バージョン（バージョン11.2.17ビルド53100以降）に更新してください。その後、Delivery Controllerをアップグレードします。これを怠ると、UIに警告メッセージが表示され、コマンドラインインストールが失敗します。

データベース

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

- SQL Server 2022、Express、Standard、およびEnterprise エディション。
  - 新規インストールの場合：既存のサポートされているSQL Serverインストールが検出されない場合、Controllerのインストール時に、累積更新プログラム14が適用されたSQL Server Express 2022がデフォルトでインストールされます。
- SQL Server 2019、Express、Standard、およびEnterprise エディション。
- SQL Server 2017、Express、Standard、および Enterprise エディション。

    - アップグレードの場合、既存のSQL Server Expressバージョンはアップグレードされません。

- SQL Server 2016 SP2、Express、Standard、および Enterprise エディション。

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

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

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

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

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

その他のデータベース情報:

- データベース
- CTX114501は、現在サポートされている最新のデータベースを一覧表示します
- データベースのサイジングに関するガイダンス
- ローカルホストキャッシュ

ウェブスタジオ

> **注：**

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

サポートされているオペレーティングシステム:

- ウィンドウズ サーバー コア 2022
- ウィンドウズ サーバー 2022
- Windows Server 2019、StandardおよびDatacenterエディション、Server Coreオプション付き
- Windows Server 2016、StandardおよびDatacenterエディション、Server Coreオプション付き

シトリックス ディレクター

サポートされているオペレーティングシステム:

- ウィンドウズ サーバー コア 2022
- ウィンドウズ サーバー 2022
- Windows Server 2019、StandardおよびDatacenter Edition、およびServer Coreオプション
- Windows Server 2016、StandardおよびDatacenterエディション、Server Coreオプション付き

要件:

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

シトリックス プロファイル マネージメント:

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

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

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

Directorの表示でサポートされているブラウザー:

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

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

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

サポートされているオペレーティングシステム:

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

要件:

- Microsoft .NET Framework 4.8がまだインストールされていない場合（またはそれ以降のバージョンがインストールされていない場合）、自動的にインストールされます。
- Microsoft Visual C++ 2015–2019 再頒布可能パッケージ。

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

複数のマルチメディアアクセラレーション機能（HDX MediaStream Windows Media Redirectionなど）を使用するには、VDAをインストールするマシンにMicrosoft Media Foundationがインストールされている必要があります。マシンにMedia Foundationがインストールされていない場合、

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

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

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

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

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

サポートされているオペレーティングシステム:

- Windows 11 (Citrix DaaS™でのみサポート)
- Windows 10 (x64のみ、Citrix DaaSでのみサポート)、現在メインストリームサポート中のすべてのバージョン。
- ウィンドウズ サーバー 2022
- Windows Server 2019、StandardおよびDatacenterエディション
- Windows Server 2016、Standard、および Datacenter エディション

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

- Microsoft .NET Framework 4.8 がまだインストールされていない場合（またはそれ以降のバージョンがインストールされていない場合）、自動的にインストールされます。
- Microsoft Visual C++ 2015–2019 再頒布可能パッケージ。

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

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

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

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

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

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

ホスト / 仮想化リソース

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

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

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

サポートされているハイパーバイザー:

- **ゼノサーバー (旧称 シトリックス ハイパーバイザー™)**

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

  詳細については、「XenServer仮想化環境」(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/install-configure/install-prepare/xenserver.html)を参照してください。
- **マイクロソフト システム センター バーチャル マシン マネージャー**

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

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

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

- **Nutanix アクロポリス**

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

  詳細については、Nutanix仮想化環境を参照してください。

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

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

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

  詳細については、VMware仮想化環境を参照してください。

サポートされているパブリッククラウドホスト:

- **アマゾン ウェブ サービス (AWS)**

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

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

- **マイクロソフト アジュール リソース マネージャー**

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

- **Nutanix クラウドおよびパートナーソリューション**

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

- **VMware クラウドおよびパートナーソリューション**

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

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

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

Active Directoryの機能レベル

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

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

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

HDX

オーディオ

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

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

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

HDX Windows Media の配信

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

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

HDX 3D Pro 機能

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

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

- GPUパススルーは以下で利用可能です。
  - XenServer®
  - ニュータニックス AHV
  - VMware vSphereおよびVMware ESX（ここでは仮想Direct Graphics Acceleration (vDGA) と呼ばれます）
  - Windows Server 2016のMicrosoft Hyper-V。ここではDiscrete Device Assignment (DDA) と呼ばれます。
- vGPU は以下で利用可能です:
  - XenServer
  - ニュータニックス AHV
  - ヴイエムウェア ブイスフィア

`<https://docs.citrix.com/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/graphics/hdx-3d-pro>`を参照してください。

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

グラフィック処理ユニット (GPU):

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

ユーザーデバイス:

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

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

ユニバーサル プリント サーバー

Universal Print Serverは、クライアントコンポーネントとサーバーコンポーネントで構成されています。UpsClientコンポーネントはVDAインストールに含まれています。ユーザーセッションで

Citrix Universal™ Print Driverを使用してプロビジョニングしたい共有プリンターが存在する各プリントサーバーにUpsServerコンポーネントをインストールします。

UpsServerコンポーネントは以下でサポートされています。

- ウィンドウズ サーバー 2022
- Windows サーバー 2019
- Windows サーバー 2016

要件:

- Microsoft Visual C++ 2015–2019 再頒布可能パッケージ
- マイクロソフト .NET フレームワーク 4.8 (最小)

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

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

詳しくは、「プリンターのプロビジョニング」を参照してください。

その他

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

バージョン互換性の詳細については、製品マトリックスを参照してください。

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

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

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

複数のNICがサポートされています。

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

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

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

この製品はPowerShellバージョン3から5をサポートしています。

技術概要

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

Citrix Virtual Apps and Desktops により、以下が可能になります。

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

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

主要コンポーネント

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

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

一般的な展開における主要コンポーネント(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/components-new-op.png)

デリバリーコントローラー™

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

- アプリケーションとデスクトップを配信する

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

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

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

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

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

データベース

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

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

仮想配信エージェント (VDA)

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

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

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

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

シトリックス ストアフロント™

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

シトリックス ワークスペース™ アプリ

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

スタジオ

Citrix Virtual Apps and Desktops展開は、Web Studio（Webベース）とCitrix Studio（Windowsベース）の2つの管理コンソールを使用して管理できます。この製品ドキュメントでは、Web Studioのみを扱います。Citrix Studioの詳細については、Citrix Virtual Apps and Desktops 7 2212以前を参照してください。

ウェブスタジオ

Web Studioは、オンプレミスのCitrix Virtual Apps and Desktops展開を構成および管理できるWebベースの管理コンソールです。これは、ユーザーエクスペリエンスの向上を目的として設計されており、Windowsベースの管理コンソールであるCitrix Studioよりも一般的に応答が高速です。「Web Studioのインストール」(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/install-configure/install-core/install-web-studio.html)を参照してください。

シトリックス スタジオ

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

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

セキュアプライベートアクセス

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

シトリックス ディレクター

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

Directorは以下を表示します。

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

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

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

Citrix ライセンスサーバー

ライセンスサーバーは、Citrix製品ライセンスを管理します。コントローラーと通信して各ユーザーセッションのライセンスを管理し、Studioと通信してライセンスファイルを割り当てます。サイトには、ライセンスファイルを保存および管理するために少なくとも1つのライセンスサーバーが必要です。

ハイパーバイザーまたはその他のサービス

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

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

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

追加コンポーネント

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

シトリックス プロビジョニング™

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

シトリックス ゲートウェイ

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

(DMZ) に展開される SSL VPN アプライアンスです。これは、企業ファイアウォールを介した単一の安全なアクセスポイントを提供します。

シトリックス SD-WAN™

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

一般的な展開の仕組み

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

展開におけるコンポーネント間の通信(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/deployment-overview.png)

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

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

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

ユーザー接続の処理方法

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

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

ユーザーの資格情報は、この経路を通ってControllerにアクセスし、ControllerはBroker Serviceと通信して必要なリソースを決定します。Citrixは、Citrix Workspaceアプリから送信される資格情報を暗号化するために、管理者がStoreFrontにSSL証明書を配置することを推奨しています。

ユーザー接続フロー(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/user-connections.png)

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

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

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

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

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

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

データアクセスが機能する仕組み

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

展開におけるデータアクセス(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/data-access.png)

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

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

DirectorはCitrix Gatewayにもアクセスして、HDXデータに関する情報を取得できます。

デスクトップとアプリケーションの配信

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

マシンカタログ

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

通常、マスターイメージを作成し、それを使用してカタログ内に同一のVMを作成します。VMの場合、そのカタログ内のマシンのプロビジョニング方法を指定できます。Citrixツール（Citrix ProvisioningまたはMCS）またはその他のツールです。あるいは、既存のイメージを使用すること

もできます。その場合、ターゲットデバイスは個別に、またはサードパーティの電子ソフトウェア配布（ESD）ツールを使用して一括で管理する必要があります。

有効なマシンタイプは次のとおりです。

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

詳しくは、「Citrix Virtual Apps and Desktops Image Management」および「マシンカタログの作成」を参照してください。

デリバリーグループ

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

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

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

詳細については、「デリバリーグループの作成」を参照してください。

アプリケーショングループ

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

詳細については、「」(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/install-configure/application-groups-create.html)を参照してください。

詳細情報

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

データベース

> **注：**

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

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

- **サイト:** (サイト構成とも呼ばれます) 実行中のサイト構成、現在のセッション状態、および接続情報を保存します。

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

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

Citrixは、データベースに関して以下を推奨します。

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

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

高可用性

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

- **AlwaysOn可用性グループ (基本可用性グループを含む):** SQL Server 2012で導入されたこのエンタープライズレベルの高可用性および災害復旧ソリューションは、1つ以上のデータベースの可用性を最大化できます。AlwaysOn可用性グループでは、SQL Serverインスタンスが Windows Server Failover Clustering (WSFC) ノードに存在する必要があります。詳細については、「SQL ServerでのWindows Server Failover Clustering」を参照してください。
- **SQL Serverデータベースミラーリング:** データベースをミラーリングすることで、アクティブなデータベースサーバーが失われた場合でも、数秒で自動フェールオーバープロセスが発生し、ユーザーは通常影響を受けません。この方法は、各データベースサーバーで完全なSQL

Serverライセンスが必要となるため、他のソリューションよりも高価です。ミラーリング環境ではSQL Server Expressエディションを使用できません。

- **SQLクラスタリング:** Microsoft SQLクラスタリングテクノロジーを使用すると、障害が発生した別のサーバーのタスクと責任を1つのサーバーが自動的に引き継ぐことができます。ただし、このソリューションのセットアップはより複雑であり、自動フェールオーバープロセスは通常、SQLミラーリングなどの代替手段よりも遅くなります。
- **ハイパーバイザーの高可用性機能を使用する:** この方法では、データベースを仮想マシンとして展開し、ハイパーバイザーの高可用性機能を使用します。このソリューションは、既存のハイパーバイザーソフトウェアを使用し、SQL Server Expressエディションも使用できるため、ミラーリングよりも安価です。ただし、データベース用に新しいマシンが起動するのに時間がかかる場合があり、ユーザーへのサービスが中断される可能性があるため、自動フェールオーバープロセスは遅くなります。

Local Host Cache機能は、SQL Serverの高可用性のベストプラクティスを補完します。Local Host Cacheを使用すると、サイトデータベースが利用できない場合でも、ユーザーはアプリケーションやデスクトップに接続および再接続できます。詳細については、「Local Host Cache」を参照してください。

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

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

データベースソフトウェアのインストール

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

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

Network Serviceアカウントを使用します。Controllerは、追加のSQL Serverロールや権限を必要としません。

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

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

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

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

サイト作成ウィザードからデータベースをセットアップする

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

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

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

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

1. SQL Server ソフトウェアを2台のサーバー (AとB) にインストールします。
2. サーバーAで、プリンシパルとして使用するデータベースを作成します。サーバーAのデータベースをバックアップし、サーバーBにコピーします。

3. サーバーBで、バックアップファイルを復元します。
4. サーバーAでミラーリングを開始します。

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

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

自動セットアップ

必要なデータベース権限がある場合は、サイト作成ウィザードの「**データベース**」ページで「**Studioからデータベースを作成および設定**」を選択します。その後、主要データベースの名前とアドレスを指定します。

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

スクリプトによるセットアップ

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

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

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

   スクリプトの保存場所を指定できます。

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

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

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

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

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

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

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

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

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

データベースのセットアップに必要な権限

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

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

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

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

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

優先データベース権限スクリプト

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

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

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

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

詳細については、コマンドレットのヘルプを参照してください。

データベースアドレスの形式

データベースアドレスは、次のいずれかの形式で指定できます。

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

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

データベースミラーリングの場合は、プリンシパルサーバーアドレスのみを指定します。Citrix Site Managerは、プリンシパルサーバーに基づいてミラーサーバーを特定します。

スタンドアロンSQLサーバー、データベースミラーリング、およびAlways On高可用性の構成方法の詳細については、このCTX記事を参照してください。

データベースの場所を変更する

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

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

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

データベースの場所を変更するには：

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

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

詳細情報

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

配信方法

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

はじめに

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

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

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

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

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

Citrix Virtual Apps™公開アプリとデスクトップ

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

ユースケース:

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

利点と考慮事項:

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

ユーザーエクスペリエンス:

- ユーザーは、StoreFront™、**スタート**メニュー、または提供されたURLから1つ以上のアプリケーションを要求します。

- アプリケーションは仮想的に配信され、ユーザーデバイス上で高解像度でシームレスに表示されます。
- プロファイル設定に応じて、ユーザーのアプリケーションセッションが終了するとユーザーの変更が保存されます。それ以外の場合、変更は削除されます。

アプリケーションの処理、ホスト、および配信:

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

セッション管理と割り当て:

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

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

VMホスト型アプリ

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

ユースケース:

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

利点と考慮事項:

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

ユーザーエクスペリエンス：

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

アプリケーションの処理、ホスト、および配信：

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

セッション管理と割り当て：

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

VDIデスクトップ

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

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

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

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

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

リモートPCアクセス

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

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

詳細については、リモートPCアクセス。

ネットワークポート

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

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

ポート情報が必要になる場合があります。

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

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

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

HDX™

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

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

仮想チャネル(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/hdx-vir-channels.png)

HDXは、次の3つの技術原則に基づいて設計されています。

- インテリジェントリダイレクト
- 適応型圧縮
- データ重複排除

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

- **インテリジェントリダイレクト** - インテリジェントリダイレクトは、画面アクティビティ、アプリケーションコマンド、エンドポイントデバイス、ネットワークおよびサーバーの機能を検査し、アプリケーションまたはデスクトップのアクティビティをどこでどのようにレンダリン

グするかを即座に決定します。レンダリングは、エンドポイントデバイスまたはホスティングサーバーのいずれかで実行できます。

- **適応型圧縮** - 適応型圧縮により、リッチなマルチメディアディスプレイを低帯域幅のネットワーク接続で配信できます。HDXはまず、入力、デバイス、ディスプレイの種類（テキスト、ビデオ、音声、マルチメディア）など、いくつかの変数を評価します。最適な圧縮コーデックと、CPUおよびGPU使用率の最適な比率を選択します。その後、各固有のユーザーと状況に基づいてインテリジェントに適応します。このインテリジェントな適応は、ユーザーごと、あるいはセッションごとに行われます。

  適応型圧縮(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/hdx-adaptive-compression.png)

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

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

デバイス上での動作

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

ネットワーク上

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

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

データセンター内

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

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

HDX インサイト

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

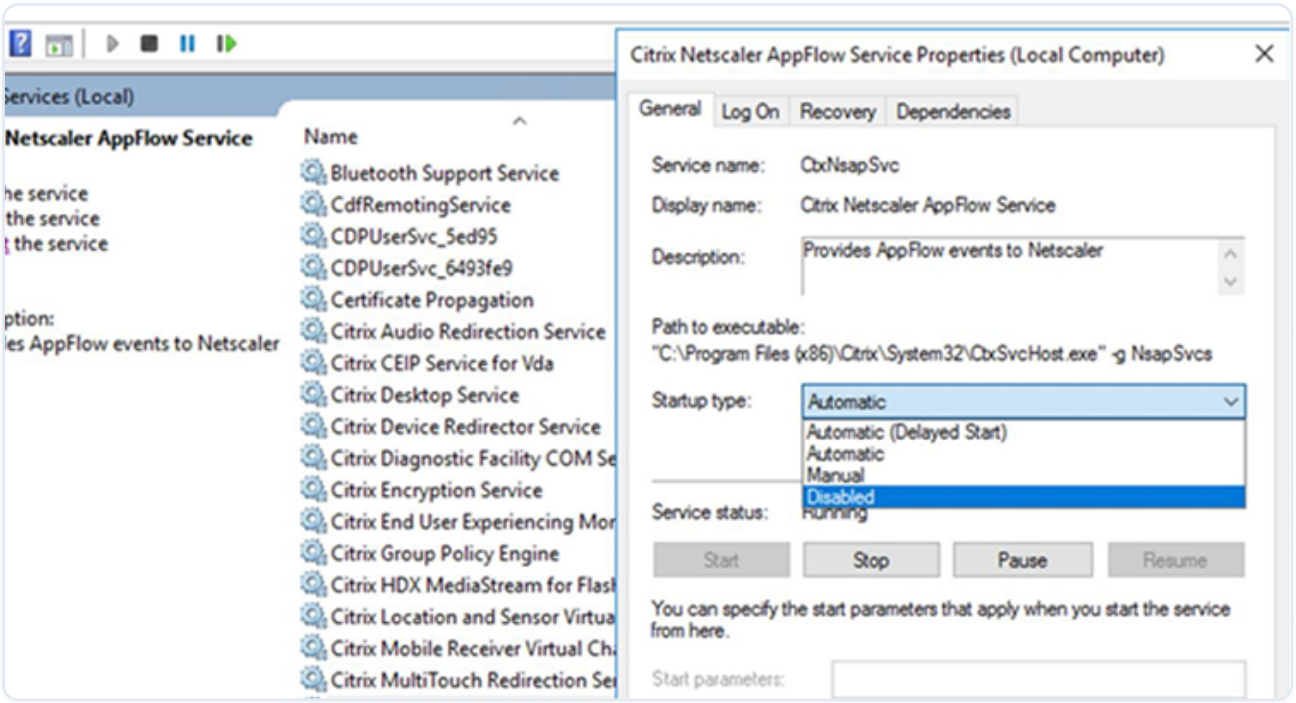
NetScalerでHDX Insight仮想チャネルを使用して、必要なすべてのデータポイントを非圧縮形式で移動させることができます。この機能を無効にすると、NetScalerデバイスは、さまざまな仮想チャネルに分散されたICA®トラフィックを復号化および解凍します。単一の仮想チャネルを使用することで、複雑さが軽減され、スケーラビリティが向上し、費用対効果が高まります。

最小要件:

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

HDX Insight仮想チャネルの有効化または無効化

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



仮想デスクトップからHDX機能を利用する

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

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

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

- HDXが高品位オーディオをどのように提供するかを確認するには、次の手順を実行します。

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

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

HDXは、ほとんどのユーザーに優れたグラフィックとビデオのエクスペリエンスをデフォルトで提供し、構成は不要です。ほとんどのユースケースで最高のエクスペリエンスを提供するCitrixポリシー設定は、デフォルトで有効になっています。

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

知っておくと良いこと:

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

自動クライアント再接続とセッションの信頼性

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

自動クライアント再接続:

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

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

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

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

自動クライアント再接続のデフォルト設定：

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

詳細については、(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/policies/reference/ica-policy-settings/auto-client-reconnect-policy-settings.html)のを参照してください。

セッションの信頼性:

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

- **デスクトップ。** セッションウィンドウが半透明になり、再接続までの時間をカウントダウンタイマーが表示します。

- **アプリケーション。** ウィンドウが半透明になり、通知領域から接続中断のポップアップが表示されます。

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

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

デフォルトのセッションの信頼性設定

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

詳細については、(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/policies/reference/ica-policy-settings/session-reliability-policy-settings.html)のを参照してください。

NetScalerと自動クライアント再接続およびセッションの信頼性:

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

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

HDX アダプティブスループット

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

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

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

この機能には、以下の要件があります。

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

ユーザーデバイスに送信される画質の向上

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

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

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

ビデオ会議のパフォーマンスを向上させる

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

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

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

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

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

ネットワークトラフィックの優先順位

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

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

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

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

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

警告:

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

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

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

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

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

リモート言語バーの表示/非表示

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

VDAから言語バー機能のクライアント制御を無効にするには：

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

Unicodeキーボードマッピング

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

Unicode キーボードレイアウトマッピングを有効または無効にする

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

KEY_LOCAL_MACHINE/SOFTWARE/Citrix/CtxKlMap

名前: EnableKlMap

種類: DWORD

値: 1

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

Unicode キーボードレイアウトマッピング互換モードを有効にする

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

HKEY_LOCAL_MACHINE/SOFTWARE/Citrix/CtxKlMap

名前: DisableWindowHook

種類: DWORD

値: 1

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

Citrix ICA® 仮想チャネル

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

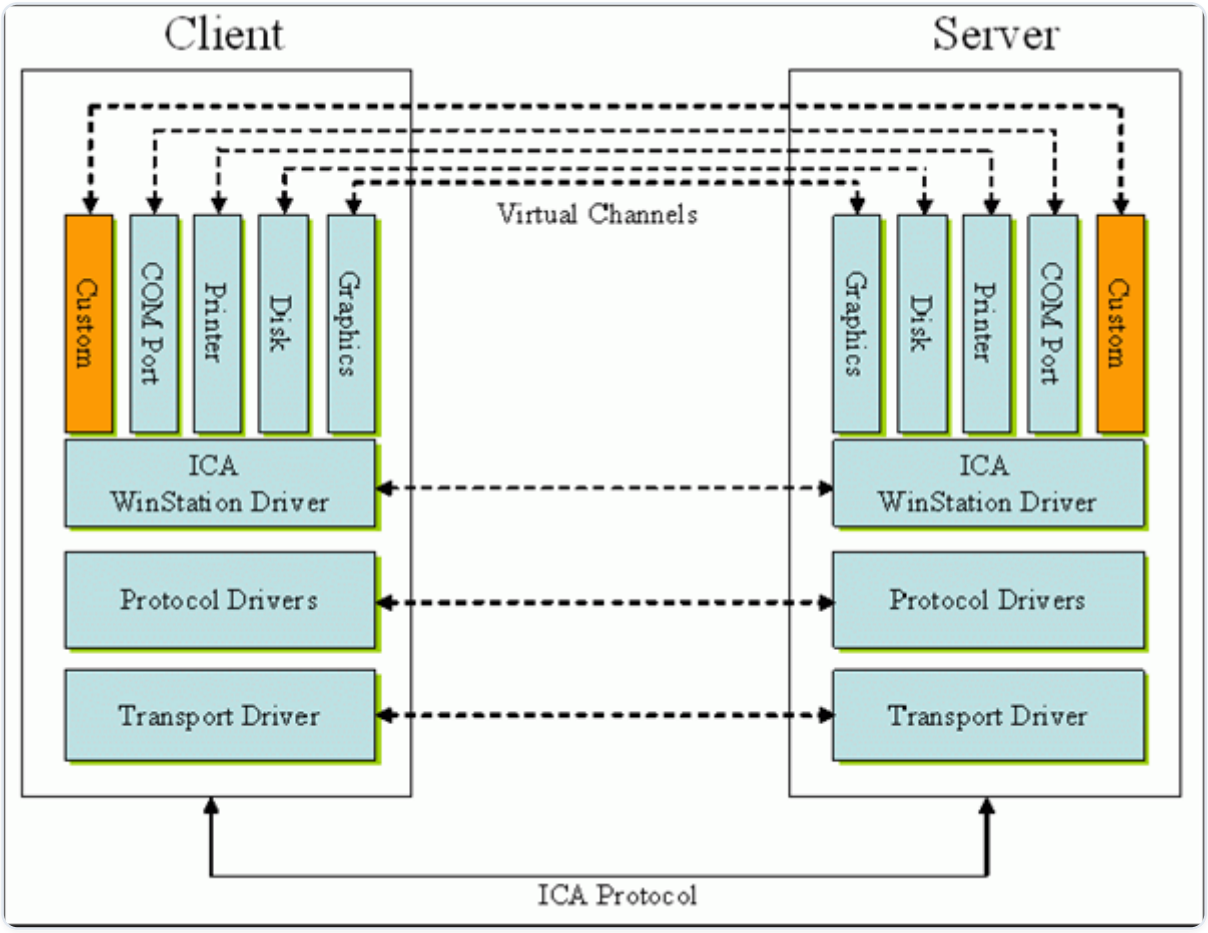
ICA仮想チャネルとは?

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

- オーディオ
- COMポート
- ディスク

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

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



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

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

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

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

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

または

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

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

> **注：**

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

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

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

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

64ビット互換性

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

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

汎用USB仮想チャネル

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

- ctxusbm.sys
- ctxusbr.sys

ICA仮想チャネルの仕組み

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

シェルによってロードされる仮想チャネルモジュール（例）：

- EUEM

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

一部はカーネルモードとしてロードされます。例:

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

サーバー側のグラフィック仮想チャネル

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

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

Windowsサービスでの特殊チャネルのホスティング

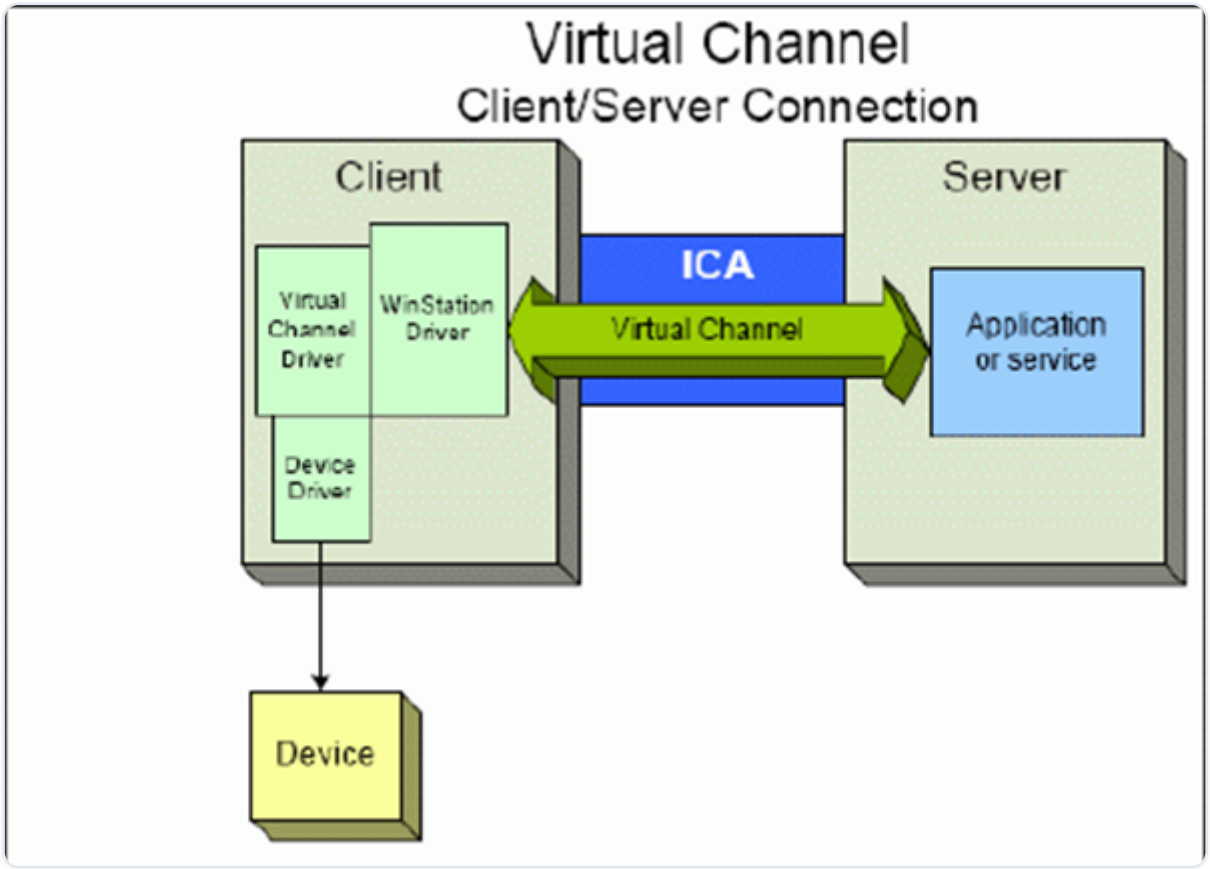
Citrix Virtual Apps and Desktopsサーバーでは、さまざまなチャネルがWindowsサービスとしてホストされます。このようなホスティングは、セッション内の複数のアプリケーションとサーバー上の複数のセッションに対して、1対多のセマンティクスを提供します。このようなサービスの例を次に示します。

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

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

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

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



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

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

- サーバーアプリケーションがクライアントに送信するデータがある場合、データは直ちにクライアントに送信されます。クライアントがデータを受信すると、WinStationドライバーはICAストリームから仮想チャネルデータをデマルチプレックスし、直ちにクライアント仮想ドライバーに渡します。
- クライアント仮想ドライバーがサーバーに送信するデータがある場合、データはWinStationドライバーが次回ポーリングしたときに送信されます。サーバーがデータを受信すると、仮想チャネルアプリケーションが読み取るまでキューに入れられます。データが受信されたことをサーバー仮想チャネルアプリケーションに通知する方法はありません。

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

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

注：

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

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

注：

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

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

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

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

仮想チャネルのパススルー機能

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

次の機能は、シングルホップまたはマルチホップで同じように動作します。

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

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

- 双方向オーディオ

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

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

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

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

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

以下の従来の仮想チャネルとその機能をサポートしています。

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

セキュリティとICA仮想チャネル

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

ベストプラクティス

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

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

仮想チャネルの命名:

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

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

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

ダブルホップサポート:

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

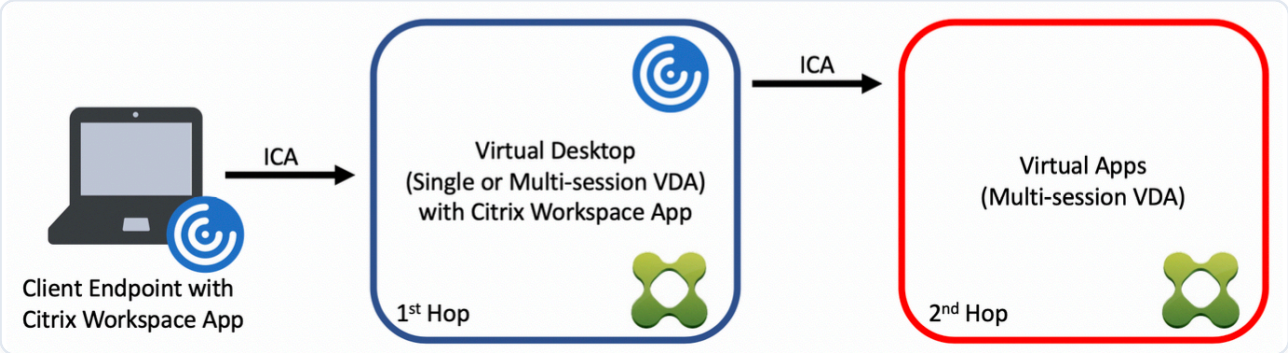
仮想チャネル	ダブルホップはサポートされていますか？
コンティニュアム (MRVC)	いいえ
コントロールVC	はい
HTML5 ビデオリダイレクト (v1)	はい
キーボード、マウス	はい
マルチタッチ	いいえ
NSAPVC	いいえ
印刷	はい
SensVC	いいえ
スマートカード	はい
ツイン	はい
USB VC	はい
WAYCOM デバイス - K2M (USB VC を使用)	はい
Webカメラビデオ圧縮	はい
Windows Mediaリダイレクト	はい

参照

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

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

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



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

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

システム要件

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

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

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

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

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

ダブルホップにおけるHDX™の展開に関する考慮事項

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

グラフィック

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

遅延

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

マルチメディア

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

USBデバイスリダイレクト

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

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

注：

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

サポートの例外

ダブルホップセッションは、以下のものを除き、ほとんどのHDX機能と機能をサポートしています。

- ブラウザコンテンツリダイレクト
- ローカルアプリアクセス
- Skype for Business向けリアルタイム最適化パック
- Microsoft Teams向け最適化

インストールと構成

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

Citrix Virtual Apps and Desktops を展開するには、次の順序を使用します。

準備

インストール準備 を確認し、必要なタスクをすべて完了します。

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

コアコンポーネントのインストール

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

サイトの作成

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

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

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

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

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

オプションコンポーネントのインストール

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

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

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

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

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

マシンカタログを作成する

Studioでサイトを作成した後、マシンカタログの作成に誘導されます。

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

デリバリーグループを作成する

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

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

アプリケーショングループの作成（オプション）

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

既知の制限事項

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

Web Studio のスマートカード認証を設定する

この記事では、Web Studio のスマートカード認証を設定および有効にするために必要な手順を概説します。

ステップ 1: スマートカードドライバーをインストールする

ステップ 2: スマートカードユーザーに証明書を発行する

ステップ 3: スマートカードユーザーの証明書を登録する

ステップ 4: Web Studio IIS サーバーを構成する

ステップ 5 (オプション): Web Studio の認証委任を構成する

ステップ 6: Web Studio のスマートカード認証を有効にする

> **注：**

> スマートカード認証は、Web Studio サーバーと同じ Active Directory ドメインのユーザーに対してのみサポートされます。

ステップ 1: スマートカードドライバーをインストールする

以下のマシンにスマートカードドライバーをインストールします。

- 証明書サービスがインストールされているドメインコントローラー。
- Web Studio サーバー
- エンドユーザーが Web Studio にアクセスするために使用するマシン
- スマートカードユーザーの証明書を登録するために使用するマシン

スマートカードドライバーはベンダーによって異なります。例えば、ITSが提供するスマートカードハードウェアを使用している場合、SaftNetドライバーは`<https://support.globalsign.com/ssl/ssl-certificates-installation/safenet-drivers>`からダウンロードしてください。

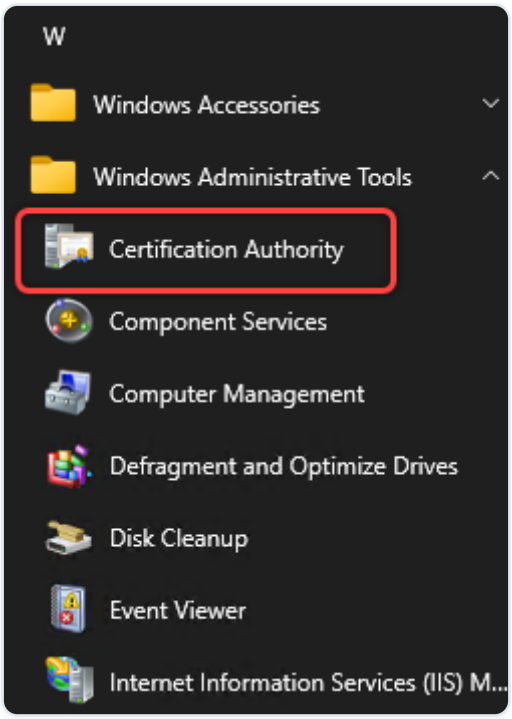
ステップ2：スマートカードユーザーの証明書を発行する

> **注:**

> 以下の手順は、プロセスを案内するための例として提供されています。

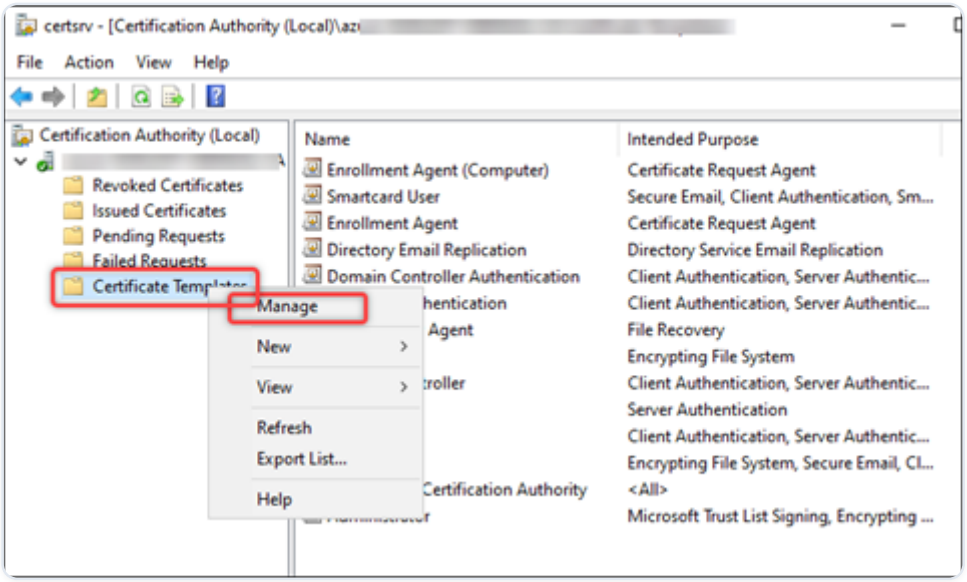
> ドメインコントローラーで、以下の手順に従ってタスクを完了します。

1. ドメインコントローラーにアクセスし、**証明機関**を開きます。



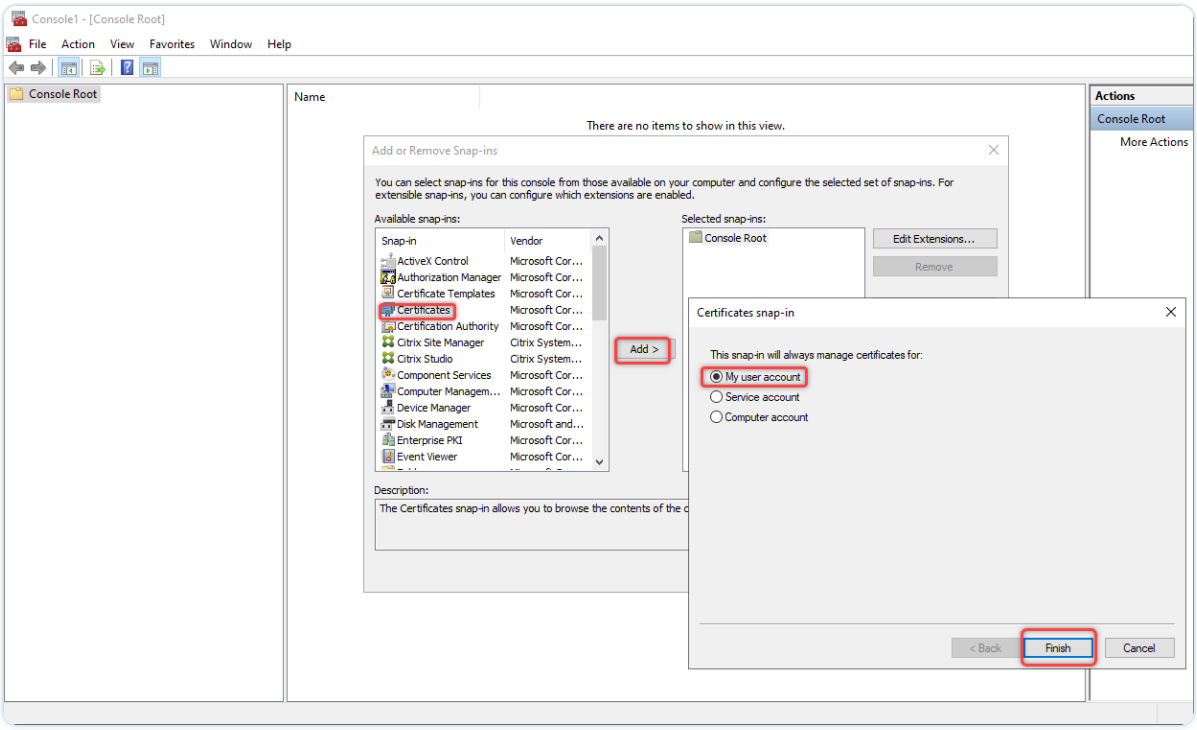
2. **登録エージェント**テンプレートを複製します。詳細な手順は次のとおりです。

   a. **証明書テンプレート**を右クリックし、**管理**を選択します。

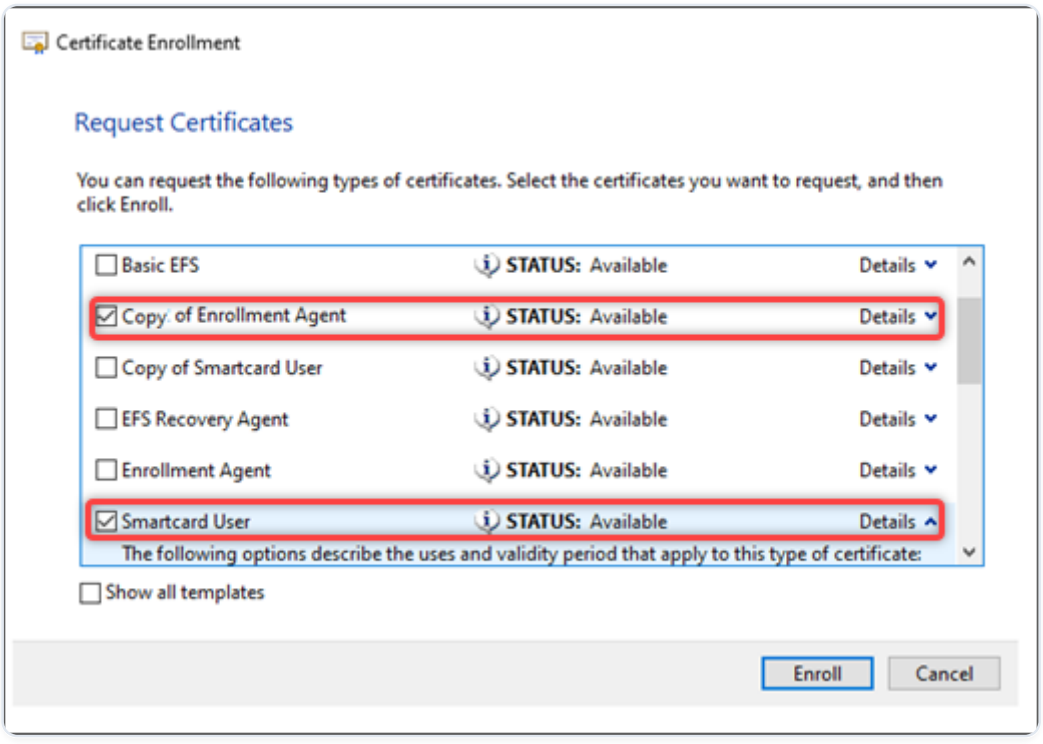


   b. **登録エージェント**を右クリックし、**テンプレートの複製**を選択します。

   c. **暗号化**タブで、**Microsoft Base Smart Card Crypto Provider**を選択し、**OK**をクリックします。**証明書テンプレート**リストに**登録エージェントのコピー**という名前のテンプレートが表示されます。



d. **サブジェクト名**タブで、**サブジェクト名に電子メールを含める**が選択されていないことを確認します。



3. スマートカードの証明書を発行します。詳細な手順は次のとおりです。

   a. 「**証明書テンプレート**」を右クリックし、「**新規 > 発行するテンプレート**」を選択します。

   b. 「**登録エージェントのコピー**」と「**スマートカードユーザー**」を選択します。

   c. **OK**をクリックします。

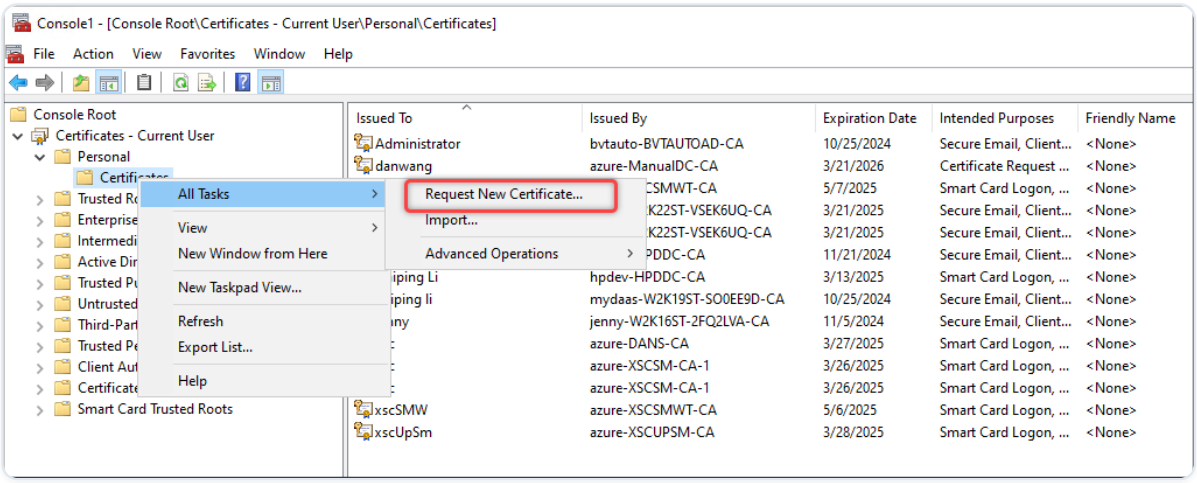
ステップ3：スマートカードユーザーの証明書を登録する

> **注:**
>
> 以下の手順は、プロセスをガイドするための例として提供されています。

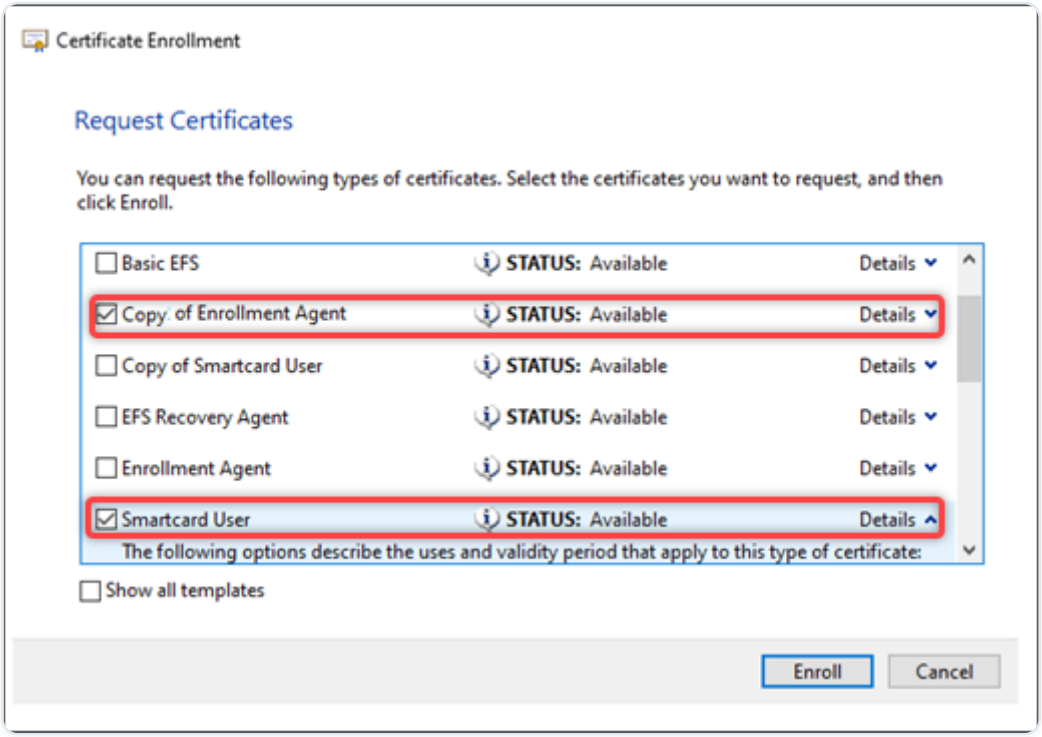
> ドメインに参加している物理Windowsマシンで、各スマートカードの証明書を登録するには、以下の手順に従います。

1. 登録用にドメインに参加している物理Windowsマシンを準備します。
    a. スマートカードドライバーがインストールされていることを確認します。
    b. スマートカードをマシンに挿入します。
    c. スマートカードに割り当てるユーザーアカウントを使用してマシンにログオンします。
2. ステップ1で準備したマシンに**証明書**スナップインを追加します。詳細な手順は次のとおりです。
    a. 「**mmc**」を開きます。
    b. 「**ファイル**」をクリックし、次に「**スナップインの追加と削除**」をクリックします。
    c. 表示される「**スナップインの追加と削除**」ウィンドウで、「**証明書**」を選択し、「**追加 >**」をクリックします。
    d. 表示されるダイアログボックスで、「**マイユーザーアカウント**」を選択し、「**完了**」をクリックします。
    e. **OK**をクリックします。

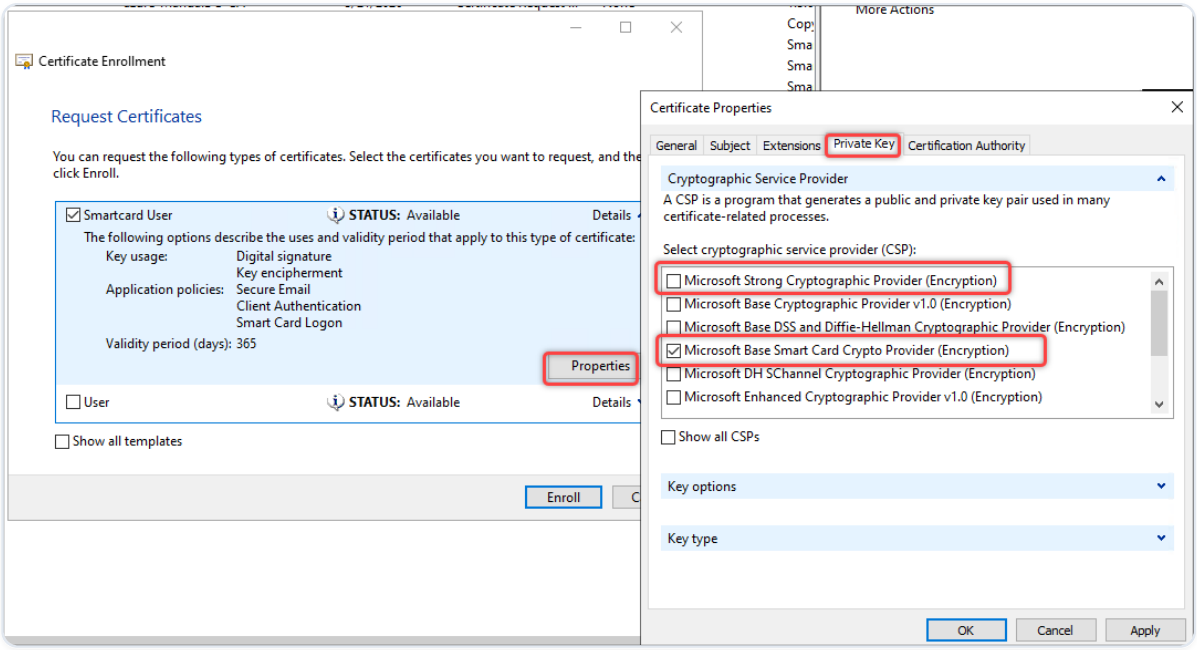
    証明書の追加(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/add-certificate-1.png)
3. 「**証明書**」スナップインの新しい証明書を要求します。詳細な手順は次のとおりです。
    a. **証明書 - 現在のユーザー > 個人**に移動し、**証明書**を右クリックして、**すべてのタスク > 新しい証明書の要求**を選択します。



b. 表示される**証明書の要求**ダイアログボックスで、**登録エージェントのコピー**と**スマートカードユーザー**を選択します。



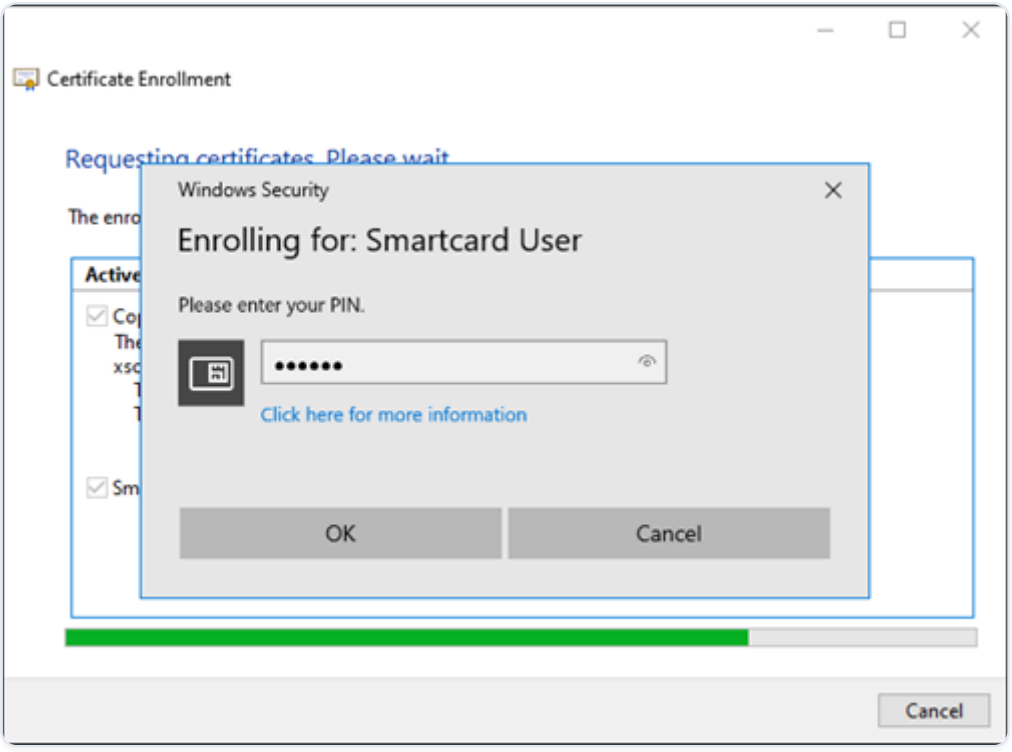
c. 上記のダイアログボックスで、**スマートカードユーザーの詳細**をクリックし、**プロパティ**をクリックします。**証明書のプロパティ**ダイアログボックスが表示されます。



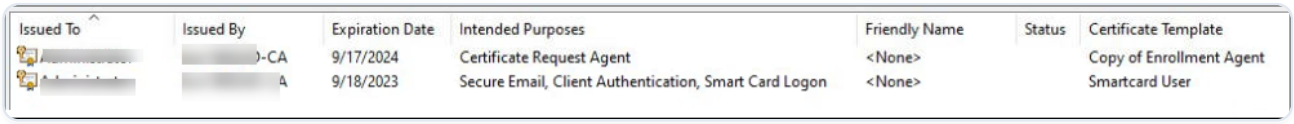
d. **秘密キー**タブで、**暗号化サービスプロバイダー**を展開し、**Microsoft Strong Cryptographic Provider (Encrption)** のチェックを外し、**Microsoft Base Smart Card Crypto Provider (Encryption)** のみを選択して、**OK**をクリックします。

e. **登録**をクリックします。

f. 表示される**Windows セキュリティ**ダイアログボックスで、スマートカードのPINコードを入力し、**OK**をクリックします。登録が完了したら、**完了**をクリックします。



登録が成功すると、次のスクリーンショットに示すように、**証明書 - 現在のユーザー -> 個人 -> 証明書**の下に2つの証明書が表示されます。



手順4：Web Studio IISサーバーを構成する

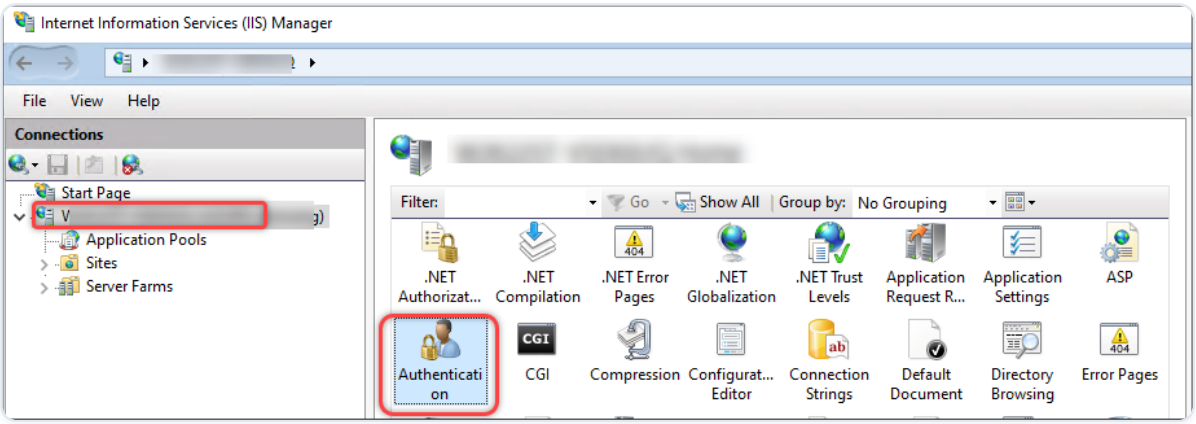
各Web Studioサーバーで、スマートカード認証用にIISを構成するには、次の手順に従います。

1. Web Studioマシンで**クライアント証明書マッピング認証**を有効にします**。

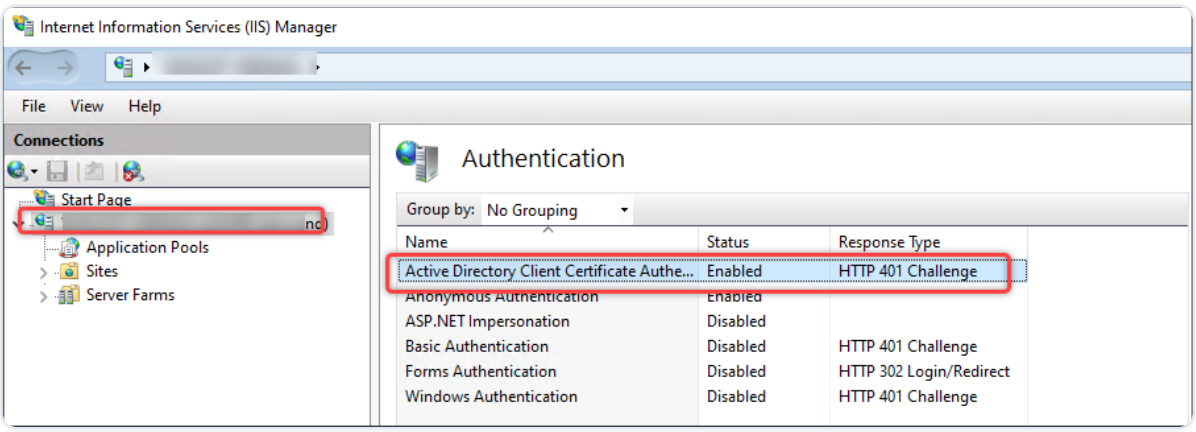
   `<clientCertificateMappingAuthentication>`要素は、IIS 7以降のデフォルトインストールでは利用できません。インストールと有効化の詳細については、このMicrosoftの記事を参照してください。

2. Web StudioマシンでIIS マネージャーを起動します。
3. 「**Active Directory クライアント証明書認証**」をマシンで有効にします。詳細な手順は次のとおりです。

   a. 左ペインでマシンを選択し、「**認証**」をダブルクリックします。

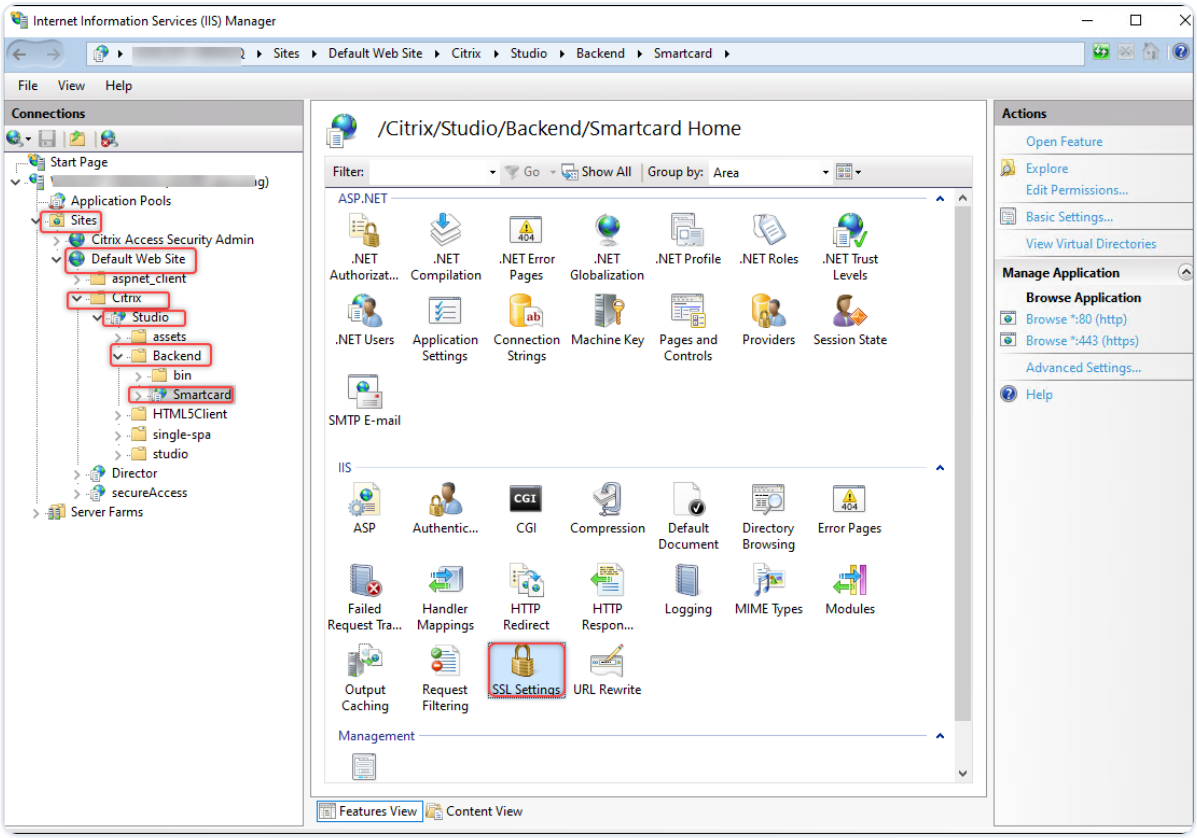


   b. 「**Active Directory クライアント証明書認証**」を有効にします。

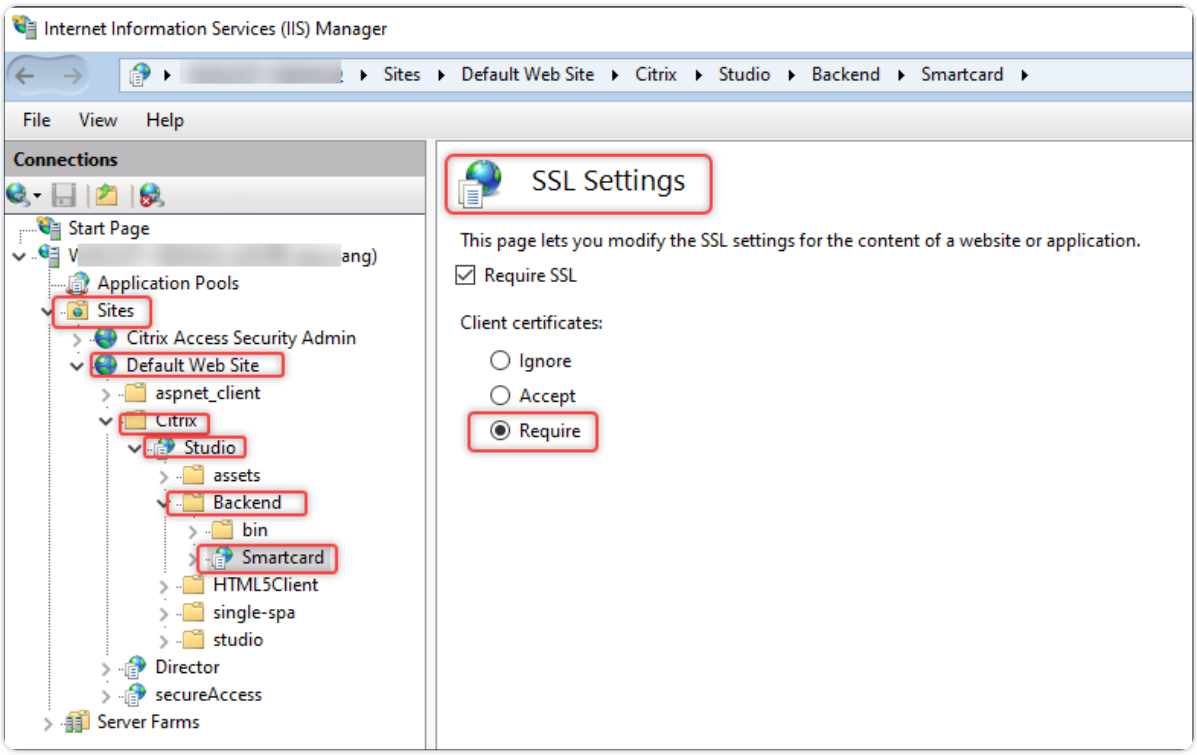


4. クライアント証明書認証を使用して、より安全なHTTPSプロトコルのWeb Studioバックエンドモジュールを構成します。

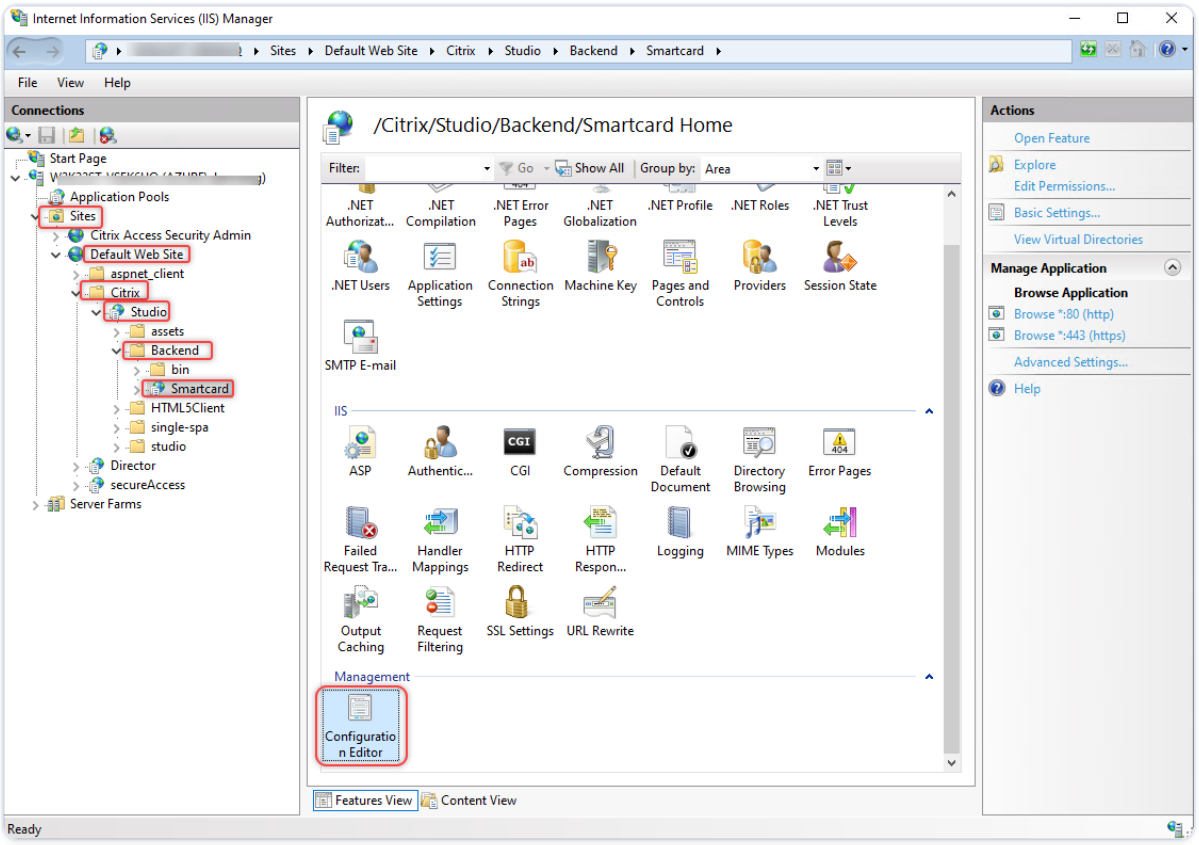
   a. **サイト > 既定のWebサイト > Studio > バックエンド > スマートカード**に移動し、**IIS**セクションで「**SSL設定**」をダブルクリックします。



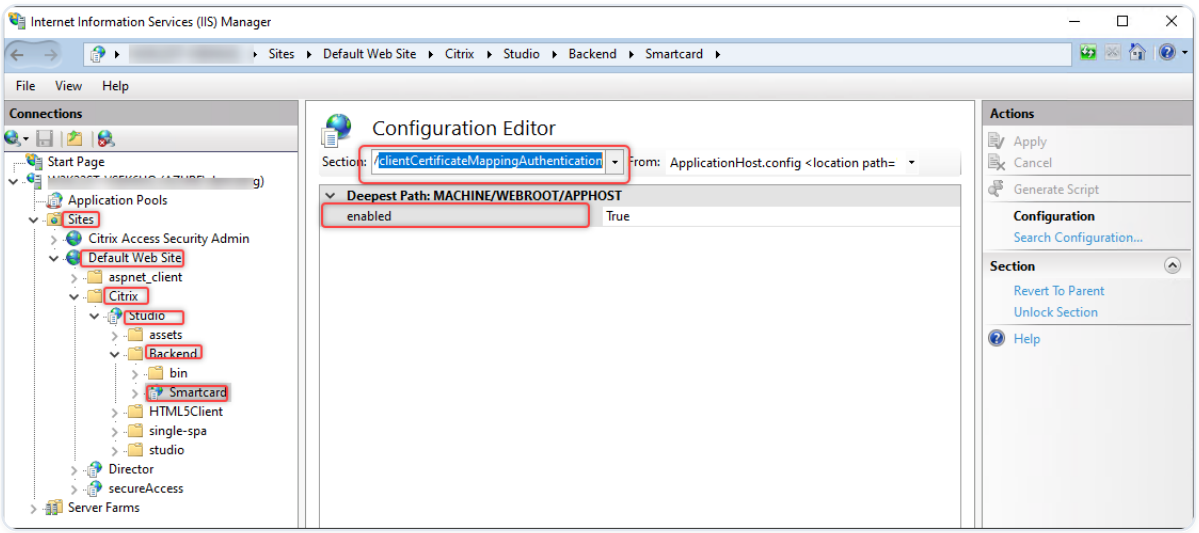
   b. 「**クライアント証明書**」で「**要求**」を選択します。



c. **サイト > 既定のWebサイト > Studio > バックエンド > スマートカード**に戻り、**IIS**セクションで「**構成エディター**」をダブルクリックします。



d. **/clientCertificateMappingAuthentication**が**有効**になっていることを確認します。



5. (Windows 2022のみ) TCP経由のTLS 1.3を無効にします。詳細な手順は次のとおりです。

a. 「**サイト > 既定の Web サイト**」に移動します。

b. 「**サイトの編集 > バインド**」をクリックします。

c. 表示される「**サイトバインド**」ダイアログボックスで、「**https**」レコードを選択し、「**編集**」をクリックします。

Windows 2022 のみ https 編集(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/iis-server-default-site-https-edit.png)

d. 表示される「**サイトバインドの編集**」ダイアログボックスで、「**TCP 経由の TLS 1.3 を無効にする**」を選択し、「**OK**」をクリックします。

Windows 2022 のみ https 編集無効(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/iis-server-default-site-https-edit-disable.png)

知っておくと良いこと:

Web Studio バックエンドは、Web Studio のモジュールであり、次の機能を提供します。

- スマートカード認証。
- 統合 Windows 認証を使用したオーケストレーションサービスからの FMA ベアラートークンの取得。

手順 5 (オプション) Web Studio の認証委任を構成する

Web Studio と Delivery Controller が異なるサーバーにインストールされている場合、各 Web Studio サーバーから Delivery Controller への HOST および HTTPS サービスに対する委任を構成する必要があります。

各 Web Studio サーバーでタスクを完了するには、次の手順に従います。

1. Delivery Controller™ オーケストレーション HTTPS 証明書をインポートする
2. Web Studio サーバーの委任を構成する
3. Web Studio IISサーバーのサービスアカウントの委任を構成する(#configure-delegation-for-the-web-studio-iis-servers-service-account)

Delivery Controller Orchestration HTTPS証明書のインポート

Web Studioサーバーで、**Delivery Controller Orchestration HTTPS**証明書を**信頼されたルート証明機関**にインポートします。詳細な手順は次のとおりです。

1. **設定 > コンピューター証明書の管理**を開始します。
2. **信頼されたルート証明機関 > 証明書**を右クリックし、**すべてのタスク > インポート**を選択します。

DDC証明書のインポート(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/web-server-ddc-cert-import.png)

3. 画面の指示に従って、**Delivery Controller Orchestration HTTPS**証明書をインポートします。

Web Studioサーバーの委任を構成する

ドメインコントローラーで、Web StudioサーバーからDelivery ControllerへのHOSTおよびHTTPサービスの委任を構成します。タスクを完了するには、次の手順に従います。

1. ドメインコントローラーで、**Active Directory管理センター**を開始します。
2. 委任用に構成するWeb Studioサーバーの**コンピューター**アカウントを見つけます（*例: Dan002*）。
3. アカウントを右クリックし、**プロパティ**を選択します。

   Studioサーバーの委任を構成する(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/kerbero-delegation-1.png)

   a. **委任**タブに移動します。

      委任設定を入力する(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/kerbero-delegation-2.png)

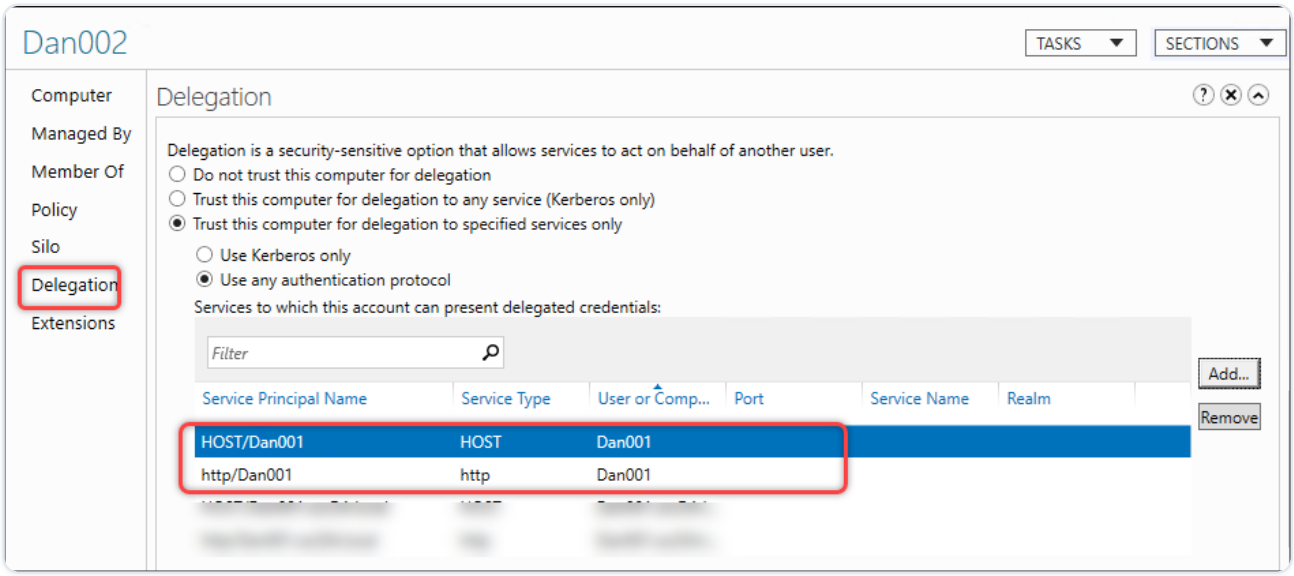
   b. **>** を選択します。

   c. このコンピューターアカウントを委任できるサービスを指定するには、 をクリックします。

   d. 表示される ダイアログボックスで、 をクリックして、Delivery Controller のコンピューター名（*例: Dan001*）を見つけます。

   e. **HOST** サービスと **HTTP** サービスを選択し、 をクリックします。

構成結果を次のスクリーンショットに示します。

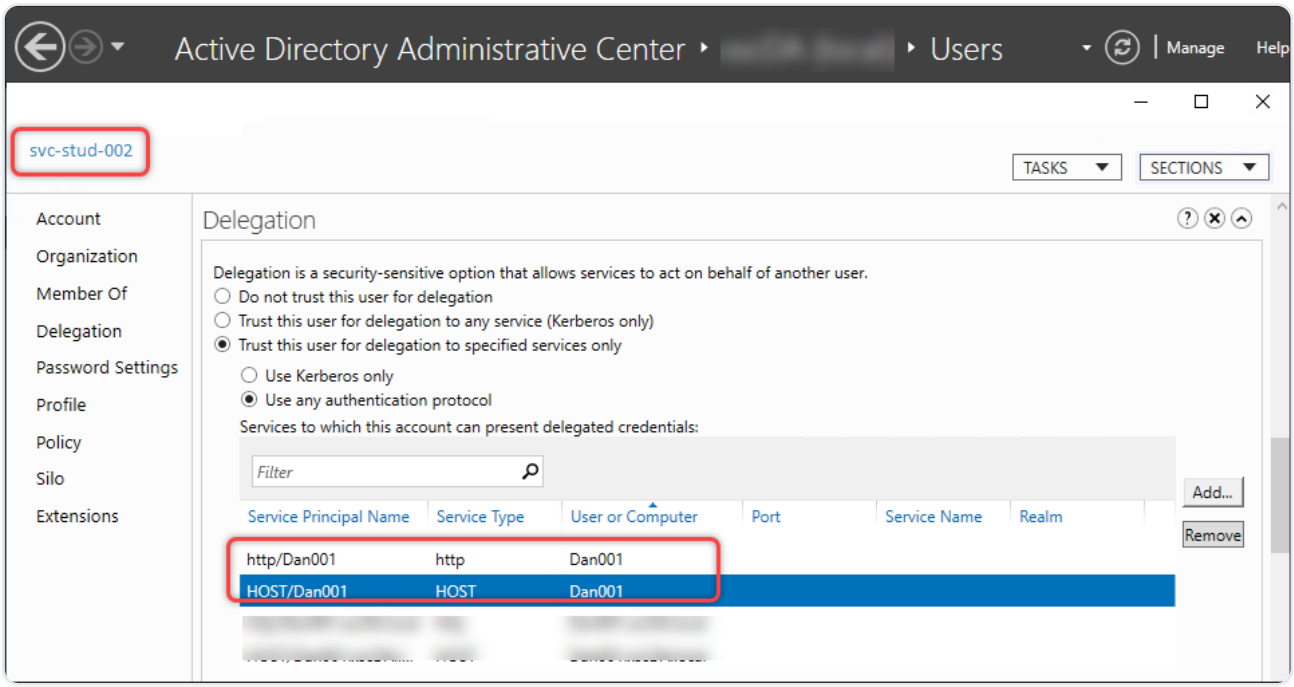


Web Studio IIS サーバーのサービスアカウントの委任を構成する

Web Studio IIS サーバーのサービスアカウントを構成している場合は、このサービスアカウントから Delivery Controller の HOST および HTTP サービスへの委任も構成する必要があります。この委任が確立されると、Web Studio サーバーはサービスアカウントを使用して、現在のスマートカードユーザーになりすまし、Delivery Group の HOST および HTTP サービスにアクセスできます。構成を完了するには、次の手順に従います。

1. ドメインコントローラーで、**Active Directory 管理センター**を起動します。
2. 委任用に構成する **ユーザー** アカウント（*例: svr-stud-002*）を見つけます。
3. アカウントを右クリックし、 を選択します。
4. 手順 2 で説明されている手順に従って、Web Studio IIS サービスアカウントを Delivery Controller の HOST および HTTP サービスに委任します。

構成結果を次のスクリーンショットに示します。



手順 6：Web Studio のスマートカード認証を有効にする

Web Studio のスマートカード認証を有効にするには、次の手順に従います。

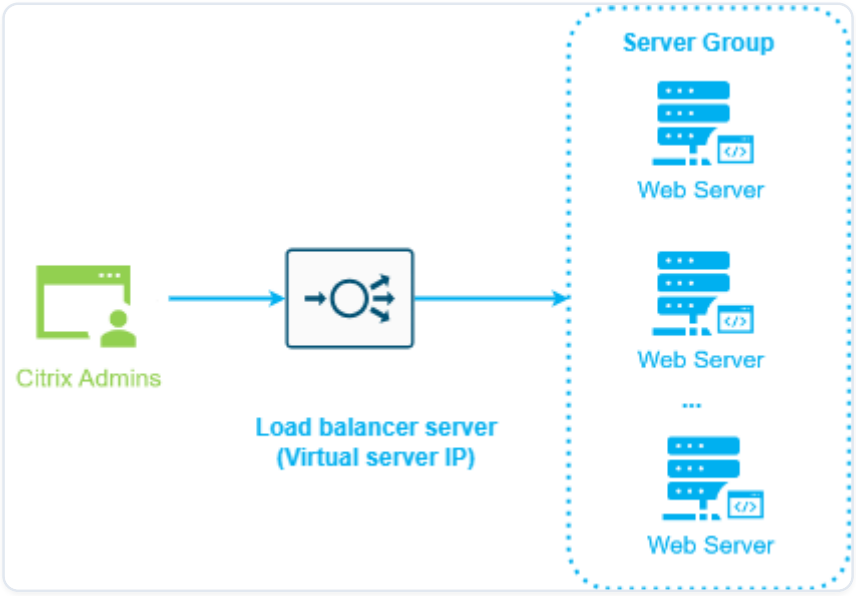
1. **Web Studio**にサインインし、左側のペインで**設定**を選択します。
2. 必要に応じて、**スマートカード認証**または**ドメイン資格情報 + スマートカード認証**を選択します。
3. 必要に応じて、**スマートカード認証**または**ドメイン資格情報またはスマートカード認証**を選択します。

4. **適用**をクリックします。

   証明書テンプレートの管理(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/enable-stud-settings.png)

負荷分散されたWeb Studio展開をセットアップする

高可用性Web Studio展開をセットアップするには、NetScaler® ADC や Windows ネットワーク負荷分散などのツールを選択できます。この記事では、NetScaler ADCアプライアンスを使用して負荷分散されたWeb Studio展開をセットアップする方法について、ステップバイステップのガイドを提供します。



証明書の要件

商用証明機関から証明書を購入する前、またはエンタープライズ証明機関から証明書を発行する前に、ニーズに基づいて以下のオプションを検討してください。

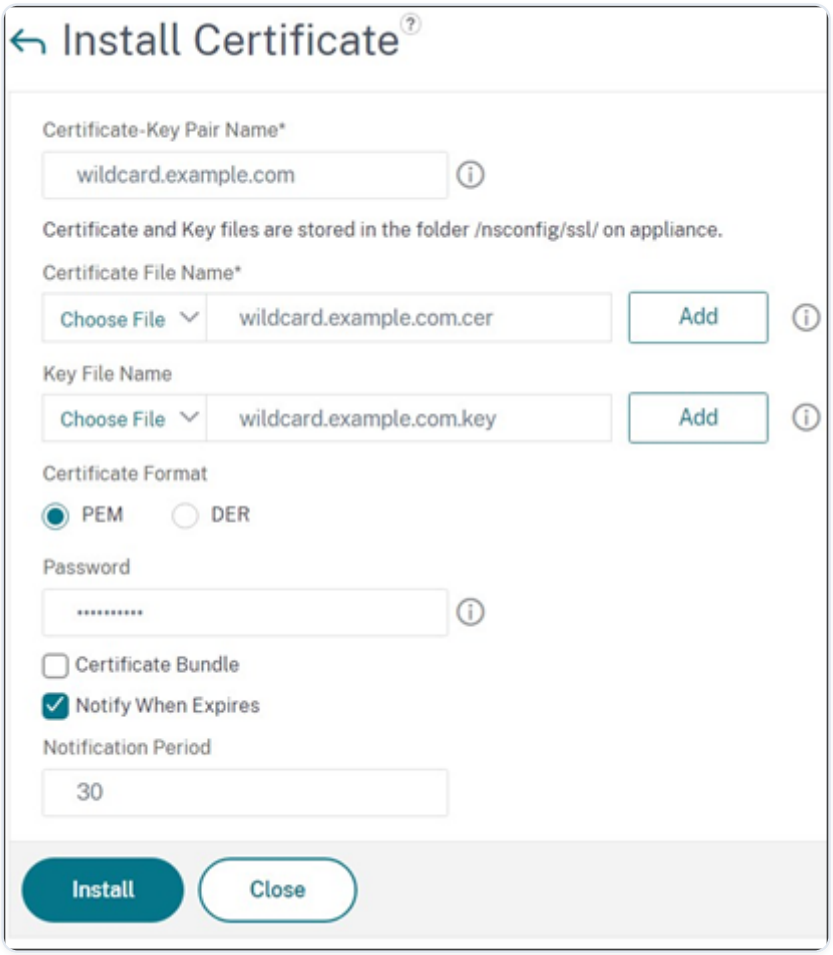
オプション	長所	短所
オプション1：NetScaler ADCアプライアンスのロードバランサーサーバーとWeb Studioサーバーの両方で、*.example.com ワイルドカード証明書を使用する。	• 構成を簡素化する • 管理が容易（単一の証明書） • 証明書を更新せずに新しいサブ	• ワイルドカード証明書が侵害された場合、すべてのサブドメインが危険にさらされる

オプション	長所	短所	
	ドメインを追加できる	• すべてのアプリケーションがワイルドカード証明書をサポートしているわけではない • 個別の証明書よりも高価になる可能性がある	
オプション2：NetScaler ADCアプライアンスのロードバランサーサーバーとWeb Studioサーバーの両方で、サブジェクト代替名 (SAN) を持つ証明書を使用する。	• 柔軟性があり、複数の特定のドメインとサブドメインを含めることができる • 複数のドメインの管理を一元化します • 複数の異なる名前をサポートし、ワイルドカードよりも柔軟性を提供します	• SANエントリの管理は、ドメイン数が増えるにつれて複雑になる可能性があります • 新しいドメインを追加するには、証明書の再発行が必要です • CAがサポートするSANエントリの数によって制限されます	
オプション3：各Web StudioサーバーとNetScaler ADCアプライアンスロードバランサーサーバーに証明書を使用する	• 各サーバーは個別に保護されます • 1つの証明書が侵害されても、他の証明書には影響しません	• 各証明書を個別に管理する必要があるため、管理オーバーヘッドが高くなります	

オプション	長所	短所	
	• 各サーバーのニーズに合わせて調整された特定の証明書を使用できます	• 更新する証明書が増え、コストが高くなる可能性があります • すべての証明書が一貫して構成されていることを確認する必要があります	

ロードバランサーでサーバー証明書を構成する

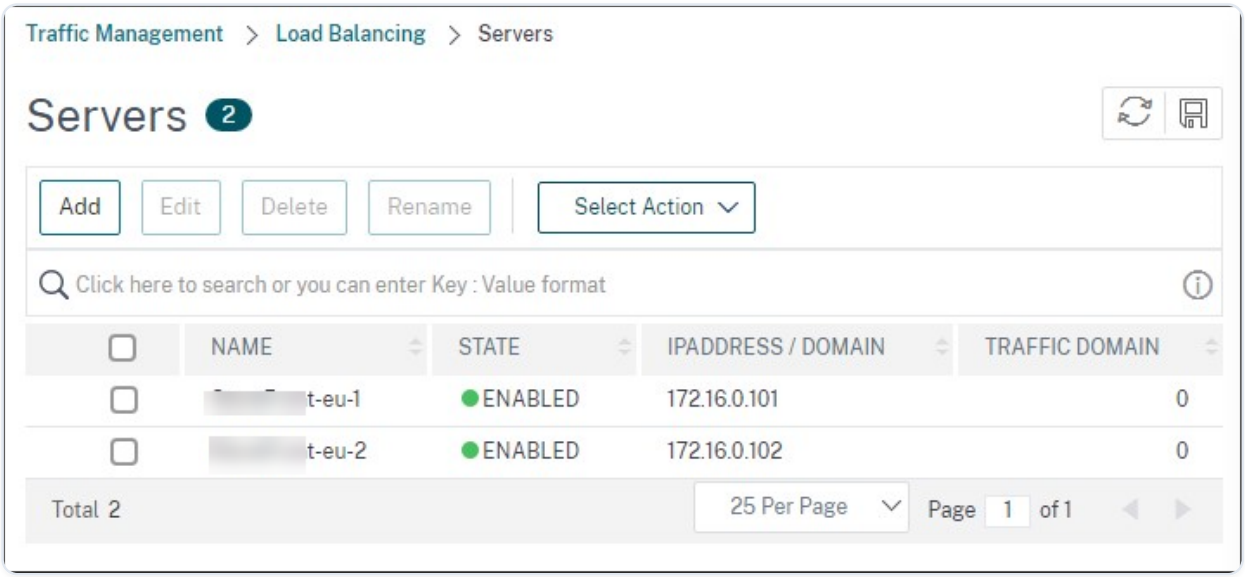
1. NetScaler ADCアプライアンス管理GUIにログオンします。
2. **トラフィック管理 > SSL > 証明書 > サーバー証明書** を選択します
3. 「**インストール**」をクリックします。
4. 「**Install Server Certificate**」ページで、証明書とキーペアの名前を入力し、「**Choose File**」をクリックして、証明書ファイルを参照します。証明書ファイルに秘密キーが含まれていない場合は、「**Key File**」を選択します。



ステップ1: Web Studioサーバーノードを追加する

すべてのWeb Studioサーバーノード (例: `Studio-eu-1` および `Studio-eu-2`) をロードバランサーに追加します。

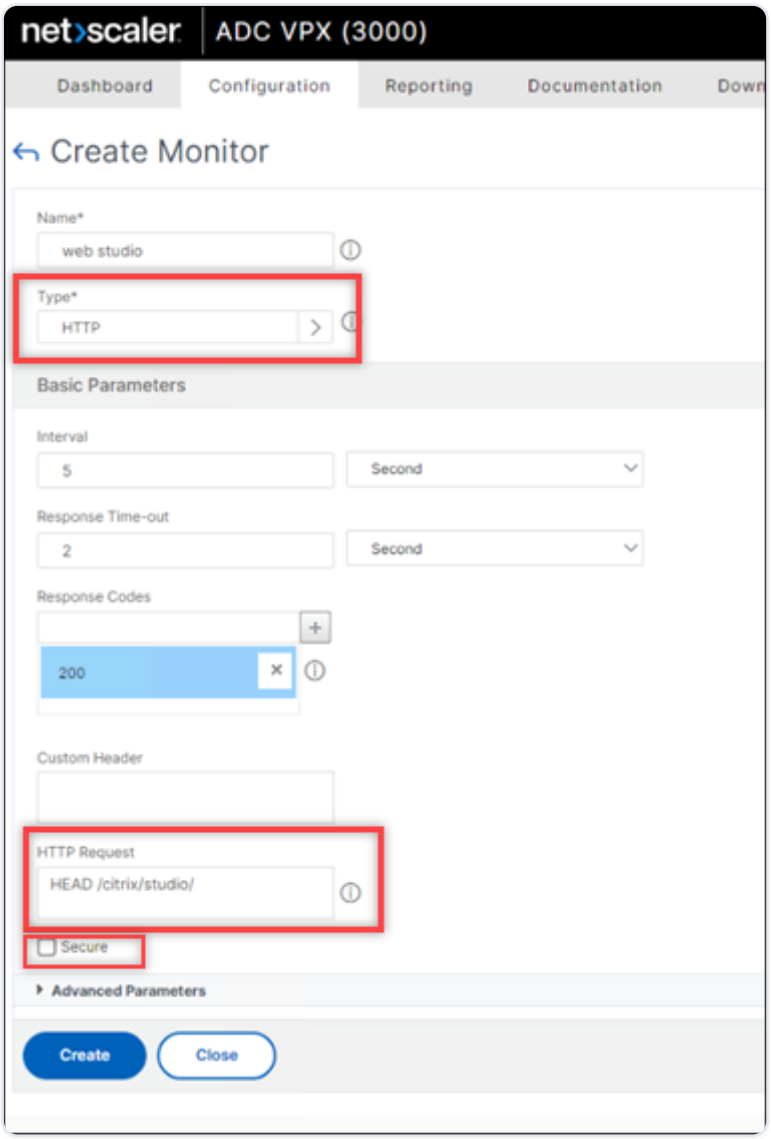
1. NetScaler ADC管理GUIにログオンします。
2. **Traffic Management > Load Balancing > Servers**に移動します。**追加**をクリックします。
3. Web Studioサーバーノードのサーバー**IP**アドレスを入力します。
4. 他のWeb Studioサーバーを追加するには、ステップ2〜3を繰り返します。



ステップ2: Web Studioサーバーノード用のモニターを追加する

すべてのWeb Studioサーバーノードのステータスを確認するために、ロードバランサーでモニターを設定します。

1. **トラフィック管理 > 負荷分散 > モニター > 追加** を選択します。
2. **構成**タブで、次の設定を完了し、その他のデフォルトはそのままにします。
   - **名前**に**Web Studio**と入力します。
   - **タイプ**に**HTTP**または**SSL**を選択します。
   - **Secure**オプションを選択します。
   - **HTTP要求**に**HEAD/citrix/studio/**と入力します。



ステップ3: Web Studioサーバーノード用のサービスグループを作成する

1. **Traffic Management > Load Balancing > Service Groups > Add**を選択します。HTTPS経由でWeb Studioサーバーに接続するには、プロトコルとしてSSLを選択し、その他の設定はデフォルトのままにして、**OK**をクリックします。
2. サービスグループ内で、**Service Group Members**の下にある**No Service Group Member**をクリックし、次の手順に従ってメンバーを追加します。

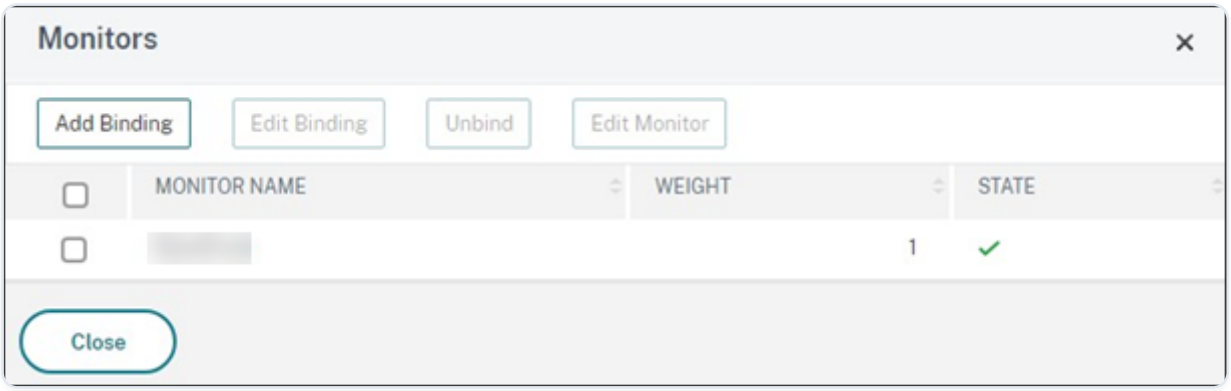
   a. **サービスベース**をクリックします。

   b. 以前に追加したすべてのサーバーを選択します。

   c. ポートに**443**を入力します。

   「サービスグループメンバーの作成」ページのスクリーンショット(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/netscaler-create-service-group-member.png)

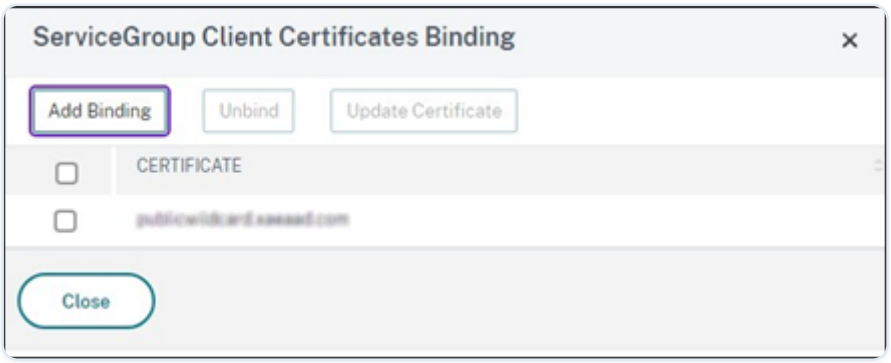
3. **Monitors**セクションを追加し、以前に作成したWeb Studioモニターを選択します。



4. **Certificates**セクションを追加し、次の設定を完了します。

   a. クライアント証明書をバインドします。

   b. 以前にインポートしたサーバー証明書の署名に使用したCA証明書、およびPKI信頼チェーンの一部である可能性のあるその他のCAをバインドします。



5. **Settings**セクションを追加し、**Insert Client IP Header**を選択して、ヘッダー名に**X-Forwarded-For**を入力します。この設定により、クライアントIPアドレスをPoliciesで使用できるようになります。

ステップ4：仮想サーバーを作成する

ユーザーがWeb Studioサーバーグループにアクセスするためのロードバランサー仮想サーバーを作成します。

1. **Traffic Management > Load Balancing > Virtual Servers**に移動し、**Add**をクリックします。
2. 名前を入力し、**Protocol**に**SSL**を選択し、**Port**に**443**を入力して、**OK**をクリックします。

   NetScaler負荷分散仮想サーバー画面のスクリーンショット(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/netscaler-lb-virtual-server.png)

3. 以前に作成した**Service Group**をロードバランシング仮想サーバーにバインドします。
4. ステップ3：Web Studioサーバーノードのサービスグループを作成するでサービスグループにバインドしたCA証明書をバインドします。

5. **Method**セクションを追加し、ロードバランシング方法を選択します。Web Studioのロードバランシングで一般的な選択肢は、**ROUNDROBIN**または**LEASTCONNECTION**です。

   負荷分散メソッドセクションのスクリーンショット(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/leastconnection.png)

6. 「**Persistence**」セクションを追加し、以下の設定を完了します。

   a. 永続化メソッドを「**COOKIEINSERT**」に設定します。

   b. タイムアウトをWeb Studio内のセッションタイムアウトと同じに設定します (デフォルトでは20分)。

   c. 今後のデバッグを容易にするために、Cookieに名前を付けます。例: **NSC_SFPersistence**。

   d. バックアップ永続性を **NONE** に設定します。

      永続性セクションのスクリーンショット(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/persistence.png)

> **注：**
>
> クライアントがHTTP Cookieの保存を許可されていない場合、後続のリクエストにはHTTP Cookieが含まれず、永続化は使用されません。

ステップ5: 仮想サーバーのDNSレコードを作成する

ドメインコントローラーで、仮想サーバーのIPアドレスをFQDNにマッピングするDNSおよびPTRレコードを作成します。ネットワーク内のWeb Studioユーザーは、このFQDNを使用してWeb Studioサーバーグループにアクセスします。たとえば、webstudio.example.comはロードバランサー仮想サーバーのIPアドレス (VIP) に解決されます。

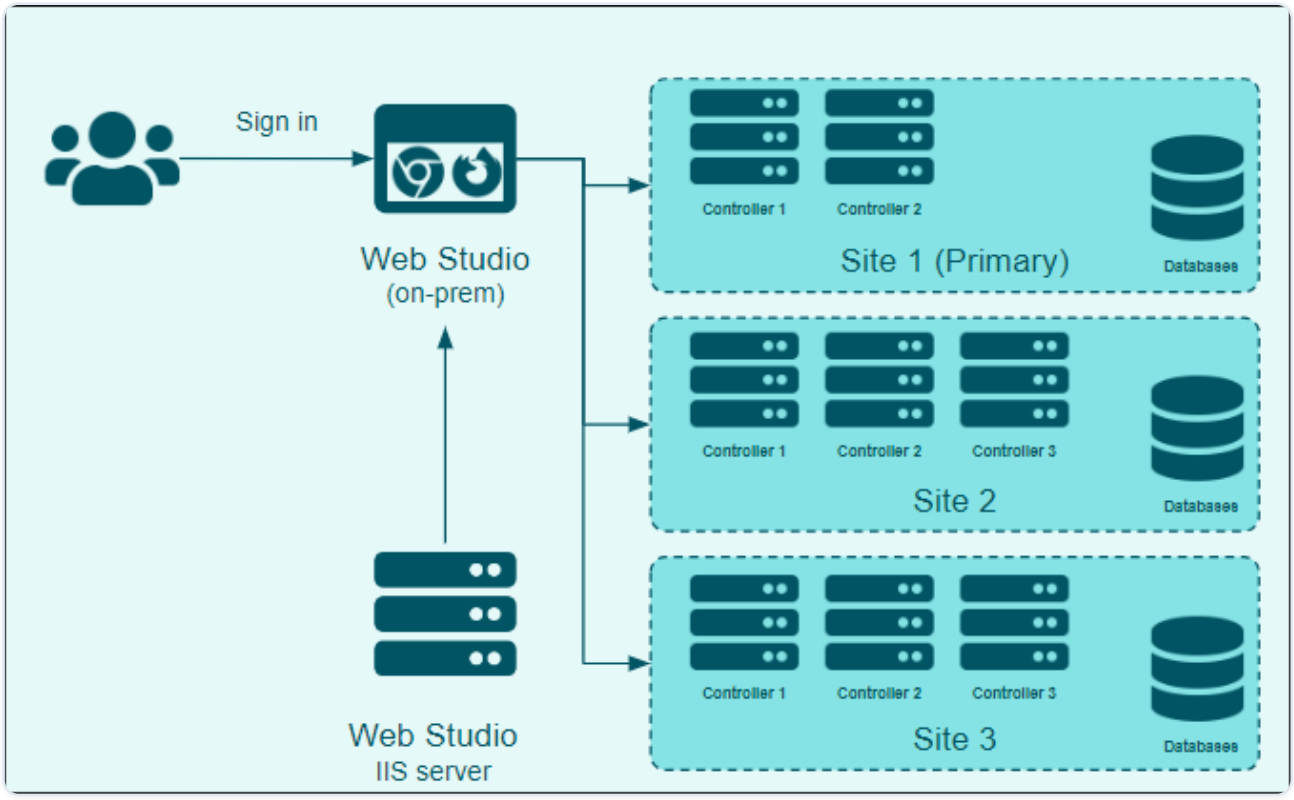
永続性セクションのスクリーンショット(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/new-dns.png)

ユーザーがWeb Studioサーバーにアクセスするためのurlを提供します: `https://<FQDN of the virtual server>/<text you entered in the HTTP Request field when creating a monitor>`。例: `https://webstudio.example.com/citrix/studio`

複数サイト管理を有効にする

デフォルトでは、1つのWeb Studioコンソールは単一のCitrix Virtual Apps and Desktops™サイトにマッピングされますが、必要に応じて、Web Studioコンソールを複数のサイトを管理するように構成できます。これにより、1つのWeb Studioをインストールするだけで、すべてのサイトを構成および管理できます。

次の図は、単一のWeb Studio展開が複数の独立したCitrix Virtual Apps and Desktopsサイトを管理する、複数サイトアーキテクチャを示しています。



利点

- 統合されたシングルサインオンエクスペリエンスで複数のサイトを管理する際の効率が向上します。
- すべての構成が1つのコンソールからアクセスできるため、トラブルシューティングが容易になります。

考慮事項

サイトを構成および展開する際は、次の点に留意してください。

- 必須バージョン:
  - Citrix Virtual Apps and Desktops 2311 およびそれ以降のバージョン。

  - Delivery Controller™のバージョンは、Web Studioのバージョンと一致するか、それ以前のバージョンである必要があります。最小要件は2311以降です。
  - この機能はWeb Studio（Webベース）専用であり、Citrix Studio（Windowsベース）では利用できません。

- シングルサインオンをサポートするには、すべてのサイトを信頼されたドメインに展開します。
- 統合されたWeb Studioコンソールを使用して、最大10個のCitrix Virtual Apps and Desktopsサイトを管理できます。

ワークフロー

始める前に

- プライマリサイトを決定し、Web Studioコンソールがプライマリサイト管理にアクセス可能であることを確認します。

> **注:**
>
> - プライマリサイトを設計する際は、追加されたサイトのアクセシビリティがプライマリサイトの可用性に依存することに注意してください。プライマリサイトのパフォーマンスの問題は、追加されたサイトへのアクセスに影響を与える可能性があります。
> - Web Studioがインストールされていない場合は、「Web Studioのインストール」を参照してください。

- Web Studioで管理する予定のサイトがすでに設定されていることを確認してください。
  - 新しいサイトを作成するには、「サイトの作成」を参照してください。
- (推奨) コンソールでサイトを切り替える際にシングルサインオンを有効にするには、すべてのサイトで統合Windows認証 (IWA) を有効にします。IWAが有効になっていないサイトでは、ログイン資格情報を使用してサインインすることもできます。

ステップ1：Web Studioコンソールにサインインする

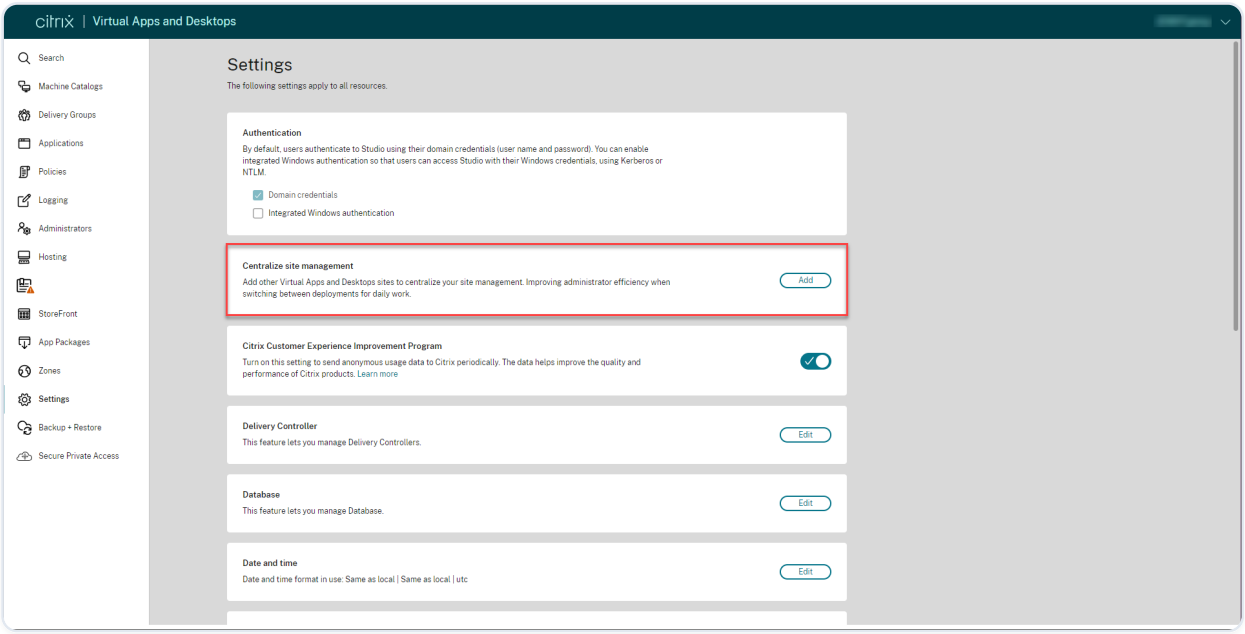
1. Webブラウザを開きます。`https://<address of the server hosting Web Studio>/Citrix/Studio`を入力します。
2. Web Studioにサインインして、プライマリサイトを管理します。

注:

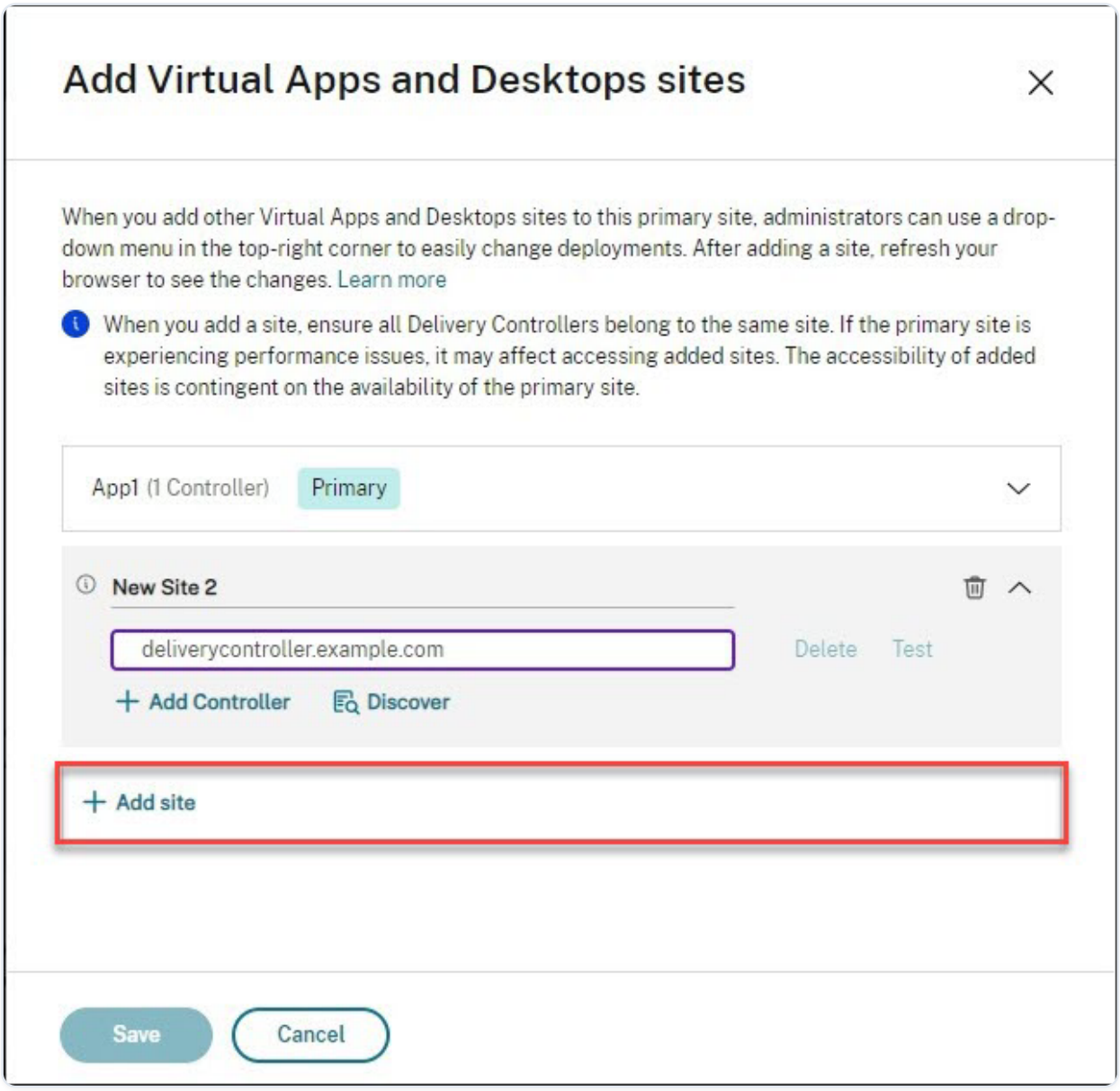
インストール時に使用するDelivery Controllerのアドレスによってサイトが識別されます。Delivery Controllerがプライマリサイトのものである場合、そのサイトにサインインします。

ステップ2：Web Studioを使用してサイトを追加する

1. **設定** > **サイト管理の集中化**に移動し、**追加**をクリックします。



2. **Virtual Apps and Desktopsサイトの追加**ページで、**サイトの追加**をクリックします。



3. Delivery Controllerを追加するには、次のいずれかの操作を実行します。

   - 「**コントローラーの追加**」をクリックし、FQDNを入力します。「**テスト**」をクリックして接続をテストします。
   - 「**検出**」をクリックします。

     a. 「**サイト検出**」ページで、サイト内にあるコントローラーのアドレスを選択または入力します。

     b. コントローラーへの完全なアクセス許可を持つ管理者の資格情報を、「**ユーザー名**」と「**パスワード**」フィールドに入力します。

     c. 「**完了**」をクリックします。

   サイト検出(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/site-discovery.png)

> **注:**
>
> 検出機能は、入力したデリバリーコントローラーのアドレスに基づいて、サイト内で到達可能なデリバリーコントローラーを自動的に追加します。

4. 「**Save**」をクリックします。

   サイト構成を管理または編集するには、「**設定**」>「**サイト管理の集中化**」に移動し、「**管理**」をクリックします。 「**管理**」オプションはプライマリサイトでのみ有効です。

   集中サイトの管理(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/centralize-site-mgmt-manage.png)

ステップ3：サイト設定の管理

サイト構成の変更を反映させるには、ブラウザーを更新してください。サイト選択ボックスは、コンソールの右上隅に表示されます。

「**設定**」ページで、「**更新**」アイコンの横にある右隅のドロップダウンメニューからサイトを選択します。 コンソールには、選択したサイトの構成が表示されます。

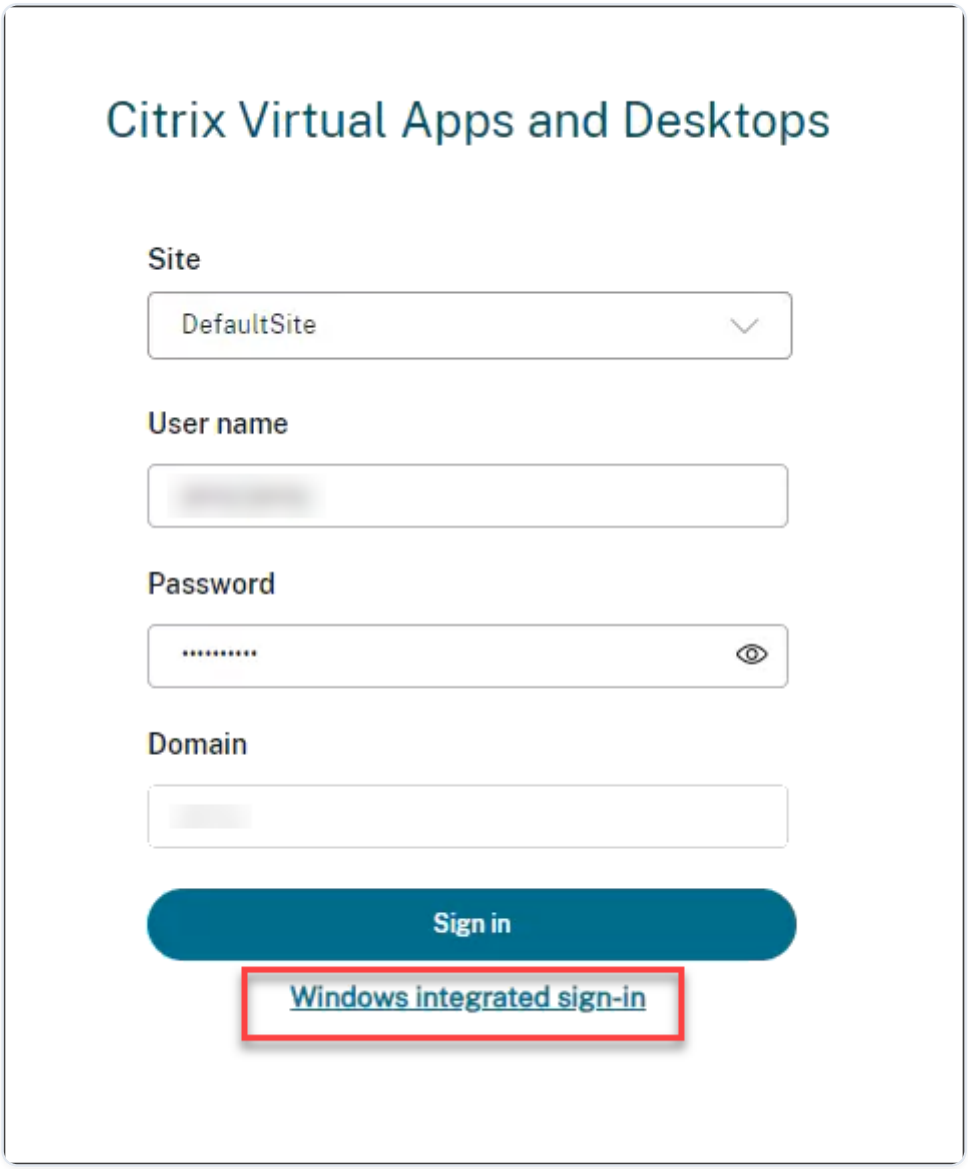
> **注:**
>
> - プライマリサイトに到達できない場合、それに関連付けられている他のサイトにアクセスすることはできません。
> - 別のサイトに切り替える際は、サインインに必要なアクセス許可またはアクセス資格情報があることを確認してください。

サイト構成後のサインインエクスペリエンス

1. Webブラウザーを開きます。`https://<address of the server hosting Web Studio>/Citrix/Studio`を入力します。
2. **サイト**フィールドからサイトを選択します。
3. **Windows統合サインイン**を選択するか、**ユーザー名**と**パスワード**を入力してサインインします。

   > **注:**

> Windows統合サインインは、選択したサイトで有効になっている場合にのみ利用できます。統合Windows認証の詳細については、「認証の管理」を参照してください。



REST API を使用して管理を自動化する

Citrix Virtual Apps and Desktops™ REST API を使用すると、Citrix Virtual Apps and Desktops 展開内のリソースの管理を自動化できます。

Citrix Virtual Apps and Desktops REST API は `<https://developer.cloud.com/citrixworkspace/citrix-daas/citrix-daas-rest-apis/docs/overview>` で利用できます。Citrix Virtual Apps and Desktops に適用されない API は、そのようにマークされています。そこにあるガイダンスに従って、API サービスへのアクセスを設定し、API を使用してリソースを管理および最適化してください。

マシンID

各マシンには、コンピューターアカウントとも呼ばれる一意のマシンIDが必要です。マシンIDは、マシン内でローカルに作成および管理することも、オンプレミスのActive Directory (AD) やAzure ADなどのディレクトリで作成および管理することもできます。Citrix®は、Active Directory参加済み、Azure Active Directory参加済み、ハイブリッドAzure Active Directory参加済み、またはドメイン非参加のマシンでの仮想アプリケーションおよびデスクトップのホストをサポートしています。

マシンIDの種類

以下のマシンIDの種類がサポートされています。

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

サポートされる構成

以下は、各シナリオでサポートされる構成の詳細です。

サポートされるインフラストラクチャ

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

サポートされているワークスペース認証IDプロバイダー

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

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

Active Directory 参加済み

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

フォレストとドメインでサポートされている機能レベルについては、「システム要件」(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/system-requirements.html)の記事に記載されています。ポリシーモデリングを使用するには、ドメインコントローラーがWindows Server 2003からWindows Server 2012 R2で実行されている必要があります。これはドメインの機能レベルには影響しません。

この製品は以下をサポートします。

- **ユーザーアカウントとコンピューターアカウントが単一のActive Directoryフォレスト内のドメインに存在する展開。** ユーザーアカウントとコンピューターアカウントは、単一フォレスト内の任意のドメインに存在できます。この種類の展開では、すべてのドメイン機能レベルとフォレスト機能レベルがサポートされます。
- **ユーザーアカウントが、Controllerおよび仮想デスクトップのコンピューターアカウントを含むActive Directoryフォレストとは異なるActive Directoryフォレストに存在する展開。** この種類の展開では、Controllerおよび仮想デスクトップのコンピューターアカウントを含むドメインは、ユーザーアカウントを含むドメインを信頼する必要があります。フォレストの信頼または外部の信頼を使用できます。この種類の展開では、すべてのドメイン機能レベルとフォレスト機能レベルがサポートされます。
- **Controllerのコンピューターアカウントが、仮想デスクトップのコンピューターアカウントを含む1つ以上の追加のActive Directoryフォレストとは異なるActive Directoryフォレストに存在する展開。** この種類の展開では、Controllerのコンピューターアカウントを含むドメインと、仮想デスクトップのコンピューターアカウントを含むすべてのドメインとの間に双方向の信頼が存在する必要があります。この種類の展開では、Controllerまたは仮想デスクトップの

コンピューターアカウントを含むすべてのドメインが「Windows 2000ネイティブ」機能レベル以上である必要があります。すべてのフォレスト機能レベルがサポートされます。

- **書き込み可能なドメインコントローラー。** 読み取り専用ドメインコントローラーはサポートされていません。

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

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

複数のActive Directoryフォレスト環境での展開

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

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

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

> **注意:**
>
> レジストリを誤って編集すると、オペレーティングシステムの再インストールが必要になるような深刻な問題が発生する可能性があります。Citrix®は、レジストリエディターの誤った使用によって生じる問題が解決できることを保証できません。レジストリエディターの使用

> は、お客様ご自身の責任において行ってください。編集する前にレジストリをバックアップしてください。

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

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

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

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

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

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

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

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

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

セットアップ中に外部信頼が設定されている場合、`ListOfSIDs` レジストリキーが必要です。Active Directory FQDNがDNS FQDNと異なる場合、またはドメインコントローラーを含むドメイ

ンのNetBIOS名がActive Directory FQDNと異なる場合、`ListOfSIDs`レジストリキーも必要です。レジストリキーを追加するには、以下の情報を使用します:

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

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

外部信頼が設定されている場合、VDAで次の変更を行います:

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

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

次の表に、サポートされている信頼の種類を示します。

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

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

Microsoft Entraハイブリッド参加済み

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

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

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

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

要件

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

制限事項

- Citrix Federated Authentication Service (FAS) を使用する場合、シングルサインオンはMicrosoft Entra IDではなくオンプレミスのADに転送されます。この場合、ユーザーログオン

時にプライマリ更新トークン (PRT) が生成されるようにMicrosoft Entra証明書ベース認証を構成することをお勧めします。これにより、セッション内のMicrosoft Entraリソースへのシングルサインオンが容易になります。そうしないと、PRTが存在せず、Microsoft EntraリソースへのSSOは機能しません。Citrix Federated Authentication Service (FAS) を使用してハイブリッド参加済みVDAへのMicrosoft Entraシングルサインオン (SSO) を実現する方法については、「ハイブリッド参加済みVDA」を参照してください。

- マシンカタログの作成または更新時にイメージの準備をスキップしないでください。イメージの準備をスキップする場合は、マスターVMがMicrosoft EntraまたはMicrosoft Entra ハイブリッド参加済みではないことを確認してください。

考慮事項

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

  a. `gpedit.msc`を実行します。

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

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

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

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

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

$MaxCount = 60
```

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

{

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

  {

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

    if ($provider -eq 'Citrix')

    {

        break;

    }



    if ($provider -eq 1)

    {

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

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

        Start-Sleep 5

        dsregcmd /join

        break

    }

  }
```

```
    Start-Sleep 1

}
```

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

次のステップ

Microsoft Entra ハイブリッド参加カタログの ID プールの作成の詳細については、Microsoft Entra ハイブリッド参加マシン ID の ID プールを参照してください。

ドメインに参加していない

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

要件

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

制限事項

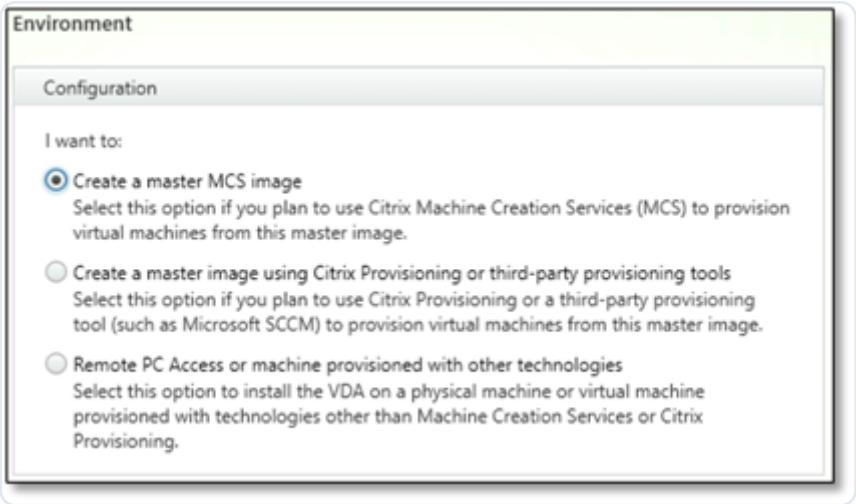
- サービス継続性はサポートされていません。
- マルチセッションのドメインに参加していないVDAを使用する場合、ローカルユーザーのプロファイルデータは保持されず、ログオフ時に削除されます。

VDAのインストールと構成

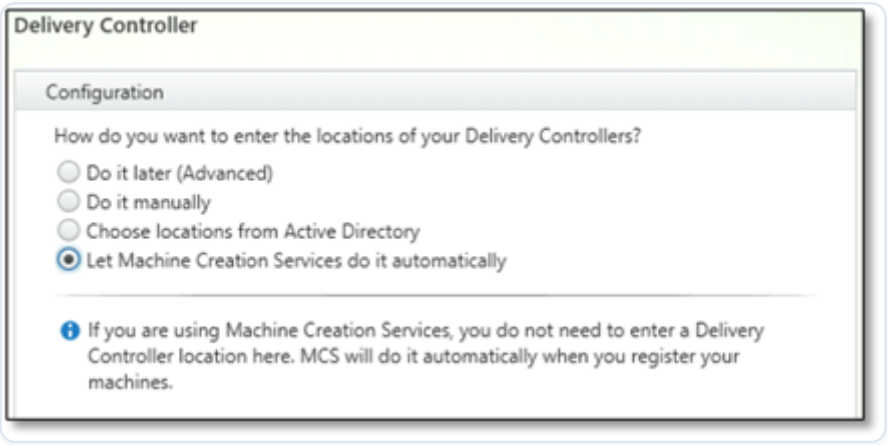
VDAをインストールする手順に従います。

1. インストールウィザードで以下のオプションを選択していることを確認してください。

   - 「環境」ページで、**「マスターMCSイメージを作成」**を選択します。



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



次のステップ

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

インストール準備

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

- 1つ以上のDelivery Controller

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

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

注:

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

- Microsoft **ボリュームシャドウコピー** サービスと **Microsoft Software Shadow Copy Provider** サービスが実行されていること。詳しくは、「ボリュームシャドウコピーサービス」を参照してください。
- **MS-Defender** のバージョンが4.18.2105.5より高いこと。詳しくは、「Microsoft Defender Antivirusのセキュリティインテリジェンスと製品の更新」を参照してください。

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

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

製品ISOには、Active Directory内のマシンにVDAをインストール、アップグレード、または削除するサンプルスクリプトが含まれています。これらのスクリプトを使用して、Machine Creation

Services (MCS) およびCitrix Provisioning (旧Provisioning Services) で使用されるイメージを管理することもできます。詳しくは、「スクリプトを使用したVDAのインストール」を参照してください。

インストール前に確認する情報

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

コンポーネントのインストール場所

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

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

- すべてのコアコンポーネントを1つのサーバーにインストールすることは、評価、テスト、または小規模な本番環境の展開で機能します。

- 将来の拡張に対応するため、コンポーネントを異なるサーバーにインストールすることを検討してください。たとえば、StudioをControllerをインストールしたサーバーとは別のマシンにインストールすると、サイトをリモートで管理できます。
- ほとんどの本番環境の展開では、コアコンポーネントを別々のサーバーにインストールすることをお勧めします。

  他のサーバーに他のコンポーネントをインストールする前に、Citrix License Serverとライセンスをインストールします。
- Server CoreOS（Delivery Controllerなど）にサポートされているコンポーネントをインストールするには、(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/install-configure/install-core/install-command.html)必要があります。このOSタイプにはグラフィカルインターフェイスがないため、Studioやその他のツールは別の場所にインストールし、それらをControllerサーバーにポイントしてください。

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

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

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

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

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

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

> **ヒント:**
>
> デフォルト値は`HostTime="UTC"`です。この値をUTC以外のもの（例: `Local`）に変更します。この変更により、ホストとの時刻同期が実質的に無効になります。

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

コンポーネントをインストールしない場所:

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

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

権限とActive Directoryの要件

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

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

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

- (/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/system-requirements.html) には、サポートされている Active Directory の機能レベルが記載されています。(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/install-configure/machine-identities/active-directory.html) に詳細情報があります。
- Active Directory ドメインサービスを実行しているドメインコントローラーが少なくとも1つ必要です。
- ドメインコントローラーに Citrix Virtual Apps and Desktops コンポーネントをインストールしないでください。
- Studio で組織単位名を指定する際に、スラッシュ (/) を使用しないでください。

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

詳細については、以下を参照してください。

- (/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/secure/best-practices.html)
- (/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/manage-deployment/delegated-administration.html)
- Active Directory 構成に関する Microsoft ドキュメント

インストールのガイダンス、考慮事項、およびベストプラクティス

いずれかのコンポーネントのインストール中

- フルプロダクトメディアから Delivery Controller、Studio、License Server、または Director をインストールまたはアップグレードする際に、Citrix インストーラーがマシン上の以前の Windows インストールからの再起動が保留中であることを検出すると、インストーラーは終了/リターンコード 9 で停止します。マシンの再起動を促されます。

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

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

- 通常、コンポーネントに前提条件がある場合、インストーラーはそれらが存在しない場合に展開します。一部の前提条件では、マシンの再起動が必要になる場合があります。
- インストール前、インストール中、インストール後にオブジェクトを作成するときは、各オブジェクトに一意の名前を指定してください。たとえば、ネットワーク、グループ、カタログ、リソースには一意の名前を付けてください。
- コンポーネントのインストールが正常に完了しなかった場合、インストールはエラーメッセージを表示して停止します。正常にインストールされたコンポーネントは保持されます。それらを再インストールする必要はありません。
- コンポーネントをインストール（またはアップグレード）すると、Citrix Analytics が自動的に収集されます。デフォルトでは、インストールが完了するとそのデータは自動的にCitrixにアップロードされます。また、コンポーネントをインストールすると、匿名データをアップロードするCitrixカスタマーエクスペリエンス向上プログラム（CEIP）に自動的に登録されます。

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

- Studioをインストール（またはアップグレード）すると、Google Analyticsが自動的に収集され（後でアップロードされ）ます。Studioのインストール後、レジストリキー `HKLM\Software\Citrix\DesktopStudio\GAEnabled` を使用してこの設定を変更できます。値が**1**の場合は収集とアップロードが有効になり、**0**の場合は収集とアップロードが無効になります。
- VDAのインストールが失敗した場合、MSIアナライザーは失敗したMSIログを解析し、正確なエラーコードを表示します。既知の問題である場合、アナライザーはCTX記事を提案します。

アナライザーは、失敗エラーコードに関する匿名化されたデータも収集します。このデータは、CEIPによって収集された他のデータに含まれます。CEIPへの登録を終了すると、収集されたMSIアナライザーデータはCitrixに送信されなくなります。

VDAのインストール中

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

  制限を承諾するか、VDAのインストールを終了して、Media Foundationのインストール後に再開することができます。グラフィカルインターフェイスでは、この選択肢はメッセージで表示されます。コマンドラインでは、`/no_mediafoundation_ack`オプションを使用して制限を承諾できます。
- VDAをインストールすると、**Direct Access Users**という新しいローカルユーザーグループが自動的に作成されます。シングルセッションOS用VDAでは、このグループはRDP接続にのみ適用されます。マルチセッションOS用VDAでは、このグループはICA®およびRDP接続に適用されます。
- VDAは、通信するための有効なControllerアドレスを持っている必要があります。そうでない場合、セッションを確立できません。Controllerアドレスは、VDAのインストール時または後で指定できます。必ず実行してください。詳細については、「VDA登録」を参照してください。

VDAインストール後およびインストール中の再起動

VDAインストールの最後に再起動が必要です。その再起動は、デフォルトで自動的に行われます。

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

VDAインストール中に必要な再起動の回数を最小限に抑えるには：

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

VDAをインストールする前にこれらの前提条件をインストールしない場合：

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

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

インストールまたはアップグレードの失敗時の復元

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

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

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

この機能が有効な状態でシングルセッションVDAのインストールまたはアップグレードが開始されると、インストーラーは実際のインストールまたはアップグレードを開始する前にシステム復元ポイントを作成します。VDAのインストールまたはアップグレードが失敗した場合、マシンは

復元ポイントの状態に戻されます。`%temp%/Citrix`フォルダーには、展開ログと復元に関するその他の情報が含まれています。

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

デフォルトでは、この機能は無効になっています。

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

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

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

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

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

インストーラー

フルプロダクトインストーラー

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

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

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

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

スタンドアロン VDA インストーラー

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

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

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

3つのスタンドアロンVDAインストーラーをダウンロードできます。

VDAServerSetup.exe:

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

VDAWorkstationSetup.exe:

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

VDAWorkstationCoreSetup.exe:

Remote PC Access展開またはコアVDIインストール用に最適化されたシングルセッションOS用VDAをインストールします。Remote PC Accessは物理マシンを使用します。コアVDIインストールは、イメージとして使用されていないVMです。このような展開のVDA接続に必要なコアサービスのみをインストールします。そのため、フルプロダクトインストーラーまたは `VDAWorkstationSetup.exe` インストーラーで有効なオプションのサブセットのみをサポートします。

このインストーラーは、以下の目的で使用されるコンポーネントをインストールまたは含みません。

- アップブイ。
- Profile Management。Citrix Profile Managementをインストールから除外すると、Citrix Directorの表示に影響します。詳細については、「VDAのインストール」を参照してください。
- マシンIDサービス。
- Citrix サポートツール。
- シトリックス ファイル for Windows。
- シトリックス ファイル for Outlook。

`VDAWorkstationCoreSetup.exe`インストーラーは、Windows向けCitrix Workspaceアプリをインストールまたは含みません。

`VDAWorkstationCoreSetup.exe`を使用することは、フルプロダクトインストーラーまたは`VDAWorkstationSetup`インストーラーを使用してシングルセッションOS VDAをインストールし、以下のいずれかを実行することと同じです。

- グラフィカルインターフェイスで、 ページでRemote PC Accessオプションを選択します。
- コマンドラインインターフェイスで: `/remotepc` オプションを指定する。
- コマンドラインインターフェイスで: `/components vda` と、有効な追加コンポーネント名をすべてリストする `/exclude` オプションを指定する。

省略されたコンポーネント/機能は、後でフルプロダクトインストーラーを実行してインストールできます。この操作により、不足しているすべてのコンポーネントをインストールできます。

`VDAWorkstationCoreSetup.exe` インストーラーは、Browser Content Redirection MSI を自動的にインストールします。この自動インストールは、VDA リリース 2003 以降のサポート対象リリースに適用されます。

Citrix インストールリターンコード

インストールログには、コンポーネントインストールの結果が Microsoft の値ではなく、Citrix のリターンコードとして含まれています。

- 0 = 成功
- 1 = 失敗
- 2 = 部分的な成功
- 3 = 部分的な成功と再起動が必要
- 4 = 失敗と再起動が必要
- 5 = ユーザーによってキャンセルされました
- 6 = コマンドライン引数が不足しています
- 7 = 新しいバージョンが見つかりました
- 8 = 成功と再起動が必要
- 9 = ファイルロック再起動
- 10 = 中止
- 11 = メディア失敗

- 12 = ライセンス失敗
- 13 = 事前チェック失敗
- 14 = 再起動保留チェック中止
- -1 = 終了

例えば、Microsoft System Center Configuration Managerなどのツールを使用する場合、インストールログにリターンコード3が含まれていると、スクリプトによるVDAインストールが失敗したように見えることがあります。これは、VDAインストーラーがユーザーが開始する必要のある再起動を待機している場合に発生する可能性があります (例えば、サーバーへのRDSロールの前提条件のインストール後など)。VDAインストールは、すべての前提条件と選択されたコンポーネントがインストールされ、インストール後にマシンが再起動されて初めて成功と見なされます。

あるいは、インストールをCMDスクリプト (Microsoftの終了コードを返します) でラップするか、Configuration Managerパッケージの成功コードを変更できます。

Windows Serverワークロード向けにMicrosoft RDSライセンスサーバーを構成する

この製品は、Windows 2016などのWindows Serverワークロードを提供する場合に、Windows Serverリモートセッション機能にアクセスします。これには通常、リモートデスクトップサービスクライアントアクセスライセンス (RDS CAL) が必要です。VDAは、RDS CALを要求するためにRDSライセンスサーバーに接続できる必要があります。ライセンスサーバーをインストールしてアクティブ化します。詳細については、Microsoftドキュメント「リモートデスクトップサービスライセンスサーバーをアクティブ化する」を参照してください。概念実証環境では、Microsoftが提供する猶予期間を使用できます。

この方法を使用すると、このサービスにライセンスサーバー設定を適用させることができます。イメージ上のRDSコンソールで、ライセンスサーバーとユーザーごとのモードを構成できます。Microsoftグループポリシー設定を使用してライセンスサーバーを構成することもできます。詳細については、Microsoftドキュメント「クライアントアクセスライセンス (CAL) を使用してRDS展開をライセンスする」を参照してください。

グループポリシー設定を使用してRDSライセンスサーバーを構成するには:

1. 利用可能なマシンにリモートデスクトップサービスライセンスサーバーをインストールします。そのマシンは常に利用可能である必要があります。Citrix製品のワークロードは、このライセンスサーバーに到達できる必要があります。

2. Microsoftグループポリシーを使用して、ライセンスサーバーのアドレスとユーザーごとのライセンスモードを指定します。詳細については、Microsoftドキュメント「RDセッションホストサーバーのリモートデスクトップライセンスモードを指定する」を参照してください。

Windows 10ワークロードには、適切なWindows 10ライセンスのアクティベーションが必要です。Windows 10ワークロードをアクティベートするには、Microsoftのドキュメントに従うことをお勧めします。

詳細情報

特定のホストタイプのリソースの場所を設定する場合:

- AWSクラウド環境
- XenServer仮想化環境
- Google Cloud環境
- Microsoft Azure Resource Managerクラウド環境
- マイクロソフト システム センター コンフィギュレーション マネージャー 環境
- マイクロソフト System Center Virtual Machine Manager 仮想化環境
- Nutanix仮想化環境
- Nutanixクラウドおよびパートナーソリューション
- VMware 仮想化環境
- VMware クラウドおよびパートナーソリューション

AWSクラウド環境

この記事では、Citrix Virtual Apps and Desktops で使用できるリソースの場所として AWS アカウントを設定する方法を説明します。このリソースの場所には、概念実証や、複数のアベイラビリティゾーンにリソースを分散させる必要のないその他の展開に最適な、基本的なコンポーネントセットが含まれています。これらのタスクを完了すると、VDA をインストールし、マシンをプロビジョニングし、マシンカタログを作成し、デリバリーグループを作成できます。

この記事のタスクを完了すると、リソースロケーションには次のコンポーネントが含まれます。

- 単一のアベイラビリティゾーン内にパブリックサブネットとプライベートサブネットを持つ仮想プライベートクラウド (VPC)。
- VPCのプライベートサブネットに配置され、Active DirectoryドメインコントローラーとDNSサーバーの両方として実行されるインスタンス。

- VPCのパブリックサブネットで踏み台ホストとして機能するインスタンス。このインスタンスは、管理目的でプライベートサブネット内のインスタンスへのRDP接続を開始するために使用されます。リソースの場所の設定が完了したら、このインスタンスをシャットダウンして、容易にアクセスできないようにすることができます。VDAインスタンスなど、プライベートサブネット内の他のインスタンスを管理する必要がある場合は、踏み台ホストインスタンスを再起動できます。

タスクの概要

パブリックサブネットとプライベートサブネットを持つ仮想プライベートクラウド（VPC）を設定します。このタスクを完了すると、AWSはパブリックサブネットにElastic IPアドレスを持つNATゲートウェイを展開します。このアクションにより、プライベートサブネット内のインスタンスがインターネットにアクセスできるようになります。パブリックサブネット内のインスタンスはインバウンドのパブリックトラフィックにアクセスできますが、プライベートサブネット内のインスタンスはアクセスできません。

セキュリティグループを構成します。 セキュリティグループは、VPC内のインスタンスのトラフィックを制御する仮想ファイアウォールとして機能します。パブリックサブネット内のインスタンスがプライベートサブネット内のインスタンスと通信できるようにするルールをセキュリティグループに追加します。また、これらのセキュリティグループをVPC内の各インスタンスに関連付けます。

DHCPオプションセットを作成します。Amazon VPCでは、DHCPおよびDNSサービスがデフォルトで提供されており、Active Directoryドメインコントローラーでの DNSの構成方法に影響します。AmazonのDHCPは無効にできず、AmazonのDNSはパブリックDNS解決にのみ使用でき、Active Directory名解決には使用できません。DHCPを介してインスタンスに渡されるドメインとネームサーバーを指定するには、DHCPオプションセットを作成します。このセットは、Active Directoryドメインサフィックスを割り当て、VPC内のすべてのインスタンスのDNSサーバーを指定します。インスタンスがドメインに参加したときにホスト（A）および逆引き（PTR）レコードが自動的に登録されるようにするには、プライベートサブネットに追加する各インスタンスのネットワークアダプタープロパティを構成します。

踏み台ホストとドメインコントローラーをVPCに追加します。踏み台ホストを介して、プライベートサブネット内のインスタンスにログオンし、ドメインを設定してインスタンスをドメインに参加させることができます。

タスク1：VPCをセットアップする

1. AWSマネジメントコンソールから、**VPC**を選択します。
2. VPCダッシュボードから、**Create VPC**を選択します。

3. 「**VPC and more**」を選択します。
4. NAT ゲートウェイ ($) の下で、「**In 1 AZ**」または「**1 per AZ**」を選択します。
5. DNS オプションの下で、「**Enable DNS hostnames**」が選択されたままにします。
6. 「**Create VPC**」を選択します。AWS は、パブリックサブネットとプライベートサブネット、インターネットゲートウェイ、ルートテーブル、およびデフォルトのセキュリティグループを作成します。

タスク 2: セキュリティグループの構成

このタスクでは、VPC 用に次のセキュリティグループを作成および構成します:

- パブリックサブネット内のインスタンスに関連付けるためのパブリックセキュリティグループ。
- プライベートサブネット内のインスタンスに関連付けるためのプライベートセキュリティグループ。

セキュリティグループを作成するには:

1. VPC ダッシュボードで、「**Security Groups**」を選択します。
2. パブリックセキュリティグループ用のセキュリティグループを作成します。「**Create Security Group**」を選択し、グループの名前タグと説明を入力します。VPC で、以前に作成した VPC を選択します。「**Yes, Create**」を選択します。

パブリックセキュリティグループの構成

1. セキュリティグループのリストから、パブリックセキュリティグループを選択します。
2. **［Inbound Rules］**タブを選択し、［Edit］**を選択して、次のルールを作成します。

タイプ	送信元
すべてのトラフィック	プライベートセキュリティグループを選択します。
すべてのトラフィック	パブリックセキュリティグループを選択します。
ICMP	0.0.0.0/0
22 (SSH)	0.0.0.0/0
80 (HTTP)	0.0.0.0/0

タイプ	送信元
443 (HTTPS)	0.0.0.0/0
1494 (ICA/HDX)	0.0.0.0/0
2598 (セッションの信頼性)	0.0.0.0/0
3389 (RDP)	0.0.0.0/0

3. 完了したら、**保存**を選択します。
4. **［Outbound Rules］タブを選択し、［Edit］**を選択して、次のルールを作成します。

タイプ	宛先
すべてのトラフィック	プライベートセキュリティグループを選択します。
すべてのトラフィック	0.0.0.0/0
ICMP	0.0.0.0/0

5. 完了したら、**保存**を選択します。

プライベートセキュリティグループを構成する

1. セキュリティグループリストから、プライベートセキュリティグループを選択します。
2. パブリックセキュリティグループからのトラフィックを設定していない場合は、TCPポートを設定する必要があります。**［Inbound Rules］タブを選択し、［Edit］**を選択して、次のルールを作成します。

タイプ	送信元
すべてのトラフィック	プライベートセキュリティグループを選択します。
すべてのトラフィック	パブリックセキュリティグループを選択します。
ICMP	パブリックセキュリティグループを選択します。

タイプ	送信元
TCP 53 (DNS)	パブリックセキュリティグループを選択します。
UDP 53 (DNS)	パブリックセキュリティグループを選択します。
80 (HTTP)	パブリックセキュリティグループを選択します。
TCP 135	パブリックセキュリティグループを選択します。
TCP 389	パブリックセキュリティグループを選択します。
UDP 389	パブリックセキュリティグループを選択します。
443 (HTTPS)	パブリックセキュリティグループを選択します。
TCP 1494 (ICA/HDX)	パブリックセキュリティグループを選択します。
TCP 2598 (セッションの信頼性)	パブリックセキュリティグループを選択します。
3389 (RDP)	パブリックセキュリティグループを選択します。
TCP 49152–65535	パブリックセキュリティグループを選択します。

3. 完了したら、**保存**を選択します。
4. **［Outbound Rules］**タブを選択し、［Edit］**を選択して、次のルールを作成します。

タイプ	宛先
すべてのトラフィック	プライベートセキュリティグループを選択します。

タイプ	宛先
すべてのトラフィック	0.0.0.0/0
ICMP	0.0.0.0/0
UDP 53 (DNS)	0.0.0.0/0

5. 完了したら、**保存**を選択します。

タスク3：インスタンスの起動

次の手順を実行して、2つのEC2インスタンスを作成し、Amazonが生成するデフォルトの管理者パスワードを復号します。

1. AWS管理コンソールから、**EC2**を選択します。
2. EC2ダッシュボードから、**インスタンスの起動**を選択します。
3. Windows Serverマシンイメージとインスタンスタイプを選択します。
4. **［Configure Instance Details］**ページで、インスタンスの名前を入力し、以前に設定したVPCを選択します。
5. **サブネット**で、各インスタンスについて次の選択を行います。
   - Bastionホスト：パブリックサブネットを選択します
   - ドメインコントローラー：プライベートサブネットを選択します
6. **「パブリック IP アドレスの自動割り当て」**で、各インスタンスについて次の選択を行います。
   - 踏み台ホスト：**［Enable］**を選択します。
   - ドメインコントローラー：**［Use default setting］または［Disable］**を選択します。
7. **「ネットワークインターフェース」**で、ドメインコントローラーのプライベートサブネットのIP範囲内のプライマリIPアドレスを入力します。
8. 必要に応じて、**「ストレージの追加」**ページでディスクサイズを変更します。
9. **「インスタンスのタグ付け」**ページで、各インスタンスにわかりやすい名前を入力します。
10. **「セキュリティグループの設定」**ページで、**「既存のセキュリティグループを選択」**を選択し、各インスタンスについて次の選択を行います。
    - バスティオンホスト: パブリックセキュリティグループを選択します。

- ドメインコントローラー: プライベートセキュリティグループを選択します。

11. 選択内容を確認し、「**起動**」を選択します。
12. 新しいキーペアを作成するか、既存のキーペアを選択します。新しいキーペアを作成する場合は、秘密鍵（.pem）ファイルをダウンロードして安全な場所に保管してください。インスタンスのデフォルトの管理者パスワードを取得する際に、秘密鍵を提供する必要があります。
13. 「**インスタンスの起動**」を選択します。「**インスタンスの表示**」を選択して、インスタンスのリストを表示します。新しく起動したインスタンスがすべてのステータスチェックに合格するまで待ってからアクセスしてください。
14. 各インスタンスのデフォルトの管理者パスワードを取得します。
    a. インスタンスリストから、インスタンスを選択し、「**接続**」を選択します。
    b. 「**RDP クライアント**」タブに移動し、「**パスワードの取得**」を選択し、プロンプトが表示されたら秘密鍵 (`.pem`) ファイルをアップロードします。
    c. 「**パスワードの復号**」を選択して、人間が読めるパスワードを取得します。AWSはデフォルトのパスワードを表示します。
15. 手順2から繰り返して、2つのインスタンスを作成します。
    - パブリックサブネットに1つの踏み台ホストインスタンス
    - ドメインコントローラーとして使用するプライベートサブネット内のインスタンスを1つ。

タスク4：DHCPオプションセットを作成する

1. VPCダッシュボードから、「**DHCPオプションセット**」を選択します。
2. 次の情報を入力します。
    - 名前タグ：セットのわかりやすい名前を入力します。
    - ドメイン名：ドメインコントローラーインスタンスを設定するときに使用する完全修飾ドメイン名を入力します。
    - ドメインネームサーバー：ドメインコントローラーインスタンスに割り当てたプライベートIPアドレスと、カンマで区切られた文字列「**AmazonProvidedDNS**」を入力します。
    - NTPサーバー：このフィールドは空白のままにします。
    - NetBIOSネームサーバー：ドメインコントローラーインスタンスのプライベートIPアドレスを入力します。
    - NetBIOSノードタイプ：「**2**」と入力します。
3. **はい、作成**を選択します。

4. 新しいセットをVPCに関連付けます。

    a. VPCダッシュボードから、**Your VPCs**を選択し、以前に設定したVPCを選択します。

    b. **アクション > DHCPオプションセットの編集**を選択します。

    c. プロンプトが表示されたら、作成した新しいセットを選択し、「**保存**」を選択します。

タスク5：インスタンスを構成する

1. RDPクライアントを使用して、踏み台ホストインスタンスのパブリックIPアドレスに接続します。プロンプトが表示されたら、管理者アカウントの資格情報を入力します。
2. 踏み台ホストインスタンスから、リモートデスクトップ接続を起動し、構成するインスタンスのプライベートIPアドレスに接続します。プロンプトが表示されたら、インスタンスの管理者資格情報を入力します。
3. プライベートサブネット内のすべてのインスタンスについて、DNS設定を構成します。

    a. **スタート > コントロールパネル > ネットワークとインターネット > ネットワークと共有センター > アダプターの設定の変更**を選択します。表示されているネットワーク接続をダブルクリックします。

    b. **プロパティ > インターネットプロトコルバージョン4 (TCP/IPv4) > プロパティ**を選択します。

    c. 「**詳細設定 > DNS**」を選択します。次の設定が有効になっていることを確認し、「**OK**」を選択します。

        - この接続のアドレスをDNSに登録する
        - この接続のDNSサフィックスをDNS登録で使用する

4. ドメインコントローラーを構成するには:

    a. Server Manager を使用して、Active Directory ドメインサービス の役割をすべてのデフォルト機能とともに追加します。

    b. インスタンスをドメインコントローラーに昇格させます。昇格中にDNSを有効にし、DHCPオプションセットを作成したときに指定したドメイン名を使用します。プロンプトが表示されたらインスタンスを再起動します。

次のステップ

- コアコンポーネントをインストールする
- VDAのインストール
- サイトを作成する

- AWS での接続の作成と管理については、AWS への接続 を参照してください。

詳細情報

- 接続とリソースの作成および管理
- マシンカタログの作成

XenServer® 仮想化環境

XenServer は運用管理を簡素化し、負荷の高いワークロード向けに高精細なユーザーエクスペリエンスを保証します。

XenServer をセットアップするには、「(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/install-configure/install-prepare.html)インストール準備」を参照してください。

次に行うこと

- コアコンポーネントのインストール
- VDAのインストール
- サイトの作成
- XenServer で接続を作成および管理するには、「(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/install-configure/connections/connection-citrix-hypervisor.html)XenServer への接続」を参照してください。

詳細情報

- 接続とリソースの作成および管理
- マシンカタログの作成

Google Cloud環境

Citrix Virtual Apps and Desktops™ を使用すると、Google Cloud 上でマシンをプロビジョニングおよび管理できます。

要件

- Citrix Cloud™アカウント。この記事で説明されている機能は、Citrix Cloudでのみ利用可能です。
- Google Cloudプロジェクト。このプロジェクトには、マシンカタログに関連付けられているすべてのコンピューティングリソースが保存されます。既存のプロジェクトでも新規のプロジェクトでもかまいません。

- Google Cloudプロジェクトで4つのAPIを有効にします。詳細については、「Enable Google Cloud APIs」を参照してください。
- Google Cloud サービスアカウント。サービスアカウントは、プロジェクトへのアクセスを有効にするために Google Cloud に対して認証を行います。詳細については、「サービスアカウントの構成と更新」を参照してください。
- Googleプライベートアクセスを有効にします。詳細については、「Enable-private-google-access」を参照してください。

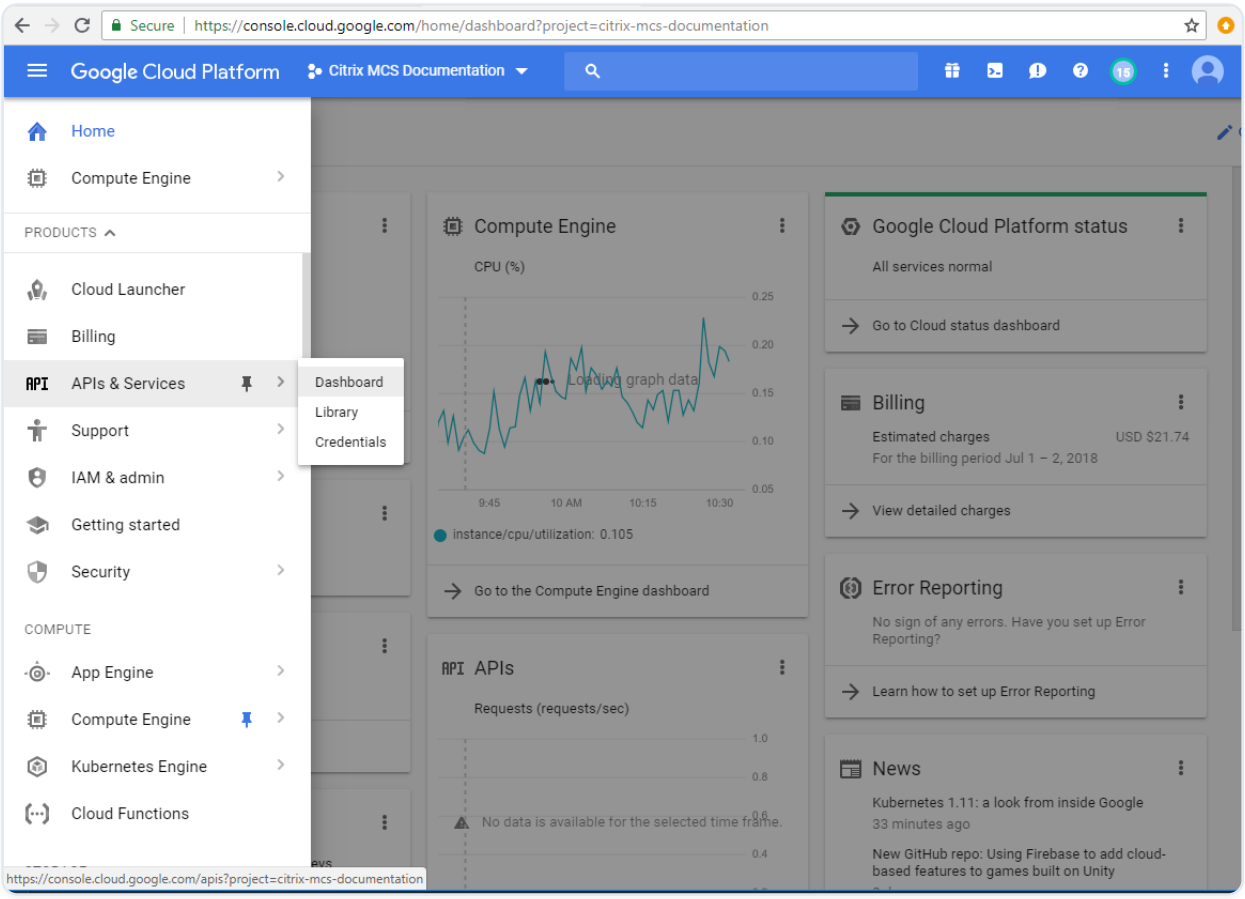
Google Cloud APIを有効にする

Web Studioを介してGoogle Cloudの機能を使用するには、Google Cloudプロジェクトで次のAPIを有効にします。

- コンピュート エンジン API
- クラウド リソース マネージャー API
- ID およびアクセス管理 (IAM) API
- クラウド ビルド API
- クラウド キー マネジメント サービス (KMS)

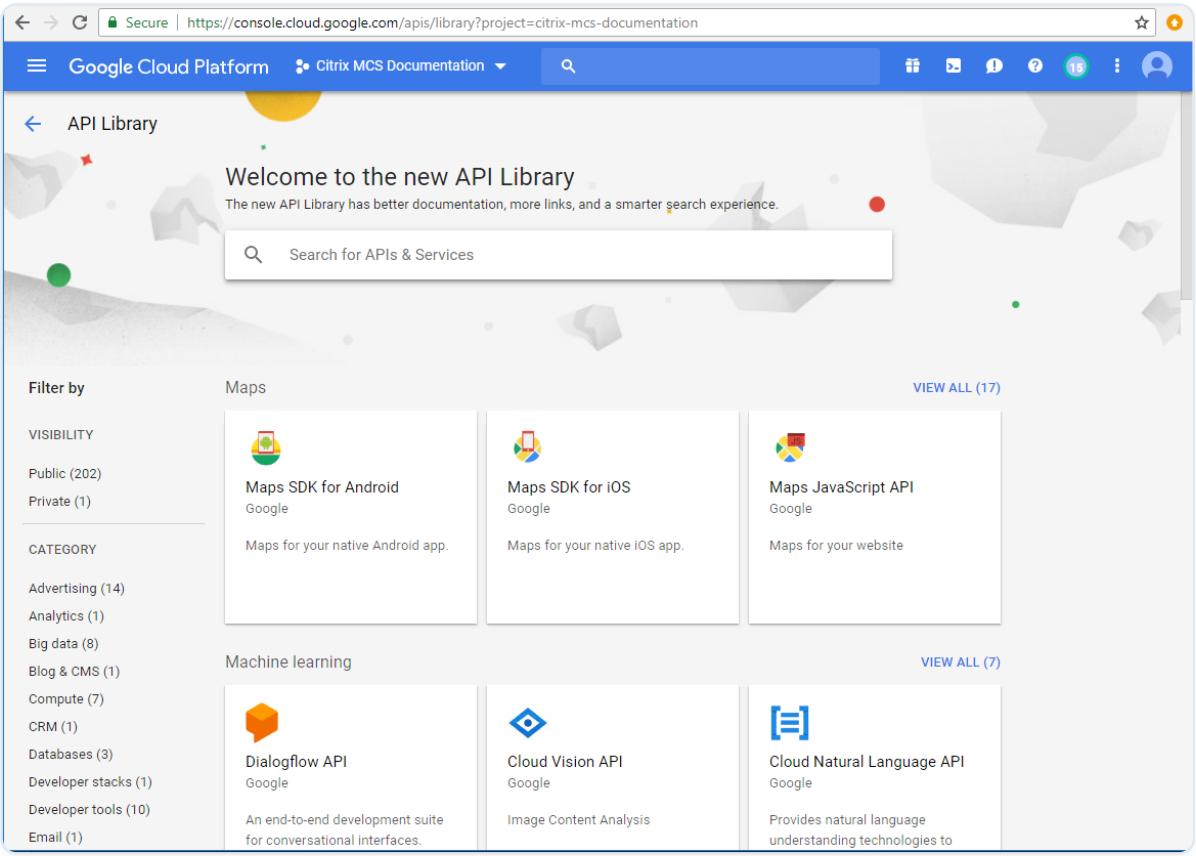
Google Cloudコンソールから、次の手順を実行します。

1. 左上のメニューで、**「APIとサービス」>「ダッシュボード」**を選択します。



2. **ダッシュボード**画面で、Compute Engine APIが有効になっていることを確認します。 有効になっていない場合は、次の手順に従ってください。

   a. 「**APIとサービス > ライブラリ**」に移動します。



b. 検索ボックスに「*Compute Engine*」と入力します。

c. 検索結果から「**Compute Engine API**」を選択します。

d. 「**Compute Engine API**」ページで、「**有効にする**」を選択します。

3. Cloud Resource Manager APIを有効にします。

a. 「**APIとサービス > ライブラリ**」に移動します。

b. 検索ボックスに「*Cloud Resource Manager*」と入力します。

c. 検索結果から「**Cloud Resource Manager API**」を選択します。

d. 「**Cloud Resource Manager API**」ページで、「**有効にする**」を選択します。APIのステータスが表示されます。

4. 同様に、**Identity and Access Management (IAM) API**と**Cloud Build API**を有効にします。

Google Cloud Shellを使用してAPIを有効にすることもできます。これを行うには：

1. Googleコンソールを開き、Cloud Shellをロードします。
2. Cloud Shellで次の4つのコマンドを実行します。

- gcloud services enable compute.googleapis.com を有効にします。
- gcloud services enable cloudresourcemanager.googleapis.com を有効にします。

- gcloud services enable iam.googleapis.com を有効にします。
- gcloud services enable cloudbuild.googleapis.com を有効にします。

3. Cloud Shellがプロンプトを表示した場合、「**承認**」をクリックします。

サービスアカウントの構成と更新

> **注：**
>
> GCPは、Cloud Build Serviceのデフォルトの動作とサービスアカウントの使用に関して、April 29, 2024以降に変更を導入します。詳細については、Cloud Build Service Account Changeを参照してください。April 29, 2024より前にCloud Build APIが有効になっている既存のGoogleプロジェクトは、この変更の影響を受けません。ただし、April 29以降も既存のCloud Build Serviceの動作を維持したい場合は、Cloud Build APIを有効にする前に、組織のポリシーを作成または適用して制約の適用を無効にすることができます。その結果、以下のコンテンツは2つに分かれています。April 29, 2024より前とApril 29, 2024以降です。新しい組織ポリシーを設定した場合は、April 29, 2024より前のセクションに従ってください。

April 29, 2024より前

Citrix Cloudは、Google Cloudプロジェクト内で3つの個別のサービスアカウントを使用します。

- *Citrix Cloudサービスアカウント*: このサービスアカウントにより、Citrix CloudはGoogleプロジェクトにアクセスし、マシンをプロビジョニングおよび管理できます。このサービスアカウントは、Google Cloudによって生成されたキーを使用してGoogle Cloudに認証します。

  ここに概説されているように、このサービスアカウントを手動で作成する必要があります。詳細については、Citrix Cloudサービスアカウントの作成を参照してください。

  このサービスアカウントは、メールアドレスで識別できます。例: `<my-service-account>@<project-id>.iam.gserviceaccount.com`。
- *Cloud Buildサービスアカウント*: このサービスアカウントは、Google Cloud APIの有効化で言及されているすべてのAPIを有効にすると自動的にプロビジョニングされます。自動的に作成されたすべてのサービスアカウントを表示するには、**Google Cloud**コンソールで**IAMと管理 > IAM**に移動し、**Googleが提供するロールの付与を含める**チェックボックスをオンにします。

  このサービスアカウントは、**プロジェクトID**と**cloudbuild**という単語で始まるメールアドレスで識別できます。例: `<project-id>@cloudbuild.gserviceaccount.com`

サービスアカウントに以下のロールが付与されていることを確認します。ロールを追加する必要がある場合は、Cloud Build サービスアカウントにロールを追加するに記載されている手順に従ってください。

  - Cloud Build サービスアカウント
  - Compute Instance 管理者
  - サービスアカウントユーザー

- *Cloud Compute サービスアカウント*: このサービスアカウントは、Compute API がアクティブ化されると、Google Cloud によって Google Cloud で作成されたインスタンスに追加されます。このアカウントには、操作を実行するための IAM 基本編集者ロールがあります。ただし、よりきめ細かな制御を行うためにデフォルトの権限を削除した場合は、次の権限を必要とする **Storage Admin** ロールを追加する必要があります。

  - resourcemanager.projects.get
  - storage.objects.create
  - storage.objects.get
  - storage.objects.list

このサービスアカウントは、**プロジェクト ID** と **compute** という単語で始まるメールアドレスで識別できます。例: `<project-id>-compute@developer.gserviceaccount.com`。

CITRIX CLOUD サービスアカウントを作成する

Citrix Cloud サービスアカウントを作成するには、次の手順に従います。

1. Google Cloud コンソールで、**IAM と管理 > サービスアカウント**に移動します。
2. **サービスアカウント**ページで、**サービスアカウントを作成**を選択します。
3. **サービスアカウントの作成**ページで、必要な情報を入力し、**作成して続行**を選択します。
4. 「**このサービスアカウントにプロジェクトへのアクセスを許可する**」ページで、「**ロールを選択**」ドロップダウンメニューをクリックし、必要なロールを選択します。さらにロールを追加する場合は、「**+別のロールを追加**」をクリックします。

   各アカウント（個人またはサービス）には、プロジェクトの管理を定義するさまざまなロールがあります。このサービスアカウントには、以下のロールを付与してください。

   - Compute 管理者
   - Storage管理者
   - Cloud Build編集者

- サービスアカウントユーザー
- クラウド データストア ユーザー
- Cloud KMS 暗号オペレーター

Cloud KMS 暗号オペレーターには、以下の権限が必要です。

- cloudkms.cryptoKeys.get
- cloudkms.cryptoKeys.list
- cloudkms.keyRings.get
- cloudkms.keyRings.list

> **注：**
>
> 新しいサービスアカウントを作成する際に利用可能なロールの完全なリストを取得するには、すべてのAPIを有効にしてください。

5. **CONTINUE**をクリックします。
6. **このサービスアカウントへのユーザーアクセスを許可**ページで、このサービスアカウントでアクションを実行するアクセス権を付与するために、ユーザーまたはグループを追加します。
7. **DONE**をクリックします。
8. IAMメインコンソールに移動します。
9. 作成されたサービスアカウントを特定します。
10. ロールが正常に割り当てられていることを検証します。

考慮事項:

サービスアカウントを作成する際は、以下を考慮してください。

- **このサービスアカウントにプロジェクトへのアクセスを許可**および**このサービスアカウントへのユーザーアクセスを許可**の手順はオプションです。これらのオプションの構成手順をスキップすることを選択した場合、新しく作成されたサービスアカウントは、**IAMと管理 > IAM**ページに表示されません。
- サービスアカウントに関連付けられたロールを表示するには、オプションの手順をスキップせずにロールを追加します。このプロセスにより、構成されたサービスアカウントにロールが表示されるようになります。

CITRIX CLOUDサービスアカウントキー

Citrix DaaSで接続を作成するには、Citrix Cloudサービスアカウントキーが必要です。キーは資格情報ファイル（.json）に含まれています。キーを作成すると、ファイルは自動的にダウンロードされ、**ダウンロード**フォルダーに保存されます。キーを作成するときは、キーの種類をJSONに設定してください。そうしないと、Web Studioはそれを解析できません。

サービスアカウントキーを作成するには、**IAMと管理 > サービスアカウント**に移動し、Citrix Cloudサービスアカウントのメールアドレスをクリックします。**キー**タブに切り替え、**キーを追加 > 新しいキーを作成**を選択します。キータイプとして**JSON**を選択していることを確認してください。

> **ヒント:**
>
> Google Cloud コンソールで、**サービスアカウント**ページを使用してキーを作成します。セキュリティ上の理由から、キーを定期的に変更することをお勧めします。既存の Google Cloud 接続を編集することで、Citrix Virtual Apps and Desktops アプリケーションに新しいキーを提供できます。

CITRIX CLOUD サービスアカウントにロールを追加する

Citrix Cloud サービスアカウントにロールを追加するには、次の手順を実行します。

1. Google Cloud コンソールで、**IAM と管理 > IAM** に移動します。
2. **IAM > 権限**ページで、作成したサービスアカウントを電子メールアドレスで特定し、見つけます。

   例: `<my-service-account>@<project-id>.iam.gserviceaccount.com`
3. 鉛筆アイコンを選択して、サービスアカウントのプリンシパルへのアクセスを編集します。
4. 選択したプリンシパルオプションの**「project-id」へのアクセスを編集**ページで、**別のロールを追加**を選択して、必要なロールをサービスアカウントに1つずつ追加し、**保存**を選択します。

CLOUD BUILD サービスアカウントにロールを追加する

Cloud Build サービスアカウントにロールを追加するには、次の手順を実行します。

1. Google Cloud コンソールで、**IAM と管理 > IAM** に移動します。
2. **IAM**ページで、**プロジェクト ID**と**cloudbuild**という単語で始まる電子メールアドレスで識別できる Cloud Build サービスアカウントを見つけます。

例: `<project-id>@cloudbuild.gserviceaccount.com`

3. 鉛筆アイコンを選択して、Cloud Build アカウントのロールを編集します。
4. 選択したプリンシパルオプションの**「"project-id"へのアクセスを編集」ページ**で、「別のロールを追加」**を選択して、必要なロールをCloud Buildサービスアカウントに1つずつ追加し、**「保存」**を選択します。

> **注：**
>
> すべてのAPIを有効にして、ロールの完全なリストを取得します。

April 29, 2024 以降

Citrix Cloudは、Google Cloudプロジェクト内で2つの異なるサービスアカウントを使用します。

- *Citrix Cloudサービスアカウント*: このサービスアカウントにより、Citrix CloudはGoogleプロジェクトにアクセスし、マシンをプロビジョニングおよび管理できます。このサービスアカウントは、Google Cloudによって生成されたキーを使用してGoogle Cloudに認証します。

  このサービスアカウントは手動で作成する必要があります。

  このサービスアカウントは、メールアドレスで識別できます。例: `<my-service-account>@<project-id>.iam.gserviceaccount.com`。
- *Cloud Computeサービスアカウント*：このサービスアカウントは、Google Cloud APIを有効にするで言及されているすべてのAPIを有効にした後に自動的にプロビジョニングされます。自動的に作成されたすべてのサービスアカウントを表示するには、**Google Cloud**コンソールで**「IAMと管理」>「IAM」**に移動し、**「Google提供のロール付与を含める」**チェックボックスを選択します。このアカウントには、操作を実行するためのIAM基本編集者ロールがあります。ただし、より詳細な制御を行うためにデフォルトの権限を削除した場合、次の権限を必要とする**Storage Admin**ロールを追加する必要があります。
  - resourcemanager.projects.get
  - storage.objects.create
  - storage.objects.get
  - storage.objects.list

  このサービスアカウントは、**プロジェクトID**と**compute**という単語で始まるメールアドレスで識別できます。例：`<project-id>-compute@developer.gserviceaccount.com.`.

サービスアカウントに次のロールが付与されていることを確認します。

- Cloud Build サービスアカウント
- Compute Instance 管理者
- サービスアカウントユーザー

CITRIX CLOUD サービスアカウントを作成する

Citrix Cloud サービスアカウントを作成するには、次の手順に従います。

1. Google Cloud コンソールで、**IAM と管理 > サービスアカウント**に移動します。
2. **サービスアカウント**ページで、**サービスアカウントを作成**を選択します。
3. **サービスアカウントの作成**ページで、必要な情報を入力し、**作成して続行**を選択します。
4. 「**このサービスアカウントにプロジェクトへのアクセスを許可する**」ページで、「**ロールを選択**」ドロップダウンメニューをクリックし、必要なロールを選択します。さらにロールを追加する場合は、「**+別のロールを追加**」をクリックします。

   各アカウント（個人またはサービス）には、プロジェクトの管理を定義するさまざまなロールがあります。このサービスアカウントには、以下のロールを付与してください。

   - Compute 管理者
   - Storage管理者
   - Cloud Build編集者
   - サービスアカウントユーザー
   - クラウド データストア ユーザー
   - Cloud KMS 暗号オペレーター

   Cloud KMS 暗号オペレーターには、以下の権限が必要です。

   - cloudkms.cryptoKeys.get
   - cloudkms.cryptoKeys.list
   - cloudkms.keyRings.get
   - cloudkms.keyRings.list

> **注：**

> 新しいサービスアカウントを作成する際に利用可能なロールの完全なリストを取得するには、すべてのAPIを有効にしてください。

5. **CONTINUE**をクリックします。
6. **このサービスアカウントへのユーザーアクセスを許可**ページで、このサービスアカウントでアクションを実行するアクセス権を付与するために、ユーザーまたはグループを追加します。
7. **DONE**をクリックします。
8. IAMメインコンソールに移動します。
9. 作成されたサービスアカウントを特定します。
10. ロールが正常に割り当てられていることを検証します。

考慮事項:

サービスアカウントを作成する際は、以下を考慮してください。

- **このサービスアカウントにプロジェクトへのアクセスを許可**および**このサービスアカウントへのユーザーアクセスを許可**の手順はオプションです。これらのオプションの構成手順をスキップすることを選択した場合、新しく作成されたサービスアカウントは、**IAMと管理 > IAM**ページに表示されません。
- サービスアカウントに関連付けられたロールを表示するには、オプションの手順をスキップせずにロールを追加します。このプロセスにより、構成されたサービスアカウントにロールが表示されるようになります。

CITRIX CLOUDサービスアカウントキー

Citrix DaaSで接続を作成するには、Citrix Cloudサービスアカウントキーが必要です。キーは資格情報ファイル（.json）に含まれています。キーを作成すると、ファイルは自動的にダウンロードされ、**ダウンロード**フォルダーに保存されます。キーを作成するときは、キーの種類をJSONに設定してください。そうしないと、Web Studioはそれを解析できません。

サービスアカウントキーを作成するには、**IAMと管理 > サービスアカウント**に移動し、Citrix Cloudサービスアカウントのメールアドレスをクリックします。**キー**タブに切り替え、**キーを追加 > 新しいキーを作成**を選択します。キータイプとして**JSON**を選択していることを確認してください。

> **ヒント:**

> Google Cloud コンソールで、**サービスアカウント**ページを使用してキーを作成します。セキュリティ上の理由から、キーを定期的に変更することをお勧めします。既存の Google Cloud 接続を編集することで、Citrix Virtual Apps and Desktops アプリケーションに新しいキーを提供できます。

CITRIX CLOUD サービスアカウントにロールを追加する

Citrix Cloud サービスアカウントにロールを追加するには、次の手順を実行します。

1. Google Cloud コンソールで、**IAM と管理 > IAM** に移動します。
2. **IAM > 権限**ページで、作成したサービスアカウントを電子メールアドレスで特定し、見つけます。

   例: `<my-service-account>@<project-id>.iam.gserviceaccount.com`
3. 鉛筆アイコンを選択して、サービスアカウントのプリンシパルへのアクセスを編集します。
4. 選択したプリンシパルオプションの**「project-id」へのアクセスを編集**ページで、**別のロールを追加**を選択して、必要なロールをサービスアカウントに1つずつ追加し、**保存**を選択します。

CLOUD COMPUTE SERVICE ACCOUNT にロールを追加する

Cloud Compute Service Account にロールを追加するには、次の手順を実行します。

1. Google Cloud コンソールで、**IAM と管理 > IAM** に移動します。
2. **IAM** ページで、**プロジェクト ID** と **compute** という単語で始まるメールアドレスで識別できる Cloud Compute Service Account を見つけます。

   例: `<project-id>-compute@developer.gserviceaccount.com`
3. 鉛筆アイコンを選択して、Cloud Build アカウントのロールを編集します。
4. 選択したプリンシパルオプションの**「"project-id"へのアクセスを編集」ページで、「別のロールを追加」を選択して、必要なロールをCloud Buildサービスアカウントに1つずつ追加し、「保存」**を選択します。

> **注：**
>
> すべてのAPIを有効にして、ロールの完全なリストを取得します。

ストレージの権限とバケット管理

Citrix Virtual Apps and Desktops は、Google Cloud サービス のクラウドビルド失敗のレポートプロセスを改善します。このサービスは Google Cloud 上でビルドを実行します。Citrix Virtual Apps and Desktops は、Google Cloud サービスがビルドログ情報をキャプチャする `citrix-mcs-cloud-build-logs-{region}-{5 random characters}` という名前のストレージバケットを作成します。このバケットには、30日後にコンテンツを削除するオプションが設定されています。このプロセスでは、接続に使用されるサービスアカウントに `storage.buckets.update` に設定された Google Cloud 権限が必要です。サービスアカウントにこの権限がない場合、Citrix Virtual Apps and Desktops はエラーを無視し、カタログ作成プロセスを続行します。この権限がないと、ビルドログのサイズが増加し、手動でのクリーンアップが必要になります。

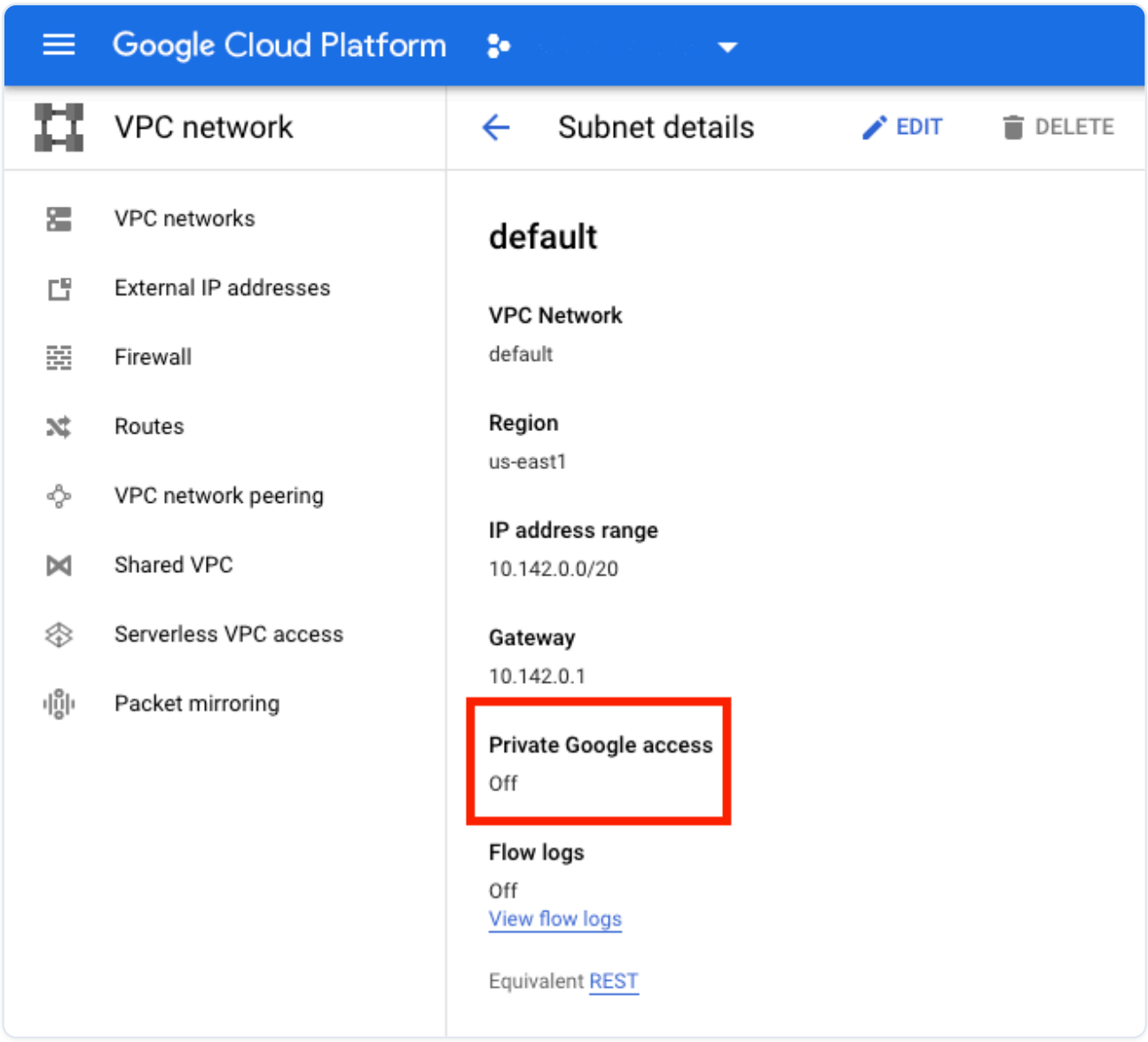
プライベート Google アクセスを有効にする

VM のネットワークインターフェイスに外部 IP アドレスが割り当てられていない場合、パケットは他の内部 IP アドレスの宛先にのみ送信されます。プライベートアクセスを有効にすると、VM は Google API および関連サービスで使用される外部 IP アドレスのセットに接続します。

> **注：**
>
> プライベート Google アクセスが有効になっているかどうかにかかわらず、パブリック IP アドレスを持つ VM と持たない VM の両方が、特にサードパーティのネットワークアプライアンスが環境にインストールされている場合、Google Public API にアクセスできる必要があります。

> MCSプロビジョニングのために、サブネット内のVMがパブリックIPアドレスなしでGoogle APIにアクセスできるようにするには、次の手順を実行します。

1. Google Cloudで、**VPC network configuration**にアクセスします。
2. サブネットの詳細画面で、「**Private Googleアクセス**」をオンにします。



詳細については、「Configuring Private Google Access」を参照してください。

重要:

ネットワークがVMのインターネットアクセスを防止するように構成されている場合、VMが接続されているサブネットに対してPrivate Googleアクセスを有効にすることに関連するリスクを組織が負うことを確認してください。

次のステップ

- コアコンポーネントのインストール
- VDAのインストール
- サイトの作成

- Google Cloud 環境での接続の作成と管理については、「Google Cloud 環境への接続」を参照してください。

詳細情報

- 接続とリソースの作成および管理
- マシンカタログの作成

HPE Moonshot 仮想化環境

Citrix Virtual Apps and Desktops™ は、Citrix が管理する HPE Moonshot プラグインを介して、HPE Moonshot ワークロードを管理します。このプラグインを使用すると、HPE Moonshot シャーシへの接続を作成し、カタログを作成し、カタログ内のマシンの電源を管理できます。

要件

Citrix が管理する HPE Moonshot プラグインを Delivery Controller にインストールします。

> **注：**
>
> - Citrix が管理する HPE Moonshot プラグインと HPE が管理する HPE Moonshot プラグインの両方がインストールされている場合、Delivery Controller は Citrix が管理する HPE Moonshot プラグインを使用します。
> - Citrix が管理する HPE Moonshot プラグインと HPE が管理する HPE Moonshot プラグインの両方がインストールされており、HPE が管理する Moonshot プラグインを使用したい場合は、Citrix が管理する HPE Moonshot プラグインをアンインストールし、`RegisterPlugin` キャッシュを更新してください。

Citrix が管理する HPE Moonshot プラグインをインストールする

Citrix が管理する HPE Moonshot プラグインをインストールするには、次の手順を実行します。

1. `E:\x64\Citrix Desktop Delivery Controller\MoonshotPlugin`.msi をインストールします。`E:\` は ISO です。
2. PowerShell を管理者として開き、次のコマンドを実行します。

```
C:\Program Files\Common Files\Citrix\HCLPlugins> .\RegisterPlugins.exe
-pluginsroot .\CitrixMachineCreation\v1.0.0.0\
```

3. プラグインの登録が成功したら、**タスクマネージャー**から次のサービスを再起動します。
    a. CitrixBrokerService
    b. CitrixHostService
    c. CitrixMachineCreationService
4. `Get-HypHypervisorPlugins` を実行して、プラグインが Delivery Controller にインストールされているか確認します。出力の **DisplayName** フィールドには **HPE Moonshot** と表示されている必要があります。

Citrix が管理する HPE Moonshot プラグインをアンインストールし、RegisterPlugin キャッシュを更新する

Citrix が管理する HPE Moonshot プラグインと HPE が管理する HPE Moonshot プラグインの両方がインストールされており、HPE が管理する Moonshot プラグインを使用したい場合は、Citrix が管理する HPE Moonshot プラグインをアンインストールし、`RegisterPlugin` キャッシュを更新する必要があります。そのためには：

1. Citrix が管理する HPE Moonshot プラグインをアンインストールします。
2. PowerShell を管理者として開き、次のコマンドを実行します。

```
cd `C:\Program Files\Common Files\Citrix\HCLPlugins\`

C:\Program Files\Common Files\Citrix\HCLPlugins> .\RegisterPlugins.exe
-PluginsRoot ` C:\Program Files\Common
Files\Citrix\HCLPlugins\ManagedMachine\v2.5.0.0\`
```

3. プラグインの登録が成功したら、**タスクマネージャー**から次のサービスを再起動します。
    a. CitrixBrokerService
    b. CitrixHostService
    c. CitrixMachineCreationService
4. `Get-HypHypervisorPlugins` を実行して、プラグインが Delivery Controller にインストールされているか確認します。出力の **DisplayName** フィールドには **HPE Moonshot Machine Manager** と表示されている必要があります。

主な手順

1. HPE 環境をセットアップします。
2. HPE Moonshot シャーシへの接続を作成します。

3. マシンカタログを作成します。

> **注：**
>
> カタログを作成する前に、1 つ以上の HPE Moonshot カートリッジノードがあることを確認し、それらのノードに VDA をインストールしてください。HPE Moonshot シャーシをハイパーバイザー、カートリッジノードを VM と考えることができます。

4. デリバリーグループを作成します。
5. 管理されていない残りの HPE Moonshot ノードを、管理対象のカタログまたはデリバリーグループに移行します。

次のステップ

- コアコンポーネントのインストール
- VDAのインストール
- サイトの作成
- HPE Moonshotで接続を作成および管理する方法については、「HPE Moonshotへの接続」を参照してください。

詳細情報

- 接続とリソースの作成および管理
- マシンカタログの作成

Microsoft Azure Resource Manager クラウド環境

Citrix Virtual Apps and Desktops™ 展開で Microsoft Azure Resource Manager を使用して仮想マシンをプロビジョニングする場合、以下について理解しておいてください。

- アジュール アクティブ ディレクトリ: `<https://docs.microsoft.com/en-in/azure/active-directory/fundamentals/active-directory-whatis/>`
- 同意フレームワーク: `<https://docs.microsoft.com/ja-jp/azure/active-directory/manage-apps/plan-an-application-integration>`
- サービスプリンシパル: `<https://docs.microsoft.com/ja-jp/azure/active-directory/develop/app-objects-and-service-principals/>`

Microsoft Azure Resource Manager をセットアップするには、インストール準備 を参照してください。

次のステップ

- コアコンポーネントのインストール
- VDAのインストール
- サイトの作成
- Azure 環境で接続を作成および管理するには、Microsoft Azure への接続 を参照してください

詳細情報

- 接続とリソースの作成および管理
- マシンカタログの作成
- CTX219211: Microsoft Azure Active Directory アカウントを設定する
- CTX219243: Azure サブスクリプションへの XenApp および XenDesktop アクセスを許可する
- CTX219271: サイト間 VPN を使用してハイブリッドクラウドを展開する

マイクロソフト システムセンター コンフィギュレーションマネージャー 環境

アプリケーションとデスクトップへのアクセスを管理するために Microsoft System Center Configuration Manager (Configuration Manager) を使用しているサイトは、以下のオプションを使用してその利用を Citrix Virtual Apps and Desktops™ に拡張できます。

- SCCM を使用した VDA のインストール。
- **Configuration Manager Wake Proxy 機能:** Remote PC Access の Wake on LAN 機能は Configuration Manager でサポートされています。詳細については、「Wake on LAN - SCCM 統合」を参照してください。
- **Citrix Virtual Apps and Desktops のプロパティ:** プロパティ を使用すると、Configuration Manager を介して管理する Citrix Virtual Desktops™ を識別できます。（一部のバージョンでは、Configuration Manager は Citrix Virtual Apps and Desktops の旧名である XenApp および XenDesktop を使用します。）

プロパティ

仮想デスクトップを管理するために、Microsoft System Center Configuration Manager でプロパティを利用できます。

Configuration Manager に表示されるブール型プロパティは、true または false ではなく、`1` または `0` として表示されます。

これらのプロパティは、`Root\Citrix\DesktopInformation` 名前空間の `Citrix_virtualDesktopInfo` クラスで利用できます。プロパティ名は Windows Management Instrumentation (WMI) プロバイダーから取得されます。

プロパティ	説明
`AssignmentType`	IsAssigned の値を設定します。有効な値は、`ClientIP`、`ClientName`、`None`、および `User` です (`IsAssigned` を `True` に設定します)。
`BrokerSiteName`	`HostIdentifier` と同じ値を返します。
`DesktopCatalogName`	デスクトップに関連付けられているマシンカタログ。
`DesktopGroupName`	デスクトップに関連付けられているデリバリーグループ。
`HostIdentifier`	`BrokerSiteName` と同じ値を返します。
`IsAssigned`	デスクトップをユーザーに割り当てるには `True`、ランダムなデスクトップの場合は `False` に設定します。
`IsMasterImage`	環境に関する決定を可能にします。たとえば、プロビジョニングされたマシンではなく、イメージにアプリケーションをインストールします。有効な値は次のとおりです。イメージとして使用されるVMでは `True`。この値は、インストール時に選択に基づいて設定されるか、そのイメージからプロビジョニングされたVMではクリアされます。
`IsVirtualMachine`	仮想マシンの場合は `True`、物理マシンの場合は `false`。
`OSChangesPersist`	デスクトップオペレーティングシステムイメージが再起動のたびにクリーンな状態にリ

プロパティ	説明
	セットされる場合は `False`。それ以外の場合は `true`。
`PersistentDataLocation`	Configuration Manager が永続データを保存する場所。これはユーザーにはアクセスできません。
`BrokerSiteName`、`DesktopCatalogName`、`DesktopGroupName`、`HostIdentifier`	デスクトップがControllerに登録されるときに決定されます。完全に登録されていないデスクトップの場合はnullです。

プロパティを収集するには、Configuration Manager でハードウェアインベントリを実行します。プロパティを表示するには、Configuration Manager Resource Explorer を使用します。これらの場合、名前にはスペースが含まれるか、プロパティ名とわずかに異なります。たとえば、`BrokerSiteName` は `Broker Site Name` として表示されます。

- Citrix VDA から Citrix WMI プロパティを収集するように Configuration Manager を構成する
- Citrix WMI プロパティを使用してクエリベースのデバイスコレクションを作成する
- Citrix WMI プロパティに基づいてグローバル条件を作成する
- グローバル条件を使用してアプリケーション展開タイプの要件を定義する

`Root\ccm_vdi` 名前空間の Microsoft クラス `CCM_DesktopMachine` で Microsoft プロパティを使用することもできます。詳細については、Microsoft のドキュメントを参照してください。

Microsoft System Center 仮想マシンマネージャー仮想化環境

Hyper-V と Microsoft System Center Virtual Machine Manager (VMM) を使用して仮想マシンを提供する場合は、このガイダンスに従ってください。

このリリースでは、システム要件に記載されているVMMバージョンがサポートされています。

> **注：**
>
> 混在するHyper-Vクラスター（異なるHyper-Vバージョンを実行しているサーバーを含む）はサポートされていません。

> Citrix Provisioning（旧Provisioning Services）およびMachine Creation Services™を使用して、以下をプロビジョニングできます。

- 第1世代でサポートされているデスクトップまたはサーバーOSのVM。
- セキュアブートのサポートを含む、第2世代でサポートされているデスクトップまたはサーバーOSのVM。

ハイパーバイザーのインストールと構成

> **重要:**
>
> すべてのDelivery Controllerは、VMMサーバーと同じフォレスト内にある必要があります。

1. サーバーにMicrosoft Hyper-VサーバーとVMMをインストールします。
2. すべてのControllerにSystem Center Virtual Machine Managerコンソールをインストールします。コンソールのバージョンは管理サーバーのバージョンと一致している必要があります。以前のコンソールでも管理サーバーに接続できますが、バージョンが異なる場合、VDAのプロビジョニングは失敗します。
3. 次のアカウント情報を確認してください。

   Studioでホストを指定するために使用するアカウントは、関連するHyper-Vマシンに対するVMM管理者またはVMM委任管理者である必要があります。このアカウントがVMMで委任管理者ロールのみを持っている場合、ホスト作成プロセス中にStudioにストレージデータが表示されません。

   Studio統合に使用されるユーザーアカウントは、各Hyper-Vサーバーのadministratorsローカルセキュリティグループのメンバーである必要もあります。この構成は、VMの作成、更新、削除などのVMライフサイクル管理をサポートします。

   Hyper-Vを実行しているサーバーにControllerをインストールすることはサポートされていません。

単一のSCVMMが異なるデータセンター内の複数のクラスターを管理する大規模な展開では、委任管理者のホストグループのスコープを制限できます。

ホストグループのスコープを制限するには、Microsoft System Center Virtual Machine Manager (VMM) コンソールで委任管理者ロールを使用します。

1. **ユーザーロールの作成ウィザード**で、ユーザーロールとしてFabric Administrator (Delegated Administrator) を選択します。
2. **メンバー**で、委任管理者として使用する Active Directory のユーザーアカウントを追加します。
3. 「**スコープ**」で、委任された管理者がアクセスできるようにするホストグループを選択します。
4. 委任された管理者ユーザーの資格情報を使用して、新しい**実行アカウント**を作成します。これらの資格情報を使用して、後でハイパーバイザー接続を作成します。メインの管理者ロールアカウントは使用しないでください。

詳細情報

- 接続とリソースの作成および管理
- マシンカタログの作成

Nutanix仮想化環境

Citrix Virtual Apps and Desktops™展開でNutanix Acropolisを使用して仮想マシンを提供する場合は、このガイダンスに従ってください。セットアッププロセスには、次のタスクが含まれます。

- Citrix Virtual Apps and Desktops環境にNutanixプラグインをインストールして登録します。
- Nutanix Acropolisハイパーバイザーへの接続を作成します。
- Nutanixハイパーバイザーで作成したマスターイメージのスナップショットを使用するマシンカタログを作成します。

詳細については、Nutanix Support Portalで入手できるNutanix Acropolis MCSプラグインインストールガイドを参照してください。

Nutanixプラグインのインストールと登録

すべてのDelivery ControllerにNutanixプラグインをインストールして登録するには、次の手順を完了します。Citrix Studioを使用してNutanixへの接続を作成します。次に、Nutanix環境で作成したマスターイメージのスナップショットを使用するマシンカタログを作成します。

> **ヒント:**

> Nutanixプラグインをインストールまたは更新する際は、Citrix Host Service、Citrix Broker Service、およびMachine Creation Services™を停止してから再起動することをお勧めします。

Nutanixプラグインのインストールについては、Nutanix Documentation siteを参照してください。

次のステップ

- コアコンポーネントのインストール
- VDAのインストール
- サイトの作成
- Nutanix 環境での接続の作成と管理については、Nutanix への接続 を参照してください。

詳細情報

- 接続とリソースの作成と管理
- マシンカタログの作成

Nutanix クラウドおよびパートナーソリューション

Citrix Virtual Apps and Desktops™ は、以下の Nutanix クラウドおよびパートナーソリューションをサポートしています。

- AWS 上のニュータニックス クラウドクラスター

AWS 上のニュータニックス クラウドクラスター

Citrix Virtual Apps and Desktops は、AWS 上の Nutanix Cloud Clusters をサポートしています。Nutanix クラスターは、プライベートクラウドまたは複数のパブリッククラウドでアプリケーションを実行する方法を簡素化します。AWS 上の Nutanix Cloud Clusters の詳細については、「Nutanix Cloud Clusters on AWS Deployment and User Guide」を参照してください。

ヒント:

このサポートは、Nutanix オンプレミス クラスターと同じ機能を提供します。サポートされるクラスターは、*Prism Element* のみです。詳細については、こちら を参照してください。

要件

AWS で Nutanix クラスターを使用するには、以下が必要です。

- Nutanix アカウント。

- 次の権限を持つ AWS アカウント:
  - IAMFullAccess
  - AWSConfigRole
  - AWSCloudFormationFullAccess

Nutanix クラスターを作成する

Nutanix クラスターを作成するには：

1. Nutanix アカウントにログインします。
2. **Nutanix cluster** オプションを見つけて、**Launch** をクリックします。**Nutanix Console** が開きます。詳細については、「Get Started with Nutanix Cluster on AWS」を参照してください。
3. **新しい VPC** を作成することを選択します。

クラスター作成プロセスは、次のエラーで失敗する可能性があります。

- クラスターは指定された時間内に作成できませんでした。クラスターを削除しています。
- ホスト Nutanix クラスター - ノード `XXXXXXXXXX: Instance i-xxxxxxxxxxxxx: disable network interface source/dest check error.`.
- ホスト Nutanix クラスター - ノード `XXXXXXXXXX: Unable to obtain instance i-xxxxxxxxxxxxx network interface info.`.

クラスターの作成に失敗した場合：

- 別のリージョンで再作成してみてください。
- 再試行する前に、Nutanix CloudFormation Stack (CFS) を削除してください。

他のリソースに加えて、Nutanix CFS は以下を作成します。

- *Nutanix Cluster xxxxxxxxxxxx* 10.0.0.0/16 という名前の VPC 1 つ
- 2つのサブネット 10.0.128.0/24 および 10.0.129.0/24
- 1つのインターネットゲートウェイ
- 1つのNATゲートウェイ

クラスターが作成されたら、**Nutanix Prism**のアドレスを取得します。

1. **Nutanix Console**に移動します。
2. コンソールの右上隅で、**Launch Prism Element** リンクにマウスオーバーし、URLをコピーします。

次のステップ

- コアコンポーネントのインストール
- VDAのインストール
- サイトの作成
- Nutanixクラウドおよびパートナーソリューションの接続を作成および管理するには、「Nutanixクラウドおよびパートナーソリューションへの接続」を参照してください。

詳細情報

- 接続とリソースの作成および管理
- マシンカタログの作成

VMware 仮想化環境

仮想マシンを提供するのにVMwareを使用する場合は、このガイダンスに従ってください。

vCenter Serverと適切な管理ツールをインストールします。(vSphere vCenter Linked Mode操作はサポートされていません。)

MCSを使用する予定がある場合は、vCenter ServerのDatastore Browser機能（`<https://kb.vmware.com/s/article/2101567>`で説明）を無効にしないでください。この機能を無効にすると、MCSは正しく動作しません。

次のステップ

- コアコンポーネントのインストール
- VDAのインストール
- サイトの作成
- VMware環境での接続の作成と管理については、「Connection to VMware」を参照してください。

詳細情報

- 接続とリソースの作成および管理
- マシンカタログの作成

VMware クラウドおよびパートナーソリューション

Citrix Virtual Apps and Desktops™ は、以下の VMware クラウドおよびパートナーソリューションをサポートしています。

- Azure VMware ソリューション (AVS)(#azure-vmware-solution-avs-integration)
- Google Cloud VMware エンジン(#google-cloud-vmware-engine)
- VMware クラウド オン Amazon Web Services (AWS)(#vmware-cloud-on-amazon-web-services-aws)

Azure VMware ソリューション (AVS) の統合

Citrix Virtual Apps and Desktop サービスは AVS をサポートしています。AVS は、Azure インフラストラクチャによって作成された vSphere クラスターを含むクラウドインフラストラクチャを提供します。Citrix Virtual Apps and Desktop サービスを活用して、オンプレミス環境で vSphere を使用する場合と同じ方法で、AVS を使用して VDA ワークロードをプロビジョニングします。

AVS クラスターのセットアップ

Citrix Virtual Apps™ and Desktop サービスで AVS を使用できるようにするには、Azure で次の手順を実行します。

- ホストクォータを要求する
- Microsoft.AVS リソース プロバイダーを登録する
- ネットワークチェックリスト
- Azure VMware Solution プライベートクラウドを作成する
- Azure VMware Solution プライベートクラウドにアクセスする
- AzureでVMwareプライベートクラウドのネットワークを構成する
- Azure VMware Solution の DHCP を構成する
- Azure VMware Solution にネットワークセグメントを追加する
- Azure VMware Solution 環境を確認する

AZURE ENTERPRISE AGREEMENTのお客様のホストクォータを要求する

Azureポータルの**ヘルプとサポート**ページで、**新しいサポートリクエスト**を選択し、次の情報を含めます。

- 問題の種類: 技術
- サブスクリプション: サブスクリプションを選択してください
- サービス: すべてのサービス > Azure VMware Solution
- リソース: 一般的な質問
- 概要: 容量が必要
- 問題の種類: 容量管理の問題

- 問題のサブタイプ: 追加のホストクォータ/容量に関する顧客からの要求

サポートチケットの に、 タブで次の情報を含めます。

- POC または本番環境
- リージョン名
- ホスト数
- その他の詳細

> **注：**
>
> AVS には最低 3 つのホストが必要であり、N+1 ホストの冗長性を使用することをお勧めします。

> サポート チケットの詳細を指定したら、 を選択して Azure にリクエストを送信します。

MICROSOFT.AVS リソース プロバイダーを登録する

ホスト クォータを要求した後、リソース プロバイダーを登録します。

1. Azure portal にサインインします。
2. Azure portal メニューで、 を選択します。
3. メニューで、サブスクリプションを入力し、 を選択します。
4. サブスクリプション リストからサブスクリプションを選択します。
5. を選択し、検索バーに **Microsoft.AVS** と入力します。
6. リソース プロバイダーが登録されていない場合は、 を選択します。

ネットワークに関する考慮事項

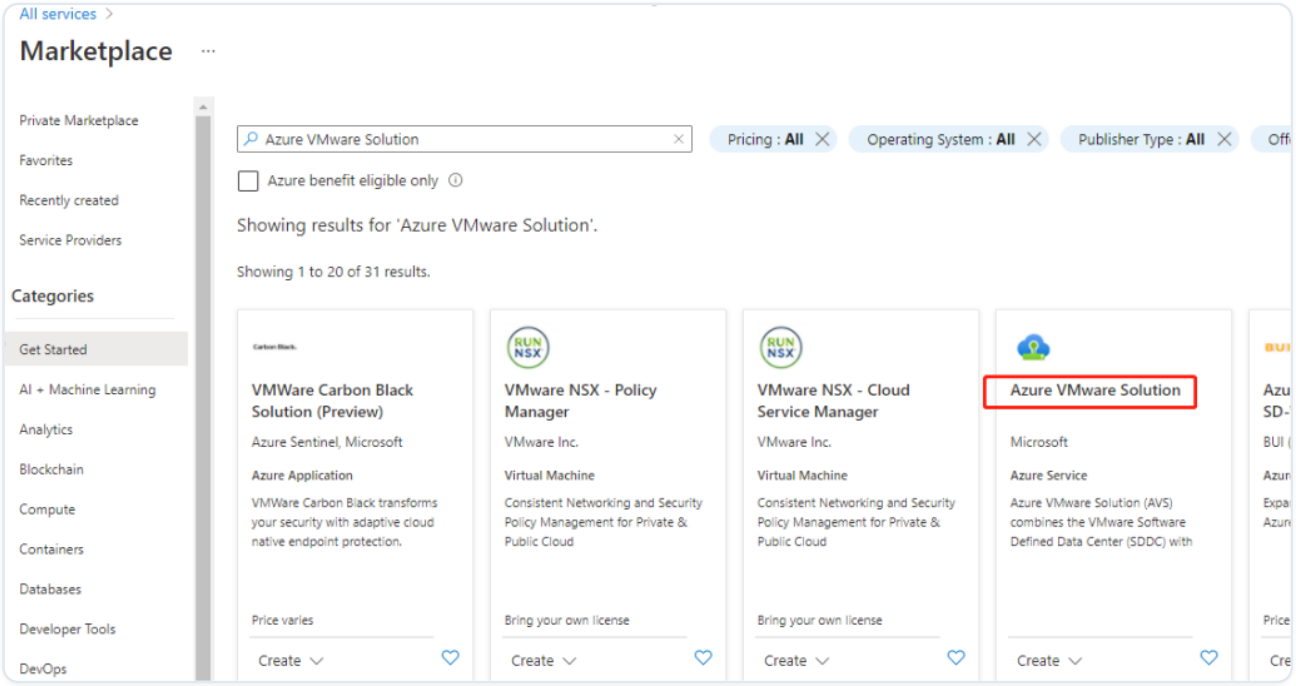
AVSは、特定のネットワークアドレス範囲とファイアウォールポートを必要とするネットワークサービスを提供します。詳細については、Azure VMware Solution のネットワーク計画チェックリストを参照してください。

AZURE VMWARE SOLUTION プライベートクラウドを作成する

環境のネットワーク要件を考慮した後、AVS プライベートクラウドを作成します。

1. Azureポータルにサインインします。
2. **新しいリソースの作成**を選択します。

3. **Marketplace の検索**テキストボックスに、*Azure VMware Solution*と入力し、リストから**Azure VMware Solution**を選択します。



image

Azure VMware Solutionウィンドウで、:

1. **作成**を選択します。
2. タブをクリックします。
3. 以下の表の情報を使用して、フィールドに値を入力します。

フィールド	値
サブスクリプション	展開に使用するサブスクリプションを選択します。Azure サブスクリプション内のすべてのリソースはまとめて請求されます。
リソースグループ	プライベートクラウドのリソースグループを選択します。Azure リソースグループは、Azure リソースがデプロイおよび管理される論理コンテナです。または、プライベートクラウド用に新しいリソースグループを作成することもできます。
場所	east us などの場所を選択します。これは、計画フェーズで定義したリージョンです。

フィールド	値
リソース名	Azure VMware Solution プライベートクラウドの名前を指定します。
SKU	AV36 を選択します。
ホスト	プライベートクラウドクラスターに割り当てられたホストの数を示します。デフォルト値は3で、デプロイ後に増減できます。
アドレスブロック	プライベートクラウドの IP アドレスブロックを指定します。CIDR はプライベートクラウド管理ネットワークを表し、vCenter Server や NSX-T Manager などのクラスター管理サービスに使用されます。/22 アドレス空間を使用します（例: 10.175.0.0/22）。アドレスは一意であり、他の Azure 仮想ネットワークやオンプレミスネットワークと重複しないようにしてください。
仮想ネットワーク	Azure VMware Solution ExpressRoute 回線は展開後の手順で確立されるため、ここは空白のままにします。

プライベートクラウドの作成画面で：

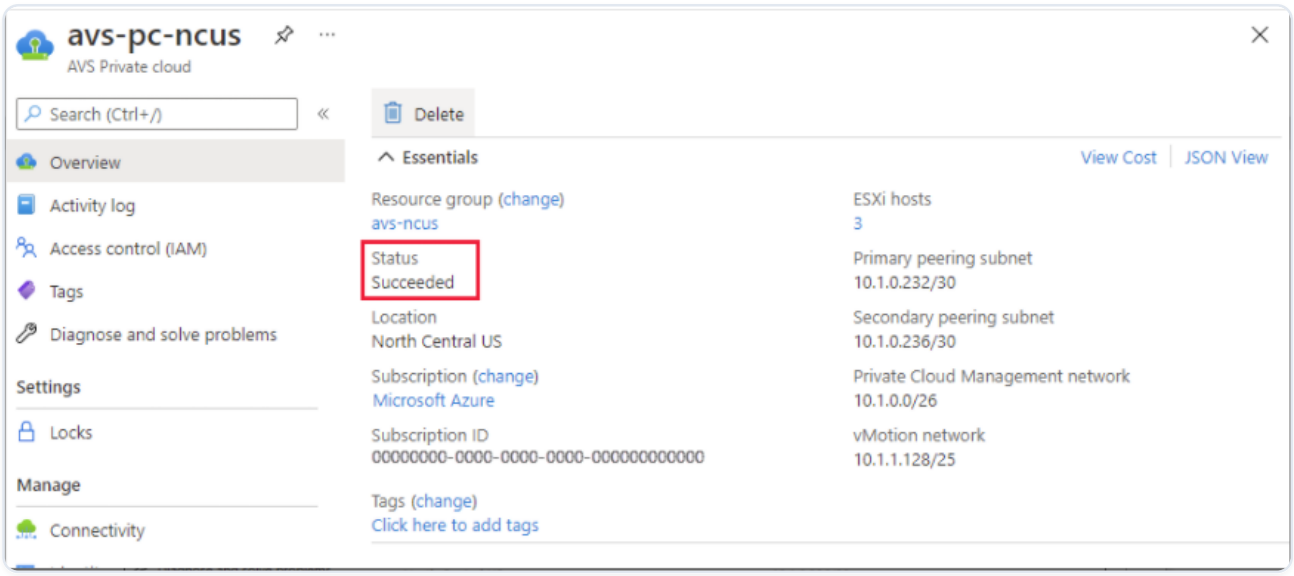
1. フィールドで、AVS が存在するリージョンを選択します。リソースグループのリージョンは AVS リージョンと同じです。
2. フィールドで、 を選択します。
3. 「**アドレスブロック**」フィールドにIPアドレスを指定します。例: 10.15.0.0/22。
4. 「**確認 + 作成**」を選択します。
5. 情報を確認したら、「**作成**」をクリックします。

Azure ASV プライベートクラウドの作成(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/azure-avs-create-private-cloud.png)

> **ヒント:**

> プライベートクラウドの作成には3〜4時間かかる場合があります。クラスターに単一のホストを追加するには30〜45分かかる場合があります。

> 展開が成功したことを確認します。作成したリソースグループに移動し、プライベートクラウドを選択します。**ステータス**が**成功**になったら、展開は完了です。



AZURE VMWARE SOLUTION プライベートクラウドへのアクセス

プライベートクラウドを作成したら、Windows VMを作成し、プライベートクラウドのローカルvCenterに接続します。
新しいWindows仮想マシンの作成

1. リソースグループで、**+ 追加**を選択し、**Microsoft Windows 10/2016/2019**を検索して選択します。
2. **Create** をクリックします。
3. 必要な情報を入力し、「**確認 + 作成**」を選択します。
4. 検証が完了したら、「**作成**」を選択して仮想マシンの作成プロセスを開始します。

プライベートクラウドのローカルvCenterに接続する

1. クラウド管理者として **vSphere Client with VMware vCenter SSO** にサインインします。

   Azure ASV vSphere ログイン(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/azure-avs-vsphere-login.png)

2. Azure portal でプライベートクラウドを選択し、 **>** を選択します。

プライベートクラウドのvCenterおよびNSX-T ManagerのURLとユーザー資格情報が表示されます。

Azure ASV セットアップ vCenter(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/azure-avs-setup-vcenter.png)

URLとユーザー資格情報を確認した後:

1. 前の手順で作成したVMに移動し、仮想マシンに接続します。
2. Windows VMでブラウザを開き、vCenterとNSX-T ManagerのURLを2つのブラウザタブで開きます。vCenterタブで、前の手順で取得した*cloudadmin@vmcp.local*ユーザーの資格情報を入力します。

AZUREでVMWAREプライベートクラウドのネットワークを構成する

ASVプライベートクラウドにアクセスした後、仮想ネットワークとゲートウェイを作成してネットワークを構成します。
仮想ネットワークを作成する

1. Azure portal にサインインします。
2. 以前に作成したリソースグループに移動します。
3. 新しいリソースを定義するには、 を選択します。
4. テキストボックスに「*仮想ネットワーク*」と入力します。仮想ネットワークリソースを見つけて選択します。
5. 「**仮想ネットワーク**」ページで、「**作成**」を選択してプライベートクラウドの仮想ネットワークを設定します。
6. 「**仮想ネットワークの作成**」ページで、仮想ネットワークの詳細を入力します。
7. 「**基本**」タブで、仮想ネットワークの名前を入力し、適切なリージョンを選択して、「**次へ：IPアドレス**」をクリックします。
8. 「**IPアドレス**」タブのIPv4アドレス空間で、以前に作成したアドレスを入力します。

> **重要:**
>
> プライベートクラウドを作成したときに使用したアドレス空間と重複しないアドレスを使用してください。

> アドレス空間を入力した後:

1. 「**+ サブネットの追加**」を選択します。
2. 「**サブネットの追加**」ページで、サブネットに名前と適切なアドレス範囲を割り当てます。

3. 「**追加**」をクリックします。
4. 「**確認 + 作成**」を選択します。
5. 情報を確認し、「**作成**」をクリックします。デプロイが完了すると、仮想ネットワークがリソースグループに表示されます。

仮想ネットワークゲートウェイを作成する
仮想ネットワークを作成した後、仮想ネットワークゲートウェイを作成します。

1. リソースグループで、「**+ 追加**」を選択して新しいリソースを追加します。
2. 「**Search the Marketplace**」テキストボックスに「*virtual network gateway*」と入力します。仮想ネットワークリソースを見つけて選択します。
3. 「**Virtual Network gateway**」ページで、「**Create**」をクリックします。
4. 「**Create virtual network gateway**」ページの「**Basics**」タブで、フィールドに値を入力します。
5. 「**Review + create**」をクリックします。

Azure ASV セットアップ vCenter(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/azure-avs-create-virtual-gateway.png)

仮想ネットワークゲートウェイの構成を確認したら、**作成**をクリックして仮想ネットワークゲートウェイを展開します。 展開が完了したら、**ExpressRoute**接続をAzure AVSプライベートクラウドを含む仮想ネットワークゲートウェイに接続します。

EXPRESSROUTEを仮想ネットワークゲートウェイに接続する

仮想ネットワークゲートウェイを展開した後、それとAzure AVSプライベートクラウドの間に接続を追加します。

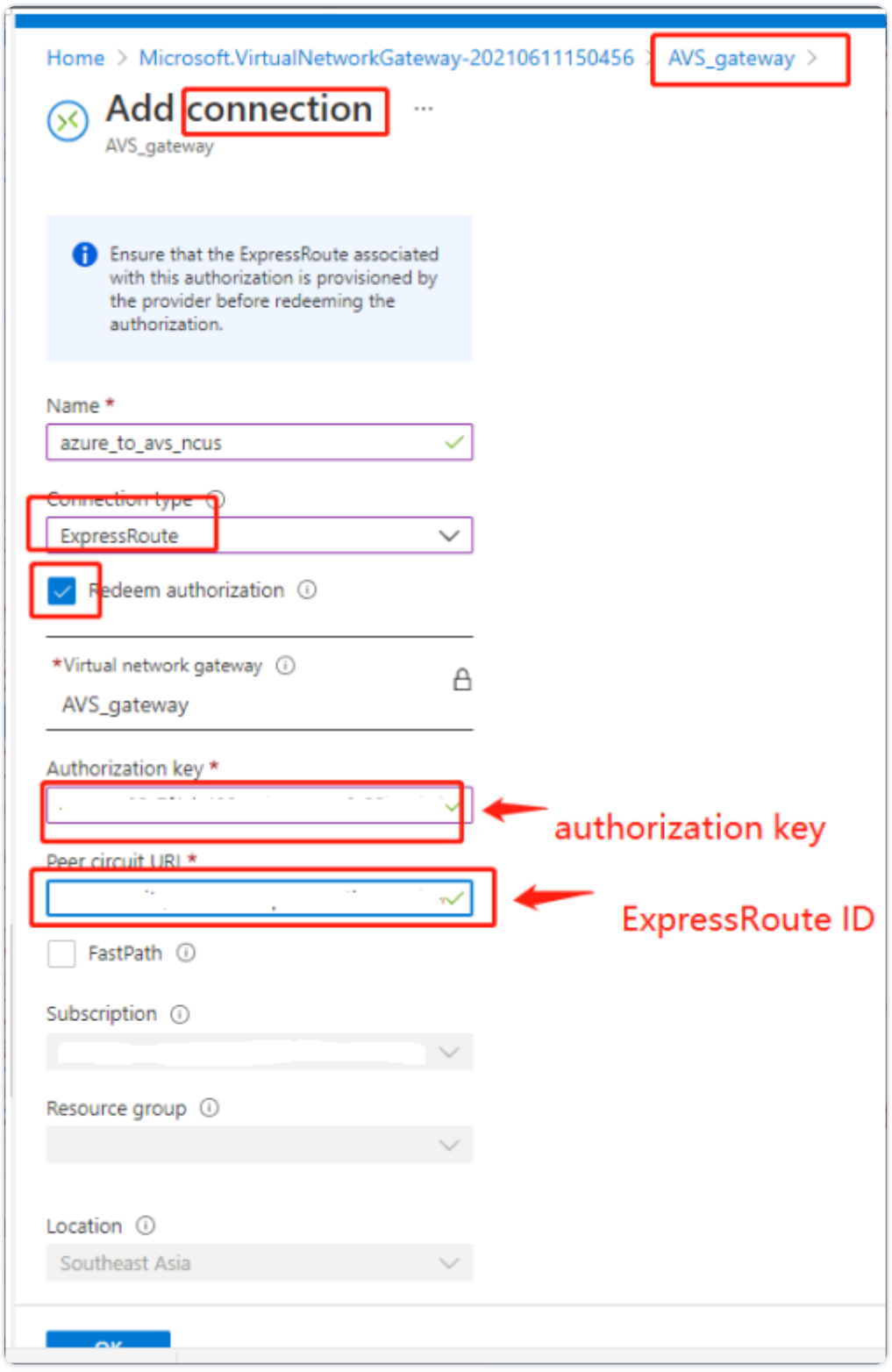
1. ExpressRoute承認キーを要求します。
2. Azureポータルで、**Azure VMware Solution private cloud**に移動します。「**Manage> Connectivity > ExpressRoute**」を選択し、次に「**+ Request an authorization key**」を選択します。

Azure ASV 承認キーの要求(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/azure-avs-expressroute.png)

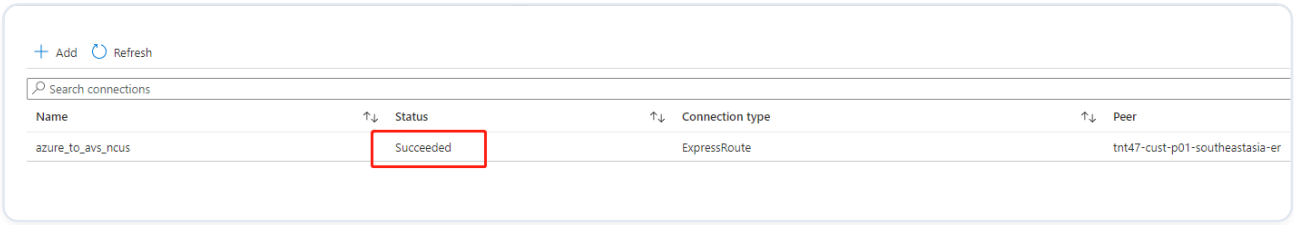
承認キーを要求した後：

1. キーの名前を入力し、「**Create**」をクリックします。キーの作成には約30秒かかる場合があります。作成されると、新しいキーはプライベートクラウドの承認キーのリストに表示されます。

2. **承認キー**と**ExpressRoute ID**をコピーします。これらはピアリングプロセスを完了するために必要です。承認キーはしばらくすると消えるため、表示されたらすぐにコピーしてください。
3. 使用する**仮想ネットワークゲートウェイ**に移動し、「**Connections> + Add**」を選択します。
4. 「**接続の追加**」ページで、フィールドの値を入力し、「**OK**」を選択します。



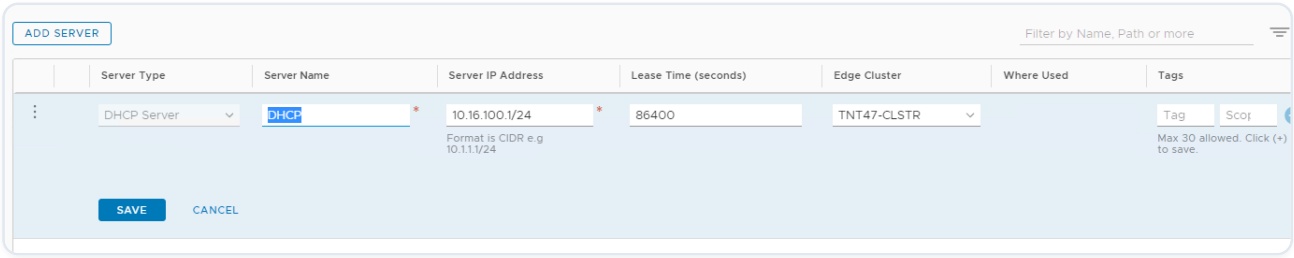
ExpressRoute回線と仮想ネットワーク間の接続が確立されます。



AZURE VMWARE SOLUTION の DHCP を構成する

ExpressRouteを仮想ゲートウェイに接続した後、DHCPを構成します。
NSX-T を使用して DHCP サーバーをホストする
NSX-T Manager で、次の手順を実行します。

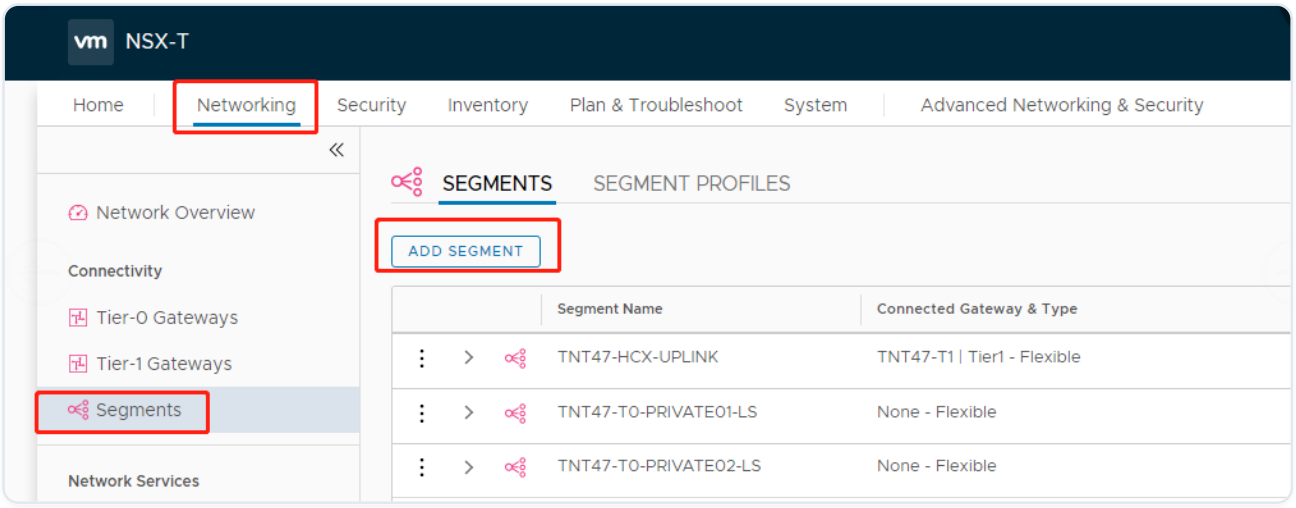
1. **「ネットワーク」>「DHCP」**の順に選択し、**「サーバーの追加」**を選択します。
2. **「サーバーの種類」で「DHCP」**を選択し、サーバー名とIPアドレスを入力します。
3. 「**保存**」をクリックします。
4. **「Tier 1 ゲートウェイ」を選択し、Tier-1 ゲートウェイの縦の省略記号を選択して、「編集」**を選択します。
5. サブネットを追加するには、**「IP割り当てなし」**を選択します。
6. **「種類」で「DHCPローカルサーバー」**を選択します。
7. **「DHCPサーバー」で「Default DHCP」を選択し、「保存」**をクリックします。
8. もう一度**Save**をクリックし、**Close Editing**を選択します。



AZURE VMWARE SOLUTIONでネットワークセグメントを追加する

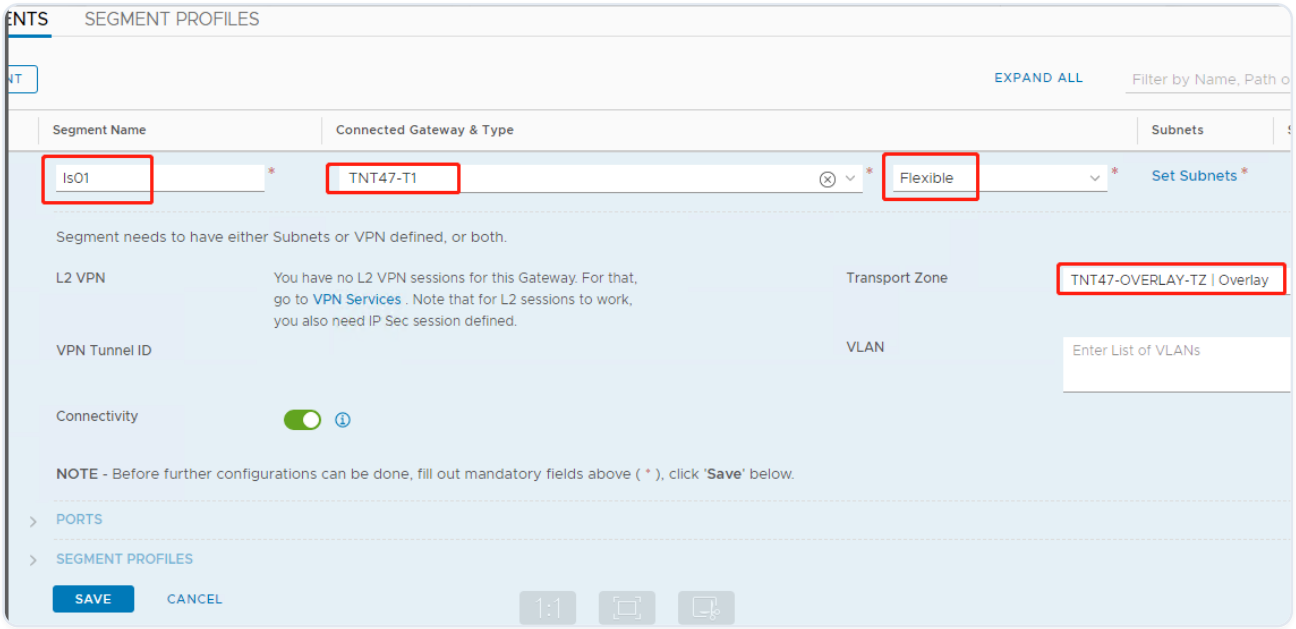
DHCPを設定した後、ネットワークセグメントを追加します。

ネットワークセグメントを追加するには、NSX-T Managerで**Networking> Segments**を選択し、**Add Segment**をクリックします。



Segments profile画面で：

1. セグメントの**name**を入力します。
2. **Tier-1 Gateway (TNTxx-T1)**を**Connected Gateway**として選択し、**Type**は**Flexible**のままにします。
3. 事前設定されたオーバーレイ**Transport Zone(TNTxx-OVERLAY-TZ)**を選択します。
4. **Set Subnets**をクリックします。



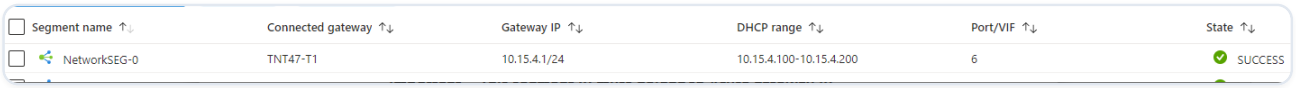
Subnetsセクションで：

1. ゲートウェイIPアドレスを入力します。
2. **Add**を選択します。

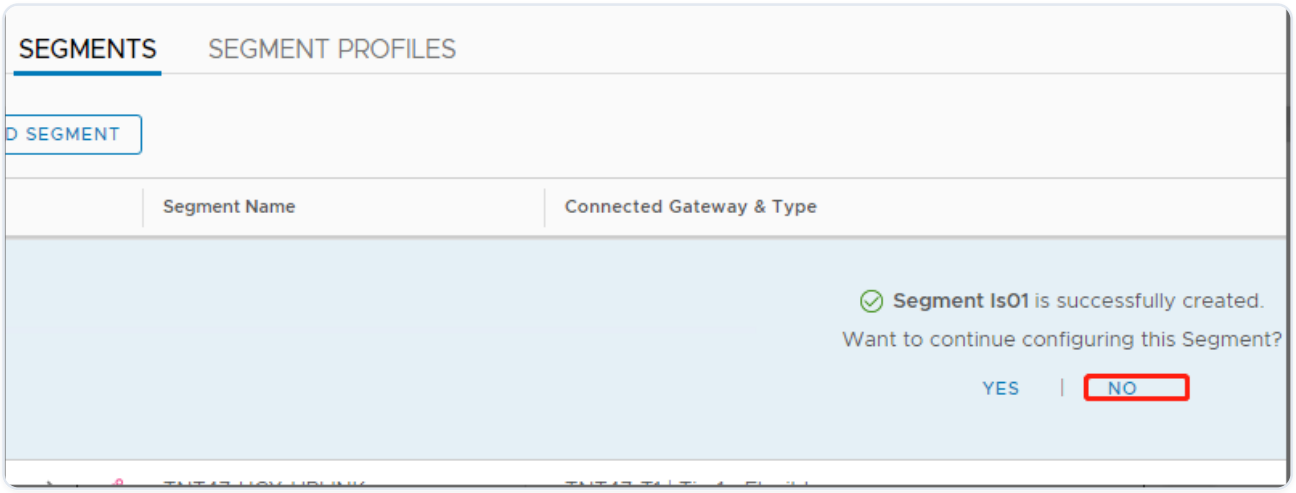
> **重要:**

> このセグメントのIPアドレスは、Azureゲートウェイの IPアドレス (10.15.0.0/22) に属している必要があります。

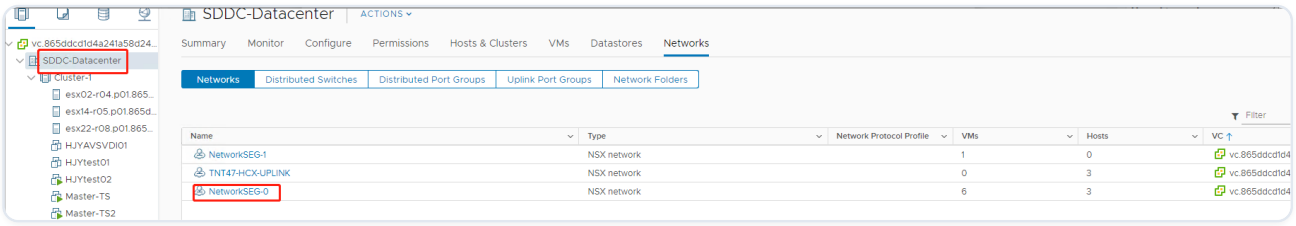
> DHCP範囲はセグメントIPアドレスに属している必要があります。



セグメントの構成を続行するオプションを拒否するには、 を選択します:

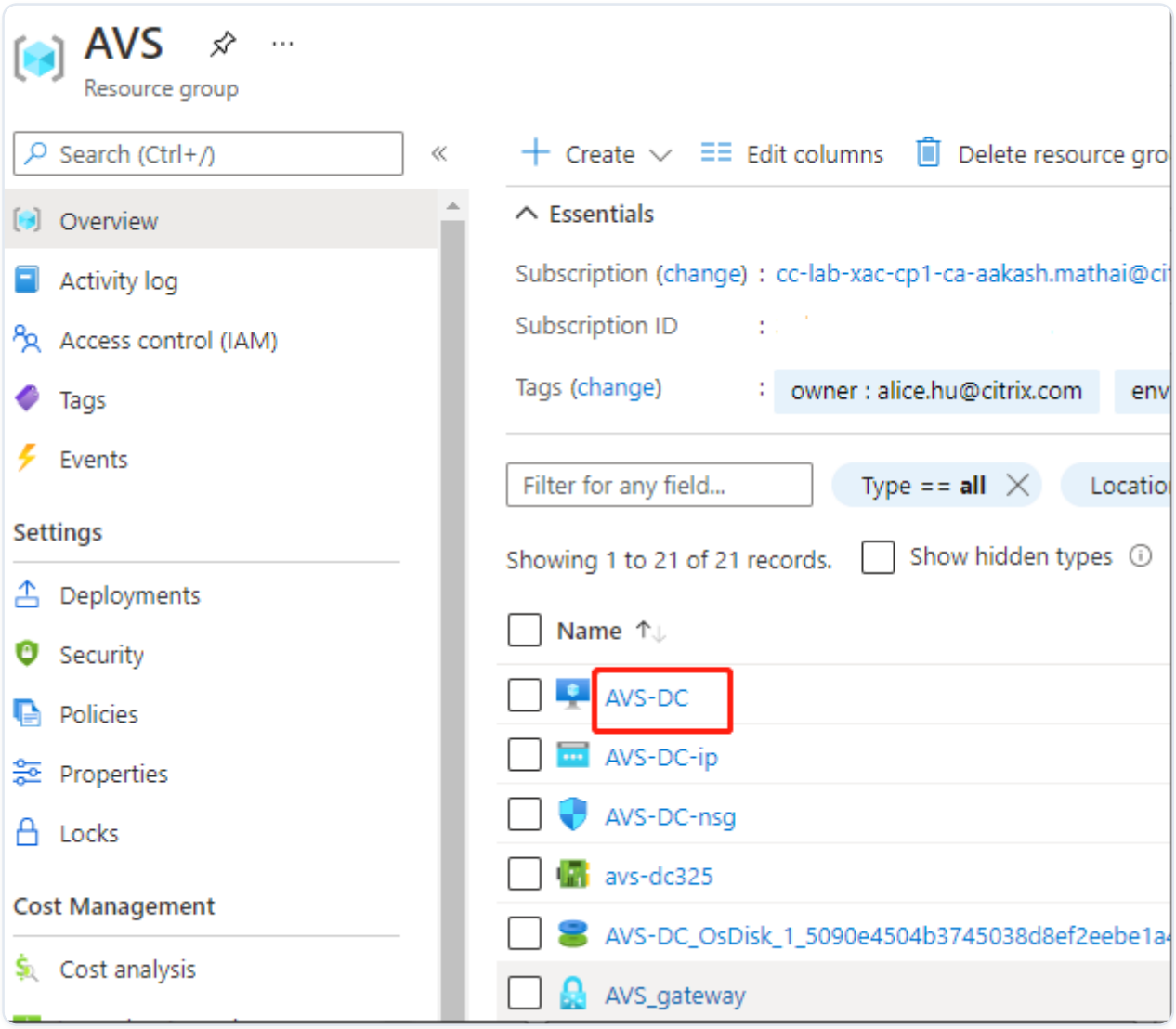


vCenterで、 > を選択します:

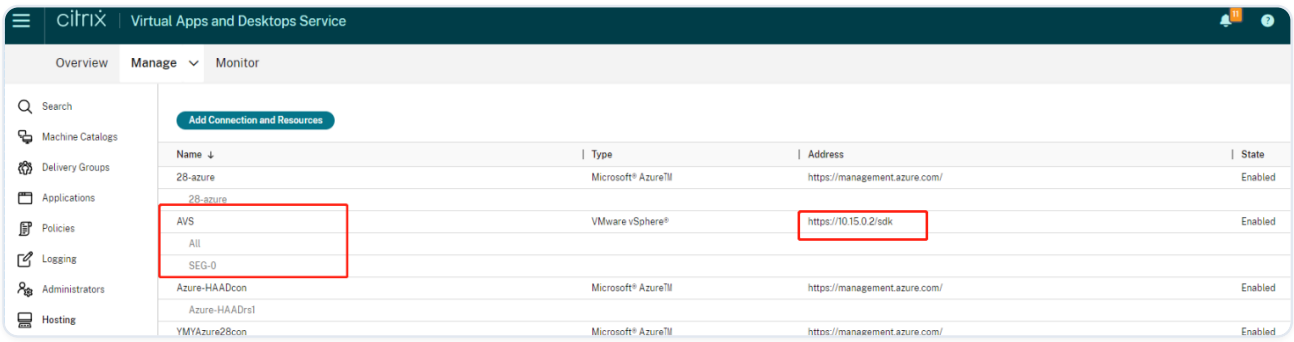


AZURE AVS環境の検証

Azureリソースグループで直接接続とコネクタを設定します。



vCenterの資格情報で接続を確認します。



グーグル クラウド ヴイエムウェア エンジン

Citrix Virtual Apps and Desktopsを使用すると、VMwareベースのオンプレミスCitrixワークロードをGoogle Cloud VMware Engineに移行できます。

Google Cloud VMware Engineを構成する

以下の手順では、Google Cloud VMware Engineでクラスターを取得してセットアップする方法について説明します。

VMWARE ENGINEポータルにアクセスする

1. **Google Cloud Console**で、ナビゲーションメニューをクリックします。
2. **Compute**セクションで、**VMware Engine**をクリックして、新しいブラウザータブでVMware Engineを開きます。

最初のプライベートクラウドを作成するための要件

Google Cloud VMware Engineへのアクセス、利用可能なVMware Engineノードクォータ、および適切なIAMロールが必要です。プライベートクラウドの作成を続行する前に、以下の要件を準備してください。

1. APIアクセスとノードクォータをリクエストします。詳細については、「APIアクセスとクォータのリクエスト」を参照してください。
2. VMware管理アプライアンスおよびHCX展開ネットワークに使用するアドレス範囲をメモします。詳細については、「ネットワーク要件」を参照してください。
3. VMware Engine Service Admin IAMロールを取得します。

最初のプライベートクラウドを作成する

1. VMware Engineポータルにアクセスします。
2. VMware Engineのホーム画面で、 をクリックします。ホスティング場所とハードウェアノードの種類が一覧表示されます。
3. プライベートクラウドのノード数を選択します。少なくとも3つのノードが必要です。
4. VMware管理ネットワークのクラスレスドメイン間ルーティング（CIDR）範囲を入力します。
5. HCX展開ネットワークのCIDR範囲を入力します。

> **重要:**
>
> CIDR範囲は、オンプレミスまたはクラウドのサブネットと重複してはなりません。
> CIDR範囲は/27以上である必要があります。

6. を選択します。
7. 設定を確認します。設定を変更するには、 をクリックします。
8. プライベートクラウドの作成を開始するには、 をクリックします。

VMware Engineが新しいプライベートクラウドを作成すると、いくつかのVMwareコンポーネントが展開され、プライベートクラウド内のクラスターの初期Autoscale™ポリシーが設定されます。

プライベートクラウドの作成には30分から2時間かかる場合があります。プロビジョニングが完了すると、メールが届きます。

GOOGLE CLOUD VMWARE ENGINE VPNゲートウェイをセットアップする

Google Cloud VMware Engineへの初期接続を確立するには、VPNゲートウェイを使用できます。これはOpenVPNベースのクライアントVPNであり、これを使用してVMware Software Defined Data Center (SDDC) vCenterに接続し、必要な初期構成を行うことができます。

VPNゲートウェイを展開する前に、SDDCが展開されているリージョンの**Edge Services**範囲を構成します。これを行うには：

1. **Google Cloud VMware Engine**ポータルにログオンし、 **>** に移動します。 をクリックします。
2. SDDCが展開されているリージョンを選択し、 と を有効にします。
3. 計画中にメモしたEdge Servicesの範囲を入力し、 をクリックします。これらのサービスを有効にするには10〜15分かかります。

   完了すると、リージョン設定ページでEdge Servicesが**** と表示されます。これらの設定を有効にすると、SDDCにパブリックIPを割り当てることができ、これはVPNゲートウェイを展開するための要件です。

VPNゲートウェイを展開するには：

1. **Google Cloud VMware Engine**ポータルで、 **>** に移動します。 をクリックします。
2. VPNゲートウェイの名前と、計画中に予約したクライアントサブネットを指定します。**次へ**をクリックします。
3. VPNアクセスを許可するユーザーを選択します。「**次へ**」をクリックします。
4. VPN経由でアクセス可能にする必要があるネットワークを指定します。「**次へ**」をクリックします。
5. 概要画面が表示されます。選択内容を確認し、「**送信**」をクリックしてVPNゲートウェイを作成します。VPNゲートウェイページに、新しいVPNゲートウェイのステータスが「**作成中**」と表示されます。
6. ステータスが「**稼働中**」に変わったら、新しいVPNゲートウェイをクリックします。
7. 「**VPN構成をダウンロード**」をクリックして、VPNゲートウェイ用に事前設定されたOpenVPNプロファイルを含むZIPファイルをダウンロードします。UDP/1194およびTCP/443経由で接続するためのプロファイルが利用可能です。好みのプロファイルを選択してOpenVPNにインポートし、接続します。
8. 「**リソース**」に移動し、SDDCを選択します。

VPNを接続する

1. VPNゲートウェイの設定を通じて、オンプレミスネットワークとプライベートクラウド間のポイントツーサイト接続を確立します。Google Cloud VMware Engine VPNゲートウェイのセットアップを参照してください。
2. Google Cloud VMware Engine VPNゲートウェイのセットアップでダウンロードしたVPN構成をアップロードします。
3. VPNクライアント（例: OpenVPN Connect）にインポートします。

詳細については、VPNを使用した接続を参照してください。

最初のサブネットを作成する

VMware EngineポータルからNSX-T Managerにアクセスする
サブネットの作成プロセスはNSX-Tで行われ、VMware Engineを介してアクセスします。NSX-T Managerにアクセスするには、次の手順を実行します。

1. **Google Cloud VMware Engine**ポータルにログオンします。
2. メインナビゲーションから、**リソース**に移動します。
3. サブネットを作成するプライベートクラウドに対応する**プライベートクラウド名**をクリックします。
4. プライベートクラウドの詳細ページで、**vSphere Management Network**タブをクリックします。
5. NSX-T Managerに対応する**FQDN**をクリックします。
6. プロンプトが表示されたら、サインイン資格情報を入力します。vIDMを設定し、Active DirectoryなどのIDソースに接続している場合は、代わりにIDソースの資格情報を使用します。

> **注意:**
>
> 生成された資格情報は、プライベートクラウドの詳細ページから取得できます。

サブネットのDHCPサービスを設定する
サブネットを作成する前に、DHCPサービスを設定します。

NSX-T マネージャーで：

1. **ネットワーキング > DHCP**に移動します。ネットワーキングダッシュボードには、DHCPサービスが1つのTier-0と1つのTier-1ゲートウェイを作成することが示されます。

2. DHCPサーバーのプロビジョニングを開始するには、**サーバーの追加**をクリックします。
3. **サーバータイプ**で**DHCP**を選択し、サーバー名とIPアドレスを指定します。
4. **保存**をクリックしてDHCPサービスを作成します。

このDHCPサービスを関連するTier-1ゲートウェイにアタッチするには、次の手順を実行します。デフォルトのTier-1ゲートウェイは、DHCPサービスによってすでにプロビジョニングされています。

1. 「**Tier 1 Gateways**」を選択し、Tier-1 ゲートウェイの縦の省略記号を選択し、「**Edit**」を選択します。
2. 「**IP Address Management**」フィールドで、「**No IP Allocation Set**」を選択します。
3. 「**Type**」に「**DHCP Local Server**」を選択します。
4. 「**DHCP Server**」には、作成した DHCP サーバーを選択します。
5. 「**保存**」をクリックします。
6. 「**Close Editing**」をクリックします。

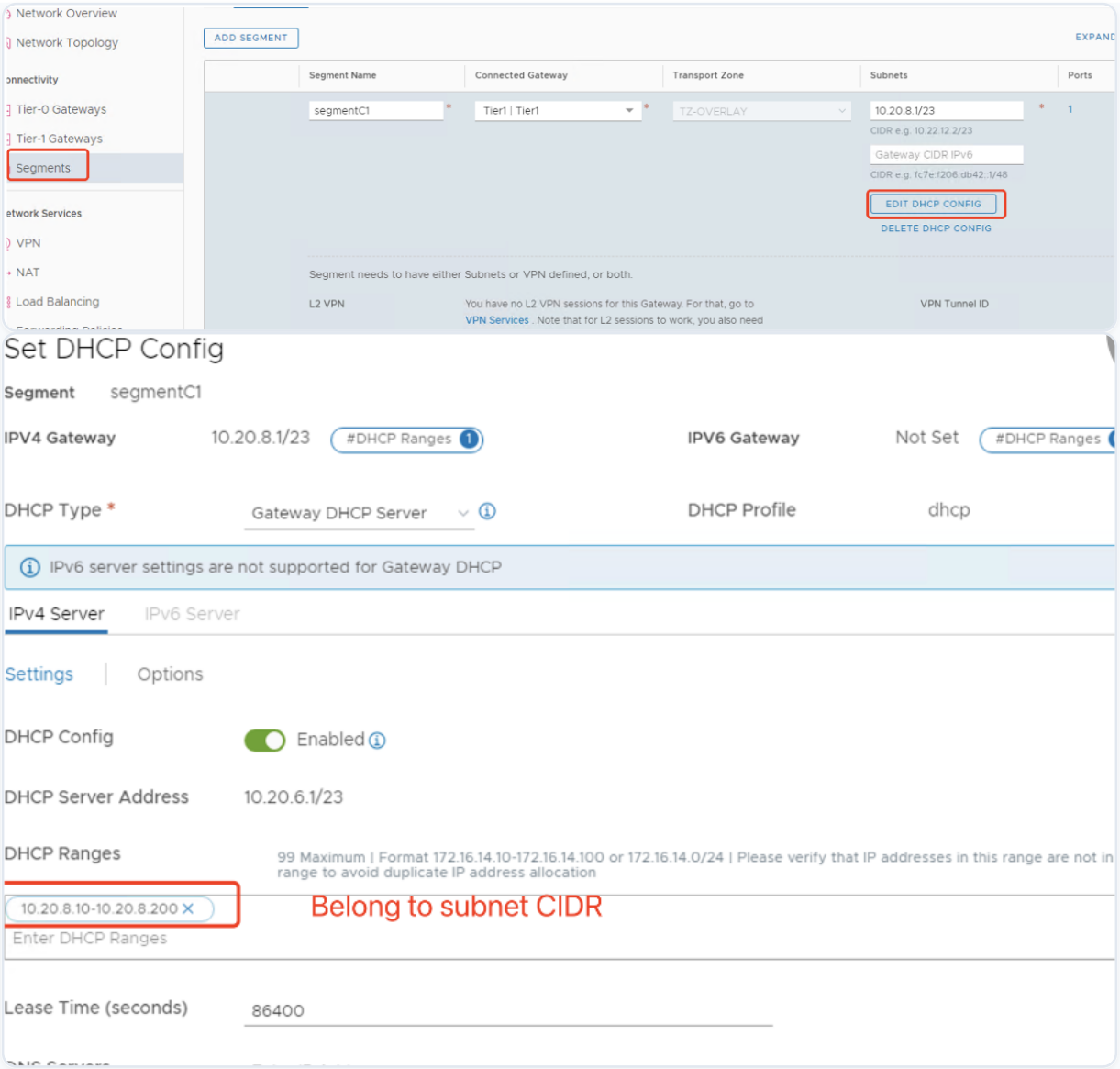
これで、NSX-T でネットワークセグメントを作成できます。NSX-T の DHCP の詳細については、DHCP に関する VMware ドキュメントを参照してください。
NSX-T でネットワークセグメントを作成する
ワークロード VM の場合、プライベートクラウドの NSX-T ネットワークセグメントとしてサブネットを作成します。

1. NSX-T Manager で、「**Networking > Segments**」に移動します。
2. 「**Add Segment**」をクリックします。
3. セグメントの名前を入力します。
4. 「**Connected Gateway**」として「**Tier-1**」を選択し、「Type」は「**Flexible**」のままにします。
5. 「**Set Subnets**」をクリックします。
6. 「**Add Subnets**」をクリックします。
7. 「**Gateway IP/Prefix Length**」にサブネット範囲を入力します。最後のオクテットが「**.1**」となるようにサブネット範囲を指定します。例: **10.12.2.1/24**。
8. DHCP範囲を指定し、**ADD**をクリックします。
9. 「**Transport Zone**」で、ドロップダウンリストから「**TZ-OVERLAY**」を選択します。
10. **Save**をクリックします。これで、VMの作成時にvCenterでこのネットワークセグメントを選択できるようになります。

特定のリージョンでは、VMware EngineからVPC networkへのプライベートサービスアクセスを使用して、最大100個の一意のルートを設定できます。これには、たとえば、プライベートクラウド管理IPアドレス範囲、NSX-Tワークロードネットワークセグメント、HCXネットワークIPアドレス範囲が含まれます。この制限には、リージョン内のすべてのプライベートクラウドが含まれます。

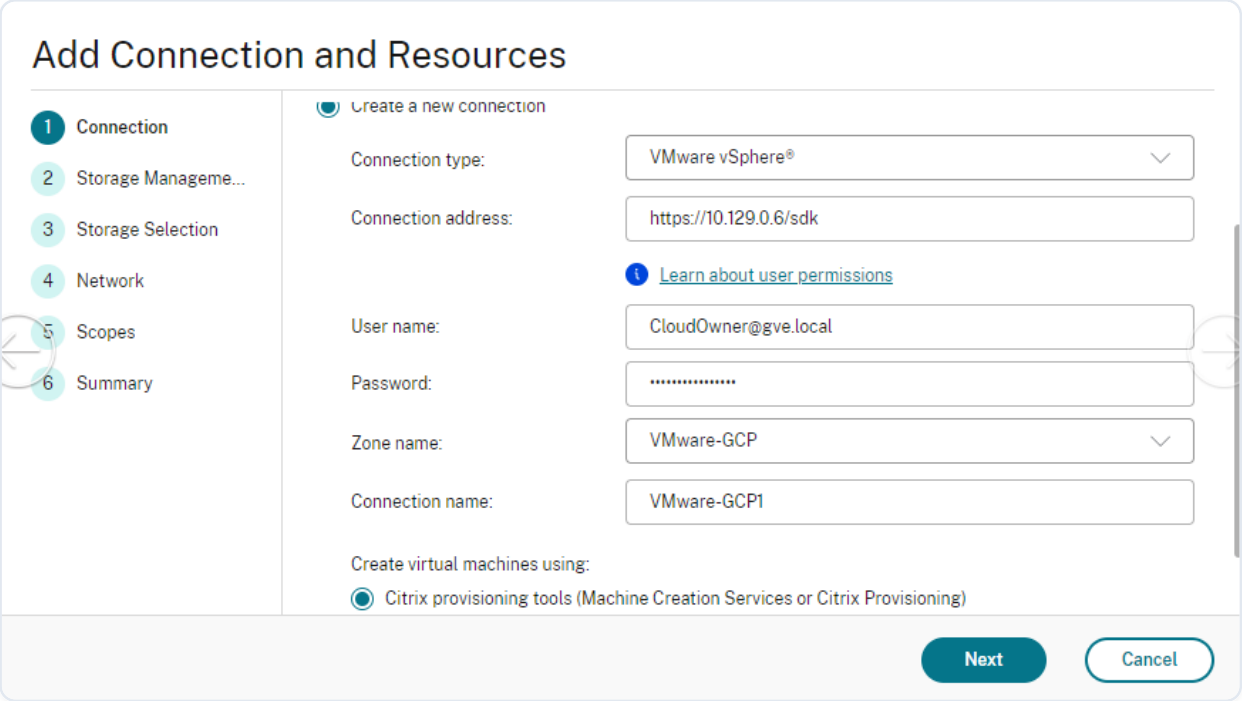
注：

Google Cloudの構成の問題により、DHCP範囲設定を複数回構成する必要があります。したがって、Google Cloudの構成後にDHCP範囲設定を構成するようにしてください。DHCP範囲を構成するには、**EDIT DHCP CONFIG**をクリックします。



CITRIX STUDIOでGOOGLE CLOUD VMWARE接続を作成する

1. vCenterでマシンを作成します。
2. Citrix Studioを起動します。
3. ホスティングノードを選択し、**Add Connection and Resources**をクリックします。
4. 「**Connection**」画面で、「**Create a new Connection**」を選択し、以下の詳細を入力します。



   a. 「**Connection type**」として「**VMware vSphere**」を選択します。
   b. 「**接続アドレス**」にvCenterのプライベートIPアドレスを入力します。
   c. vCenterの資格情報を入力します。
   d. 接続名を入力します。
   e. 仮想マシンを作成するツールを選択します。

5. **ネットワーク**画面で、NSX-Tサーバーで作成されたサブネットを選択します。
6. ウィザードを完了します。

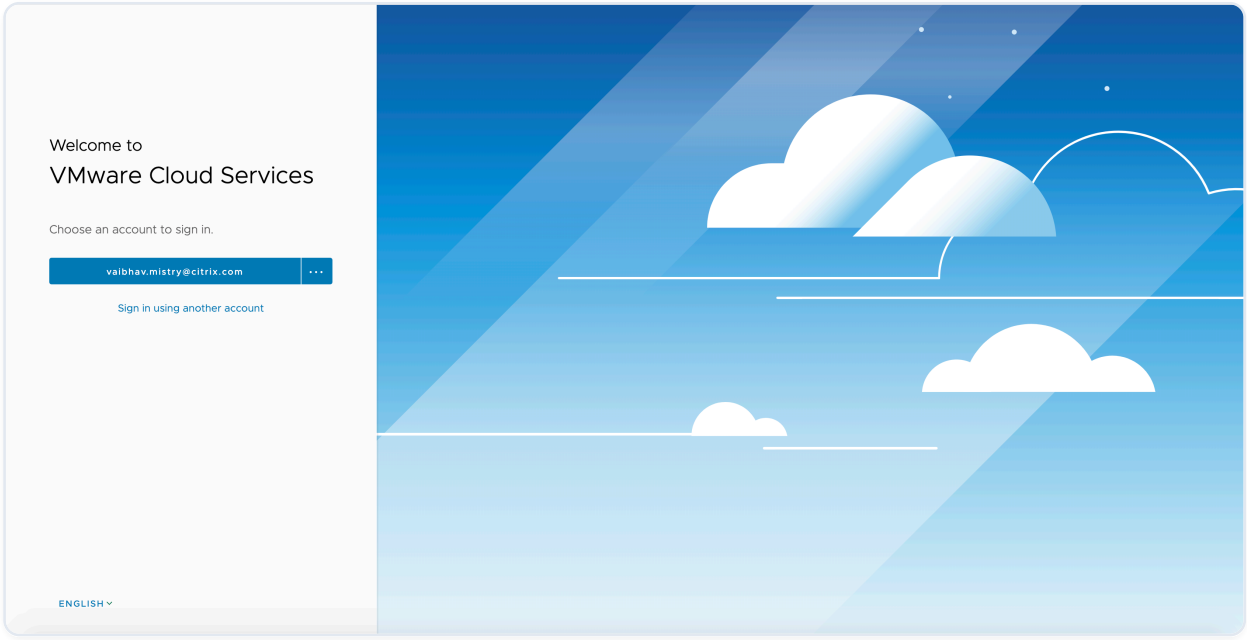
アマゾン ウェブ サービス (AWS) 上の ヴイエムウェア クラウド

Amazon Web Services (AWS) 上のVMware Cloudを使用すると、VMwareベースのオンプレミスCitrixワークロードをAWS Cloudに移行できます。

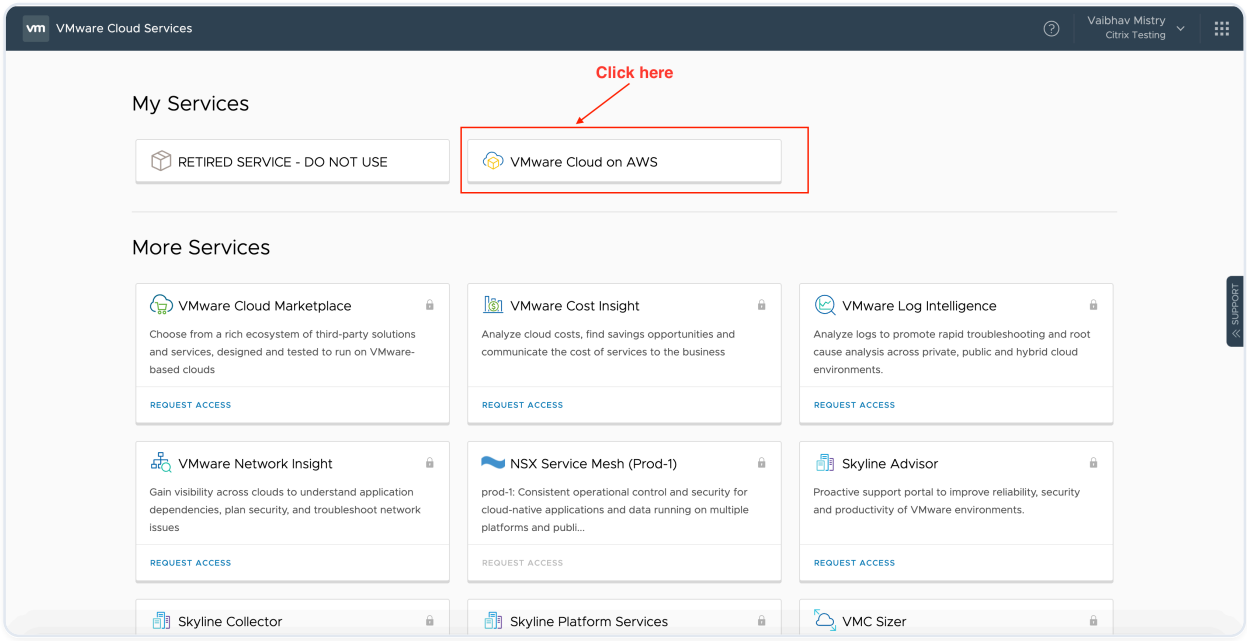
この記事では、AWS上にVMware Cloudをセットアップする手順について説明します。

VMware Cloud環境にアクセスする

1. URL `<https://console.cloud.vmware.com/>` を使用してVMware Cloudサービスにログインします。



2. 「**VMware Cloud on AWS**」をクリックします。「Software-Defined Data Centers (SDDC)」ページが表示されます。



3. 「**OPEN VCENTER**」をクリックし、次に「**SHOW CREDENTIALS**」をクリックします。後で使用するために資格情報を控えておきます。

「vCenterを開く」(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/vmc-sddc.png)

「資格情報を表示」(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/show-credentials-vmc.png)

4. Webブラウザを開き、vSphere Web ClientのURLを入力します。
5. 記載されている資格情報を入力し、**ログイン**をクリックします。vSphereクライアントのWebページは、オンプレミス環境のものと似ています。

「vSphereクライアントのWebページ」(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/vcenter-page.png)

VMwareクラウド環境について

vSphereクライアントのWebページには4つのビューがあります。

- ホストおよびクラスタービュー: 新しいクラスターを作成することはできませんが、クラウド管理者は複数のリソースプールを作成できます。

  「ホストおよびクラスタービュー」(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/host-cluster-view.png)
- VMおよびテンプレートビュー: クラウド管理者は多くのフォルダーを作成できます。

  「VMおよびテンプレートビュー」(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/vm-template-view.png)
- ストレージビュー: Citrix Studioでホスティングユニットを追加する際は、**WorkloadDatastore**ストレージを選択してください。Workload Datastoreにのみアクセスできるためです。

  「ストレージビュー」(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/storage-view.png)
- ネットワークビュー: VMwareクラウドネットワークと不透明なネットワークでは、アイコンが異なります。

  「ネットワークビュー」(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/network-view.png)

クラスターを設定した後、接続とリソースを追加するには、VMware virtualization environmentsを参照してください。

次のステップ

- コアコンポーネントのインストール
- VDAのインストール
- サイトの作成

- 接続の作成と管理については、「VMware Cloudおよびパートナーソリューションへの接続」を参照してください。

詳細情報

- 接続とリソースを作成および管理する
- マシンカタログを作成する

コアコンポーネントをインストールする

重要:

Citrix は、ライセンスコンプライアンスを含む正当な利益のために、基本的なライセンスデータを収集します。詳細については、Citrix Licensing Data を参照してください。 ライセンスサーバーがバージョン 11.17.2 ビルド 53100 以降を実行していることを確認してください。この前提条件を満たさない場合、サイトのアップグレードや作成中にエラーや推奨事項が発生する可能性があります。

コアコンポーネントは、Citrix Delivery Controller™、Citrix Studio、Web Studio、Citrix Director、および Citrix License Server です。

注：

Citrix Studio は、オンプレミスの Citrix Virtual Apps and Desktops 展開を構成および管理できる Windows ベースの管理コンソールです。Web Studio は、Citrix Studio の次世代版であり、Citrix Studio と同等の機能を備えた Web ベースの管理コンソールです。Web Studio の詳細については、「Web Studio のインストール」を参照してください。

(2003 より前のバージョンでは、コアコンポーネントに Citrix StoreFront が含まれていました。**Citrix StoreFront** タイルをクリックするか、インストールメディアで利用可能なコマンドを実行することで、StoreFront をインストールできます。)

インストールを開始する前に、この記事と「インストールの準備」を確認してください。

この記事では、コアコンポーネントのインストール時のインストールウィザードのシーケンスについて説明します。コマンドラインの同等機能も提供されています。詳細については、「コマンドラインを使用したインストール」を参照してください。

ステップ 1. 製品ソフトウェアをダウンロードしてウィザードを起動する

Citrix アカウントの資格情報を使用して、Citrix Virtual Apps and Desktops™ のダウンロードページにアクセスします。製品の ISO ファイルをダウンロードします。

ファイルを解凍します。必要に応じて、ISO ファイルを DVD に書き込みます。

コアコンポーネントをインストールするマシンに、ローカル管理者アカウントを使用してログオンします。

DVD をドライブに挿入するか、ISO ファイルをマウントします。インストーラーが自動的に起動しない場合は、**AutoSelect** アプリケーションまたはマウントされたドライブをダブルクリックします。

ステップ 2. インストールする製品を選択する



インストールする製品 (Virtual Apps または Virtual Apps and Desktops) の横にある **Start** をクリックします。

(マシンにCitrix Virtual Apps and Desktopsコンポーネントがすでにインストールされている場合、このページは表示されません。)

コマンドラインオプション: Citrix Virtual Apps をインストールするには `/xenapp` を使用します。このオプションを省略すると、Citrix Virtual Apps and Desktops がインストールされます。

ステップ 3. インストールするものを選択する

コンポーネントインストーラーのコンポーネント選択ページ(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/what-to-install-2.png)

初めて使用する場合は、**Delivery Controller** を選択します。(後のページで、このマシンにインストールする特定のコンポーネントを選択します。)

コントローラーをすでにインストールしている場合 (このマシンまたは別のマシンに)、別のコンポーネントをインストールするには、**展開の拡張**セクションからコンポーネントを選択します。

コマンドラインオプション: `/components`

ステップ 4. ライセンス契約を読んで同意する

コンポーネントインストーラーのライセンス契約ページ(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/core-license-75.png)

ライセンス契約ページで、ライセンス契約を読んだ後、内容を読んで同意したことを示します。次に、**次へ**をクリックします。

ステップ 5. インストールするコンポーネントとインストール場所を選択する

コンポーネントインストーラーのコアコンポーネントページ(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/core-components-75.png)

コアコンポーネントページで:

- **場所:** デフォルトでは、コンポーネントは `C:\Program Files\Citrix` にインストールされます。ほとんどの展開では、デフォルトで問題ありません。別の場所を指定する場合は、ネットワークサービスに対する実行権限が必要です。
- **コンポーネント:** デフォルトでは、すべてのコアコンポーネントのチェックボックスが選択されています。すべてのコアコンポーネントを1台のサーバーにインストールすることは、概念実証、テスト、または小規模な本番環境の展開には問題ありません。大規模な本番環境では、Citrix は Director、StoreFront、Secure Private Access、およびライセンスサーバーを別々のサーバーにインストールすることを推奨します。

> **注：**
>
> 複数のサーバーにコンポーネントをインストールする場合は、他のサーバーに他のコンポーネントをインストールする前に、Citrix License Server とライセンスを最初にインストールしてください。ガイダンスについては、Citrix Virtual Apps and Desktops のライセンスガイド の「自動インストール」セクションを参照してください。
>
> このマシンに必須のコアコンポーネントをインストールしないことを選択すると、アイコンで警告が表示されます。この警告は、そのコンポーネントをインストールする必要があることを通知しますが、必ずしもこのマシンにインストールする必要があるわけではありません。

Nextをクリックします。

コマンドラインオプション: `/installdir`、`/components`、`/exclude`

ハードウェアチェック

Delivery Controller をインストールまたはアップグレードすると、ハードウェアがチェックされます。マシンに推奨される RAM 容量 (5 GB) より少ない場合、インストーラーは警告を表示します。これはサイトの安定性に影響を与える可能性があります。詳細については、「ハードウェア要件」を参照してください。

グラフィカルインターフェイス: ダイアログボックスが表示されます。

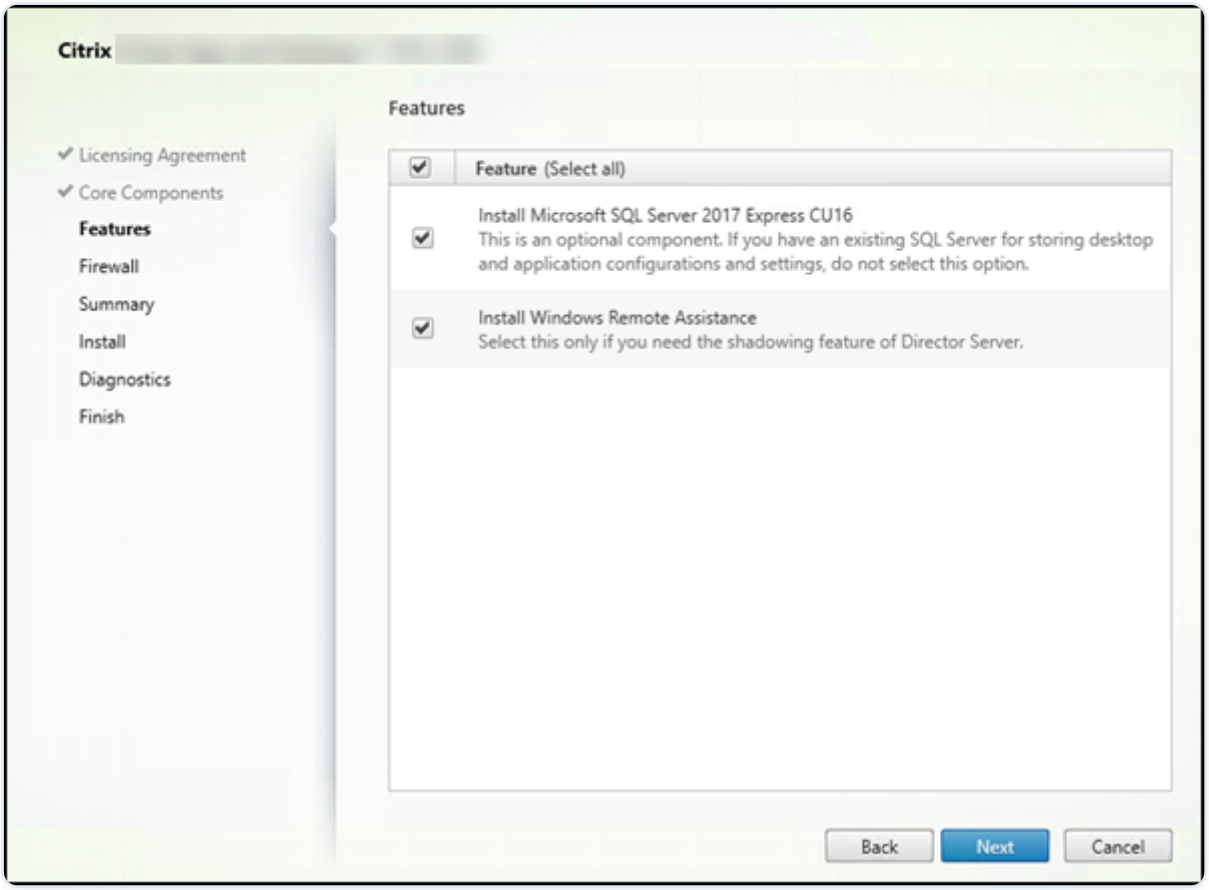
- 推奨: **キャンセル** をクリックしてインストールを停止します。マシンに RAM を追加してから、再度インストールを開始します。
- または、**次へ** をクリックしてインストールを続行します。サイトで安定性の問題が発生する可能性があります。

コマンドラインインターフェイス: インストール/アップグレードが終了します。インストールログには、検出された内容と利用可能なオプションを説明するメッセージが含まれています。

- 推奨: マシンに RAM を追加してから、再度コマンドを実行します。
- または、`/ignore_hw_check_failure` オプションを指定してコマンドを再度実行し、警告を上書きします。サイトで安定性の問題が発生する可能性があります。

アップグレード時には、OS または SQL Server のバージョンがサポートされなくなった場合にも通知されます。詳細については、「展開のアップグレード」を参照してください。

手順 6. 機能の有効化または無効化



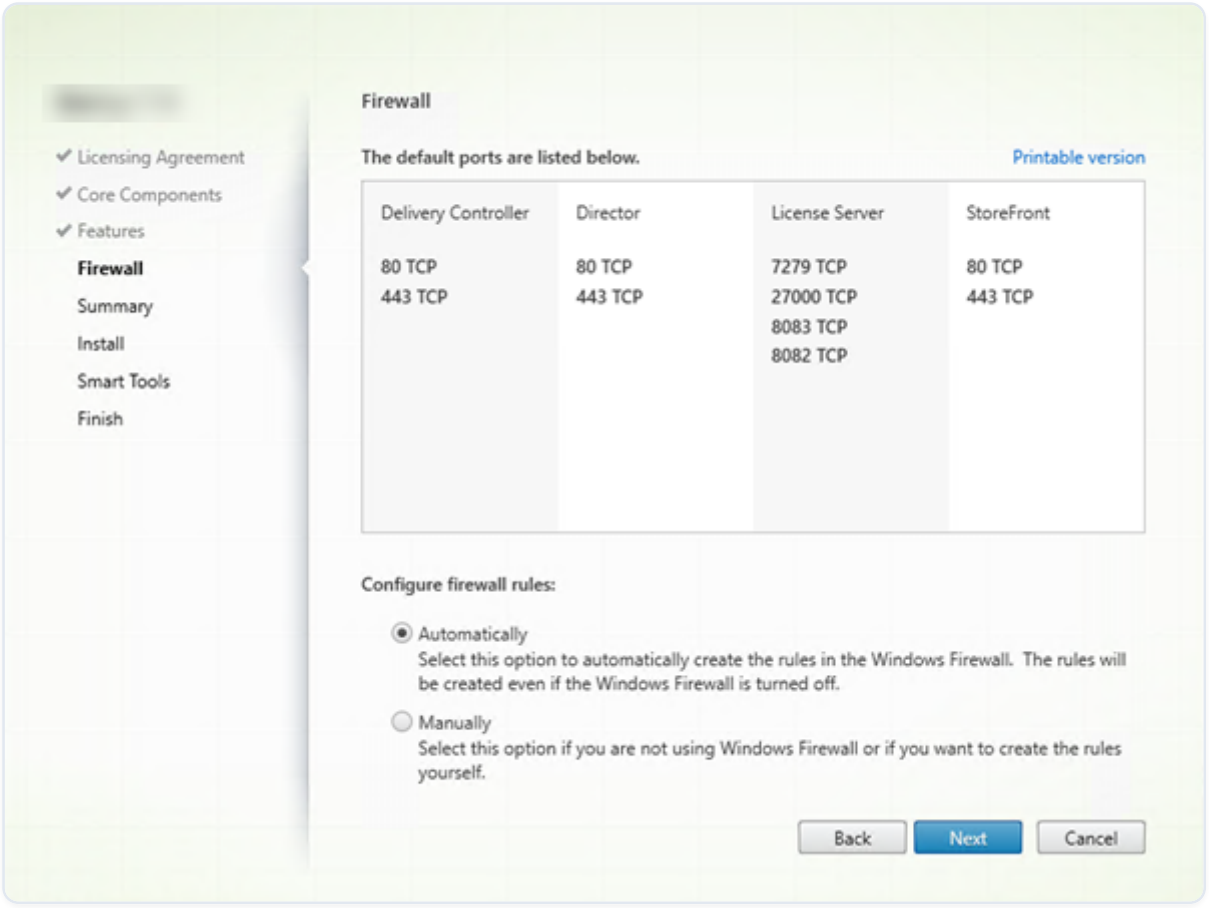
機能ページで:

- サイトデータベースとして使用するMicrosoft SQL Server Expressをインストールするかどうかを選択します。デフォルトでは、この選択は有効になっています。Citrix Virtual Apps and Desktopsデータベースに慣れていない場合は、データベースを確認してください。
- Directorをインストールすると、Windowsリモートアシスタンスが自動的にインストールされます。Directorのユーザーシャドウイングで使用するために、Windowsリモートアシストでシャドウイングを有効にするかどうかを選択します。シャドウイングを有効にすると、TCPポート3389が開きます。デフォルトでは、この機能は有効になっています。ほとんどの展開では、デフォルト設定で問題ありません。この機能は、Directorをインストールしている場合にのみ表示されます。

Nextをクリックします。

コマンドラインオプション: `/nosql` (インストールを防止するため)、`/no_remote_assistance` (有効化を防止するため)

手順7. Windowsファイアウォールポートを開く



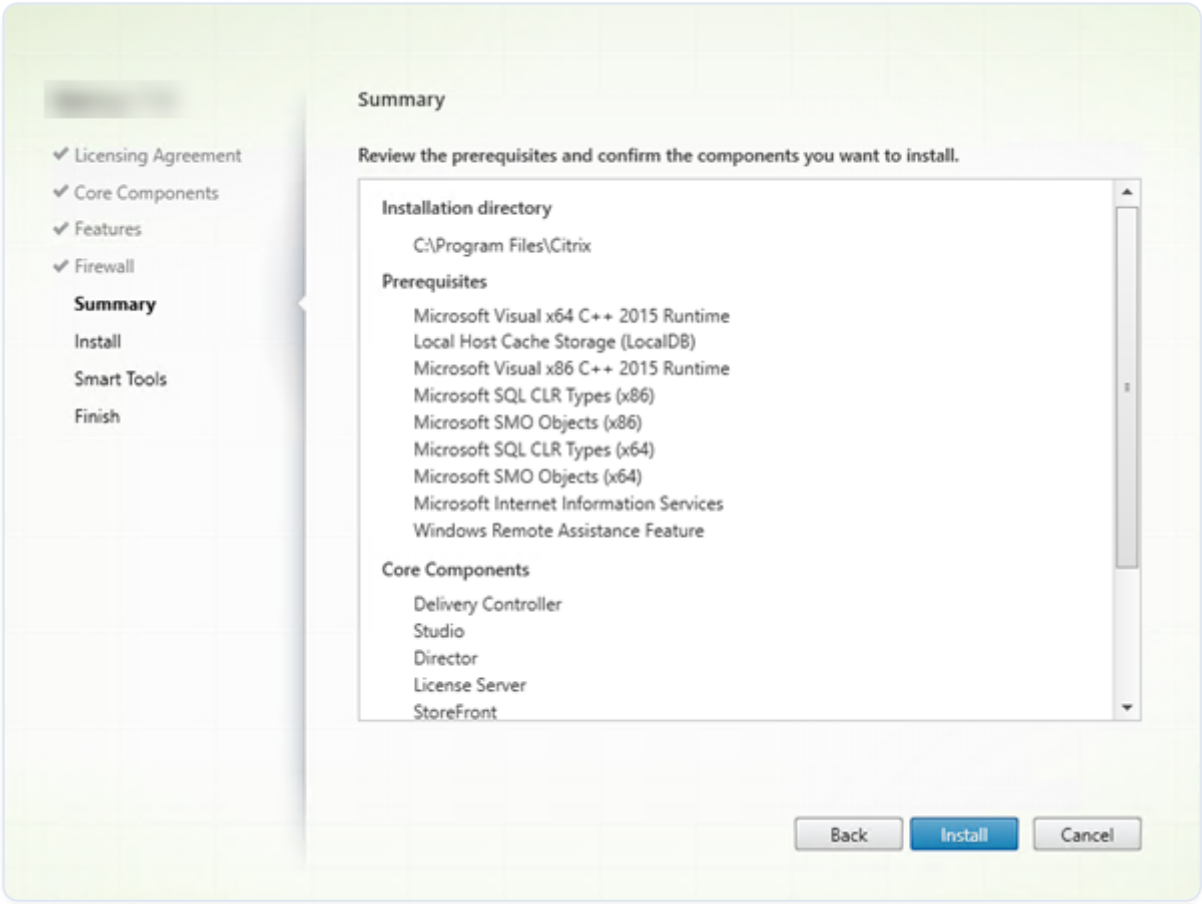
デフォルトでは、Windowsファイアウォールサービスが実行されている場合、ファイアウォールが有効になっていなくても、**ファイアウォール**ページ上のポートは自動的に開かれます。ほとんどの展開では、デフォルト設定で問題ありません。ポート情報については、ネットワークポートを参照してください。

Nextをクリックします。

(このグラフィックは、このマシンにすべてのコアコンポーネントをインストールしたときのポートリストを示しています。この種のインストールは、通常、テスト展開のみを対象としています。)

コマンドラインオプション: `/configure_firewall`

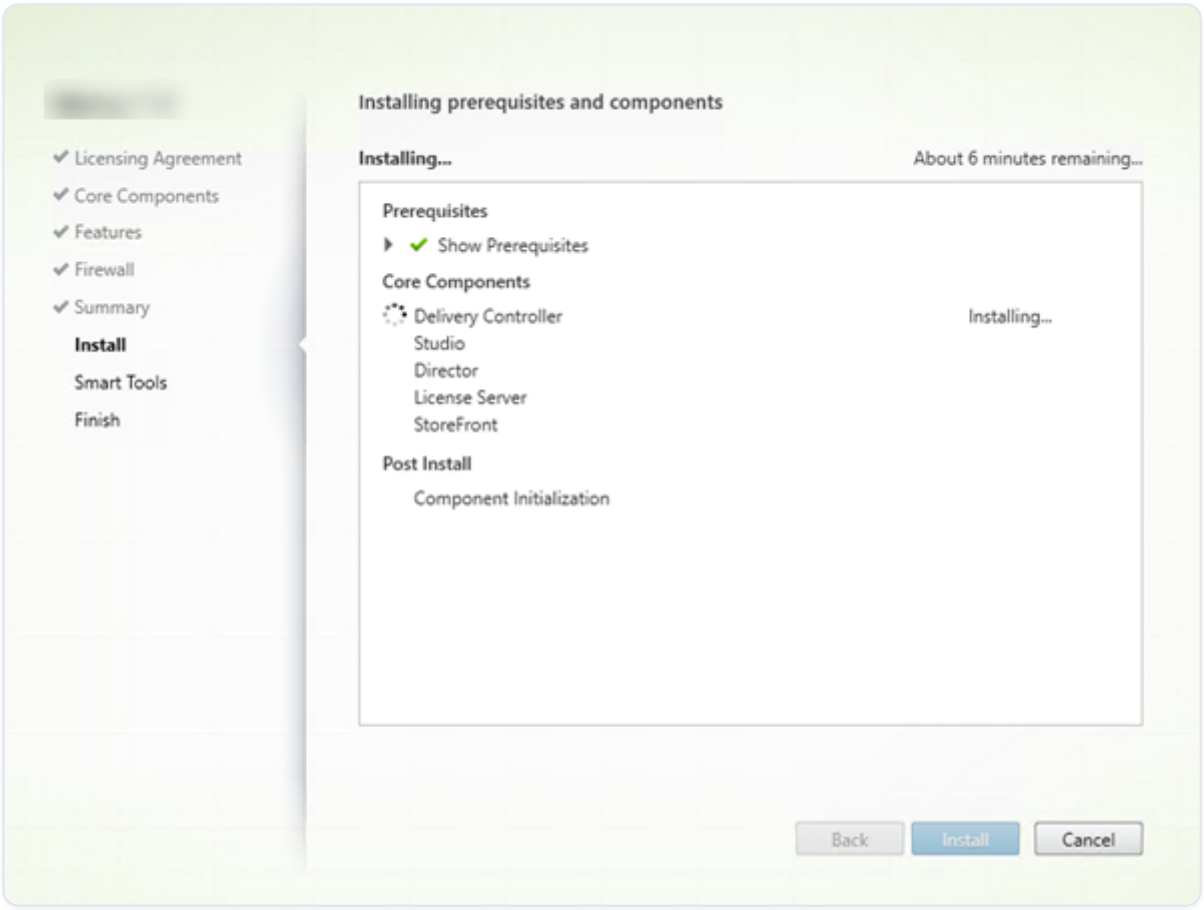
手順8. 前提条件を確認し、インストールを確定する



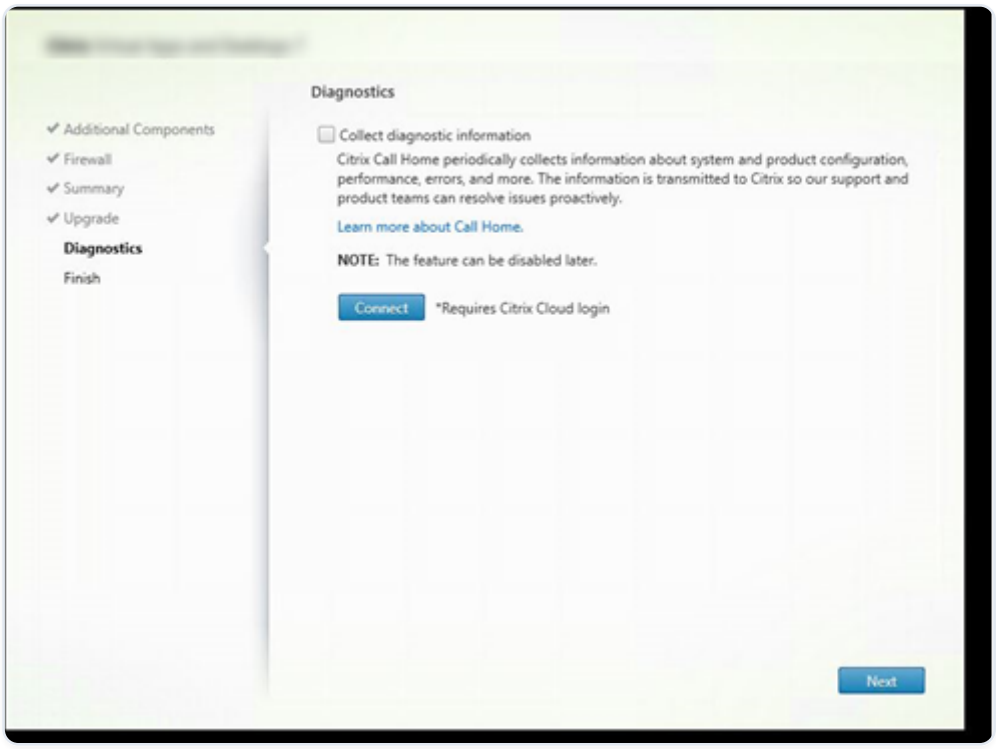
概要ページには、インストールされるものが一覧表示されます。必要に応じて、**戻る**ボタンを使用して以前のウィザードページに戻り、選択を変更します。

準備ができたら、**インストール**をクリックします。

ディスプレイにはインストールの進行状況が表示されます。



ステップ9. Cloud Software Groupとの診断情報の共有



診断ページで、Citrix Call Homeに参加するかどうかを選択します。

このページは、グラフィカルインターフェイスを使用してDelivery Controllerをインストールするときに表示されます。StoreFrontをインストールする場合（ただしControllerではない場合）、ウィザードはこのページを表示します。その他のコアコンポーネントをインストールする場合（ただしControllerまたはStoreFrontではない場合）、ウィザードはこのページを表示しません。

アップグレード中に、Call Homeがすでに有効になっている場合、またはインストーラーがCitrix Telemetry Serviceに関連するエラーを検出した場合、このページは表示されません。

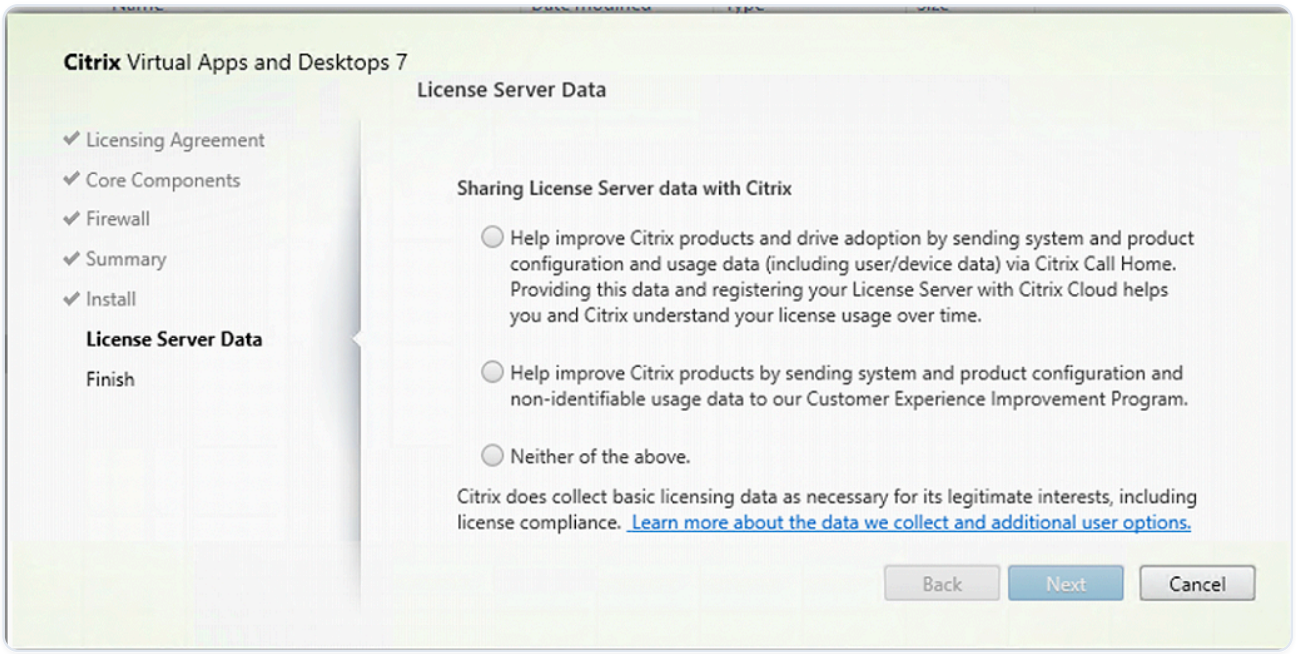
参加することを選択した場合（デフォルト）、**接続**をクリックします。プロンプトが表示されたら、Citrixアカウントの資格情報を入力します。登録の選択は、インストール後に変更できます。

資格情報が検証された後（または参加しないことを選択した場合）、**次へ**をクリックします。

診断ページで、最初に**診断情報の収集**を選択せずに**接続**をクリックした場合、**Citrix Insight Servicesに接続**ダイアログを閉じると**次へ**ボタンが無効になります。次のページに進むことはできません。**次へ**ボタンを再度有効にするには、**診断情報の収集**を選択してすぐに選択を解除します。

詳細については、Call Homeを参照してください。

ステップ10. Cloud Software Groupとのライセンスサーバーデータの共有



ライセンスサーバーデータページでは、お客様を支援するために、Call Homeデータまたはカスタマーエクスペリエンス向上プログラム（CEIP）データのいずれかを共有していただくようお願いしています。さらに、Cloud Software Groupは、正当な利益のために必要に応じて、ライセンスコンプライアンスを含む基本的なライセンスデータの収集も要求します。

ライセンスサーバーデータページは、ライセンスサーバーをインストールしたときに表示されます。

- スタンドアロンとして。
- Delivery Controllerのインストール中に、コアコンポーネントとして。

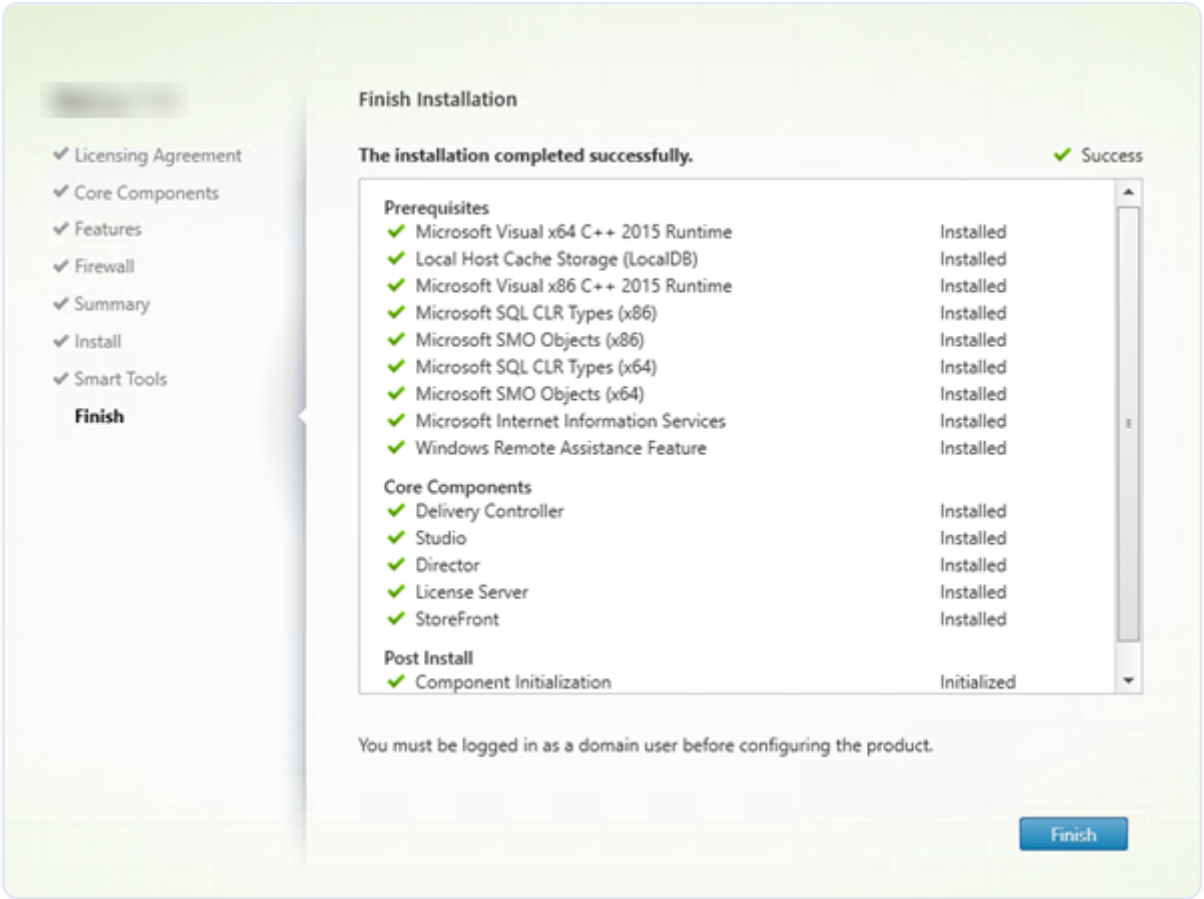
アップグレード中に、`/CITRIX.opt:` ファイルで構成がすでに設定されている場合、このページは表示されません。

ライセンスサーバーは、ライセンスデータ、Call Homeデータ、CEIPデータなど、いくつかの種類のユーザーデータを監視します。Call HomeデータとCEIPデータの収集を有効にするには、参加（オプトイン）を選択する必要があります。

コマンドラインを使用してインストールする際にCall HomeおよびCEIPデータ収集を有効にする方法の詳細については、「コアコンポーネントをインストールするためのコマンドラインオプション」を参照してください。

Cloud Software Groupのライセンスデータ収集の詳細については、「Citrixライセンスデータ収集プログラム」を参照してください。

ステップ11. このインストールを完了する



完了ページには、正常にインストールおよび初期化されたすべての前提条件とコンポーネントに緑色のチェックマークが表示されます。

完了をクリックします。

ステップ12. 残りのコアコンポーネントを他のマシンにインストールする

すべてのコアコンポーネントを1台のマシンにインストールした場合は、「次のステップ」に進みます。そうでない場合は、他のマシンでインストーラーを実行して他のコンポーネントをインストールします。他のサーバーにControllerを追加でインストールすることもできます。

次のステップ

必要なすべてのコンポーネントをインストールしたら、Studioを使用してサイトを作成します。

サイトを作成したら、VDAをインストールします。

いつでも、フルプロダクトインストーラーを使用して、以下のコンポーネントで展開を拡張できます。

- **Universal Print Serverサーバーコンポーネント:** プリントサーバーでインストーラーを起動します。

  a. **展開の拡張**セクションで**Universal Print Server**を選択します。

  b. ライセンス契約に同意します。

  c. 「**ファイアウォール**」ページでは、Windowsファイアウォールサービスが実行されている場合、ファイアウォールが有効になっていない場合でも、デフォルトでTCPポート7229および8080がファイアウォールで開かれます。ポートを手動で開きたい場合は、このデフォルトのアクションを無効にできます。

  このコンポーネントをコマンドラインからインストールするには、「Universal Print Serverをインストールするためのコマンドラインオプション」を参照してください。
- 「フェデレーション認証サービス」。
- 「セッション録画」。
- 「ワークスペース環境管理」。

Web Studio のインストール

はじめに

Citrix Studio は、Citrix Virtual Apps and Desktops 展開を構成および管理できる Windows ベースの管理コンソールです。Web Studio は、Citrix Studio の次世代であり、Citrix Studio と完全に同等の機能を提供する Web ベースの管理コンソールです。(/ja-jp/citrix-daas/overview#studio) と同じルックアンドフィールで、Web Studio はネイティブの Web エクスペリエンスを提供することで、管理エクスペリエンスを最新化します。

Web Studio は、Internet Information Service (IIS) がインストールされている任意の Windows サーバーに展開できます。展開オプションは次の 2 つです。

- 専用サーバーにインストールする:

  パフォーマンスと拡張性が重要な大規模環境では、Web Studio を専用サーバーにインストールすることをお勧めします。このサーバーは、オプションで Director もホストできます。

- Delivery Controller™ と統合する:

  迅速な展開とシンプルな環境では、Web Studio を Delivery Controller に直接インストールします。このアプローチは、管理オーバーヘッドを最小限に抑えることが優先される小規模な展開に最適です。

次の図は、Web Studio のアーキテクチャを示しています。

「Web Studio のアーキテクチャ」(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/web-studio-architecture.png)

Web Studio を稼働させるための一般的なワークフローは次のとおりです。

1. (#install-web-studio-1)。
2. (#configure-a-certificate-for-tls)。
3. (#set-up-a-site)。
4. (#add-delivery-controllers-to-web-studio-for-management)。
5. (オプション) Delivery Controller のプロキシとして Web Studio を構成する(#optional-configure-web-studio-as-a-proxy-for-delivery-controllers)
6. 「(オプション) Pendoを無効にする」(#optional-enable-or-disable-pendo)。
7. 「Web Studioにサインインする」(#sign-in-to-web-studio)。

負荷分散されたWeb Studio展開をセットアップするには、(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/install-configure/install-core/load-balance-studio.html)を参照してください。

Web Studioで利用可能な新機能

(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/whats-new.html#web-studio)の記事を参照してください。

システム要件

サポートされているオペレーティングシステム:

- Windows Server 2022、StandardおよびDatacenterエディション、Server Coreオプション付き
- Windows Server 2019、StandardおよびDatacenterエディション、Server Coreオプション付き
- Windows Server 2016、StandardおよびDatacenterエディション、Server Coreオプション付き

サポートされているブラウザー:

- マイクロソフト エッジ 92
- ファイアフォックス ESR (延長サポート版) 90
- グーグル クローム 92
- サファリ 14

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

前提条件

このWeb Studioリリースは、Citrix Virtual Apps and Desktops™ 2212以降の展開と互換性があります。

2212より前の展開の場合、まず2212にアップグレードしてからWeb Studioをインストールします。

既知の制限事項

Web StudioとCitrix Studioを相互に利用する場合、次の制限事項を考慮してください。Web Studioで作成されたテンプレートはCitrix Studioには表示されず、その逆も同様です。これは、Web Studioがテンプレートの保存にCitrix Studioとは異なるデータベースを使用するためです。回避策として、Web Studioでテンプレートからポリシーを作成し、次にCitrix Studioでこのポリシーからテンプレートを作成します。その逆も同様です。

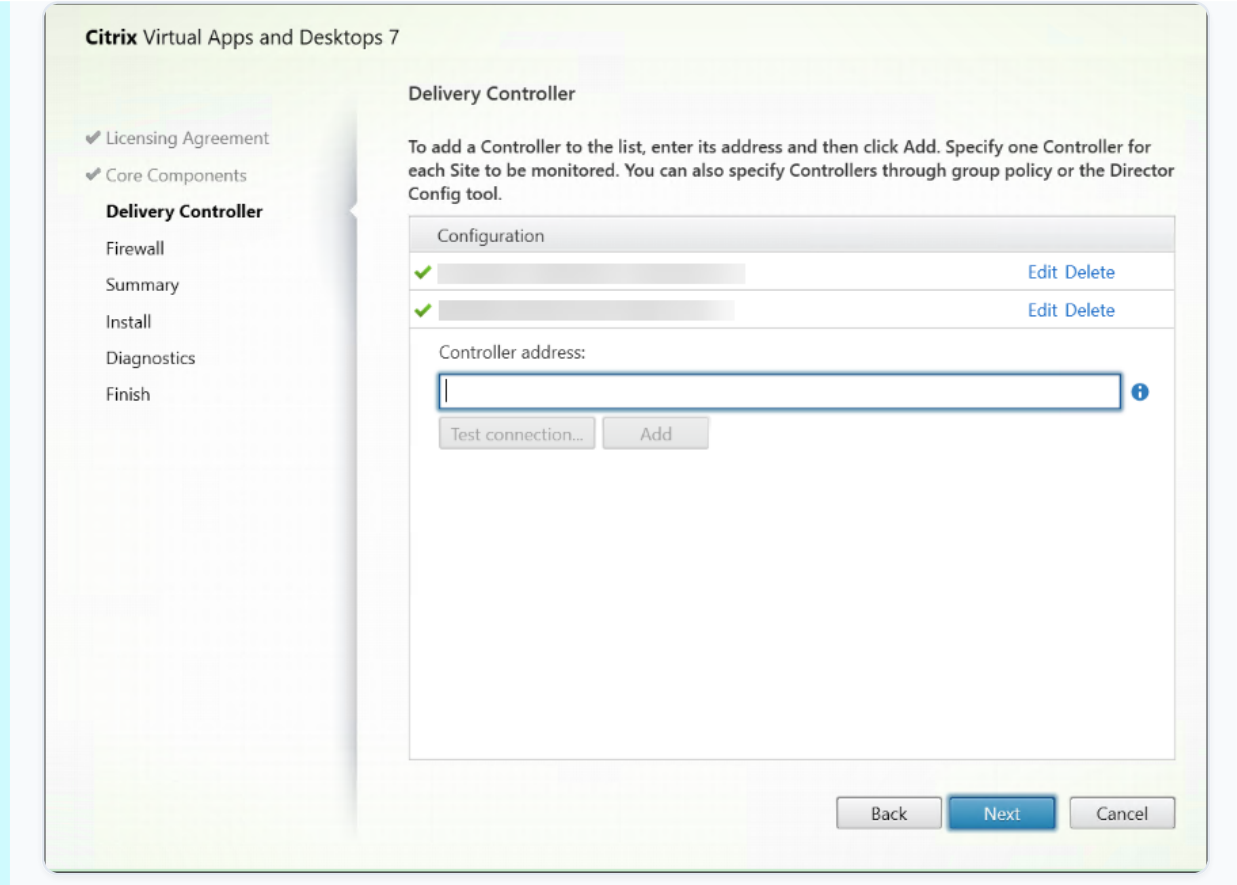
- Web Studioのインストールを成功させるには、Internet Information Services (IIS) マネージャーでデフォルトのサイト名 (**Default Web Site**) を変更しないでください。デフォルトのサイト名を変更すると、インストールが失敗します。

Web Studioのインストール

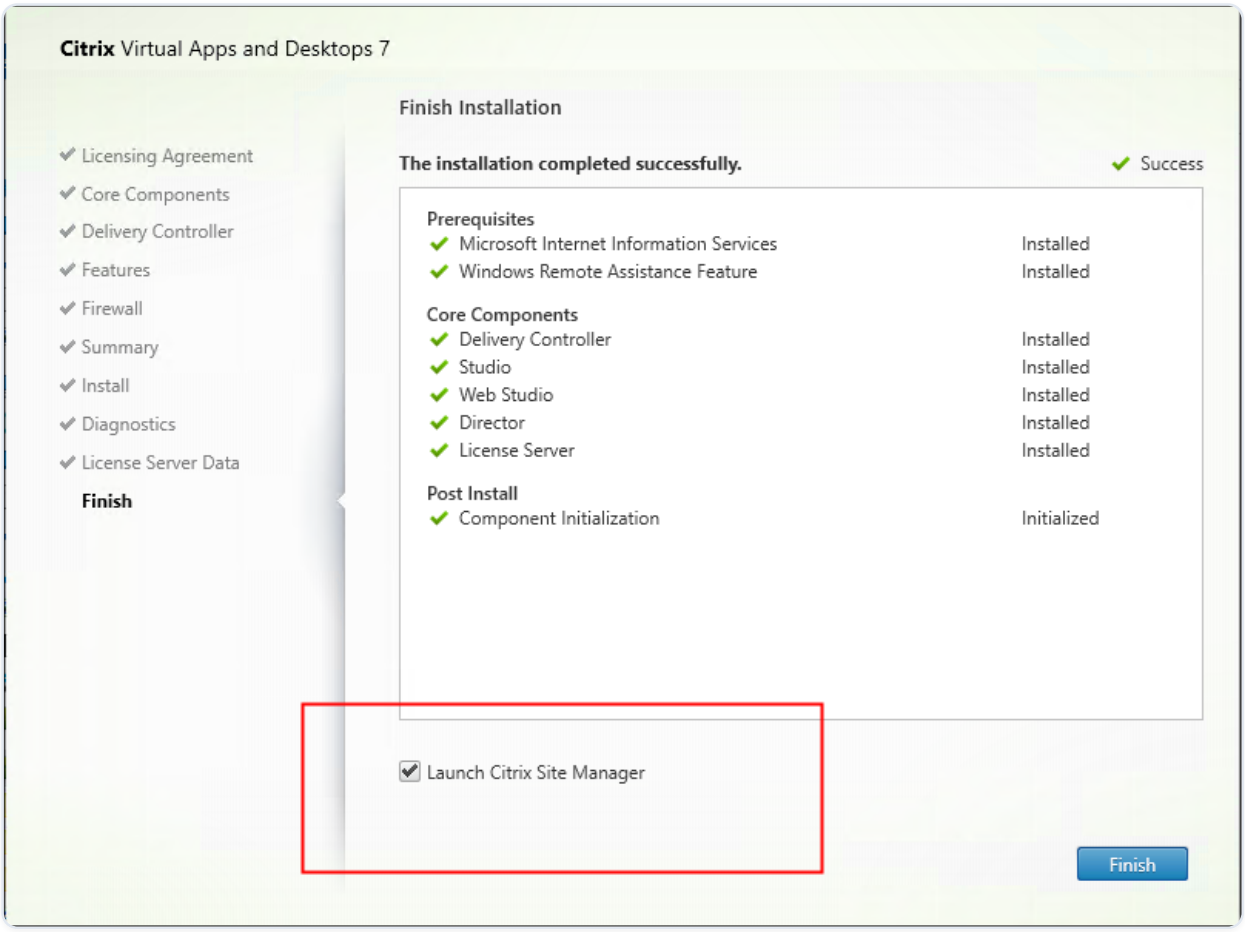
次の情報は、コアコンポーネントのインストールのガイダンスを補足するものです。Web Studioをインストールするには：

- Citrix Virtual Apps and Desktopsのフル製品ISOインストーラーを使用してWeb Studioをインストールします。ISOインストーラーは、前提条件を確認し、不足しているコンポーネントをインストールし、Web Studio Webサイトをセットアップし（Delivery Controllerのインストールに含まれている場合はDelivery Controller上に）、基本的な構成を実行します。
- インストール時にWeb Studioが含まれていなかった場合は、インストーラーを使用してWeb Studioを追加します。
- Web Studioのインストール時に、Delivery ControllerのFQDNを入力するよう求められます。

> **注：**
>
> - 複数のDelivery Controllerを追加できます。Web Studioはランダムな順序でそれらに接続を試みます。Web Studioが接続しようとしているDelivery Controllerに到達できない場合、Web Studioは自動的に他のDelivery Controllerにフォールバックします。
> - **コアコンポーネント**でDirectorが選択され、インストールされている場合、ここで追加するDelivery ControllerはWeb StudioとDirectorの両方で使用されます。
> - Delivery ControllerがTLS用に構成されている場合（推奨）、入力されたFQDNは、Delivery Controllerにインストールされている証明書の共通名またはサブジェクトの別名と一致する必要があります。



- **完了**ページでは、**サイトマネージャーを起動**チェックボックスがデフォルトで選択されており、Citrix Site Managerが自動的に開きます。後で起動するには、デスクトップのスタートメニューを開き、**Citrix > Citrix Site Manager**を選択します。Web Studioを起動する前に、Citrix Site Managerを使用してサイトを作成するか、既存のサイトに参加する必要があります。詳細については、サイトのセットアップを参照してください。



注：

コマンドラインを使用してWeb Studioをインストールすることもできます。例：`.\XenDesktopServerSetup.exe /components webstudio /controllers "ddc1.studio.local" /configure_firewall /quiet`。詳細については、コマンドラインを使用したインストールを参照してください。

TLS 用の証明書を構成する

デフォルトでは、IIS が HTTPS 用にまだ構成されていない場合、インストーラーはサーバーの FQDN を証明書の共通名として使用して自己署名証明書を作成し、ポート 443 にバインドします。この動作により、ユーザーはローカルマシンから Web Studio にアクセスできますが、他のマシンから接続するユーザーは、証明書が信頼されていないためセキュリティ警告が表示されます。この証明書を、エンタープライズまたはパブリック認証局 (CA) によって署名された証明書に置き換えることをお勧めします。詳細については、「Web Studio および Director で TLS を有効にする」を参照してください。IIS で TLS 証明書がすでに構成されている場合、インストーラーは変更を行いません。

サイトをセットアップする

Citrix Virtual Apps and Desktops 展開（サイトとも呼ばれます）をセットアップするには、Citrix Site Manager ツールを使用します。このツールは、Delivery Controller とともに自動的にインストールされます。

サイトをセットアップするには、次の手順に従います。

1. Delivery Controller で、デスクトップのスタートメニューを開き、**Citrix > Citrix Site Manager** を選択します。
2. Citrix Site Manager で、**Create a site** を選択します。サイトセットアップウィザードが表示されます。
3. サイトを作成し、その設定を次のように構成します。
   - **Introduction** ページで、サイトの名前を入力します。
   - **Databases** ページには、サイト、監視、および構成ログデータベースをセットアップするための選択肢が含まれています。詳細については、「手順 3. データベース」を参照してください。
   - **Licensing** ページで、ライセンスサーバーのアドレスを指定し、使用（インストール）するライセンスを示します。詳細については、「手順 4. ライセンス」を参照してください。
4. **Summary** ページで、すべての設定を確認し、**Submit** をクリックします。

   このコントローラーの IP アドレスは、サイトに自動的に追加されます。

> **注：**
>
> サイトを作成したユーザーは、そのサイトのフル管理者になります。詳細については、「委任管理」を参照してください。

サイトの作成後に新しいコントローラーをインストールする場合は、そのコントローラーをサイトに追加する必要があります。詳細な手順は次のとおりです。

1. この新しいControllerでCitrix Site Managerを実行します。
2. **既存のサイトに参加**を選択します。
3. 既にサイトに追加されているControllerのアドレスを入力します。
4. **Submit**をクリックします。

管理のためにDelivery ControllerをWeb Studioに追加する

Studio構成ツールを使用して、管理のためにDelivery ControllerをWeb Studioに追加します。このツールはWeb Studioのインストールフォルダーにあります。

デフォルトでは、このツールは次のデフォルトフォルダーにインストールされます。

- `C:\Program Files\Citrix\Web Studio\Tool\StudioConfig.exe`

Web Studioで管理したいサイトに対して、次の2つのDelivery Controller (`ddc1.studio.local` と `ddc2.studio.local`) を構成するとします。次のPowerShellコマンドを実行します。

- `.\StudioConfig.exe --server "ddc1.studio.local,ddc2.studio.local"`

注：

- このツールにはコンピューターの管理者権限が必要です。
- IISサーバーのキャッシュ設定により、Delivery Controllerの構成変更がすぐに反映されない場合があります。すぐに反映させるには、Web Studioサーバーに移動し、インターネットインフォメーションサービス (IIS) マネージャーを開き、*Server_name* **> Sites > Default Web Site**に移動して、 ペインで**Restart**を選択します。
- 新しいFQDNでDelivery Controllerを再展開する場合、`StudioConfig.exe` を使用してWeb Studioで、および `C:\Program Files\Citrix\Web Studio\Site\assets\json\manifest.json` ファイルでFQDNを更新します。`manifest.json` ファイルを更新しないと、古いFQDNがWeb Studioのサインインウィンドウに表示されたままになります。その結果、サインイン時に代替として新しいFQDNを入力する必要があります。
- サポートされているすべてのパラメーターを表示するには、`StudioConfig.exe --help` を実行します。

(オプション) Web StudioをDelivery Controllerのプロキシとして構成する

デフォルトでは、Web Studioコンソールを使用して展開を管理する場合、Webブラウザーを介してWeb StudioサーバーとDelivery Controllerの両方に接続します。Web StudioサーバーをDelivery Controllerのプロキシとして構成するオプションが提供されています。その結果、展開を管理する際にはWeb Studioサーバーにのみ接続することになります。

このセクションでは、Web StudioサーバーをDelivery Controllerのプロキシとして構成する方法を説明します。Web StudioとDelivery Controllerは異なるサーバーにインストールされていることを前提としています。

開始する前に、必要なすべてのコアコンポーネントが展開環境にインストールされていることを確認してください。詳細については、「コアコンポーネントのインストール」を参照してください。

Web Studio のプロキシモードを有効にするには、次の手順に従います。

1. Web Studio サーバーで、Windows PowerShell を管理者として実行します。
2. 次のコマンドを実行します。`fqdn_of_webstudio_machine` は Web Studio サーバーの FQDN に置き換えてください。

   `& "c:\Program Files\Citrix\Web Studio\Tool\StudioConfig.exe" --enableproxy --proxyserver "fqdn_of_webstudio_machine"`

   > **注：**
   >
   > ロードバランスされた Web Studio 展開環境がある場合は、`fqdn_of_webstudio_machine` をロードバランサーサーバー (仮想サーバーとも呼ばれます) の FQDN に置き換えてください。詳細については、「ロードバランスされた Web Studio 展開環境のセットアップ」を参照してください。

Web Studio のプロキシモードを無効にするには、この PowerShell コマンドを実行します。

```
& "c:\Program Files\Citrix\Web Studio\Tool\StudioConfig.exe" --disableproxy
```

(オプション) Pendo を有効または無効にする

バージョン 2411 以降、Web Studio は Pendo を統合しており、これはデフォルトで有効になっています。Pendo は、Citrix プライバシーポリシー に従って使用状況データを収集します。また、Web Studio の右下隅にアイコンを追加し、コンテキストに応じた機能情報とフィードバックオプションを提供します。使用状況データを共有したくない場合は、Studio 構成ツールを使用して Pendo を無効にできます。

このツールは Web Studio のインストールフォルダーにあります。デフォルトでは、ツールは次のフォルダーにインストールされます: `C:\Program Files\Citrix\Web Studio\Tool\StudioConfig.exe`。

Pendo を無効にするには、次の手順に従います。

1. Web Studio にサインインします。右下隅にアイコンが表示されている場合、Pendo は有効になっています。
2. Web Studio サーバーで、Windows PowerShell を管理者として実行します。 この PowerShell コマンドを実行します。

```
& "c:\Program Files\Citrix\Web Studio\Tool\StudioConfig.exe" --disablependo
```

Pendo を有効にするには、このコマンドを実行します。

```
& "c:\Program Files\Citrix\Web Studio\Tool\StudioConfig.exe" --enablependo
```

Web Studio にサインインする

1. デフォルトのポート番号 443 が使用されている場合は、`https://<address of the server hosting Web Studio>/Citrix/Studio` で Web Studio にアクセスします。別のポートが構成されている 場合は、`https://<address of the server hosting Web Studio>:<port number>/Citrix/Studio` を使用します。

   Web StudioにDelivery Controllerを(#add-delivery-controllers-to-web-studio-for-management)追加しており、それらに到達可能な場合、サインインページが表示されます。

   > **注：**
   >
   > 以下の場合は、**サインインできません**ページが表示されます。
   >
   > - サイトにDelivery Controllerが指定されていません。接続するためにDelivery Controllerを追加するよう求められます。
   > - 指定されたDelivery Controllerに到達できません。接続を確認するには、**テスト**をクリックします。または、代替のDelivery Controllerを入力して**接続**をクリックします。

2. **ユーザー名**、**パスワード**、**ドメイン**を入力します。
3. **サインイン**をクリックします。

次のステップ

1. VDAのインストール
2. Web Studioを使用して、次の方法で仮想アプリとデスクトップをユーザーに配信します。
    a. マシンカタログを作成する(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/install-configure/machine-catalogs-create.html)
    b. デリバリーグループを作成する(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/install-configure/delivery-groups-create.html)
    c. アプリケーショングループを作成する（オプション）(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/install-configure/application-groups-create.html)

コマンドラインを使用したインストール

> **重要:**
>
> - アップグレード中で、現在のバージョンでPersonal vDiskまたはAppDisksソフトウェアが使用されているかインストールされている場合は、「PvD、AppDisks、およびサポートされていないホストの削除」を参照してください。
> - Citrixは、ライセンスコンプライアンスを含む正当な利益のために、必要に応じて基本的なライセンスデータを収集します。詳細については、「Citrixライセンスデータ」を参照してください。

はじめに

この記事は、Windowsオペレーティングシステムを搭載したマシンにコンポーネントをインストールする場合に適用されます。Linuxオペレーティングシステム用VDAについては、「Linux Virtual Delivery Agent」を参照してください。

この記事では、製品のインストールコマンドを発行する方法について説明します。インストールを開始する前に、「インストールの準備」を確認してください。この記事には、利用可能なインストーラーの説明が含まれています。

コマンドの実行状況と戻り値を確認するには、元の管理者であるか、**管理者として実行**を使用する必要があります。詳細については、Microsoftのコマンドドキュメントを参照してください。

インストールコマンドを直接使用することに加えて、Active Directory内のマシンにVDAをインストール、アップグレード、または削除するサンプルスクリプトが製品ISOに用意されています。詳細については、「スクリプトを使用したVDAのインストール」を参照してください。

このCitrix Virtual Apps and Desktopsのバージョンでサポートされていないバージョンにインストールまたはアップグレードしようとすると、オプションに関する情報を示すメッセージが表示されます。「以前のオペレーティングシステム」を参照してください。

Citrixがコンポーネントインストールの結果を報告する方法については、「Citrixインストールのリターンコード」を参照してください。

フルプロダクトインストーラーを使用する

フルプロダクトインストーラーのコマンドラインインターフェイスにアクセスするには：

1. Citrixから製品パッケージをダウンロードします。ダウンロードサイトにアクセスするには、Citrixアカウントの資格情報が必要です。
2. ファイルを解凍します。必要に応じて、ISOファイルをDVDに書き込みます。
3. ローカル管理者アカウントを使用して、コンポーネントをインストールするサーバーにログオンします。
4. DVDをドライブに挿入するか、ISOファイルをマウントします。
5. メディア上の `\x64\XenDesktop Setup` ディレクトリから、適切なコマンドを実行します。

   コアコンポーネントをインストールするには： コアコンポーネントのインストールに関するコマンドラインオプションに記載されているオプションを使用して、`XenDesktopServerSetup.exe` を実行します。

   VDAをインストールするには： VDAのインストールに関するコマンドラインオプションに記載されているオプションを使用して、`XenDesktopVDASetup.exe` を実行します。

   StoreFrontをインストールするには： インストールメディアの `x64 > StoreFront` フォルダーで `CitrixStoreFront-x64.exe` を実行します。

   Universal Print Serverをインストールするには： Universal Print Serverのインストールに関するコマンドラインオプションのガイダンスに従ってください。

   Federated Authentication Serviceをインストールするには： Citrixでは、グラフィカルインターフェイスを使用することをお勧めします。

   Session Recordingをインストールするには： Session Recordingのガイダンスに従ってください。

Workspace Environment Managementをインストールするには： Workspace Environment Managementのガイダンスに従ってください。

Secure Private Accessをインストールするには： インストールメディアの `x64 > XenDesktop` Setupフォルダーで `XenDesktopSPASetup.exe` を実行します。Secure Private Accessのインストールに関するコマンドラインオプションのガイダンスに従ってください。

コアコンポーネントをインストールするためのコマンドラインオプション

`XenDesktopServerSetup.exe` コマンドでコアコンポーネントをインストールする場合、以下のパラメーターオプションが有効です。オプションの詳細については、コアコンポーネントのインストールを参照してください。

注：

- コアコンポーネントをインストールするためのコマンドラインオプションを使用している間は、`/exclude` を使用しないでください。
- `/components` を使用して1つのコンポーネントをアップグレードすると、他のコンポーネントもアップグレードされる場合があります。これは、異なるコンポーネント間の互換性の問題を回避するためです。
- 1つのコンポーネントのみをアップグレードする場合は、そのコンポーネントの個別のインストーラーを使用してください。展開のアップグレードを参照してください。

- ***/ceipoptin*** *ceipoptin など.*

  Call Home データとカスタマーエクスペリエンス向上プログラム (CEIP) データの収集を有効にします。有効な値は次のとおりです。

  - `DIAGNOSTIC`: Citrix Licensing が Call Home データを収集できるようにするには、この値を選択します。
  - `ANONYMOUS`: Citrix Licensing が未識別の CEIP データ (ユーザーを特定しないデータ) を収集できるようにするには、この値を選択します。
  - `NONE`: Citrix Licensing による CEIP データの収集を無効にするには、この値を選択します。

  Call Home データ収集の詳細については、「Citrix Licensing Call Home」を参照してください。

CEIP データ収集の詳細については、「Citrix Licensing Customer Experience Improvement Program」を参照してください。

CEIP データの詳細については、「Citrix Licensing CEIP data elements」を参照してください。

ライセンスサーバーのライセンスデータの詳細については、「Citrix Licensing Data」を参照してください。

- **/components** *コンポーネント* ...

  インストールまたは削除するコンポーネントのコンマ区切りリスト。有効な値は次のとおりです。

  - `CONTROLLER`: コントローラー
  - `DESKTOPSTUDIO`: スタジオ
  - `WEBSTUDIO`: ウェブスタジオ
  - `DESKTOPDIRECTOR`: ディレクター
  - `LICENSESERVER`: Citrixライセンスサーバー
  - `SECUREPRIVATEACCESS`: セキュアプライベートアクセス

  このオプションが省略された場合、すべてのコンポーネントがインストールされます (または、`/remove` オプションも指定されている場合は削除されます)。

  (2003より前のリリースでは、有効な値には`STOREFRONT`が含まれていました。バージョン2003以降では、Use the full-product installerで言及されている専用のStoreFrontインストールコマンドを使用してください。).

- **/configure_firewall**

  Windows ファイアウォールサービスが実行されている場合、ファイアウォールが有効になっていなくても、インストールされるコンポーネントが使用するWindows ファイアウォールのすべてのポートを開きます。サードパーティのファイアウォールを使用している場合、またはファイアウォールを使用していない場合は、ポートを手動で開く必要があります。

- **/ディスエーブルエクスペリエンスメトリクス**

  インストール、アップグレード、または削除中に収集された分析データがCitrixに自動的にアップロードされるのを防ぎます。

- **/help** または **/h**

  コマンドのヘルプを表示します。

- **/ignore_hw_check_failure**

  ハードウェアチェックが失敗した場合 (たとえば、RAM不足のため) でも、Delivery Controllerのインストールまたはアップグレードを続行できるようにします。詳細については、Hardware checkを参照してください。

- **/ignore_site_test_failure**

  Controllerのアップグレード中にのみ有効です。通常、サイトテストの失敗はすべて無視され、アップグレードが続行されます。省略された場合 (またはfalseに設定された場合)、サイトテストの失敗があると、アップグレードを実行せずにインストーラーが失敗します。デフォルト = false

  アップグレード中に、サポートされていないSQL Serverバージョンが検出された場合、このオプションは無視されます。詳細については、SQL Server version checkを参照してください。

- **/installdir *ディレクトリ***

  コンポーネントがインストールされる既存の空のディレクトリ。デフォルト = `c:\Program Files\Citrix`。

- **/logpath *パス***

  ログファイルの場所。指定されたフォルダーは存在している必要があります。インストーラーは作成しません。デフォルト = `TEMP%\Citrix\XenDesktop Installer`

- **/no_remote_assistance**

  Director のインストール時にのみ有効です。Windows リモートアシスタンスを使用するユーザーシャドウイング機能を無効にします。

- **再起動なし**

  インストール後の再起動を防止します。(ほとんどのコアコンポーネントでは、再起動はデフォルトで有効になっていません。)

- **再開しない**

  デフォルトでは、インストール中にマシンの再起動が必要な場合、再起動が完了するとインストーラーは自動的に再開します。デフォルトを上書きするには、`/noresume`を指定します。これは、メディアを再マウントする必要がある場合や、自動インストール中に情報を取得したい場合に役立ちます。

- **SQLなし**

Controller をインストールするサーバーへの Microsoft SQL Server Express のインストールを防止します。このオプションを省略すると、サイトデータベースとして使用するために SQL Server Express がインストールされます。

このオプションは、ローカルホストキャッシュに使用される SQL Server Express LocalDB のインストールには影響しません。

- **サイレント** または **パッシブ**

  インストール中にユーザーインターフェイスは表示されません。インストールプロセスの唯一の証拠は、Windows タスクマネージャーにあります。このオプションを省略すると、グラフィカルインターフェイスが起動します。

- **/削除**

  `/components` オプションで指定されたコアコンポーネントを削除します。

- **/すべて削除**

  インストールされているすべてのコアコンポーネントを削除します。

- **/SKIPHDXDRIVERCHECK**

  VDA Meta-installer への HDX™ ドライバーのチェックをスキップします。

- **/エクスペリエンスメトリックを送信**

  インストール、アップグレード、または削除中に収集された分析データを Citrix に自動的に送信します。このオプションを省略した場合 (または `/disableexperiencemetrics` が指定されている場合)、分析データはローカルで収集されますが、自動的には送信されません。

- **一時ディレクトリ** *directory*

  インストール中に一時ファイルを保持するディレクトリ。デフォルト = `c:\Windows\Temp`。

- **ゼナップ**

  Citrix Virtual Apps をインストールします。このオプションを省略すると、Citrix Virtual Apps and Desktops™ がインストールされます。

コアコンポーネントのインストール例

次のコマンドは、サーバーにDelivery Controller™、Studio、Citrix Licensing、およびSQL Server Expressをインストールします。コンポーネント通信に必要なファイアウォールポートは自動的に開かれます。

`\x64\XenDesktop Setup\XenDesktopServerSetup.exe /components controller,desktopstudio,licenseserver /configure_firewall`

次のコマンドは、サーバーにCitrix Virtual Apps™ Controller、Studio、およびSQL Server Expressをインストールします。コンポーネント通信に必要なファイアウォールポートは自動的に開かれます。

`\x64\XenDesktop Setup\\XenDesktopServerSetup.exe /xenapp /components controller,desktopstudio /configure_firewall`

次のコマンドは、サーバーにDelivery Controller、Secure Private Access、およびSQL Server Expressをインストールします。コンポーネント通信に必要なファイアウォールポートは自動的に開かれます。

`\x64\XenDesktop Setup XenDesktopServerSetup.exe /xenapp /components controller,secureprivateaccess /configure_firewall`

スタンドアロンVDAインストーラーを使用する

ダウンロードサイトにアクセスするには、Citrixアカウントの資格情報が必要です。インストールを開始する前に、管理者権限を昇格させるか、**管理者として実行**を使用する必要があります。

1. Citrixから適切なパッケージをダウンロードします。
   - マルチセッションOS Virtual Delivery Agent: `VDAServerSetup_xxxx.exe`
   - シングルセッションOS Virtual Delivery Agent: `VDAWorkstationSetup_xxxx.exe`
   - シングルセッションOS Core Services Virtual Delivery Agent: `VDAWorkstationCoreSetup_xxxx.exe`
2. まず、パッケージから既存のディレクトリにファイルを抽出し、その後インストールコマンドを実行するか、単にパッケージを実行します。

   ファイルをインストールする前に抽出するには、絶対パスを指定して`/extract`を使用します（例: `C:\YourExtractFolder\VDAWorkstationCoreSetup.exe /extract %temp%\CitrixVDAInstallMedia`）。ディレクトリは存在している必要があります。存在しない場合、抽出は失敗します。その後、別のコマンドで、この記事に記載されている有効なオプションを使用して、適切なコマンドを実行します。

   - `VDAServerSetup_XXXX.exe` の場合は、`<extract folder>\Extract\Image-Full\x64\XenDesktop Setup\XenDesktopVDASetup.exe` を実行します

- `VDAWorkstationCoreSetup_XXXX.exe` の場合は、`<extract folder>\Extract\Image-Full\x64\XenDesktop Setup\XenDesktopRemotePCSetup.exe` を実行します
- `VDAWorkstationSetup_XXXX.exe` の場合は、`<extract folder>\Extract\Image-Full\x64\XenDesktop Setup\XenDesktopVDASetup.exe` を実行します

ダウンロードしたパッケージを実行するには、その名前（`VDAServerSetup.exe`、`VDAWorkstationSetup.exe`、または`VDAWorkstationCoreSetup.exe`）を実行します。この記事に記載されている有効なオプションを使用してください。

フル製品インストーラーに慣れている場合:

- スタンドアロンの`VDAServerSetup.exe`または`VDAWorkstationSetup.exe`インストーラーを、名前以外はすべて`XenDesktopVdaSetup.exe`コマンドであるかのように実行します。
- 「`VDAWorkstationCoreSetup.exe`」インストーラーは、他のインストーラーで利用できるオプションのサブセットをサポートしているため、異なります。

VDA をインストールするためのコマンドラインオプション

以下のオプションは、次のコマンド (インストーラー) のいずれかまたは複数で有効です: `VDAServerSetup_xxxx.exe`、`VDAWorkstationSetup_xxxx.exe`、および `VDAWorkstationCoreSetup_xxxx.exe`。

オプションの詳細については、「VDA のインストール」を参照してください。

- **/コンポーネント** *コンポーネント*\[,*コンポーネント*\]

  インストールまたは削除するコンポーネントのコンマ区切りリスト。有効な値は次のとおりです。

  - `VDA`: バーチャル デリバリー エージェント
  - `PLUGINS`: Windows 用 Citrix Workspace™ アプリ

  VDA と Windows 用 Citrix Workspace アプリをインストールするには、`/components vda,plugins` を指定するか、コンポーネントをまったく指定しないでください。コンポーネントが指定されていない場合、デフォルトでは VDA のみがインストールされます。

  VDA のみをインストールし、Citrix Workspace アプリのインストールを除外するには、`/components vda` を指定します。

  このオプションは、`VDAWorkstationCoreSetup_xxxx.exe` インストーラーを使用する場合は無効です。そのインストーラーでは Citrix Workspace アプリをインストールできません。

- **/controllers** "*コントローラー\[コントローラー\]*"

  VDA が通信できるコントローラーのスペース区切りの FQDN を、半角の引用符で囲んで指定します。`/site_guid` と `/controllers` の両方のオプションを指定しないでください。

- **/ディスエーブルエクスペリエンスメトリクス**

  インストール、アップグレード、または削除中に収集された分析がCitrixに自動的にアップロードされるのを防ぎます。

- **/enable_hdx_ports**

  Windows ファイアウォールサービスが検出された場合、ファイアウォールが有効になっていなくても、VDAおよび有効な機能（Windows リモートアシスタンスを除く）に必要なポートをWindows ファイアウォールで開きます。別のファイアウォールを使用している場合、またはファイアウォールを使用していない場合は、ファイアウォールを手動で構成する必要があります。ポート情報については、ネットワークポートを参照してください。

  HDX アダプティブトランスポートが使用する UDP ポートを開くには、この `/enable_hdx_ports` オプションに加えて、`/enable_hdx_udp_ports` オプションを指定します。

- **/enable_hdx_udp_ports**

  Windows ファイアウォールサービスが検出された場合、ファイアウォールが有効になっていなくても、HDX アダプティブトランスポートが使用する Windows ファイアウォールの UDP ポートを開きます。別のファイアウォールを使用している場合、またはファイアウォールを使用していない場合は、ファイアウォールを手動で構成する必要があります。ポート情報については、「ネットワークポート」を参照してください。

  VDAが使用する追加ポートを開くには、この`/enable_hdx_udp_ports`オプションに加えて、`/enable_hdx_ports`オプションを指定します。

- **/enable_hdx_tls_dtls**

  HDX Direct V1用にTCPおよびUDPポート443を開きます。

- **/enable_real_time_transport**

  オーディオパケットにUDPを使用するかどうかを有効または無効にします（オーディオ用のRealTime Audio Transport）。この機能を有効にすると、オーディオパフォーマンスが向上する可能性があります。Windowsファイアウォールサービスが検出されたときにUDPポートを自動的に開く場合は、`/enable_hdx_ports`オプションを含めます。

- **/enable_remote_assistance**

Directorで使用するために、Windowsリモートアシスタンスのシャドウイング機能を有効にします。このオプションを指定すると、Windowsリモートアシスタンスはファイアウォールで動的ポートを開きます。

- **/enablerestore** または **/enablerestorecleanup**

  （シングルセッションVDAにのみ有効）VDAのインストールまたはアップグレードが失敗した場合に、復元ポイントへの自動復帰を有効にします。

  インストール/アップグレードが正常に完了した場合：

  - `/enablerestorecleanup`は、インストーラーに復元ポイントを削除するよう指示します。
  - `/enablerestore`は、使用されなかった場合でも、復元ポイントを保持するようにインストーラーに指示します。

  詳細については、インストールまたはアップグレードの失敗時の復元を参照してください。

- **/enable_ss_ports**

  Windows ファイアウォールサービスが検出された場合、ファイアウォールが有効になっていなくても、画面共有に必要なポートをWindows ファイアウォールで開きます。別のファイアウォールを使用している場合、またはファイアウォールを使用していない場合は、手動でファイアウォールを構成する必要があります。

- **/exclude** "*コンポーネント*"\[,"*コンポーネント*"\]

  1つ以上のコンマ区切りのオプションコンポーネントのインストールを防止します。各コンポーネントは、ストレート引用符で囲まれています。たとえば、MCSによって管理されていないイメージにVDAをインストールまたはアップグレードする場合、Machine Identity Serviceコンポーネントは必要ありません。有効な値は次のとおりです。

マルチセッションOS	シングルセッションOS	シングルセッションOSコアサービス
`Citrix App Protection Component`	`Citrix App Protection Component`	`Citrix App Protection Component`
`Citrix Authentication Identity Assertion VDA Plug-in`	`Citrix Authentication Identity Assertion VDA Plug-in`	`Citrix Authentication Identity Assertion VDA Plug-in`

マルチセッションOS	シングルセッションOS	シングルセッションOSコアサービス
Citrix Backup and Restore	Citrix Backup and Restore	
Citrix Browser Content Redirection	Citrix Browser Content Redirection	Citrix Browser Content Redirection
Citrix HyperV Filter Driver	Citrix HyperV Filter Driver	
Citrix MCS IODriver	Citrix MCS IODriver	
Citrix Personalization for App-V - VDA	Citrix Personalization for App-V - VDA	Citrix Personalization for App-V - VDA
Citrix Profile Management	Citrix Profile Management	
Citrix Profile Management WMI Plug-in	Citrix Profile Management WMI Plug-in	
Citrix Rendezvous V2	Citrix Rendezvous V2	
Citrix Telemetry Service	Citrix Telemetry Service	Citrix Telemetry Service
Citrix Universal Print Client	Citrix Universal Print Client	Citrix Universal Print Client
Citrix Vda Log Capture Service	Citrix Vda Log Capture Service	Citrix Vda Log Capture Service
Citrix VDA Upgrade Agent	Citrix VDA Upgrade Agent	
CSE Component	CSE Component	CSE Component
Director VDA Plug-in	Director VDA Plug-in	Director VDA Plug-in
Machine Identity Service	Machine Identity Service	

マルチセッションOS	シングルセッションOS	シングルセッションOSコアサービス
`Machine Management Provider`	`Machine Management Provider`	`Machine Management Provider`
	`User Personalization Layer`	
`VDA Monitor Plug-in`	`VDA Monitor Plug-in`	`VDA Monitor Plug-in`
`VDA WMI Proxy Plug-in`	`VDA WMI Proxy Plug-in`	`VDA WMI Proxy Plug-in`

Citrix Profile Managementをインストールから除外する（`/exclude "Citrix Profile Management"`）と、Citrix DirectorでのVDAの監視とトラブルシューティングに影響します。**ユーザー詳細**ページと**エンドポイント**ページでは、パーソナライゼーションパネルとログオン期間パネルが機能しません。**ダッシュボード**ページと**トレンド**ページでは、平均ログオン期間パネルはProfile Managementがインストールされているマシンのみのデータを表示します。

サードパーティのユーザープロファイル管理ソリューションを使用している場合でも、Citrixは Citrix Profile Management Serviceをインストールして実行することを推奨します。Citrix Profile Management Serviceを有効にする必要はありません。

`/exclude`と`/includeadditional`の両方を同じコンポーネント名で指定した場合、そのコンポーネントはインストールされません。

このオプションは、`VDAWorkstationCoreSetup.exe`インストーラーを使用している場合は無効です。このインストーラーは、これらの項目の多くを自動的に除外します。

- **/h** または **/help**

  コマンドのヘルプを表示します。

- **/includeadditional** "*コンポーネント*"\[,"*コンポーネント*"\]

  1つ以上のコンマ区切りのオプションコンポーネントのインストールを含めます。各コンポーネントは、ストレート引用符で囲まれています。このオプションは、リモートPCアクセス展開を作成し、デフォルトで含まれていない他のコンポーネントをインストールしたい場合に役立ちます。有効な値は次のとおりです。

マルチセッションOS	シングルセッションOS
`Citrix Backup and Restore`	`Citrix Backup and Restore`
`Citrix MCS IODriver`	`Citrix MCS IODriver`
`Citrix Personalization for App-V - VDA`	`Citrix Personalization for App-V - VDA`
`Citrix Profile Management`	`Citrix Profile Management`
`Citrix Profile Management WMI Plug-in`	`Citrix Profile Management WMI Plug-in`
`Citrix Rendezvous V2`	`Citrix Rendezvous V2`
`Citrix VDA Upgrade Agent`	`Citrix VDA Upgrade Agent`
`Citrix Web Socket Vda Registration Tool`	`Citrix Web Socket Vda Registration Tool`
`Machine Identity Service`	`Machine Identity Service`
	`User Personalization Layer`

`/exclude` と `/includeadditional` の両方を同じコンポーネント名で指定した場合、そのコンポーネントはインストールされません。

- **/installdir** *ディレクトリ*

  既存の空のディレクトリにコンポーネントがインストールされます。デフォルト = `c:\Program Files\Citrix`。

- **/install_mcsio_driver**

  使用しないでください。代わりに `/includeadditional "Citrix MCS IODriver"` または `/exclude "Citrix MCS IODriver"` を使用してください。

- **/logpath** *パス*

  ログファイルの場所。指定されたフォルダーは存在している必要があります。インストーラーは作成しません。デフォルト = "`%TEMP%\Citrix\XenDesktop Installer`"

  このオプションはグラフィカルインターフェイスでは利用できません。

- **/マスターイメージ**

  VMにVDAをインストールする場合にのみ有効です。他のマシンを作成するために使用されるイメージとしてVDAをセットアップします。このオプションは`/mastermcsimage`と同等です。

  このオプションは、`VDAWorkstationCoreSetup_xxxx.exe`インストーラーを使用している場合は無効です。

- **/マスターMCSイメージ**

  このマシンがMachine Creation Servicesでイメージとして使用されることを指定します。このオプションは`/masterimage`と同等です。

- **/マスターPVSイメージ**

  このマシンが、Citrix Provisioning™またはサードパーティのプロビジョニングツール（Microsoft System Center Configuration Managerなど）を使用してVMをプロビジョニングするためのイメージとして使用されることを指定します。

- **/websockettoken** *WebSocketトークン*

  Web Socket VDAを作成します。WebSocketTokenは、必要なトークン用です。

- **/no_mediafoundation_ack**

  Microsoft Media Foundationがインストールされていないことを確認し、いくつかのHDXマルチメディア機能がインストールされず、動作しないことを承認します。このオプションが省略され、Media Foundationがインストールされていない場合、前提条件が満たされていないため、VDAのインストールは終了します。ほとんどのサポートされているWindowsエディションには、Nエディションを除いて、Media Foundationがすでにインストールされています。Windowsの機能 > メディア機能 を *手動* で 有効にした場合、Citrix Meta Installerが探すレジストリキーに値が設定されていない可能性があります。インストールプロセスを開始する前に、`SOFTWARE\Microsoft\Windows\CurrentVersion\Setup\Windows-Features\WindowsMediaVersion` レジストリキーをチェックして、値が存在し、空ではないことを確認してください。

- **デスクトップエクスペリエンスなし**

  拡張デスクトップエクスペリエンス機能は利用できなくなりました。このオプション（およびポリシー設定）は、指定されても無視されます。

マルチセッションOS用のVDAをインストールする場合にのみ有効です。拡張デスクトップエクスペリエンス機能の有効化を防止します。この機能は、拡張デスクトップエクスペリエンスCitrixポリシー設定でも制御されます。

- **再起動なし**

  インストール後の再起動を防止します。VDAは再起動するまで使用できません。

- **再開しない**

  デフォルトでは、インストール中にマシンの再起動が必要な場合、再起動が完了するとインストーラーは自動的に再開します。デフォルトを上書きするには、`/noresume`を指定します。これは、メディアを再マウントする必要がある場合や、自動インストール中に情報を取得したい場合に役立ちます。

- **物理マシン**

  RemotePCインストールの場合、この引数を`/remotepc`とともに使用してください。そうしないと、特定のユーザーシナリオでVDAが期待どおりに動作しない可能性があります。

- **ポート番号** *port*

  `/reconfig`オプションが指定されている場合にのみ有効です。VDAとController間の通信を有効にするポート番号。以前に構成されたポートは、ポート80でない限り無効になります。

- **/proxyconfig** "*アドレスまたはPACファイルパス*"

  環境でGateway ServiceなどのサービスとRendezvous V2プロトコルを使用する予定があり、アウトバウンド接続のためにネットワークに非透過型プロキシがある場合は、ここでプロキシを指定します。HTTPプロキシのみがサポートされています。Rendezvousプロトコルで使用するプロキシのアドレスまたはPACファイルパス。機能の詳細については、Rendezvous protocolを参照してください。

  - プロキシアドレスの形式: `http://<url-or-ip>:<port>`
  - PACファイルの形式: `http://<url-or-ip>:<port>/<path>/<filename>.pac`

- **サイレント** または **パッシブ**

  インストール中にユーザーインターフェイスは表示されません。インストールと構成プロセスの唯一の証拠は、Windowsタスクマネージャーにあります。このオプションを省略すると、グラフィカルインターフェイスが起動します。

- **/再構成**

`/portnumber`、`/controllers`、または`/enable_hdx_ports`オプションと組み合わせて使用すると、以前に構成されたVDA設定をカスタマイズします。このオプションを`/quiet`オプションも指定せずに指定すると、VDAをカスタマイズするためのグラフィカルインターフェイスが起動します。

- **/リモートPC**

  Remote PC Access展開（シングルセッションOS）またはブローカー接続（マルチセッションOS）の場合にのみ有効です。追加コンポーネントのインストールを除外します（`/exclude`および`/includeadditional`オプションのコンポーネントリストを参照）。

  このオプションは、`VDAWorkstationCoreSetup.exe`インストーラーを使用する場合は無効です。そのインストーラーは、これらのコンポーネントのインストールを自動的に除外します。

  `/remotepc` は `/servervdi` オプションと互換性がありません。

- **/削除**

  `/components`オプションで指定されたコンポーネントを削除します。

- **/remove_appdisk_ack**

  AppDisks™ VDAプラグインがインストールされている場合、VDAインストーラーがそれをアンインストールすることを承認します。

- **/remove_pvd_ack**

  Personal vDiskがインストールされている場合、VDAインストーラーがそれをアンインストールすることを承認します。

- **/すべて削除**

  VDAを削除します。Citrix Workspaceアプリ（インストールされている場合）は削除しません。

- **/REMOVEALLWITHCWA**

  VDA とともに CWA を削除します。

- **/エクスペリエンスメトリックを送信**

  インストール、アップグレード、または削除中に収集された分析データをCitrixに自動的に送信します。このオプションが省略された場合（または`/disableexperiencemetrics`オプションが指定された場合）、分析データはローカルで収集されますが、自動的には送信されません。

- **サーバーVDI**

  サポートされている Windows マルチセッションマシンにシングルセッション OS 用 VDA をインストールします。Windows マルチセッションマシンにマルチセッション OS 用 VDA をインストールする場合は、このオプションを省略してください。

  このオプションを使用する前に、Server VDI を参照してください。

  このオプションは、フルプロダクト VDA インストーラーでのみ使用してください。

- **サイトGUID** *guid*

  サイトのActive Directory組織単位（OU）のグローバル一意識別子。これは、検出にActive Directoryを使用している場合に、仮想デスクトップをサイトに関連付けます（自動更新が推奨されるデフォルトの検出方法です）。サイトGUIDは、Studioに表示されるサイトプロパティです。`/site_guid`と`/controllers`の両方のオプションを指定しないでください。

- **一時ディレクトリ** *directory*

  インストール中に一時ファイルを保持するディレクトリ。デフォルト = `c:\Windows\Temp`。

  このオプションはグラフィカルインターフェイスでは利用できません。

- **仮想マシン**

  VDAをVMにインストールする場合にのみ有効です。BIOS情報がVMに渡されることで物理マシンとして表示される、インストーラーによる物理マシンの検出を上書きします。

  このオプションはグラフィカルインターフェイスでは利用できません。

- **XenDesktopクラウド**

  VDAがCitrix DaaS (Citrix Cloud™) 展開にインストールされていることを示します。

VDA のインストール例

フルプロダクトインストーラーで VDA をインストールする:

次のコマンドは、シングルセッション OS 用 VDA と Citrix Workspace アプリを、VM のデフォルトの場所にインストールします。この VDA はイメージとして使用され、MCS を使用して VM をプロビジョニングします。VDA は、`mydomain` ドメイン内の `Contr-Main` という名前のサーバー上の Controller に最初に登録されます。VDA はユーザーパーソナライゼーションレイヤーと Windows リモートアシスタンスを使用します。

```
\x64\XenDesktop Setup\XenDesktopVdaSetup.exe /quiet /components vda,plugins /
controllers "Contr-Main.mydomain.local" /enable_hdx_ports /includeadditional
"user personalization layer" /mastermcsimage /enable_remote_assistance
```

VDAWorkstationCoreSetup スタンドアロンインストーラーでシングルセッション OS VDA をインストールする:

次のコマンドは、リモート PC アクセスまたは VDI 展開で使用するために、シングルセッション OS にコアサービス VDA をインストールします。Citrix Workspace アプリおよびその他の非コアサービスはインストールされません。Controller のアドレスが指定され、Windows ファイアウォールサービス内のポートは自動的に開かれます。管理者が再起動を処理します。

```
VDAWorkstationCoreSetup .exe /quiet /controllers "Contr-East.domain.com" /
enable_hdx_ports /noreboot
```

VDAをカスタマイズする

VDA をインストールした後、いくつかの設定をカスタマイズできます。製品メディアの `\x64\XenDesktop Setup` ディレクトリから、VDA のインストールに関するコマンドラインオプション で説明されている次のオプションのいずれかまたは複数を使用して、`XenDesktopVdaSetup.exe` を実行します。

- `/reconfigure` (VDAをカスタマイズする際に必須)
- `/h` または `/help`
- `/quiet`
- `/noreboot`
- `/controllers`
- `/portnumber port`
- `/enable_hdx_ports`

VDA のトラブルシューティング

- デリバリーグループの Studio 表示で、**詳細**ペインの**インストール済み VDA バージョン**エントリが、マシンにインストールされているバージョンと異なる場合があります。マシンの Windows のプログラムと機能の表示には、実際の VDA バージョンが表示されます。
- VDAをインストールした後、それがDelivery Controllerに登録されるまで、ユーザーにアプリやデスクトップを提供することはできません。

VDA登録方法と登録問題のトラブルシューティングについては、「VDA登録」を参照してください。

Universal Print Serverをインストールするためのコマンドラインオプション

次のオプションは、`XenDesktopPrintServerSetup.exe`コマンドで有効です。

- **/enable_upsserver_port**

このオプションが指定されていない場合、インストーラーはグラフィカルインターフェイスから**Firewall**ページを表示します。インストーラーにWindowsファイアウォールルールを自動的に追加させるには**Automatically**を選択し、管理者がファイアウォールを手動で構成する場合は**Manually**を選択します。

プリントサーバーにソフトウェアをインストールした後、「プリンターのプロビジョニング」のガイダンスを使用してUniversal Print Serverを構成します。

Secure Private Accessをインストールするためのコマンドラインオプション

次のオプションは、以下で有効です。

1. CVADインストーラー: `XenDesktopSPASetup.exe`
2. SPAオンプレミスインストーラー: `SecurePrivateAccessSetup_XXXX.exe`

- **/enable_spa_ports**

  Windowsファイアウォールサービスが検出された場合、ファイアウォールが有効になっていなくても、Secure Private Accessに必要なWindowsファイアウォールのポートを開きます。別のファイアウォールを使用している場合、またはファイアウォールを使用していない場合は、ファイアウォールを手動で構成する必要があります。ポート情報については、「ネットワークポート」を参照してください。

- **ノーSQL**

  Secure Private Accessをインストールするサーバーへの Microsoft SQL Server Expressのインストールを防止します。このオプションを省略すると、サイトデータベースとして使用するためにSQL Server Expressがインストールされます。

- **/help または /h または /?**

  コマンドのヘルプを表示します

- **再起動なし**

インストール後の再起動を防止します。再起動するまでSecure Private Accessは使用できません。

- **/quiet または /passive**

  インストール中にユーザーインターフェイスは表示されません。インストールと構成プロセスの唯一の証拠は、Windowsタスクマネージャーにあります。このオプションを省略すると、グラフィカルインターフェイスが起動します。

- **/削除**

  Secure Private Accessを削除します。

オプションの詳細については、Secure Private Accessインストーラーを参照してください。

詳細情報

Citrixがコンポーネントインストールの結果を報告する方法については、Citrixインストールのリターンコードを参照してください。

VDAのインストール

> **重要:**
>
> - アップグレード中で、現在のバージョンにPersonal vDiskまたはAppDisksソフトウェアがインストールされている場合は、PvD、AppDisks、およびサポートされていないホストの削除を参照してください。
> - Citrix®によって配布されるバイナリは署名されています。署名されたバイナリは、Citrixが生成した証明書または信頼できるサードパーティの証明書によって検証されていることを示します。

> Windowsマシン用のVDAには、マルチセッションOS用VDAとシングルセッションOS用VDAの2種類があります。(Linuxマシン用VDAについては、Linux Virtual Delivery Agentドキュメントを参照してください。)

インストールを開始する前に、インストールの準備を確認し、すべての準備タスクを完了してください。

VDAをインストールする前に、コアコンポーネントをインストールします。VDAをインストールする前にサイトを作成することもできます。

この記事では、VDAをインストールする際のインストールウィザードのシーケンスについて説明します。コマンドラインでの同等の操作も提供されています。詳細については、コマンドラインを使用したインストールを参照してください。

ステップ1. 製品ソフトウェアをダウンロードしてウィザードを起動する

フル製品インストーラーを使用している場合:

1. 製品ISOをまだダウンロードしていない場合:
   - Citrixアカウントの資格情報を使用して、Citrix Virtual Apps and Desktops™ダウンロードページにアクセスします。製品ISOファイルをダウンロードします。
   - ファイルを解凍します。必要に応じて、ISOファイルをDVDに書き込みます。
2. VDAをインストールするイメージまたはマシンでローカル管理者アカウントを使用します。DVDをドライブに挿入するか、ISOファイルをマウントします。インストーラーが自動的に起動しない場合は、マウントされたドライブ上の**AutoSelect**アプリケーションをダブルクリックします。

   インストールウィザードが起動します。

スタンドアロンパッケージを使用している場合:

1. Citrixアカウントの資格情報を使用して、Citrix Virtual Apps and Desktopsダウンロードページにアクセスします。適切なパッケージをダウンロードします:
   - `VDAServerSetup_2402.exe`: マルチセッションOS VDA バージョン
   - `VDAWorkstationSetup_2402.exe`: シングルセッションOS VDA バージョン
   - `VDAWorkstationCoreSetup_2402.exe`: シングルセッションOSコアサービスVDA バージョン
2. パッケージを右クリックし、**管理者として実行**を選択します。

   インストールウィザードが起動します。

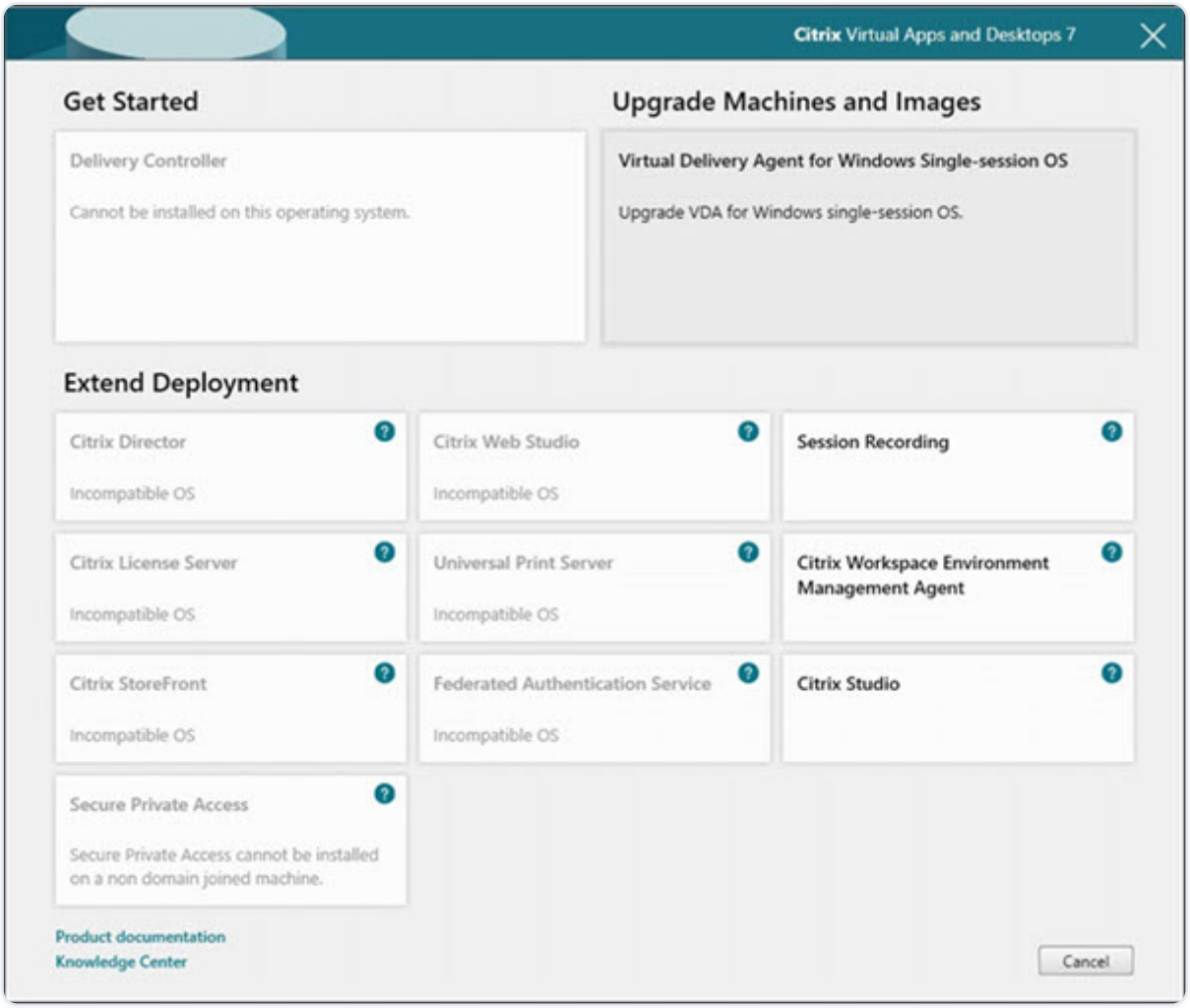
ステップ2. インストールする製品を選択する



インストールする製品（Citrix Virtual AppsまたはCitrix Virtual Desktops）の横にある**開始**をクリックします。（マシンにCitrix Virtual AppsまたはCitrix Virtual Desktopsコンポーネントがすでにインストールされている場合、このページは表示されません。）

コマンドラインオプション: Citrix Virtual Appsをインストールするための`/xenapp`。このオプションが省略された場合、Citrix Virtual Desktopsがインストールされます。

ステップ3. VDAを選択する



Virtual Delivery Agentエントリを選択します。インストーラーは、シングルセッションOSまたはマルチセッションOSのどちらで実行されているかを認識しているため、適切なVDAタイプのみを提供します。

例えば、Windows Server 2019マシンでインストーラーを実行すると、マルチセッションOS用VDAオプションが利用可能です。シングルセッションOS用VDAオプションは提供されません。

このCitrix Virtual Apps and Desktopsバージョンでサポートされていないオペレーティングシステムに Windows VDAをインストール（またはアップグレード）しようとすると、オプションに関する情報を示すメッセージが表示されます。

ステップ4. VDAの使用方法を指定する

VDAインストーラーの環境ページ(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/vda-ss-environment.png)

環境ページで、VDAをどのように使用するかを指定します。このマシンをイメージとして使用して、さらに多くのマシンをプロビジョニングするかどうかを示します。

選択したオプションは、Citrix Provisioning™ツールが自動的にインストールされるかどうか（もしあれば）、およびVDAインストーラーの追加コンポーネントページのデフォルト値に影響します。

VDAをインストールすると、複数のMSI（プロビジョニング用およびその他）が自動的にインストールされます。これらのインストールを防止する唯一の方法は、コマンドラインインストールで`/exclude`オプションを使用することです。

次のいずれかを選択してください。

- **マスターMCSイメージを作成する:** Machine Creation Services™を使用してVMをプロビジョニングする予定がある場合は、このオプションを選択してVDAをVMイメージにインストールします。このオプションは、Machine Identity Serviceをインストールします。これがデフォルトのオプションです。

  コマンドラインオプション: `/mastermcsimage` または `/masterimage`

> **重要:**
>
> インストールメディアまたはISOイメージはローカルにマウントする必要があります。ソフトウェアのインストールを目的として、ネットワークドライブからISOイメージをマウントすることはサポートされていません。

- **Citrix Provisioningまたはサードパーティのプロビジョニングツールを使用してマスターイメージを作成する:** Citrix Provisioningまたはサードパーティのプロビジョニングツール（Microsoft System Center Configuration Managerなど）を使用してVMをプロビジョニングする予定がある場合は、このオプションを選択してVDAをVMイメージにインストールします。

  コマンドラインオプション: `/masterpvsimage`

- （マルチセッションOSマシンでのみ表示）**サーバーへの仲介接続を有効にする:** 他のマシンをプロビジョニングするためのイメージとして使用されない物理マシンまたは仮想マシンにVDAをインストールするには、このオプションを選択します。

  コマンドラインオプション: `/remotepc`

- （シングルセッションOSマシンでのみ表示）**Remote PC Accessを有効にする:** Remote PC Accessで使用する物理マシンにVDAをインストールするには、このオプションを選択します。

  コマンドラインオプション: `/remotepc`

Nextをクリックします。

このページは表示されません。

- VDAをアップグレードする場合
- `VDAWorkstationCoreSetup_2308.exe`、`VDAServerSetup_2308.exe`、または`VDAWorkstationSetup_2308.exe`インストーラーを使用している場合

ステップ5. インストールするコンポーネントとインストール場所を選択します

VDAインストーラーのコアコンポーネントページ(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/vda-ss-core-components.png)

コアコンポーネントページで:

- **場所:** デフォルトでは、コンポーネントは`C:\Program Files\Citrix`にインストールされます。このデフォルトは、ほとんどの展開で問題ありません。別の場所を指定する場合、その場所にはネットワークサービスに対して`execute`権限が必要です。
- **コンポーネント:** デフォルトでは、Citrix Workspaceアプリ for WindowsはVDAと一緒にインストールされません。`VDAWorkstationCoreSetup.exe`インストーラーを使用している場合、Citrix Workspaceアプリ for Windowsはインストールされないため、このチェックボックスは表示されません。

Nextをクリックします。

コマンドラインオプション: VDAとCitrix Workspaceアプリ for Windowsをインストールするには、`/installdir`、`/components vda,plugin`

> **注：**

> 以下のシナリオでは、VDAのインストール、アップグレード、またはアンインストール中にCitrix Workspace™ Appをインストール、アップグレード、またはアンインストールすることを選択できます。

> - VDAのインストール中に、Citrix Workspace Appをインストールすることを選択できます。デフォルトでは、VDAのインストール中にCitrix Workspaceアプリはインストールされません。

- VDAのアップグレード中に、Citrix WorkspaceアプリがVDAにまだインストールされていない場合、Citrix Workspace Appをインストールすることを選択できます。
- VDAのアップグレード中に、Citrix Workspaceアプリのバージョンをアップグレードできる場合、Citrix Workspaceアプリをアップグレードするオプションが表示されます。
- VDAのアンインストール中に、Citrix Workspace Appをアンインストールしないことを選択できます。デフォルトでは、VDAのアンインストール中にCitrix Workspaceアプリはアンインストールされます。

ステップ6. 追加コンポーネントをインストールします

VDAインストーラーの追加コンポーネントページ(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/vda-ss-addtnl-components.png)

「**追加コンポーネント**」ページには、VDA とともに他の機能やテクノロジーのインストールを有効または無効にするためのチェックボックスが含まれています。コマンドラインインストールでは、`/exclude` または `/includeadditional` オプションを使用して、利用可能なコンポーネントを明示的に除外または含めることができます。

- **/includeadditional** "*コンポーネント*"\["*コンポーネント*"\] ...
- **/除外** "*コンポーネント*"\["*コンポーネント*"\] ...

次の表は、このページの項目のデフォルト設定を示しています。デフォルト設定は、「**環境**」ページで選択したオプションによって異なります。

追加コンポーネントページ	環境ページ：「MCS を使用したマスターイメージ」または「CITRIX PROVISIONING を使用したマスターイメージ」が選択されている場合	環境ページ：「サーバーへの仲介接続を有効にする」（マルチセッションOSの場合）または「リモートPCアクセス」（シングルセッションOSの場合）が選択されている場合
Citrix App-V 向けパーソナライゼーション - VDA	選択されていません	選択されていません
ユーザーパーソナライゼーションレイヤー	選択されていません	このユースケースでは無効なため表示されません。
Citrix プロファイル管理	選択済み	選択されていません

追加コンポーネントページ	環境ページ：「MCS を使用したマスターイメージ」または「CITRIX PROVISIONING を使用したマスターイメージ」が選択されている場合	環境ページ：「サーバーへの仲介接続を有効にする」（マルチセッションOSの場合）または「リモートPCアクセス」（シングルセッションOSの場合）が選択されている場合
Citrix プロファイル管理 WMI プラグイン	選択済み	選択されていません
Citrix VDA アップグレードエージェント	選択されていません	選択されていません
Citrix バックアップおよび復元	選択されていません	選択されていません
シトリックス MCS IOドライバー	選択されていません	選択されていません
シトリックス ランデブー V2	選択されていません	選択されていません

このページは、次の場合には表示されません。

- `VDAWorkstationCoreSetup.exe` インストーラーを使用している場合。また、追加コンポーネントのコマンドラインオプションは、そのインストーラーでは無効です。
- VDA をアップグレードしていて、すべての追加コンポーネントがすでにインストールされている場合。一部の追加コンポーネントがすでにインストールされている場合、そのページにはインストールされていないコンポーネントのみが表示されます。

次のチェックボックスをオンまたはオフにします。(コンポーネントはインストーラーで異なる順序で表示される場合があります。)

- **Citrix Personalization for App-V:** Microsoft App-V パッケージのアプリケーションを使用する場合は、このコンポーネントをインストールします。詳細については、「App-V アプリケーションの展開と配信」を参照してください。

  コマンドラインオプション: コンポーネントのインストールを有効にするには `/includeadditional "Citrix Personalization for App-V – VDA"`、コンポーネントのインストールを防止するには `/exclude "Citrix Personalization for App-V – VDA"`。

- **Citrixユーザーパーソナライゼーションレイヤー:** ユーザーパーソナライゼーションレイヤー用のMSIをインストールします。詳細については、「ユーザーパーソナライゼーションレイヤー」を参照してください。

  このコンポーネントは、シングルセッションのWindows 10マシンにVDAをインストールする場合にのみ表示されます。

  コマンドラインオプション: コンポーネントのインストールを有効にするには `/includeadditional "User Personalization Layer"`、コンポーネントのインストールを防止するには `/exclude "User Personalization Layer"`。

- **Citrix Profile Management:** このコンポーネントは、ユーザープロファイル内のユーザーパーソナライゼーション設定を管理します。詳細については、「Profile Management」を参照してください。

  Citrix Profile Managementをインストールから除外すると、Citrix DirectorによるVDAの監視とトラブルシューティングに影響します。**ユーザーの詳細**ページと**エンドポイント**ページでは、**パーソナライゼーション**パネルと**ログオン期間**パネルが機能しません。**ダッシュボード**ページと**傾向**ページでは、**平均ログオン期間**パネルはProfile Managementがインストールされているマシンのみのデータを表示します。

  サードパーティのユーザープロファイル管理ソリューションを使用している場合でも、Citrixは Citrix Profile Management Serviceをインストールして実行することをお勧めします。Citrix Profile Management Serviceを有効にする必要はありません。

  コマンドラインオプション: コンポーネントのインストールを有効にするには `/includeadditional "Citrix Profile Management"`、コンポーネントのインストールを防止するには `/exclude "Citrix Profile Management"`。

- **Citrix Profile Management WMIプラグイン:** このプラグインは、WMI（Windows Management Instrumentation）オブジェクト（プロファイルプロバイダー、プロファイルタイプ、サイズ、ディスク使用量など）でProfile Managementのランタイム情報を提供します。WMIオブジェクトは、Directorにセッション情報を提供します。

  コマンドラインオプション: コンポーネントのインストールを有効にするには `/includeadditional "Citrix Profile Management WMI Plug-in"`、コンポーネントのインストールを防止するには `/exclude "Citrix Profile Management WMI Plug-in"`。

- **VDAアップグレードエージェント:** Citrix DaaS（旧Citrix Virtual Apps and Desktopsサービス）の展開にのみ適用されます。VDAがVDAアップグレード機能に参加できるようにします。この機能を使用して、管理コンソールからカタログのVDAを即座に、またはスケジュールされた時

間にアップグレードできます。このエージェントがインストールされていない場合、マシン上でVDAインストーラーを実行することでVDAをアップグレードできます。

コマンドラインオプション: コンポーネントのインストールを有効にするには `/includeadditional "Citrix VDA Upgrade Agent"`、コンポーネントのインストールを防止するには `/exclude "Citrix VDA Upgrade Agent"`。

- **ストレージ最適化のためのMCSIOライトキャッシュ:** Citrix MCS I/Oドライバーをインストールします。詳細については、「ハイパーバイザーによって共有されるストレージ」および「一時データ用のキャッシュの構成」を参照してください。

  コマンドラインオプション: コンポーネントのインストールを有効にするには `/includeadditional "Citrix MCS IODriver"`、コンポーネントのインストールを防止するには `/exclude "Citrix MCS IODriver"`。

- **プロキシ構成:** 環境でGateway Service、VDA Upgrade ServiceなどでRendezvousプロトコルを使用する予定があり、ネットワークにアウトバウンド接続用の非透過型プロキシがある場合は、このコンポーネントをインストールし、ここでプロキシを指定します。HTTPプロキシのみがサポートされています。

  このコンポーネントをインストールする場合は、**Rendezvousプロキシ構成**ページでプロキシのアドレスまたはPACファイルのパスを指定します。機能の詳細については、「Rendezvousプロトコル」を参照してください。

  コマンドラインオプション: コンポーネントのインストールを有効にするには `/includeadditional "Citrix Rendezvous V2"`、コンポーネントのインストールを防止するには `/exclude "Citrix Rendezvous V2"`。

- **Citrix Backup and Restore:** VDAのインストールまたはアップグレードが失敗した場合、このコンポーネントはマシンをインストールまたはアップグレード前のバックアップ状態に戻すことができます。

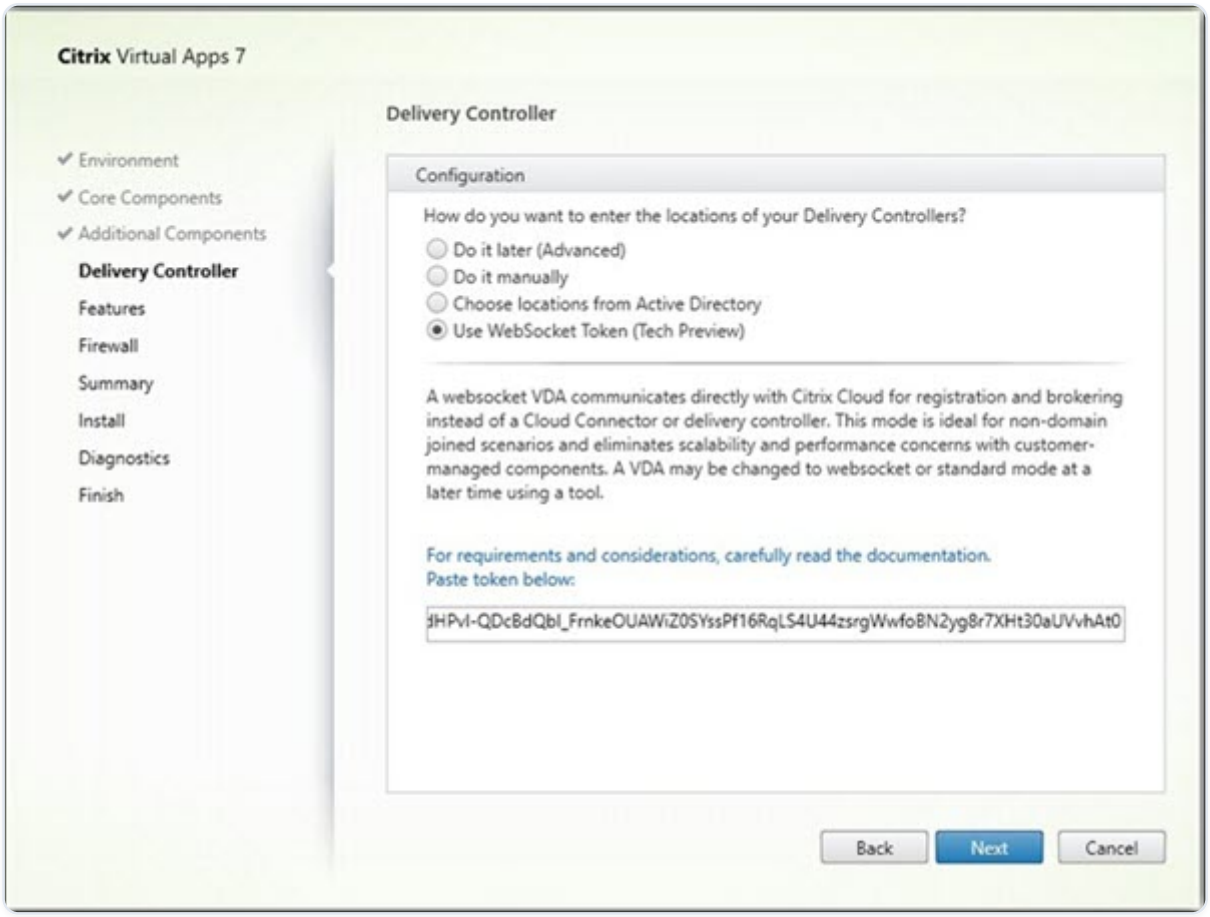
  インストール準備に記載されているMicrosoftの前提条件が満たされていることを確認してください。

  コマンドラインオプション: コンポーネントのインストールを有効にするには `/includeadditional "Citrix Backup and Restore"`、コンポーネントのインストールを防止するには `/exclude "Citrix Backup and Restore"`。

> **注：**

> MCSストレージ最適化が有効になっている場合、Windowsサーバーまたはデスクトップオペレーティングシステムのバックアップまたは復元が失敗する可能性があります。これを解決するには、メタインストーラーでMCSストレージ最適化オプションを無効にしてください。

手順7. Delivery Controller™アドレス



Delivery Controllerページで、インストールされているControllerのアドレスを入力する方法を選択します。Citrixでは、VDAのインストール中にアドレスを指定することをお勧めします（**手動で実行**）。VDAは、この情報がないとControllerに登録できません。VDAが登録できない場合、ユーザーはそのVDA上のアプリケーションやデスクトップにアクセスできません。

- **手動で実行:** (デフォルト) インストールされているControllerのFQDNを入力し、**追加**をクリックします。複数のControllerをインストールしている場合は、それらのアドレスも追加します。
- **後で実行 (詳細設定):** このオプションを選択すると、ウィザードは続行する前にその操作を実行するかどうかを確認します。後でアドレスを指定するには、インストーラーを再実行するか、Citrixグループポリシーを使用できます。ウィザードは**概要**ページでも通知します。
- **Active Directoryから場所を選択:** マシンがドメインに参加しており、ユーザーがドメインユーザーである場合にのみ有効です。

- **WebSocketトークンを使用 (テクニカルプレビュー):** WebSocket VDAを作成します。WebSocketTokenは、必要なトークン用です。
- **Machine Creation Servicesに自動的に実行させる:** MCSを使用してマシンをプロビジョニングする場合にのみ有効です。

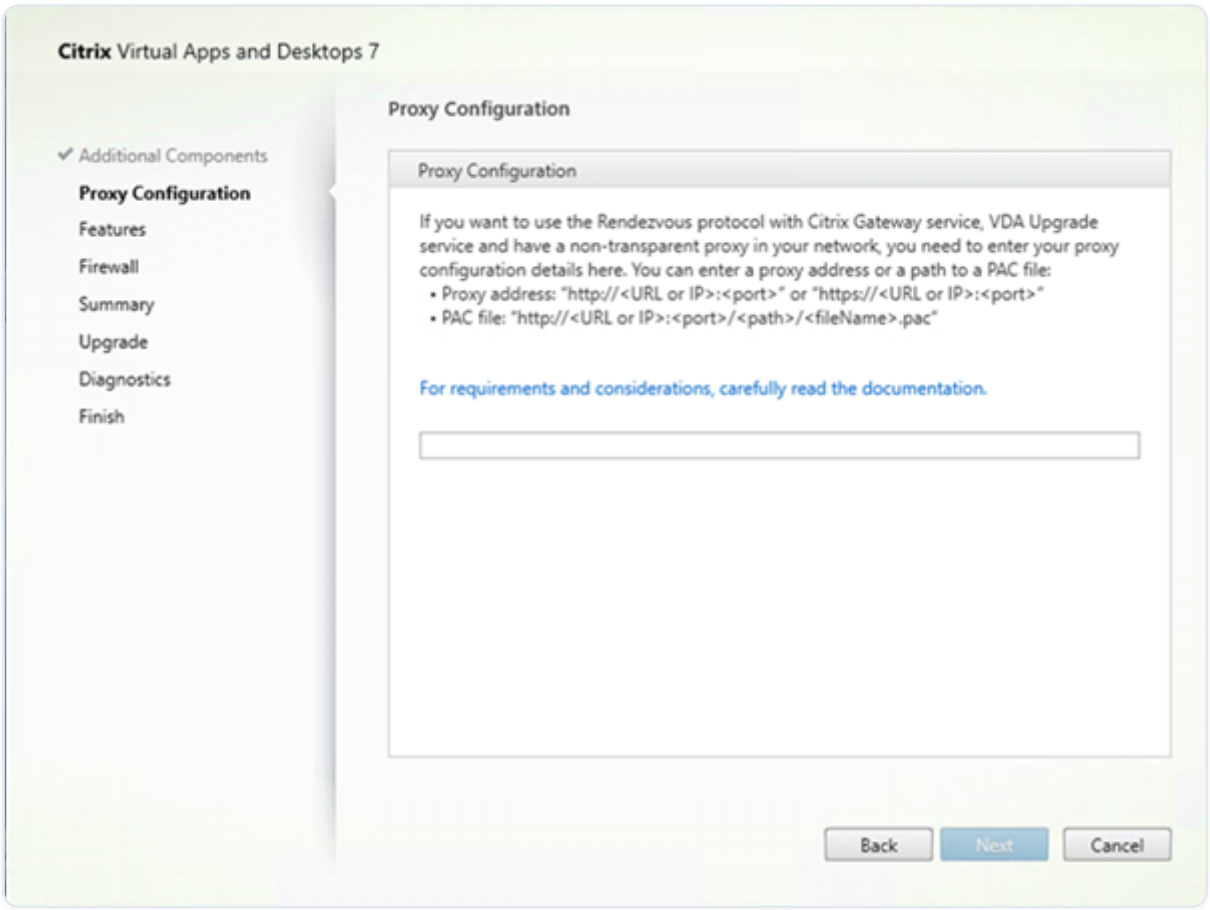
次へをクリックします。**後で実行 (詳細設定)**を選択した場合、Controllerアドレスを後で指定することを確認するよう求められます。

その他の考慮事項:

- アドレスには英数字以外の文字を含めることはできません。
- VDAのインストール時とグループポリシーでアドレスを指定した場合、ポリシー設定がインストール時に指定された設定を上書きします。
- VDAの登録を成功させるには、Controllerとの通信に使用されるファイアウォールポートが開いている必要があります。このアクションは、ウィザードの**ファイアウォール**ページでデフォルトで有効になっています。
- Controllerの場所を指定した後（VDAのインストール中またはインストール後）、Controllerが追加または削除されたときにVDAを更新するために、自動更新機能を使用できます。VDAがControllerを検出して登録する方法の詳細については、「VDA登録」を参照してください。

コマンドラインオプション: `/controllers`

ステップ8. プロキシ構成



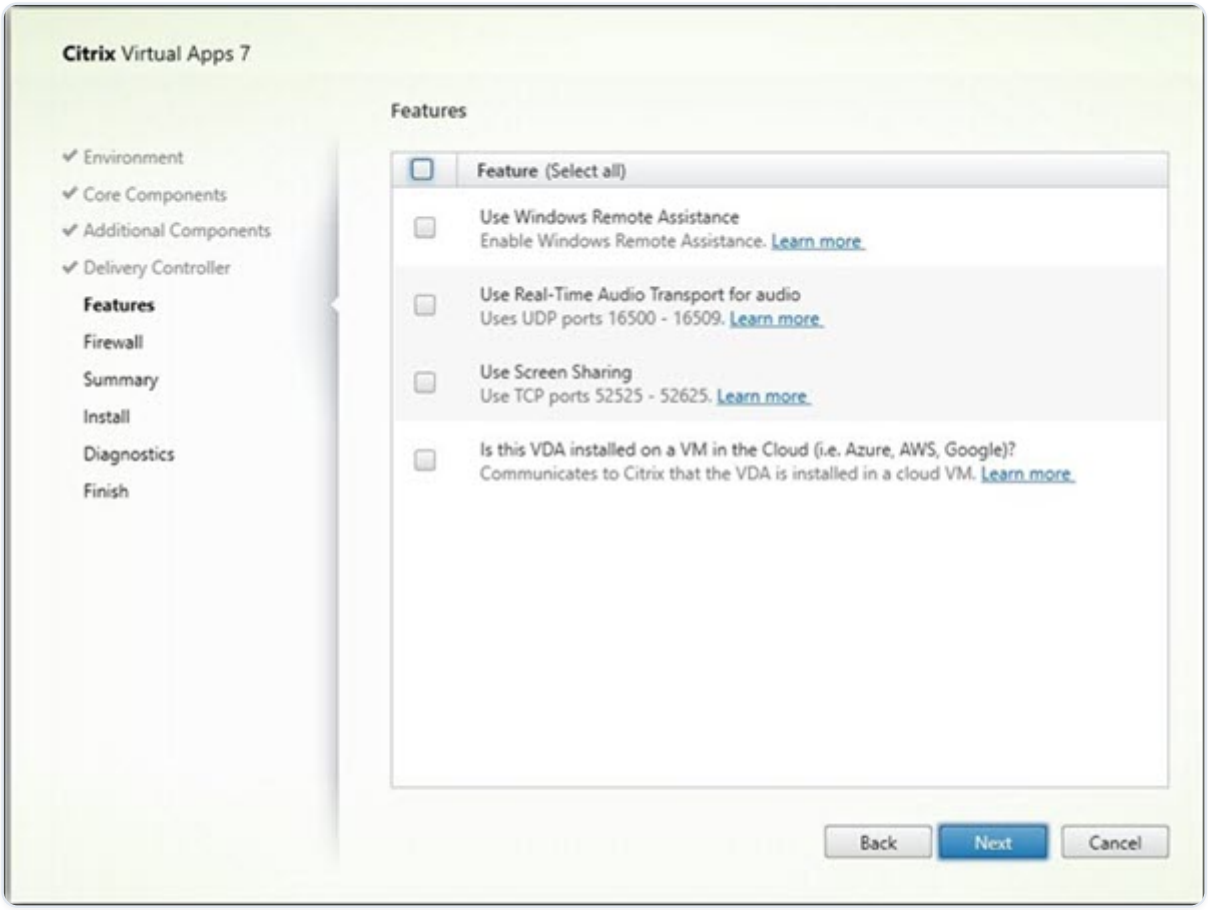
プロキシ構成ページは、**追加コンポーネント**ページで**プロキシ構成**チェックボックスを有効にした場合にのみ表示されます。

1. プロキシソースをプロキシアドレスで指定するか、PACファイルパスで指定するかを選択します。
2. プロキシアドレスまたはPACファイルパスを指定します。
   - プロキシアドレスの形式: `http://<url-or-ip>:<port>`
   - PACファイルの形式: `http://<url-or-ip>:<port>/<path>/<filename>.pac`

接続テストを成功させるには、プロキシポートのファイアウォールが開いている必要があります。プロキシへの接続ができない場合でも、VDAのインストールを続行するかどうかを選択できます。

コマンドラインオプション: `/proxyconfig`

ステップ9. 機能の有効化または無効化



機能ページで、チェックボックスを使用して、使用する機能を有効または無効にします。

- **Windows リモートアシスタンスを使用する:** この機能が有効な場合、Windows リモートアシスタンスはDirectorのユーザーシャドウ機能とともに使用されます。Windows リモートアシスタンスは、ファイアウォールで動的ポートを開きます。(デフォルト = 無効)

  コマンドラインオプション: `/enable_remote_assistance`

- **オーディオにリアルタイムオーディオトランスポートを使用する:** ネットワークでVoice-over-IPが広く使用されている場合は、この機能を有効にします。この機能は、遅延を減らし、損失の多いネットワークでのオーディオの回復力を向上させます。RTP over UDPトランスポートを使用してオーディオデータを送信できます。(デフォルト = 無効)

  コマンドラインオプション: `/enable_real_time_transport`

- **画面共有を使用する:** 有効にすると、画面共有で使用されるポートがWindowsファイアウォールで開かれます。(デフォルト = 無効)

  コマンドラインオプション: `/enable_ss_ports`

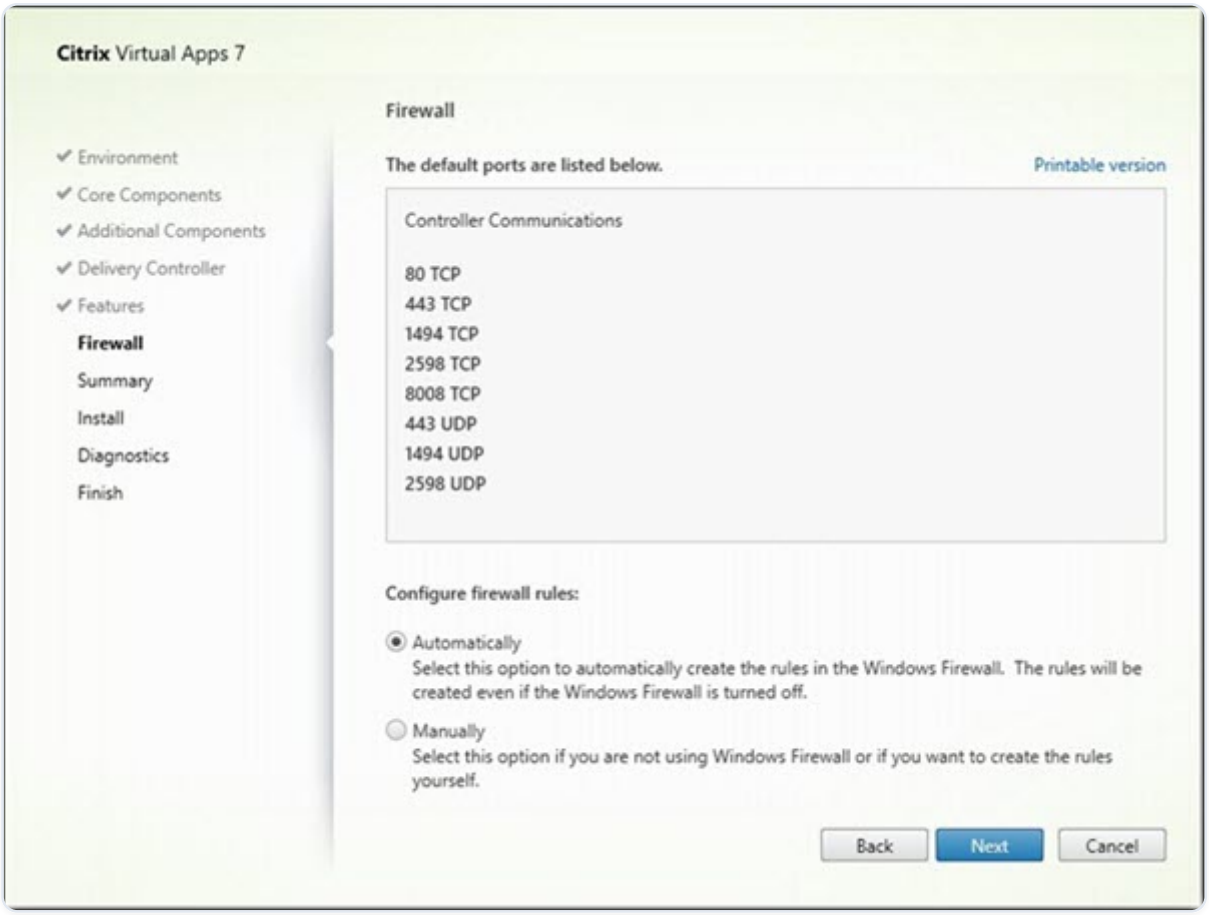
- **このVDAはクラウド内のVMにインストールされていますか:** この設定は、Citrixがテレメトリ目的でオンプレミスおよびサービス (Citrix Cloud™) VDA展開のリソースの場所を正しく識別

するのに役立ちます。この機能は、顧客側の利用には影響しません。展開でCitrix DaaSを使用している場合は、この設定を有効にします。(デフォルト = 無効).

コマンドラインオプション: `/xendesktopcloud`

Nextをクリックします。

手順 10. ファイアウォールポート

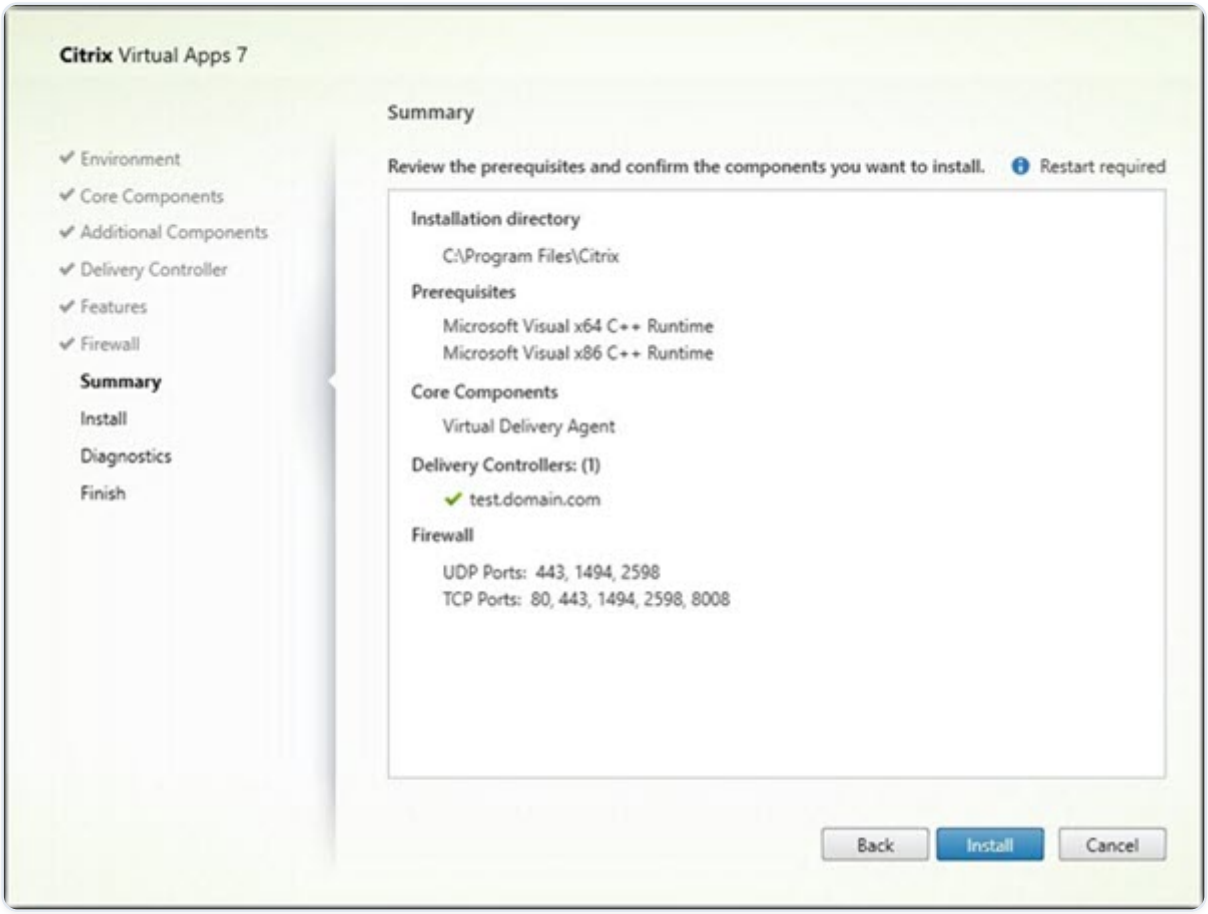


ファイアウォールページでは、デフォルトで、Windowsファイアウォールサービスが実行されている場合、ファイアウォールが有効になっていなくてもポートは自動的に開かれます。このデフォルト設定は、ほとんどの展開で問題ありません。ポート情報については、「ネットワークポート」を参照してください。

Nextをクリックします。

コマンドラインオプション: `/enable_hdx_ports`

手順 11. 前提条件を確認し、インストールを確定する



概要ページには、インストールされるものが一覧表示されます。**戻る**ボタンを使用して、以前のウィザードページに戻り、選択を変更します。

準備ができたら、**インストール**をクリックします。

前提条件がまだインストールまたは有効になっていない場合、マシンは1回以上再起動する可能性があります。インストールの準備を参照してください。

ステップ12. 診断

VDAインストーラーの診断ページ(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/vda-ss-diagnostics.png)

診断ページで、Citrix Call Homeに参加するかどうかを選択します。参加することを選択した場合（デフォルト）、**接続**をクリックします。プロンプトが表示されたら、Citrixアカウントの資格情報を入力します。

資格情報が検証された後（または参加しないことを選択した場合）、**次へ**をクリックします。

フル製品インストーラーを使用している場合、**診断**ページで最初に**診断情報の収集**を選択せずに**接続**をクリックすると、**Citrix Insight Servicesへの接続**ダイアログを閉じた後、**次へ**ボタンが無

効になります。次のページに進むことはできません。**次へ**ボタンを再度有効にするには、**診断情報の収集**を選択し、すぐに選択を解除します。

詳細については、Call Homeを参照してください。

ステップ13. このインストールを完了する

VDAインストーラーのインストール完了ページ(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/vda-ss-finish.png)

完了ページには、正常にインストールおよび初期化されたすべての前提条件とコンポーネントの緑色のチェックマークが表示されます。

完了をクリックします。デフォルトでは、マシンは自動的に再起動します。この自動再起動を無効にすることはできますが、マシンが再起動するまでVDAは使用できません。

次のステップ

必要に応じて、上記のプロシージャを繰り返して、他のマシンまたはイメージにVDAをインストールします。

すべてのVDAをインストールしたら、Studioを起動します。まだサイトを作成していない場合、Studioはそのタスクに自動的に誘導します。それが完了すると、Studioはマシンカタログとデリバリーグループの作成に誘導します。参照：

- サイトの作成
- マシンカタログの作成
- 「デリバリーグループの作成」(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/install-configure/delivery-groups-create.html)

シトリックス オプティマイザー

Citrix Optimizerは、Citrix管理者がさまざまなコンポーネントを削除および最適化することでVDAを最適化するのに役立つWindows OS用のツールです。

VDAをインストールし、最終的な再起動を完了した後、Citrix Optimizerをダウンロードしてインストールします。「CTX224676」を参照してください。CTXの記事には、ダウンロードパッケージと、Citrix Optimizerのインストールおよび使用方法に関する手順が含まれています。

VDAをカスタマイズする

インストール済みのVDAをカスタマイズするには：

1. Windowsのプログラムの削除または変更機能から、「**Citrix Virtual Delivery Agent**」または「**Citrix Remote PC Access/VDI Core Services VDA**」を選択します。その後、右クリックして「**変更**」を選択します。
2. 「**Virtual Delivery Agent Settingsのカスタマイズ**」を選択します。インストーラーが起動したら、以下を変更できます。

   - Controllerアドレス
   - Controllerに登録するTCP/IPポート（デフォルト = 80）
   - Windowsファイアウォールポートを自動的に開くかどうか

トラブルシューティング

- コンポーネントインストールの結果をCitrixが報告する方法については、「Citrixインストールリターンコード」(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/install-configure/install-prepare.html#citrix-installation-return-codes)を参照してください。
- デリバリーグループのStudio表示では、**詳細**ペインの**インストール済みVDAバージョン**エントリが、マシンにインストールされているバージョンと異なる場合があります。マシンのWindowsのプログラムと機能の表示には、実際のVDAバージョンが表示されます。
- VDAがインストールされても、Delivery Controllerに登録されるまでは、ユーザーにアプリやデスクトップを配信できません。

  VDA登録方法と登録問題のトラブルシューティング方法については、「VDA登録」(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/manage-deployment/vda-registration.html)を参照してください。

既知の制限事項

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

VDAインストールに関連するWindows Defenderアクセス制御の構成

お客様は、署名されていないバイナリの読み込みを禁止するために、Windows Defenderアクセス制御 (WDAC) 設定を構成します。VDAインストーラーを通じて配布される署名されていないバイナリは、VDAのインストールを制限するため、禁止されます。

Citrix® は現在、すべてのCitrix生成バイナリをCitrixコード署名証明書で署名しています。さらに、Citrixは、当社の製品とともに配布されるサードパーティ製バイナリも、それらのサードパーティ製バイナリを信頼できるバイナリとして認証する証明書で署名しています。

重要:

署名されていないサードパーティ製バイナリを含む古いVDAから、署名されたバイナリを含む新しいVDAバージョンにアップグレードしても、常にアップグレードされたマシンに署名されたバイナリが配置されるとは限りません。 これは、OS内のメカニズムにより、システムのアップグレードで同じバージョンのバイナリが置き換えられないためです。 サードパーティ製バイナリは署名されていますが、サードパーティによって制御されているそのバージョンはCitrixによって更新できないため、これらのバイナリは更新されません。この制限を回避するには：

1. バイナリを許可リストに含めます。これにより、バイナリに署名する必要がなくなります。
2. 古いVDAをアンインストールし、新しいVDAをインストールします。これはVDAの新規インストールに似ており、署名されたバージョンがインストールされます。

ウィザードを使用して新しいベースポリシーを作成する

WDACを使用すると、信頼できるバイナリをシステムで実行できるように追加できます。WDACのインストール後、**Windows Defender Application Control Policy Wizard** が自動的に開きます。

バイナリを追加するには、新しいベースWDACポリシーを作成する必要があります。ベースポリシーを作成するためのCitrix推奨ガイドラインは、このセクションで提供されています。

- Windowsオペレーティングコンポーネント、Microsoft Storeからインストールされたアプリ、すべてのMicrosoft署名済みソフトウェア、およびサードパーティのWindowsハードウェア互換ドライバーを承認するため、ベーステンプレートとして を選択します。
- 新しいWindows Defender Application Controlポリシーを適用する前にテストできるため、 を選択します。
- アプリケーションが識別され信頼されるレベルを指定し、参照ファイルを提供するために、に を追加します。ルールタイプとして「発行元」を選択すると、Citrix証明書のいずれかで署名された参照ファイルを選択できます。

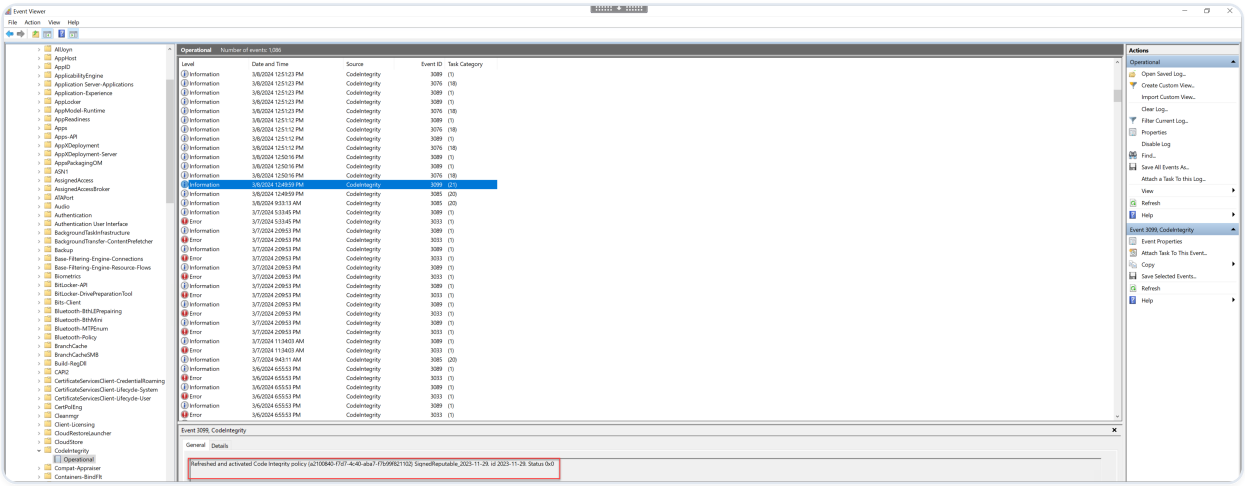
- ルールを追加したら、`.XML` および `.CIP` ファイルが保存されているフォルダーに移動します。`.XML` ファイルには、ポリシーで定義されているすべてのルールが含まれています。任意のルールを変更、追加、または削除するように構成できます。
- WDACポリシーを展開する前に、`.XML` ファイルをバイナリ形式に変換する必要があります。WDACファイルは、`.XML` ファイルを `.CIP` ファイルに変換します。
- `.CIP` ファイルを C:\WINDOWS\System32\CodeIntegrity\CiPolicies\Active にコピーして貼り付け、マシンを再起動します。生成されたポリシーは監査モードで適用されます。
- ベースポリシーを作成する手順については、ウィザードで新しいベースポリシーを作成するを参照してください。

このポリシーが適用されると、WDACは、指定された発行元/CA機関によって署名されているCitrixファイルについて警告を発しません。

同様に、サードパーティによって署名されたファイルに対して、発行元レベルのルールを作成できます。

適用されたポリシーを確認する

1. マシンが再起動された後、**イベントビューアー**を開き、**アプリケーションとサービスログ > Microsoft > Windows > CodeIntegrity > Operational**に移動します。
2. 適用されたポリシーがアクティブになっていることを確認します。



3. ポリシーに違反したログを探し、そのファイルのプロパティを確認します。まず、署名されていることを確認します。署名されていない場合で、このマシンがVDAアップグレードを経ている場合、これは上記の制限で説明されているケースである可能性が高いです。署名されている場合、このファイルは、前述のとおり、代替証明書で署名されている可能性があります。

Citrix証明書で署名されたCitrix生成ファイルの例は `C:\Windows\System32\drivers\picadm.sys` です。 Citrixサードパーティ証明書で署名されたサー

ドパーティバイナリの例は`C:\Program Files\Citrix\IcaConfigTool\Microsoft.Practices.Unity.dll`です。

SCCM を使用した VDA のインストール

概要

Microsoft Endpoint Configuration Manager (旧称 System Center Configuration Manager (SCCM)) は、企業全体のデバイスとアプリケーションの管理、展開、およびセキュリティを可能にする Windows 製品です。

> **注：**
>
> 以下の記事では、Citrix® が環境をテストした方法に基づいた推奨事項のみを説明しています。これらの手順は、必要に応じてカスタマイズできます。Citrix は、顧客のニーズに合わせてこれに必要な更新や調整について責任を負いません。

推奨事項

- SCCM または類似のソフトウェア配布ツールを使用して Virtual Delivery Agent (VDA) を正常に展開するには、Citrix は、一連の手順で VDA インストーラーを使用することを推奨します。
- Citrix は、VDA のインストールまたはアップグレードの一部として VDA Cleanup Utility を使用することを推奨しません。VDA インストーラーが以前に失敗した場合にのみ、VDA Cleanup Utility を使用してください。

始める前に

VDA のインストール中に必要な再起動の回数は、環境によって異なります。例:

- 保留中の更新や以前のソフトウェアインストールからの再起動のために、再起動が必要になる場合があります。
- 他のプロセスによって以前にロックされていたファイルは更新が必要になる場合があり、追加の再起動を強制します。
- VDA インストーラーの一部のオプションコンポーネント (Citrix Profile Management や Citrix Files など) は、再起動が必要になる場合があります。
- VDA をアップグレードする場合、インストールされているマシンは、セッションがない状態でメンテナンスモードになっている必要があります。

- マシンで VDA のインストールが初めて実行されると、使用されている VDA インストーラーはそのマシンにコピーされます。 VDA のインストールに関する詳細については、インストーラーを参照してください。

SCCM タスクシーケンサーは、必要なすべての再起動を管理します。

SCCM を使用して VDA を展開するための主要な手順

以下の手順では、仮想マシンに SCCM を使用して VDA を展開する方法について説明します。

1. VDA をインストールする。
2. 組織単位 (OU) を作成する。
3. マシンを検証する。
4. VDA を使用してコンテンツを配布する。

ステップ 1: VDA をインストールする

すべての前提条件を特定した後、**SCCM タスク シーケンサー**を使用して次のタスクを完了します。

1. インストールメディアのアクセス可能なコピーから、またはVDAスタンドアロンインストーラーのいずれかからVDAをインストールします。

   - `VDAWorkstationSetup_XXXX.exe`
   - `VDAServerSetup_XXXX.exe`
   - `VDAWorkstationCoreSetup_XXXX.exe`

   VDAインストーラーの詳細については、「インストーラー」を参照してください。

   > **注：**
   >
   > VDAをアップグレードする場合、VDAがインストールされているマシンは、セッションがないメンテナンスモードである必要があります。

2. マシンでVDAのインストールが初めて実行されると、使用されているVDAインストーラーがそのマシンにコピーされます。

   - `VDAWorkstationCoreSetup_XXXX.exe`以外のVDAインストーラーを使用すると、VDAインストーラーは`%ProgramData%\Citrix\XenDesktopSetup\XenDesktopVdaSetup.exe`にコピーされます。

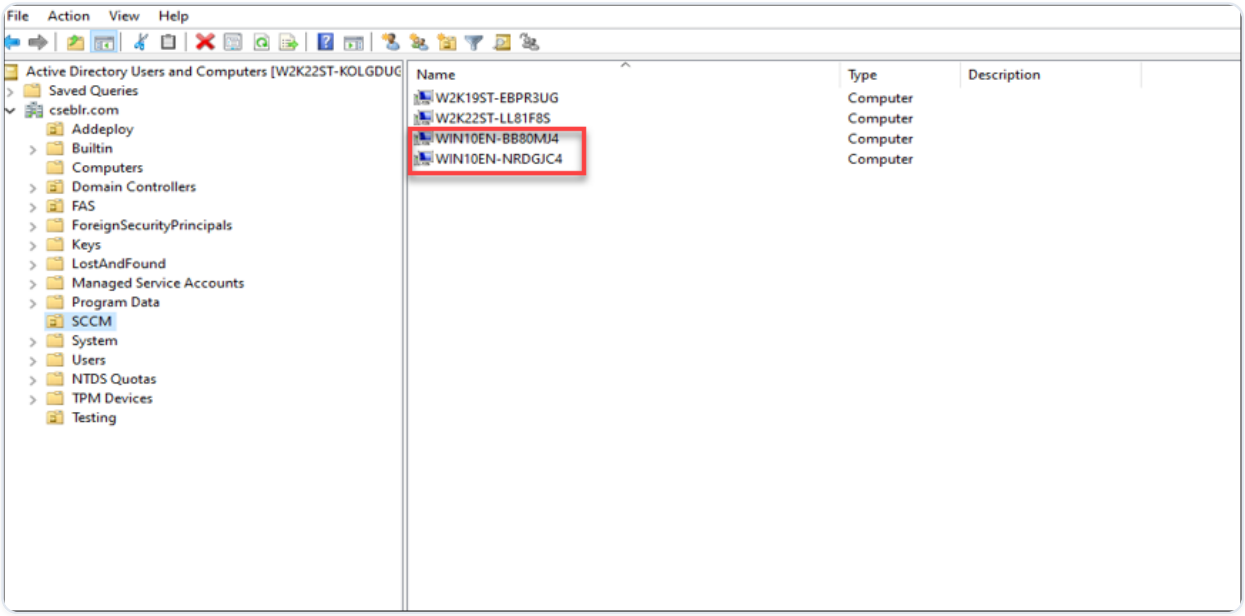
- `VDAWorkstationCoreSetup_XXXX.exe`を使用すると、VDAインストーラーは`%ProgramData%\Citrix\XenDesktopSetup\XenDesktopRemotePCSetup.exe.`にコピーされます。

3. VDAインストーラーのディレクトリの場所は、レジストリ`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\MetaInstall”“MetaInstallerInstallLocation”`にも保存されます。
4. コマンドラインオプションに`/NOREBOOT`、`/NORESUME`、および`/QUIET`を追加します。

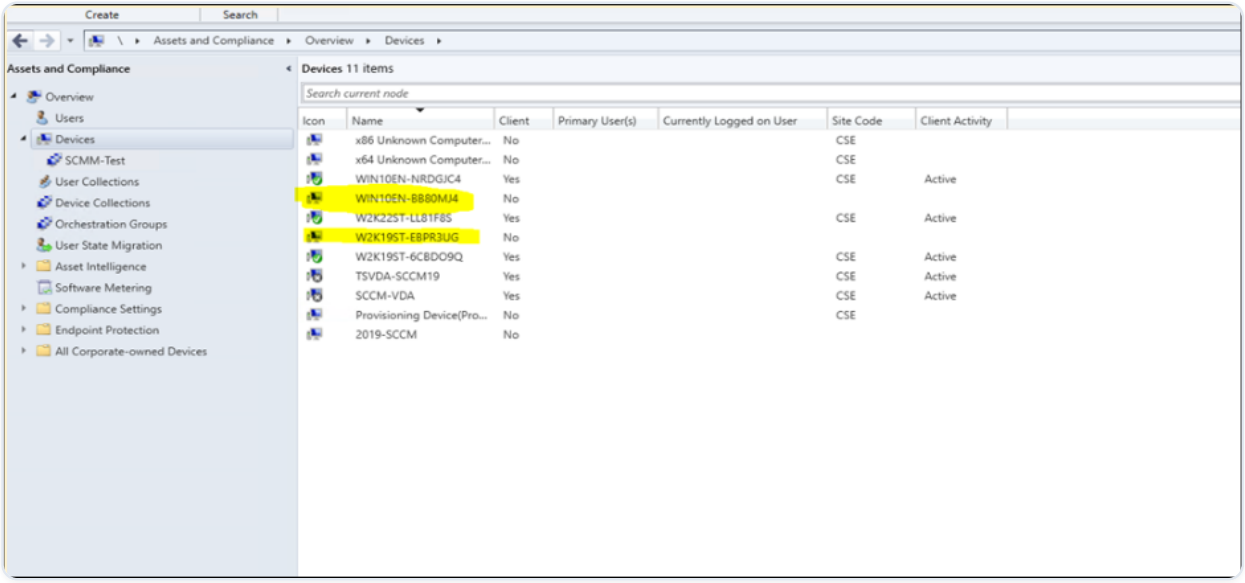
   - `/QUIET`: インストール中にユーザーインターフェイスを表示しないようにします。これにより、SCCMがインストールプロセスを制御できます。
   - `/NOREBOOT`: VDAインストーラーが自動的に再起動するのを抑制します。SCCMは必要に応じて再起動をトリガーします。
   - `/NORESUME`: 通常、インストール中に再起動が必要な場合、VDAインストーラーはrunonceレジストリキー(`\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce`)を設定します。Windowsは、マシンが再起動したときにこのキーを使用してVDAインストーラーを開きます。SCCMはインストールを監視して終了コードをキャプチャできないため、これはSCCMにとって問題となります。

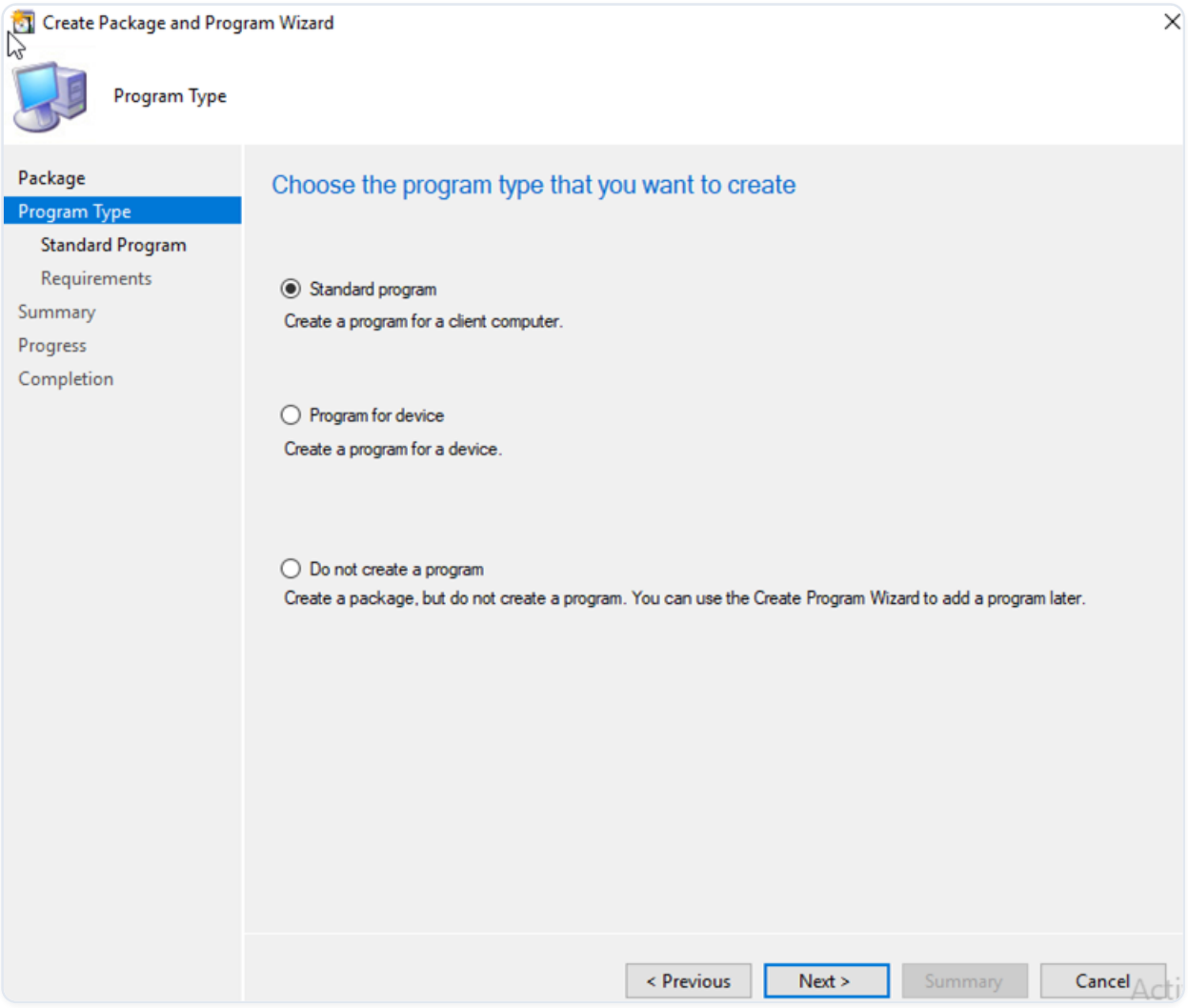
ステップ2: 組織単位 (OU) を作成する

1. OU に追加するドメイン参加済み仮想マシンを 2 台作成します。仮想マシンが最初に作成されると、**Computers** フォルダーにあります。仮想マシンを **SCCM** フォルダーに移動します。例: WIN10EN-BB80MJ4.cseblr.com W2K19ST-EBPR3UG.cseblr.com

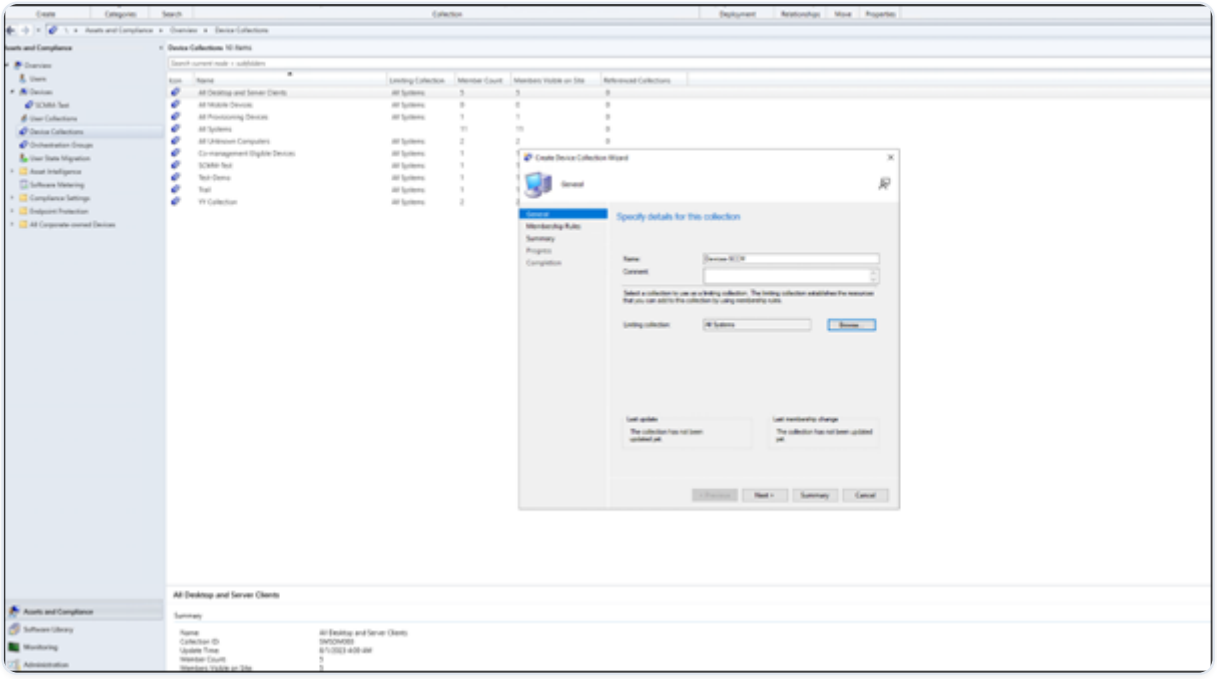


2. Microsoft Configuration Manager で、`\Administration\Overview\Hierarchy Configuration\Discovery Methods\` に移動します。
3. **Active Directory システム検出**をクリックし、**Active Directory システム検出を有効にする**チェックボックスを選択して、新しく作成された仮想マシンの自動検出を有効にします。
4.  アイコンをクリックして、新しいコンテナーを選択します。
5. **場所**セクションで、SCCM 仮想マシンが配置されている**パス**を追加します。
6. `\Administration\Overview\Site Configuration\Sites` に移動し、SCCM VDA を右クリックします。
7. **クライアントインストール設定 > クライアントプッシュインストール**を選択します。**クライアントプッシュインストールのプロパティ**ウィンドウが開きます。
8. VM が `Enabled` に設定されると、以下の画像に示すように VM のリストが表示されます。





9. OU を作成するために**デバイスコレクション**を作成します。コレクション名の**名前**を入力します。



10. ウィザードの指示に従います。

メンバーシップルール(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/sccm-membership-rules.png)

OUが作成されます。

OUの作成(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/sccm-create-device-collection-wizard.png)

11. 作成したVMを、新しく作成したデバイスコレクションに追加します。

    a. VMを右クリックします。「**選択した項目を追加 > 既存のデバイスコレクションに選択した項目を追加**」を選択します。

       項目の追加(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/sccm-add-item-to-device-collection.png)

    b. 「**コレクションの選択**」ウィンドウで、必要なデバイス名を選択します。この例では、`Devices-SCCM`です。

       デバイスリスト(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/sccm-list.png)

    `Devices-SCCM`は、「**資産とコンプライアンス > 概要 > デバイスコレクション**」に表示されます。

    デバイスがリスト表示されました(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/devices-sccm.png)

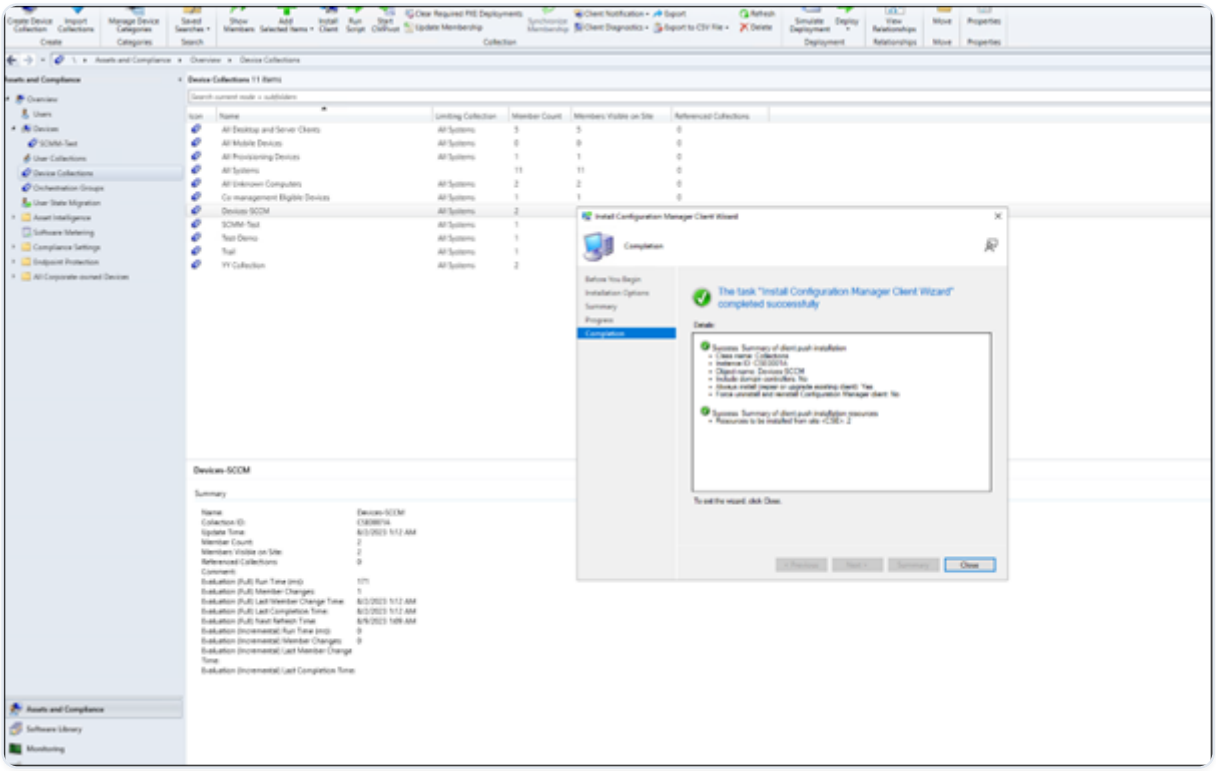
12. デバイスコレクターで「**クライアントのインストール**」を選択します。

    クライアントのインストール(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/sccm-install-client.png)

13. 必要なインストール「**サイト**」を選択します。

    サイトのインストール(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/sccm-install-client-1.png)

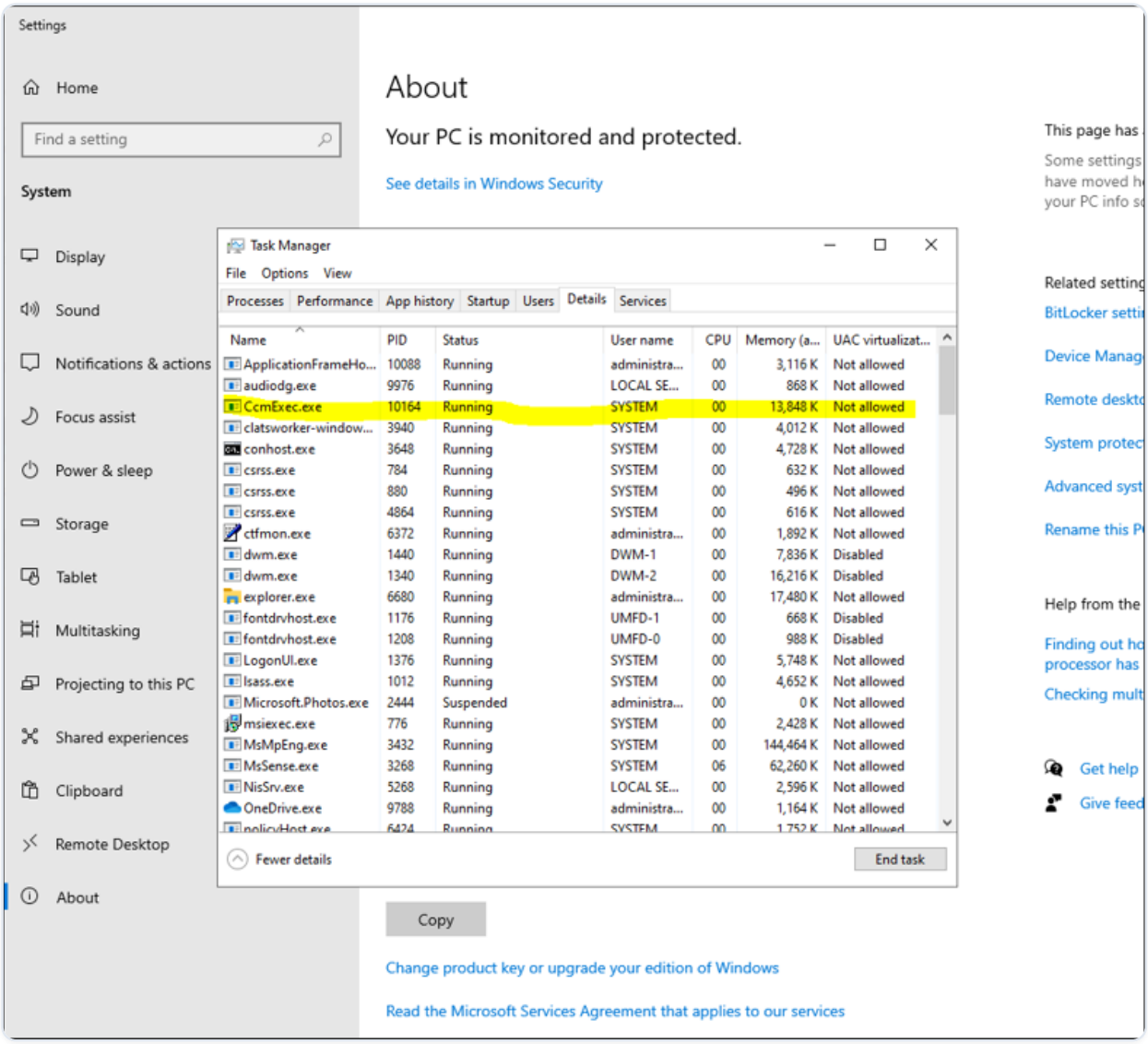
14. ウィザードの指示に従います。**Install Configuration Manager Client Wizard** が正常に完了しました。



詳細については、Microsoft ドキュメントの コレクションの管理 を参照してください。

ステップ 3: マシンの検証

1. クライアントマシンで、`CCMExec` プロセスが実行されていることを確認して、クライアントがインストールされていることを検証します。



2. SCCM 上の VM でクライアントが実行されていることを確認します。

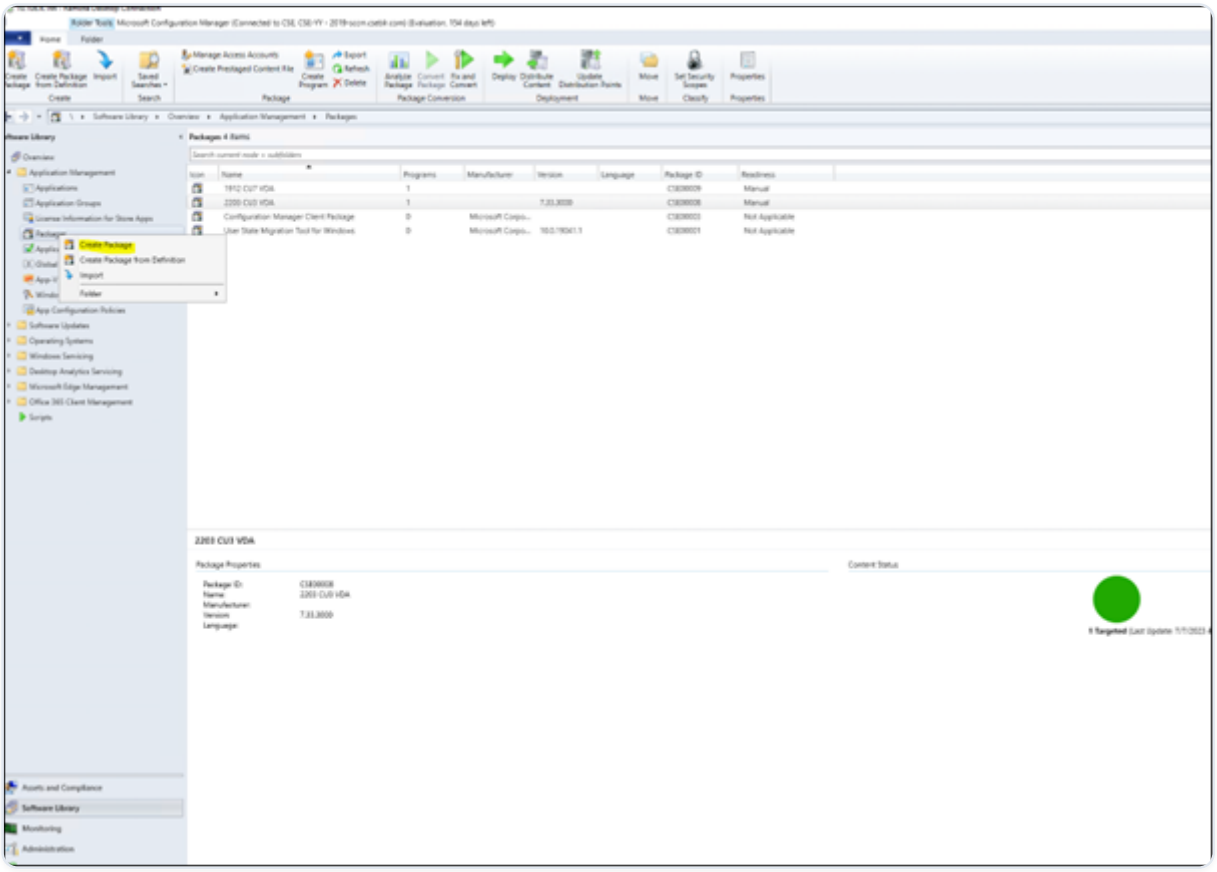
ステップ 4: VDA を使用してコンテンツを配布する

次の手順では、展開された VDA を使用して、関連付けられた仮想マシンにコンテンツを配布する方法について説明します。

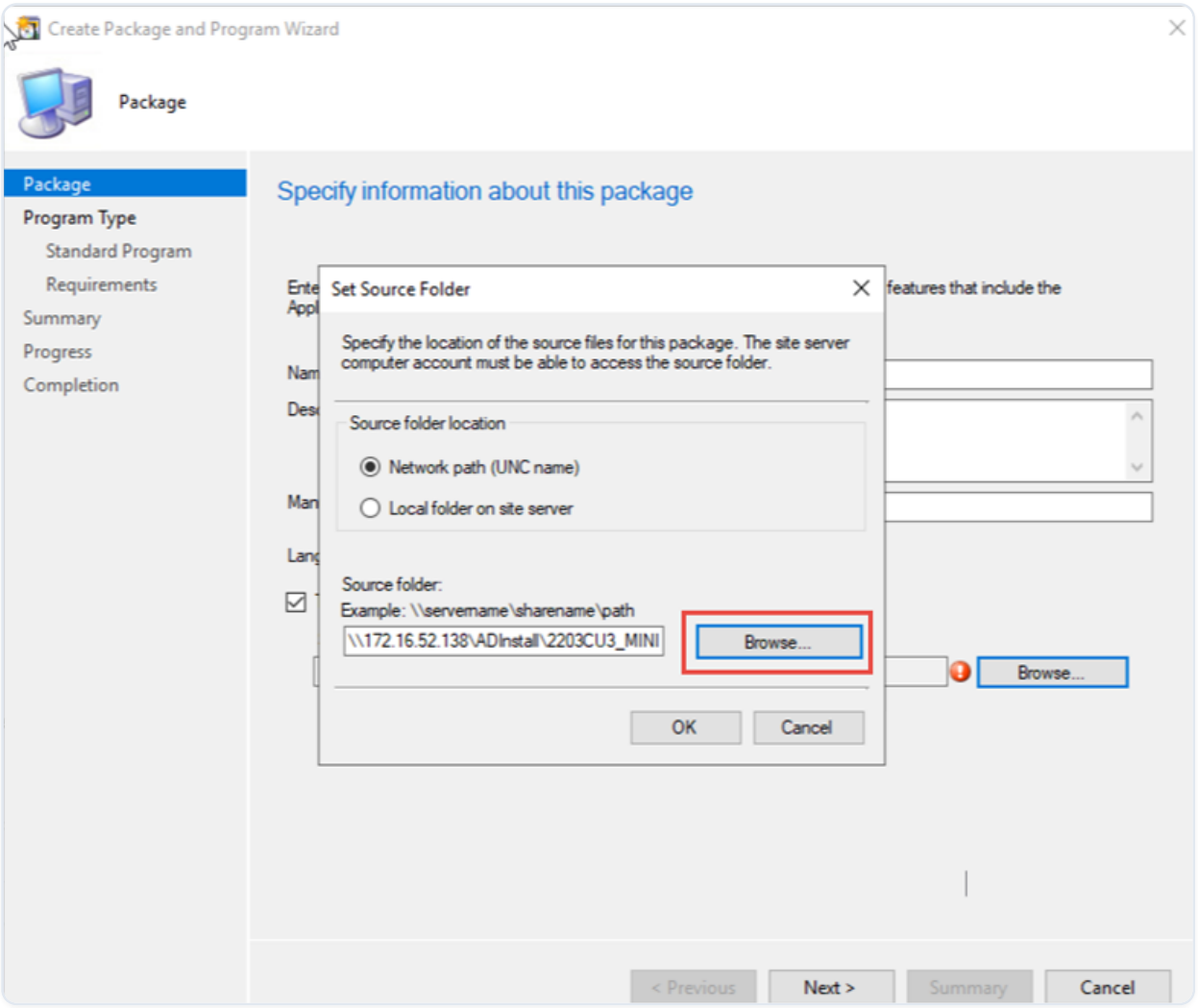
1. パッケージの作成
2. コンテンツの配布

パッケージの作成

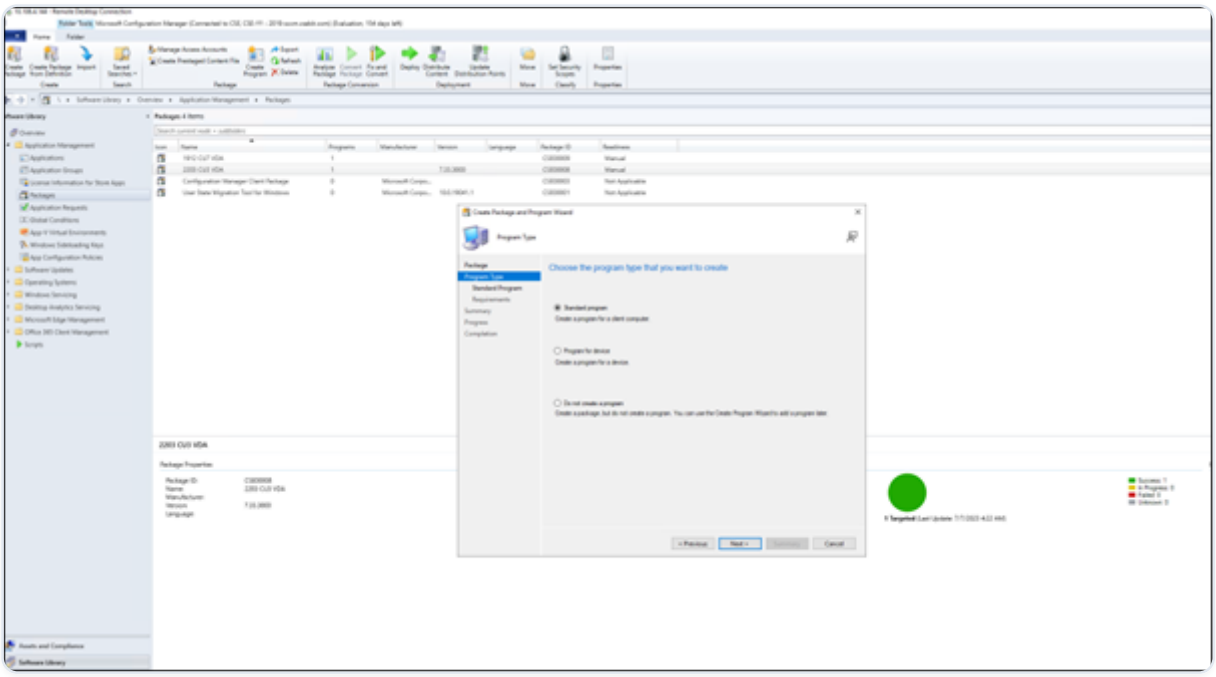
1. パッケージを作成するには、目的の VDA を右クリックし、 をクリックします。



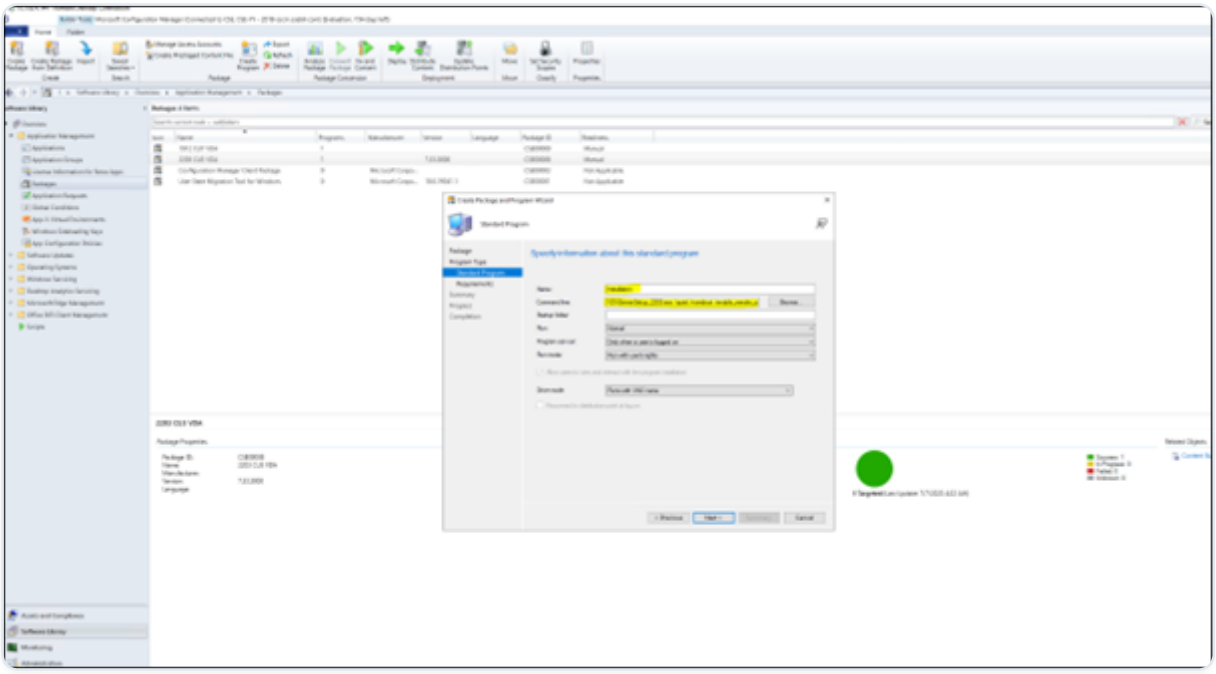
2. をクリックして、このパッケージのソースファイルの場所を指定します。



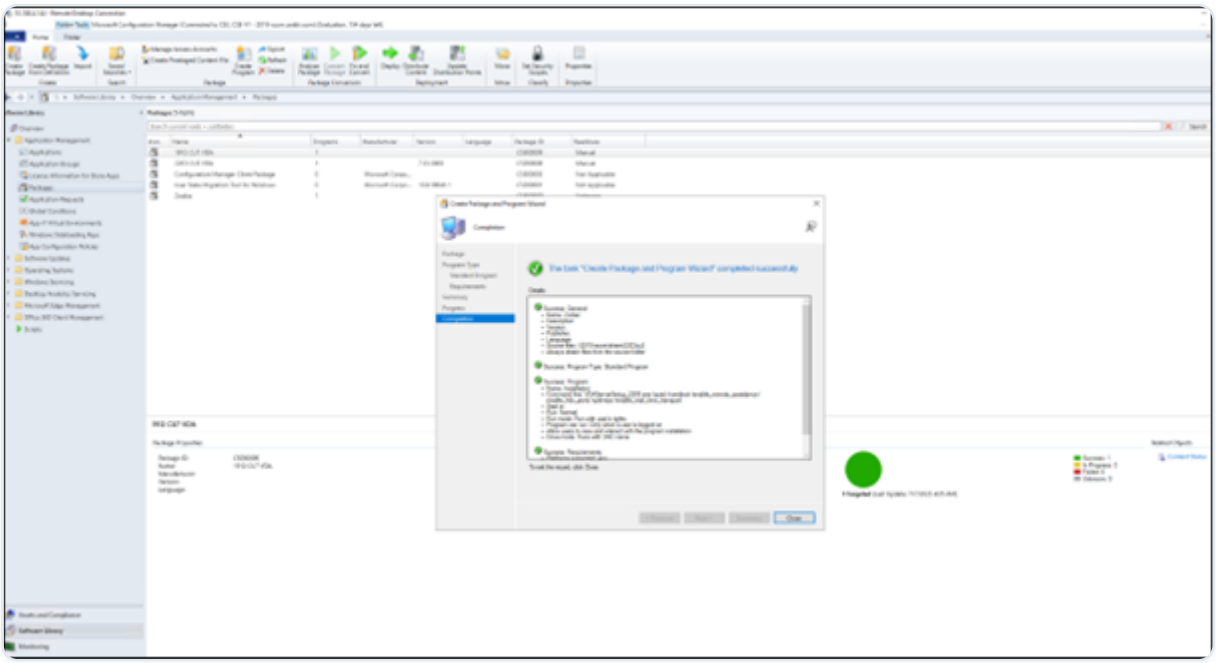
3. 必要なパッケージの種類を選択します。



4. パッケージの**名前**と**コマンドライン**を入力します。



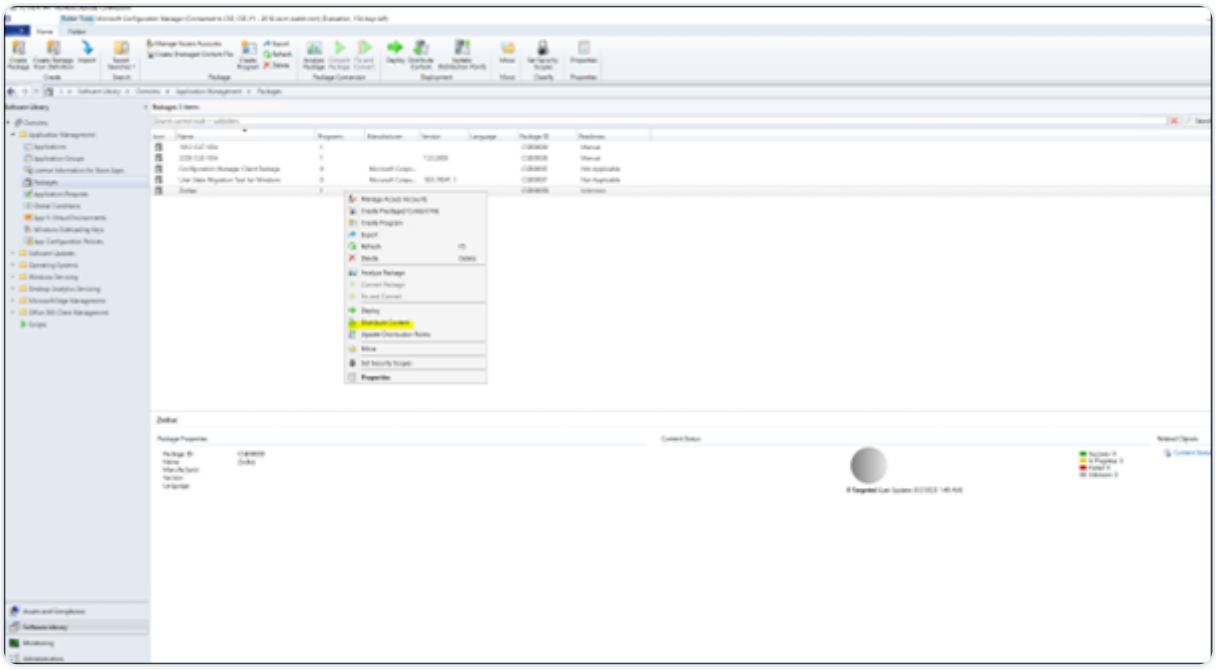
5. **Next**をクリックします。



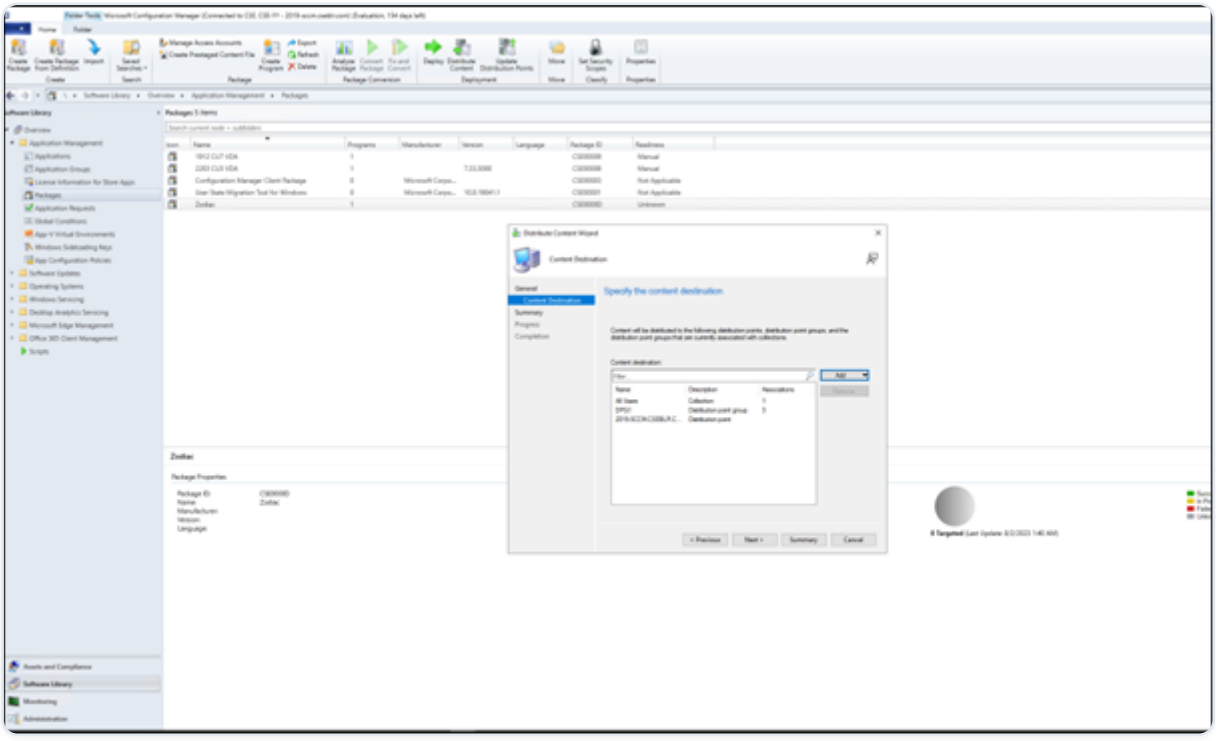
詳細については、Microsoft ドキュメントのConfiguration Manager のパッケージとプログラムを参照してください。

コンテンツの配布

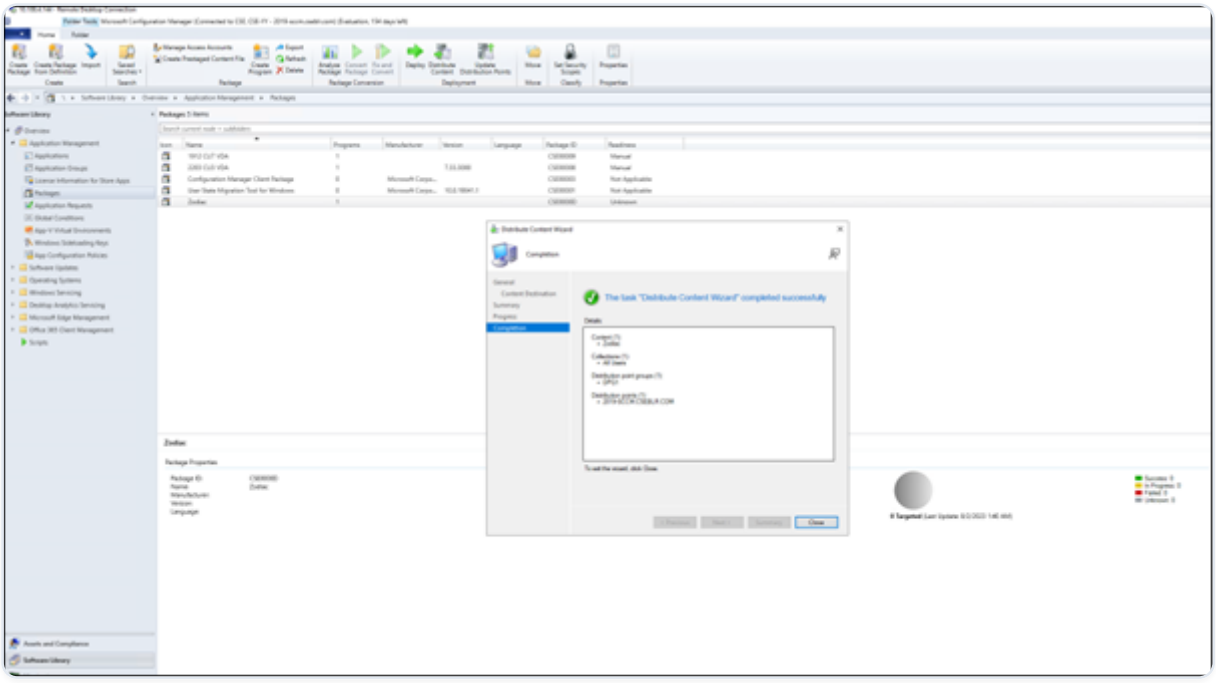
1. 作成したパッケージ名を右クリックします。
2. **コンテンツの配布**を選択します。



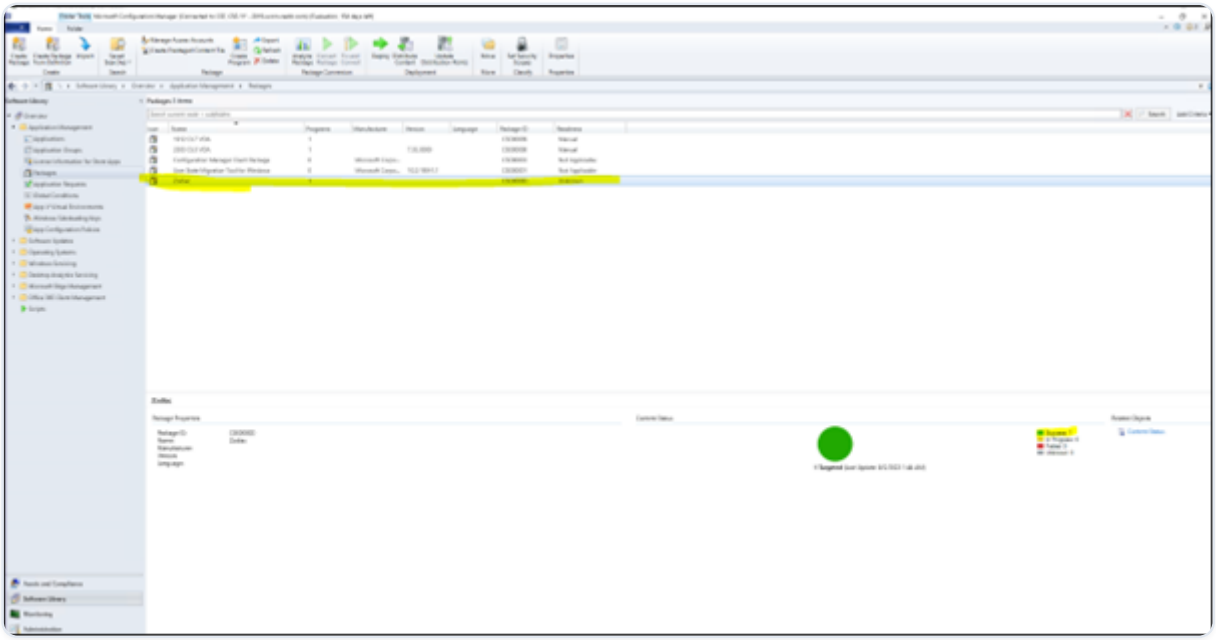
3. **コンテンツの配布ウィザード**ウィンドウで、作成したパッケージのソースファイルの場所を選択します。この例では、`2019-SCCM` です。**次へ**をクリックします。



4. パッケージ (この例では、`Zodiac`) が展開可能であることを確認します。



以下の画像は、パッケージが展開可能であることを示しています。

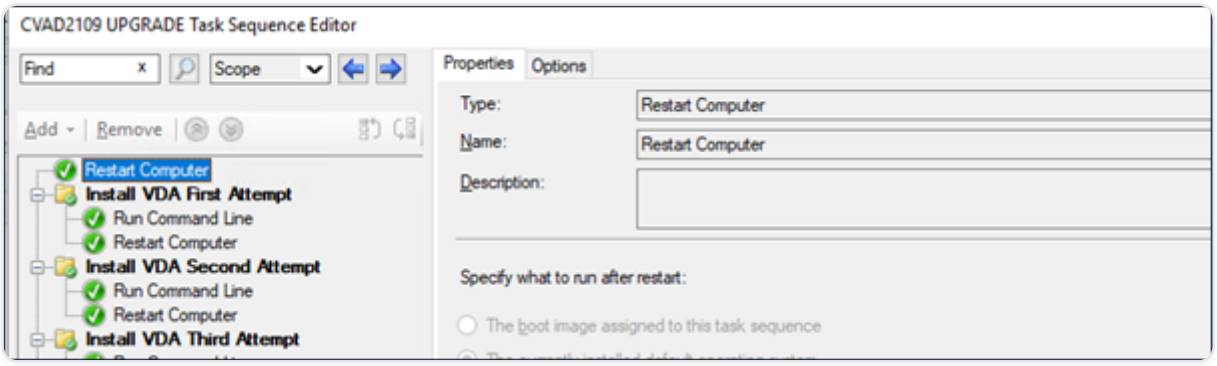


詳細については、Microsoft ドキュメントの「Configuration Manager のコンテンツの展開と管理」を参照してください。

SCCM を使用したインストールシーケンスの例

次の例は、インストールシーケンスを示しています。

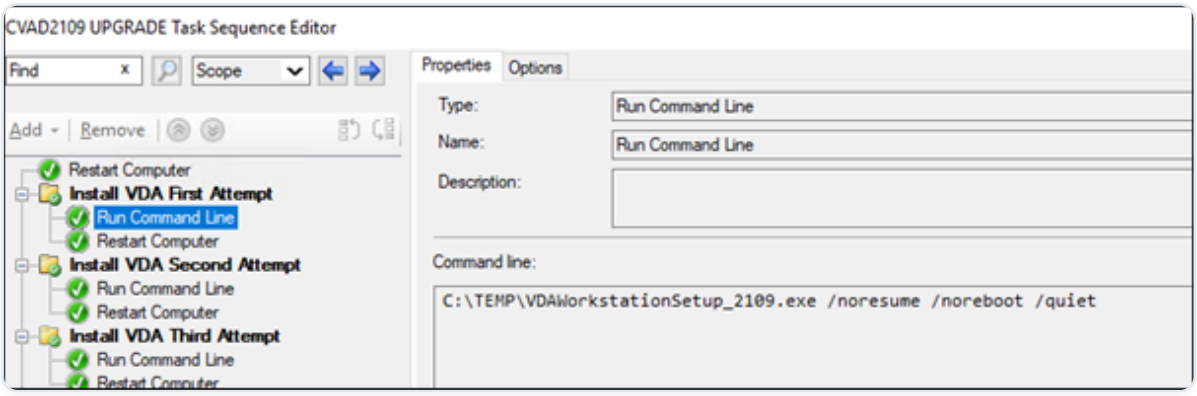
1. **コンピューターの再起動:** マシンを再起動して準備します。



2. **VDA のインストール (初回試行):** VDA のインストールを開始します。

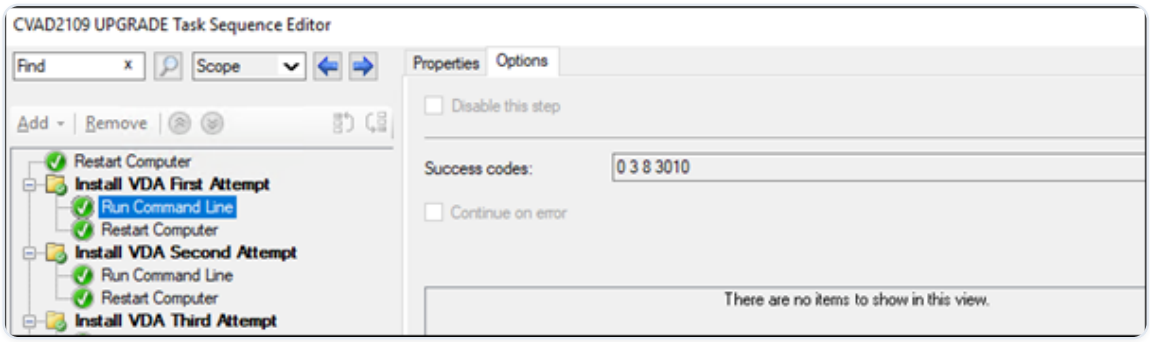
   a. コマンドラインオプションに `/quiet`、`/noreboot`、および `/noresume` オプションを追加します。

   b. 選択した VDA インストーラー (ローカルイメージまたは最小インストーラーのいずれか) を実行します。

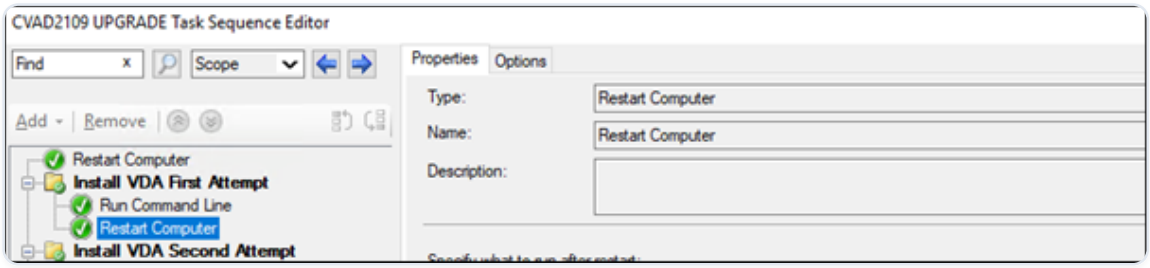


   c. SCCM はリターンコードをキャプチャする必要があります。

   - リターンコードが 0 または 8 の場合、インストールは完了しており、再起動が必要です。



   - リターンコードが 3 の場合は、マシンを再起動してから、**VDA のインストール (2 回目の試行)** に制御を渡します。



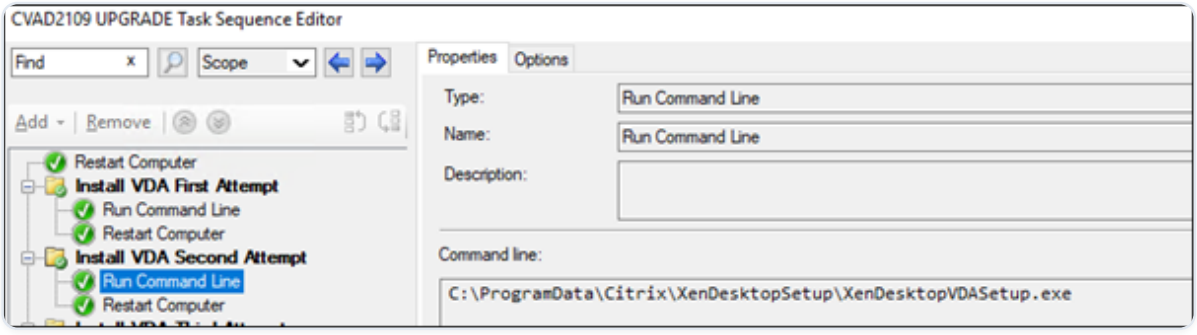
3. **VDAの2回目のインストール:** VDAのインストールを続行します。

   a. **VDAの1回目のインストール**の後、ファイル `%programdata%\Citrix\XenDesktopSetup\CitrixVirtualDesktopAgent.xml` が存在する場合、インストールは完了しておらず、再起動が完了した後に続行する必要があります。



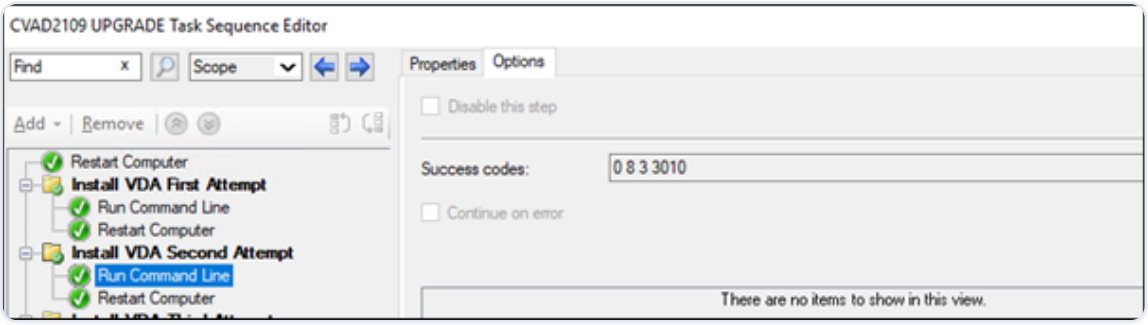
   b. **VDAの2回目のインストール**は、ファイル `%programdata%\Citrix\XenDesktopSetup\CitrixVirtualDesktopAgent.xml` が存在しなくなるか、0または8以外のリターンコードが返されるまで繰り返されます。その他のリターンコードはエラーとして扱い、VDAの2回目のインストールはエラーを報告して停止する必要があります。

   c. 適切なVDAインストーラー（ほとんどの場合 `XenDesktopVdaSetup.exe`、または `VDAWorkstationCoreSetup_XXXX.exe` が使用された場合は `XenDesktopRemotePCSetup.exe`）を、コマンドラインパラメーターなしでファイル `%programdata%\ Citrix\XenDesktopSetup\` ディレクトリから実行して、VDAのインストールを再開します。（VDAインストーラーは、インストーラーの初回実行時に保存されたパラメーターを使用します。）



d. VDAインストーラーからのリターンコードを確認します。

- 0または8：成功、インストール完了、再起動が必要です。



- 3：インストールは完了していません。マシンを再起動し、ファイル `%programdata%\Citrix\XenDesktopSetup\CitrixVirtualDesktopAgent.xml` が存在しなくなるか、0または8が返されるまでVDAの2回目のインストールを繰り返します。その他のリターンコードはエラーとして扱い、VDAの2回目のインストールはエラーを報告して終了する必要があります。

リターンコードの詳細については、Citrixインストールリターンコードを参照してください。

VDAインストールコマンドの例

利用可能なインストールオプションは、使用するインストーラーによって異なります。コマンドラインオプションの詳細については、以下の記事を参照してください。

- VDAのインストール
- コマンドラインを使用したインストール

Remote PC Access のインストールコマンド

- 次のコマンドは、シングルセッションコア VDA インストーラー（`VDAWorkstationCoreSetup.exe`）を使用します。

  ```
  VDAWorkstationCoreSetup.exe /quiet /controllers “control.domain.com” /enable_hdx_ports /noresume /noreboot
  ```

- 次のコマンドは、シングルセッションフル VDA インストーラー（`VDAWorkstationSetup.exe`）を使用します。

  ```
  VDAWorkstationSetup.exe /quiet /remotepc /physicalmachine /controllers “control.domain.com” /enable_hdx_ports /noresume /noreboot
  ```

専用 VDI のインストールコマンド

- 次のコマンドは、シングルセッションフル VDA インストーラー（`VDAWorkstationSetup.exe`）を使用します。

  ```
  VDAWorkstationSetup.exe /quiet /components vda /controllers “control.domain.com” /enable_hdx_ports /enable_remote_assistance /noresume /noreboot
  ```

スクリプトを使用してVDAをインストールする

> **注:**
>
> Citrixは、お客様の運用環境に合わせて調整されたスクリプトによって引き起こされる問題について責任を負いません。インストール関連のCitrixの問題については、Citrixサポートポータルを使用して、関連するインストールログとともにテクニカルサポートケースをオープンしてください。

> この記事は、Windowsオペレーティングシステムを搭載したマシンにVDAをインストールする場合に適用されます。Linuxオペレーティングシステム用VDAの詳細については、Linux Virtual Delivery Agentのドキュメントを参照してください。

インストールメディアには、Active Directory内のマシンにVirtual Delivery Agent (VDA) をインストール、アップグレード、または削除するサンプルスクリプトが含まれています。これらのスクリプトは、Machine Creation Services™およびCitrix Provisioning (旧Provisioning Services) で使用されるマスターイメージの保守にも使用できます。

必要なアクセス権:

- スクリプトには、VDAインストールコマンドが配置されているネットワーク共有への「Everyone読み取り」アクセス権が必要です。インストールコマンドは、製品版ISOでは`XenDesktopVdaSetup.exe`、スタンドアロンインストーラーでは`VDAWorkstationSetup.exe`または`VDAServerSetup.exe`です。
- ログの詳細は各ローカルマシンに保存されます。レビューと分析のために結果を集中してログに記録するには、スクリプトに適切なネットワーク共有への「Everyone読み取り/書き込み」アクセス権が必要です。

スクリプト実行の結果を確認するには、中央ログ共有を調べます。キャプチャされたログには、スクリプトログ、インストーラーログ、MSIインストールログが含まれます。各インストールまたは削除の試行は、タイムスタンプ付きのフォルダーに記録されます。フォルダーのタイトルは、PASSまたはFAILのプレフィックスで操作結果を示します。標準のディレクトリ検索ツールを使用して、中央ログ共有で失敗したインストールまたは削除を見つけることができます。これらのツールは、ターゲットマシンでローカルに検索する代替手段を提供します。

インストールを開始する前に、インストールの準備のタスクを読み、完了してください。

スクリプトを使用してVDAをインストールまたはアップグレードする

1. インストールメディアの`\Support\AdDeploy\`からサンプルスクリプト**InstallVDA.bat**を入手します。Citrixは、スクリプトをカスタマイズする前に元のスクリプトのバックアップを作成することをお勧めします。
2. スクリプトを編集します:
   - インストールするVDAのバージョンを指定します: `SET DESIREDVERSION`。完全な値は、インストールメディアのProductVersion.txtファイルに記載されています。ただし、完全に一致している必要はありません。
   - インストーラーが呼び出されるネットワーク共有を指定します。レイアウトのルート（ツリーの最上位）を指します。スクリプトの実行時に、適切なバージョンのインストーラー（32ビットまたは64ビット）が自動的に呼び出されます。例: `SET DEPLOYSHARE=\\fileserver1\share1`。
   - オプションで、集中ログを保存するためのネットワーク共有の場所を指定します。例: `SET LOGSHARE=\\fileserver1\log1)`。
   - コマンドラインを使用したインストールで説明されているように、VDA構成オプションを指定します。`/quiet`と`/noreboot`オプションはスクリプトにデフォルトで含まれており、必須です: `SET COMMANDLINEOPTIONS=/QUIET /NOREBOOT /NORESUME`。
3. グループポリシーのスタートアップスクリプトを使用して、スクリプトをマシンを含むOUに割り当てます。このOUには、VDAをインストールするマシンのみを含める必要があります。そのOU内のマシンが再起動されると、スクリプトはすべてのマシンで実行されます。サポートされているオペレーティングシステムを持つ各マシンにVDAがインストールされます。

スクリプトを使用してVDAを削除する

1. インストールメディアの`\Support\AdDeploy\`からサンプルスクリプトUninstallVDA.batを入手します。Citrixは、スクリプトをカスタマイズする前に元のスクリプトのバックアップを作成することをお勧めします。

2. スクリプトを編集します。
   - 削除するVDAのバージョンを指定します: `SET CHECK\_VDA\_VERSION`。完全な値は、インストールメディアのProductVersion.txtファイル（例: 7.0.0.3018）で確認できます。ただし、完全一致は必須ではありません。
   - オプションで、集中ログを保存するためのネットワーク共有の場所を指定します。
3. グループポリシーのスタートアップスクリプトを使用して、スクリプトをマシンを含むOUに割り当てます。このOUには、VDAを削除するマシンのみを含める必要があります。OU内のマシンが再起動されると、スクリプトはすべてのマシンで実行されます。各マシンからVDAが削除されます。

トラブルシューティング

- スクリプトは、スクリプトの実行状況を記述する内部ログファイルを生成します。スクリプトは、展開開始から数秒以内に`Kickoff_VDA_Startup_Script`ログを中央ログ共有にコピーします。これにより、全体的なプロセスが機能していることを確認できます。このログが期待どおりに中央ログ共有にコピーされない場合は、ローカルマシンを検査してさらにトラブルシューティングを行ってください。スクリプトは、各マシンの`%temp%`フォルダーに2つのデバッグログファイルを配置します。
  - `Kickoff_VDA_Startup_Script_<DateTimeStamp>.log`
  - `VDA_Install_ProcessLog_<DateTimeStamp>.log`

  これらのログを確認して、スクリプトが次の状態であることを確認します。
  - 期待どおりに実行されている。
  - ターゲットオペレーティングシステムを適切に検出している。
  - `DEPLOYSHARE`共有の`ROOT`を指すように正しく構成されている（`AutoSelect.exe`という名前のファイルが含まれている）。
  - `DEPLOYSHARE`と`LOG`の両方の共有に対して認証できる。
- コンポーネントインストールの結果をCitrixがどのように報告するかについては、Citrixインストールリターンコードを参照してください。
- デリバリーグループのStudio表示では、「**詳細**」ペインの「**インストール済みVDAバージョン**」エントリが、マシンにインストールされているバージョンと異なる場合があります。マシンのプログラムと機能の表示には、実際のVDAバージョンが表示されます。
- VDAがインストールされた後、Delivery Controllerに登録されるまで、ユーザーにアプリやデスクトップを配信することはできません。

VDAの登録方法と登録の問題のトラブルシューティング方法については、「VDA登録」を参照してください。

サードパーティ製VDAの展開方法

Microsoft System Center Configuration Manager (SCCM) や、Ansible、Microsoft Intune などの類似のソフトウェア配布ツールを使用して Virtual Delivery Agent (VDA) を正常に展開するには、Citrix® はVDAインストーラーを段階的に使用することをお勧めします。

> **注:**
>
> 以下の記事では、Citrix が環境をテストした方法に基づいた推奨事項のみを説明しています。これらの手順は、お客様のニーズに合わせてカスタマイズできます。Citrix は、お客様のニーズに合わせてこれに必要な更新や調整について責任を負いません。

- SCCM を使用した VDA のインストール
- Ansible を使用した VDA のインストール
- Microsoft Intune を使用した VDA のインストール

Ansible を使用した VDA のインストール

概要

この記事では、Ansible を使用して VDA を展開する方法について説明します。詳細については、Ansible ドキュメントを参照してください。

> **注：**
>
> この記事は、Citrix® が環境をテストした方法に基づいた推奨事項のみを説明しています。これらの手順は、お客様のニーズに合わせてカスタマイズできます。Citrix は、お客様のニーズに合わせて必要な更新や調整について責任を負いません。

Ansible を使用して VDA を展開するための主要な手順

1. 仮想マシン環境の構成。
2. Ansible のインストール
3. Kerberos の構成

a. Kerberos のインストール

b. Kerberos の構成

4. Ansible の構成

ステップ 1: 仮想マシン環境を構成する

Windows サーバーで次のコマンドを実行します。

1. PS RemoteSigned を設定します。 `Set-ExecutionPolicy RemoteSigned`
2. WinRM を暗号化なしで使用するように設定します。 `winrm set winrm/config/service '@{AllowUnencrypted="true"}'`

> **注：**
>
> このステップでエラーが発生した場合は、次のコマンドを使用します。 `Enable-PSRemoting -Force`

3. ファイアウォールポート5985を開きます。 `New-NetFirewallRule -DisplayName "Allow WinRm port 5985" -Direction Inbound -Profile Any -Action Allow -LocalPort 5985 -Protocol tcp`

ステップ2：ANSIBLEのインストール

Ubuntu 20.4以降でAnsibleをインストールするには、次のコマンドを実行します。

- `sudo apt update`
- `sudo apt install software-properties-common`
- `sudo add-apt-repository --yes --update ppa:ansible/ansible`
- `sudo apt install ansible`
- `sudo apt install python3-pip`

ステップ2I：KERBEROSのインストール

Kerberosをインストールするには、次のコマンドを実行します。

`sudo apt install python3-dev libkrb5-dev krb5-user`

ステップ2II：KERBEROSの構成

Kerberosを構成するには、次のコマンドを実行します。

`Edit /etc/krb5.conf`

```
[libdefaults]
        default_realm = [redacted]

# The following krb5.conf variables are only for MIT Kerberos.
        kdc_timesync = 1
        ccache_type = 4
        forwardable = true
        proxiable = true

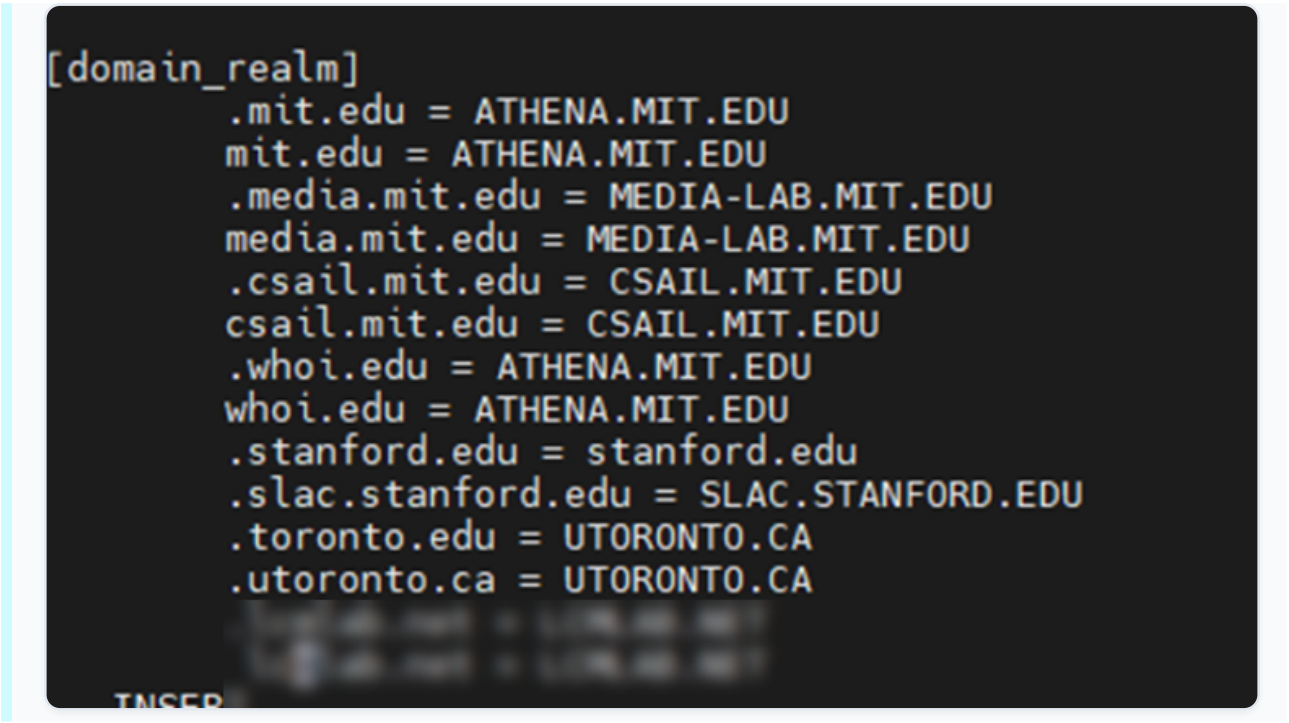
# The following encryption type specification will be used by MIT Kerberos
# if uncommented.  In general, the defaults in the MIT Kerberos code are
# correct and overriding these specifications only serves to disable new
# encryption types as they are added, creating interoperability problems.
#
# The only time when you might need to uncomment these lines and change
# the enctypes is if you have local software that will break on ticket
# caches containing ticket encryption types it doesn't know about (such as
# old versions of Sun Java).

#       default_tgs_enctypes = des3-hmac-sha1
#       default_tkt_enctypes = des3-hmac-sha1
#       permitted_enctypes = des3-hmac-sha1

# The following libdefaults parameters are only for Heimdal Kerberos.
        fcc-mit-ticketflags = true

[realms]
        LTSRLAB.NET = {
                kdc = [redacted]
                admin_server = [redacted]
        }
        ATHENA.MIT.EDU = {
                kdc = [redacted]
```

> **注：**
>
> Kerberosレルム名には大文字を使用します。



ステップ3：ANSIBLEの構成

Ansibleホストを構成するには、次の手順を実行します。

1. 次のコマンドを実行します。

   `Edit /etc/ansible/hosts`

2. Delivery Controller `Install.yaml` ファイルを構成します

   `/QUIET /NOREBOOT /NORESUME /OPTIMIZE /VERBOSELOG /COMPONENTS VDA /CONTROLLERS 'MyDDC.xd.local' /ENABLE_HDX_PORTS /ENABLE_REAL_TIME_TRANSPORT`

「デリバリーコントローラー」(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/delivery-controller-yaml-1.png)

「デリバリーコントローラー」(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/delivery-controller-yaml-2.png)

「デリバリーコントローラー」(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/delivery-controller-yaml-3.png)

「デリバリーコントローラー」(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/delivery-controller-yaml-4.png)

1. 以下のコマンドでyamlファイルを実行します。 `sudo ansible-playbook install.yml -vvv` (詳細モード)
2. 設定ファイルで、他の追加設定とともに複数のホストを構成できます。

`Edit /etc/ansible/hosts`

「Ansibleホスト」(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/ansible-hosts.png)

Microsoft Intune を使用した VDA のインストール

概要

この記事では、Microsoft Intune を使用して VDA を展開する方法について説明します。詳細については、Microsoft のドキュメントを参照してください。

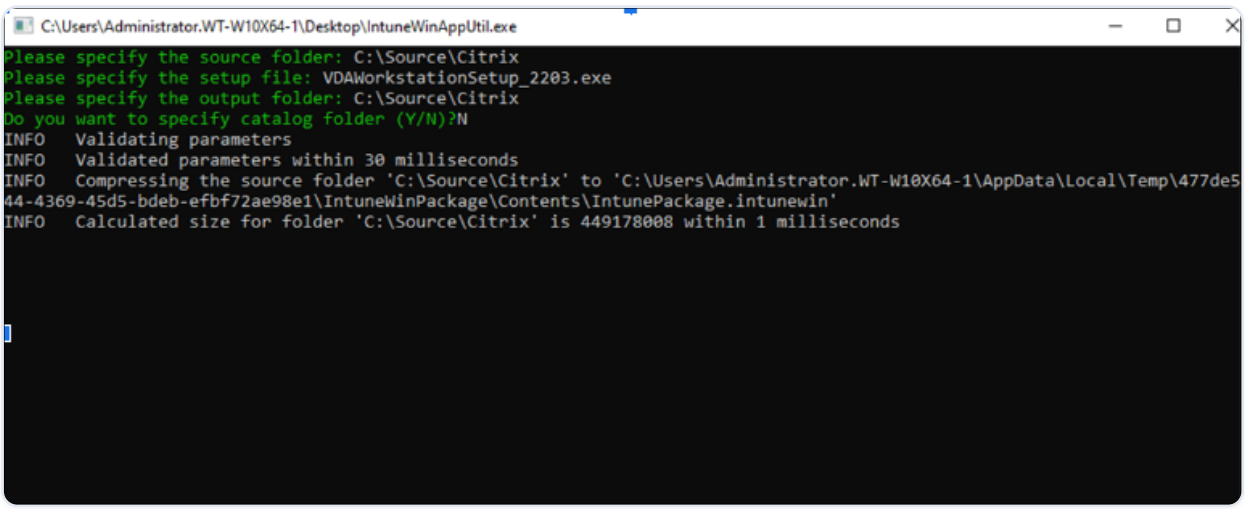
> **注：**
>
> 以下の記事は、Citrix® が環境をテストした方法に基づいた推奨事項のみを説明しています。これらの手順は、お客様のニーズに合わせてカスタマイズできます。Citrix は、お客様のニーズに合わせてこれに必要な更新や調整について責任を負いません。

Microsoft Intune を使用して VDA を展開するための主要な手順

1. Citrix VDA のインストールを準備する。
2. Microsoft 365 Developer Program サブスクライバーを設定する。
3. アプリを追加して割り当てる。
4. 登録済みデバイスにアプリをインストールする。

ステップ 1: CITRIX VDA のインストールを準備する

1. 更新された IntuneWinAppUtil.exe を GitHub からダウンロードします。
2. **管理者として実行**を使用して `IntuneWinAppUtil.exe` ファイルを実行します。
3. 次のデータを入力します。



a. **ソースフォルダーを指定してください**: アプリケーションのセットアップファイルが含まれているフォルダーを入力します。例: C:\source\Citrix。

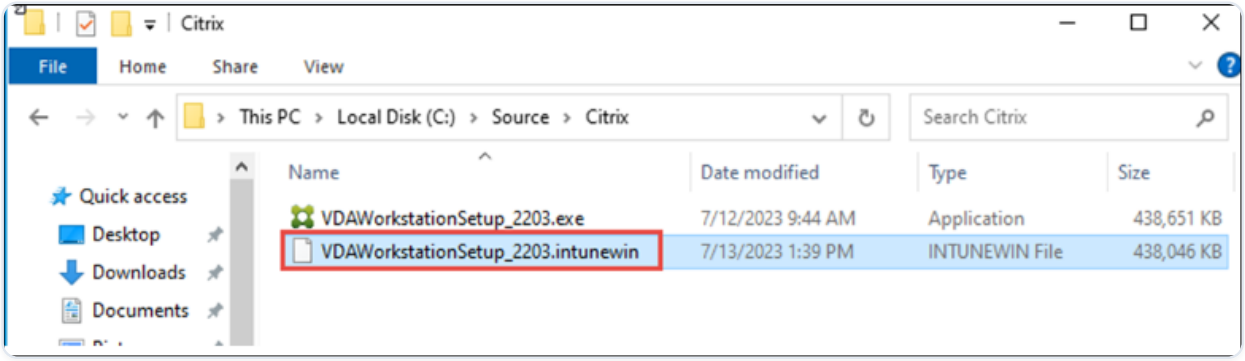
b. **セットアップファイルを指定してください**: セットアップファイル名 (setup.exe や setup.msi など) を入力します。例: VDAWorkstationSetup_2203.exe。

c. **出力フォルダーを指定してください**: .intunewin ファイルを生成する出力フォルダーのパスを入力します。例: C:\source\Citrix。

d. **カタログフォルダーを指定しますか (Y/N)**: N と入力します。

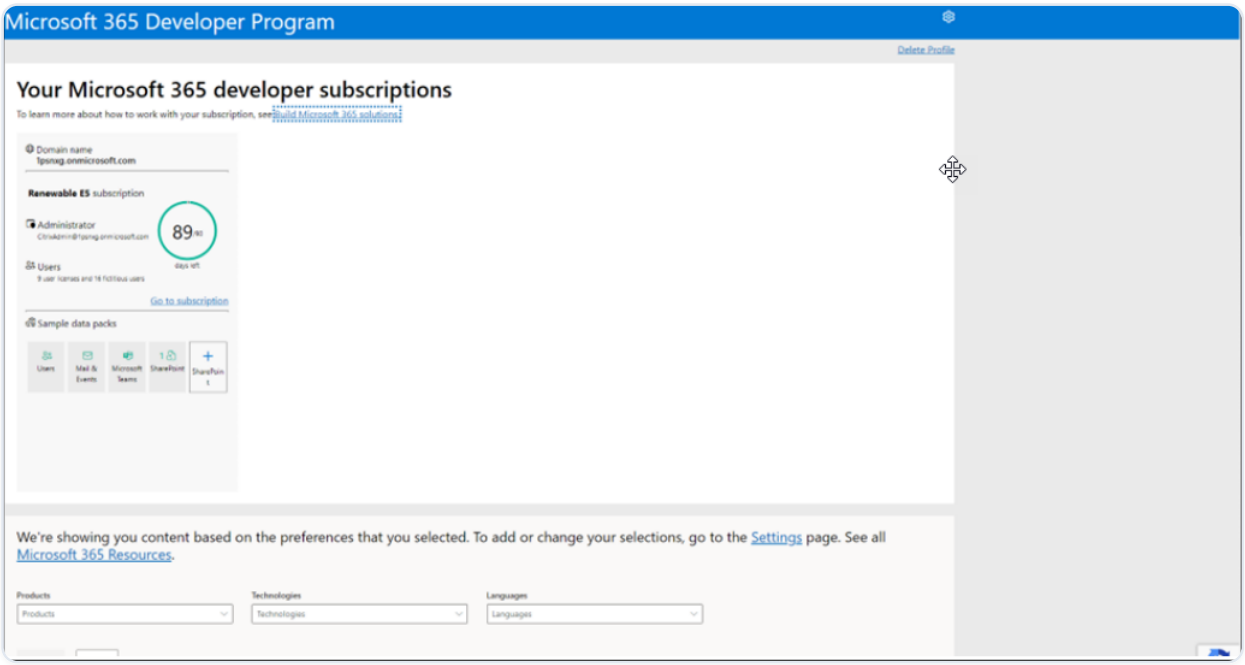
> **注：**
>
> **Win32 Content Prep Tool** の実行中は数分間お待ちください。`.intunewin` ファイルが生成されると、コマンドプロンプトの下部にステータスが 100% と表示されます。

4. プロセスが完了したら、出力フォルダー (この例では `C:\source\Citrix`) に移動して、Microsoft Intune 展開ファイルを取得します。
5. Microsoft Intune の無料試用版にサインアップします。

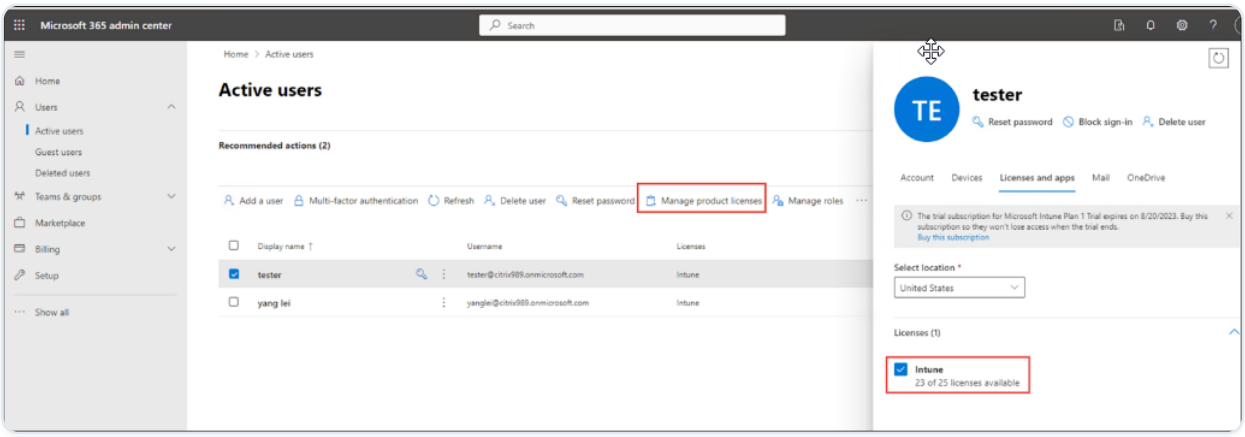


ステップ 2: MICROSOFT 365 DEVELOPER PROGRAM サブスクライバーを設定する

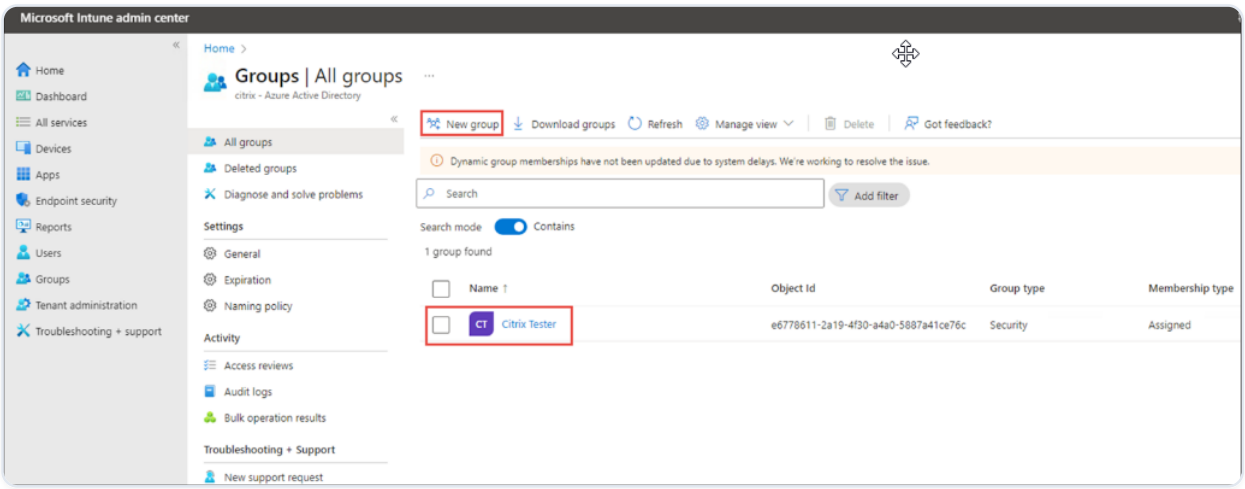
1. サブスクリプションをアクティブ化するために、インスタントサンドボックスを作成します。開発者サンドボックスを取得するには、Microsoft 365 Developer Program ダッシュボード に移動し、**新しいサブスクリプションの追加**を選択します。



2. Microsoft 365 管理センターでユーザーを作成し、そのユーザーにライセンスを割り当てます。



3. グループを作成します。



4. グループが作成されたら、そのグループに MDM 機関を提供する必要があります。自動登録を設定します。アクティブ化には 1 分ほどかかる場合があります。 または、次の手順を実行して、MDM 機関をグループに手動で追加することもできます。

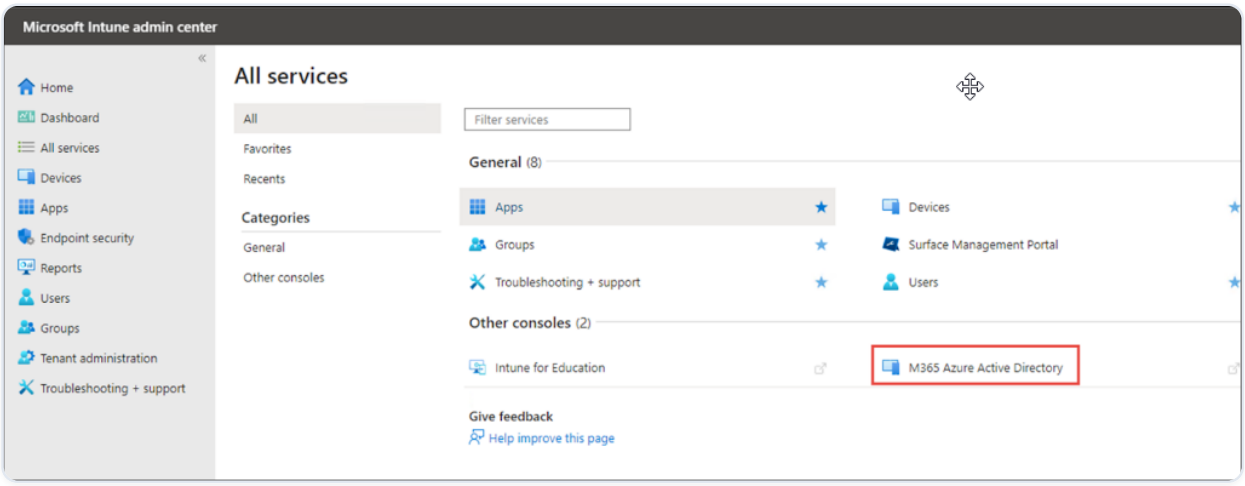
a. **すべてのサービス > Microsoft Entra** に移動します。

b. 「**設定 > モビリティ**」に移動し、「**Microsoft Intune**」を選択します。

c. 作成したばかりのグループを選択します。これにより、MDMユーザー範囲のページが開きます。

d. 「**保存**」をクリックします。

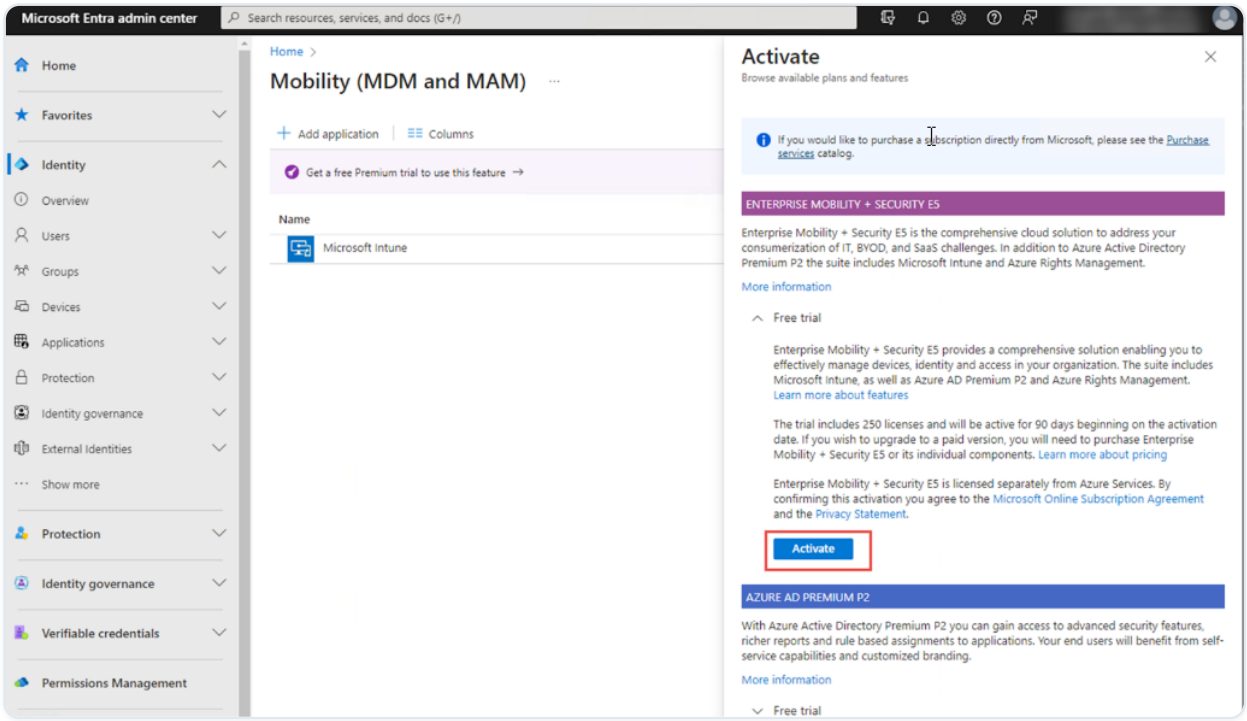
5. 「**すべてのサービス**」タブで、「**M365 Azure Active Directory**」をクリックします。



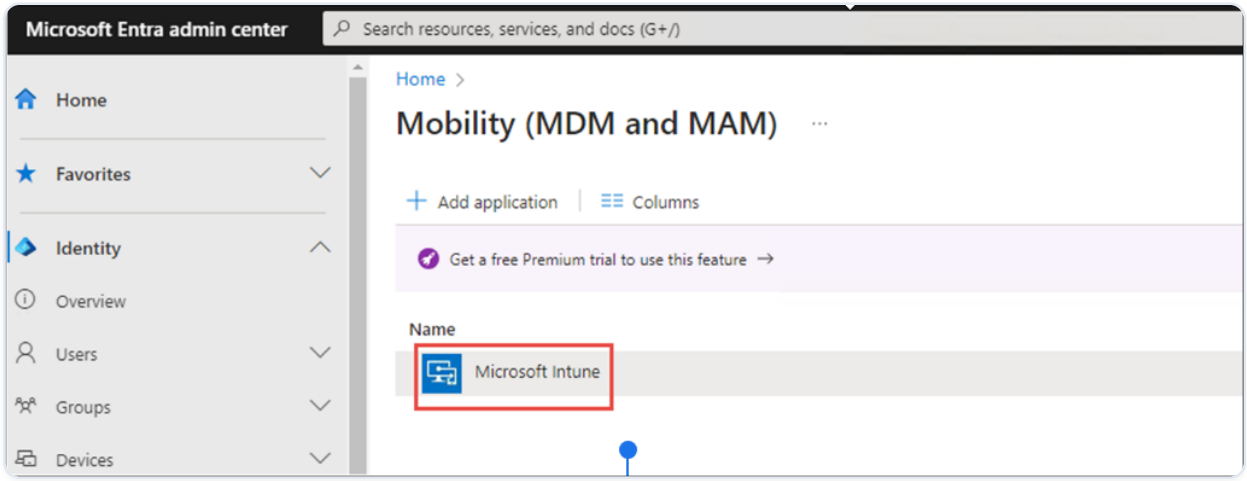
6. 「**この機能を使用するために無料のPremium試用版を入手**」をクリックします。



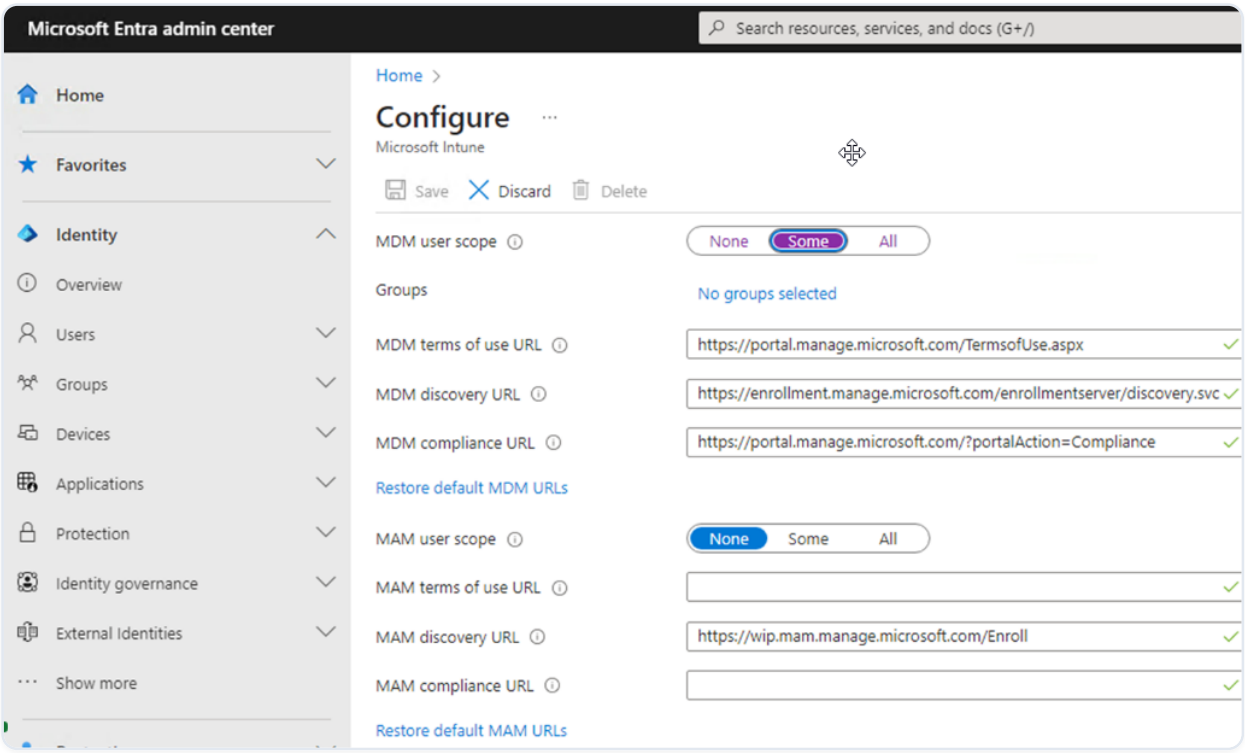
7. 「**アクティブ化**」をクリックします。



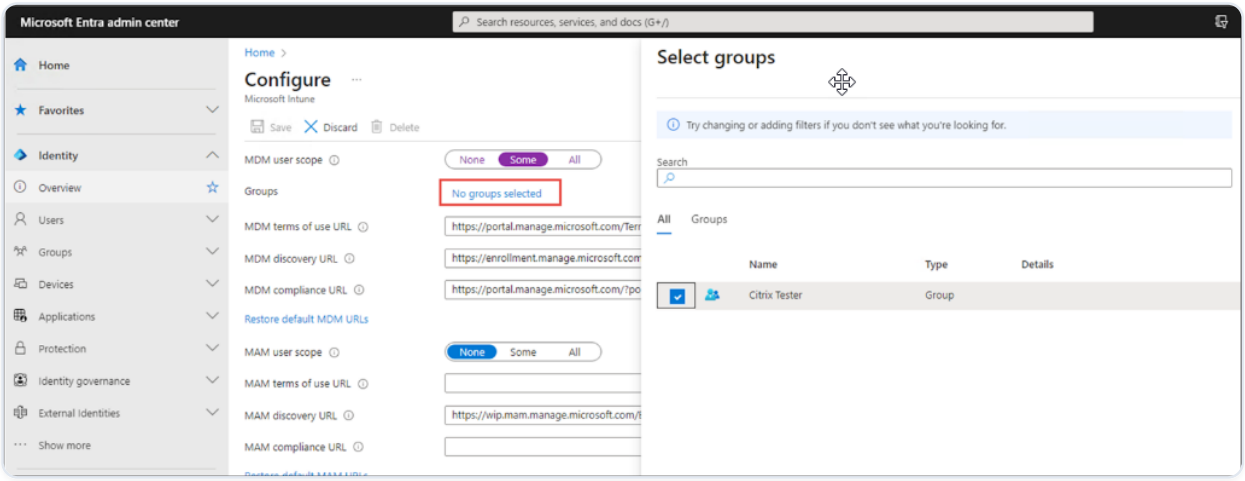
8. 次に、「**Microsoft Intune**」をクリックします。



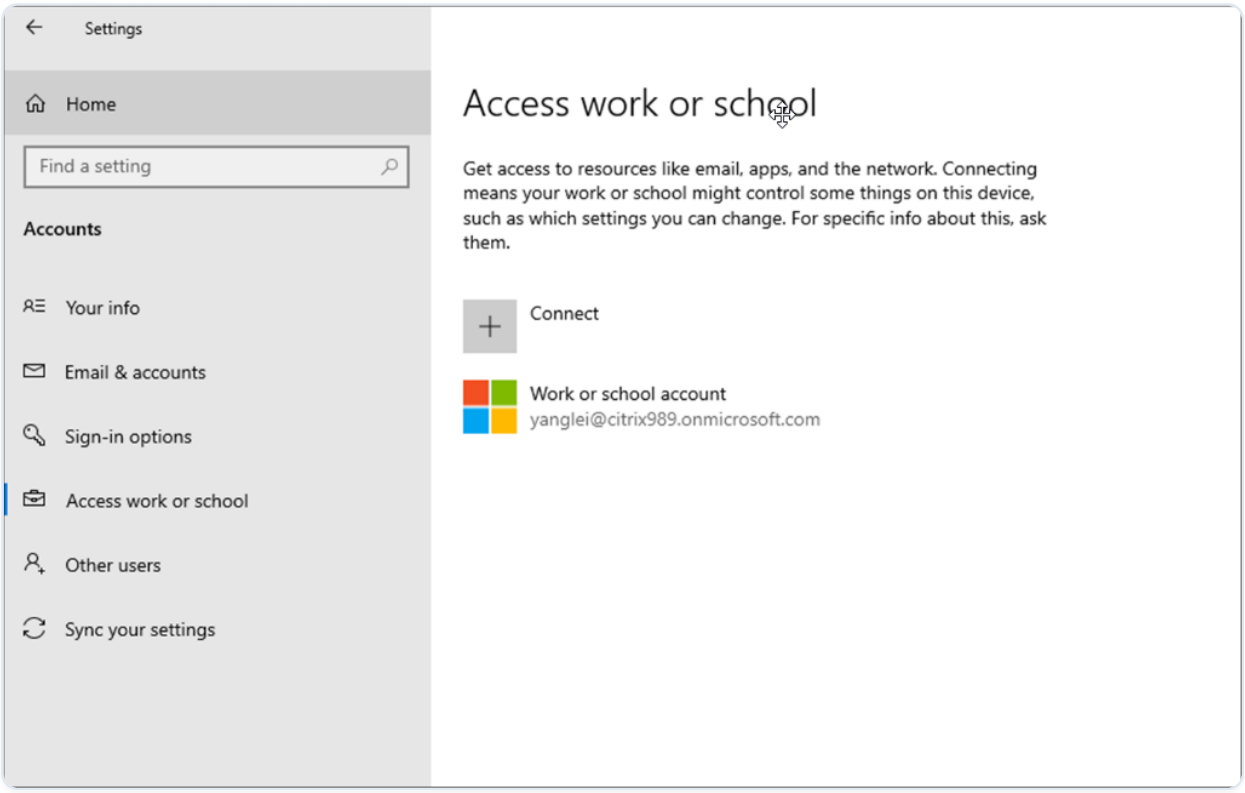
9. 「**構成**」タブで、必要な構成を入力します。



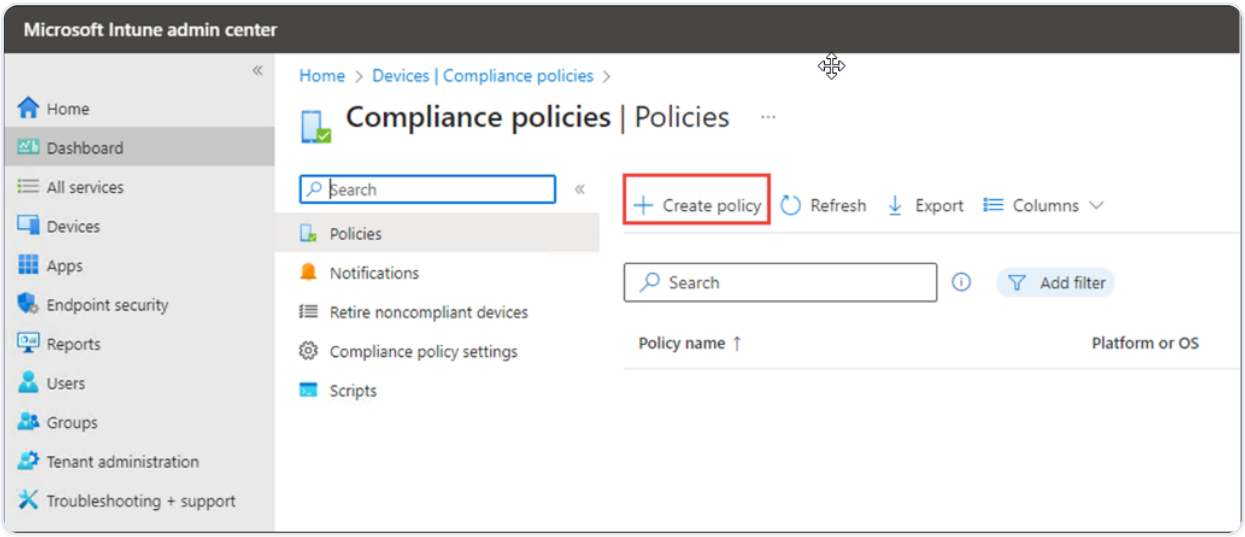
10. グループを追加するには、「**グループが選択されていません**」をクリックします。



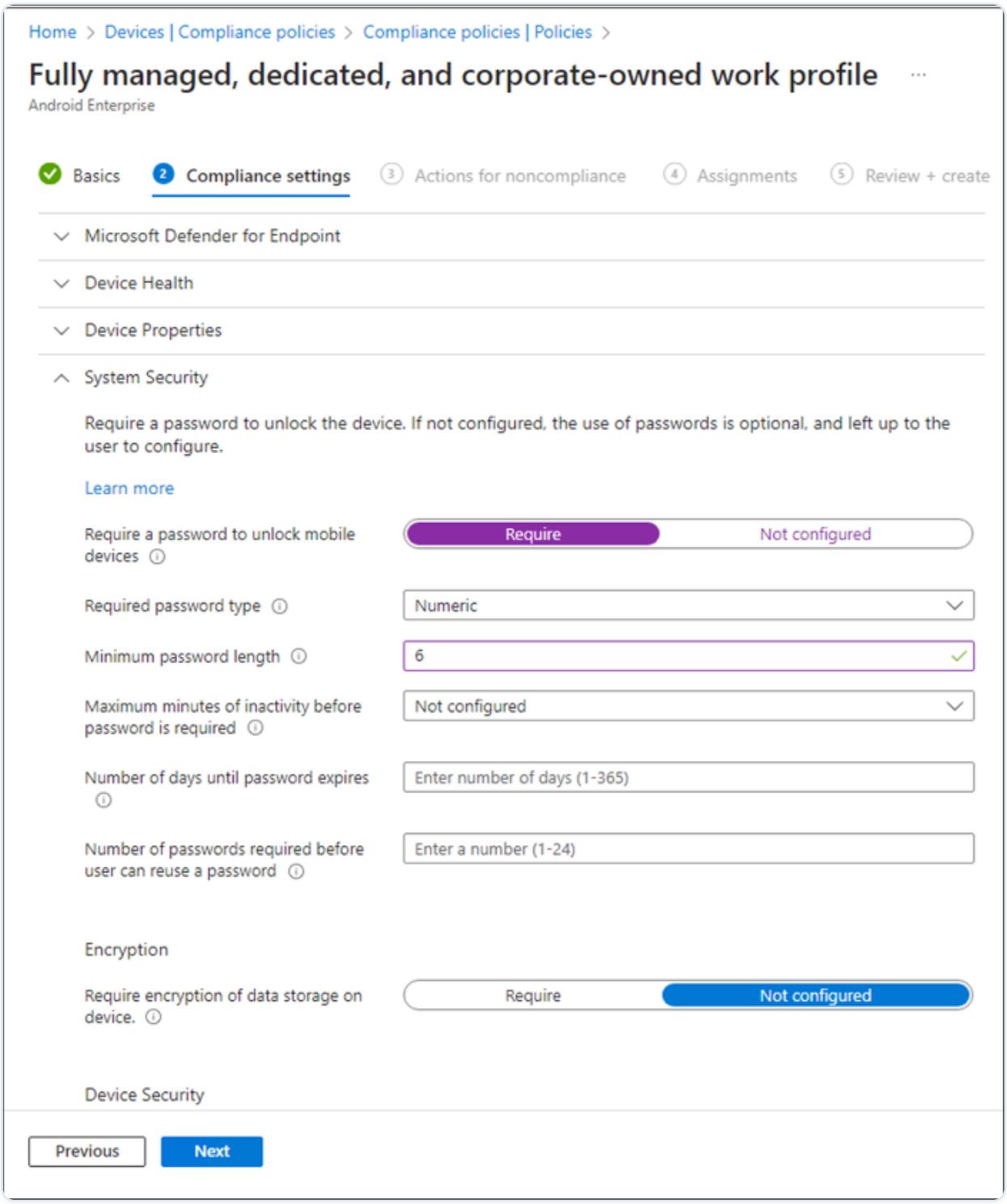
11. デバイスを登録します。



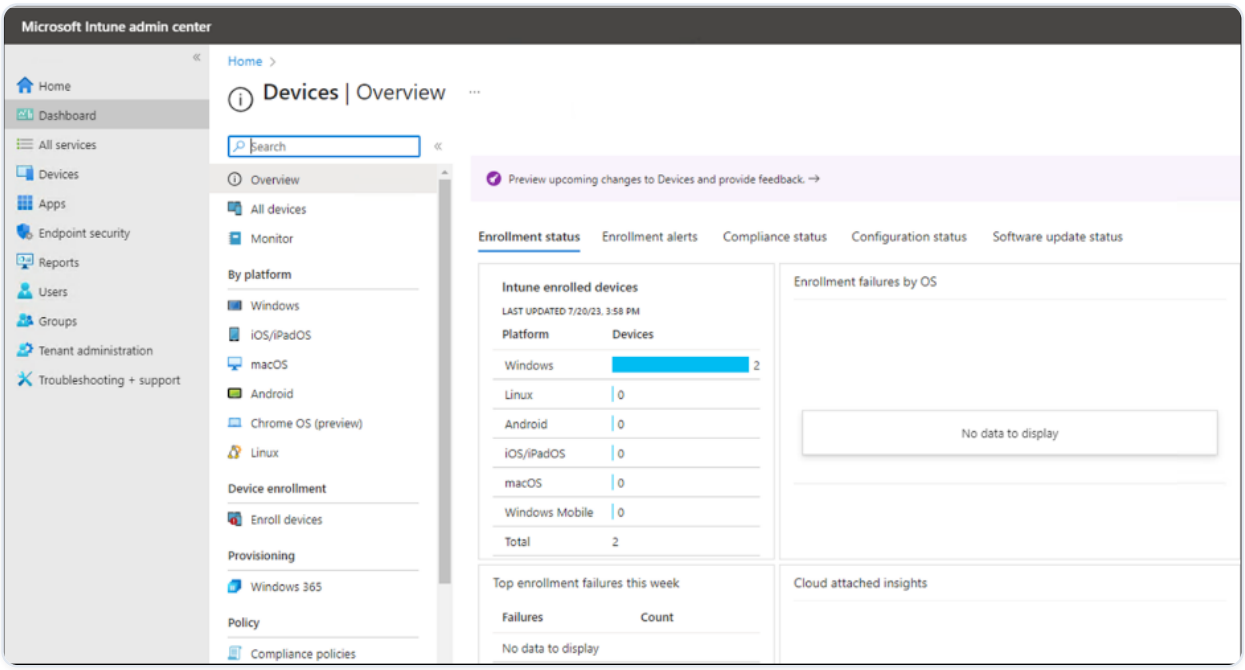
12. 新しく作成したデバイスのコンプライアンスを`Compliant`に変更するためのデバイスコンプライアンスポリシーを作成します。



13. 新しく作成したグループを追加するには、 タブに移動します。



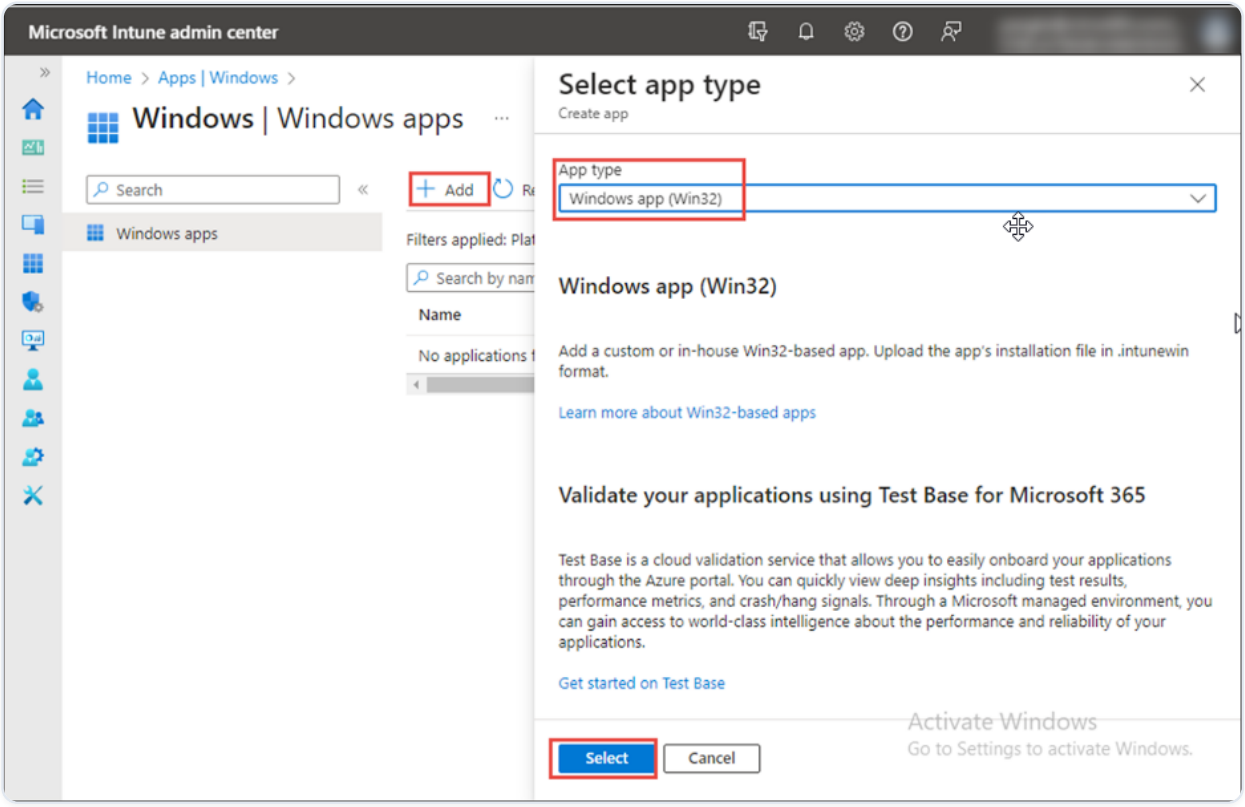
14. デバイスの登録を確認します。



詳細については、Microsoft 365 developer programを参照してください。

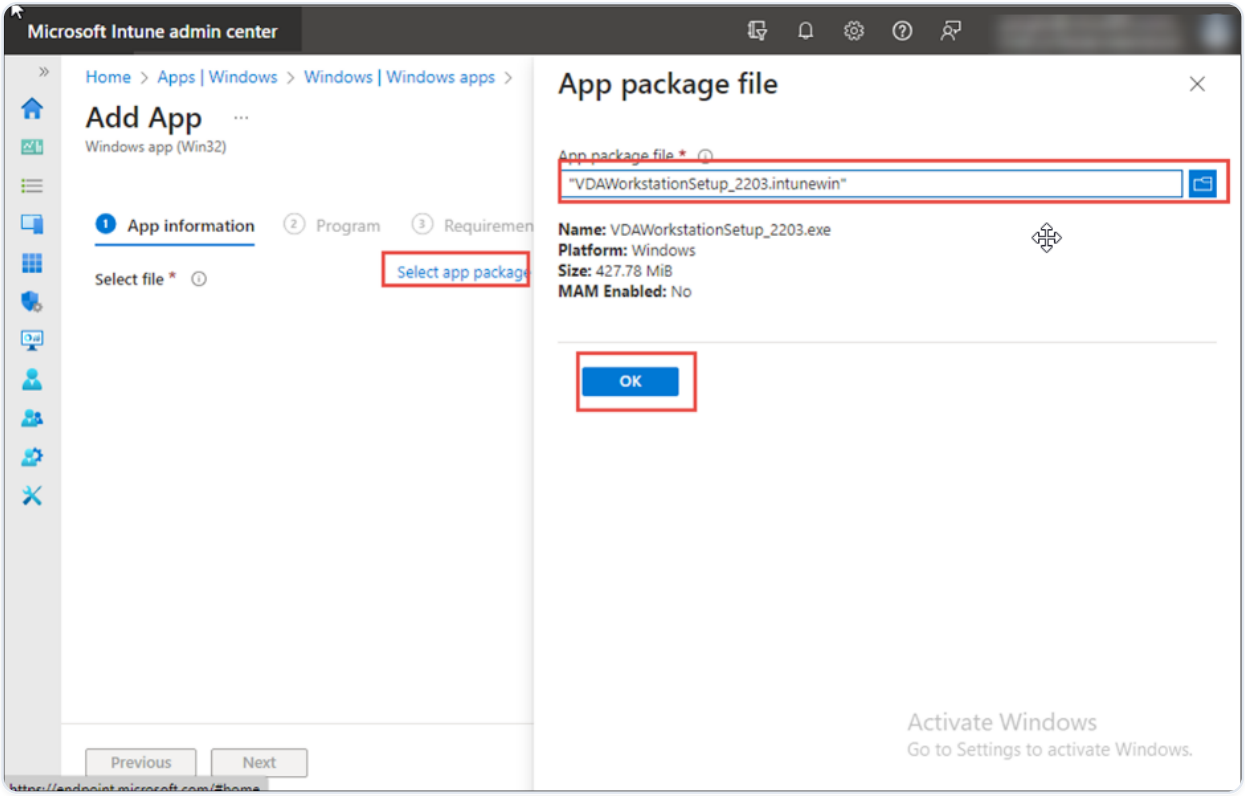
ステップ3：アプリの追加と割り当て

1. Microsoft Intune admin centerにサインインします。
2. **>** **>** を選択するか、 **>** **>** に移動します。



3. ペインで、 **>** を選択し、 をクリックします。
4. ペインで、 をクリックします。 をクリックします。

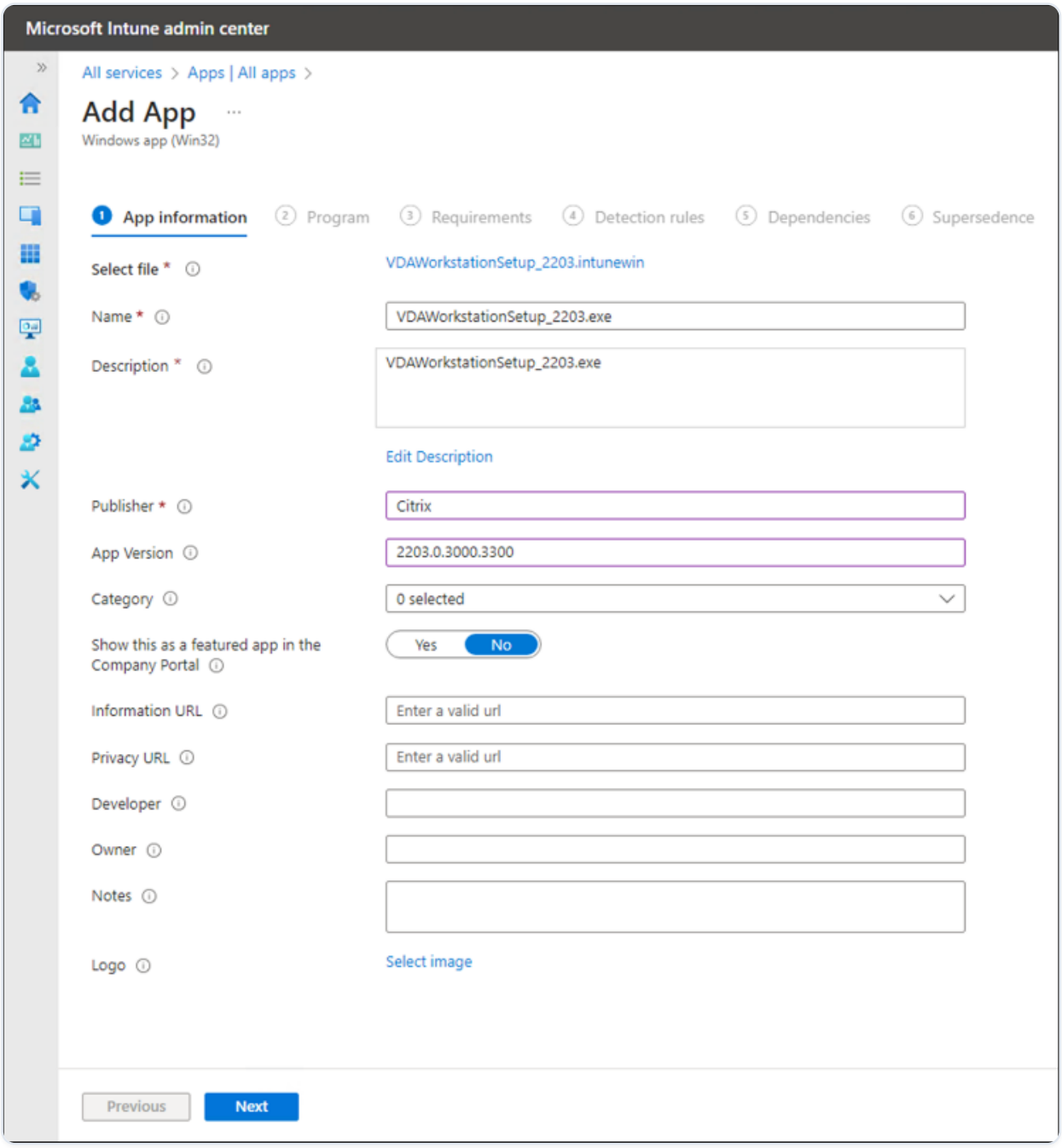
5. 拡張子`.intunewin`の準備済みファイルを選択します。準備済みファイルは、Citrix VDAのインストール準備のステップで作成されます。アプリに関する詳細情報を含むページが表示されます。



注：

- サーバーコアマシンを使用している場合は、VDAワークステーションコアを使用する必要があります。
- Windows 10デスクトップOSを使用している場合は、VDAワークステーションを使用する必要があります。
- サーバーOS（例：Windows 2022）を使用している場合は、VDAサーバーセットアップを使用する必要があります。
- この例ではバージョン2203を使用していますが、これはすべてのバージョンに適用できます。

6. **App package file**ペインで**OK**をクリックします。
7. 次の画面で、**App Information**タブの下にあるアプリの**Name**を入力し、Windowsアプリの**Description**を入力します。**Publisher**名として`Citrix`を入力し、ここで追加のアプリ情報を指定できます。**Next**をクリックします。

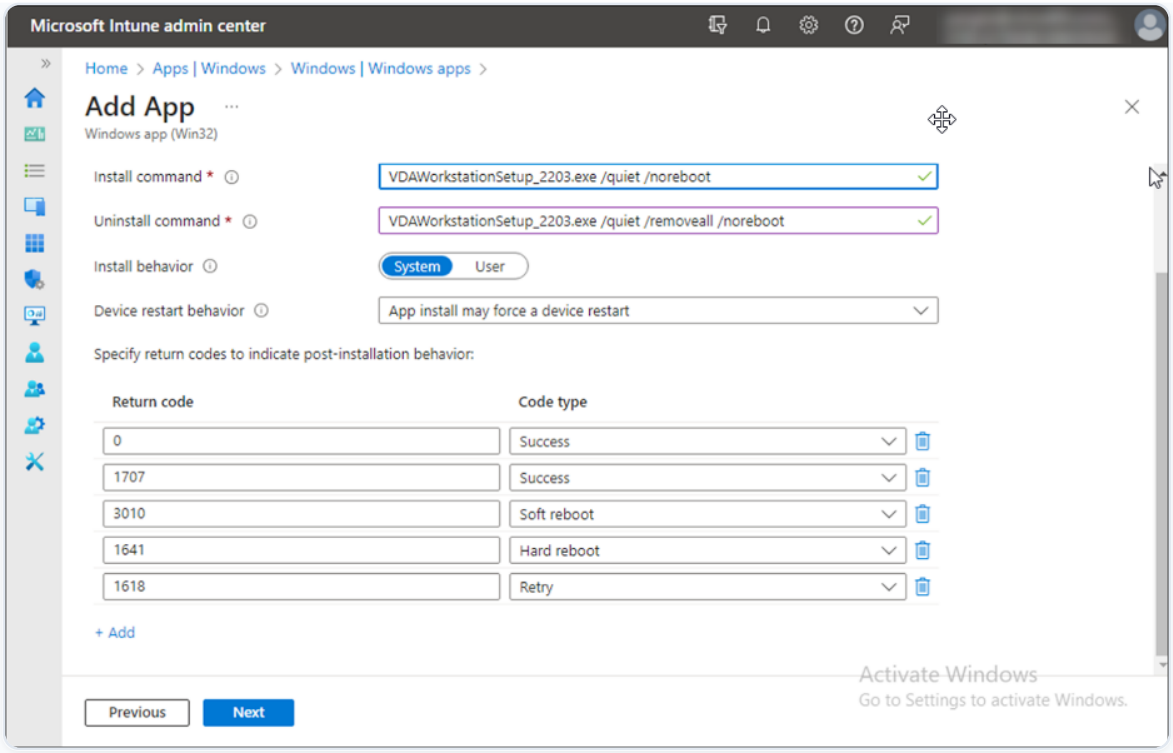


8. 次の画面で、次の値を入力します。

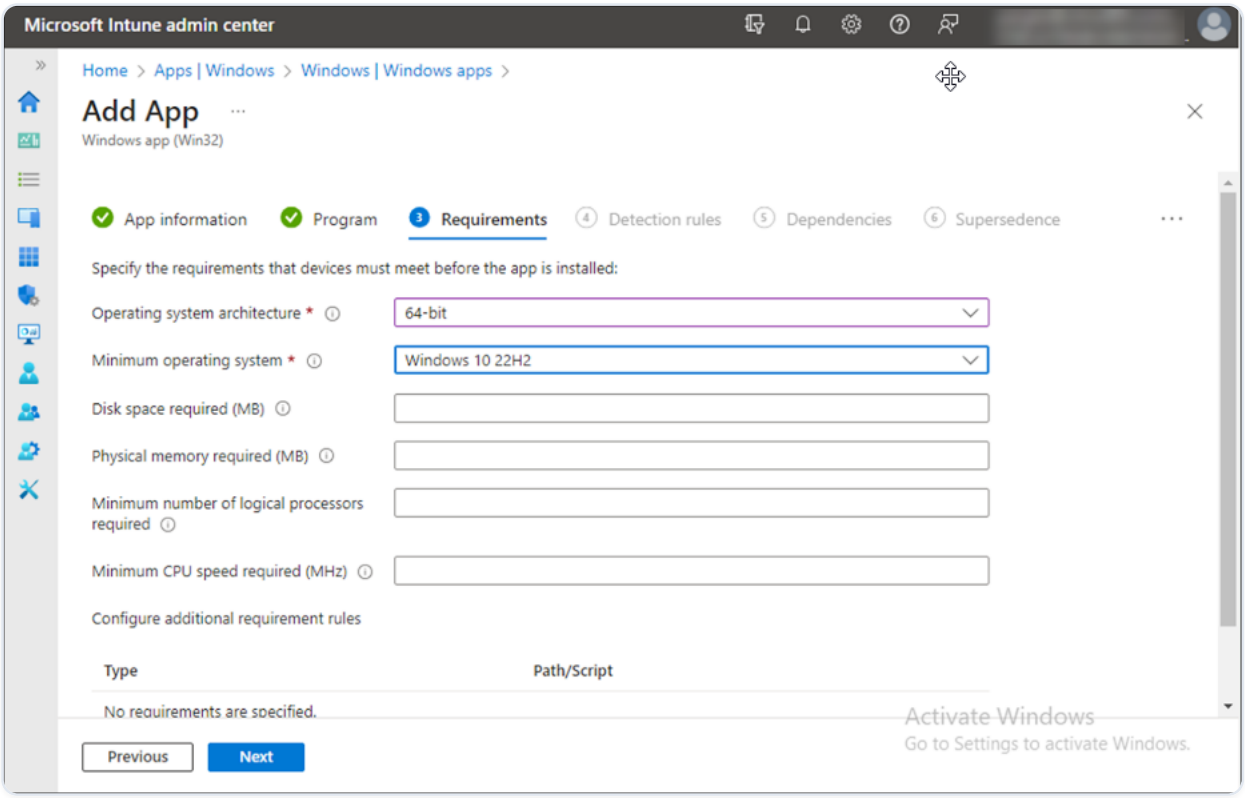
   - **インストールコマンド**: `VDAWorkstationSetup_2203.exe /quiet /noreboot`
   - **アンインストールコマンド**: `VDAWorkstationSetup_2203.exe /quiet /removeall /noreboot`
   - **インストール動作**:
     - **システム**: このオプションを選択すると、グループ内のすべてのデバイスにアプリがインストールされます。
     - **ユーザー**: このオプションを選択すると、グループ内の特定のユーザーデバイスにのみアプリがインストールされます。

9. **Next**をクリックします。

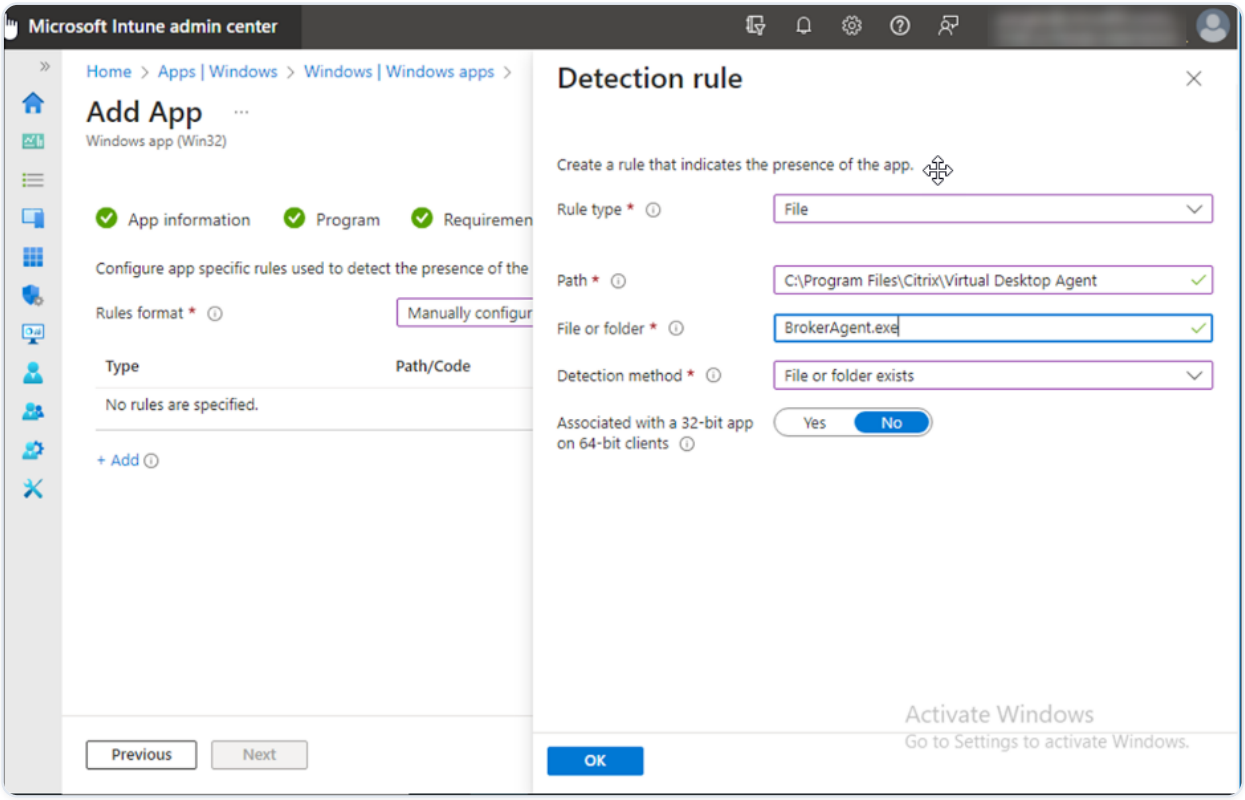
> **注：**
>
> - この例ではバージョン2203を使用していますが、どのバージョンでも使用できます。
> - コマンドに`/noreboot`を追加しても、インストールまたは展開中に再起動が発生しないという意味ではなく、強制的な再起動が適用されるだけです。 スクリプトの詳細については、「VDAをインストールするためのコマンドラインオプション」を参照してください。
> - **デバイスの再起動動作**については、**Intune will force a mandatory device restart**を選択します。
> - 「**リターンコード**」テキストボックスに、インストール後の成功のために`0`、`3`、`8`を入力します。 その他のリターンコードについては、「Citrix インストールリターンコード」を参照してください。



10. 次の画面で、「**要件**」タブの下に、必要な値を入力します。「**次へ**」をクリックします。



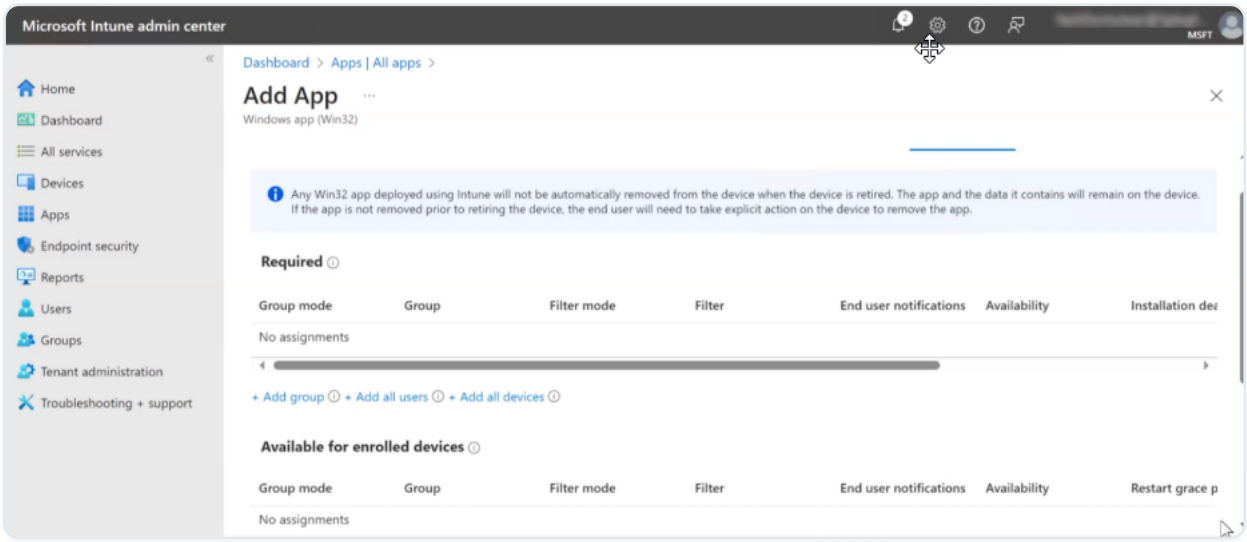
11. 次の画面で、「**検出ルール**」タブの下に、Broker エージェントを追加するための「**検出ルール**」を追加します。「**OK**」をクリックします。



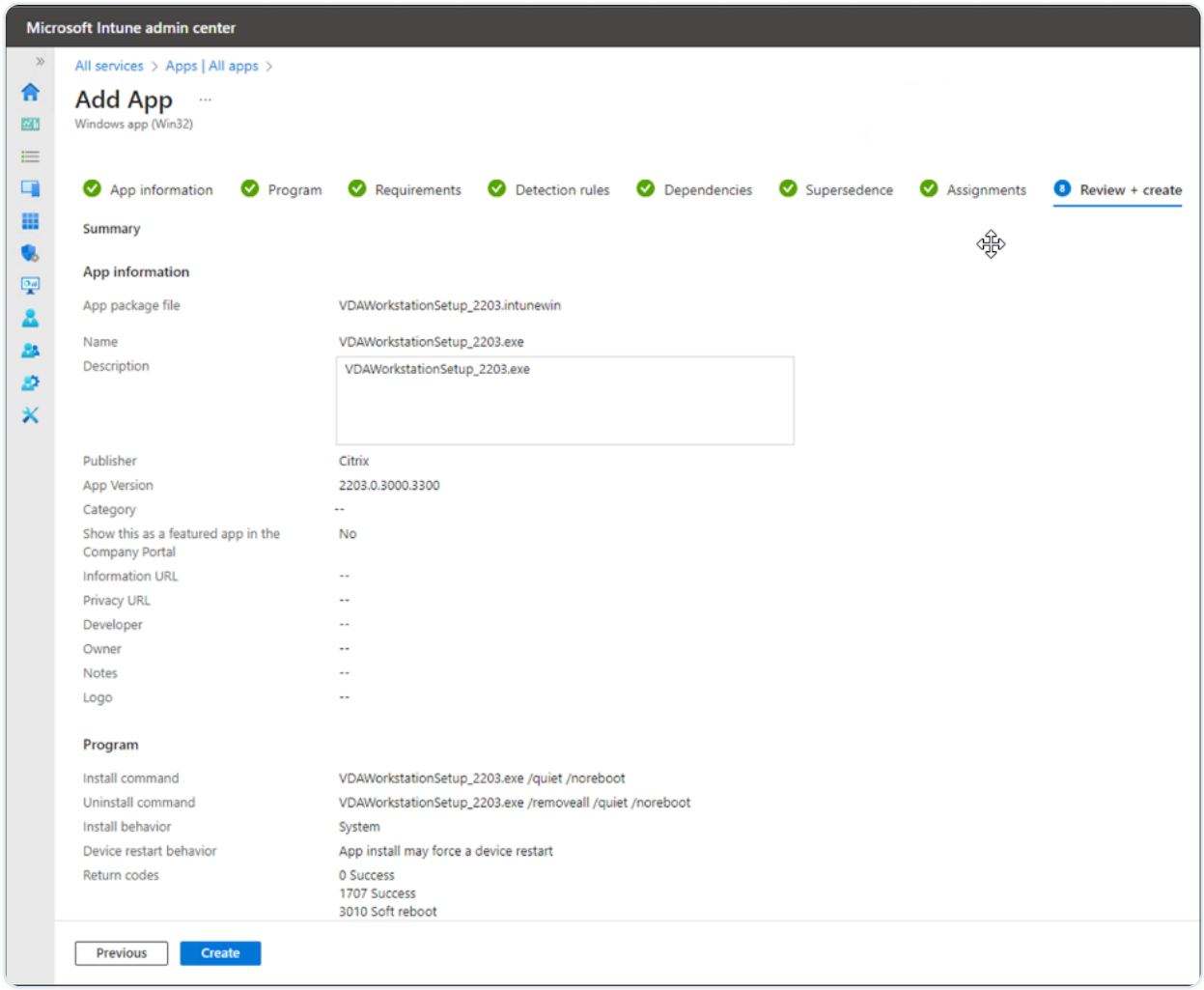
12. 「**割り当て**」タブで、デバイスを次のように追加できます。

    - **必須**: 更新が自動的に行われるデバイス。

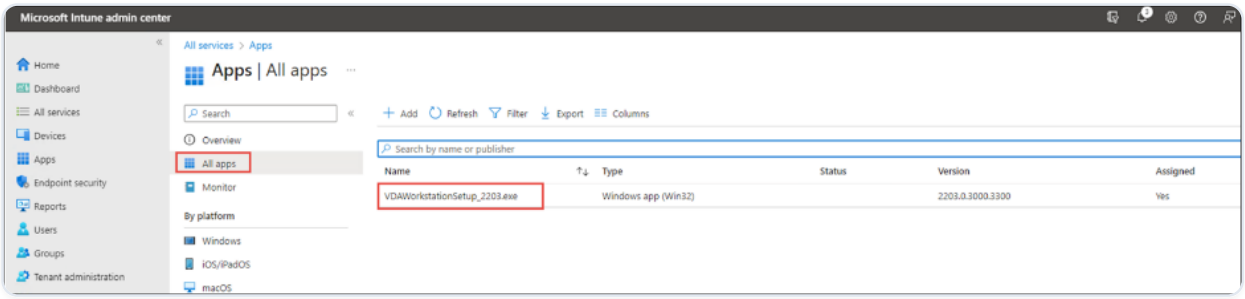
- **登録済みデバイスで利用可能**: 更新が手動で行われるデバイス。



13. 詳細を確認し、「**作成**」をクリックします。



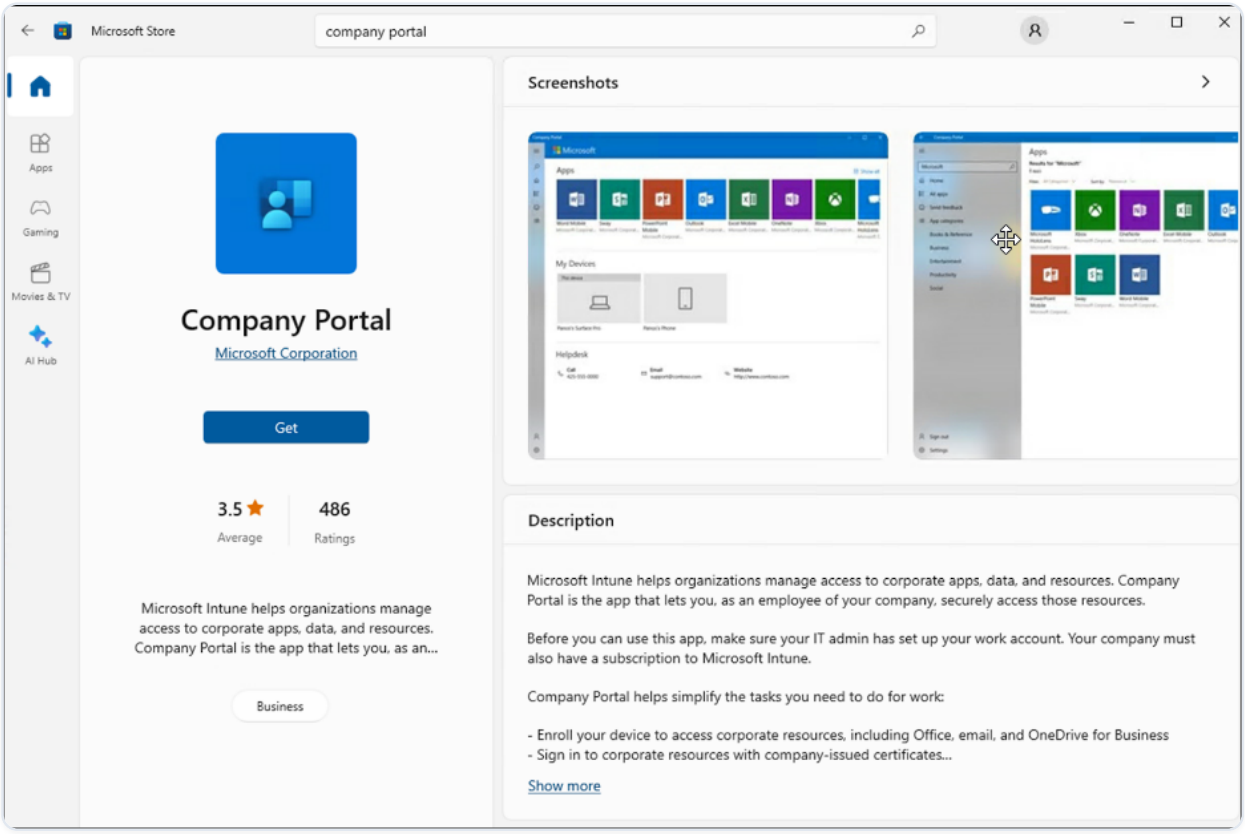
アプリが正常に割り当てられました。



詳細については、「アプリの追加と割り当て」を参照してください。

ステップ 4: 登録済みデバイスにアプリをインストールする

1. 登録済みのWindows 10デスクトップデバイスにサインインします。 デバイスはMicrosoft Intuneに登録されている必要があります。また、アプリに割り当てたグループに含まれるアカウントを使用してデバイスにサインインする必要があります。詳細については、Microsoftのドキュメントを参照してください。
2. 「**スタート**」メニューから「**Microsoft Store**」を開きます。
3. 「**Company Portal**」アプリを検索してインストールします。



4. 「**Company Portal**」アプリを実行します。
5. Microsoft Intuneを使用して追加したアプリをクリックします。 Intuneユーザーにアプリを正常に割り当てなかった場合、次のメッセージが表示されます。 `Your IT administrator did not make any apps available to you.`

6. 「**インストール**」をクリックします。

サイトを作成する

> **注：**
>
> サイト作成中、ハイブリッド権限ライセンスを有効にするライセンスを追加した後、サイト作成が完了するまで、パブリッククラウドホスト（Microsoft Azure、Google Cloud Platform、Amazon Web Servicesなど）は接続タイプリストに表示されません。

> サイトとは、Citrix Virtual Apps and Desktops™展開に付ける名前です。これには、Delivery Controllerとその他のコアコンポーネント、Virtual Delivery Agent (VDA)、ホストへの接続、マシンカタログ、およびデリバリーグループが含まれます。サイトは、コアコンポーネントをインストールした後、最初のマシンカタログとデリバリーグループを作成する前に作成します。

ControllerがServer Coreにインストールされている場合は、Citrix Virtual Apps and Desktops SDKのPowerShellコマンドレットを使用してサイトを作成します。

サイトを作成すると、Citrixカスタマーエクスペリエンス向上プログラム（CEIP）に自動的に登録されます。CEIPは匿名の統計情報と使用状況情報を収集し、Citrixに送信します。最初のデータパッケージは、サイト作成後約7日後にCitrixに送信されます。サイト作成後いつでも登録を変更できます。Web Studioの左ペインで**設定**を選択し、**Citrixカスタマーエクスペリエンス向上プログラム**の設定を見つけます。詳細については、`<http://more.citrix.com/XD-CEIP>`を参照してください。

サイトを作成したユーザーは、フル管理者になります。詳細については、委任管理を参照してください。

サイトを作成する前にこの記事を確認して、何が期待できるかを知っておいてください。

ステップ1. サイト作成ウィザードを開く - Citrix Site Manager

Citrix Virtual Apps and Desktops展開（サイトとも呼ばれます）を設定するには、Citrix Site Managerツールを使用します。このツールは、Delivery Controllerをインストールすると自動的にインストールされます。

このツールを実行するには、Delivery Controllerでデスクトップのスタートメニューを開き、**Citrix > Citrix Site Manager**を選択します。Web Studioのインストールを参照してください。

ステップ2. サイト名

はじめにページで、サイトの名前を入力します。

ステップ3. データベース

データベースページには、サイト、監視、および構成ログデータベースの設定に関する選択肢が含まれています。データベースの設定の選択肢と要件の詳細については、データベースを参照してください。

> **注:**
>
> SQL Server Always On ListenerがTLS暗号化用に構成されている場合、データベース作成権限を持つ資格情報の入力を求められることがあります。有効な管理者資格情報を入力しても、データベースの作成は失敗します。SQL Server証明書に、Subject Alternative Names (SAN) にリスナーのDNS名が含まれていることを確認してください。詳細については、`<https://docs.microsoft.com/ja-jp/sql/database-engine/availability-groups/windows/listeners-client-connectivity-application-failover#SSLcertificates>` を参照してください。

> サイトデータベースとして使用するためにSQL Server Expressをインストールすることを選択した場合（デフォルト）、そのソフトウェアのインストール後に再起動が発生します。サイトデータベースとして使用するためにSQL Server Expressソフトウェアをインストールしないことを選択した場合、その再起動は発生しません。

デフォルトのSQL Server Expressを使用しない場合は、サイトを作成する前に、SQL Serverソフトウェアがマシンにインストールされていることを確認してください。システム要件にサポートされているバージョンが記載されています。

サイトにDelivery Controllerを追加したい場合で、すでに他のサーバーにControllerソフトウェアをインストールしている場合は、このページからそれらのControllerを追加できます。データベースを設定するスクリプトを生成する予定がある場合は、スクリプトを生成する前にControllerを追加してください。

ステップ4. ライセンス

> **注:**

ライセンスサーバーがバージョン11.17.2ビルド53100以降で実行されていることを確認してください。この前提条件を満たさない場合、サイトのアップグレードや作成中にエラーや推奨事項が発生する可能性があります。

ライセンスページで、ライセンスサーバーのアドレスを指定し、使用する（インストールする）ライセンスを示します。

- ライセンスサーバーのアドレスを`name:[port]`の形式で指定します。*名前*はFQDN、NetBIOS、またはIPアドレスである必要があります。FQDNを推奨します。ポート番号を省略した場合、デフォルトは27000です。**接続**をクリックします。ライセンスサーバーへの接続が成功するまで、次のページに進むことはできません。
- 接続が確立されると、デフォルトで**既存のライセンスを使用**が選択されます。表示には、現在インストールされているライセンスに基づいて、この製品が構成できる互換性のある製品が一覧表示されます。
  - この製品をリストされている製品のいずれか（例：Citrix Virtual Apps PremiumまたはCitrix Virtual Desktops™ Premium）として、それらのライセンスのいずれかを使用して構成したい場合は、そのエントリを選択します。
  - この製品で使用するためにライセンスを割り当ててダウンロード済み（Citrix Manage Licenses Toolを使用）だが、まだライセンスをインストールしていない場合：
    - **ライセンスファイルを参照**をクリックします。
    - ファイルエクスプローラーで、ダウンロードしたライセンスを見つけて選択します。関連する製品がサイト作成ウィザードの**ライセンス**ページに表示されます。使用したいエントリを選択します。
  - 目的の製品が表示されない場合、または割り当て済みでダウンロード済みのライセンスがない場合は、ライセンスを割り当て、ダウンロードしてインストールできます。これを行うには、ライセンスサーバーがインターネットにアクセスできる必要があります。目的の製品のライセンスアクセスコードが必要です。Citrixからそのコードがメールで送信されます。
    - **割り当ててダウンロード**をクリックします。
    - **ライセンスの割り当て**ダイアログで、Citrixから送信されたライセンスアクセスコードを入力します。**ライセンスを割り当てる**をクリックします。
    - 新しいライセンスに関連付けられている製品が、サイト作成ウィザードの**ライセンス**ページに表示されます。使用するエントリを選択します。

または、**30日間の無料試用版を使用**を選択し、後でライセンスをインストールします。詳細については、ライセンスドキュメントを参照してください。

ステップ5. 概要

概要ページには、指定した情報が一覧表示されます。変更する場合は、**戻る**ボタンを使用します。完了したら、**完了**をクリックします。

詳細情報

ホスト接続、ネットワーク、およびストレージ

ハイパーバイザーまたはその他のサービス上のVMを使用してアプリケーションとデスクトップを配信している場合、オプションでそのホストへの最初の接続を作成できます。その接続のストレージおよびネットワークリソースを指定することもできます。サイト作成後、この接続とリソースを変更したり、さらに接続を作成したりできます。詳細については、接続とリソースを参照してください。

- **接続**ページで指定する情報については、接続とリソースを参照してください。
  - ハイパーバイザーまたはその他のサービス上のVMを使用しない場合（またはWeb Studioを使用して専用ブレードPC上のデスクトップを管理する場合）は、接続の種類として**なし**を選択します。
  - Remote PC Accessサイトを構成していて、Wake on LAN機能を使用する予定がある場合は、**Microsoft System Center Virtual Machine Manager**または**Remote PC Wake on LAN**の種類を選択します。詳細については、Wake on LANを参照してください。

  接続の種類に加えて、Citrixツール（Machine Creation Services™など）またはその他のツールを使用してVMを作成するかどうかを指定します。
- **ストレージ**ページと**ネットワーク**ページで指定する情報については、ホストストレージ、ストレージ管理、およびストレージの選択を参照してください。
- ハイブリッド権限ライセンスを所有しており、パブリッククラウドホスト接続（AWSなど）を追加している場合、それらの接続がここに一覧表示されます。これらのパブリッククラウドホスト接続を表示するには、追加後数分経ってからWeb Studioを更新してください。

リモートPCアクセス

Remote PC Accessの展開については、Remote PC Accessを参照してください。

Wake on LAN機能を使用する場合は、サイトを作成する前にMicrosoft System Center Configuration Managerで構成手順を完了してください。詳細については、Configuration ManagerとRemote PC Access Wake on LANを参照してください。

接続とリソースの作成および管理

重要:

Citrix Virtual Apps and Desktops™ 7 2006以降、現在の展開で以下のいずれかのテクノロジーを使用している場合、それらのテクノロジーを使用するサポート終了（EOL）項目を削除した後にのみ、現在のリリースに展開をアップグレードできます。

- パーソナル vDisk (PvD)
- AppDisks™
- パブリッククラウドホストの種類：Citrix CloudPlatform、Microsoft Azure Classic

詳細については、「PVD、AppDisks、およびサポートされていないホストの削除」を参照してください。

注：

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

展開にパブリッククラウドホスト接続を使用する場合は、新規インストールまたは現在のリリースへのアップグレードを完了するためにHybrid Rights Licenseが必要です。

インストーラーがサポートされていないテクノロジーの1つ以上、またはHybrid Rights Licenseなしのホスト接続を検出すると、アップグレードが一時停止または停止し、説明メッセージが表示されます。インストーラーのログに詳細が含まれています。詳しくは、「展開のアップグレード」を参照してください。

Hybrid Rights Licenseがホスト接続に与える影響

Hybrid Rights Licenseの資格に基づいて、パブリッククラウドホストへのホスト接続が影響を受ける3つのシナリオがあります。

- パブリッククラウドホストへの新しいホスト接続を作成するには、Hybrid Rights Licenseが必要です。
- Hybrid Rights Licenseを所有しているがライセンスの有効期限が切れている場合、パブリッククラウドホストへの既存の接続は資格なしとマークされ、メンテナンスモードに入ります。既存のホスト接続がメンテナンスモードの場合、次の操作はできません。
  - ホスト接続の追加または変更
  - カタログの作成とイメージの更新
  - 電源操作を実行する
- 権限のないホスト接続が権限ありに変更されると、既存のホスティング接続が再度有効になります。

はじめに

サイトを作成するときに、ホスティングリソースへの最初の接続をオプションで作成できます。後で、その接続を変更したり、他の接続を作成したりできます。接続の構成には、サポートされているハイパーバイザーの中から接続タイプを選択すること、およびその接続のリソースから選択するストレージとネットワークが含まれます。

読み取り専用管理者は、接続とリソースの詳細を表示できます。接続とリソースの管理タスクを実行するには、完全な管理者である必要があります。詳細については、「委任管理」を参照してください。

接続タイプに関する情報の場所

サポートされている仮想化プラットフォームを使用して、Citrix Virtual AppsまたはCitrix Virtual Desktops環境でマシンをホストおよび管理できます。「システム要件」の記事に、サポートされている種類が記載されています。

詳細については、以下の情報源を参照してください。

- **XenServer (旧シトリックス ハイパーバイザー™):**
  - XenServer仮想化環境。
  - XenServer®ドキュメント。

- **ニュータニックス アクロポリス:**
  - Nutanix仮想化環境。
  - Nutanixドキュメント。
- **ヴイエムウェア:**
  - VMware仮想化環境。
  - VMware製品ドキュメント。
- **Microsoft ハイパーV:**
  - Microsoft System Center Virtual Machine Manager 仮想化環境の記事。
  - Microsoft ドキュメント。
- **パブリッククラウドホスト接続（AWS、Google Cloud、Microsoft Azure、Nutanix Cloudおよびパートナーソリューション、VMware Cloudおよびパートナーソリューション）：** パブリッククラウドホストに関する情報については、「リソースタイプのセットアップ」を参照してください。

> **注：**
>
> 情報源はCitrix DaaS™のドキュメントを参照するよう指示しています。Citrix DaaS製品のパブリッククラウドホストに慣れている場合、オンプレミスバージョンにはいくつかの違いがあります。オンプレミスのVirtual Apps and Desktopsでは、管理インターフェイスはWeb Studioとして知られています。更新はサービスに約4週間ごとに展開されます。そのため、サービスで利用可能な特定の機能がオンプレミスバージョンでは利用できない場合があります。

ホストストレージ

サポートされているハイパーバイザーによって管理されている場合、ストレージ製品はサポートされます。Citrix Supportは、これらのストレージ製品ベンダーが問題のトラブルシューティングと解決を支援し、必要に応じてナレッジセンターにそれらの問題を文書化します。

マシンをプロビジョニングする際、データはタイプ別に分類されます。

- マスターイメージを含むオペレーティングシステム（OS）データ。

- 一時データ。このデータには、MCSプロビジョニングマシンに書き込まれるすべての非永続データ、Windowsページファイル、ユーザープロファイルデータ、およびShareFileと同期されるすべてのデータが含まれます。このデータは、マシンが再起動するたびに破棄されます。

各データタイプに個別のストレージを提供することで、各ストレージデバイスの負荷を軽減し、パフォーマンスを向上させ、ホストの利用可能なリソースを最大限に活用できます。また、異なるデータタイプに適切なストレージを使用できるようになります。一部のデータでは、永続性と回復性が他のデータよりも重要です。

ストレージは共有（中央に配置され、どのホストからも独立しており、すべてのホストで使用される）することも、ハイパーバイザーにローカルに配置することもできます。たとえば、中央共有ストレージは、1つ以上のWindows Server 2012クラスター化ストレージボリューム（接続ストレージの有無にかかわらず）、またはストレージベンダーのアプライアンスである場合があります。中央ストレージは、ハイパーバイザーストレージ制御パスやパートナープラグインを介した直接アクセスなど、独自の最適化を提供する可能性もあります。

一時データをローカルに保存することで、共有ストレージにアクセスするためにネットワークを介する必要がなくなります。また、共有ストレージデバイスの負荷も軽減されます。共有ストレージはより高価になる可能性があるため、データをローカルに保存することで費用を削減できます。これらの利点は、ハイパーバイザーサーバー上の十分なストレージの可用性と比較検討する必要があります。

接続を作成する際、ハイパーバイザー間で共有されるストレージ、またはハイパーバイザーにローカルなストレージの2つのストレージ管理方法のいずれかを選択します。

1つ以上のXenServerホストで一時データストレージにローカルストレージを使用する場合、プール内の各ストレージの場所に一意の名前があることを確認してください。（XenCenter®で名前を変更するには、ストレージを右クリックして名前プロパティを編集します。）

ハイパーバイザーで共有されるストレージ

ハイパーバイザー間で共有されるストレージ方式は、長期的な永続性が必要なデータを中央に保存し、一元的なバックアップと管理を提供します。このストレージにはOSディスクが格納されます。

この方法を選択すると、一時的なマシンデータにローカルストレージ（同じハイパーバイザープール内のサーバー上）を使用するかどうかを選択できます。この方法は、共有ストレージ内のデータほど永続性や回復性を必要としません。これは*一時データキャッシュ*と呼ばれます。ローカルディスクは、メインOSストレージへのトラフィックを削減するのに役立ちます。このディスクは、マシンが再起動するたびにクリアされます。ディスクはライトスルーメモリキャッシュを介してアクセスされます。一時データにローカルストレージを使用する場合、プロビジョニングされた

VDAは特定のハイパーバイザーホストに紐付けられます。そのホストが故障すると、VMは起動できません。

例外: Microsoft System Center Virtual Machine Managerは、クラスター共有ボリューム（CSV）を使用する場合、ローカルストレージ上の一時データキャッシュディスクを許可しません。

一時データをローカルに保存するための接続を作成し、各VMのキャッシュディスクサイズとメモリサイズの非デフォルト値を有効にして構成します。デフォルト値は接続タイプに合わせて調整されており、ほとんどのケースで十分です。詳細については、「マシンカタログの作成」を参照してください。

ハイパーバイザーは、ディスクイメージをローカルで読み取りキャッシュすることにより、最適化テクノロジーを提供することもできます。たとえば、XenServerはIntelliCache™を提供し、中央ストレージへのネットワークトラフィックを削減します。

ハイパーバイザーのローカルストレージ

ハイパーバイザーにローカルなストレージ方式では、データをハイパーバイザーにローカルに保存します。この方式では、マスターイメージやその他のOSデータがサイト内のハイパーバイザーに転送されます。このプロセスは、最初のマシン作成時と将来のイメージ更新時に発生します。このプロセスにより、管理ネットワークでかなりのトラフィックが発生します。イメージ転送には時間がかかり、イメージは各ホストで異なるタイミングで利用可能になります。

接続とリソースを作成する

サイトの作成時に、最初の接続をオプションで作成できます。サイト作成ウィザードには、以下のセクションで説明する接続関連のページが含まれています。

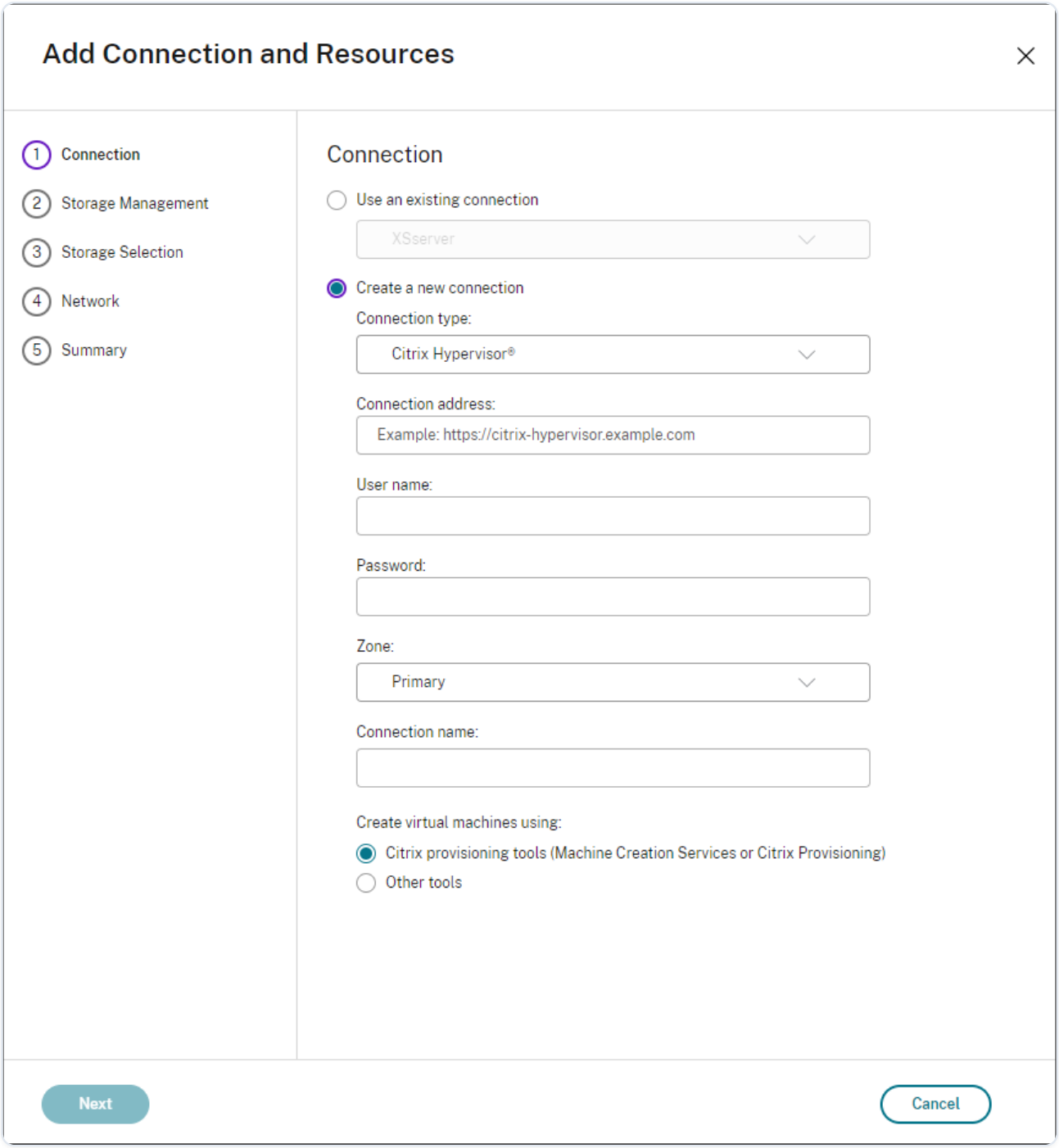
サイトの作成後に接続を作成する場合は、手順1から開始します。

> **重要:**
>
> 接続を作成する前に、ホストリソース（ストレージとネットワーク）が利用可能である必要があります。

1. Web Studioにサインインします。
2. 左ペインで**ホスティング**を選択します。
3. アクションバーで を選択します。

4. ウィザードは、以下のページ（特定のページの内容は選択した接続タイプによって異なります）を案内します。各ページを完了したら、 をクリックして ページに進みます。

接続



「**接続**」ページで：

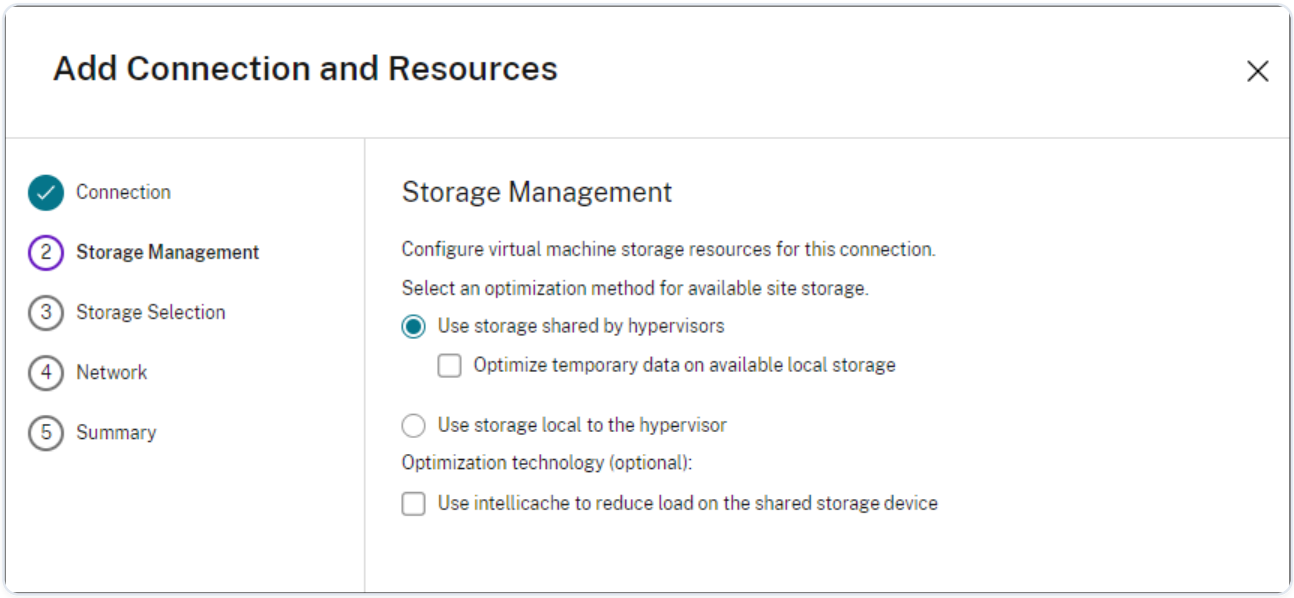
- 接続を作成するには、 を選択します。既存の接続と同じホスト構成に基づいて接続を作成するには、 を選択し、関連する接続を選択します。
- フィールドで、使用しているハイパーバイザーを選択します。パブリッククラウドホスト接続は、Hybrid Rights Licenseを使用している場合にのみドロップダウンリストに表示されます。

または、PowerShellコマンド `Get-HypHypervisorPlugin [-ZoneUid] $rluid [-IncludeUnavailable]` false/true を使用して、以下を取得できます。

- サードパーティ製プラグインを含む、Citrixがサポートするすべてのハイパーバイザープラグインのリスト。
- ハイパーバイザープラグインの可用性。可用性ステータスが **false** の場合、ハイパーバイザープラグインが正しくインストールされていないか、Hybrid Rights Licenseの資格がないことが考えられます。

- 接続アドレスと資格情報フィールドは、選択した接続タイプによって異なります。要求された情報を入力します。
- 接続名を入力します。この名前はWeb Studioに表示されます。
- 仮想マシンの作成に使用するツールを選択します: Web Studioツール (Machine Creation Services™ や Citrix Provisioning など) またはその他のツール。

ストレージ管理



ストレージ管理の種類と方法については、「ホストストレージ」を参照してください。

Hyper-V または VMware ホストへの接続を構成している場合は、クラスター名を参照して選択します。その他の接続タイプでは、クラスター名は要求されません。

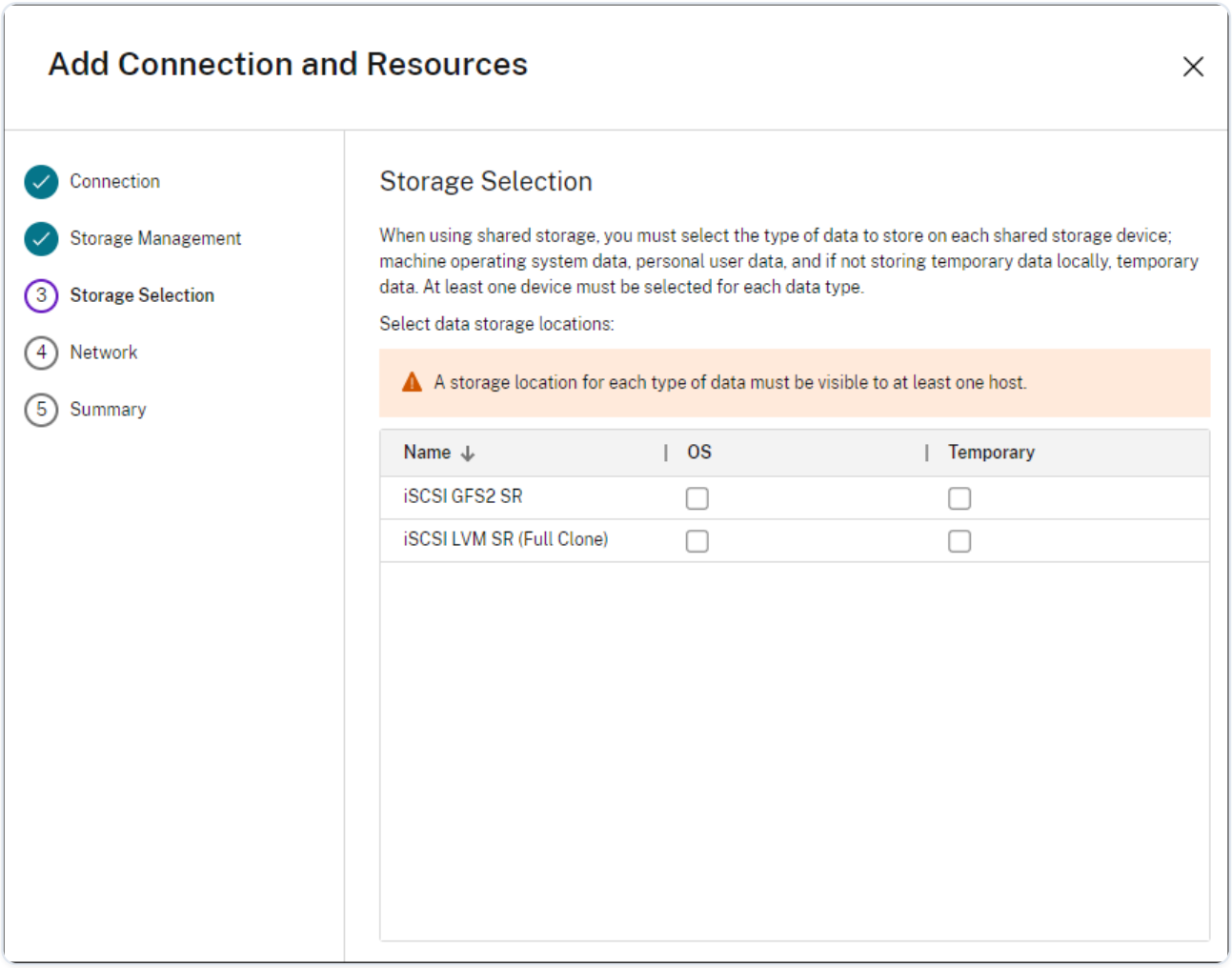
ストレージ管理方法を選択します。ハイパーバイザーによって共有されるストレージ、またはハイパーバイザーにローカルなストレージ。

- ハイパーバイザーで共有されるストレージを選択した場合、利用可能なローカルストレージに一時データを保持するかどうかを指定します。(この接続を使用するマシンカタログで、デフォルト以外のサイズの一時ストレージを指定できます。) **例外:** クラスター共有ボリューム (CSV)

を使用する場合、Microsoft System Center Virtual Machine Manager はローカルストレージ上の一時データキャッシュディスクを許可しません。Web Studio でそのストレージ管理設定を構成すると失敗します。

XenServer プールで共有ストレージを使用する場合、共有ストレージデバイスの負荷を軽減するために IntelliCache を使用するかどうかを指定します。「XenServer 接続で IntelliCache を使用する」を参照してください。

ストレージの選択



ストレージの選択の詳細については、「ホストストレージ」を参照してください。

利用可能なデータタイプごとに、少なくとも1つのホストストレージデバイスを選択します。前のページで選択したストレージ管理方法によって、このページで選択できるデータタイプが決まります。ウィザードの次のページに進む前に、サポートされているデータタイプごとに少なくとも1つのストレージデバイスを選択してください。

「**ストレージの選択**」ページの下部には、ハイパーバイザーで共有されるストレージを選択し、前のページで「**利用可能なローカルストレージ上の一時データを最適化**」を有効にした場合に、

さらに多くの構成オプションが含まれています。一時データに使用するローカルストレージデバイスを選択できます。

現在選択されているストレージデバイスの数が表示されます (上記のグラフィックでは「1 storage device selected」)。そのエントリにカーソルを合わせると、選択されているデバイス名が表示されます。

1. 使用するストレージデバイスを変更するには、**選択**をクリックします。
2. **ストレージの選択**ダイアログボックスで、ストレージデバイスのチェックボックスをオンまたはオフにして、**OK**をクリックします。

ネットワーク

ネットワークページで、リソースの名前を入力します。この名前は、接続に関連付けられたストレージとネットワークの組み合わせを識別するためにWeb Studioに表示されます。

VMが使用するネットワークを1つ以上選択します。

概要

概要ページで、選択内容を確認します。完了したら、**完了**をクリックします。

注意: 一時データをローカルに保存すると、この接続を使用するマシンを含むマシンカタログを作成する際に、一時データストレージの非デフォルト値を構成できます。「マシンカタログの作成」を参照してください。

接続設定の編集

この手順を使用して接続の名前を変更したり、接続を作成したりしないでください。それらの接続は異なる操作です。現在ホストしているマシンに新しいアドレスがある場合にのみ、アドレスを変更してください。別のアドレスを別のマシンに入力すると、接続のマシンカタログが破損します。

このリソースにアクセスするマシンカタログは、適切なGPU固有のマスターイメージを使用する必要があるため、接続の**GPU**設定を変更することはできません。接続を作成してください。

1. Web Studioにサインインします。
2. 左ペインで**ホスティング**を選択します。
3. 接続を選択し、アクションバーで**接続の編集**を選択します。
4. 接続を編集する際に利用できる設定のガイダンスに従ってください。

5. 完了したら、**適用**をクリックして行った変更を適用し、ウィンドウを開いたままにするか、**保存**をクリックして変更を適用し、ウィンドウを閉じます。

接続プロパティページ:

- 接続アドレスと資格情報を変更するには、**設定の編集...**を選択し、新しい情報を入力します。
- XenServer接続の高可用性サーバーを指定するには、**サーバーの編集...**を選択し、サーバーを選択します。Citrixでは、プールマスターに障害が発生した場合にXenServerとの通信を可能にするため、プール内のすべてのサーバーを選択することをお勧めします。

> **注：**
>
> HTTPSを使用しており、高可用性サーバーを構成したい場合は、プール内のすべてのサーバーにワイルドカード証明書をインストールしないでください。各サーバーには個別の証明書が必要です。

詳細設定ページ:

- Remote PC Accessで使用されるMicrosoft System Center Configuration Manager (ConfMgr) Wake on LAN接続タイプの場合、**ConfMgr Wake Proxy**、マジックパケット、およびパケット送信情報を入力します。
- スロットリングしきい値設定を使用すると、接続で許可される最大電源アクション数を指定できます。これらの設定は、電源管理設定が同時に起動するマシンが多すぎたり少なすぎたりする場合に役立ちます。各接続タイプには、ほとんどのケースに適した特定のデフォルト値があり、変更してはなりません。
- **同時アクション (すべてのタイプ)** 設定では、この接続で同時に発生できる最大絶対数と、この接続を使用するすべてのマシンの最大割合という2つの値を指定します。絶対値とパーセンテージ値の両方を指定する必要があります。実際に適用される制限は、これらの値のうち小さい方です。

  たとえば、34台のマシンがある展開で、**Simultaneous actions (all types)**が絶対値10、パーセンテージ値10に設定されている場合、適用される実際の制限は3です（つまり、34の10パーセントを最も近い整数に丸めたもので、絶対値10台のマシンよりも小さい）。
- **Maximum new actions per minute**は絶対数です。パーセンテージ値はありません。
- 「**接続オプション**」フィールドには、Citrixサポート担当者の指示または明示的なドキュメントの指示がある場合にのみ情報を入力してください。

共有テナントページ:

この接続のサブスクリプションとAzure Compute Galleryを共有するテナントとサブスクリプションを追加します。これにより、カタログを作成または更新する際に、それらのテナントとサブスクリプションから共有イメージを選択できます。

- この接続に関連付けられているアプリケーションの**アプリケーションID**と**アプリケーションシークレット**を入力します。この情報を使用して、Azureに認証できます。セキュリティを確保するために、定期的にキーを変更することをお勧めします。
- 共有テナントとサブスクリプションを指定します。最大8つの共有テナントを追加できます。各テナントにつき、最大8つのサブスクリプションを追加できます。
- 完了したら、**保存**と**適用**をクリックします。

「**接続オプション**」フィールドには、Citrixサポート担当者の指示がある場合にのみ情報を入力してください。

ネットワークの編集

接続のネットワークを変更できます。次の手順を実行します。

1. に移動します。
2. 接続の下にあるターゲットリソースを選択し、アクションバーで を選択します。
3. 仮想マシンが使用するネットワークを1つ以上選択します。
4. 変更を保存して終了するには、**保存**をクリックします。

接続のメンテナンスモードをオンまたはオフにする

接続のメンテナンスモードをオンにすると、新しい電源操作が接続に保存されているマシンに影響を与えるのを防ぎます。ユーザーは、マシンがメンテナンスモードの場合、マシンに接続できません。ユーザーがすでに接続している場合、メンテナンスモードはログオフ時に有効になります。

1. Web Studioにサインインします。
2. 左ペインで**ホスティング**を選択します。
3. 接続を選択します。メンテナンスモードをオンにするには、アクションバーで**Turn On Maintenance Mode**を選択します。メンテナンスモードをオフにするには、**Turn Off Maintenance Mode**を選択します。

個々のマシンに対してメンテナンスモードをオンまたはオフにすることもできます。また、マシンカタログまたはデリバリーグループ内のマシンに対してメンテナンスモードをオンまたはオフにすることもできます。

接続を削除する

接続を削除すると、多数のマシンが削除され、データが失われる可能性があります。影響を受けるマシン上のユーザーデータがバックアップされているか、不要であることを確認してください。

接続を削除する前に、以下を確認してください。

- すべてのユーザーが接続に保存されているマシンからログオフしていること。
- 切断されたユーザーセッションが実行されていないこと。
- プールされたマシンと専用マシンのメンテナンスモードがオンになっていること。
- 接続で使用されているマシンカタログ内のすべてのマシンは電源がオフになります。

カタログによって参照されている接続を削除すると、マシンカタログは使用できなくなります。この接続がカタログによって参照されている場合、カタログを削除するオプションがあります。カタログを削除する前に、他の接続で使用されていないことを確認してください。

1. Web Studioにサインインします。
2. 左ペインで**ホスティング**を選択します。
3. 接続を選択し、アクションバーで**接続の削除**を選択します。
4. この接続にマシンが保存されている場合、マシンを削除するかどうかを尋ねられます。削除する場合は、関連するActive Directoryコンピューターアカウントをどうするかを指定します。

接続の名前を変更またはテストする

1. Web Studioにサインインします。
2. 左ペインで**ホスティング**を選択します。
3. 接続を選択し、アクションバーで または を選択します。

接続上のマシンの詳細を表示する

1. Web Studioにサインインします。
2. 左ペインで**ホスティング**を選択します。
3. 接続を選択し、アクションバーで**マシンの表示**を選択します。

上部のペインには、接続を介してアクセスされるマシンが一覧表示されます。マシンを選択すると、下部のペインにその詳細が表示されます。開いているセッションのセッション詳細も提供されます。

検索機能を使用して、マシンをすばやく見つけます。ウィンドウ上部のリストから保存された検索を選択するか、新しい検索を作成します。マシン名の全部または一部を入力して検索するか、高度な検索に使用する式を作成できます。式を作成するには、 をクリックし、プロパティと演算子のリストから選択します。

接続上のマシンを管理する

1. Web Studioにサインインします。
2. 左ペインで**ホスティング**を選択します。
3. 接続を選択し、 ペインで を選択します。
4. アクションバーで次のいずれかを選択します。一部のアクションは、マシンの状態と接続ホストの種類によっては利用できません。

アクション	説明
起動	マシンが電源オフまたは一時停止状態の場合に起動します。
一時停止	マシンをシャットダウンせずに一時停止し、マシンリストを更新します。
シャットダウン	オペレーティングシステムにシャットダウンを要求します。
強制シャットダウン	マシンを強制的に電源オフにし、マシンリストを更新します。
再起動	オペレーティングシステムにシャットダウンを要求し、その後マシンを再起動します。オペレーティングシステムがこれに応じられない場合、デスクトップは現在の状態のままになります。
メンテナンスモードを有効にする	マシンへの接続を一時的に停止します。この状態のマシンにはユーザーは接続できません。ユーザーが接続している場合、メンテナンスモードはログオフ時に有効になります。（上記のように、接続を介してアクセスされるすべて

アクション	説明
	のマシンに対してメンテナンスモードをオンまたはオフにすることもできます。）
デリバリーグループから削除	Delivery Groupからマシンを削除しても、そのDelivery Groupが使用するMachine Catalogからは削除されません。マシンは、ユーザーが接続していない場合にのみ削除できます。マシンを削除している間、ユーザーが一時的に接続できないようにするには、メンテナンスモードをオンにします。
削除	マシンを削除すると、ユーザーはそのマシンにアクセスできなくなり、マシンはMachine Catalogから削除されます。マシンを削除する前に、すべてのユーザーデータがバックアップされているか、不要になっていることを確認してください。マシンは、ユーザーが接続していない場合にのみ削除できます。マシンを削除している間、ユーザーが一時的に接続できないようにするには、メンテナンスモードをオンにします。

マシンのシャットダウンを伴う操作の場合、マシンが10分以内にシャットダウンしないと、電源がオフになります。シャットダウン中にWindowsが更新プログラムのインストールを試みると、更新が完了する前にマシンの電源がオフになるリスクがあります。

ストレージの編集

接続を使用するVMのオペレーティングシステムデータと一時データを保存するために使用されるサーバーのステータスを表示できます。また、各データタイプのストレージにどのサーバーを使用するかを指定することもできます。

1. Web Studioにサインインします。
2. 左ペインで**ホスティング**を選択します。
3. 接続を選択し、アクションバーで**ストレージの編集**を選択します。
4. 左側のペインで、データタイプ（オペレーティングシステムまたは一時）を選択します。
5. 選択したデータタイプについて、1つ以上のストレージデバイスのチェックボックスをオンまたはオフにします。

6. **OK**をクリックします。

リスト内の各ストレージデバイスには、その名前とストレージステータスが含まれています。有効なストレージステータスの値は次のとおりです。

- **使用中:** ストレージはマシンの作成に使用されています。
- **廃止済み:** ストレージは既存のマシンにのみ使用されています。このストレージには新しいマシンは追加されません。
- **未使用:** ストレージはマシンの作成に使用されていません。

現在**使用中**のデバイスのチェックボックスをオフにすると、そのステータスは**廃止済み**に変わります。既存のマシンはそのストレージデバイスを引き続き使用し（データを書き込むこともできます）、そのため、マシンの作成に使用されなくなった後でも、その場所がいっぱいになる可能性があります。

リソースの削除、名前の変更、またはテスト

1. Web Studioにサインインします。
2. 左ペインで**ホスティング**を選択します。
3. リソースを選択し、アクションバーで適切なエントリ（**リソースの削除**、**リソースの名前変更**、または**リソースのテスト**）を選択します。

孤立したAzureリソースの検出

孤立したリソースは、システム内に存在する使用されていないリソースであり、不要な費用につながる可能性があります。

この機能を使用すると、Citrix Virtual Apps and Desktopsサイトのホストにある孤立したAzureリソースを検出できます。

Web Studioで次の手順を実行します。

1. 「**管理**」から、左ペインで「**ホスティング**」を選択します。
2. 接続を選択し、アクションバーで「**孤立したリソースの検出**」を選択します。「**孤立したリソースの検出**」ダイアログボックスには、孤立したリソースのレポートが表示されます。
3. 孤立したリソースのレポートを表示するには、「**レポートの表示**」を選択します。

または、PowerShellを使用して孤立したAzureリソースを検出できます。詳細については、「孤立したリソースのリストを取得する」を参照してください。

孤立したリソースの原因を理解し、その後の対処方法については、「Citrixで孤立したAzureリソースを効率的に管理する」を参照してください。

接続タイマー

ポリシー設定を使用して、3つの接続タイマーを構成できます。

- 「**最大接続タイマー**」：ユーザーデバイスと仮想デスクトップ間の途切れない接続の最大期間を決定します。「**セッション接続タイマー**」および「**セッション接続タイマー間隔**」ポリシー設定を使用します。
- 「**接続アイドルタイマー**」：ユーザーからの入力がない場合に、仮想デスクトップへの途切れないユーザーデバイス接続が維持される期間を決定します。「**セッションアイドルタイマー**」および「**セッションアイドルタイマー間隔**」ポリシー設定を使用します。
- **接続解除タイマー:** 接続が解除され、ロックされた仮想デスクトップが、セッションがログオフされるまでロックされたままになる時間を決定します。「**接続解除セッションタイマー**」および「**接続解除セッションタイマー間隔**」ポリシー設定を使用します。

これらの設定のいずれかを更新する場合は、展開全体で一貫性があることを確認してください。

詳細については、ポリシー設定のドキュメントを参照してください。

孤立したリソースのリストを取得する

MCS によって作成されたものの、MCS によって追跡されなくなった孤立したリソースのリストを取得できます。これは現在、Azure 環境に適用されます。リストを取得するには、PowerShell コマンドを使用できます。接続を使用してフィルタリングできます。

> **注：**
>
> - プロビジョニングまたはイメージの更新が進行中の場合、PowerShell コマンドは拒否されます。
> - すべてのCitrixタグが付けられた顧客管理リソースは、孤立リソースとして検出されます。ただし、そのリソースに値がtrueのCitrixDetectIgnoreという別のタグを追加すると、孤立リソースの検出中にそのリソースは無視されます。

制限事項

- 組み込みのフル管理者またはクラウド管理者ロールの管理者ユーザーのみが、PowerShellコマンドを実行して孤立リソースのリストを取得できます。

- 孤立したリソースの誤認識を避けるため、孤立したリソースをフィルタリングしている間はVMの電源を入れないでください。
- 負荷が高い可能性がある場合、約2,000件のレコードが孤立として表示されます。

孤立リソースのリストを表示するには：

1. **PowerShell**ウィンドウを開きます。
2. 次のコマンドを実行します。
   a. 接続UIDを取得します。接続UIDは、HypervisorConnectionUid属性の値です。

```
Get-ChildItem xdhyp:\connections | where { $_.PluginId -like
'Azure*' }"
```

   b. 孤立したリソースのリストを取得します。

```
get-provorphanedresource -HypervisorConnectionUid <connection uid>
```

サブスクリプションIDから孤立リソースのリストを表示するには：

1. **PowerShell**ウィンドウを開きます。
2. 次のコマンドを実行します。
   a. サブスクリプションIDを使用して接続UIDを見つけます。接続UIDはHypervisorConnectionUid属性の値です。

```
Get-ChildItem xdhyp:\connections | where { $_.CustomProperties
-match '<subscriptionId>' }
```

   b. 孤立リソースのリストを取得します。

```
get-provorphanedresource -HypervisorConnectionUid <connection uid>
```

注：

削除する前にリソースを慎重に確認してください。

次のステップ

特定のホストタイプへの接続については、以下を参照してください。

- AWSへの接続
- XenServerへの接続
- Google Cloud環境への接続
- Microsoft Azureへの接続
- マイクロソフト システムセンター バーチャルマシンマネージャー への接続
- Nutanixへの接続
- Nutanixクラウドおよびパートナーソリューションへの接続
- VMwareへの接続
- VMwareクラウドおよびパートナーソリューションへの接続

初期展開プロセス中の場合は、マシンカタログを作成します。

AWSへの接続

(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/install-configure/connections.html)では、接続を作成するウィザードについて説明します。以下の情報では、AWSクラウド環境に固有の詳細について説明します。

> **注:**
>
> AWSへの接続を作成する前に、まずAWSアカウントをリソースの場所として設定を完了する必要があります。(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/install-configure/install-prepare/aws.html)を参照してください。

接続を作成する

Web Studioから接続を作成する場合：

- APIキーとシークレットキーの値を指定する必要があります。これらの値を含むキーファイルをAWSからエクスポートし、インポートできます。また、リージョン、アベイラビリティゾーン、VPC名、サブネットアドレス、ドメイン名、セキュリティグループ名、および資格情報も指定する必要があります。
- ルートAWSアカウントの資格情報ファイル（AWSコンソールから取得）は、標準のAWSユーザー向けにダウンロードされた資格情報ファイルと同じ形式ではありません。そのため、

Citrix Virtual Apps and Desktops™管理では、このファイルを使用してAPIキーとシークレットキーのフィールドに入力することはできません。AWS Identity Access Management (IAM) の資格情報ファイルを使用していることを確認してください。

注:

接続を作成した後、APIキーとシークレットキーの更新が失敗する場合があります。この問題を解決するには、プロキシサーバーまたはファイアウォールの制限を確認し、次のアドレスにアクセスできることを確認してください: `https://*.amazonaws.com`。

ホスト接続のデフォルト値

AWSクラウド環境でホスト接続を作成すると、次のデフォルト値が表示されます。

オプション	絶対値	パーセンテージ
同時実行アクション（すべての種類）	125	100
1分あたりの新規アクションの最大数	125	

MCS は、デフォルトで最大 100 の同時プロビジョニング操作をサポートしています。

サービスエンドポイントURL

標準ゾーンサービスエンドポイントURL

MCSを使用すると、APIキーとAPIシークレットを持つ新しいAWS接続が追加されます。この情報と認証済みアカウントを使用して、MCSはAWS DescribeRegions EC2 API呼び出しを使用して、サポートされているゾーンをAWSに照会します。クエリは、汎用EC2サービスエンドポイントURL `https://ec2.amazonaws.com/` を使用して行われます。MCSを使用して、サポートされているゾーンのリストから接続のゾーンを選択します。優先されるAWSサービスエンドポイントURLは、そのゾーンに対して自動的に選択されます。ただし、サービスエンドポイントURLを作成した後、そのURLを設定または変更することはできません。

IAM権限を定義する

このセクションの情報を使用して、AWS上のCitrix Virtual Apps and DesktopsのIAM権限を定義します。AmazonのIAMサービスでは、複数のユーザーを持つアカウントが許可されており、それらのユーザーはさらにグループに編成できます。これらのユーザーは、アカウントに関連する操作を

実行する能力を制御するために、異なる権限を持つことができます。IAM権限の詳細については、IAM JSON ポリシーリファレンスを参照してください。

新しいユーザーグループにIAM権限ポリシーを適用するには：

1. AWSマネジメントコンソールにログインし、ドロップダウンリストから**IAMサービス**を選択します。
2. **新しいユーザーグループの作成**を選択します。
3. 新しいユーザーグループの名前を入力し、**続行**を選択します。
4. **Permissions**ページで、**Custom Policy**を選択します。**Select**を選択します。
5. **権限ポリシー**の名前を入力します。
6. **Policy Document**セクションで、関連する権限を入力します。

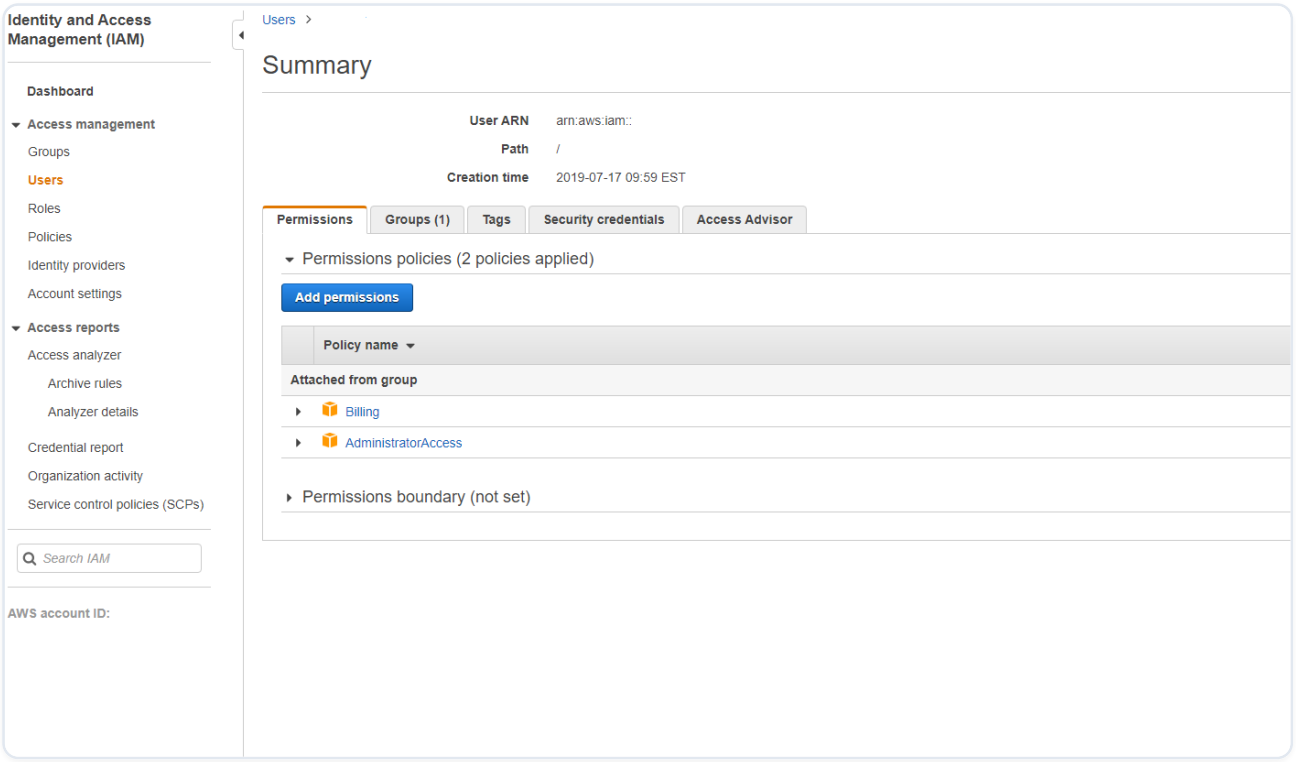
ポリシー情報を入力したら、**Continue**を選択してユーザーグループを完了します。グループ内のユーザーには、Citrix Virtual Apps and Desktopsに必要なアクションのみを実行する権限が付与されます。

> **重要:**
>
> 前の例で提供されているポリシーステキストを使用して、Citrix Virtual Apps and DesktopsがAWSアカウント内でアクションを実行するために使用するアクションを、特定のリソースに制限することなくリストします。Citrixは、テスト目的でこの例を使用することをお勧めします。本番環境では、リソースにさらなる制限を追加することを選択できます。

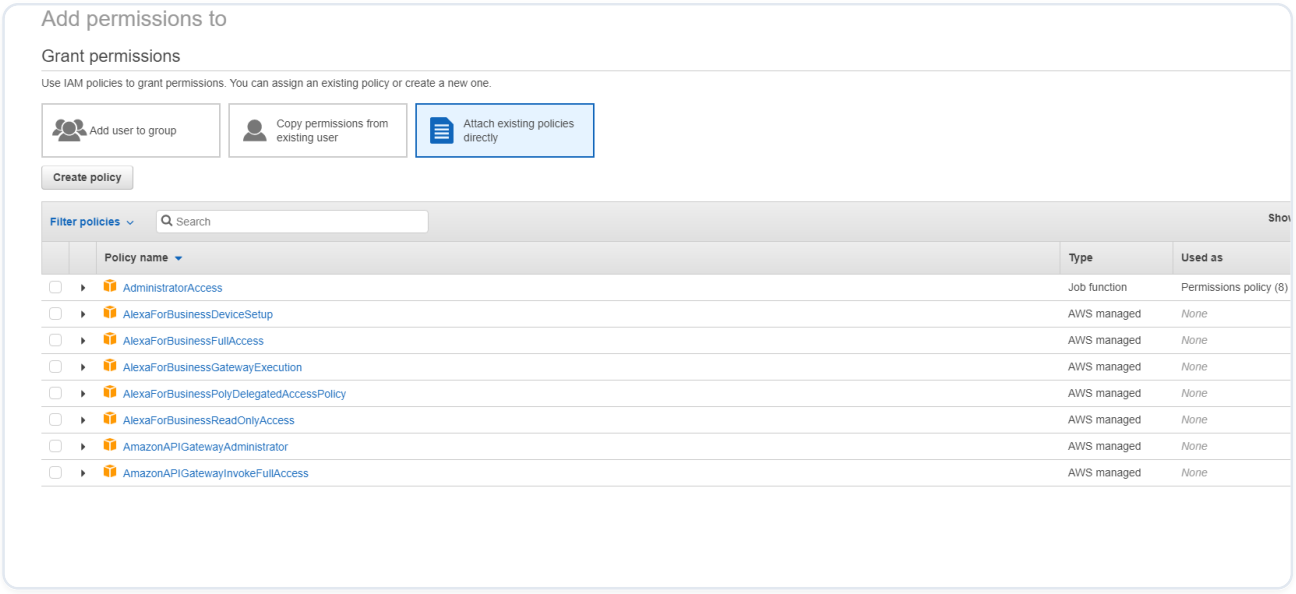
IAM権限を設定する

AWSマネジメントコンソールの**IAM**セクションで権限を設定します。

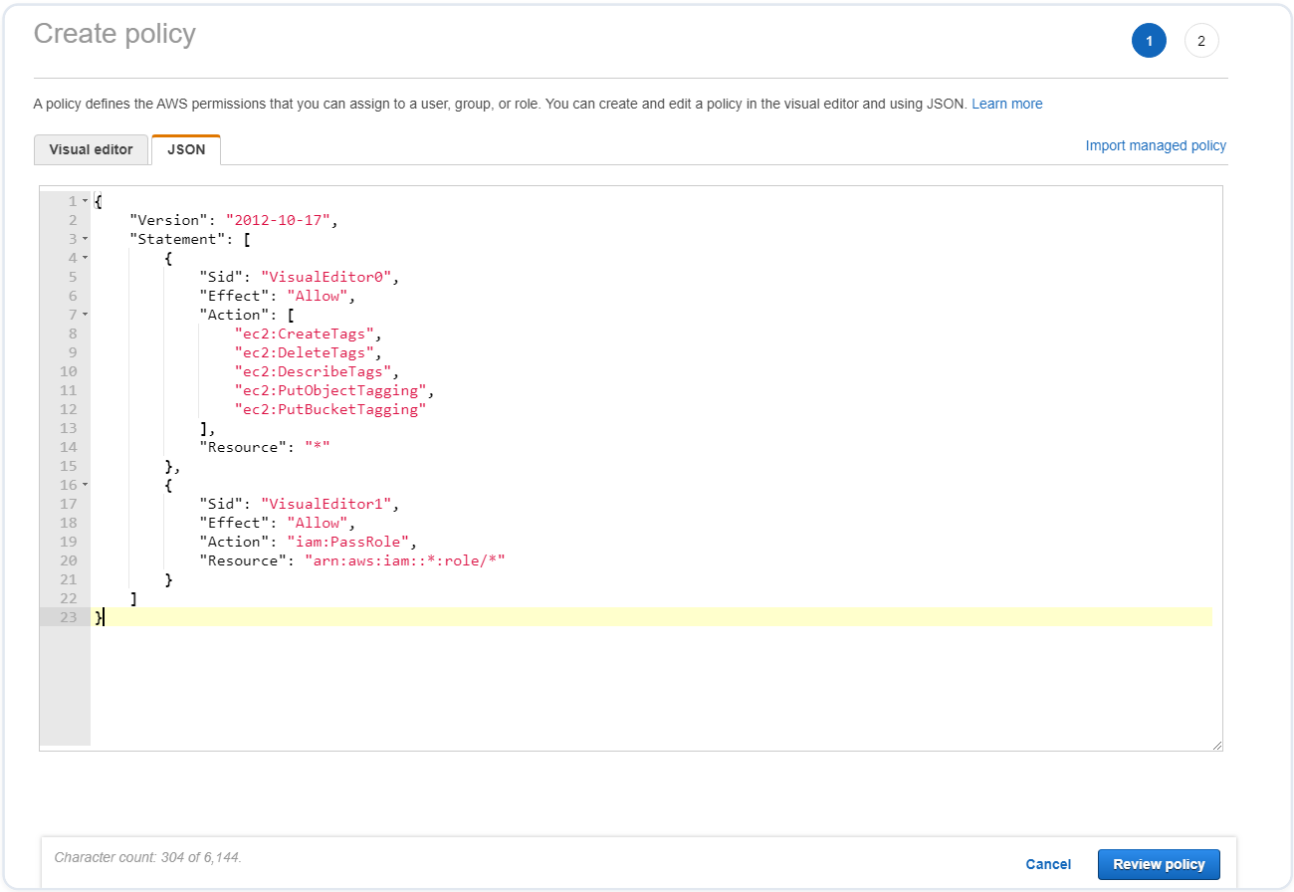
1. **概要**パネルで、**アクセス許可**タブを選択します。
2. **アクセス許可の追加**を選択します。



アクセス許可の追加先画面で、アクセス許可を付与します。



「**JSON**」タブで、以下を例として使用します。



ヒント:

記載されているJSONの例には、お使いの環境に必要なすべての権限が含まれていない場合があります。詳細については、「AWS で Citrix Virtual Apps and Desktops を実行するための ID およびアクセス管理権限を定義する方法」を参照してください。

必要なAWS権限

このセクションには、AWS権限の完全なリストが含まれています。

注：

iam:PassRole 権限は、**role_based_auth** の場合にのみ必要です。

ホスト接続の作成

AWSからの情報を使用して、新しいホスト接続が追加されます。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeImages",
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceTypes",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:DescribeRegions",
                "ec2:DescribeSnapshots",
                "ec2:DescribeLaunchTemplates"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

VM の電源管理

マシンインスタンスの電源がオンまたはオフになります。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:AttachVolume",
                "ec2:CreateVolume",
                "ec2:DeleteVolume",
                "ec2:DescribeInstances",
                "ec2:DescribeVolumes",
                "ec2:DetachVolume",
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:DescribeInstanceStatus"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

仮想マシンの作成、更新、または削除

AWSインスタンスとしてプロビジョニングされたVMを使用して、マシンカタログが作成、更新、または削除されます。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:AttachVolume",
                "ec2:AssociateIamInstanceProfile",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateImage",
                "ec2:CreateLaunchTemplate",
                "ec2:CreateSecurityGroup",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:DeleteVolume",
                "ec2:DescribeAccountAttributes",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeIamInstanceProfileAssociations",
                "ec2:DescribeImages",
                "ec2:DescribeInstances",
```

```
                "ec2:DescribeInstanceTypes",

                "ec2:DescribeInstanceStatus"

                "ec2:DescribeLaunchTemplates",

                "ec2:DescribeLaunchTemplateVersions",

                "ec2:DescribeNetworkInterfaces",

                "ec2:DescribeRegions",

                "ec2:DescribeSecurityGroups",

                "ec2:DescribeSnapshots",

                "ec2:DescribeSubnets",

                "ec2:DescribeTags",

                "ec2:DescribeSpotInstanceRequests",

                "ec2:DescribeInstanceCreditSpecifications",

                "ec2:DescribeInstanceAttribute",

                "ec2:GetLaunchTemplateData",

                "ec2:DescribeVolumes",

                "ec2:DescribeVpcs",

                "ec2:DetachVolume",

                "ec2:DisassociateIamInstanceProfile",

                "ec2:RunInstances",

                "ec2:StartInstances",

                "ec2:StopInstances",

                "ec2:TerminateInstances"
```

```
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateSecurityGroup",
                "ec2:DeleteSecurityGroup",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupIngress"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "s3:CreateBucket",
                "s3:DeleteBucket",
                "s3:PutBucketAcl",
                "s3:PutBucketTagging",
```

```
                "s3:PutObject",
                "s3:GetObject",
                "s3:DeleteObject",
                "s3:PutObjectTagging"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:s3:::citrix*"
        },
        {
            "Action": [
                "ebs:StartSnapshot",
                "ebs:GetSnapshotBlock",
                "ebs:PutSnapshotBlock",
                "ebs:CompleteSnapshot",
                "ebs:ListSnapshotBlocks",
                "ebs:ListChangedBlocks",
                "ec2:CreateSnapshot"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
```

```
}
```

注：

セキュリティグループに関連するEC2セクションは、カタログ作成時に準備VM用に分離セキュリティグループを作成する必要がある場合にのみ必要です。これが完了すると、これらの権限は不要になります。

ディスクの直接アップロードとダウンロード

直接ディスクアップロードは、マシンカタログプロビジョニングにおけるボリュームワーカーの要件を排除し、代わりにAWSが提供するパブリックAPIを使用します。この機能により、追加のストレージアカウントに関連するコストと、ボリュームワーカー操作を維持する複雑さが軽減されます。

注:

ボリュームワーカーのサポートは非推奨になりました。

以下の権限をポリシーに追加する必要があります。

- `ebs:StartSnapshot`
- `ebs:GetSnapshotBlock`
- `ebs:PutSnapshotBlock`
- `ebs:CompleteSnapshot`
- `ebs:ListSnapshotBlocks`
- `ebs:ListChangedBlocks`
- `ec2:CreateSnapshot`
- `ec2:DeleteSnapshot`
- `ec2:DescribeLaunchTemplates`

重要:

- ボリュームワーカーAMIやボリュームワーカーVMなどのボリュームワーカー操作なしで、既存のマシンカタログにVMを追加できます。
- 以前にボリュームワーカーを使用していた既存のカタログを削除すると、ボリュームワーカー関連を含むすべてのアーティファクトが削除されます。

作成されたボリュームのEBS暗号化

AMIが暗号化されている場合、またはEBSがすべての新しいボリュームを暗号化するように構成されている場合、EBSは新しく作成されたボリュームを自動的に暗号化できます。ただし、この機能を実装するには、IAMポリシーに次の権限を含める必要があります。

```
{
     "Version": "2012-10-17",
     "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                 "kms:CreateGrant",
                 "kms:Decrypt",
                 "kms:DescribeKey",
                 "kms:GenerateDataKeyWithoutPlainText",
                 "kms:ReEncryptTo",
                 "kms:ReEncryptFrom"
            ],
            "Resource": "*"
        }
```

```
    ]

}
```

注:

ユーザーの判断により、リソースと条件ブロックを含めることで、権限を特定のキーに限定できます。例：**条件付きKMS権限**：

```
{

     "Version": "2012-10-17",

     "Statement": [

        {

            "Effect": "Allow",

            "Action": [

                 "kms:CreateGrant",

                 "kms:Decrypt",

                 "kms:DescribeKey",

                 "kms:GenerateDataKeyWithoutPlainText",

                 "kms:ReEncryptTo",

                 "kms:ReEncryptFrom"

            ],

            "Resource": [

                "arn:aws:kms:us-east-2:123456789012:key/abcd1234-
a123-456d-a12b-a123b4cd56ef"
```

```
            ],
            "Condition": {
                "Bool": {
                    "kms:GrantIsForAWSResource": true
                }
            }
        }
    ]
}
```

次のキーポリシーステートメントは、アカウントがIAMポリシーを使用してKMSキーに対するすべてのアクション (kms:*) の権限を委任できるようにするために必要な、KMSキーのデフォルトのキーポリシー全体です。

```
{
"Sid": "Enable IAM policies",
"Effect": "Allow",
"Principal": {
"AWS": "arn:aws:iam::111122223333:root"
},
"Action": "kms:",
"Resource": ""
}
```

詳細については、「AWS Key Management Service 公式ドキュメント」を参照してください。

IAMロールベース認証

ロールベース認証をサポートするために、次の権限が追加されます。

```
{

     "Version": "2012-10-17",

     "Statement": [

        {

            "Effect": "Allow",

            "Action": "iam:PassRole",

            "Resource": "arn:aws:iam::*:role/*"

        }

    ]

}
```

最小限のIAM権限ポリシー

以下のJSONは、現在サポートされているすべての機能に使用できます。このポリシーを使用して、ホスト接続の作成、VMの作成、更新、削除、および電源管理を行うことができます。 このポリシーは、「IAM権限の定義」セクションで説明されているようにユーザーに適用することも、**role_based_auth** セキュリティキーとシークレットキーを使用してロールベース認証を使用することもできます。

> **重要:**
>
> **role_based_auth** を使用するには、まずサイト内のすべてのDelivery Controllerで目的のIAMロールを構成します。Web Studioを使用してホスティング接続を追加し、認証キーとシークレットに role_based_auth を指定します。これらの設定を持つホスティング接続は、ロールベース認証を使用します。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:AttachVolume",
                "ec2:AssociateIamInstanceProfile",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateImage",
                "ec2:CreateLaunchTemplate",
                "ec2:CreateNetworkInterface",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:DeleteLaunchTemplate",
                "ec2:DeleteNetworkInterface",
                "ec2:DeleteSecurityGroup",
                "ec2:DeleteSnapshot",
                "ec2:DeleteTags",
                "ec2:DeleteVolume",
                "ec2:DeregisterImage",
                "ec2:DescribeAccountAttributes",
```

```
                "ec2:DescribeAvailabilityZones",

                "ec2:DescribeIamInstanceProfileAssociations",

                "ec2:DescribeImages",

                "ec2:DescribeInstances",

                "ec2:DescribeInstanceTypes",

                "ec2:DescribeInstanceStatus",

                "ec2:DescribeLaunchTemplates",

                "ec2:DescribeLaunchTemplateVersions",

                "ec2:DescribeNetworkInterfaces",

                "ec2:DescribeRegions",

                "ec2:DescribeSecurityGroups",

                "ec2:DescribeSnapshots",

                "ec2:DescribeSubnets",

                "ec2:DescribeTags",

                "ec2:DescribeSpotInstanceRequests",

                "ec2:DescribeInstanceCreditSpecifications",

                "ec2:DescribeInstanceAttribute",

                "ec2:GetLaunchTemplateData",

                "ec2:DescribeVolumes",

                "ec2:DescribeVpcs",

                "ec2:DetachVolume",

                "ec2:DisassociateIamInstanceProfile",
```

```
                "ec2:RebootInstances",
                "ec2:RunInstances",
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateSecurityGroup",
                "ec2:DeleteSecurityGroup",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupIngress"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
```

```
            "Action": [
                "s3:CreateBucket",
                "s3:DeleteBucket",
                "s3:DeleteObject",
                "s3:GetObject",
                "s3:PutBucketAcl",
                "s3:PutObject",
                "s3:PutBucketTagging",
                "s3:PutObjectTagging"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:s3:::citrix*"
        },
        {
            "Action": [
                "ebs:StartSnapshot",
                "ebs:GetSnapshotBlock",
                "ebs:PutSnapshotBlock",
                "ebs:CompleteSnapshot",
                "ebs:ListSnapshotBlocks",
                "ebs:ListChangedBlocks",
                "ec2:CreateSnapshot"
```

```
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "kms:CreateGrant",
                "kms:Decrypt",
                "kms:DescribeKey",
                "kms:GenerateDataKeyWithoutPlainText",
                "kms:GenerateDataKey",
                "kms:ReEncryptTo",
                "kms:ReEncryptFrom"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "arn:aws:iam::*:role/*"
        }
```

```
    ]

}
```

注:

- SecurityGroupsに関連するEC2セクションは、カタログ作成中に準備VM用に分離セキュリティグループを作成する必要がある場合にのみ必要です。これが完了すると、これらの権限は不要になります。
- KMSセクションは、EBSボリューム暗号化を使用する場合にのみ必要です。
- iam:PassRole 権限セクションは、**role_based_auth** の場合にのみ必要です。
- 要件と環境に基づいて、フルアクセスではなく特定のリソースレベルの権限を追加できます。詳細については、AWSドキュメントのDemystifying EC2 Resource-Level Permissions および Access management for AWS resources を参照してください。

次のステップ

- 初期展開プロセス中の場合は、「マシンカタログの作成」を参照してください。
- AWS固有の情報については、AWSカタログの作成を参照してください。

詳細情報

- 接続とリソース
- マシンカタログの作成

XenServer®への接続

「接続とリソースの作成および管理」(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/install-configure/connections.html)では、接続を作成するウィザードについて説明します。以下の情報は、XenServer仮想化環境に固有の詳細を扱っています。

注:

> XenServerへの接続を作成する前に、まずXenServerアカウントをリソースの場所として設定を完了する必要があります。「XenServer仮想化環境」(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/install-configure/install-prepare/xenserver.html)を参照してください。

XenServerへの接続を作成する

XenServer（旧Citrix Hypervisor™）への接続を作成する際は、VM Power Admin以上の権限を持つユーザーの資格情報を指定する必要があります。

Citrixでは、XenServerとの通信を保護するためにHTTPSを使用することを推奨しています。HTTPSを使用するには、XenServerにインストールされているデフォルトの SSL証明書を置き換える必要があります。

XenServerサーバーで高可用性が有効になっている場合、それを構成できます。Citrix Virtual Apps and Desktopsのバージョン2507 LTSRより前のバージョンでは、プール内のすべてのサーバーにワイルドカード証明書をインストールすることはできません。各サーバーに個別の証明書が必要です。

XenServerがvGPUをサポートしている場合、GPUの種類とグループを選択するか、パススルーすることができます。表示は、選択に専用GPUリソースがあるかどうかを示します。

1つ以上のXenServerホストで一時データストレージにローカルストレージを使用する場合、プール内の各ストレージの場所に一意の名前があることを確認してください。（XenCenter®で名前を変更するには、ストレージを右クリックして名前プロパティを編集します。）

Citrix Provisioning（旧Provisioning Services）およびMachine Creation Services™（MCS）を使用して、以下をプロビジョニングできます。

- サポートされているデスクトップまたはサーバーOS VM用のレガシーBIOS。
- セキュアブートを含む、サポートされているデスクトップまたはサーバーOS VM用のUEFI。

> **注:**
>
> MCSを構成する際には、プールオペレーター以上の権限が必要です。

XenServer接続にIntelliCache™を使用する

IntelliCacheを使用すると、共有ストレージとローカルストレージの組み合わせを使用できるため、ホスト型VDI展開の費用対効果が高まります。これにより、パフォーマンスが向上し、ネットワークトラフィックが削減されます。ローカルストレージは共有ストレージからマスターイメージ

をキャッシュするため、共有ストレージへの読み取り回数が減少します。共有デスクトップの場合、差分ディスクへの書き込みは、共有ストレージではなくホスト上のローカルストレージに書き込まれます。

- IntelliCacheを使用する場合、共有ストレージはNFSである必要があります。
- Citrixでは、可能な限り最速のデータ転送を確保するために、高性能なローカルストレージデバイスを使用することを推奨しています。

IntelliCacheを使用するには、この製品とXenServerの両方で有効にする必要があります。

- XenServerをインストールする際に、**Enable thin provisioning (Optimized storage for Virtual Desktops)** を選択します。Citrixは、IntelliCacheが有効なサーバーと有効でないサーバーが混在するプールをサポートしていません。詳細については、XenServerのドキュメントを参照してください。
- Citrix Virtual Apps and Desktops™では、IntelliCacheはデフォルトで無効になっています。この設定はXenServer接続を作成するときにのみ変更でき、後でIntelliCacheを無効にすることはできません。XenServer接続を追加する際：
  - ストレージの種類として**「Shared」**を選択します。
  - 「**IntelliCache を使用**」チェックボックスをオンにします。

必要なXenServer権限

XenServerの権限はロールベース（RBAC）です。XenServerのロールベースアクセス制御（RBAC）機能を使用すると、ユーザー、ロール、および権限を割り当てて、XenServerへのアクセス権を持つユーザーと、それらのユーザーが実行できるアクションを制御できます。XenServer RBACシステムは、ユーザー（またはユーザーグループ）を定義されたロール（名前付きの権限セット）にマッピングします。ロールには、特定の操作を実行するための関連するXenServer権限があります。

詳細については、「Role-based access control」を参照してください。

権限が増加する順序でのロール階層は、次のとおりです。Read-Only → VM Operator → VM Admin → VM Power Admin → Pool Operator → Pool Admin。

次のセクションでは、各プロビジョニングタスクに必要な最小ロールをまとめます。

ホスト接続の作成

タスク	必要な最小ロール
XenServerから取得した情報を使用してホスト接続を追加する	読み取り専用
ユーザーとその割り当てられた役割を表示する	読み取り専用

VMの電源管理

タスク	必要な最小限の役割
VMの電源をオンまたはオフにする	VMオペレーター

VMの作成、更新、または削除

タスク	必要な最小限の役割
既存のスナップショットスケジュールにVMを追加または削除する	VM電源管理者
スナップショットスケジュールの追加、変更、削除	プールオペレーター
マスターイメージの公開	プールオペレーター（スイッチポートロックが必要）
マシンカタログの作成	プールオペレーター: スイッチポートロックが必要
VMの追加または削除（GPU対応VMではない）	VM管理者
VMの追加または削除（GPU対応VM）	プールオペレーター
仮想ディスクまたはCDデバイスの追加、削除、または構成	VM管理者
タグの管理	VMオペレーター

RBACの役割と権限の詳細については、「RBACの役割と権限」を参照してください。

スイッチポートロックの詳細については、「スイッチポートロックの使用」を参照してください。

次のステップ

- 初期展開プロセス中の場合は、「マシンカタログの作成」を参照してください。
- XenServer 固有の情報については、XenServer カタログの作成を参照してください。

詳細情報

- 接続とリソース
- マシンカタログの作成

Google Cloud環境への接続

接続とリソースの作成および管理では、接続を作成するウィザードについて説明します。以下の情報は、Google Cloud環境に固有の詳細を扱っています。

> **注:**
>
> Google Cloud環境への接続を作成する前に、まずリソースロケーションとしてGoogle Cloudアカウントの設定を完了する必要があります。Google Cloud環境を参照してください。

接続の追加

接続とリソースの作成のガイダンスに従ってください。以下の説明は、ホスティング接続の設定について案内します。

1. **管理 > 構成**から、左側のペインで**ホスティング**を選択します。
2. アクションバーで**「接続とリソースの追加」**を選択します。
3. **「接続」ページで、「新しい接続の作成」と「Citrix provisioning™ tools」を選択し、「次へ」**を選択します。
   - **接続の種類**。メニューから**Google Cloud**を選択します。
   - **接続名**。接続の名前を入力します。
4. **「リージョン」**ページで、メニューからプロジェクト名を選択し、使用するリソースを含むリージョンを選択してから、**「次へ」**を選択します。

5. 「**ネットワーク**」ページで、リソースの名前を入力し、メニューから仮想ネットワークを選択し、サブセットを選択してから、「**次へ**」を選択します。リソース名は、リージョンとネットワークの組み合わせを識別するのに役立ちます。名前に「*(Shared)*」サフィックスが付いている仮想ネットワークは、共有VPCを表します。共有VPCのサブネットレベルのIAMロールを構成した場合、共有VPCの特定のサブネットのみがサブネットリストに表示されます。

   > **注:**
   >
   > - リソース名には1～64文字を含めることができ、空白のみ、または文字`\ / ; : # . * ? = < > | [ ] { } " ' ( ) ' )`を含めることはできません。

6. 「**概要**」ページで情報を確認し、「**完了**」を選択して「**接続とリソースの追加**」ウィンドウを終了します。

接続とリソースを作成すると、作成した接続とリソースが一覧表示されます。接続を構成するには、接続を選択し、アクションバーで該当するオプションを選択します。

同様に、接続の下に作成されたリソースを削除、名前変更、またはテストできます。これを行うには、接続の下のリソースを選択し、アクションバーで該当するオプションを選択します。

サービスエンドポイントURL

次のURLにアクセスできる必要があります。

- `https://oauth2.googleapis.com`
- `https://cloudresourcemanager.googleapis.com`
- `https://compute.googleapis.com`
- `https://storage.googleapis.com`
- `https://cloudbuild.googleapis.com`

Google Cloudプロジェクト

Google Cloudプロジェクトには基本的に2つのタイプがあります。

- プロビジョニングプロジェクト：この場合、現在の管理者アカウントがプロジェクト内のプロビジョニングされたマシンを所有します。このプロジェクトはローカルプロジェクトとも呼ばれます。

- 共有VPCプロジェクト: プロビジョニングプロジェクトで作成されたマシンが、共有VPCプロジェクトのVPCを使用するプロジェクト。プロビジョニングプロジェクトに使用される管理者アカウントは、このプロジェクトで限られた権限、具体的にはVPCを使用する権限のみを持ちます。

GCP管理トラフィックのセキュアな環境を作成する

Google Cloudプロジェクトへのプライベートアクセスを許可できます。この実装により、機密データを処理するためのセキュリティが強化されます。これを実現するには、次のいずれかを実行できます。

- Cloud BuildサービスアカウントのVPCサービスコントロールの以下のイングレスルールを含めます。この手順を実行する場合は、GCP管理トラフィックのセキュアな環境を作成するための以下の手順に従わないでください。

```
Ingress Rule 1

From:

Identities:

<ProjectID>@cloudbuild.gserviceaccount.com

Source > All sources allowed

To:

Projects =

All projects

Services =

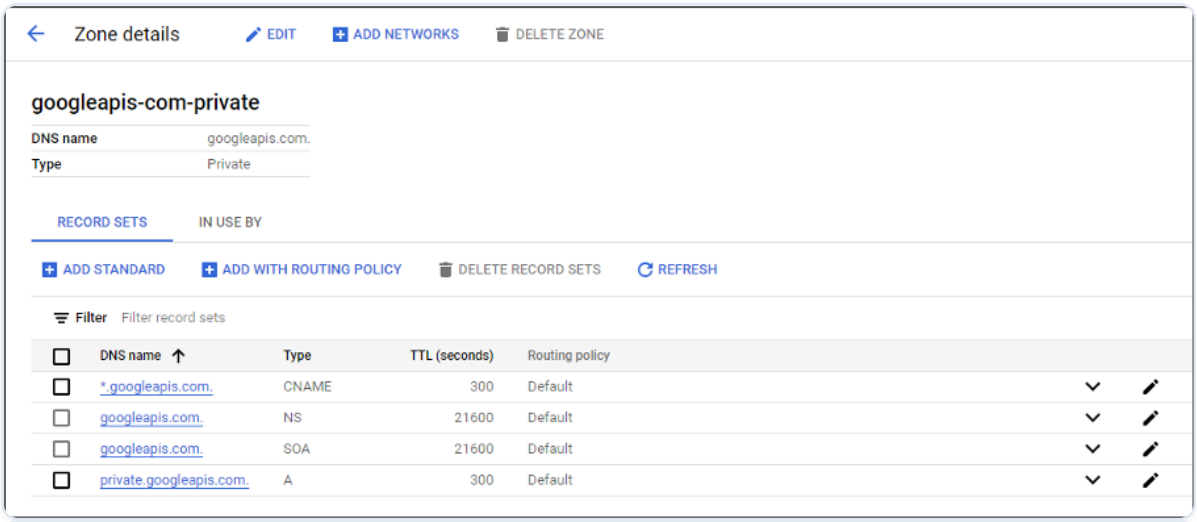
Service name: All services
```

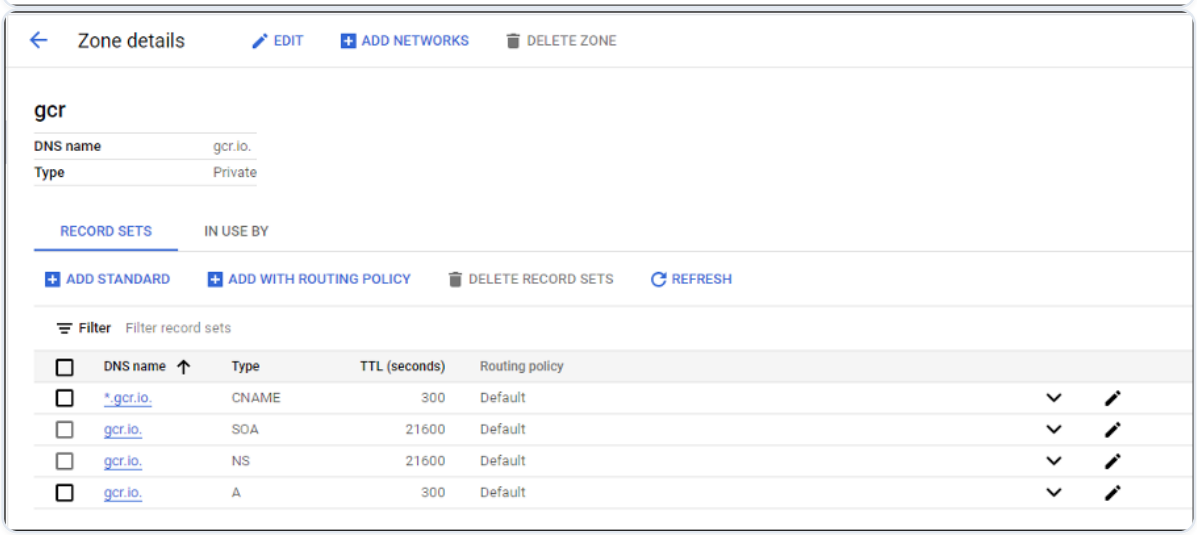
- プライベートワーカープールを使用している場合は、`CustomProperties`に`UsePrivateWorkerPool`を追加します。プライベートワーカープールの詳細については、プライベートプール概要を参照してください。

GCP管理トラフィックのセキュアな環境を作成するための要件

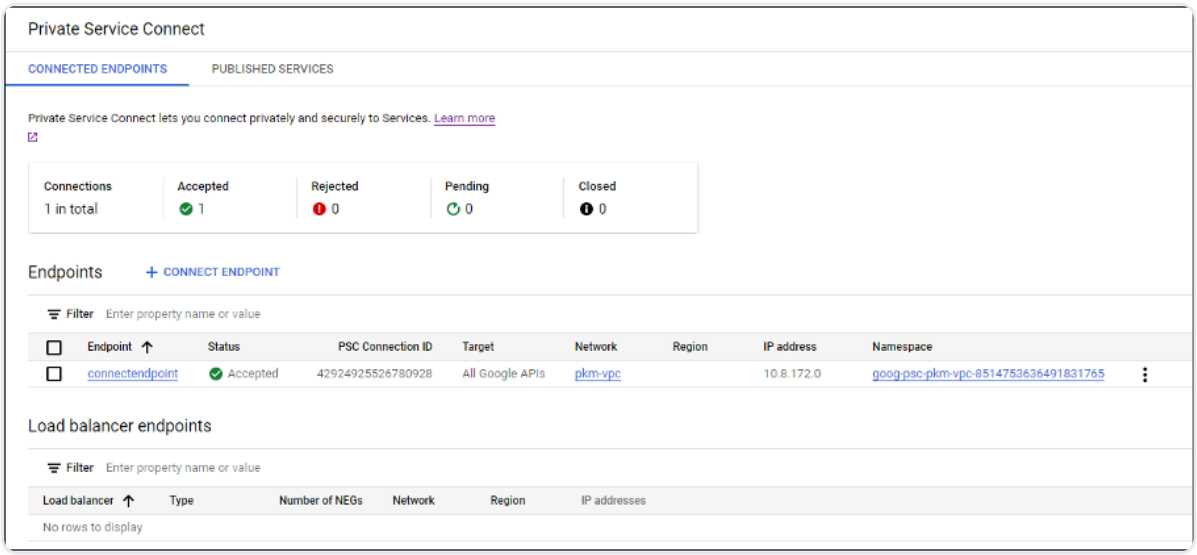
GCP管理トラフィックのセキュアな環境を作成するための要件は次のとおりです。

- カスタムプロパティを更新する際は、ホスティング接続がメンテナンスモードであることを確認してください。
- プライベートワーカープールを使用するには、次の変更が必要です。
  - Citrix Cloud™サービスアカウントには、以下のIAMロールを追加します。
    - Cloud Build サービスアカウント
    - Compute Instance 管理者
    - サービスアカウントユーザー
    - サービスアカウントトークン作成者
    - Cloud Build WorkerPool オーナー
  - ホスティング接続の作成に使用するのと同じプロジェクトにCitrix Cloudサービスアカウントを作成します。
  - DNS構成で説明されているように、`private.googleapis.com`および`gcr.io`のDNSゾーンを設定します。

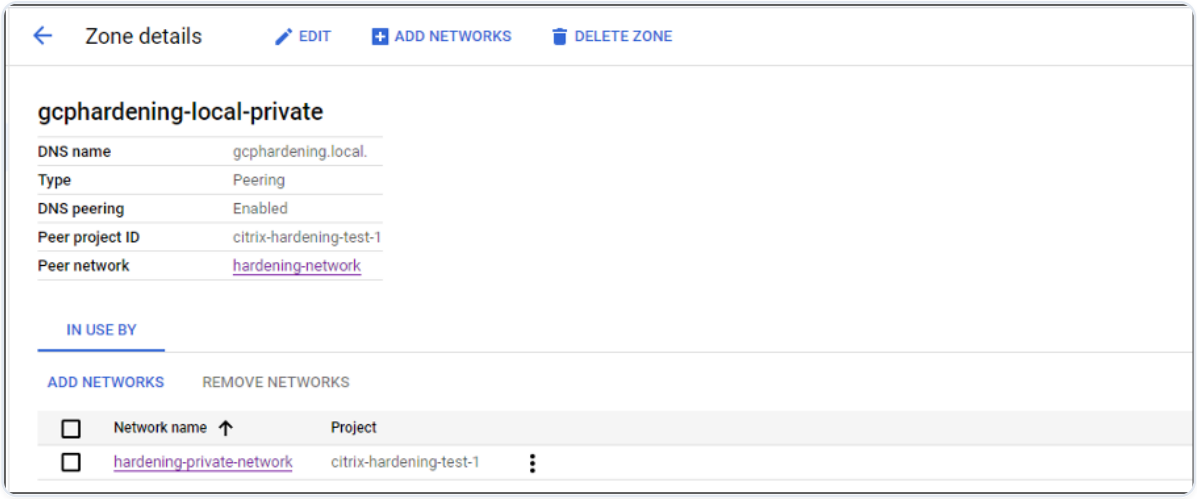




- プライベートネットワークアドレス変換 (NAT) を設定するか、プライベートサービス接続を使用します。詳細については、「エンドポイントを介したGoogle APIへのアクセス」を参照してください。



- ピアリングされたVPCを使用している場合は、ピアリングされたVPCへのCloud DNSゾーンピアリングを作成します。詳細については、「ピアリングゾーンの作成」を参照してください。



- VPCサービスコントロールで、APIとVMがインターネットと通信できるようにエグレスルールを設定します。イングレスルールはオプションです。例：

```
Egress Rule 1

From:

Identities:ANY_IDENTITY

To:
```

```
Projects =

All projects

Service =

Service name: All services
```

プライベートワーカープールを有効にする

プライベートワーカープールを有効にするには、ホスト接続でカスタムプロパティを次のように設定します。

1. Delivery ControllerホストからPowerShellウィンドウを開くか、Remote PowerShell SDKを使用します。Remote PowerShell SDKの詳細については、「SDKとAPI」を参照してください。
2. 次のコマンドを実行します。
   a. `Add-PSSnapin citrix*`
   b. `cd XDHyp:\Connections\`
   c. `dir`
3. 接続から`CustomProperties`をメモ帳にコピーします。
4. プロパティ設定`<Property xsi:type="StringProperty" Name="UsePrivateWorkerPool" Value="True"/>`を追加します。例：

```
```

<CustomProperties xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns="http://schemas.citrix.com/2014/xd/machinecreation">

<Property xsi:type="StringProperty" Name="UsePrivateWorkerPool"
Value="True"/>

</CustomProperties>

```
```

5. PowerShellウィンドウで、変更されたカスタムプロパティに変数を割り当てます。例：`$customProperty = '<CustomProperties…</CustomProperties>'`。

6. `$gcpServiceAccount = "<ENTER YOUR SERVICE ACCOUNT EMAIL HERE>"`を実行します。
7. `$gcpPrivateKey = "<ENTER YOUR SERVICE ACCOUNT PRIVATE KEY HERE AFTER REMOVING ALL INSTANCES OF \n >"`を実行します。
8. `$securePassword = ConvertTo-SecureString $gcpPrivateKey -AsPlainText -Force`を実行します。
9. 既存のホスト接続を更新するには、以下を実行します。

```
Set-Item -PassThru -Path @('XDHyp:\\Connections\\<ENTER YOUR CONNECTION NAME HERE>') -SecurePassword $securePassword -UserName $gcpServiceAccount -CustomProperties $customProperty
```

必要なGCP権限

このセクションには、GCP権限の完全なリストが含まれています。機能が正しく動作するように、このセクションに記載されている権限の完全なセットを使用してください。

注:

GCPは、Cloud Build Servicesのデフォルトの動作とサービスアカウントの使用に関して、April 29, 2024以降に変更を導入します。詳細については、Cloud Build Service Account Changeを参照してください。April 29, 2024より前にCloud Build APIが有効になっている既存のGoogleプロジェクトは、この変更の影響を受けません。ただし、April 29以降も既存のCloud Build Serviceの動作を維持したい場合は、APIを有効にする前に、制約の適用を無効にする組織ポリシーを作成または適用できます。新しい組織ポリシーを設定した場合、このセクションの既存の権限と、**Cloud Build Service Account Change前**とマークされている項目を引き続き使用できます。そうでない場合は、既存の権限と、**Cloud Build Service Account Change後**とマークされている項目に従ってください。

ホスト接続の作成

- プロビジョニングプロジェクトのCitrix Cloudサービスアカウントに必要な最小限の権限：

```
compute.instanceTemplates.list

compute.instances.list

compute.networks.list
```

```
compute.projects.get

compute.regions.list

compute.subnetworks.list

compute.zones.list

resourcemanager.projects.get
```

次の Google 定義ロールには、上記にリストされている権限があります:

- Compute 管理者
- クラウド データストア ユーザー

- 共有 VPC プロジェクト内の Citrix Cloud サービスアカウントの共有 VPC に必要な追加の権限:

```
compute.networks.list

compute.subnetworks.list

resourcemanager.projects.get
```

次の Google 定義ロールには、上記にリストされている権限があります:

- コンピュート ネットワーク ユーザー

仮想マシンの電源管理

電源管理のみのカタログの場合に、プロビジョニングプロジェクト内のCitrix Cloudサービスアカウントに必要な最小限の権限:

```
compute.instanceTemplates.list

compute.instances.list

compute.instances.get

compute.instances.reset

compute.instances.resume
```

```
compute.instances.start

compute.instances.stop

compute.instances.suspend

compute.networks.list

compute.projects.get

compute.regions.list

compute.subnetworks.list

compute.zones.list

resourcemanager.projects.get

compute.zoneOperations.get
```

次のGoogle定義のロールは、上記の権限を持っています:

- Compute管理者
- クラウド データストア ユーザー

仮想マシンの作成、更新、または削除

- プロビジョニングプロジェクト内のCitrix Cloudサービスアカウントに必要な最小限の権限:

```
cloudbuild.builds.create

cloudbuild.builds.get

cloudbuild.builds.list

compute.acceleratorTypes.list

compute.diskTypes.get

compute.diskTypes.list

compute.disks.create
```

```
compute.disks.createSnapshot

compute.disks.delete

compute.disks.get

compute.disks.list

compute.disks.setLabels

compute.disks.use

compute.disks.useReadOnly

compute.firewalls.create

compute.firewalls.delete

compute.firewalls.list

compute.globalOperations.get

compute.images.create

compute.images.delete

compute.images.get

compute.images.list

compute.images.setLabels

compute.images.useReadOnly

compute.instanceTemplates.create

compute.instanceTemplates.delete

compute.instanceTemplates.get

compute.instanceTemplates.list

compute.instanceTemplates.useReadOnly
```

```
compute.instances.attachDisk

compute.instances.create

compute.instances.delete

compute.instances.detachDisk

compute.instances.get

compute.instances.list

compute.instances.reset

compute.instances.resume

compute.instances.setDeletionProtection

compute.instances.setLabels

compute.instances.setMetadata

compute.instances.setServiceAccount

compute.instances.setTags

compute.instances.start

compute.instances.stop

compute.instances.suspend

compute.machineTypes.get

compute.machineTypes.list

compute.networks.list

compute.networks.updatePolicy

compute.nodeGroups.list

compute.nodeTemplates.get
```

```
compute.projects.get

compute.regions.list

compute.snapshots.create

compute.snapshots.delete

compute.snapshots.list

compute.snapshots.get

compute.snapshots.setLabels

compute.snapshots.useReadOnly

compute.subnetworks.get

compute.subnetworks.list

compute.subnetworks.use

compute.zoneOperations.get

compute.zoneOperations.list

compute.zones.get

compute.zones.list

iam.serviceAccounts.actAs

resourcemanager.projects.get

storage.buckets.create

storage.buckets.delete

storage.buckets.get

storage.buckets.list

storage.buckets.update
```

```
storage.objects.create

storage.objects.delete

storage.objects.get

storage.objects.list

compute.networks.get

compute.resourcePolicies.use
```

以下のGoogle定義ロールには、上記にリストされている権限があります:

- Compute管理者
- Storage管理者
- Cloud Build編集者
- サービスアカウントユーザー
- クラウド データストア ユーザー

- 共有VPCプロジェクトのVPCとサブネットワークを使用してホスティングユニットを作成するために、共有VPCプロジェクト内のCitrix Cloudサービスアカウントの共有VPCに追加で必要な権限:

```
compute.firewalls.list

compute.networks.list

compute.projects.get

compute.regions.list

compute.subnetworks.get

compute.subnetworks.list

compute.subnetworks.use

compute.zones.list
```

```
resourcemanager.projects.get
```

以下のGoogle定義ロールには、上記にリストされている権限があります:

- コンピュートネットワークユーザー
- クラウド データストア ユーザー

MCSに準備指示ディスクをダウンロードする際に必要な最小限の権限:

- (Cloud Buildサービスアカウント変更前): プロビジョニングプロジェクトのCloud Buildサービスアカウントにこれらの権限を割り当てます。
- (Cloud Buildサービスアカウント変更後): プロビジョニングプロジェクトのCloud Computeサービスアカウントにこれらの権限を割り当てます。

```
compute.disks.create

compute.disks.delete

compute.disks.get

compute.disks.list

compute.disks.setLabels

compute.disks.use

compute.disks.useReadOnly

compute.images.get

compute.images.list

compute.images.useReadOnly

compute.instances.create

compute.instances.delete

compute.instances.get

compute.instances.getSerialPortOutput
```

```
compute.instances.list

compute.instances.setLabels

compute.instances.setMetadata

compute.instances.setServiceAccount

compute.machineTypes.list

compute.networks.get

compute.networks.list

compute.projects.get

compute.subnetworks.list

compute.subnetworks.use

compute.subnetworks.useExternalIp

compute.zoneOperations.get

compute.zones.list

iam.serviceAccounts.actAs

logging.logEntries.create

pubsub.topics.publish

resourcemanager.projects.get

source.repos.get

source.repos.list

storage.buckets.create

storage.buckets.get

storage.buckets.list
```

```
storage.objects.create

storage.objects.delete

storage.objects.get

storage.objects.list
```

以下のGoogle定義ロールには、上記にリストされている権限があります:

- Cloud Build サービスアカウント (Cloud Build サービスアカウント変更後はCloud Compute サービスアカウント)
- コンピュートインスタンス管理者
- サービスアカウントユーザー

- MCSに準備指示ディスクをダウンロードする際に、Google Cloud Buildサービスによってプロビジョニングプロジェクトの Cloud Compute サービスアカウントに必要とされる最小限の権限:

```
resourcemanager.projects.get

storage.objects.create

storage.objects.get

storage.objects.list
```

以下のGoogle定義ロールには、上記にリストされている権限があります:

- コンピュートネットワークユーザー
- ストレージアカウントユーザー
- クラウド データストア ユーザー

MCSに準備指示ディスクをダウンロードする際に、共有VPCに必要とされる追加の権限:

- (Cloud Buildサービスアカウント変更前): プロビジョニングプロジェクトのCloud Buildサービスアカウントにこれらの権限を割り当てます。
- (Cloud Buildサービスアカウント変更後): プロビジョニングプロジェクトのCloud Compute サービスアカウントにこれらの権限を割り当てます。

```
compute.firewalls.list

compute.networks.list

compute.subnetworks.list

compute.subnetworks.use

resourcemanager.projects.get
```

以下のGoogle定義ロールには、上記にリストされている権限があります:

- コンピュートネットワークユーザー
- ストレージアカウントユーザー
- クラウド データストア ユーザー

- プロビジョニングプロジェクトのCitrix CloudサービスアカウントのCloud Key Management Service (KMS) に必要な追加権限:

```
cloudkms.cryptoKeys.get

cloudkms.cryptoKeys.list

cloudkms.keyRings.get

cloudkms.keyRings.list
```

以下のGoogle定義ロールには、上記にリストされている権限があります:

- Compute KMS 閲覧者

一般的な権限

以下は、MCSでサポートされているすべての機能について、プロビジョニングプロジェクトのCitrix Cloudサービスアカウントの権限です。これらの権限は、今後最高の互換性を提供します:

```
resourcemanager.projects.get

cloudbuild.builds.create

cloudbuild.builds.get
```

```
cloudbuild.builds.list

compute.acceleratorTypes.list

compute.diskTypes.get

compute.diskTypes.list

compute.disks.create

compute.disks.createSnapshot

compute.disks.delete

compute.disks.get

compute.disks.setLabels

compute.disks.use

compute.disks.useReadOnly

compute.firewalls.create

compute.firewalls.delete

compute.firewalls.list

compute.globalOperations.get

compute.images.create

compute.images.delete

compute.images.get

compute.images.list

compute.images.setLabels

compute.images.useReadOnly

compute.instanceTemplates.create
```

```
compute.instanceTemplates.delete

compute.instanceTemplates.get

compute.instanceTemplates.list

compute.instanceTemplates.useReadOnly

compute.instances.attachDisk

compute.instances.create

compute.instances.delete

compute.instances.detachDisk

compute.instances.get

compute.instances.list

compute.instances.reset

compute.instances.resume

compute.instances.setDeletionProtection

compute.instances.setLabels

compute.instances.setMetadata

compute.instances.setTags

compute.instances.start

compute.instances.stop

compute.instances.suspend

compute.instances.update

compute.instances.updateAccessConfig

compute.instances.updateDisplayDevice
```

```
compute.instances.updateSecurity

compute.instances.updateShieldedInstanceConfig

compute.instances.updateShieldedVmConfig

compute.machineTypes.get

compute.machineTypes.list

compute.networks.list

compute.networks.updatePolicy

compute.nodeGroups.list

compute.nodeTemplates.get

compute.projects.get

compute.regions.list

compute.snapshots.create

compute.snapshots.delete

compute.snapshots.list

compute.snapshots.get

compute.snapshots.setLabels

compute.snapshots.useReadOnly

compute.subnetworks.get

compute.subnetworks.list

compute.subnetworks.use

compute.subnetworks.useExternalIp

compute.zoneOperations.get
```

```
compute.zoneOperations.list

compute.zones.get

compute.zones.list

resourcemanager.projects.get

storage.buckets.create

storage.buckets.delete

storage.buckets.get

storage.buckets.list

storage.buckets.update

storage.objects.create

storage.objects.delete

storage.objects.get

storage.objects.list

cloudkms.cryptoKeys.get

cloudkms.cryptoKeys.list

cloudkms.keyRings.get

cloudkms.keyRings.list

compute.disks.list

compute.instances.setServiceAccount

compute.networks.get

compute.networks.use

compute.networks.useExternalIp
```

```
iam.serviceAccounts.actAs

compute.resourcePolicies.use
```

次のステップ

- 初期展開プロセス中の場合は、「マシンカタログの作成」を参照してください。
- Google Cloud Platform (GCP)固有の情報については、Google Cloud Platformカタログの作成を参照してください。

詳細情報

- 接続とリソース
- マシンカタログの作成

HPE Moonshotへの接続

接続とリソースの作成および管理では、接続を作成するウィザードについて説明します。以下の情報は、HPE Moonshotに固有の詳細を扱います。

> **注:**
>
> HPE Moonshotへの接続を作成する前に、まずHPEアカウントの設定を完了する必要があります。HPE Moonshot仮想化環境を参照してください。

接続を作成する

HPE Moonshotへの接続は、以下を使用して作成できます。

- ウェブスタジオ
- PowerShellコマンド

Web Studioを使用して接続を作成する

1. **接続とリソースの追加**ページで、接続の種類として**HPE Moonshot**を選択します。
2. Moonshot iLO Chassis Managerの接続アドレスを入力します。アドレスには、IPアドレス、ホスト名、またはFQDNを使用できます。
3. シャーシの管理資格情報と、わかりやすい接続名を入力します。

接続設定は、次のいずれかの状況で停止します。

- Citrix Virtual Apps and Desktops™がエラーのある公開CA署名付き証明書を受信した場合：エラーメッセージが表示されます。画面の指示に従って問題を修正してください。修正しないと、接続の作成に進むことはできません。
- Citrix Virtual Apps and DesktopsがプライベートCA署名付き証明書を受信した場合。警告ページが表示されます。受信したサムプリントをサーバーのサムプリントと比較して、証明書の有効性を確認します。有効な場合は、**証明書を信頼する**を選択し、**OK**をクリックして接続の作成に進みます。Citrix Virtual Apps and Desktopsは証明書を信頼し、将来の検証のためにサムプリントを保存します。

PowerShellコマンドを使用して接続を作成する

PowerShellコマンドを使用して接続を作成する場合、次の情報を提供します。

- IP: HPEサーバーのIPアドレス
- ユーザー名: HPEユーザー名
- パスワード: HPEパスワード

例:

```
New-Item -ConnectionType "Custom" -HypervisorAddress $IP -Metadata
@{"Citrix_Orchestration_Hypervisor_Secret_Allow_Edit"="false"} -Path
@("XDHyp:\Connections\$connectionName") -Persist -PluginId
"HPMoonshotFactory" -Scope @() -SecurePassword $Password -UserName
$UserName -sslthumbprint $SslThumbprint New-BrokerHypervisorConnection
-HypHypervisorConnectionUid $HypervisorConnectionID
```

> **注：**
>
> `sslthumbprint`パラメーターは、プライベートCA署名付き証明書の場合にのみ必要です。

証明書とサムプリントの検証

HPE Moonshot への接続を正常に作成するには、証明書にエラーがなく、サムプリントが正しい値である必要があります。証明書とサムプリントの検証に関連するユースケースは次のとおりです。

- 公開CA署名証明書にエラーがあります。接続は正常に作成されません。エラーの詳細を確認し、問題を解決してください。
- エラーのない公開CA署名証明書。接続は正常に作成され、`SslThumbprints`の値は**Null**です。
- エラーがなく、`sslthumbprint`値を持つプライベートCA署名証明書。正しい`SslThumbprints`値で接続が正常に作成されます。
- サムプリント値が正しくないプライベートCA署名証明書。接続は正常に作成されません。
- エラーのないプライベートCA署名証明書。接続は正常に作成されます。接続作成時、`SSlThumbprints`は**Null**です。`SSlThumbprints`値はサイトサービスによって値に更新されます。

接続の管理

このセクションでは、接続を管理する方法について詳しく説明します。

- Web Studioを使用して証明書の問題を修正する
- PowerShellコマンドを使用してサムプリント値を更新する

証明書の問題を修正する

証明書の問題が発生すると、Citrix Virtual Apps and DesktopsはHPE Moonshot接続をブロックし、関連するHPE Moonshotノードでのワークロードの配信と管理を妨げます。**ホスト接続**リストの接続の横にエラーアイコンが表示されます。特定の問題と解決策については、次の表を参照してください。

問題	解決策
公開CA署名証明書に証明書エラーが発生する	接続をクリックし、**トラブルシューティング**タブを選択します。エラーの詳細を表示し、問題を解決します。
受信した証明書はプライベートCA署名済みであるか、期限切れです。	証明書のサムプリントを更新するには、ホスト接続を編集します。詳細な手順： 1. 接続を選択し、**接続の編集**をクリックします。

問題	解決策	
	2. **接続プロパティ**ページで、**設定の編集**をクリックします。 3. HPE Moonshotシャーシに接続するためのパスワードを入力し、**保存**をクリックします。 4. 表示される**警告**ページで、受信したサムプリントをサーバーのものと比較して、証明書の有効性を確認します。 5. 同じである場合は、**証明書を信頼する**を選択し、**OK**をクリックします。	

サムプリント値を更新する

接続を作成した後、`Set-Item` PowerShellコマンドを使用して接続のサムプリント値を更新できます。たとえば、次のコマンドを実行します。

1. 接続の接続詳細を取得します。例：

```
Get-Item -LiteralPath xdhyp:\connections\SinMoonshot-101
```

2. サムプリント値を更新します。例:

```
Set-Item -LiteralPath xdhyp:\connections\SinMoonshot-101 -Username
Administrator -SslThumbprint xxxxxxxxxxx12AD048480631BB7AB10D69xxxxx
```

3. 更新されたサムプリント値を確認します。例:

```
Get-Item -LiteralPath xdhyp:\connections\SinMoonshot-101
```

注:

`Set-Item` コマンドで誤ったサムプリント値を指定すると、更新は失敗します。

次のステップ

- 初期展開プロセス中の場合は、「マシンカタログの作成」を参照してください。
- AWS固有の情報については、「HPE Moonshotマシンカタログの作成」を参照してください。

詳細情報

- 接続とリソース
- マシンカタログの作成

Microsoft Azure への接続

注：

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

(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/install-configure/connections.html)では、接続を作成するウィザードについて説明します。以下の情報は、Azure Resource Managerクラウド環境に固有の詳細を扱います。

注：

Microsoft Azure への接続を作成する前に、リソースの場所として Azure アカウントの設定を完了する必要があります。「Microsoft Azure Resource Manager クラウド環境」を参照してください。

サービスプリンシパルと接続の作成

接続を作成する前に、接続がAzureリソースにアクセスするために使用するサービスプリンシパルを設定する必要があります。接続は2つの方法で作成できます。

- Web Studio を使用してサービスプリンシパルと接続を同時に作成する
- 以前に作成したサービスプリンシパルを使用して接続を作成する

このセクションでは、次のタスクを完了する方法を示します。

- Web Studio を使用してサービスプリンシパルと接続を作成する
- (/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/install-configure/connections/connection-azure-resource-manager.html#create-a-service-principal-using-powershell)
- (/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/install-configure/connections/connection-azure-resource-manager.html#get-the-application-secret-in-azure)
- 既存のサービスプリンシパルを使用して接続を作成する](/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/install-configure/connections/connection-azure-resource-manager.html#create-a-connection-using-an-existing-service-principal)

考慮事項

- Citrix® は、共同作成者ロールを持つサービスプリンシパルの使用を推奨しています。ただし、最小限の権限のリストについては、「最小限の権限」セクションを参照してください。
- 最初の接続を作成するとき、Azure は必要な権限を付与するよう求めます。今後の接続では、引き続き認証が必要ですが、Azure は以前の同意を記憶しており、プロンプトを再度表示することはありません。
- 認証に使用されるアカウントは、Azure RBAC を使用してサブスクリプション内でロールを割り当てる権限を持っている必要があります。例として、サブスクリプションの所有者、ロールベースのアクセス制御管理者、またはユーザーアクセス管理者などです。
- 認証に使用されるアカウントは、サブスクリプションのディレクトリのメンバーである必要があります。注意すべきアカウントの種類は、「職場または学校」と「個人用 Microsoft アカウント」の2種類です。詳細については、CTX219211 を参照してください。
- 既存の Microsoft アカウントをサブスクリプションのディレクトリのメンバーとして追加して使用することはできますが、ユーザーが以前にディレクトリのリソースのいずれかへのゲストアクセスを許可されていた場合、問題が発生する可能性があります。この場合、ディレクトリ内に必要な権限を付与しないプレースホルダーエントリが存在し、エラーが返される可能性があります。

  ディレクトリからリソースを削除し、明示的に追加し直すことで、これを修正します。ただし、このオプションは、アカウントがアクセスできる他のリソースに意図しない影響を与える可能性があるため、慎重に実行してください。

- 特定のアカウントが実際にはメンバーであるにもかかわらず、ディレクトリゲストとして検出される既知の問題があります。このような構成は、通常、古くから確立されたディレクトリアカウントで発生します。回避策: ディレクトリにアカウントを追加し、適切なメンバーシップ値を取得します。
- リソースグループは単にリソースのコンテナであり、自身のリージョン以外のリージョンからのリソースを含むことができます。これは、リソースグループのリージョンに表示されるリソースが利用可能であると期待している場合、混乱を招く可能性があります。
- 必要な数のマシンをホストするのに十分な大きさのネットワークとサブネットがあることを確認してください。これにはある程度の先見性が必要ですが、Microsoft はアドレス空間の容量に関するガイダンスを提供し、適切な値を指定するのに役立ちます。

Web Studio を使用してサービスプリンシパルと接続を作成する

> **重要:**
>
> この機能は、Azure China サブスクリプションではまだ利用できません。

> Web Studio を使用すると、単一のワークフローでサービスプリンシパルと接続の両方を作成できます。サービスプリンシパルは、接続に Azure リソースへのアクセスを許可します。サービスプリンシパルを作成するために Azure に認証すると、アプリケーションが Azure に登録されます。登録されたアプリケーションには、秘密鍵 (クライアントシークレットまたはアプリケーションシークレットと呼ばれます) が作成されます。登録されたアプリケーション (この場合は接続) は、クライアントシークレットを使用して Azure AD に認証します。

開始する前に、以下の前提条件を満たしていることを確認してください。

- サブスクリプションの Azure Active Directory テナントにユーザーアカウントがあること。
- 認証に使用されるアカウントは、Azure RBAC を使用してサブスクリプション内でロールを割り当てる権限を持っている必要があります。例として、サブスクリプションの所有者、ロールベースのアクセス制御管理者、またはユーザーアクセス管理者などです。
- 認証のためのグローバル管理者、アプリケーション管理者、またはアプリケーション開発者の権限があること。これらの権限は、ホスト接続の作成後に取り消すことができます。ロールの詳細については、「Azure AD の組み込みロール」を参照してください。

接続とリソースの追加ウィザードを使用して、サービスプリンシパルと接続を一緒に作成します。

1. **接続**ページで、**新しい接続の作成**、**Microsoft Azure**接続タイプ、およびAzure環境を選択します。
2. 仮想マシンを作成するために使用するツールを選択し、**次へ**を選択します。
3. ページで、Azure サブスクリプション ID と接続の名前を入力します。サブスクリプション ID を入力すると、 ボタンが有効になります。

   > **注：**
   >
   > 接続名には 1～64 文字を含めることができ、空白のみ、または文字 `\/;:#.*?=<>|[]{}"'()'` を含めることはできません。

4. を選択し、Azure Active Directory アカウントのユーザー名とパスワードを入力します。
5. **サインイン**を選択します。
6. 「**Accept**」を選択して、Citrix Virtual Apps and Desktops™ に一覧表示された権限を付与します。Citrix Virtual Apps and Desktops は、指定されたユーザーに代わって Azure リソースを管理できるようにするサービスプリンシパルを作成します。
7. 「**Accept**」を選択すると、ウィザードの「**Connection**」ページに戻ります。

   > **注：**
   >
   > Azure への認証が正常に完了すると、「**Create new**」ボタンと「**Use existing**」ボタンが消えます。「**Connection successful**」というテキストが緑色のチェックマークとともに表示され、Azure サブスクリプションへの接続が成功したことを示します。

8. 「**Connection Details**」ページで、「**Next**」を選択します。

   > **注：**
   >
   > Azure への認証が正常に完了し、必要な権限の付与に同意するまで、次のページに進むことはできません。

9. 接続のリソースを構成します。リソースには、リージョンとネットワークが含まれます。
   - 「**地域**」ページで、地域を選択します。

- 「**ネットワーク**」ページで、次の操作を行います。
  - リージョンとネットワークの組み合わせを識別しやすくするために、1〜64文字のリソース名を入力します。リソース名には、空白のみを含めることや、文字 `\/;:#.*?=<>|[]{}"'()'` を含めることはできません。
  - 仮想ネットワーク/リソースグループのペアを選択します。（同じ名前の仮想ネットワークが複数ある場合、ネットワーク名とリソースグループをペアにすることで、一意の組み合わせが提供されます。）前のページで選択した地域に仮想ネットワークがない場合は、そのページに戻り、仮想ネットワークがある地域を選択してください。

10. 「**概要**」ページで、設定の概要を確認し、「**完了**」を選択してセットアップを完了します。

アプリケーションIDを表示する

接続を作成した後、その接続がAzureリソースへのアクセスに使用するアプリケーションIDを表示できます。

「**Add Connection and Resources**」リストで、接続を選択して詳細を表示します。「**Details**」タブにはアプリケーションIDが表示されます。

PowerShellを使用してサービスプリンシパルを作成する

PowerShellを使用してサービスプリンシパルを作成するには、Azure Resource Managerサブスクリプションに接続し、以下のセクションで提供されているPowerShellコマンドレットを使用します。

次の項目を準備してください。

- **SubscriptionId:** VDAをプロビジョニングするサブスクリプションのAzure Resource Manager `SubscriptionID`。
- 「**ActiveDirectoryID**」: Azure AD に登録したアプリケーションのテナントID。
- 「**ApplicationName**」: Azure AD で作成するアプリケーションの名前。

詳細な手順は次のとおりです。

Azure Resource Manager サブスクリプションに接続します。

```
`Connect-AzAccount`
```

1. サービスプリンシパルを作成する Azure Resource Manager サブスクリプションを選択します。

   `Get-AzSubscription -SubscriptionId $subscriptionId | Select-AzSubscription`

2. AD テナントにアプリケーションを作成します。

   ```
   $AzureADApplication = New-AzADApplication -DisplayName $ApplicationName
   ```

3. サービスプリンシパルを作成します。

   ```
   New-AzADServicePrincipal -ApplicationId $AzureADApplication.AppId
   ```

4. サービスプリンシパルにロールを割り当てます。

   ```
   New-AzRoleAssignment -RoleDefinitionName Contributor -ServicePrincipalName $AzureADApplication.AppId –scope /subscriptions/$SubscriptionId
   ```

5. PowerShell コンソールの出力ウィンドウから ApplicationId をメモします。ホスト接続を作成する際に、その ID を指定します。

Azure でアプリケーションシークレットを取得する

既存のサービスプリンシパルを使用して接続を作成するには、まず Azure portal でサービスプリンシパルのアプリケーションIDとシークレットを取得する必要があります。

詳細な手順は次のとおりです。

1. Web Studio から、または PowerShell を使用して「**Application ID**」を取得します。
2. Azureポータルにサインインします。
3. Azure で、「**Azure Active Directory**」を選択します。
4. Azure AD の「**App registrations**」から、アプリケーションを選択します。
5. **証明書とシークレット**に移動します。
6. **クライアントシークレット**をクリックします。

既存のサービスプリンシパルを使用して接続を作成する

サービスプリンシパルが既にある場合は、それを使用して Web Studio で接続を作成できます。

次の項目を準備してください。

- SubscriptionId
- ActiveDirectoryID (テナントID)
- アプリケーションID
- アプリケーションシークレット

  詳細については、「アプリケーションシークレットの取得」を参照してください。
- シークレットの有効期限

詳細な手順は次のとおりです。

接続とリソースの追加ウィザードで、次の手順を実行します。

1. **接続**ページで、**新しい接続の作成**、**Microsoft Azure**接続タイプ、およびAzure環境を選択します。
2. 仮想マシンを作成するために使用するツールを選択し、**次へ**を選択します。
3. 「**接続の詳細**」ページで、Azure サブスクリプション ID と接続の名前を入力します。

   > **注：**
   >
   > 接続名には 1～64 文字を含めることができ、空白のみ、または文字 `\/;:#.*?=<>|[]{}"'()'` を含めることはできません。

4. **既存を使用**を選択します。**既存のサービスプリンシパルの詳細**ウィンドウで、既存のサービスプリンシパルに対して次の設定を入力します。詳細を入力すると、**保存**ボタンが有効になります。**保存**を選択します。有効な詳細情報を提供するまで、このページから先に進むことはできません。

   - **サブスクリプションID**。AzureサブスクリプションIDを入力します。サブスクリプションIDを取得するには、Azureポータルにサインインし、**サブスクリプション > 概要**に移動します。
   - **Active Directory ID** (テナント ID)。Azure AD に登録したアプリケーションのディレクトリ (テナント) ID を入力します。
   - **アプリケーション ID**。Azure AD に登録したアプリケーションのアプリケーション (クライアント) ID を入力します。
   - **アプリケーションシークレット**。シークレットキー (クライアントシークレット) を作成します。登録済みアプリケーションは、このキーを使用して Azure AD に対して認証を行います。セキュリティ上の理由から、キーを定期的に変更することをお勧めします。キーは後で取得できないため、必ず保存してください。
   - **シークレットの有効期限**。アプリケーションシークレットの有効期限が切れる日付を入力します。シークレットキーの有効期限が切れる 14 日前から、「**ホスティング**」ノードの特定のホスト接続に警告アイコンが表示されます。ただし、シークレットキーの有効期限が切れると、エラーが発生します。

     > **注：**

> セキュリティ上の理由から、有効期限は現在から2年を超えることはできません。

- **認証 URL**。このフィールドは自動的に入力され、編集できません。
- **管理 URL**。このフィールドは自動的に入力され、編集できません。
- **ストレージサフィックス**。このフィールドは自動的に入力され、編集できません。

  AzureでMCSカタログを作成するには、以下のエンドポイントへのアクセスが必要です。これらのエンドポイントへのアクセスにより、ネットワークとAzureポータルおよびそのサービス間の接続が最適化されます。

  - 認証URL: `<https://login.microsoftonline.com/>`
  - 管理URL: `<https://management.azure.com/>`。これはAzure Resource Managerプロバイダー APIのリクエストURLです。管理のエンドポイントは環境によって異なります。たとえば、Azure Globalの場合は`<https://management.azure.com/>`、Azure US Governmentの場合は`<https://management.usgovcloudapi.net/>`です。
  - ストレージサフィックス: `<https://*.core.windows.net./>`。これはストレージサフィックスのワイルドカード文字(*)です。例: `https://demo.table.core.windows.net/`。

5. **保存**を選択すると、「**接続の詳細**」ページに戻ります。「**次へ**」を選択して次のページに進みます。
6. 接続のリソースを構成します。リソースは、リージョンとネットワークで構成されます。
   - 「**地域**」ページで、地域を選択します。
   - 「**ネットワーク**」ページで、次の操作を行います。
     - リージョンとネットワークの組み合わせを識別しやすくするために、1〜64 文字のリソース名を入力します。リソース名には空白のみ、または文字 `\/;:#.*?=<>|[]{}"'()'` を含めることはできません。
     - 仮想ネットワーク/リソースグループのペアを選択します。（同じ名前の仮想ネットワークが複数ある場合、ネットワーク名とリソースグループをペアにすることで、一意の組み合わせが提供されます。）前のページで選択した地域に仮想ネットワークがない場合は、そのページに戻り、仮想ネットワークがある地域を選択してください。
7. 「**概要**」ページで、設定の概要を確認し、「**完了**」を選択してセットアップを完了します。

サービスプリンシパルと接続を管理する

このセクションでは、サービスプリンシパルと接続を管理する方法について詳しく説明します。

- Azureスロットル設定を構成する
- Azureでイメージ共有を有効にする
- Web Studio を使用して共有テナントを接続に追加する
- PowerShellを使用してイメージ共有を実装する
- アプリケーションシークレットとシークレットの有効期限を管理する

Azure スロットリング設定の構成

Azure Resource Manager は、サブスクリプションとテナントに対する要求を調整し、プロバイダーの特定のニーズに合わせて定義された制限に基づいてトラフィックをルーティングします。詳細については、Microsoft サイトのResource Manager 要求のスロットリングを参照してください。サブスクリプションとテナントには制限があり、多数のマシンを管理すると問題が発生する可能性があります。たとえば、多数のマシンを含むサブスクリプションでは、電源操作に関連するパフォーマンスの問題が発生する可能性があります。

> **ヒント:**
>
> 詳細については、「Machine Creation Services を使用した Azure パフォーマンスの向上」を参照してください。
>
> これらの問題を軽減するために、MCS の内部スロットリングを削除して、Azure から利用可能な要求クォータをより多く使用できます。

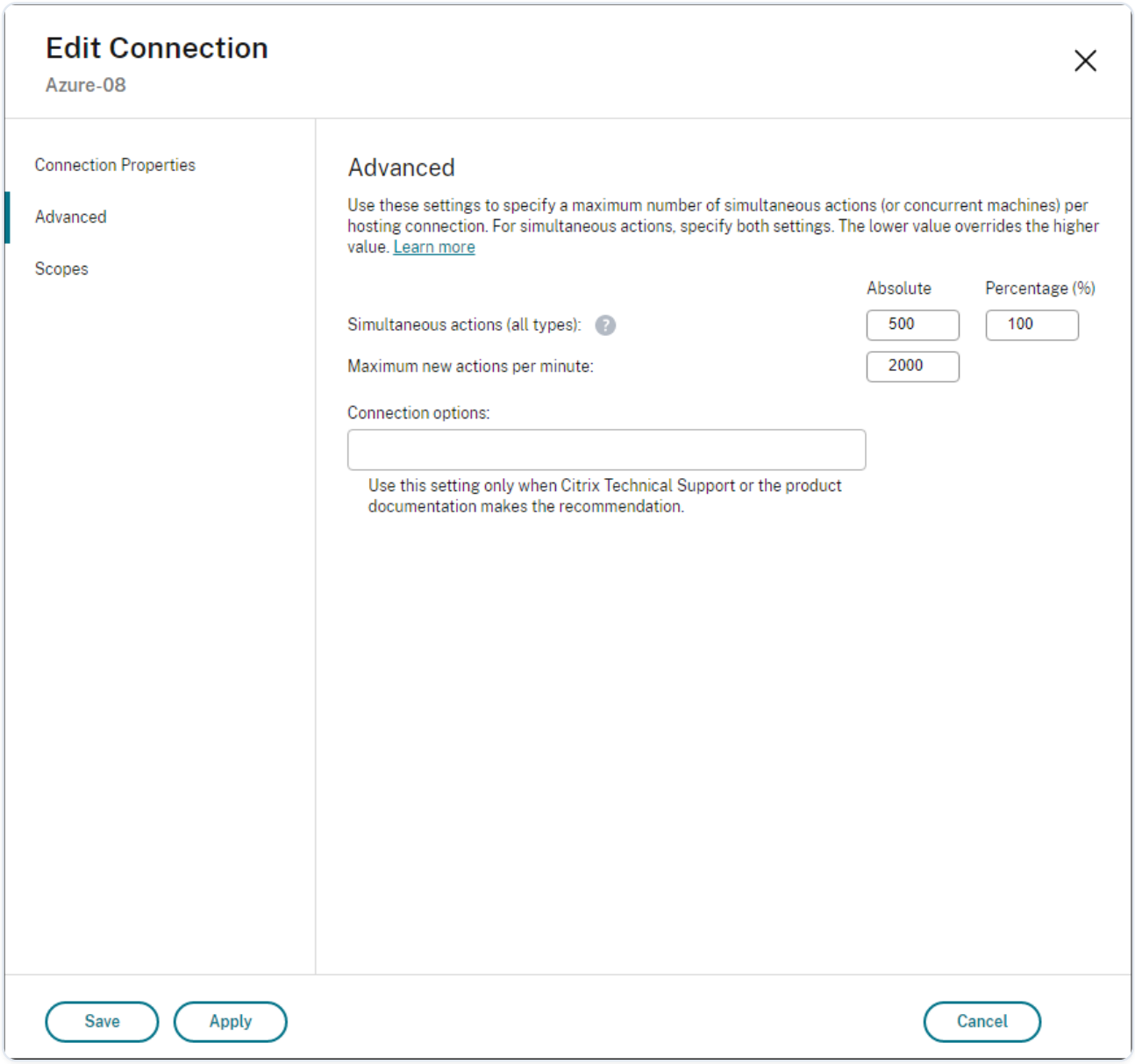
たとえば、1,000 台の VM を含む大規模なサブスクリプションで VM の電源をオンまたはオフにする場合は、次の最適な設定をお勧めします。

- 絶対同時操作数: 500
- 1 分あたりの最大新規操作数: 2000
- 操作の最大同時実行数: 500

Web Studio を使用して、特定の Azure 接続の Azure 操作を構成します。

1. Web Studio で、左側のペインの を選択します。
2. 接続を選択します。

3. ウィザードで、 を選択します。
4. ページで、構成オプションを使用して、同時アクションの数、1 分あたりの最大新規アクション数、および追加の接続オプションを指定します。



MCS はデフォルトで最大 500 の同時操作をサポートします。または、Remote PowerShell SDK を使用して、同時操作の最大数を設定することもできます。

PowerShell プロパティ `MaximumConcurrentProvisioningOperations` を使用して、Azure プロビジョニングの同時操作の最大数を指定します。このプロパティを使用する際は、以下を考慮してください。

- `MaximumConcurrentProvisioningOperations` のデフォルト値は 500 です。
- PowerShell コマンド `Set-item` を使用して、`MaximumConcurrentProvisioningOperations` パラメーターを構成します。

Azure でのイメージ共有を有効にする

マシンカタログを作成または更新する際、異なるAzureテナントおよびサブスクリプション（Azure Compute Galleryを介して共有）から共有イメージを選択できます。テナント内またはテナント間でイメージ共有を有効にするには、Azureで必要な設定を行う必要があります。

- テナント内でのイメージ共有（サブスクリプション間）
- テナント間でのイメージ共有

テナント内でのイメージ共有（サブスクリプション間）

別のサブスクリプションに属するAzure Compute Galleryのイメージを選択するには、そのサブスクリプションのサービスプリンシパル (SPN) とイメージを共有する必要があります。

たとえば、Studioで次のように構成されているサービスプリンシパル (SPN 1) がある場合：

サービスプリンシパル: SPN 1

サブスクリプション: subscription 1

テナント: tenant 1

イメージは別のサブスクリプションにあり、Studio では次のように構成されています。

サブスクリプション: subscription 2

テナント: tenant 1

subscription 2のイメージをsubscription 1 (SPN 1) と共有したい場合は、subscription 2に移動し、リソースグループをSPN1と共有します。

イメージは、Azure ロールベースのアクセス制御 (RBAC) を使用して別の SPN と共有する必要があります。Azure RBAC は、Azure リソースへのアクセスを管理するために使用される承認システムです。Azure RBAC の詳細については、Microsoft ドキュメント Azure ロールベースのアクセス制御 (Azure RBAC) とは を参照してください。アクセスを許可するには、リソースグループスコープでサービスプリンシパルに共同作成者ロールを割り当てます。Azure ロールを割り当てるには、ユーザーアクセス管理者や所有者などの `Microsoft.Authorization/roleAssignments/write` 権限が必要です。別の SPN とイメージを共有する方法の詳細については、Microsoft ドキュメント Azure portal を使用して Azure ロールを割り当てる を参照してください。

PowerShell コマンドを使用して別のサブスクリプションからイメージを選択する方法については、「」(#select-an-image-from-a-different-subscription) を参照してください。

テナント間で画像を共有する

Azure Compute Gallery を使用してテナント間でイメージを共有するには、アプリケーション登録を作成します。

たとえば、2つのテナント (テナント1とテナント2) があり、テナント1とイメージギャラリーを共有したい場合は、次の手順を実行します。

1. テナント1のアプリケーション登録を作成します。詳細については、「アプリ登録の作成」を参照してください。
2. ブラウザを使用してサインインを要求することで、テナント2にアプリケーションへのアクセスを許可します。`Tenant2 ID` をテナント1のテナントIDに置き換えます。`Application (client) ID` を作成したアプリケーション登録のアプリケーションIDに置き換えます。置換が完了したら、URLをブラウザに貼り付け、サインインプロンプトに従ってテナント2にサインインします。例:

   ```
   https://login.microsoftonline.com/<Tenant 2 ID>/oauth2/authorize?
   client_id=<Application (client)
   ID>&response_type=code&redirect_uri=https%3A%2F%2Fwww.microsoft.com%2F
   ```

   詳細については、「テナント2へのアクセス許可」を参照してください。
3. アプリケーションに Tenant 2 リソースグループへのアクセス権を付与します。Tenant 2 としてサインインし、ギャラリーイメージを持つリソースグループにアプリケーション登録アクセス権を付与します。詳細については、テナント間の要求を認証する を参照してください。

PowerShell コマンドを使用して別のテナントのイメージからカタログを作成するには:

1. 「」(#update-hosting-connection-custom-properties-with-shared-tenant-ids)。
2. 「」(#select-an-image-from-a-different-tenant)。

Web Studio を使用して共有テナントを接続に追加する

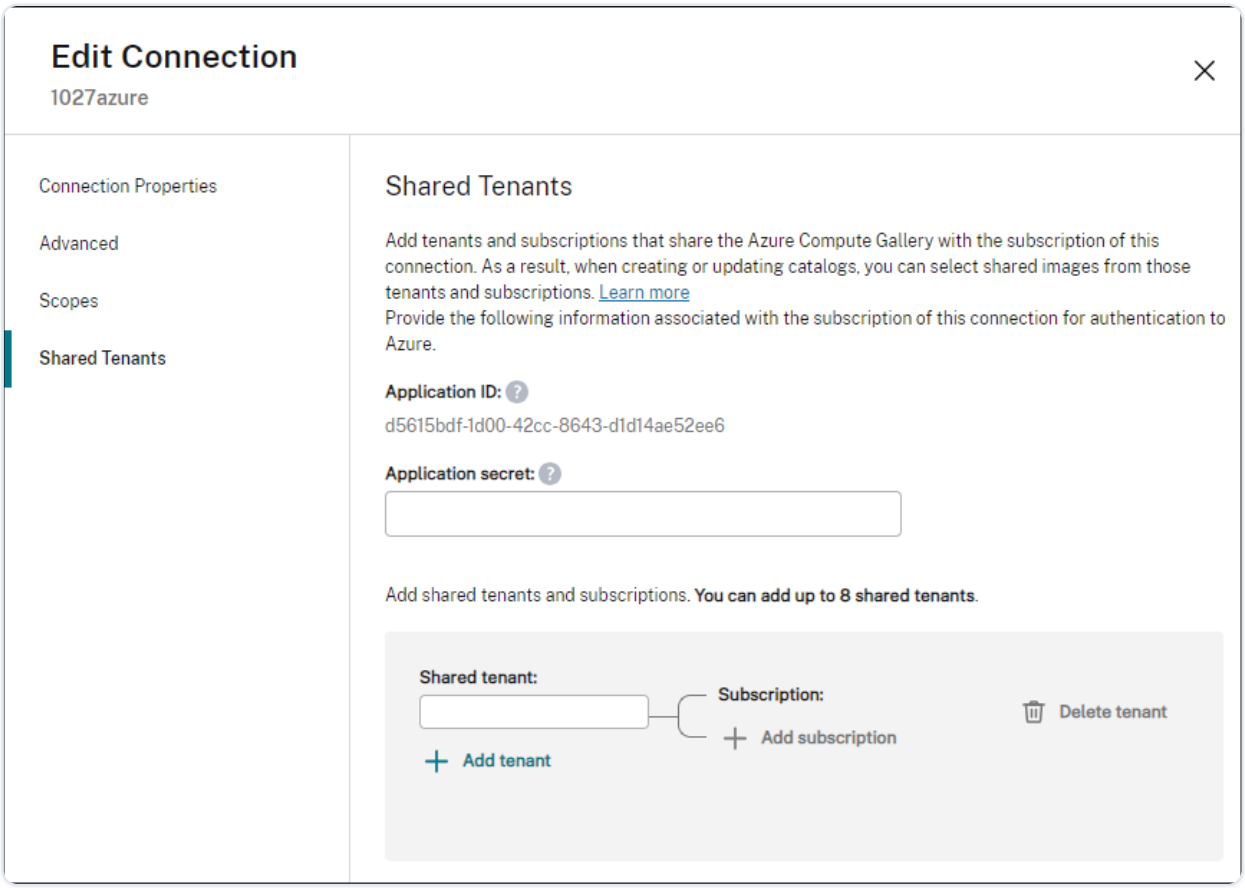
Web Studio でマシンカタログを作成または更新する際、異なる Azure テナントおよびサブスクリプション (Azure Compute Gallery を介して共有) から共有イメージを選択できます。この機能では、関連するホスト接続の共有テナントおよびサブスクリプション情報を提供する必要があります。

> **注：**

テナント間でイメージ共有を有効にするために、Azure で必要な設定が構成されていることを確認してください。詳細については、「テナント間で画像を共有する」を参照してください。

接続に対して次の手順を実行します。

1. Web Studio で、左側のペインの を選択します。
2. 接続を選択し、アクションバーで**接続の編集**を選択します。



3. 「**共有テナント**」で、以下を実行します。
   - 接続のサブスクリプションに関連付けられているアプリケーション ID とアプリケーションシークレットを指定します。Citrix Virtual Apps and Desktops は、この情報を使用して Azure AD に対して認証を行います。
   - 接続のサブスクリプションと Azure Compute Gallery を共有するテナントとサブスクリプションを追加します。テナントごとに最大8つの共有テナントと8つのサブスクリプションを追加できます。
4. 完了したら、**適用**を選択して行った変更を適用し、ウィンドウを開いたままにするか、**OK**を選択して変更を適用し、ウィンドウを閉じます。

PowerShellを使用したイメージ共有の実装

このセクションでは、PowerShellを使用してイメージを共有するプロセスについて説明します。

- 別のサブスクリプションからイメージを選択する
- 共有テナントIDでホスティング接続のカスタムプロパティを更新する
- 別のテナントからイメージを選択する

別のサブスクリプションからイメージを選択する

同じAzureテナント内の別の共有サブスクリプションに属するAzure Compute Galleryのイメージを選択して、PowerShellコマンドを使用してMCSカタログを作成および更新できます。

1. ホスティングユニットのルートフォルダーに、Citrixは`sharedsubscription`という新しい共有サブスクリプションフォルダーを作成します。
2. テナント内のすべての共有サブスクリプションを一覧表示します。

```
Get-ChildItem -Path "XDhyp:
\HostingUnits\azres\sharedsubscription.folder"
```

3. 1つの共有サブスクリプションを選択し、その共有サブスクリプションのすべての共有リソースグループを一覧表示します。

```
Get-ChildItem -Path "XDhyp:
\HostingUnits\azres\image.folder\abc123.sharedsubscription"
```

4. リソースグループを選択し、そのリソースグループのすべてのギャラリーを一覧表示します。

```
Get-ChildItem -Path "XDhyp:
\HostingUnits\azres\image.folder\abc123.sharedsubscription\
xyz.resourcegroup"
```

5. ギャラリーを選択し、そのギャラリーのすべてのイメージ定義を一覧表示します。

```
Get-ChildItem -Path "XDhyp:
\HostingUnits\azres\image.folder\abc123.sharedsubscription\xyz.resource
group\testgallery.gallery"
```

6. 1つのイメージ定義を選択し、そのイメージ定義のすべてのイメージバージョンを一覧表示します。

```
Get-ChildItem -Path "XDhyp:
\HostingUnits\azres\image.folder\abc123.sharedsubscription\xyz.resource
group\sigtestdef.imagedefinition"
```

7. 次の要素を使用してMCSカタログを作成および更新します。

   - リソースグループ
   - ギャラリー
   - ギャラリーイメージ定義
   - ギャラリーイメージバージョン

   Remote PowerShell SDK を使用したカタログの作成方法については、`<https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/>` を参照してください。

共有テナントIDでホスティング接続のカスタムプロパティを更新する

`Set-Item` を使用して、共有テナントIDとサブスクリプションIDでホスティング接続のカスタムプロパティを更新します。`CustomProperties` にプロパティ `SharedTenants` を追加します。`Shared Tenants` の形式は次のとおりです。

```
[{"Tenant":"94367291-119e-457c-bc10-25337231f7bd","Subscriptions":
["7bb42f40-8d7f-4230-a920-be2781f6d5d9"]},{"Tenant":"50e83564-c4e5-4209-
b43d-815c45659564","Subscriptions":["06ab8944-6a88-47ee-
a975-43dd491a37d0"]}]
```

例:

```
Set-Item -CustomProperties "<CustomProperties xmlns=`"http://
schemas.citrix.com/2014/xd/machinecreation`" xmlns:xsi=`"http://
www.w3.org/2001/XMLSchema-instance`">

<Property xsi:type=`"StringProperty`" Name=`"SubscriptionId`"
Value=`"123`" />

<Property xsi:type=`"StringProperty`" Name=`"ManagementEndpoint`"
Value=`"https://management.azure.com/`" />

<Property xsi:type=`"StringProperty`" Name=`"AuthenticationAuthority`"
Value=`"https://login.microsoftonline.com/`" />
```

```
<Property xsi:type=`"StringProperty`" Name=`"StorageSuffix`"
Value=`"core.windows.net`" />

<Property xsi:type=`"StringProperty`" Name=`"TenantId`" Value=`"123abc`" /
>

<Property xsi:type=`"StringProperty`" Name=`"SharedTenants`"
Value=`"`[ { 'Tenant':'123abc', 'Subscriptions':['345', '567'] } ]`"` />

</CustomProperties>"

-LiteralPath @("XDHyp:\Connections\aazure") -PassThru -UserName "advc345"
-SecurePassword

$psd
```

注：

複数のテナントを追加できます。各テナントは複数のサブスクリプションを持つことができます。

別のテナントからイメージを選択する

PowerShellコマンドを使用してMCSカタログを作成および更新するために、別のAzureテナントに属するAzure Compute Galleryのイメージを選択できます。

1. ホスティングユニットのルートフォルダーに、Citrixは`sharedsubscription`という新しい共有サブスクリプションフォルダーを作成します。
2. すべての共有サブスクリプションを一覧表示します。

   ```
   Get-ChildItem XDHyp:\HostingUnits\azres\sharedsubscription.folder
   ```

3. 1つの共有サブスクリプションを選択し、その共有サブスクリプションのすべての共有リソースグループを一覧表示します。

   ```
   Get-ChildItem XDHyp:
   \HostingUnits\azres\image.folder\abc123.sharedsubscription
   ```

4. リソースグループを選択し、そのリソースグループのすべてのギャラリーを一覧表示します。

```
Get-ChildItem XDHyp:
\HostingUnits\azres\image.folder\abc123.sharedsubscription\
xyz.resourcegroup
```

5. ギャラリーを選択し、そのギャラリーのすべてのイメージ定義を一覧表示します。

```
Get-ChildItem XDHyp:
\HostingUnits\azres\image.folder\abc123.sharedsubscription\xyz.resource
group\efg.gallery
```

6. 1つのイメージ定義を選択し、そのイメージ定義のすべてのイメージバージョンを一覧表示します。

```
Get-ChildItem XDHyp:
\HostingUnits\azres\image.folder\abc123.sharedsubscription\xyz.resource
group\efg.gallery\hij.imagedefinition
```

7. 次の要素を使用してMCSカタログを作成および更新します。

   - リソースグループ
   - ギャラリー
   - ギャラリーイメージ定義
   - ギャラリーイメージバージョン

   Remote PowerShell SDK を使用したカタログの作成方法については、`<https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/>` を参照してください。

アプリケーションシークレットとシークレットの有効期限を管理する

シークレットの有効期限が切れる前に、接続のアプリケーションシークレットを必ず変更してください。シークレットキーの有効期限が切れる14日前から、**Hosting** ノードの特定のホスト接続に警告アイコンが表示されます。ただし、シークレットキーの有効期限が切れると、エラーが発生します。

AZURE でアプリケーションシークレットを作成する

Azure portal を介して、接続のアプリケーションシークレットを作成できます。

1. **Azure Active Directory** を選択します。
2. Azure AD の **App registrations** から、アプリケーションを選択します。
3. **証明書とシークレット**に移動します。
4. **>** をクリックします。
5. シークレットの説明を入力し、期間を指定します。完了したら、**Add** を選択します。

> **注：**
>
> クライアントシークレットは後で取得できないため、必ず保存してください。

6. クライアントシークレットの値と有効期限をコピーします。
7. Web Studio で、対応する接続を編集し、**Application secret** および **Secret expiration date** フィールドの内容をコピーした値に置き換えます。

シークレットの有効期限を変更する

Web Studio を使用して、使用中のアプリケーションシークレットの有効期限を追加または変更できます。

> **注：**
>
> シークレットキーの有効期限が切れる14日前から、**Hosting** ノードの特定のホスト接続に警告アイコンが表示されます。

1. **接続とリソースの追加**ウィザードで、接続を右クリックし、**接続の編集**をクリックします。
2. **接続プロパティ**ページで、**シークレットの有効期限**をクリックして、使用中のアプリケーションシークレットの有効期限を追加または変更します。

必要なAzure権限

このセクションには、Azure に必要な最小限の一般的な権限が含まれています。

最小限の権限

最小限の権限は、より優れたセキュリティ制御を提供します。ただし、追加の権限を必要とする新機能は、最小限の権限のみを使用しているため失敗します。

ホスト接続の作成

Azure から取得した情報を使用して、新しいホスト接続を追加します。

```
"Microsoft.Network/virtualNetworks/read",

"Microsoft.Compute/virtualMachines/read",

"Microsoft.Compute/disks/read",
```

VM の電源管理

マシンインスタンスの電源をオンまたはオフにします。

```
"Microsoft.Compute/virtualMachines/read",

"Microsoft.Resources/subscriptions/resourceGroups/read",

"Microsoft.Compute/virtualMachines/deallocate/action",

"Microsoft.Compute/virtualMachines/start/action",

"Microsoft.Compute/virtualMachines/restart/action",
```

仮想マシンの作成、更新、または削除

マシンカタログを作成し、マシンを追加、削除、更新し、マシンカタログを削除します。

以下は、マスターイメージがマネージドディスクである場合、またはスナップショットがホスティング接続と同じリージョンにある場合に必要となる最小限の権限のリストです。

```
"Microsoft.Resources/subscriptions/resourceGroups/read",

"Microsoft.Resources/deployments/validate/action",

"Microsoft.Compute/virtualMachines/read",

"Microsoft.Compute/virtualMachines/write",

"Microsoft.Compute/virtualMachines/delete",

"Microsoft.Compute/virtualMachines/deallocate/action",

"Microsoft.Compute/snapshots/read",
```

```
"Microsoft.Compute/snapshots/write",

"Microsoft.Compute/snapshots/delete",

"Microsoft.Compute/snapshots/beginGetAccess/action",

"Microsoft.Compute/snapshots/endGetAccess/action",

"Microsoft.Compute/disks/read",

"Microsoft.Compute/disks/write",

"Microsoft.Compute/disks/delete",

"Microsoft.Compute/disks/beginGetAccess/action",

"Microsoft.Compute/disks/endGetAccess/action",

"Microsoft.Network/virtualNetworks/read",

"Microsoft.Network/virtualNetworks/subnets/join/action",

"Microsoft.Network/virtualNetworks/subnets/read",

"Microsoft.Network/networkSecurityGroups/read",

"Microsoft.Network/networkSecurityGroups/write",

"Microsoft.Network/networkSecurityGroups/delete",

"Microsoft.Network/networkSecurityGroups/join/action",

"Microsoft.Network/networkInterfaces/read",

"Microsoft.Network/networkInterfaces/write",

"Microsoft.Network/networkInterfaces/delete",

"Microsoft.Network/networkInterfaces/join/action",
```

以下の機能については、最小限の権限に加えて、以下の追加権限が必要です。

- マスターイメージがホスティング接続と同じリージョンにあるストレージアカウント内のVHD である場合：

```
"Microsoft.Storage/storageAccounts/read",

"Microsoft.Storage/storageAccounts/listKeys/action",
```

- マスターイメージが共有イメージギャラリーのImageVersionである場合:

```
"Microsoft.Compute/galleries/read",

"Microsoft.Compute/galleries/images/read",

"Microsoft.Compute/galleries/images/versions/read",
```

- マスターイメージがマネージドディスクである場合、スナップショットまたはVHDがホスティング接続のリージョンとは異なるリージョンにある場合:

```
"Microsoft.Storage/storageAccounts/read",

"Microsoft.Storage/storageAccounts/listKeys/action",

"Microsoft.Storage/storageAccounts/write",

"Microsoft.Storage/storageAccounts/delete",
```

- Citrix管理のリソースグループを使用する場合:

```
"Microsoft.Resources/subscriptions/resourceGroups/write",

"Microsoft.Resources/subscriptions/resourceGroups/delete",
```

- マスターイメージを共有イメージギャラリーに配置する場合:

```
"Microsoft.Compute/galleries/write",

"Microsoft.Compute/galleries/images/write",

"Microsoft.Compute/galleries/images/versions/write",
```

```
"Microsoft.Compute/galleries/read",

"Microsoft.Compute/galleries/images/read",

"Microsoft.Compute/galleries/images/versions/read",

"Microsoft.Compute/galleries/delete",

"Microsoft.Compute/galleries/images/delete",

"Microsoft.Compute/galleries/images/versions/delete",
```

- Azure専用ホストサポートを使用する場合:

```
"Microsoft.Compute/hostGroups/read",

"Microsoft.Compute/hostGroups/write",

"Microsoft.Compute/hostGroups/hosts/read",
```

- カスタマーマネージドキー (CMK) を使用してサーバー側暗号化 (SSE) を使用する場合:

```
"Microsoft.Compute/diskEncryptionSets/read",
```

- ARM テンプレート (マシンプロファイル) を使用して VM を展開する場合:

```
"Microsoft.Resources/deployments/write",

"Microsoft.Resources/deployments/operationstatuses/read",

"Microsoft.Resources/deployments/read",

"Microsoft.Resources/deployments/delete",
```

- Azure テンプレート仕様をマシンプロファイルとして使用する場合:

```
"Microsoft.Resources/templateSpecs/read",

"Microsoft.Resources/templateSpecs/versions/read",
```

アンマネージドディスクを使用したマシンの作成、更新、削除

マスターイメージが VHD であり、管理者が提供するリソースグループを使用する場合に必要となる最小限の権限のリストは次のとおりです。

```
"Microsoft.Resources/subscriptions/resourceGroups/read",

"Microsoft.Storage/storageAccounts/delete",

"Microsoft.Storage/storageAccounts/listKeys/action",

"Microsoft.Storage/storageAccounts/read",

"Microsoft.Storage/storageAccounts/write",

"Microsoft.Compute/virtualMachines/deallocate/action",

"Microsoft.Compute/virtualMachines/delete",

"Microsoft.Compute/virtualMachines/read",

"Microsoft.Compute/virtualMachines/write",

"Microsoft.Resources/deployments/validate/action",

"Microsoft.Network/networkInterfaces/delete",

"Microsoft.Network/networkInterfaces/join/action",

"Microsoft.Network/networkInterfaces/read",

"Microsoft.Network/networkInterfaces/write",

"Microsoft.Network/networkSecurityGroups/delete",

"Microsoft.Network/networkSecurityGroups/join/action",

"Microsoft.Network/networkSecurityGroups/read",

"Microsoft.Network/networkSecurityGroups/write",

"Microsoft.Network/virtualNetworks/subnets/read",

"Microsoft.Network/virtualNetworks/read",
```

```
"Microsoft.Network/virtualNetworks/subnets/join/action"
```

一般権限

共同作成者ロールは、すべてのリソースを管理するためのフルアクセス権を持っています。この権限セットは、新機能の取得を妨げるものではありません。

以下の権限セットは、現在の機能セットで必要とされる以上の権限が含まれていますが、今後も最高の互換性を提供します。

```
"Microsoft.Compute/diskEncryptionSets/read",

"Microsoft.Compute/disks/beginGetAccess/action",

"Microsoft.Compute/disks/delete",

"Microsoft.Compute/disks/endGetAccess/action",

"Microsoft.Compute/disks/read",

"Microsoft.Compute/disks/write",

"Microsoft.Compute/galleries/delete",

"Microsoft.Compute/galleries/images/delete",

"Microsoft.Compute/galleries/images/read",

"Microsoft.Compute/galleries/images/versions/delete",

"Microsoft.Compute/galleries/images/versions/read",

"Microsoft.Compute/galleries/images/versions/write",

"Microsoft.Compute/galleries/images/write",

"Microsoft.Compute/galleries/read",

"Microsoft.Compute/galleries/write",

"Microsoft.Compute/hostGroups/hosts/read",
```

```
"Microsoft.Compute/hostGroups/read",

"Microsoft.Compute/hostGroups/write",

"Microsoft.Compute/snapshots/beginGetAccess/action",

"Microsoft.Compute/snapshots/delete",

"Microsoft.Compute/snapshots/endGetAccess/action",

"Microsoft.Compute/snapshots/read",

"Microsoft.Compute/snapshots/write",

"Microsoft.Compute/virtualMachines/deallocate/action",

"Microsoft.Compute/virtualMachines/delete",

"Microsoft.Compute/virtualMachines/read",

"Microsoft.Compute/virtualMachines/restart/action",

"Microsoft.Compute/virtualMachines/start/action",

"Microsoft.Compute/virtualMachines/write",

"Microsoft.Network/networkInterfaces/delete",

"Microsoft.Network/networkInterfaces/join/action",

"Microsoft.Network/networkInterfaces/read",

"Microsoft.Network/networkInterfaces/write",

"Microsoft.Network/networkSecurityGroups/delete",

"Microsoft.Network/networkSecurityGroups/join/action",

"Microsoft.Network/networkSecurityGroups/read",

"Microsoft.Network/networkSecurityGroups/write",

"Microsoft.Network/virtualNetworks/subnets/read",
```

```
"Microsoft.Network/virtualNetworks/read",

"Microsoft.Network/virtualNetworks/subnets/join/action",

"Microsoft.Resources/deployments/operationstatuses/read",

"Microsoft.Resources/deployments/read",

"Microsoft.Resources/deployments/validate/action",

"Microsoft.Resources/deployments/write",

"Microsoft.Resources/deployments/delete",

"Microsoft.Resources/subscriptions/resourceGroups/read",

"Microsoft.Resources/subscriptions/resourceGroups/write",

"Microsoft.Resources/subscriptions/resourceGroups/delete",

"Microsoft.Storage/storageAccounts/delete",

"Microsoft.Storage/storageAccounts/listKeys/action",

"Microsoft.Storage/storageAccounts/read",

"Microsoft.Storage/storageAccounts/write",

"Microsoft.Resources/templateSpecs/read",

"Microsoft.Resources/templateSpecs/versions/read",
```

必要な Azure ホスト接続権限を構成する

ホスト接続に紐付けられた Azure のサービスプリンシパルまたはユーザーアカウントがすべての MCS 操作を実行するために必要な最小限の権限は、ARM テンプレートを使用して簡単に構成できます。この ARM テンプレートは、以下を自動化します。

- 操作に必要な最小限の権限を持つ Azure ロールの作成。
- このロールを既存のAzureサービスプリンシパルにサブスクリプションレベルで割り当てる。

このARMテンプレートは、Azure PortalまたはPowerShellコマンドを使用して展開できます。詳細については、「CVAD操作用ARMテンプレート」を参照してください。

次のステップ

- 初期展開プロセス中の場合は、「マシンカタログの作成」を参照してください。
- Azure固有の情報については、「Microsoft Azureカタログの作成」を参照してください。

詳細情報

- 接続とリソース
- マシンカタログの作成

マイクロソフト システムセンター 仮想マシンマネージャー への接続

接続とリソースの作成および管理では、接続を作成するウィザードについて説明しています。以下の情報は、Microsoft System Center Virtual Machine Manager (VMM) に固有の詳細を扱っています。

> **注:**
>
> VMM への接続を作成する前に、まず VMM アカウントをリソースの場所として設定する必要があります。(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/install-configure/install-prepare/msscvmm.html)を参照してください。

接続を作成する

MCSを使用してVMをプロビジョニングした場合は、接続作成ウィザードで次の操作を行います。

- ホストサーバーの完全修飾ドメイン名としてアドレスを入力します。
- 以前に設定した管理者アカウントの資格情報を入力します。このアカウントには、新しいVMを作成する権限が必要です。
- 「ホストの詳細」ダイアログボックスで、VMの作成時に使用するクラスターまたはスタンドアロンホストを選択します。

> **重要**

> 単一のHyper-Vホスト展開を使用している場合でも、クラスターまたはスタンドアロンホストを参照してください。

次のステップ

- 初期展開プロセス中の場合は、「マシンカタログの作成」を参照してください。
- SMB 3 ファイル共有でMCSを使用してマシンカタログを作成する方法については、(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/install-configure/machine-catalogs-create/create-machine-catalog-mscvmm.html)を参照してください。

詳細情報

- 接続とリソース
- マシンカタログの作成

Nutanixへの接続

接続とリソースの作成および管理では、接続を作成するウィザードについて説明しています。以下の情報はNutanixに固有の詳細を扱っています。

> **注:**
>
> Nutanixへの接続を作成する前に、まず、リソースの場所としてNutanixアカウントの設定を完了する必要があります。Nutanix仮想化環境を参照してください。

Nutanixへの接続を作成する

以下の情報は、接続とリソースのガイダンスを補足するものです。Nutanix接続を作成するには、その記事の一般的なガイダンスに従い、Nutanixに固有の詳細に注意してください。

接続とリソースの追加ウィザードで、**接続**ページでNutanix接続の種類を選択し、アドレスと資格情報、および接続の名前を指定します。**ネットワーク**ページで、ホスティングユニットのネットワークを選択します。

選択できる接続の種類は、**Nutanix AHV**、**Nutanix AHV DRaaS**、**Nutanix AHV PC**です。

- **Nutanix AHV**の場合、Prism Element（PE）クラスターのアドレスと資格情報を指定します。
- **Nutanix AHV PC**の場合、Prism Central（PC）のアドレスと資格情報を指定します。

> **注:**
>
> 現在、接続タイプNutanix AHV PCは、Azure上のNutanix Cloud Cluster（NC2）への接続を作成する場合にのみ使用されます。また、マシンカタログは、Azure接続上のNC2内の単一クラスターでのみホストできます。

- **Nutanix AHV DRaaS**の場合、DRaaSテナントのアドレスとユーザー名を指定します。プライベートおよびパブリックのNutanix DRaaS資格情報ファイル（`.pem`）をインポートします。

> **ヒント:**
>
> Nutanix AHV（Prism Element）をリソースとして使用してマシンを展開する場合は、VMのディスクが格納されているコンテナを選択します。

次のステップ

- 初期展開プロセス中の場合は、「マシンカタログの作成」を参照してください。
- Nutanix固有の情報については、「Nutanixカタログの作成」を参照してください。

詳細情報

- 接続とリソース
- マシンカタログの作成

Nutanix クラウドおよびパートナーソリューションへの接続

接続とリソースの作成および管理では、接続を作成するウィザードについて説明します。以下の情報では、Nutanix クラウドおよびパートナーソリューションに固有の詳細について説明します。

Citrix Virtual Apps and Desktops™ は、以下の Nutanix クラウドおよびパートナーソリューションをサポートしています。

- AWS 上のニュータニックス クラウドクラスター

> **注:**
>
> Nutanix クラウドおよびパートナーソリューションへの接続を作成する前に、まず、それぞれのNutanixアカウントをリソースの場所として設定を完了する必要があります。「Nutanix

> クラウドおよびパートナーソリューション」を参照してください。(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/install-configure/install-prepare/nutanix-cloud-patrner-solutions.html).

Nutanix Prismへの接続

Nutanix クラスターを作成したら、Nutanix Prism に接続します。

Nutanix Prism に接続するには:

1. 10.0.129.0/24サブネットに踏み台VMを作成します。
2. 踏み台VMにRDP接続し、前のセクションでコピーした**Prism Element**のURLにアクセスします。
3. デフォルトの資格情報 `admin:nutanix/4u` を使用してログインします。パスワードを変更することを忘れないでください。

Nutanixクラスター上にVMを作成する

Nutanix Prismに接続した後、Nutanixクラスター上にVMを作成します。

VMにインターネットアクセスが必要な場合

1. AWS コンソールに移動します。
2. Nutanix CFS によって作成された VPC と同じ VPC に、新しいサブネット 10.0.130.0/24 を作成します。
3. このサブネットのルートテーブルに、すべての非ローカルトラフィックを上記のNATゲートウェイに転送するルートを追加します。
4. 踏み台VMにRDP接続し、前のセクションでコピーした**Prism Element**のURLにアクセスしてログインします。
5. 新しいネットワークを追加します。**Settings>Network Configuration>Create Subnet** に移動します。AWS で使用したのと同じサブネット 10.0.130.0/24 を使用します。
6. その新しいサブネットにすべての VM (AD、CC、VDA など) を作成します。

VM がインターネットアクセスを必要としない場合

1. 踏み台VMにRDP接続し、前のセクションでコピーした**Prism Element**のURLにアクセスしてログインします。
2. 新しいネットワークを追加します。**Settings>Network Configuration>Create Subnet** に移動します。サブネット 10.0.129.0/24 を使用します。
3. そのサブネットにすべての VM (AD、CC、VDA など) を作成します。

> **ヒント:**
>
> VM の時刻とタイムゾーン情報が正しく設定されていることを確認してください。これは特に AD に当てはまります。

ホスト接続を作成する

1. Web Studio を起動します。
2. ホスティングノードを選択し、 をクリックします。
3. **Connection** 画面で、**Create a new Connection** を選択し、**Connection address** に `https://xxx.xxx.xxx.xxx:9440` を入力します。
4. UI に従ってウィザードを完了します。

> **注:**
>
> Web Studio で Nutanix のオプションを表示するには、Nutanix ゾーンで使用されていない場合でも、すべてのコネクタ VM に nutanix プラグインがインストールされている必要があります。

次のステップ

- 初期展開プロセス中の場合は、「マシンカタログの作成」を参照してください。
- Nutanix 固有の情報については、「Nutanix カタログの作成」を参照してください。(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/install-configure/machine-catalogs-create/create-machine-catalog-nutanix.html)

詳細情報

- 接続とリソース
- マシンカタログの作成

VMwareへの接続

接続とリソースの作成および管理では、接続を作成するウィザードについて説明しています。以下の情報は、VMware仮想化環境に固有の詳細を扱っています。

> **注:**
>
> VMwareへの接続を作成する前に、まずVMwareアカウントをリソースの場所として設定を完了する必要があります。「VMware仮想化環境」(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/install-configure/install-prepare/vmware.html)を参照してください。

接続を作成する

接続作成ウィザードで：

1. VMware接続の種類を選択します。
2. vCenter SDKのアクセスポイントのアドレスを指定します。
3. 以前に設定した、VMを作成する権限を持つVMwareユーザーアカウントの資格情報を指定します。ユーザー名はdomain/usernameの形式で指定します。

VMware SSLサムプリント

VMware SSLサムプリント機能により、VMware vSphereハイパーバイザーへのホスト接続を手動で作成する必要がなくなります。接続を作成する前に、サイト内のDelivery Controllerとハイパーバイザーの証明書との間に信頼関係を手動で作成する必要はなくなりました。

VMware SSLサムプリント機能は、信頼されていない証明書のサムプリントをサイトデータベースに保存します。この構成により、ハイパーバイザーは、Controllerによって信頼されていない場合でも、Citrix Virtual Apps and Desktops™によって継続的に信頼されていると識別されることが保証されます。

StudioでvSphereホスト接続を作成する際、接続先のマシンの証明書を表示できるダイアログボックスが表示されます。その後、それを信頼するかどうかを選択できます。

必要な権限

この記事に記載されている権限の一部またはすべてを持つVMwareユーザーアカウントと1つ以上のVMwareロールを作成します。ロールの作成は、Citrix DaaS™のさまざまな操作をいつでも要求するためにユーザーの権限に必要とされる特定の粒度レベルに基づいて行います。ユーザー固有の権限をいつでも付与するには、**子に伝播**オプションを選択した状態で、少なくともデータセンターレベルでそれぞれのロールに関連付けます。ただし、`StorageProfile`権限と特定の`Tags`権限については、**子に伝播**なしで、ルートvCenter Serverレベルで権限を適用します。各テーブルの注記を参照してください。

次の表は、Citrix Virtual Apps and Desktopsの操作と、必要な最小限のVMware権限とのマッピングを示しています。

> **注:**
>
> 権限リストの表示名、特に*ユーザーインターフェイス*は、一部のvSphereバージョンで異なります。たとえば、vSphere 6.7では、*ユーザーインターフェイス*権限は、このページに記載されている必要な権限で説明されている**Settings**および**Memory**ではなく、**Change Memory**および**Change Settings**です。

接続とリソースを追加する

SDK	ユーザーインターフェイス
システム. 匿名、システム. 読み取り、およびシステム. 表示	自動的に追加されます。組み込みの読み取り専用ロールを使用できます。

電源管理

SDK	ユーザーインターフェイス
VirtualMachine.Interact.PowerOff	仮想マシン > インタラクション > 電源オフ
VirtualMachine.Interact.PowerOn	仮想マシン > インタラクション > 電源オン
VirtualMachine.Interact.Reset	仮想マシン > インタラクション > リセット
VirtualMachine.Interact.Suspend	仮想マシン > インタラクション > サスペンド
Datastore.Browse	Datastore > データストアの参照

マシンのプロビジョニング (Machine Creation Services™)

MCS を使用してマシンをプロビジョニングするには、次の権限が必要です。

SDK	ユーザーインターフェイス
Datastore.AllocateSpace	Datastore > スペースの割り当て
Datastore.Browse	Datastore > データストアの参照

SDK	ユーザーインターフェイス
Datastore.FileManagement	Datastore > 低レベルファイル操作
Network.Assign	Network > ネットワークの割り当て
Resource.AssignVMToPool	リソース > 仮想マシンをリソースプールに割り当てる
VirtualMachine.Config.AddExistingDisk	仮想マシン > 構成 > 既存のディスクを追加
VirtualMachine.Config.AddNewDisk	仮想マシン > 構成 > 新しいディスクを追加
仮想マシン.構成.デバイスの追加または削除	仮想マシン > 構成 > デバイスの追加または削除
VirtualMachine.Config.AdvancedConfig	仮想マシン > 構成 > 詳細設定
VirtualMachine.Config.RemoveDisk	仮想マシン > 構成 > ディスクの削除
VirtualMachine.Config.CPUCount	仮想マシン > 構成 > CPU数の変更
VirtualMachine.Config.Memory	仮想マシン > 構成 > メモリの変更
VirtualMachine.Config.Settings	仮想マシン > 構成 > 設定の変更
VirtualMachine.Interact.PowerOff	仮想マシン > 操作 > 電源オフ
VirtualMachine.Interact.PowerOn	仮想マシン > 操作 > 電源オン
VirtualMachine.Interact.Reset	仮想マシン > 操作 > リセット
VirtualMachine.Interact.Suspend	仮想マシン > 操作 > サスペンド
VirtualMachine.Inventory.CreateFromExisting	仮想マシン > インベントリ > 既存から作成
VirtualMachine.Inventory.Create	仮想マシン > インベントリ > 新規作成
VirtualMachine.Inventory.Delete	仮想マシン > インベントリ > 削除
VirtualMachine.Provisioning.Clone	仮想マシン > プロビジョニング > 仮想マシンのクローン作成

SDK	ユーザーインターフェイス
VirtualMachine.State.CreateSnapshot	vSphere 5.0、Update 2、vSphere 5.1、Update 1、および vSphere 6.x、Update 1: 仮想マシン > 状態 > スナップショットの作成; vSphere 5.5: 仮想マシン > スナップショット管理 > スナップショットの作成

イメージの更新とロールバック

SDK	ユーザーインターフェイス
Datastore.AllocateSpace	データストア > スペースの割り当て
Datastore.Browse	データストア > データストアの参照
Datastore.FileManagement	データストア > 低レベルファイル操作
Network.Assign	ネットワーク > ネットワークの割り当て
Resource.AssignVMToPool	リソース > 仮想マシンをリソースプールに割り当てる
VirtualMachine.Config.AddExistingDisk	仮想マシン > 構成 > 既存のディスクを追加
VirtualMachine.Config.AddNewDisk	仮想マシン > 構成 > 新しいディスクを追加
VirtualMachine.Config.AdvancedConfig	仮想マシン > 構成 > 詳細設定
VirtualMachine.Config.RemoveDisk	仮想マシン > 構成 > ディスクの削除
VirtualMachine.Interact.PowerOff	仮想マシン > 操作 > 電源オフ
VirtualMachine.Interact.PowerOn	仮想マシン > 操作 > 電源オン
VirtualMachine.Interact.Reset	仮想マシン > 操作 > リセット
VirtualMachine.Inventory.CreateFromExisting	仮想マシン > インベントリ > 既存から作成
VirtualMachine.Inventory.Create	仮想マシン > インベントリ > 新規作成
VirtualMachine.Inventory.Delete	仮想マシン > インベントリ > 削除

SDK	ユーザーインターフェイス
VirtualMachine.Provisioning.Clone	仮想マシン > プロビジョニング > 仮想マシンのクローン作成

プロビジョニングされたマシンの削除

SDK	ユーザーインターフェイス
Datastore.Browse	データストア > データストアの参照
Datastore.FileManagement	Datastore > 低レベルファイル操作
VirtualMachine.Config.RemoveDisk	仮想マシン > 構成 > ディスクの削除
VirtualMachine.Interact.PowerOff	仮想マシン > 操作 > 電源オフ
VirtualMachine.Inventory.Delete	仮想マシン > インベントリ > 削除

ストレージプロファイル (vSAN)

vSANデータストアでカタログ作成中にストレージポリシーを表示、作成、または削除するには、以下の権限が必要です。

SDK	ユーザーインターフェイス
StorageProfile.Update	プロファイル駆動型ストレージ > プロファイル駆動型ストレージの更新。vSphere 8 の場合: VMストレージポリシー > VMストレージポリシーの更新
StorageProfile.View	PROFILE-DRIVEN STORAGE > プロファイル駆動型ストレージビュー。vSphere 8 の場合: VM ストレージポリシー > VM ストレージポリシーの表示

注:

ストレージプロファイルの権限は、**子に伝播**せずに、ルートvCenter Serverレベルで適用します。

タグとカスタム属性

タグとカスタム属性を使用すると、vSphereインベントリで作成されたVMにメタデータを添付でき、これらのオブジェクトの検索とフィルタリングが容易になります。タグまたはカテゴリを作成、編集、割り当て、削除するには、次の権限が必須です。

SDK	ユーザーインターフェイス
InventoryService.Tagging.CreateTag	vSphere タグ付け > vSphere タグの作成
InventoryService.Tagging.CreateCategory	vSphere タグ付け > vSphere タグカテゴリの作成
InventoryService.Tagging.EditTag	vSphere タグ付け > vSphere タグの編集
InventoryService.Tagging.EditCategory	vSphere タグ付け > vSphere タグカテゴリの編集
InventoryService.Tagging.DeleteTag	vSphere タグ付け > vSphere タグの削除
InventoryService.Tagging.DeleteCategory	vSphere タグ付け > vSphere タグカテゴリの削除
InventoryService.Tagging.AttachTag	vSphere タグ付け > vSphere タグの割り当てまたは割り当て解除
InventoryService.Tagging.ObjectAttachable	vSphere タグ付け > オブジェクトへの vSphere タグの割り当てまたは割り当て解除
Global.ManageCustomFields	グローバル > カスタム属性の管理
Global.SetCustomField	グローバル > カスタム属性の設定

注：

- MCS がマシンカタログを作成すると、ターゲット VM に特別な名前タグを付けます。これらのタグは、マスターイメージを MCS によって作成された VM と区別し、MCS によって作成された VM がイメージ準備に使用されるのを防ぎます。vCenter の `XdProvisioned` 属性の値によって違いを識別できます。MCS が VM を作成する場合、この属性は **True** に設定されます。

- ルート vCenter Server レベルで `InventoryService.Tagging.AttachTag` 権限を、**子への伝播**なしで適用します。

暗号化操作

暗号化操作の特権は、誰がどの種類のオブジェクトに対してどの種類の暗号化操作を実行できるかを制御します。vSphere Native Key Provider は `Cryptographer.*` 特権を使用します。暗号化操作には、以下の最小限の権限が必要です。

注：

これらの権限は、vTPM を搭載した VM を使用して MCS マシンカタログを作成するために必要です。

SDK	ユーザーインターフェイス
Cryptographer.Access	特権 > すべての特権 > 暗号化操作 > 直接アクセス
Cryptographer.AddDisk	特権 > すべての特権 > 暗号化操作 > ディスクの追加
Cryptographer.Clone	特権 > すべての特権 > 暗号化操作 > クローン
Cryptographer.Encrypt	特権 > すべての特権 > 暗号化操作 > 暗号化
Cryptographer.EncryptNew	特権 > すべての特権 > 暗号化操作 > 新規暗号化
Cryptographer.Decrypt	特権 > すべての特権 > 暗号化操作 > 復号化
Cryptographer.Migrate	特権 > すべての特権 > 暗号化操作 > 移行
Cryptographer.ReadKeyServersInfo	特権 > すべての特権 > 暗号化操作 > KMS情報の読み取り

マシンのプロビジョニング (Citrix Provisioning™)

Citrix Provisioningコンソールを介してCitrix Virtual Apps and Desktopsセットアップウィザードおよびデバイスのエクスポートウィザードを使用してVMをプロビジョニングするには、テンプレートをクローンおよび展開するためのこれらの権限が必要です。ホスティング接続の作成時に権限を設定します。マシンのプロビジョニング（Machine Creation Services）のすべての権限と、以下の権限が必要です。

SDK	ユーザーインターフェイス
VirtualMachine.Config.AddRemoveDevice	仮想マシン > 構成 > デバイスの追加または削除
VirtualMachine.Config.CPUCount	仮想マシン > 構成 > CPU数の変更
VirtualMachine.Config.Memory	仮想マシン > 構成 > メモリ
VirtualMachine.Config.Settings	仮想マシン > 構成 > 設定
VirtualMachine.Provisioning.CloneTemplate	仮想マシン > プロビジョニング > テンプレートのクローン作成
VirtualMachine.Provisioning.DeployTemplate	仮想マシン > プロビジョニング > テンプレートの展開
VApp.Export	vApp > エクスポート

> **注：**
>
> マシンプロファイルを使用してMCSマシンカタログを作成するには、`VApp.Export`が必要です。

証明書を取得してインポートする

vSphere通信を保護するため、Citrix®はHTTPではなくHTTPSを使用することを推奨します。

HTTPSにはデジタル証明書が必要です。組織のセキュリティポリシーに準拠した認証局から発行されたデジタル証明書を使用してください。

認証局から発行されたデジタル証明書を使用できない場合は、VMwareがインストールした自己署名証明書を使用できます。この方法は、組織のセキュリティポリシーで許可されている場合にのみ使用してください。VMware vCenter証明書を各Delivery Controllerに追加します。

1. vCenter Serverを実行しているコンピューターの完全修飾ドメイン名（FQDN）を、そのサーバーのhostsファイル（`%SystemRoot%/WINDOWS/system32/Drivers/etc/`）に追加します。この手順は、vCenter Serverを実行しているコンピューターのFQDNがドメインネームシステムにまだ存在しない場合にのみ必要です。
2. 以下の3つの方法のいずれかを使用してvCenter証明書を取得します。

   vCenterサーバーから。

   a. rui.crt ファイルを vCenter サーバーから Delivery Controllers でアクセス可能な場所にコピーします。
   b. Controller で、エクスポートされた証明書の場所に移動し、rui.crt ファイルを開きます。

   Web ブラウザーを使用して証明書をダウンロードします。 Internet Explorer を使用している場合は、Internet Explorer を右クリックし、**管理者として実行**を選択して証明書をダウンロードまたはインストールします。

   a. Web ブラウザーを開き、vCenter サーバーへの安全な Web 接続を行います (例: `<https://server1.domain1.com)>`)。
   b. セキュリティ警告を受け入れます。
   c. 証明書エラーが表示されているアドレスバーをクリックします。
   d. 証明書を表示し、 タブをクリックします。
   e. プロンプトが表示されたら名前を指定して、**ファイルにコピーして .CER 形式でエクスポート**を選択します。
   f. エクスポートされた証明書を保存します。
   g. エクスポートされた証明書の場所に移動し、.CER ファイルを開きます。

   管理者として実行している Internet Explorer から直接インポートします。

   - Web ブラウザーを開き、vCenter サーバーへの安全な Web 接続を行います (例: `<https://server1.domain1.com)>`)。
   - セキュリティ警告を受け入れます。
   - 証明書エラーが表示されているアドレスバーをクリックします。
   - 証明書を表示します。

3. 各Controllerの証明書ストアに証明書をインポートします。

    a. **証明書のインストール**オプションをクリックし、**ローカルコンピューター**を選択して、**次へ**をクリックします。

    b. **証明書をすべて次のストアに配置する**を選択し、**参照**をクリックします。**信頼されたユーザー**を選択し、**OK**をクリックします。**次へ**をクリックし、**完了**をクリックします。

    インストール後にvSphereサーバーの名前を変更した場合は、新しい証明書をインポートする前に、そのサーバーで新しい自己署名証明書を生成する必要があります。

次のステップ

- 初期展開プロセス中の場合は、「マシンカタログの作成」を参照してください。
- VMware固有の情報については、「VMwareカタログの作成」を参照してください。

詳細情報

- 接続とリソース
- マシンカタログの作成

VMware クラウドおよびパートナーソリューションへの接続

Azure VMware Solution (AVS) クラスター(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/install-configure/install-prepare/vmware-cloud-partner-solutions.html#azure-vmware-solution-avs-integration)、Google Cloud VMware Engine(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/install-configure/install-prepare/vmware-cloud-partner-solutions.html#google-cloud-vmware-engine)、およびVMware Cloud on AWS(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/install-configure/install-prepare/vmware-cloud-partner-solutions.html#vmware-cloud-on-amazon-web-services-aws)をセットアップした後、接続を作成します。接続の作成については、VMwareへの接続を参照してください。

次のステップ

- 初期展開プロセス中の場合は、「マシンカタログの作成」を参照してください。
- VMware固有の情報については、VMwareカタログの作成を参照してください。

詳細情報

- 接続とリソース
- マシンカタログの作成

イメージ管理

はじめに

MCSカタログの作成または更新プロセスには、次の2つのフェーズがあります。

- マスタリング: ソースイメージが公開イメージに変換されます
- クローニング: 公開イメージから新しいVMが作成されます

イメージ管理機能を使用すると、MCSはマスタリングフェーズをプロビジョニングワークフロー全体から分離します。

単一のソースイメージからさまざまなMCSイメージバージョン（Prepared Image）を準備し、複数の異なるMCSマシンカタログでそれを使用できます。この実装により、ストレージと時間のコストが大幅に削減され、VMの展開とイメージの更新プロセスが簡素化されます。

このイメージ管理機能を使用する利点は次のとおりです。

- カタログを作成せずに、準備済みイメージを事前に生成します。
- カタログの作成や更新など、複数のシナリオで準備済みイメージを再利用します。
- カタログの作成または更新時間を大幅に短縮します。

> **注：**
>
> - この機能は現在、AzureおよびVMware仮想化環境に適用できます。
> - 準備済みイメージを使用せずにMCSマシンカタログを作成できます。その場合、この機能の利点を得ることはできません。
> - この機能は、Citrix Virtual Apps and Desktops™ 2402 LTSR CU2から一般提供されています。

ユースケース

イメージ管理機能のユースケースの一部を次に示します。

- *バージョン管理*: イメージバージョンを使用すると、次のことができます。
  - 特定のイメージに対する異なるイテレーションや更新を管理する。
  - 異なる目的のためにイメージの複数のバージョンを維持する。

- *論理的なグループ化*: 複数のイメージ定義を作成して、次のことを行えます。
  - プロジェクト、部門、アプリケーション、デスクトップの種類など、さまざまな基準に基づいてイメージのバージョンを論理的にグループ化する。
  - 組織内でイメージをより効率的に管理する。

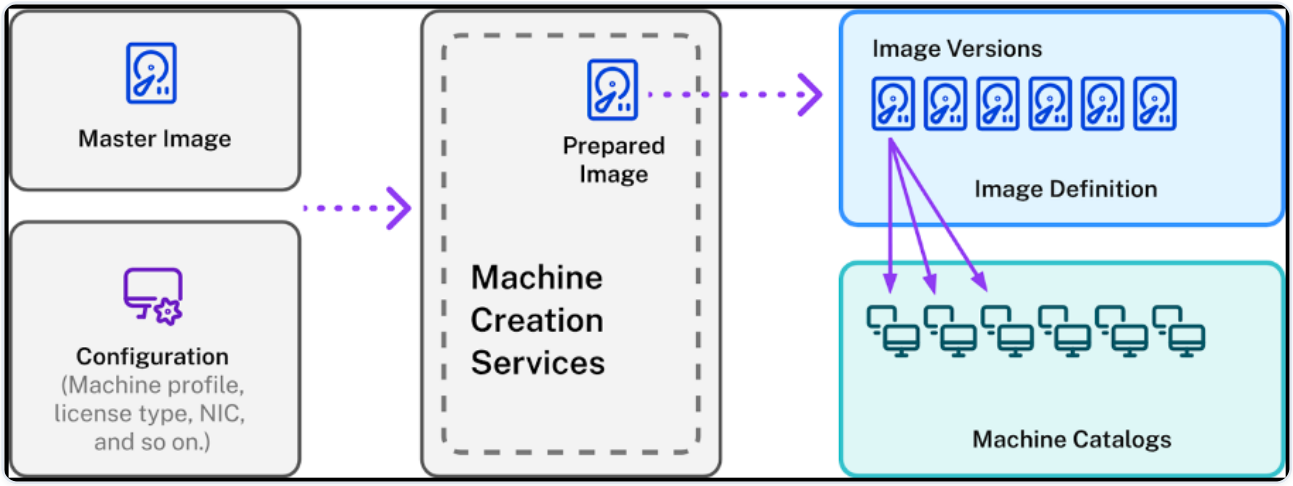
準備されたイメージとは何ですか?

イメージ管理機能により、MCSはマスタリングフェーズをカタログ作成または更新の全体的なワークフローから切り離し、プロセスを2つの段階に分けます。

1. 単一のソースイメージから準備されたイメージを作成する。
2. 準備されたイメージを使用して、MCSマシンカタログを作成または更新する。

準備されたイメージは事前に作成できます。単一の準備されたイメージを使用して、複数のMCSプロビジョニング済みマシンカタログを作成または更新できます。

イメージからWeb Studioを使用する場合に、準備されたイメージが複数のMCSマシンカタログでどのように使用されるかを理解してください。



イメージ定義: イメージ定義は、イメージのバージョンの論理的なグループ化です。イメージ定義には、次の情報が含まれます。

- イメージが作成された理由
- どのOS用であるか
- イメージの使用に関するその他の情報。

カタログはイメージ定義から作成されるのではなく、イメージ定義に基づいて作成されたイメージバージョンから作成されます。

イメージバージョン: イメージバージョンは、イメージ定義のバージョン管理を行います。イメージ定義には複数のイメージバージョンを含めることができます。イメージバージョンを準備済みイメージとして使用して、カタログを作成または更新します。

または、PowerShellコマンドを使用してプロビジョニングスキームを作成し、カタログを作成または更新する場合は、環境の必要に応じて、マスターイメージバージョンスペックに基づいて準備済みイメージバージョンスペックを作成する必要があります。

要件

- Windowsマスターイメージの場合、VDAイメージバージョン2311以降のみがサポートされます。MCS/IOコンポーネントは明示的に選択してインストールする必要があります。MCS I/O構成の有効化または無効化は、デフォルトでは有効になっていないため、マシンカタログの作成または更新時に決定する必要があります。

制限事項

現在、この機能は以下をサポートしていません。

- AzureでのNIC
- 永続データディスク機能
- マルチセッションの休止状態
- イメージタイプの変更

Web Studioを使用したイメージライフサイクル管理

Web Studioを使用する場合のイメージのライフサイクルは次のとおりです。

1. 準備済みイメージの作成: イメージ定義とその初期イメージバージョンを作成します。
2. 初期イメージバージョンからイメージバージョンを作成します。
3. イメージバージョンを準備済みイメージとして使用してカタログを作成します。
4. 別の準備済みイメージでマシンカタログを更新します。
5. イメージ定義とバージョンを管理する: イメージバージョンの名前と説明、およびイメージ定義の説明を編集します。
6. イメージバージョンを削除します。
7. イメージ定義を削除します。

または、PowerShell を使用してイメージを管理することもできます。PowerShell を使用したイメージライフサイクル管理を参照してください。

準備済みイメージを使用してカタログを作成または更新する

準備済みイメージを作成し、その準備済みイメージを使用して、次の方法で MCS マシンカタログを作成または更新します。

- ウェブスタジオ
- PowerShell コマンド

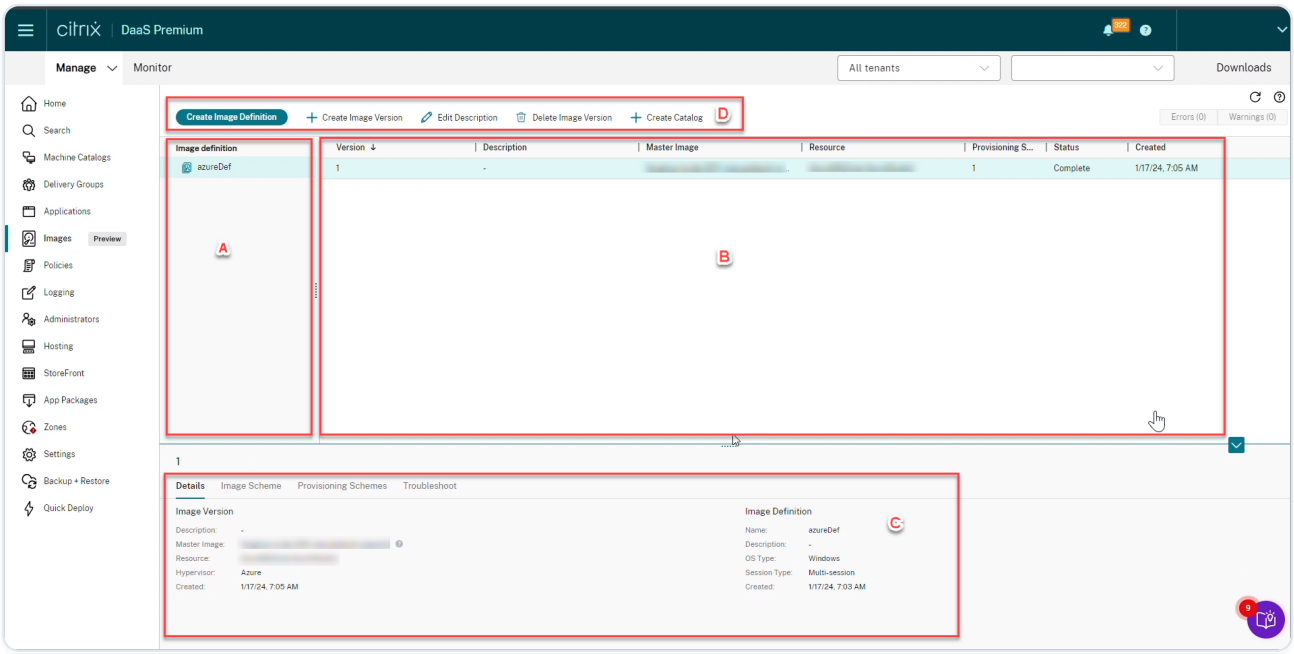
Web Studio を使用する

次のトピックを参照してください。

- イメージノードについて
- イメージ定義と初期イメージバージョンを作成する
- イメージバージョンを作成する
- イメージノードからマシンカタログを作成する
- マシンカタログノードからマシンカタログを作成する
- 別の準備済みイメージでマシンカタログを更新する
- イメージ定義とバージョンを管理する

「イメージ」ノードについて

イメージノードを使用して、MCSで準備されたイメージを作成および管理します。そのメインビューは4つの部分に分かれています。



ラベル	部分	説明
A	イメージ定義	以前に作成されたイメージ定義を一覧表示します。
B	イメージバージョン	選択したイメージ定義のイメージバージョンを表示します。
C	詳細	• **詳細**タブには、選択したイメージ定義またはバージョンに関する詳細情報（マスターイメージ、リソース、ハイパーバイザー、イメージ定義の名前、OSタイプ、セッションタイプなど）が表示されます。 • **イメージスキーム**タブには、ハードディスク、マシンサイズ、ライセンスタイプ、ディスク暗号化セット、マシンプロファイルなど、イメージの準備に使用されるテンプレートに関

ラベル	部分	説明	
		する情報が表示されます。 • **プロビジョニングスキーム**タブには、カタログの作成に使用されたプロビジョニングスキーム名が表示されます。 • **トラブルシューティング**タブには、選択したイメージバージョンのエラー状態が表示されます。	
D	アクションバー	**「Create Image Version」**、**「Edit Description」**、**「Delete Image Version」**、**「Create Catalog」**など、イメージ定義とバージョンに対して実行できるアクションを一覧表示します。	

準備されたイメージを使用してマシンカタログを作成する

準備済みイメージを使用して MCS マシンカタログを作成する主な手順は次のとおりです。

1. イメージ定義と初期イメージバージョンを作成します。
2. イメージバージョンを準備済みイメージとして使用してカタログを作成します。

イメージ定義と初期イメージバージョンを作成する

イメージ定義と初期イメージバージョンを作成するには、次の手順を実行します。

1. Web Studioにサインインし、**Images**ノードを選択します。**Introduction**ページで**Next**をクリックします。
2. **イメージ定義**ページで、イメージ定義の**OSタイプ**と**セッションタイプ**を指定します。
3. **Image**ページで、**Resources**と、イメージバージョンを作成するためのテンプレートとして使用するマスターイメージを選択します。**Use a machine profile**チェックボックスを選択し、マシンプロファイルを選択できます。

   > **注:**
   >
   > イメージを選択する前に、マスターイメージにVDA 2311以降がインストールされており、MCSIOドライバーがVDAにインストールされていることを確認してください。

4. (Azureのみ) **Storage and Licenses Types**ページで、イメージ準備プロセスの一部として使用するストレージとライセンスの種類を選択します。

   > **注:**
   >
   > **イメージ**ページでマシンプロファイルを選択すると、プロファイル設定に基づいてマシンプロファイルのライセンスタイプが事前に選択されます。

5. **マシン仕様**ページで:

   - Azureの場合、マシンサイズを選択します。**Image**ページでマシンプロファイルを選択した場合、マシンプロファイルのマシンサイズがデフォルトで選択されます。
   - VMwareの場合、マシンプロファイルを選択すると、マシンプロファイルから派生した仮想CPUカウントが表示され、変更できません。マシンプロファイルを選択しない場合、マスターイメージから派生したメモリサイズのみが表示されます。

6. **NIC**ページで、準備イメージのNICを選択または追加します。各NICについて、関連する仮想ネットワークを選択します。

VMwareの場合、マシンプロファイルを選択しない場合、マスターイメージに関連付けられているNICがデフォルトで選択されます。マシンプロファイルを選択した場合、NICはマシンプロファイルから派生し、その数は変更できません。

> **注:**
>
> Azureでは複数のNICはサポートされていません。

7. (Azureのみ) **Disk Settings**ページで、顧客管理の暗号化キー (CMEK) を選択します。マシンプロファイルにCMEKがないが、マスターイメージにある場合、マスターイメージからCMEKが事前に選択されます。
8. 「**Version Description**」ページで、作成された初期イメージバージョンの説明を入力します。
9. 「**概要**」ページで、イメージ定義と作成された初期イメージバージョンの詳細を確認します。イメージ定義の名前と説明を入力します。「**完了**」をクリックします。

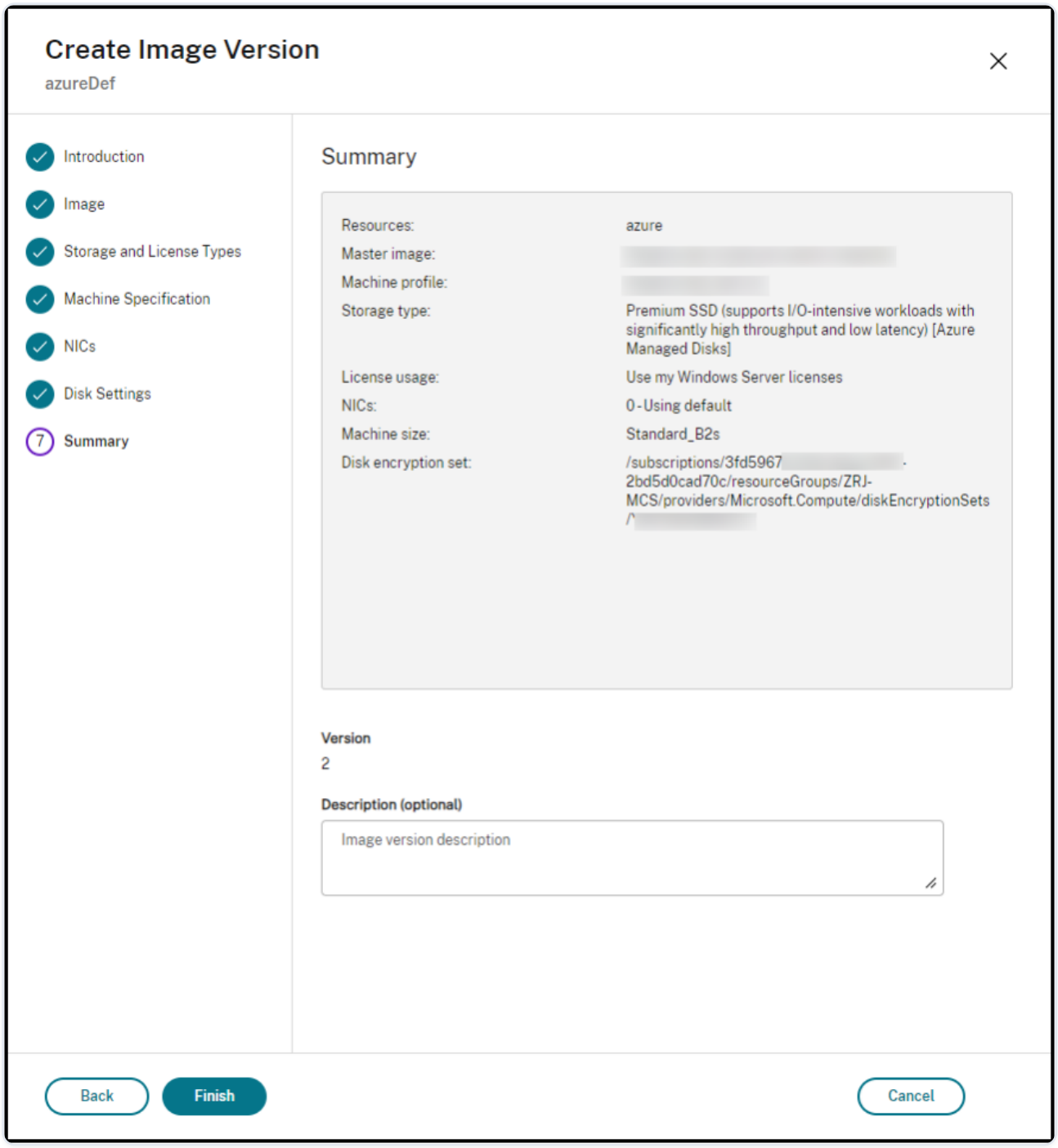
イメージバージョンを作成する

イメージバージョンを使用すると、特定のイメージに対するさまざまなイテレーションや更新を管理できます。この機能により、さまざまな目的のためにイメージの複数のバージョンを維持できます。

初期イメージバージョンからイメージバージョンを作成するには、次の手順を実行します。

> **注:**
>
> すべてのイメージバージョンのホスティングユニットは同じである必要があります。

1. **Images**ノードに移動し、イメージバージョンを選択して、**Create Image Version**を選択します。
2. イメージバージョンの構成を最初に構成したイメージバージョンと異なるものにしたい場合は、**Create Image Version**ダイアログの**Image**、**Storage and License Types**、**Machine Specification**、**NICs**、および**Disk Settings**ページで設定を構成します。
3. イメージバージョンの説明を追加します。「**Finish**」をクリックします。



「イメージ」ノードからマシンカタログを作成する

「**イメージ**」ノードの「**カタログの作成**」オプションを使用して、イメージバージョンでカタログを作成します。

または、**マシンカタログ**ノードでカタログを作成する際にバージョンを選択し、カタログ作成ワークフローで準備済みイメージオプションにリンクできます。「マシンカタログノードからマシンカタログを作成する」を参照してください。(#create-a-machine-catalog-from-the-machine-catalogs-node)

「**イメージ**」ノードからMCSマシンカタログを作成するには、次の手順を実行します。

1. イメージバージョンを選択し、「**カタログの作成**」をクリックします。「**はじめに**」ページで「**次へ**」をクリックします。
2. **デスクトップエクスペリエンス**ページで、必要なデスクトップエクスペリエンスを選択します。
3. **イメージ**ページから**ディスク設定**ページまで、設定は選択したイメージバージョンに基づいて事前に選択されています。
4. (Azureの場合) **Resource Group**ページで、新しいリソースグループを作成するか、既存のリソースグループを使用してこのカタログのリソースを配置するかを選択できます。
5. 次のページで設定を完了します。
6. **概要**ページで、マシンカタログの詳細を確認します。マシンカタログの名前と説明を入力します。**完了**をクリックします。
7. 作成されたマシンカタログを表示するには、**マシンカタログ**ノードに移動します。

「マシンカタログ」ノードからマシンカタログを作成する

マシンカタログノードからMCSマシンカタログを作成するには、次の手順を実行します。

1. 左側のナビゲーションペインで**マシンカタログ**をクリックします。
2. **マシンカタログの作成**をクリックします。**マシンカタログのセットアップ**ページが表示されます。**はじめに**、**マシンタイプ**、**マシン管理**の各ページで**次へ**をクリックします。
3. **イメージ**ページで：
   a. **準備済みイメージ**を選択します。
   b. 「**準備済みイメージ**」の下で、イメージ定義のイメージバージョンを選択します。
   c. イメージバージョン名をクリックします。選択したイメージバージョンの詳細を表示するには、下線が引かれているバージョン番号をクリックします。
   d. 選択したイメージバージョンがマシンプロファイルで構成されている場合は、マシンプロファイルを選択します。選択したイメージバージョンがマシンプロファイルで構成されていない場合、マシンプロファイルを使用することはできません。
4. 次のページで設定を構成します。
5. 「**ディスク設定**」ページで、選択した準備済みイメージがディスク暗号化セットを使用している場合、その暗号化セットを削除することはできませんが、キーを別の暗号化キーに変更することはできます。
6. (Azureの場合) **Resource Group**ページで、新しいリソースグループを作成するか、既存のリソースグループを使用してこのカタログのリソースを配置するかを選択できます。

7. 次のページで設定を完了します。
8. **概要**ページで、マシンカタログの詳細を確認します。マシンカタログの名前と説明を入力します。**完了**をクリックします。

別の準備済みイメージでマシンカタログを更新する

既存のMCSマシンカタログを別の準備済みイメージで更新するには、次の手順を実行します。

1. 左側のナビゲーションペインで をクリックし、更新するマシンカタログを選択します。右クリックして を選択します。
2. **イメージ**ページで、準備済みイメージを選択します。
3. **ロールアウト戦略**ページで、選択した準備済みイメージでこのカタログを更新するタイミングを選択します。
4. ページで詳細を確認します。 をクリックします。

カタログに対して行われたイメージ変更の履歴を表示できます。履歴を表示するには、次の手順を実行します。

1. マシンカタログを選択します。
2. タブの フィールドで、 をクリックします。

イメージ定義とバージョンを管理する

イメージ定義とバージョンを編集および削除して、作成されたさまざまなイメージバージョンと定義の使用を管理できます。

イメージ定義を編集する

イメージ定義の名前と説明を編集できます。

イメージ定義を編集するには、次の手順を実行します。

1. ノードに移動し、イメージ定義を選択して、 を選択します。

イメージバージョンを編集する

イメージバージョンの説明を編集して、そのイメージバージョンの目的を指定できます。

イメージバージョンを編集するには、次の手順を実行します。

1. **イメージ**ノードに移動し、イメージバージョンを選択して、**説明の編集**を選択します。

イメージバージョンを削除する

イメージバージョンを削除するには、次の手順を実行します。

1. **イメージ**ノードに移動し、イメージバージョンを選択して、**イメージバージョンの削除**を選択します。

> **注:**
>
> イメージバージョンがマシンカタログで使用されている場合、そのイメージバージョンを削除することはできません。

イメージ定義を削除する

イメージ定義を削除するには、次の手順を実行します。

1. **イメージ**ノードに移動し、イメージ定義を選択して、**イメージ定義の削除**を選択します。

> **注:**
>
> イメージ定義にイメージバージョンが含まれている場合、そのイメージ定義を削除することはできません。

PowerShell を使用したイメージライフサイクル管理

PowerShell コマンドを使用してプロビジョニングスキームを作成する場合は、環境の必要に応じて、マスターイメージバージョン仕様に基づいて準備されたイメージバージョン仕様を作成する必要があります。

マスターイメージバージョン仕様: マスターイメージバージョン仕様は、イメージバージョンに追加または作成された特定のイメージです。ハイパーバイザー内の既存のイメージをマスターイメージバージョン仕様として追加するか、環境の必要に応じてマスターイメージバージョン仕様に基づいて準備されたイメージバージョン仕様を作成できます。準備されたイメージバージョン仕様は、複数のプロビジョニングスキームに使用できます。

PowerShell コマンドを使用する場合のイメージのライフサイクルは次のとおりです。

1. イメージを作成する:
    a. イメージ定義を作成します。
    b. イメージバージョンを作成します。
    c. マスターイメージバージョン仕様を追加します。
    d. 準備済みイメージバージョン仕様を作成します。

2. 準備済みイメージバージョン仕様を使用してMCSマシンカタログを作成します。
    a. ブローカーカタログを作成します。
    b. ID プールを作成します。
    c. `New-ProvScheme`コマンドを使用して、準備済みイメージバージョン仕様のUidパラメーターを持つプロビジョニングスキームを作成します。
    d. ブローカーカタログをプロビジョニングスキームにリンクします。
3. MCSマシンカタログにVMを作成します。
4. `Set-ProvScheme`コマンドを使用して、プロビジョニングスキームの準備済みイメージバージョン仕様を変更します。
5. イメージ定義とバージョンを管理します: イメージバージョンとイメージ定義を編集します。
6. MCSマシンカタログを削除します: 削除順序は、準備済みイメージバージョン仕様 > マスターイメージバージョン仕様 > イメージバージョン > イメージ定義です。イメージバージョン仕様を削除する前に、準備済みイメージバージョン仕様がどのMCSマシンカタログにも関連付けられていないことを確認してください。

PowerShell を使用する

PowerShellコマンドを使用して、次のことができます。

- 準備済みイメージを作成する
- 準備済みイメージバージョン仕様を使用してカタログを作成する
- 準備されたイメージバージョン仕様を使用してカタログを更新する
- イメージ定義、イメージバージョン、および準備されたイメージバージョン仕様を削除する
- イメージ定義とイメージバージョンを管理する
- イメージ定義、イメージバージョン、準備されたイメージバージョン仕様、およびプロビジョニングスキームの詳細を取得する

準備済みイメージを作成する

準備済みイメージバージョン仕様を作成するための詳細な PowerShell コマンドは次のとおりです。

1. `Test-ProvImageDefinitionNameAvailable command` を使用して、利用可能なイメージ定義名を確認します。例:

```
Test-ProvImageDefinitionNameAvailable -ImageDefinitionName <string[]>
```

2. `New-ProvImageDefinition` コマンドを使用してイメージ定義を作成します。例:

```
New-ProvImageDefinition -ImageDefinitionName image1 -OsType Windows
-VdaSessionSupport MultiSession
```

3. `New-ProvImageVersion` コマンドを使用してイメージバージョンを作成します。例:

```
New-ProvImageVersion -ImageDefinitionName image1 -Description "version
1"
```

4. `Add-ProvImageVersionSpec` コマンドを使用して、マスターイメージバージョン仕様をイメージバージョンに追加します。例:

```
Add-ProvImageVersionSpec -ImageDefinitionName  image1  -
ImageVersionNumber  1 -HostingUnitName azure -MasterImagePath "XDHyp:
\HostingUnits\azure\image.folder\azureresourcegroup.resourcegroup\win20
22-snapshot.snapshot"
```

> **注:**
>
> ホスティングユニットのイメージバージョンには、マスターイメージバージョン仕様を1つだけ追加できます。

5. `New-ProvImageVersionSpec` コマンドを使用して、マスターイメージバージョン仕様から準備済みイメージバージョン仕様を作成します。例：

```
New-ProvImageVersionSpec

-SourceImageVersionSpecUid  c6e7384c-b2f8-46d6-9519-29a2c57ed3cb

-NetworkMapping @{"0"="XDHyp:
\HostingUnits\azure\virtualprivatecloud.folder\azureresourcegroup.resou
rcegroup\azure-vnet-eastus.virtualprivatecloud\dev.network"

-ServiceOffering "XDHyp:
```

```
\HostingUnits\azure\serviceoffering.folder\Standard_B2ms.serviceofferin
g" -CustomProperties "<CustomProperties xmlns=`"http://
schemas.citrix.com/2014/xd/machinecreation`" xmlns:xsi=`"http://
www.w3.org/2001/XMLSchema-instance`"></CustomProperties>"
-RunAsynchronously
```

注:

1つのホスティングユニットと準備タイプには、準備済みインスタンスを1つのみ持つことができます。

Azure でイメージ定義、イメージバージョン、および準備されたイメージバージョン仕様を作成するための PowerShell コマンドの完全なセットの例:

```
$ImageDefintion = New-ProvImageDefinition

-ImageDefinitionName image1 -OsType Windows -VdaSessionSupport
MultiSession

 $ImageVersion = New-ProvImageVersion -ImageDefinitionName
$ImageDefintion.ImageDefinitionName -Description "version 1"

$MasterImagePath = "XDHyp:
\HostingUnits\azure\image.folder\azureresourcegroup.resourcegroup\win2022-
snapshot.snapshot"

$SourceImageVersionSpec = Add-ProvImageVersionSpec -ImageDefinitionName
$ImageVersion.ImageDefinitionName -ImageVersionNumber
$ImageVersion.ImageVersionNumber -HostingUnitName azure -MasterImagePath
$MasterImagePath

$Task = New-ProvImageVersionSpec -SourceImageVersionSpecUid
 $SourceImageVersionSpec.ImageVersionSpecUid -NetworkMapping @{"0"="XDHyp:
\HostingUnits\azure\virtualprivatecloud.folder\azureresourcegroup.resource
group\azure-vnet-eastus.virtualprivatecloud\dev.network"} -ServiceOffering
"XDHyp:
\HostingUnits\azure\serviceoffering.folder\Standard_B2ms.serviceoffering"
-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com/
2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`"></CustomProperties>" -RunAsynchronously
```

```
Get-ProvTask -TaskId $Task.TaskId
```

VMware でイメージ定義、イメージバージョン、および準備されたイメージバージョン仕様を作成するための PowerShell コマンドの完全なセットの例:

```
$ImageDefintion = New-ProvImageDefinition -ImageDefinitionName image2
-OsType Windows -VdaSessionSupport SingleSession

$ImageVersion = New-ProvImageVersion -ImageDefinitionName
$ImageDefintion.ImageDefinitionName -Description "version 1"

$MasterImagePath = "XDHyp:\HostingUnits\vmware\win10-master.vm\win10-
master-snap.snapshot"

$SourceImageVersionSpec = Add-ProvImageVersionSpec -ImageDefinitionName
$ImageVersion.ImageDefinitionName -ImageVersionNumber
$ImageVersion.ImageVersionNumber -HostingUnitName vmware -MasterImagePath
$MasterImagePath

$Task = New-ProvImageVersionSpec -SourceImageVersionSpecUid
 $SourceImageVersionSpec.ImageVersionSpecUid -NetworkMapping @{"0"="XDHyp:
\HostingUnits\vmware\\DSwitch-VM Network.network"} -VMCpuCount 2
-VMMemoryMB 4096 -RunAsynchronously

Get-ProvTask -TaskId $Task.TaskId
```

注:

- イメージ定義内のすべてのイメージバージョン仕様は、同じホスティングユニットに属している必要があります。
- イメージバージョンには、マスターイメージバージョン仕様を1つ、準備済みイメージバージョン仕様を1つだけ含めることができます。
- すべてのイメージバージョン仕様はマシンプロファイルを持つか、またはどのイメージバージョン仕様もマシンプロファイルを持たないかのいずれかである必要があります。
- イメージバージョン仕様の作成中にリソースグループを指定することはできません。

準備済みイメージバージョン仕様を使用してカタログを作成する

`New-ProvScheme` コマンドを使用して、準備済みイメージバージョン仕様から MCS マシンカタログを作成します。例:

```
New-ProvScheme -ProvisioningSchemeName <string> -ImageVersionSpecUid
<Guid> -HostingUnitUid <Guid> -IdentityPoolUid <Guid> [-VMCpuCount <int>]
[-VMMemoryMB <int>] [-UseWriteBackCache] [-NetworkMapping <Hashtable>] [-
CleanOnBoot] [-Scope <string[]>] [-Metadata <Hashtable>] [-ServiceOffering
<string>] [-SecurityGroup <string[]>] [-TenancyType <string>] [-
MachineProfile <string>] [-CustomProperties <string>] [-
ResetAdministratorPasswords] [-UseFullDiskCloneProvisioning] [-
RunAsynchronously] [-PurgeJobOnSuccess] [-ProvisioningSchemeType
<ProvisioningSchemeType>]
```

または、,

```
New-ProvScheme -ProvisioningSchemeName <string> -ImageVersionSpecUid
<Guid> -HostingUnitName <string> -IdentityPoolName <string> [-VMCpuCount
<int>] [-VMMemoryMB <int>] [-UseWriteBackCache] [-NetworkMapping
<Hashtable>] [-CleanOnBoot] [-Scope <string[]>] [-Metadata <Hashtable>] [-
ServiceOffering <string>] [-SecurityGroup <string[]>] [-TenancyType
<string>] [-MachineProfile <string>] [-CustomProperties <string>] [-
ResetAdministratorPasswords] [-UseFullDiskCloneProvisioning] [-
RunAsynchronously] [-PurgeJobOnSuccess] [-ProvisioningSchemeType
<ProvisioningSchemeType>]
```

Azure でカタログを作成するための PowerShell コマンドの完全なセットの例:

```
$Catalog = New-BrokerCatalog  -AllocationType "Random"  -IsRemotePC $False
 -MinimumFunctionalLevel "L7_20" -Name "azurecatalog" -PersistUserChanges
"Discard" -ProvisioningType "MCS" -Scope @() -SessionSupport
"MultiSession"

$IdentityPool = New-AcctIdentityPool  -AllowUnicode  -Domain "azure.local"
-IdentityPoolName "azurecatalog" -IdentityType "ActiveDirectory"  -
NamingScheme "azure##" -NamingSchemeType "Numeric" -Scope @()

$PreparedImageVersionSpec = Get-ProvImageVersionSpec -ImageDefinitionName
image1 -ImageVersionNumber 1 -Filter "PreparationType -eq 'Mcs'"

$Task = New-ProvScheme -ProvisioningSchemeName azurecatalog
```

```
-ImageVersionSpecUid $PreparedImageVersionSpec.ImageVersionSpecUid
-HostingUnitName azure -IdentityPoolName azurecatalog -CleanOnBoot -Scope
@() -SecurityGroup @() -ServiceOffering "XDHyp:
\HostingUnits\azure\serviceoffering.folder\Standard_B2s.serviceoffering"
-NetworkMapping @{"0"="XDHyp:
\HostingUnits\azure\virtualprivatecloud.folder\azureresourcegroup.resource
group\azure-vnet-eastus.virtualprivatecloud\dev.network"}
-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com/
2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`"><Property xsi:type=`"StringProperty`"
Name=`"StorageAccountType`" Value=`"StandardSSD_LRS`" /></
CustomProperties>" -RunAsynchronously

Get-ProvTask -TaskId $Task.TaskId

$ProvScheme = Get-ProvScheme -ProvisioningSchemeName azurecatalog

Set-BrokerCatalog -Name $Catalog.Name -ProvisioningSchemeId
$ProvScheme.ProvisioningSchemeUid
```

VMware でカタログを作成するための PowerShell コマンドの完全なセットの例:

```
$Catalog = New-BrokerCatalog  -AllocationType "Random"  -IsRemotePC $False
 -MinimumFunctionalLevel "L7_20" -Name "vmwarecatalog" -PersistUserChanges
"Discard" -ProvisioningType "MCS" -Scope @() -SessionSupport
"MultiSession"

$IdentityPool = New-AcctIdentityPool  -AllowUnicode  -Domain
"vmware.local" -IdentityPoolName "vmwarecatalog" -IdentityType
"ActiveDirectory"  -NamingScheme "vmware##" -NamingSchemeType "Numeric"
-Scope @()

$PreparedImageVersionSpec = Get-ProvImageVersionSpec -ImageDefinitionName
image2 -ImageVersionNumber 1 -Filter "PreparationType -eq 'Mcs'"

$Task = New-ProvScheme -ProvisioningSchemeName vmwarecatalog
-ImageVersionSpecUid $PreparedImageVersionSpec.ImageVersionSpecUid
-HostingUnitName vmware -IdentityPoolName vmwarecatalog -CleanOnBoot
-Scope @() -SecurityGroup @() -NetworkMapping @{"0"="XDHyp:
\HostingUnits\vmware\\DSwitch-VM Network.network"} -VMCpuCount 2
-VMMemoryMB 4096 -RunAsynchronously

Get-ProvTask -TaskId $Task.TaskId
```

```
$ProvScheme = Get-ProvScheme -ProvisioningSchemeName vmwarecatalog

Set-BrokerCatalog -Name $Catalog.Name -ProvisioningSchemeId
$ProvScheme.ProvisioningSchemeUid
```

準備されたイメージバージョン仕様を使用してカタログを更新する

`Set-ProvSchemeImage` コマンドを使用してカタログを更新できます。例:

```
Set-ProvSchemeImage -ProvisioningSchemeUid <Guid> -ImageVersionSpecUid
<Guid> [-DoNotStoreOldImage] [-RunAsynchronously] [-PurgeJobOnSuccess]
```

または、,

```
Set-ProvSchemeImage -ProvisioningSchemeName <string> -ImageVersionSpecUid
<Guid> [-DoNotStoreOldImage] [-RunAsynchronously] [-PurgeJobOnSuccess]
```

カタログを更新するための PowerShell コマンドの完全なセットの例:

```
$PreparedImageVersionSpec = Get-ProvImageVersionSpec -ImageDefinitionName
image1 -ImageVersionNumber 2 -Filter "PreparationType -eq 'Mcs'"

Set-ProvSchemeImage -ProvisioningSchemeName azurecatalog
-ImageVersionSpecUid $PreparedImageVersionSpec.ImageVersionSpecUid
-RunAsynchronously
```

イメージ定義、イメージバージョン、および準備されたイメージバージョン仕様を削除する

イメージ定義、イメージバージョン、および準備されたイメージバージョン仕様を削除する前に、次の点を考慮してください:

- イメージ定義にイメージバージョンが含まれている場合、そのイメージ定義は削除できません。
- イメージバージョンにイメージバージョン仕様が含まれている場合、そのイメージバージョンは削除できません。
- マスターイメージバージョン仕様が他の準備済みイメージバージョン仕様で使用されている場合、そのマスターイメージバージョン仕様は削除できません。

- 準備済みイメージバージョン仕様がプロビジョニングスキームで使用されている場合、その準備済みイメージバージョン仕様は削除できません。

詳細な手順は次のとおりです。

1. 準備済みイメージバージョン仕様を削除します。例：

```
$PreparedImageVersionSpec = Get-ProvImageVersionSpec
-ImageDefinitionName image1 -ImageVersionNumber 1 -Filter
"PreparationType -eq 'Mcs'"

Remove-ProvImageVersionSpec -ImageVersionSpecUid
$PreparedImageVersionSpec.ImageVersionSpecUid -RunAsynchronously
```

> **注:**
>
> マスターイメージバージョン仕様は、関連付けられた準備済みイメージバージョン仕様がない場合にのみ削除できます。

2. マスターイメージバージョン仕様を削除します。例：

```
$MasterImageVersionSpec = Get-ProvImageVersionSpec -ImageDefinitionName
image1 -ImageVersionNumber 1 -Filter "PreparationType -eq 'None'"

Remove-ProvImageVersionSpec -ImageVersionSpecUid
$PreparedImageVersionSpec.ImageVersionSpecUid -RunAsynchronously
```

3. イメージバージョンを削除します。例：

```
Remove-ProvImageVersion -ImageDefinitionName image1 -ImageVersionNumber
1
```

4. イメージ定義を削除します。例：

```
Remove-ProvImageDefinition -ImageDefinitionName image1
```

PowerShellコマンドの完全なセットの例：

```
$PreparedImageVersionSpec = Get-ProvImageVersionSpec -ImageDefinitionName
image1 -ImageVersionNumber 1 -Filter "PreparationType -eq 'Mcs'"

$Task = Remove-ProvImageVersionSpec -ImageVersionSpecUid
$PreparedImageVersionSpec.ImageVersionSpecUid -RunAsynchronously

$MasterImageVersionSpec = Get-ProvImageVersionSpec -ImageDefinitionName
image1 -ImageVersionNumber 1 -Filter "PreparationType -eq 'None'"

$Task = Remove-ProvImageVersionSpec -ImageVersionSpecUid
$PreparedImageVersionSpec.ImageVersionSpecUid -RunAsynchronously

Remove-ProvImageVersion -ImageDefinitionName image1 -ImageVersionNumber 1

Remove-ProvImageDefinition -ImageDefinitionName image1
```

イメージ定義とイメージバージョンの管理

イメージ定義の名前変更と編集、およびイメージバージョンの編集が可能です。

- `Rename-ProvImageDefinition` コマンドを使用してイメージ定義の名前を変更します。例：

  ```
  Rename-ProvImageDefinition -ImageDefinitionUid <Guid>
  -NewImageDefinitionName <string>
  ```

  または、,

  ```
  Rename-ProvImageDefinition -ImageDefinitionName <string>
  -NewImageDefinitionName <string>
  ```

- `Set-ProvImageDefinition` コマンドを使用してイメージ定義を編集します。例：

  ```
  Set-ProvImageDefinition -ImageDefinitionUid <Guid> [-Description
  <string>]
  ```

  または、,

  ```
  Set-ProvImageDefinition -ImageDefinitionName <string> [-Description
  <string>]
  ```

- `Set-ProvImageVersion` コマンドを使用してイメージバージョンを編集します。例：

```
Set-ProvImageVersion -ImageVersionUid <Guid> [-Description <string>]
```

または、,

```
Set-ProvImageVersion -ImageDefinitionName <string> -ImageVersionNumber
<int> [-Description <string>]
```

イメージ定義、イメージバージョン、準備済みイメージバージョン仕様、およびプロビジョニングスキームの詳細を取得する

- `Get-ProvImageDefinition` コマンドを使用してイメージ定義の詳細を取得します。例:

```
Get-ProvImageDefinition [-ImageDefinitionName <string>] [-
ImageDefinitionUid <Guid>] [-ReturnTotalRecordCount] [-MaxRecordCount
<int>] [-Skip <int>] [-SortBy <string>] [-Filter <string>]
```

- `Get-ProvImageVersion` コマンドを使用してイメージバージョンの詳細を取得します。例:
  - イメージ定義内のイメージバージョンを一覧表示するには、,

```
Get-ProvImageVersion -ImageDefinitionUid <Guid>
```

または、,

```
Get-ProvImageVersion -ImageDefinitionName <string>
```

  - イメージバージョンの詳細を取得するには、,

```
Get-ProvImageVersion -ImageVersionUid <Guid>
```

または、,

```
Get-ProvImageVersion -ImageDefinitionName <string>
-ImageVersionNumber <int>
```

- `Get-ProvImageVersionSpec` コマンドを使用して準備済みイメージバージョン仕様を取得します。例:
  - イメージバージョン内のすべての準備済みイメージバージョン仕様を一覧表示するには、,

    ```
    Get-ProvImageVersionSpec -ImageVersionUid <Guid>
    ```

  - 準備済みイメージバージョン仕様内のマスターイメージバージョン仕様を一覧表示するには、,

    ```
    Get-ProvImageVersionSpec -ImageVersionUid <Guid> -Filter
    'PreparationType -eq "None"'
    ```

  - マスターイメージに関連付けられているイメージバージョン内の準備済みイメージバージョン仕様を一覧表示するには、,

    ```
    Get-ProvImageVersionSpec -ImageVersionUid <Guid> -Filter
    'PreparationType -eq "MCS" -and SourceImageVersionSpecUid -eq
    "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"'
    ```

  - イメージバージョン内の成功した準備済みイメージバージョン仕様を取得するには、,

    ```
    Get-ProvImageVersionSpec -ImageVersionUid <Guid> -Filter
    'PreparationType -eq "MCS" -and SourceImageVersionSpecUid -eq
    "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" -and ImageVersionSpecStatus
    -eq "Complete"'
    ```

  - 準備済みイメージバージョン仕様の詳細を取得するには、,

    ```
    Get-ProvImageVersionSpec -ImageVersionSpecUid <Guid>
    ```

- `Get-ProvScheme` コマンドを使用してプロビジョニングスキームの詳細を取得します。例:

  ```
  Get-ProvScheme [[-ProvisioningSchemeName] <String>] [-
  ProvisioningSchemeUid <Guid>] [-ScopeId <Guid>] [-ScopeName <String>]
  [-ReturnTotalRecordCount] [-MaxRecordCount <Int32>] [-Skip <Int32>] [-
  SortBy <String>] [-Filter <String>] [-FilterScope <Guid>]
  ```

- `Get-ProvSchemeImageVersionSpecHistory` コマンドを使用してプロビジョニングスキームの準備済みイメージバージョン仕様の履歴を取得します。例:

```
Get-ProvSchemeImageVersionSpecHistory [-ProvisioningSchemeName
<String>] [-ProvisioningSchemeUid <Guid>] [-ImageVersionSpecUid <Guid>]
[-ImageVersionSpecHistoryUid <Guid>] [-ReturnTotalRecordCount] [-
MaxRecordCount <Int32>] [-Skip <Int32>] [-SortBy <String>] [-Filter
<String>] [-FilterScope <Guid>]
```

マシンカタログを作成する

重要:

Citrix Virtual Apps and Desktops™ 7 2006以降、現在の展開で以下のいずれかのテクノロジーを使用している場合、それらのテクノロジーを使用するサポート終了 (EOL) アイテムを削除した後にのみ、現在のリリースにアップグレードできます。

- パーソナル vDisk (PvDs)
- AppDisks™
- パブリッククラウドホストの種類: Citrix CloudPlatform、Microsoft Azure Classic

詳細については、「PVD、AppDisks、およびサポートされていないホストの削除」を参照してください。

注：

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

展開にパブリッククラウドホスト接続を使用する場合は、新規インストールまたは現在のリリースへのアップグレードを完了するためにハイブリッド権限ライセンスが必要です。

インストーラーがサポートされていないテクノロジーまたはハイブリッド権限ライセンスのないホスト接続を1つ以上検出すると、アップグレードは一時停止または停止します。説明メッセージが表示されます。インストーラーログには詳細が含まれています。詳細については、「展開のアップグレード」を参照してください。

はじめに

物理マシンまたは仮想マシンのコレクションは、マシンカタログと呼ばれる単一のエンティティとして管理されます。カタログ内のすべてのマシンは、マルチセッションOSまたはシングルセッションOS、およびWindowsまたはLinuxマシンという同じ種類のオペレーティングシステムを持っています。

Web Studioは、サイトを作成した後、最初のマシンカタログを作成するようにガイドします。最初のカタログを作成した後、Web Studioは最初のデリバリーグループを作成するようにガイドします。後で、作成したカタログを変更したり、さらにカタログを作成したりできます。

> **ヒント:**
>
> 既存の展開をアップグレードすると、Machine Creation Services (MCS) ストレージ最適化 (MCS I/O) 機能が有効になり、追加の構成は不要です。Virtual Delivery Agent (VDA) とDelivery ControllerのアップグレードがMCS I/Oのアップグレードを処理します。

概要

VM のカタログを作成するときは、それらの VM をプロビジョニングする方法を指定します。Machine Creation Services™ (MCS) を使用できます。または、独自のツールを使用してマシンを提供することもできます。

考慮事項:

- MCSは、仮想マシンイメージからの単一のシステムディスクをサポートします。そのイメージに接続されている残りのデータディスクは無視されます。
- MCSを使用してVMをプロビジョニングする場合、カタログに同一のVMを作成するためにマスターイメージ (またはイメージのスナップショット) を提供します。カタログを作成する前に、まずツールを使用してマスターイメージを作成および構成します。このプロセスには、イメージにVirtual Delivery Agent (VDA) をインストールすることが含まれます。次に、Web Studioでマシンカタログを作成します。そのイメージ (またはスナップショット) を選択し、カタログに作成するVMの数を指定し、追加情報を構成します。

- マシンがすでに利用可能な場合でも、それらのマシン用に1つ以上のマシンカタログを作成する必要があります。
- PowerShell SDK を直接使用してカタログを作成する場合、イメージまたはスナップショットではなく、ハイパーバイザーテンプレート (**VMTemplates**) を指定できます。
- テンプレートを使用してカタログをプロビジョニングすることは、実験的な機能と見なされます。この方法を使用すると、仮想マシンの準備が失敗する可能性があります。その結果、テンプレートを使用してカタログを公開することはできません。

MCS または Citrix Provisioning™ を使用して最初のカタログを作成する場合、サイトを作成したときに構成したホスト接続を使用します。後で（最初のカタログとデリバリーグループを作成した後）、その接続に関する情報を変更したり、さらに接続を作成したりできます。

カタログ作成ウィザードを完了すると、正しく構成されていることを確認するためにテストが自動的に実行されます。テストが完了すると、テストレポートを表示できます。Web Studio からいつでもテストを実行できます。

> **注：**
>
> MCSはWindows 10 IoT CoreおよびWindows 10 IoT Enterpriseをサポートしていません。詳細については、Microsoftサイトを参照してください。

> Citrix Provisioning ツールに関する技術的な詳細については、「Citrix Virtual Apps and Desktops Image Management」を参照してください。

RDS ライセンスチェック

Web Studio は現在、Windows マルチセッションOSマシンを含むマシンカタログを作成する際に、有効なMicrosoft RDSライセンスのチェックを実行しません。Windows **マルチセッションOSマシン**のMicrosoft RDSライセンスのステータスを表示するには、Citrix Directorに移動します。**マシン詳細**パネルでMicrosoft RDSライセンスのステータスを表示します。このパネルは、**マシン詳細とユーザー詳細**ページにあります。詳細については、「Microsoft RDS license health」を参照してください。

VDA登録

ブローカーセッションを起動する際、VDAはDelivery Controller™に登録されている必要があります。未登録のVDAは、利用可能なリソースの活用不足につながる可能性があります。VDAが登録されない理由はさまざまあり、その多くは管理者がトラブルシューティングできます。Web

Studioは、カタログ作成ウィザードおよびカタログからデリバリーグループにマシンを追加した後に、トラブルシューティング情報を提供します。

ウィザードを使用して既存のマシンを追加すると、コンピューターアカウント名の一覧に、各マシンがカタログに追加するのに適しているかどうかが示されます。各マシンの横にあるアイコンにカーソルを合わせると、そのマシンに関する情報メッセージが表示されます。

メッセージが問題のあるマシンを特定した場合、そのマシンを削除するか、追加します。たとえば、マシンに関する情報が取得できない可能性があることを示すメッセージが表示された場合でも、そのマシンを追加します。

詳細については、以下を参照してください。

- VDA登録のトラブルシューティングガイダンスについては、CTX136668
- VDAのバージョンと機能レベル
- VDA登録方法

MCSカタログ作成の概要

カタログ作成ウィザードで情報を提供した後の、デフォルトのMCSアクションの概要を以下に示します。

- マスターイメージ（スナップショットではない）を選択した場合、MCSはスナップショットを作成します。
- MCSはスナップショットの完全なコピーを作成し、そのコピーをホスト接続で定義されている各ストレージの場所に配置します。
- MCSはマシンをActive Directoryに追加し、一意のIDを作成します。
- MCSは、ウィザードで指定された数のVMを作成し、各VMに2つのディスクを定義します。VMごとに2つのディスクに加えて、マスターも同じストレージ場所に保存されます。複数のストレージ場所が定義されている場合、それぞれに次のディスクタイプが割り当てられます。
    - 作成されたばかりのVM間で共有される、読み取り専用のスナップショットの完全なコピー。
    - 各VMに一意のIDを付与する一意の16 MBのIDディスク。各VMはIDディスクを取得します。
    - VMへの書き込みを保存するための一意の差分ディスク。このディスクは、(ホストストレージがサポートしている場合)シンプロビジョニングされ、必要に応じてマスターイメージの最大サイズまで拡張されます。各VMには差分ディスクが割り当てられます。差分ディスクには、セッション中に加えられた変更が保持されます。専用デスクトップの場合、こ

れは永続的です。プールされたデスクトップの場合、デリバリーコントローラーを介した再起動のたびに削除され、新しいものが作成されます。

あるいは、静的デスクトップを配信するためにVMを作成する際、カタログ作成ウィザードの**マシン**ページで、シック（完全コピー）VMクローンを指定できます。完全クローンは、すべてのデータストアにマスターイメージを保持する必要はありません。各VMは独自のファイルを持っています。

MCSストレージに関する考慮事項

MCSのストレージソリューション、構成、容量を決定する際には、多くの要因があります。以下の情報は、ストレージ容量に関する適切な考慮事項を提供します。

容量に関する考慮事項:

- ディスク

  DeltaまたはDifferencing (Diff) ディスクは、ほとんどのMCS展開において、各VMで最大のスペースを消費します。MCSによって作成される各VMには、作成時に最低2つのディスクが割り当てられます。

  - Disk0 = 差分ディスク: マスターベースイメージからコピーされたOSが含まれます。
  - Disk1 = IDディスク: 16 MB - 各VMのActive Directoryデータを格納します。

  製品の進化に伴い、特定のユースケースや機能の消費を満たすために、さらにディスクを追加する必要がある場合があります。例:

  - MCSストレージ最適化は、各VMのライトキャッシュスタイルのディスクを作成します。
  - MCSは、前のセクションで説明したDeltaディスクのシナリオとは対照的に、フルクローンを使用する機能を追加しました。

  ハイパーバイザーの機能も考慮に入れる必要があるかもしれません。例:

  - XenServer IntelliCacheは、各XenServerのローカルストレージに読み取りディスクを作成します。このオプションにより、共有ストレージの場所に保持されている可能性のあるマスターイメージに対するIOPSを節約できます。

- ハイパーバイザーのオーバーヘッド

  ハイパーバイザーはそれぞれ、VMのオーバーヘッドとなる特定のファイルを使用します。また、ハイパーバイザーは管理および一般的なログ記録操作にもストレージを使用します。オーバーヘッドを含めるためのスペースを計算します。

    - ログファイル
    - ハイパーバイザー固有のファイル。例:
        - VMwareは、**VMストレージ**フォルダーにファイルを追加します。VMwareのベストプラクティスを参照してください。
        - 仮想マシンの合計サイズ要件を計算します。仮想ディスクに20 GB、スワップファイルに16 GB、ログファイルに100 MBを使用し、合計36.1 GBを消費する仮想マシンを考慮してください。
    - XenServerのスナップショット; VMwareのスナップショット。

- プロセスオーバーヘッド

  カタログの作成、マシンの追加、カタログの更新には、それぞれ固有のストレージへの影響があります。例：

    - 初期カタログ作成では、ベースディスクのコピーを各ストレージの場所にコピーする必要があります。
        - また、一時的に準備VMを作成する必要があります。
    - カタログにマシンを追加する場合、ベースディスクを各ストレージの場所にコピーする必要はありません。カタログの作成は、選択された機能によって異なります。
    - カタログを更新すると、各ストレージの場所に余分なベースディスクが作成されます。カタログの更新では、カタログ内の各VMが一定期間2つの差分ディスクを持つため、一時的なストレージのピークも発生します。

その他の考慮事項：

- **RAMサイジング：** I/O最適化ディスク、ライトキャッシュ、スナップショットファイルなど、特定のハイパーバイザーファイルとディスクのサイズに影響します。
- **シンプロビジョニング/シックプロビジョニング:** シンプロビジョニング機能があるため、NFSストレージが推奨されます。

Machine Creation Services (MCS) ストレージ最適化

Machine Creation Services (MCS) ストレージ最適化機能 (MCS I/O と呼ばれる) を使用すると、次のようになります。

- ライトキャッシュコンテナは、Citrix Provisioning と同じ機能である *ファイルベース*です。たとえば、Citrix Provisioning のライトキャッシュファイル名は `D:\vdiskdif.vhdx` で、MCS I/O のライトキャッシュファイル名は `D:\mcsdif.vhdx` です。

- ライトキャッシュディスクに書き込まれたWindowsクラッシュダンプファイルのサポートを含めることで、診断の改善を実現します。
- MCS I/O は、最適な多層書き込みキャッシュソリューションを提供するために、*RAM 内キャッシュとハードディスクへのオーバーフロー*というテクノロジーを保持しています。この機能により、管理者は各層（RAM とディスク）のコストとパフォーマンスのバランスを取り、目的のワークロード要件を満たすことができます。

書き込みキャッシュ方式を *ディスクベース*から *ファイルベース*に更新するには、次の変更が必要です。

1. MCS I/O は、RAMのみのキャッシュをサポートしなくなりました。マシンカタログ作成時にWeb Studioでディスクサイズを指定します。
2. VM の書き込みキャッシュディスクは、VM を初めて起動するときに自動的に作成およびフォーマットされます。VM が起動すると、書き込みキャッシュファイル `mcsdif.vhdx` がフォーマットされたボリューム `MCSWCDisk` に書き込まれます。
3. ページファイルはこのフォーマットされたボリューム `MCSWCDisk` にリダイレクトされます。その結果、このディスクサイズはディスク領域の合計量を考慮します。これには、ディスクサイズと生成されたワークロードの差分に加えて、ページファイルサイズが含まれます。これは通常、VM の RAM サイズに関連付けられます。

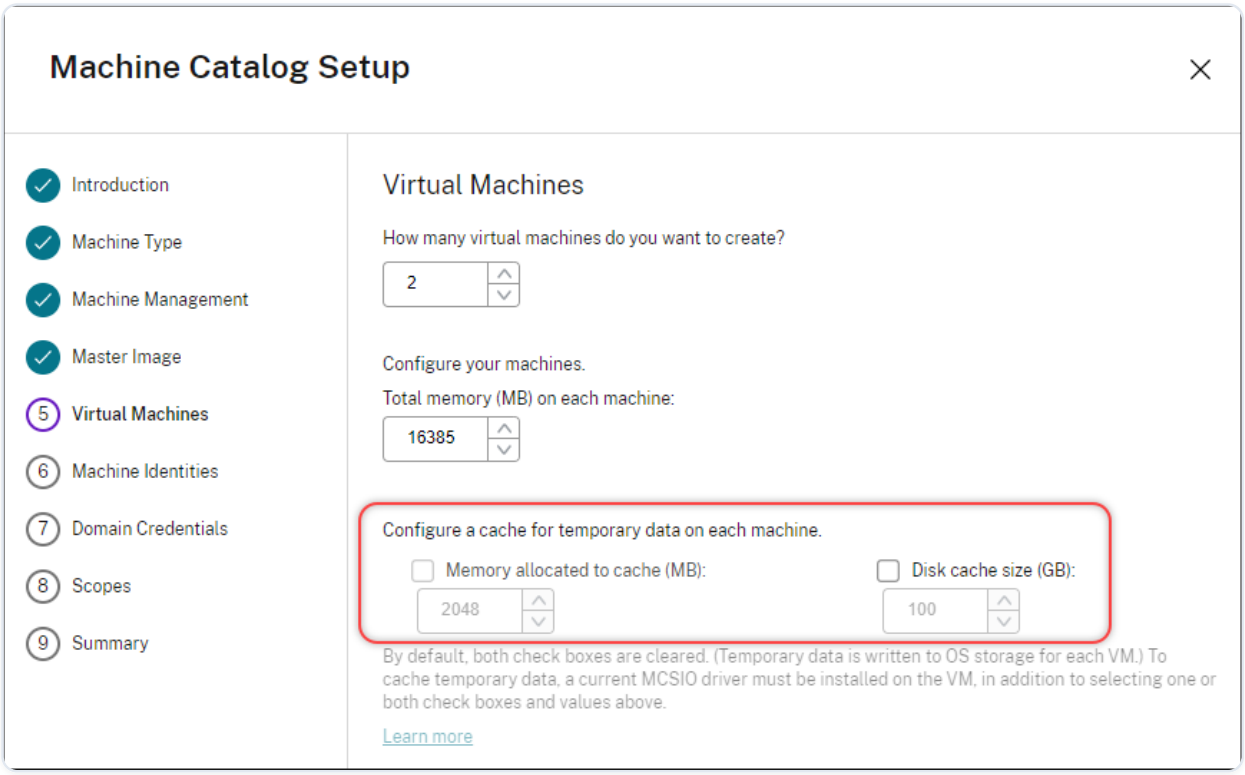
MCSストレージ最適化の更新を有効にする

MCS I/O ストレージ最適化機能を有効にするには、Delivery Controller とVDAを最新バージョンのCitrix Virtual Apps and Desktopsにアップグレードします。

> **注：**
>
> MCS I/O が有効になっている既存の展開をアップグレードする場合、追加の構成は不要です。VDA と Delivery Controller のアップグレードによって MCS I/O のアップグレードが処理されます。

> MCSストレージ最適化の更新を有効にする際は、次の点を考慮してください。

- マシンカタログを作成する際、管理者はRAMとディスクサイズを設定できます。



- 既存のマシンカタログを、バージョン1903用に構成されたVDAを含む新しいVMスナップショットに更新すると、次の動作が発生します。新しいスナップショットは、既存のカタログのMCS I/O設定をRAMとディスクサイズに引き続き使用します。既存の生ディスクはフォーマットされます。

重要:

MCSストレージの最適化は、Citrix Virtual Apps and Desktopsバージョン1903で変更されました。このリリースでは、ファイルベースのライトキャッシュテクノロジーがサポートされており、パフォーマンスと安定性が向上しています。MCS I/Oによって提供される新しい機能は、以前のCitrix Virtual Apps and Desktopsリリースと比較して、より高いライトキャッシュストレージ要件を必要とする場合があります。Citrixは、割り当てられたワークフローと追加のページファイルサイズに十分なディスク容量があることを確認するために、ディスクサイズを再評価することを推奨します。ページファイルサイズは通常、システムRAMの量に関連しています。既存のカタログディスクサイズが不十分な場合は、マシンカタログを作成し、より大きなライトキャッシュディスクを割り当ててください。

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

MCS I/Oライトバックキャッシュディスクに特定のドライブ文字を割り当てることができます。この実装により、使用するアプリケーションのドライブ文字とMCS I/Oライトバックキャッシュディスクのドライブ文字との間の競合を回避できます。MCS I/Oライトバックキャッシュディスクにドライブ文字を割り当てるには、PowerShellコマンドを使用できます。サポートされているハイパーバイザーは、Azure、GCP、VMware、SCVMM、およびXenServerです。

> **注：**
>
> この機能には、VDAバージョン2305以降が必要です。

制限事項

- Windowsオペレーティングシステムのみに適用
- ライトバックキャッシュディスクに適用可能なドライブ文字：`E`から`Z`
- Azure一時ディスクがライトバックキャッシュディスクとして使用されている場合は適用されません
- 新しいマシンカタログを作成する場合にのみ適用されます

ライトバックキャッシュディスクにドライブ文字を割り当てる

ライトバックキャッシュディスクにドライブ文字を割り当てるには：

1. **PowerShell**ウィンドウを開きます。
2. `asnp citrix*`を実行します。
3. まだ作成されていない場合は、IDプールを作成します。
4. プロパティ`WriteBackCacheDriveLetter`を指定して、`New-ProvScheme`コマンドを使用してプロビジョニングスキームを作成します。例：

```
New-ProvScheme -CleanOnBoot `

-HostingUnitName "<name>" `

-IdentityPoolName $schemeName `

-ProvisioningSchemeName $schemeName `
```

```
-InitialBatchSizeHint 1 `

-UseWriteBackCache -WriteBackCacheDiskSize 127
-WriteBackCacheMemorySize 256 -WriteBackCacheDriveLetter E `

-MasterImageVM "XDHyp:\HostingUnits\<name>\image.folder\abcd-
resources.resourcegroup\MCSIOMasterVm_OsDisk_1_d3e2d6352xxxxxxxxx2130aa
145ec77.manageddisk" `

-NetworkMapping @{"0"="XDHyp:\\HostingUnits\\name\
\virtualprivatecloud.folder\\East US.region\
\virtualprivatecloud.folder\\abcd-resources.resourcegroup\\abcd-
resources-vnet.virtualprivatecloud\\default.network"} `

-ServiceOffering "XDHyp:\\HostingUnits\\<name>\\serviceoffering.folder\
\Standard_D2s_v5.serviceoffering" `

-CustomProperties '<CustomProperties xmlns="http://schemas.citrix.com/
2014/xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks"
Value="true" />

<Property xsi:type="StringProperty" Name="OsType" Value="Windows" />

<Property xsi:type="StringProperty" Name="StorageType"
Value="Premium_LRS"/>

<Property xsi:type="StringProperty" Name="PersistWBC" Value="false" />

<Property xsi:type="StringProperty" Name="PersistOsDisk"
Value="false" />

<Property xsi:type="StringProperty" Name="PersistVm" Value="false" />

<Property xsi:type="StringProperty" Name="WBCDiskStorageType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="UseTempDiskForWBC"
Value="false" />

<Property xsi:type="StringProperty" Name="ResourceGroups" Value="abcd-
```

```
group1" />

<Property xsi:type="StringProperty" Name="LicenseType"
Value="Windows_Client" />

<Property xsi:type="StringProperty" Name="SchemaVersion" Value="2" />

</CustomProperties>'
```

5. カタログの作成を完了します。詳細については、`<https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/>`を参照してください。

マスターイメージを準備する

接続ホストの作成については、「」(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/install-configure/connections.html)を参照してください。

マスターイメージには、オペレーティングシステム、仮想化されていないアプリケーション、VDA、およびその他のソフトウェアが含まれています。

知っておくと良いこと:

- マスターイメージは、クローンイメージ、ゴールデンイメージ、ベースVM、またはベースイメージとも呼ばれることがあります。ホストベンダーは異なる用語を使用します。
- ホストに、作成されるマシンの数に対応できる十分なプロセッサ、メモリ、ストレージがあることを確認してください。
- デスクトップとアプリケーションに必要なハードディスク容量を正しく構成してください。この値は後で変更したり、マシンカタログで変更したりすることはできません。
- Remote PC Accessのマシンカタログはマスターイメージを使用しません。

マスターイメージに以下のソフトウェアをインストールして構成します:

- ハイパーバイザー用の統合ツール（Citrix VM Tools、Hyper-V Integration Services、VMware toolsなど）。この手順を省略すると、アプリケーションやデスクトップが正しく機能しない可能性があります。
- VDA。Citrixは、最新機能にアクセスできるように、最新バージョンをインストールすることを推奨します。マスターイメージにVDAをインストールしないと、カタログの作成が失敗します。

- 必要に応じて、アンチウイルスソフトウェアや電子ソフトウェア配布エージェントなどのサードパーティツール。ユーザーとマシンタイプに適した設定（更新機能など）でサービスを構成します。
- 仮想化しないサードパーティアプリケーション。Citrixはアプリケーションの仮想化を推奨します。仮想化により、アプリケーションの追加または再構成後にマスターイメージを更新する必要がなくなるため、コストが削減されます。また、インストールされるアプリケーションが少ないほど、マスターイメージのハードディスクサイズが小さくなり、ストレージコストが節約されます。
- App-Vアプリケーションを公開する予定がある場合は、推奨設定のApp-Vクライアント。App-VクライアントはMicrosoftから入手できます。
- MCSを使用する場合、Microsoft Windowsをローカライズする際は、ロケールと言語パックをインストールしてください。プロビジョニング中にスナップショットが作成されると、プロビジョニングされたVMはインストールされているロケールと言語パックを使用します。

重要:

MCSを使用している場合は、マスターイメージでSysprepを実行しないでください。

マスターイメージを準備するには：

1. ハイパーバイザーの管理ツールを使用してマスターイメージを作成し、オペレーティングシステムとすべてのサービスパックおよび更新プログラムをインストールします。vCPUの数を指定します。PowerShellを使用してマシンカタログを作成する場合は、vCPU値を指定することもできます。Web Studioを使用してカタログを作成する場合、vCPUの数を指定することはできません。デスクトップとアプリケーションに必要なハードディスク容量を構成します。この値は後で変更したり、カタログ内で変更したりすることはできません。
2. ハードディスクがデバイスロケーション0に接続されていることを確認します。ほとんどの標準マスターイメージテンプレートでは、この場所がデフォルトで構成されていますが、一部のカスタムテンプレートではそうでない場合があります。
3. 上記のソフトウェアをマスターイメージにインストールして構成します。
4. MCSを使用していない場合は、アプリケーションとデスクトップがメンバーであるドメインにマスターイメージを参加させます。マシンが作成されるホストでマスターイメージが利用可能であることを確認します。MCSを使用している場合、マスターイメージをドメインに参加させる必要はありません。プロビジョニングされたマシンは、カタログ作成ウィザードで指定されたドメインに参加します。

5. Citrixは、マスターイメージのスナップショットを作成して名前を付けることを推奨します。カタログ作成時にスナップショットではなくマスターイメージを指定した場合、Web Studioはスナップショットを作成します。そのスナップショットに名前を付けることはできません。

ボリュームライセンス認証

MCSは、WindowsオペレーティングシステムとMicrosoft Officeのアクティベーションを自動化および管理するためのボリュームライセンス認証をサポートしています。MCSがボリュームライセンス認証でサポートする3つのモデルは次のとおりです。

- キー管理サービス (KMS)
- Active Directoryベースのアクティベーション (ADBA)
- 複数ライセンス認証キー (MAK)

マシンカタログを作成した後で、アクティベーション設定を変更できます。

キー管理サービス (KMS)

KMSは、専用システムを必要とせず、他のサービスを提供するシステム上で簡単に共同ホストできる軽量サービスです。この機能は、Citrixがサポートするすべてのバージョンでサポートされています。イメージ準備中に、MCSはMicrosoft WindowsおよびMicrosoft Office KMSのリアームを実行します。コマンド `Set-Provserviceconfigurationdata` を実行することでリアームをスキップできます。イメージ準備中のMicrosoft Windows KMSリアームおよびMicrosoft Office KMSリアームの詳細については、Machine Creation Services: Image Preparation Overview and Fault-Findingを参照してください。KMSアクティベーションの詳細については、Key Management Serviceを使用してアクティベートするを参照してください。

> **注：**
>
> コマンド `Set-Provserviceconfigurationdata` の実行後に作成されたすべてのマシンカタログは、コマンドで指定されたものと同じ設定になります。

Active Directoryベースのアクティベーション (ADBA)

ADBAを使用すると、マシンのドメイン接続を介してアクティベートできます。マシンはドメインに参加するとすぐにアクティベートされます。これらのマシンは、ドメインに参加し、ドメインと連絡を取り合っている限り、アクティベートされたままになります。この機能は、Citrixがサポートするすべてのバージョンでサポートされています。Active Directoryベースのアクティ

ベーションの詳細については、「Active Directoryベースのアクティベーション」を参照してください。

マルチプルアクティベーションキー (MAK)

MAKは、Microsoftサーバーの助けを借りて、ボリュームをアクティベートし、Windowsシステムを認証する方法です。MicrosoftからMAKキーを購入する必要があります。このキーには、固定されたアクティベーションカウントが割り当てられています。Windowsシステムがアクティベートされるたびに、アクティベーションカウントが減少します。システムをアクティベートする方法は2つあります。

- オンラインアクティベーション: アクティベートしたいWindowsシステムがインターネットアクセスを持っている場合、製品キーをインストールするとシステムは自動的にWindowsをアクティベートします。このプロセスにより、対応するMAKのアクティベーションカウントが1減少します。
- オフラインアクティベーション: Windowsシステムがオンラインアクティベーションを行うためにインターネットに接続できない場合、MCSはMicrosoftサーバーから確認IDとインストールIDを取得し、Windowsシステムをアクティベートします。このアクティベーション方法は、非永続的なマシンカタログに役立ちます。

> **注：**
>
> - MCSはMAKを使用したMicrosoft Officeのアクティベーションをサポートしていません。
> - 必要なVDAの最小バージョンは2303です。

主な要件

- Delivery Controller はインターネットアクセスが必要です。
- 更新する新しいイメージが元のMAKキーと異なる場合は、新しいカタログを作成します。
- マスターイメージにMAKキーをインストールします。WindowsシステムにMAKキーをインストールする手順については、MAKアクティベーションの展開を参照してください。
- イメージ準備を使用しない場合：

  a. `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform\Activation` の下にレジストリDWORD値 `Manual` を追加します。

  b. 値を `1` に設定します。

アクティベーション数

MAKキーの残りのアクティベーション数を確認したり、VMが2つ以上のアクティベーションを消費しているかどうかを確認したりするには、ボリュームアクティベーション管理ツール (VAMT) を使用します。VAMTのインストールを参照してください。

MAKを使用してWindowsシステムをアクティベートする

MAKを使用してWindowsシステムをアクティベートするには：

1. マスターイメージにプロダクトキーをインストールします。この手順で1つのアクティベーションカウントが消費されます。
2. MCSマシンカタログを作成します。
3. イメージ準備を使用しない場合：

   a. `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform\Activation`の下にレジストリDWORD値`Manual`を追加します。

   b. 値を`1`に設定します。

   この方法では、オンラインアクティベーションのオプションが無効になります。
4. マシンカタログにVMを追加します。
5. VM の電源をオンにします。
6. オンラインアクティベーションかオフラインアクティベーションかに応じて、Windows システムがアクティベートされます。

   - オンラインアクティベーションの場合、プロダクトキーのインストール後に Windows システムがアクティベートされます。
   - オフラインアクティベーションの場合、MCS はプロビジョニングされた VM と通信して Windows システムのアクティベーションステータスを取得します。その後、MCS は Microsoft サーバーから確認 ID とインストール ID を取得します。これらの ID は Windows システムのアクティベーションに使用されます。

トラブルシューティング

プロビジョニングされた VM がインストール済みの MAK キーでアクティベートされない場合は、PowerShell ウィンドウで `Get-ProvVM` または `Get-ProvScheme` コマンドを実行します。

- `Get-ProvScheme` コマンド: 最新のマスターイメージから MCS マシンカタログに関連付けられているパラメーター `WindowsActivationType` を参照してください。

- `Get-ProvVM` コマンド。パラメーター `WindowsActivationType`、`WindowsActivationStatus`、`WindowsActivationStatusErrorCode`、および `WindowsActivationStatusError` を参照してください。

エラーを確認し、問題を解決するための手順を検証できます。

Web Studio を使用してマシンカタログを作成する

カタログを作成する前に:

- このセクションを確認して、選択する項目と提供する情報について学習してください。
- マシンをホストするハイパーバイザー、クラウドサービス、およびその他のリソースへの接続が作成されていることを確認してください。
- マシンをプロビジョニングするためのマスターイメージを作成した場合は、そのイメージに VDA がインストールされていることを確認してください。

カタログ作成ウィザードを開始するには：

1. これが最初に作成するカタログである場合、正しい選択肢（「マシンをセットアップし、アプリとデスクトップを実行するためのマシンカタログを作成する」など）に誘導されます。カタログ作成ウィザードが開きます。
2. すでにカタログを作成済みで、別のカタログを作成したい場合は、次の手順に従います。

    a. Web Studio にサインインし、左側のペインで **Machine Catalogs** を選択し、アクションバーで **Create Machine Catalog** を選択します。

    b. フォルダーを使用してカタログを整理するには、デフォルトの**Machine Catalogs**フォルダーの下にフォルダーを作成します。詳細については、(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/install-configure/machine-catalogs-manage.html#create-a-catalog-folder)を参照してください。

    c. カタログを作成したいフォルダーを選択し、**Create Machine Catalog**をクリックします。カタログ作成ウィザードが開きます。

ウィザードは次の項目について説明します。表示されるウィザードページは、選択内容によって異なります。

オペレーティングシステム

各カタログには、1種類のマシンのみが含まれます。1つ選択してください。

- **マルチセッションOS：** マルチセッションOSカタログは、ホストされた共有デスクトップを提供します。マシンはサポートされているバージョンのWindowsまたはLinuxオペレーティング

システムを実行できますが、カタログに両方を含めることはできません。（そのOSの詳細については、Linux VDAのドキュメントを参照してください。）

- **シングルセッションOS：** シングルセッションOSカタログは、さまざまなユーザーに割り当てることができるVDIデスクトップを提供します。
- **Remote PC Access:** Remote PC Accessカタログは、ユーザーに物理的なオフィスデスクトップマシンへのリモートアクセスを提供します。Remote PC Accessは、セキュリティを提供するためにVPNを必要としません。

マシン管理

このページは、リモートPCアクセス カタログを作成する際には表示されません。

マシン管理ページには、マシンの管理方法と、マシンの展開に使用するツールが示されます。

カタログ内のマシンをWeb Studio経由で電源管理するかどうかを選択します。

- マシンはWeb Studioを介して電源管理されます。たとえば、VMやブレードPCなどです。このオプションは、ホストへの接続をすでに構成している場合にのみ利用可能です。
- マシンはWeb Studioを介して電源管理されません。たとえば、物理マシンなどです。

マシンがWeb Studioを介して電源管理されることを指定した場合は、VMの作成に使用するツールを選択します。

- **Citrix Provisioning テクノロジー**
  - **Citrix Machine Creation Services (MCS)** MCSを使用してプロビジョニングおよびイメージ化されたVMのカタログを作成します。MCSは、マスターイメージからクローンされたイメージをこれらのVMにコピーします。
  - **Citrix Provisioning Services (PVS)** MCSを使用してプロビジョニングされ、PVSを使用してイメージ化されたVMのカタログを作成します。これらのVMはPVSターゲットデバイスとして機能し、PVSサーバーは単一の共有ディスクイメージをそれらにストリーミングできます。

> **注：**
>
> このオプションは、Citrix Cloud™に登録されているPVSサイトでのみ利用可能であり、現在、Azureリソースに限定されています。

- **その他のサービスまたはテクノロジー** データセンターにすでに存在するマシンを管理するツール。Citrixでは、カタログ内のマシンの一貫性を確保するために、Microsoft System Center Configuration Managerまたはその他のサードパーティ製アプリケーションを使用することをお勧めします。

デスクトップの種類（デスクトップエクスペリエンス）

このページは、シングルセッションOSマシンを含むカタログを作成している場合にのみ表示されます。

デスクトップエクスペリエンスページでは、ユーザーがログオンするたびに何が起こるかを決定します。次のいずれかを選択します。

- ユーザーはログオンするたびに新しい（ランダムな）デスクトップに接続します。
- ユーザーはログオンするたびに同じ（静的な）デスクトップに接続します。

イメージとマシンプロファイル

このページは、MCSを使用してVMを作成している場合にのみ表示されます。

1. マシンカタログのイメージの種類を選択し、次にイメージを選択します。2種類のイメージが利用可能です。

   - **マスターイメージ。** イメージ準備プロセスをまだ経ていないイメージです。イメージ準備プロセスは、カタログ作成が開始されると自動的に開始されます。

     > **注：**
     >
     > - MCSを使用している場合、マスターイメージでSysprepを実行しないでください。
     > - スナップショットではなくマスターイメージを指定した場合、Web Studioはスナップショットを作成しますが、名前を付けることはできません。

   - **準備済みイメージ。** イメージ準備プロセスを経たイメージで、VM作成に直接使用できます。カタログ作成時にマスターイメージではなく準備済みイメージを選択すると、より高速で信頼性の高いマシンカタログ作成が保証され、イメージライフサイクル管理が合理化されます。

> **注：**
>
> - 準備されたイメージを使用して作成されたVMは、ハイバネーションをサポートしていません。
> - 現在、準備されたイメージを使用してカタログを作成することは、AzureおよびVMware環境でのみ利用可能です。

準備されたイメージの作成方法の詳細については、Image management (preview)を参照してください。

イメージを選択する際、必要に応じて、選択したイメージにメモを追加できます。

最新の製品機能を使用できるようにするには、マスターイメージに最新のVDAバージョンがインストールされていることを確認してください。デフォルトの最小VDA選択を変更しないでください。ただし、以前のVDAバージョンを使用する必要がある場合は、VDA versions and functional levelsを参照してください。

ウィザードで以前に選択したマシン管理テクノロジーと互換性のないスナップショットまたはVMを選択すると、エラーメッセージが表示されます。

2. 既存のVMをマシンプロファイルとして使用するには、**Use a machine profile**を選択し、その後、VMを選択します。

> **注：**
>
> 現在、マシンプロファイルの使用は、Azure、AWS、GCP、およびVMware VMに限定されています。

> VMware展開の場合、マシンプロファイルを使用してマシンカタログを作成する際、仮想マシンを保持するフォルダーを指定する必要があります。

仮想マシンフォルダーの場所を指定するには、カタログ作成ウィザードで**Virtual Machines**ページに移動し、**Select a folder to place the machines**セクションに移動して仮想マシンフォルダーの場所を選択します。指定されていない場合、システムは選択されたマシンプロファイルのフォルダーをデフォルトの場所と見なします。

3. カタログの最小機能レベルを選択します。最新の製品機能を使用できるようにするには、マスターイメージに最新のVDAバージョンがインストールされていることを確認してください。

マシン

Remote PC Accessカタログを作成している場合、このページは表示されません。

このページのタイトルは、**Machine Management**ページで選択した内容によって異なります: **Machines**、**Virtual Machines**、または**VMs and users**。

MCSを使用する場合:

- 作成する仮想マシンの数を指定します。作成しない場合は**0**（ゼロ）を入力します。後で、**Add machines**を実行して、空のカタログにVMを作成できます。
- 各 VM が持つメモリ量 (MB 単位) を選択します。
- 作成された各VMにはハードディスクがあります。そのサイズはマスターイメージで設定されます。カタログでハードディスクのサイズを変更することはできません。
- 展開に複数のゾーンが含まれている場合、カタログのゾーンを選択できます。
- 静的デスクトップVMを作成する場合は、仮想マシンコピーモードを選択します。詳細については、「仮想マシンコピーモード」を参照してください。
- vDiskを使用しないランダムデスクトップVMを作成する場合は、各マシンの一時データに使用するキャッシュを構成できます。詳細については、「一時データ用のキャッシュの構成」を参照してください。

他のツールを使用する場合:

Active Directoryマシンアカウント名を追加（またはリストをインポート）します。VMを追加/インポートした後で、そのVMのActive Directoryアカウント名を変更できます。**デスクトップエクスペリエンス**ページで静的マシンを指定した場合、追加する各VMのActive Directoryユーザー名をオプションで指定できます。

名前を追加またはインポートした後、このページにいる間は、**削除**ボタンを使用してリストから名前を削除できます。

他のツールを使用する場合（ただしMCSではない場合）:

追加（またはインポート）された各マシンに表示されるアイコンとツールヒントは、カタログに追加できない可能性のあるマシンや、Delivery Controllerに登録できないマシンを特定するのに役立ちます。詳細については、「VDAのバージョンと機能レベル」を参照してください。

仮想マシン作成時にSIDを追加する

新しい仮想マシンを作成する際に、マシンを一意に識別するためにパラメーター`ADAccountSid`を追加できるようになりました。

これを行うには：

1. サポートされているIDタイプでカタログを作成します。
2. `NewProvVM` を使用してカタログにマシンを追加します。例：

```
New-ProvVM  -ProvisioningSchemeName "name"  -ADAccountSid @("SID ")  -
RunAsynchronously
```

ただし、次の条件のいずれかに該当するマシンをプロビジョニングすることはできません。

- カタログIDプールにないADアカウント
- 利用可能な状態ではないADアカウント

仮想マシンのコピーモード

マシンページで指定するコピーモードによって、MCSがマスターイメージからシン（高速コピー）クローンを作成するか、シック（完全コピー）クローンを作成するかが決まります。(デフォルト = シンクローン)

- ストレージをより効率的に使用し、マシンの作成を高速化するには、高速コピーのクローンを使用します。
- マシン作成後のIOPSを削減できる可能性があり、より優れたデータ回復と移行サポートのために、完全コピーのクローンを使用します。

VDAのバージョンと機能レベル

カタログの機能レベルは、カタログ内のマシンで利用できる製品機能を制御します。新しい製品バージョンで導入された機能を使用するには、新しいVDAが必要です。機能レベルを設定すると、そのバージョンで導入されたすべての機能（および機能レベルが変更されない場合はそれ以降のバージョンで導入された機能）がカタログ内のマシンで利用可能になります。ただし、以前のVDAバージョンを使用しているカタログ内のマシンは登録できません。

マシン（または**デバイス**）ページの下部にあるメニューで、最小VDAレベルを選択できます。これにより、カタログの最小機能レベルが設定されます。デフォルトでは、オンプレミス展開の場合、最新の機能レベルが選択されます。Citrixの推奨に従って、常にVDAとコアコンポーネントを最新バージョンにインストールおよびアップグレードする場合は、この選択を変更する必要はありません。ただし、古いVDAバージョンを使い続ける必要がある場合は、正しい値を選択してください。

Citrix Virtual Apps and Desktopsのリリースには、新しいVDAバージョンが含まれていない場合や、新しいVDAが機能レベルに影響を与えない場合があります。そのような場合、機能レベルは、インストールまたはアップグレードされたコンポーネントよりも古いVDAバージョンを示すことがあります。各リリースの新機能の記事には、デフォルトの機能レベルの変更が示されています。

選択された機能レベルは、その上のマシンリストに影響します。リストでは、各エントリの横にあるツールヒントが、その機能レベルでマシンのVDAがカタログと互換性があるかどうかを示します。

各マシンのVDAが選択された最小機能レベルを満たしていないか、超えていない場合、ページにメッセージが表示されます。ウィザードを続行できます。これらのマシンは、後でControllerに登録できない可能性があります。または、次のことができます。

- 古いVDAを含むマシンをリストから削除し、VDAをアップグレードしてから、カタログに再度追加します。
- 最新の製品機能へのアクセスを妨げる、より低い機能レベルを選択します。

マシンタイプが誤っているためにカタログに追加されなかった場合も、メッセージが表示されます。例としては、サーバーをシングルセッションOSカタログに追加しようとする場合や、ランダム割り当て用に作成されたシングルセッションOSマシンを静的マシンのカタログに追加する場合などがあります。

重要:

リリース1811で、追加の機能レベルとして **1811 (またはそれ以降)** が追加されました。このレベルは、将来のCitrix Virtual Apps and Desktops機能で使用することを目的としています。**7.9 (またはそれ以降)** の選択はデフォルトのままです。このデフォルトは、現在のすべての展開で有効です。

1811 (またはそれ以降) を選択した場合、そのカタログ内の以前のVDAバージョンはControllerに登録できません。ただし、カタログにバージョン1811以降のサポートされているVDAのみが含まれている場合、それらはすべて登録の対象となります。これには、バージョン1903および現在のリリース以前の他の19XXリリースを含む、後のCitrix Virtual Apps and Desktopsリリース用に構成されたVDAを含むカタログが含まれます。

一時データのキャッシュを構成する

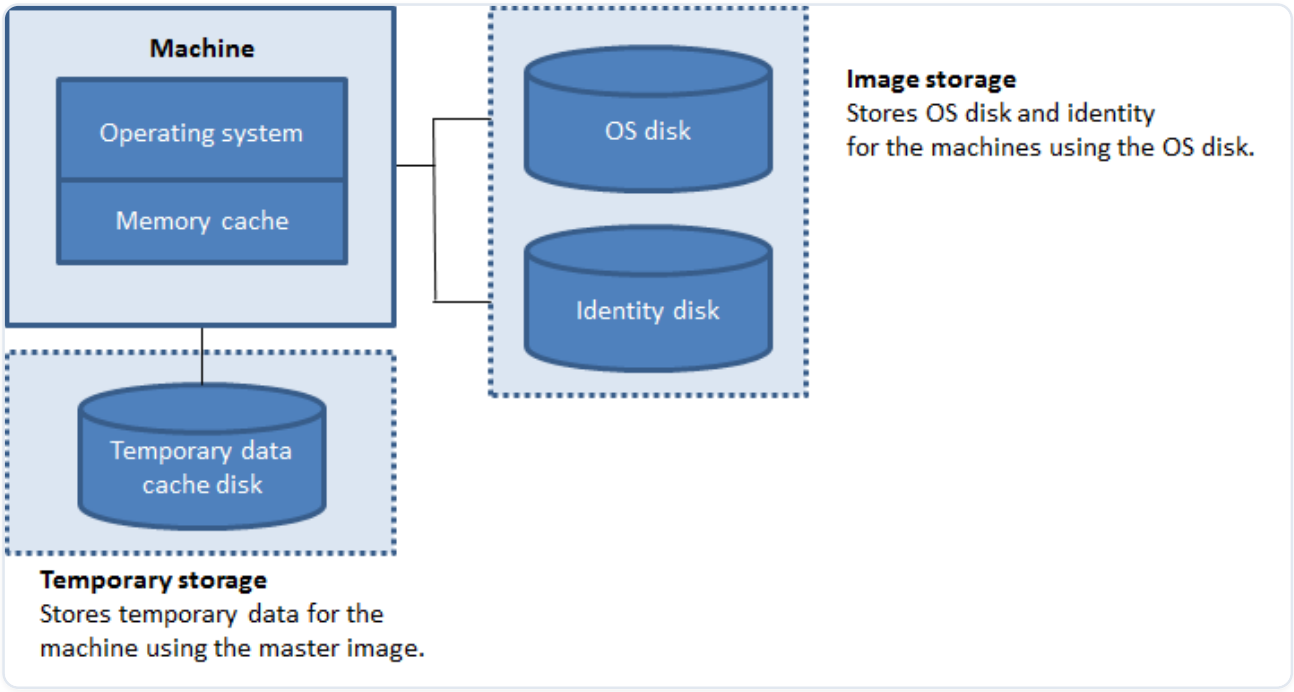
VMに一時データをローカルでキャッシュすることはオプションです。MCSを使用してカタログ内のプールされた（専用ではない）マシンを管理する場合、マシン上の一時データキャッシュの使用を有効にできます。カタログが一時データ用のストレージを指定する接続を使用している場合、カタログ作成時に一時データキャッシュ情報を有効にして構成できます。

重要:

この機能には、現在のMCS I/Oドライバーが必要です。このドライバーのインストールは、VDAをインストールまたはアップグレードする際のオプションです。デフォルトでは、このドライバーはインストールされません。

カタログが使用する接続を作成するときに、一時データが共有ストレージを使用するかローカルストレージを使用するかを指定します。詳細については、「接続とリソース」を参照してください。各マシンの一時データキャッシュを構成するには、次の2つのオプションを使用できます。**キャッシュに割り当てられるメモリ (MB)** と **ディスクキャッシュサイズ (GB)** 。デフォルトでは、これら2つのオプションはオフになっています。キャッシュに割り当てられるメモリ (MB) オプションを有効にするには、ディスクキャッシュサイズ (GB) チェックボックスをオンにします。**ディスクキャッシュサイズ** チェックボックスが選択されていない場合、**キャッシュに割り当てられるメモリ** オプションはグレー表示されます。接続タイプによっては、これらのオプションのデフォルト値が異なる場合があります。一般的に、デフォルト値はほとんどの場合で十分です。ただし、次のものに必要な領域を考慮してください。

- Windows自体によって作成される一時データファイル（Windowsページファイルを含む）。
- ユーザープロファイルデータ。
- ユーザーのセッションに同期されるShareFileデータ。
- セッションユーザーによって作成またはコピーされる可能性のあるデータ、またはユーザーがセッション内にインストールする可能性のあるアプリケーション。



各マシンの一時データキャッシュを構成するには、次の3つのシナリオに注意してください。

- ディスクキャッシュサイズチェックボックスとキャッシュに割り当てられるメモリチェックボックスを選択しない場合、一時データはキャッシュされません。各VMの差分ディスク（OSストレージ内）に直接書き込まれます。（これはバージョン7.8以前のプロビジョニングアクションです。）
- ディスクキャッシュサイズチェックボックスとキャッシュに割り当てられるメモリチェックボックスを選択した場合、一時データは最初にメモリキャッシュに書き込まれます。メモリキャッシュが構成された制限（キャッシュに割り当てられるメモリの値）に達すると、最も古いデータは一時データキャッシュディスクに移動されます。

重要:

- ディスクキャッシュの容量が不足すると、ユーザーセッションは使用できなくなります。
- Nutanixホスト接続を使用している場合、この機能は利用できません。
- マシン作成後、マシンカタログ内のキャッシュ値を変更することはできません。

注：

- ディスクキャッシュのみでメモリキャッシュなしでライトバックキャッシュを構成することは非推奨になりました。一時データ用のキャッシュを有効にするには、**ディスクキャッシュサイズ (GB)** と **キャッシュに割り当てられるメモリ (MB)** の両方を選択し、メモリキャッシュに0より大きいサイズを指定することをお勧めします。
- メモリキャッシュは、各マシンの総メモリ量の一部です。したがって、「キャッシュに割り当てられたメモリ」オプションを有効にする場合は、各マシンの総メモリ量を増やすことを検討してください。
- ディスクキャッシュサイズをデフォルト値から変更すると、パフォーマンスに影響を与える可能性があります。サイズは、ユーザーの要件とマシンにかかる負荷に合わせる必要があります。

NIC

このページは、リモートPCアクセス カタログを作成する際には表示されません。

ネットワークインターフェイスカードページで、複数のNICを使用する予定がある場合は、各カードに仮想ネットワークを関連付けます。たとえば、特定のセキュアネットワークにアクセスするために1つのカードを割り当て、より一般的に使用されるネットワークにアクセスするために別のカードを割り当てることができます。このページからNICを追加または削除することもできます。

マシンアカウント

このページは、リモートPCアクセス カタログを作成する場合にのみ表示されます。

マシンアカウントページで、ユーザーまたはユーザーグループに対応する追加するActive Directoryマシンアカウントまたは組織単位（OU）を指定します。OU名にスラッシュ（/）を使用しないでください。

OUを追加する際、ドメインがリストに表示されない場合は、次のことができます。

- 完全一致で検索します。
- すべてのドメインを参照して見つけます。

以前に構成した電源管理接続を選択するか、電源管理を使用しないことを選択できます。電源管理を使用したいが、適切な接続がまだ構成されていない場合は、後でその接続を作成し、マシンカタログを編集して電源管理設定を更新できます。

マシンID

このページは、MCSを使用してVMを作成する場合にのみ表示されます。

カタログ内の各マシンには一意のIDが必要です。このページでは、カタログ内のマシンのIDを構成できます。マシンはプロビジョニング後にIDに結合されます。カタログ作成後にIDの種類を変更することはできません。

このページで設定を構成するための一般的なワークフローは次のとおりです。

1. リストからIDを選択します。
2. アカウントを作成するか既存のアカウントを使用するか、およびそれらのアカウントの場所（ドメイン）を指定します。

次のいずれかのオプションを選択できます。

- **オンプレミスActive Directory**。組織が所有し、その組織に属するActive Directoryアカウントでサインインするマシン。これらはオンプレミスに存在します。
- **ハイブリッドAzure Active Directory参加済み**。組織が所有し、その組織に属するActive Directory Domain Servicesアカウントでサインインするマシン。これらはクラウドとオンプレミスに存在します。要件、制限、および考慮事項については、「ハイブリッドAzure Active Directory参加済み」を参照してください。

> **注：**
>
> - ハイブリッド Azure Active Directory 参加を使用する前に、Azure 環境が前提条件を満たしていることを確認してください。`<https://docs.microsoft.com/ja-jp/azure/active-directory/devices/hybrid-azuread-join-managed-domains>`を参照してください。
> - このオプションでは、マスターイメージがオペレーティングシステムの前提条件を満たしている必要があります。詳細については、Microsoft のドキュメントを参照してください: `<https://learn.microsoft.com/ja-jp/azure/active-directory/devices/concept-azure-ad-join-hybrid>`。

> **重要:**
>
> - IDの種類として**オンプレミスActive Directory**または**ハイブリッドAzure Active Directory参加済み**を選択した場合、カタログ内の各マシンには対応するActive Directoryコンピューターアカウントが必要です。

> アカウントを作成する場合、マシンが存在するOUにコンピューターアカウントを作成する権限が必要です。カタログ内の各マシンは一意の名前を持つ必要があります。作成するマシンのアカウント命名スキームを指定します。詳細については、マシンアカウントの命名スキームを参照してください。

> **注：**
>
> OU名にスラッシュ（`/`）を使用しないようにしてください。

> 既存のアカウントを使用する場合は、アカウントを参照するか、**インポート**をクリックしてアカウント名を含む.csvファイルを指定します。インポートするファイルの内容は、次の形式を使用する必要があります。

- ADcomputeraccountname.domain

追加するすべてのマシンに対して十分なアカウントがあることを確認してください。Web Studioインターフェイスがそれらのアカウントを管理します。したがって、そのインターフェイスですべてのアカウントのパスワードをリセットできるようにするか、すべてのアカウントで同じパスワードを指定してください。

物理マシンまたは既存のマシンを含むカタログの場合、既存のアカウントを選択またはインポートし、各マシンをActive Directoryコンピューターアカウントとユーザーアカウントの両方に割り当てます。

マシンアカウントの命名規則

カタログ内の各マシンには、一意の名前が必要です。カタログを作成する際には、マシンアカウントの命名規則を指定する必要があります。名前に表示される連番または文字のプレースホルダーとして、ワイルドカード（ハッシュマーク）を使用します。

命名スキームを指定する際は、以下の規則に注意してください。

- 命名スキームには少なくとも1つのワイルドカードを含める必要があります。すべてのワイルドカードはまとめて配置する必要があります。
- ワイルドカードを含む名前全体は、2文字以上15文字以下である必要があります。少なくとも1つの非数字文字と1つの#（ワイルドカード）文字を含める必要があります。
- 名前にスペースや次の文字を含めることはできません: `,~!@'$%\^&.()}{\/*?"<>|=+[];:_".`。

- 名前をハイフン（-）で終わらせることはできません。

また、命名スキームを指定する際は、将来の拡張のために十分なスペースを確保してください。例を挙げます。「veryverylong#」というスキームで1,000個のマシンアカウントを作成した場合、最後に作成されるアカウント名（veryverylong1000）は16文字になります。したがって、この命名スキームでは、最大15文字を超えるマシン名が1つ以上生成されます。

シーケンシャル値が数字（0-9）か文字（A-Z）かを示すことができます。

- **0-9**。選択した場合、指定されたワイルドカードは連番に解決されます。

> **注：**
>
> ワイルドカードが1つの場合、アカウント名は1から始まります。2つの場合、アカウント名は01から始まります。3つの場合、アカウント名は001から始まります。以降も同様です。

- **A-Z**。選択した場合、指定されたワイルドカードは連続する文字に解決されます。

例えば、PC-Sales-## (**0-9** が選択されている場合) という命名スキームでは、PC-Sales-01、PC-Sales-02、PC-Sales-03 などのアカウントが作成されます。

オプションで、アカウント名の開始文字を指定できます。

- **0-9** を選択すると、アカウントは指定された数字から順に命名されます。前のフィールドで使用するワイルドカードの数に応じて、1桁以上の数字を入力します。たとえば、2つのワイルドカードを使用する場合は、2桁以上の数字を入力します。
- **A-Z** を選択すると、アカウントは指定された文字から順に命名されます。前のフィールドで使用するワイルドカードの数に応じて、1文字以上の文字を入力します。たとえば、2つのワイルドカードを使用する場合は、2文字以上の文字を入力します。

ドメイン資格情報

資格情報の入力を選択し、ターゲットのActive Directoryドメインでアカウント操作を実行する権限を持つ管理者の資格情報を入力します。

名前の確認オプションを使用して、ユーザー名が有効か一意であるかを確認します。このオプションは、たとえば次のような場合に役立ちます。

- 複数のドメインに同じユーザー名が存在する場合。目的のユーザーを選択するよう求められます。

- ドメイン名を思い出せない場合。ドメイン名を指定せずにユーザー名を入力できます。チェックが成功すると、ドメイン名が自動的に入力されます。

> **注：**
>
> **マシンID**で選択したIDの種類が**ハイブリッドAzure Active Directory参加済み**の場合、入力する資格情報には`Write userCertificate`権限が付与されている必要があります。

概要、名前、および説明

「**概要**」ページで、指定した設定を確認します。カタログの名前と説明を入力します。この情報はWeb Studioに表示されます。

完了したら、**「完了」をクリックしてカタログの作成を開始します。 完了したら、**「完了」**を選択してカタログの作成を開始します。

マシンカタログに、新しいカタログがインラインの進行状況バーとともに表示されます。

作成の進行状況の詳細を表示するには：

1. マシンカタログにマウスを合わせます。
2. 表示されるツールヒントで、**詳細の表示**をクリックします。

   以下の内容を確認できる段階的な進行状況グラフが表示されます。

   - 手順の履歴
   - 現在のステップの進行状況と実行時間
   - 残りのステップ

MCSの時刻同期

時刻同期は、マスターイメージと、参加しているマシンIDカタログのタイプによって決定されます。マスターイメージとカタログに応じて、次の時刻同期方法が適用されます。

マスターイメージ	カタログ	結果の時刻同期方法
NDJ	ADまたはハイブリッドAzure AD	デフォルトではNT5DSです。マスターイメージのレジストリ設定を使用して、MCSが時

マスターイメージ	カタログ	結果の時刻同期方法
		刻同期設定を変更するのを無効にできます。
NDJ	NDJまたはAzure AD	元の時刻同期設定と同じ
ADまたはハイブリッドAzure AD	ADまたはハイブリッドAzure AD	元の時刻同期設定と同じ
アジュール AD	アジュール AD	元の時刻同期設定と同じ

注：

元の時刻同期は、以下のレジストリ設定によって制御されており、変更できません。

- Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Config

値: MaxAllowedPhaseOffset、MaxNegPhaseCorrection、およびMaxPosPhaseCorrection

- Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Parameters

値: Type

MCSが時刻同期設定を変更しないようにするには、マスターイメージで以下のレジストリ設定の値を設定します。

- `Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix`
- 名前: TimeSyncMethodKeep
- 種類: DWORD
- 0 (または、値TimeSyncMethodKeepが構成されていない場合): 元の時刻同期設定を保持しません。
- 1: 元の時刻同期設定とデフォルトのパラメーター値を保持します。

カスタムプロパティの設定に関する重要な考慮事項

GCPおよびAzure環境では、カスタムプロパティを`New-ProvScheme`と`Set-ProvScheme`で正しく設定する必要があります。存在しないカスタムプロパティを指定すると、次のエラーメッセージが表示され、コマンドは実行に失敗します。

- Azureの場合: `Invalid property found: <invalid property>. Ensure that the CustomProperties parameter supports the property.`.
- GCPの場合: `Invalid property found: <invalid property>. Ensure that the value supplied for the property is supported in the Hypervisor.`.

トラブルシューティング

> **重要:**

> Web Studio を使用してマシンカタログを作成した後、`Get-ProvTask` PowerShell コマンドを使用して、マシンカタログ作成に関連するタスクを取得することはできません。この制限は、カタログが正常に作成されたかどうかにかかわらず、Web Studio がマシンカタログ作成後にそれらのタスクを削除するためです。

> Citrix は、サポートチームが解決策を提供できるよう、ログを収集することをお勧めします。Citrix Provisioning を使用している場合は、次の手順でログファイルを生成します。

1. マスターイメージで、値 1 (DWORD (32 ビット) 値として) を持つ次のレジストリキーを作成します: `HKLM\Software\Citrix\MachineIdentityServiceAgent\LOGGING`。
2. マスターイメージをシャットダウンし、スナップショットを作成します。
3. Delivery Controller で、次の PowerShell コマンドを実行します: `Set-ProvServiceConfigurationData -Name ImageManagementPrep_NoAutoShutdown -Value $True`。
4. そのスナップショットに基づいてカタログを作成します。
5. ハイパーバイザー上に準備 VM が作成されたら、ログインして `C:\` のルートから次のファイル (Image-prep.log および PvsVmAgentLog.txt) を抽出します。
6. マシンをシャットダウンすると、その時点で障害が報告されます。
7. イメージ準備マシンの自動シャットダウンを再度有効にするには、次の PowerShell コマンドを実行します: `Remove-ProvServiceConfigurationData -Name ImageManagementPrep_NoAutoShutdown`。

イメージ準備に関する問題

MCS は単一のイメージから多数のマシンを作成するため、すべてのマシンが一意であり、正しくライセンスされていることを保証するためにいくつかの手順が実行されます。イメージ準備はカタログ作成プロセスの一部です。この準備により、プロビジョニングされたすべてのマシンが一意の IP アドレスを持ち、KMS サーバーに一意のインスタンスとして正しく通知されることが保証されます。MCS 内では、マスターイメージのスナップショットを選択した後にイメージ準備が行われます。カタログが選択されたマシンから自身を分離できるようにコピーが作成されます。元の VM に基づいて、ネットワーク接続が切断された *準備* VM が作成されます。ネットワーク接続を切断することで、他のマシンとの競合を防ぎ、準備された VM が新しくコピーされたディスクにのみ接続されるようにします。

イメージ準備を実行するために必要な手順を含む小さな *指示* ディスクが、準備された VM に接続されます。この準備された VM が起動し、イメージ準備プロセスが開始されます。イメージ準備には、次のプロセスが含まれます。

- DHCP を有効にします。DHCP を有効にすると、プロビジョニングされたマシンが IP アドレスの競合を引き起こさないことが保証されます。DHCP はすべてのネットワークカードで有効になります。
- Microsoft Windows KMS の再アーム。KMS を再アームすると、Microsoft Windows が正しくライセンスされていることが保証されます。再アームされた OS が呼び出され、KMS ライセンスサーバーに新しいインスタンスとして正しく報告されます。
- Microsoft Office KMS の再アーム (Microsoft Office がインストールされている場合)。Microsoft Office を再アームすると、Microsoft Office の任意のバージョン (2010 以降) が KMS サーバーに正しく登録されることが保証されます。Microsoft Office の再アームが呼び出されると、KMS ライセンスサーバーに新しいインスタンスとして報告されます。

> **ヒント:**

> イメージ準備プロセスが完了すると、命令ディスクはハイパーバイザーから取得されます。ハイパーバイザーには、イメージ準備プロセスから収集された情報が含まれています。

> イメージ準備段階が失敗する理由はさまざまです。次のような失敗メッセージが表示されます: Image Preparation Office Rearm Failed.

これらの失敗については、以下のセクションで説明します。

DHCPを有効にする

これらの失敗は、静的IPアドレスをサポートしないネットワークカードが原因で発生します。たとえば、Dell SonicWallネットワークカードの以前のバージョンなどです。SonicWallカードはファイアウォールネットワークカードであるため、カードをDHCPに設定しても意味がありません。これはDHCPのみをサポートしているためです。これはCitrix Virtual Apps and Desktopsの後のバージョンで修正されました。ただし、他の種類のネットワークカードでこの問題が見られる場合は、フォーラムまたはサポート担当者を通じてCitrixに報告する必要があります。

> **注：**
>
> 以下の例のこのPowerShell設定は、Citrix Virtual Apps and Desktopsサイトに適用されるため、すべての新しいカタログと既存のカタログに対して実行されるイメージ更新に影響します。

> 他のネットワークカードでこの問題が発生した場合は、Delivery ControllerでPowerShellコマンドを実行することで解決できます。

```
Set-ProvServiceConfigurationData -Name ImageManagementPrep_Excluded_Steps -Value EnableDHCP
```

Microsoft Officeの再アクティブ化

Microsoft Officeの再アクティブ化段階で発生する可能性のあるKMS再アクティブ化の失敗はさまざまです。主な失敗は次のとおりです。

- 一部のMicrosoft Officeランタイム、たとえば **Access Runtime** は、Officeの再アクティブ化を呼び出し、失敗の原因となることがあります。
- Microsoft OfficeのKMSバージョンがインストールされていません。
- 再アクティブ化回数が上限を超えました。

エラーが誤検知である場合は、Delivery Controllerで次のPowerShellコマンドを実行することで解決できます。

```
Set-ProvServiceConfigurationData -Name ImageManagementPrep_Excluded_Steps -Value OfficeRearm
```

Microsoft Windowsの再アクティブ化

Microsoft Windowsの再アクティブ化段階で発生する可能性のあるKMSの失敗はさまざまです。主な失敗は次のとおりです。

- インストールされている Windows のバージョンが KMS を使用してアクティブ化されていません。たとえば、MAK (Multiple Activation Key) を使用しています。
- リアーム回数を超過しました。

Microsoft Windows のバージョンが正しくライセンスされている場合は、Delivery Controller で次の PowerShell コマンドを実行して OS のリアームをクリアできます。

```
Set-ProvServiceConfigurationData -Name ImageManagementPrep_Excluded_Steps -Value OsRearm
```

完全な失敗の事例

イメージ準備マシンは設計上ネットワークに接続されていないため、イメージ準備段階では完全な失敗しか報告できない場合があります。この失敗タイプの例は次のとおりです: マスター VM イメージの準備に失敗しました。選択したイメージにサポートされている OS (Windows 7 など) と正しいバージョンの VDA (7.0 以降) がインストールされていることを確認してください。

完全な失敗の主な原因は次のとおりです。

VIRTUAL DELIVERY AGENT (VDA) がインストールされていない、または VDA バージョン 5.X がインストールされている

マスターイメージに VDA 7.x がインストールされていない場合、イメージ準備は 20 分後にタイムアウトし、上記のエラーを報告します。これは、イメージ準備段階を実行して成功または失敗を報告するためのソフトウェアがマスターイメージにインストールされていないためです。これを解決するには、マスターイメージとして選択されたスナップショットに VDA (最小バージョン 7) がインストールされていることを確認してください。

`DISKPART SAN` ポリシー

マスターイメージに設定されている `DISKPART SAN` ポリシーが原因で、イメージ準備段階全体が失敗する可能性があります。イメージ準備指示ディスクをオンラインにするように設定されていない場合、マシンはシャットダウンされ、イメージ準備は 20 分後に失敗を報告します。マスターイメージでこれを確認するには、次のコマンドを実行します。

```
C:\>; Diskpart.exe

DISKPART>; San
```

このコマンドは現在のポリシーを返します。*Online All* でない場合は、次のコマンドを実行して変更します。

```
DISKPART>; San policy=OnlineAll
```

マスターイメージをシャットダウンし、そのマシンのスナップショットを作成してから、それをベース MCS イメージとして使用します。

イメージ準備が別の理由で失敗した場合

イメージ準備が失敗し、明確な失敗理由がない場合、MCS カタログの作成時にイメージ準備プロセスをバイパスできます。ただし、このプロセスをバイパスすると、サイトで KMS ライセンスとネットワーク (DHCP) の問題が発生する可能性があります。次の PowerShell コマンドを使用します。

```
Set-ProvServiceConfigurationData -Name
ImageManagementPrep_DoImagePreparation -Value $false
```

可能な場合は常に、Citrix サポートチームのためにログを収集してください。フォーラムまたはサポート担当者を通じて Citrix に問題を報告してください。ログを収集するには:

1. マスターイメージ上で、値1（「DWORD (32-bit) value」として）を持つ以下のレジストリキーを作成します。`HKLM\Software\Citrix\MachineIdentityServiceAgent\LOGGING`。
2. マスターイメージをシャットダウンし、スナップショットを作成します。Delivery Controllerで、Citrix PowerShellスナップインをロードした状態でPowerShellを起動し、`Set-ProvServiceConfigurationData -Name ImageManagementPrep_NoAutoShutdown -Value $True`を実行します。
3. そのスナップショットに基づいてカタログを作成します。
4. ハイパーバイザー上に準備VMが作成されたら、ログインしてC:\のルートから抽出します。

```
Image-prep.log

PvsVmAgentLog.txt
```

マシンをシャットダウンします。この時点で、障害が報告されます。

イメージ準備マシンの自動シャットダウンを再度有効にするには、以下のPowerShellコマンドを実行します。

`Remove-ProvServiceConfigurationData -Name` `ImageManagementPrep_NoAutoShutdown`

次のステップ

特定のクラウドサービスカタログの作成については、以下を参照してください。

- AWS カタログを作成する

- XenServerカタログを作成する
- Google Cloud Platform カタログを作成する
- Microsoft Azure カタログを作成する
- Microsoft System Center Virtual Machine Manager カタログを作成する
- Nutanix カタログを作成する
- VMwareカタログを作成する

これが最初に作成するカタログである場合、Web Studioはデリバリーグループの作成を案内します。

設定プロセス全体を確認するには、インストールと構成を参照してください。

Web StudioとPowerShellを使用してCitrix Provisioningカタログを作成できます。 この実装には、次の利点があります。

- MCSとCitrix Provisioningカタログの両方を管理するための単一の統合コンソール。
- ID管理ソリューション、オンデマンドプロビジョニングなど、Citrix Provisioningカタログの新機能があります。

現在、この機能はAzureおよびVMwareワークロードでのみ利用可能です。ただし、VMware環境では、現在PowerShellコマンドのみを使用してカタログを作成できます。詳細については、Citrix StudioでCitrix Provisioningカタログを作成するを参照してください。

詳細情報

- 接続とリソースの作成および管理
- マシンカタログの管理

AWSカタログを作成する

マシンカタログの作成では、マシンカタログを作成するウィザードについて説明します。以下の情報は、AWS仮想化環境に固有の詳細を扱っています。

> **注：**
>
> AWSカタログを作成する前に、AWSへの接続の作成を完了する必要があります。AWSへの接続を参照してください。

制限事項

Citrix Virtual Apps and Desktops™ 2203 LTSR以降では、MCS AWSプラグインが `DescribeInstanceTypes` AWS APIコールを実行し、それが成功すると、MCSはAPI応答から作成されたインベントリ名を使用します。

したがって、CVAD 1912から2203以降にアップグレードする場合は、AWS上の `DefineInstanceType` 権限を無効にし、`Set-ProvScheme` コマンドを使用して既存のカタログを更新してAWSの命名スキームに合わせます。その後、カタログの更新が完了し、サービス提供がAWSの命名スキームに一致したら、`DescribeInstanceType` 権限を再度追加します。

イメージ準備中のネットワーク設定

イメージ準備中に、元のVMに基づいて準備用仮想マシン（VM）が作成されます。この準備用VMはネットワークから切断されます。準備用VMからネットワークを切断するために、すべてのインバウンドおよびアウトバウンドトラフィックを拒否するネットワークセキュリティグループが作成されます。このネットワークセキュリティグループは永続化され、再利用されます。ネットワークセキュリティグループの名前は `Citrix.XenDesktop.IsolationGroup-GUID` で、GUIDはランダムに生成されます。

AWSテナンシーを構成する

AWSは以下のテナンシーオプションを提供します。

- 共有テナンシー（デフォルトタイプ）：異なる顧客の複数のAmazon EC2インスタンスが、同じ物理ハードウェア上に存在する可能性があります。
- 専用テナンシー：EC2インスタンスは、デプロイした他のインスタンスと同じハードウェア上でのみ実行されます。他の顧客は同じハードウェアを使用しません。

PowerShellを使用して、MCSでAWS専用ホストをプロビジョニングできます。

PowerShellを使用してAWS専用ホストテナンシーを構成する

PowerShellを通じてホストテナンシーが定義されたマシンカタログを作成できます。

Amazon 専用ホストは、インスタンス容量を持つ物理サーバーであり、完全に専用であるため、既存のソケットごとまたはVMごとのソフトウェアライセンスを使用できます。

専用ホストには、インスタンスタイプに基づいて事前に設定された利用率があります。たとえば、C4 Largeインスタンスタイプの単一の割り当てられた専用ホストは、16インスタンスの実行に制限されています。詳細については、AWSサイトを参照してください。

AWSホストへのプロビジョニングの要件は次のとおりです。

- インポートされたBYOL（bring your own license）イメージ（AMI）。専用ホストでは、既存のライセンスを使用および管理します。
- プロビジョニング要求を満たすのに十分な利用率を持つ専用ホストの割り当て。
- **自動配置**を有効にします。

PowerShell を使用して AWS の専用ホストにプロビジョニングするには、**New-ProvScheme** コマンドレットでパラメーター `TenancyType` を *Host* に設定して使用します。

詳細については、Citrix Developer Documentation を参照してください。

AMI からマシンプロパティをキャプチャする

AWS で Machine Creation Services (MCS) を使用してマシンをプロビジョニングするカタログを作成する場合、そのカタログのマスター/ゴールデンイメージを表す AMI を選択します。その AMI から、MCS はディスクのスナップショットを使用します。以前のリリースでは、マシンにロールやタグを設定したい場合、AWS コンソールを使用して個別に設定していました。この機能はデフォルトで有効になっています。

> **ヒント:**
>
> AWS インスタンスプロパティのキャプチャを使用するには、AMI に関連付けられた VM が必要です。
>
> このプロセスを改善するために、**MCS は** AMI が取得されたインスタンスからプロパティを読み取り、そのマシンの Identity Access Management (IAM) ロールとタグを、特定のカタログ用にプロビジョニングされたマシンに適用します。このオプション機能を使用すると、カタログ作成プロセスは選択された AMI ソースインスタンスを見つけ、限られたプロパティセットを読み取ります。これらのプロパティは AWS Launch Template に保存され、そのカタログのマシンをプロビジョニングするために使用されます。カタログ内のすべてのマシンは、キャプチャされたインスタンスプロパティを継承します。

キャプチャされるプロパティには以下が含まれます。

- IAM ロール – プロビジョニングされたインスタンスに適用されます。
- タグ - プロビジョニングされたインスタンス、そのディスク、および NIC に適用されます。これらのタグは、S3 バケットとオブジェクト、AMI、スナップショット、起動テンプレートなど、一時的な Citrix® リソースに適用されます。

> **ヒント:**
>
> 一時的な Citrix リソースのタグ付けはオプションであり、カスタムプロパティ `AwsOperationalResourcesTagging` を使用して構成できます。

AWS インスタンスプロパティをキャプチャする

AWS ホスティング接続のプロビジョニングスキームを作成する際に、カスタムプロパティ `AwsCaptureInstanceProperties` を指定することで、この機能を使用できます。

`New-ProvScheme -CustomProperties "AwsCaptureInstanceProperties,true" …<standard provscheme parameters`

詳細については、Citrix Developer Documentation を参照してください。

> **注：**
>
> `AwsCaptureInstanceProperties` は非推奨です。代わりに、VM のマシンプロパティを指定するには、マシンプロファイルを使用することをお勧めします。

マシンプロファイルからマシンプロパティをキャプチャする

MCS を使用して AWS マシンをプロビジョニングするためのカタログを作成する際、マシンプロファイルを使用して特定のマシンプロパティ設定をプリセットできます。

そのためには、次の手順に従います。

1. マシンプロファイルを、このカタログを作成するリソースと同じアベイラビリティゾーンに保存します。
2. カタログ作成ウィザードの**マシンテンプレート**ページで、**マシンプロファイルを使用**を選択します。選択したリソースと同じアベイラビリティゾーンにあるマシンプロファイルが表示されます。
3. 必要に応じてマシンプロファイルを選択します。

> **注：**

> マシンプロファイルまたは AMI のいずれかを使用して、マシンプロパティをキャプチャできます。Web Studio で**マシンプロファイルを使用**を選択すると、**仮想マシンにマシンテンプレートプロパティを適用**オプションは自動的に非表示になります。

AWS オペレーションリソースにタグを付ける

MCS を使用して AWS でマシンをプロビジョニングするためのカタログを作成する際、IAM ロールとタグプロパティをそれらのマシンに適用するかどうかを制御できます。また、マシンタグをオペレーションリソースに適用するかどうかも制御できます。

Amazon マシンイメージ (AMI) は、Amazon Cloud 環境内で仮想マシンを作成するために使用される仮想アプライアンスの一種であり、一般にEC2と呼ばれます。AMIを使用して、EC2環境を使用するサービスを展開します。AWS向けMCSを使用してマシンをプロビジョニングするカタログを作成するときは、そのカタログのゴールデンイメージとして機能する**AMI**を選択します。

> **重要:**
>
> インスタンスプロパティと起動テンプレートをキャプチャしてカタログを作成することは、オペレーションリソースのタグ付けを使用するために必要です。

> AWS カタログを作成するには、まずゴールデンイメージとするインスタンスの AMI を作成する必要があります。MCS はそのインスタンスからタグを読み取り、起動テンプレートに組み込みます。その後、起動テンプレートのタグは、AWS 環境で作成されたすべての Citrix リソースに適用されます。これには以下が含まれます。

- 仮想マシン
- VMディスク
- VMネットワークインターフェイス
- S3 バケット
- S3 オブジェクト
- 起動テンプレート
- AMI

オペレーションリソースにタグを付ける

PowerShell を使用してリソースにタグを付けるには：

1. DDC ホストから PowerShell ウィンドウを開きます。
2. コマンド `asnp citrix` を実行して、Citrix固有のPowerShellモジュールをロードします。

プロビジョニングされた VM のリソースにタグを付けるには、新しいカスタムプロパティ `AwsOperationalResourcesTagging` を使用します。このプロパティの構文は次のとおりです。

```
New-ProvScheme -CustomProperties "AwsCaptureInstanceProperties,true;
AwsOperationalResourcesTagging,true" …<standard provscheme parameters>
```

次のステップ

- これが最初に作成されたカタログである場合、Web Studioはデリバリーグループの作成を案内します。
- 構成プロセス全体を確認するには、「」(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/install-configure.html)を参照してください。
- カタログを管理するには、マシンカタログの管理 および AWS カタログの管理 を参照してください。

VM上のタグをコピーする

マシンプロファイルで指定されたNICとディスク（IDディスク、ライトバックキャッシュディスク、OSディスク）のタグを、MCSマシンカタログで新しく作成されたVMにコピーできます。これらのタグは、マシンプロファイルソース（AWS VMインスタンスまたはAWS起動テンプレートバージョン）のいずれかで指定できます。この機能は、永続および非永続マシンカタログとVMに適用されます。

> **注：**
>
> - AWS EC2 コンソールでは、**起動テンプレートバージョンリソースタグ**の下に**ネットワークインターフェイスのタグ付け**の値が表示されません。ただし、PowerShell コマンド `aws ec2 describe-launch-template-versions --launch-template-id lt-0bb652503d45dcbcd --versions 12` を実行してタグの仕様を確認できます。
> - マシンプロファイルソース（VMまたは起動テンプレートバージョン）に2つのネットワークインターフェイス（eni-1とeni-2）があり、eni-1にタグt1、eni-2にタグt2がある場合、VMは両方のネットワークインターフェイスのタグを取得します。

マシンプロファイルを使用してカタログを作成する

AWSでMachine Creation Services™ (MCS)を使用してマシンをプロビジョニングするためのカタログを作成する際、EC2インスタンス (VM) または起動テンプレートバージョンからハードウェアプロパティをキャプチャし、プロビジョニングされたマシンに適用するためにマシンプロファイルを使用できるようになりました。キャプチャされるプロパティには、例えば、EBSボリュームプロパティ、インスタンスタイプ、EBS最適化、およびその他のサポートされているAWS構成が含まれます。カタログを編集する際、プロビジョニングされたマシンのマシンプロファイルは、別のVMまたは起動テンプレートを提供することで変更できます。

> **注：**
>
> EBSボリュームプロパティは、マシンプロファイルからのみ派生します。

重要な考慮事項

MCSマシンカタログを作成する際の重要な考慮事項:

- `New-ProvScheme` および `Set-ProvScheme` コマンドでマシンハードウェアプロパティパラメーターを追加すると、パラメーターで指定された値がマシンプロファイルの値を上書きします。
- `AwsCaptureInstanceProperties` を `true` に設定し、`MachineProfile` プロパティを設定しない場合、IAM ロールとタグのみがキャプチャされます。
- `AwsCaptureInstanceProperties` と `MachineProfile` の両方を同時に設定することはできません。

  > **注:
  >
  > `AwsCaptureInstanceProperties` は非推奨です。

- 次のプロパティの値を明示的に指定する必要があります。
  - TenancyType
  - セキュリティグループ
  - NICまたは仮想ネットワーク

- `AwsOperationalResourcesTagging` は、`AwsCaptureInstanceProperties` を有効にするか、マシンプロファイルを指定した場合にのみ有効にできます。

MCSマシンカタログ作成後の重要な考慮事項：

- カタログに追加された新しいVMのみが変更の影響を受けます。
- マシンプロファイルベースのカタログを非マシンプロファイルベースのカタログに変更することはできません。

マシンプロファイルを使用してマシンカタログを作成する

マシンプロファイルを使用してマシンカタログを作成するには：

1. **PowerShell**ウィンドウを開きます。
2. Citrix固有のPowerShellモジュールをロードするために`asnp citrix*`を実行します。
3. まだ作成されていない場合は、IDプールを作成します。例：

```
New-AcctIdentityPool -IdentityPoolName idPool -NamingScheme ms##
-Domain abcdf -NamingSchemeType Numeric
```

4. New-ProvSchemeコマンドを実行します。例：

```
New-ProvScheme -ProvisioningSchemeName demet-test-1

-HostingUnitUid aa633238-9xxd-4cf6-80e8-232a758a1xx1

-IdentityPoolUid 34d5b088-e312-416f-907d-16573xxxxxc4

-CleanOnBoot

-MasterImageVM 'XDHyp:\HostingUnits\cvad-test-scalestress\citrix-demet-
ami.0 (ami-0ca813xxxxxx061ef).template'

-MachineProfile 'XdHyp:\HostingUnits\cvad-test-scalestress\us-
east-1a.availabilityzone\machine-profile-instance i (i-0xxxxxxxx).vm'
```

5. カタログの作成を完了します。詳細については、Citrix PowerShell SDKを参照してください。

マシンプロファイルで最初にプロビジョニングされたカタログのマシンプロファイルを更新するには：

1. `Set-ProvScheme`コマンドを実行します。例：

```
Set-ProvScheme `

-ProvisioningSchemeUid "<ID" `

-MachineProfile "XDHyp:\HostingUnits\abc\us-
east-1a.availabilityzone\citrix-cvad-machineprofile-instance
(i-0xxxxxxxx).vm"
```

起動テンプレートバージョンでカタログを作成する

起動テンプレートバージョンをマシンプロファイルの入力として使用して、MCSマシンカタログを作成できます。また、マシンプロファイルカタログの入力をVMから起動テンプレートバージョンに、または起動テンプレートバージョンからVMに更新することもできます。

AWS EC2コンソールでは、起動テンプレートのインスタンス構成情報をバージョン番号とともに提供できます。マシンカタログの作成または更新時に、起動テンプレートバージョンをマシンプロファイルの入力として指定すると、そのバージョンの起動テンプレートのプロパティがプロビジョニングされたVDA VMにコピーされます。

以下のプロパティは、マシンプロファイルの入力として、または`New-ProvScheme`または`Set-ProvScheme`コマンドのパラメーターとして明示的に指定できます。`New-ProvScheme`または`Set-ProvScheme`コマンドで指定された場合、これらのプロパティのマシンプロファイル値よりも優先されます。

- サービスオファリング
- ネットワーク
- セキュリティグループ
- テナンシータイプ

注：

マシンプロファイルの起動テンプレートでサービスオファリングが提供されていない場合、または`New-ProvScheme`コマンドのパラメーターとして提供されていない場合、適切なエラーが発生します。

マシンプロファイルの入力として起動テンプレートバージョンを使用してカタログを作成するには:

1. **PowerShell**ウィンドウを開きます。
2. Citrix固有のPowerShellモジュールをロードするために`asnp citrix*`を実行します。
3. 起動テンプレートの起動テンプレートバージョンの一覧を取得します。例:

```
XDHyp:\HostingUnits\test\test-mp-sard (lt-01xxxxx).launchtemplate> ls |
Select FullPath
```

4. 作成されていない場合は、IDプールを作成します。例:

```
New-AcctIdentityPool `

-IdentityPoolName "abc11" `

-NamingScheme "abc1-##" `

-NamingSchemeType Numeric `

-Domain "citrix-xxxxxx.local" `

-ZoneUid "xxxxxxxx" `
```

5. マシンプロファイルの入力として起動テンプレートバージョンを使用してプロビジョニングスキームを作成します。例:

```
New-ProvScheme `

-ProvisioningSchemeName "MPLT1" `

-HostingUnitUid "c7f71f6a-3f45-4xxx-xxxx-xxxxxxxxxx" `

-IdentityPoolUid "bf3a6ba2-1f80-4xxx-xxxx-xxxxxxxxx" `

-MasterImageVM "XDHyp:\HostingUnits\xxxd-ue1a\apollo-non-persistent-
vda-win2022 (ami-0axxxxxxxxxx).template" `

-CleanOnBoot `

-MachineProfile "XDHyp:\HostingUnits\xxxx-ue1a\machineprofiletest
(lt-01xxxxx).launchtemplate\lt-01xxxxx (1).launchtemplateversion"
```

サービスオファリング、セキュリティグループ、テナンシー、ネットワークなどのパラメータを上書きすることもできます。例：

```
New-ProvScheme `

-ProvisioningSchemeName "MPLT1" `

-HostingUnitUid " c7f71f6a-3f45-4xxx-xxxx-xxxxxxxxxx" `

-IdentityPoolUid " bf3a6ba2-1f80-4xxx-xxxx-xxxxxxxxx" `

-MasterImageVM "XDHyp:\HostingUnits\xxxd-ue1a\apollo-non-persistent-
vda-win2022 (ami-0axxxxxxxxxx).template" `

-CleanOnBoot `

-MachineProfile "XDHyp:\HostingUnits\xxxx-ue1a\machineprofiletest
(lt-01xxxx).launchtemplate\lt-01xxxx (1).launchtemplateversion" `

-ServiceOffering "XDHyp:\HostingUnits\xxxd-ue1a\T3 Large
Instance.serviceoffering"
```

6. プロビジョニングスキームをブローカーカタログとして登録します。例：

```
New-BrokerCatalog -Name "MPLT1" `

-AllocationType Random `

-Description "Machine profile catalog" `

-ProvisioningSchemeId fe7df345-244e-4xxxx-xxxxxxxxx `

-ProvisioningType Mcs `

-SessionSupport MultiSession `

-PersistUserChanges Discard
```

7. カタログの作成を完了します。詳細については、Citrix PowerShell SDKを参照してください。

マシンプロファイルカタログの入力を、VMから起動テンプレートバージョンへ、または起動テンプレートバージョンからVMへ更新することもできます。例:

- マシンプロファイルカタログの入力をVMから起動テンプレートバージョンに更新するには:

```
Set-ProvScheme -ProvisioningSchemeName "CloudServiceOfferingTest" `

-MachineProfile "XDHyp:\HostingUnits\xxxx-ue1a\machineprofiletest
(lt-0bxxxxxxxxxxxx).launchtemplate\lt-0bxxxxxxxxxxxx
(1).launchtemplateversion"
```

- マシンプロファイルカタログの入力を起動テンプレートバージョンからVMに更新するには:

```
Set-ProvScheme -ProvisioningSchemeName "CloudServiceOfferingTest" `

-MachineProfile "XDHyp:\HostingUnits\sard-ue1a\us-
east-1a.availabilityzone\apollo-non-persistent-vda-win2022-2
(i-08xxxxxxxx).vm"
```

VMインスタンスをフィルタリングする

マシンプロファイルVMとして使用するAWS EC2インスタンスは、マシンカタログが正しく作成され機能するために互換性がある必要があります。マシンプロファイルの入力VMとして使用できるAWS EC2インスタンスを一覧表示するには、`Get-HypInventoryItem`コマンドを使用できます。このコマンドは、ホスティングユニットで利用可能なVMのインベントリをページングおよびフィルタリングできます。

ページネーション:

Get-HypInventoryItem は、2つのページネーションモードをサポートしています。

- ページングモードでは、`-MaxRecords` と `-Skip` パラメーターを使用してアイテムのセットを返します。
  - `-MaxRecords`: デフォルトは **1** です。これは、返すアイテムの数を制御します。
  - `-Skip`: デフォルトは **0** です。これは、ハイパーバイザー内のリストの絶対的な先頭（または絶対的な末尾）からスキップするアイテムの数を制御します。
- スクロールモードでは、`-MaxRecords`、`-ForwardDirection`、および `-ContinuationToken` パラメーターを使用してレコードのスクロールを可能にします。
  - `-ForwardDirection`: デフォルトは **True** です。これは `-MaxRecords` とともに使用され、一致するレコードの次のセットまたは前のセットのいずれかを返します。

    - `-ContinuationToken`: これは、直後（または `ForwardDirection` が **false** の場合は直前）のアイテムを返しますが、`ContinuationToken` で指定されたアイテムは含まれません。

ページネーションの例:

- 最も名前の小さいマシンテンプレートの単一レコードを返します。`AdditionalData` フィールドには `TotalItemsCount` と `TotalFilteredItemsCount` があります。

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template
```

- 最も名前の小さいマシンテンプレートのレコードを10件返します。

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template -MaxRecords 10 | select Name
```

- 最も名前の大きいレコードで終わるレコードの配列を返します。

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template -ForwardDirection $False -MaxRecords 10 | select
Name
```

- 指定された `ContinuationToken` に関連付けられたマシンテンプレートから始まるレコードの配列を返します。

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template -ContinuationToken "ami-07xxxxxxxxx"
-MaxRecords 10
```

フィルタリング:

フィルタリングには、以下の追加のオプションパラメータがサポートされています。これらのパラメータは、ページネーションオプションと組み合わせることができます。

- `-ContainsName "my_name"`: 指定された文字列がAMI名の一部と一致する場合、そのAMIは `Get` 結果に含まれます。例:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template -MaxRecords 100 -ContainName ‘apollo’ | select
Name
```

- `-Tags '{ "Key0": "Value0", "Key1": "Value1", "Key2": "Value2" }'`: AMIがこれらのタグの少なくとも1つを持っている場合、そのAMIは`Get`結果に含まれます。例:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template -MaxRecords 100 -Tags '{"opex owner": "Not
tagged"}' | select Name
```

> **注：**
>
> 2つのタグ値がサポートされています。**タグなし**タグ値は、タグのリストに指定されたタグがない項目と一致します。**すべての値**タグ値は、タグの値に関係なくタグを持つ項目と一致します。それ以外の場合、一致は、項目がタグを持ち、その値がフィルターで指定されたものと等しい場合にのみ発生します。

- `-Id "ami-0a2d913927e0352f3"`: AMIが指定されたIDと一致する場合、そのAMIは`Get`結果に含まれます。例:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template -Id ami-xxxxxxxxxxxx
```

AdditionalData パラメータでのフィルタリング:

`AdditionalData`フィルターパラメータは、テンプレートまたはVMを、その機能、サービス提供、またはAdditionalDataにある任意のプロパティに基づいてリストします。例:

```
(Get-HypInventoryItem -ResourceType "launchtemplateversion" -LiteralPath
"XDHyp:\HostingUnits\aws" -MaxRecords 200).AdditionalData
```

互換性のないVMを示す`-Warn`パラメータを追加することもできます。VMには、**Warning**という名前の`AdditionalData`フィールドが含まれます。例:

```
(Get-HypInventoryItem -ResourceType "launchtemplateversion" -LiteralPath
"XDHyp:\HostingUnits\aws" -MaxRecords 200 -Template "ami-015xxxxxxxx"
-Warn $true).AdditionalData
```

詳細情報

- 接続とリソースの作成および管理
- AWSへの接続
- マシンカタログの作成

XenServer®カタログを作成する

マシンカタログの作成では、マシンカタログを作成するウィザードについて説明します。以下の情報は、XenServer仮想化環境に固有の詳細を扱っています。

> **注：**
>
> XenServerカタログを作成する前に、XenServerへの接続の作成を完了する必要があります。XenServerへの接続を参照してください。

XenServer接続を使用してマシンカタログを作成する

GPU対応マシンには、専用のマスターイメージが必要です。これらのVMには、GPUをサポートするビデオカードドライバーが必要です。GPU対応マシンを構成して、VMがGPUを操作に使用するソフトウェアで動作できるようにします。

1. XenCenter®で、標準VGA、ネットワーク、およびvCPUを備えたVMを作成します。
2. VM構成を更新して、GPUの使用（パススルーまたはvGPUのいずれか）を有効にします。
3. サポートされているオペレーティングシステムをインストールし、RDPを有効にします。
4. Citrix VM ToolsとNVIDIAドライバーをインストールします。
5. パフォーマンスを最適化するために、Virtual Network Computing (VNC) 管理コンソールをクリアし、VMを再起動します。
6. RDPを使用するように求められます。RDPを使用してVDAをインストールし、VMを再起動します。
7. 必要に応じて、他のGPUマスターイメージのベースラインテンプレートとしてVMのスナップショットを作成します。

8. RDPを使用して、XenCenterで構成され、GPU機能を使用する顧客固有のアプリケーションをインストールします。

制限事項

- Citrix Hypervisor 8.2 でホストされているVMを含むCitrix Virtual Apps and Desktops展開が、単一のMCSカタログで複数のGFS2 SRを使用している場合、カタログ内のVMは展開中にVDIにアクセスできません。「VDIは現在使用中です」というエラーが報告されます。
- XenServerは、GFS2 SRを使用したMCSフルクローンVMをサポートしていません。

詳細については、制約を参照してください。

マシンプロファイルを使用してマシンカタログを作成する

MCS を使用してマシンをプロビジョニングするカタログを作成する場合、マシンプロファイルを使用して仮想マシンからハードウェアプロパティをキャプチャし、カタログ内の新しくプロビジョニングされた VM に適用できます。`MachineProfile` パラメーターが使用されていない場合、ハードウェアプロパティはマスターイメージ VM またはスナップショットからキャプチャされます。

> **注：**
>
> 現在、マシンプロファイルの入力として使用できるのは VM のみです。

> マシンプロファイル入力のパラメーターの値を上書きするために、次のパラメーターを明示的に構成できます。

- `VMCpuCount`
- `VMMemory`
- `NetworkMapping`

マシンプロファイルを使用してカタログを作成するには：

1. PowerShellウィンドウを開きます。
2. `asnp citrix*`を実行します。
3. ID プールを作成します。ID プールは、作成する VM の Active Directory (AD) アカウントのコンテナです。例：

```
New-AcctIdentityPool -Domain "citrix-xxxxxx.local" -IdentityPoolName
"ExampleIdentityPool" -NamingScheme "abc1-##" -NamingSchemeType
"Numeric" -Scope @() -ZoneUid "xxxxxxxx"
```

4. Active Directoryで必要なADコンピューターアカウントを作成します。

```
$password = "password123" | ConvertTo-SecureString -AsPlainText -Force

New-AcctADAccount -IdentityPoolName "ExampleIdentityPool" -Count 10
-ADUserName "citrix-xxxxxx\admin1" -ADPassword $password

Set-AcctAdAccountUserCert -IdentityPoolName "ExampleIdentityPool"
-ADUserName "citrix-xxxxxx\admin1" -ADPassword $password
```

5. カタログを作成するには、`New-ProvScheme`コマンドを実行します。例:

```
New-ProvScheme -CleanOnBoot -HostingUnitName "ExampleHostingUnit"
-IdentityPoolName "ExampleIdentityPool" -InitialBatchSizeHint 2
-CustomProperties '<CustomProperties xmlns="http://schemas.citrix.com/
2014/xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks"
Value="true" />

</CustomProperties>'

-MasterImageVM "XDHyp:
\HostingUnits\ExampleHostingUnit\ExampleVDA.vm\ExampleVDA.snapshot"
-ProvisioningSchemeName "ExampleCatalog" -Scope @() -SecurityGroup @()

-MachineProfile "XDHyp:
\HostingUnits\ExampleHostingUnit\ExampleMachineProfile.vm"
```

6. プロビジョニングスキームをブローカーカタログとして登録します。例：

```
$ConfigZone = Get-ConfigZone | Where-Object { $_.Name -eq "xxxxxx" }

New-BrokerCatalog -Name "MPLT1" -AllocationType Random -Description
"Machine profile catalog" -ProvisioningSchemeId fe7df345-244e-4xxxx-
```

```
xxxxxxxxx -ProvisioningType Mcs -SessionSupport MultiSession
-PersistUserChanges Discard -ZoneUid ($ConfigZone.Uid)
```

7. カタログにVMを追加します。

新しいマシンプロファイルでカタログを更新するには：

1. `Set-ProvScheme`コマンドを実行します。例：

```
Set-ProvScheme -ProvisioningSchemeName "ExampleCatalog" -MachineProfile
"XDHyp:
\HostingUnits\ExampleHostingUnit\ExampleMachineProfileVm.vm\ExampleMach
ineProfileSnapshot.snapshot"
```

   Set-ProvScheme コマンドの詳細については、Set-ProvSchemeを参照してください。

注：

- この場合、`Set-ProvScheme` コマンドはカタログ内の既存の VM のマシンプロファイルを変更しません。カタログに追加された新しく作成された VM のみが新しいマシンプロファイルを持ちます。
- マシンプロファイルベースのマシンカタログを、非マシンプロファイルベースのマシンカタログに変換することはできません。

次のステップ

- これが最初に作成されたカタログである場合、Web Studioはデリバリーグループの作成を案内します。
- 構成プロセス全体を確認するには、「」(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/install-configure.html)を参照してください。
- カタログを管理するには、マシンカタログの管理およびXenServer カタログの管理を参照してください。

詳細情報

- 接続とリソースの作成および管理
- XenServerへの接続

- マシンカタログの作成

Google Cloud Platformカタログを作成する

(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/install-configure/machine-catalogs-create.html)は、マシンカタログを作成するウィザードについて説明しています。以下の情報は、Google Cloud環境に固有の詳細を扱っています。

> **注：**

> Google Cloud Platform (GCP) カタログを作成する前に、GCPへの接続の作成を完了する必要があります。(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/install-configure/connections/connection-gcp.html)を参照してください。

マスターVMインスタンスと永続ディスクを準備する

> **ヒント:**

> 永続ディスクは、仮想ディスクを指すGoogle Cloudの用語です。

> マスターVMインスタンスを準備するには、計画しているマシンカタログ内のクローンVDAインスタンスに必要な構成と一致するプロパティを持つVMインスタンスを作成および構成します。この構成は、インスタンスのサイズとタイプにのみ適用されるわけではありません。メタデータ、タグ、GPU割り当て、ネットワークタグ、サービスアカウントのプロパティなどのインスタンス属性も含まれます。

マスタリングプロセスの一環として、MCSはマスターVMインスタンスを使用してGoogle Cloudの*インスタンステンプレート*を作成します。このインスタンステンプレートは、マシンカタログを構成するクローンVDAインスタンスの作成に使用されます。クローンインスタンスは、インスタンステンプレートが作成されたマスターVMインスタンスのプロパティ（VPC、サブネット、永続ディスクのプロパティを除く）を継承します。

マスターVMインスタンスのプロパティを要件に合わせて構成したら、インスタンスを起動し、そのインスタンスの永続ディスクを準備します。

ディスクのスナップショットを手動で作成することをお勧めします。そうすることで、意味のある命名規則を使用してバージョンを追跡し、マスターイメージの以前のバージョンを管理するため

のより多くのオプションが得られ、マシンカタログの作成時間を節約できます。独自のスナップショットを作成しない場合、MCSが一時的なスナップショットを作成します（これはプロビジョニングプロセスの終了時に削除されます）。

マシンカタログを作成する

マシンカタログは、次の2つの方法で作成できます。

- Web Studio を使用してマシンカタログを作成する
- PowerShell を使用してマシンカタログを作成する

Web Studio を使用してマシンカタログを作成する

> **注：**
>
> マシンカタログを作成する前に、リソースを作成してください。マシンカタログを構成する際は、Google Cloud が定めた命名規則を使用してください。詳細については、バケットとオブジェクトの命名ガイドラインを参照してください。

(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/install-configure/machine-catalogs-create.html)のガイダンスに従ってください。以下の説明は、Google Cloud カタログに固有のものです。

1. Web Studio にサインインし、左側のペインで を選択します。
2. アクションバーで を選択します。
3. ページで、 を選択し、 を選択します。
   - Citrix Virtual Apps and Desktops™ は、シングルセッションOSもサポートしています。
4. ページで、 と オプションを選択し、 を選択します。複数のリソースがある場合は、メニューから1つ選択します。
5. ページで、必要に応じてこれらの手順を完了し、 をクリックします。
   a. マスターイメージとしてスナップショットまたはVMを選択します。単一テナンシー機能を使用する場合は、ノードグループプロパティが正しく構成されているイメージを選択してください。ゾーン選択を有効にするを参照してください。
   b. 既存のVMをマシンプロファイルとして使用するには、 を選択し、VMを選択します。

   > **注：**

> 現在、このカタログ内のVMは、ディスク暗号化セットID、マシンサイズ、ストレージタイプ、およびゾーン設定をマシンプロファイルから継承します。

c. カタログの最小機能レベルを選択します。単一テナンシー機能を使用する場合は、ノードグループプロパティが正しく構成されているイメージを選択してください。

6. ページで、このマシンカタログのオペレーティングシステムを格納するために使用するストレージの種類を選択します。以下の各ストレージオプションには、独自の価格とパフォーマンス特性があります。（IDディスクは常にゾーン標準永続ディスクを使用して作成されます。）

   - 標準永続ディスク
   - バランス永続ディスク
   - SSD永続ディスク

   Google Cloud のストレージオプションの詳細については、`<https://cloud.google.com/compute/docs/disks/>`を参照してください。

7. ページで、作成するVMの数を指定し、VMの詳細な仕様を表示してから、 を選択します。マシンカタログに単一テナントノードグループを使用する場合は、予約済みの単一テナントノードが利用可能なゾーン**のみ**を選択してください。ゾーン選択を有効にするを参照してください。

8. ページで、Active Directory アカウントを選択し、 を選択します。

   - **新しいActive Directoryアカウントを作成**を選択した場合は、ドメインを選択し、Active Directoryで作成されるプロビジョニングされたVMコンピューターアカウントの命名スキームを表す文字のシーケンスを入力します。アカウントの命名スキームは1〜64文字で、空白スペース、非ASCII文字、または特殊文字を含めることはできません。
   - **既存のActive Directoryアカウントを使用**を選択した場合は、**参照**を選択して、選択したマシン用の既存のActive Directoryコンピューターアカウントに移動します。

9. **ドメイン資格情報**ページで、**資格情報を入力**を選択し、ユーザー名とパスワードを入力して、**保存**を選択し、**次へ**を選択します。

   - 入力する資格情報には、Active Directoryアカウント操作を実行する権限が必要です。

10. **概要**ページで、情報を確認し、カタログの名前を指定して、**完了**を選択します。

> **注：**
>
> バージョン2402以降、GCPカタログ名は以下の規則に準拠する必要があります。

- 小文字で始まること。
- 小文字 (a-z)、数字、ハイフンのみを含めること。
- 小文字または数字で終わること。 これらの規則に準拠していない既存のGCPカタログの名前を変更しようとすると、エラーメッセージが表示され、更新された規則に従って名前を変更するように案内されます。

マシンカタログの作成には時間がかかる場合があります。マシンがターゲットノードグループに作成されていることを確認するには、Google Cloudコンソールに移動します。

手動で作成されたGoogle Cloudマシンをインポートする

Google Cloudへの*接続を作成*し、その後、Google Cloudマシンを含む*カタログを作成*できます。その後、Citrix Virtual Apps and Desktopsを介してGoogle Cloudマシンを手動で電源サイクルできます。この機能を使用すると、次のことができます。

- 手動で作成したGoogle CloudマルチセッションOSマシンをCitrix Virtual Apps and Desktopsマシンカタログにインポートします。
- 手動で作成したGoogle CloudマルチセッションOSマシンをCitrix Virtual Apps and Desktopsカタログから削除します。
- 既存のCitrix Virtual Apps and Desktopsの電源管理機能を使用して、Google Cloud WindowsマルチセッションOSマシンの電源を管理します。たとえば、それらのマシンの再起動スケジュールを設定します。

この機能は、既存のCitrix Virtual Apps and Desktopsプロビジョニングワークフローの変更や、既存の機能の削除を必要としません。手動で作成したGoogle Cloudマシンをインポートする代わりに、Web StudioでMCSを使用してマシンをプロビジョニングすることをお勧めします。

共有仮想プライベートクラウド

共有仮想プライベートクラウド（VPC）は、共有サブネットが利用可能になるホストプロジェクトと、そのリソースを使用する1つ以上のサービスプロジェクトで構成されます。共有VPCは、共有企業Googleクラウド資産の一元的な制御、使用、管理を提供するため、大規模なインストールに適したオプションです。詳細については、Googleドキュメントサイトを参照してください。

この機能により、Machine Creation Services（MCS）は、共有VPCに展開されたマシンカタログのプロビジョニングと管理をサポートします。このサポートは、現在ローカルVPCで提供されているサポートと機能的に同等ですが、2つの点で異なります。

1. ホスト接続の作成に使用されるサービスアカウントに追加の権限を付与する必要があります。このプロセスにより、MCSは共有VPCリソースにアクセスして使用できるようになります。
2. イングレスとエグレス用にそれぞれ1つずつ、2つのファイアウォールルールを作成する必要があります。これらのファイアウォールルールは、イメージマスタリングプロセス中に使用されます。

必要な新しい権限

ホスト接続を作成する際には、特定の権限を持つGoogle Cloudサービスアカウントが必要です。これらの追加権限は、共有VPCベースのホスト接続の作成に使用されるすべてのサービスアカウントに付与する必要があります。

> **ヒント:**
>
> これらの追加の権限は、Citrix Virtual Apps and Desktopsにとって新しいものではありません。これらはローカルVPCの実装を容易にするために使用されます。共有VPCでは、これらの追加の権限により、他の共有VPCリソースへのアクセスが可能になります。

> Shared VPCをサポートするために、ホスト接続に関連付けられたサービスアカウントに最大4つの追加権限を付与する必要があります。

1. **compute.firewalls.list** - この権限は必須です。MCSがShared VPCに存在するファイアウォールルールのリストを取得できるようにします。
2. **compute.networks.list** - この権限は必須です。MCSがサービスアカウントで利用可能なShared VPCネットワークを識別できるようにします。
3. **compute.subnetworks.list** – この権限は、VPCの使用方法によってオプションです。MCSが可視Shared VPC内のサブネットを識別できるようにします。この権限はローカルVPCを使用する際にはすでに必要ですが、Shared VPCホストプロジェクトでも割り当てる必要があります。
4. **compute.subnetworks.use** - この権限は、VPCの使用方法によってオプションです。プロビジョニングされたマシンカタログでサブネットリソースを使用するために必要です。この権限はローカルVPCを使用する際にはすでに必要ですが、Shared VPCホストプロジェクトでも割り当てる必要があります。

これらの権限を使用する際には、マシンカタログの作成に使用される権限の種類に基づいて異なるアプローチがあることを考慮してください。

- プロジェクトレベルの権限:

    - ホストプロジェクト内のすべてのShared VPCへのアクセスを許可します。
    - 権限 #3 と #4 をサービスアカウントに割り当てる必要があります。
- サブネットレベルの権限:
    - Shared VPC内の特定のサブネットへのアクセスを許可します。
    - 権限 #3 と #4 はサブネットレベルの割り当てに固有のものであるため、サービスアカウントに直接割り当てる必要はありません。

組織のニーズとセキュリティ基準に合ったアプローチを選択してください。

> **ヒント:**
>
> プロジェクトレベルとサブネットレベルの権限の違いの詳細については、Google Cloud のドキュメントを参照してください。

ファイアウォールルール

マシンカタログの準備中に、カタログのマスターイメージシステムディスクとして機能するマシンイメージが準備されます。このプロセスが発生すると、ディスクは一時的に仮想マシンに接続されます。このVMは、すべてのインバウンドおよびアウトバウンドネットワークトラフィックを防止する分離された環境で実行する必要があります。これは、イングレス用とエグレス用の2つのすべて拒否ファイアウォールルールによって実現されます。Google CloudローカルVPCを使用する場合、MCSはこのファイアウォールをローカルネットワークに作成し、マスタリング用のマシンに適用します。マスタリングが完了すると、ファイアウォールルールはイメージから削除されます。

共有VPCを使用するために必要な新しい権限の数を最小限に抑えることをお勧めします。共有VPCはより上位の企業リソースであり、通常、より厳格なセキュリティプロトコルが導入されています。このため、ホストプロジェクトの共有VPCリソースに、イングレス用とエグレス用の2つのファイアウォールルールを作成してください。それらに最高の優先順位を割り当てます。次の値を使用して、これらの各ルールに新しいターゲットタグを適用します。

`citrix-provisioning-quarantine-firewall`

MCSがマシンカタログを作成または更新するとき、このターゲットタグを含むファイアウォールルールを検索します。次に、ルールの正確性を確認し、カタログのマスターイメージを準備するために使用されるマシンに適用します。ファイアウォールルールが見つからない場合、またはルールは見つかったものの、ルールやその優先順位が正しくない場合は、次のようなメッセージが表示されます。

`"Unable to find valid INGRESS and EGRESS quarantine firewall rules for VPC <name> in project <project>. " Please ensure you have created 'deny all' firewall rules with the network tag 'citrix-provisioning-quarantine-firewall' and proper priority." "Refer to Citrix Documentation for details."`

共有 VPC の構成

Web Studio で共有 VPC をホスト接続として追加する前に、プロビジョニングする予定のプロジェクトからサービスアカウントを追加するために、次の手順を完了してください。

1. IAM ロールを作成します。
2. CVAD ホスト接続の作成に使用するサービスアカウントを、共有 VPC ホストプロジェクトの IAM ロールに追加します。
3. プロビジョニングする予定のプロジェクトから Cloud Build サービスアカウントを、共有 VPC ホストプロジェクトの IAM ロールに追加します。
4. ファイアウォールルールを作成します。

IAMロールを作成する

ロールのアクセスレベルを決定します — *プロジェクトレベルアクセス*、またはより制限されたモデルである *サブネットレベルアクセス* を使用します。

IAMロールのプロジェクトレベルアクセス。プロジェクトレベルのIAMロールには、次の権限を含めます。

- compute.firewalls.list
- compute.networks.list
- compute.subnetworks.list
- compute.subnetworks.use

プロジェクトレベルのIAMロールを作成するには：

1. Google Cloudコンソールで、**IAMと管理 > ロール**に移動します。
2. 「**ロール**」ページで、「**ロールを作成**」を選択します。
3. 「**ロールを作成**」ページで、ロール名を指定します。「**権限を追加**」を選択します。
    a. **権限の追加**ページで、ロールに権限を個別に追加します。権限を追加するには、**テーブルをフィルタリング**フィールドに権限の名前を入力します。権限を選択し、**追加**を選択します。
    b. 「**作成**」を選択します。

サブネットレベルのIAMロール。このロールは、**ロールを作成**を選択した後に、権限`compute.subnetworks.list`と`compute.subnetworks.use`の追加を省略します。このIAMアクセスレベルの場合、権限`compute.firewalls.list`と`compute.networks.list`を新しいロールに適用する必要があります。

サブネットレベルのIAMロールを作成するには：

1. Google Cloudコンソールで、**VPCネットワーク** > **共有VPC**に移動します。**共有VPC**ページが表示され、ホストプロジェクトに含まれる共有VPCネットワークのサブネットが表示されます。
2. 「**共有VPC**」ページで、アクセスするサブネットを選択します。
3. 右上隅で「**メンバーを追加**」を選択して、サービスアカウントを追加します。
4. 「**メンバーを追加**」ページで、次の手順を実行します。
    a. 「**新しいメンバー**」フィールドにサービスアカウントの名前を入力し、メニューからサービスアカウントを選択します。
    b. 「**ロールを選択**」フィールドを選択し、次に「**Compute Network User**」を選択します。
    c. 「**保存**」を選択します。
5. Google Cloud コンソールで、「**IAM と管理**」>「**ロール**」に移動します。
6. 「**ロール**」ページで、「**ロールを作成**」を選択します。
7. 「**ロールを作成**」ページで、ロール名を指定します。「**権限を追加**」を選択します。
    a. 「**権限を追加**」ページで、ロールに個別に権限を追加します。権限を追加するには、「**テーブルをフィルタ**」フィールドに権限の名前を入力します。権限を選択し、「**追加**」を選択します。
    b. 「**作成**」を選択します。

ホストプロジェクトのIAMロールにサービスアカウントを追加する

IAMロールを作成したら、ホストプロジェクトのサービスアカウントを追加するために次の手順を実行します。

1. Google Cloud コンソールで、ホストプロジェクトに移動し、次に「**IAM と管理 > IAM**」に移動します。
2. 「**IAM**」ページで、「**追加**」を選択してサービスアカウントを追加します。
3. 「**メンバーを追加**」ページで、:

a. 「**新しいメンバー**」フィールドにサービスアカウントの名前を入力し、メニューからサービスアカウントを選択します。

b. ロールフィールドを選択し、作成したIAMロールを入力して、メニューからそのロールを選択します。

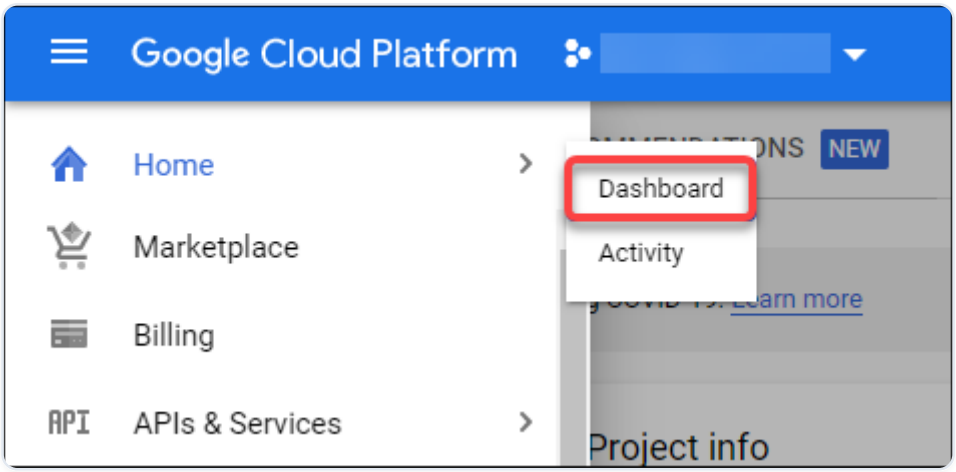
c. 「**保存**」を選択します。

これで、サービスアカウントがホストプロジェクト用に構成されました。

クラウドビルドサービスアカウントを共有VPCに追加する

すべてのGoogle Cloudサブスクリプションには、プロジェクトID番号の後に`cloudbuild.gserviceaccount`が続くサービスアカウントがあります。例: `705794712345@cloudbuild.gserviceaccount`。

Google Cloud コンソールで **Home** と **Dashboard** を選択すると、プロジェクトのプロジェクト ID 番号を確認できます。



画面の **Project Info** エリアの下にある **Project Number** を見つけます。

Cloud Buildサービスアカウントを共有VPCに追加するには、次の手順を実行します。

1. Google Cloudコンソールで、ホストプロジェクトに移動し、**IAMと管理** > **IAM**に移動します。
2. 「**権限**」ページで、「**追加**」を選択してアカウントを追加します。
3. 「**メンバーを追加**」ページで、次の手順を実行します。

   a. 「**新しいメンバー**」フィールドにCloud Buildサービスアカウントの名前を入力し、メニューからサービスアカウントを選択します。

   b. 「**ロールを選択**」フィールドを選択し、`Computer Network User`と入力して、メニューからロールを選択します。

   c. 「**保存**」を選択します。

ファイアウォールルールを作成する

マスタリングプロセスの一環として、MCS は選択されたマシンイメージをコピーし、それを使用してカタログ用のマスターイメージシステムディスクを準備します。マスタリング中、MCS はディスクを一時的な仮想マシンに接続し、その仮想マシンが準備スクリプトを実行します。この VM は、すべてのインバウンドおよびアウトバウンドネットワークトラフィックを禁止する分離された環境で実行する必要があります。分離された環境を作成するために、MCS は2つの *すべて拒否* ファイアウォールルール（イングレスルールとエグレスルール）を必要とします。したがって、*ホストプロジェクト* に次の2つのファイアウォールルールを作成します。

1. Google Cloud コンソールで、ホストプロジェクトに移動し、次に **VPC ネットワーク > ファイアウォール** に移動します。
2. 「**ファイアウォール**」ページで、「**ファイアウォールルールを作成**」を選択します。
3. 「**ファイアウォールルールを作成**」ページで、以下を完了します。
   - **名前**。ルールの名前を入力します。
   - **ネットワーク**。イングレスファイアウォールルールが適用される共有 VPC ネットワークを選択します。
   - **優先度**。値が小さいほど、ルールの優先度が高くなります。小さい値（例: 10）をお勧めします。
   - **トラフィックの方向**。**イングレス** を選択します。
   - **一致時のアクション**。**拒否** を選択します。
   - **ターゲット**。デフォルトの **指定されたターゲットタグ** を使用します。
   - **ターゲットタグ**。`citrix-provisioning-quarantine-firewall` と入力します。
   - **ソースフィルター**。デフォルトの **IP 範囲** を使用します。
   - **ソース IP 範囲**。すべてのトラフィックに一致する範囲を入力します。`0.0.0.0/0` と入力します。
   - **プロトコルとポート**。「**すべて拒否**」を選択します。
4. 「**作成**」を選択してルールを作成します。
5. 手順 1〜4 を繰り返して別のルールを作成します。**Direction of traffic** には **Egress** を選択します。

接続の追加

Google Cloud 環境への接続を追加します。接続の追加を参照してください。

ゾーン選択を有効にする

Citrix Virtual Apps and Desktops はゾーン選択をサポートしています。ゾーン選択を使用すると、VM を作成するゾーンを指定できます。ゾーン選択を使用すると、管理者は選択したゾーンに単一テナントノードを配置できます。単一テナンシーを構成するには、Google Cloud で以下を完了する必要があります。

- Google Cloud の単一テナントノードを予約する
- VDA マスターイメージを作成する

Google Cloud の単一テナントノードを予約する

単一テナントノードを予約するには、Google Cloud のドキュメントを参照してください。

> **重要:**
>
> ノードテンプレートは、ノードグループに予約されているシステムのパフォーマンス特性を示すために使用されます。これらの特性には、vGPU の数、ノードに割り当てられるメモリ量、およびノード上に作成されるマシンに使用されるマシンタイプが含まれます。詳細については、Google Cloud のドキュメントを参照してください。

VDA マスターイメージの作成

単一テナントノードにマシンを正常に展開するには、マスター VM イメージを作成する際に追加の手順を実行する必要があります。Google Cloud のマシンインスタンスには、*ノードアフィニティラベル*と呼ばれるプロパティがあります。単一テナントノードに展開されるカタログのマスターイメージとして使用されるインスタンスには、**ターゲットノードグループ**の名前と一致する*ノードアフィニティラベル*が必要です。これを実現するには、次の点に留意してください。

- 新しいインスタンスの場合は、インスタンスの作成時に Google Cloud コンソールでラベルを設定します。詳細については、単一テナント VM のプロビジョニングを参照してください。
- 既存のインスタンスの場合は、**gcloud** コマンドラインを使用してラベルを設定します。詳細については、ノードアフィニティラベルの構成を参照してください。

> **注：**
>
> 共有 VPC で単一テナンシーを使用する場合は、共有仮想プライベートクラウドを参照してください。

マシンカタログを作成する

ノードアフィニティラベルを設定したら、マシンカタログを構成します。

顧客管理の暗号化キー (CMEK)

MCS カタログに顧客管理の暗号化キー (CMEK) を使用できます。この機能を使用する場合、Google Cloud Key Management Service `CryptoKey Encrypter/Decrypter` ロールを Compute Engine サービスエージェントに割り当てます。Citrix Virtual Apps and Desktops アカウントは、キーが保存されているプロジェクトで適切な権限を持っている必要があります。詳細については、「Cloud KMS キーを使用してリソースを保護する」を参照してください。

Compute Engine サービスエージェントは次の形式です: `service-<Project_Number>@compute-system.iam.gserviceaccount.com`。この形式は、デフォルトの Compute Engine サービスアカウントとは異なります。

> **注：**
>
> この Compute Engine サービスアカウントは、Google Console の「**IAM 権限**」表示に表示されない場合があります。そのような場合は、Cloud KMS キーを使用してリソースを保護する で説明されているように、`gcloud` コマンドを使用してください。

Citrix Virtual Apps and Desktops アカウントに権限を割り当てる

Google Cloud KMS の権限はさまざまな方法で構成できます。*プロジェクトレベル*の KMS 権限または*リソースレベル*の KMS 権限のいずれかを付与できます。詳細については、権限とロール を参照してください。

プロジェクトレベルの権限

1つのオプションは、Citrix Virtual Apps and Desktops アカウントに Cloud KMS リソースを参照するためのプロジェクトレベルの権限を付与することです。これを行うには、カスタムロールを作成し、次の権限を追加します。

- `cloudkms.keyRings.list`
- `cloudkms.keyRings.get`
- `cloudkms.cryptokeys.list`
- `cloudkms.cryptokeys.get`

このカスタムロールを Citrix Virtual Apps and Desktops に割り当てます。これにより、インベントリ内の関連プロジェクトでリージョンキーを参照できます。

リソースレベルの権限

もう1つのオプションであるリソースレベルの権限の場合、Google Cloud コンソールで、MCS プロビジョニングに使用する `cryptoKey` を参照します。Citrix Virtual Apps and Desktops アカウントを、カタログプロビジョニングに使用するキーリングまたはキーに追加します。

> **ヒント:**
>
> このオプションでは、Citrix Virtual Apps and Desktops アカウントが Cloud KMS リソースに対するプロジェクトレベルのリスト権限を持っていないため、インベントリでプロジェクトのリージョンキーを参照できません。ただし、以下で説明するように、`ProvScheme` カスタムプロパティで正しい `cryptoKeyId` を指定することで、CMEK を使用してカタログをプロビジョニングすることは可能です。

カスタムプロパティを使用した CMEK でのプロビジョニング

PowerShellでプロビジョニングスキームを作成する際に、`ProvScheme CustomProperties` で `CryptoKeyId` プロパティを指定します。例:

```
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

    <Property xsi:type="StringProperty" Name="CryptoKeyId"
Value="<yourCryptoKeyId>" />

</CustomProperties>'
```

`cryptoKeyId` は次の形式で指定する必要があります。

`projectId:location:keyRingName:cryptoKeyName`

たとえば、IDが `my-example-project-1` のプロジェクトで、`us-east1` リージョンのキーリング `my-example-key-ring` にあるキー `my-example-key` を使用したい場合、`ProvScheme` カスタム設定は次のようになります。

```
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

    <Property xsi:type="StringProperty" Name="CryptoKeyId" Value="my-
example-project-1:us-east1:my-example-key-ring:my-example-key" />
```

```
</CustomProperties>'
```

このプロビジョニングスキームに関連するすべてのMCSプロビジョニング済みディスクとイメージは、この顧客管理暗号化キーを使用します。

ヒント:

グローバルキーを使用する場合、顧客プロパティの場所は**リージョン**名ではなく`global`と記述する必要があります。上記の例では**us-east1**です。例: `<Property xsi:type="StringProperty" Name="CryptoKeyId" Value="my-example-project-1:global:my-example-key-ring:my-example-key" />`。

顧客管理キーのローテーション

Google Cloudは、既存の永続ディスクまたはイメージでのキーのローテーションをサポートしていません。マシンがプロビジョニングされると、作成時に使用されていたキーのバージョンに紐付けられます。ただし、新しいバージョンのキーを作成でき、その新しいキーは、新しくプロビジョニングされたマシンや、新しいマスターイメージでカタログが更新されたときに作成されるリソースに使用されます。

キーリングに関する重要な考慮事項

キーリングの名前変更や削除はできません。また、キーリングを構成する際に予期せぬ料金が発生する可能性があります。キーリングを削除または削除すると、Google Cloudはエラーメッセージを表示します。

```
Sorry, you can't delete or rename keys or key rings. We were concerned
about the security implications of allowing multiple keys or key versions
over time to have the same resource name, so we decided to make names
immutable. (And you can't delete them, because we wouldn't be able to do a
true deletion--there would still have to be a tombstone tracking that this
name had been used and couldn't be reused).

We're aware that this can make things untidy, but we have no immediate
plans to change this.

If you want to avoid getting billed for a key or otherwise make it
unavailable, you can do so by deleting all the key versions; neither keys
```

```
nor key rings are billed for, just the active key versions within the
keys.
```

ヒント:

詳細については、「コンソールからキーリングを編集または削除する」を参照してください。

均一なバケットレベルのアクセス互換性

Citrix Virtual Apps and Desktops は、Google Cloud の統一されたバケットレベルのアクセス制御ポリシーと互換性があります。この機能は、ストレージバケットを含むリソースの操作を許可するために、サービスアカウントに権限を付与する IAM ポリシーの使用を強化します。統一されたバケットレベルのアクセス制御により、Citrix Virtual Apps and Desktops は、アクセス制御リスト (ACL) を使用して、ストレージバケットまたはそこに保存されているオブジェクトへのアクセスを制御できます。Google Cloud の統一されたバケットレベルのアクセスに関する概要情報については、「統一されたバケットレベルのアクセス」を参照してください。構成情報については、「統一されたバケットレベルのアクセスを要求する」を参照してください。

PowerShell を使用してマシンカタログを作成する

このセクションでは、PowerShell を使用してカタログを作成する方法について詳しく説明します。

- 永続的なライトバックキャッシュディスクを持つカタログを作成する
- MCSIO で起動パフォーマンスを向上させる
- マシンプロファイルを使用してマシンカタログを作成する
- インスタンステンプレートとしてマシンプロファイルを持つマシンカタログを作成する
- PowerShell を使用してシールドされた VM でカタログを作成する
- 単一テナントノードに Windows 11 VM を作成する

永続的なライトバックキャッシュディスクを持つカタログを作成する

永続的なライトバックキャッシュディスクを持つカタログを構成するには、PowerShell パラメーター `New-ProvScheme` `CustomProperties` を使用します。

ヒント:

ここで PowerShell パラメーターを使用するのは、クラウドベースのホスティング接続の場合のみです。オンプレミスソリューション（XenServer® など）で永続的なライトバックキャッシュディスクを使用してマシンをプロビジョニングする場合、ディスクは自動的に永続化されるため、PowerShell は必要ありません。

このパラメーターは、MCSプロビジョニングされたマシンに対してライトバックキャッシュディスクがどのように永続化されるかを決定するために使用される追加のプロパティ `PersistWBC` をサポートします。`PersistWBC` プロパティは、`UseWriteBackCache` パラメーターが指定され、かつ `WriteBackCacheDiskSize` パラメーターがディスクが作成されることを示すように設定されている場合にのみ使用されます。

注：

この動作は、AzureとGCPの両方に適用され、電源サイクル時にデフォルトのMCSIOライトバックキャッシュディスクが削除され、再作成されます。ディスクの削除と再作成を避けるために、ディスクを永続化することを選択できます。

`PersistWBC` プロパティを `true` に設定すると、Citrix Virtual Apps and Desktops 管理者が管理インターフェイスからマシンをシャットダウンしても、ライトバックキャッシュディスクは削除されません。

`PersistWBC` プロパティを `false` に設定すると、Citrix Virtual Apps and Desktops 管理者が管理インターフェイスからマシンをシャットダウンしたときに、ライトバックキャッシュディスクが削除されます。

注：

`PersistWBC` プロパティが省略された場合、プロパティはデフォルトで `false` になり、管理インターフェイスからマシンがシャットダウンされるとライトバックキャッシュは削除されます。

たとえば、CustomProperties パラメーターを使用して `PersistWBC` を `true` に設定する場合：

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="ResourceGroups"
Value="benvaldev5RG3" />

<Property xsi:type="StringProperty" Name="PersistWBC" Value="true" />

</CustomProperties>
```

注：

`PersistWBC`プロパティは、`New-ProvScheme` PowerShellコマンドレットを使用してのみ設定できます。作成後にプロビジョニングスキームの`CustomProperties`を変更しようとしても、マシンカタログや、マシンがシャットダウンされたときのライトバックキャッシュディスクの永続性には影響しません。

たとえば、`New-ProvScheme`を設定してライトバックキャッシュを使用し、同時に`PersistWBC`プロパティを`true`に設定します。

```
New-ProvScheme

-CleanOnBoot

-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com/
2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`"><Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`"
Value=`"true`" /><Property xsi:type=`"StringProperty`"
Name=`"StorageAccountType`" Value=`"Premium_LRS`" /><Property
xsi:type=`"StringProperty`" Name=`"ResourceGroups`"
Value=`"benvaldev5RG3`" /><Property xsi:type=`"StringProperty`"
Name=`"PersistWBC`" Value=`"true`" /></CustomProperties>"

-HostingUnitName "adSubnetScale1"
```

```
-IdentityPoolName "BV-WBC1-CAT1"

-MasterImageVM "XDHyp:
\HostingUnits\adSubnetScale1\image.folder\GoldImages.resourcegroup\W10MCSI
O-01_OsDisk_1_a940e6f5bab349019d57ccef65d2c7e3.manageddisk"

-NetworkMapping @{"0"="XDHyp:\HostingUnits\adSubnetScale1\
\virtualprivatecloud.folder\CloudScale02.resourcegroup\adVNET.virtualpriva
tecloud\adSubnetScale1.network"}

-ProvisioningSchemeName "BV-WBC1-CAT1"

-ServiceOffering "XDHyp:
\HostingUnits\adSubnetScale1\serviceoffering.folder\Standard_D2s_v3.servic
eoffering"

-UseWriteBackCache

-WriteBackCacheDiskSize 127

-WriteBackCacheMemorySize 256
```

MCSIOで起動パフォーマンスを向上させる

MCSIOが有効な場合、AzureおよびGCPマネージドディスクの起動パフォーマンスを向上させることができます。この機能を構成するには、`New-ProvScheme`コマンドでPowerShell `PersistOSDisk`カスタムプロパティを使用します。`New-ProvScheme`に関連するオプションは次のとおりです。

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="Resource ``````<!--NeedCopy-->

````````Groups" Value="benvaldev5RG3" />

<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="true" />
```
```

```
</CustomProperties>
```

この機能を有効にするには、`PersistOSDisk` カスタムプロパティを `true` に設定します。例：

```
New-ProvScheme

-CleanOnBoot

-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com/
2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`"><Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`"
Value=`"true`" /><Property xsi:type=`"StringProperty`"
Name=`"StorageAccountType`" Value=`"Premium_LRS`" /><Property
xsi:type=`"StringProperty`" Name=`"ResourceGroups`"
Value=`"benvaldev5RG3`" /><Property xsi:type=`"StringProperty`"
Name=`"PersistOsDisk`" Value=`"true`" /></CustomProperties>"

-HostingUnitName "adSubnetScale1"

-IdentityPoolName "BV-WBC1-CAT1"

-MasterImageVM "XDHyp:
\HostingUnits\adSubnetScale1\image.folder\GoldImages.resourcegroup\W10MCSI
O-01_OsDisk_1_a940e6f5bab349019d57ccef65d2c7e3.manageddisk"

-NetworkMapping @{"0"="XDHyp:\HostingUnits\adSubnetScale1\
\virtualprivatecloud.folder\CloudScale02.resourcegroup\adVNET.virtualpriva
tecloud\adSubnetScale1.network"}

-ProvisioningSchemeName "BV-WBC1-CAT1"

-ServiceOffering "XDHyp:
\HostingUnits\adSubnetScale1\serviceoffering.folder\Standard_D2s_v3.servic
eoffering"

-UseWriteBackCache

-WriteBackCacheDiskSize 127

-WriteBackCacheMemorySize 256
```

マシンプロファイルを使用してマシンカタログを作成する

Machine Creation Services (MCS) を使用してマシンをプロビジョニングするためのカタログを作成する場合、仮想マシンからハードウェアプロパティをキャプチャし、カタログ内の新しくプロビジョニングされたVMに適用するために、マシンプロファイルを使用できます。`MachineProfile`パラメーターが使用されていない場合、ハードウェアプロパティはマスターイメージVMまたはスナップショットからキャプチャされます。 明示的に定義する一部のプロパティ（例: `StorageType`、`CatalogZones`、`CryptoKeyIs`）は、マシンプロファイルから無視されます。

- マシンプロファイルを使用してカタログを作成するには、`New-ProvScheme`コマンドを使用します。例: `New-ProvScheme –MachineProfile "path to VM"`。`MachineProfile`パラメーターを指定しない場合、ハードウェアプロパティはマスターイメージVMからキャプチャされます。
- 新しいマシンプロファイルでカタログを更新するには、`Set-ProvScheme`コマンドを使用します。例: `Set-ProvScheme –MachineProfile "path to new VM"`。このコマンドは、カタログ内の既存のVMのマシンプロファイルを変更しません。カタログに追加された新しく作成されたVMのみが新しいマシンプロファイルを持ちます。
- マスターイメージを更新することもできますが、マスターイメージを更新してもハードウェアプロパティは更新されません。ハードウェアプロパティを更新する場合は、`Set-ProvScheme`コマンドを使用してマシンプロファイルを更新する必要があります。これらの変更は、カタログ内の新しいマシンにのみ適用されます。既存のマシンのハードウェアプロパティを更新するには、`Set-ProvVMUpdateTimeWindow`コマンドを`-StartsNow`および`-DurationInMinutes -1`パラメーターとともに使用できます。

> **注：**
>
> - `StartsNow`は、スケジュールされた開始時刻が現在の時刻であることを示します。
> - 負の数（例: –1）を指定した`DurationInMinutes`は、スケジュールの時間枠に上限がないことを示します。

マシンプロファイルをインスタンステンプレートとして使用してマシンカタログを作成する

マシンプロファイルの入力としてGCPインスタンステンプレートを選択できます。インスタンステンプレートはGCPの軽量リソースであるため、非常に費用対効果が高いです。

マシンプロファイルをインスタンステンプレートとして使用して新しいマシンカタログを作成する

1. PowerShellウィンドウを開きます。
2. `asnp citrix*`を実行して、Citrix固有のPowerShellモジュールをロードします。
3. 次のコマンドを使用して、GCPプロジェクトでインスタンステンプレートを見つけます。

```
cd XDHyp:\HostingUnits\<HostingUnitName>\instanceTemplates.folder
```

4. NewProvSchemeコマンドを使用して、マシンプロファイルをインスタンステンプレートとして新しいマシンカタログを作成します。

```
New-ProvScheme -ProvisioningSchemeName <CatalogName>  -HostingUnitName
<HostingUnitName> -IdentityPoolName <identity pool name> -MasterImageVM

XDHyp:\HostingUnits\<HostingUnitName> \Base.vm\Base.snapshot
-MachineProfile XDHyp:
\HostingUnits\<HostingUnitName>\instanceTemplates.folder\mytemplate.tem
plate
```

   New-ProvSchemeコマンドの詳細については、https://developer-docs.citrix.com/projects/citrix-daas-sdk/en/latest/MachineCreation/New-ProvScheme/を参照してください。

5. PowerShell コマンドを使用してマシンカタログの作成を完了します。Remote PowerShell SDK を使用してカタログを作成する方法については、https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/ を参照してください。

既存のマシンカタログのマシンプロファイルをインスタンステンプレートに変更する

既存のマシンカタログのマシンプロファイルをインスタンステンプレートに変更する詳細な手順は次のとおりです。

1. PowerShell ウィンドウを開きます。
2. Citrix固有のPowerShellモジュールをロードするために`asnp citrix*`を実行します。
3. 次のコマンドを実行します。

```
Set-ProvScheme -ProvisioningSchemeName  <CatalogName> -MachineProfile
XDHyp:
```

```
\HostingUnits\<HostingUnitName>\instanceTemplates.folder\<TemplateName>
.template
```

Set-ProvSchemeコマンドの詳細については、https://developer-docs.citrix.com/projects/citrix-daas-sdk/en/latest/MachineCreation/Set-ProvScheme/を参照してください。

PowerShell を使用して、シールドされたVMでカタログを作成する

シールドされたVMプロパティを持つMCSマシンカタログを作成できます。シールドされた仮想マシンは、セキュアブート、仮想トラステッドプラットフォームモジュール、UEFIファームウェア、整合性監視などの高度なプラットフォームセキュリティ機能を使用して、Compute Engineインスタンスの検証可能な整合性を提供する一連のセキュリティ制御によって強化されています。

MCSは、マシンプロファイルワークフローを使用してカタログを作成することをサポートしています。マシンプロファイルワークフローを使用する場合、VMインスタンスのシールドされたVMプロパティを有効にする必要があります。その後、このVMインスタンスをマシンプロファイルの入力として使用できます。

マシンプロファイルワークフローを使用して、シールドされたVMでMCSマシンカタログを作成するには。

1. Google Cloud コンソールでVMインスタンスのシールドされたVMオプションを有効にします。クイックスタート: シールドされたVMオプションを有効にするを参照してください。
2. VMインスタンスを使用して、マシンプロファイルワークフローでMCSマシンカタログを作成します。
    a. PowerShell ウィンドウを開きます。
    b. Citrix固有のPowerShellモジュールをロードするために`asnp citrix*`を実行します。
    c. まだ作成されていない場合は、IDプールを作成します。
    d. `New-ProvScheme`コマンドを実行します。例：

```
New-ProvScheme -ProvisioningSchemeName <catalog-name>

-HostingUnitName gcp-hostint-unit

-MasterImageVM XDHyp:\HostingUnits\gcp-hostint-unit\catalog-vda.vm

-MachineProfile XDHyp:\HostingUnits\gcp-hostint-unit\catalog-
machine.vm
```

3. マシンカタログの作成を完了します。

新しいマシンプロファイルでマシンカタログを更新するには:

1. `Set-ProvScheme`コマンドを実行します。例：

```
Set-ProvScheme -ProvisioningSchemeName <catalog-name>

-MasterImageVM XDHyp:\HostingUnits\<hostin-unit>\catalog-vda.vm

-MachineProfile "DHyp:\HostingUnits\<hostin-unit>\catalog-machine.vm
```

`Set-ProvScheme` で行った変更を既存のVMに適用するには、`Set-ProvVMUpdateTimeWindow` コマンドを実行します。

1. `Set-ProvVMUpdateTimeWindow` コマンドを実行します。例:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog -VMName
<List-Of-Vm-Names> -StartsNow -DurationInMinutes -1
```

2. VMを再起動します。

単一テナントノード上にWindows 11 VMを作成する

GCPでWindows 11 VMを作成できます。ただし、マスターイメージにWindows 11をインストールする場合は、マスターイメージ作成プロセス中にvTPMを有効にする必要があります。また、マシンプロファイルソース（VMまたはインスタンステンプレート）でvTPMを有効にする必要があります。

単一テナントノード上にWindows 11 VMを作成するための主な手順は次のとおりです。

1. Google Cloud仮想化環境をセットアップします。詳細については、「Google Cloud環境」を参照してください。
2. VDAをインストールします。「VDAのインストール」を参照してください。
3. Google Cloud環境への接続を作成します。詳細については、「Google Cloud環境への接続」を参照してください。
4. Windows 11 Bring Your Own License (BYOL) マスターイメージを作成し、そのイメージをGoogle Cloudにインポートします。「Windows 11 BYOLマスターイメージの作成」を参照してください。

5. マシンプロファイルソースを作成します: 単一テナントノード上にVMをプロビジョニングし、ソースマシンプロファイルのvTPMを有効にします。「単一テナントノード上でのVMのプロビジョニング」を参照してください。
6. vTPMが有効なWindows 11マシンプロファイルソースを使用してMCSマシンカタログを作成します。マシンプロファイルソースは、単一テナントノードで説明されているインスタンスタイプと同じである必要があります。「Windows 11マシンプロファイルソースを使用したMCSマシンカタログの作成」を参照してください。

Windows 11 BYOLマスターイメージを作成する

Windows 11 BYOLマスターイメージを作成し、そのマスターイメージをGoogle Cloudにインポートするには、2つのオプションがあります。

- Google Cloud Cloud Build Tools を使用する
- 他のハイパーバイザーでマスターイメージを作成する

GOOGLE CLOUD CLOUD BUILD TOOLS を使用する

1. Windows 11 ISO、GCP SDK、.NET Framework、および PowerShell インストーラーファイルを GCP ストレージバケットにアップロードします。
2. クラウドビルド `.yaml` ファイル内のファイルパスをパラメーターとして指定します。
3. コマンドラインから以下の Cloud Build を実行して、最終的な Windows 11 イメージをビルドします。GCP は、GCP の Daisy ワークフローを使用して、選択したプロジェクトでマスターイメージをブートストラップして作成し、マスターイメージは GCP にインポートされます。

```
gcloud compute instances import INSTANCE-NAME--source-uri=gs://BUCKET/
IMAGE-OVF-FILE.ovf --guest-os-features=UEFI_COMPATIBLE --byol --
machine-type=MACHINE-TYPE --zone=ZONE
```

> **注：**
>
> すべての大文字のテキストを実際の詳細リソースに置き換えます。

詳細については、「カスタム Windows BYOL イメージの作成」を参照してください。

他のハイパーバイザーでマスターイメージを作成する

1. 他のハイパーバイザーを使用して Windows 11 マスターイメージを作成します。
2. マスターイメージを OVF 形式でローカルマシンにエクスポートします。

3. ローカルの gcloud CLI を使用して、OVF ファイルを GCP ストレージバケットにアップロードします。

```
gsutil cp LOCAL_IMAGE_PATH_OVF_FILES gs://BUCKET_NAME/
```

4. コマンドラインから以下の Cloud Build を実行して、最終的な Windows 11 イメージをビルドします。GCP は、GCP の Daisy ワークフローを使用して、選択したプロジェクトでマスターイメージをブートストラップして作成し、マスターイメージは GCP にインポートされます。

```
gcloud compute instances import INSTANCE-NAME --source-uri=gs://BUCKET/
IMAGE-OVF-FILE.ovf --guest-os-features=UEFI_COMPATIBLE --byol --
machine-type=MACHINE-TYPE --zone=ZONE
```

> **注：**
>
> すべての大文字のテキストを実際のリソースの詳細に置き換えてください。

単一テナントノードでのVMのプロビジョニング

単一テナントノードを使用して、VMを他のプロジェクトのVMから物理的に分離したり、同じホストハードウェア上にVMをグループ化したりできます。単一テナントノードの詳細については、GCPドキュメント「Sole-tenancy overview」を参照してください。

単一テナントノードでのVM（マシンプロファイルソース）のプロビジョニングについては、GCPドキュメント「Provision VMs on sole-tenant nodes」を参照してください。

> **注：**
>
> - ノードグループと同じインスタンスタイプとリージョンを選択します。
> - Shielded VMセクションでvTPMを有効にします。詳細については、「Quickstart: Enable Shielded VM options」を参照してください。
> - ソースVMでBitlockerを無効にします。

Windows 11のマシンプロファイルソースを使用してMCSマシンカタログを作成する

Web StudioまたはPowerShellコマンドを使用して、Windows 11 VMを作成するためのMCSマシンカタログを作成できます。

注：

- マスターイメージには、Windows 11のスナップショットまたはVMを選択します。
- マシンプロファイルソースには、Windows 11 VMをマシンプロファイルとして選択します。マシンプロファイルソースは、単一テナントノードで説明されているものと同じインスタンスタイプである必要があります。

Web Studioの使用方法については、Web Studioを使用してマシンカタログを作成するを参照してください。

PowerShellコマンドについては、マシンプロファイルを使用してマシンカタログを作成するを参照してください。

カタログを作成し、VM の電源をオンにすると、Google Cloud コンソールで単一テナントノード上で実行されている Windows 11 VM を確認できます。

Google Cloud マーケットプレイス

Citrixが**Google Cloud Marketplace**で提供するイメージを参照して選択し、マシンカタログを作成できます。現在、MCSはこの機能に対してマシンプロファイルワークフローのみをサポートしています。

Google Cloud MarketplaceでCitrix VDA VM製品を検索するには、https://console.cloud.google.com/marketplaceにアクセスしてください。

Google Cloud MarketplaceでカスタムイメージまたはCitrix ready®イメージを使用して、マシンカタログのイメージを更新できます。

注：

マシンプロファイルにストレージタイプ情報が含まれていない場合、値はカスタムプロパティから派生します。

サポートされているGoogle Cloud Marketplaceイメージは次のとおりです。

- Windows 2019シングルセッション
- Windows 2019 マルチセッション
- ウブントゥ

Citrix対応イメージをマシンカタログ作成のソースとして使用する例:

```
New-ProvScheme -ProvisioningSchemeName GCPCatalog \

-HostingUnitName GcpHu -IdentityPoolName gcpPool -CleanOnBoot \

-MasterImageVM XDHyp:\HostingUnits\GcpHu\images.folder\citrix-daas-
win2019-single-vda-v20220819.publicimage \

-MachineProfile XDHyp:\HostingUnits\GcpHu\Base.vm
```

次のステップ

- これが最初に作成されたカタログである場合、Web Studioはデリバリーグループを作成するようにガイドします。
- 構成プロセス全体を確認するには、インストールと構成を参照してください。
- カタログを管理するには、マシンカタログを管理するおよびGoogle Cloud Platformカタログを管理するを参照してください。

詳細情報

- 接続とリソースを作成および管理する
- Google Cloud環境への接続
- マシンカタログを作成する

HPE Moonshot マシンカタログを作成する

(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/install-configure/machine-catalogs-create.html)は、マシンカタログを作成するウィザードについて説明しています。以下の情報は、HPE Moonshot環境に固有の詳細を扱っています。

注:

- HPE Moonshotへの接続を作成する
- 1つ以上のHPE Moonshotノードが利用可能であることを確認し、それらのノードにVDAをインストールしてください。
- 最初のHPE Moonshotカートリッジイメージの作成については、OS Deployment on Moonshot User Guideを参照してください。

HPE Moonshotマシンカタログは、以下を使用して作成できます。

- ウェブスタジオ
- PowerShellコマンド

Web Studioを使用してマシンカタログを作成する

マシンカタログのセットアップウィザードで、:

1. **オペレーティングシステム**ページで、**マルチセッションOS**または**シングルセッションOS**を選択します。
2. **マシン管理**ページで、**電源管理されているマシン**と**別のサービスまたはテクノロジー**を選択します。
3. **仮想マシン**ページで、マシンとそのActive Directoryマシンアカウントを追加します。次のいずれかを実行できます。
   - **マシンの追加**をクリックして、マシンを手動で追加します。**VMの選択**ウィンドウが表示されます。以前に作成したHPE Moonshotシャーシ接続を展開し、追加するノード（VM）を選択します。次に、関連するマシンアカウント名を追加します。
   - 「**CSVファイルの追加**」をクリックして、マシンを一括追加します。CSVファイルを使用してマシンを追加する方法については、「CSVファイルを使用してマシンをカタログに一括追加する」を参照してください。

スコープページと**概要**ページには、HPE Moonshot固有の情報は含まれていません。

PowerShellコマンドを使用してマシンカタログを作成する

ブローカーカタログを作成し、マシンをブローカーカタログにインポートするには、`New-BrokerCatalog`および`New-BrokerMachine` PowerShellコマンドを実行します。

例:

```
New-BrokerCatalog  -AdminAddress "MyDDC.MyDomain.local" -AdminClientIP
"103.14.252.249" -AllocationType "Random" -IsRemotePC $False
-MachinesArePhysical $False -MinimumFunctionalLevel "L7_20" -Name "BurMC"
-PersistUserChanges "OnLocal" -ProvisioningType "Manual" -Scope @()
-SessionSupport "MultiSession" -ZoneUid "e166e2cb-25dc-4578-bc07-
bcf2a82d1463"

New-BrokerMachine  -AdminAddress "MyDDC.MyDomain.local" -AdminClientIP
"103.14.252.249" -CatalogUid 3 -HostedMachineId "c10n1"
-HypervisorConnectionUid 4 -IsReserved $False -MachineName
"S-1-5-21-2589939477-3963209805-1860259709-1121"
```

次のステップ

- これが最初に作成するカタログである場合、Web Studioは(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/install-configure/delivery-groups-create.html)に誘導します。
- 構成プロセス全体を確認するには、(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/install-configure.html)を参照してください。
- カタログを管理するには、(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/install-configure/machine-catalogs-manage.html)および(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/install-configure/machine-catalogs-manage/manage-machine-catalog-hpe-moonshot.html)を参照してください。

詳細情報

- 接続とリソースの作成および管理
- HPE Moonshotへの接続
- マシンカタログの作成

Microsoft Azureカタログの作成

注：

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

(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/install-configure/machine-catalogs-create.html)では、マシンカタログを作成するウィザードについて説明しています。以下の情報は、Microsoft Azure Resource Managerクラウド環境に固有の詳細を扱っています。

注：

Microsoft Azureカタログを作成する前に、Microsoft Azureへの接続の作成を完了する必要があります。Microsoft Azureへの接続を参照してください。

マシンカタログの作成

マシンカタログは、次の2つの方法で作成できます。

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

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

イメージは、ディスク、スナップショット、またはAzure Compute Gallery内のイメージ定義のイメージバージョンであり、マシンカタログ内のVMを作成するために使用されます。マシンカタログを作成する前に、Azure Resource Managerでイメージを作成します。イメージに関する一般的な情報については、「マシンカタログの作成」を参照してください。

注：

ホスト接続で構成されているリージョンとは異なるリージョンからマスターイメージを使用するサポートは非推奨です。Azure Compute Galleryを使用して、マスターイメージを目的のリージョンにレプリケートしてください。

MCSマシンカタログを作成する際、DHCPの有効化やライセンスのリアームなどの準備タスクを実行するために、元のVMに基づいて一時的なVMが作成されます。この一時的なVMは準備VMと呼ばれます。この準備VMの名前は**Preparati-84x9n**という形式に従い、最後の5文字は重複を避けるためにランダムに生成されます。この準備VMの命名規則は固定されており、カスタマイズできません。準備タスクが完了すると、準備VMは破棄されます。

準備VMからネットワークを切断するために、すべてのインバウンドおよびアウトバウンドトラフィックを拒否するネットワークセキュリティグループが作成されます。ネットワークセキュリ

ティグループは、カタログごとに1回自動的に作成されます。ネットワークセキュリティグループの名前は`Citrix-Deny-All-a3pgu-GUID`で、GUIDはランダムに生成されます。例: `Citrix-Deny-All-a3pgu-3f161981-28e2-4223-b797-88b04d336dd1`。

マシンカタログ作成ウィザードで:

- 「**マシンタイプ**」および「**マシン管理**」ページには、Azure固有の情報は含まれていません。マシンカタログの作成の記事のガイダンスに従ってください。
- **イメージ**ページで、このカタログにマシンを作成するためのテンプレートとして使用するイメージを選択します。

  使用するイメージの種類として**マスターイメージ**を選択する場合は、**イメージの選択**をクリックし、必要に応じてマスターイメージを選択するために次の手順に従います。

  a. (テナント内またはテナント間で共有イメージが構成されている接続にのみ適用) イメージが存在するサブスクリプションを選択します。

  b. リソースグループを選択します。

  c. Azure VHD、Azure Compute Gallery、またはAzureイメージバージョンに移動します。必要に応じて、選択したイメージにメモを追加します。

  イメージを選択する際は、次の点を考慮してください。

  - イメージにCitrix VDAがインストールされていることを確認します。
  - VMに接続されているVHDを選択する場合は、次の手順に進む前にVMをシャットダウンする必要があります。

> **注：**
>
> - カタログ内のマシンを作成した接続（ホスト）に対応するサブスクリプションは、緑色の点で示されます。その他のサブスクリプションは、Azure Compute Galleryがそのサブスクリプションと共有されているものです。これらのサブスクリプションでは、共有ギャラリーのみが表示されます。共有サブスクリプションの構成方法については、テナント内でイメージを共有する（サブスクリプション間）およびテナント間でイメージを共有するを参照してください。
> - 信頼された起動が有効になっているイメージまたはスナップショットを選択する場合、**セキュリティの種類**として信頼された起動を持つマシンプロファイルを使用することは必須です。その後、マシンプロファイルでSecureBootとvTPMの値を指定する

ことで、それらを有効または無効にできます。信頼された起動はShared Image Galleryではサポートされていません。Azureの信頼された起動に関する情報については、`<https://docs.microsoft.com/ja-jp/azure/virtual-machines/trusted-launch>`を参照してください。

- 信頼された起動が有効なWindowsで、エフェメラルOSディスクを使用してプロビジョニングスキームを作成できます。信頼された起動が有効なイメージを選択する場合、vTPMが有効な信頼された起動を持つマシンプロファイルを選択する必要があります。エフェメラルOSディスクを使用してマシンカタログを作成するには、「エフェメラルOSディスクを使用してマシンを作成する方法」を参照してください。
- イメージのレプリケーションが進行中でも、イメージをマスターイメージとして選択し、セットアップを完了できます。ただし、イメージのレプリケーション中はカタログ作成に時間がかかる場合があります。MCSでは、カタログ作成開始から1時間以内にレプリケーションが完了する必要があります。レプリケーションがタイムアウトすると、カタログ作成は失敗します。Azureでレプリケーションステータスを確認できます。レプリケーションがまだ保留中の場合、またはレプリケーションが完了した後に再度試してください。
- Azureでマシンカタログのマスターイメージを選択すると、MCSは選択したマスターイメージとマシンプロファイルに基づいてOSタイプを識別します。MCSが識別できない場合は、マスターイメージに一致するOSタイプを選択します。
- Gen2イメージを使用してGen2 VMカタログをプロビジョニングすることで、起動時間のパフォーマンスを向上させることができます。ただし、Gen1イメージを使用してGen2マシンカタログを作成することはサポートされていません。同様に、Gen2イメージを使用してGen1マシンカタログを作成することもサポートされていません。また、世代情報を持たない古いイメージはすべてGen1イメージです。

使用するイメージの種類として**準備済みイメージ**を選択する場合は、**イメージの選択**をクリックし、必要に応じて準備済みイメージを選択します。

VMの作成を成功させるには、イメージにCitrix VDA 2311以降がインストールされており、VDAにMCSIOが存在することを確認してください。

イメージを選択すると、**マシンプロファイルを使用する (Azure Active Directoryでは必須)** チェックボックスが自動的に選択されます。**マシンプロファイルの選択**をクリックして、リソースグループのリストからVMまたはARMテンプレート仕様を参照します。カタログ内のVMは、選択したマシンプロファイルから構成を継承できます。

ARMテンプレート仕様がマシンカタログを作成するためのマシンプロファイルとして使用できることを確認するために検証します。ARMテンプレート仕様を検証する方法は2つあります。

- リソースグループリストからARMテンプレート仕様を選択した後、**次へ**をクリックします。ARMテンプレート仕様にエラーがある場合、エラーメッセージが表示されます。
- 次のPowerShellコマンドのいずれかを実行します。
  - `Test-ProvInventoryItem -HostingUnitName <string> -InventoryPath <string>`
  - `Test-ProvInventoryItem -HostingUnitUid <Guid> -InventoryPath <string>`

VMがマシンプロファイルから継承できる構成の例は次のとおりです。

- アクセラレーテッドネットワーク
- ブート診断
- ホストディスクキャッシュ (OSおよびMCSIOディスクに関連)
- マシンサイズ (別途指定がない限り)
- VMに配置されたタグ

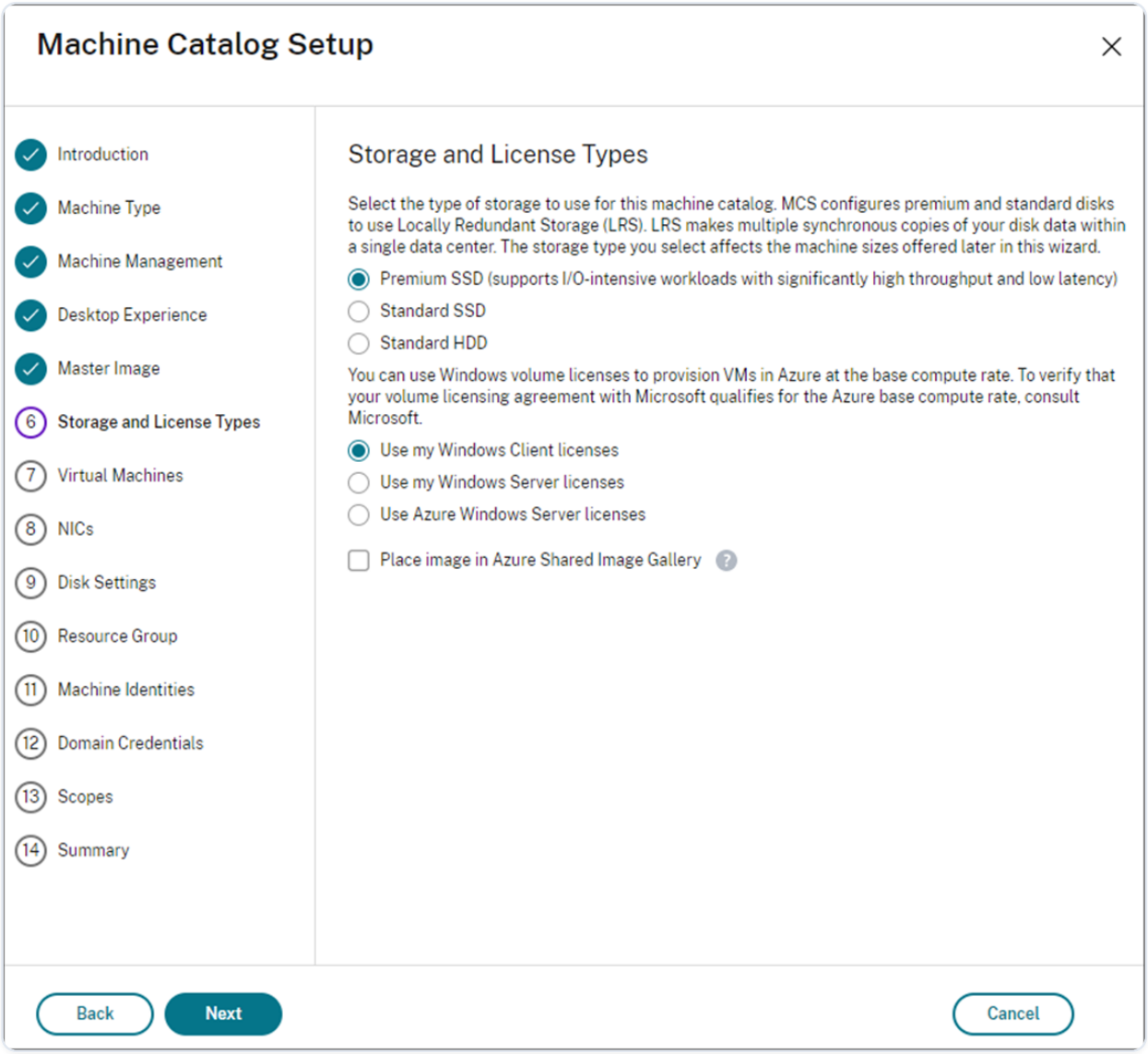
カタログを作成した後、イメージがマシンプロファイルから継承する構成を表示できます。**マシンカタログ**ノードでカタログを選択し、下部のペインで詳細を表示します。次に、**テンプレートプロパティ**タブをクリックして、マシンプロファイルのプロパティを表示します。**タグ**セクションには最大3つのタグが表示されます。VMに配置されているすべてのタグを表示するには、**すべて表示**をクリックします。

MCSでAzure専用ホストにVMをプロビジョニングする場合は、**専用ホストグループを使用**チェックボックスを有効にしてから、リストからホストグループを選択します。ホストグループは、専用ホストのコレクションを表すリソースです。専用ホストは、1つ以上のVMをホストする物理サーバーを提供するサービスです。サーバーはAzureサブスクリプション専用であり、他のサブスクライバーと共有されることはありません。専用ホストを使用すると、AzureはVMがそのホストで実行されている唯一のマシンであることを保証します。この機能は、規制要件または内部セキュリティ要件を満たす必要があるシナリオに適しています。ホストグループとその使用に関する考慮事項の詳細については、「Azure 専用ホスト」を参照してください。

> **重要:**

- Azure自動配置が有効になっているホストグループのみが表示されます。
- ホストグループを使用すると、ウィザードの後半で提供される**仮想マシン**ページが変更されます。選択したホストグループに含まれるマシンサイズのみがそのページに表示されます。また、可用性ゾーンは自動的に選択され、選択できません。

- **ストレージとライセンスの種類**ページは、Azure Resource Managerイメージを使用する場合にのみ表示されます。



マシンカタログで使用できるストレージの種類は次のとおりです。

- I/O負荷の高いワークロードを持つVMに適した、高性能で低遅延のディスクストレージオプションとして、「**Premium SSD**」を提供します。
- **Standard SSD**。低いIOPSレベルで一貫したパフォーマンスを必要とするワークロードに適した、費用対効果の高いストレージオプションを提供します。

- **Standard HDD**。待機時間に影響を受けにくいワークロードを実行する VM に適した、信頼性の高い低コストのディスクストレージオプションを提供します。
- **Azureエフェメラルosディスク**。VMのローカルディスクを再利用してオペレーティングシステムディスクをホストする、費用対効果の高いストレージオプションを提供します。または、PowerShellを使用してエフェメラルOSディスクを使用するマシンを作成することもできます。詳細については、「Azureエフェメラルディスク」を参照してください。エフェメラルOSディスクを使用する際は、次の考慮事項に注意してください。
  - Azure エフェメラル OS ディスクと MCS I/O は同時に有効にできません。
  - エフェメラル OS ディスクを使用するマシンを更新するには、VM のキャッシュディスクまたは一時ディスクのサイズを超えないイメージを選択する必要があります。
  - ウィザードの後半で提供される**電源サイクル中に VM とシステムディスクを保持**オプションは使用できません。

> **注：**
>
> 選択したストレージの種類に関係なく、IDディスクは常にStandard SSDを使用して作成されます。

> ストレージの種類によって、ウィザードの**仮想マシン**ページで提供されるマシンのサイズが決まります。MCSは、プレミアムディスクと標準ディスクをローカル冗長ストレージ（LRS）を使用するように構成します。LRSは、単一のデータセンター内でディスクデータの複数の同期コピーを作成します。AzureエフェメラルOSディスクは、VMのローカルディスクを使用してオペレーティングシステムを保存します。Azureストレージの種類とストレージレプリケーションの詳細については、以下を参照してください。

- `<https://docs.microsoft.com/ja-jp/azure/storage/common/storage-introduction/>`
- `<https://docs.microsoft.com/ja-jp/azure/virtual-machines/premium-storage-performance/>`
- `<https://docs.microsoft.com/ja-jp/azure/storage/common/storage-redundancy/>`

既存のWindowsライセンスまたはLinuxライセンスを使用するかどうかを選択します。

- Windowsライセンス：WindowsライセンスをWindowsイメージ（Azureプラットフォームサポートイメージまたはカスタムイメージ）とともに使用すると、AzureでWindows VMを低コストで実行できます。ライセンスには次の2種類があります。
  - **Windows Serverライセンス**。Windows ServerまたはAzure Windows Serverライセンスを使用でき、Azureハイブリッド特典を利用できます。詳細については、`<https://azure.microsoft.com/ja-jp/pricing/hybrid-benefit/>`を参照してください。Azureハイブリッド特典は、AzureでVMを実行するコストを基本コンピューティング料金に削減し、Azureギャラリーからの追加のWindows Serverライセンスのコストを免除します。
  - **Windowsクライアントライセンス**。Windows 10およびWindows 11ライセンスをAzureに持ち込むことができ、追加のライセンスなしでAzureでWindows 10およびWindows 11 VMを実行できます。詳細については、「クライアントアクセスライセンスと管理ライセンス」を参照してください。

プロビジョニングされたVMがライセンス特典を使用しているかどうかは、次のPowerShellコマンドを実行して確認できます: `Get-AzVM -ResourceGroup MyResourceGroup -Name MyVM`。

- Windows Serverライセンスタイプの場合、ライセンスタイプが **Windows_Server** であることを確認します。詳細な手順は `<https://docs.microsoft.com/ja-jp/azure/virtual-machines/windows/hybrid-use-benefit-licensing/>` で入手できます。
- Windows Clientライセンスタイプの場合、ライセンスタイプが **Windows_Client** であることを確認します。詳細な手順は `<https://docs.microsoft.com/ja-jp/azure/virtual-machines/windows/windows-desktop-multitenant-hosting-deployment/>` で入手できます。

あるいは、`Get-Provscheme` PowerShell SDKを使用して検証を行うこともできます。例: `Get-Provscheme -ProvisioningSchemeName "My Azure Catalog"`。このコマンドレットの詳細については、`<https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/MachineCreation/Get-ProvScheme/>` を参照してください。

- Linuxライセンス：BYOS（bring-your-own-subscription）Linuxライセンスを使用すると、ソフトウェアの料金を支払う必要はありません。BYOS料金には、コンピューティングハードウェア料金のみが含まれます。ライセンスには次の2種類があります。
  - **RHEL_BYOS**: RHEL_BYOSタイプを正常に使用するには、AzureサブスクリプションでRed Hat Cloud Accessを有効にします。

- **SLES_BYOS**: SLESのBYOSバージョンには、SUSEからのサポートが含まれています。

LicenseTypeの値を、`New-ProvScheme` および `Set-ProvScheme` のLinuxオプションに設定できます。

`New-ProvScheme` でLicenseTypeをRHEL_BYOSに設定する例:

```
New-ProvScheme -CleanOnBoot -ProvisioningSchemeName "azureCatalog"
-RunAsynchronously -Scope @() -SecurityGroup @() -CustomProperties
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance"><Property xsi:type="StringProperty" Name="UseManagedDisks"
Value="true" /><Property xsi:type="StringProperty"
Name="StorageAccountType" Value="StandardSSD_LRS" /><Property
xsi:type="StringProperty" Name="ResourceGroups" Value="hu-dev-mcs" /
><Property xsi:type="StringProperty" Name="OsType" Value="Linux" /
><Property xsi:type="StringProperty" Name="LicenseType"
Value="RHEL_BYOS" /></CustomProperties>'
```

`Set-ProvScheme` でLicenseTypeをSLES_BYOSに設定する例:

```
Set-ProvScheme -ProvisioningSchemeName "azureCatalog"
-CustomProperties '<CustomProperties xmlns="http://
schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance"><Property
xsi:type="StringProperty" Name="UseManagedDisks" Value="true" /
><Property xsi:type="StringProperty" Name="StorageAccountType"
Value="StandardSSD_LRS" /><Property xsi:type="StringProperty"
Name="ResourceGroups" Value="hu-dev-mcs" /><Property
xsi:type="StringProperty" Name="OsType" Value="Linux" /><Property
xsi:type="StringProperty" Name="LicenseType" Value="SLES_BYOS" /></
CustomProperties>'
```

> **注：**
>
> `LicenseType` の値が空の場合、デフォルト値はOsTypeの値に応じてAzure Windows Server LicenseまたはAzure Linux Licenseになります。

> LicenseType を空に設定する例:

```
Set-ProvScheme -ProvisioningSchemeName "azureCatalog"
-CustomProperties '<CustomProperties xmlns="http://
schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance"><Property
xsi:type="StringProperty" Name="UseManagedDisks" Value="true" /
><Property xsi:type="StringProperty" Name="StorageAccountType"
Value="StandardSSD_LRS" /><Property xsi:type="StringProperty"
Name="ResourceGroups" Value="hu-dev-mcs" /><Property
xsi:type="StringProperty" Name="OsType" Value="Linux" /></
CustomProperties>'
```

ライセンスの種類とその利点については、以下のドキュメントを参照してください。

- `<https://docs.microsoft.com/ja-jp/dotnet/api/microsoft.azure.management.compute.models.virtualmachine.licensetype?view=azure-dotnet>`
- `<https://docs.microsoft.com/ja-jp/azure/virtual-machines/linux/azure-hybrid-benefit-linux>`

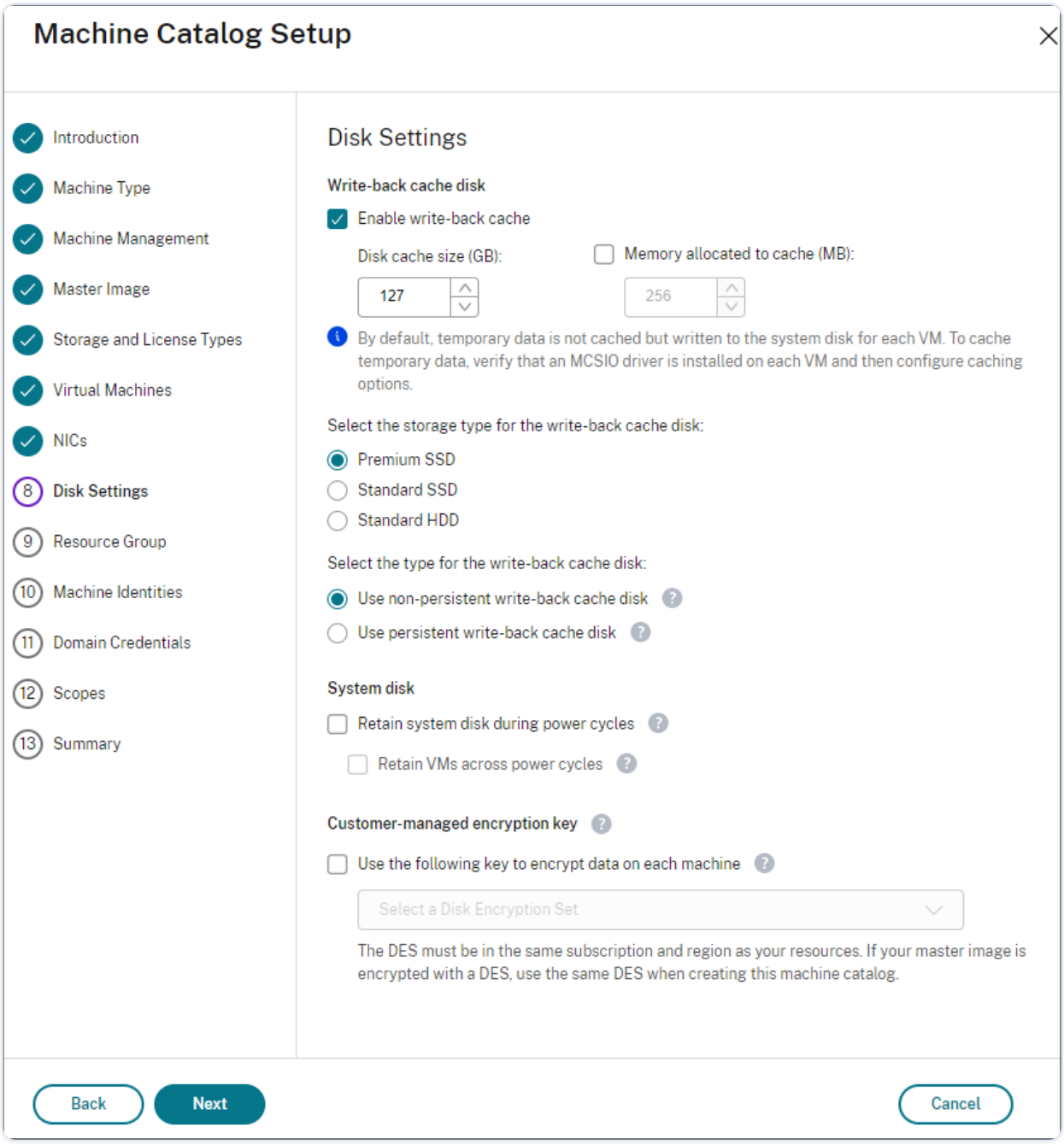
Azure Compute Gallery（旧Azure Shared Image Gallery）は、イメージを管理および共有するためのリポジトリです。これにより、組織全体でイメージを利用できるようになります。大規模な非永続マシンカタログを作成する際には、VDA OSディスクのリセットを高速化できるため、イメージをSIGに保存することをお勧めします。**準備されたイメージをAzure Compute Galleryに配置**を選択すると、**Azure Compute Gallery設定**セクションが表示され、追加のAzure Compute Gallery設定を指定できます。

- **仮想マシンとイメージレプリカの比率**。Azureが保持する仮想マシンとイメージレプリカの比率を指定できます。デフォルトでは、Azureは非永続マシン40台ごとに1つのイメージレプリカを保持します。永続マシンの場合、この数値はデフォルトで1,000です。
- **最大レプリカ数**。Azure に保持させたいイメージレプリカの最大数を指定できます。デフォルトは 10 です。

> **注：**

> イメージを保存するために、ACG にギャラリーが作成されます。このギャラリーは、VM 作成のために MCS からのみアクセス可能であり、**イメージの選択**ページには表示されません。

- **仮想マシン**ページで、作成する VM の数を指定します。少なくとも 1 つを指定し、マシンサイズを選択する必要があります。カタログ作成後、カタログを編集することでマシンサイズを変更できます。
- **NICs**ページにはAzure固有の情報は含まれていません。マシンカタログの作成の記事のガイダンスに従ってください。
- **ディスク設定**ページで、ライトバックキャッシュを有効にするかどうかを選択します。MCS ストレージ最適化機能が有効になっている場合、カタログ作成時に以下の設定を構成できます。これらの設定は、Azure と GCP の両方の環境に適用されます。



ライトバックキャッシュを有効にした後、以下を実行できます。

- 一時データをキャッシュするために使用するディスクとRAMのサイズを構成します。詳細については、「一時データのキャッシュの構成」を参照してください。
- ライトバックキャッシュディスクのストレージタイプを選択します。ライトバックキャッシュディスクには、次のストレージオプションを使用できます。
  - プレミアム SSD
  - スタンダード SSD
  - スタンダード HDD

- プロビジョニングされたVMに対してライトバックキャッシュディスクを永続化するかどうかを選択します。オプションを有効にするには、**ライトバックキャッシュを有効にする**を選択します。デフォルトでは、**非永続ライトバックキャッシュディスクを使用する**が選択されています。
- ライトバックキャッシュディスクの種類を選択します。
  - **非永続ライトバックキャッシュディスクを使用する**。選択した場合、ライトバックキャッシュディスクは電源サイクル中に削除されます。そこにリダイレクトされたデータはすべて失われます。VMの一時ディスクに十分な空き容量がある場合、コストを削減するためにライトバックキャッシュディスクをホストするために使用されます。カタログ作成後、プロビジョニングされたマシンが一時ディスクを使用しているかどうかを確認できます。これを行うには、カタログをクリックし、**テンプレートプロパティ**タブの情報を確認します。一時ディスクが使用されている場合、**非永続ライトバックキャッシュディスク**が表示され、その値は**はい（VMの一時ディスクを使用）**となります。そうでない場合、非永続ライトバックキャッシュディスクが表示され、その値は**いいえ（VMの一時ディスクを使用しない）**となります。
  - **永続ライトバックキャッシュディスクを使用する**。選択した場合、ライトバックキャッシュディスクはプロビジョニングされたVMに対して永続的になります。このオプションを有効にすると、ストレージコストが増加します。
- 電源サイクル中にVDAのVMとシステムディスクを保持するかどうかを選択します。

  電源サイクル中に VM とシステムディスクを保持する。ライトバックキャッシュを有効にするを選択した場合に利用可能です。デフォルトでは、VM とシステムディスクはシャットダウン時に削除され、起動時に再作成されます。VM の再起動時間を短縮したい場合は、このオプションを選択します。このオプションを有効にすると、ストレージコストも増加することに注意してください。
- **ストレージコストの節約**を有効にするかどうかを選択します。有効にすると、VM シャットダウン時にストレージディスクを Standard HDD にダウングレードすることで、ストレージコストを節約できます。VM は再起動時に元の設定に戻ります。このオプションは、ストレージディスクとライトバックキャッシュディスクの両方に適用されます。または、PowerShell を使用することもできます。VM シャットダウン時にストレージタイプを下位層に変更するを参照してください。

> **注：**

> Microsoftは、VMシャットダウン中のストレージタイプの変更に制限を課しています。また、Microsoftが将来的にストレージタイプの変更をブロックする可能性もあります。詳細については、このMicrosoft記事を参照してください。

  - カタログでプロビジョニングされたマシン上のデータを暗号化するかどうかを選択します。顧客管理の暗号化キーによるサーバー側暗号化により、マネージドディスクレベルで暗号化を管理し、カタログ内のマシン上のデータを保護できます。詳細については、Azure サーバー側暗号化を参照してください。

- **リソースグループ** ページで、リソースグループを作成するか、既存のグループを使用するかを選択します。

  - リソースグループを作成することを選択した場合は、**次へ** を選択します。
  - 既存のリソースグループを使用することを選択した場合、**利用可能なプロビジョニングリソースグループ**リストからグループを選択します。**注意**: カタログで作成するマシンを収容するのに十分な数のグループを選択してください。少なすぎるグループを選択すると、メッセージが表示されます。後でカタログに VM を追加する予定がある場合は、必要最小限よりも多く選択することをお勧めします。カタログ作成後、カタログにリソースグループを追加することはできません。

  詳細については、Azure リソースグループを参照してください。

- **マシンID**ページで、IDタイプを選択し、このカタログ内のマシン用のIDを構成します。VM を **Azure Active Directory に参加済み**として選択した場合、それらを Azure AD セキュリティグループに追加できます。詳細な手順は次のとおりです。

  a. **IDタイプ**フィールドから、**Azure Active Directory に参加済み**を選択します。**Azure AD セキュリティグループ (オプション)**オプションが表示されます。
  b. **Azure AD セキュリティグループ: 新規作成**をクリックします。
  c. グループ名を入力し、**作成**をクリックします。
  d. 画面の指示に従って Azure にサインインします。 グループ名が Azure に存在しない場合、緑色のアイコンが表示されます。それ以外の場合は、新しい名前を入力するよう求めるエラーメッセージが表示されます。
  e. VM のマシンアカウントの命名スキームを入力します。

  カタログ作成後、Citrix Virtual Apps and Desktops™ はユーザーに代わって Azure にアクセスし、セキュリティグループと、そのグループの動的メンバーシップルールを作成します。この

ルールに基づき、このカタログで指定された命名スキームを持つ VM は自動的にセキュリティグループに追加されます。

このカタログに異なる命名スキームを持つ VM を追加するには、Azure にサインインする必要があります。その後、Citrix Virtual Apps and Desktops は Azure にアクセスし、新しい命名スキームに基づいて動的メンバーシップルールを作成できます。

このカタログを削除する際、Azure からセキュリティグループを削除するには、Azure へのサインインも必要です。

- **ドメイン資格情報**ページと**概要**ページには、Azure 固有の情報は含まれていません。マシンカタログの作成の記事のガイダンスに従ってください。

ウィザードを完了します。

Azure一時ディスクがライトバックキャッシュディスクとして適格であるための条件

Azure一時ディスクをライトバックキャッシュディスクとして使用できるのは、以下のすべての条件が満たされている場合のみです。

- Azure一時ディスクは永続的なデータには適さないため、ライトバックキャッシュディスクは非永続的である必要があります。
- 選択したAzure VMサイズには一時ディスクが含まれている必要があります。
- エフェメラルOSディスクを有効にする必要はありません。
- ライトバックキャッシュファイルをAzure一時ディスクに配置することを受け入れます。
- Azure一時ディスクのサイズは、（ライトバックキャッシュディスクサイズ + ページングファイル用の予約スペース + 1 GBのバッファースペース）の合計サイズよりも大きい必要があります。

非永続的なライトバックキャッシュディスクのシナリオ

次の表は、マシンカタログの作成時に一時ディスクをライトバックキャッシュに使用する場合の3つの異なるシナリオについて説明しています。

シナリオ	結果
ライトバックキャッシュに一時ディスクを使用するためのすべての条件が満たされています。	WBCファイル `mcsdif.vhdx` は一時ディスクに配置されます。

シナリオ	結果
一時ディスクには、ライトバックキャッシュの使用に十分なスペースがありません。	VHDディスク `MCSWCDisk` が作成され、WBCファイル `mcsdif.vhdx` がこのディスクに配置されます。
一時ディスクにはライトバックキャッシュの使用に十分なスペースがありますが、`UseTempDiskForWBC` が **false** に設定されています。	VHDディスク `MCSWCDisk` が作成され、WBCファイル `mcsdif.vhdx` がこのディスクに配置されます。

Azure テンプレート仕様を作成する

Azure ポータルで Azure テンプレート仕様を作成し、Web Studio および PowerShell コマンドで使用して、MCS マシンカタログを作成または更新できます。

既存のVMのAzureテンプレートスペックを作成するには：

1. Azureポータルに移動します。リソースグループを選択し、VMとネットワークインターフェースを選択します。上部にある**...**メニューから、**テンプレートのエクスポート**をクリックします。
2. カタログプロビジョニング用のテンプレート仕様を作成する場合は、**パラメーターを含める**チェックボックスをオフにします。
3. 後でテンプレート仕様を変更するには、**ライブラリに追加**をクリックします。
4. **テンプレートのインポート**ページで、**名前**、**サブスクリプション**、**リソースグループ**、**場所**、**バージョン**などの必要な情報を入力します。**次へ: テンプレートの編集**をクリックします。
5. カタログをプロビジョニングする場合は、独立したリソースとしてネットワークインターフェイスも必要です。したがって、テンプレート仕様で指定されている `dependsOn` を削除する必要があります。例:

   ```
   "dependsOn": [

   "[resourceId('Microsoft.Network/networkInterfaces', 'tnic937')]"

   ],
   ```

6. **レビュー+作成**を作成し、テンプレートスペックを作成します。
7. **テンプレート仕様**ページで、作成したばかりのテンプレート仕様を確認します。テンプレート仕様をクリックします。左側のパネルで、**バージョン**をクリックします。

8. **新しいバージョンの作成**をクリックして、新しいバージョンを作成できます。新しいバージョン番号を指定し、現在のテンプレートスペックに変更を加え、**レビュー+作成**をクリックしてテンプレートスペックの新しいバージョンを作成します。

以下のPowerShellコマンドを使用して、テンプレートスペックとテンプレートバージョンの情報を取得できます。

- テンプレートスペックの情報を取得するには、以下を実行します。

```
get-item XDHyp:
\HostingUnits\East\machineprofile.folder\abc.resourcegroup\bggTemplateS
pec.templatespec
```

- テンプレートスペックバージョンの情報を取得するには、以下を実行します。

```
get-item XDHyp:
\HostingUnits\East\machineprofile.folder\abc.resourcegroup\bggTemplateS
pec.templatespec\bgg1.0.templatespecversion
```

カタログの作成または更新でテンプレート仕様を使用する

MCSマシンカタログは、マシンプロファイル入力としてテンプレート仕様を使用して作成または更新できます。これを行うには、Web StudioまたはPowerShellコマンドを使用できます。

- Web Studioについては、「Web StudioでAzure Resource Managerイメージを使用してマシンカタログを作成する」を参照してください。
- PowerShellについては、「PowerShellを使用してカタログを作成または更新する際にテンプレート仕様を使用する」を参照してください。

Azureサーバー側暗号化

Citrix Virtual Apps and Desktopsは、Azure Key Vaultを介したAzureマネージドディスクの顧客管理暗号化キーをサポートしています。このサポートにより、独自の暗号化キーを使用してマシンカタログのマネージドディスクを暗号化することで、組織およびコンプライアンス要件を管理できます。詳細については、「Azure Disk Storageのサーバー側暗号化」を参照してください。

マネージドディスクでこの機能を使用する場合：

- ディスクの暗号化に使用するキーを変更するには、`DiskEncryptionSet` で現在のキーを変更します。その `DiskEncryptionSet` に関連付けられているすべてのリソースは、新しいキーで暗号化されるように変更されます。

- キーを無効にするか削除すると、そのキーを使用しているディスクを持つVMは自動的にシャットダウンします。シャットダウン後、キーが再度有効になるか、新しいキーを割り当てない限り、VMは使用できません。そのキーを使用しているカタログは電源をオンにできず、VMを追加することもできません。

顧客管理暗号化キーを使用する際の重要な考慮事項

この機能を使用する際は、以下を考慮してください。

- 顧客管理キーに関連するすべてのリソース（Azure Key Vault、ディスク暗号化セット、VM、ディスク、スナップショット）は、同じサブスクリプションとリージョンに存在する必要があります。
- 顧客管理暗号化キーを有効にすると、後で無効にすることはできません。顧客管理暗号化キーを無効にするか削除する場合は、すべてのデータを顧客管理暗号化キーを使用していない別のマネージドディスクにコピーしてください。
- サーバー側暗号化と顧客管理キーを使用して暗号化されたカスタムイメージから作成されたディスクは、同じ顧客管理キーを使用して暗号化する必要があります。これらのディスクは同じサブスクリプション内にある必要があります。
- サーバー側暗号化と顧客管理キーで暗号化されたディスクから作成されたスナップショットは、同じ顧客管理キーで暗号化する必要があります。
- 顧客管理キーで暗号化されたディスク、スナップショット、およびイメージは、別のリソースグループやサブスクリプションに移動できません。
- 現在または以前にAzure Disk Encryptionを使用して暗号化されたマネージドディスクは、顧客管理キーを使用して暗号化することはできません。
- ディスク暗号化セットのリージョンごとの制限については、Microsoft サイトを参照してください。

> **注：**
>
> Azure サーバー側暗号化の構成については、クイックスタート: Azure portal を使用して Key Vault を作成する を参照してください。

Azureカスタマーマネージド暗号化キー

マシンカタログを作成する際、カタログにプロビジョニングされたマシン上のデータを暗号化するかどうかを選択できます。カスタマーマネージド暗号化キーによるサーバー側暗号化を使用すると、マネージドディスクレベルで暗号化を管理し、カタログ内のマシン上のデータを保護でき

ます。ディスク暗号化セット（DES）は、カスタマーマネージドキーを表します。この機能を使用するには、まずAzureでDESを作成する必要があります。DESは次の形式です。

- `/subscriptions/12345678-1234-1234-1234-123456789012/resourceGroups/Sample-RG/providers/Microsoft.Compute/diskEncryptionSets/SampleEncryptionSet`

リストからDESを選択します。選択するDESは、リソースと同じサブスクリプションおよびリージョンにある必要があります。イメージがDESで暗号化されている場合は、マシンカタログの作成時に同じDESを使用します。カタログ作成後にDESを変更することはできません。

暗号化キーを使用してカタログを作成し、後でAzureで対応するDESを無効にした場合、カタログ内のマシンの電源をオンにしたり、マシンを追加したりすることはできなくなります。

「顧客管理キーを使用したマシンカタログの作成」を参照してください。

ホストでのAzureディスク暗号化

ホストでの暗号化機能を備えたMCSマシンカタログを作成できます。現在、MCSはこの機能に対してマシンプロファイルのワークフローのみをサポートしています。VMまたはテンプレート仕様をマシンプロファイルの入力として使用できます。

この暗号化方法は、Azureストレージを介してデータを暗号化しません。VMをホストするサーバーがデータを暗号化し、その後、暗号化されたデータがAzureストレージサーバーを介して流れます。したがって、この暗号化方法はデータをエンドツーエンドで暗号化します。

制限事項：

ホストでのAzureディスク暗号化は次のとおりです。

- すべてのAzureマシンサイズでサポートされているわけではありません
- Azure ディスク暗号化と互換性がありません

ホストでの暗号化機能を持つマシンカタログを作成するには：

1. サブスクリプションでホストでの暗号化機能が有効になっているかどうかを確認します。これを行うには、`<https://learn.microsoft.com/ja-jp/rest/api/resources/features/get?tabs=HTTP/>`を参照してください。有効になっていない場合は、サブスクリプションでこの機能を有効にする必要があります。サブスクリプションで機能を有効にする方法については、`<https://learn.microsoft.com/ja-jp/azure/virtual-machines/disks-enable-host-based-encryption-portal?tabs=azure-powershell#prerequisites/>`を参照してください。

2. 特定のAzure VMサイズがホストでの暗号化をサポートしているかどうかを確認します。これを行うには、PowerShellウィンドウで次のいずれかを実行します。

```
PS XDHyp:\Connections\<your connection>\east
us.region\serviceoffering.folder>
```

```
PS XDHyp:\HostingUnits\<your hosting unit>\serviceoffering.folder>
```

3. ホストでの暗号化が有効になっているVMまたはテンプレート仕様を、マシンプロファイルの入力としてAzureポータルで作成します。

   - VMを作成する場合は、ホストでの暗号化をサポートするVMサイズを選択します。VMを作成すると、VMプロパティの**ホストでの暗号化**が有効になります。
   - テンプレート仕様を使用する場合は、`securityProfile`内でパラメーター`Encryption at Host`を**true**として割り当てます。

4. VMまたはテンプレート仕様のいずれかを選択して、マシンプロファイルワークフローでMCSマシンカタログを作成します。

   - OSディスク/データディスク：顧客管理キーとプラットフォーム管理キーを介して暗号化されます
   - エフェメラルOSディスク：プラットフォーム管理キーのみを介して暗号化されます
   - キャッシュディスク: 顧客管理キーとプラットフォーム管理キーによって暗号化されます

   Web StudioまたはPowerShellコマンドを実行して、マシンカタログを作成できます。

マシンプロファイルからホストでの暗号化情報を取得する

`AdditionalData` パラメーターを指定して PowerShell コマンドを実行すると、マシンプロファイルからホストでの暗号化情報を取得できます。`EncryptionAtHost` パラメーターが **True** の場合、そのマシンプロファイルでホストでの暗号化が有効になっていることを示します。

例: マシンプロファイルの入力が VM の場合、次のコマンドを実行します。

```
(get-item XDHyp:
\HostingUnits\myAzureNetwork\machineprofile.folder\abc.resourcegroup\def.v
m).AdditionalData
```

例: マシンプロファイルの入力がテンプレート仕様の場合、次のコマンドを実行します。

```
(get-item XDHyp:
\HostingUnits\myAzureNetwork\machineprofile.folder\abc.resourcegroup\def_t
emplatespec.templatespec\EncryptionAtHost.templatespecversion).AdditionalD
ata
```

マネージドディスクの二重暗号化

二重暗号化を使用してマシンカタログを作成できます。この機能で作成されたカタログはすべて、プラットフォームキーと顧客管理キーの両方でサーバー側が暗号化されます。Azure Key Vault、暗号化キー、およびディスク暗号化セット (DES) はお客様が所有および管理します。

二重暗号化は、プラットフォーム側暗号化（デフォルト）と顧客管理暗号化（CMEK）です。したがって、暗号化アルゴリズム、実装、または侵害されたキーに関連するリスクを懸念するセキュリティ意識の高いお客様は、この二重暗号化を選択できます。永続的なOSディスクとデータディスク、スナップショット、およびイメージはすべて、二重暗号化によって保存時に暗号化されます。

注：

- Web StudioおよびPowerShellコマンドを使用して、二重暗号化されたマシンカタログを作成および更新できます。PowerShellコマンドについては、「二重暗号化されたマシンカタログを作成する」を参照してください。
- 二重暗号化を使用してマシンカタログを作成または更新するには、マシンプロファイルに基づかないワークフローまたはマシンプロファイルに基づくワークフローを使用できます。
- マシンプロファイルに基づかないワークフローを使用してマシンカタログを作成する場合、保存されている `DiskEncryptionSetId` を再利用できます。
- マシンプロファイルを使用する場合、VM またはテンプレート仕様をマシンプロファイルの入力として使用できます。

制限事項:

- 二重暗号化は、Ultra Disks または Premium SSD v2 ディスクではサポートされていません。
- 二重暗号化は、アンマネージドディスクではサポートされていません。
- カタログに関連付けられているDiskEncryptionSetキーを無効にすると、そのカタログのVMが無効になります。

- お客様が管理するキーに関連するすべてのリソース（Azure Key Vault、ディスク暗号化セット、VM、ディスク、スナップショット）は、同じサブスクリプションとリージョンにある必要があります。
- サブスクリプションごとに、リージョンあたり最大50個のディスク暗号化セットしか作成できません。
- 異なる`DiskEncryptionSetId`を持つ`DiskEncryptionSetId`が既に存在するマシンカタログを更新することはできません。

Azureリソースグループ

Azureプロビジョニングリソースグループは、ユーザーにアプリケーションとデスクトップを提供するVMをプロビジョニングする方法を提供します。MCSマシンカタログを作成する際に、既存の空のAzureリソースグループを追加することも、新しいリソースグループを作成することもできます。Azureリソースグループの詳細については、Microsoftドキュメントを参照してください。

Azureリソースグループの使用法

Azureリソースグループあたりの仮想マシン、マネージドディスク、スナップショット、およびイメージの数に制限はありません。（Azureリソースグループあたり240個のVM、800個のマネージドディスクという制限は削除されました。）

- フルスコープのサービスプリンシパルを使用してマシンカタログを作成する場合、MCSは1つのAzureリソースグループのみを作成し、そのグループをカタログに使用します。
- ナロースコープのサービスプリンシパルを使用してマシンカタログを作成する場合、カタログ用に空の、事前に作成されたAzureリソースグループを提供する必要があります。

Azureエフェメラルディスク

Azureエフェメラルディスクを使用すると、キャッシュディスクまたは一時ディスクを再利用して、Azure対応仮想マシンのOSディスクを保存できます。この機能は、標準のHDDディスクよりも高性能なSSDディスクを必要とするAzure環境で役立ちます。Azureエフェメラルディスクを使用してカタログを作成する方法については、Azureエフェメラルディスクを使用してカタログを作成するを参照してください。

> **注：**
>
> 永続カタログはエフェメラルOSディスクをサポートしていません。

> エフェメラルOSディスクでは、プロビジョニングスキームでマネージドディスクと共有イメージギャラリーを使用する必要があります。

エフェメラルOS一時ディスクの保存

エフェメラルOSディスクをVMの一時ディスクまたはリソースディスクに保存するオプションがあります。この機能により、キャッシュがない、またはキャッシュが不十分なVMでエフェメラルOSディスクを使用できます。このようなVMには、`Ddv4`などのエフェメラルOSディスクを保存するための一時ディスクまたはリソースディスクがあります。

次の点を考慮してください。

- エフェメラルディスクは、VMキャッシュディスクまたはVMの一時（リソース）ディスクのいずれかに保存されます。キャッシュディスクがOSディスクの内容を保持するのに十分な大きさでない限り、一時ディスクよりもキャッシュディスクが優先されます。
- 更新の場合、キャッシュディスクより大きく、一時ディスクより小さい新しいイメージは、エフェメラルOSディスクをVMの一時ディスクに置き換える結果となります。

AzureエフェメラルディスクとMachine Creation Services (MCS) ストレージ最適化 (MCS I/O)

AzureエフェメラルOSディスクとMCS I/Oは同時に有効にできません。

重要な考慮事項は次のとおりです。

- エフェメラルOSディスクとMCS I/Oの両方を同時に有効にしてマシンカタログを作成することはできません。
- PowerShellパラメーター（`UseWriteBackCache`および`UseEphemeralOsDisk`）を`New-ProvScheme`または`Set-ProvScheme`で**true**に設定すると、適切なエラーメッセージが表示されて失敗します。
- 両方の機能が有効になっている既存のマシンカタログについては、引き続き以下を行うことができます。
  - マシンカタログを更新する。
  - VMを追加または削除する。
  - マシンカタログを削除する。

アジュール コンピュート ギャラリー

Azure Compute Gallery (旧称 Azure Shared Image Gallery) を、AzureでMCSプロビジョニングされたマシンの公開イメージリポジトリとして使用します。公開イメージをギャラリーに保存するこ

とで、OSディスクの作成とハイドレーションを高速化し、非永続VMの起動時間とアプリケーション起動時間を改善できます。共有イメージギャラリーには、次の3つの要素が含まれています。

- *ギャラリー*: イメージはここに保存されます。MCSは、マシンカタログごとに1つのギャラリーを作成します。
- *ギャラリーイメージ定義*: この定義には、公開イメージに関する情報（オペレーティングシステムの種類と状態、Azureリージョン）が含まれます。MCSは、カタログ用に作成されたイメージごとに1つのイメージ定義を作成します。
- *ギャラリーイメージバージョン*: 共有イメージギャラリー内の各イメージは複数のバージョンを持つことができ、各バージョンは異なるリージョンに複数のレプリカを持つことができます。各レプリカは、公開イメージの完全なコピーです。

> **注：**
>
> 共有イメージギャラリー機能は、マネージドディスクとのみ互換性があります。レガシーマシンカタログでは使用できません。

> 詳細については、Azure Compute Galleryの概要を参照してください。

PowerShell を使用して Azure Compute Gallery イメージでマシンカタログを作成または更新する方法については、「Azure Compute Gallery イメージを使用してマシンカタログを作成または更新する」を参照してください。

Azure 機密 VM

Azure 機密コンピューティング VM は、仮想デスクトップがメモリ内で暗号化され、使用中に保護されることを保証します。

MCSを使用してAzure機密VMを含むカタログを作成できます。このようなカタログを作成するには、マシンプロファイルワークフローを使用する必要があります。VMとARMテンプレート仕様の両方をマシンプロファイル入力として使用できます。

機密VMに関する重要な考慮事項

サポートされているVMサイズと機密VMを使用したマシンカタログの作成に関する重要な考慮事項は次のとおりです。

- サポートされているVMサイズ：機密VMは以下のVMサイズをサポートしています。
    - DCasv5 シリーズ

    - DCadsv5 シリーズ
    - ECasv5 シリーズ
    - ECadsv5 シリーズ

- 機密VMを使用してマシンカタログを作成します。
    - Web Studio および PowerShell コマンドを使用して、Azure 機密VMでマシンカタログを作成できます。
    - Azure機密VMを含むマシンカタログを作成するには、マシンプロファイルベースのワークフローを使用する必要があります。VMまたはテンプレート仕様をマシンプロファイル入力として使用できます。
    - マスターイメージとマシンプロファイルの入力は、両方とも同じ機密セキュリティタイプで有効にする必要があります。セキュリティタイプは次のとおりです。
        - **VMGuestStateOnly**: VMゲストの状態のみが暗号化された機密VM
        - **DiskWithVMGuestState**: プラットフォーム管理キーまたは顧客管理キーでOSディスクとVMゲストの状態の両方が暗号化された機密VM。通常のOSディスクとエフェメラルOSディスクの両方を暗号化できます。
    - AdditionalDataパラメーターを使用して、マネージドディスク、スナップショット、Azure Compute Galleryイメージ、VM、ARMテンプレート仕様など、さまざまなリソースタイプの機密VM情報を取得できます。例：

      ```
      PS C:\Users\username> (get-item XDHyp:
      \HostingUnits\mynetwork\image.folder\username-dev-testing-
      rg.resourcegroup\username-dev-tsvda.vm).AdditionalData
      ```

      追加データフィールドは次のとおりです。
        - DiskSecurityType
        - ConfidentialVMDiskEncryptionSetId
        - DiskSecurityProfiles

      マシンサイズの機密コンピューティングプロパティを取得するには、次のコマンドを実行します: `(Get-Item -path "XDHyp:\Connections\my-connection-name\East US.region\serviceoffering.folder\abc.serviceoffering").AdditionalData`

      追加データフィールドは`ConfidentialComputingType`です。

- マスターイメージまたはマシンプロファイルを、機密から非機密セキュリティタイプへ、または非機密から機密セキュリティタイプへ変更することはできません。
- 誤った構成に対しては、適切なエラーメッセージが表示されます。

マスターイメージとマシンプロファイルの準備

機密VMのセットを作成する前に、以下の手順に従ってマスターイメージとマシンプロファイルを準備します。

1. Azureポータルで、次のような特定の構成で機密VMを作成します。
   - **セキュリティの種類**: 機密仮想マシン
   - **機密OSディスク暗号化**: 有効。
   - **キー管理**: プラットフォーム管理キーによる機密ディスク暗号化 機密VMの作成について詳しくは、この Microsoft の記事を参照してください。
2. 作成したVMでマスターイメージを準備します。作成したVMに必要なアプリケーションとVDAをインストールします。

   > **注：**
   >
   > VHDを使用した機密VMの作成はサポートされていません。代わりに、Azure Compute Gallery、マネージドディスク、またはスナップショットを使用してください。

3. 次のいずれかの方法でマシンプロファイルを作成します。
   - 手順1で作成した既存のVMが必要なマシンプロパティを備えている場合は、それを使用します。
   - マシンプロファイルとしてARMテンプレート仕様を選択する場合は、必要に応じてテンプレート仕様を作成します。具体的には、*SecurityEncryptionType* や *diskEncryptionSet* (顧客管理キーの場合) など、機密VMの要件を満たすパラメーターを構成します。詳しくは、(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/install-configure/machine-catalogs-create/create-machine-catalog-citrix-azure.html#create-an-azure-template-spec)を参照してください。

     > **注：**

- マスターイメージとマシンプロファイルが同じセキュリティキータイプであることを確認してください。
- 顧客管理キーによる機密OSディスク暗号化を必要とする機密VMを作成するには、マスターイメージとマシンプロファイルの両方でディスク暗号化セットIDが同じであることを確認してください。

Web Studio または PowerShell コマンドを使用して機密VMを作成する

機密VMのセットを作成するには、マスターイメージと、目的の機密VMから派生したマシンプロファイルを使用してマシンカタログを作成します。

Web Studio を使用してカタログを作成するには、「マシンカタログの作成」に記載されている手順に従ってください。以下の考慮事項に留意してください。

- **イメージ**ページで、機密VMの作成用に準備したマスターイメージとマシンプロファイルを選択します。マシンプロファイルの選択は必須であり、選択したマスターイメージと同じセキュリティ暗号化タイプに一致するプロファイルのみが選択可能です。
- 「**仮想マシン**」ページでは、機密VMをサポートするマシンサイズのみが選択肢として表示されます。
- 「**ディスク設定**」ページでは、選択したマシンプロファイルから継承されるため、ディスク暗号化セットを指定することはできません。

Azure Marketplace (アジュール マーケットプレイス)

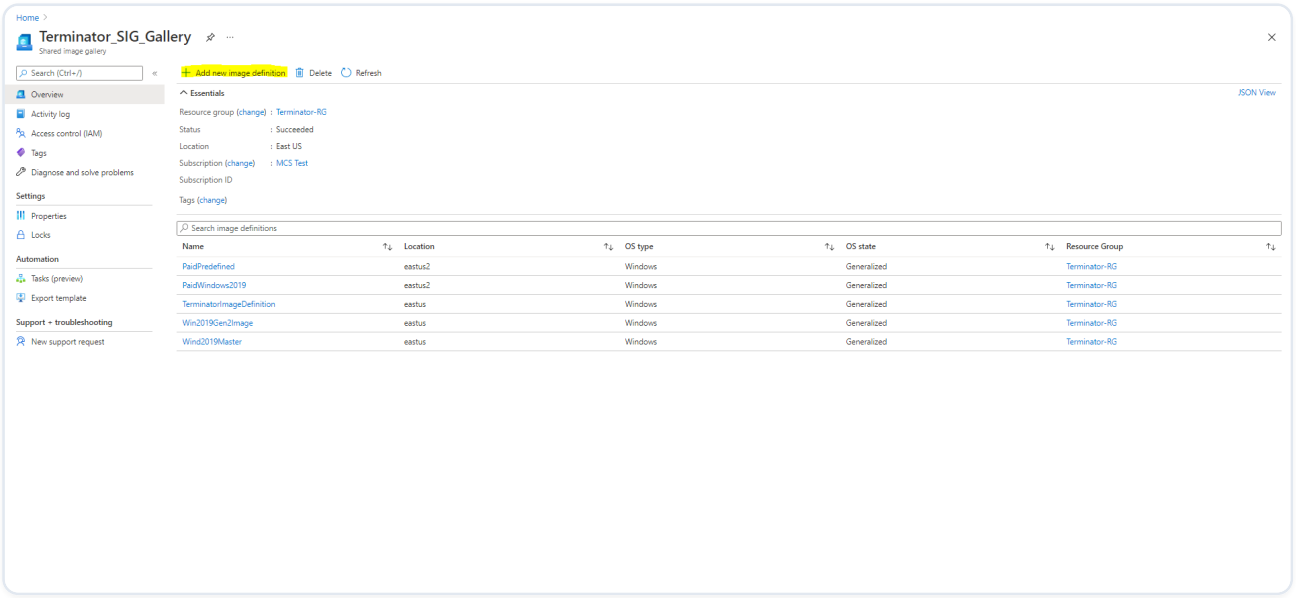
Citrix Virtual Apps and Desktops は、プラン情報を含むAzure上のマスターイメージを使用してマシンカタログを作成することをサポートしています。詳細については、「Microsoft Azure Marketplace」を参照してください。

ヒント:

標準のWindows Serverイメージなど、Azure Marketplaceで見つかる一部のイメージには、プラン情報が追加されていません。Citrix Virtual Apps and Desktops の機能は、有料イメージ向けです。

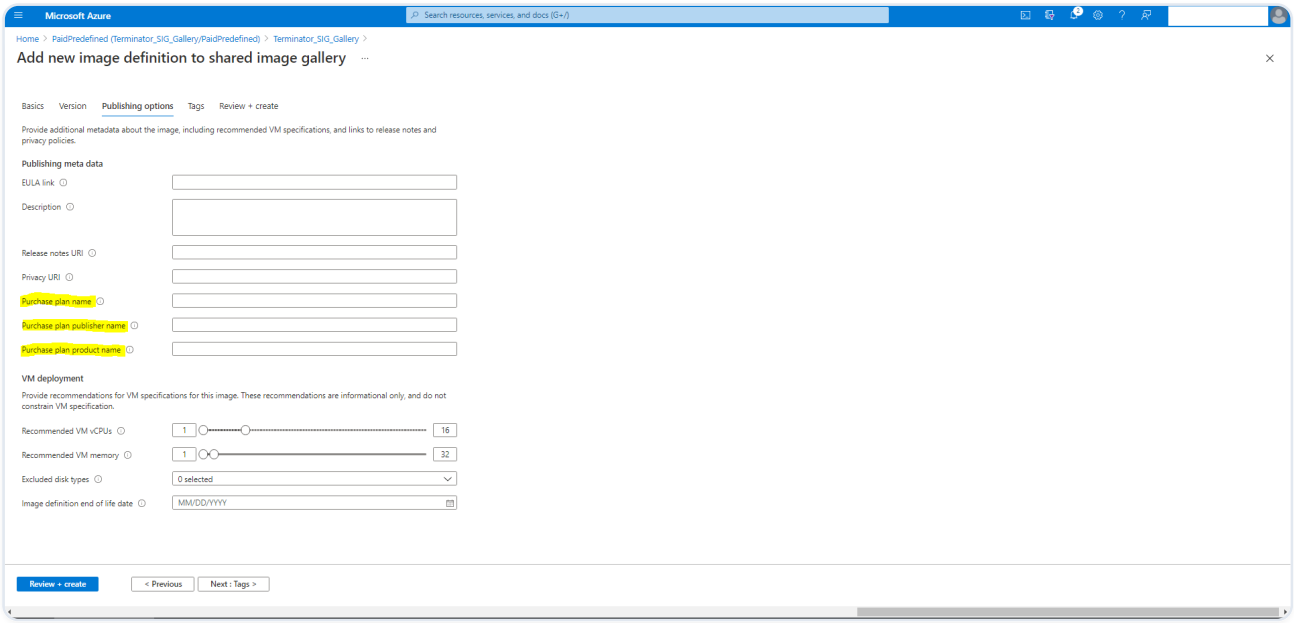
Shared Image Gallery で作成されたイメージに Azure プラン情報が含まれていることを確認します

このセクションの手順を使用して、Web Studio で Shared Image Gallery のイメージを表示します。これらのイメージは、オプションでマスターイメージとして使用できます。イメージを Shared Image Gallery に配置するには、ギャラリーでイメージ定義を作成します。

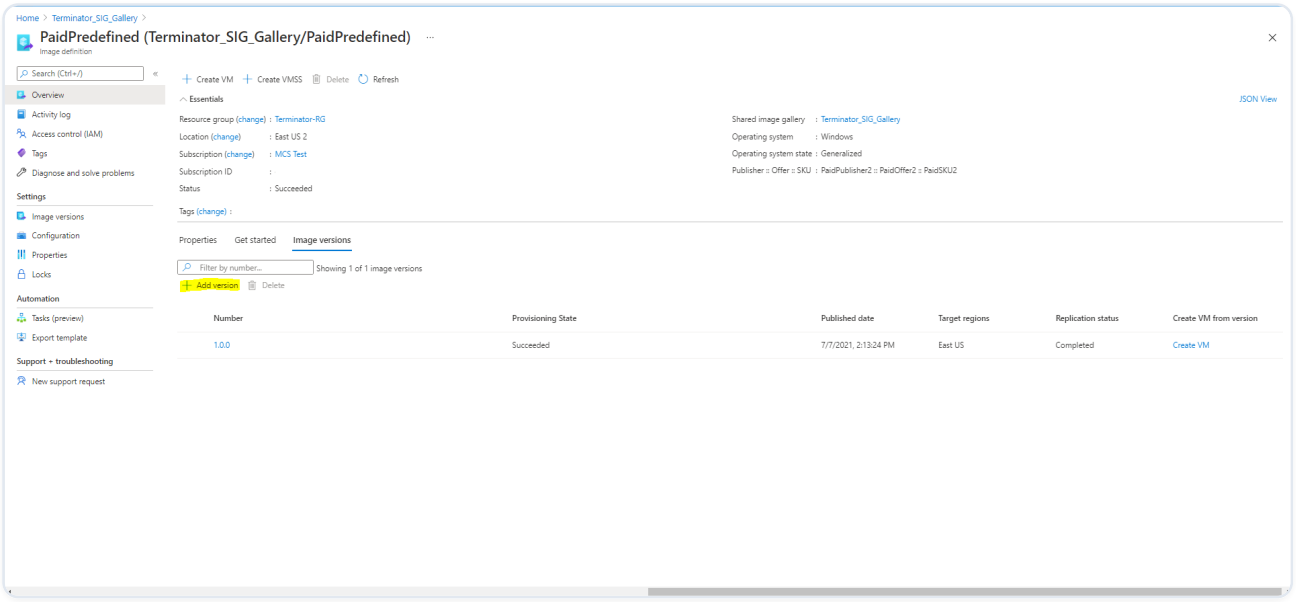


公開オプションページで、購入プラン情報を確認します。

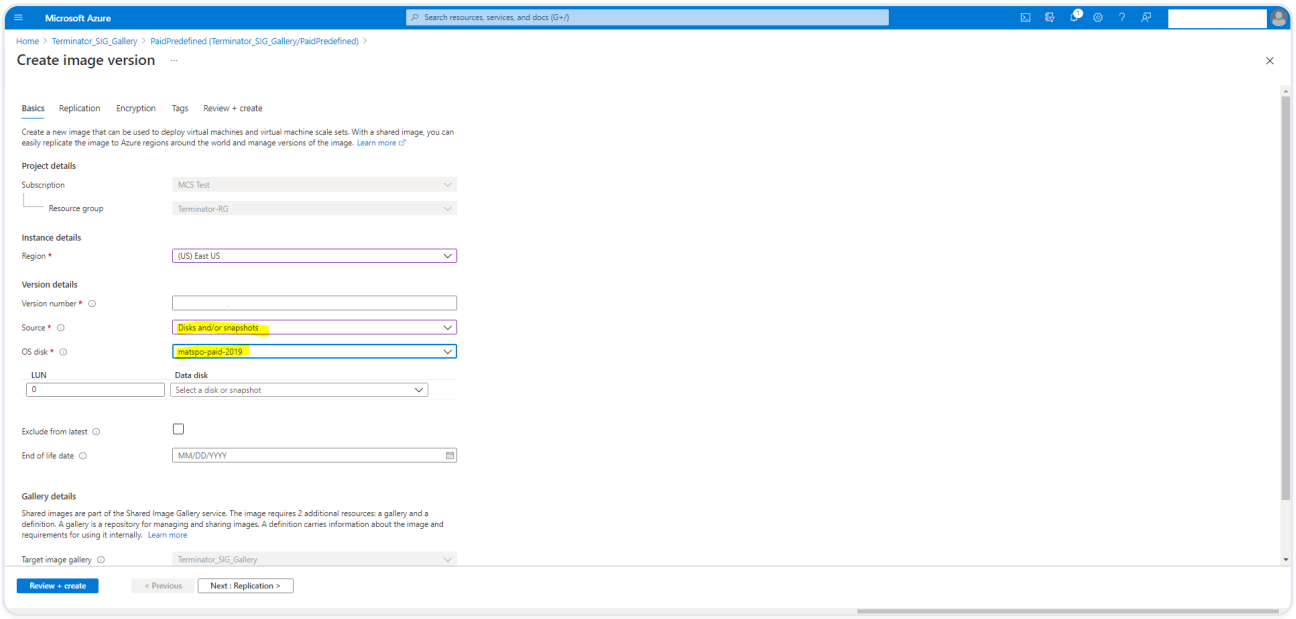
購入プラン情報フィールドは最初は空です。これらのフィールドに、イメージに使用された購入プラン情報を入力します。購入プラン情報を入力しないと、マシンカタログのプロセスが失敗する可能性があります。



購入プラン情報を確認した後、定義内にイメージバージョンを作成します。これはマスターイメージとして使用されます。**バージョンの追加**をクリックします。



バージョン詳細セクションで、イメージスナップショットまたはマネージドディスクをソースとして選択します。



PowerShell を使用してマシンカタログを作成する

このセクションでは、PowerShell を使用してカタログを作成する方法について詳しく説明します。

- 非永続的なライトバックキャッシュディスクを持つカタログを作成する
- 永続的なライトバックキャッシュディスクを持つカタログを作成する
- MCSIO で起動パフォーマンスを向上させる
- PowerShellを使用してカタログを作成または更新する際にテンプレート仕様を使用する
- 信頼された起動によるマシンカタログ

- マシンプロファイルのプロパティ値を使用する
- 顧客管理の暗号化キーを使用してマシンカタログを作成する(#create-a-machine-catalog-with-customer-managed-encryption-key)
- 二重暗号化でマシンカタログを作成する
- Azure エフェメラルディスクを持つカタログを作成する
- Azure 専用ホスト
- Azure Compute Gallery イメージを使用してマシンカタログを作成または更新する
- Shared Image Gallery を構成する
- 指定された可用性ゾーンにマシンをプロビジョニングする
- ストレージの種類
- ページファイルの場所
- ページファイル設定の更新(#update-page-file-setting)
- Azure Spot VMを使用してカタログを作成する(#create-a-catalog-using-azure-spot-vms)
- バックアップVMサイズを構成する
- すべてのリソースのタグをコピーする
- Azure Monitor Agentがインストールされたカタログ VMのプロビジョニング(#provision-catalog-vms-with-azure-monitor-agent-installed)

非永続的なライトバックキャッシュディスクを持つカタログの作成

非永続的なライトバックキャッシュディスクを持つカタログを構成するには、PowerShellパラメーター`New-ProvScheme CustomProperties`を使用します。カスタムプロパティ`UseTempDiskForWBC`は、ライトバックキャッシュファイルを保存するためにAzure一時ストレージを使用することを受け入れるかどうかを示します。一時ディスクをライトバックキャッシュディスクとして使用したい場合は、`New-ProvScheme`を実行する際にこれをtrueに構成する必要があります。このプロパティが指定されていない場合、パラメーターはデフォルトで**False**に設定されます。

例えば、`CustomProperties`パラメーターを使用して`UseTempDiskForWBC`を**true**に設定する場合：

```
-CustomProperties '<CustomProperties xmlns=" http://schemas.citrix.com/
2014/xd/machinecreation" xmlns:xsi=" http://www.w3.org/2001/XMLSchema-
instance"> `

<Property xsi:type="StringProperty" Name="PersistWBC" Value="false"/> `
```

```
<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="false"/> `

<Property xsi:type="StringProperty" Name="PersistVm" Value="false"/> `

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="Premium_LRS"/> `

<Property xsi:type="StringProperty" Name="WBCDiskStorageType"
Value="Premium_LRS"/> `

<Property xsi:type="StringProperty" Name="LicenseType"
Value="Windows_Client"/> `

<Property xsi:type="StringProperty" Name="UseTempDiskForWBC" Value="true"/
> `

</CustomProperties>'
```

注：

ライトバックキャッシュファイルにAzureローカル一時ストレージを使用するようにマシンカタログをコミットした後、後でVHDを使用するように変更することはできません。

永続的なライトバックキャッシュディスクを持つカタログを作成する

永続的なライトバックキャッシュディスクを持つカタログを構成するには、PowerShellパラメーター`New-ProvScheme CustomProperties`を使用します。このパラメーターは、MCSプロビジョニングされたマシンに対してライトバックキャッシュディスクがどのように永続化するかを決定するために使用される追加のプロパティ`PersistWBC`をサポートします。`PersistWBC`プロパティは、`UseWriteBackCache`パラメーターが指定され、`WriteBackCacheDiskSize`パラメーターがディスクが作成されることを示すように設定されている場合にのみ使用されます。

`PersistWBC`をサポートする前の`CustomProperties`パラメーターで見つかったプロパティの例は次のとおりです。

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />
```

```
<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="ResourceGroups"
Value="benvaldev5RG3" />

</CustomProperties>
```

これらのプロパティを使用する場合、`CustomProperties`パラメーターからプロパティが省略されていると、それらはデフォルト値を含むことに注意してください。`PersistWBC`プロパティには、**true**または**false**の2つの可能な値があります。

`PersistWBC`プロパティを**true**に設定すると、Citrix Virtual Apps and Desktops管理者がWeb Studioを使用してマシンをシャットダウンしても、ライトバックキャッシュディスクは削除されません。

`PersistWBC`プロパティを**false**に設定すると、Citrix Virtual Apps and Desktops管理者がWeb Studioを使用してマシンをシャットダウンしたときに、ライトバックキャッシュディスクが削除されます。

注：

`PersistWBC`プロパティが省略された場合、プロパティはデフォルトで**false**になり、Web Studioを使用してマシンがシャットダウンされるとライトバックキャッシュは削除されます。

例えば、`CustomProperties`パラメーターを使用して`PersistWBC`をtrueに設定する場合：

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="ResourceGroups"
```

```
Value="benvaldev5RG3" />

<Property xsi:type="StringProperty" Name="PersistWBC" Value="true" />

</CustomProperties>
```

重要:

`PersistWBC`プロパティは、`New-ProvScheme` PowerShellコマンドレットを使用してのみ設定できます。作成後にプロビジョニングスキームの`CustomProperties`を変更しようとしても、マシンカタログや、マシンがシャットダウンされたときのライトバックキャッシュディスクの永続性には影響しません。

例えば、`New-ProvScheme`をライトバックキャッシュを使用するように設定し、同時に`PersistWBC`プロパティをtrueに設定する場合：

```
New-ProvScheme

-CleanOnBoot

-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com/
2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`"><Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`"
Value=`"true`" /><Property xsi:type=`"StringProperty`"
Name=`"StorageAccountType`" Value=`"Premium_LRS`" /><Property
xsi:type=`"StringProperty`" Name=`"ResourceGroups`"
Value=`"benvaldev5RG3`" /><Property xsi:type=`"StringProperty`"
Name=`"PersistWBC`" Value=`"true`" /></CustomProperties>"

-HostingUnitName "adSubnetScale1"

-IdentityPoolName "BV-WBC1-CAT1"

-MasterImageVM "XDHyp:
\HostingUnits\adSubnetScale1\image.folder\GoldImages.resourcegroup\W10MCSI
O-01_OsDisk_1_a940e6f5bab349019d57ccef65d2c7e3.manageddisk"

-NetworkMapping @{"0"="XDHyp:\HostingUnits\adSubnetScale1\
\virtualprivatecloud.folder\CloudScale02.resourcegroup\adVNET.virtualpriva
tecloud\adSubnetScale1.network"}
```

```
-ProvisioningSchemeName "BV-WBC1-CAT1"

-ServiceOffering "XDHyp:
\HostingUnits\adSubnetScale1\serviceoffering.folder\Standard_D2s_v3.servic
eoffering"

-UseWriteBackCache

-WriteBackCacheDiskSize 127

-WriteBackCacheMemorySize 256
```

MCSIOで起動パフォーマンスを向上させる

MCSIOが有効になっている場合、AzureおよびGCPマネージドディスクの起動パフォーマンスを向上させることができます。この機能を構成するには、`New-ProvScheme` コマンドでPowerShell `PersistOSDisk` カスタムプロパティを使用します。`New-ProvScheme` に関連するオプションは次のとおりです。

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="Resource ``````<!--NeedCopy-->

````````Groups" Value="benvaldev5RG3" />

<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="true" />

</CustomProperties>
```

この機能を有効にするには、`PersistOSDisk` カスタムプロパティを `true` に設定します。例：

```
New-ProvScheme

-CleanOnBoot
```
```

```
-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com/
2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`"><Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`"
Value=`"true`" /><Property xsi:type=`"StringProperty`"
Name=`"StorageAccountType`" Value=`"Premium_LRS`" /><Property
xsi:type=`"StringProperty`" Name=`"ResourceGroups`"
Value=`"benvaldev5RG3`" /><Property xsi:type=`"StringProperty`"
Name=`"PersistOsDisk`" Value=`"true`" /></CustomProperties>"

-HostingUnitName "adSubnetScale1"

-IdentityPoolName "BV-WBC1-CAT1"

-MasterImageVM "XDHyp:
\HostingUnits\adSubnetScale1\image.folder\GoldImages.resourcegroup\W10MCSI
O-01_OsDisk_1_a940e6f5bab349019d57ccef65d2c7e3.manageddisk"

-NetworkMapping @{"0"="XDHyp:\HostingUnits\adSubnetScale1\
\virtualprivatecloud.folder\CloudScale02.resourcegroup\adVNET.virtualpriva
tecloud\adSubnetScale1.network"}

-ProvisioningSchemeName "BV-WBC1-CAT1"

-ServiceOffering "XDHyp:
\HostingUnits\adSubnetScale1\serviceoffering.folder\Standard_D2s_v3.servic
eoffering"

-UseWriteBackCache

-WriteBackCacheDiskSize 127

-WriteBackCacheMemorySize 256
```

PowerShell を使用してカタログを作成または更新する際にテンプレート仕様を使用する

テンプレート仕様をマシンプロファイルの入力として使用して、MCSマシンカタログを作成または更新できます。これを行うには、Web StudioまたはPowerShellコマンドを使用できます。

Web Studioについては、「Web StudioでAzure Resource Managerイメージを使用してマシンカタログを作成する」を参照してください。(#create-a-machine-catalog-using-an-azure-resource-manager-image-in-web-studio)

PowerShell コマンドを使用する手順:

1. **PowerShell** ウィンドウを開きます。
2. `asnp citrix*` を実行します。
3. カタログを作成または更新します。

    - カタログを作成するには:

        a. テンプレート仕様をマシンプロファイルの入力として使用して、`New-ProvScheme` コマンドを使用します。例:

        ```
        New-ProvScheme -MasterImageVM "XDHyp:/HostingUnits/azure/
        image.folder/fgthj.resourcegroup/nab-ws-
        vda_OsDisk_1_xxxxxxxxxxa.manageddisk"

        MachineProfile "XDHyp:/HostingUnits/azure/machineprofile.folder/
        fgthj.resourcegroup/test.templatespec/V1.templatespecversion"

        -ProvisioningSchemeName <String>

        -HostingUnitName <String>

        -IdentityPoolName <String>

        [-ServiceOffering <String>][-CustomProperties <String>

        [-LoggingId <Guid>]

        [-BearerToken <String>][-AdminAddress <String>]

        [<CommonParameters>]
        ```

        b. カタログの作成を完了します。

    - カタログを更新するには、テンプレート仕様をマシンプロファイルの入力として使用して、`Set-ProvScheme` コマンドを使用します。例:

        ```
        Set-ProvScheme -MasterImageVm 'XDHyp://Connections/Azure/East
        Us.region/vm.folder/MasterDisk.vm'

        MachineProfile 'XDHyp:/HostingUnits/azure/machineprofile.folder/
        fgthj.resourcegroup/testing.templatespec/V1.templatespecversion'
        ```

```
[-ProvisioningSchemeName] <String>

[-CustomProperties <String>][-ServiceOffering <String>] [-PassThru]

[-LoggingId <Guid>] [-BearerToken <String>][-AdminAddress <String>]
[<CommonParameters>]
```

信頼できる起動を持つマシンカタログ

信頼できる起動を持つマシンカタログを正常に作成するには、以下を使用します。

- 信頼できる起動を持つマシンプロファイル
- トラステッド起動をサポートするVMサイズ
- トラステッド起動をサポートするWindows VMバージョン。現在、Windows 10、Windows 11、Windows Server 2016、2019、2022がトラステッド起動をサポートしています。

重要:

MCSは、トラステッド起動が有効なVMを使用して新しいカタログを作成することをサポートしています。ただし、既存の永続カタログと既存のVMを更新するには、Azureポータルを使用する必要があります。非永続カタログのトラステッド起動を更新することはできません。詳細については、Microsoftドキュメント「既存のAzure VMでトラステッド起動を有効にする」を参照してください。

Citrix Virtual Apps and Desktopsの提供インベントリアイテムを表示し、VMサイズがトラステッド起動をサポートしているかどうかを判断するには、次のコマンドを実行します。

1. PowerShell ウィンドウを開きます。
2. Citrix固有のPowerShellモジュールをロードするには、**asnp citrix***を実行します。
3. 次のコマンドを実行します。

```
$s = (ls XDHyp:\HostingUnits\<name of hosting
unit>\serviceoffering.folder\"<VM size>.serviceoffering)
```

4. `$s | select -ExpandProperty Additionaldata` を実行します。
5. `SupportsTrustedLaunch` 属性の値を確認します。

- `SupportsTrustedLaunch`が**True**の場合、VMサイズはトラステッド起動をサポートしています。
- `SupportsTrustedLaunch`が**False**の場合、VMサイズはトラステッド起動をサポートしていません。

AzureのPowerShellに従って、トラステッド起動をサポートするVMサイズを判断するには、次のコマンドを使用できます。

```
(Get-AzComputeResourceSku | where {$_.Locations.Contains($region) -and
($_.Name -eq "<VM size>") })[0].Capabilities
```

Azure PowerShellコマンドを実行した後、VMサイズがトラステッド起動をサポートしているかどうかを説明する例を次に示します。

- *例1*: Azure VMがGeneration 1のみをサポートしている場合、そのVMはトラステッド起動をサポートしていません。したがって、Azure PowerShellコマンドを実行しても、`TrustedLaunchDisabled`機能は表示されません。
- *例2*: Azure VMがGeneration 2のみをサポートし、`TrustedLaunchDisabled`機能が**True**の場合、Generation 2 VMサイズはトラステッド起動でサポートされません。
- *例3*: Azure VMがGeneration 2のみをサポートし、PowerShellコマンドを実行しても`TrustedLaunchDisabled`機能が表示されない場合、Generation 2 VMサイズはトラステッド起動でサポートされます。

Azure仮想マシンのトラステッド起動の詳細については、Microsoftドキュメント「Azure仮想マシンのトラステッド起動」を参照してください。

トラステッド起動でマシンカタログを作成する

1. トラステッド起動が有効なマスターイメージを作成します。Microsoftドキュメント「トラステッド起動VMイメージ」を参照してください。
2. セキュリティの種類を **trusted launch virtual machines** として VM またはテンプレート仕様を作成します。VM またはテンプレート仕様の作成の詳細については、Microsoft ドキュメント「Deploy a trusted launch VM」を参照してください。
3. Web StudioまたはPowerShellコマンドを使用してマシンカタログを作成します。
   - Web Studio を使用する場合は、Web Studio で Azure Resource Manager イメージを使用してマシンカタログを作成する を参照してください。

- PowerShell コマンドを使用する場合は、VM またはテンプレート仕様をマシンプロファイルの入力として、`New-ProvScheme` コマンドを使用します。カタログを作成するためのコマンドの完全なリストについては、カタログの作成 を参照してください。

  VMをマシンプロファイルの入力とする`New-ProvScheme`の例:

  ```
  New-ProvScheme -CleanOnBoot -HostingUnitName "name"
  -IdentityPoolName "name" -InitialBatchSizeHint 1

  -MasterImageVM "XDHyp:/HostingUnits/azure/image.folder/
  fgthj.resourcegroup/nab-ws-vda_OsDisk_1_xxxxxxxxxxa.manageddisk"

  -MachineProfile "XDHyp:
  \HostingUnits\<adnet>\machineprofile.folder\<def.resourcegroup>\<mac
  hine profile vm.vm>"

  -ProvisioningSchemeName <String>

  -HostingUnitName <String>

  -IdentityPoolName <String>

  [-ServiceOffering <String>][-CustomProperties <String>]

  [<CommonParameters>]
  ```

  テンプレート仕様をマシンプロファイルの入力とする`New-ProvScheme`の例:

  ```
  New-ProvScheme -CleanOnBoot -HostingUnitName "name"
  -IdentityPoolName "name" -InitialBatchSizeHint 1

  -MasterImageVM "XDHyp:/HostingUnits/azure/image.folder/
  fgthj.resourcegroup/nab-ws-vda_OsDisk_1_xxxxxxxxxxa.manageddisk"

  MachineProfile "XDHyp:/HostingUnits/azure/machineprofile.folder/
  fgthj.resourcegroup/test.templatespec/V1.templatespecversion"

  -ProvisioningSchemeName <String>

  -HostingUnitName <String>

  -IdentityPoolName <String>
  ```

```
[-ServiceOffering <String>][-CustomProperties <String>]

[<CommonParameters>]
```

信頼された起動でマシンカタログを作成する際のエラー

信頼された起動でマシンカタログを作成する際に、以下のシナリオで適切なエラーが発生します。

シナリオ	エラー
アンマネージドカタログの作成中にマシンプロファイルを選択した場合	`MachineProfileNotSupportedForUnmanagedCatalog`
マスターイメージとしてアンマネージドディスクを使用してカタログを作成する際に、信頼された起動をサポートするマシンプロファイルを選択した場合	`SecurityTypeNotSupportedForUnmanagedDisk`
セキュリティの種類として信頼された起動を持つマスターイメージソースを使用してマネージドカタログを作成する際に、マシンプロファイルを選択しなかった場合	`MachineProfileNotFoundForTrustedLaunchMasterImage`
マスターイメージのセキュリティの種類と異なるセキュリティの種類を持つマシンプロファイルを選択した場合	`SecurityTypeConflictBetweenMasterImageAndMachineProfile`
信頼された起動をサポートしないVMサイズを選択したが、カタログ作成時に信頼された起動をサポートするマスターイメージを使用した場合	`MachineSizeNotSupportTrustedLaunch`

マシンプロファイルプロパティ値の使用

マシンカタログは、カスタムプロパティで定義されている次のプロパティを使用します。

- アベイラビリティゾーン
- 専用ホストグループID
- ディスク暗号化セットID
- OSの種類

- ライセンスの種類
- ストレージの種類

これらのカスタムプロパティが明示的に定義されていない場合、プロパティ値は、マシンプロファイルとして使用されるARMテンプレート仕様またはVMから設定されます。さらに、`ServiceOffering`が指定されていない場合、マシンプロファイルから設定されます。

> **注：**
>
> マシンプロファイルに一部のプロパティが欠落しており、カスタムプロパティで定義されていない場合、該当する場合、プロパティのデフォルト値が適用されます。

> 次のセクションでは、`New-ProvScheme`と`Set-ProvScheme`におけるいくつかのシナリオについて説明します。この場合、`CustomProperties`はすべてのプロパティを定義しているか、値がMachineProfileから派生しています。

- New-ProvSchemeのシナリオ
  - MachineProfileにすべてのプロパティがあり、CustomPropertiesが定義されていない場合。例:

    `New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit\machineprofile.folder\azure.resourcegroup\mpA.vm"`

    カタログのカスタムプロパティとして、次の値が設定されます:

    ```
    Get-ProvScheme | select CustomProperties

    <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
    machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
    instance">

    <Property xsi:type="StringProperty" Name="StorageAccountType"
    Value="<mpA-value>"/>

    <Property xsi:type="StringProperty" Name="OSType" Value="<mpA-
    value>"/>

    <Property xsi:type="StringProperty" Name="LicenseType" Value="<mpA-
    value>"/>
    ```

```
<Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
Value="<mpA-value>"/>

<Property xsi:type="StringProperty" Name="DedicatedHostGroupId"
Value="<mpA-value>"/>

<Property xsi:type="StringProperty" Name="Zones" Value="<mpA-
value>"/>

</CustomProperties>
```

- MachineProfileに一部のプロパティがあり、CustomPropertiesが定義されていない場合。例: MachineProfileにはLicenseTypeとOsTypeのみがあります。

  `New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit\machineprofile.folder\azure.resourcegroup\mpA.vm"`

  カタログのカスタムプロパティとして、次の値が設定されます:

  ```
  Get-ProvScheme | select CustomProperties

  <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
  machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
  instance">

  <Property xsi:type="StringProperty" Name="OSType" Value="<mpA-
  value>"/>

  <Property xsi:type="StringProperty" Name="LicenseType" Value="<mpA-
  value>"/>

  </CustomProperties>
  ```

- MachineProfileとCustomPropertiesの両方がすべてのプロパティを定義している場合。例:

  `New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit\machineprofile.folder\azure.resourcegroup\mpA.vm" -CustomProperties $CustomPropertiesA`

  カスタムプロパティが優先されます。カタログのカスタムプロパティとして、次の値が設定されます。

```
Get-ProvScheme | select CustomProperties

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="<CustomPropertiesA-value>"/>

<Property xsi:type="StringProperty" Name="OSType"
Value="<CustomPropertiesA-value>"/>

<Property xsi:type="StringProperty" Name="LicenseType"
Value="<CustomPropertiesA-value>"/>

<Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
Value="<CustomPropertiesA-value>"/>

<Property xsi:type="StringProperty" Name="DedicatedHostGroupId"
Value="<CustomPropertiesA-value>"/>

<Property xsi:type="StringProperty" Name="Zones"
Value="<CustomPropertiesA-value>"/>

</CustomProperties>
```

- MachineProfileで一部のプロパティが定義され、CustomPropertiesで一部のプロパティが定義されている場合。例:
  - CustomProperties は LicenseType と StorageAccountType を定義します
  - MachineProfile は LicenseType、OsType、および Zones を定義します

`New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit\machineprofile.folder\azure.resourcegroup\mpA.vm" -CustomProperties $CustomPropertiesA`

カタログのカスタムプロパティとして、次の値が設定されます:

```
Get-ProvScheme | select CustomProperties

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
```

```
instance">

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="<CustomPropertiesA-value>"/>

<Property xsi:type="StringProperty" Name="OSType" Value="<mpA-
value>"/>

<Property xsi:type="StringProperty" Name="LicenseType"
Value="<CustomPropertiesA-value>"/>

<Property xsi:type="StringProperty" Name="Zones" Value="<mpA-
value>"/>

</CustomProperties>
```

- 一部のプロパティは MachineProfile で定義され、一部のプロパティは CustomProperties で定義されています。さらに、ServiceOffering は定義されていません。例:
  - CustomProperties は StorageType を定義します
  - MachineProfile は LicenseType を定義します

```
New-ProvScheme -MachineProfile "XDHyp:
\HostingUnits\azureunit\machineprofile.folder\azure.resourcegroup\mp
.vm"

-ServiceOffering "XDHyp:
\HostingUnits\azureunit\serviceoffering.folder\<explicit-machine-
size>.serviceoffering"
```

カタログのカスタムプロパティとして、次の値が設定されます:

```
Get-ProvScheme | select ServiceOffering

serviceoffering.folder\<explicit-machine-size>.serviceoffering



Get-ProvScheme | select CustomProperties

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
```

```
instance">

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="explicit-storage-type"/>

<Property xsi:type="StringProperty" Name="LicenseType" Value="value-
from-machineprofile"/>

</CustomProperties>
```

- OsType が CustomProperties にも MachineProfile にも含まれていない場合、次のようになります:
  - 値はマスターイメージから読み取られます。
  - マスターイメージがアンマネージドディスクの場合、OsType は Windows に設定されます。例:

`New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit\machineprofile.folder\azure.resourcegroup\mpA.vm" -MasterImageVM "XDHyp:\HostingUnits\azureunit\image.folder\linux-master-image.manageddisk"`

マスターイメージからの値は、この場合 Linux のカスタムプロパティに書き込まれます。

```
Get-ProvScheme | select CustomProperties

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="OSType" Value="Linux"/>

</CustomProperties>
```

- Set-ProvScheme シナリオ
  - 既存のカタログ (以下を含む):
    - カスタムプロパティ（`StorageAccountType`およびOsType）
    - ゾーンを定義する MachineProfile `mpA.vm`
  - 更新:

- StorageAccountType を定義する MachineProfile mpB.vm
- LicenseType と OsType を定義する新しいカスタムプロパティセット $CustomPropertiesB

`Set-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit\machineprofile.folder\azure.resourcegroup\mpB.vm" -CustomProperties $CustomPropertiesB`

カタログのカスタムプロパティとして、次の値が設定されます:

```
Get-ProvScheme | select CustomProperties

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="<mpB-value>"/>

<Property xsi:type="StringProperty" Name="OSType"
Value="<CustomPropertiesB-value>"/>

<Property xsi:type="StringProperty" Name="LicenseType"
Value="<CustomPropertiesB-value>"/>

    </CustomProperties>
```

- 既存のカタログ (以下を含む):
  - S`torageAccountType` および OsType の CustomProperties
  - StorageAccountType と LicenseType を定義する MachineProfile `mpA.vm`
- 更新:
  - StorageAccountType と OsType を定義する新しいカスタムプロパティセット $CustomPropertiesB。

`Set-ProvScheme -CustomProperties $CustomPropertiesB`

カタログのカスタムプロパティとして、次の値が設定されます:

```
Get-ProvScheme | select CustomProperties

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="<CustomPropertiesB-value>"/>

<Property xsi:type="StringProperty" Name="OSType"
Value="<CustomPropertiesB-value>"/>

<Property xsi:type="StringProperty" Name="LicenseType" Value="<mp-A-
value>"/>

</CustomProperties>
```

- 既存のカタログ (以下を含む):
  - カスタムプロパティ（`StorageAccountType`およびOsType）
  - ゾーンを定義するMachineProfile `mpA.vm`
- 更新:
  - StorageAccountType と LicenseType を定義する MachineProfile mpB.vm
  - `ServiceOffering`は指定されていません

`Set-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit\machineprofile.folder\azure.resourcegroup\mpB.vm"`

カタログのカスタムプロパティとして、次の値が設定されます:

```
Get-ProvScheme | select ServiceOffering

serviceoffering.folder\<value-from-machineprofile>.serviceoffering



Get-ProvScheme | select CustomProperties

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
```

```
instance">

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="<mpB-value>"/>

<Property xsi:type="StringProperty" Name="OSType" Value="<prior-
CustomProperties-value>"/>

<Property xsi:type="StringProperty" Name="LicenseType" Value="<mpB-
value>"/>

</CustomProperties>
```

Azure Monitor Agentがインストールされたカタログ VMをプロビジョニングする

Azure監視は、Azureおよびオンプレミス環境からのテレメトリデータを収集、分析し、それに基づいて行動するために使用できるサービスです。

Azure Monitor Agent (AMA) は、仮想マシンなどのコンピューティングリソースから監視データを収集し、そのデータを Azure Monitor に配信します。現在、イベントログ、Syslog、パフォーマンスメトリックの収集をサポートしており、Azure Monitor Metrics および Azure Monitor Logs データソースに送信します。

監視データ内のVMを一意に識別して監視を有効にするには、AMAを拡張機能としてインストールしたMCSマシンカタログのVMをプロビジョニングできます。

要件

- 権限: 必要な Azure 権限 で指定されている最小限の Azure 権限と、Azure Monitor を使用するための以下の権限があることを確認してください。
  - `Microsoft.Compute/virtualMachines/extensions/read`
  - `Microsoft.Compute/virtualMachines/extensions/write`
  - `Microsoft.Insights/DataCollectionRuleAssociations/Read`
  - `Microsoft.Insights/dataCollectionRuleAssociations/write`
  - `Microsoft.Insights/DataCollectionRules/Read`
- データ収集ルール: Azure portal でデータ収集ルールを設定します。DCR の設定については、データ収集ルールの作成 を参照してください。DCR はプラットフォーム固有 (Windows または Linux) です。必要なプラットフォームに応じて DCR を作成してください。 AMA はデータ

収集ルール (DCR) を使用して、VM などのリソースと、Azure Monitor Metrics や Azure Monitor Logs などのデータソース間のマッピングを管理します。

- 既定のワークスペース: Azure portal でワークスペースを作成します。ワークスペースの作成については、Log Analytics ワークスペースの作成 を参照してください。ログとデータを収集すると、その情報はワークスペースに保存されます。ワークスペースには一意のワークスペース ID とリソース ID があります。ワークスペース名は、特定のリソースグループに対して一意である必要があります。ワークスペースを作成したら、データソースとソリューションを設定して、そのデータをワークスペースに保存します。
- 監視拡張機能をホワイトリストに登録: 拡張機能 `AzureMonitorWindowsAgent` および `AzureMonitorLinuxAgent` は、Citrix が定義したホワイトリスト登録済みの拡張機能です。ホワイトリスト登録済みの拡張機能のリストを表示するには、PoSH コマンド `Get-ProvMetadataConfiguration` を使用します。
- マスターイメージ: Microsoft は、既存のマシンから新しいマシンを作成する前に、そのマシンから拡張機能を削除することを推奨しています。拡張機能が削除されていない場合、残存ファイルや予期しない動作につながる可能性があります。詳細については、「既存の VM から VM を再作成する場合」を参照してください。

AMA を有効にしてカタログ VM をプロビジョニングするには:

1. マシンプロファイルテンプレートを設定します。
    - VMをマシンプロファイルテンプレートとして使用する場合：
        a. Azure portal で VM を作成します。
        b. VMの電源を入れます。
        c. **リソース**の下のデータ収集ルールにVMを追加します。これにより、テンプレートVMにエージェントのインストールが呼び出されます。

> **注：**
>
> Linuxカタログを作成する必要がある場合は、Linuxマシンを設定します。

    - テンプレート仕様をマシンプロファイルテンプレートとして使用する場合：
        a. テンプレート仕様を設定します。
        b. 生成されたテンプレート仕様に、次の拡張機能とデータ収集ルール関連付けを追加します。

```
{
"type": "Microsoft.Compute/virtualMachines/extensions",
"apiVersion": "2022-03-01",
"name": "<vm-name>/AzureMonitorWindowsAgent",
"dependsOn": [
    "Microsoft.Compute/virtualMachines/<vm-name>"
],
"location": "<azure-region>",
"properties": {
    "publisher": "Microsoft.Azure.Monitor",
    "type": "AzureMonitorWindowsAgent",
    "typeHandlerVersion": "1.0",
    "autoUpgradeMinorVersion": true,
    "enableAutomaticUpgrade": true
}
},
 {
    "type": "Microsoft.Insights/dataCollectionRuleAssociations",
    "apiVersion": "2021-11-01",
    "name": "<associatio-name>",
    "scope": "Microsoft.Compute/virtualMachines/<vm-name>",
    "dependsOn": [
```

```
     "Microsoft.Compute/virtualMachines/<vm-name>",

    "Microsoft.Compute/virtualMachines/<vm-name>/extensions/
AzureMonitorWindowsAgent"

    ],

    "properties": {

       "description": "Association of data collection rule.
Deleting this association will break the data collection for this
Arc server.",

     "dataCollectionRuleId": "/subscriptions/<azure-
subscription>/resourcegroups/<azure-resource-group>/providers/
microsoft.insights/datacollectionrules/<azure-data-collection-
rule>"

     }

    }
```

2. 既存のMCSマシンカタログを作成または更新します。

   - 新しいMCSカタログを作成するには:

     a. Web Studio で、その VM またはテンプレート仕様をマシンプロファイルとして選択します。

     b. カタログを作成するための次の手順に進みます。

   - 既存の MCS カタログを更新するには、次の PoSH コマンドを使用します。

     - 新しい VM に更新されたマシンプロファイルテンプレートを取得させるには、次のコマンドを実行します。

```
Set-ProvScheme -ProvisioningSchemeName "name"

-MachineProfile "XDHyp:
\HostingUnits\Unit1\machineprofile.folder\abc.resourcegroup\ab-
machine-profile.vm"
```

- 既存の VM を更新されたマシンプロファイルテンプレートで更新するには：

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
-StartsNow -DurationInMinutes -1
```

3. カタログVMの電源を入れます。
4. Azure portal に移動し、モニター拡張機能が VM にインストールされていること、および VM が DCR のリソースの下に表示されていることを確認します。数分後、監視データが Azure Monitor に表示されます。

トラブルシューティング

Azure Monitor Agentのトラブルシューティングガイダンスについては、以下を参照してください。

- https://learn.microsoft.com/ja-jp/azure/azure-monitor/agents/azure-monitor-agent-troubleshoot-windows-vm/
- https://learn.microsoft.com/ja-jp/azure/azure-resource-manager/troubleshooting/create-troubleshooting-template/

顧客管理の暗号化キーでマシンカタログを作成する

顧客管理の暗号化キーを使用してマシンカタログを作成する詳細な手順は次のとおりです。

1. PowerShellウィンドウを開きます。
2. Citrix固有のPowerShellモジュールをロードするために `asnp citrix*` を実行します。
3. `cd xdhyp:/` を入力します。
4. `cd .\HostingUnits\(your hosting unit)` を入力します。
5. `cd diskencryptionset.folder` を入力します。
6. ディスク暗号化セットのリストを取得するには、`dir` を入力します。
7. ディスク暗号化セットのIDをコピーします。
8. ディスク暗号化セットのIDを含めるカスタムプロパティ文字列を作成します。例：

```
$customProperties = "<CustomProperties xmlns=`"http://
schemas.citrix.com/2014/xd/machinecreation`" xmlns:xsi=`"http://
www.w3.org/2001/XMLSchema-instance`">

<Property xsi:type=`"StringProperty`" Name=`"StorageAccountType`"
Value=`"Standard_LRS`" />
```

```
<Property xsi:type=`"StringProperty`" Name=`"persistWBC`"
Value=`"False`" />

<Property xsi:type=`"StringProperty`" Name=`"PersistOsDisk`"
Value=`"false`" />

<Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`"
Value=`"true`" />

<Property xsi:type=`"StringProperty`" Name=`"DiskEncryptionSetId`"
Value=`"/subscriptions/0xxx4xxx-xxb-4bxx-xxxx-xxxxxxxx/resourceGroups/
abc/providers/Microsoft.Compute/diskEncryptionSets/abc-des`"/>

</CustomProperties>
```

9. まだ作成されていない場合は、IDプールを作成します。例：

```
New-AcctIdentityPool -IdentityPoolName idPool -NamingScheme ms##
-Domain def.local -NamingSchemeType Numeric
```

10. New-ProvSchemeコマンドを実行します。例：

```
New-ProvScheme -CleanOnBoot -HostingUnitName "name" -IdentityPoolName
"name" -InitialBatchSizeHint 1

-MasterImageVM "XDHyp:\HostingUnits\azure-
res2\image.folder\def.resourcegroup\def.snapshot"

-NetworkMapping @{"0"="XDHyp:\HostingUnits\azure-res2\
\virtualprivatecloud.folder\def.resourcegroup\def-
vnet.virtualprivatecloud\subnet1.network"}

-ProvisioningSchemeName "name"

-ServiceOffering "XDHyp:\HostingUnits\azure-
res2\serviceoffering.folder\Standard_DS2_v2.serviceoffering"

-MachineProfile "XDHyp:
\HostingUnits\<adnet>\machineprofile.folder\<def.resourcegroup>\<machin
e profile vm.vm>"
```

```
-CustomProperties $customProperties
```

11. マシンカタログの作成を完了します。

二重暗号化でマシンカタログを作成する

Web Studio および PowerShell コマンドを使用して、二重暗号化されたマシンカタログを作成および更新できます。

二重暗号化でマシンカタログを作成する詳細な手順は次のとおりです。

1. プラットフォーム管理キーと顧客管理キーを使用して、Azure Key Vault と DES を作成します。Azure Key Vault と DES の作成方法については、「Azure portal を使用してマネージドディスクの保存時の二重暗号化を有効にする」を参照してください。
2. ホスティング接続で利用可能な DiskEncryptionSets を参照するには：

   a. **PowerShell** ウィンドウを開きます。

   b. 次の PowerShell コマンドを実行します。

      i. `asnp citrix*`

      ii. `cd xdhyp:`:

      iii. `cd HostingUnits`

      iv. `cd YourHostingUnitName`（例えば、azure-east）

      v. `cd diskencryptionset.folder`

      vi. `dir`

   `DiskEncryptionSet`のIDを使用して、カスタムプロパティでカタログを作成または更新できます。
3. マシンプロファイルワークフローを使用する場合は、VMまたはテンプレート仕様をマシンプロファイルの入力として作成します。

   - VMをマシンプロファイルの入力として使用する場合は、:

     a. Azure PortalでVMを作成します。

     b. **ディスク>キー管理**に移動して、任意の`DiskEncryptionSetID`でVMを直接暗号化します。

   - テンプレート仕様をマシンプロファイルの入力として使用する場合は、:

a. テンプレートで、`properties>storageProfile>osDisk>managedDisk`の下に`diskEncryptionSet`パラメーターを追加し、二重暗号化DESのIDを追加します。

4. マシンカタログを作成します。

- Web Studio を使用している場合は、マシンカタログの作成 の手順に加えて、次のいずれかを実行します。
  - マシンプロファイルベースのワークフローを使用しない場合は、 ページで、 を選択します。次に、ドロップダウンから二重暗号化 DES を選択します。カタログの作成を続行します。
  - マシンプロファイルワークフローを使用している場合は、 ページでマスターイメージとマシンプロファイルを選択します。マシンプロファイルのプロパティにディスク暗号化セット ID があることを確認します。

  カタログで作成されたすべてのマシンは、選択した DES に関連付けられたキーによって二重に暗号化されます。
- PowerShellコマンドを使用する場合は、次のいずれかを実行します。
  - マシンプロファイルベースのワークフローを使用しない場合は、`New-ProvScheme`コマンドにカスタムプロパティ`DiskEncryptionSetId`を追加します。例:

```
New-ProvScheme -CleanOnBoot -CustomProperties '<CustomProperties
xmlns="http://schemas.citrix.com/2014/xd/machinecreation"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks"
Value="true" />

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
Value="/subscriptions/12345678-xxxx-1234-1234-123456789012/
resourceGroups/Sample-RG/providers/Microsoft.Compute/
diskEncryptionSets/SampleEncryptionSet" />

</CustomProperties>'

-HostingUnitName "Redacted"

-IdentityPoolName "Redacted"
```

```
-InitialBatchSizeHint 1

-MasterImageVM "Redacted"

-NetworkMapping @{"0"="Redacted"}

-ProvisioningSchemeName "Redacted"

-ServiceOffering "Redacted"
```

- マシンプロファイルベースのワークフローを使用する場合は、`New-ProvScheme`コマンドでマシンプロファイル入力を利用します。例:

```
New-ProvScheme -CleanOnBoot

-HostingUnitName azure-east

-IdentityPoolName aio-ip

-InitialBatchSizeHint 1

-MasterImageVM XDHyp:\HostingUnits\azure-
east\image.folder\abc.resourcegroup\fgb-vda-snapshot.snapshot

-NetworkMapping @{"0"="XDHyp:\HostingUnits\azure-
east\virtualprivatecloud.folder\apa-
resourceGroup.resourcegroup\apa-resourceGroup-
vnet.virtualprivatecloud\default.network"}

-ProvisioningSchemeName aio-test

-MachineProfile XDHyp:\HostingUnits\azure-
east\machineprofile.folder\abc.resourcegroup\abx-
mp.templatespec\1.0.0.templatespecversion
```

5. リモートPowerShell SDKを使用してカタログの作成を完了します。リモートPowerShell SDKを使用してカタログを作成する方法については、https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/を参照してください。カタログで作成されたすべてのマシンは、選択したDESに関連付けられたキーによって二重に暗号化されます。

暗号化されていないカタログを二重暗号化を使用するように変換する

マシンカタログの暗号化タイプ（カスタムプロパティまたはマシンプロファイルを使用）は、カタログが以前に暗号化されていなかった場合にのみ更新できます。

- マシンプロファイルベースのワークフローを使用しない場合は、`Set-ProvScheme`コマンドにカスタムプロパティDiskEncryptionSetIdを追加します。例:

```
Set-ProvScheme -ProvisioningSchemeName "SampleProvSchemeName"

-CustomProperties '<CustomProperties xmlns="http://schemas.citrix.com/
2014/xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="DiskEncryptionSetId" Value="/
subscriptions/12345678-xxxx-1234-1234-123456789012/resourceGroups/
Sample-RG/providers/Microsoft.Compute/diskEncryptionSets/
SampleEncryptionSet" />

</CustomProperties>'
```

- マシンプロファイルベースのワークフローを使用する場合は、`Set-ProvScheme`コマンドでマシンプロファイル入力を利用します。例:

```
Set-ProvScheme -ProvisioningSchemeName mxiao-test -MachineProfile
XDHyp:\HostingUnits\azure-
east\machineprofile.folder\aelx.resourcegroup\elx-
mp.templatespec\1.0.0.templatespecversion
```

成功すると、カタログに追加するすべての新しいVMは、選択したDESに関連付けられたキーによって二重暗号化されます。

カタログが二重暗号化されていることを確認する

- ウェブスタジオで:

a. **マシンカタログ**に移動します。

b. 確認するカタログを選択します。画面下部にある**テンプレートプロパティ**タブをクリックします。

c. **Azureの詳細**の下で、**ディスク暗号化セット**のディスク暗号化セットIDを確認します。カタログのDES IDが空白の場合、カタログは暗号化されていません。

d. Azure Portal で、DES ID に関連付けられている DES の暗号化の種類がプラットフォーム管理キーと顧客管理キーであることを確認します。

- PowerShellコマンドを使用する:

a. **PowerShell** ウィンドウを開きます。

b. `asnp citrix*` を実行して、Citrix 固有の PowerShell モジュールをロードします。

c. `Get-ProvScheme` を使用して、マシンカタログの情報を取得します。例:

```
Get-ProvScheme -ProvisioningSchemeName "SampleProvSchemeName"
```

d. マシンカタログの DES ID カスタムプロパティを取得します。例:

```
<Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
Value="/subscriptions/12345678-1234-1234-1234-123456789012/
resourceGroups/Sample-RG/providers/Microsoft.Compute/
diskEncryptionSets/SampleEncryptionSet" />
```

e. Azure Portal で、DES ID に関連付けられている DES の暗号化の種類がプラットフォーム管理キーと顧客管理キーであることを確認します。

Azureエフェメラルディスクを使用してカタログを作成する

エフェメラルディスクを使用するには、`New-ProvScheme` の実行時にカスタムプロパティ `UseEphemeralOsDisk` を **true** に設定する必要があります。

注：

カスタムプロパティ `UseEphemeralOsDisk` が **false** に設定されているか、値が指定されていない場合、プロビジョニングされたすべてのVDAはプロビジョニングされたOSディスクを引き続き使用します。

以下は、プロビジョニングスキームで使用するカスタムプロパティのセットの例です。

```
"CustomProperties": [

            {
```

```
            "Name": "UseManagedDisks",
            "Value": "true"
        },
        {
            "Name": "StorageType",
            "Value": "Standard_LRS"
        },
        {
            "Name": "UseSharedImageGallery",
            "Value": "true"
        },
        {
            "Name": "SharedImageGalleryReplicaRatio",
            "Value": "40"
        },
        {
            "Name": "SharedImageGalleryReplicaMaximum",
            "Value": "10"
        },
        {
            "Name": "LicenseType",
            "Value": "Windows_Server"
```

```
            },
            {
                "Name": "UseEphemeralOsDisk",
                "Value": "true"
            }
        ],
```

カタログのエフェメラルディスクを構成する

カタログのAzureエフェメラルOSディスクを構成するには、`Set-ProvScheme`で`UseEphemeralOsDisk`パラメーターを使用します。`UseEphemeralOsDisk`パラメーターの値を**true**に設定します。

注：

この機能を使用するには、`UseManagedDisks`と`UseSharedImageGallery`のパラメーターも有効にする必要があります。

例:

```
Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="UseSharedImageGallery"
Value="true" />

<Property xsi:type="StringProperty" Name="UseEphemeralOsDisk"
Value="true" />

</CustomProperties>'
```

エフェメラルディスクに関する重要な考慮事項

`New-ProvScheme` を使用してエフェメラルOSディスクをプロビジョニングするには、次の制約を考慮してください。

- カタログに使用されるVMサイズは、エフェメラルOSディスクをサポートしている必要があります。
- VMサイズに関連付けられているキャッシュまたは一時ディスクのサイズは、OSディスクのサイズ以上である必要があります。
- 一時ディスクのサイズは、キャッシュディスクのサイズよりも大きくする必要があります。

以下の際にもこれらの問題を考慮してください:

- プロビジョニングスキームを作成する際。
- プロビジョニングスキームを変更する際。
- イメージを更新する際。

Azure専用ホスト

MCSを使用して、Azure専用ホストにVMをプロビジョニングできます。Azure専用ホストにVMをプロビジョニングする前に:

- ホストグループを作成します。
- そのホストグループにホストを作成します。
- カタログと仮想マシンを作成するために、十分なホスト容量が予約されていることを確認してください。

次のPowerShellスクリプトを使用して、ホストテナンシーが定義されたマシンのカタログを作成できます。

```
New-ProvScheme <otherParameters> -CustomProperties '<CustomProperties
xmlns="http://schemas.citrix.com/2014/xd/machinecreation"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

 <Property xsi:type="StringProperty" Name="HostGroupId"
Value="myResourceGroup/myHostGroup" />

 ...other Custom Properties...

 </CustomProperties>
```

MCSを使用してAzure専用ホストに仮想マシンをプロビジョニングする場合、以下を考慮してください。

- *専用ホスト*はカタログのプロパティであり、カタログ作成後に変更することはできません。専用テナンシーは現在、Azureではサポートされていません。
- ホスティングユニットのリージョンにある、事前に構成されたAzureホストグループが、`HostGroupId` パラメーターを使用する際に必要です。
- Azureの自動配置が必要です。この機能は、ホストグループに関連付けられたサブスクリプションをオンボードするための要求を行います。詳細については、VM Scale Set on Azure Dedicated Hosts - Public Preview を参照してください。自動配置が有効になっていない場合、MCSはカタログ作成中にエラーをスローします。

Azure Compute Galleryイメージを使用してマシンカタログを作成または更新する

マシンカタログの作成に使用するイメージを選択する際、Azure Compute Gallery で作成したイメージを選択できます。

これらのイメージを表示するには、次の操作を行う必要があります。

1. Citrix Virtual Apps and Desktops サイトを構成します。
2. Azure Resource Manager に接続します。
3. Azure portal で、リソースグループを作成します。詳細については、「ポータルを使用して Azure Compute Gallery を作成する」を参照してください。
4. リソースグループで、Azure Compute Gallery を作成します。
5. Azure Compute Gallery で、イメージ定義を作成します。
6. イメージ定義で、イメージバージョンを作成します。

Azure Compute Gallery のイメージを使用してマシンカタログを作成または更新するには、次の PowerShell コマンドを使用します。

1. PowerShell ウィンドウを開きます。
2. Citrix固有のPowerShellモジュールをロードするために`asnp citrix*`を実行します。
3. リソースグループを選択し、そのリソースグループのすべてのギャラリーを一覧表示します。

```
Get-ChildItem -LiteralPath @("XDHyp:
\HostingUnits\testresource\image.folder\sharedImageGalleryTest.resource
group")
```

4. ギャラリーを選択し、そのギャラリーのすべてのイメージ定義を一覧表示します。

```
Get-ChildItem -LiteralPath @("XDHyp:
\HostingUnits\testresource\image.folder\sharedImageGalleryTest.resource
group\sharedImageGallery.sharedimagegallery")
```

5. 1つのイメージ定義を選択し、そのイメージ定義のすべてのイメージバージョンを一覧表示します。

```
Get-ChildItem -LiteralPath @("XDHyp:
\HostingUnits\testresource\image.folder\sharedImageGalleryTest.resource
group\sharedImageGallery.sharedimagegallery\sigtestimage.imagedefinitio
n")
```

6. 次の要素を使用してMCSカタログを作成および更新します。

   - リソースグループ
   - ギャラリー
   - ギャラリーイメージ定義
   - ギャラリーイメージバージョン

   Remote PowerShell SDK を使用してカタログを作成する方法については、https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/ を参照してください。

共有イメージギャラリーの構成

`New-ProvScheme` コマンドを使用して、Shared Image Gallery をサポートするプロビジョニングスキームを作成します。`Set-ProvScheme` コマンドを使用して、プロビジョニングスキームのこの機能を有効または無効にし、レプリカ比率とレプリカの最大値を変更します。

Shared Image Gallery 機能をサポートするために、プロビジョニングスキームに3つのカスタムプロパティが追加されました。

`UseSharedImageGallery`

- 公開されたイメージの保存に Shared Image Gallery を使用するかどうかを定義します。**True** に設定すると、イメージは Shared Image Gallery イメージとして保存され、それ以外の場合はスナップショットとして保存されます。
- 有効な値は**True**と**False**です。

- プロパティが定義されていない場合、デフォルト値は**False**です。

`SharedImageGalleryReplicaRatio`

- マシンとギャラリーイメージバージョンレプリカの比率を定義します。
- 有効な値は0より大きい整数です。
- プロパティが定義されていない場合、デフォルト値が使用されます。永続OSディスクのデフォルト値は1000、非永続OSディスクのデフォルト値は40です。

`SharedImageGalleryReplicaMaximum`

- 各ギャラリーイメージバージョンに対するレプリカの最大数を定義します。
- 有効な値は0より大きい整数です。
- プロパティが定義されていない場合、デフォルト値は10です。
- Azure は現在、ギャラリーイメージの単一バージョンに対して最大10個のレプリカをサポートしています。プロパティが Azure でサポートされている値よりも大きい値に設定されている場合、MCS は指定された値を使用しようとします。Azure はエラーを生成し、MCS はそれをログに記録し、現在のレプリカ数は変更されません。

> **ヒント:**
>
> MCS プロビジョニングカタログの公開イメージを保存するために Shared Image Gallery を使用する場合、MCS はカタログ内のマシンの数、レプリカ比率、およびレプリカの最大値に基づいて、ギャラリーイメージバージョンのレプリカ数を設定します。レプリカ数は、カタログ内のマシンの数をレプリカ比率で除算し（最も近い整数に切り上げ）、その値を最大レプリカ数で制限することによって計算されます。たとえば、レプリカ比率が20、最大値が5の場合、0～20台のマシンには1つのレプリカが作成され、21～40台には2つのレプリカ、41～60台には3つのレプリカ、61～80台には4つのレプリカ、81台以上には5つのレプリカが作成されます。

ユースケース：Shared Image Gallery のレプリカ比率とレプリカの最大値の更新

既存のマシンカタログは Shared Image Gallery を使用しています。`Set-ProvScheme` コマンドを使用して、カタログ内のすべての既存マシンおよび将来のマシンのカスタムプロパティを更新します。

```
Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<Property xsi:type="StringProperty" Name="StorageType"
Value="Standard_LRS"/> <Property xsi:type="StringProperty"
Name="UseManagedDisks" Value="True"/> <Property xsi:type="StringProperty"
Name="UseSharedImageGallery" Value="True"/> <Property
xsi:type="IntProperty" Name="SharedImageGalleryReplicaRatio" Value="30"/>
<Property xsi:type="IntProperty" Name="SharedImageGalleryReplicaMaximum"
Value="20"/></CustomProperties>'
```

ユースケース：スナップショットカタログを Shared Image Gallery カタログに変換する

このユースケースの場合：

1. `UseSharedImageGallery`フラグを**True**に設定して`Set-ProvScheme`を実行します。オプションで`SharedImageGalleryReplicaRatio`および`SharedImageGalleryReplicaMaximum`プロパティを含めます。
2. カタログを更新します。
3. マシンをパワーサイクルして、強制的に更新します。

例:

```
Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<Property xsi:type="StringProperty" Name="StorageType"
Value="Standard_LRS"/> <Property xsi:type="StringProperty"
Name="UseManagedDisks" Value="True"/> <Property xsi:type="StringProperty"
Name="UseSharedImageGallery" Value="True"/> <Property
xsi:type="IntProperty" Name="SharedImageGalleryReplicaRatio" Value="30"/>
<Property xsi:type="IntProperty" Name="SharedImageGalleryReplicaMaximum"
Value="20"/></CustomProperties>'
```

ヒント:

パラメーター`SharedImageGalleryReplicaRatio`と`SharedImageGalleryReplicaMaximum`は必須ではありません。`Set-ProvScheme`コマンドが完了しても、共有イメージギャラリーのイメージはまだ作成されていません。カタログ

がギャラリーを使用するように構成されると、次回のカタログ更新操作で公開されたイメージがギャラリーに保存されます。カタログ更新コマンドは、ギャラリー、ギャラリーイメージ、およびイメージバージョンを作成します。マシンを再起動すると更新され、必要に応じてレプリカ数が更新されます。その時点から、既存のすべての非永続マシンは共有イメージギャラリーのイメージを使用してリセットされ、新しくプロビジョニングされたすべてのマシンはそのイメージを使用して作成されます。古いスナップショットは数時間以内に自動的にクリーンアップされます。

ユースケース: 共有イメージギャラリーカタログをスナップショットカタログに変換する

このユースケースの場合：

1. `UseSharedImageGallery` フラグを **False** に設定するか、未定義のままにして `Set-ProvScheme` を実行します。
2. カタログを更新します。
3. マシンをパワーサイクルして、強制的に更新します。

例:

```
Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<Property xsi:type="StringProperty" Name="StorageType"
Value="Standard_LRS"/> <Property xsi:type="StringProperty"
Name="UseManagedDisks" Value="True"/> <Property xsi:type="StringProperty"
Name="UseSharedImageGallery" Value="False"/></CustomProperties>'
```

ヒント:

スナップショットから共有イメージギャラリーカタログへの更新とは異なり、各マシンのカスタムデータは新しいカスタムプロパティを反映するようにまだ更新されていません。元の共有イメージギャラリーのカスタムプロパティを表示するには、次のコマンドを実行します: `Get-ProvVm -ProvisioningSchemeName catalog-name`。`Set-ProvScheme` コマンドが完了しても、イメージスナップショットはまだ作成されていません。カタログがギャラリーを使用しないように構成されると、次回のカタログ更新操作で公開されたイメージがスナップショットとして保存されます。その時点から、既存のすべての非永続マシンはスナップショットを使用してリセットされ、新しくプロビジョニングされたすべてのマシンはスナップショットから作成されます。マシンを再起動すると更新され、その時点でカスタムマシン

データが更新され、`UseSharedImageGallery` が **False** に設定されていることが反映されます。古い共有イメージギャラリーのアセット（ギャラリー、イメージ、バージョン）は数時間以内に自動的にクリーンアップされます。

指定された可用性ゾーンにマシンをプロビジョニングする

Azure環境では、特定の可用性ゾーンにマシンをプロビジョニングできます。これはPowerShellを使用して実現できます。

注：

ゾーンが指定されていない場合、MCSはAzureにそのリージョン内にマシンを配置させます。複数のゾーンが指定されている場合、MCSはそれらのゾーンにマシンをランダムに分散させます。

PowerShellによる可用性ゾーンの構成

PowerShellを使用して、`Get-Item` で提供されるインベントリアイテムを表示できます。たとえば、*米国東部リージョン*の `Standard_B1ls` サービス提供を表示するには:

```
$serviceOffering = Get-Item -path "XDHyp:\Connections\my-connection-
name\East US.region\serviceoffering.folder\Standard_B1ls.serviceoffering"
```

ゾーンを表示するには、アイテムの`AdditionalData`パラメーターを使用します:

`$serviceOffering.AdditionalData`

可用性ゾーンが指定されていない場合、マシンのプロビジョニング方法に変更はありません。

PowerShellを介して可用性ゾーンを構成するには、`New-ProvScheme`操作で利用可能な**Zones**カスタムプロパティを使用します。**Zones**プロパティは、マシンをプロビジョニングする可用性ゾーンのリストを定義します。これらのゾーンには、1つ以上の可用性ゾーンを含めることができます。たとえば、ゾーン1および3の`<Property xsi:type="StringProperty" Name="Zones" Value="1, 3"/>`です。

プロビジョニングスキームのゾーンを更新するには、`Set-ProvScheme`コマンドを使用します。

無効なゾーンが提供された場合、プロビジョニングスキームは更新されず、無効なコマンドを修正する方法に関する指示を提供するエラーメッセージが表示されます。

ヒント:

無効なカスタムプロパティを指定すると、プロビジョニングスキームは更新されず、関連するエラーメッセージが表示されます。

ストレージの種類

MCSを使用するAzure環境の仮想マシンに対して、異なるストレージの種類を選択します。ターゲットVMの場合、MCSは以下をサポートします。

- OSディスク: プレミアムSSD、SSD、またはHDD
- ライトバックキャッシュディスク: プレミアムSSD、SSD、またはHDD

これらのストレージの種類を使用する場合、以下を考慮してください。

- 選択したストレージの種類をVMがサポートしていることを確認してください。
- 構成でAzureエフェメラルディスクを使用している場合、ライトバックキャッシュディスク設定のオプションは表示されません。

ヒント:

`StorageType` はOSタイプとストレージアカウント用に構成されます。`WBCDiskStorageType` はライトバックキャッシュストレージタイプ用に構成されます。通常のカタログの場合、`StorageType` が必要です。`WBCDiskStorageType` が構成されていない場合、`StorageType` が `WBCDiskStorageType` のデフォルトとして使用されます。

WBCDiskStorageType が構成されていない場合、StorageType が WBCDiskStorageType のデフォルトとして使用されます。

ストレージの種類を構成する

VMのストレージタイプを構成するには、`New-ProvScheme` の `StorageType` パラメーターを使用します。`StorageType` パラメーターの値をサポートされているストレージタイプのいずれかに設定します。

以下は、プロビジョニングスキームにおける `CustomProperties` パラメーターの設定例です。

```
Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="StorageType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="LicenseType"
Value="Windows_Client" />

</CustomProperties>'
```

ゾーン冗長ストレージを有効にする

カタログ作成時にゾーン冗長ストレージを選択できます。これは、Azure マネージドディスクを複数の可用性ゾーン間で同期的にレプリケートし、あるゾーンでの障害から他のゾーンの冗長性を利用して回復できるようにします。

ストレージタイプのカスタムプロパティで **Premium_ZRS** および **StandardSSD_ZRS** を指定できます。ZRSストレージは、既存のカスタムプロパティを使用するか、**MachineProfile** テンプレートを介して設定できます。ZRSストレージは、`-StartsNow` および `-DurationInMinutes -1` パラメーターを持つ `Set-ProvVMUpdateTimeWindow` コマンドでもサポートされており、既存のマシンをLRSからZRSストレージに変更できます。

制限事項:

- マネージドディスクのみをサポート
- プレミアムおよび標準ソリッドステートドライブ (SSD) のみでサポート
- `StorageTypeAtShutdown` には対応していません
- 一部のリージョンでのみ利用可能です。
- 大規模にZRSディスクを作成すると、Azureのパフォーマンスが低下します。そのため、最初の電源投入時には、マシンをより小さなバッチ（一度に300台未満のマシン）で起動してください。

ゾーン冗長ストレージをディスクストレージタイプとして設定する

初期カタログ作成時にゾーン冗長ストレージを選択することも、既存のカタログでストレージタイプを更新することもできます。

POWERSHELLコマンドを使用してゾーン冗長ストレージを選択する

`New-ProvScheme` PowerShellコマンドを使用してAzureで新しいカタログを作成する場合、`StorageAccountType`の値として`Standard_ZRS`を使用します。 例:

```
<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="StandardSSD_ZRS" />
```

この値を設定すると、それが適切に使用できるかどうかを判断する動的APIによって検証されます。ZRSの使用がカタログに対して有効でない場合、以下の例外が発生する可能性があります。

- **StorageTypeAtShutdownNotSupportedForZrsDisks**: StorageTypeAtShutdownカスタムプロパティはZRSストレージでは使用できません。
- **StorageAccountTypeNotSupportedInRegion**: この例外は、ZRSをサポートしていないAzureリージョンでZRSストレージを使用しようとすると発生します。
- **ZrsRequiresManagedDisks**: ゾーン冗長ストレージはマネージドディスクでのみ使用できます。

以下のカスタムプロパティを使用して、ディスクストレージタイプを設定できます。

- `StorageType`
- `WBCDiskStorageType`
- `IdentityDiskStorageType`

> **注：**
>
> カタログ作成時、カスタムプロパティが設定されていない場合は、マシンプロファイルのOSディスク`StorageType`が使用されます。

マシンプロファイルからVMとNICの診断設定をキャプチャする

マシンカタログの作成時、既存のマシンカタログの更新時、および既存のVMの更新時に、マシンプロファイルからVMとNICの診断設定をキャプチャできます。

VMまたはテンプレート仕様をマシンプロファイルのソースとして作成できます。

主な手順

1. Azureで必要なIDを設定します。これらのIDはテンプレート仕様で指定する必要があります。

- ストレージアカウント
- Log Analyticsワークスペース
- 標準ティアの価格設定のEvent Hub名前空間

2. マシンプロファイルのソースを作成します。
3. 新しいマシンカタログを作成するか、既存のカタログを更新するか、既存のVMを更新します。

Azureで必要なIDを設定する

Azureで次のいずれかを設定します。

- ストレージアカウント
- ログ分析ワークスペース
- Standardティアの価格設定を持つイベントハブ名前空間

ストレージアカウントを設定する

Azureで標準ストレージアカウントを作成します。テンプレート仕様では、ストレージアカウントの完全なresourceIdを`storageAccountId`として指定します。

VMがストレージアカウントにデータをログ記録するように設定されると、データは`insights-metrics-pt1m`コンテナの下で見つけることができます。

ログ分析ワークスペースを設定する

ログ分析ワークスペースを作成します。テンプレート仕様では、ログ分析ワークスペースの完全なresourceIdをworkspaceIdとして指定します。

VMがワークスペースにデータをログ記録するように設定されると、Azureのログでデータをクエリできます。Azureのログで次のコマンドを実行すると、リソースによってログ記録されたすべてのメトリックの数を表示できます。

```
AzureMetrics | summarize Count=count() by ResourceId
```

イベントハブを設定する

Azureポータルでイベントハブを設定するには、次の手順を実行します。

1. 標準ティアの価格設定でイベントハブ名前空間を作成します。
2. 名前空間の下にイベントハブを作成します。
3. イベントハブの下にある**キャプチャ**に移動します。トグルをONにして、Avro出力タイプでキャプチャします。

4. ログをキャプチャするために、既存のストレージアカウントに新しいコンテナを作成します。
5. テンプレートスペックで、次の形式で`eventHubAuthorizationRuleId`を指定します: `/subscriptions/093f4c12-704b-4b1d-8339-f339e7557f60/resourcegroups/matspo/providers/Microsoft.EventHub/namespaces/matspoeventhub/authorizationrules/RootManageSharedAccessKey`
6. イベントハブの名前を指定します。

VMがイベントハブにデータをログするように設定されると、データは構成されたストレージコンテナにキャプチャされます。

マシンプロファイルソースを作成する

VMまたはテンプレートスペックをマシンプロファイルソースとして作成できます。

診断設定を含むVMベースのマシンプロファイルを作成する

VMをマシンプロファイルとして作成する場合は、まずテンプレートVM自体に診断設定をセットアップします。詳細な手順については、MicrosoftドキュメントのAzure Monitorの診断設定を参照してください。

VMまたはNICに関連付けられた診断設定が現在存在することを確認するには、次のコマンドを実行できます。

```
az monitor diagnostic-settings list --resource-group matspo --resource matspo-tog-cc2659 --resource-type microsoft.network/networkInterfaces
```

```
az monitor diagnostic-settings list --resource-group matspo --resource matspo-tog-cc2 --resource-type microsoft.compute/virtualMachines
```

診断設定を含むテンプレートスペックベースのマシンプロファイルを作成する

診断設定がすでに有効になっているVMを使用し、それをARMテンプレートスペックにエクスポートする場合、これらの設定はテンプレートに自動的に含まれません。ARMテンプレート内で診断設定を手動で追加または変更する必要があります。

ただし、VMをマシンプロファイルとして使用する場合、MCSは、重要な診断設定が正確にキャプチャされ、MCSカタログ内のリソースに適用されることを保証します。

1. VMとNICを定義する標準テンプレート仕様を作成します。
2. スペックに従って診断設定をデプロイするための追加リソースを追加します: Microsoft.Insights diagnosticSettings。スコープには、テンプレート内のVMまたはNICを部分的なIDを持つ名前

で参照します。たとえば、テンプレートスペック内のtest-VMという名前のVMにアタッチされた診断設定を作成する場合、スコープを次のように指定します。

```
"scope": "microsoft.compute/virtualMachines/test-VM",
```

3. テンプレートスペックをマシンプロファイルソースとして使用します。

診断設定を含むカタログを作成または更新する

マシンプロファイルソースを作成した後、`New-ProvScheme` コマンドを使用してマシンカタログを作成し、`Set-ProvScheme` コマンドを使用して既存のマシンカタログを更新し、`Request-ProvVMUpdate` コマンドを使用して既存のVMを更新できます。

ページファイルの場所

Azure環境では、VMが最初に作成されるときに、ページファイルが適切な場所に設定されます。ページファイルの設定は、`<page file location>[min size] [max size]` の形式で構成されます（サイズはMB単位です）。詳細については、Microsoftドキュメント「適切なページファイルを決定する方法」を参照してください。

イメージ準備中に`ProvScheme`を作成すると、MCSは特定のルールに基づいてページファイルの場所を決定します。`ProvScheme`を作成した後：

- 受信VMサイズによってページファイル設定が異なる場合、VMサイズの変更はブロックされます。
- マシンプロファイルの更新によってサービスオファリングが変更され、ページファイル設定が異なる場合、マシンプロファイルの更新はブロックされます。
- エフェメラルOSディスク (EOS) およびMCSIOプロパティは変更できません。

ページファイルの場所の決定

EOSやMCSIOのような機能には、それぞれ独自の期待されるページファイルの場所があり、互いに排他的です。次の表は、各機能の期待されるページファイルの場所を示しています。

機能	期待されるページファイルの場所
EOS	OSディスク
MCSIO	まずAzure一時ディスク、それ以外の場合はライトバックキャッシュディスク

注：

イメージ準備がプロビジョニングスキームの作成から切り離されていても、MCSはページファイルの場所を正しく決定します。デフォルトのページファイルの場所はOSディスク上です。

ページファイル設定のシナリオ

次の表は、イメージ準備中およびプロビジョニングスキーム更新中のページファイル設定のいくつかの可能なシナリオについて説明しています。

状況	シナリオ	結果
イメージの準備	ソースイメージのページファイルが一時ディスクに設定されているが、プロビジョニングスキームで指定されたVMサイズには一時ディスクがない	ページファイルはOSディスクに配置されます
イメージの準備	ソースイメージのページファイルがOSディスクに設定されているが、プロビジョニングスキームで指定されたVMサイズには一時ディスクがある。	ページファイルは一時ディスクに配置されます
イメージの準備	ソースイメージのページファイルは一時ディスクに設定されていますが、プロビジョニングスキームではエフェメラルOSディスクが有効になっています。	ページファイルはOSディスクに配置されます
プロビジョニングスキームの更新	プロビジョニングスキームを更新しようとすると、元のVMサイズには一時ディスクがあり、ターゲットVMには一時ディスクがありません。	エラーメッセージとともに変更を拒否します
プロビジョニングスキームの更新	プロビジョニングスキームを更新しようとすると、元の	エラーメッセージとともに変更を拒否します

状況	シナリオ	結果
	VMサイズには一時ディスクがなく、ターゲットVMには一時ディスクがあります。	

ページファイル設定の更新

場所とサイズを含むページファイル設定は、PowerShellコマンドを使用して明示的に指定することもできます。これにより、MCSによって決定された値が上書きされます。これを行うには、`New-ProvScheme`コマンドを実行し、次のカスタムプロパティを含めます。

- `PageFileDiskDriveLetterOverride`: ページファイルの場所のディスクドライブ文字
- `InitialPageFileSizeInMB`: 初期ページファイルサイズ (MB)
- `MaxPageFileSizeInMB`: ページファイルの最大サイズ (MB)

カスタムプロパティの使用例:

```
-CustomProperties '<CustomProperties xmlns="http://schemas.citrix.com/
2014/xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance"> `

<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="false"/> `

<Property xsi:type="StringProperty" Name="PersistVm" Value="false"/> `

<Property
xsi:type="StringProperty" Name="PageFileDiskDriveLetterOverride" Value="d"/>
`


<Property
xsi:type="StringProperty" Name="InitialPageFileSizeInMB" Value="2048"/> `

<Property xsi:type="StringProperty" Name="MaxPageFileSizeInMB" Value="8196"/
> `

<Property
xsi:type="StringProperty" Name="StorageAccountType" Value="Premium_LRS"/> `

<Property
xsi:type="StringProperty" Name="LicenseType" Value="Windows_Client"/> `
```

```
</CustomProperties>'
```

制約:

- ページファイル設定は、`New-ProvScheme`コマンドを実行してプロビジョニングスキームを作成するときにのみ更新でき、後で変更することはできません。
- すべてのページファイル設定関連プロパティ (`PageFileDiskDriveLetterOverride`、`InitialPageFileSizeInMB`、および`MaxPageFileSizeInMB`) をカスタムプロパティで指定するか、いずれも指定しないでください。
- 初期ページファイルサイズは16 MBから16777216 MBの間である必要があります。
- 最大ページファイルサイズは、初期ページファイルサイズ以上で、かつ16777216 MB未満である必要があります。
- この機能はWeb Studioではサポートされていません。

Azure Spot VMを使用してカタログを作成する

Azure Spot VMを使用すると、Azureの未使用のコンピューティング容量を大幅なコスト削減で活用できます。ただし、Azure Spot VMを割り当てる機能は、現在の容量と価格設定に依存します。そのため、Azureは強制排除ポリシーに従って、実行中のVMを強制排除したり、VMの作成に失敗したり、VMの電源投入に失敗したりする可能性があります。したがって、Azure Spot VMは、一部の重要でないアプリケーションやデスクトップに適しています。詳細については、Azure Spot Virtual Machinesの使用を参照してください。

制限事項

- すべてのVMサイズがAzure Spot VMでサポートされているわけではありません。詳細については、制限事項を参照してください。

  VMサイズがSpot VMをサポートしているかどうかを確認するには、次のPowerShellコマンドを実行します。VMサイズがSpot VMをサポートしている場合、`SupportsSpotVM`は**True**になります。

  ```
  (Get-Item "XDHyp:\HostingUnits\azure-res-
  conn2\serviceoffering.folder\Standard_D2ds_v4.serviceoffering").
  AdditionalData
  ```

- 現在、Azure Spot VMは休止状態をサポートしていません。

要件

Azure Spot VMカタログのマシンプロファイルソース（VMまたはテンプレート仕様）を作成する際、(VMを使用している場合は) Azure Spot Instanceを選択するか、(テンプレート仕様を使用している場合は) `priority`を`Spot`として設定する必要があります。

Azure Spot VMを使用してカタログを作成する手順

1. マシンプロファイルソース（VMまたは起動テンプレート）を作成します。

   - Azureポータルを使用してVMを作成するには、Azureポータルを使用してAzure Spot Virtual Machinesを展開するを参照してください。
   - テンプレート仕様を作成するには、テンプレート仕様の**resources > type: Microsoft.Compute/virtualMachines > properties**の下に次のプロパティを追加します。例：

     ```
     "priority": "Spot",

     "evictionPolicy": "Deallocate",

     "billingProfile": {

     "maxPrice": 0.01

     }
     ```

注：

- 削除ポリシーは**Deallocate**または**Delete**にすることができます。
  - 非永続VMの場合、MCSは常に削除ポリシーを**Delete**に設定します。VMが削除された場合、非永続ディスク（例：OSディスク）とともに削除されます。永続ディスク（例：IDディスク）は削除されません。ただし、カタログタイプが永続的であるか、`PersistOsDisk`カスタムプロパティがTrueに設定されている場合、OSディスクは永続的です。同様に、`PersistWbc`カスタムプロパティが**True**に設定されている場合、WBCディスクは永続的です。
  - 永続VMの場合、MCSは常に削除ポリシーをDeallocateに設定します。VMが削除された場合、割り当て解除されます。ディスクに変更は加えられません。

- 最大価格は、1時間あたりに支払ってもよい価格です。**容量のみ**を使用している場合、これは**-1**です。最大価格は、null、-1、またはゼロより大きい小数のみです。詳細については、価格を参照してください。

2. マシンプロファイルがAzure Spot VM対応であるかどうかを確認するには、次のPowerShellコマンドを実行します。`SpotEnabled`パラメーターが**True**で、`SpotEvictionPolicy`が**Deallocate**または**Delete**に設定されている場合、マシンプロファイルはAzure Spot VM対応です。例：

   - マシンプロファイルのソースがVMの場合、次のコマンドを実行します。

     ```
     (Get-Item "XDHyp:\HostingUnits\azure-res-
     conn2\machineprofile.folder\fifthcolumn.resourcegroup\kb-spot-
     delete.vm"). AdditionalData
     ```

   - マシンプロファイルのソースがテンプレート仕様の場合、次のコマンドを実行します。

     ```
     (Get-Item "XDHyp:\HostingUnits\azure-res-
     conn2\machineprofile.folder\fifthcolumn.resourcegroup\fc-aeh-
     templatespec.templatespec\14.0.0-spot-
     delete.templatespecversion").AdditionalData
     ```

3. `New-ProvScheme` PowerShellコマンドを使用して、マシンプロファイルでマシンカタログを作成します。

`Set-ProvScheme`コマンドを使用してカタログを更新できます。既存のVMをPowerShellコマンド`Set-ProvVmUpdateTimeWindow`を使用して更新することもできます。マシンプロファイルは次回の電源投入時に更新されます。

実行中のAzure Spot VMでの強制排除

コンピューティング容量が利用できない場合、または時間あたりの価格が設定された最大価格よりも高い場合、Azureは実行中のSpot VMを強制排除します。デフォルトでは、強制排除の通知はされません。VMは単にフリーズし、強制排除されます。Microsoftは、強制排除を監視するためにScheduled Eventsを使用することを推奨しています。強制排除を継続的に監視するを参照してください。VM内からスクリプトを実行して、強制排除前に通知を受け取ることもできます。たとえば、MicrosoftはPythonでポーリングスクリプトScheduledEvents.csを提供しています。

トラブルシューティング

- プロビジョニングされたVMのcustomMachineDataで、`Get-ProvVM`コマンドを使用してSpot VMのプロパティを確認できます。優先度フィールドが**Spot**に設定されている場合、Spotが使用されています。
- Azure PortalでVMがSpotを使用しているかどうかを確認できます。

  a. Azure PortalでVMを見つけます。

  b. **概要**ページに移動します。

  c. 下にスクロールして、**Azure Spot**セクションを見つけます。

    - Spotが使用されていない場合、このフィールドは空です。
    - Spotが使用されている場合、**Azure Spot**および**Azure Spot eviction policy**フィールドが設定されます。

1. 構成ページで、VMの課金プロファイルまたは1時間あたりの最大価格を確認できます。

バックアップVMサイズの構成

パブリッククラウドでは、特定のVMサイズで容量が不足する場合があります。また、Azure Spot VMを使用している場合、Azureの容量要件に基づいてVMはいつでも強制終了されます。Azureの容量不足またはSpot VMの電源投入失敗の場合、MCSはバックアップVMサイズにフォールバックします。MCSマシンカタログの作成または更新時に、カスタムプロパティ`BackupVmConfiguration`を使用してバックアップVMサイズのリストを提供できます。MCSは、リストで指定された順序でバックアップVMサイズにフォールバックしようとします。

MCSがVMに特定のバックアップ構成を使用する場合、次回のシャットダウンまでその構成を使い続けます。次回の電源投入時には、MCSはプライマリVM構成を起動しようとします。失敗した場合、MCSはリストに従ってバックアップVMサイズ構成を再度起動しようとします。

この機能は、以下でサポートされています。

- マシンプロファイルを使用するカタログ
- 永続的および非永続的なMCSマシンカタログ
- 現在のAzure環境

重要な考慮事項

- リストには複数のバックアップVMサイズを指定できます。
- リストは一意である必要があります。

- リスト内の各VMにインスタンスタイププロパティを追加できます。タイプは**Spot**または**Regular**のいずれかです。タイプが指定されていない場合、MCSはVMを**Regular**と見なします。
- 既存のカタログのバックアップVMサイズリストは、`Set-ProvScheme` PowerShellコマンドを使用して変更できます。
- カタログに関連付けられたプロビジョニングスキームから作成された既存のVMは、`Set-ProvVMUpdateTimeWindow`コマンドを使用して更新できます。
- 選択した数の既存のMCS VMのバックアップVMサイズリストは、`Set-ProvVM`コマンドを使用して構成できます。ただし、更新を適用するには、`Set-ProvVMUpdateTimeWindow`を使用してVMの更新時間枠を設定し、その時間枠内でVMを起動します。VMで`Set-ProvVm`コマンドが使用された場合、プロビジョニングスキームのリストが後で更新されても、VMはその特定のVMに設定されたバックアップVMサイズリストを引き続き使用します。VMにプロビジョニングスキームのバックアップリストを使用させるには、`Set-ProvVM`を`-RevertToProvSchemeConfiguration`と共に使用できます。

バックアップVMサイズでカタログを作成する

> **注：**
>
> Studio UI のフリーズの問題に対処するには、PowerShell コマンドを実行する際に、すべてのシングルクォートを `"` に置き換えてください。

1. **PowerShell**ウィンドウを開きます。
2. Citrix 固有の PowerShell モジュールをロードするには、`asnp citrix*` を実行します。
3. Broker カタログを作成します。このカタログには、これから作成されるマシンが投入されます。
4. ID プールを作成します。これは、作成されるマシン用に作成された AD アカウントのコンテナになります。
5. マシンプロファイルを使用してプロビジョニングスキームを作成します。「バックアップ構成を構成する方法」を参照してください。
6. プロビジョニングスキームの一意の ID で BrokerCatalog を更新します。
7. VM を作成してカタログに追加します。

既存のカタログを更新する

`Set-ProvScheme` コマンドを使用してプロビジョニングスキームを更新できます。「バックアップ構成を構成する方法」を参照してください。

既存のVMを更新する

`Set-ProvVMUpdateTimeWindow` PowerShell コマンドを使用して、カタログ内の既存の VM を更新できます。このコマンドは、指定された時間枠内で次回の電源投入時に、カタログに関連付けられたプロビジョニングスキームから作成された VM を更新します。例:

- `Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName azure-catalog -StartTimeInUTC "3/12/2022 3am" -DurationInMinutes 60`
- `Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName azure-catalog -StartsNow -DurationInMinutes 60`

注：

`StartsNow`はスケジュールされた開始時間を示します。`DurationInMinutes`はスケジュールの時間枠です。

選択した数の既存のMCS VMのバックアップVMサイズリストは、`Set-ProvVM`コマンドを使用して構成できます。ただし、更新を適用するには、`Set-ProvVMUpdateTimeWindow`を使用してVMの更新時間枠を設定し、その時間枠内でVMを起動します。例：

1. 選択した既存のMCS VMのバックアップVMサイズリストを構成するには、`Set-ProvVM`コマンドを実行します。例：

```
Set-ProvVM -ProvisioningSchemeName "name" -VMName "Vm-001"

-CustomProperties

"<CustomProperties xmlns=`"http://schemas.citrix.com/2014/xd/
machinecreation`"xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`">

<Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`"
Value=`"true`" />

<Property xsi:type=`"StringProperty`" Name=`"StorageAccountType`"
```

```
Value=`"Premium_LRS`" />

<Property xsi:type=`"StringProperty`" Name=`"LicenseType`"
Value=`"Windows_Server`"/>

<Property xsi:type=`"StringProperty`" Name=`"PersistWBC`"
Value=`"true`"/>

<Property xsi:type=`"StringProperty`" Name=`"BackupVmConfiguration`"
Value=`"[{&quot;ServiceOffering&quot;: &quot;Standard_D2as_v4&quot;,
&quot;Type&quot;: &quot;Spot&quot;}, {&quot;ServiceOffering&quot;:
&quot;Standard_D2s_v3&quot;, &quot;Type&quot;: &quot;Regular&quot;},
{&quot;ServiceOffering&quot;: &quot;Standard_D2s_v3&quot;,
&quot;Type&quot;: &quot;Spot&quot;}]`"/>

</CustomProperties>"
```

2. 更新を適用するには、`Set-ProvVMUpdateTimeWindow`コマンドを実行します。例：

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName azure-catalog
-StartsNow -DurationInMinutes 60
```

すべてのリソースにタグをコピーする

マシンプロファイルで指定されたタグを、新しいVMまたはマシンカタログ内の既存のVMのすべてのリソース（複数のNICやディスク（OSディスク、IDディスク、ライトバックキャッシュディスクなど））にコピーできます。マシンプロファイルのソースは、VMまたはARMテンプレート仕様にすることができます。

注：

リソースにタグを保持するには、タグにポリシーを追加するか（タグコンプライアンスのポリシー定義を割り当てるを参照）、マシンプロファイルソースにタグを追加する必要があります。

前提条件

そのVMのVM、ディスク、NICにタグを付けるには、マシンプロファイルソース（VMまたはARMテンプレート仕様）を作成します。

- VMをマシンプロファイルの入力として使用したい場合は、AzureポータルでVMとすべてのリソースにタグを適用します。Azureポータルでタグを適用するを参照してください。
- ARMテンプレート仕様をマシンプロファイルの入力として使用したい場合は、各リソースの下に次のタグブロックを追加します。

```
 "tags": {

"TagC": "Value3"

},
```

注：

テンプレート仕様には、最大1つのディスクと少なくとも1つのNICを含めることができます。

新しいマシンカタログ内のVMのリソースにタグをコピーする

1. VMまたはARMテンプレート仕様をマシンプロファイルの入力として使用して、非永続または永続カタログを作成します。
2. カタログにVMを追加して電源をオンにします。マシンプロファイルで指定されたタグが、そのVMの対応するリソースにコピーされていることを確認する必要があります。

注：

マシンプロファイルで提供されるNICの数と、VMで使用するNICの数に不一致がある場合、エラーが発生します。

既存のVMのリソース上のタグを変更する

1. すべてのリソースにタグを付けたマシンプロファイルを作成します。
2. 既存のマシンカタログを、更新されたマシンプロファイルで更新します。例：

```
Set-ProvScheme -ProvisioningSchemeName <YourCatalogName>
-MachineProfile <PathToYourMachineProfile>
```

3. 更新を適用したいVMの電源をオフにします。
4. VMのスケジュールされたアップデートを要求します。例:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName <YourCatalogName>  -
VMName machine1 -StartsNow -DurationInMinutes -1
```

5. VMの電源をオンにします。
6. マシンプロファイルで指定されたタグが、対応するリソースにコピーされていることを確認する必要があります。

注：

マシンプロファイルで提供されるNICの数と、`Set-ProvScheme`で提供されるNICの数に不一致がある場合、エラーが発生します。

次のステップ

- これが最初に作成されたカタログである場合、Web Studioはデリバリーグループの作成を案内します。
- 構成プロセス全体を確認するには、「」(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/install-configure.html)を参照してください。
- カタログを管理するには、「」(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/install-configure/machine-catalogs-manage.html)および「」(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/install-configure/machine-catalogs-manage/manage-machine-catalog-azure.html)を参照してください。

詳細情報

- 接続とリソースの作成および管理
- マイクロソフト Azure リソース マネージャーへの接続
- マシンカタログの作成

Microsoft System Center Virtual Machine Managerカタログを作成する

(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/install-configure/machine-catalogs-create.html)では、マシンカタログを作成するウィザードについて説明しています。以下の情報は、Microsoft System Center Virtual Machine Manager (VMM) 仮想化環境に固有の詳細を扱っています。

> **注：**
>
> VMMカタログを作成する前に、VMMへの接続の作成を完了する必要があります。(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/install-configure/connections/connection-mscvmm.html)を参照してください。

マスターVMを作成する

1. マスターVMにVDAをインストールし、パフォーマンスを向上させるためにデスクトップを最適化するオプションを選択します。
2. バックアップとして使用するために、マスターVMのスナップショットを作成します。
3. 仮想デスクトップを作成します。

SMB 3ファイル共有上のMCS

VMストレージ用のSMB 3ファイル共有でMCSを使用して作成されたマシンカタログの場合、資格情報が次の要件を満たしていることを確認してください。これらの要件により、ControllerのHypervisor Communications Library（HCL）からの呼び出しがSMBストレージに正常に接続されます。

- VMMユーザーの資格情報には、SMBストレージへの完全な読み取り/書き込みアクセス権が含まれている必要があります。
- VMライフサイクルイベント中のストレージ仮想ディスク操作は、VMMユーザー資格情報を使用してHyper-Vサーバー経由で実行されます。

SMBストレージを使用する場合は、Controllerから個々のHyper-Vマシンへの認証資格情報セキュリティサポートプロバイダー（CredSSP）を有効にします。このプロセスは、Windows Server 2012上のHyper-VとVMM 2012 SP1で使用します。詳細については、CTX137465を参照してください。

HCLは`CredSSP`を使用してHyper-Vマシンへの接続を開きます。この機能は、Kerberosで暗号化されたユーザー資格情報をHyper-Vマシンに渡します。リモートHyper-Vマシン上のセッションでの**PowerShell**コマンドは、提供された資格情報で実行されます。この場合、ストレージへの通信コマンドが正しく機能するように、VMMユーザーの資格情報が使用されます。

次のタスクでは、HCLで生成され、SMB 3.0ストレージに対して動作するためにHyper-Vマシンに送信されるPowerShellスクリプトを使用します。

- **マスターイメージの統合**: マスターイメージは、MCSプロビジョニングスキーム（マシンカタログ）を作成します。マスターVMをクローンしてフラット化し、新しく作成されたディスクからVMを作成できるようにします（元のマスターVMへの依存関係を削除します）。

  root\\virtualization\\v2名前空間のConvertVirtualHardDisk

  例:

```
$ims = Get-WmiObject -class $class -namespace "root\\virtualization\\v2";

$result = $ims.ConvertVirtualHardDisk($diskName, $vhdastext)

$result
```

- **差分ディスクの作成:** マスターイメージを統合して生成されたマスターイメージから差分ディスクを作成します。その後、差分ディスクは新しいVMに接続されます。

  root\\virtualization\\v2名前空間のCreateVirtualHardDisk

  例:

```
$ims = Get-WmiObject -class $class -namespace "root\\virtualization\\v2";

$result = $ims.CreateVirtualHardDisk($vhdastext);

$result
```

- **IDディスクのアップロード:** HCLはIDディスクをSMBストレージに直接アップロードできません。そのため、Hyper-VマシンがIDディスクをストレージにアップロードしてコピーする必要があります。Hyper-VマシンはControllerからディスクを読み取ることができないため、HCLはまず次のようにHyper-Vマシン経由でIDディスクをコピーする必要があります。

  a. HCLは、管理者共有を介してIDをHyper-Vマシンにアップロードします。
  b. Hyper-Vマシンは、PowerShellリモートセッションで実行されているPowerShellスクリプトを介して、ディスクをSMBストレージにコピーします。Hyper-Vマシン上にフォルダーが作成され、そのフォルダーのアクセス許可はVMMユーザーのみにロックされます（リモートPowerShell接続を介して）。
  c. HCLは、管理者共有からファイルを削除します。

d. HCLがIDディスクのHyper-Vマシンへのアップロードを完了すると、リモートPowerShellセッションはIDディスクをSMBストレージにコピーします。その後、Hyper-Vマシンから削除します。

IDディスクフォルダーは、削除された場合でも再利用できるように再作成されます。

- **IDディスクのダウンロード:** アップロードと同様に、IDディスクはHyper-Vマシンを経由してHCLに渡されます。次のプロセスでは、Hyper-Vサーバー上にVMMユーザー権限のみを持つフォルダーが存在しない場合に作成します。

  a. Hyper-Vマシンは、PowerShellスクリプトを介してSMBストレージからローカルのHyper-Vストレージにディスクをコピーします。このスクリプトは、PowerShell V3リモートセッションで実行されます。

  b. HCL は、Hyper-V マシンの管理者共有からディスクをメモリに読み込みます。

  c. HCL は、管理者共有からファイルを削除します。

マシンプロファイルを使用してカタログを作成する

マシンプロファイルを使用して、System Center Virtual Machine Manager (SCVMM)環境でMCSマシンカタログを作成および更新できます。また、ネストされた仮想化とvTPMを有効にすることもできます。

重要な考慮事項

- マスターイメージはスナップショットのみで、VM にすることはできません。
- マシンプロファイルのソースとして使用できるのは VM のみです。
- Hyper-V コンソールから VTPM を構成できますが、SCVMM コンソールからは構成できません。
- マスターイメージで vTPM が有効になっている場合は、マシンプロファイルソースで vTPM を有効にする必要があります。
- vTPM は第2世代のマシンでのみサポートされています。
- 次のパラメーターは、個別に指定された場合、マシンプロファイルでキャプチャされた値を上書きします。
  - VMCpuCount
  - VMMemoryMB
  - ディスクストレージ
- 既存のカタログは、`Set-ProvScheme`コマンドを使用して更新できます。

マシンプロファイルを使用してカタログを作成する手順

1. マシンプロファイルのソースとなるVMを作成します。詳しくは、「VMMファブリックでの仮想マシンのプロビジョニング」を参照してください。一度選択した**Generation**は変更できません。
   - ネストされた仮想化を有効にする場合は、**Select Source**ページで**Enable Nested Virtualization**チェックボックスをオンにします。
   - vTPMを有効にする場合は、VMを作成した後、Hyper-Vホストにログオンし、**Hyper-Vマネージャー**でVMを見つけます。VMを右クリックし、**Settings**に移動します。**Security**で、**Enable Trusted Platform Module**チェックボックスをオンにします。
2. **PowerShell**ウィンドウを開きます。
3. Citrix固有のPowerShellモジュールをロードするために`asnp citrix*`を実行します。
4. Brokerカタログを作成します。このカタログには、これから作成されるマシンが格納されます。
5. IDプールを作成します。これは、作成されるマシン用に作成されたADアカウントのコンテナになります。
6. マシンプロファイルを使用してプロビジョニングスキームを作成します。例：

```
New-ProvScheme -HostingUnitName "<hostingunit name>"

-IdentityPoolName "ID1" -MasterImageVM "XDHyp:\HostingUnits\HU1\<path
to the checkpoint/snapshot>"

-ProvisioningSchemeName "<catalogname>"  -MachineProfile "XDHyp:\<path
to the machine profile VM>"
```

7. プロビジョニングスキームの一意のIDでBrokerカタログを更新します。
8. カタログにVMを作成して追加します。

Set-ProvSchemeコマンドを使用して、既存のカタログを更新できます。例：

```
Set-ProvScheme -ProvisioningSchemeName "<catalogname>" -MachineProfile
"XDHyp:\<path to the machine profile VM>"
```

次のステップ

- これが最初に作成されたカタログである場合、Web Studio は デリバリーグループの作成 に誘導します
- 構成プロセス全体を確認するには、インストールと構成 を参照してください
- カタログを管理するには、マシンカタログの管理 および Microsoft System Center Virtual Machine Manager カタログの管理 を参照してください

詳細情報

- 接続とリソースの作成および管理
- マイクロソフト システムセンター バーチャルマシンマネージャー への接続
- マシンカタログの作成

Nutanixカタログを作成する

「(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/install-configure/machine-catalogs-create.html)」では、マシンカタログを作成するウィザードについて説明します。以下の情報は、Nutanix仮想化環境に固有の詳細を扱っています。

> **注：**
>
> Nutanixカタログを作成する前に、Nutanixへの接続の作成を完了する必要があります。「(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/install-configure/connections/connection-nutanix.html)」を参照してください。

Nutanixスナップショットを使用してマシンカタログを作成する

選択したスナップショットは、カタログ内のVMを作成するために使用されるテンプレートです。カタログを作成する前に、Nutanixでイメージとスナップショットを作成してください。詳細については、Nutanixのドキュメントを参照してください。

カタログ作成ウィザードで：

- **Operating System**ページと**Machine Management**ページには、Nutanix固有の情報は含まれていません。
- **Container**または**Cluster and Container**ページはNutanix固有のものです。

リソースとしてNutanix AHV XIを使用してマシンを展開する場合、**Container**ページが表示されます。VMのIDディスクが配置されるコンテナを選択します。

リソースとしてNutanix AHV Prism Central (PC) を使用してマシンを展開する場合、**Cluster and Container**ページが表示されます。VMの展開に使用するクラスターを選択し、次にコンテナを選択します。

- **Image**ページで、イメージスナップショットを選択します。Citrix Virtual Apps and Desktopsで使用するには、Acropolisスナップショット名に「XD_」というプレフィックスを付ける必要があります。必要に応じて、Acropolisコンソールを使用してスナップショットの名前を変更してください。スナップショットの名前を変更した場合は、カタログ作成ウィザードを再起動して、更新されたリストを表示してください。
- **Virtual Machines**ページで、仮想CPUの数とvCPUあたりのコア数を指定します。
- **Network Cards**ページで、NICの種類を選択して関連ネットワークをフィルター処理します。NICの種類は**VLAN**と**OVERLAY**の2つです。マスターイメージに含まれるNICを1つ以上選択し、各NICに関連付けられた仮想ネットワークを選択します。
- **Machine Identities**、**Domain Credentials**、**Scopes**、および**Summary**ページには、Nutanix固有の情報は含まれていません。

制限事項

Nutanixホスト接続（特にNutanix AHVプラグイン2.7.1）でMCSカタログを作成すると、プロビジョニングされたVMのハードディスクサイズがWeb Studioで誤って表示されます。表示されるサイズは実際のストレージサイズ（50 GB）よりもはるかに小さい（1 GB）です。ハードディスクサイズはNutanixコンソールで正しく表示されます。

次のステップ

- これが最初に作成されたカタログである場合、Web Studioはデリバリーグループの作成を案内します。
- 構成プロセス全体を確認するには、インストールと構成を参照してください。
- カタログを管理するには、「マシンカタログの管理」を参照してください。

詳細情報

- 接続とリソースの作成および管理
- Nutanixへの接続
- Nutanixクラウドおよびパートナーソリューションへの接続
- マシンカタログの作成

VMwareカタログを作成する

(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/install-configure/machine-catalogs-create.html)では、マシンカタログを作成するウィザードについて説明します。以下の情報では、VMware仮想化環境に固有の詳細について説明します。

注：

VMwareカタログを作成する前に、VMwareへの接続の作成を完了する必要があります。(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/install-configure/connections/connection-vmware-virtualization-environments.html)を参照してください。

マスターVMを作成する

マスターVMを使用して、マシンカタログでユーザーデスクトップとアプリケーションを提供します。ハイパーバイザーで、次の操作を行います。

1. マスターVMにVDAをインストールし、パフォーマンスを向上させるデスクトップの最適化オプションを選択します。
2. バックアップとして使用するために、マスターVMのスナップショットを作成します。

注：

MCSを使用して、vSAN 8.0環境でVMをプロビジョニングできます。

マシンプロファイルを使用してマシンカタログを作成する

マシンプロファイルを使用してMCSマシンカタログを作成できます。マシンプロファイルの入力元はVMwareテンプレートです。マシンプロファイルは、VMwareテンプレートからハードウェアプロパティを取得し、カタログ内の新しくプロビジョニングされたVMに適用します。

注：

- マスターイメージ入力（スナップショット）とマシンプロファイル入力（VMwareテンプレート）は、両方ともvTPMが有効であるか、両方ともvTPMが無効である必要があります。このルールは、`New-ProvScheme`と`Set-ProvScheme`の両方に適用されます。

- マスターイメージでvTPMが有効になっている場合、VMwareテンプレートはマスターイメージと同じVMソースからのみ取得できます。
- 暗号化されたストレージポリシーは、フルクローンのみをサポートします。
- マシンプロファイルベースのカタログは、提供されたVMwareテンプレートを利用してストレージコントローラー情報を収集し、接続されている仮想ディスクに依存します。テンプレートには、仮想マシンの仮想ディスクを構成するために使用されるストレージコントローラー情報を取得するために必要な仮想ディスクを含める必要があります。

マシンプロファイル内のVMwareテンプレートは、カタログへのVMのプロビジョニングを許可するために、カタログのライフサイクル中に存在する必要があります。VMwareテンプレートがないと、新しいVMをプロビジョニングできません。VMwareテンプレートが削除された場合は、`Set-ProvScheme`コマンドを使用して新しいテンプレートを提供する必要があります。

- MCSはVMwareテンプレートのプロパティをキャプチャします。Get-Provschemeコマンドを使用して、VMwareテンプレートの保存されたプロパティを参照する新しいVMwareテンプレートを作成できます。
- あるいは、マシンカタログとプロビジョニングされたVMが存在する場合、MCSでプロビジョニングされたマシンを使用して新しいVMwareテンプレートを作成することもできます。

異なるOSに基づいて、異なる構成でマシンカタログを作成できます。

- マスターイメージにWindows 11がインストールされている場合、マスターイメージでvTPMを有効にする必要があります。したがって、マシンプロファイルのソースであるVMwareテンプレートにはvTPMがアタッチされている必要があります。
- マスターイメージにvTPMがアタッチされていないWindows 10がインストールされている場合、非vTPM VMwareテンプレートをマシンプロファイルのソースとして使用してマシンカタログを作成できます。

暗号化されたストレージポリシーが適用されたマシンプロファイルテンプレートを使用して、フルコピーディスクモードでマシンカタログを作成できる別の構成があります。

- 「暗号化ストレージポリシー」は、マシンプロファイルテンプレートで設定する必要があります。マスターVMでは設定しないでください。
- フルコピー複製アプローチは、永続的なシングルセッションオペレーティングシステムのプロビジョニングにのみ利用可能です。

マシンプロファイルを入力としてPowerShellコマンドを使用してマシンカタログを作成するには：

1. **PowerShell**ウィンドウを開きます。
2. `asnp citrix*`を実行します。
3. 次のコマンドを実行します。

   - vTPMがアタッチされたVMwareテンプレートをマシンプロファイル入力のソースとして、Windows 11がインストールされたマスターイメージでマシンカタログを作成するには：

```
$identityPool = New-AcctIdentityPool  -IdentityPoolName "<string>"

-NamingScheme "<string>-###"

-NamingSchemeType Numeric

-Domain "<domain name"

-ZoneUid "<Uid>"  -Scope @()
```

```
$provScheme =New-ProvScheme  -CleanOnBoot

-HostingUnitName "vSanRg"

-IdentityPoolName "<string>"

-InitialBatchSizeHint 1

-MasterImageVM "XDHyp:\HostingUnits\<hosting unit name>\<snapshot
name>.snapshot"

-NetworkMapping @{"0"="XDHyp:\HostingUnits\<hosting unit name>\
\<network name>.network"}

-ProvisioningSchemeName "<string>"

-Scope @() -VMCpuCount 4

-VMMemoryMB 6144

-MachineProfile "XDHyp:\HostingUnits\<hosting unit name>\<template
```

```
name>.template" -TenancyType Shared

-FunctionalLevel "L7_20"
```

```
$catalog = New-BrokerCatalog

-AllocationType "Static"

-PersistUserChanges  "OnLocal"

-Description "<string>"

-IsRemotePC $False

-MinimumFunctionalLevel 'L7_9'

-Name "<catalog name>"

-ProvisioningType 'MCS'

-Scope @()

-SessionSupport "SingleSession" -ZoneUid "<Uid>"
```

```
Set-BrokerCatalog -Name "<string>"

-ProvisioningSchemeId $provScheme.ProvisioningSchemeUid.Guid
```

- 非vTPM VMwareテンプレートをマシンプロファイルのソースとして、Windows 10がインストールされたマスターイメージでマシンカタログを作成するには：

```
$identityPool = New-AcctIdentityPool

-IdentityPoolName "<string>"

-NamingScheme "<string>-###" -NamingSchemeType Numeric

-Domain "<domain name>"

-ZoneUid "<Uid>"  -Scope @()
```

```
$provScheme =New-ProvScheme

-CleanOnBoot -HostingUnitName "<string>"

-IdentityPoolName "<string>"

-InitialBatchSizeHint 1

-MasterImageVM "XDHyp:\HostingUnits\<hosting unit name>\<snapshot
name>.snapshot

-NetworkMapping @{"0"="XDHyp:\HostingUnits\<hosting unit name>\
\<string>.network"}

-ProvisioningSchemeName "<string>"  -Scope @() -VMCpuCount 4  -
VMMemoryMB 8192

-MachineProfile "XDHyp:\HostingUnits\<hosting unit name>\<template
name>.template"

-TenancyType Shared  -FunctionalLevel "L7_20"
```

```
$catalog = New-BrokerCatalog

-AllocationType "Static"

-PersistUserChanges  "OnLocal"

-Description "<string>"

-IsRemotePC $False

-MinimumFunctionalLevel 'L7_9' -Name "<string>" -ProvisioningType
'MCS' -Scope @()

-SessionSupport "SingleSession" -ZoneUid "<Uid"
```

```
Set-BrokerCatalog -Name "<string>"

-ProvisioningSchemeId $provScheme.ProvisioningSchemeUid.Guid
```

- 暗号化されたストレージポリシーが適用されたマシンプロファイルテンプレートを使用して、フルコピーディスクモードでマシンカタログを作成するには：

```
$identityPool = New-AcctIdentityPool

-IdentityPoolName "<string>"

-NamingScheme "<string>-###"

-NamingSchemeType Numeric

-Domain "<domain name>"

-ZoneUid "<Uid>"  -Scope @()
```

```
$provScheme =New-ProvScheme

-HostingUnitName "<string>"

-IdentityPoolName "<string>"

-InitialBatchSizeHint 1

-MasterImageVM "XDHyp:\HostingUnits\<hosting unit name>\<snapshot
name>.snapshot"

-NetworkMapping @{"0"="XDHyp:\HostingUnits\<hosting unit name>\
\<string>.network"}

-ProvisioningSchemeName "<string>"

-Scope @() -VMCpuCount 4  -VMMemoryMB 8192 -MachineProfile "XDHyp:
\HostingUnits\<hosting unit name>\<template name>.template"

-TenancyType Shared

-FunctionalLevel "L7_20" -UseFullDiskCloneProvisioning
```

```
$catalog = New-BrokerCatalog

-AllocationType "Static"
```

```
-PersistUserChanges  "OnLocal"

-Description "<string>"  -IsRemotePC $False

-MinimumFunctionalLevel 'L7_9'

-Name "<string>" -ProvisioningType 'MCS' -Scope @()

-SessionSupport "SingleSession" -ZoneUid "<Uid>"
```

```
Set-BrokerCatalog -Name "<string>"

-ProvisioningSchemeId $provScheme.ProvisioningSchemeUid.Guid
```

マシンプロファイルを更新するには、Set-ProvSchemeコマンドを使用します。例：

```
Set-ProvScheme -ProvisioningSchemeName 'name' -IdentityPoolName 'name'
-MachineProfile 'XDHyp:\HostingUnits\<hosting unit name>\<template
name>.template'
```

複数のNICの確認

マシンプロファイルを使用し、`New-ProvScheme`および`Set-ProvScheme`コマンドで`NetworkMapping`パラメーターを使用する場合、複数のNICの事前チェック中にさまざまなエラーメッセージが表示されます。

複数のNICの事前チェックリストは次のとおりです。

- マシンプロファイルテンプレートからのNIC数のみが使用され、検証されます。これらのNICが指すネットワークは、ホスティングユニットネットワークに対して使用または検証されません。
- マシンプロファイルテンプレートのNIC数がホスティングユニットのネットワーク数よりも多い場合、エラーメッセージが表示されます。
- マシンプロファイルテンプレートのNIC数がゼロの場合、エラーメッセージが表示されます。マシンプロファイルテンプレートのNIC数が1の場合：
  - `New-ProvScheme`または`Set-ProvScheme`コマンドでネットワークマッピングが指定されておらず、ホスティングユニットネットワークが1つの場合、そのホスティングユニットネットワークが使用されます。

    - ネットワークマッピングが指定されている場合、それが有効であれば、指定されたネットワークマッピングが使用されます。

- マシンプロファイルテンプレートのNIC数が1より大きい場合、またはホスティングユニットネットワーク数が1より大きい場合：

    - コマンドでは有効なネットワークマッピングが必要であり、各NICのマッピングを提供する必要があります（つまり、NetworkMappingの数はマシンプロファイルのNIC数と同じである必要があります）。
    - ホスティングユニット内で複数のNICを同じネットワークにマッピングすることはできません。
    - `NetworkMapping`数とマシンプロファイルのNIC数は、ホスティングユニットネットワーク数以下である必要があります。
    - `NetworkMapping`は、0からn-1までの各IDに対して提供する必要があります。ここでnは、マシンプロファイルテンプレート内のネットワークアダプターの数です。

トラブルシューティング

カタログの作成に失敗した場合は、CTX294978を参照してください。

次のステップ

- これが最初に作成されたカタログである場合、Web Studioはデリバリーグループの作成を案内します。
- 構成プロセス全体を確認するには、「」(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/install-configure.html)を参照してください。
- カタログを管理するには、マシンカタログの管理およびVMwareカタログの管理を参照してください。

詳細情報

- 接続とリソースの作成および管理
- VMwareへの接続
- マシンカタログの作成

異なるマシンID結合タイプのIDプール

MCSを使用すると、オンプレミスAD参加、Microsoft Entraハイブリッド、またはドメイン非参加のマシンをプロビジョニングできます。

Web Studioでマシンを構成する方法については、マシンカタログの作成を参照してください。

マシンIDが結合されたカタログを作成する方法に関する具体的な情報については、以下を参照してください。

- Microsoft Entraハイブリッド参加済みマシンIDのIDプール
- ドメインに参加していないマシンIDのIDプール

Microsoft Entra ハイブリッド参加済みマシンIDのIDプール

この記事では、Microsoft Entra ハイブリッド参加済みカタログを作成する方法について説明します。

要件、制限、および考慮事項については、「Microsoft Entra ハイブリッド参加済み」を参照してください。

Web Studio を使用する

以下の情報は、マシンカタログの作成 のガイダンスを補足するものです。ハイブリッド Azure AD 参加済みカタログを作成するには、その記事の一般的なガイダンスに従い、ハイブリッド Azure AD 参加済みカタログに固有の詳細に注意してください。

カタログ作成ウィザードで：

- 「**マシンID**」ページで、「**Microsoft Entra ハイブリッド参加済み**」を選択します。作成されたマシンは組織が所有し、その組織に属するActive Directory Domain Servicesアカウントでサインインします。これらはクラウドとオンプレミスの両方に存在します。

> **注:**
>
> IDの種類として **Microsoft Entra ハイブリッド参加済み** を選択した場合、カタログ内の各マシンには対応するADコンピューターアカウントが必要です。

PowerShell を使用する

以下は、Web Studio での操作に相当する PowerShell の手順です。Remote PowerShell SDK を使用してカタログを作成する方法については、`<https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/>` を参照してください。

オンプレミスのAD参加済みカタログとMicrosoft Entraハイブリッド参加済みカタログの違いは、IDプールとマシンアカウントの作成にあります。

Microsoft Entra ハイブリッド参加済みカタログのアカウントとともにIDプールを作成するには：

```
New-AcctIdentityPool -AllowUnicode -IdentityType "HybridAzureAD" -Domain
"corp.local" -IdentityPoolName "HybridAADJoinedCatalog" -NamingScheme
"HybridAAD-VM-##" -NamingSchemeType "Numeric" -OU
"CN=AADComputers,DC=corp,DC=local" -Scope @() -ZoneUid "81291221-
d2f2-49d2-ab12-bae5bbd0df05"

New-AcctADAccount -IdentityPoolName "HybridAADJoinedCatalog" -Count 10
-ADUserName "corp\admin1" -ADPassword $password

Set-AcctAdAccountUserCert -IdentityPoolName "HybridAADJoinedCatalog" -All
-ADUserName "corp\admin1" -ADPassword $password
```

注:

`$password` は、書き込み権限を持つADユーザーアカウントの一致するパスワードです。

Microsoft Entra ハイブリッド参加済みカタログを作成するために使用される他のすべてのコマンドは、従来のオンプレミスAD参加済みカタログの場合と同じです。

Microsoft Entra ハイブリッド参加プロセスのステータスを表示する

Web Studio では、デリバリーグループ内の Microsoft Entra ハイブリッド参加済みマシンが電源オン状態の場合に、Microsoft Entra ハイブリッド参加プロセスのステータスが表示されます。ステータスを表示するには、検索 を使用してそれらのマシンを特定し、下部ペインの **詳細** タブで各マシンの **マシンID** を確認します。**マシンID** には次の情報が表示されます。

- Microsoft Entraハイブリッド参加済み
- Azure AD にまだ参加していません

注：

- マシンが最初に電源オンになったときに、Microsoft Entra ハイブリッド参加が遅延する場合があります。これは、デフォルトのマシンID同期間隔（Microsoft Entra Connect の30分）が原因です。マシンは、Microsoft Entra Connect を介してマシンIDが Microsoft Entra ID に同期された後にのみ、Microsoft Entra ハイブリッド参加状態になります。
- マシンがMicrosoft Entraハイブリッド参加状態にならなかった場合、それらはデリバリーコントローラーに登録されません。登録ステータスは**初期化中**と表示されます。

また、Web Studio を使用して、マシンが利用できない理由を確認できます。これを行うには、**検索** ノードでマシンをクリックし、下部ペインの **詳細** タブで **登録** を確認し、ツールチップを読んで追加情報を確認します。

トラブルシューティング

マシンがMicrosoft Entraハイブリッド参加に失敗した場合は、次の操作を行います。

- マシンアカウントが Microsoft Entra ID ポータルを通じて Microsoft Entra ID に同期されているか確認します。同期されている場合、**Azure AD にまだ参加していません** と表示され、登録が保留中であることを示します。

  マシンアカウントをMicrosoft Entra IDに同期するには、以下を確認してください。

  - マシンアカウントが、Microsoft Entra IDと同期するように構成されているOU内にあること。**userCertificate**属性を持たないマシンアカウントは、同期するように構成されているOU内にあってもMicrosoft Entra IDに同期されません。
  - **userCertificate**属性がマシンアカウントに設定されていること。属性を表示するには、Active Directory Explorerを使用します。
  - マシンアカウントが作成された後、Microsoft Entra Connectが少なくとも1回同期されている必要があります。同期されていない場合は、Microsoft Entra ConnectマシンのPowerShellコンソールで`Start-ADSyncSyncCycle -PolicyType Delta`コマンドを手動で実行して、即時同期をトリガーします。

- Microsoft Entra ハイブリッド参加済み用の Citrix 管理デバイスキーペアがマシンに正しくプッシュされているか、**HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix** の下の **DeviceKeyPairRestored** の値をクエリして確認します。

  値が1であることを確認します。そうでない場合、考えられる理由は次のとおりです。

  - プロビジョニングスキームに関連付けられたIDプールの`IdentityType`が`HybridAzureAD`に設定されていません。これは`Get-AcctIdentityPool`を実行して確認できます。
  - マシンがマシンカタログと同じプロビジョニングスキームを使用してプロビジョニングされていません。
  - マシンがローカルドメインに参加していません。ローカルドメイン参加は、Microsoft Entra ハイブリッド参加の前提条件です。

- MCSでプロビジョニングされたマシンで`dsregcmd /status /debug`コマンドを実行して、診断メッセージを確認します。
  - Microsoft Entra ハイブリッド参加が成功した場合、コマンドラインの出力で **AzureAdJoined** と **DomainJoined** が **YES** になります。
  - そうでない場合、問題をトラブルシューティングするにはMicrosoftのドキュメントを参照してください: `<https://docs.microsoft.com/ja-jp/azure/active-directory/devices/troubleshoot-hybrid-join-windows-current>`。
  - エラーメッセージ「**Server Message: The user certificate is not found on the device with id: xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx**」が表示された場合は、ユーザー証明書を修復するために次のPowerShellコマンドを実行します。

    ```
    Repair-AcctIdentity -IdentityAccountName TEST\VM1 -Target
    UserCertificate
    ```

    ユーザー証明書の問題の詳細については、CTX566696を参照してください。

ドメインに参加していないカタログを作成する

この記事では、Citrix Virtual Apps and Desktops を使用して、ドメインに参加していないカタログを作成する方法について説明します。

要件、制限、および考慮事項については、ドメインに参加していないを参照してください。

マシンカタログを作成する前に、次のものが必要です。

1. 新しいリソースの場所
   - Citrix Cloud™ 管理 UI > 左上のハンバーガーメニュー > **リソースの場所** に移動します。
   - **+ リソースの場所** をクリックします。
   - 新しいリソースの場所の名前を入力し、**保存** をクリックします。

2. ホスティング接続を作成します。詳細については、接続の作成と管理セクションを参照してください。

Citrix Virtual Apps and Desktops を使用すると、ワークグループまたはドメインに参加していないマシンに基づいてカタログを作成できます。ドメインに参加していないマシンの作成は、アカウントIDプールがどのように作成されるかによって異なります。アカウントIDプールは、カタログプロビジョニング中に MCS がマシン名を作成および追跡するために使用するメカニズムです。

現在、ドメインに参加していないカタログは、PowerShell コマンドを使用してのみ作成できます。

PowerShell を使用する

Remote PowerShell SDK を使用して、ドメインに参加していないカタログのIDプールを作成できます。

PowerShell パラメーターの **WorkgroupMachine** と **IdentityType** を使用して、ドメインに参加していないカタログのIDプールを作成します。これらのパラメーターにより、ドメイン管理者資格情報を含むすべての AD 固有のパラメーターを指定する必要がなくなります。

```
New-AcctIdentityPool -AllowUnicode -IdentityType "Workgroup"
-WorkgroupMachine -IdentityPoolName "NonDomainJoinedCatalog" -NamingScheme
"NDJ-VM-##" -NamingSchemeType "Numeric" -Scope @() -ZoneUid "81291221-
d2f2-49d2-ab12-bae5bbd0df05"
```

ドメインに参加していないカタログを作成するために使用されるその他のすべてのコマンドは、従来のオンプレミス Active Directory に参加しているカタログの場合と同じです。

マシンカタログを管理する

注：

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

はじめに

マシンカタログへのマシンの追加または削除、名前の変更、説明の変更、またはカタログのActive Directoryコンピューターアカウントの管理を行うことができます。

カタログの保守には、各マシンが最新のOSアップデートを適用していることを確認することも含まれます。これには、ウイルス対策の更新、オペレーティングシステムのアップグレード、または構成の変更が含まれます。

- Machine Creation Services™ (MCS) を使用して作成されたプールされたランダムマシンを含むカタログは、カタログで使用されるマスターイメージを更新し、その後マシンを更新することでマシンを保守します。この方法により、多数のユーザーマシンを効率的に更新できます。
- 静的で永続的に割り当てられたマシンを含むカタログ、およびリモートPCアクセス マシンカタログの場合、ユーザーのマシンへの更新はWeb Studioの外部で管理します。このタスクは、個別に、またはサードパーティのソフトウェア配布ツールを使用してまとめて実行します。

ホストハイパーバイザーへの接続の作成と管理については、「接続とリソース」を参照してください。

> **注：**
>
> MCSはWindows 10 IoT CoreおよびWindows 10 IoT Enterpriseをサポートしていません。詳細については、Microsoftサイトを参照してください。

永続インスタンスについて

永続的または専用インスタンスを使用して作成されたMCSカタログを更新する場合、カタログ用に作成された新しいマシンはすべて更新されたイメージを使用します。既存のインスタンスは引き続き元のインスタンスを使用します。イメージの更新プロセスは、他の種類のカタログと同じ方法で行われます。以下を考慮してください。

- 永続ディスクカタログの場合、既存のマシンは新しいイメージに更新されませんが、カタログに追加される新しいマシンは新しいイメージを使用します。
- 非永続ディスクカタログの場合、マシンイメージはマシンがリセットされる次回のタイミングで更新されます。
- 永続マシンカタログの場合、イメージを更新すると、それを使用するカタログインスタンスも更新されます。
- 永続化しないカタログの場合、異なるマシンに異なるイメージを使用したい場合は、イメージは別々のカタログに存在する必要があります。

マシンカタログを管理する

マシンカタログは、次の2つの方法で管理できます。

- Web Studioの使用
- PowerShellを使用する

Web Studioを使用する

このセクションでは、Web Studioを使用してカタログを管理する方法について詳しく説明します。

- カタログの詳細を表示する
- カタログにマシンを追加する
- カタログからマシンを削除する
- カタログを編集する
- カタログの名前を変更する
- カタログを別のゾーンに移動する
- カタログを削除する
- カタログ内のActive Directoryコンピューターアカウントを管理する
- カタログを更新する
- 機能レベルを変更する、または変更を元に戻す(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/install-configure/machine-catalogs-manage.html#change-the-functional-level-or-undo-the-change)
- カタログをクローンする(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/install-configure/machine-catalogs-manage.html#clone-a-catalog)
- フォルダーを使用してカタログを整理する(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/install-configure/machine-catalogs-manage.html#organize-catalogs-using-folders)

カタログの詳細を表示

1. 検索機能を使用して特定のマシンカタログを見つけます。手順については、インスタンスの検索を参照してください。
2. 検索結果から、必要に応じてカタログを選択します。
3. カタログ列の説明については、次の表を参照してください。

4. このカタログに関する詳細情報については、下部の詳細ペインにあるタブをクリックしてください。

列	説明	
マシンカタログ	カタログの名前と割り当ての種類。割り当ての種類は次のとおりです。 • ランダム: カタログ内のマシンはユーザーにランダムに割り当てられます。 • 永続: カタログ内のマシンはユーザーに永続的に割り当てられます。	
マシンタイプ	カタログ内のマシンでサポートされているセッションの種類。指定できる値は次のとおりです。 • OSの種類: マルチセッションOS (仮想); ユーザーデータ: 破棄。 • OSの種類: マルチセッションOS (仮想); ユーザーデータ: ローカルディスク上 • OSの種類: シングルセッションOS (リモートPCアクセス) • OSの種類: シングルセッションOS (仮想); ユーザーデータ: 破棄	

列	説明
	• OSの種類: シングルセッションOS (仮想); ユーザーデータ: ローカルディスク上
マシン数	カタログ内のマシンの数とプロビジョニング方法。指定できるプロビジョニング方法には、Machine Creation Services (MCSマシン)、手動、Citrix Provisioning™ Services があります。
割り当て済み数	デリバリーグループに割り当てられているカタログ内のマシンの数。
フォルダ	**マシンカタログ**ツリー内のカタログの場所。カタログが存在するフォルダーの名前（末尾のバックスラッシュを含む）が表示されます。カタログがルートレベルにある場合は `-` が表示されます。
VDAアップグレード	VDAアップグレードの状態。可能な値は、未構成、スケジュール済み、利用可能、および最新です。
イメージステータス	カタログのイメージ更新ステータス。非永続マシンカタログにのみ適用されます。指定できる値は、完全に更新済み、部分的に更新済み、更新保留中、準備中です。

マシンをカタログに追加する

開始する前に:

- 仮想化ホストに、追加のマシンを収容するのに十分なプロセッサ、メモリ、ストレージがあることを確認してください。
- 未使用のActive Directoryコンピューターアカウントが十分にあることを確認してください。既存のアカウントを使用している場合、追加できるマシンの数は利用可能なアカウントの数によって制限されます。
- Web Studioを使用して追加のマシン用のActive Directoryコンピューターアカウントを作成する場合、適切なドメイン管理者権限が必要です。

カタログにマシンを追加するには:

1. Web Studioにサインインします。
2. 左側のペインで**Machine Catalogs**を選択します。
3. マシンカタログを選択し、アクションバーで**マシンの追加**を選択します。
4. 追加する仮想マシンの数を選択します。
5. 追加するVMの数に対して既存のActive Directoryアカウントが不足している場合は、アカウントが作成されるドメインと場所を選択します。連続する数字または文字が表示される場所を示すには、ハッシュマークを使用してアカウントの命名スキームを指定します。OU名にスラッシュ（/）を使用しないでください。名前は数字で始めることはできません。たとえば、PC-Sales-##（0-9を選択）という命名スキームでは、PC-Sales-01、PC-Sales-02、PC-Sales-03などのコンピューターアカウントが作成されます。
6. 既存のActive Directoryアカウントを使用する場合は、アカウントを参照するか、**インポート**をクリックしてアカウント名を含む.csvファイルを指定します。追加するすべてのマシンに対して十分なアカウントがあることを確認してください。Web Studioはこれらのアカウントを管理します。Web Studioがすべてのアカウントのパスワードをリセットすることを許可するか、すべてのアカウントで同じである必要があるアカウントパスワードを指定します。

マシンはバックグラウンドプロセスとして作成され、多数のマシンを作成する場合は時間がかかることがあります。Web Studioを閉じてもマシンの作成は続行されます。

カタログからマシンを削除する

マシンカタログからマシンを削除すると、ユーザーはそのマシンにアクセスできなくなるため、マシンを削除する前に、以下を確認してください。

- ユーザーデータがバックアップされているか、不要になっていること。
- すべてのユーザーがログオフしていること。メンテナンスモードをオンにすると、マシンへの新しい接続が停止します。
- マシンが電源オフになっていること。

カタログからマシンを削除するには：

1. Web Studioにサインインします。
2. 左側のペインで**Machine Catalogs**を選択します。
3. カタログを選択し、アクションバーで**マシンを表示**を選択します。
4. 1つ以上のマシンを選択し、アクションバーで**削除**を選択します。

削除するマシンを削除するかどうかを選択します。マシンを削除することを選択した場合、それらのマシンのActive Directoryアカウントを保持するか、無効にするか、削除するかを指定します。

カタログを編集する

1. **説明**ページで、カタログの説明を変更します。
2. 左側のペインで**Machine Catalogs**を選択します。
3. カタログを選択し、アクションバーで**マシンカタログの編集**を選択します。
4. **スコープ**ページで、スコープを変更します。
5. カタログの種類によっては、他のページが表示される場合があります。

   Azure Resource Managerイメージを使用して作成されたカタログの場合、次のページが表示されます。行った変更は、後でカタログに追加するマシンにのみ適用されることに注意してください。既存のマシンは変更されません。

   - **Virtual Machines**ページで、マシンを作成するマシンサイズと可用性ゾーンを変更します。

     > **注：**
     >
     > - カタログがサポートするマシンサイズのみが表示されます。
     > - 必要に応じて、**Show only machine sizes used in other machine catalogs**を選択して、マシンサイズリストをフィルターします。

   - **Machine Profile**ページで、マシンプロファイルを使用するか変更するかを選択します。
   - （カタログが専用グループホストで構成されている場合にのみ表示）**専用ホストグループ**ページで、ホストグループを変更するかどうかを選択します。

- **ストレージとライセンスの種類**ページで、ストレージの種類、ライセンスの種類、およびAzure Computer Galleryの設定を変更するかどうかを選択します（**準備されたイメージをAzure Galleryに配置**が使用されている場合にのみ利用可能）。

> **注：**
>
> 新しく選択した設定が現在のマシンサイズをサポートしていない場合、設定を変更するとマシンサイズの設定がリセットされることを通知する警告ダイアログボックスが表示されます。続行することを選択すると、**仮想マシン**メニューの横に赤い点が表示され、新しいマシンサイズを選択するように促されます。

- **ライセンスの種類**ページで、WindowsライセンスまたはLinuxライセンスの設定を変更するかどうかを選択します。

Remote PC Accessカタログの場合、以下のページが表示されます。

- **電源管理**ページで、電源管理設定を変更し、電源管理接続を選択します。
- **組織単位**ページで、Active Directory OUを追加または削除します。

6. 行った変更を適用するには**適用**をクリックし、終了するには**保存**をクリックします。

カタログの名前を変更する

1. Web Studioにサインインします。
2. 左側のペインで**Machine Catalogs**を選択します。
3. カタログを選択し、アクションバーで**マシンカタログの名前を変更**を選択します。
4. 新しい名前を入力します。

カタログを別のゾーンに移動する

展開に複数のゾーンがある場合、カタログをあるゾーンから別のゾーンに移動できます。

カタログ内のVMを含むハイパーバイザーとは異なるゾーンにカタログを移動すると、パフォーマンスに影響します。

1. Web Studioにサインインします。
2. 左側のペインで**Machine Catalogs**を選択します。
3. カタログを選択し、アクションバーで**移動**を選択します。

4. カタログを移動するゾーンを選択します。

カタログを削除する

カタログを削除する前に、以下を確認してください。

- すべてのユーザーがログオフしており、切断されたセッションは実行されていません。
- カタログ内のすべてのマシンでメンテナンスモードがオンになっており、新しい接続が確立できないこと。
- カタログ内のすべてのマシンが電源オフになっていること。
- カタログはデリバリーグループに関連付けられていません。つまり、デリバリーグループにはそのカタログのマシンが含まれていません。

カタログを削除するには：

1. Web Studioにサインインします。
2. 左側のペインで**Machine Catalogs**を選択します。
3. カタログを選択し、アクションバーで**マシンカタログの削除**を選択します。
4. カタログ内のマシンを削除するかどうかを指定します。マシンを削除することを選択した場合、それらのマシンのActive Directoryコンピューターアカウントを保持するか、無効にするか、削除するかを指定します。

カタログ内のActive Directoryコンピューターアカウントを管理する

マシンカタログ内のActive Directoryアカウントを管理するには、次の操作を実行できます。

- シングルセッションOSおよびマルチセッションOSカタログからActive Directoryコンピューターアカウントを削除して、未使用のマシンアカウントを解放します。これらのアカウントは、他のマシンに使用できます。
- カタログにマシンが追加されたときにコンピューターアカウントがすでに存在するように、アカウントを追加します。OU名にスラッシュ（/）を使用しないでください。

Active Directoryアカウントを管理するには：

1. Web Studioにサインインします。
2. 左側のペインで**Machine Catalogs**を選択します。
3. カタログを選択し、アクションバーで**Manage AD accounts**を選択します。

4. コンピューターアカウントを追加するか削除するかを選択します。アカウントを追加する場合は、アカウントのパスワードをどうするかを指定します。すべてリセットするか、すべてのアカウントに適用されるパスワードを入力します。

   現在のアカウントパスワードが不明な場合は、パスワードをリセットできます。パスワードリセットを実行する権限が必要です。パスワードを入力すると、インポート時にアカウントのパスワードが変更されます。アカウントを削除する際は、Active Directory内のアカウントを保持するか、無効にするか、削除するかを選択します。

カタログからマシンを削除したり、カタログを削除したりする際に、Active Directoryアカウントを保持するか、無効にするか、削除するかを指定します。

カタログを更新する

カタログ内のマシンを更新する前に、マスターイメージのコピーまたはスナップショットを保存することをお勧めします。データベースは、各マシンカタログで使用されたマスターイメージの履歴レコードを保持します。カタログ内のマシンをロールバックまたは元に戻して、マスターイメージの以前のバージョンを使用します。ユーザーがデスクトップに展開した更新プログラムで問題が発生した場合に、このタスクを実行します。これにより、ユーザーのダウンタイムが最小限に抑えられます。マスターイメージを削除、移動、または名前変更しないでください。それらを使用してカタログを元に戻すことはできません。

マシンが更新されると、自動的に再起動します。

マスターイメージを更新または作成する

マシンカタログを更新する前に、既存のマスターイメージを更新するか、ホストハイパーバイザー上に新しいマスターイメージを作成します。

1. ハイパーバイザーで、現在のVMのスナップショットを取得し、そのスナップショットに意味のある名前を付けます。このスナップショットは、必要に応じてカタログ内のマシンを元に戻す（ロールバックする）ために使用できます。
2. 必要に応じて、マスターイメージの電源をオンにし、ログオンします。
3. 更新プログラムをインストールするか、マスターイメージに必要な変更を加えます。
4. VMの電源をオフにします。
5. VMのスナップショットを取得します。Web Studioでカタログが更新されたときに認識されるような、意味のある名前を付けます。Web Studioでスナップショットを作成することもできますが、Citrixではハイパーバイザー管理コンソールを使用して作成することをお勧めします。その後、Web Studioでそのスナップショットを選択します。このプロセスにより、自動生成され

た名前ではなく、意味のある名前と説明を提供できます。GPUマスターイメージの場合、マスターイメージはXenServer®コンソールからのみ変更できます。

マスターイメージを変更する

カタログ内のすべてのマシンに更新プログラムを準備して展開するには：

1. Web Studioにサインインします。
2. 左側のペインで**Machine Catalogs**を選択します。
3. カタログを選択し、アクションバーで **［マスターイメージの変更］** を選択します。
4. **［イメージ］** ページで、展開するホストとイメージを選択します。

> **ヒント:**
>
> MCSで作成されたカタログの場合、イメージにメモを追加して注釈を付けることができます。メモには最大500文字を含めることができます。マスターイメージを変更するたびに、メモを追加したかどうかにかかわらず、メモ関連のエントリが作成されます。メモを追加せずにカタログを更新した場合、エントリはnull (-) として表示されます。イメージのメモ履歴を表示するには、カタログを選択し、下部ペインで **［テンプレートプロパティ］** をクリックし、 **［メモ履歴の表示］** をクリックします。

5. 「**展開戦略**」ページで、マシンカタログ内のマシンを新しいマスターイメージで更新するタイミング（次回のシャットダウン時または即時）を選択します。

> **注：**
>
> **［ロールアウト戦略］** ページは永続VMでは利用できません。ロールアウトは非永続VMにのみ適用されるためです。

6. 「**概要**」ページで情報を確認し、「**完了**」をクリックします。各マシンは更新後に自動的に再起動します。

更新の進行状況を追跡するには、「**マシンカタログ**」でカタログを見つけ、インラインの進行状況バーと段階的な進行状況グラフを表示します。

Web StudioではなくPowerShell SDKを直接使用してカタログを更新する場合は、ハイパーバイザーテンプレート（**VMTemplates**）を指定します。これは、イメージまたはイメージのスナップショットの代替として使用します。

展開戦略：

次回のシャットダウン時にイメージを更新すると、現在使用されていないマシン、つまりアクティブなユーザーセッションがないマシンにすぐに影響します。使用中のシステムは、現在のアクティブセッションが終了したときに更新を受け取ります。以下を考慮してください。

- 該当するマシンでの更新が完了するまで、新しいセッションを起動することはできません。
- シングルセッションOSマシンでは、マシンが使用されていないとき、またはユーザーがログオンしていないときに、マシンはすぐに更新されます。
- 子マシンを持つマルチセッションOSの場合、再起動は自動的に行われません。更新されたマスターイメージを適用するには、Studio、PowerShell、またはWorkspaceを使用してマシンを再起動します。マシンまたはハイパーバイザーからの再起動では、更新は適用されません。

> **ヒント:**
>
> ホスト接続の詳細設定を使用して、再起動されるマシンの数を制限します。これらの設定を使用して、特定のカタログに対して実行されるアクションを変更します。詳細設定はハイパーバイザーによって異なります。

マスターイメージをロールバックする

更新された、または新しいマスターイメージを展開した後、それをロールバックできます。このプロセスは、新しく更新されたマシンで問題が発生した場合に必要になることがあります。ロールバックすると、カタログ内のマシンは最後に正常に動作したイメージにロールバックされます。新しいイメージを必要とする新機能は利用できなくなります。展開と同様に、マシンのロールバックには再起動が含まれます。

1. Web Studioにサインインします。
2. 左側のペインで**Machine Catalogs**を選択します。
3. カタログを選択し、アクションバーで を選択します。
4. 展開操作の前のセクションで説明されているように、以前のマスターイメージをマシンに適用するタイミングを指定します。

ロールバックは、元に戻す必要があるマシンにのみ適用されます。新しいまたは更新されたマスターイメージで更新されていないマシンは、通知メッセージを受信せず、強制的にログオフされることもありません。

ロールバックの進行状況を追跡するには、 でカタログを見つけて、インラインの進行状況バーと段階的な進行状況グラフを表示します。

機能レベルを変更または変更を元に戻す

マシンのVDAを新しいバージョンにアップグレードした後、マシンカタログの機能レベルを変更します。Citrixは、すべての最新機能にアクセスできるように、すべてのVDAを最新バージョンにアップグレードすることを推奨します。

マシンカタログの機能レベルを変更する前に、次の点に注意してください。

- アップグレードされたマシンを起動して、Controllerに登録させます。このプロセスにより、Web Studioはカタログ内のマシンがアップグレードを必要としていることを判断できます。

カタログの機能レベルを変更するには：

1. Web Studioにサインインします。
2. 左側のペインで**Machine Catalogs**を選択します。
3. カタログを選択します。下ペインの**「詳細」**タブにバージョン情報が表示されます。
4. **機能レベルの変更**を選択します。Web Studioがカタログのアップグレードが必要であると検出した場合、メッセージが表示されます。プロンプトに従ってください。1台以上のマシンをアップグレードできない場合、その理由を説明するメッセージが表示されます。すべてのマシンが適切に機能するように、Citrixは**変更**をクリックして続行する前に、マシンの問題を解決することを推奨します。

カタログの変更が完了した後、カタログを選択し、アクションバーで**機能レベルの変更を元に戻す**を選択することで、マシンを以前のVDAバージョンに戻すことができます。

カタログを複製する

カタログを複製する前に、次の考慮事項に注意してください。

- オペレーティングシステムおよびマシン管理に関連する設定は変更できません。複製されたカタログは、元のカタログからこれらの設定を継承します。
- カタログの複製には時間がかかる場合があります。必要に応じて、**「進行状況を非表示」**を選択して、バックグラウンドで複製を実行します。

- クローンされたカタログは元の名前を継承し、サフィックス `Copy` を持ちます。名前は変更できます。「カタログの名前を変更する」を参照してください。
- クローン作成が完了したら、クローンされたカタログをデリバリーグループに割り当てるようにしてください。

1. Web Studioにサインインし、左側のペインで**マシンカタログ**を選択します。
2. カタログを選択し、アクションバーで を選択します。
3. ウィンドウで、クローンされたカタログの設定を表示し、必要に応じて設定を構成します。 を選択して次のページに進みます。
4. ページで、設定の概要を表示し、 を選択してクローン作成を開始します。
5. 必要に応じて、 を選択して、バックグラウンドでクローン作成を実行します。

フォルダーを使用してカタログを整理する

フォルダーを作成してカタログを整理し、簡単にアクセスできるようにすることができます。たとえば、イメージの種類別または組織構造別にカタログを整理できます。

カタログフォルダーを作成する

開始する前に、まずカタログの整理方法を計画してください。次の点を考慮してください。

- フォルダーは最大5レベルまでネストできます（デフォルトのルートフォルダーを除く）。
- カタログフォルダーには、カタログとサブフォルダーを含めることができます。
- Web Studioのすべてのノード（**マシンカタログ**、**デリバリーグループ**、**アプリケーション**、**アプリケーショングループ**など）は、バックエンドで同じフォルダーツリーを共有します。フォルダーの名前変更や移動の際に名前の競合を避けるため、異なるノード間で最上位フォルダーには一意の名前を使用してください。

  `New-BrokerAdminFolder` SDKコマンドレットを使用してフォルダーを作成し、それを**マシンカタログ**ノードの下に表示させたい場合は、`Set-BrokerAdminFolderMetadata` コマンドレットを使用して `ContainsMachineCatalogs` メタデータを追加する必要があります。

  例:

  ```
  Set-BrokerAdminFolderMetadata -AdminFolderId {adminFolderUid} -Name
  ContainsMachineCatalogs -Value true
  ```

カタログフォルダーを作成するには、次の手順に従います。

1. 左側のペインで**Machine Catalogs**を選択します。
2. フォルダー階層でフォルダーを選択し、**アクション**バーで**フォルダーの作成**を選択します。
3. 新しいフォルダーの名前を入力し、**完了**をクリックします。

> **ヒント:**
>
> 意図しない場所にフォルダーを作成した場合でも、正しい場所にドラッグして移動できます。

カタログを移動する

カタログはフォルダー間で移動できます。詳細な手順は次のとおりです。

1. 左側のペインで**Machine Catalogs**を選択します。
2. フォルダー別にカタログを表示します。フォルダー階層の上にある**すべて表示**をオンにすると、すべてのカタログを一度に表示することもできます。
3. カタログを右クリックし、**マシンカタログの移動**を選択します。
4. カタログの移動先のフォルダーを選択し、**完了**をクリックします。

> **ヒント:**
>
> カタログをフォルダーにドラッグできます。

カタログフォルダーの管理

カタログフォルダーの削除、名前の変更、移動ができます。

フォルダーとそのサブフォルダーにカタログが含まれていない場合にのみ、フォルダーを削除できます。

フォルダーを管理するには、以下の手順に従います。

1. 左側のペインで**Machine Catalogs**を選択します。
2. フォルダー階層でフォルダーを選択し、必要に応じて**アクション**バーでアクションを選択します。
    - フォルダーの名前を変更するには、**フォルダー名の変更**を選択します。

- フォルダーを削除するには、**フォルダーの削除**を選択します。
- フォルダーを移動するには、**フォルダーの移動**を選択します。

3. 画面の指示に従って、残りの手順を完了します。

PowerShell を使用する

このセクションでは、PowerShellを使用してカタログを管理する方法について詳しく説明します。

- カタログに関連付けられている警告とエラーを取得する(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/install-configure/machine-catalogs-manage.html#retrieve-warnings-and-errors-associated-with-a-catalog)
- イメージに説明を追加する
- OSディスクをリセットする
- 既存のプロビジョニングスキームのネットワーク設定を変更する
- マシンカタログのバージョンを管理する(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/install-configure/machine-catalogs-manage.html#manage-versions-of-a-machine-catalog)
- マシンプロファイルに基づかないマシンカタログを、マシンプロファイルに基づくマシンカタログに変換する(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/install-configure/machine-catalogs-manage.html#convert-a-non-machine-profile-based-machine-catalog-to-machine-profile-based-machine-catalog)
- アクティブなコンピューターアカウントのID情報を修復する
- 既存のマシンカタログのキャッシュ構成を変更する
- ローカルファイル共有アクセスによるVDA更新のサポート(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/install-configure/machine-catalogs-manage.html#vda-update-support-via-local-file-share-access)

カタログに関連付けられた警告とエラーを取得する

履歴エラーと警告を取得して、MCSマシンカタログの問題を理解し、それらの問題を修正できます。

PowerShellコマンドを使用して、次のことができます。

- エラーまたは警告のリストを取得する
- 警告の状態を**新規**から**確認済み**に変更する
- エラーまたは警告を削除する

PowerShellコマンドを実行するには:

1. PowerShell ウィンドウを開きます。
2. Citrix 固有の PowerShell モジュールをロードするには、`asnp citrix*` を実行します。

エラーと警告のリストを取得するには：

`Get-ProvOperationEvent` コマンドを実行します。

- パラメーターなしの場合：すべてのエラーと警告を取得します
- `LinkedObjectType` および `LinkedObjectUid` パラメーターを使用する場合：特定のプロビジョニングスキームに関連付けられているすべてのエラーと警告を取得します
- `EventId` パラメーターを使用する場合：このイベント ID に一致する特定のエラーまたは警告を取得します
- `Filter`パラメーターを使用: カスタマイズされたフィルターでエラーまたは警告を取得します

エラーまたは警告の状態を **New** から **Acknowledged** に変更するには：

`Confirm-ProvOperationEvent` コマンドを実行します。

- `EventId` パラメーターを使用する場合：このイベント ID に一致する特定のエラーまたは警告の状態を設定します。特定のイベントのエラーまたは警告の `EventId` は、`Get-ProvOperationEvent` コマンドの出力として取得できます。
- `LinkedObjectType` および `LinkedObjectUid` パラメーターを使用する場合：特定のプロビジョニングスキームに関連付けられているすべてのエラーと警告の状態を設定します
- `All` パラメーターを使用する場合：すべてのエラーと警告の状態を **Acknowledged** に設定します

エラーまたは警告を削除するには：

`Remove-ProvOperationEvent` コマンドを実行します。

- `EventId` パラメーターを使用する場合: このイベントIDに一致する特定のエラーまたは警告を削除します。特定のイベントまたは警告の `EventId` は、`Get-ProvOperationEvent` コマンドの出力として取得できます。
- `LinkedObjectType` および `LinkedObjectUid` パラメーターを使用する場合: 特定のプロビジョニングスキームに関連付けられているすべてのエラーと警告を削除します。
- `All` パラメーターを使用する場合: すべてのエラーと警告を削除します。

詳しくは、Citrix PowerShell SDKを参照してください。

イメージに説明を追加する

マシンカタログのイメージ更新に関連する変更について、情報提供の記述を追加できます。この機能を使用して、カタログの作成時、またはカタログの既存のマスターイメージを更新する際に説明を追加します。カタログ内の各マスターイメージの情報を表示することもできます。イメージの説明を追加または表示するには、次のコマンドを使用します。

- マスターイメージを使用してマシンカタログを作成する際にメモを追加するには、`NewProvScheme`コマンドで`MasterImageNote`パラメーターを使用します。例：

```
C:\PS>New-ProvScheme -ProvisioningSchemeName <name> -HostingUnitName
<name> -IdentityPoolName <name> -MasterImageVM

XDHyp:\HostingUnits\<hosting unit name>\<vm name>.vm\Base.snapshot
-MasterImageNote "Note"
```

- マシンカタログに関連付けられているマスターイメージを更新するには、`Publish-ProvMasterVMImage`コマンドで`MasterImageNote`パラメーターを使用します。例：

```
C:\PS>Publish-ProvMasterVMImage -ProvisioningSchemeName <name>
-MasterImageVM XDHyp:\HostingUnits\<hosting unit name>\<vm
name>.vm\base.snapshot -MasterImageNote "Note"
```

- 各イメージの情報を表示するには、Get-ProvSchemeMasterVMImageHistoryコマンドを使用します。例：

```
C:\PS>Get-ProvSchemeMasterVMImageHistory -ProvisioningSchemeName
MyScheme -Showall
```

ロールバックの進行状況を追跡するには、 でカタログを見つけて、インラインの進行状況バーと段階的な進行状況グラフを表示します。

次のような特定のシナリオでは、ロールバックできません。（ オプションは表示されません）。

- ロールバックする権限がありません。
- カタログがMCSを使用して作成されていません。
- カタログがOSディスクのイメージを使用して作成されています。

- カタログの作成に使用されたスナップショットが破損しています。
- カタログ内のマシンに対するユーザーの変更が保持されません。
- カタログ内のマシンが実行中です。

OSディスクをリセットする

MCSで作成されたマシンカタログ内の永続VMのOSディスクをリセットするには、PowerShellコマンド`Reset-ProvVMDisk`を使用します。現在、この機能はAWS、Azure、XenServer、Google Cloud、SCVMM、VMwareの仮想化環境に適用できます。

PowerShellコマンドを正常に実行するには、以下を確認してください。

- ターゲットVMが永続MCSカタログ内にあること。
- MCSマシンカタログが正常に機能していること。
- これは、プロビジョニングスキームとホストが存在し、プロビジョニングスキームに正しいエントリがあることを意味します。
- ハイパーバイザーがメンテナンスモードではないこと。
- ターゲットVMの電源がオフになっており、メンテナンスモードになっていること。

OSディスクをリセットするには、次の手順を実行します。

1. PowerShell ウィンドウを開きます。
2. Citrix固有のPowerShellモジュールをロードするには、**asnp citrix***を実行します。
3. 次のいずれかの方法でPowerShellコマンド`Reset-ProvVMDisk`を実行します。
    - VMのリストをコンマ区切りリストとして指定し、各VMでリセットを実行します。

      ```
      Reset-ProvVMDisk -ProvisioningSchemeName "xxx" -VMName ("abc","def")
      -OS
      ```

    - `Get-ProvVM`コマンドからの出力としてVMのリストを指定し、各VMでリセットを実行します。

      ```
      (Get-ProvVM -ProvisioningSchemeName "xxx") | Reset-ProvVMDisk "abc"
      -OS
      ```

    - 名前で単一のVMを指定します。

```
Reset-ProvVMDisk -ProvisioningSchemeName "xxx" -VMName "abc" -OS
```

- `Get-ProvVM`コマンドによって返されるVMごとに個別のリセットタスクを作成します。各タスクは、ハイパーバイザーの機能チェック、各VMの接続チェックなど、同じ冗長なチェックを実行するため、これは効率的ではありません。

```
Get-ProvVM -ProvisioningSchemeName "xxx" | Reset-ProvVMDisk
-ProvisioningSchemeName "xxx" -OS
```

4. リセットされるVMのリストと、回復不能な操作であるという警告メッセージが表示された確認プロンプトが表示されます。回答を入力せずに**Enter**キーを押すと、それ以上のアクションは実行されません。

> **注：**
>
> リセットプロセスが完了するまで、VMをメンテナンスモードから解除したり、電源をオンにしたりしないでください。

> PowerShellコマンド`-WhatIf`を実行して、実行されるアクションを出力し、アクションを実行せずに終了できます。

次のいずれかの方法を使用して、確認プロンプトをバイパスすることもできます。

- `-Force`パラメーターを指定します。

```
Reset-ProvVMDisk -ProvisioningSchemeName "xxx" -VMName "abc" -OS
-Force
```

- `-Confirm:$false`パラメーターを指定します。

```
Reset-ProvVMDisk -ProvisioningSchemeName "xxx" -VMName "abc" -OS
-Confirm:$false
```

- `Reset-ProvVMDisk`を実行する前に、`$ConfirmPreference`を**None**に変更します。

```
PS C:\Windows\system32> $ConfirmPreference='None'

PS C:\Windows\system32> $ConfirmPreference

None

PS C:\Windows\system32> Reset-ProvVMDisk -ProvisioningSchemeName
"xxx" -VMName "abc" -OS
```

5. `Reset-ProvVMDisk`コマンドによって返されるタスクのステータスを取得するには、`Get-ProvTask`を実行します。

既存のプロビジョニングスキームのネットワーク設定を変更する

既存のプロビジョニングスキームのネットワーク設定を変更して、新しいVMが新しいサブネットワーク上に作成されるようにすることができます。ネットワーク設定を変更するには、`Set-ProvScheme`コマンドで`-NetworkMapping`パラメーターを使用します。

注：

この機能は、Citrix Virtual Apps and Desktops 2203 LTSR CU3以降のバージョンでサポートされています。

既存のプロビジョニングスキームのネットワーク設定を変更するには、次の手順を実行します。

1. PowerShellウィンドウで、コマンド `asnp citrix*` を実行してPowerShellモジュールをロードします。
2. 変更するネットワークパスに移動するには、`(Get-Provscheme -ProvisioningSchemeName "name").NetworkMaps` を実行します。
3. 新しいネットワーク設定に変数を割り当てます。例:

```
$NewNetworkMap = @{"0"= "XDHYP:\HostingUnits\MyNetworks\Network
0.network"}
```

4. `Set-ProvScheme -ProvisioningSchemeName "name" -NetworkMapping $NewNetworkMap` を実行します。

5. 既存のプロビジョニングスキームの新しいネットワーク設定を確認するには、`(Get-Provscheme -ProvisioningSchemeName "name").NetworkMaps` を実行します。

マシンカタログのバージョンを管理する

MCSマシンカタログが`Set-ProvScheme`コマンドで更新されると、現在の構成がバージョンとして保存されます。その後、PowerShellコマンドを使用して、マシンカタログのさまざまなバージョンを管理できます。次のことができます。

- マシンカタログのバージョンリストを表示する
- 以前のバージョンを使用してマシンカタログを更新する
- そのマシンカタログのVMで使用されていないバージョンは手動で削除する
- マシンカタログで保持される最大バージョン数を変更する（デフォルトは99）

バージョンには、マシンカタログの次の情報が含まれます。

- VMCpuCount
- VMMemoryMB
- CustomProperties
- ServiceOffering
- MachineProfile
- NetworkMapping
- SecurityGroup

マシンカタログのさまざまなバージョンを管理するには、次のコマンド（例として提供）を実行します。

- マシンカタログのさまざまなバージョンの構成詳細を表示するには：

```
Get-ProvSchemeVersion -ProvisioningSchemeName AzureCatalog
```

- マシンカタログの特定のバージョンの構成詳細を表示するには：

```
Get-ProvSchemeVersion -ProvisioningSchemeName AzureCatalog -Version 2
```

- マシンカタログに関連付けられているバージョンの総数を確認するには：

```
(Get-ProvSchemeVersion -ProvisioningSchemeName AzureCatalog).Count
```

- 以前のバージョンを使用してマシンカタログを更新するには：

```
Set-ProvScheme -ProvisioningSchemeName AzureCatalog -Version 2
```

- そのマシンカタログのVMによって使用されていないバージョンを手動で削除するには：

```
Remove-ProvSchemeVersion -ProvisioningSchemeName AzureCatalog -Version
3
```

- マシンカタログで保持される最大バージョン数を設定します（デフォルトは99）。この設定は、すべてのカタログに適用されます。たとえば、この場合、すべてのMCSプロビジョニング済みカタログに対して最大15バージョンが保持されます。

```
Set-ProvServiceConfigurationData -Name "MaxProvSchemeVersions" -Value
15
```

バージョン数が最大バージョン数に達した場合、マシンカタログ内のいずれかのVMで古いバージョンが使用されていると、新しいバージョンを作成できません。その場合は、次のいずれかを実行してください。

- マシンカタログによって保持される最大バージョン数の制限を増やします。
- 古いバージョンを使用している一部のVMを更新して、それらの古いバージョンがどのVMからも参照されなくなり、削除できるようにします。

マシンプロファイルベースではないマシンカタログをマシンプロファイルベースのマシンカタログに変換する

VM、テンプレート仕様（Azureの場合）、または起動テンプレート（AWSの場合）をマシンプロファイルの入力として使用して、マシンプロファイルベースではないマシンカタログをマシンプロファイルベースのマシンカタログに変換できます。カタログに追加される新しいVMは、明示的なカスタムプロパティによって上書きされない限り、マシンプロファイルからプロパティ値を取得します。

> **注：**

> 既存のマシンプロファイルベースのマシンカタログを、マシンプロファイルベースではないマシンカタログに変更することはできません。

> これを行うには：

1. 永続的または非永続的なマシンカタログを、VMを使用して、マシンプロファイルなしで作成します。
2. **PowerShell**ウィンドウを開きます。
3. マシンプロファイルからのプロパティ値を、マシンカタログに追加された新しいVMに適用するには、`Set-ProvScheme`コマンドを実行します。例:
   - Azureの場合:

     ```
     Set-ProvScheme -ProvisioningSchemeName xxxx -MachineProfile XDHyp:
     \HostingUnits\<HostingUnitName>\machineprofile.folder\<ResourceGroup
     Name>\<TemplateSpecName>\<VersionName>
     ```

   - AWSの場合:

     ```
     Set-ProvScheme -ProvisioningSchemeName xxxx -MachineProfile "XDHyp:
     \HostingUnits\<hosting-unit>\<launch-
     template>.launchtemplate\<launch-template-
     version>.launchtemplateversion"
     ```

アクティブなコンピューターアカウントのID情報を修復する

ID関連の問題があるアクティブなコンピューターアカウントのID情報をリセットできます。マシンパスワードと信頼キーのみをリセットするか、IDディスクのすべての構成をリセットするかを選択できます。この実装は、永続的および非永続的な両方のMCSマシンカタログに適用できます。

> **注：**
>
> 現在、この機能はAzureおよびVMware仮想化環境でのみサポートされています。

条件

IDディスクを正常にリセットするには、以下を確認してください。

- VMをシャットダウンし、メンテナンスモードに設定します
- PowerShellコマンドにパラメーター-OSを含めないでください

IDディスクのリセット

IDディスクをリセットするには：

1. **PowerShell**ウィンドウを開きます。
2. Citrix固有のPowerShellモジュールをロードするために`asnp citrix*`を実行します。
3. ID情報をリセットします。
   - マシンパスワードと信頼キーのみをリセットするには、次のコマンドを実行します。

     ```
     Repair-AcctIdentity -IdentityAccountName TEST\VM1
     -PrivilegedUserName TEST\admin1 -PrivilegedUserPassword $password
     -Target IdentityInfo
     ```

     コマンドで使用されるパラメーターの説明は次のとおりです。

     - IdentityAccountName：修復する必要があるIDアカウントの名前。
     - PrivilegedUserName：IDプロバイダー（ADまたはAzureAD）に対する書き込み権限を持つユーザーアカウント。
     - PrivilegedUserPassword：PrivilegedUserNameのパスワード。
     - Target：修復アクションのターゲット。アカウントパスワード/信頼キーを修復するためのIdentityInfo、およびハイブリッドAzureAD参加済みマシンIDのユーザー証明書属性を修復するためのUserCertificateを指定できます。
   - IDディスクのすべての構成をリセットするには、次のコマンドを次の順序で実行します。

     ```
     Repair-AcctIdentity -IdentityAccountName TEST\VM1
     -PrivilegedUserName TEST\admin1 -PrivilegedUserPassword $password
     -Target IdentityInfo
     ```

     ```
     Reset-ProvVMDisk ProvisioningSchemeName <name> -VMName <name>  -
     Identity
     ```

   - IDディスクを完全に再作成するには:

```
Reset-ProvVMDisk -ProvisioningSchemeName <name> -VMname <name>
-Identity -Recreate
```

4. アクションを確定するには「**y**」と入力します。`-Force` パラメーターを使用して確認プロンプトをスキップすることもできます。例:

```
Reset-ProvVMDisk -ProvisioningSchemeName <name> -VMName <name>
-Identity -Force
```

5. 更新されたIDディスク設定を確認するには、`Get-ProvVM -ProvisioningSchemeName <name -VMName <name>` を実行します。IDディスクの属性（例: `IdentityDiskId`）は更新されている必要があります。`StorageId` と `IdentityDiskIndex` は変更されていてはなりません。

既存のマシンカタログのキャッシュ構成を変更する

MCSIOを有効にして非永続カタログを作成した後、Set-ProvSchemeコマンドを使用して以下のパラメータを変更できます。

- WriteBackCacheMemorySize
- WriteBackCacheDiskSize

この機能は現在、以下に適用されます。

- GCPおよびMicrosoft Azure環境、および
- MCSIOが有効な非永続カタログ

要件

キャッシュ構成を変更するための要件は次のとおりです。

- VDA を最新バージョン (2308 以降) に更新します。
- 既存のマシンカタログでパラメーター `UseWriteBackCache` を有効にします。`UseWriteBackCache` が有効なマシンカタログを作成するには、`New-ProvScheme` を使用します。例:

```
New-ProvScheme -ProvisioningSchemeName $CatalogName -HostingUnitUid
$HostingUnitUid `

-IdentityPoolUid $acctPool.IdentityPoolUid -CleanOnBoot `
```

```
-MasterImageVM $MasterImage `
-ServiceOffering $ServiceOffering `
-NetworkMap $NetworkMap `
-SecurityGroup $SecurityGroup `
-UseWriteBackCache -WriteBackCacheDiskSize 8
```

キャッシュ構成を変更する

Set-ProvSchemeコマンドを実行します。例:

```
Set-ProvScheme -ProvisioningSchemeName $provScheme.ProvisioningSchemeName
-WriteBackCacheDisk32 -WriteBackCacheMemorySize 128
```

注：

- 少なくとも 1 GB のキャッシュディスクストレージが必要なため、`WriteBackCacheDiskSize` の値はゼロより大きくする必要があります。
- `WriteBackCacheMemorySize` の値は、マシンカタログのメモリサイズよりも小さくする必要があります。
- これらの変更は、変更後にカタログに追加された新しい VM にのみ影響します。既存の VM はこれらの変更の影響を受けません。

ローカルファイル共有アクセスによるVDAアップデートのサポート

PowerShellコマンドレットを介してVDAインストーラーの場所を指定することで、各VDAがCitrix Managed Azure CDNから新しいVDAインストーラーを取得できるようにするためのネットワークルールを提供する手間を省くことができます。

PowerShellコマンドレット

ローカルファイル共有からインストーラーを使用できるようにする、**New-VusCatalogSchedule** および **New-VusMachineUpgrade** コマンドレットに2つの新しいオプションパラメータが追加されました。

- **VdaWorkstationPackageUri** - ワークステーションOS VDAインストーラーへのUNCパスを指定します。
- **VdaServerPackageUri** - サーバーOS VDAインストーラーへのUNCパスを指定します。

前提条件

- VDA 2311に付属するVUSエージェントインストーラー
- VDAアップグレードエージェントをバージョン7.40.0.35以降にアップグレード（VDAインストーラーバージョン2311以降を使用）
- Virtual Apps and Desktops Remote PowerShell SDK バージョン 7.40 以降 (Jan 10, 2024 以降にリリース)

ファイル共有のアクセス許可を設定する方法

VDAインストーラーパッケージを含むネットワーク共有には、Local System (NT AUTHORITY\SYSTEMプリンシパル) として実行されるVDAアップグレードエージェントサービスに対する読み取りアクセス権が必要です。

- **ドメイン参加済みファイル共有のアクセス許可**

  VDAマシンがドメインに参加している場合、**ローカルシステム**アカウント（VUAはローカルシステムとして実行されます）は、ネットワーク共有にアクセスする際にコンピューターの資格情報を使用します。

  最小特権のアクセス許可は、Domain Computers に **読み取り** アクセスを付与することで設定できます。

  a. ファイルを共有するネットワーク上のユーザーを選択します。
  b. **詳細な共有設定** をクリックし、**ファイルとプリンターの共有** をオンにします。

- **ドメインに参加していないファイル共有のアクセス許可**

  VDA マシンがドメインに参加していない場合、**ローカルシステム** アカウント (VUA はローカルシステムとして実行されます) は、ネットワーク共有にアクセスするときに **ANONYMOUS LOGON** を使用します。

  a. 共有フォルダーを選択します。
  b. パスワード保護を無効にします。

     a. フォルダーの **プロパティ** に移動します。
     b. **ネットワークと共有センター** を選択します。

c. **パスワード保護共有** をオフにします。

c. **詳細な共有** をクリックして、共有アクセス許可を付与します。

a. **アクセス許可** を選択します。

b. **ANONYMOUS LOGON** に **読み取り** 共有アクセス許可を付与します。

d. フォルダーのアクセス許可を付与するには、**セキュリティ** タブを選択します。

a. 共有フォルダーにアクセス許可を追加するには、**編集** をクリックします。

b. 共有フォルダーを選択し、**ANONYMOUS LOGON** にフォルダーのアクセス許可を付与します。

e. **詳細設定**をクリックして、**ファイルとプリンターの共有**をオンにします。

f. 共有フォルダー名を**ネットワークアクセスセキュリティポリシー**に追加します。

> **注：**
>
> 変更をすぐに有効にするには、マシンを再起動します。

ローカルファイル共有からのVDAアップデート

1. VDAインストーラーをダウンロードし、共有ファイルに配置します。

> **注：**
>
> Virtual Upgrade Serviceを使用すると、Current ReleaseトラックまたはLTSRトラックのいずれかを選択できます。
>
> **例：** マシンカタログがCurrent Release（2311）に設定されており、VDAバージョンが2305の場合、VDAをバージョン2311にアップグレードする必要があります。

a. 弊社のWebサイトの**ダウンロード**ページに移動します。

b. 製品として**Citrix Virtual Apps and Desktops**を選択します。

c. **シトリックス バーチャルアプリ＆デスクトップ 7 2311, 全エディション**を選択します。

d. **製品ISOに含まれるが個別にパッケージ化されているコンポーネント**の展開可能な項目からVDAインストーラーを選択します。

2. カタログの種類に基づいて、関連するVDAインストーラーを選択します。

   - カタログの種類が**マルチセッション**の場合は、**マルチセッションOS VDAインストーラー**をダウンロードします。
   - カタログの種類が**シングルセッション**の場合は、**シングルセッションOS VDAインストーラー**をダウンロードします。
   - カタログタイプが**Remote PC Access**の場合は、**Single-session OS Core Services VDA installer**をダウンロードします。

> **注：**
>
> ファイル共有インストーラーのバージョンは、VUSによってクラウドに公開された最新のインストーラーバージョンと**正確に**一致している必要があります。

トラブルシューティング

- 「Power State Unknown」ステータスのマシンについては、ガイダンスとしてCTX131267を参照してください。
- 不明な電源状態を継続的に表示するVMを修正するには、How to fix VMs that continuously show an unknown power stateを参照してください。

次のステップ

特定のクラウドサービスカタログの管理については、以下を参照してください。

- AWSカタログの管理
- XenServerカタログを管理する(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/install-configure/machine-catalogs-manage/manage-machine-catalog-citrix-hypervisor.html)
- Google Cloud Platformカタログの管理
- Microsoft Azureカタログを管理する(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/install-configure/machine-catalogs-manage/manage-machine-catalog-azure.html)
- Microsoft System Center Virtual Machine Managerカタログを管理する(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/install-configure/machine-catalogs-manage/manage-machine-catalog-mscvmm.html)
- VMwareカタログを管理する(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/install-configure/machine-catalogs-manage/manage-machine-catalog-vmware.html)

AWSカタログを管理する

マシンカタログの管理では、マシンカタログを管理するウィザードについて説明します。以下の情報は、AWSクラウド環境に固有の詳細を扱います。

> **注：**
>
> AWSカタログを管理する前に、AWSカタログの作成を完了する必要があります。AWSカタログの作成を参照してください。

タグを削除する

カタログまたはVMを作成すると、MCSによって作成されたタグが以下のリソースに作成されます。

- 仮想マシン
- ルートディスクボリューム
- 識別ディスクボリューム
- NIC
- ルートディスクイメージ (AMI)
- 起動テンプレート
- AMIまたはルートディスクのスナップショット

Citrix®データベースからVMとマシンカタログを削除し、MCSによって作成されたタグを削除できます。以下を使用できます。

- `Remove-ProvVM`を`ForgetVM`パラメーターとともに使用して、マシンカタログから単一のVMまたはVMのリストからVMとMCSによって作成されたタグを削除します。
- `Remove-ProvScheme`を`ForgetVM`パラメーターとともに使用して、Citrixデータベースからマシンカタログを削除し、マシンカタログからリソースを削除します。

この機能は、永続VMにのみ適用されます。

これを行うには：

1. **PowerShell**ウィンドウを開きます。
2. Citrix固有のPowerShellモジュールをロードするために`asnp citrix*`を実行します。
3. VMを削除する前にVMをロック解除します。例：

```
Unlock-ProvVM -ProvisioningSchemeName "<name>" -VMID "<id"
```

4. 以下のいずれかのコマンドを実行して、リソースからVM、マシンカタログ、およびMCSによって作成されたタグを削除します。

   - `Remove-ProvVM`を`ForgetVM`とともに実行して、Citrixデータベースから VMを、VMからタグを削除します。例：

     ```
     Remove-ProvVM -ProvisioningSchemeName "<name>" -VMName "<name>"
     -ForgetVM
     ```

   - `Remove-ProvScheme`を実行して、Citrixデータベースからマシンカタログを削除し、マシンカタログからリソースを削除します。例：

     ```
     Run Remove-ProvScheme -ProvisioningSchemeName "<name>" -ForgetVM
     ```

5. VMがDelivery Controller™から削除されていることを確認しますが、ハイパーバイザーからは削除されていません。

   a. `Get-ProvVM -ProvisioningSchemeName "<name>" -VMName "<name>"`を実行します。これは何も返さないはずです。

   b. AWS EC2コンソールに移動します。VMは表示されますが、タグは削除されています。以下のリソースからタグが削除されます。

      - 仮想マシン
      - ルートディスクボリューム
      - 識別ディスクボリューム
      - NIC

6. マシンカタログを削除する場合は、そのカタログがDelivery Controllerから削除されていることを確認します。

   a. `Get-ProvScheme -ProvisioningSchemeName "forgetvmdemo"`を実行します。これはエラーを返すはずです。

   b. AWS EC2コンソールで、以下のリソースが削除されていることを確認します。

      - ルートディスクイメージ (AMI)
      - 起動テンプレート

- AMIまたはルートディスクのスナップショット

MCSによって作成されたリソースを識別する

以下は、MCS がリソースに追加するタグです。表のタグは「"key":"value"」として表されます。

リソース名	タグ
IDディスク	"名前": "VMName_IdentityDisk"
	"Xd構成": "Xdプロビジョニング済み=true"
	"CitrixプロビジョニングスキームID": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
イメージ	"Xd構成": "Xdプロビジョニング済み=true"
	"CitrixプロビジョニングスキームID": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
NIC	"説明": "XD NIC"
	"Xd構成": "Xdプロビジョニング済み=true"
	"CitrixプロビジョニングスキームID": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
OSディスク	"名前": "VMName_rootDisk"
	"Xd設定": "XdProvisioned=True"
	"CitrixプロビジョニングスキームID": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	[when AwsCaptureInstanceProperties = true] "Citrix リソース": ""
	[when AwsCaptureInstanceProperties = true and AwsOperationalResourcesTagging = true] 「CitrixOperationalResource」: 「」
PrepVM	"Name": "準備 - カタログ名 - xxxxxxxxxx"
	"Xd構成": "Xdプロビジョニング済み=true"

リソース名	タグ
	"CitrixプロビジョニングスキームID": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	[when AwsCaptureInstanceProperties = true] "Citrix リソース": ""
	[when AwsCaptureInstanceProperties = true and AwsOperationalResourcesTagging = true] 「CitrixOperationalResource」: 「」
公開されたスナップショット	"Xd構成": "Xdプロビジョニング済み=true"
	ボリュームワーカーAMIのスナップショットでない場合、「CitrixProvisioningSchemeId」: 「xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx」
テンプレート	[when AwsCaptureInstanceProperties = true] "XdConfig" の値は "XdProvisioned=true" です。
	[when AwsCaptureInstanceProperties = true] "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	[when AwsCaptureInstanceProperties = true] 「CitrixResource」: 「」
	[when AwsCaptureInstanceProperties = true and AwsOperationalResourcesTagging = true] 「CitrixOperationalResource」: 「」
カタログ内のVM	"Xd構成": "Xdプロビジョニング済み=true"
	"CitrixプロビジョニングスキームID": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	[when AwsCaptureInstanceProperties = true] 「CitrixResource」: 「」
	[when AwsCaptureInstanceProperties = true] "AWS EC2起動テンプレートID":"lt-xxxx"

リソース名	タグ
	[when AwsCaptureInstanceProperties = true] "AWS EC2起動テンプレートバージョン": "n"
	[when AwsCaptureInstanceProperties = true and AwsOperationalResourcesTagging = true] 「CitrixOperationalResource」: 「」
ボリュームワーカーAMI	"Xd構成": "Xdプロビジョニング済み=true"
ボリュームワーカーブートストラッパー	"名前": "XenDesktop® Temp"
	"Xd構成": "Xdプロビジョニング済み=true"
	"Citrixプロビジョニングスキームid": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	[when AwsCaptureInstanceProperties = true and AwsOperationalResourcesTagging = true] 「CitrixVolumeWorkerBootstrapper」: 「」
ボリュームワーカーインスタンス	"名前": "Citrix.XD.Volumeworker-xxxx-xx-xx-xx-xxxx"
	"Xd構成": "Xdプロビジョニング済み=true"

詳細情報

- 接続とリソースの作成および管理
- AWSへの接続
- マシンカタログの作成
- AWS カタログを作成する
- マシンカタログの管理

XenServer®カタログを管理する

マシンカタログの管理では、マシンカタログを管理するウィザードについて説明します。以下の情報は、XenServer仮想化環境に固有の詳細を扱います。

> **注：**

XenServerカタログを管理する前に、XenServerカタログの作成を完了する必要があります。「XenServerカタログの作成」を参照してください。

MCSによって作成されたリソースを識別する

以下は、MCS がリソースに追加するタグです。表のタグは「"key":"value"」として表されます。

リソース名	タグ
公開されたベースディスクと、各ネットワークまたはローカルストレージ上のそのコピー	"Citrixプロビジョニングスキーム ID": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
IDディスク	"Citrixプロビジョニングスキーム ID": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
OSディスク	"Citrixプロビジョニングスキーム ID": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
準備用 VM	"Citrixプロビジョニングスキーム ID": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
カタログ内のVM	"Citrixプロビジョニングスキーム ID": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
WBCディスク	"Citrixプロビジョニングスキーム ID": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"

詳細情報

- 接続とリソースの作成および管理
- XenServerへの接続
- マシンカタログの作成
- XenServerカタログを作成する
- マシンカタログの管理

Google Cloud Platformカタログを管理する

マシンカタログの管理では、マシンカタログを管理するウィザードについて説明します。以下の情報は、Google Cloud環境に固有の詳細を扱います。

> **注：**
>
> Google Cloud Platformカタログを管理する前に、Google Cloud Platformカタログの作成を完了する必要があります。Google Cloud Platformカタログの作成を参照してください。

マシンカタログの管理

カタログにマシンを追加したり、マシンを更新したり、更新をロールバックしたりするには、「マシンカタログの管理」を参照してください。

電源管理

Citrix DaaS™を使用すると、Google Cloudマシンの電源管理を行うことができます。左ペインの**検索**ノードを使用して、電源管理したいマシンを見つけます。以下の電源操作が利用可能です。

- 削除
- 起動
- 再起動
- 強制再起動
- シャットダウン
- 強制シャットダウン
- デリバリーグループに追加
- タグの管理
- メンテナンスモードをオンにする

Autoscaleを使用してGoogle Cloudマシンを電源管理することもできます。これを行うには、Google Cloudマシンをデリバリーグループに追加し、そのデリバリーグループでAutoscaleを有効にします。Autoscaleの詳細については、「Autoscale」を参照してください。

PowerShellを使用してプロビジョニングされたマシンを更新する

`Set-ProvScheme`コマンドはプロビジョニングスキームを変更しますが、既存のマシンには影響しません。PowerShellコマンド`Set-ProvVMUpdateTimeWindow`を使用すると、現在のプロビジョニングスキームを既存の永続マシンまたは非永続マシン、あるいはマシンセットに適用できるようになります。現在、GCPでは、この機能でサポートされているプロパティ更新はマシンプロファイルです。

更新できるもの:

- 単一のVM
- 特定のVMのリスト、またはプロビジョニングスキームIDに関連付けられている既存のすべてのVM
- プロビジョニングスキーム名に関連付けられた特定のVMのリスト、またはすべての既存のVM

既存のVMを更新するには：

1. 既存のマシンの構成を確認します。例えば、,

   ```
   Get-ProvScheme | select ProvisioningSchemeName,
   ProvisioningSchemeVersion
   ```

2. プロビジョニングスキームを更新します。例えば、,

   ```
   `Set-ProvScheme –ProvisioningSchemeName "my-catalog" –MachineProfile
   "XDHyp:\HostingUnits\<hosting-unit>\machineprofileinstance.vm"
   ```

3. VMの現在のプロパティが現在のプロビジョニングスキームと一致しているか、およびVMに保留中の更新アクションがあるかを確認します。例えば、,

   ```
   Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
   ProvisioningSchemeVersion
   ```

   特定のバージョンのマシンを見つけることもできます。例えば、,

   ```
   Get-ProvVM -Filter "ProvisioningSchemeVersion -eq 1" | select VMName,
   ProvisioningSchemeVersion
   ```

4. 既存のマシンを更新します。

   - すべての既存のマシンを更新するには：

     ```
     Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
     -StartsNow -DurationInMinutes -1
     ```

   - 特定のマシンのリストを更新するには：

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
-VMName <List-Of-Vm-Names> -StartsNow -DurationInMinutes -1
```

- `Get-ProvVM`の出力に基づいてマシンを更新するには：

```
Get-ProvVM -ProvisioningSchemeName "my-catalog" | Set-
ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog -StartsNow
-DurationInMinutes -1
```

5. 更新がスケジュールされているマシンを見つける。例：

```
Get-ProvVM -Filter "ProvisioningSchemeUpdateAfter" | select VMName,
ProvisioningSchemeUpdateAfter
```

6. マシンを再起動します。次回の電源投入時に、プロパティの変更が既存のマシンに適用されます。以下のコマンドを使用して更新されたステータスを確認できます。

```
Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
ProvisioningSchemeVersion
```

既存のカタログのディスク関連のカスタムプロパティを変更する

既存のカタログおよびカタログの既存のVMの、以下のディスク関連のカスタムプロパティを変更できます。

- `PersistOSDisk`
- `PersistWBC`
- `StorageType`
- `IdentityDiskStorageType`
- `WbcDiskStorageType`

注：

- `StorageType` プロパティは OS ディスク用です

- `PersistOsDisk` プロパティは、ライトバックキャッシュが有効な非永続カタログに対してのみ設定できます

この実装により、カタログ作成後でも異なるディスクに異なるストレージタイプを選択できるようになり、さまざまなストレージタイプに関連する価格のバランスを取ることができます。

これを行うには、PowerShell コマンド `Set-ProvScheme` と `Set-ProvVMUpdateTimeWindow` を使用します。

1. **PowerShell**ウィンドウを開きます。
2. `asnp citrix*`を実行します。
3. カスタムプロパティを取得するには、`Get-ProvVM -VMName <VM name>` を実行します。
4. カスタムプロパティ文字列を変更します。
   a. カスタムプロパティをメモ帳にコピーし、カスタムプロパティを変更します。
   b. **PowerShell** ウィンドウで、メモ帳から変更されたカスタムプロパティを貼り付け、変更されたカスタムプロパティに変数を割り当てます。例:

```
$cp =  '<CustomProperties xmlns=http://schemas.citrix.com/2014/xd/
machinecreation xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="CatalogZones" Value="" />

<Property xsi:type="StringProperty" Name="PersistWBC" Value="true" /
>

<Property xsi:type="StringProperty" Name="PersistOSDisk"
Value="true" />

<Property xsi:type="StringProperty" Name="WBCDiskStorageType"
Value="pd-standard" />

<Property xsi:type="StringProperty" Name="StorageType" Value="pd-
standard" />

</CustomProperties>'
```

5. 既存のカタログを更新します。例:

```
Set-ProvScheme -ProvisioningSchemeName <yourCatalogName>
-CustomProperties $cp
```

6. 既存の VM を更新します。例:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog -VMName
<List-Of-Vm-Names> -StartsNow -DurationInMinutes -1
```

7. VM を再起動します。次回の電源投入時に、カスタムプロパティの変更が既存の VM に適用されます。

偶発的なマシン削除からの保護

Citrix DaaSでは、偶発的な削除を防ぐために、Google Cloud上のMCSリソースを保護できます。プロビジョニングされたVMを構成するには、`deletionProtection`フラグをTRUEに設定します。

デフォルトでは、MCSまたはGoogle Cloudプラグインを介してプロビジョニングされたVMは、InstanceProtectionが有効な状態で作成されます。この実装は、永続カタログと非永続カタログの両方に適用されます。非永続カタログは、インスタンスがテンプレートから再作成されるときに更新されます。既存の永続マシンについては、Google Cloudコンソールでフラグを設定できます。フラグの設定の詳細については、「Googleドキュメントサイト」を参照してください。永続カタログに追加される新しいマシンは、`deletionProtection`が有効な状態で作成されます。

`deletionProtection`フラグを設定したVMインスタンスを削除しようとすると、リクエストは失敗します。ただし、`compute.instances.setDeletionProtection`権限が付与されているか、IAMの**Compute Admin**ロールが割り当てられている場合は、フラグをリセットしてリソースを削除できるようにすることができます。

MCSによって作成されたリソースを識別する

以下は、MCS がリソースに追加するタグです。表のタグは「"key":"value"」として表されます。

リソース名	タグ
IDディスク	"CitrixResource": "内部"
	"Citrixプロビジョニングスキーム ID": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"

リソース名	タグ
イメージ	"CitrixResource": "内部"
	"CitrixプロビジョニングスキームID": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
OSディスク	"CitrixResource": "内部"
	"CitrixプロビジョニングスキームID": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
PrepVM	"CitrixResource": "内部"
	"CitrixプロビジョニングスキームID": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
公開されたスナップショット	"CitrixResource": "内部"
ストレージバケット	"Citrixresource": "内部向け"
テンプレート	"CitrixResource": "内部"
	"CitrixプロビジョニングスキームID": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
カタログ内のVM	"CitrixResource": "内部"
	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx". プラグインは、MCSでプロビジョニングされたVMにもこのラベルを追加します: "citrix-provisioning-scheme-id": "provSchemeId"。このラベルを使用して、GCPコンソールでカタログによってフィルタリングできます。
WBCディスク	"CitrixResource": "内部"
	CitrixプロビジョニングスキームID": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"

注：

> MCSによって作成されたリソースとして識別するために**CitrixResource**タグが追加されている場合、VMはCitrixインベントリに表示されません。タグを削除または名前変更することで、表示させることができます。

詳細情報

- 接続とリソースの作成および管理
- Google Cloud環境への接続
- マシンカタログの作成
- Google Cloud Platform カタログを作成する
- マシンカタログの管理

HPE Moonshot カタログの管理

マシンカタログの管理では、マシンカタログを管理するウィザードについて説明しています。以下の情報は、HPE Moonshot カタログに固有の詳細を扱っています。

> **注：**

> HPE Moonshotカタログを管理する前に、HPE Moonshotカタログの作成を完了する必要があります。

電源管理

Citrix Virtual Apps and Desktops™では、HPE Moonshotマシンの電源管理を行うことができます。電源管理を行うマシンを見つけるには、ナビゲーションペインの**検索**ノードを使用します。以下の電源操作が利用可能です。

- 起動
- シャットダウン
- 強制シャットダウン
- 再起動
- リセット

> **注：**

> **一時停止**および**再開**の電源操作はサポートされていません。

詳細情報

- 接続とリソースの作成および管理
- HPE Moonshotへの接続
- マシンカタログの作成
- HPE Moonshotマシンカタログの作成
- マシンカタログの管理

Microsoft Azureカタログを管理する

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

マシンカタログの管理では、マシンカタログを管理するウィザードについて説明します。以下の情報は、Microsoft Azure Resource Managerクラウド環境に固有の詳細を扱います。

> **注：**
>
> Microsoft Azureカタログを管理する前に、Microsoft Azureカタログの作成を完了する必要があります。Microsoft Azureカタログの作成を参照してください。

VMシャットダウン時にストレージタイプを下位層に変更する

VMをシャットダウンするときに、管理ディスクのストレージタイプを下位層に切り替えることで、ストレージコストを節約できます。これを行うには、`StorageTypeAtShutdown`カスタムプロパティを使用します。

VMをシャットダウンすると、ディスクのストレージタイプは下位層（`StorageTypeAtShutdown`カスタムプロパティで指定）に変更されます。VMの電源をオンにすると、ストレージタイプは元

の状態（`StorageType`カスタムプロパティまたは`WBCDiskStorageType`カスタムプロパティで指定）に戻ります。

> **重要:**
>
> ディスクはVMが少なくとも一度電源オンになるまで存在しません。したがって、VMを最初に電源オンにしたときにストレージタイプを変更することはできません。

要件

- 管理ディスクに適用されます。これは、カスタムプロパティ`UseManagedDisks`をtrueに設定することを意味します。
- 永続OSディスクを持つ永続および非永続カタログに適用されます。これは、カスタムプロパティ`persistOsDisk`をtrueに設定することを意味します。
- 永続WBCディスクを持つ非永続カタログに適用されます。これは、カスタムプロパティ`persistWBC`をtrueに設定することを意味します。

制限

- Microsoftによると、ディスクの種類は1日2回しか変更できません。Microsoftドキュメントを参照してください。Citrixによると、VMの起動または割り当て解除アクションがあるたびに`StorageType`の更新が行われます。したがって、VMあたりの電源アクションの数を1日2回に制限してください。たとえば、午前中にVMを起動するための電源アクションを1回、夕方にVMを割り当て解除するための電源アクションを1回実行します。

ストレージの種類を下位層に変更する

手順を進める前に、要件と制限を参照してください。

1. カスタムプロパティ`StorageTypeAtShutdown`を追加し、値をStandard_LRS (HDD)に設定して、`New-ProvScheme`を使用してカタログを作成します。PowerShellを使用してカタログを作成する方法については、`<https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/>`を参照してください。

   > **注：**
   >
   > `StorageTypeAtShutdown`が空またはStandard_LRS (HDD)以外の値を持つ場合、操作は失敗します。

永続カタログの作成中にカスタムプロパティを設定する例：

```
$customProperties='<CustomProperties xmlns="http://schemas.citrix.com/
2014/xd/machinecreation"

xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks"
Value="true" />

<Property xsi:type="StringProperty" Name="StorageType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="ResourceGroups" Value="" />

<Property xsi:type="StringProperty" Name="LicenseType"
Value="Windows_Client" />

<Property xsi:type="StringProperty" Name="SchemaVersion" Value="2" />

<Property xsi:type="StringProperty" Name="OsType" Value="Windows" />

<Property xsi:type="StringProperty" Name="StorageTypeAtShutdown"
Value="Standard_LRS" />

</CustomProperties>'
```

非永続カタログの作成中にカスタムプロパティを設定する例：

```
$customProperties='<CustomProperties xmlns="http://schemas.citrix.com/
2014/xd/machinecreation"

xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks"
Value="true" />

<Property xsi:type="StringProperty" Name="StorageType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="WbcDiskStorageType"
Value="Standard_SSD_LRS" />
```

```
<Property xsi:type="StringProperty" Name="ResourceGroups" Value="" />

<Property xsi:type="StringProperty" Name="LicenseType"
Value="Windows_Client" />

<Property xsi:type="StringProperty" Name="SchemaVersion" Value="2" />

<Property xsi:type="StringProperty" Name="OsType" Value="Windows" />

<Property xsi:type="BooleanProperty" Name="persistWBC" Value=true />

<Property xsi:type="BooleanProperty" Name="persistOsDisk" Value=true />

<Property xsi:type="StringProperty" Name="StorageTypeAtShutdown"
Value="Standard_LRS" />

</CustomProperties>'
```

注：

マシンプロファイルを使用する場合、カスタムプロパティは`MachineProfile`で定義されたプロパティよりも優先されます。

2. VMをシャットダウンし、AzureポータルでVMのストレージタイプを確認します。ディスクのストレージタイプは、`StorageTypeAtShutdown`カスタムプロパティで指定されたように、下位の層に変更されます。
3. VMをオンにします。ディスクのストレージの種類は、以下に記載されているストレージの種類に戻ります。
   - OSディスクの`StorageType`カスタムプロパティ
   - WBCディスクの`WBCDiskStorageType`カスタムプロパティ（`CustomProperties`で指定した場合のみ）。それ以外の場合は、`StorageType`に記載されているストレージの種類に戻ります。

既存のカタログに`StorageTypeAtShutdown`を適用する

手順を進める前に、要件と制限を参照してください。

既存のカタログにVMを追加するには、`Set-ProvScheme`を使用します。この機能は、`Set-ProvScheme`の実行後に追加された新しいVMに適用されます。既存のマシンには影響しません。

既存のカタログにVMを追加する際にカスタムプロパティを設定する例：

```
$customProperties='<CustomProperties xmlns="http://schemas.citrix.com/
2014/xd/machinecreation"

xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="StorageType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="WbcDiskStorageType"
Value="Standard_SSD_LRS" />

<Property xsi:type="StringProperty" Name="ResourceGroups" Value="" />

<Property xsi:type="StringProperty" Name="LicenseType"
Value="Windows_Client" />

<Property xsi:type="StringProperty" Name="SchemaVersion" Value="2" />

<Property xsi:type="StringProperty" Name="OsType" Value="Windows" />

<Property xsi:type="BooleanProperty" Name="persistWBC" Value=true />

<Property xsi:type="BooleanProperty" Name="persistOsDisk" Value=true />

<Property xsi:type="StringProperty" Name="StorageTypeAtShutdown"
Value="Standard_LRS" />

</CustomProperties>'



$ProvScheme = Get-Provscheme -ProvisioningSchemeName $CatalogName
```

```
Set-ProvScheme -ProvisioningSchemeName $ProvScheme.ProvisioningSchemeName
-CustomProperties $customProperties
```

既存のVMのストレージタイプをシャットダウン時に下位層に変更する

手順を進める前に、要件と制限を参照してください。

VMがシャットダウンされているときに、既存のVMのストレージタイプを下位の層に変更することで、ストレージコストを節約できます。これを行うには、`StorageTypeAtShutdown`カスタムプロパティを使用します。

VMのシャットダウン時に、カタログ内の既存マシンのストレージタイプを下位層に変更するには：

1. PowerShellウィンドウを開きます。
2. Citrix固有のPowerShellモジュールをロードするために、`asnp citrix*`を実行します。
3. `Get-Provscheme -ProvisioningSchemeName $CatalogName`を実行します。
4. カスタムプロパティ文字列を変更します。

   ```
   $customProperties = '<CustomProperties xmlns="http://
   schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http://
   www.w3.org/2001/XMLSchema-instance">

   <Property xsi:type="StringProperty" Name="StorageTypeAtShutdown"
   Value="Standard_LRS" />

   </CustomProperties>'
   ```

5. 既存のカタログのプロビジョニングスキームを更新します。この更新は、`Set-ProvScheme`の実行後に追加された新しいVMに適用されます。

   ```
   Set-ProvScheme -ProvisioningSchemeName $CatalogName -CustomProperties
   $customProperties
   ```

6. 既存のVMを更新して`StorageTypeAtShutdown`を有効にします。

   ```
   Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName $CatalogName
   -StartsNow -DurationInMinutes -1
   ```

7. 次回マシンを起動すると、マシンの`StorageTypeAtShutdown`プロパティが更新されます。ストレージタイプは次回のシャットダウン時に変更されます。
8. カタログ内の各VMの`StorageTypeAtShutdown`値を表示するには、次のコマンドを実行します。

```
Get-ProvVM -ProvisioningSchemeName <catalog-name> | foreach { $vmName =
$_.VMName; $storageTypeAtShutdown = ($_.CustomVmData | ConvertFrom-
Json).StorageTypeAtShutdown.DiskStorageAccountType; return New-Object
psobject -Property @{ "VMName" = $vmName; "StorageTypeAtShutdown" =
$storageTypeAtShutdown } }
```

プロビジョニングされたマシンを現在のプロビジョニングスキームの状態に更新する

`Set-ProvScheme`コマンドはプロビジョニングスキームを変更します。ただし、既存のマシンには影響しません。PowerShellコマンド`Set-ProvVMUpdateTimeWindow`を使用すると、現在のプロビジョニングスキームを既存の永続的または非永続的なマシン、またはマシンのセットに適用できます。また、既存のMCSプロビジョニング済みマシンの構成更新のタイムスロットをスケジュールすることもできます。スケジュールされたタイムスロット中の電源オンまたは再起動は、スケジュールされたプロビジョニングスキームの更新をマシンに適用します。現在、Azureでは、`ServiceOffering`、`MachineProfile`、および次のカスタムプロパティを更新できます。

- `StorageType`
- `WBCDiskStorageType`
- `IdentityDiskStorageType`
- `LicenseType`
- `DedicatedHostGroupId`
- `PersistWBC`
- `PersistOsDisk`
- `PersistVm`

注：

- Azure環境でマネージドディスクを使用するカタログの場合、`StorageType`、`WBCDiskStorageType`、および`IdentityDiskStorageType`カスタムプロパティのみを更新できます。

- `Set-ProvVMUpdateTimeWindow`を2回実行した場合、最新のコマンドが有効になります。

更新できるもの:

- 単一のVM
- 特定のVMのリスト、またはプロビジョニングスキームIDに関連付けられている既存のすべてのVM
- 特定のVMのリスト、またはプロビジョニングスキーム名（マシンカタログ名）に関連付けられている既存のすべてのVM

プロビジョニングスキームに以下の変更を加えると、Azureの永続カタログの場合、VMインスタンスが再作成されます:

- `MachineProfile`を変更する
- 削除 `LicenseType`
- 削除 `DedicatedHostGroupId`

注：

既存のマシンのOSディスクとそのすべてのデータはそのまま残り、新しいVMがそのディスクに接続されます。

既存のVMを更新する前に:

1. 既存のマシンの構成を確認します。例えば、,

   ```
   Get-ProvScheme | select ProvisioningSchemeName,
   ProvisioningSchemeVersion
   ```

2. プロビジョニングスキームを更新します。例えば、,

   - マシンプロファイルの入力としてVMを使用する場合:

```
Set-ProvScheme -ProvisioningSchemeName "my-catalog" -MachineProfile
"XDHyp:\HostingUnits\<hosting-unit>\machineprofile.folder\<resource-
group>.resourcegroup\<virtual-machine>.vm"
```

- マシンプロファイルの入力としてテンプレート仕様を使用する場合:

```
Set-ProvScheme -ProvisioningSchemeName "my-catalog"

-MachineProfile "XDHyp:\HostingUnits\<hosting-
unit>\machineprofile.folder\<resource-
group>.resourcegroup\<template-spec>.templatespec\<template-spec-
version>.templatespecversion"

-ServiceOffering "XDHyp:\HostingUnits\<hosting-
unit>\serviceoffering.folder\<service-offering>.serviceoffering"
```

- サービス提供のみの場合:

```
Set-ProvScheme -ProvisioningSchemeName "my-catalog" -ServiceOffering
"XDHyp:\HostingUnits\<hosting-unit>\serviceoffering.folder\<service-
offering>.serviceoffering"
```

3. VMの現在のプロパティが現在のプロビジョニングスキームと一致しているか、およびVMに保留中の更新アクションがあるかを確認します。例えば、,

```
Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
ProvisioningSchemeVersion
```

特定のバージョンのマシンを見つけることもできます。例えば、,

```
Get-ProvVM -Filter "ProvisioningSchemeVersion -eq 1" | select VMName,
ProvisioningSchemeVersion
```

既存のマシンに次回の再起動時に適用される更新を要求するには:

1. 既存のマシンを更新し、次回の再起動時に更新が適用されるようにするには、次のコマンドを実行します。

   - すべての既存のマシンを更新するには。例えば、,

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
-StartsNow -DurationInMinutes -1
```

- 特定の仮想マシンのリストを更新する場合。例：

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
-VMName <List-Of-Vm-Names> -StartsNow -DurationInMinutes -1
```

- Get-ProvVM の出力に基づいてマシンを更新する場合。例：

```
Get-ProvVM -ProvisioningSchemeName "my-catalog" | Set-
ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog -StartsNow
-DurationInMinutes -1
```

注：

- `StartsNow` は、スケジュールされた開始時刻が現在の時刻であることを示します。
- 負の数（例：–1）の `DurationInMinutes` は、スケジュールの時間枠に上限がないことを示します。

2. 更新がスケジュールされているマシンを見つける。例：

```
Get-ProvVM -Filter "ProvisioningSchemeUpdateAfter" | select VMName,
ProvisioningSchemeUpdateAfter
```

3. マシンを再起動します。次回の電源投入時に、プロパティの変更が既存のマシンに適用されます。以下のコマンドを使用して、更新されたステータスを確認できます。例：

```
Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
ProvisioningSchemeVersion
```

スケジュールされた時間枠内で次回起動時に最新のプロビジョニング設定に更新するようにVMをスケジュールするには：

1. 次のコマンドを実行します。

- 開始時刻を現在時刻として更新をスケジュールするには

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
-VMName vm1 -StartsNow -DurationInMinutes 120
```

- 週末に更新をスケジュールするには

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName “ my-catalog “
-VMName “vm1” -StartTimeInUTC “10/15/2022 9:00am” -DurationInMinutes
(New –TimeSpan –Days 2).TotalMinutes
```

注：

- `VMName` はオプションです。指定しない場合、更新はカタログ全体に対してスケジュールされます。
- `StartTimeInUTC` の代わりに `StartsNow` を使用して、スケジュール開始時刻が現在時刻であることを示します。
- `DurationInMinutes` はオプションです。デフォルトは120分です。負の数（例：–1）は、スケジュールの時間枠に上限がないことを示します。

2. 更新ステータスを確認します。

```
Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
ProvisioningSchemeUpdateUntil, ProvisioningSchemeVersion
```

3. VM の電源を入れます。スケジュールされた時間枠の後にマシンの電源を入れた場合、構成の更新は適用されません。スケジュールされた時間枠内にマシンの電源を入れた場合、,

- マシンがオフになっていて、
  - マシンを起動しない場合、構成の更新は適用されません
  - マシンを起動すると、構成の更新が適用されます
- マシンの電源が入っていて、
  - マシンを再起動しない場合、構成の更新は適用されません

    - マシンを再起動すると、構成の更新が適用されます。

構成の更新をキャンセルするには：

単一のVM、複数のVM、またはカタログ全体の構成更新をキャンセルすることもできます。構成更新をキャンセルするには：

1. `Clear-ProvVMUpdateTimeWindow` を実行します。例：

    - 単一のVMに対してスケジュールされた構成更新をキャンセルするには：

    ```
    Clear-ProvVMUpdateTimeWindow -ProvisioningSchemeName “ my-catalog “
    -VMName “vm1”
    ```

    - 複数のVMに対してスケジュールされた構成更新をキャンセルするには：

    ```
    Clear-ProvVMUpdateTimeWindow -ProvisioningSchemeName "my-catalog"
    -VMName "vm1","vm2"
    ```

    > **注：**
    >
    > VM は同じカタログのものである必要があります。

個々のVMのプロパティを更新する

永続的なMCSマシンカタログ内の個々のVMのプロパティは、PowerShellコマンド `Set-ProvVM` を使用して更新できます。ただし、更新はすぐに適用されません。更新を適用するには、PowerShellコマンド `Set-ProvVMUpdateTimeWindow` を使用して時間枠を設定する必要があります。

この実装により、マシンカタログ全体を更新することなく、個々のVMを効率的に管理できます。現在、この機能はAzure環境にのみ適用されます。

現在、更新できるプロパティは次のとおりです。

- `CustomProperties`
- `ServiceOffering`
- `MachineProfile`

この機能を使用すると、次のことができます。

- VMのプロパティを更新する
- マシンカタログの更新後もVMで更新されたプロパティを保持する
- VMに適用された構成の更新を元に戻す

VMのプロパティを更新する前に：

1. **PowerShell**ウィンドウを開きます。
2. Citrix固有のPowerShellモジュールをロードするために`asnp citrix*`を実行します。
3. 既存のマシンカタログの構成を確認します。例：

```
Get-ProvScheme -ProvisioningSchemeName AzureCatalog
```

4. 更新を適用するVMの構成を確認します。例：

```
Get-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
```

VMのプロパティを更新する

VMのプロパティを更新するには、次の手順を実行します。

1. 更新を適用したいVMの電源をオフにします。
2. VMのプロパティを更新します。例えば、VMのストレージタイプ (`StorageType`) カスタムプロパティを更新したい場合は、以下を実行します。

```
Set-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
-CustomProperties "...<Property Name='StorageType'
Value='Premium_LRS' />..."
```

マシンカタログ内の2つのVMのプロパティを同時に更新できます。例:

```
Set-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
-CustomProperties "...<Property Name='StorageType'
Value='Premium_LRS' />..."
```

```
Set-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine2
-CustomProperties "...<Property Name='StorageType'
Value='StandardSSD_LRS' />..."
```

> **注：**
>
> 更新はすぐに適用されません。

3. 更新対象として指定されたプロパティのリストと構成バージョンを取得します。例:

```
Get-ProvVMConfiguration -ProvisioningSchemeName AzureCatalog -VMName
machine1
```

`Version` のプロパティ値と、更新対象のプロパティ (この場合は `StorageType`) を確認します。

4. 構成バージョンを確認します。例:

```
Get-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
```

`ProvVMConfigurationVersion` のプロパティ値を確認します。更新はまだ適用されていません。VMはまだ古い構成のままです。

5. スケジュールされた更新を要求します。例:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName AzureCatalog
-StartsNow -DurationInMinutes -1
```

スケジュールされた更新の詳細については、プロビジョニングされたマシンを現在のプロビジョニングスキームの状態に更新する を参照してください。

> **注：**
>
> 保留中のプロビジョニングスキームの更新も適用されます。

6. VMを再起動します。例:

```
New-BrokerHostingPowerAction -MachineName machine1 -Action TurnOn
```

7. 構成バージョンを確認します。例:

```
Get-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
```

`ProvVMConfigurationVersion` のプロパティ値を確認します。更新が適用されました。VMは新しい構成になりました。

8. VMにさらに構成アップデートを適用するには、VMをオフにして、手順を繰り返します。

マシンカタログの更新後にVMで更新されたプロパティを保持する

VMで更新されたプロパティを保持するには、以下を実行します。

1. 更新を適用したいVMの電源をオフにします。
2. マシンカタログを更新します。たとえば、VMサイズ (`ServiceOffering`) とストレージタイプ (`StorageType`) を変更したい場合は、以下を実行します。

```
Set-ProvScheme -ProvisioningSchemeName AzureCatalog -ServiceOffering
Standard_E4_v3 -CustomProperties "...<Property Name='StorageType'
Value='StandardSSD_LRS' />..."
```

3. マシンカタログの構成詳細を取得します。例:

```
Get-ProvScheme -ProvisioningSchemeName AzureCatalog
```

`ProvisioningSchemeVersion` が1つ増えました。VMサイズとストレージタイプも更新されます。

4. VMのプロパティを更新します。たとえば、VMにマシンプロファイルを提供します。

```
Set-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
-MachineProfile "XDHyp:\HostingUnits\<hosting-
unit>\machineprofile.folder\<resource-group>.resourcegroup\<template-
spec>.templatespec\<template-spec-version>.templatespecversion"
```

注：

マシンプロファイルの入力には、タグと異なるVMサイズ (`ServiceOffering`) が指定されています。

5. VM上の構成アップデートとマシンカタログのアップデートをマージした後にVMが持つプロパティのリストを取得します。例:

```
Get-ProvVMConfigurationResultantSet -ProvisioningSchemeName
AzureCatalog -VMName machine1
```

> **注：**
>
> VMに対するすべてのアップデートは、マシンカタログで行われたアップデートを上書きします。

6. VMのスケジュールされたアップデートを要求します。例:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName AzureCatalog -VMName
machine1 -StartsNow -DurationInMinutes -1
```

7. VMを再起動します。例:

```
New-BrokerHostingPowerAction -MachineName machine1 -Action TurnOn
```

   VMは、マシンプロファイルから派生した更新済みのVMサイズを保持します。マシンプロファイルで指定されたタグ値もVMに適用されます。ただし、ストレージタイプは最新のプロビジョニングスキームから派生します。

8. VMの構成バージョンを取得します。例:

```
Get-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
```

   `ProvisioningSchemeVersion` と `ProvVMConfigurationVersion` に最新バージョンが表示されます。

VMに適用された構成の更新を元に戻す

1. VMに更新を適用した後、VMをシャットダウンします。
2. 次のコマンドを実行して、VMに適用された更新を削除します。例:

```
Set-ProvVM -RevertToProvSchemeConfiguration -ProvisioningSchemeName
AzureCatalog -VMName machine1
```

3. VMのスケジュールされたアップデートを要求します。例:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName AzureCatalog -VMName
machine1 -StartsNow -DurationInMinutes -1
```

4. VMを再起動します。例:

```
New-BrokerHostingPowerAction -MachineName machine1 -Action TurnOn
```

5. VMの構成バージョンを確認します。例:

```
Get-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
```

`ProvVMConfigurationVersion` の値が、マシンカタログの構成バージョンになります。

Azure VM、スナップショット、OS ディスク、およびギャラリーイメージ定義の情報を取得する

OSディスクと種類、スナップショット、ギャラリーイメージ定義を含むAzure VMの情報を表示できます。この情報は、マシンカタログが割り当てられている場合、マスターイメージ上のリソースに対して表示されます。この機能を使用して、LinuxまたはWindowsイメージを表示および選択します。PowerShellプロパティ`TemplateIsWindowsTemplate`が`AdditionDatafield`パラメーターに追加されました。このフィールドには、VMタイプ、OSディスク、ギャラリーイメージ情報、OSタイプ情報など、Azure固有の情報が含まれています。`TemplateIsWindowsTemplate`を**True**に設定するとOSタイプがWindowsであることを示し、`TemplateIsWindowsTemplate`を**False**に設定するとOSタイプがLinuxであることを示します。

ヒント:

`TemplateIsWindowsTemplate` PowerShell プロパティによって表示される情報は、Azure API から派生しています。このフィールドが空の場合があります。たとえば、データディスクからのスナップショットには `TemplateIsWindowsTemplate` フィールドが含まれていません。これは、OS の種類をスナップショットから取得できないためです。

たとえば、PowerShell を使用して、Windows OS の種類に対して Azure VM `AdditionData` パラメーターを **True** に設定します。

```
PS C:\Users\username> (get-item XDHyp:
\HostingUnits\mynetwork\image.folder\username-dev-testing-
rg.resourcegroup\username-dev-tsvda.vm).AdditionalData

Key Value

ServiceOfferingDescription Standard_B2ms

HardDiskSizeGB 127

ResourceGroupName FENGHUAJ-DEV-TESTING-RG

ServiceOfferingMemory 8192

ServiceOfferingCores 2

TemplateIsWindowsTemplate True

ServiceOfferingWithTemporaryDiskSizeInMb 16384

SupportedMachineGenerations Gen1,Gen2
```

MCSによって作成されたリソースを識別する

以下は、MCSがリソースに追加するタグです。表のタグは「"key":"value"」として表されます。

リソース名	タグ
ID ディスク	"Citrixプロビジョニングスキーム ID" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	"CitrixResource" : "内部"
イメージ	"Citrixプロビジョニングスキーム ID" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	"CitrixResource" : "内部"

リソース名	タグ
NIC	"CitrixプロビジョニングスキームID" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	"CitrixResource" : "内部"
OSディスク	"CitrixプロビジョニングスキームID" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	"CitrixResource" : "内部"
PrepVM	"CitrixプロビジョニングスキームID" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	"CitrixResource" : "内部"
公開スナップショット	"CitrixプロビジョニングスキームID" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	"CitrixResource" : "内部"
リソースグループ	"CitrixResource" : "内部"
	CitrixSchemaVersion: 2.0
	"CitrixプロビジョニングスキームID" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
ストレージアカウント	"CitrixプロビジョニングスキームID" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	"CitrixResource" : "内部"
カタログ内のVM	"CitrixプロビジョニングスキームID" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	"CitrixResource" : "内部"
WBCディスク	"CitrixプロビジョニングスキームID" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	"CitrixResource" : "内部"

注：

MCSによって作成されたリソースとして識別するために**CitrixResource**タグが追加されている場合、VMはCitrixインベントリに表示されません。タグを削除または名前変更することで、表示させることができます。

詳細情報

- 接続とリソースの作成および管理
- Microsoft Azureへの接続
- マシンカタログの作成
- Microsoft Azureカタログの作成
- マシンカタログの管理

Microsoft System Center Virtual Machine Manager カタログを管理する

マシンカタログの管理では、マシンカタログを管理するウィザードについて説明します。以下の情報は、Microsoft System Center Virtual Machine Manager (VMM) 仮想化環境に固有の詳細を扱っています。

注：

VMMカタログを管理する前に、VMMカタログの作成を完了する必要があります。Microsoft System Center Virtual Machine Managerカタログの作成を参照してください。

MCSによって作成されたリソースを識別する

以下は、MCS がリソースに追加するタグです。表のタグは「"key":"value"」として表されます。

リソース名	タグ
準備用 VM	タグ文字列は以下のとおりです: "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	カスタムプロパティエントリ: "XdConfig:"XdProvisioned=True"

リソース名	タグ
カタログ内のVM	タグ文字列は以下のとおりです: "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	カスタムプロパティエントリ: "XdConfig:"XdProvisioned=True"

詳細情報

- 接続とリソースの作成および管理
- マイクロソフト システムセンター バーチャルマシンマネージャー への接続
- マシンカタログの作成
- Microsoft System Center Virtual Machine Manager カタログを作成する
- マシンカタログの管理

VMwareカタログの管理

マシンカタログの管理では、マシンカタログを管理するウィザードについて説明します。以下の情報は、VMware仮想化環境に固有の詳細を扱っています。

> **注:**
>
> VMwareカタログを管理する前に、VMwareカタログの作成を完了する必要があります。「VMwareカタログを作成する」を参照してください。

マシンカタログのフォルダーIDを更新する

MCSマシンカタログのフォルダーIDは、`Set-ProvScheme`コマンドのカスタムプロパティで`FolderId`を指定することで更新できます。フォルダーIDの更新後に作成されたVMは、この新しいフォルダーIDの下に作成されます。このプロパティが`CustomProperties`で指定されていない場合、VMはマスターイメージが配置されているフォルダーの下に作成されます。

マシンカタログのフォルダーIDを更新するには、次の手順を実行します。

1. Webブラウザーを開き、**vSphere Web Client**のURLを入力します。
2. 資格情報を入力し、**ログイン**をクリックします。

3. **vSphere Web Client**でVM配置フォルダーを作成します。
4. PowerShellウィンドウを開きます。
5. **asnp citrix®***を実行して、Citrix固有のPowerShellモジュールをロードします。
6. `Set-ProvScheme`の`CustomProperties`で`FolderID`を指定します。この例では、フォルダーIDの値は`group-v2406`です。

```
Set-ProvScheme -ProvisioningSchemeUid
"50bb319c-2e83-4a37-9ea1-94f630687372" -CustomProperties
"<CustomProperties xmlns=""http://schemas.citrix.com/2014/xd/
machinecreation"" xmlns:xsi=""http://www.w3.org/2001/XMLSchema-
instance""><Property xsi:type=""StringProperty"" Name=""FolderId""
Value=""group-v2406"" /></CustomProperties>"
```

7. Studioを使用してマシンカタログにVMを追加します。
8. vSphere Web Clientで新しいVMを確認します。新しいVMは新しいフォルダーの下に作成されます。

vSphereでフォルダーIDを検索する

VMのフォルダーIDを見つけるには、任意のESXiまたはvCenterサーバーシステムでManaged Object Browser (MOB) にアクセスします。

MOBは、すべてのESX/ESXiおよびvCenterサーバーシステムに組み込まれているWebベースのサーバーアプリケーションです。このvSphereユーティリティを使用すると、VM、データストア、リソースプールなどのオブジェクトに関する詳細情報を表示できます。

1. Webブラウザーを開き、`http://x.x.x.x/mob`と入力します。ここで、x.x.x.xはvCenter ServerまたはESX/ESXiホストのIPアドレスです。例：`<https://10.60.4.70/mob>`。
2. MOBの**Home**ページで、プロパティ**content**の値をクリックします。
3. **rootFolder**の値をクリックします。
4. **childEntity**の値をクリックします。
5. **vmFolder**の値をクリックします。
6. フォルダーIDは**childEntity**の値にあります。

VMのストレージ移行

既存のVMのディスクストレージを古いストレージから新しいストレージに移動できます。移行中、MCSは電源管理、OSディスクのリセットなどのVM機能を保持します。新しいディスクスト

レージを使用して、新しいVMをマシンカタログに追加することもできます。これを行うには、PowerShellコマンド `Move-ProvVMDisk` を使用します。

現在、フルクローン永続VMのみを移行できます。

新しいストレージは、次の条件を満たす必要があります。

- 古いストレージと同じクラスター内にある必要があります。
- VMが実行されているホストは、古いデータストアと新しいデータストアの両方にアクセスできる必要があります。

次のタスクを実行できます。

- ディスクストレージの移行
- 古いストレージを非推奨にする

ディスクストレージの移行

ディスクストレージを移行するには：

1. 既存のホスティングユニットに新しいストレージを追加します。古いストレージを**Superseded**に変更します。これはWeb StudioまたはPowerShellコマンドを使用して実行できます。
    - Web Studioを使用する場合は、ストレージの編集を参照してください。
    - PowerShellコマンドを使用する場合：
        - 既存のホスティングユニットに新しいストレージを追加するには、`Add-Hyphostingunitstorage` を実行します。
        - 古いストレージでの新しいVM作成を無効にするには、**Superseded** を true に設定して `Set-Hyphostingunitstorage` を実行します。
2. VMをシャットダウンし、**メンテナンスモード**をオンにします。
3. VMのディスクストレージを新しいストレージに移動し、ストレージ情報を更新します。例:

```
Move-ProvVMDisk -ProvisioningSchemeName "myFullCloneProvScheme" -VMName
("VMware-TestVM01", "VMware-TestVM02") -DiskType OS,Identity
-DestinationStorageId datastore1,datastore1
```

4. 移行のタスクIDを取得します。例:

```
,(Get-ProvVM -ProvisioningSchemeName xxxxx) | Move-ProvVMDisk
-ProvisioningSchemeName xxxxx -DiskType OS,Identity
-DestinationStorageId datastore1,datastore1
```

5. 移行のステータスを確認します。

   - `(Get-ProvTask -TaskID xxxxxxxxx).DiskMovedVirtualMachines`: ディスク移行が成功したVMのリストを提供します。これには、すでに新しいストレージに移行されたVMも含まれます。
   - `(Get-ProvTask -TaskID xxxxxxxxx).DiskMoveFailedVirtualMachines`: 移行に失敗したVMのリストを提供します。
   - `(Get-ProvTask -TaskID xxxxxxxxx).NotStartedVirtualMachines`: 移行がまだ開始されていないVMのリストを提供します。
   - `Get-ProvVM -ProvisioningSchemeName xxxxx -VMName "VMware-TestVM01`: 移行後の更新されたVMプロパティを提供します。`StorageId`、`AssignedImage`、`BootedImage`、`IdentityDiskId`、`IdentityDiskStorage`、`LastBootTime` などのプロパティを確認してください。

スナップショット付きのMCSで作成されたVMのディスクを移行した後、**Consolidation is required in the VSphere Client** という警告が表示されることがあります。統合してデータ損失を回避するには:

1. VMware VMのバックアップを取ります。たとえば、すべてのVMファイルをデータストア上の別のフォルダーに転送します。
2. 警告が表示されたら、**Consolidate** をクリックし、**OK** をクリックして統合を確定します。

古いストレージの廃止

VMディスク移行後に古いストレージを廃止するには:

1. ホスティングユニットの各ディスクストレージにおけるベースディスクとマシン数の情報を取得します。例:

```
$result=Get-ProvSchemeResourceInStorage -ProvisioningSchemeName xxxxx

$result

$result.ProvResourceInStorage | Format-List -Property *
```

移行が成功すると、MCS は古いベースディスクを自動的に削除し、古いストレージにはマシンが存在しなくなります。したがって、コマンドの実行後、古いストレージにマシンとベースディスクが存在しないことを確認してください。

2. ホスティングユニットから古いストレージを完全に削除するには、`Remove-Hyphostingunitstorage` を実行します。Web Studio を使用して古いストレージを削除することもできます。

MCSによって作成されたリソースを識別する

以下は、MCS がリソースに追加するタグです。表のタグは「"key":"value"」として表されます。

リソース名	タグ
準備用 VM	"Citrixプロビジョニングスキーム ID": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	"XdConfig:"XdProvisioned=真"
カタログ内のVM	"Citrixプロビジョニングスキーム ID": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	"XdConfig:"XdProvisioned=真"

詳細情報

- 接続とリソースの作成および管理
- VMwareへの接続
- マシンカタログの作成
- VMwareカタログを作成する
- マシンカタログの管理

電源管理

Citrix Virtual Apps and Desktops™ を使用すると、さまざまなサポート対象のハイパーバイザーとクラウドサービスで、MCSプロビジョニングされたVMの電源管理を行うことができます。電源管理操作により、以下が提供されます。

- 最適なユーザーエクスペリエンス
- コスト管理と電力節約

利用可能な電源操作は次のとおりです。

- 起動
- シャットダウン
- 再起動
- 一時停止
- 再開
- 強制再起動
- 強制シャットダウン

> **注：**
>
> - 非永続VMの場合、電源サイクル（シャットダウン/起動および再起動）によりOSディスクがリセットされます。
> - 電源操作の機能と動作は、ハイパーバイザーまたはクラウドサービスによって異なります。

> この記事では、特定のサポート対象ハイパーバイザーに関連する主要な電源管理機能について説明します。

- AWS VMの電源管理
- Azure VMの電源管理

AWS VM の電源管理

必要な権限については、必要なAWS権限を参照してください。

インスタンスの休止

休止プロセスは、インスタンスのインメモリ状態と、プライベート IP アドレスおよび Elastic IP アドレスを保存し、中断したところから正確に再開できるようにします。

インスタンスに休止が指示されると、インメモリ状態をルート EBS ボリューム内のファイルに書き込み、その後シャットダウンします。Amazon EBS ボリュームは、インスタンスにアタッチできる耐久性のあるブロックレベルストレージデバイスです。ボリュームをインスタンスにアタッチすると、物理ハードドライブと同じように使用できます。インスタンスのルート EBS ボリューム

を暗号化します。暗号化により、メモリから EBS ボリュームにコピーされる機密データが適切に保護されます。EBS 暗号化の詳細については、「Amazon EBS 暗号化」を参照してください。

サポートされているインスタンス休止の制限事項は次のとおりです。

- 最大 150 GB までのインスタンスメモリ (RAM) のみがサポートされます
- UEFI ブートモードはサポートされていません
- 汎用 SSD とプロビジョンド IOPS SSD のみが EBS ボリュームタイプとしてサポートされます。

休止をサポートする VM の作成

休止をサポートする VM を作成するには：

1. ホスト接続を作成します。「AWS への接続」を参照してください。
2. EBSルートが暗号化され、**Stop-Hibernate**プロパティが有効になっているインスタンスを起動します。インスタンスの起動方法、ルートEBSボリュームの暗号化、および休止状態の有効化の詳細については、`<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/launching-instance.html/>`を参照してください。このインスタンスをマスターイメージとして使用してAMIを作成します。
3. マスターイメージを準備します。
    a. マスターイメージに VDA をインストールします。Citrix では、最新機能にアクセスできるように、最新バージョンをインストールすることをお勧めします。マスターイメージに VDA をインストールしないと、カタログ作成が失敗します。VDA のインストール方法の詳細については、「VDA のインストール」を参照してください。
    b. マスターイメージを、アプリケーションとデスクトップが属するドメインに参加させます。マスターイメージが、マシンが作成されるホストで利用可能であることを確認してください。
4. そのインスタンスから AMI を作成します。インスタンスから AMI を作成する方法については、「Amazon EC2 インスタンスから AMI を作成する」を参照してください。
5. `New-ProvScheme` コマンドを使用してマシンカタログを作成します。`AwsCaptureInstanceProperties` カスタムプロパティを **True** に設定します。

```
New-ProvScheme  -AdminAddress "xxx" -CleanOnBoot

-CustomProperties "AwsCaptureInstanceProperties,true;"

-HostingUnitName "xxx" -IdentityPoolName $catalog_name
```

```
-InitialBatchSizeHint 1

-MasterImageVM "xyz.template" -NetworkMapping @{"0"="XDHyp:
\HostingUnits\MyConn\\us-east-2a.availabilityzone\10.0.0.0``/24
(vpc-0f1771e45671aedcd).network"}

-ProvisioningSchemeName $catalog_name

-RunAsynchronously -Scope @() -SecurityGroup @("xxx") -ServiceOffering
"xxx"
```

PowerShell コマンドを使用してマシンカタログを作成する方法については、`<https://developer-docs.citrix.com/projects/citrix-daas-sdk/en/latest/>` を参照してください。

ハイバネート可能な VM は、次の場合に作成されます。

- **Stop-Hibernate** プロパティが有効になっているマスターイメージから作成された AMI を選択した場合。
- マスター VM がドメインに参加しており、VDA がインストールされている場合。
- 休止状態を処理できる正しいVMサイズ（サービス提供）を選択します。

次の場合、**New-ProvScheme**コマンドは適切なエラーメッセージを表示して失敗します。

- マスターVMは休止状態が有効になっていますが、サービス提供は休止状態を処理できません。
- マスターVMがドメインに参加しておらず、VDAがインストールされていない場合。

サービス提供とAMIの休止状態

サービス提供とAMI（テンプレート）の休止状態を取得するには、次のコマンドを実行します。

- `Get-HypConfigurationObjectForItem 'XDHyp:\HostingUnits\MyConn\WIN2016-ADDC-2021.09.10.145334-a1968709-10c4-47d5-9642-21e743159a7b (ami-0e6c5b33a52d2a6b6).template'`
- `Get-HypConfigurationObjectForItem 'XDHyp:\HostingUnits\MyConn\R6i Sixteen Extra Large Instance.serviceoffering'`

既存の休止状態対応プロビジョニングスキームのサービス提供を更新する

1. `Set-ProvScheme`コマンドを実行します。例：

```
Set-ProvScheme -ProvisioningSchemeName <String> -ServiceOffering
<String>
```

サービス提供に互換性がない場合、システムは例外メッセージを表示します。

休止状態をサポートするマシンカタログを更新する

既存のマシンカタログを休止状態をサポートしないマシンカタログで更新しようとすると、適切なエラーメッセージが表示されて更新が失敗します。

休止状態のVMの電源管理

休止状態のVMに対して、以下の電源管理操作を実行できます。

1. 実行中の状態からVMをサスペンドします。
2. 一時停止状態からVMを再開します。
3. 一時停止状態からVMを再起動します。

Azure VM の電源管理

必要な権限については、「必要な Azure 権限」を参照してください。

Azure オンデマンドプロビジョニング

Azureオンデマンドプロビジョニングでは、VMはプロビジョニングが完了した後、Citrix Virtual Apps and Desktops™が電源オンアクションを開始したときにのみ作成されます。

MCS を使用して Azure Resource Manager でマシンカタログを作成する場合、Azure オンデマンドプロビジョニング機能は次のとおりです。

- ストレージコストを削減します
- カタログ作成を高速化します

MCS カタログを作成すると、Azure portal にリソースグループ内のネットワークセキュリティグループ、ネットワークインターフェイス、ベースイメージ、およびIDディスクが表示されます。

Azureポータルには、Citrix Virtual Apps and DesktopsがVMの電源オンアクションを開始するまでVMは表示されません。マシンには次の違いを持つ2つのタイプがあります。

- プールされたマシンの場合、オペレーティングシステムディスクとライトバックキャッシュはVMが存在する場合にのみ存在します。コンソールでプールされたマシンをシャットダウンすると、VMはAzureポータルに表示されません。定期的にマシンをシャットダウンする場合（たとえば、勤務時間外）、ストレージコストを大幅に節約できます。

- 専用マシンの場合、オペレーティングシステムディスクはVMが最初に電源オンされたときに作成されます。AzureポータルのVMは、マシンIDが削除されるまでストレージに残ります。コンソールで専用マシンをシャットダウンしても、VMはAzureポータルに表示されたままです。

> **注：**
>
> オンデマンドプロビジョニング機能の前に作成されたAzureカタログ（「レガシー」カタログ）のサポートは非推奨です。したがって、Azureレガシーカタログ VMを再作成してください。カタログはオンデマンドとしてプロビジョニングされ、ストレージコストを節約できます。

電源サイクル時にプロビジョニングされた仮想マシンを保持する

電源サイクル時にプロビジョニングされた仮想マシンを保持するかどうかを選択します。PowerShellパラメーター `New-ProvScheme CustomProperties` を使用します。このパラメーターは、電源サイクル時にプロビジョニングされた仮想マシンが保持されるかどうかを決定するために使用される追加のプロパティ `PersistVm` をサポートします。電源オフ時に仮想マシンを保持するには `PersistVm` プロパティを**true**に設定し、電源オフ時に仮想マシンが保持されないようにするにはプロパティを**false**に設定します。

> **注：**
>
> `PersistVm` プロパティは、 `CleanOnBoot` および `UseWriteBackCache` プロパティが有効になっているプロビジョニングスキームにのみ適用されます。非永続仮想マシンに対して `PersistVm` プロパティが指定されていない場合、それらは電源オフ時にAzure環境から削除されます。

> 「次の例では、 `New-ProvScheme CustomProperties` パラメーターは `PersistVm` プロパティを **true** に設定します。」:

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="StorageType"
Value="Standard_LRS" />
```

```
<Property xsi:type="StringProperty" Name="PersistWBC" Value="false" />

<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="true" />

<Property xsi:type="StringProperty" Name="PersistVm" Value="true" />

<Property xsi:type="StringProperty" Name="ResourceGroups" Value="demo-
resourcegroup" />

<Property xsi:type="StringProperty" Name="LicenseType"
Value="Windows_Client" />

</CustomProperties>
```

「次の例では、`New-ProvScheme CustomProperties` パラメーターは、`PersistVM` を **true** に設定することでライトバックキャッシュを保持します。」:

```
 New-ProvScheme

 -AzureAdJoinType "None"

 -CleanOnBoot

 -CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com/
2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`"><Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`"
Value=`"true`" /><Property xsi:type=`"StringProperty`"
Name=`"StorageType`" Value=`"Standard_LRS`" /><Property
xsi:type=`"StringProperty`" Name=`"PersistWBC`" Value=`"false`" /
><Property xsi:type=`"StringProperty`" Name=`"PersistOsDisk`"
Value=`"true`" /><Property xsi:type=`"StringProperty`" Name=`"PersistVm`"
Value=`"true`" /><Property xsi:type=`"StringProperty`"
Name=`"ResourceGroups`" Value=`"demo-resourcegroup`" /><Property
xsi:type=`"StringProperty`" Name=`"LicenseType`"
Value=`"Windows_Client`" /></CustomProperties>"

 -HostingUnitName "demo"

 -IdentityPoolName "NonPersistent-MCSIO-PersistVM"

 -MasterImageVM "XDHyp:\HostingUnits\demo\image.folder\scale-
test.resourcegroup\demo-snapshot.snapshot"
```

```
 -NetworkMapping @ {"0"="XDHyp:\HostingUnits\demo\
\virtualprivatecloud.folder\East US.region\virtualprivatecloud.folder\ji-
test.resourcegroup\jitest-vnet.virtualprivatecloud\default.network"}

-ProvisioningSchemeName "NonPersistent-MCSIO-PersistVM"

 -ServiceOffering "XDHyp:
\HostingUnits\demo\serviceoffering.folder\Standard_B2ms.serviceoffering"
-UseWriteBackCache

 -WriteBackCacheDiskSize 127

 -WriteBackCacheMemorySize 256
```

ヒント:

`PersistVm`プロパティは、プロビジョニングされた仮想マシンを保持するかどうかを決定します。`PersistOsdisk`プロパティは、OSディスクを永続化するかどうかを決定します。プロビジョニングされた仮想マシンを保持するには、まずOSディスクを保持します。仮想マシンを削除せずにOSディスクを削除しないでください。`PersistVm`パラメーターを指定せずに`PersistOsdisk`プロパティを使用できます。

ストレージタイプの変更失敗時の電源オン動作をカスタマイズする

電源オン時に、Azureでの障害により、管理ディスクのストレージタイプが目的のタイプに変更できない場合があります。このようなシナリオでは、VMはオフのままで、障害メッセージが送信されます。ただし、ストレージが構成されたタイプに復元できない場合でもVMの電源をオンにするか、VMをオフのままにするかを選択できます。

- カスタムプロパティ`FailSafeStorageType`を **true** (デフォルト設定) に構成した場合、または`New-ProvScheme`または`Set-ProvScheme`コマンドで指定しない場合:
  - 電源オン時に、VMは誤ったストレージタイプで電源オンされます。
  - シャットダウン時、VMは誤ったストレージタイプでオフのままになります。
- `New-ProvScheme`または`Set-ProvScheme`コマンドでカスタムプロパティ`FailSafeStorageType`を **false** に構成した場合:
  - 電源オン時に、VMは誤ったストレージタイプでオフのままになります。

- シャットダウン時、VMは誤ったストレージタイプでオフのままになります。

マシンカタログを作成するには：

1. PowerShellウィンドウを開きます。
2. Citrix固有のPowerShellモジュールをロードするには、`asnp citrix*`を実行します。
3. まだ作成されていない場合は、IDプールを作成します。
4. `New-ProvScheme`でカスタムプロパティを追加します。例：

```
New-ProvScheme -HostingUnitName "Azure-Resources-1" -IdentityPoolName
"name" -InitialBatchSizeHint 1

-MasterImageVM "XDHyp:\HostingUnits\Azure-
Resources-1\image.folder\abc.resourcegroup\def.snapshot"

-NetworkMapping @{"0"="XDHyp:\HostingUnits\Azure-
Resources-1\ght.folder\abc.resourcegroup\abc-
vnet.virtualprivatecloud\default.network"}

-ProvisioningSchemeName "name"

-ServiceOffering "XDHyp:\HostingUnits\Azure-
Resources-1\serviceoffering.folder\Standard_DS2_v2.serviceoffering"

-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com/
2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`">

<Property xsi:type=`"StringProperty`" Name=`"StorageType`"
Value=`"Premium_LRS`" />

<Property xsi:type=`"StringProperty`" Name=`"StorageTypeAtShutdown`"
Value=`"Standard_LRS`" />

<Property xsi:type=`"StringProperty`" Name=`"FailSafeStorageType`"
Value=`"true`" />

</CustomProperties>"
```

5. マシンカタログを作成します。Remote PowerShell SDKを使用してカタログを作成する方法については、`<https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/>`を参照してください。

既存のマシンカタログを更新して、`FailSafeStorageType`カスタムプロパティを含めます。この更新は既存のVMには影響しません。

1. `Set-ProvScheme`コマンドでカスタムプロパティを更新します。例：

```
Set-ProvScheme -ProvisioningSchemeName <String> -CustomProperties "

<CustomProperties xmlns=`"http://schemas.citrix.com/2014/xd/
machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-instance`">

<Property xsi:type=`"StringProperty`" Name=`"StorageType`"
Value=`"Premium_LRS`" />

<Property xsi:type=`"StringProperty`" Name=`"IdentityDiskStorageType`"
Value=`"Premium_LRS`" />

<Property xsi:type=`"StringProperty`" Name=`"FailSafeStorageType`"
Value=`"false`" />

</CustomProperties>"
```

Set-ProvSchemeで行われた変更を既存のVMに適用するには、`-StartsNow`および`-DurationInMinutes -1`パラメーターを指定して`Set-ProvVMUpdateTimeWindow`コマンドを実行します。

1. `-StartsNow`と`-DurationInMinutes -1`のパラメータを指定して`Set-ProvVMUpdateTimeWindow`コマンドを実行します。例:

   ```
   Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog -VMName
   <List-Of-Vm-Names> -StartsNow -DurationInMinutes -1
   ```

2. VMを再起動します。

休止状態対応VMを作成する

Azure環境では、休止状態をサポートするMCSマシンカタログを作成できます。この機能を使用すると、VMを中断し、ユーザーが再度サインインしたときにVMの以前の状態に再接続できます。

休止状態機能は以下に適用されます。

- シングルセッションOS
- 永続VMと非永続VM
- 静的およびランダム (プールされた) VDI デスクトップ

VDI デスクトップが静的かランダムかに関わらず、VM を休止状態にした後、同じセッションに再開できます。

このセクションでは、以下を参照してください。

- 前提条件
- 制限事項
- 休止状態対応のマシンカタログを作成および管理する
- 既存の休止状態対応 VM 用のマシンカタログを作成する
- 休止状態プロパティを確認する
- VM の電源管理 (手動および自動)

休止状態を使用するための前提条件

休止状態を使用するには、以下のタスクを完了していることを確認してください。

- Windows と Linux の両方のマスターイメージに Azure VM Agent をインストールします。Windows イメージのページファイルは一時ディスクに配置できます。マシンカタログで休止状態が有効になっている場合、MCS はページファイルの場所をベースディスクの C: ドライブに設定します。
- MCS は、生成されたリソースの休止状態プロパティを自動的に設定します。休止状態をサポートするために、マスターリソースのプロパティを構成する必要はありません。
- 休止状態をサポートするサブスクリプション内の VM サイズを使用してください。
- VM が休止状態機能を継承できるように、休止状態対応のマシンプロファイル (VM またはテンプレート仕様) を作成します。VM の作成については、休止状態の概要 を参照してください。

> **注：**
>
> Microsoftによると、OSディスクから休止状態が有効なVMを展開できます。この機能は現在一部のリージョンでサポートされており、まもなくすべてのリージョンで利用可能

> になります。詳細については、「OSディスクから休止状態が有効なVMを展開する」を参照してください。

> テンプレート仕様を作成するには、次の手順を実行します。

a. Azure Portalを開きます。テンプレートで使用する構成を持つVMを選択します。左ペインで**テンプレートのエクスポート**を選択します。
b. **パラメーターを含める**チェックボックスをオフにします。コンテキストをコピーし、JSONファイルとして保存します（例: `VMExportTemplate.json`）。
c. パラメーター`hibernationEnabled`がテンプレート上で`true`であることを確認します。パラメーターが`true`でない場合は、使用したVM構成を確認してください。テンプレートファイルでサポートされているVMサイズを指定できます。ただし、カタログ作成時にマシンサイズを指定することもできます。
d. ネットワークインターフェースリソースのテンプレートをJSONファイル`VMExportTemplate.json`に追加します。これにより、2つのリソースを持つARMテンプレートファイルが作成されます。
e. このテンプレートファイルをARMテンプレート仕様としてインポートするには、**Azure Portal > テンプレート仕様 > テンプレートのインポート > ローカルテンプレートファイルの選択**を選択します。
f. ARMテンプレート仕様が作成されたら、それをマシンプロファイルとして使用できます。

> **注：**
>
> Citrix Studioに同期されるまで数分かかる場合があります。

詳細については、Microsoftドキュメント休止状態を使用するための前提条件を参照してください。

制限事項

- シングルセッションOSマシンカタログ（永続的および非永続的）のみがサポートされています。
- エフェメラルOSディスクおよびMCS I/O機能は、Azureの休止状態をサポートしていません。
- 自動Windowsアップデート中に休止状態が失敗する可能性があります。

詳細については、Microsoftドキュメントを参照してください。

休止状態対応のマシンカタログを作成および管理する

休止状態対応のVMを作成するには、以下を使用して休止状態対応のマシンカタログを作成および管理できます。

- Web Studio、または
- PowerShellコマンド

WEB STUDIOを使用してカタログを作成する

1. **マシンカタログの作成**を選択します。カタログ作成ウィザードが開きます。
2. **マシンタイプ**ページで、このカタログの**シングルセッションOS**マシンタイプを選択します。
3. **マシン管理**ページで、次のように設定を選択します。
   a. 「**電源管理されているマシン（仮想マシンやブレードPCなど）**」を選択します。
   b. 「**Citrix Machine Creation Services™ (MCS)**」を選択します。
4. **デスクトップエクスペリエンス**ページで、必要に応じてランダムまたは静的デスクトップエクスペリエンスを選択します。
5. **イメージ**ページで、マスターイメージを選択します。「**マシンプロファイルを使用する**」チェックボックスをオンにし、ハイバネーションをサポートするマシンプロファイルを選択します。ツールヒントをクリックして、マシンプロファイルがハイバネーションをサポートしているかどうかを確認します。
6. **ストレージとライセンスの種類**ページで、このカタログに使用するストレージとライセンスを選択します。
7. **仮想マシン**ページで、VMの数、VMサイズ、およびアベイラビリティゾーンを選択します。

> **注：**
>
> ハイバネーションをサポートするマシンサイズのみが選択肢として表示されます。

8. **NIC**ページで、VMが使用するNICを追加します。
9. **ディスク設定**ページで、ライトバックキャッシュディスクのストレージの種類とサイズを選択します。
10. **リソースグループ**ページで、VMをプロビジョニングするリソースグループを選択します。
11. **マシンID**ページで、「**新しいActive Directoryアカウントを作成する**」を選択します。次に、アカウント命名スキームを指定します。

12. **ドメイン資格情報**ページで、「**資格情報を入力**」をクリックします。ターゲットのActive Directoryドメインでアカウント作成を実行するために、ドメイン資格情報を入力します。
13. 「**概要**」ページで、マシンカタログの名前を入力し、「**完了**」をクリックします。

MCSマシンカタログの作成が完了したら、カタログリストでそのカタログを見つけ、「**テンプレートプロパティ**」タブをクリックします。パラメーター「**休止状態**」の値は「**サポート対象**」である必要があります。

マシンカタログを編集する場合は、以下の制限事項を考慮してください。

- 現在のマシンカタログが休止状態をサポートしている場合、次のことはできません。
  - VMサイズを休止状態に対応していないものに変更する。
  - マシンプロファイルを休止状態に対応していないものに変更する。
- 現在のマシンカタログが休止状態をサポートしていない場合、次のことはできません。
  - 現在、Web Studioを使用してマシンプロファイルを休止状態対応のものに変更します。

既存の休止状態対応VMを管理するためのマシンカタログを作成する

既に休止状態対応VMがあり、それらを一時停止および再開したい場合は、それらのVMを電源管理のためにインポートするマシンカタログを作成します。

> **注：**
>
> 休止状態に対応しているVMと対応していないVMの両方を含むマシンカタログを作成できます。ただし、休止状態に関連する機能が必要な場合は、休止状態に対応しているVMのみを含むマシンカタログを作成する必要があります。

> Web Studioを使用して既存の休止状態対応VMのカタログを作成するには、画面の指示に従って手順を完了し、以下の主要な設定に注意してください。

1. 「**マシン管理**」ページで、「**電源管理されているマシン**」を選択し、マシンの展開方法として「**その他のサービスまたはテクノロジー**」を選択します。
2. 「**仮想マシン**」ページで、休止状態に対応しているVMのみを追加またはインポートします。

POWERSHELLコマンドを使用してマシンカタログを作成する

休止状態を使用するためのすべての要件を満たした後、`New-ProvScheme`コマンドを使用して休止状態対応のマシンカタログを作成できます。Remote PowerShell SDKを使用してカタログを作成する方法については、New-ProvSchemeを参照してください。

カタログの作成中に、以下のPowerShellコマンドを使用して、VMサイズとマシンプロファイルが休止状態をサポートしているかどうかを確認できます。

- VMサイズの場合、次のコマンドを実行し、プロパティ`supportsHibernation`が**True**であるかどうかを確認します。例：

```
Get-ChildItem -AdminAddress "MyDDC.MyDomain.local" -LiteralPath
@("XDHyp:\HostingUnits\ <VirtualNetwork> \serviceoffering.folder") |
select Name, AdditionalData | ConvertTo-Json
```

- マシンプロファイルの場合、次のコマンドを実行し、プロパティ`supportsHibernation`が**True**であるかどうかを確認します。例：

```
Get-ChildItem -AdminAddress "MyDDC.MyDomain.local" -LiteralPath
@("XDHyp:\HostingUnits\ <VirtualNetwork>
\machineprofile.folder\abc.resourcegroup")|select Name, AdditionalData|
ConvertTo-Json
```

マシンカタログを編集する場合は、次の制限事項を考慮してください。

- 現在のマシンカタログが休止状態をサポートしている場合、次のことはできません。
  - VMサイズを休止状態非対応のものに変更する
  - マシンプロファイルを休止状態非対応のものに変更する
- 現在のマシンカタログが休止状態をサポートしていない場合、次のことはできません。
  - 現在、Web Studioを使用してマシンプロファイルを休止状態対応のものに変更します。

Remote PowerShell SDKを使用してカタログのVMサイズとマシンプロファイルを変更する方法については、`<https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/MachineCreation/Set-ProvScheme/>`を参照してください。

休止状態プロパティの確認

PowerShellコマンドを使用して、マシンカタログ、VM、およびブローカーマシンの休止状態プロパティを確認できます。

- プロビジョニングスキームの休止状態プロパティを確認するには、次のPowerShellコマンドを実行します。`HibernationEnabled`パラメーターは`True`である必要があります。

```
(Get-ProvScheme -provisioningSchemeName <YourSchemeName>).VMMetadata
-join "" |  ConvertFrom-Json | Select HibernationEnabled
```

- プロビジョニングVMの休止状態プロパティを確認するには、次のPowerShellコマンドを実行します。`SupportsHibernation`パラメーターは`True`である必要があります。

```
(Get-ProvVM -VMName <YourVMName>).CustomVmData | ConvertFrom-Json |
Select SupportsHibernation
```

- ブローカーマシンの休止状態容量を確認するには、次のPowerShellコマンドを実行します。**Suspend** および **Resume** の電源アクションは、休止状態機能を示します。

```
(Get-BrokerMachine -MachineName
<YourMachineName>).SupportedPowerActions
```

休止状態対応VMの電源管理

休止状態対応VMに対して、以下の電源管理操作を実行できます。

- 実行状態からVMを**一時停止**する
- 一時停止状態からVMを**再開**する
- 一時停止状態からVMを**強制シャットダウン**する
- 一時停止状態からVMを**強制再起動**する

詳細については、以下を参照してください。

- 一時停止
- 再開

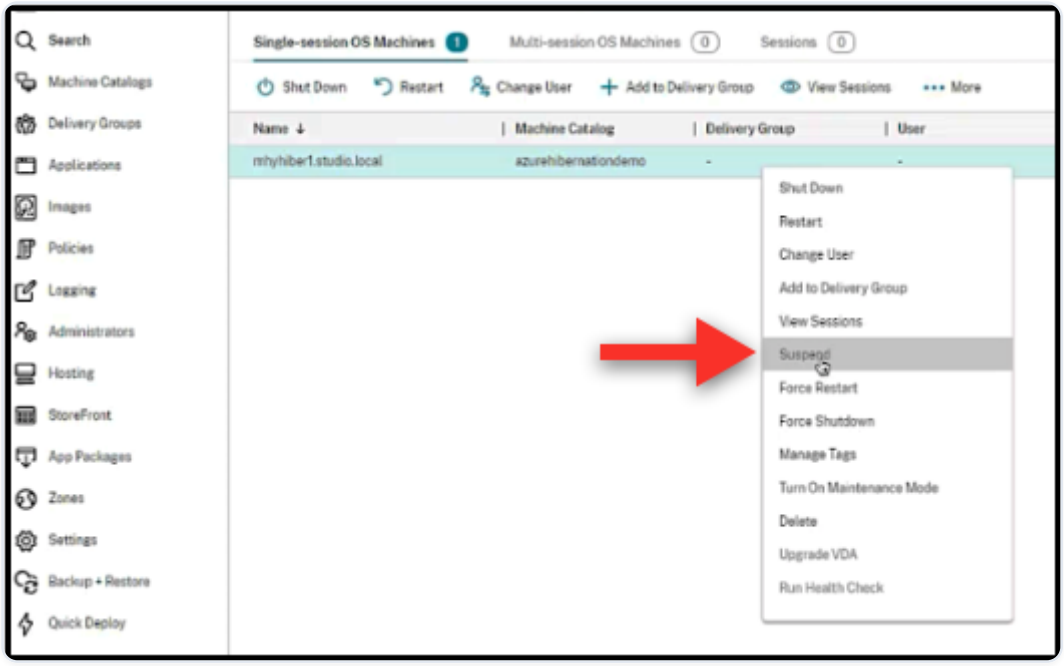
一時停止

VMを一時停止するには、以下のいずれかの方法を使用できます。

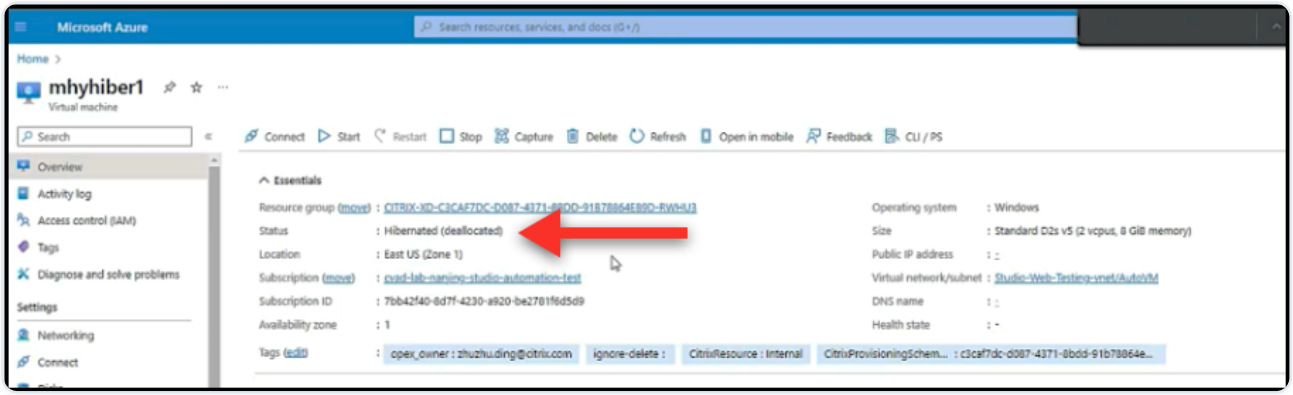
- Web Studioを使用して**手動で**
- タイムアウトポリシーを使用して**自動的に**: 詳細については、その他の設定を参照してください。

VMを手動で一時停止するには：

1. VMを右クリックし、**一時停止**を選択します。アクションを確定するには、**はい**をクリックします。**電源状態**が**一時停止中**から**一時停止済み**に変わります。



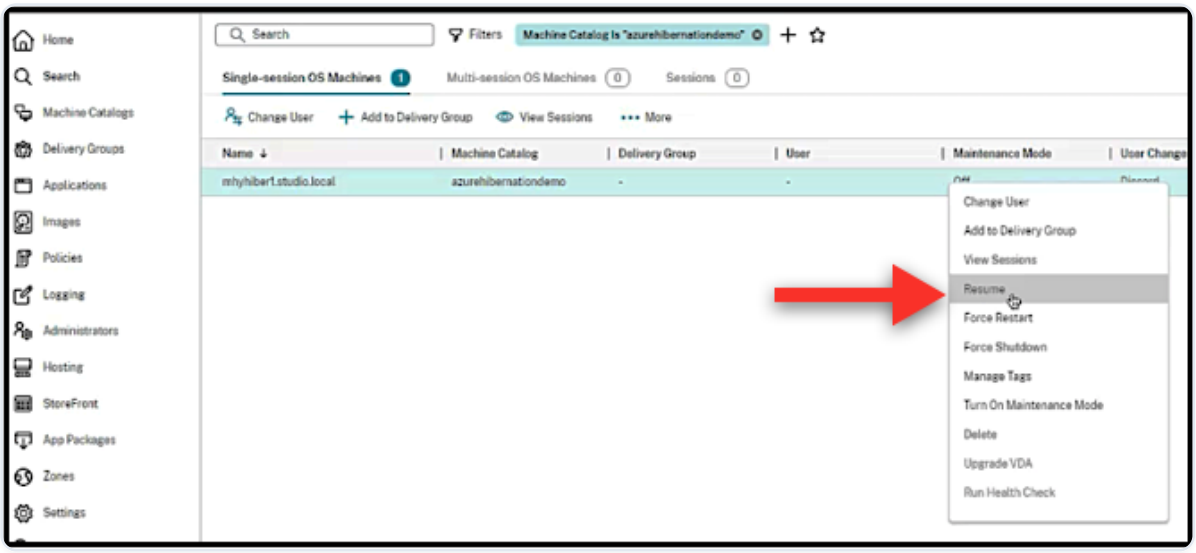
AzureポータルでVMのステータスを確認できます。



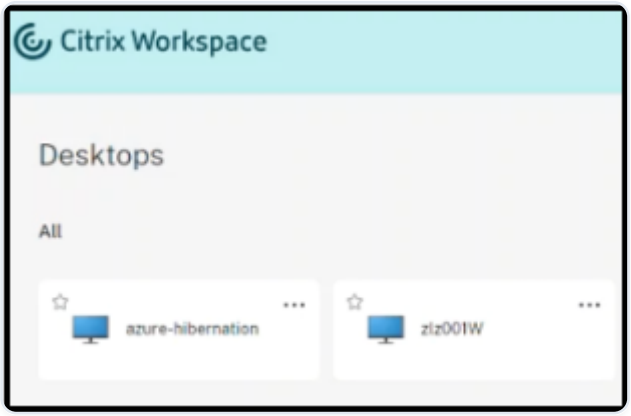
再開

休止状態のVMを再開するには、次のいずれかの方法を使用します。

- **手動で：**
  - 管理者はWeb Studioを使用してVMを再開できます。



- エンドユーザーは、デスクトップアイコンをクリックすると、Citrix Workspace™メニューを使用してVMを起動できます。



- **自動的に：**
  - Autoscale™は、ピーク時間を正しく構成した場合、休止状態のマシンを自動的に電源オンにできます。タイムスケジュールをクリックすることで、ピーク時間を30分間隔で設定できます。各青いフレームは、ピーク時間としてマークされたタイムスロットを表します。ピーク時間には、連続したタイムスロットと非連続のタイムスロットを設定できます。
    - 連続したタイムスロット

      「連続したピーク時間帯」(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/consecutive-peak-time-autoscale.png)
    - 連続しない時間帯

      「連続しないピーク時間帯」(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/non-consecutive-peak-time-autoscale.png)

> **注：**
>
> **Manage Autoscale > Load-based Settings**で、**Action**が**Suspend**に構成されている場合、そのデリバリーグループ内のすべてのVMが休止状態機能を持っていることを確認してください。そうでない場合、休止状態にできないVMは実行され続けます。

> 「オートスケール負荷ベース設定の管理」(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/azure-hibernation-autoscale.png)

詳細情報

Citrix Azureの休止状態の詳細については、Citrix Tech Zoneの記事を参照してください。

セキュリティポリシー

この記事では、さまざまなサポート対象クラウドサービスにおけるセキュリティ機能について説明します。セキュリティ機能には、次のものが含まれます。

- セキュリティグループ(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/install-configure/security-policies/security-group.html)
- セキュアブート(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/install-configure/security-policies/secure-boot.html)
- 暗号化機能(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/install-configure/security-policies/encryption-capabilities.html)

セキュリティグループ

セキュリティグループは、仮想ネットワーク内のリソース間のネットワークトラフィックをフィルタリングするためのセキュリティルールのグループです。セキュリティルールは、いくつかの種類のリソースに対するインバウンドネットワークトラフィックまたはアウトバウンドネットワークトラフィックを許可または拒否します。各ルールは次のプロパティを指定します。

- 名前: ネットワークセキュリティグループ内の一意の名前
- 優先度: ルールは優先度順に処理され、数値が小さいほど優先度が高いため、数値が小さいものから先に処理されます
- 送信元または宛先: 任意、または個別のIPアドレス、クラスレスドメイン間ルーティング (CIDR) ブロック (例: 10.0.0.0/24)、サービスタグ、またはアプリケーションセキュリティグループ

- プロトコル: 各セキュリティグループのルールを追加する際のベースとなるプロトコル
- 方向: ルールがインバウンドトラフィックまたはアウトバウンドトラフィックに適用されるかどうか
- ポート範囲: 個別のポートまたはポート範囲を指定できます
- アクション: 許可または拒否

サポートされているハイパーバイザーの詳細については、以下を参照してください。

- AWS のセキュリティグループ
- Microsoft Azure のセキュリティグループ
- Google Cloud Platform のセキュリティグループ

AWS のセキュリティグループ

セキュリティグループは、VPC 内のインスタンスのトラフィックを制御する仮想ファイアウォールとして機能します。パブリックサブネット内のインスタンスがプライベートサブネット内のインスタンスと通信できるようにするルールをセキュリティグループに追加します。これらのセキュリティグループをVPC内の各インスタンスに関連付けることもできます。インバウンドルールはインスタンスへの受信トラフィックを制御し、アウトバウンドルールはインスタンスからの送信トラフィックを制御します。

イメージ準備中のネットワーク設定の詳細については、イメージ準備中のネットワーク設定を参照してください。

インスタンスを起動するときに、1つ以上のセキュリティグループを指定できます。セキュリティグループを構成するには、「セキュリティグループの構成」(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/install-configure/install-prepare/aws.html#task-2-configure-security-groups)を参照してください。

Microsoft Azure のセキュリティグループ

Citrix Virtual Apps and Desktops は、Azure のネットワークセキュリティグループをサポートしています。ネットワークセキュリティグループは、サブネットに関連付けられることが想定されています。詳細については、ネットワークセキュリティグループを参照してください。

イメージの準備中に作成されるネットワークセキュリティグループの詳細については、「Azure Resource Manager イメージを使用してマシンカタログを作成する」(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/install-configure/machine-catalogs-create/create-machine-catalog-citrix-azure.html#create-a-machine-catalog-using-an-azure-resource-manager-image-in-web-studio)を参照してください。

Google Cloud Platform のセキュリティグループ

マシンカタログの準備中に、カタログのマスターイメージシステムディスクとして機能するマシンイメージが準備されます。このプロセスが発生すると、ディスクは一時的に仮想マシンに接続されます。この VM は、すべてのインバウンドおよびアウトバウンドネットワークトラフィックを防止する分離された環境で実行する必要があります。これは、すべてのトラフィックを拒否するファイアウォールルールによって実現されます。詳細については、「ファイアウォールルール」(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/install-configure/machine-catalogs-create/create-machine-catalog-gcp.html#firewall-rules)を参照してください。

セキュアブートとvTPM

セキュアブートは、システムの起動を担当するUnified Extensible Firmware Interface (UEFI) の機能です。これにより、起動プロセス中に信頼できるソフトウェアのみがロードされることが保証されます。

トラステッドプラットフォームモジュール (TPM) は、暗号化キーやその他の機密データを安全に保存するためのハードウェアチップです。仮想トラステッドプラットフォームモジュール (vTPM) は、TPM と同じ機能を実行しますが、暗号化コプロセッサ機能をソフトウェアで実行します。TPM はセキュリティを強化できますが、セキュアブートの要件ではありません。

サポートされているクラウドサービスの詳細については、以下を参照してください。

- Google Cloud Platform でのセキュアブートとvTPM
- Microsoft Azure でのセキュアブートとvTPM
- VMware でのvTPM

Google Cloud Platform でのセキュアブートとvTPM

Google Cloud Platform (GCP) でシールドされた仮想マシンをプロビジョニングできます。シールドされた VM の検証可能な整合性は、次の機能を使用することで実現されます。

- セキュアブート
- vTPM対応メジャーブート
- 整合性監視

シールドされたVMでカタログを作成するためのPowerShellの使用方法について詳しくは、「Using PowerShell to create a catalog with shielded VM」を参照してください。

> **注：**

> マスターイメージにWindows 11をインストールする場合、マスターイメージ作成プロセス中にvTPMを有効にする必要があります。また、カタログ作成にマシンプロファイルを使用する場合、マシンプロファイルソース（VMまたはインスタンステンプレート）でvTPMを有効にする必要があります。単一テナントノードでのWindows 11 VMの作成について詳しくは、「Create Windows 11 VMs on the sole-tenant node」を参照してください。

Microsoft Azureにおけるセキュアブートとv TPM

Azure 環境では、Trusted Launch が有効なマシンカタログを作成できます。Azure は、第 2 世代 VM のセキュリティを向上させるシームレスな方法として Trusted Launch を提供します。Trusted Launch は、高度で永続的な攻撃手法から保護します。Trusted Launch を有効にするには、マシンプロファイルベースのカタログ構成を使用します。Trusted Launch の根幹には、VM のセキュアブートがあります。Trusted Launch は、クラウドによるリモートアテステーションを実行するために vTPM も使用します。これは、プラットフォームのヘルスチェックと、信頼に基づく決定を行うために使用されます。セキュアブートと vTPM は個別に有効にできます。Trusted Launch を使用したマシンカタログの作成の詳細については、「Trusted Launch を使用したマシンカタログ」を参照してください。

VMware における vTPM

MCS は、vTPM を使用したマシンカタログの作成をサポートしています。マスターイメージに Windows 11 がインストールされている場合、マスターイメージで vTPM を有効にすることが必須です。マシンプロファイルベースの構成が使用され、vTPM が有効になっている場合、カタログ内の VM は VM テンプレートから同じ vTPM コンテンツを継承します。マシンプロファイルが使用されておらず、マスターイメージで vTPM が有効になっている場合、カタログ内の VM は空の vTPM を持ちます。詳細については、「マシンプロファイルを使用してマシンカタログを作成する」を参照してください。

暗号化機能

暗号化機能は、共有仮想マシンホスト上の悪意のあるゲストによる攻撃や、ホスト上のすべての仮想マシンを管理するハイパーバイザー制御ソフトウェアによる攻撃から、仮想マシンのコンテンツを保護します。

サポートされているクラウドサービスの詳細については、以下を参照してください。

- AWS の暗号化機能
- Google Cloud Platform の暗号化機能
- Microsoft Azure の暗号化機能

AWS の暗号化機能

このセクションでは、AWS 仮想化環境における暗号化機能について説明します。

自動暗号化

アカウントで作成された新しい Amazon EBS ボリュームとスナップショットコピーの自動暗号化を有効にできます。詳細については、「自動暗号化」を参照してください。

Google Cloud Platform の暗号化機能

このセクションでは、Google Cloud Platform (GCP) 仮想化環境における暗号化機能について説明します。

Googleマネージド暗号化キーで許可されているよりもキー操作を詳細に制御する必要がある場合は、顧客管理の暗号化キーを使用できます。顧客管理の暗号化キーを使用する場合、オブジェクトがバケットに保存されるときにCloud Storageによってキーで暗号化され、オブジェクトがリクエスターに提供されるとCloud Storageによって自動的に復号化されます。詳細については、「顧客管理の暗号化キー」を参照してください。

MCS カタログに顧客管理の暗号化キー (CMEK) を使用できます。詳細については、「顧客管理の暗号化キー (CMEK) の使用」を参照してください。

Microsoft Azure の暗号化機能

このセクションでは、Azure仮想化環境における暗号化機能について説明します。

Azureサーバー側暗号化

ほとんどのAzureマネージドディスクは、Azure Storage暗号化で暗号化されています。これは、サーバー側暗号化 (SSE) を使用してデータを保護し、セキュリティとコンプライアンスのコミットメントを満たすのに役立ちます。Citrix Virtual Apps and Desktopsは、Azure Key Vaultを介したAzureマネージドディスクの顧客管理の暗号化キーをサポートしています。詳細については、「Azureサーバー側暗号化」を参照してください。

ホストでのAzureディスク暗号化

ホストでの暗号化機能を備えたMCSマシンカタログを作成できます。

この暗号化方法は、Azureストレージを介してデータを暗号化しません。VMをホストするサーバーがデータを暗号化し、その後、暗号化されたデータがAzureストレージサーバーを介して流れます。したがって、この暗号化方法はデータをエンドツーエンドで暗号化します。

ホストでの暗号化機能を備えたMCSマシンカタログの作成の詳細については、ホストでのAzureディスク暗号化を参照してください。

Azure二重暗号化

二重暗号化は、プラットフォーム側暗号化（デフォルト）と顧客管理暗号化（CMEK）です。したがって、暗号化アルゴリズム、実装、または侵害されたキーに関連するリスクを懸念するセキュリティ意識の高いお客様は、この二重暗号化を選択できます。永続的なOSおよびデータディスク、スナップショット、イメージはすべて、二重暗号化によって保存時に暗号化されます。詳細については、マネージドディスクの二重暗号化を参照してください。

Azure機密VM

Azure機密コンピューティングVMは、仮想デスクトップがメモリ内で暗号化され、使用中に保護されることを保証します。

MCSを使用して、Azure機密VMを含むカタログを作成できます。このようなカタログを作成するには、マシンプロファイルワークフローを使用する必要があります。マシンプロファイルの入力として、VMとARMテンプレート仕様の両方を使用できます。

詳細については、Azure機密VMを参照してください。

デリバリーグループの作成

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

> デリバリーグループは、1つ以上のマシンカタログから選択されたマシンの集合です。デリバリーグループは、どのユーザーがそれらのマシンを使用できるか、およびそれらのユーザーが利用できるアプリケーションとデスクトップを指定します。

サイトを作成し、マシンカタログを作成した後、デリバリーグループを作成することは、展開を構成する次のステップです。後で、最初のデリバリーグループの初期設定を変更したり、他のデリバリーグループを作成したりできます。また、デリバリーグループの作成時ではなく、編集時にのみ構成できる機能と設定もあります。

> **注：**

> MMCベースのStudioを使用してデリバリーグループを作成またはアップグレードすると、Autoscale™はデフォルトで有効になります。

> リモートPCアクセスの場合、サイトを作成すると、「Remote PC Access Desktops」という名前のデリバリーグループが自動的に作成されます。

デリバリーグループを作成するには：

1. デリバリーグループなしでサイトとマシンカタログを作成した場合、Web Studioはデリバリーグループを作成するための正しい開始場所に案内します。
2. すでにデリバリーグループを作成しており、別のデリバリーグループを作成したい場合は、次の手順に従ってください。
    a. **デリバリーグループ**を選択します。アクションペインで**デリバリーグループの作成**を選択します。
    b. フォルダーを使用してデリバリーグループを整理するには、デフォルトの**デリバリーグループ**フォルダーの下にフォルダーを作成します。詳細については、フォルダーの作成を参照してください。
    c. グループを作成するフォルダーを選択し、**デリバリーグループの作成**をクリックします。グループ作成ウィザードが開きます。
3. ウィザードが起動すると**はじめに**ページが表示されますが、これは今後このウィザードを起動する際に表示しないように削除できます。
4. ウィザードはその後、次のセクションで説明されているページを案内します。各ページの作業が完了したら、最後のページに到達するまで**次へ**をクリックします。

ステップ1. マシン

マシンページで、カタログを選択し、そのカタログから使用したいマシンの数を選択します。

知っておくと良いこと:

- 選択したカタログ内では、少なくとも1台のマシンが未使用のまま残しておく必要があります。
- カタログは複数のデリバリーグループで指定できます。マシンは1つのデリバリーグループでのみ使用できます。
- デリバリーグループは複数のカタログからマシンを使用できます。ただし、それらのカタログには同じマシンタイプ（マルチセッションOS、シングルセッションOS、またはリモートPCアクセス）が含まれている必要があります。つまり、デリバリーグループ内でマシンタイプを

混在させることはできません。同様に、展開にWindowsマシンのカタログとLinuxマシンのカタログがある場合、デリバリーグループにはどちらかのOSタイプのマシンを含めることができますが、両方を含めることはできません。

- Citrixは、すべてのマシンを最新のVDAバージョンでインストールまたはアップグレードすることを推奨します。必要に応じてカタログとデリバリーグループをアップグレードします。デリバリーグループを作成する際、異なるVDAバージョンがインストールされているマシンを選択した場合、デリバリーグループは最も古いVDAバージョンと互換性があります。これはグループの*機能レベル*と呼ばれます。例えば、マシンの1つにVDAバージョン7.1がインストールされており、他のマシンに現在のバージョンがインストールされている場合、グループ内のすべてのマシンは、VDA 7.1でサポートされていた機能のみを使用できます。これは、より新しいVDAバージョンを必要とする一部の機能が、そのデリバリーグループでは利用できない可能性があることを意味します。
- Remote PCアクセス カタログ内の各マシンは、デリバリーグループに自動的に関連付けられます。Remote PCアクセス サイトを作成すると、「Remote PC Access Machines」という名前のカタログと「Remote PC Access Desktops」という名前のデリバリーグループが自動的に作成されます。
- 以下の互換性チェックが実行されます。
  - MinimumFunctionalLevelは互換性がある必要があります
  - SessionSupportは互換性がある必要があります
  - AllocationTypeはSingleSessionと互換性がある必要があります
  - ProvisioningType は互換性がある必要があります
  - PersistChanges は MCS および Citrix Provisioning™ と互換性がある必要があります
  - RemotePC カタログは Remote PC Access カタログとのみ互換性があります
  - AppDisk 関連のチェック

ステップ 2. 負荷分散

デリバリーグループの作成中に負荷分散設定を構成するには：

1. Web Studioにサインインします。
2. 左側のナビゲーションで、 をクリックします。
3. ページで、 をクリックします。
4. ウィザードで、 をクリックします。 ウィザードが開きます。
5. ウィザードで、必要なマシンカタログを選択し、 をクリックします。 ウィザードが開きます。

6. ウィザードで、 チェックボックスをオンにします。
7. 必要に応じて、 または オプションを選択し、 をクリックします。

   デリバリーグループの作成中の負荷分散設定(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/load-balance-create-delivery-group.png)

既存のデリバリーグループの編集中に負荷分散設定を構成するには：

1. Web Studioにサインインします。
2. 左ペインで、**デリバリーグループ**をクリックします。
3. 一覧から**デリバリーグループ**を選択し、**編集**をクリックします。**デリバリーグループの編集**ウィザードが開きます。
4. **デリバリーグループの編集**ページで、**負荷分散**をクリックします。
5. **サイト全体の構成を上書き**チェックボックスをオンにします。
6. 必要に応じて、**水平負荷分散**または**垂直負荷分散**オプションを選択し、**保存**をクリックします。

   デリバリーグループの編集中における負荷分散設定(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/load-balance-edit-delivery-group.png)

> **注：**
>
> 垂直負荷分散設定が適用されている場合、**同時ログオン許容数**および**最大セッション数**ポリシーが適切に構成されていることを確認してください。
>
> デリバリーグループの作成または編集中における垂直負荷分散のポリシー設定(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/related-policy-settings-for-vertical-load-balancing-creating-dg.png)
>
> サイトおよびデリバリーグループレベルでの負荷分散について詳しくは、「マシンの負荷分散」を参照してください。

手順3. 配信の種類

このページは、静的（割り当て済み）シングルセッションOSマシンを含むカタログを選択した場合にのみ表示されます。

配信の種類ページで、**アプリケーション**または**デスクトップ**のいずれかを選択します。両方を有効にすることはできません。

マルチセッションOSまたはシングルセッションOSのランダム（プールされた）カタログからマシンを選択した場合、配信の種類はアプリケーションとデスクトップであると見なされます。アプリケーション、デスクトップ、またはその両方を配信できます。

手順4. ユーザー

デリバリーグループ内のアプリケーションとデスクトップを使用できるユーザーとユーザーグループを指定します。

ユーザーリストの指定場所

Active Directoryのユーザーリストは、以下の作成または編集時に指定されます。

- Web Studioでは構成されないサイトのユーザーアクセスリスト。デフォルトでは、アプリケーションのエンタイトルメントポリシー規則にはすべてのユーザーが含まれます。詳細については、PowerShell SDKの`BrokerAppEntitlementPolicyRule`コマンドレットを参照してください。
- アプリケーショングループ（構成されている場合）。
- デリバリーグループ。
- アプリケーション。

StoreFront™を介してアプリケーションにアクセスできるユーザーのリストは、上記のユーザーリストの共通部分によって形成されます。たとえば、他のグループへのアクセスを不必要に制限することなく、特定の部門にアプリケーションAの使用を構成するには、次のようにします。

- すべてのユーザーを含むデフォルトのアプリケーションエンタイトルメントポリシー規則を使用します。
- デリバリーグループのユーザーリストを構成して、すべての本社ユーザーがデリバリーグループで指定された任意のアプリケーションを使用できるようにします。
- （アプリケーショングループが構成されている場合）アプリケーショングループのユーザーリストを構成して、管理および財務ビジネスユニットのメンバーがアプリケーションAからLにアクセスできるようにします。
- アプリケーションAのプロパティを構成して、その可視性を管理および財務の売掛金担当者のみに制限します。

認証済みユーザーと未認証ユーザー

ユーザーには、認証済みと未認証（未認証は匿名とも呼ばれます）の2種類があります。デリバリーグループでは、いずれか一方または両方のタイプを構成できます。

- **認証済み:** アプリケーションとデスクトップにアクセスするには、名前で指定したユーザーとグループメンバーが、スマートカードやユーザー名とパスワードなどの資格情報をStoreFrontまたはCitrix Workspace™アプリに提示する必要があります。シングルセッションOSマシンを含むデリバリーグループの場合、後でデリバリーグループを編集してユーザーデータ（ユーザーのリスト）をインポートできます。
- **未認証（匿名）:** マルチセッションOSマシンを含むデリバリーグループの場合、ユーザーはStoreFrontまたはCitrix Workspaceアプリに資格情報を提示せずにアプリケーションとデスクトップにアクセスできます。たとえば、キオスクではアプリケーションに資格情報が必要な場合がありますが、Citrixアクセス ポータルとツールは必要ありません。最初のDelivery Controllerをインストールすると、匿名ユーザーグループが作成されます。

  認証されていないユーザーにアクセスを許可するには、デリバリーグループ内の各マシンにVDA for Windows Server OS（最小バージョン7.6）がインストールされている必要があります。認証されていないユーザーが有効になっている場合、認証されていないStoreFrontストアが必要です。

  認証されていないユーザーアカウントは、セッションが起動されるとオンデマンドで作成され、Anon*XYZ*という名前になります。ここで*XYZ*は一意の3桁の値です。

  認証されていないユーザーセッションには、デフォルトで10分間のアイドルタイムアウトがあり、クライアントが切断されると自動的にログオフされます。再接続、クライアント間のローミング、およびWorkspace Controlはサポートされていません。

次の表は、**ユーザー**ページでの選択肢について説明しています。

アクセスを有効にする対象	ユーザーとユーザーグループを追加/割り当てますか？	「認証されていないユーザーにアクセスを許可する」チェックボックスを有効にしますか？
認証済みユーザーのみ	はい	いいえ
認証されていないユーザーのみ	いいえ	はい
認証済みユーザーと未認証ユーザーの両方	はい	はい

ステップ5. アプリケーション

知っておくと良いこと:

- Remote PC Accessデリバリーグループにアプリケーションを追加することはできません。
- デフォルトでは、追加する新しいアプリケーションはApplicationsという名前のフォルダーに配置されます。別のフォルダーを指定することもできます。詳細については、「アプリケーションの管理」の記事を参照してください。
- アプリケーションをデリバリーグループに追加するとき、または後で、そのプロパティを変更できます。詳細については、「アプリケーションの管理」の記事を参照してください。
- アプリケーションを追加しようとして、そのフォルダーに同じ名前のアプリケーションが存在する場合、追加しようとしているアプリケーションの名前を変更するよう求められます。拒否した場合、そのアプリケーションは、そのアプリケーションフォルダー内で一意になる接尾辞を付けて追加されます。
- アプリケーションを複数のデリバリーグループに追加する場合、それらすべてのデリバリーグループでアプリケーションを表示するための十分な権限がないと、表示の問題が発生する可能性があります。そのような場合は、より高い権限を持つ管理者に相談するか、アプリケーションが追加されたすべてのデリバリーグループを含むようにスコープを拡張してください。
- 同じ名前のアプリケーションを同じユーザーに2つ公開する場合、Web Studioで「アプリケーション名（ユーザー向け）」プロパティを変更してください。そうしないと、ユーザーはCitrix Workspaceアプリで重複した名前を目にすることになります。

追加をクリックして、アプリケーションソースを表示します。

- **スタートメニューから:** 選択したカタログのマスターイメージから作成されたマシンで検出されたアプリケーション。このソースを選択すると、検出されたアプリケーションのリストが表示された新しいページが起動します。追加したいアプリケーションを選択し、**OK**をクリックします。
- **手動：** デリバリーグループ内のVDAまたはネットワーク上の別の場所にあるアプリケーション。このソースを選択すると、新しいページが開き、次の方法で追加するアプリケーションを指定できます。
    - 実行可能ファイルへのパス、作業ディレクトリ、オプションのコマンドライン引数、および管理者とユーザーの表示名を入力します。
    - デリバリーグループ内のVDAからアプリケーションを選択します。これを行うには、**参照**をクリックし、VDAにアクセスするための資格情報を入力し、VDAに接続されるまで待機してから、VDAからアプリケーションを選択します。選択したアプリケーションのプロパティが、ページのフィールドに自動的に入力されます。

- **既存:** 以前にサイトに追加されたアプリケーション（おそらく別のデリバリーグループ内）。このソースを選択すると、検出されたアプリケーションのリストが表示された新しいページが起動します。アプリケーションを追加し、**OK**をクリックします。
- **App-V:** App-Vパッケージ内のアプリケーション。このソースを選択すると、App-Vサーバーまたはアプリケーションライブラリを選択する新しいページが起動します。表示されたリストから追加したいアプリケーションを選択し、**OK**をクリックします。詳細については、「App-Vアプリケーションの展開と配信」を参照してください。

アプリケーションソースまたはアプリケーションが利用できないか無効な場合、表示されないか、選択できません。たとえば、サイトにアプリケーションが追加されていない場合、**既存**ソースは利用できません。または、アプリケーションが選択したカタログ内のマシンのサポートされているセッションタイプと互換性がない場合があります。

ステップ6. デスクトップ

このページのタイトルは、**マシン**ページで選択したカタログによって異なります。

- プールされたマシンを含むカタログを選択した場合、このページのタイトルは**デスクトップ**になります。
- 割り当てられたマシンを含むカタログを選択し、**デリバリーの種類**ページで「デスクトップ」を指定した場合、このページは**デスクトップユーザー割り当て**というタイトルになります。
- 割り当てられたマシンを含むカタログを選択し、**デリバリーの種類**ページで「アプリケーション」を指定した場合、このページは**アプリケーションマシンユーザー割り当て**というタイトルになります。

追加をクリックします。ダイアログボックスで:

- 表示名と説明のフィールドに、Citrix Workspaceアプリに表示される情報を入力します。
- デスクトップにタグ制限を追加するには、**このタグを持つマシンへの起動を制限する**を選択し、ドロップダウンリストからタグを選択します。詳しくは、「タグ」を参照してください。
- ラジオボタンを使用して、デスクトップを起動するか、デスクトップの起動時にマシンを割り当てます。ユーザーは、このデリバリーグループにアクセスできるすべてのユーザー、または特定のユーザーとユーザーグループのいずれかです。
- グループに割り当てられたマシンが含まれている場合は、ユーザーあたりの最大デスクトップ数を指定します。これは1以上の値である必要があります。
- デスクトップ（プールされたマシン用）またはデスクトップ割り当てルール（割り当てられたマシン用）を有効または無効にします。デスクトップを無効にすると、デスクトップの配信が

停止します。デスクトップ割り当てルールを無効にすると、ユーザーへのデスクトップの自動割り当てが停止します。

- ダイアログボックスでの作業が完了したら、**OK**をクリックします。

サイト内のデスクトップの最大インスタンス数（PowerShellのみ）

サイト内のデスクトップの最大インスタンス数を構成するには（PowerShellのみ）：

- PowerShellで、適切なBrokerEntitlementPolicyRuleコマンドレットをMaxPerEntitlementInstancesパラメーターとともに使用します。たとえば、次のコマンドレットは、`tsvda-desktop` ルールを変更して、サイトで許可されるデスクトップの同時インスタンスの最大数を2に設定します。2つのデスクトップインスタンスが実行されている場合、3番目のサブスクライバーがデスクトップを起動しようとするとエラーが発生します。

  ```
  Set-BrokerEntitlementPolicyRule -Name tsvda-desktop
  -MaxPerEntitlementInstances 2
  ```

- ガイダンスについては、Get-Help コマンドレットを使用してください。たとえば、`Get-Help Set-BrokerEntitlementPolicyRule-Parameter MaxPerEntitlementInstances`。

ステップ7. 概要

デリバリーグループの名前を入力します。説明を（オプションで）入力することもできます。これはCitrix WorkspaceアプリとWeb Studioに表示されます。

概要情報を確認し、**「完了」**をクリックします。

デリバリーグループの管理

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

はじめに

この記事では、管理コンソールからデリバリーグループを管理する手順について説明します。グループ作成時に指定した設定を変更するだけでなく、デリバリーグループの作成時には利用できないその他の設定も構成できます。

手順のカテゴリには、全般、ユーザー、マシン、セッションがあります。一部のタスクは複数のカテゴリにまたがります。たとえば、「ユーザーがマシンに接続できないようにする」はマシンのカテゴリで説明されていますが、ユーザーにも影響します。あるカテゴリでタスクが見つからない場合は、関連するカテゴリを確認してください。

その他の関連情報については、以下の記事も参照してください。

- 「アプリケーション」(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/manage-deployment/applications-manage.html)には、デリバリーグループ内のアプリケーションの管理に関する情報が含まれています。
- デリバリーグループの管理には、Delivery Group Administratorの組み込みロール権限が必要です。詳細については、「委任管理」(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/manage-deployment/delegated-administration.html)を参照してください。

全般

- グループの詳細を表示(#view-group-details)
- 配信タイプの変更(#change-the-delivery-type-of-a-delivery-group)
- StoreFront™アドレスの変更(#change-storefront-addresses)
- 機能レベルの変更(#change-the-functional-level)
- Remote PC Accessデリバリーグループの管理(#manage-remote-pc-access-delivery-groups)
- フォルダーを使用してデリバリーグループを整理する
- アプリ保護の管理

グループの詳細を表示

1. 検索機能を使用して特定のデリバリーグループを見つけます。手順については、インスタンスの検索を参照してください。
2. 検索結果から、必要に応じてグループを選択します。
3. グループの列の説明については、次の表を参照してください。
4. このグループの詳細については、下部の詳細ペインのタブをクリックしてください。

列	説明
デリバリーグループ	グループ名とセッションの種類。セッションの種類には、シングルセッションOSとマルチセッションOSが含まれます。
配信中	このグループから配信されるリソースの種類。可能な値には、アプリケーション、デスクトップ、およびアプリケーションとデスクトップが含まれます。デリバリーグループが専用マシンで構成されている場合、「静的マシン割り当て」が表示されます。
使用中のセッション	セットアップされているマシンの数と、切断状態のマシンの数。
割り当て済み数	デリバリーグループに割り当てられているカタログ内のマシンの数。
フォルダ	**デリバリーグループ**ツリー内でのグループの場所。グループが存在するフォルダーの名前（末尾のバックスラッシュを含む）が表示されます。グループがルートレベルにある場合は `-` が表示されます。

デリバリーグループのデリバリーの種類を変更する

デリバリーの種類は、グループが提供できるもの（アプリケーション、デスクトップ、またはその両方）を示します。

アプリケーションのみまたは**デスクトップとアプリケーション**のタイプを**デスクトップのみ**のタイプに変更する前に、グループからすべてのアプリケーションを削除してください。

1. 左側のペインで、**［デリバリーグループ］**を選択します。
2. グループを選択し、アクションバーで をクリックします。
3. ページで、目的のデリバリーの種類を選択します。
4. **［適用］をクリックして変更を適用し、ウィンドウを開いたままにします。または、［保存］**をクリックして変更を適用し、ウィンドウを閉じます。

StoreFrontアドレスを変更する

1. 左側のペインで、**［デリバリーグループ］**を選択します。

2. グループを選択し、アクションバーで をクリックします。
3. **［StoreFront］**ページで、StoreFrontのURLを選択または追加します。これらのURLは、デリバリーグループ内の各マシンにインストールされているCitrix Workspace™アプリによって使用されます。
4. **［適用］をクリックして変更を適用し、ウィンドウを開いたままにします。または、**［保存］**をクリックして変更を適用し、ウィンドウを閉じます。

左側のペインで**［StoreFront］**を選択して、StoreFrontサーバーアドレスを指定することもできます。

機能レベルを変更する

デリバリーグループ内のマシン上のVDAと、デリバリーグループで使用されるマシンを含むマシンカタログをアップグレードした後、デリバリーグループの機能レベルを変更します。

開始する前に：

- Citrix Provisioning™（旧Provisioning Services）を使用している場合は、Citrix Provisioningコンソールで VDAバージョンをアップグレードします。
- アップグレードされたVDAを含むマシンを起動して、Delivery Controllerに登録できるようにします。このプロセスにより、デリバリーグループで何がアップグレードされる必要があるかがコンソールに通知されます。
- 以前のVDAバージョンを引き続き使用する必要がある場合、新しい製品機能は利用できません。詳しくは、アップグレードのドキュメントを参照してください。

デリバリーグループの機能レベルを変更するには：

1. 左側のペインで、**［デリバリーグループ］**を選択します。
2. グループを選択し、アクションバーの**機能レベルの変更**をクリックします。**機能レベルの変更**アクションは、アップグレードされたVDAが検出された場合にのみ表示されます。
3. **変更**をクリックします。

ディスプレイには、どのマシンが機能レベルに変更できないか、およびその理由が表示されます。その後、変更アクションをキャンセルし、マシンの問題を解決してから、変更アクションを再度実行できます。

変更が完了したら、マシンを以前の状態に戻すことができます。デリバリーグループを選択し、アクションバーで を選択します。

Remote PC Accessデリバリーグループの管理

Remote PC Accessマシンカタログ内のマシンが割り当てられていない場合、そのマシンは一時的にそのカタログに関連付けられたデリバリーグループに割り当てられます。この一時的な割り当てにより、後でマシンをユーザーに割り当てることができます。

デリバリーグループとマシンカタログの関連付けには優先度値があります。優先度は、マシンがシステムに登録されるとき、またはユーザーがマシン割り当てを必要とするときに、マシンに割り当てられるデリバリーグループを決定します。値が小さいほど優先度が高くなります。Remote PC Accessマシンカタログに複数のデリバリーグループ割り当てがある場合、ソフトウェアは最も優先度の高い一致を選択します。この優先度値を設定するには、PowerShell SDKを使用します。

リモートPCアクセス マシンカタログは、最初に作成されたときにデリバリーグループに関連付けられます。後でカタログに追加されたマシンアカウントまたは組織単位は、デリバリーグループに追加できます。この関連付けは、オン/オフを切り替えることができます。

Remote PC Accessマシンカタログとデリバリーグループの関連付けを追加または削除するには：

1. 左側のペインで**デリバリーグループ**を選択します。
2. Remote PC Accessグループを選択します。
3. **詳細**セクションで、**マシンカタログ**タブをクリックし、Remote PC Accessカタログを選択します。
4. 関連付けを追加または復元するには、**デスクトップの追加**をクリックします。関連付けを削除するには、**関連付けの削除**をクリックします。

フォルダーを使用したデリバリーグループの整理

デリバリーグループに簡単にアクセスできるように、フォルダーを作成できます。

必要な役割

デフォルトでは、デリバリーグループフォルダーを作成および管理するには、Cloud Administrator、Full Administrator、またはDelivery Group Administratorの組み込み役割が必要です。必要に応じて、デリバリーグループフォルダーの作成と管理のための役割をカスタマイズできます。詳しくは、「必要な権限」を参照してください。

デリバリーグループフォルダーを作成する

開始する前に、デリバリーグループの整理方法を計画してください。次の点を考慮してください。

- フォルダーは最大5レベルまでネストできます（デフォルトのルートフォルダーを除く）。
- フォルダーには、デリバリーグループとサブフォルダーを含めることができます。

- Web Studioのすべてのノード（**マシンカタログ**、**デリバリーグループ**、**アプリケーション**、**アプリケーショングループ**など）は、バックエンドで同じフォルダーツリーを共有します。フォルダーの名前変更や移動の際に名前の競合を避けるため、異なるノード間で最上位フォルダーに一意の名前を使用してください。

  `New-BrokerAdminFolder` SDKコマンドレットを使用してフォルダーを作成し、それを**デリバリーグループ**ノードの下に表示したい場合は、`Set-BrokerAdminFolderMetadata`コマンドレットを使用して`ContainsDeliveryGroups`メタデータを追加する必要があります。

  例:

  ```
  Set-BrokerAdminFolderMetadata -AdminFolderId {adminFolderUid} -Name
  ContainsDeliveryGroups -Value true
  ```

デリバリーグループフォルダーを作成するには、次の手順に従います。

1. 左側のペインで**デリバリーグループ**を選択します。
2. フォルダー階層でフォルダーを選択し、**アクション**バーで **Create Folder** を選択します。
3. 新しいフォルダーの名前を入力し、**Done** をクリックします。

ヒント:

意図しない場所にフォルダーを作成してしまった場合は、正しい場所にドラッグできます。

デリバリーグループを移動する

デリバリーグループはフォルダー間で移動できます。詳細な手順は次のとおりです。

1. 左側のペインで**デリバリーグループ**を選択します。
2. フォルダーごとにグループを表示します。フォルダー階層の上にある **View all** をオンにすると、すべてのグループを一度に表示することもできます。
3. グループを右クリックし、**Move Delivery Group** を選択します。
4. グループを移動するフォルダーを選択し、**Done** をクリックします。

ヒント:

グループをフォルダーにドラッグできます。

デリバリーグループフォルダーの管理

デリバリーグループフォルダーを削除、名前変更、移動できます。

フォルダーとそのサブフォルダーにデリバリーグループが含まれていない場合にのみ、フォルダーを削除できることに注意してください。

フォルダーを管理するには、次の手順に従います。

1. 左側のペインで**デリバリーグループ**を選択します。
2. フォルダー階層でフォルダーを選択し、必要に応じて**アクション**バーでアクションを選択します。
    - フォルダーの名前を変更するには、**Rename Folder**を選択します。
    - フォルダーを削除するには、**Delete Folder**を選択します。
    - フォルダーを移動するには、**Move Folder**を選択します。
3. 画面の指示に従って、残りの手順を完了してください。

必要な権限

次の表に、デリバリーグループフォルダーに対してアクションを実行するために必要な権限を示します。

アクション	必要な権限
デリバリーグループフォルダーの作成	デリバリーグループフォルダーを作成
デリバリーグループフォルダーを削除	デリバリーグループフォルダーを削除
デリバリーグループフォルダーを移動	デリバリーグループフォルダーを移動
デリバリーグループフォルダーの名前を変更	デリバリーグループフォルダーを編集
デリバリーグループをフォルダーに移動	デリバリーグループフォルダーを編集およびデリバリーグループのプロパティを編集

アプリ保護の管理

以下の情報は、`<https://docs.citrix.com/ja-jp/citrix-workspace-app/app-protection.html>` のアプリ保護に関する記事を補足するものです。以下の詳細に注意してください。

- 有効なアプリ保護の資格が必要です。アプリ保護機能を購入するには、Citrix の営業担当者にお問い合わせください。
- アプリ保護には XML 信頼が必要です。XML 信頼を有効にするには、**設定 > XML 信頼を有効にする** に移動します。
- 画面キャプチャ防止について：
  - Windows および macOS では、保護されたコンテンツのウィンドウのみが空白になります。保護されたウィンドウが最小化されていない場合、アプリ保護はアクティブになります。
  - Linux では、キャプチャ全体が空白になります。保護されたウィンドウが最小化されているかどうかにかかわらず、アプリ保護はアクティブになります。

デリバリーグループのアプリ保護方法を選択するには、次の手順に従います。

1. 左側のペインで **デリバリーグループ** を選択します。
2. グループを選択し、アクションバーで**編集**を選択します。
3. **アプリ保護** ページで、**キーロギング対策** と **画面キャプチャ対策** を有効にできます。

ユーザー

- ユーザー設定の変更
- ユーザーの追加または削除

デリバリーグループのユーザー設定を変更する

このページの名前は、**ユーザー設定** または **基本設定** のいずれかで表示されます。

1. 左側のペインで **デリバリーグループ** を選択します。
2. グループを選択し、アクションバーで をクリックします。
3. **ユーザー設定** (または **基本設定**) ページで、次の表の設定のいずれかを変更します。
4. 変更を適用してウィンドウを開いたままにするには、**適用**をクリックします。または、変更を適用してウィンドウを閉じるには、**保存**をクリックします。

設定	説明
説明	Citrix Workspace（またはStoreFront）が使用し、ユーザーに表示されるテキスト。

設定	説明
デリバリーグループを有効にする	デリバリーグループが有効になっているかどうか。
タイムゾーン	このデリバリーグループのマシンが存在する必要があるタイムゾーン。このオプションには、サイトでサポートされているタイムゾーンが一覧表示されます。**注：**デリバリーグループのタイムゾーンを変更すると、そのデリバリーグループ内のマシンが再起動される場合があります。これを回避するには、稼働時間外にタイムゾーン設定を変更してください。
Secure ICA® を有効にする	ICAプロトコルを暗号化するSecureICAを使用して、デリバリーグループ内のマシンとの通信を保護します。デフォルトのレベルは128ビットです。レベルはSDKを使用して変更できます。Citrixは、パブリックネットワークを通過する際にTLS暗号化などのより多くの暗号化方法を使用することを推奨しています。また、SecureICAはデータ整合性をチェックしません。

デリバリーグループでのユーザーの追加または削除

ユーザーに関する詳細については、「ユーザー」を参照してください。

1. 左側のペインで**デリバリーグループ**を選択します。
2. グループを選択し、アクションバーで をクリックします。
3. **ユーザー**ページで:
    - ユーザーを追加するには、**追加**をクリックし、追加するユーザーを指定します。
    - ユーザーを削除するには、1人以上のユーザーを選択し、**削除**をクリックします。
    - 認証されていないユーザーによるアクセスを許可するには、チェックボックスをオンまたはオフにします。
4. 変更を適用してウィンドウを開いたままにするには、**適用**をクリックします。または、変更を適用してウィンドウを閉じるには、**保存**をクリックします。

ユーザーリストのインポートまたはエクスポート

物理的なシングルセッションOSマシンを含むデリバリーグループの場合、デリバリーグループの作成後に.csvファイルからユーザー情報をインポートできます。ユーザー情報を.csvファイルにエクスポートすることもできます。.csvファイルには、以前の製品バージョンのデータを含めることができます。

CSVファイルの最初の行には、コンマで区切られた2つの列ヘッダーが含まれている必要があります。最初のヘッダーが `Machine Account` で、2番目のヘッダーが `User Names` であることを確認してください。（追加のヘッダーを含めることはできますが、サポートされていません。）ファイルの以降の行には、コンマで区切られたデータが含まれます。`Machine Account` エントリは、コンピューターSID、FQDN、またはドメインとコンピューター名のペアにすることができます。

ユーザー情報をインポートまたはエクスポートするには：

1. 左側のペインで**デリバリーグループ**を選択します。
2. グループを選択し、アクションバーで をクリックします。
3. **マシン割り当て**ページで、**リストのインポート**または**リストのエクスポート**を選択し、ファイルの場所を参照します。
4. 「**適用**」をクリックして変更を適用し、ウィンドウを開いたままにします。または、「**保存**」をクリックして変更を適用し、ウィンドウを閉じます。

マシン

- マシンからユーザーへの割り当てを変更する
- ユーザーあたりの最大マシン数を変更する
- マシンを更新する
- デスクトップのタグ制限を追加、変更、または削除する
- マシンを削除する
- マシンへのアクセスを制限する
- ユーザーがマシンに接続するのを防ぐ（メンテナンスモード）
- マシンをシャットダウンして再起動する
- マシンの再起動スケジュールを作成および管理する
- 1回限りの再起動スケジュールを有効にする
- 管理対象マシンをロードする
- 管理対象マシンの電源を管理する

デリバリーグループ内のマシンからユーザーへの割り当てを変更する

MCSでプロビジョニングされたシングルセッションOSマシンの割り当てを変更できます。マルチセッションOSマシンまたはCitrix Provisioningでプロビジョニングされたマシンの割り当ては変更できません。

1. 左側のペインで「**デリバリーグループ**」を選択します。
2. グループを選択し、アクションバーで をクリックします。
3. **デスクトップ**または**デスクトップ割り当てルール**ページ（ページタイトルはデリバリーグループが使用するマシンカタログの種類によって異なります）で、新しいユーザーを指定します。
4. 「**適用**」をクリックして変更を適用し、ウィンドウを開いたままにします。または、「**保存**」をクリックして変更を適用し、ウィンドウを閉じます。

デリバリーグループ内のユーザーあたりの最大マシン数を変更する

1. 左側のペインで「**デリバリーグループ**」を選択します。
2. グループを選択し、アクションバーで をクリックします。
3. **デスクトップ割り当てルール**ページで、ユーザーあたりの最大デスクトップ数を設定します。
4. 変更を適用してウィンドウを開いたままにするには、**適用**をクリックします。または、変更を適用してウィンドウを閉じるには、**保存**をクリックします。

デリバリーグループ内のマシンを更新する

1. 左側のペインで**デリバリーグループ**を選択します。
2. グループを選択し、アクションバーで**マシンの表示**をクリックします。
3. マシンを選択し、アクションバーで**マシンの更新**をクリックします。

別のイメージを選択するには、**「イメージ」**を選択し、スナップショットを選択します。

変更を適用してマシンユーザーに通知するには、**「エンドユーザーへのロールアウト通知」**を選択します。次に、以下を指定します。

- マスターイメージを更新するタイミング: 今すぐ、または次回の再起動時
- 再起動の配布時間（グループ内のすべてのマシンの更新を開始するまでの合計時間）
- ユーザーに再起動が通知されるかどうか
- ユーザーが受信するメッセージ

デスクトップのタグ制限を追加、変更、または削除する

タグ制限の追加、変更、削除は、起動対象となるデスクトップに予期せぬ影響を与える可能性があります。「タグ」の考慮事項と注意点を確認してください。

1. 左側のペインで**デリバリーグループ**を選択します。
2. グループを選択し、アクションバーで をクリックします。
3. **デスクトップ**ページで、デスクトップを選択し、**編集**をクリックします。
4. タグ制限を追加するには、**タグを持つマシンへの起動を制限する**を選択し、タグを選択します。
5. タグ制限を変更または削除するには、次のいずれかを実行します。
   - 別のタグを選択します。
   - **このタグを持つマシンへの起動を制限する**のチェックを外して、タグ制限を削除します。
6. 変更を適用してウィンドウを開いたままにするには、**適用**をクリックします。または、変更を適用してウィンドウを閉じるには、**保存**をクリックします。

デリバリーグループからマシンを削除する

マシンを削除すると、デリバリーグループから削除されます。デリバリーグループが使用するマシンカタログからは削除されません。したがって、そのマシンは別のデリバリーグループに割り当てることができます。

マシンは、削除する前にシャットダウンする必要があります。削除中にユーザーがマシンに接続するのを一時的に停止するには、シャットダウンする前にマシンをメンテナンスモードにします。

マシンには個人データが含まれている可能性があるため、別のユーザーにマシンを割り当てる前に注意してください。マシンの再イメージングを検討してください。

1. 左側のペインで**デリバリーグループ**を選択します。
2. グループを選択し、アクションバーで**マシンの表示**をクリックします。
3. マシンがシャットダウンされていることを確認します。
4. マシンを選択し、アクションバーで**デリバリーグループから削除**をクリックします。

マシンが使用する接続を介して、デリバリーグループからマシンを削除することもできます。

デリバリーグループ内のマシンへのアクセスを制限する

デリバリーグループ内のマシンへのアクセスを制限するために行った変更は、使用する方法に関係なく、以前の設定に優先します。次のことができます。

- **委任管理スコープを使用して管理者へのアクセスを制限する:** 管理者がすべてのアプリケーションにアクセスできるスコープと、特定のアプリケーションのみにアクセスできる別のスコープを作成して割り当てます。詳細については、「委任管理」を参照してください。
- **SmartAccessポリシー式を使用してユーザーアクセスを制限する：** ポリシー式を使用して、Citrix Gateway経由のユーザー接続をフィルタリングします。

  a. 左ペインで****を選択します。

  b. グループを選択し、アクションバーで をクリックします。

  c. ****ページで、**を選択します。

  d. これらの接続のサブセットを選択するには、****を選択します。次に、Citrix Gatewayサイトを定義し、許可されるユーザーアクセスシナリオのSmartAccessポリシー式を追加、編集、または削除します。詳細については、Citrix Gatewayのドキュメントを参照してください。

  e. 変更を適用してウィンドウを開いたままにするには、****をクリックします。または、変更を適用してウィンドウを閉じるには、**をクリックします。

- **除外フィルターを使用してユーザーアクセスを制限する：** SDKで設定したアクセスポリシーに除外フィルターを使用します。アクセスポリシーは、接続を絞り込むためにデリバリーグループに適用されます。たとえば、マシンアクセスをユーザーのサブセットに制限したり、許可されるユーザーデバイスを指定したりできます。除外フィルターは、アクセスポリシーをさらに絞り込みます。たとえば、セキュリティのために、ユーザーまたはデバイスのサブセットへのアクセスを拒否できます。デフォルトでは、除外フィルターは無効になっています。

  たとえば、企業ネットワークサブネット上の教育ラボで、そのラボから特定のデリバリーグループへのアクセスを防止する場合などです。ラボ内のマシンを誰が使用しているかに関係なく、次のコマンドを使用します: `Set-BrokerAccessPolicy -Name VPDesktops_Direct -ExcludedClientIPFilterEnabled $True -`。

  アスタリスク (*) ワイルドカードを使用して、同じポリシー式で始まるすべてのタグに一致させます。たとえば、あるマシンにタグ `VPDesktops_Direct` を追加し、別のマシンに `VPDesktops_Test` を追加した場合、`Set-BrokerAccessPolicy` スクリプトでタグを `VPDesktops_*` に設定すると、両方のマシンにフィルターが適用されます。

Webブラウザーを使用している場合、またはストアでCitrix Workspaceアプリのユーザーエクスペリエンス機能が有効になっている場合は、クライアント名除外フィルターを使用できません。

デリバリーグループ内のマシンへのユーザー接続を防止する（メンテナンスモード）

マシンへの新しい接続を一時的に停止する必要がある場合は、デリバリーグループ内の1台またはすべてのマシンでメンテナンスモードをオンにできます。これは、パッチを適用したり、管理ツールを使用したりする前に行うことがあります。

- マルチセッションOSマシンがメンテナンスモードの場合、ユーザーは既存のセッションに接続できますが、新しいセッションを開始することはできません。
- シングルセッションOSマシン（またはリモートPCアクセスを使用するPC）がメンテナンスモードの場合、ユーザーは接続または再接続できません。現在の接続は、切断またはログオフするまで接続されたままになります。

メンテナンスモードをオンまたはオフにするには：

1. 左ペインで****を選択します。
2. グループを選択します。
3. デリバリーグループ内のすべてのマシンでメンテナンスモードをオンにするには、アクションバーの****をクリックします。

   1台のマシンでメンテナンスモードをオンにするには、アクションバーの**をクリックします。**マシンを選択し、アクションバーの**をクリックします。
4. デリバリーグループ内の1台またはすべてのマシンでメンテナンスモードをオフにするには、上記の手順に従い、アクションバーの****をクリックします。

Windowsリモートデスクトップ接続（RDC）の設定も、マルチセッションOSマシンがメンテナンスモードであるかどうかに影響します。メンテナンスモードは、次のいずれかが発生した場合にオンになります。

- 前述のとおり、メンテナンスモードがオンに設定されています。
- RDCが**このコンピューターへの接続を許可しない**に設定されています。
- RDCが****に設定されていません。設定は、または**のいずれかです。

以下のメンテナンスモードをオンまたはオフにすることもできます。

- 接続。その接続を使用しているマシンに影響します。
- マシンカタログ。そのカタログ内のマシンに影響します。

デリバリーグループ内のマシンをシャットダウンして再起動する

この手順は、Remote PC Accessマシンではサポートされていません。

1. 左ペインで****を選択します。
2. グループを選択し、アクションバーで**マシン表示**をクリックします。
3. マシンを選択し、アクションバーで次のいずれかのエントリをクリックします。

   - **強制シャットダウン：** マシンの電源を強制的にオフにし、マシンリストを更新します。
   - **再起動：** オペレーティングシステムにシャットダウンを要求し、その後マシンを再起動します。オペレーティングシステムがこれに応じられない場合、マシンは現在の状態のままになります。
   - **強制再起動：** オペレーティングシステムを強制的にシャットダウンし、その後マシンを再起動します。
   - **一時停止:** マシンをシャットダウンせずに一時停止し、マシンの一覧を更新します。
   - **シャットダウン:** オペレーティングシステムにシャットダウンを要求します。

強制ではないアクションの場合、マシンが10分以内にシャットダウンしないと、電源がオフになります。シャットダウン中にWindowsが更新プログラムのインストールを試みると、更新が完了する前にマシンの電源がオフになるリスクがあります。

Citrixでは、シングルセッションOSマシンのユーザーがセッション内で**シャットダウン**を選択できないようにすることをお勧めします。詳細については、Microsoftのポリシーに関するドキュメントを参照してください。

接続でマシンをシャットダウンおよび再起動することもできます。

デリバリーグループ内のマシンの再起動スケジュールを作成および管理する

> **注：**

> - Autoscale™が有効なデリバリーグループに再起動スケジュールが適用されると、そのマシンは電源がオフになり、Autoscaleが電源をオンにするまでそのままになります。
> - ランダムなシングルセッションマシンに再起動スケジュールが適用されると、コストを節約するために、それらのマシンは再起動されるのではなく電源がオフになります。マシンの電源をオンにするには、Autoscaleを使用することをお勧めします。

- デリバリーグループのタイムゾーンを変更すると、そのデリバリーグループ内のマシンが再起動される可能性があります。これを避けるには、稼働時間外にタイムゾーン設定を変更するようにしてください。

再起動スケジュールは、デリバリーグループ内のマシンが定期的に再起動されるタイミングを指定します。デリバリーグループに対して1つ以上のスケジュールを作成できます。スケジュールは、次のいずれかに影響します。

- グループ内のすべてのマシン。
- グループ内の1つまたは複数（ただしすべてではない）のマシン。マシンは、マシンに適用するタグによって識別されます。これはタグ制限と呼ばれます。タグがアクションをそのタグを持つアイテムのみに制限するためです。

たとえば、すべてのマシンが1つのデリバリーグループにあるとします。すべてのマシンを週に1回再起動し、経理チームが使用するマシンを毎日再起動したいとします。これを実現するには、すべてのマシンに対して1つのスケジュールを設定し、経理のマシンのみに対して別のスケジュールを設定します。

スケジュールには、再起動が開始される曜日と時刻、および期間が含まれます。

スケジュールを有効または無効にできます。スケジュールを無効にすることは、テスト中、特別な期間中、またはスケジュールが必要になる前に準備する際に役立ちます。

管理コンソールから自動電源オンまたはシャットダウンにスケジュールを使用することはできません。再起動のみに使用できます。

スケジュールの重複

複数のスケジュールが重複する可能性があります。上記の例では、両方のスケジュールが経理部門の仮想マシンに影響を与えます。これらのマシンは日曜日に2回再起動される可能性があります。スケジューリングコードは、意図したよりも頻繁に同じマシンを再起動しないように設計されていますが、保証はできません。

- スケジュールの開始時刻と期間が正確に一致する場合、マシンが再起動されるのは1回だけである可能性が高くなります。
- スケジュールの開始時刻と期間が異なるほど、複数回の再起動が発生する可能性が高くなります。

- スケジュールによって影響を受けるマシンの数も、重複の可能性に影響します。この例では、すべてのマシンに影響する週次スケジュールは、それぞれに指定された期間に応じて、経理部門の仮想マシンに対する日次スケジュールよりも早く再起動を開始する可能性があります。

再起動スケジュールの詳細については、「再起動スケジュールの内部」を参照してください。

再起動スケジュールの表示

1. 左側のペインで**デリバリーグループ**を選択します。
2. グループを選択し、アクションバーで をクリックします。
3. **Restart Schedule**ページを選択します。

Restart Scheduleページには、構成された各スケジュールについて次の情報が含まれています。

- スケジュール名。
- 使用されているタグ制限（ある場合）。
- マシンの再起動がどのくらいの頻度で発生するか。
- マシンユーザーが通知を受け取るかどうか。
- スケジュールが有効になっているかどうか。

タグの追加（適用）

タグ制限を使用する再起動スケジュールを構成する場合は、スケジュールが影響するマシンにタグが追加されていることを確認してください。上記の例では、経理チームが使用する各マシンにタグが適用されています。詳細については、「タグ」を参照してください。

1台のマシンに複数のタグを適用できますが、再起動スケジュールで指定できるタグは1つだけです。

1. 左側のペインで**デリバリーグループ**を選択します。
2. スケジュールによって制御されるマシンを含むグループを選択します。
3. 「**マシンの表示**」をクリックし、タグを追加するマシンを選択します。
4. アクションバーで「**タグの管理**」をクリックします。
5. タグが存在する場合は、タグ名の横にあるチェックボックスをオンにします。タグが存在しない場合は、「**作成**」をクリックし、タグの名前を指定します。タグが作成されたら、新しく作成されたタグ名の横にあるチェックボックスをオンにします。
6. 「**タグの管理**」ダイアログで「**保存**」をクリックします。

再起動スケジュールの作成

> **注：**
>
> 再起動スケジュールは、電源管理されているすべてのマルチセッションマシンと、電源管理されていないマルチセッションマシンに適用できます。

1. 左側のペインで「**デリバリーグループ**」を選択します。
2. グループを選択し、アクションバーで をクリックします。
3. 「**再起動スケジュール**」ページで、「**追加**」をクリックします。
4. 「**再起動スケジュールの追加**」ページで、次のようにします。
   - スケジュールを有効にするには、「**はい**」を選択します。スケジュールを無効にするには、「**いいえ**」を選択します。
   - スケジュール名と説明を入力します。
   - 「**タグに制限**」で、タグの制限を適用します。
   - 「**メンテナンスモードのマシンを含める**」で、メンテナンスモードのマシンをこのスケジュールに含めるかどうかを選択します。代わりにPowerShellを使用するには、「メンテナンスモードのマシンのスケジュールされた再起動」を参照してください。
   - 「**再起動頻度**」で、再起動の発生頻度（毎日、毎週、毎月、または1回）を選択します。「**毎週**」または「**毎月**」を選択した場合は、1つ以上の特定の日を指定できます。
   - 「**繰り返し間隔**」で、スケジュールを実行する頻度を指定します。
   - 「**開始日**」で、スケジュールの初回実行の開始日を指定します。
   - 「**再起動開始時刻**」で、再起動を開始する時刻を24時間形式で指定します。
   - 「**再起動期間**」について：
     - 自然な再起動を使用しない場合は、「**すべてのマシンを同時に再起動**」または「**すべてのマシンを一定期間内に再起動**」を選択します。
     - 自然な再起動を使用する場合は、「**すべてのセッションがドレインされた後にすべてのマシンを再起動**」を選択します。

       自然な再起動を使用するように構成された再起動スケジュールを開始すると、次のようになります。

- デリバリーグループに属するすべてのアイドル状態のマシンはすぐに再起動されます
- 1つ以上の有効なセッションを持つデリバリーグループに属する各マシンは、すべてのセッションがログオフされたときに再起動されます。

> **注：**
>
> 自然な再起動スケジュールは、電源管理されたマシンのみを再起動できます。

- 「**ユーザーへの通知の送信**」で、再起動が開始される前に該当するマシンに通知メッセージを表示するかどうかを選択します。デフォルトでは、メッセージは表示されません。
- 再起動が開始される15分前にメッセージを表示することを選択した場合、（「**通知頻度**」で）最初のメッセージの後に5分ごとにメッセージを繰り返すように選択できます。デフォルトでは、メッセージは繰り返されません。
- 通知のタイトルとテキストを入力します。デフォルトのテキストはありません。

  メッセージに再起動までのカウントダウンを含める場合は、変数 **%m%** を含めます。すべてのマシンを同時に再起動することを選択しない限り、メッセージは再起動前の適切なタイミングで各マシンに表示されます。

5. をクリックして変更を適用し、 ウィンドウを閉じます。
6. 「**適用**」をクリックして変更を適用し、ウィンドウを開いたままにします。または、「**保存**」をクリックして変更を適用し、ウィンドウを閉じます。

ドレイン後の再起動

PowerShell を使用してマシンの再起動スケジュールを作成または更新する場合 (`New-BrokerRebootSchedulev2` または `Set-BrokerRebootSchedulev2`)、別の再起動期間値を使用できます。

`-UseNaturalReboot <Boolean>` パラメーターでドレイン後の再起動機能を有効にすると、すべてのセッションがドレインされた後にすべてのマシンが再起動されます。再起動時刻になると、マシンはドレイン状態になり、すべてのセッションがログオフされると再起動されます。

この機能は、シングルセッションまたはマルチセッションマシンを含むデリバリーグループでサポートされています。このオプションは、電源管理されているマシンと電源管理されていないマシンの両方で使用できます。

オンプレミス環境では、この機能は PowerShell を使用する場合にのみサポートされます。この機能は Web Studio では利用できません。

再起動スケジュールの編集、削除、有効化、または無効化

1. 左側のペインで を選択します。
2. グループを選択し、アクションバーで をクリックします。
3. **再起動スケジュール**ページで、スケジュールのチェックボックスを選択します。
    - スケジュールを編集するには、 をクリックします。再起動スケジュールの作成 のガイダンスに従って、スケジュール構成を更新します。
    - スケジュールを有効または無効にするには、 をクリックします。 チェックボックスをオンまたはオフにします。
    - スケジュールを削除するには、 をクリックします。削除を確認します。スケジュールを削除しても、影響を受けるマシンに適用されているタグには影響しません。

データベース障害により遅延したスケジュールされた再起動

> **注：**
>
> この機能はPowerShellでのみ利用可能です。

> デリバリーグループ内のマシン (VDA) のスケジュールされた再起動が開始される前にサイトデータベースの停止が発生した場合、停止が終了すると再起動が開始されます。これにより、予期しない結果が生じる可能性があります。

たとえば、デリバリーグループの再起動を非稼働時間中 (03:00 から) に発生するようにスケジュールしたとします。スケジュールされた再起動が開始される1時間前 (02:00) にサイトデータベースの停止が発生しました。停止は6時間 (08:00 まで) 続きました。Delivery Controller とサイトデータベース間の接続が復元されると、再起動スケジュールが開始されます。VDA の再起動は元のスケジュールから5時間後に開始され、稼働時間中に VDA が再起動されることになります。

この状況を回避するために、`New-BrokerRebootScheduleV2` および `Set-BrokerRebootScheduleV2` コマンドレットで `MaxOvertimeStartMins` パラメーターを使用できます。この値は、再起動スケジュールが開始できる、スケジュールされた開始時刻を超える最大分数を示します。

- その時間内 (スケジュールされた時間 + `MaxOvertimeStartMins`) にデータベース接続が復元された場合、VDAの再起動が開始されます。
- その時間内にデータベース接続が復元されない場合、VDAの再起動は開始されません。
- このパラメーターが省略されているか、値がゼロの場合、停止期間に関係なく、データベースへの接続が復元されたときにスケジュールされた再起動が開始されます。

詳細については、コマンドレットのヘルプを参照してください。この機能は PowerShell でのみ利用できます。Web Studio で再起動スケジュールを構成する際には、この値を設定できません。

メンテナンスモードのマシンのスケジュールされた再起動

> **注：**
>
> この機能は PowerShell でのみ利用できます。オプション `IgnoreMaintenanceMode` は、Citrix Virtual Apps and Desktops 7 2006 以降でサポートされています。

> 再起動スケジュールがメンテナンスモードのマシンに影響するかどうかを示すには、`BrokerRebootScheduleV2` コマンドレットで `IgnoreMaintenanceMode` オプションを使用します。

たとえば、次のコマンドレットは、メンテナンスモードのマシン (メンテナンスモードではないマシンに加えて) を再起動するスケジュールを作成します。

```
New-Brokerrebootschedulev2 rebootSchedule1 -DesktopGroupName <myDesktopGroup> -IgnoreMaintenanceMode $true
```

次のコマンドレットは、既存の再起動スケジュールを変更します。

```
Set-Brokerrebootschedulev2 rebootSchedule1 -IgnoreMaintenanceMode $true
```

詳細については、コマンドレットのヘルプを参照してください。この機能はPowerShellでのみ利用可能です。

1回限りの再起動スケジュールを有効にする

PowerShell を使用して1回限りの再起動スケジュールを有効にする場合は、次の `BrokerCatalogRebootSchedule` PowerShell コマンドを使用して、再起動スケジュールを作成、変更、削除します。

- Get-BrokerCatalogRebootSchedule

- New-BrokerCatalogRebootSchedule
- Set-BrokerCatalogRebootSchedule
- ブローカーカタログの再起動スケジュールを削除
- ブローカーカタログの再起動スケジュール名を変更

制限事項:

- タイムゾーンが構成されていないカタログに関連付けられたカタログ再起動スケジュールは作成されますが、開始されません。
- カタログ再起動スケジュールが作成されると、その再起動スケジュールはデリバリーグループに属するカタログVMでのみ実行されます。

例、,

- **BankTellers** という名前のカタログ内のVMの再起動スケジュールを、Feb 3, 2022 の午前2時から午前4時の間に開始するように作成します。

```
C:\PS> New-BrokerCatalogRebootSchedule -Name BankTellers -CatalogName
BankTellers  -StartDate "2022-02-03" -StartTime "02:00" -Enabled $true
-RebootDuration 120
```

- UID 17を持つカタログ内のVMの再起動スケジュールを、Feb 3, 2022の午前1時から午前5時の間に開始するように作成します。再起動の10分前に、各VMは、すべてのユーザーセッションで、タイトルが「**WARNING: Reboot pending**」、メッセージが「**Save your work**」のメッセージボックスを表示するように設定されます。

```
C:\PS> New-BrokerCatalogRebootSchedule -Name 'Update reboot'
-CatalogUid 17 -StartDate "2022-02-03" -StartTime "01:00" -Enabled
$true -RebootDuration 240 -WarningTitle "WARNING: Reboot pending"
-WarningMessage "Save your work" -WarningDuration 10
```

- **Old Name** という名前のカタログ再起動スケジュールを **New Name** に変更します。

```
C:\PS> Rename-BrokerCatalogRebootSchedule -Name "Old Name" -NewName
"New Name"
```

- UID 1 を持つすべてのカタログ再起動スケジュールを表示し、その後、UID 1 を持つカタログ再起動スケジュールを **New Name** に変更します。

```
C:\PS> Get-BrokerCatalogRebootSchedule -Uid 1 | Rename-
BrokerCatalogRebootSchedule -NewName "New Name" -PassThru
```

- **Accounting**という名前のカタログ再起動スケジュールを、各VMの再起動の10分前に、タイトルが「**WARNING: Reboot pending**」、メッセージが「**Save your work**」のメッセージを表示するように設定します。このメッセージは、そのVM上のすべてのユーザーセッションに表示されます。

```
C:\PS> Set-BrokerCatalogRebootSchedule -Name Accounting -WarningMessage
"Save your work" -WarningDuration 10 -WarningTitle "WARNING: Reboot
pending"
```

- 無効になっているすべての再起動スケジュールを表示し、その後、無効になっているすべての再起動スケジュールを有効にします。

```
C:\PS> Get-BrokerCatalogRebootSchedule -Enabled $false | Set-
BrokerCatalogRebootSchedule -Enabled $true
```

- UID 17を持つカタログ再起動スケジュールを、各VMの再起動の15分前、10分前、5分前に「**Rebooting in %m% minutes**」というメッセージを表示するように設定します。

```
C:\PS> Set-BrokerCatalogRebootSchedule 17 -WarningMessage "Rebooting in
%m% minutes." -WarningDuration 15 -WarningRepeatInterval 5
```

- 「**MyCatalog**」という名前のカタログのタイムゾーンを構成します。

```
C:\PS> Set-BrokerCatalog -Name "MyCatalog" -TimeZone &lt;TimeZone>
```

デリバリーグループ内の負荷管理されたマシン

負荷管理できるのはマルチセッションOSマシンのみです。

負荷管理は、サーバーの負荷を測定し、現在の環境条件でどのサーバーを選択するかを決定します。この選択は、以下に基づいています。

- **サーバーメンテナンスモードのステータス:** マルチセッションOSマシンは、メンテナンスモードがオフの場合にのみ負荷分散の対象となります。

- **サーバー負荷インデックス:** マルチセッションOSマシンを提供するサーバーが接続を受け入れる可能性を決定します。このインデックスは、セッション数やCPU、ディスク、メモリ使用量などのパフォーマンスメトリックの設定といった負荷評価子の組み合わせです。負荷評価子は、負荷管理ポリシー設定で指定されます。

  サーバー負荷インデックスが10000の場合、サーバーが完全に負荷されていることを示します。他に利用可能なサーバーがない場合、ユーザーはセッションを起動したときに、デスクトップまたはアプリケーションが利用できないというメッセージを受け取る可能性があります。

  ロードインデックスは、Director (Monitor)、Web Studio (Manage) 検索、およびSDKで監視できます。

  コンソール表示で、**サーバー負荷インデックス**列（デフォルトでは非表示）を表示するには、マシンを選択し、列ヘッダーを右クリックして、**列の選択**を選択します。**マシンカテゴリ**で、**負荷インデックス**を選択します。

  SDKでは、`Get-BrokerMachine` コマンドレットを使用します。詳細については、「CTX202150」を参照してください。

- **同時ログオン許容ポリシー設定**: サーバーへの同時ログオン要求の最大数。（この設定は、XenApp 6.xバージョンでの負荷調整に相当します。）

  すべてのサーバーが同時ログオン許容設定以上の場合、次のログオン要求は、保留中のログオンが最も少ないサーバーに割り当てられます。複数のサーバーがこれらの条件を満たす場合、ロードインデックスが最も低いサーバーが選択されます。

デリバリーグループ内の電源管理されたマシン

電源管理できるのは、仮想シングルセッションOSマシンのみであり、物理マシン（リモートPCアクセス マシンを含む）はできません。GPU機能を備えたシングルセッションOSマシンは一時停止できないため、電源オフ操作は失敗します。マルチセッションOSマシンでは、再起動スケジュールを作成できます。

プールされたマシンを含むデリバリーグループでは、仮想シングルセッションOSマシンは次のいずれかの状態になります。

- ランダムに割り当てられ、使用中
- 割り当てられておらず、未接続

静的マシンを含むデリバリーグループでは、仮想シングルセッションOSマシンは次のようになります。

- 永続的に割り当てられ、使用中
- 永続的に割り当てられ、未接続（ただし準備完了）
- 割り当てられておらず、未接続

通常の使用では、静的デリバリーグループには通常、永続的に割り当てられたマシンと割り当てられていないマシンの両方が含まれます。最初は、デリバリーグループの作成時に手動で割り当てられたマシンを除き、すべてのマシンが割り当てられていません。ユーザーが接続すると、マシンは永続的に割り当てられます。これらのデリバリーグループ内の割り当てられていないマシンは完全に電源管理できますが、永続的に割り当てられたマシンは部分的にしか管理できません。

- **プールとバッファー:** プールされたデリバリーグループと、割り当てられていないマシンを持つ静的デリバリーグループの場合、プール（この場合）とは、電源オン状態に保たれ、ユーザーが接続できる状態になっている、割り当てられていない、または一時的に割り当てられたマシンのセットです。ユーザーはログオン後すぐにマシンを取得します。プールサイズ（電源オン状態に保たれるマシンの数）は、時間帯によって構成可能です。静的デリバリーグループの場合は、SDKを使用してプールを構成します。

  バッファーとは、プール内のマシンの数がしきい値を下回ったときに電源がオンになる、割り当てられていないマシンの追加のスタンバイセットです。しきい値は、デリバリーグループサイズのパーセンテージです。大規模なデリバリーグループの場合、しきい値を超えるとかなりの数のマシンがオンになる可能性があります。そのため、デリバリーグループのサイズを慎重に計画するか、SDKを使用してデフォルトのバッファーサイズを調整してください。
- **電源状態タイマー:** 電源状態タイマーを使用すると、ユーザーが指定された時間切断された後にマシンを一時停止できます。たとえば、ユーザーが10分以上切断された場合、勤務時間外にマシンは自動的に一時停止します。

  タイマーは、平日と週末、およびピーク時と非ピーク時の間隔で構成できます。
- **永続的に割り当てられたマシンの部分的な電源管理:** 永続的に割り当てられたマシンについては、電源状態タイマーを設定できますが、プールやバッファーは設定できません。マシンは各ピーク期間の開始時にオンになり、各非ピーク期間の開始時にオフになります。消費されたマシンを補うために利用可能になるマシンの数について、割り当てられていないマシンで得られるようなきめ細かな制御はできません。

仮想シングルセッションOSマシンの電源管理

1. 左ペインで**Delivery Groups**を選択します。
2. グループを選択し、アクションバーで**Edit Delivery Group**をクリックします。
3. **Power Management**ページで、**Power manage machines**の**Weekdays**を選択します。デフォルトでは、平日は月曜日から金曜日です。

4. ランダムなデリバリーグループの場合、**Machines to be powered on**で**Edit**をクリックし、平日のプールサイズを指定します。次に、電源をオンにするマシンの数を選択します。
5. **Peak hours**で、各日のピーク時間と非ピーク時間を設定します。
6. 平日のピーク時間と非ピーク時間の電源状態タイマーを設定します。**During peak hours > When disconnected**で、デリバリーグループ内の切断されたマシンを一時停止するまでの遅延（分単位）を指定し、**Suspend**を選択します。**During off-peak hours > When disconnected**で、デリバリーグループ内のログオフされたマシンをシャットダウンするまでの遅延を指定し、**Shutdown**を選択します。このタイマーは、ランダムなマシンを持つデリバリーグループでは使用できません。
7. **Power manage machines**で**Weekend**を選択し、週末のピーク時間と電源状態タイマーを構成します。
8. **Apply**をクリックして変更を適用し、ウィンドウを開いたままにします。または、**Save**をクリックして変更を適用し、ウィンドウを閉じます。

SDKを使用して、次の操作を行います。

- 電源状態タイマーに応じてマシンを中断するのではなくシャットダウンするか、タイマーを接続解除ではなくログオフに基づいて設定したい場合。
- デフォルトの平日と週末の定義を変更する。
- 電源管理を無効にします。CTX217289を参照してください。

切断されたセッションを持つVDIマシンが異なる時間帯に移行する際の電源管理

> **重要:**
>
> この機能強化は、切断されたセッションを持つVDIマシンにのみ適用されます。ログオフされたセッションを持つVDIマシンには適用されません。
>
> 以前のリリースでは、アクション（切断アクション="**Suspend**" または "**Shutdown**"）が必要な時間帯に移行するVDIマシンは、電源がオンのままでした。このシナリオは、アクション（切断アクション="**Nothing**"）が不要な時間帯（ピーク時またはオフピーク時）にマシンが切断された場合に発生しました。

Citrix Virtual Apps and Desktops 7 1909以降、指定された切断時間が経過すると、宛先時間帯に構成されている切断アクションに応じて、マシンは中断または電源オフされます。

たとえば、VDIデリバリーグループに対して次の電源ポリシーを構成します。

- `PeakDisconnectAction`を「Nothing」に設定します
- `OffPeakDisconnectAction`を「Shutdown」に設定します
- `OffPeakDisconnectTimeout`を「10」に設定します

電源ポリシーの切断アクションに関する詳細については、https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/about_Broker_PowerManagement/#power-policyおよびhttps://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/Get-BrokerDesktopGroup/を参照してください。

以前のリリースでは、ピーク時にセッションが切断されたVDIマシンは、ピークからオフピークに移行しても電源がオンのままでした。Citrix Virtual Apps and Desktops 7 1909以降、期間移行時に`OffPeakDisconnectAction`および`OffPeakDisconnectTimeout`ポリシーアクションがVDIマシンに適用されます。その結果、マシンはオフピークに移行してから10分後に電源がオフになります。

以前の動作に戻したい場合（つまり、切断されたセッションを持つマシンがピークからオフピークへ、またはオフピークからピークへ移行しても何もアクションを実行しない場合）、次のいずれかを実行します:

- `LegacyPeakTransitionDisconnectedBehaviour`レジストリ値を`1`に設定します。これは以前の動作を有効にする*true*に相当します。デフォルトでは、値は`0`、つまり*false*であり、これは期間移行時に切断電源ポリシーアクションをトリガーします。
  - パス: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\DesktopServer`
  - 名前: `LegacyPeakTransitionDisconnectedBehaviour`
  - 種類: `REG_DWORD`
  - データ: `0x00000001 (1)`
- `Set-BrokerServiceConfigurationData` PowerShellコマンドを使用して設定を構成します。例:
  - `PS C:\> Set-BrokerServiceConfigurationData HostingManagement.LegacyPeakTransitionDisconnectedBehaviour -SettingValue $true`

期間移行時に電源ポリシーアクションを適用する前に、マシンは次の基準を満たす必要があります。

- 切断されたセッションがあること。

- 保留中の電源アクションがないこと。
- 異なる時間帯に移行するVDI（シングルセッション）デリバリーグループに属していること。
- 特定の時間帯（ピーク時またはオフピーク時）にセッションが切断され、電源アクションが割り当てられている期間に移行すること。

カタログの電源オン状態のVDAの割合を変更する

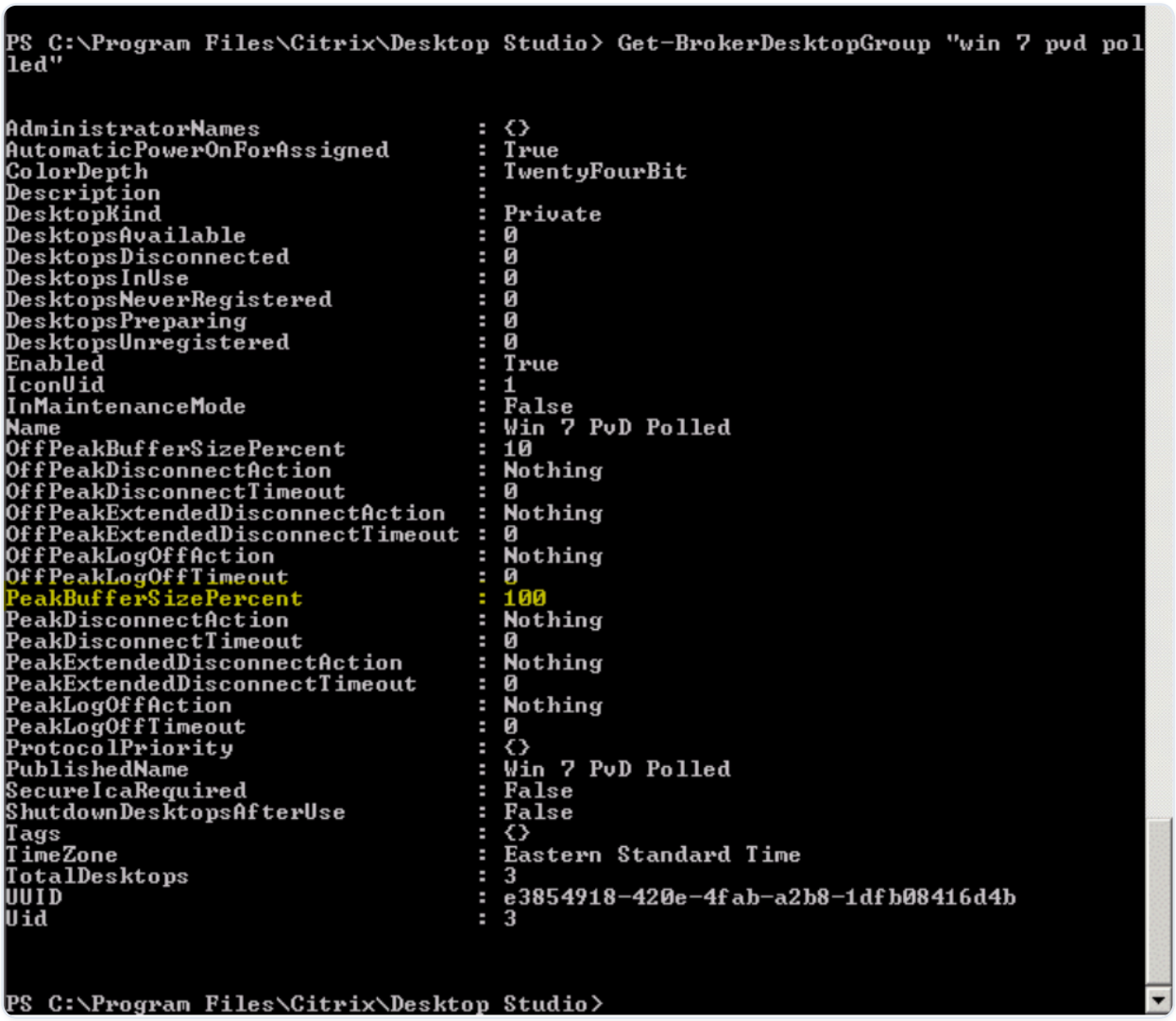
1. デリバリーグループの**電源管理**セクションから、デリバリーグループのピーク時間を調整します。
2. デスクトップグループ名をメモします。
3. 管理者権限でPowerShellを起動し、次のコマンドを実行します。「Desktop Group Name」を、実行中のVDAの割合が変更されたデスクトップグループの名前に置き換えます。

   ```
   asnp Citrix*
   ```

   ```
   # Set-BrokerDesktopGroup "Desktop Group Name" -PeakBufferSizePercent 100
   ```

   値が100の場合、VDAの100%が準備完了状態であることを意味します。
4. 次のコマンドを実行してソリューションを確認します。

   ```
   #Get-BrokerDesktopGroup "Desktop Group Name"
   ```



変更が有効になるまで最大1時間かかる場合があります。

ユーザーがログオフした後にVDAをシャットダウンするには、次のように入力します。

```
# Set-BrokerDesktopGroup "Desktop Group Name" -ShutDownDesktopsAfterUse $True
```

ピーク時にVDAを再起動して、ユーザーがログオフした後にすぐに使用できるようにするには、次のように入力します。

```
# Set-BrokerDesktopGroup "Desktop Group Name"
-AutomaticPowerOnForAssignedDuringPeak $True
```

セッション

- セッションのログオフまたは切断、またはユーザーへのメッセージ送信
- セッションのプレ起動とセッションの維持を構成する
- メンテナンスモードのマシンから切断された場合のセッション再接続を制御する

- セッションローミングを構成する

セッションのログオフまたは切断

1. 左ペインで**Delivery Groups**を選択します。
2. デリバリーグループを選択し、アクションバーで**View Machines**を選択します。
3. 中央ペインでマシンを選択し、アクションバーで**View Sessions**を選択してから、セッションを選択します。
    - または、中央ペインで**Session**タブを選択し、セッションを選択します。
4. セッションからログオフするには、アクションバーで**Log off**を選択します。セッションが閉じられ、ユーザーはログアウトされます。マシンが特定のユーザーに割り当てられていない限り、他のユーザーが利用できるようになります。
5. セッションを切断するには、アクションバーで**Disconnect**を選択します。アプリケーションはセッション内で実行を継続し、マシンはそのユーザーに割り当てられたままになります。ユーザーは同じマシンに再接続できます。

シングルセッションOSマシンでは、未使用のセッションを自動的に処理するように電源状態タイマーを構成できます。詳細については、「電源管理されたマシン」を参照してください。

デリバリーグループにメッセージを送信する

1. 左ペインで**Delivery Groups**を選択します。
2. デリバリーグループを選択し、アクションバーで**View Machines**を選択します。
3. 中央ペインで、メッセージを送信するマシンを選択します。
4. アクションバーで**View Sessions**を選択します。
5. 中央ペインで、すべてのセッションを選択し、アクションバーで**メッセージの送信**を選択します。
6. メッセージを入力し、**OK**をクリックします。必要に応じて、重大度レベルを指定できます。オプションには、**重大**、**質問**、**警告**、**情報**があります。

または、Citrix Directorを使用してメッセージを送信することもできます。詳しくは、「ユーザーへのメッセージの送信」を参照してください。

デリバリーグループでセッションの事前起動とセッションの維持を構成する

これらの機能は、マルチセッションOSマシンでのみサポートされています。

セッションの事前起動とセッションの維持機能は、要求される前にセッションを開始すること（セッションの事前起動）と、ユーザーがすべてのアプリケーションを閉じた後もアプリケーションセッションをアクティブに保つこと（セッションの維持）により、指定されたユーザーがアプリケーションにすばやくアクセスできるようにします。

デフォルトでは、セッションの事前起動とセッションの維持は使用されません。セッションは、ユーザーがアプリケーションを起動したときに開始（起動）され、セッション内の最後に開いたアプリケーションが閉じるまでアクティブなままになります。

考慮事項:

- デリバリーグループはアプリケーションをサポートしている必要があり、マシンはマルチセッションOS用のVDA（最小バージョン7.6）を実行している必要があります。
- これらの機能は、Windows向けCitrix Workspaceアプリを使用している場合にのみサポートされ、追加のCitrix Workspaceアプリ構成も必要です。手順については、お使いのWindows向けCitrix Workspaceアプリバージョンの製品ドキュメントで「session prelaunch」を検索してください。
- Citrix Workspace app for HTML5はサポートされていません。
- セッションの事前起動を使用している場合、ユーザーのマシンがサスペンドまたは休止状態になると、事前起動は機能しません（セッションの事前起動設定にかかわらず）。ユーザーはマシン/セッションをロックできます。ただし、ユーザーがCitrix Workspaceアプリからログオフすると、セッションは終了し、事前起動は適用されなくなります。
- セッションの事前起動を使用している場合、物理クライアントマシンはサスペンドまたは休止状態の電源管理機能を使用できません。クライアントマシンのユーザーはセッションをロックできますが、ログオフしないでください。
- 事前起動および維持されているセッションは同時接続ライセンスを消費しますが、これは接続されている場合に限ります。ユーザー/デバイスライセンスを使用している場合、ライセンスは90日間有効です。未使用の事前起動および維持されているセッションは、デフォルトで15分後に切断されます。この値はPowerShellで構成できます（`New/Set-BrokerSessionPreLaunch` コマンドレット）。
- これらの機能が互いに補完し合うように調整するには、ユーザーのアクティビティパターンを慎重に計画し、監視することが不可欠です。最適な構成は、ユーザーがより早くアプリケーションを利用できるという利点と、ライセンスの使用とリソースの割り当てにかかるコストとのバランスを取ります。
- Citrix Workspaceアプリで、スケジュールされた時刻にセッションの事前起動を構成することもできます。

未使用の事前起動セッションと残存セッションがアクティブなままになる期間

ユーザーがアプリケーションを起動しない場合に、未使用のセッションがアクティブなままになる期間を指定する方法はいくつかあります。構成されたタイムアウトとサーバー負荷のしきい値です。これらすべてを構成できます。最初に発生したイベントにより、未使用のセッションが終了します。

- **タイムアウト:** 構成されたタイムアウトは、未使用の事前起動セッションまたは残存セッションがアクティブなままになる分、時間、または日数を指定します。タイムアウトを短く設定しすぎると、事前起動セッションは、ユーザーにアプリケーションへのより迅速なアクセスという利点を提供する前に終了します。タイムアウトを長く設定しすぎると、サーバーに十分なリソースがないため、受信ユーザー接続が拒否される可能性があります。

  このタイムアウトは、管理コンソールからではなく、SDKからのみ有効にできます (`New/Set-BrokerSessionPreLaunch` コマンドレット)。タイムアウトを無効にすると、そのデリバリーグループのコンソール表示や**デリバリーグループの編集**ページには表示されません。
- **しきい値:** サーバー負荷に基づいて事前起動セッションと残存セッションを自動的に終了することで、サーバーリソースが利用可能であると仮定して、セッションが可能な限り開いたままになることを保証します。未使用の事前起動セッションと残存セッションは、新しいユーザーセッションにリソースが必要なときに自動的に終了されるため、接続拒否を引き起こしません。

  2つのしきい値を構成できます。デリバリーグループ内のすべてのサーバーの平均負荷率と、グループ内の単一サーバーの最大負荷率です。しきい値を超えると、事前起動または残存状態にあった時間が最も長いセッションが終了されます。負荷がしきい値を下回るまで、セッションは1分間隔で1つずつ終了されます。しきい値を超えている間は、新しい事前起動セッションは開始されません。

Controllerに登録されていないVDAを持つサーバーと、メンテナンスモードのサーバーは、完全にロードされていると見なされます。計画外の停止により、容量を解放するために事前起動セッションと残存セッションが自動的に終了します。

セッションの事前起動を有効にするには

1. グループを選択し、アクションバーで**デリバリーグループの編集**をクリックします。
2. **アプリケーションの事前起動**ページで、セッションを起動するタイミングを選択して、セッションの事前起動を有効にします。
   - ユーザーがアプリケーションを起動したとき。これはデフォルト設定です。セッションの事前起動は無効になっています。

- デリバリーグループ内の任意のユーザーがCitrix Workspaceアプリ for Windowsにログオンしたとき。
- ユーザーおよびユーザーグループのリスト内のいずれかのユーザーがCitrix Workspaceアプリ for Windowsにログオンしたとき。このオプションを選択する場合は、ユーザーまたはユーザーグループも指定してください。

アプリケーションの事前起動セッションページ(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/dws-session-2.png)

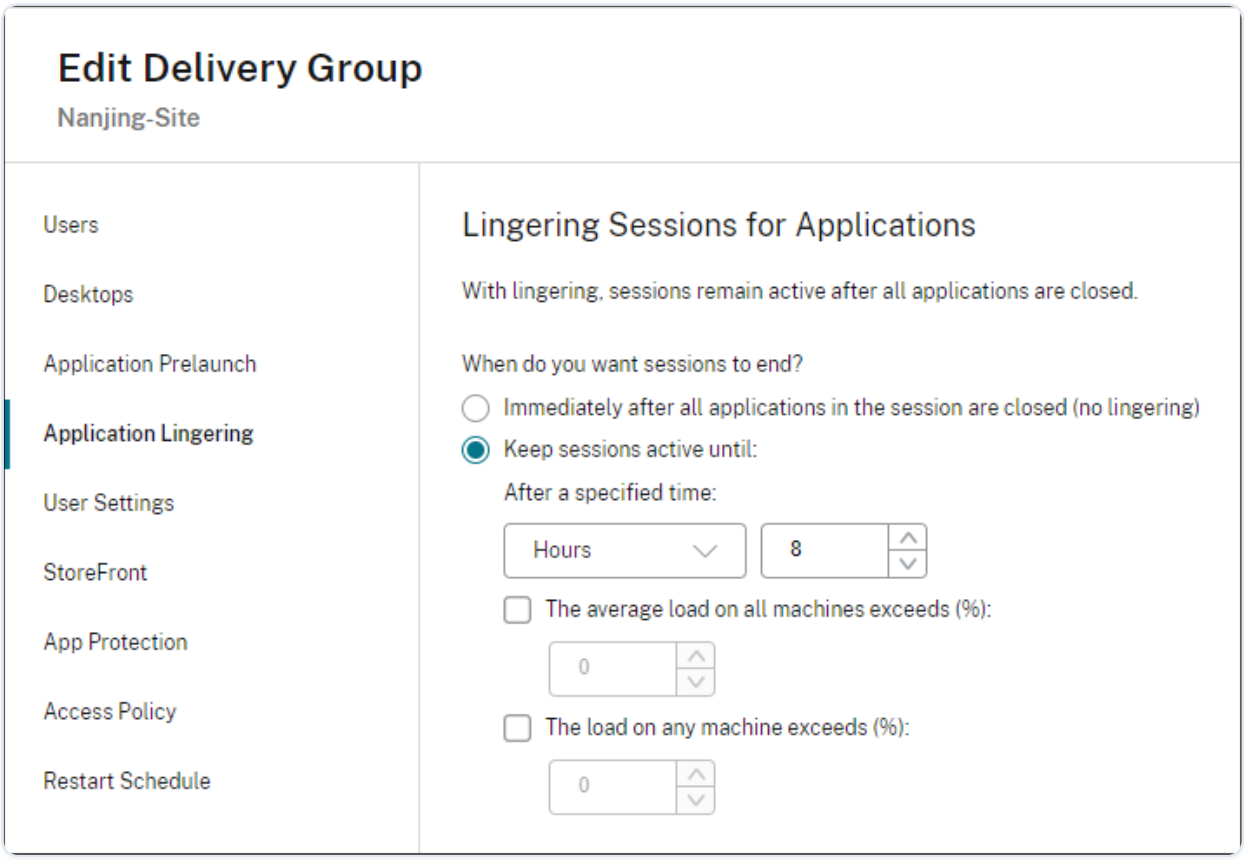
3. ユーザーがアプリケーションを起動すると、事前起動されたセッションは通常のセッションに置き換えられます。ユーザーがアプリケーションを起動しない場合（事前起動されたセッションが未使用の場合）、以下の設定がそのセッションがアクティブなままになる期間に影響します。

   - 指定された時間間隔が経過したとき。時間間隔は変更できます（1〜99日、1〜2376時間、または1〜142,560分）。
   - デリバリーグループ内のすべてのマシンの平均負荷が指定された割合（1〜99%）を超えたとき。
   - デリバリーグループ内のいずれかのマシンの負荷が指定された割合（1〜99%）を超えたとき。

   まとめ：事前起動されたセッションは、ユーザーがアプリケーションを起動する、指定された時間が経過する、または指定された負荷しきい値を超える、のいずれかのイベントが発生するまでアクティブなままです。

セッションの維持を有効にするには

1. 左側のペインで**デリバリーグループ**を選択します。
2. グループを選択し、アクションバーで**デリバリーグループの編集**をクリックします。
3. **アプリケーションの維持**ページで、**セッションをアクティブなままにする期間**を選択して、セッションの維持を有効にします。



4. ユーザーが別のアプリケーションを起動しない場合、残存セッションがアクティブなままになる期間に影響する設定がいくつかあります。

   - 指定された時間間隔が経過した場合。時間間隔は、1～99日、1～2376時間、または1～142,560分に変更できます。
   - デリバリーグループ内のすべてのマシンの平均負荷が指定された割合（1～99%）を超えた場合。
   - デリバリーグループ内のいずれかのマシンの負荷が指定された割合（1～99%）を超えた場合。

   まとめ：残存セッションは、ユーザーがアプリケーションを起動する、指定された時間が経過する、または指定された負荷しきい値を超える、のいずれかのイベントが発生するまでアクティブなままです。

メンテナンスモードのマシンから切断された場合のセッション再接続を制御する

> **注：**
>
> この機能はPowerShellでのみ利用可能です。

> メンテナンスモードのマシンで切断されたセッションが、デリバリーグループ内のマシンに再接続できるかどうかを制御できます。

バージョン2106より前は、メンテナンスモードのマシンから切断されたシングルセッションのプールされたデスクトップセッションの再接続は許可されていませんでした。バージョン2106以降では、メンテナンスモードのマシンから切断された後の再接続（セッションの種類に関係なく）を許可または禁止するようにデリバリーグループを構成できます。

デリバリーグループを作成または編集する際（`New-BrokerDesktopGroup`、`Set-BrokerDesktopGroup`）、`-AllowReconnectInMaintenanceMode <boolean>`パラメーターを使用して、メンテナンスモードのマシンから切断されたマシンへの再接続を許可または禁止します。

- trueに設定すると、セッションはグループ内のマシンに再接続できます。
- 「false」に設定されている場合、セッションはグループ内のマシンに再接続できません。

デフォルト値:

- シングルセッション: 無効
- マルチセッション: 有効

セッションローミングの構成

デフォルトでは、デリバリーグループに対してセッションローミングが有効になっています。セッションはユーザーとともにクライアントデバイス間をローミングします。ユーザーがセッションを起動し、別のデバイスに移動すると、同じセッションが使用され、アプリケーションは両方のデバイスで同時に利用可能になります。複数のデバイスでアプリケーションを表示できます。アプリケーションは、デバイスや現在のセッションの有無にかかわらず追従します。多くの場合、アプリケーションに割り当てられたプリンターやその他のリソースも追従します。または、PowerShellを使用することもできます。詳しくは、「セッションローミング」を参照してください。

アプリケーションのセッションローミングの構成

アプリケーションのセッションローミングを構成するには、次の手順に従います。

1. コンソールで、左側のペインの**デリバリーグループ**を選択します。
2. グループを選択し、アクションバーで**「デリバリーグループの編集」**を選択します。
3. **「ユーザー」ページで、「ユーザーがデバイス間を移動するときにセッションをローミングする」**チェックボックスをオンにして、セッションローミングを有効にします。

- 有効にすると、ユーザーがアプリケーションセッションを起動して別のデバイスに移動した場合、同じセッションが使用され、両方のデバイスで利用可能になります。無効にすると、セッションはデバイス間をローミングしなくなります。

4. **「OK」**を選択して変更を適用し、ウィンドウを閉じます。

デスクトップのセッションローミングを構成する

デスクトップのセッションローミングを構成するには、次の手順に従います。

1. コンソールで、左側のペインの**デリバリーグループ**を選択します。
2. グループを選択し、アクションバーで**編集**を選択します。
3. **デスクトップ**ページで、デスクトップを選択し、**編集**を選択します。
4. **セッションローミング**チェックボックスをオンにして、セッションローミングを有効にします。

- 有効にすると、ユーザーがデスクトップを起動してから別のデバイスに移動した場合、同じセッションが使用され、アプリケーションは両方のデバイスで利用可能になります。無効にすると、セッションはデバイス間をローミングしなくなります。

OKを選択して変更を適用し、ウィンドウを閉じます。

トラブルシューティング

- Delivery Controllerに登録されていないVDAは、ブローカーセッションの起動時に考慮されません。これにより、利用可能なはずのリソースが十分に活用されないことになります。VDAが登録されない理由はさまざまであり、その多くは管理者がトラブルシューティングできます。詳細表示には、カタログ作成ウィザードと、デリバリーグループにカタログを追加した後のトラブルシューティング情報が表示されます。

  デリバリーグループを作成した後、デリバリーグループの詳細ペインには、登録可能だが登録されていないマシンの数が表示されます。たとえば、1台以上のマシンが電源オンでメンテナンスモードではないが、現在Controllerに登録されていない場合などです。「登録されていないが、登録されるべき」マシンを表示するときは、詳細ペインの**トラブルシューティング**タブで考えられる原因と推奨される是正措置を確認してください。

  機能レベルに関するメッセージについては、「VDAのバージョンと機能レベル」を参照してください。

  VDA登録のトラブルシューティングについては、「CTX136668」を参照してください。

- デリバリーグループの表示では、詳細ペインの**インストール済みVDAバージョン**が、マシンに実際にインストールされているバージョンと異なる場合があります。マシンのWindowsのプログラムと機能の表示には、実際のVDAバージョンが表示されます。
- **電源状態不明**のステータスのマシンについては、ガイダンスとしてCTX131267を参照してください。

アプリケーショングループの作成

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

はじめに

アプリケーショングループを使用すると、アプリケーションのコレクションを管理できます。異なるデリバリーグループ間で共有されるアプリケーション、またはデリバリーグループ内のユーザーのサブセットによって使用されるアプリケーションに対してアプリケーショングループを作成します。アプリケーショングループはオプションであり、同じアプリケーションを複数のデリバリーグループに追加する代替手段を提供します。デリバリーグループを複数のアプリケーショングループに関連付けたり、アプリケーショングループを複数のデリバリーグループに関連付けたりできます。

アプリケーショングループを使用すると、より多くのデリバリーグループを使用する場合と比較して、アプリケーション管理とリソース制御の利点が得られます。

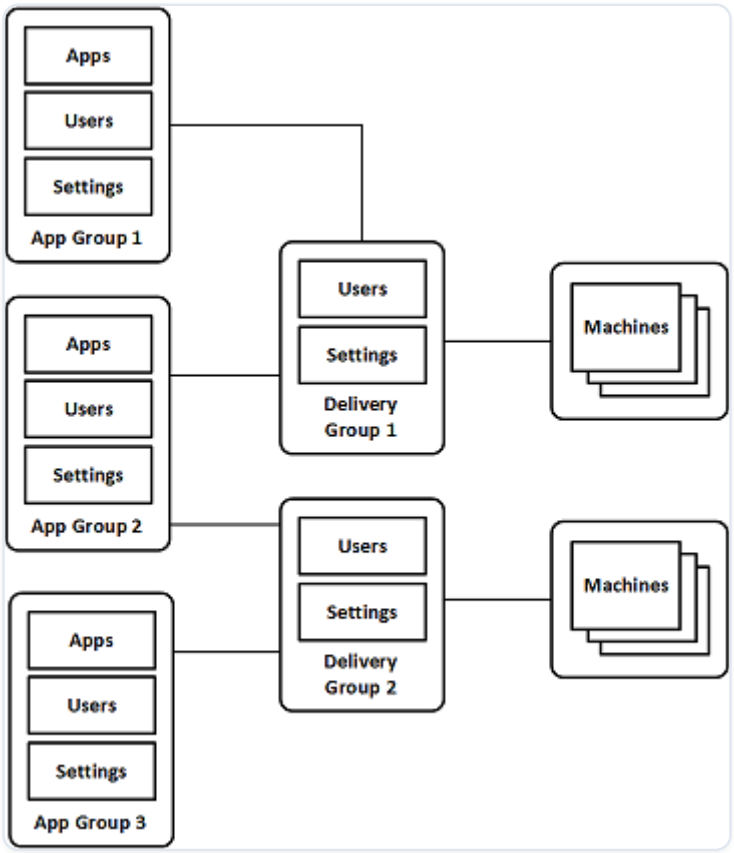
- アプリケーションとその設定を論理的にグループ化することで、それらのアプリケーションを単一の単位として管理できます。たとえば、同じアプリケーションを個々のデリバリーグループに1つずつ追加（公開）する必要はありません。
- アプリケーショングループ間のセッション共有は、リソース消費を節約できます。それ以外の場合、アプリケーショングループ間のセッション共有を無効にすることが有益な場合もあります。
- タグ制限機能を使用すると、選択したデリバリーグループ内のマシンのサブセットのみを考慮して、アプリケーショングループからアプリケーションを公開できます。タグ制限を使用すると、既存のマシンを複数の公開タスクに使用できるため、追加のマシンの展開と管理に関連す

るコストを節約できます。タグ制限は、デリバリーグループ内のマシンを細分化（またはパーティション分割）するものと考えることができます。タグ制限付きのアプリケーショングループまたはデスクトップを使用すると、デリバリーグループ内のマシンのサブセットを分離してトラブルシューティングする際に役立ちます。

構成例

例 1:

次の図は、アプリケーショングループを含むCitrix Virtual Apps and Desktops展開を示しています。



この構成では、アプリケーションはデリバリーグループではなくアプリケーショングループに追加されます。デリバリーグループは、どのマシンが使用されるかを指定します。（図には示されていませんが、マシンはマシンカタログ内にあります。）

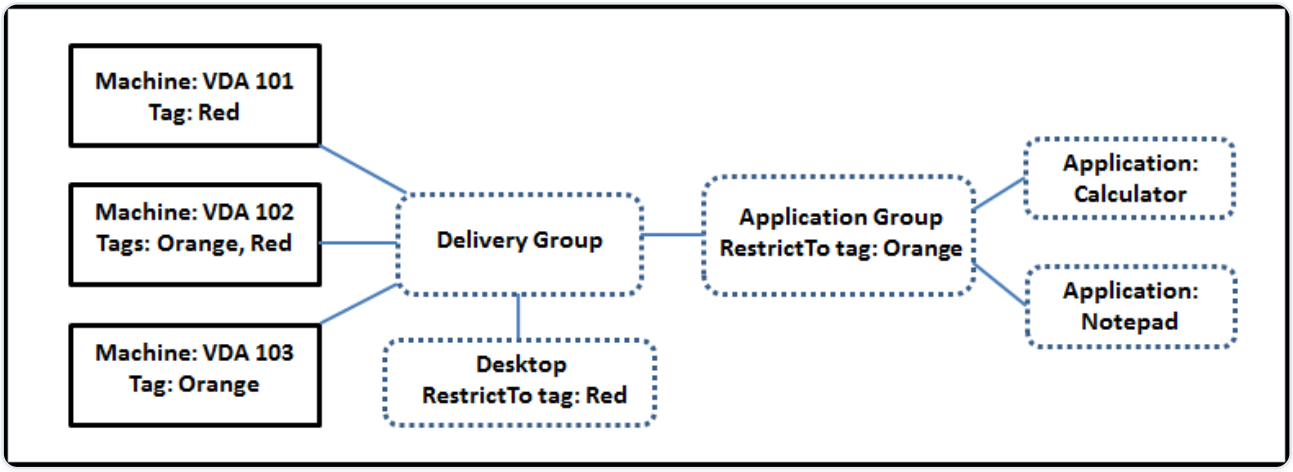
アプリケーショングループ1はデリバリーグループ1に関連付けられています。アプリケーショングループ1で指定されたユーザーがアプリケーショングループ1のアプリケーションにアクセスします。これらのグループは、デリバリーグループ1のユーザーリストにも含まれている場合にのみ表示されます。この構成は、アプリケーショングループのユーザーリストが、関連付けられたデリバリーグループのユーザーリストのサブセット（制限）であるというガイダンスに従います。アプリケーショングループ1の設定（アプリケーショングループ間のアプリケーションセッション共有、関連付けられたデリバリーグループなど）は、そのグループ内のアプリケーションとユーザーに

適用されます。デリバリーグループ1の設定は、アプリケーショングループ1と2のユーザーに適用されます。これは、これらのアプリケーショングループがそのデリバリーグループに関連付けられているためです。

アプリケーショングループ2は、2つのデリバリーグループ（1と2）に関連付けられています。これらの各デリバリーグループには、アプリケーショングループ2で優先度が割り当てられ、アプリケーションが起動されるときにデリバリーグループがチェックされる順序を示します。優先度が等しいデリバリーグループはロードバランスされます。アプリケーショングループ2で指定されたユーザーがアプリケーショングループ2のアプリケーションにアクセスします。ただし、それらのユーザーはデリバリーグループ1とデリバリーグループ2のユーザーリストにも含まれている必要があります。

例 2:

このシンプルなレイアウトでは、タグ制限を使用して、特定のデスクトップおよびアプリケーションの起動に考慮されるマシンを制限します。このサイトには、1つの共有デリバリーグループ、1つの公開デスクトップ、および2つのアプリケーションで構成された1つのアプリケーショングループがあります。



3台のマシン（VDA 101～103）のそれぞれにタグが追加されています。

アプリケーショングループは「Orange」タグ制限付きで作成されました。その各アプリケーションは、そのデリバリーグループ内で「Orange」タグを持つマシン（VDA 102および103）でのみ起動されます。

アプリケーショングループ（およびデスクトップ）でタグ制限を使用するためのより包括的な例とガイダンスについては、「タグ」を参照してください。

ガイダンスと考慮事項

Citrixでは、アプリケーションをアプリケーショングループまたはデリバリーグループのいずれかに追加することをお勧めします。両方に追加することはお勧めしません。そうしないと、2種類のグループにアプリケーションが存在することで複雑さが増し、管理が難しくなる可能性があります。

デフォルトでは、アプリケーショングループは有効になっています。アプリケーショングループを作成した後、グループを編集してこの設定を変更できます。「アプリケーショングループの管理」を参照してください。

デフォルトでは、アプリケーショングループ間のアプリケーションセッション共有は有効になっています。「アプリケーショングループ間のセッション共有」を参照してください。

Citrixでは、デリバリーグループを現在のバージョンにアップグレードすることをお勧めします。このプロセスには、次のものが必要です。

1. デリバリーグループで使用されているマシン上のVDAをアップグレードする。
2. それらのマシンを含むマシンカタログのアップグレード。
3. デリバリーグループのアップグレード。

詳細については、「デリバリーグループの管理」を参照してください。

アプリケーショングループを使用するには、コアコンポーネントが最小バージョン7.9である必要があります。

アプリケーショングループを作成するには、Delivery Group Administrator の組み込みロールの委任管理権限が必要です。詳細については、「委任管理」(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/manage-deployment/delegated-administration.html) を参照してください。

この記事では、アプリケーションを複数のアプリケーショングループに「関連付ける」ことについて言及しています。これは、利用可能なソースからそのアプリケーションのインスタンスを追加する操作とは区別されます。同様に、デリバリーグループは、互いの追加やコンポーネントではなく、アプリケーショングループに関連付けられます。

アプリケーショングループとのセッション共有

アプリケーションセッション共有が有効になっている場合、すべてのアプリケーションは同じアプリケーションセッションで起動します。これにより、より多くのアプリケーションセッションを起動するコストが削減され、コピー＆ペースト操作など、クリップボードを使用するアプリケーション機能の使用が可能になります。ただし、状況によってはセッション共有をクリアできます。

アプリケーショングループを使用する場合、デリバリーグループのみを使用する場合に利用できる標準のセッション共有動作を拡張する、次の3つの方法でアプリケーションセッション共有を構成できます。

- アプリケーショングループ間でセッション共有が有効。
- 同じアプリケーショングループ内のアプリケーション間でのみセッション共有が有効。
- セッション共有が無効。

アプリケーショングループ間のセッション共有

アプリケーショングループ間でアプリケーションセッション共有を有効にすることも、または、同じアプリケーショングループ内のアプリケーションにのみアプリケーションセッション共有を制限するために無効にすることもできます。

- **アプリケーショングループ間のセッション共有を有効にすることが役立つ例:**

  アプリケーショングループ1にはWordやExcelなどのMicrosoft Officeアプリケーションが含まれています。アプリケーショングループ2にはメモ帳や電卓などの他のアプリケーションが含まれており、両方のアプリケーショングループが同じデリバリーグループに接続されています。両方のアプリケーショングループにアクセスできるユーザーがWordを起動してアプリケーションセッションを開始し、次にメモ帳を起動します。コントローラーが、ユーザーの既存のWordを実行しているセッションがメモ帳の実行に適していると判断した場合、メモ帳は既存のセッション内で起動されます。既存のセッションからメモ帳を実行できない場合（たとえば、タグ制限によってセッションが実行されているマシンが除外される場合など）、セッション共有を使用するのではなく、適切なマシン上に新しいセッションが作成されます。

- **アプリケーショングループ間のセッション共有を無効にすることが役立つ例:**

  同じマシンにインストールされている他のアプリケーションとうまく相互運用できない一連のアプリケーションの構成。たとえば、同じソフトウェアスイートの2つの異なるバージョンや、同じWebブラウザーの2つの異なるバージョンなどです。ユーザーが同じセッションで両方のバージョンを起動することを許可しないようにしたい場合。

  ソフトウェアスイートのバージョンごとにアプリケーショングループを作成し、各バージョンのソフトウェアスイートのアプリケーションを対応するアプリケーショングループに追加します。これらのアプリケーショングループのそれぞれでグループ間のセッション共有が無効になっている場合、それらのグループで指定されたユーザーは、同じバージョンのアプリケーションを同じセッションで実行できます。ユーザーは同時に他のアプリケーションを実行できますが、同じセッションでは実行できません。異なるバージョンのアプリケーション、またはアプリケーショングループに含まれていないアプリケーションを起動すると、そのアプリケーションは新しいセッションで起動されます。

このアプリケーショングループ間のセッション共有機能は、セキュリティサンドボックス機能ではありません。これは完璧ではなく、ユーザーが他の手段（例えば、Windows Explorer経由など）でセッションにアプリケーションを起動するのを防ぐことはできません。

マシンが容量に達している場合、新しいセッションはそのマシンでは開始されません。必要に応じて、セッション共有を使用して、新しいアプリケーションがそのマシンの既存のセッションで開始されます。

アプリケーションセッション共有が許可されているアプリケーショングループに対してのみ、事前起動セッションを利用可能にできます。（セッションリンガー機能を使用するセッションは、すべてのアプリケーショングループで利用可能です。）これらの機能は、アプリケーショングループに関連付けられている各デリバリーグループで有効にして構成する必要があります。アプリケーショングループ内でこれらを構成することはできません。

デフォルトでは、アプリケーショングループを作成する際に、アプリケーショングループ間のアプリケーションセッション共有が有効になります。グループ作成時にこれを変更することはできません。アプリケーショングループを作成した後、グループを編集してこの設定を変更できます。アプリケーショングループの管理を参照してください。

アプリケーショングループ内でのセッション共有を無効にする

同じアプリケーショングループ内のアプリケーション間でのアプリケーションセッション共有を防ぐことができます。

- **アプリケーショングループ内でのセッション共有を無効にすることが役立つ例:**

  ユーザーに、別々のモニターでアプリケーションの複数の同時フルスクリーンセッションにアクセスさせたい場合。

  アプリケーショングループを作成し、そこにアプリケーションを追加します。

デフォルトでは、アプリケーショングループを作成すると、アプリケーションセッション共有が有効になります。グループの作成時にこの設定を変更することはできません。アプリケーショングループを作成した後、グループを編集してこの設定を変更できます。「アプリケーショングループの管理」を参照してください。

アプリケーショングループを作成する

アプリケーショングループを作成するには：

1. Web Studioにサインインします。

2. 左側のペインで［**アプリケーション**］を選択し、［**アプリケーショングループ**］タブを選択します。
3. フォルダーを使用してアプリケーショングループを整理するには、**アプリケーショングループ**ルートフォルダーの下にフォルダーを作成します。詳細については、フォルダーを使用してアプリケーショングループを整理するを参照してください。
4. グループを作成するフォルダーを選択し、**アプリケーション グループの作成**をクリックします。グループ作成ウィザードが**はじめに**ページで起動します。このページは、今後のウィザード起動時に表示しないように設定できます。
5. ウィザードに従って、以下に説明するページで設定を構成します。各ページでの作業が完了したら、**次へ**を選択して**概要**ページに進みます。

手順1. デリバリーグループ

デリバリーグループページには、すべてのデリバリーグループと、各グループに含まれるマシンの数が一覧表示されます。

- 「**互換性のあるデリバリーグループ**」リストには、選択可能なデリバリーグループが含まれています。互換性のあるデリバリーグループには、ランダムな（永続的または静的に割り当てられていない）マルチセッションまたはシングルセッションOSマシンが含まれます。
- 「**互換性のないデリバリーグループ**」リストには、選択できないデリバリーグループが含まれています。各エントリには、静的に割り当てられたマシンが含まれるなど、互換性がない理由が説明されています。

アプリケーショングループは、アプリケーションを配信できる共有（プライベートではない）マシンを含むデリバリーグループに関連付けることができます。

以下の両方の条件が満たされている場合、デスクトップのみを配信する共有マシンを含むデリバリーグループを選択することもできます。

- デリバリーグループに共有マシンが含まれており、XenDesktopバージョン7.9より前のバージョンで作成されていること。
- デリバリーグループの編集権限があること。

アプリケーショングループ作成ウィザードがコミットされると、デリバリーグループの種類は自動的に「デスクトップとアプリケーション」に変換されます。

関連付けられたデリバリーグループがないアプリケーショングループを作成することはできますが（アプリケーションを整理するため、または現在使用されていないアプリケーションのストレージとして機能させるためなど）、少なくとも1つのデリバリーグループが指定されるまで、そのアプリケーショングループをアプリケーションの配信に使用することはできません。また、デ

リバリーグループが指定されていない場合、「**スタートから**」メニューソースからアプリケーショングループにアプリケーションを追加することはできません。

選択したデリバリーグループは、アプリケーションの配信に使用されるマシンを指定します。アプリケーショングループに関連付けるデリバリーグループの横にあるチェックボックスをオンにします。

タグ制限を追加するには、「**タグを持つマシンへの起動を制限する**」を選択し、ドロップダウンリストからタグを選択します。

手順2. ユーザー

アプリケーショングループでアプリケーションユーザーを指定します。前のページで選択したデリバリーグループ内のすべてのユーザーとユーザーグループを許可するか、それらのデリバリーグループから特定のユーザーとユーザーグループを選択します。指定されたユーザーに利用を制限する場合、デリバリーグループで指定されたユーザーのうち、アプリケーショングループで指定されたユーザーのみが、このグループのアプリケーションにアクセスできます。基本的に、アプリケーショングループのユーザーリストは、デリバリーグループのユーザーリストに対するフィルターとして機能します。

認証されていないユーザーによるアプリケーションの使用の有効化または無効化は、アプリケーショングループではなく、デリバリーグループでのみ利用できます。

展開でユーザーリストが指定される場所については、「ユーザーリストが指定される場所」を参照してください。

ステップ3. アプリケーション

知っておくと良いこと:

- デフォルトでは、追加する新しいアプリケーションは「**Applications**」という名前のフォルダーに配置されます。別のフォルダーを指定できます。アプリケーションを追加しようとしたときに、そのフォルダーに同じ名前のアプリケーションが存在する場合、追加しようとしているアプリケーションの名前を変更するよう求められます。提案された一意の名前に同意すると、その新しい名前でアプリケーションが追加されます。そうでない場合は、追加する前に自分で名前を変更する必要があります。詳細については、「アプリケーションフォルダーの管理」を参照してください。
- アプリケーションのプロパティ（設定）は、追加時または後で変更できます。「アプリケーションプロパティの変更」を参照してください。同じ名前の2つのアプリケーションを同じユーザーに公開する場合、Web Studioで「**アプリケーション名（ユーザー向け）**」プロパティ

を変更します。そうしないと、ユーザーはCitrix Workspaceアプリで重複する名前を目にします。

- アプリケーションを複数のアプリケーショングループに追加する場合、それらのすべてのグループでアプリケーションを表示するのに十分な権限がないと、表示の問題が発生する可能性があります。そのような場合は、より高い権限を持つ管理者に相談するか、アプリケーションが追加されたすべてのグループを含むようにスコープを拡張してください。

アプリケーションソースを表示するには、ドロップダウンメニューから「**追加**」をクリックします。

- **スタートメニューから**：選択したデリバリーグループ内のマシンで検出されたアプリケーション。このソースを選択すると、検出されたアプリケーションのリストが表示された新しいページが起動します。追加するアプリケーションのチェックボックスをオンにして、「**OK**」をクリックします。

  以下のいずれかを選択した場合、このソースは選択できません。

  - 関連付けられたデリバリーグループがないアプリケーショングループ。
  - 関連付けられたデリバリーグループにマシンが含まれていないアプリケーショングループ。
  - マシンが含まれていないデリバリーグループ。

- **手動で定義**：サイト内またはネットワーク内の別の場所にあるアプリケーション。このソースを選択すると、実行可能ファイルへのパス、作業ディレクトリ、オプションのコマンドライン引数、管理者とユーザーの表示名を入力する新しいページが起動します。この情報を入力したら、「**OK**」をクリックします。
- **既存**：以前にサイトに追加されたアプリケーション。このソースを選択すると、検出されたアプリケーションのリストが表示された新しいページが起動します。追加するアプリケーションのチェックボックスをオンにして、「**OK**」をクリックします。サイトにアプリケーションがない場合、このソースは選択できません。
- **App-V**：App-Vパッケージ内のアプリケーション。このソースを選択すると、**App-Vサーバー**または**アプリケーションライブラリ**を選択する新しいページが起動します。表示された画面から、追加するアプリケーションのチェックボックスをオンにして、「**OK**」をクリックします。詳細については、「App-Vアプリケーションの展開と配信」を参照してください。サイトでApp-Vが構成されていない場合、このソースは選択できません（または表示されない場合があります）。

記載されているように、「**追加**」ドロップダウンメニューの一部のエントリは、その種類の有効なソースがない場合、選択できません。互換性のないソースはまったく表示されません（たとえ

ば、アプリケーショングループにアプリケーショングループを追加することはできないため、アプリケーショングループを作成するときにそのソースは表示されません）。

ステップ4. スコープ

このページは、以前にカスタムスコープを作成した場合にのみ表示されます。デフォルトでは、**すべて**のスコープが選択されています。詳細については、委任管理を参照してください。

ステップ5. 概要

アプリケーショングループの名前を入力します。説明を（オプションで）入力することもできます。

概要情報を確認し、**「完了」**をクリックします。

アプリケーショングループの管理

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

はじめに

この記事では、作成したアプリケーショングループを管理する方法について説明します。

アプリケーショングループまたはデリバリーグループ内のアプリケーションの管理方法については、アプリケーションを参照してください。これには、以下の方法が含まれます。

- アプリケーショングループ内のアプリケーションを追加または削除する。
- アプリケーショングループの関連付けを変更する。

アプリケーショングループの管理には、Delivery Group Administratorの組み込みロールの委任管理権限が必要です。詳細については、委任管理を参照してください。

アプリケーショングループを有効または無効にする

アプリケーショングループが有効になっている場合、そのグループに追加されたアプリケーションを配信できます。アプリケーショングループを無効にすると、そのグループ内の各アプリケーションが無効になります。ただし、それらのアプリケーションが他の有効なアプリケーショングループにも関連付けられている場合、それらの他のグループから配信できます。アプリケーションがアプリケーショングループに関連付けられたデリバリーグループに明示的に追加された場合、アプリケーショングループを無効にしても、それらのデリバリーグループ内のアプリケーションには影響しません。

アプリケーショングループは作成時に有効になります。グループ作成時にこの設定を変更することはできません。

1. 左ペインで**アプリケーション**を選択し、**アプリケーショングループ**タブを選択します。
2. アプリケーショングループを選択し、アクションバーで**アプリケーショングループの編集**を選択します。
3. **設定**ページで、**アプリケーショングループを有効にする**チェックボックスをオンまたはオフにします。
4. ウィンドウを開いたままにするには**適用**をクリックし、変更を適用してウィンドウを閉じるには**保存**をクリックします。

アプリケーショングループ間のアプリケーションセッション共有を有効または無効にする

アプリケーションセッション共有は、アプリケーショングループの作成時に有効になります。この構成は、グループの作成時に変更できません。詳細については、「アプリケーショングループとのセッション共有」を参照してください。

1. 左側のペインで を選択し、 タブを選択します。
2. アプリケーショングループを選択し、アクションバーで を選択します。
3. ページで、 チェックボックスをオンまたはオフにします。
4. をクリックしてウィンドウを開いたままにするか、 をクリックして変更を適用し、ウィンドウを閉じます。

アプリケーショングループ内でのアプリケーションセッション共有を無効にする

同じアプリケーショングループ内のアプリケーション間でのセッション共有は、アプリケーショングループの作成時にデフォルトで有効になります。アプリケーショングループ間でのアプリケー

ションセッション共有を無効にしても、同じアプリケーショングループ内のアプリケーション間でのセッション共有は有効のままです。

PowerShell SDKを使用して、アプリケーションセッション共有を無効にしたアプリケーショングループを構成できます。場合によっては、このオプションが望ましいことがあります。たとえば、ユーザーに非シームレスアプリケーションを別のモニターの全画面表示アプリケーションウィンドウで起動させたい場合があります。

アプリケーショングループ内でアプリケーションセッション共有を無効にすると、そのグループ内の各アプリケーションは新しいアプリケーションセッションで起動します。同じアプリケーションを実行している適切な切断されたセッションが利用可能な場合、そのセッションが再接続されます。たとえば、メモ帳を実行している切断されたセッションがある状態でメモ帳を起動すると、新しいセッションを作成する代わりにそのセッションが再接続されます。複数の適切な切断されたセッションが利用可能な場合、ランダムではあるものの決定論的な方法で、いずれかのセッションが再接続のために選択されます。同じ状況が再発した場合、同じセッションが選択されますが、それ以外の場合にセッションが予測可能であるとは限りません。

PowerShell SDKを使用して、既存のアプリケーショングループ内のすべてのアプリケーションのアプリケーションセッション共有を無効にするか、アプリケーションセッション共有を無効にしたグループを作成します。

PowerShellコマンドレットの例

セッション共有を無効にするには、Broker PowerShellコマンドレット `New-BrokerApplicationGroup` または `Set-BrokerApplicationGroup` を使用し、パラメーター `SessionSharingEnabled` を `False` に、パラメーター `SingleAppPerSession` を `True` に設定します。

- たとえば、グループ内のすべてのアプリケーションでアプリケーションセッション共有を無効にしたアプリケーショングループを作成するには、次のようにします。

  ```
  New-BrokerApplicationGroup AppGr1 -SessionSharingEnabled $False
  -SingleAppPerSession $True
  ```

- たとえば、既存のアプリケーショングループ内のすべてのアプリケーション間でアプリケーションセッション共有を無効にするには、次のようにします。

  ```
  Set-BrokerApplicationGroup AppGR1 -SessionSharingEnabled $False
  -SingleAppPerSession $True
  ```

考慮事項

- `SingleAppPerSession` プロパティを有効にするには、`SessionSharingEnabled` プロパティを False に設定する必要があります。両方のプロパティを同時に有効にすることはできません。`SessionSharingEnabled` パラメーターは、アプリケーショングループ間のセッション共有を指します。
- アプリケーションセッション共有は、アプリケーショングループに関連付けられているがデリバリーグループには関連付けられていないアプリケーションでのみ機能します。デリバリーグループに直接関連付けられているすべてのアプリケーションは、デフォルトでセッションを共有します。
- アプリケーションが複数のアプリケーショングループに割り当てられている場合は、グループの設定が競合しないようにしてください。たとえば、一方のグループのオプションが `True` に設定され、もう一方のグループのオプションが `False` に設定されている場合、予期しない動作が発生します。

アプリケーショングループの名前を変更する

1. 左側のペインで を選択し、 タブを選択します。
2. アプリケーショングループを選択し、アクションバーで を選択します。
3. 新しい一意の名前を指定し、 をクリックします。

アプリケーショングループとのデリバリーグループの関連付けを追加、削除、または優先度を変更する

アプリケーショングループは、アプリケーションを配信できる共有（プライベートではない）マシンを含むデリバリーグループに関連付けることができます。

以下の両方の条件が満たされている場合、デスクトップのみを配信する共有マシンを含むデリバリーグループを選択することもできます。

- デリバリーグループには共有マシンが含まれており、バージョン7.9より前のバージョンで作成されました。
- デリバリーグループの編集権限があること。

ダイアログがコミットされると、デリバリーグループの種類は自動的に「デスクトップとアプリケーション」に変換されます。

1. 左側のペインで を選択し、 タブを選択します。
2. アプリケーショングループを選択し、アクションバーで を選択します。

3. ページを選択します。
4. デリバリーグループを追加するには、 をクリックします。利用可能なデリバリーグループのチェックボックスをオンにします。（互換性のないデリバリーグループは選択できません。）選択が完了したら、 をクリックします。
5. デリバリーグループを削除するには、削除するグループのチェックボックスをオンにして、 をクリックします。確認を求められたら削除を確定します。
6. デリバリーグループの優先度を変更するには、デリバリーグループのチェックボックスをオンにして、 をクリックします。優先度（0 = 最高）を入力し、 をクリックします。
7. 変更を適用してウィンドウを開いたままにするには、**適用**をクリックするか、変更を適用してウィンドウを閉じるには、**保存**をクリックします。

アプリケーショングループのタグ制限を追加、変更、または削除する

タグ制限の追加、変更、削除は、アプリケーション起動の対象となるマシンに予期せぬ影響を与える可能性があります。タグの考慮事項と注意事項を確認してください。

1. 左側のペインで**アプリケーション**を選択し、**アプリケーショングループ**タブを選択します。
2. アプリケーショングループを選択し、アクションバーで**アプリケーショングループの編集**を選択します。
3. **デリバリーグループ**ページを選択します。
4. タグ制限を追加するには、**タグを持つマシンへの起動を制限する**を選択し、ドロップダウンリストからタグを選択します。
5. タグ制限を変更または削除するには、別のタグを選択するか、**このタグを持つマシンへの起動を制限する**のチェックを外してタグ制限を完全に削除します。
6. 変更を適用してウィンドウを開いたままにするには、**適用**をクリックするか、変更を適用してウィンドウを閉じるには、**保存**をクリックします。

アプリケーショングループのユーザーを追加または削除する

ユーザーの詳細については、「アプリケーショングループの作成」を参照してください。

1. 左側のペインで**アプリケーション**を選択し、**アプリケーショングループ**タブを選択します。
2. アプリケーショングループを選択し、アクションバーで**アプリケーショングループの編集**を選択します。
3. **ユーザー**ページを選択します。関連付けられたデリバリーグループのすべてのユーザーにアプリケーショングループ内のアプリケーションの使用を許可するか、特定のユーザーとグループのみに許可するかを指定します。ユーザーを追加するには、**追加**をクリックし、追加するユー

ザーを指定します。ユーザーを削除するには、1人以上のユーザーを選択し、**削除**をクリックします。

4. 変更を適用してウィンドウを開いたままにするには、**適用**をクリックするか、変更を適用してウィンドウを閉じるには、**保存**をクリックします。

アプリケーショングループ内のアプリケーションアイコンを追加、変更、または削除する

アプリケーションアイコンを追加、変更、または削除するには、次の手順を実行します。

1. 左ペインで **Applications** を選択します。
2. **Applications** タブで、アプリケーションを選択し、**Properties** を選択します。

   アプリケーショングループレベルで変更を行うには、**Application Groups** タブに移動し、グループ内のアプリケーションを選択して、**Properties** を選択します。
3. **Delivery** ページを選択し、**Change** を選択します。**Select Icon** ウィンドウが表示されます。
4. **Select Icon** ウィンドウで、次のいずれかを実行します。

   - アイコンを追加するには、**Add** を選択し、アイコンを参照します。
   - アイコンを削除するには、アイコンを選択し、**Remove** を選択します。
   - アイコンを変更するには、アプリケーションのアイコンを選択します。

   > **重要:**
   >
   > - サイズが200 KBを超えるアイコンを追加することはできません。
   > - .iconファイルのみを追加できます。
   > - 組み込みアイコンを削除することはできません。
   > - 使用中のアプリケーションのアイコンを削除することはできません。

5. **Save** を選択して変更を適用し、ウィンドウを閉じます。

アプリケーショングループのスコープを変更する

スコープは、作成した場合にのみ変更できます (すべてのスコープは編集できません)。詳細については、「委任管理」を参照してください。

1. 左側のペインで を選択し、次に タブを選択します。

2. アプリケーショングループを選択し、次にアクションバーで を選択します。
3. ページを選択します。スコープの横にあるチェックボックスをオンまたはオフにします。
4. 加えた変更を適用してウィンドウを開いたままにするには をクリックするか、変更を適用してウィンドウを閉じるには をクリックします。

アプリケーショングループのスコープを変更する

スコープは、作成した場合にのみ変更できます (すべてのスコープは編集できません)。詳細については、「委任管理」を参照してください。

1. 左側のペインで を選択し、次に タブを選択します。
2. アプリケーショングループを選択し、次にアクションバーで を選択します。
3. ページを選択します。変更するスコープの横にあるチェックボックスをオンまたはオフにします。
4. 加えた変更を適用してウィンドウを開いたままにするには を選択するか、変更を適用してウィンドウを閉じるには を選択します。

アプリケーショングループを削除する

アプリケーションは、少なくとも1つのデリバリーグループまたはアプリケーショングループに関連付けられている必要があります。アプリケーショングループを削除した結果、1つ以上のアプリケーションがどのグループにも属さなくなった場合、そのグループを削除するとそれらのアプリケーションも削除されるという警告が表示されます。その後、削除を確定またはキャンセルできます。

アプリケーションを削除しても、元のソースから削除されるわけではありません。ただし、再度利用可能にする場合は、もう一度追加する必要があります。

1. 左ペインで**アプリケーション**を選択し、**アプリケーション グループ**タブを選択します。
2. アプリケーション グループを選択し、アクション バーで**グループの削除**を選択します。
3. プロンプトが表示されたら、削除を確定します。

フォルダーを使用してアプリケーション グループを整理する

フォルダーを作成してアプリケーション グループを整理し、簡単にアクセスできるようにすることができます。

必要な役割

デフォルトでは、次の組み込みロールのいずれかを持っている場合、アプリケーション グループのフォルダーを作成および管理できます。

- クラウド管理者
- フル管理者
- アプリケーション グループ管理者

カスタム ロールを作成することで、管理アクションを他のユーザーに委任できます。次の表に、各アクションに必要な権限を示します。

アクション	必要な権限
アプリケーション グループ フォルダーの作成	アプリケーション グループ フォルダーの作成
アプリケーション グループ フォルダーの削除	アプリケーション グループ フォルダーの削除
アプリケーション グループ フォルダーの移動	アプリケーション グループ フォルダーの移動
アプリケーショングループフォルダーの名前を変更	アプリケーショングループフォルダーの編集
アプリケーショングループをフォルダーに移動	アプリケーショングループフォルダーの編集、アプリケーショングループプロパティの編集

詳しくは、「役割の作成と管理」を参照してください。

フォルダーの作成と管理

アクションバーまたは右クリックメニューを使用して、アプリケーショングループフォルダーを作成および管理できます。さらに、アプリケーショングループまたはフォルダーをフォルダーツリー内の目的の場所にドラッグすることもできます。

知っておくと良いこと:

- フォルダーは最大5レベルまでネストできます（デフォルトのルートフォルダーを除く）。
- フォルダーには、アプリケーショングループとサブフォルダーを含めることができます。フォルダーを削除できるのは、そのフォルダーとサブフォルダーにアプリケーショングループが含まれていない場合のみです。

- Web Studioのすべてのノード（**マシンカタログ**、**デリバリーグループ**、**アプリケーション**、**アプリケーショングループ**など）は、バックエンドで同じフォルダーツリーを共有します。フォルダーの名前変更または移動時に名前の競合を避けるため、異なるノード間で最上位フォルダーに一意の名前を使用してください。

  `New-BrokerAdminFolder` SDKコマンドレットを使用してフォルダーを作成し、それを**アプリケーショングループ**ノードの下に表示させたい場合は、`Set-BrokerAdminFolderMetadata` コマンドレットを使用して `ContainsApplicationGroups` メタデータを追加する必要があります。

  例:

  ```
  Set-BrokerAdminFolderMetadata -AdminFolderId {adminFolderUid} -Name
  ContainsApplicationGroups -Value true
  ```

リモートPCアクセス

注：

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

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

Remote PC Accessは、仮想デスクトップとアプリケーションを提供するのと同じCitrix Virtual Apps and Desktopsコンポーネントを使用します。その結果、Remote PC Accessの展開と構成の要件とプロセスは、仮想リソースを提供するためのCitrix Virtual Apps and Desktopsの展開に必要なものと同じです。この統一性により、一貫した統合された管理エクスペリエンスが提供されま

す。ユーザーは、Citrix HDX™を使用してオフィスPCセッションを配信することで、最高のユーザーエクスペリエンスを得られます。

この機能は、**Remote PC Access**タイプのマシンカタログで構成されており、次の機能を提供します。

- OUを指定してマシンを追加する機能。この機能により、PCの一括追加が容易になります。
- オフィスWindows PCにログオンするユーザーに基づいた自動ユーザー割り当て。シングルユーザーおよび複数ユーザーの割り当てをサポートしています。デフォルトでは、次に割り当てられていないマシンに複数のユーザーを自動的に割り当てます。自動割り当てをシングルユーザーに制限するには、Web Studioにサインインし、**設定**に移動して、**Remote PC Access の複数ユーザーの自動割り当てを有効にする**設定をオフにします。

Citrix Virtual Apps and Desktopsは、他の種類のマシンカタログを使用することで、物理PCのより多くのユースケースに対応できます。これらのユースケースには、次のものが含まれます。

- 物理Linux PC
- プールされた物理PC（つまり、ランダムに割り当てられ、専用ではないもの）

> **注:**
>
> サポートされているOSバージョンの詳細については、シングルセッションOSおよびLinux VDAのVDAのシステム要件を参照してください。

> オンプレミス展開の場合、Remote PC AccessはCitrix Virtual Apps and Desktops AdvancedまたはPremiumライセンスでのみ有効です。セッションは、他のCitrix Virtual Desktops™セッションと同じ方法でライセンスを消費します。Citrix Cloudの場合、Remote PC AccessはCitrix DaaS（旧Citrix Virtual Apps and Desktopsサービス）およびWorkspace Premium Plusで有効です。

考慮事項

Citrix Virtual Apps and Desktops全般に適用されるすべての技術要件と考慮事項はRemote PC Accessにも適用されますが、物理PCの使用事例により関連性が高い、または排他的なものもあります。

> **重要:**

Windows 11物理システム（および一部のWindows 10を実行しているシステム）には、仮想化ベースのセキュリティ機能が含まれており、その結果、VDAソフトウェアがそれらを仮想マシンとして誤って検出します。この問題を軽減するには、以下のオプションがあります。

- VDAコマンドラインインストールの一部として、「/remotepc」オプションとともに「/physicalmachine」オプションを使用する
- 上記のオプションを使用しなかった場合は、VDAのインストール後に以下のレジストリ値を追加します `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`
  - 名前: ForceEnableRemotePC
  - 種類: DWORD
  - データ: 1

展開に関する考慮事項

Remote PC Accessの展開を計画する際には、いくつかの一般的な決定を下します。

- 既存のCitrix Virtual Apps and Desktops展開にRemote PC Accessを追加できます。このオプションを選択する前に、次の点を考慮してください。
  - 現在のDelivery ControllerまたはCloud Connectorは、Remote PC Access VDAに関連する追加の負荷をサポートするために適切にサイジングされていますか？
  - オンプレミスサイトのデータベースおよびデータベースサーバーは、Remote PC Access VDAに関連する追加の負荷をサポートするために適切にサイジングされていますか？
  - 既存のVDAと新しいRemote PC Access VDAは、サイトあたりの最大サポートVDA数を超えますか？
- VDAは自動プロセスを通じてオフィスPCに展開する必要があります。利用可能なオプションは次のとおりです。
  - SCCMなどの電子ソフトウェア配布 (ESD) ツール: SCCMを使用してVDAをインストールする。
  - 展開スクリプト: スクリプトを使用してVDAをインストールする。
- Remote PC Accessのセキュリティに関する考慮事項を確認してください。

注：

> Remote PC Access を設計する際は、リモート PC の GPU に接続され、現在構成/動作している物理モニターの数を考慮する必要があります。モニターが Citrix セッションで使用されていなくても、GPU によって検出された場合、そのモニターの存在は GPU がサポートする最大モニター数にカウントされます。

マシンカタログに関する考慮事項

必要なマシンカタログの種類は、ユースケースによって異なります。

- Remote PC Accessマシンカタログ
  - Windows専用PC
  - Windows専用マルチユーザーPC。このユースケースは、複数のユーザーが異なるシフトでリモートからアクセスできる物理的なオフィスPCに適用されます。
  - プールされたWindows PC。このユースケースは、コンピューターラボのように、複数のランダムなユーザーがアクセスできる物理PCに適用されます。
- シングルセッションOSマシンカタログ
  - 静的 - 専用Linux PC
  - ランダム - プールされたLinux PC

マシンカタログの種類を特定したら、次の点を考慮してください。

- 1台のマシンは、一度に1つのマシンカタログにのみ割り当てることができます。
- 委任された管理を容易にするために、地理的な場所、部門、または各カタログの管理を適切な管理者に委任しやすくするその他のグループに基づいてマシンカタログを作成することを検討してください。
- マシンアカウントが存在するOUを選択する際は、より詳細な粒度を得るために下位レベルのOUを選択します。そのような粒度が必要ない場合は、上位レベルのOUを選択できます。たとえば、Bank/Officers/Tellersの場合、より詳細な粒度を得るには**Tellers**を選択します。それ以外の場合は、要件に基づいて**Officers**または**Bank**を選択できます。
- Remote PC Accessマシンカタログに割り当てられた後にOUを移動または削除すると、VDAの関連付けに影響を与え、今後の割り当てで問題が発生します。したがって、マシンカタログのOU割り当ての更新がActive Directoryの変更計画で考慮されるように、適切に計画してください。
- OU構造のためにマシンカタログにマシンを追加するOUを選択するのが容易でない場合、OUを選択する必要はありません。後でPowerShellを使用してカタログにマシンを追加できます。

デリバリーグループでデスクトップ割り当てが正しく構成されていれば、ユーザーの自動割り当ては引き続き機能します。ユーザー割り当てとともにマシンカタログにマシンを追加するサンプルスクリプトは、GitHubで入手できます。

- 統合されたWake on LANは、**Remote PC Access**タイプのマシンカタログでのみ利用可能です。

Linux VDAに関する考慮事項

以下の考慮事項は、Linux VDAに固有のものです。

- 物理マシンでは、Linux VDAを非3Dモードでのみ使用してください。NVIDIAドライバーの制限により、HDX 3Dモードが有効になっている場合、PCのローカル画面をブラックアウトできず、セッションのアクティビティが表示されます。この画面を表示することはセキュリティリスクです。
- 物理Linuxマシンには、シングルセッションOSタイプのマシンカタログを使用します。
- 自動ユーザー割り当てはLinuxマシンでは利用できません。
- ユーザーがすでにローカルでPCにログオンしている場合、StoreFront™からPCを起動しようとすると失敗します。
- 省電力オプションはLinuxマシンでは利用できません。

技術要件と考慮事項

このセクションでは、物理PCの技術要件と考慮事項について説明します。

- 以下はサポートされていません。
  - KVMスイッチ、またはセッションを切断できるその他のコンポーネント。
  - ハイブリッドPC（オールインワンPC、NVIDIA Optimus搭載ノートPC、PCを含む）。
  - デュアルブートマシン。
- キーボードとマウスはPCに直接接続してください。モニターや、電源を切ったり切断したりできるその他のコンポーネントに接続すると、これらの周辺機器が利用できなくなる可能性があります。入力デバイスをモニターなどのコンポーネントに接続する必要がある場合は、それらのコンポーネントの電源を切らないでください。
- PCはActive Directory Domain Servicesドメインに参加している必要があります。
- セキュアブートはWindows 10およびWindows 11でのみサポートされています。
- PCにはアクティブなネットワーク接続が必要です。信頼性と帯域幅を向上させるには、有線接続が推奨されます。

- Wi-Fiを使用する場合は、次の操作を行います。

  a. 電源設定でワイヤレスアダプターをオンのままにするように設定します。

  b. ユーザーがログオンする前にワイヤレスネットワークに自動的に接続できるように、ワイヤレスアダプターとネットワークプロファイルを構成します。そうしないと、ユーザーがログオンするまでVDAは登録されません。ユーザーがログオンするまで、PCはリモートアクセスに利用できません。

  c. Delivery ControllerまたはCloud ConnectorがWi-Fiネットワークから到達可能であることを確認します。

- ラップトップコンピューターでRemote PC Accessを使用できます。ラップトップがバッテリーで動作するのではなく、電源に接続されていることを確認してください。ラップトップの電源オプションをデスクトップPCのオプションと一致するように構成します。例：

  a. 休止状態機能を無効にします。

  b. スリープ機能を無効にします。

  c. 蓋を閉じたときの動作を**何もしない**に設定します。

  d. 「電源ボタンを押したときの動作」を**シャットダウン**に設定します。

  e. ビデオカードとNICの省電力機能を無効にします。

- Remote PC Accessは、Windows 10を搭載したSurface Proデバイスでサポートされています。前述のラップトップと同じガイドラインに従ってください。
- ドッキングステーションを使用している場合、ラップトップのドッキング解除と再ドッキングが可能です。ラップトップをドッキング解除すると、VDAはWi-Fi経由でDelivery ControllerまたはCloud Connectorに再登録されます。ただし、ラップトップを再ドッキングしても、ワイヤレスアダプターを切断しない限り、VDAは有線接続に切り替わりません。一部のデバイスには、有線接続が確立されたときにワイヤレスアダプターを切断する組み込み機能が提供されています。その他のデバイスでは、ワイヤレスアダプターを切断するためにカスタムソリューションまたはサードパーティ製ユーティリティが必要です。前述のWi-Fiに関する考慮事項を確認してください。

  Remote PC Accessデバイスのドッキングとドッキング解除を有効にするには、次の操作を行います。

  a. **スタート**メニューで、**設定 > システム > 電源とスリープ**を選択し、**スリープ**を**なし**に設定します。

  b. 「**デバイスマネージャー > ネットワークアダプター > イーサネットアダプター**」で「**電源の管理**」に移動し、「**電力節約のために、コンピューターでこのデバイスの電源をオフに**

できるようにする」のチェックを外します。「**このデバイスで、コンピューターのスタンバイ状態を解除できるようにする**」がオンになっていることを確認してください。

- 同じオフィスPCにアクセスする複数のユーザーには、Citrix Workspaceで同じアイコンが表示されます。ユーザーがCitrix Workspaceにログオンすると、そのリソースが他のユーザーによってすでに使用されている場合、利用不可として表示されます。
- オフィスPCにアクセスする各クライアントデバイス（たとえば、自宅のPC）にCitrix Workspaceアプリをインストールします。

構成シーケンス

このセクションでは、**Remote PC Access**タイプのマシンカタログを使用する場合にRemote PC Accessを構成する方法の概要を説明します。その他の種類のマシンカタログの作成方法については、マシンカタログの作成を参照してください。

1. オンプレミスサイトのみ - 統合されたWake on LAN機能を使用するには、Wake on LANに記載されている前提条件を構成してください。
2. Remote PC Access用に新しいCitrix Virtual Apps and Desktopsサイトが作成された場合：

   a. **Remote PC Access**サイトタイプを選択します。

   b. **電源の管理**ページで、デフォルトのRemote PC Accessマシンカタログの電源管理を有効または無効にするかを選択します。この設定は、後でマシンカタログのプロパティを編集して変更できます。Wake on LANの構成の詳細については、Wake on LANを参照してください。

   c. **ユーザー**ページと**マシンアカウント**ページで情報を入力します。

   これらの手順を完了すると、**Remote PC Access Machines**という名前のマシンカタログと、**Remote PC Access Desktops**という名前のデリバリーグループが作成されます。
3. 既存のCitrix Virtual Apps and Desktopsサイトに追加する場合：

   a. **Remote PC Access**タイプのマシンカタログを作成します（ウィザードの「オペレーティングシステム」ページ）。マシンカタログの作成方法の詳細については、マシンカタログの作成を参照してください。ターゲットPCがRemote PC Accessで使用できるよう、適切なOUを割り当ててください。

   b. マシンカタログ内のPCへのユーザーアクセスを提供するために、デリバリーグループを作成します。デリバリーグループの作成方法の詳細については、デリバリーグループの作成を参照してください。デリバリーグループを、PCへのアクセスを必要とするユーザーを含むActive Directoryグループに割り当ててください。

4. オフィスPCにVDAを展開します。

   - シングルセッションOSコアVDAインストーラー（VDAWorkstationCoreSetup.exe）を使用することをお勧めします。
   - シングルセッションフルVDAインストーラー（VDAWorkstationSetup.exe）を`/remotepc/physicalmachine`オプションとともに使用することもできます。これは、コアVDAインストーラーを使用した場合と同じ結果になります。

     > **注：**
     >
     > RemotePCのインストールでは、特定のユーザーシナリオでVDAが期待どおりに動作するように、`/physicalmachine`引数を`/remotepc`とともに使用します。

   - ヘルプデスクチームがCitrix Directorを介してリモートサポートを提供できるように、Windowsリモートアシスタンスを有効にすることを検討してください。これを行うには、`/enable_remote_assistance`オプションを使用します。詳細については、「コマンドラインを使用したインストール」を参照してください。
   - Directorでログオン期間情報を表示するには、シングルセッションのフルVDAインストーラーを使用し、**Citrix User Profile Management WMI Plugin** コンポーネントを含める必要があります。このコンポーネントを含めるには、`/includeadditional`オプションを使用します。詳細については、「コマンドラインを使用したインストール」を参照してください。
   - SCCMを使用してVDAを展開する方法については、「SCCMを使用したVDAのインストール」を参照してください。
   - 展開スクリプトを使用してVDAを展開する方法については、「スクリプトを使用したVDAのインストール」を参照してください。

   手順2～4を正常に完了すると、ユーザーがPCにローカルでログオンしたときに、自分のマシンに自動的に割り当てられます。

5. ユーザーに、オフィスPCにリモートでアクセスするために使用する各クライアントデバイスにCitrix Workspaceアプリをダウンロードしてインストールするよう指示します。Citrix Workspaceアプリは、`https://www.citrix.com/downloads/`またはサポートされているモバイルデバイスのアプリケーションストアから入手できます。

レジストリを介して管理される機能

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

複数ユーザーの自動割り当てを無効にする

各Delivery Controller™で、次のレジストリ設定を追加します。

`HKEY_LOCAL_MACHINE\Software\Citrix\DesktopServer`

- 名前: AllowMultipleRemotePCAssignments
- 種類: DWORD
- データ: 0

スリープモード (最小バージョン 7.16)

Remote PC Accessマシンをスリープ状態にするには、VDAにこのレジストリ設定を追加し、マシンを再起動します。再起動後、オペレーティングシステムの省電力設定が適用されます。事前設定されたアイドルタイマーが経過すると、マシンはスリープモードに入ります。マシンがウェイクアップすると、Delivery Controllerに再登録されます。

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`

- 名前: DisableRemotePCSleepPreventer
- 種類: DWORD
- データ: 1

セッション管理

デフォルトでは、ローカルユーザーがそのマシンでセッションを開始したとき（CTRL+ATL+DELを押すことによって）、リモートユーザーのセッションは自動的に切断されます。この自動的な動作を防ぐには、オフィスPCに以下のレジストリエントリを追加し、その後、マシンを再起動します。

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA\RemotePC`

- 名前: SasNotification

- 種類: DWORD
- データ: 1

デフォルトでは、接続メッセージがタイムアウト期間内に確認されない場合、リモートユーザーがローカルユーザーよりも優先されます。この動作を設定するには、以下の設定を使用します。

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA\RemotePC`

- 名前: RpcaMode
- 種類: DWORD
- データ:
  - 1 - 指定されたタイムアウト期間内にメッセージングUIに応答しない場合、リモートユーザーが常に優先されます。この設定が構成されていない場合、この動作がデフォルトです。
  - 2 - ローカルユーザーが優先されます。

Remote PC Accessモードを適用するためのタイムアウトは、デフォルトで30秒です。このタイムアウトは構成できますが、30秒未満に設定しないでください。タイムアウトを構成するには、このレジストリ設定を使用します。

`HKLM\SOFTWARE\Citrix\PortICA\RemotePC`

- 名前: RpcaTimeout
- 種類: DWORD
- データ: タイムアウトの秒数（10進値）

ユーザーが強制的にコンソールアクセスを取得したい場合: ローカルユーザーは、10秒の間にCtrl+Alt+Delを2回押すことで、リモートセッションのローカル制御を取得し、切断イベントを強制できます。

レジストリ変更とマシンの再起動後、リモートユーザーが使用中にローカルユーザーがCtrl+Alt+Delを押してそのPCにログオンしようとすると、リモートユーザーにプロンプトが表示されます。このプロンプトは、ローカルユーザーの接続を許可するか拒否するかを尋ねます。接続を許可すると、リモートユーザーのセッションは切断されます。

セッション管理のログ記録

Remote PC Accessには、アクティブなICA®セッションを持つPCに誰かがアクセスしようとしたときにログを記録する機能が追加されました。これにより、不要なアクティビティや予期しないア

クティビティがないか環境を監視し、インシデントを調査する必要がある場合にそのようなイベントを監査できます。

イベントはWindowsイベントビューアーを使用してログに記録され、**Applications and Services > Citrix > HostCore > ICA Service > Admin**にあります。

Remote PC Accessを使用すると、3つの異なるイベントがログに記録されます。

Ctrl+Alt+Delイベント

このイベントは、アクティブなリモートセッション中にローカルユーザーがコンソールキーボードでCtrl+Alt+Delを押したときに表示されます。

イベントの詳細

- ログ名: アプリケーションとサービス
- イベントID: 43, 44, 45
- ソース: ICA サービス

イベント ID 43

このイベント ID は、SasNotification レジストリ値が存在しない場合、または SasNotification レジストリ値が 0 の場合に表示されます。

- メッセージ:

```
Ctrl+Alt+Del has been pressed on the endpoint.

The session management behavior is set to automatically disconnect the
remote session.
```

イベント ID 44

このイベント ID は、SasNotification レジストリ値が 1 で、RpcaMode レジストリ値が 1 の場合、または RpcaMode レジストリ値が存在しない場合に表示されます。

- メッセージ:

```
Ctrl+Alt+Del has been pressed on the endpoint.

The session management behavior is set to notify the remote user. The
user preference is set to remote user.
```

イベント ID 45

このイベント ID は、SasNotification レジストリ値が 1 で、RpcaMode レジストリ値が 2 の場合に表示されます。

- メッセージ:

```
Ctrl+Alt+Del has been pressed on the endpoint.

The session management behavior is set to notify the remote user.

The user preference is set to local user.
```

リモートセッション切断イベント

このイベントは、さまざまな理由でリモートセッションが切断された場合に表示されます。

イベントの詳細

- ログ名: アプリケーションとサービス
- イベント ID: 46, 47, 48
- ソース: ICA Service

イベントID 46

このイベントIDは、リモートセッションが切断され、SasNotification レジストリ値が存在しないか、SasNotification レジストリ値が0である場合に表示されます。

- メッセージ:

```
The remote session for &lt;remoteUserName> has been disconnected.
```

イベントID 47

このイベントIDは、リモートユーザーがセッションの切断に同意し、SasNotification レジストリ値が1であり、RpcaMode レジストリ値が1であるか、RpcaMode レジストリ値が2であるか、または RpcaMode レジストリ値が存在しない場合に表示されます。

- メッセージ:

```
The remote session for &lt;remoteUserName> has been disconnected
because the user accepted the request to disconnect the session.
```

イベントID 48

このイベントIDは、リモートユーザーが指定されたタイムアウト期間内に切断要求を拒否せず、SasNotification レジストリ値が1であり、RpcaMode レジストリ値が2である場合に表示されます。

- メッセージ:

```
The remote session for &lt;remoteUserName> has been disconnected
because the user did not decline the disconnection request within the
configured timeout period (&lt;timeout period>).
```

Ctrl+Alt+Del 2回押しイベント

このイベントは、10秒以内にCtrl+Alt+Delが2回押された場合に表示されます。

イベントの詳細

- ログ名: アプリケーションとサービス
- イベントID: 49
- ソース: ICA Service

イベントID 49

このイベントIDは、Ctrl+Alt+Delが10秒以内に2回押されたときに表示されます。

- メッセージ:

```
The remote session for &lt;remoteUserName> has been forcibly
disconnected.
```

Wake on LAN (ウェイク・オン・ラン)

Remote PC AccessはWake on LANをサポートしており、ユーザーは物理PCをリモートで起動できます。この機能により、ユーザーは使用していないときにオフィスPCの電源を切ったままにして、エネルギーコストを節約できます。また、誤ってマシンの電源が切れてしまった場合でも、リモートアクセスを可能にします。

Wake on LAN機能を使用すると、デリバリーコントローラーからの指示があった場合、PC上で実行されているVDAから、そのPCが存在するサブネットにマジックパケットが直接送信されます。これにより、追加のインフラストラクチャコンポーネントやマジックパケット配信のためのサードパーティソリューションに依存することなく、この機能が動作します。

Wake on LAN機能は、レガシーなSCCMベースのWake on LAN機能とは異なります。SCCMベースのWake on LANの詳細については、「Wake on LAN – SCCM統合」を参照してください。

制限事項

Wake on LAN機能を使用するRemote PC Accessは、ピーク時の自動電源オンをサポートしていません。

システム要件

Wake on LAN機能を使用するためのシステム要件は次のとおりです。

- コントロールプレーン:
  - シトリックス DaaS™
  - シトリックス バーチャルアプリおよびデスクトップ 2009以降
- 物理PC:
  - VDAバージョン2009以降
  - Windows 10またはWindows 11。サポートの詳細については、VDAシステム要件を参照してください。
  - BIOS/UEFIでWake on LANが有効になっていること
  - Windows構成内のネットワークアダプターのプロパティでWake on LANが有効になっていること

Wake on LANの構成

オンプレミスのCitrix Virtual Apps and Desktopsを使用している場合、統合Wake on LANの構成はPowerShellを使用してのみサポートされます。

Wake on LANを構成するには:

1. まだ Remote PC Access マシンカタログがない場合は、作成します。
2. まだ Wake on LAN ホスト接続がない場合は、作成します。

> **注：**
>
> Wake on LAN機能を使用するには、「Microsoft Configuration Manager Wake on LAN」タイプのホスト接続がある場合、新しいホスト接続を作成します。

3. Wake on LAN ホスト接続の一意の識別子を取得します。
4. Wake on LAN ホスト接続をマシンカタログに関連付けます。

Wake on LAN ホスト接続を作成するには：

```
# Load Citrix SnapIns

Add-PSSnapIn -Name "*citrix*"



# Provide the name of the Wake on LAN host connection

[string]$connectionName = "Remote PC Access Wake on LAN"



# Create the hypervisor connection

$hypHc = New-Item -Path xdhyp:\Connections `

                -Name $connectionName `

                -HypervisorAddress "N/A" `

                -UserName "woluser" `

                -Password "wolpwd" `

                -ConnectionType Custom `

                -PluginId VdaWOLMachineManagerFactory `

                -CustomProperties "<CustomProperties></CustomProperties>"
`

                -Persist



$bhc = New-BrokerHypervisorConnection -HypHypervisorConnectionUid
$hypHc.HypervisorConnectionUid
```

```
# Wait for the connection to be ready before trying to use it

while (-not $bhc.IsReady)

{

    Start-Sleep -s 5

    $bhc = Get-BrokerHypervisorConnection -HypHypervisorConnectionUid
$hypHc.HypervisorConnectionUid

}
```

ホスト接続の準備ができたら、次のコマンドを実行してホスト接続の一意の識別子を取得します。

```
$bhc = Get-BrokerHypervisorConnection -Name "<WoL Connection Name>"

$hypUid = $bhc.Uid
```

接続の一意の識別子を取得したら、次のコマンドを実行して、その接続を Remote PC Access マシンカタログに関連付けます。

```
Get-BrokerCatalog -Name "<Catalog Name>" | Set-BrokerCatalog
-RemotePCHypervisorConnectionUid $hypUid
```

設計上の考慮事項

Remote PC Access で Wake on LAN を使用する予定がある場合は、次の点を考慮してください。

- 複数のマシンカタログで同じ Wake on LAN ホスト接続を使用できます。
- ある PC が別の PC を起動するには、両方の PC が同じサブネット内にあり、同じ Wake on LAN ホスト接続を使用している必要があります。PC が同じマシンカタログ内にあるか、異なるマシンカタログ内にあるかは関係ありません。
- ホスト接続は特定のゾーンに割り当てられます。展開に複数のゾーンが含まれている場合は、各ゾーンに Wake on LAN ホスト接続が必要です。これはマシンカタログにも当てはまります。

- マジックパケットはグローバルブロードキャストアドレス255.255.255.255を使用してブロードキャストされます。このアドレスがブロックされていないことを確認してください。
- そのサブネット内のマシンを起動できるようにするには、Wake on LAN接続ごとに、サブネット内に少なくとも1台のPCが電源オンになっている必要があります。

運用上の考慮事項

Wake on LAN機能を使用する際の考慮事項は次のとおりです。

- 統合されたWake on LAN機能を使用してPCを起動できるようにするには、VDAが少なくとも1回登録されている必要があります。
- Wake on LANはPCを起動するためにのみ使用できます。再起動やシャットダウンなどの他の電源操作はサポートしていません。
- Wake on LAN接続が作成されると、Web Studioに表示されます。ただし、オンプレミスのCitrix Virtual Apps and Desktopsを使用している場合、Web Studio内でのそのプロパティの編集はサポートされていません。
- マジックパケットは次の2つの方法のいずれかで送信されます。

  a. ユーザーが自分のPCへのセッションを起動しようとし、VDAが未登録の場合

  b. 管理者がWeb StudioまたはPowerShellから手動で電源オンコマンドを送信した場合

- デリバリーコントローラーはPCの電源状態を認識していないため、Web Studioでは電源状態の下に**サポートされていません**と表示されます。デリバリーコントローラーは、VDA登録状態を使用してPCがオンかオフかを判断します。

Wake on LAN – SCCM統合

SCCM統合Wake on LANは、Remote PC Accessの代替Wake on LANオプションであり、オンプレミスのCitrix Virtual Apps and Desktopsでのみ利用可能です。

システム要件

SCCM統合Wake on LAN機能を使用するためのシステム要件は次のとおりです。

- シトリックス バーチャル アプリケーションズ アンド デスクトップ 1912 以降
- 物理PC:
  - VDA バージョン 1912 以降
  - Windows 10。サポートの詳細については、VDA システム要件を参照してください。
  - BIOS/UEFIでWake on LANが有効になっていること

  - Windows構成内のネットワークアダプターのプロパティでWake on LANが有効になっていること

- システムセンターコンフィギュレーションマネージャー (SCCM) 2012 R2 以降

SCCM 統合型 Wake on LAN の構成

以下の前提条件を完了してください。

1. 組織内で SCCM 2012 R2、2016、または 2019 を構成します。次に、すべての Remote PC Access マシンに SCCM クライアントを展開し、スケジュールされた SCCM インベントリサイクルが実行されるのを待つか、必要に応じて手動で強制実行します。
2. Wake Proxy のサポートについては、SCCM でオプションを有効にします。Remote PC Access Wake on LAN 機能を使用する PC を含む組織内の各サブネットについて、3 台以上のマシンがセンチネルマシンとして機能できることを確認してください。
3. マジックパケットのサポートについては、サブネット指向ブロードキャストまたはユニキャストのいずれかを使用してマジックパケットを送信できるように、ネットワークルーターとファイアウォールを構成します。
4. 各PCのBIOS/UEFI設定でWake on LANを構成します。
5. まだVDAを展開していない場合は、物理PCにVDAを展開します。

前提条件に対処した後、Delivery Controller が SCCM と通信できるように、次の手順を完了します。

1. SCCM のホスト接続を作成します。詳細については、接続とリソースを参照してください。
   - 接続の種類として **Microsoft Configuration Manager Wake on LAN** を選択します。
   - 入力された資格情報には、スコープ内のコレクションへのアクセス権があり、**Remote Tools Operator** ロールが必要です。
2. Web Studioで接続を選択し、**接続の編集**を選択して、**詳細**をクリックします。
3. Wake on LANの処理に適したオプションを選択します。
   - Wake-upプロキシを使用している場合は、最初のオプションである**Microsoft System Center Configuration Manager Wake-upプロキシ**を選択します。
   - マジックパケットを使用している場合は、2番目のオプションである**Delivery Controllerによって送信されるWake on LANパケット**を選択します。
     - 適切な送信方法（**サブネット指向ブロードキャスト**または**ユニキャスト**）を選択します。

ホスト接続を作成したら、その接続をRemote PC Accessカタログに関連付けます。

- 新しいRemote PC Accessカタログを作成する場合は、カタログ作成ウィザードの**オペレーティングシステム**ページで、カタログの種類として**Remote PC Access**を選択し、ドロップダウンリストから適切な接続を選択します。
- 既存のRemote PC AccessカタログにWake on LANを追加するには：

  a. Web Studioの**マシンカタログ**ノードに移動し、マシンカタログを選択して、**マシンカタログの編集**を選択します。

  b. **電源管理**タブを選択し、マシンカタログの電源管理を有効にするには**はい**を選択します。

  c. ドロップダウンリストから適切な接続を選択し、**OK**をクリックします。

トラブルシューティング

モニターのブランキングが機能しない

アクティブなHDXセッション中にWindows PCのローカルモニターが空白にならない場合（ローカルモニターにセッションで発生していることが表示される場合）、それはGPUベンダーのドライバーの問題である可能性があります。この問題を解決するには、次のレジストリ値を設定して、Citrix Indirect Display driver (IDD) にグラフィックカードのベンダードライバーよりも高い優先順位を与えます。

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics\AdapterMerits`

- 名前: CitrixIDD
- 種類: DWORD
- データ: 3

ディスプレイアダプターの優先順位とモニターの作成の詳細については、Knowledge Centerの記事CTX237608を参照してください。

セッション管理通知が有効になっているマシンでCtrl+Alt+Delを選択すると、セッションが切断されます

SasNotificationレジストリ値によって制御されるセッション管理通知は、VDAでRemote PC Accessモードが有効になっている場合にのみ機能します。物理PCでHyper-Vの役割または仮想化ベースのセキュリティ機能が有効になっている場合、そのPCは仮想マシンとして報告されます。VDAが仮想マシン上で実行されていることを検出すると、Remote PC Accessモードを自動的に無効にします。Remote PC Accessモードを有効にするには、次のレジストリ値を追加します。

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`

- 名前: ForceEnableRemotePC
- 種類: DWORD
- データ: 1

設定を有効にするには、PCを再起動します。

診断情報

Remote PC Accessに関する診断情報は、Windowsアプリケーションイベントログに書き込まれます。情報メッセージはスロットリングされません。エラーメッセージは、重複するメッセージを破棄することでスロットリングされます。

- 3300（情報）: マシンがカタログに追加されました
- 3301（情報）: マシンがデリバリーグループに追加されました
- 3302（情報）: マシンがユーザーに割り当てられました
- 3303 (エラー): 例外

電源管理

Remote PC Accessの電源管理が有効になっている場合、サブネット指向ブロードキャストでは、Controllerとは異なるサブネットにあるマシンを起動できないことがあります。サブネット指向ブロードキャストを使用してサブネット間で電源管理が必要で、AMTサポートが利用できない場合は、Wake-upプロキシまたはユニキャスト方式を試してください。これらの設定が電源管理接続の詳細プロパティで有効になっていることを確認してください。

アクティブなリモートセッションはローカルのタッチスクリーン入力を記録します

VDA が Remote PC Access モードを有効にすると、マシンはアクティブなセッション中にローカルのタッチスクリーン入力を無視します。物理 PC で Hyper-V ロールまたは仮想化ベースのセキュリティ機能が有効になっている場合、その PC は仮想マシンとして報告されます。VDA が仮想マシン上で実行されていることを検出すると、Remote PC Access モードを自動的に無効にします。Remote PC Access モードを有効にするには、次のレジストリ設定を追加します。

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`

- 名前: ForceEnableRemotePC
- 種類: DWORD
- データ: 1

設定を有効にするには、PC を再起動してください。

その他のリソース

以下は Remote PC Access に関するその他のリソースです。

- ソリューション設計ガイダンス: Remote PC Access Design Decisions。
- Remote PC Access アーキテクチャの例: Citrix Remote PC Access ソリューションのリファレンスアーキテクチャ。

コンテンツの公開

> **注：**

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

> Microsoft WordドキュメントやWebリンクなど、リソースへのURLまたはUNCパスであるアプリケーションを公開できます。この機能は「公開コンテンツ」として知られています。コンテンツを公開する機能により、ユーザーへのコンテンツ配信方法に柔軟性が加わります。既存のアクセス制御とアプリケーション管理の恩恵を受けることができます。また、コンテンツを開くためにローカルアプリケーションを使用するか、公開アプリケーションを使用するかを指定することもできます。

公開されたコンテンツは、StoreFront™およびCitrix Workspace™アプリの他のアプリケーションと同様に表示されます。ユーザーはアプリケーションにアクセスするのと同じ方法でアクセスします。クライアントでは、リソースは通常どおり開きます。

- ローカルにインストールされたアプリケーションが適切な場合、そのアプリケーションが起動されてリソースが開かれます。
- ファイルの種類に関連付けが定義されている場合、公開されたアプリケーションが起動されてリソースが開かれます。

コンテンツはPowerShell SDKを使用して公開します。Web Studioを使用してコンテンツを公開することはできません。ただし、公開後にWeb Studioを使用してアプリケーションのプロパティを編集することはできます。

構成の概要と準備

コンテンツの公開には、次の主要なプロパティを持つ `New-BrokerApplication` コマンドレットを使用します。（すべてのコマンドレットプロパティの説明については、コマンドレットのヘルプを参照してください。）

```
New-BrokerApplication –ApplicationType PublishedContent
-CommandLineExecutable location -Name app-name -DesktopGroup delivery-
group-name
```

`ApplicationType` プロパティは `PublishedContent` である必要があります。

`CommandLineExecutable` プロパティは、公開コンテンツの場所を指定します。以下の形式がサポートされており、255文字の制限があります。

- HTMLウェブサイトアドレス（例: `<http://www.citrix.com>`）
- ウェブサーバー上のドキュメントファイル（例: `https://www.citrix.com/press/pressrelease.doc`）
- FTPサーバー上のディレクトリ（例: `ftp://ftp.citrix.com/code`）
- FTPサーバー上のドキュメントファイル（例: `ftp://ftp.citrix.com/code/Readme.txt` >）
- UNC ディレクトリパス (例: `file://myServer/myShare or \\\\myServer\\myShare`)
- UNC ファイルパス (例: `file://myServer/myShare/myFile.asf` または `\\myServer\myShare\myFile.asf`)

正しいSDKがあることを確認してください。

- Citrix DaaS (旧Citrix Virtual Apps and Desktopsサービス) の展開の場合、ダウンロード して、Citrix Virtual Apps and Desktops Remote PowerShell SDKをインストールします。
- オンプレミスのCitrix Virtual Apps and Desktops展開の場合、Delivery Controllerとともにインストールされているの PowerShell SDKを使用します。公開コンテンツアプリケーションを追加するには、最低バージョン7.11のDelivery Controllerが必要です。

以下の手順では例を使用します。例では、次のようになります:

- マシンカタログが作成されています。
- `PublishedContentApps` という名前のデリバリーグループが作成されています。このグループは、カタログからマルチセッションOSマシンを使用します。WordPadアプリケーションがグループに追加されています。

- デリバリーグループ名、`CommandLineExecutable` の場所、およびアプリケーション名が割り当てられます。

はじめに

PowerShell SDKを含むマシンで、PowerShellを開きます。

次のコマンドレットは、適切なPowerShell SDKスナップインを追加し、返されたデリバリーグループレコードを割り当てます。

`Add-PsSnapin Citrix* $dg = Get-BrokerDesktopGroup –Name PublishedContentApps`

Citrix DaaSを使用している場合は、Citrix Cloud™の資格情報を入力して認証します。複数の顧客がいる場合は、1つを選択します。

URLを公開する

場所とアプリケーション名を割り当てた後、次のコマンドレットは、Citrixのホームページをアプリケーションとして公開します。

```
$citrixUrl = "https://www.citrix.com/"

$appName = "Citrix Home Page"



New-BrokerApplication –ApplicationType PublishedContent –
CommandLineExecutable $citrixURL –Name $appName –DesktopGroup $dg.Uid
```

成功を確認します:

- StoreFrontを開き、PublishedContentAppsデリバリーグループ内のアプリケーションにアクセスできるユーザーとしてログオンします。デフォルトのアイコンを持つ新しく作成されたアプリケーションが表示されます。アイコンのカスタマイズについては、`<https://www.citrix.com/blogs/2013/08/21/xd-tipster-changing-delivery-group-icons-revisited-xd7/>` を参照してください。
- **Citrix Home Page**アプリケーションをクリックします。URLは、ローカルで実行されているデフォルトブラウザの新しいタブで起動します。

UNCパスにあるリソースを公開する

この例では、管理者は`PublishedResources`という名前の共有をすでに作成しています。場所とアプリケーション名を割り当てた後、以下のコマンドレットはその共有内のRTFファイルとDOCXファイルをリソースとして公開します。

```
$rtfUNC = "\\GMSXJ-EDGE0.xd.local\\PublishedResources\\PublishedRTF.rtf"

$rtfAppName = "PublishedRTF"



New-BrokerApplication –ApplicationType PublishedContent

–CommandLineExecutable $rtfUNC -Name $rtfAppName

-DesktopGroup $dg.Uid



$docxUNC = "\\GMSXJ-EDGE0.xd.local\PublishedResources\PublishedDOCX.docx"

$docxAppName = "PublishedDOCX"



New-BrokerApplication –ApplicationType PublishedContent

–CommandLineExecutable $docxUNC -Name $docxAppName

-DesktopGroup $dg.Uid
```

成功を確認する:

- StoreFrontウィンドウを更新して、新しく公開されたドキュメントを表示します。
- **PublishedRTF**および**PublishedDOCX**アプリケーションをクリックします。各ドキュメントは、ローカルで実行されているWordPadで開きます。

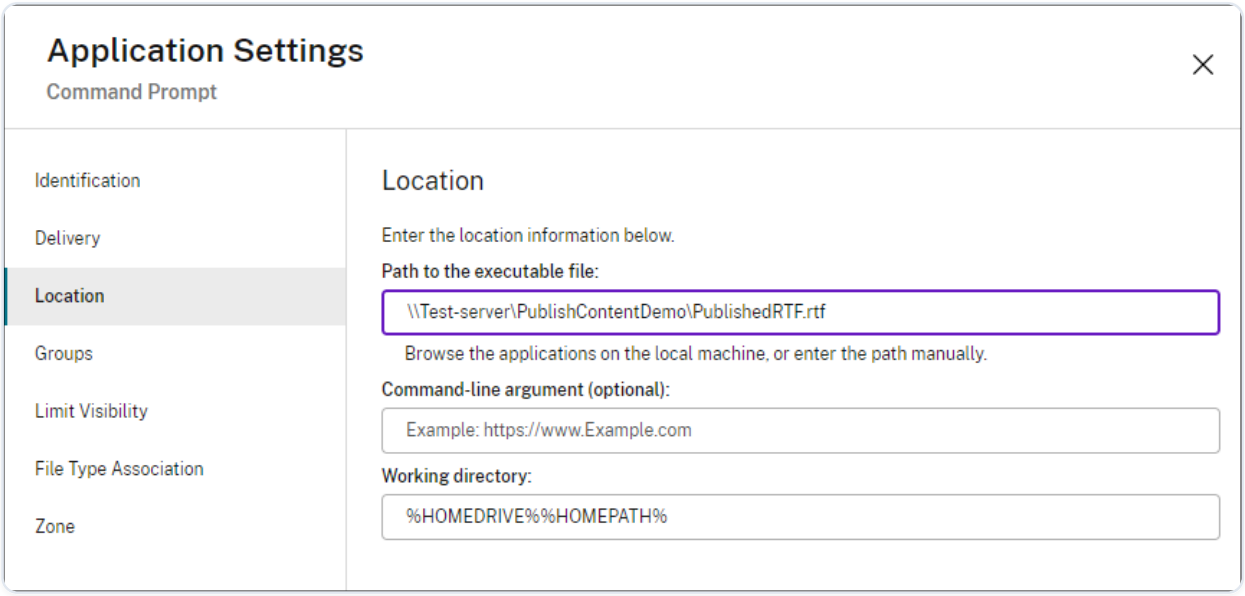
PublishedContentアプリケーションの表示と編集

公開されたコンテンツは、他のアプリケーションタイプに使用するのと同じ方法で管理します。

`PublishedContent`アプリケーションを表示および編集するには、次の手順に従います。

1. Web Studioにサインインし、左ペインで**アプリケーション**を選択します。
2. **アプリケーション**タブで、PublishedContentアプリケーションを選択し、**プロパティ**を選択します。

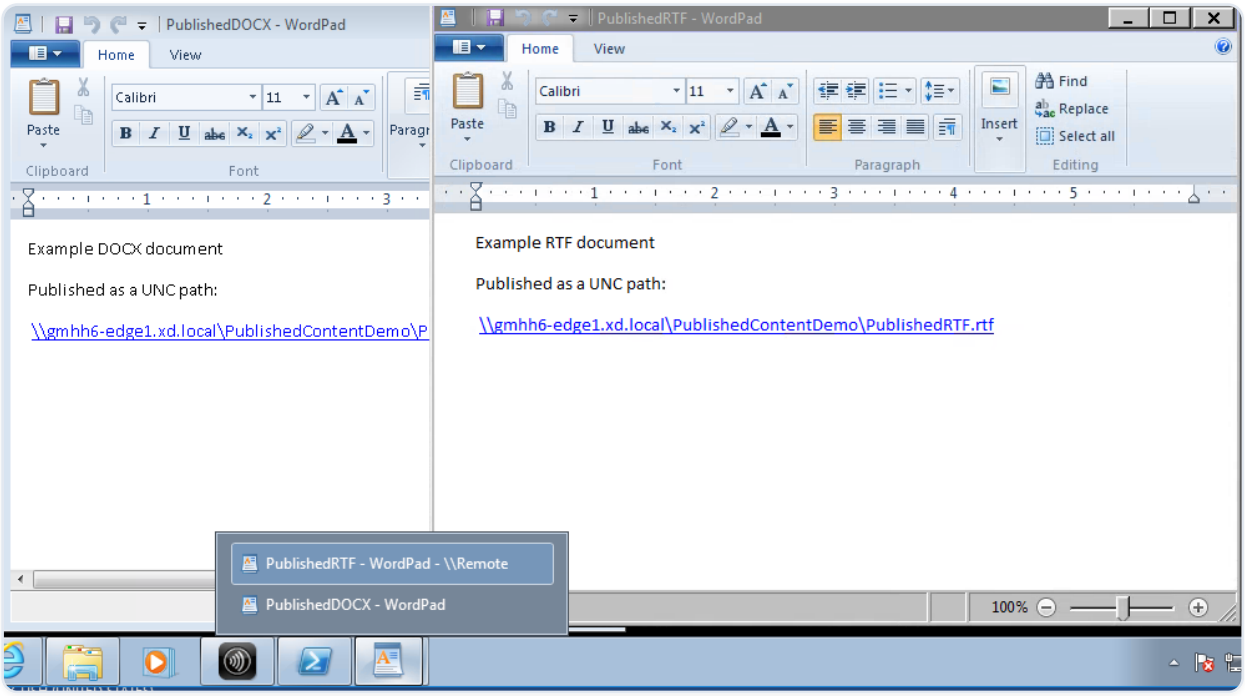
   アプリケーションのプロパティ（ユーザーの可視性、グループの関連付け、ショートカットなど）は、公開されたコンテンツに適用されます。ただし、**場所**ページでは、コマンドライン引数または作業ディレクトリのプロパティを変更することはできません。
3. リソースを変更するには、そのページの**実行可能ファイルへのパス**フィールドを変更します。



4. 公開アプリケーションを使用して`PublishedContent`アプリケーション（ローカルアプリケーションではなく）を開くには、次の手順に従います。

   この例では、公開されたWordPadアプリケーションが編集され、.rtfファイル用のファイルタイプ関連付けが作成されます。

   a. デリバリーグループのメンテナンスモードをオンにします。
   b. **ファイルタイプ関連付け**プロパティを編集します。
   c. 完了したら、メンテナンスモードをオフにします。
   d. StoreFrontを更新してファイルタイプ関連付けの変更を読み込み、**PublishedRTF**および**PublishedDOCX**アプリケーションをクリックします。違いに注目してください。**PublishedDOCX**は引き続きローカルのWordPadで開きます。しかし、**PublishedRTF**はファイルタイプ関連付けにより、公開されたWordPadで開くようになりました。



詳細情報

- マシンカタログの作成
- デリバリーグループの作成
- アプリケーションプロパティの変更

サーバー VDI

Server VDI (Virtual Desktop Infrastructure) 機能を使用して、単一ユーザー向けにサーバーオペレーティングシステムからデスクトップを配信します。

- エンタープライズ管理者は、サーバーオペレーティングシステムをVDIデスクトップとして配信できます。これは、エンジニアやデザイナーなどのユーザーにとって価値があります。
- サービスプロバイダーは、クラウドからデスクトップを提供できます。これらのデスクトップは、Microsoft Services Provider License Agreement (SPLA) に準拠しています。

サポート:

- Citrix Virtual Apps and Desktops™ および Citrix DaaS (旧称 Citrix Virtual Apps and Desktops service) の展開では、Server VDI は Windows Server 2022、Windows Server 2019、および Windows Server 2016 でサポートされています。
- すべてのServer VDI展開は、ユーザーパーソナライゼーションレイヤーテクノロジーをサポートしています。

- Server VDIがスキャナーなどのTWAINデバイスで動作するには、Windows Serverのデスクトップエクスペリエンス機能がインストールされている必要があります。
- 以下の機能はServer VDIでは使用できません:
  - ホスト型アプリケーション
  - ローカルアプリアクセス
  - 直接（ブローカーなし）デスクトップ接続
  - リモートPCアクセス

Server VDIのインストールと構成

1. Windowsサーバーをインストール用に準備します。
   - Windows Server Managerを使用して、リモートデスクトップサービスロールサービスがインストールされていないことを確認します。以前にインストールされていた場合は、削除してください。これらのロールサービスがインストールされていると、VDAのインストールは失敗します。
   - 「**各ユーザーを単一セッションに制限する**」プロパティが有効になっていることを確認します。Windowsサーバーで、ターミナルサーバー設定のレジストリを編集します。

     `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server`

     `DWORD fSingleSessionPerUser = 1`
2. Citrix Virtual Apps and Desktopsインストーラーのコマンドラインインターフェイスを使用して、サポートされているサーバーまたはサーバーマスターイメージにVDAをインストールし、`/servervdi`オプションを指定します。(デフォルトでは、インストーラーのグラフィカルインターフェイスは、サーバーオペレーティングシステム上のWindowsシングルセッションOS VDAをブロックします。コマンドラインを使用すると、この動作が上書きされます。)次のいずれかのコマンドを使用します。
   - Citrix Virtual Apps and Desktops展開の場合:
     - `XenDesktopVdaSetup.exe /servervdi`
     - `VDAWorkstationSetup.exe /servervdi`
   - Citrix DaaS™展開の場合:
     - `VDAWorkstationSetup.exe /servervdi`

   その他のオプション:

- Delivery ControllerまたはCloud Connectorを指定するには、`/controllers`を使用します。
- ファイアウォールを手動で構成する場合を除き、ファイアウォールでポートを開くには、`/enable_hdx_ports`を使用します。
- イメージにVDAをインストールし、そのイメージからMCSを使用してサーバーVMを作成する場合は、`/mastermcsimage`（または`/masterimage`）を使用します。
- すべてのオプションの詳細については、「コマンドラインを使用したインストール」を参照してください。

3. Server VDI用のマシンカタログを作成します。カタログ作成ウィザードで:
   - **オペレーティングシステム**ページで、**シングルセッションOS**を選択します。
   - **概要**ページで、Server VDIであることを明確に識別できるマシンカタログ名と管理者向けの記述を指定します。これは、カタログがServer VDIをサポートしていることをStudioで示す唯一のインジケーターです。

   Studioで検索を使用すると、VDAがマルチセッションマシンにインストールされている場合でも、Server VDIカタログは**シングルセッションOSマシン**タブに表示されます。
4. デリバリーグループを作成し、作成したServer VDIカタログを選択します。

VDAのインストール中にDelivery ControllerまたはCloud Connectorを指定しなかった場合は、後で指定することを忘れないでください。詳細については、「VDA登録」を参照してください。

ユーザーパーソナライゼーションレイヤー

> **注：**

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

> Citrix Virtual Apps and Desktopsのユーザーパーソナライゼーションレイヤー機能は、非永続マシンカタログの機能を拡張し、ユーザーのデータとローカルにインストールされたアプリケーションをセッション間で保持します。基盤となるCitrix App Layeringテクノロジーを搭載

したユーザーパーソナライゼーションレイヤー機能は、非永続マシンカタログでCitrix ProvisioningおよびMachine Creation Services™ (MCS) をサポートします。

マスターイメージ内のVirtual Delivery Agentとともに、ユーザーパーソナライゼーションレイヤーコンポーネントをインストールします。VHDファイルには、ユーザーがローカルにインストールしたアプリケーションが保存されます。イメージにマウントされたVHDは、ユーザー自身の仮想ハードドライブとして機能します。

重要:

Citrix Virtual Apps and Desktopsでユーザーパーソナライゼーションレイヤーを展開するか、イメージテンプレートで有効になっているApp Layeringユーザーレイヤーを展開できますが、両方を展開することはできません。App Layering内のレイヤーにユーザーパーソナライゼーションレイヤー機能をインストールしないでください。

この機能はPersonal vDisk (PvD) に代わるものであり、非永続（プールされた）デスクトップ環境のユーザーに永続的なワークスペースエクスペリエンスも提供します。

ユーザーパーソナライゼーションレイヤー機能を展開するには、記事に詳述されている手順を使用してインストールおよび構成します。

アプリケーションのサポート

以下の例外を除き、ユーザーがデスクトップにローカルでインストールするすべてのアプリケーションは、ユーザーパーソナライゼーションレイヤーでサポートされます。

例外

以下のアプリケーションは例外であり、ユーザーパーソナライゼーションレイヤーではサポートされません。

- MS OfficeやVisual Studioなどのエンタープライズアプリケーション。
- ネットワークスタックまたはハードウェアを変更するアプリケーション。例：VPNクライアント。
- ブートレベルドライバーを持つアプリケーション。例：ウイルススキャナー。
- ドライバーストアを使用するドライバーを持つアプリケーション。例：プリンタードライバー。

> **注：**
>
> Windowsグループポリシーオブジェクト (GPO) を使用してプリンターを利用可能にできます。

サポートされていないアプリケーションをローカルにインストールすることをユーザーに許可しないでください。代わりに、これらのアプリケーションはマスターイメージに直接インストールしてください。

ローカルユーザーまたは管理者アカウントを必要とするアプリケーション

ユーザーがアプリケーションをローカルにインストールすると、そのアプリはユーザーレイヤーに格納されます。その後、ユーザーがローカルユーザーまたはグループを追加または編集しても、その変更はセッションを超えて保持されません。

> **重要:**
>
> 必要なローカルユーザーまたはグループは、マスターイメージに追加してください。

要件

ユーザーパーソナライゼーションレイヤー機能には、以下のコンポーネントが必要です。

- シトリックス バーチャル アプリケーションズ アンド デスクトップ 7 1909 以降
- Virtual Delivery Agent (VDA)、バージョン1912以降
- Citrix Provisioning™、バージョン1909以降
- Windowsファイル共有 (SMB)、またはオンプレミスAD認証が有効なAzure Files

ユーザーパーソナライゼーションレイヤー機能は、OSがシングルセッションとして展開されている場合、以下のWindowsバージョンで展開できます。サポートは、シングルセッション上の単一ユーザーに限定されます。

- ウィンドウズ 11 エンタープライズ x64
- Windows 10 Enterprise x64、バージョン1607以降
- Windows Server 2016 (Azure Files がサポートされています)
- Windows Server 2019 (Azure Files がサポートされています)
- Windows Server 2022 (Azure Files がサポートされています)

Citrix Virtual Apps and Desktops 7 では、ユーザーパーソナライゼーションレイヤーでの Azure Files の使用は、Windows Server 2022、Windows Server 2019、Windows Server 2016、および Windows 10 クライアントでサポートされています。

> **注：**

> サーバーOSを使用している場合、Server VDIのみがサポートされます。展開の詳細については、Server VDIの記事を参照してください。

> ユーザーパーソナライゼーションレイヤーは、マシンごとに一度に1人のユーザーのみをサポートし、その後、ディスクをリセットするためにマシンを再起動する必要があります。ユーザーパーソナライゼーションレイヤーは、マルチセッションサーバーオペレーティングシステムでは使用できず、シングルセッションサーバーシステムでのみ使用できます。ユーザーパーソナライゼーションレイヤーは、非永続デスクトップでのみサポートされます。

> ユーザーパーソナライゼーションレイヤー機能がインストールされている場合は、アンインストールします。最新リリースをインストールする前に、マスターイメージを再起動します。

ファイル共有を設定する

ユーザーパーソナライゼーションレイヤー機能には、Windows Server Message Block (SMB) ストレージが必要です。Windowsファイル共有を作成するには、使用しているWindowsオペレーティングシステムの通常の手順に従ってください。

Azureベースのカタログでは Azure Files を使用する方法の詳細については、「ユーザーパーソナライゼーションレイヤー用のAzure Filesストレージを設定する」を参照してください。

推奨事項

ユーザーパーソナライゼーションレイヤーの展開を成功させるには、このセクションの推奨事項に従ってください。

マイクロソフト システムセンター コンフィグレーションマネージャー (SCCM)

ユーザーパーソナライゼーションレイヤー機能でSCCMを使用している場合は、VDI環境でイメージを準備するためのMicrosoftのガイドラインに従ってください。詳細については、このMicrosoft TechNet記事を参照してください。

ユーザーレイヤーのサイズ

ユーザーレイヤーは、ディスク上のスペースが使用されるにつれて拡張するシンプロビジョニングディスクです。ユーザーレイヤーに許可されるデフォルトサイズは10 GBで、これは推奨される最小値です。

> **注：**
>
> インストール中に値がゼロ (0) に設定されている場合、デフォルトのユーザーレイヤーサイズは10 GBに設定されます。

> ユーザーレイヤーのサイズを変更したい場合は、**User Layer Size** ポリシーに別の値を入力できます。「**オプション: User Layer Size in GBの横にあるをクリックします。**」の下にある「**ステップ5: デリバリーグループのカスタムポリシーを作成する**」を参照してください。

ユーザーレイヤーのサイズを上書きするためのツール (オプション)

Windowsツールを使用してユーザーレイヤーファイル共有にクォータを定義することで、ユーザーレイヤーのサイズを上書きできます。

以下のMicrosoftクォータツールのいずれかを使用して、**Users**という名前のユーザーレイヤーディレクトリにハードクォータを設定します。

- ファイルサーバーリソースマネージャー (FSRM)
- クォータマネージャー

> **注：**
>
> クォータを増やすと、新しいユーザーレイヤーに影響し、既存のユーザーレイヤーが拡張されます。クォータを減らすと、新しいユーザーレイヤーのみに影響します。既存のユーザーレイヤーのサイズが小さくなることはありません。

ユーザーパーソナライゼーションレイヤーを展開する

ユーザーパーソナライゼーション機能を展開する際は、Web Studio内でポリシーを定義します。その後、その機能が展開されるマシンカタログにバインドされているデリバリーグループにポリシーを割り当てます。

マスターイメージにユーザーパーソナライゼーションレイヤーの設定がない場合、サービスはアイドル状態のままであり、オーサリングアクティビティを妨げません。

マスターイメージでポリシーを設定すると、サービスはマスターイメージ内でユーザーレイヤーを実行およびマウントしようとします。マスターイメージは予期しない動作や不安定性を示します。

ユーザーパーソナライゼーションレイヤー機能を展開するには、以下の手順をこの順序で完了します。

- ステップ1：Citrix Virtual Apps and Desktops環境の可用性を確認します。
- ステップ2：マスターイメージを準備します。
- ステップ3：マシンカタログを作成します。
- ステップ4：デリバリーグループを作成します。
- ステップ5：デリバリーグループのカスタムポリシーを作成します。

> **注：**
>
> イメージ上のWindows 10をアップグレードした後、初めてログインするのに通常よりも時間がかかります。ユーザーレイヤーは新しいバージョンのWindows 10用に更新する必要があり、その結果、ログオン時間が増加します。

ステップ 1: Citrix Virtual Apps and Desktops 環境が利用可能であることを確認する

この新機能を使用するために、Citrix Virtual Apps and Desktops 環境が利用可能であることを確認してください。セットアップの詳細については、「Citrix Virtual Apps and Desktops のインストールと構成」を参照してください。

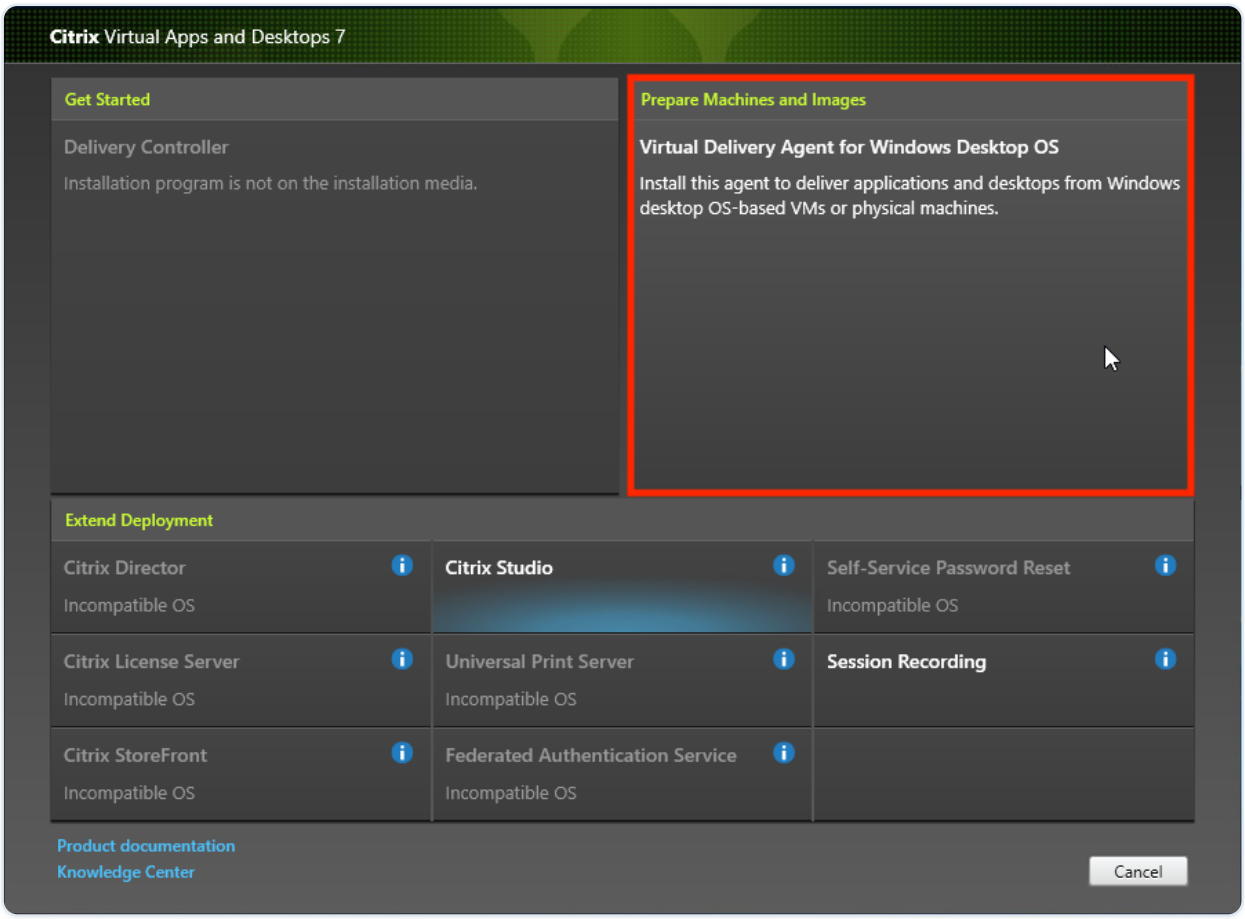
ステップ 2: マスターイメージを準備する

マスターイメージを準備するには:

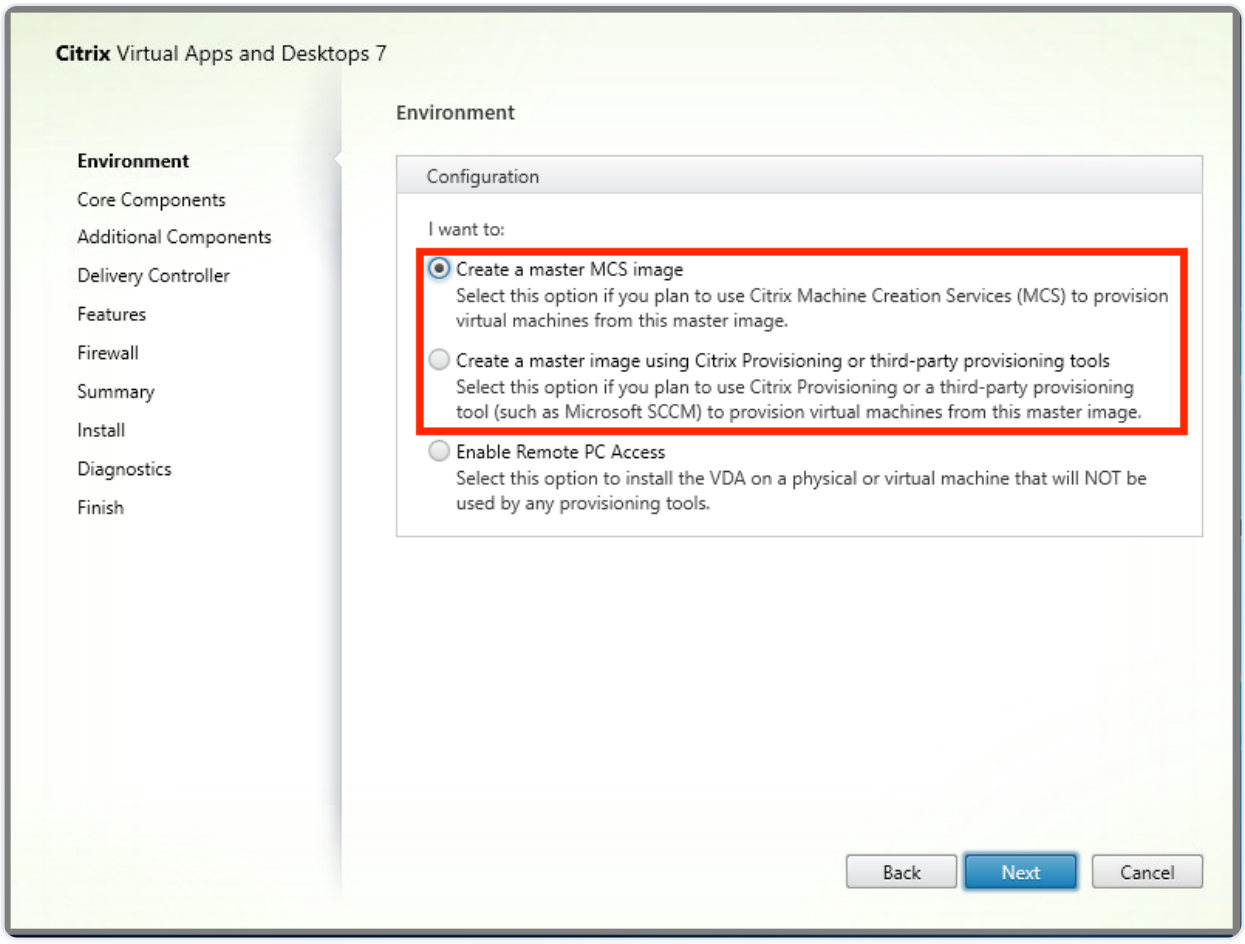
1. マスターイメージを見つけます。組織のエンタープライズアプリケーションと、ユーザーが一般的に役立つその他のアプリをインストールします。
2. Server VDI を展開する場合は、Server VDI の記事の手順に従ってください。オプションコンポーネントである**ユーザーパーソナライゼーションレイヤー**を必ず含めてください。詳細については、「VDA をインストールするためのコマンドラインオプション」を参照してください。

3. Windows 10 を使用している場合は、Virtual Delivery Agent (VDA) 1912 以降をインストールします。古いバージョンの VDA がすでにインストールされている場合は、まず古いバージョンをアンインストールしてください。新しいバージョンをインストールする際は、オプションコンポーネントである**Citrix User Personalization Layer**を次のように選択してインストールしてください。

   a. **Virtual Delivery Agent for Windows Desktop OS**タイルをクリックします:

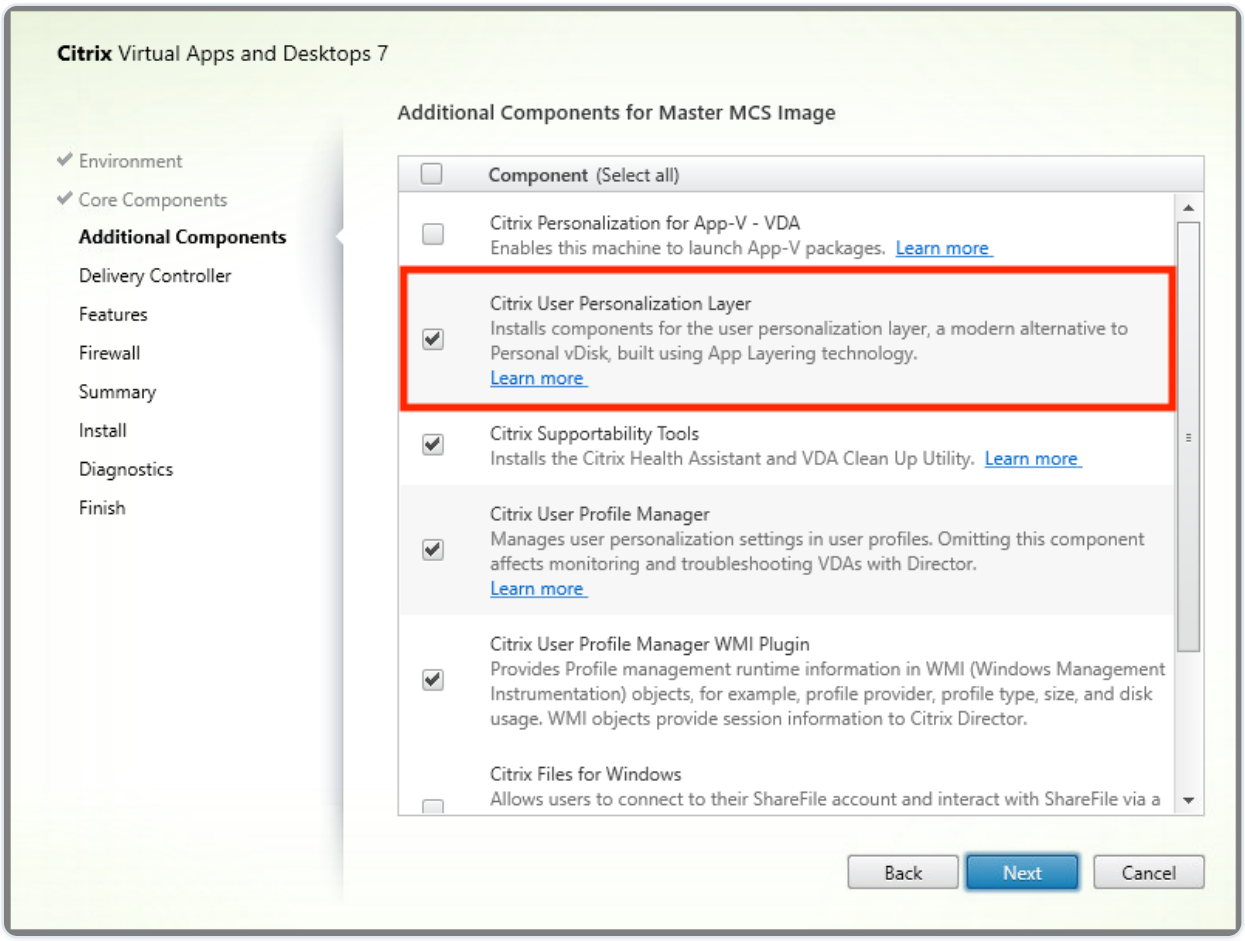


   a. **環境:「マスター MCS イメージを作成する」**または**「Citrix Provisioning またはサードパーティのプロビジョニングツールを使用してマスターイメージを作成する」**のいずれかを選択します。



a. **コアコンポーネント:** 「次へ」をクリックします。

b. **追加コンポーネント:** 「**Citrix User Personalization Layer**」をチェックします。



a. 残りのインストール画面を進み、必要に応じて VDA を構成し、「**インストール**」をクリックします。インストール中にイメージが 1 回以上再起動します。

4. **Windows Update**は無効のままにしてください。ユーザーパーソナライゼーションレイヤーインストーラーは、イメージ上のWindows Updateを無効にします。更新は無効のままにしてください。

イメージをWeb Studioにアップロードする準備ができました。

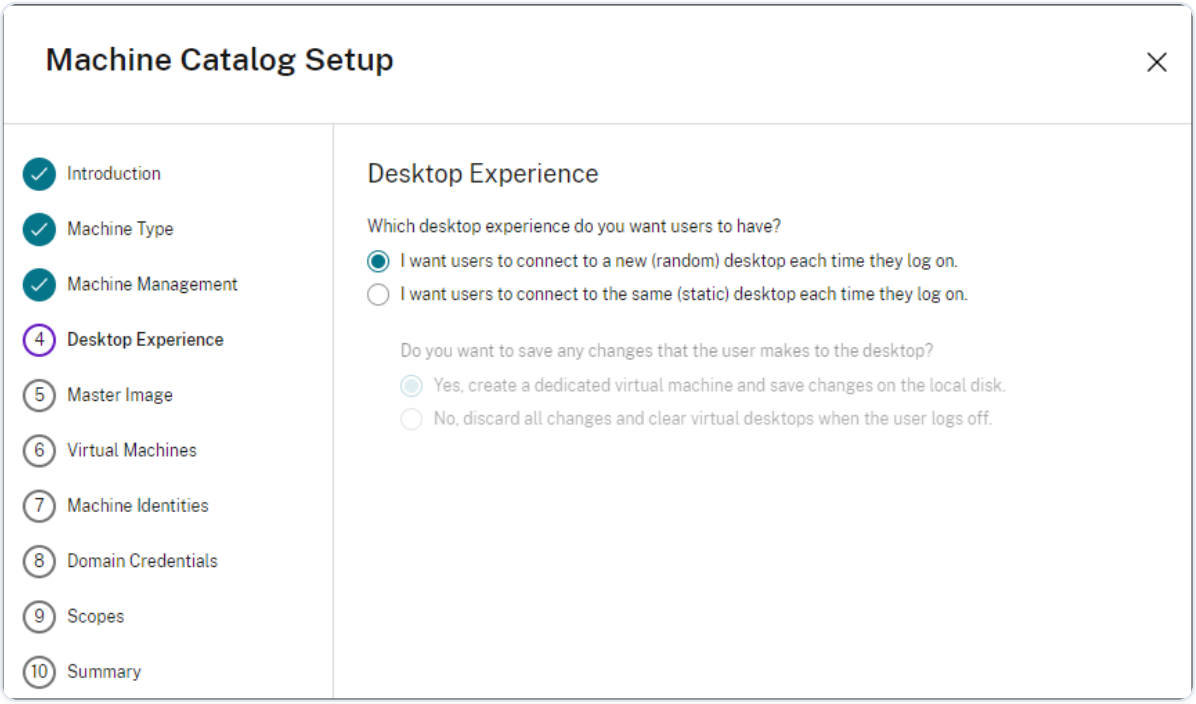
> **注：**
>
> ユーザーパーソナライゼーションレイヤー (UPL) を単にアップグレードしたい場合は、新しいバージョンのUPLとスタンドアロンパッケージを使用してアップグレードできます。VDAをアップグレードする必要はありません。

ステップ3：マシンカタログを作成する

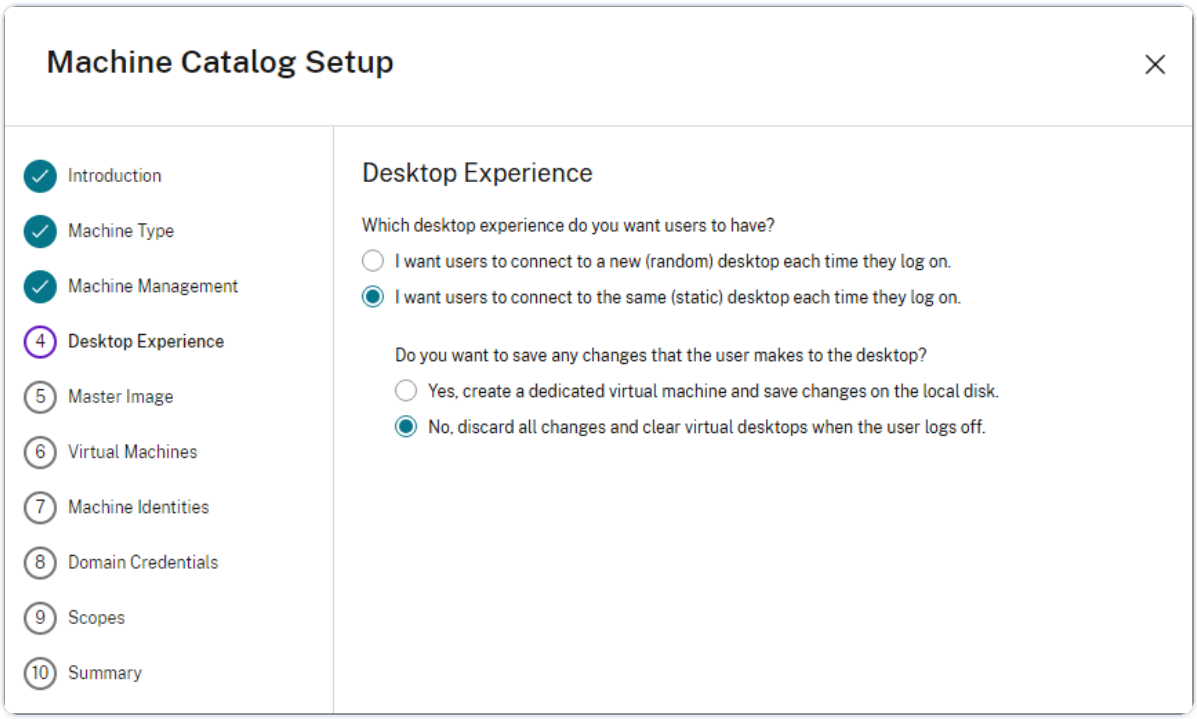
Web Studioで、マシンカタログを作成する手順に従います。カタログ作成時には、以下のオプションを使用します。

1. **オペレーティングシステム**を選択し、**シングルセッションOS**に設定します。
2. **マシン管理**を選択し、**電源管理されているマシン**に設定します。たとえば、仮想マシンやブレードPCなどです。
3. **デスクトップエクスペリエンス**を選択し、以下の例のように、**プールされたランダム**または**プールされた静的**カタログタイプに設定します。

   - **プールされたランダム:**



   - **プールされた静的:** プールされた静的を選択した場合、次のスクリーンショットに示すように、ユーザーがログオフするときにすべての変更を破棄し、仮想デスクトップをクリアするようにデスクトップを構成します。



> **注：**
>
> ユーザーパーソナライゼーションレイヤーは、Citrix Personal vDiskを使用するように構成されている、または専用仮想マシンとして割り当てられているプールされた静的カタログをサポートしていません。

4. MCSを使用している場合は、**イメージ**と、前のセクションで作成したイメージのスナップショットを選択します。
5. 環境の必要に応じて、残りのカタログプロパティを構成します。

ステップ 4: デリバリーグループを作成する

作成したマシンカタログのマシンを含め、**デリバリーグループ**を作成して構成します。詳細については、「デリバリーグループの作成」を参照してください。

ステップ 5: デリバリーグループのカスタムポリシーを作成する

Virtual Delivery Agent 内でユーザーレイヤーのマウントを有効にするには、構成パラメーターを使用して以下を指定します。

- ネットワーク上のどこでユーザーレイヤーにアクセスするか。
- ユーザーレイヤーディスクの最大許容サイズ。

パラメーターを Web Studio でカスタム Citrix ポリシーとして定義し、デリバリーグループに割り当てます。

1. Web Studio にサインインし、左ペインで を選択します。

   Studio でポリシーを選択(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/upl-studio-select-policies.png)

2. アクションバーで を選択します。 ウィンドウが表示されます。
3. 検索フィールドに `user layer` と入力します。利用可能なポリシーのリストに、次の3つのポリシーが表示されます。

   - ユーザーレイヤーの除外
   - ユーザーレイヤーリポジトリパス
   - ユーザーレイヤーサイズ (GB)

   > **注：**
   >
   > サイズを増やすと、新しいユーザーレイヤーに影響し、既存のユーザーレイヤーが拡張されます。サイズを減らすと、新しいユーザーレイヤーにのみ影響します。既存のユーザーレイヤーのサイズが小さくなることはありません。

   ユーザーレイヤーポリシーの選択(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/user-layer-policies.png)

4. **User Layer Repository Path** の横にあるチェックボックスをオンにして、**Edit** をクリックします。**Edit Setting** ウィンドウが表示されます。
5. **Value** フィールドにパスを入力し、**Save** をクリックします。

   - **パス形式:** `\\server-name-or-address\share-name\folder`
   - **パスの例:** `\\Server\Share\UPLUsers`
   - **結果のパスの例: CoolCompanyDomain** の **Alex** という名前のユーザーの場合、パスは次のとおりです。 `\\Server\Share\UPLUsers\Users\CoolCompanyDomain_Alex\A_OK`

   リポジトリパス(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/upl-user-layer-repo-enter-path-no-variables.png)

`%USERNAME%` および `%USERDOMAIN%` 変数、マシン環境変数、および Active Directory (AD) 属性を使用してパスをカスタマイズできます。これらの変数を展開すると、明示的なパスになります。

環境変数の例:

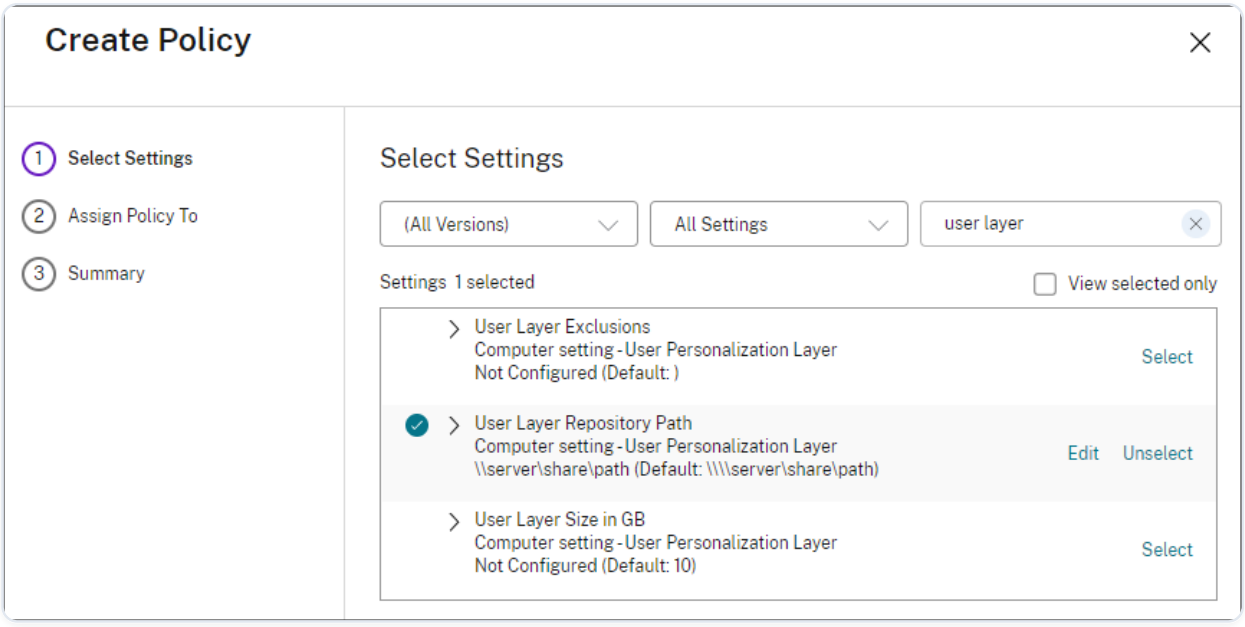
- **パス形式:** `\\Server-name-or-address\share-name\folder-with-environment-variables`
- **パスの例:** `\\Server\Share\UPLUserLayers\%USERNAME%\%USERDOMAIN%`
- **結果のパスの例: CoolCompanyDomain** の **Alex** という名前のユーザーの場合、パスは次のようになります。 `\\Server\Share\UPLUserLayers\Alex\CoolCompanyDomain\A_OK`

環境変数を含むリポジトリパス(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/upl-user-layer-repo-enter-path-variables.png)

カスタム AD 属性の例:

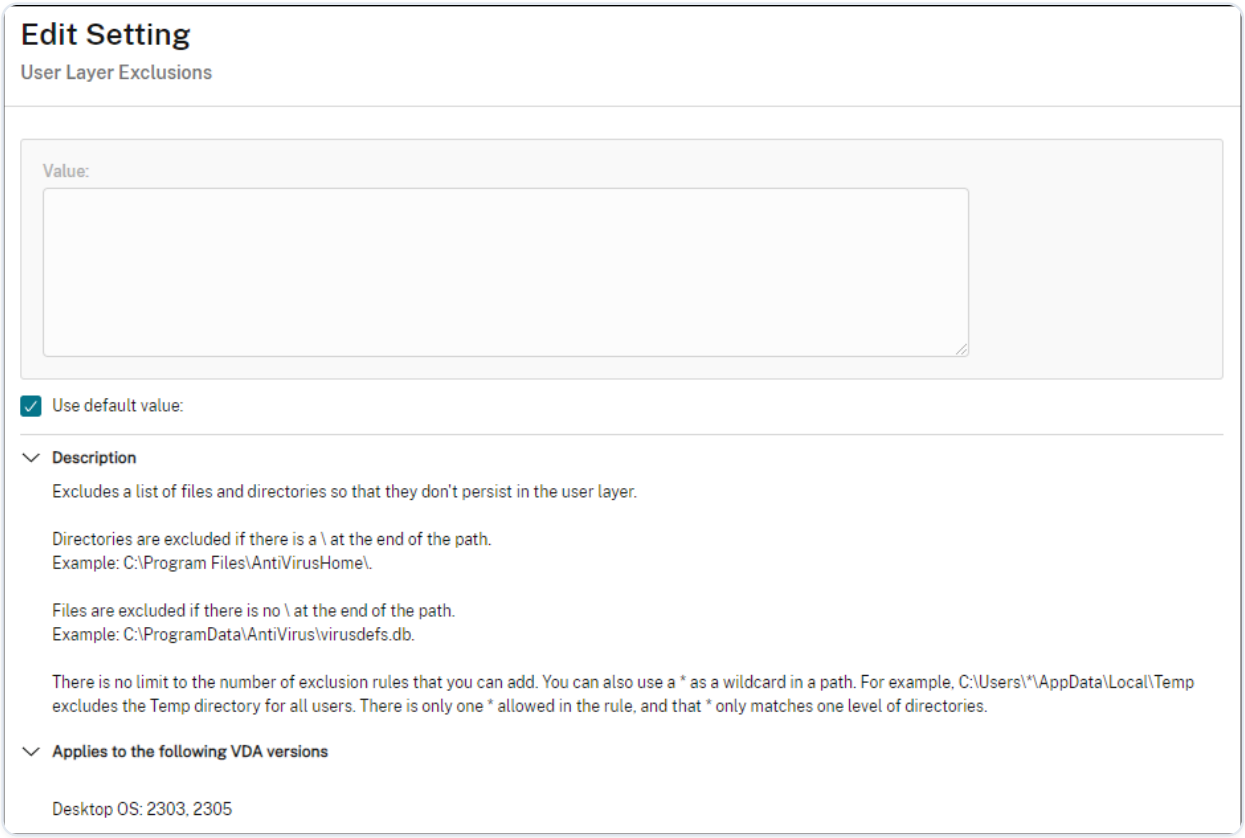
- パス形式: `\\Server-name-or-address\share-name\AD-attribute`
- パスの例: `\\Server\share#sAMAccountName#`
- 結果のパスの例: `\\Server\share\JohnSmith` (現在のユーザーに対して #sAMAccountName# が JohnSmith に解決される場合)

6. オプション: **User Layer Size in GB** の横にあるチェックボックスをオンにして、**Edit** をクリックします。

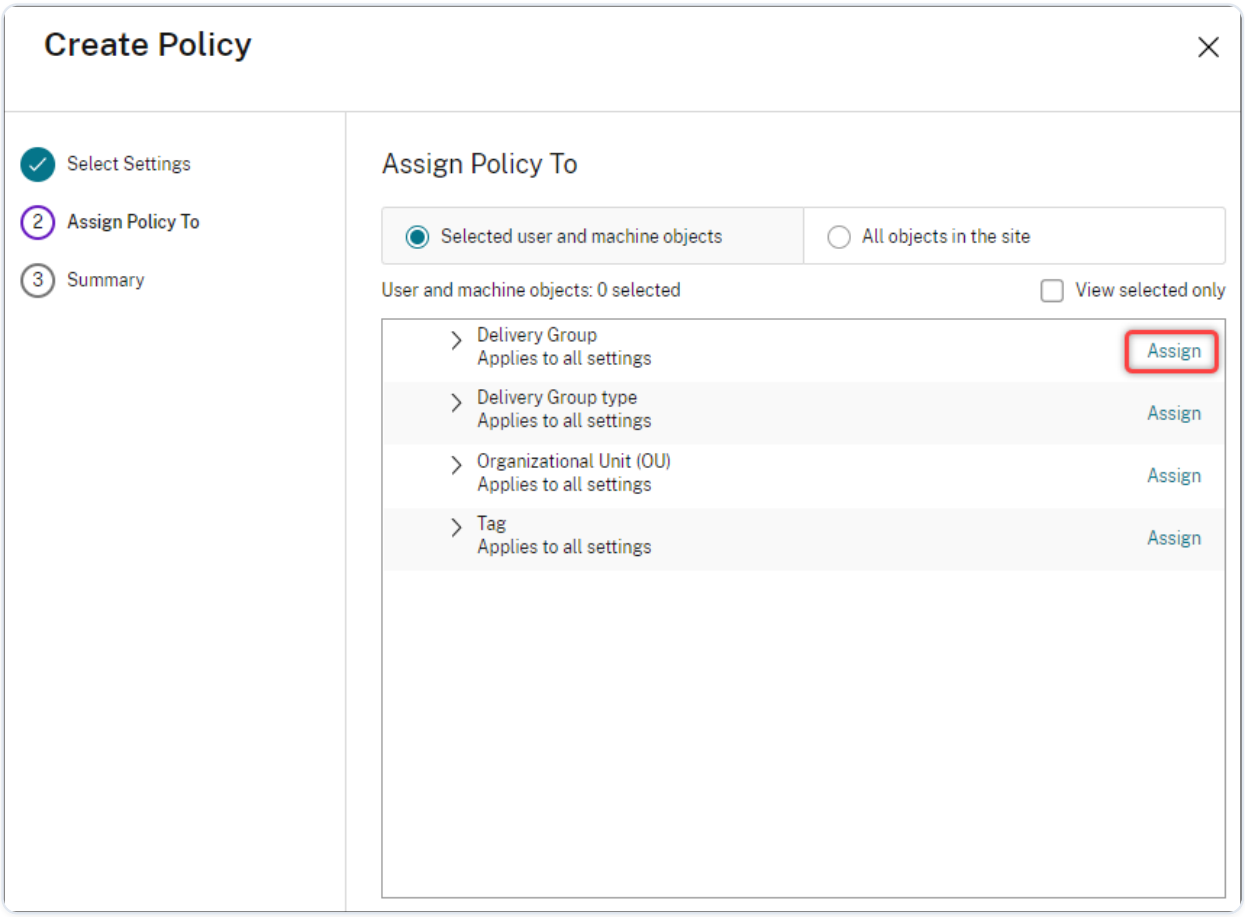


設定の編集ウィンドウが表示されます。

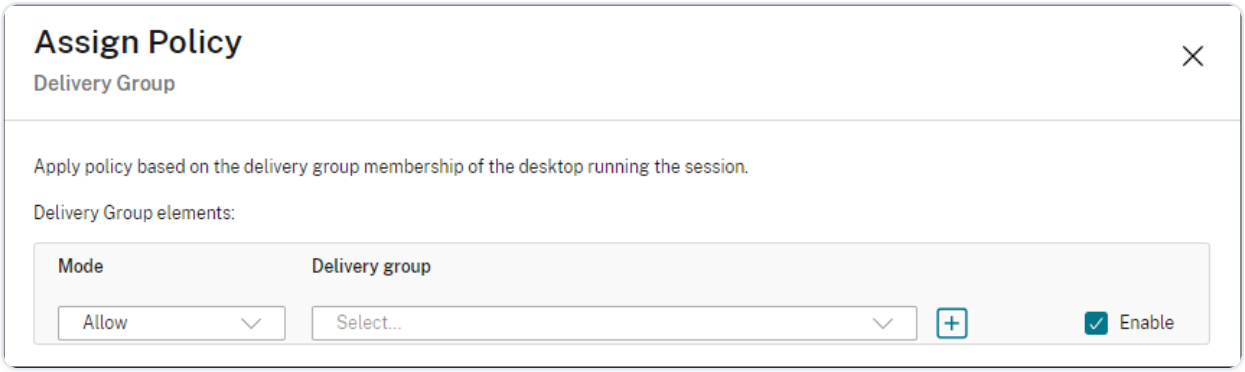
7. オプション: デフォルト値の **10 GB** を、各ユーザーレイヤーが拡張できる最大サイズに変更します。**Save** をクリックします。
8. オプション: **User Layer Exclusions** の横にあるチェックボックスをオンにして、**Edit** をクリックします。



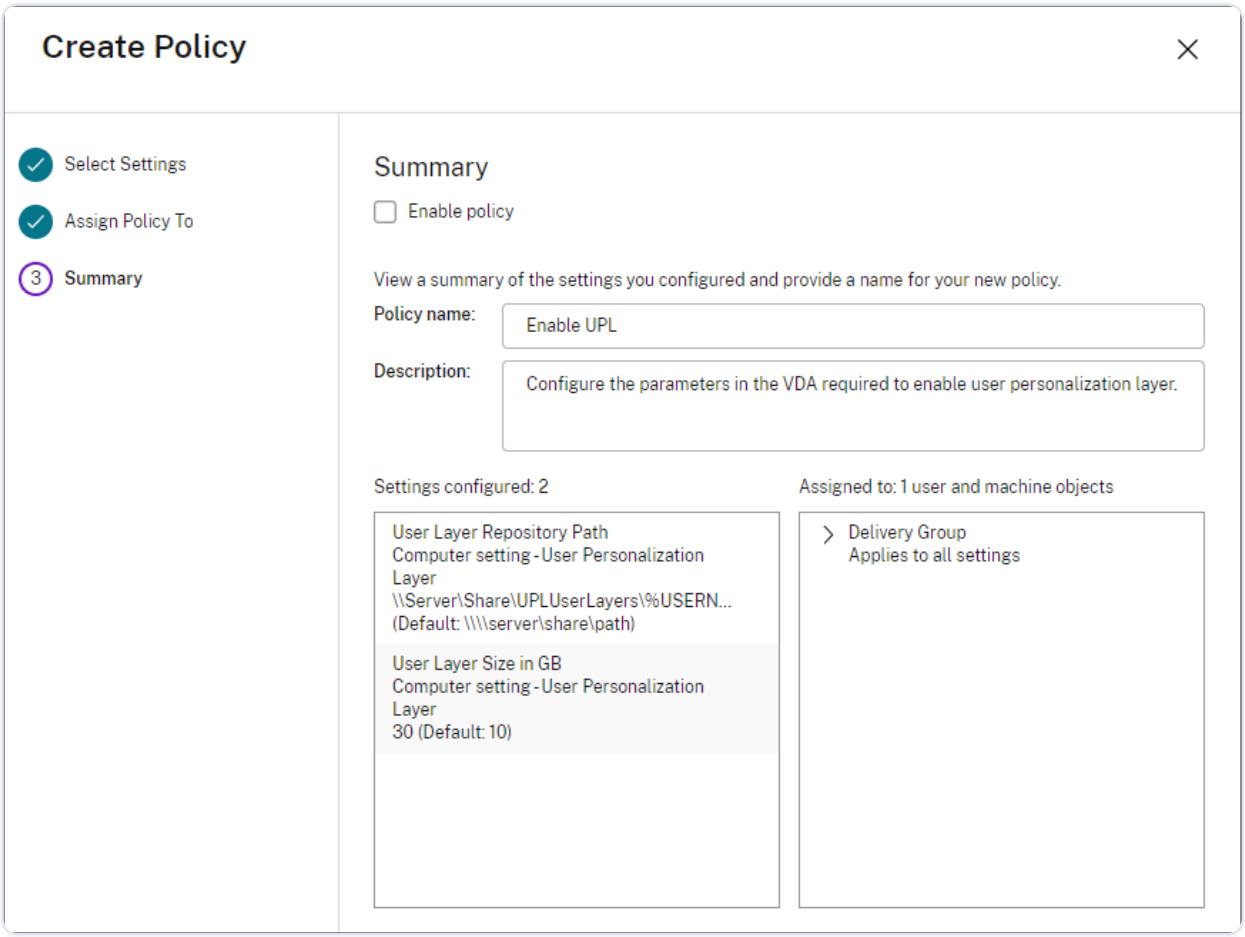
9. オプション: 除外するファイルとフォルダーを指定し、**Save** をクリックします。詳細については、Citrix App Layering のドキュメント を参照してください。
10. 割り当てるユーザーとマシンを設定するには、**Next** をクリックします。この画像で強調表示されている **Delivery Group Assign** リンクをクリックします。



11. **Delivery Group** メニューで、前のセクションで作成したデリバリーグループを選択します。**OK** をクリックします。



12. ポリシーの名前を入力します。ポリシーを有効にするには、チェックボックスをオンにして、**Finish** をクリックします。



ユーザーレイヤーフォルダーのセキュリティ設定を構成する

ドメイン管理者として、ユーザーレイヤーのストレージ場所を複数指定できます。ストレージ場所ごとに（デフォルトの場所を含め）、`\Users` サブフォルダーを作成します。次の設定を使用して、各場所を保護します。

設定名	値	適用先	
作成者/所有者	変更	サブフォルダーとファイルのみ	
所有者の権限	変更	サブフォルダーとファイルのみ	
ユーザーまたはグループ	フォルダーの作成/データの追加、フォルダーの横断/ファイルの実行、フォルダーの一覧表示/データの読み取り、属性の読み取り	選択したフォルダーのみ	

設定名	値	適用先	
システム	フルコントロール	選択されたフォルダー、サブフォルダー、およびファイル	
ドメイン管理者、および選択された管理者グループ	フルコントロール	選択されたフォルダー、サブフォルダー、およびファイル	

ユーザーレイヤーメッセージ

ユーザーがユーザーレイヤーにアクセスできない場合、次のいずれかの通知メッセージが表示されます。

- **ユーザーレイヤーが使用中です**

  `We were unable to attach your user layer because it is in use. Any changes you make to application settings or data will not be saved. Be sure to save any work to a shared network location.`.

- **ユーザーレイヤーが利用できません**

  `We were unable to attach your user layer. Any changes you make to application settings or data will not be saved. Be sure to save any work to a shared network location.`.

- **ユーザーサインアウト後にシステムがリセットされませんでした**

  `This system was not shut down properly. Please log off immediately and contact your system administrator.`.

トラブルシューティング時に使用するログファイル

ログファイル ulayersvc.log には、変更がログに記録されるユーザーパーソナライゼーションレイヤーソフトウェアの出力が含まれています。

```
C:\ProgramData\Unidesk\Logs\ulayersvc.log
```

ユーザーレイヤー/UPL領域の再利用

ユーザーレイヤー/UPL領域の再利用を使用して、ユーザーがログオフするたびにVHDXファイルを自動的に圧縮できます。 詳細については、「ユーザーレイヤー/UPL領域の再利用」を参照してください。

制限事項

ユーザーパーソナライゼーションレイヤー機能をインストールして使用する際は、以下の制限事項に注意してください。

- App Layering内のレイヤーにユーザーパーソナライゼーションレイヤーソフトウェアを展開しようとしないでください。Citrix Virtual Apps and Desktopsでユーザーパーソナライゼーションレイヤーを展開するか、App Layeringイメージテンプレートでユーザーレイヤーを有効にするかのいずれかであり、両方ではありません。どちらのプロセスでも、必要なユーザーレイヤーが生成されます。
- 永続的なマシンカタログでユーザーパーソナライゼーションレイヤー機能を構成しないでください。
- 「セッションホスト」は使用しないでください。
- 新しいOSインストールを実行しているイメージ (Windows 10の同じバージョンであっても) でマシンカタログを更新しないでください。ベストプラクティスは、マシンカタログ作成時に使用した同じマスターイメージ内でOSの更新を適用することです。
- ブート時ドライバーやその他の初期ブートパーソナライゼーションは使用しないでください。
- PvDデータをユーザーパーソナライゼーションレイヤー機能に移行しないでください。
- 既存のユーザーレイヤーを完全なApp Layering製品からユーザーパーソナライゼーションレイヤー機能に移行しないでください。
- 異なるマスターOSイメージを使用して作成されたユーザーレイヤーにアクセスするために、ユーザーレイヤーのSMBパスを変更しないでください。
- ユーザーがセッションからログアウトし、再度ログインすると、新しいセッションはプール内の別のマシンで実行されます。VDI環境では、Microsoft Software Centerは、最初のマシンではアプリケーションを**インストール済み**として表示しますが、2番目のマシンでは**利用不可**として表示します。

  アプリケーションの実際のステータスを確認するには、ユーザーにSoftware Centerでアプリケーションを選択し、**インストール**をクリックするよう指示します。すると、SCCMがステータスを実際の値に更新します。

- ユーザーパーソナライゼーションレイヤー機能が有効になっているVDA内で、Software Centerが起動直後に停止することがあります。この問題を回避するには、XenDesktop VDI環境でのSCCMの実装に関するMicrosoftの推奨事項に従ってください。また、Software Centerを起動する前に、`ccmexec`サービスが実行されていることを確認してください。
- グループポリシー (コンピューター設定) では、ユーザーレイヤー設定は、マスターイメージに適用された設定を上書きします。そのため、GPOを使用してコンピューター設定で行った変更は、次回のセッションログイン時にユーザーに常に適用されるとは限りません。

  この問題を回避するには、次のコマンドを発行するユーザーログオンスクリプトを作成します。

  ```
  gpupdate /force
  ```

  たとえば、あるお客様は、ユーザーがログインするたびに次のコマンドを実行するように設定しました。

  ```
  gpudate /Target:Computer /force
  ```

  最良の結果を得るには、ユーザーがログインした後で、コンピューター設定への変更をユーザーレイヤーに直接適用します。
- ドメインユーザーアカウントは、マスターイメージに最後にログインしたユーザーであってはなりません。そうしないと、そのイメージからプロビジョニングされたマシンで問題が発生する可能性があります。
- 純粋なAzure AD環境でUPLが有効になっている場合、Azure上で実行されているWindowsの根本的な問題により、カスタム証明書は保持されません。Microsoftが将来の機能強化でこの問題を修正した場合、この記事を更新します。

コンポーネントの削除

コンポーネントを削除するには、プログラムの削除または変更を行うWindows機能を使用することをお勧めします。または、コマンドラインまたはインストールメディア上のスクリプトを使用してコンポーネントを削除することもできます。

コンポーネントを削除しても、前提条件は削除されず、ファイアウォール設定も変更されません。たとえば、Delivery Controller™を削除しても、SQL Serverソフトウェアとデータベースは削除されません。

Web Interfaceを含む以前の展開からControllerをアップグレードした場合は、Web Interfaceコンポーネントを個別に削除する必要があります。インストーラーを使用してWeb Interfaceを削除することはできません。

以下に記載されていない機能の削除については、その機能のドキュメントを参照してください。

準備

Controllerを削除する前に、サイトから削除してください。詳しくは、「Controllerを削除する」を参照してください。

StudioとDirectorを削除する前に、それらを閉じます。

Windowsのプログラムの削除または変更機能を使用してコンポーネントを削除する

Windowsのプログラムの削除または変更機能から：

- Controller、Studio、Director、License Server、またはStoreFrontを削除するには、**Citrix Virtual Apps *version*** または **Citrix Virtual Apps and Desktops™ *version*** を右クリックして、**アンインストール**を選択します。インストーラーが起動します。削除するコンポーネントを選択します。

  または、**Citrix StoreFront**を右クリックして**アンインストール**を選択することで、StoreFront™を削除できます。
- VDAを削除するには、**Citrix Virtual Delivery Agent *version*** を右クリックして、**アンインストール**を選択します。インストーラーが起動し、削除するコンポーネントを選択できます。デフォルトでは、削除後にマシンは自動的に再起動します。
- Universal Print Serverを削除するには、**Citrix Universal™ Print Server**を右クリックして、**アンインストール**を選択します。

コマンドラインを使用してコアコンポーネントを削除する

`\x64\XenDesktop Setup`ディレクトリから、`XenDesktopServerSetup.exe`コマンドを実行します。

- 1つ以上のコンポーネントを削除するには、`/remove`および`/components`オプションを指定します。
- すべてのコンポーネントを削除するには、`/removeall`オプションを指定します。

コマンドとパラメーターの詳細については、「コマンドラインを使用したインストール」を参照してください。

例えば、次のコマンドはWeb Studioを削除します。

```
\x64\XenDesktop Setup\XenDesktopServerSetup.exe /remove /components webstudio
```

コマンドラインを使用してVDAを削除する

`\x64\XenDesktop Setup`ディレクトリから、`XenDesktopVdaSetup.exe`コマンドを実行します。

- 1つ以上のコンポーネントを削除するには、`/remove`オプションと`/components`オプションを使用します。例えば、VDAとCitrix Workspaceアプリを削除するには、`/remove /components vda,plugin`を使用します。
- `/removeall`オプションはVDAのみを削除します。Citrix Workspaceアプリは削除しません。

コマンドとパラメーターの詳細については、コマンドラインを使用したインストールを参照してください。

デフォルトでは、削除後にマシンは自動的に再起動します。

Active Directoryでスクリプトを使用してVDAを削除するには、スクリプトを使用したVDAのインストールまたは削除を参照してください。

アップグレードと移行

はじめに

注:

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

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

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

注:

- **「バージョン交差」の警告**

> 異なるLTSRバージョンは、そのメンテナンスサイクルが重複することがよくありますのでご注意ください。アップグレードを開始する前に、現在の累積更新プログラム（CU）とターゲットLTSR（またはその後のCU）の両方の**リリース日**を確認する必要があります。 現在の環境のリリース日がターゲットLTSRまたはLTSR CUのリリース日よりも**後**である場合、Citrixは新しいLTSRの次のCUを待つことを強く推奨します。それ以外の場合、古いコードが既存のセキュリティ更新プログラム、安定性パッチ、および機能強化を上書きする可能性があります。
>
> - **「サポート対象外の状態」条項**
>
>   リリース日が古いバージョンへのアップグレードを試みることは、技術的には**コアコンポーネントのダウングレード**と見なされます。この特定の構成は、**「部分的な成功」**ステータスになる可能性があります。

> アップグレードすると、新しいマシンやサイトを設定することなく、展開がCitrix Virtual Apps and Desktops 7 **Current Release (CR)**に変更されます。これはインプレースアップグレードとして知られています。

アップグレードにより、利用資格のある最新の機能とテクノロジーにアクセスできるようになります。アップグレードには、以前のバージョンからの修正、明確化、および機能強化も含まれる場合があります。

アップグレードの概要

1. アップグレードを開始する前に、展開のアップグレードの記事を確認してください。これは、アップグレードの準備方法と実装方法を学ぶための主要な情報源です。
2. 現在のカスタマーサクセスサービスの日付が有効であり、期限切れになっていないことを確認してください。詳細については、Customer Success Services renewal licensesの記事を参照してください。
3. 準備ガイドを完了してください。
4. コアコンポーネントをアップグレードするためにインストーラーを実行します。
5. システムデータベースとサイトをアップグレードします。
6. イメージ上のVDA（またはマシンに直接）をアップグレードします。
7. その他のコンポーネントをアップグレードします。

各準備およびアップグレードの手順は、Upgrade a deploymentで詳しく説明されています。

アップグレード可能なバージョン

Citrix Virtual Apps and Desktops 2402 LTSRへは、以下からアップグレードできます。

- Virtual Apps and Desktops 2203 LTSR（CUの有無にかかわらず、CU5までを含む）
- Virtual Apps and Desktops 1912 LTSR（CUの有無にかかわらず、CU9までを含む）
- 現在サポートされているCitrix Virtual Apps and DesktopsのCRバージョン

> 注:
>
> - アップグレードプロセスを開始する前に、Citrix®は、お客様が管理された環境でアップグレードをテストし、特定の要件を満たしていることを確認することを推奨します。さらに、スムーズな移行を確実にするために、非推奨リストや既知の問題を含むすべての関連製品ドキュメントを確認することをお勧めします。このアプローチは、本番システムへの潜在的な中断を軽減し、全体的なアップグレードエクスペリエンスを向上させるのに役立ちます。
> - Citrix Virtual Apps and Desktops 1912 LTSRは、まもなくサポート終了フェーズに達します。 サポートされているバージョンの一覧については、Product Matrixを参照してください。

よくある質問

このセクションでは、Citrix Virtual Apps and Desktops のアップグレードに関するよくある質問に回答します。

- **Virtual Apps and Desktops 環境をアップグレードする正しい順序は何ですか？**

  推奨されるアップグレードシーケンスの図と説明については、アップグレードシーケンス および アップグレード手順 を参照してください。

- **私のサイトには複数の Delivery Controller (異なるゾーンに) があります。一部のみをアップグレードした場合、どうなりますか？同じメンテナンス期間中にサイト内のすべての Controller をアップグレードする必要がありますか？**

  各 Controller 上のさまざまなサービスが相互に通信するため、すべての Delivery Controller を同じメンテナンス期間中にアップグレードすることがベストプラクティスです。異なるバージョンを維持すると、問題が発生する可能性があります。メンテナンス期間中には、Controller

の半分をアップグレードし、サイトをアップグレードしてから、残りの Controller をアップグレードすることをお勧めします。詳細については、アップグレード手順 を参照してください。

- **最新バージョンに直接アップグレードできますか、それとも段階的なアップグレードを行う必要がありますか？**

  アップグレード先のバージョンの **新機能** の記事で明示的に記載されていない限り、ほとんどの場合、中間リリースをスキップして最新バージョンにアップグレードできます。

- **お客様は Long Term Service Release (LTSR) 環境から Current Release にアップグレードできますか？**

  はい。お客様は Long Term Service Release に長期間留まる必要はありません。お客様は、ビジネス要件と機能に基づいて、LTSR 環境を Current Release に移行できます。

- **コンポーネントの混在バージョンは許可されますか？**

  各サイト内では、Citrix はすべてのコンポーネントを同じバージョンにアップグレードすることを推奨しています。一部のコンポーネントで以前のバージョンを使用することはできますが、最新バージョンのすべての機能が利用できるとは限りません。詳細については、混在環境に関する考慮事項 を参照してください。

- **Current Release はどのくらいの頻度でアップグレードする必要がありますか？**

  Current Release は、リリース日から 6 か月後に End of Maintenance (EOM) に達します。Citrix は、お客様が最新の Current Release を採用することを推奨しています。Current Release は、リリース日から 18 か月後に End of Life (EOL) に達します。

- **推奨されるのは、LTSR へのアップグレードですか、それとも CR へのアップグレードですか？**

  Current Release (CR) は、最新かつ最も革新的なアプリ、デスクトップ、およびサーバー仮想化の機能を提供します。これにより、最先端のテクノロジーを維持し、競合他社の一歩先を行くことができます。

  長期サービスリリース (LTSR) は、長期間にわたって同じベースバージョンを維持することを好む大規模なエンタープライズ生産環境に最適です。

- **ライセンスをアップグレードする必要がありますか？**

  現在のライセンスの有効期限が切れておらず、アップグレード先のリリースで有効であることを確認してください。CTX111618 を参照してください。更新については、「Customer Success Services renewal licenses」を参照してください。

- **アップグレードにはどのくらい時間がかかりますか？**

展開のアップグレードにかかる時間は、インフラストラクチャとネットワークによって異なります。そのため、正確な時間をお伝えすることはできません。

- **ベストプラクティスは何ですか？**

  準備ガイド を理解し、それに従っていることを確認してください。

- **どのオペレーティングシステムがサポートされていますか？**

  アップグレード先のバージョンの「システム要件」の記事に、サポートされているOSが記載されています。

  現在の展開でサポートされなくなったオペレーティングシステムを使用している場合は、「以前のオペレーティングシステム」を参照してください。

- **VMware vSphere (vCenter + ESXi) のどのバージョンがサポートされていますか？**

  CTX131239 には、サポートされているホストとバージョン、および既知の問題へのリンクが記載されています。

- **私のバージョンはいつEOLになりますか？**

  製品マトリックス を確認してください。

- **最新リリースにおける既知の問題は何ですか？**

  - シトリックス バーチャル アプリケーションズ アンド デスクトップ
  - StoreFront
  - シトリックス プロビジョニング
  - シトリックス ライセンス サーバー
  - Windows向けCitrix Workspaceアプリ(/ja-jp/citrix-workspace-app-for-windows/about.html#known-issues)

詳細情報

長期サービスリリース (LTSR) 展開の更新には累積更新プログラム (CU) が使用されます。CUはLTSRのベースラインコンポーネントを更新し、各CUには独自のメタインストーラーが含まれています。

各CUには専用のドキュメントがあります。たとえば、2203 LTSRの場合、最新のCUについては、そのLTSRの**「新機能」**ページにあるリンクを確認してください。各CUページには、サポートされているバージョン情報、手順、およびCUダウンロードパッケージへのリンクが含まれています。

移行

クラウドへの移行

Citrix Virtual Apps and Desktopsの自動構成ツールを使用して、オンプレミス展開をクラウドに移行できます。詳しくは、「クラウドへの移行」を参照してください。

レガシー移行

移行とは、以前の展開から新しいバージョンにデータを移動することです。このプロセスには、新しいコンポーネントのインストールと新しいサイトの作成、古いファームからのデータのエクスポート、そして新しいサイトへのデータのインポートが含まれます。

XenAppおよびXenDesktopのバージョン、または以前のCitrix Virtual Apps and Desktopsのバージョンを移行するためのサポートされているツールやスクリプトはありません。この製品ドキュメントに記載されているCitrix Virtual Apps and Desktopsのバージョンについては、*アップグレード*がサポートされています。

以前のXenApp 6.xの移行コンテンツについては、以下を参照してください。これらのスクリプトはサポートも保守もされていません。

- XenApp 6.xバージョンのオープンソース移行スクリプトは`<https://github.com/citrix/xa65migrationtool>`で入手できます。Citrixはこれらの移行スクリプトをサポートまたは保守していません。
- **「7.xでの変更点」**、**「XenApp 6.5ワーカーを新しいVDAにアップグレードする」**、および**「XenApp 6.xの移行」**については、`<https://docs.citrix.com/ja-jp/legacy-archive/citrix-virtual-apps-and-desktops.html>`にあるCitrix Virtual Apps and Desktopsのレガシーアーカイブを参照してください。

展開をアップグレードする

> **注：**
>
> 従来、さまざまなオンプレミスコンポーネントのアクティベーションに使用されてきたファイルベースのライセンスシステムは、April 15, 2026にサポート終了（EOL）となります。License Activation Service (LAS) は、Citrix製品スイート全体の製品アクティベーションのための次世代テクノロジーです。April 15, 2026以降、Citrixオンプレミスコンポーネントをアクティベートおよびライセンス供与する唯一の方法はLASになります。サポートを継続するに

は、Citrix Virtual Apps and Desktopsの展開がLAS互換バージョンである必要があります。LAS互換の最小要件となるCVADバージョンは次のとおりです。

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

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

はじめに

注：

この記事では、Web Studioを含む展開のアップグレードについて説明します。Citrix Studioを含むアップグレードについては、Citrix Virtual Apps and Desktops™ 7 2212以前の同等の記事を参照してください。

新しいマシンやサイトを最初にセットアップすることなく、特定の展開を新しいバージョンにアップグレードできます。これはインプレースアップグレードと呼ばれます。

アップグレードできるCitrix Virtual Apps and Desktopsのバージョンについては、(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/upgrade-migrate.html#versions-you-can-upgrade)を参照してください。

Citrix Virtual Apps and Desktopsのいずれかのリリースにアップグレードする前に、現在のCustomer Success Servicesの有効期限が切れていないことを確認してください。詳細については、(/ja-jp/licensing/current-release/customer-success-services.html#customer-success-services-renewal-licenses)の記事を参照してください。

アップグレードを開始するには、新しいバージョンのインストーラーを実行して、以前にインストールされたコアコンポーネント、VDA、および特定のその他のコンポーネントをアップグレードします。その後、データベースとサイトをアップグレードします。

新しいバージョンが提供されている場合、フルプロダクトインストーラー（およびスタンドアロンVDAインストーラー）でインストールできるすべてのコンポーネントをアップグレードできます。フルプロダクトインストーラーでインストールされないその他のコンポーネント（Citrix Provisioning™やProfile Managementなど）については、そのコンポーネントのドキュメントを参照してください。ホストのアップグレードについては、該当するドキュメントを参照してください。

アップグレードを開始する前に、この記事のすべての情報を確認してください。

アップグレードシーケンス

次の図はアップグレードシーケンスのステップを示しています。アップグレード手順 には、図の各ステップの詳細が記載されています。

アップグレードシーケンスのフロー図

> **注：**
>
> 障害を回避するには、新しいマシンカタログの作成、マシンカタログの削除、デリバリーグループ内のマシンの更新など、プロビジョニングおよびデリバリーグループ関連のタスクを実行する前に、すべてのDelivery Controllerとデータベースをアップグレードする必要があります。

ハイブリッドライツライセンス

ハイブリッドライツライセンスは、お客様が永続ライセンスからクラウドサービスサブスクリプションに移行またはアップグレードする際に、クラウドサービスサブスクリプションに加えて提供される期間ベースのサブスクリプションライセンスです。DaaSサブスクリプションでハイブリッドライツアドオンを購入することもできます。

SaaS属性を持つハイブリッドライツライセンスをお持ちの場合、Citrix Virtual Apps and Desktops LTSR 2203以降にアップグレードすると、Citrix Virtual Apps and Desktops LTSR 1912では利用できなかった機能にアクセスできるようになります。これらの機能には、Microsoft Azure、AWS EC2、Google Cloudなどのパブリッククラウドでのワークロードのプロビジョニングとホスティングが含まれます。新しいライセンスファイルを展開する前に、ライセンスサーバーを最新バー

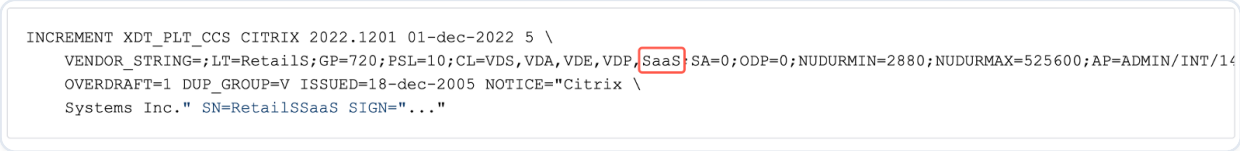
ジョンに更新してください。この前提条件を満たさない場合、サイトのアップグレードおよび作成中にエラーや推奨事項が発生する可能性があります。

SaaS属性のないハイブリッドライツライセンスにアクセスできる場合は、次の手順に従ってSaaS属性を持つ新しいハイブリッドライツライセンスにアクセスしてください。

注：

- 新しいライセンスコードが記載されたメールが届きます。詳細については、「ライセンスアクセスコードの使用」を参照してください。
- 既存のライセンスは取り消されます。取り消されたライセンスは、ライセンスサーバーから削除し、その後新しいライセンスをインストールする必要があります。詳細については、「ライセンスファイルの削除」を参照してください。

1. citrix.com のライセンス管理ポータルにアクセスし、クラウドプロビジョニング権限が有効になっている（SaaS属性を持つ）新しいハイブリッドライツライセンスファイルをダウンロードします。詳細については、「ライセンスのダウンロード」を参照してください。次の画像は、IncrementsセクションにあるSaaS属性を持つハイブリッドライツライセンスファイルを示しています。



2. ハイブリッドライツライセンスファイルをライセンスサーバーにインストールします。詳細については、「ライセンスのインストール」を参照してください。
3. ライセンスのエディションまたはモデルに変更がある場合は、brokerコマンドを実行してエディションとモデルを設定し、インプレースアップグレードを開始してください。Brokerコマンドの詳細については、「Broker PowerShell SDK」セクションを参照してください。

Citrix Virtual Apps and Desktops Current ReleasesおよびLong Term Service Releasesでのパブリッククラウドサポートの詳細については、「CTX270373」を参照してください。

アップグレード手順

ほとんどの主要な製品コンポーネントは、コンポーネントを含むマシンで製品インストーラーを実行することでアップグレードできます。

1台のマシンに複数のコンポーネント（例：StudioとLicense Server）が含まれている場合、製品メディアにそれらのソフトウェアの新しいバージョンが含まれていれば、そのマシン上のすべてのコンポーネントがアップグレードされます。

インストーラーを使用するには：

- フル製品インストーラーのグラフィカルインターフェイスを実行するには、マシンにログオンし、メディアを挿入するか、新しいリリースのISOドライブをマウントします。**AutoSelect**をダブルクリックします。
- コマンドラインインターフェイスを使用するには、適切なコマンドを発行します。「コマンドラインを使用したインストール」を参照してください。

ステップ1：準備

アップグレードを開始する前に、準備が整っていることを確認してください。必要なタスクを読み、完了してください：

- PVD、AppDisks™、およびサポートされていないホストの削除
- PvDまたはAppDiskコンポーネントを持つVDA
- 制限事項
- 混在環境に関する考慮事項
- 以前のオペレーティングシステム
- 準備
- サイトの事前テスト
- SQL Serverのバージョンチェック

ステップ2：License Serverのアップグレード

インストールに新しいバージョンのCitrix License Serverソフトウェアが含まれている場合、他のコンポーネントよりも先にこのコンポーネントをアップグレードしてください。

まだLicense Serverが新しいバージョンと互換性があるかどうかを判断していない場合は、他のコアコンポーネントをアップグレードする前に、License Serverでインストーラーを実行することが不可欠です。

ステップ3：StoreFront™のアップグレード

インストールメディアに新しいバージョンのStoreFrontソフトウェアが含まれている場合は、StoreFrontサーバーがインストールされているマシンでインストーラーを実行します。

- グラフィカルインターフェイスで、**Extend deployment**セクションから**Citrix StoreFront**を選択します。
- コマンドラインから、Citrix Virtual Apps and Desktopsインストールメディアの`x64`フォルダーにある`CitrixStoreFront-x64.exe`を実行します。

ステップ4：Directorのアップグレード

インストールメディアに新しいバージョンのDirectorソフトウェアが含まれている場合は、Directorがインストールされているマシンでインストーラーを実行します。

ステップ5：Citrix Provisioningのアップグレード

Citrix Provisioningインストールメディアは、Citrix Virtual Apps and Desktopsインストールメディアとは別に提供されています。Citrix Provisioningサーバーおよびターゲットデバイスソフトウェアのインストールとアップグレード方法については、Citrix Provisioning製品ドキュメントを参照してください。

ステップ6：Delivery Controllerの半分をアップグレードする

たとえば、サイトに4つのControllerがある場合、そのうちの2つでインストーラーを実行します。

Controllerの半分をアクティブなままにしておくことで、ユーザーはサイトにアクセスできます。VDAは残りのControllerに登録できます。Controllerの数が少ないため、サイトの容量が低下する場合があります。アップグレードは、最終的なデータベースアップグレード手順中に新しいクライアント接続の確立に一時的な中断を引き起こすだけです。アップグレードされたControllerは、サイト全体がアップグレードされるまで要求を処理できません。

サイトにControllerが1つしかない場合、アップグレード中は動作しません。

実際のアップグレードが開始される前に、最初のControllerで事前サイトテストが実行されます。詳細については、事前サイトテストを参照してください。

ステップ 7: Studio のアップグレード

Web Studio をまだアップグレードしていない場合（別のコンポーネントと同じマシンにあったため）、Studio が含まれているマシンでインストーラーを実行します。

> **注：**
>
> Web Studio をアップグレードした後、バージョン情報がすぐに更新されない場合があります。Web Studio がすでに最新の状態であっても、アップグレードを促されることがありま

す。この問題に対処するには、Web Studio サーバーに移動し、インターネットインフォメーションサービス (IIS) マネージャーを開き、 > > に移動して、 ペインで を選択します。

ステップ 8: Studio の再起動

アップグレードされた Web Studio を再起動します。アップグレードプロセスが自動的に再開されます。

ステップ 9: データベースとサイトのアップグレード

注：

障害を回避するため、新しいマシンカタログの作成、マシンカタログの削除、デリバリーグループ内のマシンの更新など、プロビジョニングおよびデリバリーグループ関連のタスクを実行する前に、すべての Delivery Controller とデータベースをアップグレードする必要があります。

SQL Server データベースのスキーマを更新するために必要な権限については、準備 を確認してください。

- SQL Server データベーススキーマを更新する十分な権限がある場合は、自動データベースアップグレードを開始できます。データベースとサイトを自動的にアップグレードする に進みます。
- データベース権限が不十分な場合は、スクリプトを使用する手動アップグレードを開始し、データベース管理者（必要な権限を持つユーザー）の助けを借りて進めることができます。手動アップグレードの場合、Studio ユーザーがスクリプトを生成し、サービスを有効/無効にするスクリプトを実行します。データベース管理者は、SQLCMD ユーティリティまたは SQLCMD モードの SQL Server Management Studio を使用して、データベーススキーマを更新する他のスクリプトを実行します。データベースとサイトを手動でアップグレードする に進みます。
- マルチゾーン展開でデータベースとサイトを自動的にアップグレードする場合、Citrix は、dbschema のアップグレードを、サイトの SQL Server データベースをホストするのと同じゾーンで実行することを推奨します。そうしないと、データベースとサイトの自動アップグレードが失敗する可能性があります。

Citrix は、アップグレード前にデータベースをバックアップすることを強く推奨します。CTX135207 を参照してください。データベースのアップグレード中は、製品サービスが無効にな

ります。その間、Controller はサイトの新しい接続を仲介できないため、慎重に計画してください。

データベースとサイトを自動的にアップグレードする

1. 新しくアップグレードされた Studio を起動します。
2. サイトのアップグレードを自動的に開始することを示し、準備ができたことを確認します。

データベースとサイトのアップグレードが進行します。

データベースとサイトを手動でアップグレードする

1. 新しくアップグレードされたStudioを起動します。
2. サイトを手動でアップグレードすることを示します。ウィザードはライセンスサーバーの互換性を確認し、確認を求めます。
3. データベースをバックアップしたことを確認します。

   ウィザードは、スクリプトとアップグレード手順のチェックリストを生成して表示します。アップグレード対象の製品バージョン以降、データベースのスキーマが変更されていない場合、そのスクリプトは生成されません。たとえば、ログデータベースのスキーマが変更されない場合、`UpgradeLoggingDatabase.sql`スクリプトは生成されません。
4. 次のスクリプトを、表示されている順序で実行します。

   - `DisableServices.ps1`: Studioユーザーは、製品サービスを無効にするために、ControllerでこのPowerShellスクリプトを実行します。
   - `UpgradeSiteDatabase.sql`: データベース管理者は、サイトデータベースを含むサーバーでこのSQLスクリプトを実行します。
   - `UpgradeMonitorDatabase.sql`: データベース管理者は、モニターデータベースを含むサーバーでこのSQLスクリプトを実行します。
   - `UpgradeLoggingDatabase.sql`: データベース管理者は、構成ログデータベースを含むサーバーでこのSQLスクリプトを実行します。このスクリプトは、このデータベースが変更された場合（たとえば、ホットフィックスを適用した後など）にのみ実行してください。
   - `EnableServices.ps1`: Studioユーザーは、製品サービスを有効にするために、ControllerでこのPowerShellスクリプトを実行します。

   データベースのアップグレードが完了し、製品サービスが有効になると、Studioは環境と構成を自動的にテストし、HTMLレポートを生成します。問題が特定された場合は、データベース

のバックアップを復元できます。問題を解決した後、データベースを再度アップグレードできます。

5. チェックリストのタスクが完了したら、**Finish upgrade** をクリックします。

ステップ10：残りのDelivery Controllerをアップグレードする

新しくアップグレードされたStudioから、ナビゲーションペインで**Citrix Studio** *サイト名*を選択します。**共通タスク**タブで、**残りのDelivery Controllerをアップグレード**を選択します。

> **注：**
>
> **残りのDelivery Controllerをアップグレード**を利用可能にするには、サイト用に少なくとも1つのマシンカタログと1つのデリバリーグループを作成します。

> アップグレードを完了し、完了を確認した後、Studioを閉じてから再度開きます。Studioは、Controllerのサービスをサイトに登録するため、またはゾーンIDが存在しない場合にゾーンIDを作成するために、追加のサイトアップグレードを促すことがあります。

ステップ11：VDAのアップグレード

> **重要:**
>
> VDAをバージョン1912以降にアップグレードする場合は、「VDAを1912以降にアップグレードする」を参照してください。

> VDAを含むマシンで製品インストーラーを実行します。

Machine Creation Services™とマスターイメージを使用してマシンを作成した場合は、ホストに移動し、マスターイメージ上のVDAをアップグレードします。利用可能なVDAインストーラーのいずれかを使用できます。

- グラフィックインターフェイスのガイダンスについては、「VDAのインストール」を参照してください。
- コマンドラインのガイダンスについては、「コマンドラインを使用したインストール」を参照してください。

Citrix Provisioningを使用してマシンを作成した場合は、アップグレードに関するガイダンスについて「Citrix Provisioning製品ドキュメント」を参照してください。

ステップ12：マシンカタログとデリバリーグループの更新

- 「アップグレードされたVDAを持つマシンを使用するカタログを更新する」。
- 「アップグレードされたVDAを持つマシンを使用するカタログをアップグレードする」。
- 「アップグレードされたVDAを持つマシンを使用するデリバリーグループをアップグレードする」。

ステップ13：アップグレード後

展開内の他のコンポーネントをアップグレードします。ガイダンスについては、以下の製品ドキュメントを参照してください。

- StoreFront
- AppDNA
- シトリックス・アップ・レイヤリング
- HDX リアルタイム最適化パック
- プロファイル管理
- シトリックス・プロビジョニング
- セッションレコーディング
- ワークスペース環境管理

Microsoft SQL Server Express LocalDBソフトウェアを新しいバージョンに置き換える必要がある場合は、「SQL Server Express LocalDBの置き換え」を参照してください。

Dbschemaのアップグレード

展開を更新すると、いくつかのデータベーススキーマをアップグレードできます。次の表に、そのプロセスでアップグレードされるデータベーススキーマを示します。

From\To	1912 CU1	1912 CU2	1912 CU3	1912 CU4	1912 CU5	2203
7.15 RTM or 7.15 CU releases	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config; Logging
1912 RTM	Config	Site, Config	Site, Config	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config; Logging
1912 CU1		Site	Site, Config	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config; Logging
1912 CU2			Site, Config	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config; Logging
1912 CU3				Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config; Logging
1912 CU4					Site, Config	Site; Monitor; Config; Logging
1912 CU5						Site; Monitor; Config; Logging
2112						Site; Monitor; Config

用語の定義:

- サイト: サイトデータストア。Dbschemaの更新はサイトデータストアに対して行われます。

- モニター: モニターデータストア。Dbschemaの更新はモニターデータストアに対して行われます。
- 構成: 構成テーブル。構成テーブルで、Desktop Studioのバージョン、ライセンス情報、またはその両方が更新されます。
- ログ: ログデータストア。ログデータストアに対してDbschemaの更新が行われます。

VDAを2203以降にアップグレードする

Personal vDisk (PvD)コンポーネントがVDAにインストールされたことがある場合、そのVDAはバージョン2203以降にアップグレードできません。新しいVDAを使用するには、現在のVDAをアンインストールしてから、新しいVDAをインストールする必要があります。

この指示は、PvDを一度も使用したことがない場合でも適用されます。

以前のバージョンでPvDコンポーネントがインストールされた可能性がある方法は次のとおりです。

- VDAインストーラーのグラフィカルインターフェイスでは、PvDは**追加コンポーネント**ページでオプションとして提供されていました。
- コマンドラインでは、`/baseimage`オプションによってPvDがインストールされました。このオプションを指定した場合、またはこのオプションを含むスクリプトを使用した場合は、PvDがインストールされました。

VDAにPvDがインストールされているかどうかわからない場合は、マシンまたはイメージで新しいVDA（2203以降）のインストーラーを実行してください。

- PvDがインストールされている場合、互換性のないコンポーネントがあることを示すメッセージが表示されます。
  - グラフィカルインターフェイスから、メッセージが表示されているページで**キャンセル**をクリックし、インストーラーを閉じたいことを確認します。
  - CLIからは、コマンドは表示されたメッセージとともに単に失敗します。
- PvDがインストールされていない場合、アップグレードが続行されます。

対処法

VDAにPvDがインストールされていない場合は、通常のアップグレード手順に従ってください。

VDA に PvD がインストールされている場合:

1. 現在の VDA をアンインストールします。

2. 新しい VDA をインストールします。

Windows 10 (1607 以前、更新プログラムなし) マシンで PvD の使用を継続する場合は、VDA 7.15 LTSR がサポートされる最新バージョンです。

> **注：**

> *XenApp および XenDesktop 7.15 LTSR で Windows 7 デスクトップと Personal vDisk を使用できますか？*

> Citrix は、January 2016 に発表された XenApp および XenDesktop 7.6 LTSR から Personal vDisk (PvD) を除外しました。さらに、Citrix は PvD テクノロジーの非推奨を発表し、今後は Citrix App Layering の使用を開始することを推奨しています。Citrix App Layering (バージョン 4.4 以降) は、XenApp および XenDesktop 7.15 LTSR の互換性のあるコンポーネントです。しかし、Windows 7 上で既存の PvD 展開を使用しているお客様が Citrix App Layering テクノロジーに移行できるよう、Citrix は XenApp および XenDesktop 7.15 LTSR 累積更新プログラム (CU) を通じて、Windows 7 デスクトップ向け PvD 展開の期間限定サポートを Jan 14, 2020 まで提供することを決定しました。PvD コンポーネントは LTSR CU から削除され、Jan 14, 2020 以降はサポートされません。さらに、Jan 14, 2020 以降に Windows 7 で PvD を使用すると、LTSR サイトは非準拠になります。また、Windows 10 用 PvD は引き続き 7.15 LTSR から除外されます。したがって、お客様は 7.15 LTSR サイトでこれを使用しないでください。

PvD、AppDisks、およびサポートされていないホストを削除する

Citrix Virtual Apps and Desktops 7 Current Release 展開では、以下のテクノロジーとホストタイプはサポートされていません。

- カタログ内のユーザー VM の隣にデータを保存するための **Personal vDisk (PvD)**。ユーザーパーソナライゼーションレイヤー機能がユーザーの永続性を処理するようになりました。
- デリバリーグループで使用されるアプリケーションを管理するための **AppDisks**。
- **ホストタイプ:** Azure Classic、CloudPlatform (元の Citrix 製品)。
    - このリリースでサポートされているホストタイプについては、「システム要件」を参照してください。
    - ARM および AWS を引き続き使用できる代替方法については、「CTX270373」を参照してください。

現在の展開で PvD または AppDisks を使用している場合、あるいはサポートされていないホストタイプ (Microsoft Azure Classic など) への接続がある場合は、それらのテクノロジーを使用する項目を削除した後にのみ、バージョン 2006 (またはそれ以降のサポートされているバージョン) にアップグレードできます。現在の展開でパブリッククラウドホスト接続 (AWS など) を使用している場合は、アップグレードする前にハイブリッド権限ライセンスがあることを確認してください。インストーラーがサポートされていないテクノロジーまたはハイブリッド権限ライセンスのないホスト接続を 1 つ以上検出すると、アップグレードは一時停止または停止し、説明メッセージが表示されます。インストーラーログに詳細が含まれています。

アップグレードを確実に成功させるために、サポートされていない項目を削除するための該当するガイダンスを確認し、それに従ってください。

- PvD を削除する
- AppDisk を削除する
- サポートされていないホスト項目を削除する

展開でPvDまたはAppDiskを使用していなかったとしても、関連するMSIが以前のVDAのインストールまたはアップグレードに含まれていた可能性があります。VDAをバージョン2006（またはそれ以降のサポートされているバージョン）にアップグレードする前に、そのソフトウェアを使用したことがなくても、削除する必要があります。グラフィカルインターフェイスを使用する場合、その削除は自動的に行われるか、CLIを使用する際に削除オプションを含めることができます。詳細については、「PvDまたはAppDiskコンポーネントを持つVDAのアップグレード」を参照してください。

PvD を削除する

PvDを使用するように構成されているすべてのマシンを削除するまで、展開のアップグレードは成功しません。これはカタログとデリバリーグループに影響します。

グループおよびカタログからPvDを削除するには：

1. Studioで、デリバリーグループにPvDを使用するカタログのマシンが含まれている場合、それらのマシンをグループから削除します。
2. Studioで、PvDを使用するマシンを含むすべてのカタログを削除します。

VDAのアップグレード： 展開のアップグレードでは、VDAにAppDiskまたはPvDコンポーネントがインストールされているかどうかは検出されません。ただし、VDAインストーラーは検出します。詳細については、「PvDまたはAppDiskコンポーネントを持つVDA」を参照してください。

AppDisk を削除する

AppDiskを使用するすべてのデリバリーグループからAppDiskを削除し、その後AppDisk自体を削除するまで、展開のアップグレードは続行できません。

1. Studioのナビゲーションペインで**デリバリーグループ**を選択します。
2. グループを選択し、アクションペインで**AppDiskの管理**をクリックします。
3. グループからAppDiskを削除するアクションをクリックします。
4. AppDiskを使用する各デリバリーグループに対して、手順2と3を繰り返します。
5. Studioのナビゲーションペインで**AppDisks**を選択します。
6. AppDiskを選択し、AppDiskを削除するアクションをクリックします。
7. 各AppDiskに対して、手順5と6を繰り返します。

VDAのアップグレード: 展開のアップグレードでは、VDAにAppDiskまたはPvDコンポーネントがインストールされているかどうかは検出されません。ただし、VDAインストーラーは検出します。詳細については、「PvDまたはAppDiskコンポーネントがインストールされているVDA」を参照してください。

サポートされていないホストアイテムを削除する

サイトがCitrix CloudPlatformやMicrosoft Azure Classicなどのサポートされていないホストタイプへの接続を持っている場合、バージョン2006（またはそれ以降のサポートされているバージョン）への展開のアップグレードは続行できません。アップグレードを試みる前に、次のタスクを完了してください。

Studioから:

- サポートされていないホストへのすべての接続を削除します。
- デリバリーグループに、サポートされていないホストのマスターイメージで作成されたカタログのマシンが含まれている場合は、それらのマシンをグループから削除します。
- サポートされていないホストのマスターイメージを使用して作成されたすべてのカタログを削除します。

PvDまたはAppDiskコンポーネントがインストールされているVDA

PvDおよびAppDiskテクノロジーを有効にするコンポーネントがVDAにインストールされている場合、それらのコンポーネントが削除されるまで、そのVDAはアップグレードできません。

> **注：**

> バージョン1912にアップグレードする場合、現在のVDAをアンインストールしてから新しいVDAをインストールする必要がありました。このバージョンでは、Citrixがコンポーネントを削除してアップグレードを続行するかどうかを尋ねられます。

> AppDiskおよびPvDコンポーネントは、それらのテクノロジーを一度も使用していなくても、以前のVDAバージョンでインストールされている可能性があります。

- グラフィカルインターフェイス: VDAインストーラーの**追加コンポーネント**ページには、**Citrix AppDisk / Personal vDisk**オプションが含まれていました。7.15 LTSRおよびそれ以前の7.xリリースでは、このオプションがデフォルトで有効になっていました。したがって、デフォルトを受け入れた場合（または、このオプションが提供されたリリースで明示的に有効にした場合）、そのコンポーネントがインストールされました。
- CLI: `/baseimage`オプションを指定すると、コンポーネントがインストールされました。

対処法

VDAインストーラーが現在インストールされているVDAでAppDisksまたはPvDコンポーネントを検出しない場合、アップグレードは通常どおり続行されます。

インストーラーが現在インストールされているVDAでAppDisksまたはPvDコンポーネントを検出した場合:

- グラフィカルインターフェイス: アップグレードが一時停止します。サポートされていないコンポーネントを自動的に削除するかどうかを尋ねるメッセージが表示されます。**OK**をクリックすると、コンポーネントは自動的に削除され、アップグレードが続行されます。
- CLI: コマンドの失敗を避けるため、コマンドに次のオプションを含めます:
  - `/remove_appdisk_ack`
  - `/remove_pvd_ack`

制限事項

アップグレードには次の制限が適用されます:

- **選択的なコンポーネントのインストール:** いずれかのコンポーネントを新しいバージョンにインストールまたはアップグレードしても、アップグレードが必要な他のコンポーネント（別のマシン上）をアップグレードしないことを選択した場合、Studioが通知します。たとえば、アップグレードにControllerとStudioの新しいバージョンが含まれているとします。Controller

はアップグレードしますが、Studioがインストールされているマシンでインストーラーを実行しません。Studioをアップグレードするまで、Studioはサイトの管理を続行できません。

VDAをアップグレードする必要はありませんが、利用可能なすべての機能を使用できるように、すべてのVDAをアップグレードすることをCitrixは推奨します。

- **早期リリースまたはテクノロジープレビューバージョン:** 早期リリース、テクノロジープレビュー、またはプレビューバージョンからアップグレードすることはできません。
- **以前のオペレーティングシステム上のコンポーネント:** MicrosoftまたはCitrixによってサポートされなくなったオペレーティングシステムに現在のVDAをインストールすることはできません。詳細については、「以前のオペレーティングシステム」を参照してください。
- **混在環境/サイト:** 以前のバージョンのサイトと現在のバージョンのサイトを継続して実行する必要がある場合は、「混在環境に関する考慮事項」を参照してください。
- **製品の選択:** 以前のバージョンからアップグレードする場合、インストール時に設定された製品（Citrix Virtual AppsまたはCitrix Virtual Apps and Desktops）を選択または指定することはありません。

混在環境に関する考慮事項

アップグレードする際は、エディションとバージョンのすべての新規機能と強化された機能にアクセスできるように、すべてのコンポーネントとVDAをアップグレードすることをお勧めします。

たとえば、以前のControllerバージョンを含む展開で現在のVDAを使用することはできますが、現在のリリースでの新機能は利用できない場合があります。最新ではないバージョンを使用すると、VDA登録の問題が発生することもあります。

環境によっては、すべてのVDAを最新バージョンにアップグレードできない場合があります。その場合、マシンカタログを作成するときに、マシンにインストールされているVDAバージョンを指定できます。（これは機能レベルと呼ばれます。）デフォルトでは、この設定は推奨される最小VDAバージョンを指定します。ほとんどの展開では、デフォルト値で十分です。カタログにデフォルトよりも古いVDAが含まれている場合にのみ、設定を以前のバージョンに変更することを検討してください。マシンカタログ内でVDAバージョンを混在させることはお勧めしません。

カタログがデフォルトの最小VDAバージョン設定で作成され、1つ以上のマシンがデフォルトバージョンよりも古いVDAを持っている場合、それらのマシンはControllerに登録できず、動作しません。

詳しくは、「VDAのバージョンと機能レベル」を参照してください。

異なるバージョンを持つ複数のサイト

環境に異なる製品バージョンのサイト（たとえば、XenDesktop 7.18サイトとCitrix Virtual Apps and Desktops 1909サイト）が含まれている場合、Citrixでは、StoreFrontを使用して異なる製品バージョンからのアプリケーションとデスクトップを集約することをお勧めします。詳しくは、StoreFrontのドキュメントを参照してください。

混在環境では、各リリースに対応するStudioおよびDirectorのバージョンを引き続き使用しますが、異なるバージョンは別々のマシンにインストールされていることを確認してください。

以前のオペレーティングシステム

サポートされているオペレーティングシステム（OS）バージョンを実行しているマシンに、コンポーネントの以前のバージョンをインストールしたとします。現在、より新しいコンポーネントバージョンを使用したいが、そのOSはコンポーネントの現在のバージョンではサポートされなくなっています。

たとえば、Windows Server 2008 R2マシンにサーバーVDAをインストールしたとします。現在、そのVDAを現在のリリースにアップグレードしたいが、アップグレード先の現在のリリースではWindows Server 2008 R2はサポートされていません。

許可されていないオペレーティングシステムにコンポーネントをインストールまたはアップグレードしようとすると、「このオペレーティングシステムにはインストールできません」などのエラーメッセージが表示されます。

これらの考慮事項は、Current ReleaseおよびLong Term Service Releaseバージョンのアップグレードに適用されます。（LTSRバージョンにCUを適用することには影響しません。）

サポートされているOSについては、以下のリンクを参照してください。

- Citrix Virtual Apps and Desktops（最新リリース）：
  - デリバリーコントローラー、スタジオ、ディレクター、VDA、ユニバーサルプリントサーバー
  - フェデレーション認証サービス
  - StoreFront、Self-Service Password Reset、およびSession Recordingについては、現在のリリースのシステム要件の記事を参照してください。
- LTSRについては、ご使用のLTSRバージョンおよびCUのコンポーネントリストを参照してください。（メインのCitrix Virtual Apps and Desktops製品ドキュメントページから、ご使用のLTSRバージョンを選択してください。）

無効なオペレーティングシステム

次の表は、現在のリリースでコンポーネントのインストール/アップグレードに無効な以前のオペレーティングシステムを示しています。各OSでサポートされる最新の有効なコンポーネントバージョンと、インストールおよびアップグレードが無効になったコンポーネントバージョンを示します。

表内のオペレーティングシステムには、サービスパックと更新プログラムが含まれます。

オペレーティングシステム | コンポーネント/機能 | 最新の有効なバージョン | インストール/アップグレードが不可能になったバージョン

Windows 7および Windows 8	VDA	7.15 LTSR	7.16
Windows 7および Windows 8	その他のインストーラーコンポーネント	7.17	7.18
Windows 10 バージョン 1607 以前	VDA	7.15 LTSR	7.16
Windows 10 x86 バージョン	VDA	1906.2.0	1909
Windows サーバー 2008 R2	VDA	7.15 LTSR	7.16
Windows サーバー 2008 R2	その他のインストーラーコンポーネント	7.17	7.18
Windows サーバー 2012	VDA	7.15 LTSR	7.16
Windows サーバー 2012	その他のインストーラーコンポーネント	7.17	7.18
ウィンドウズ サーバー 2012 R2	その他のインストーラーコンポーネント *	1912 LTSR	2003
ウィンドウズ サーバー 2012 R2	サーバーVDI	7.15 LTSR	7.16

Windows XPおよびWindows Vistaは、7.xのコンポーネントまたはテクノロジーでは無効です。

* Delivery Controller、Studio、Director、およびVDAに適用されます。

実行できること

選択肢があります。次のことができます。

- 現在のOSを継続する
- マシンの再イメージ化またはアップグレード
- 新しいマシンを追加してから古いマシンを削除する(#add-new-machines-and-then-remove-old-machines)

現在のOSを継続して使用する

これらの方法はVDAで実行可能です。以前のOSを搭載したマシンを引き続き使用する場合は、次のいずれかを選択できます。

- インストールされているコンポーネントバージョンを継続して使用する。
- 最新の有効なコンポーネントバージョンをダウンロードし、そのバージョンにコンポーネントをアップグレードします。（これは、最新の有効なコンポーネントバージョンがまだインストールされていないことを前提としています。）

たとえば、Windows 7 SP1マシンに7.14 VDAがインストールされているとします。Windows 7 OSマシンで有効な最新のVDAバージョンは、XenApp and XenDesktop 7.15 LTSRです。7.14を継続して使用するか、7.15 LTSR VDAをダウンロードしてVDAをそのバージョンにアップグレードすることができます。これらの以前のVDAバージョンは、新しいバージョンのDelivery Controllerを含む展開で動作します。たとえば、7.15 LTSR VDAはCitrix Virtual Apps and Desktops 7 1808 Controllerに接続できます。

マシンの再イメージ化またはアップグレード

これらの方法は、VDAや、コアコンポーネント（Delivery Controllerなど）がインストールされていないその他のマシンで実行可能です。次のいずれかを選択してください。

- マシンをサービスから外し（メンテナンスモードをオンにしてすべてのセッションを閉じ）、サポートされているWindows OSバージョンに再イメージ化してから、コンポーネントの最新バージョンをインストールできます。
- 再イメージ化せずにVDAマシンでOSをアップグレードするには、まずアップグレード先のOSでサポートされているVDAバージョンをインストールするか、OSのアップグレード後にVDAをアップグレードする必要があります。そうしないと、Citrixソフトウェアはサポートされませ

ん。VDAをアンインストールせずにインプレースアップグレードを実行する場合、以下の最小OSバージョンにアップグレードできます。

- 2023年7月 Windows 11 用累積更新プログラム (KB5028185) 以降がインストールされている Windows 11 (ビルド 22621.1992 以降)。
- 2023年7月 Windows 10 用動的更新プログラム (KB5028311) がインストールされている Windows 10。

- アップグレードを計画しているWindowsのバージョンが上記のガイドラインに合致しない場合は、OSをアップグレードする前にVDAをアンインストールし、OSのアップグレードが完了した後にサポートされているVDAバージョンをインストールする必要があります。

新しいマシンを追加してから古いマシンを削除する

この方法は、Delivery Controller™またはその他のコアコンポーネントを含むマシンでOSをアップグレードする必要がある場合に実行可能です。

Citrix は、サイト内のすべての Controller が同じ OS を使用することを推奨しています。以下のアップグレードシーケンスは、異なる Controller が異なる OS を使用する期間を最小限に抑えます。

1. サイト内のすべての Delivery Controller のスナップショットを取得し、サイトデータベースをバックアップします。
2. サポートされているオペレーティングシステムを搭載したクリーンなサーバーに新しい Delivery Controller をインストールします。たとえば、2 台の Windows Server 2016 マシンに Controller をインストールします。
3. 新しい Controller をサイトに追加します。
4. 現在のリリースで無効なオペレーティングシステムで実行されている Controller を削除します。たとえば、2 台の Windows Server 2008 R2 マシン上の 2 台の Controller を削除します。Delivery Controllers で Controller を削除するための推奨事項に従ってください。

準備

アップグレードを開始する前に、以下の情報を確認し、必要なタスクを完了してください。

> **注：**

> VDA のアップグレードは アップグレードシーケンス の後半で行われますが、アップグレードを開始する前にインストーラーを選択し、手順を確認して、何が予想されるかを知っておくことをお勧めします。

インストーラーとインターフェイスを選択する

製品 ISO のフルプロダクトインストーラーを使用してコンポーネントをアップグレードします。VDA は、フルプロダクトインストーラーまたはスタンドアロン VDA インストーラーのいずれかを使用してアップグレードできます。すべてのインストーラーは、グラフィカルインターフェイスとコマンドラインインターフェイスを提供します。

詳細については、インストーラー を参照してください。

インストールの詳細: 準備作業を完了し、インストーラーを開始する準備ができたら、インストール記事には、表示される内容（グラフィカルインターフェイスを使用している場合）または入力する内容（コマンドラインインターフェイスを使用している場合）が示されています。

- グラフィカルインターフェイスを使用してコアコンポーネントをインストール/アップグレードする
- コマンドラインを使用してコアコンポーネントをインストール/アップグレードする
- グラフィカルインターフェイスを使用して VDA をインストール/アップグレードする
- コマンドラインを使用して VDA をインストール/アップグレードする

`VDAWorkstationCoreSetup.exe` インストーラーを使用してシングルセッションVDAを最初にインストールした場合、Citrixはそのインストーラーを使用してアップグレードすることを推奨します。フルプロダクトVDAインストーラーまたは `VDAWorkstationSetup.exe` インストーラーを使用してVDAをアップグレードすると、アップグレードから明示的に除外しない限り、元々除外されていたコンポーネントがインストールされる可能性があります。

VDAを現在のリリースにアップグレードする際、アップグレードプロセス中にマシンの再起動が発生します。（この要件は7.17リリースから始まりました。）これは回避できません。再起動後、アップグレードは自動的に再開されます（コマンドラインで `/noresume` を指定しない限り）。

データベース操作

サイト、監視、および構成ログデータベースをバックアップします。CTX135207 の指示に従ってください。アップグレード後に問題が発見された場合、バックアップを復元できます。

サポートされなくなったSQL Serverバージョンのアップグレードについては、SQL Server version check を参照してください。（これは、サイト、モニター、および構成ログデータベースに使用されるSQL Serverを指します。）

Microsoft SQL Server Express LocalDBは、ローカルホストキャッシュで使用するために自動的にインストールされます。以前のバージョンを置き換える必要がある場合、新しいバージョンはSQL Server Express LocalDB 2019である必要があります。コンポーネントとサイトをアップグレードした後にSQL Server Express LocalDBを新しいバージョンに置き換える方法の詳細については、Replace SQL Server Express LocalDB を参照してください。

Citrixライセンスが最新であることを確認する

Citrixライセンスの管理に関する包括的な情報については、Activate, upgrade, and manage Citrix licenses を参照してください。

フルプロダクトインストーラーを使用してライセンスサーバーをアップグレードできます。または、ライセンスコンポーネントを個別にダウンロードしてアップグレードすることもできます。Upgrade を参照してください。

アップグレードする前に、Customer Success Services / Software Maintenance / Subscription Advantage の日付が新しい製品バージョンに対して有効であることを確認してください。日付は2021.11.15以降である必要があります。

Citrixライセンスサーバーの互換性を確認する

Citrixライセンスサーバーが新しいバージョンと互換性があることを確認してください。これには2つの方法があります。

- 他のCitrixコンポーネントをアップグレードする前に、Delivery Controllerを含むマシンでISOレイアウトから`XenDesktopServerSetup.exe`インストーラーを実行します。互換性の問題がある場合、インストーラーは問題の解決策を推奨する手順とともに報告します。
- インストールメディアの`XenDesktop Setup`ディレクトリから、コマンド`.\LicServVerify.exe -h <license-server-fqdn> -p 27000 -v`を実行します。表示により、ライセンスサーバーが互換性があるかどうかが示されます。ライセンスサーバーに互換性がない場合は、ライセンスサーバーをアップグレードしてください。

StoreFrontの変更をバックアップする

アップグレードを開始する前に、`C:\inetpub\wwwroot\Citrix\<StoreName>\App_Data`内の *default.ica* や *usernamepassword.tfrm* などのファイルを変更している場合は、ストアごとにバックアップしてください。アップグレード後にそれらを復元して、変更を元に戻すことができます。

アプリケーションとコンソールを閉じる

アップグレードを開始する前に、管理コンソールやPowerShellセッションなど、ファイルロックを引き起こす可能性のあるすべてのプログラムを閉じます。

マシンを再起動すると、ファイルロックがすべて解除され、保留中のWindowsアップデートがないことが確認されます。

アップグレードを開始する前に、サードパーティの監視エージェントサービスをすべて停止し、無効にします。

適切な権限があることを確認する

ドメインユーザーであることに加えて、製品コンポーネントをアップグレードするマシンではローカル管理者である必要があります。

サイトデータベースとサイトは、自動または手動でアップグレードできます。データベースを自動アップグレードする場合、Studioユーザーの権限には、SQL Serverデータベーススキーマを更新する機能（たとえば、`db_securityadmin` または `db_owner` データベースロール）が含まれている必要があります。詳細については、「データベース」を参照してください。

Studioユーザーがこれらの権限を持っていない場合、手動データベースアップグレードを開始するとスクリプトが生成されます。StudioユーザーはStudioから一部のスクリプトを実行します。データベース管理者は、SQL Server Management Studioなどのツールを使用して他のスクリプトを実行します。

その他の準備タスク

- 必要に応じて、テンプレートをバックアップし、ハイパーバイザーをアップグレードする
- 事業継続計画で定められたその他の準備タスクを完了する。

サイトの事前テスト

Delivery Controllerとサイトをアップグレードする際、実際のアップグレードが開始される前にサイトの事前テストが実行されます。これらのテストでは、以下を確認します。

- サイトデータベースにアクセスでき、バックアップされていること
- 重要なCitrixサービスへの接続が正しく機能している
- Citrixライセンスサーバーのアドレスが利用可能である
- 構成ログデータベースに到達できる

- パブリッククラウドホスト接続（例：AWS）を追加する場合は、ハイブリッド権限ライセンスがあることを確認してください。そうしないと、事前サイトテストが一時停止または停止し、説明メッセージが表示されます。

テストの実行後、結果のレポートを表示できます。その後、検出された問題を修正し、テストを再度実行できます。事前サイトテストを実行せず、問題を解決しないと、サイトの動作に影響を与える可能性があります。

テスト結果を含むレポートは、インストールログと同じディレクトリにあるHTMLファイル（`PreliminarySiteTestResult.html`）です。そのファイルが存在しない場合は作成されます。ファイルが存在する場合は、その内容が上書きされます。

テストを実行する

- インストーラーのグラフィカルインターフェイスを使用してアップグレードする場合、ウィザードにはテストを開始してレポートを表示できるページが含まれています。テストが実行され、レポートを確認し、見つかった問題を解決した後、テストを再実行できます。テストが正常に完了したら、「次へ」をクリックしてウィザードを続行します。
- コマンドラインインターフェイスを使用してアップグレードする場合、テストは自動的に実行されます。デフォルトでは、テストが失敗した場合、アップグレードは実行されません。レポートを確認し、問題を解決した後、コマンドを再実行してください。

Citrixは、Controllerとサイトのアップグレードを続行する前に、常に事前サイトテストを実行し、問題を解決することを推奨します。テストを実行するわずかな時間で得られる潜在的なメリットは十分にあります。ただし、この推奨されるアクションを上書きすることもできます。

- グラフィカルインターフェイスでアップグレードする場合、テストをスキップしてアップグレードを続行することを選択できます。
- コマンドラインからアップグレードする場合、テストをスキップすることはできません。デフォルトでは、サイトテストが失敗すると、アップグレードを実行せずにインストーラーが失敗します。ほとんどの場合、`/ignore_site_test_failure` オプションを含めると、テストの失敗は無視され、アップグレードが続行されます。（例外については、SQL Serverのバージョンチェック を参照してください。）

複数のControllerをアップグレードする場合

1つのControllerでアップグレードを開始し、その後、同じサイト内の別のControllerでアップグレードを開始する場合（最初のアップグレードが完了する前）：

- 最初のControllerで事前サイトテストが完了している場合、他のControllerのウィザードには事前サイトテストページは表示されません。

- 最初のControllerでのテストが進行中に、別のControllerでアップグレードを開始すると、その別のControllerのウィザードにサイトテストページが表示されます。ただし、最初のControllerでのテストが完了すると、最初のControllerからのテスト結果のみが保持されます。

サイトの健全性に関連しないテストの失敗

- 予備サイトテストがメモリ不足で失敗した場合は、より多くのメモリを確保してからテストを再実行してください。
- アップグレードの権限はあるが、サイトテストを実行する権限がない場合、予備サイトテストは失敗します。これを解決するには、テストを実行する権限を持つユーザーアカウントでインストーラーを再実行してください。

SQL Serverバージョンの確認

Citrix Virtual Apps and Desktopsの展開を成功させるには、サイト、モニター、および構成ログデータベース用にサポートされているバージョンのMicrosoft SQL Serverが必要です。サポートされなくなったSQL ServerバージョンでCitrix展開をアップグレードすると、機能上の問題が発生し、サイトがサポート対象外になります。

アップグレード先のCitrixリリースでサポートされているSQL Serverのバージョンについては、そのリリースのシステム要件の記事を参照してください。

Controllerをアップグレードする際、Citrixインストーラーは、サイト、モニター、および構成ログデータベースに使用されている現在インストールされているSQL Serverのバージョンを確認します。

- チェックの結果、現在インストールされているSQL Serverのバージョンが、アップグレード先のCitrixリリースでサポートされているバージョンではないと判断された場合：
  - グラフィカルインターフェイス：アップグレードはメッセージとともに停止します。「**I understand**」をクリックし、次に「**Cancel**」をクリックしてCitrixインストーラーを閉じます。（アップグレードを続行することはできません。）
  - コマンドラインインターフェイス：コマンドは失敗します（コマンドに`/ignore_db_check_failure`オプションを含めた場合でも）。

  SQL Serverのバージョンをアップグレードしてから、Citrixのアップグレードを再度開始してください。
- チェックで現在インストールされているSQL Serverのバージョンを特定できない場合は、現在インストールされているバージョンがアップグレード先のバージョンでサポートされているか（システム要件）を確認してください。

- グラフィカルインターフェイス：アップグレードはメッセージとともに停止します。
  - 現在インストールされているSQL Serverのバージョンがサポートされている場合は、「**I understand**」をクリックしてメッセージを閉じ、次に「**Next**」をクリックしてCitrixのアップグレードを続行します。
  - 現在インストールされているSQL Serverのバージョンがサポートされていない場合は、**I understand**をクリックしてメッセージを閉じ、**Cancel**をクリックしてCitrixアップグレードを終了します。SQL Serverをサポートされているバージョンにアップグレードしてから、Citrixアップグレードを再度開始してください。
- コマンドラインインターフェイス：コマンドがメッセージとともに失敗します。メッセージを閉じた後：
  - 現在インストールされているSQL Serverのバージョンがサポートされている場合は、`/ignore_db_check_failure`オプションを指定してコマンドを再度実行します。
  - 現在インストールされているSQL Serverのバージョンがサポートされていない場合は、SQL Serverをサポートされているバージョンにアップグレードしてください。コマンドを再度実行して、Citrixアップグレードを開始します。

SQL Serverのアップグレード

新しいSQL Serverサーバーを立ち上げてサイトデータベースを移行する場合、接続文字列を更新する必要があります。

サイトが現在、サイトデータベースにSQL Server Express（Citrixがサイト作成時に自動的にインストールしたもの）を使用している場合：

1. 最新のSQL Server Expressバージョンをインストールします。
2. データベースをデタッチします。
3. データベースを新しいSQL Server Expressにアタッチします。
4. 接続文字列を移行します。

詳細については、接続文字列の構成およびMicrosoft SQL Serverの製品ドキュメントを参照してください。

SQL Server Express LocalDBの置き換え

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

CitrixはSQL Server Express LocalDBを自動的に更新しません。SQL Server Express LocalDBのバージョンを更新するには、このセクションのガイダンスに従ってください。

- Delivery ControllerをCitrix Virtual Apps and Desktopsバージョン2203 LTSR以降のバージョンにアップグレードする場合、サポートされるバージョンはSQL Server Express LocalDB 2019またはSQL Server Express LocalDB 2022です。

必要なもの:

- Citrix Virtual Apps and Desktopsのインストールメディア。
- Windows SysinternalsツールボックスのPsExecツール。

手順:

1. Citrix Virtual Apps and Desktopsのコンポーネント、データベース、およびサイトのアップグレードを完了します。（これらのデータベースアップグレードは、サイト、監視、および構成ログデータベースに影響します。SQL Server Express LocalDBを使用するローカルホストキャッシュデータベースには影響しません。）
2. SQL Server Express LocalDBを更新するDelivery Controllerにログオンします。
3. MicrosoftからPsExecをダウンロードし、そのDelivery Controller上のC:\Tempなどのアクセスしやすい場所に配置します。
4. Windowsシステムサービスから、Delivery Controller上のCitrix High Availability Serviceを停止します。
5. Delivery Controllerでコマンドプロンプトを開き、PsExecのある場所（例: `C:\Temp`）に移動してから、次のコマンドを実行してNetwork Serviceアカウントでコマンドプロンプトを昇格させます。

   ```
   psexec -i -u "NT AUTHORITY\NETWORKSERVICE" cmd
   ```

6. `whoami`を実行して、コマンドプロンプトがNetwork Serviceアカウントとして実行されていることを確認します。次の出力が表示されるはずです: `nt authority\networkservice`。
7. コマンドプロンプトを使用して、SQL LocalDBインスタンスに移動します。

   - SQL LocalDB 2014からアップグレードする場合:

     ```
     cd "C:\Program Files\Microsoft SQL Server\120\Tools\Binn"
     ```

   - SQL LocalDB 2017からアップグレードする場合:

```
cd "C:\Program Files\Microsoft SQL Server\140\Tools\Binn"
```

- SQL LocalDB 2019からアップグレードする場合:

```
cd "C:\Program Files\Microsoft SQL Server\150\Tools\Binn"
```

8. SQL LocalDBインスタンスを停止して削除します: `CitrixHA`。

```
SqlLocalDB stop CitrixHA



SqlLocalDB delete CitrixHA
```

9. Delivery Controllerから以下のファイルを削除します:

```
C:\Windows\ServiceProfiles\NetworkService\HADatabaseName.*

C:\Windows\ServiceProfiles\NetworkService\HADatabaseName_log.*

C:\Windows\ServiceProfiles\NetworkService\HAImportDatabaseName.* (if
exists)

C:\Windows\ServiceProfiles\NetworkService\HAImportDatabaseName_log.*
(if exists)
```

10. プログラムを削除するためのネイティブWindows機能を使用して、Delivery Controllerから既存のSQL LocalDB SQL Server Expressをアンインストールします。
11. アンインストールが完了したら、Delivery Controllerを再起動します。
12. Windowsシステムサービスから、Delivery Controller上のCitrix High Availability Serviceを停止します。
13. Citrix Virtual Apps and Desktopsのインストールメディアを Delivery Controllerにマウントします。
14. Delivery Controllerに管理者としてSQL Server Express LocalDB 2022をインストールします。

    a. Citrix Virtual Apps and Desktopsのインストールメディアの `Support > SQLLocalDB` フォルダーにある `sqllocaldb.msi` ファイルを使用します。たとえば、インストールメディアが `E drive` ドライブにマウントされている場合、ファイルは `E:`

`\Support\SQLLocalDB\sqllocaldb.msi`にあります。インストールを完了するには再起動が必要です。

b. 新しいSQL LocalDBは`C:\Program Files\Microsoft SQL Server\160\Tools\Binn`にある必要があります。

15. Windowsシステムサービスから、Delivery Controller上のCitrix High Availability Serviceを開始します。
16. Delivery Controllerのコマンドプロンプトで、`C:\Program Files\Microsoft SQL Server\160\Tools\Binn`に移動し、`SqlLocalDB i`を実行してCitrixHAインスタンスが作成されたことを確認します。返されたインスタンスのリストに`CitrixHA`が含まれている必要があります。

> **注：**
>
> Citrix High Availability Serviceの開始後、CitrixHAデータベースが作成されるまでに最大15分かかる場合があります。

17. 必要に応じてHigh Availability Service（セカンダリブローカー）が引き継ぐことができることを確認するために、ローカルホストキャッシュデータベースファイルが作成されていることを確認します。
    a. Delivery Controllerで、`C:\Windows\ServiceProfiles\NetworkService`を参照します。
    b. `HaDatabaseName.mdf`と`HaDatabaseName_log.ldf`が作成されていることを確認します。
18. 残りのDelivery Controllerで手順を繰り返します。

VDAアップグレードエージェントのプロキシサポート

VDAアップグレードエージェントのプロキシサポートは、2311 VDAで追加されました。

2311 VDA (バージョン: 7.40) のVDAアップグレードエージェントは、プロキシを介してトラフィックを認識し、送信できます。

VDAアップグレードエージェント (VUA) は、Hostname:Port (IP:Port) およびPACファイルの形式でプロキシをサポートしています。

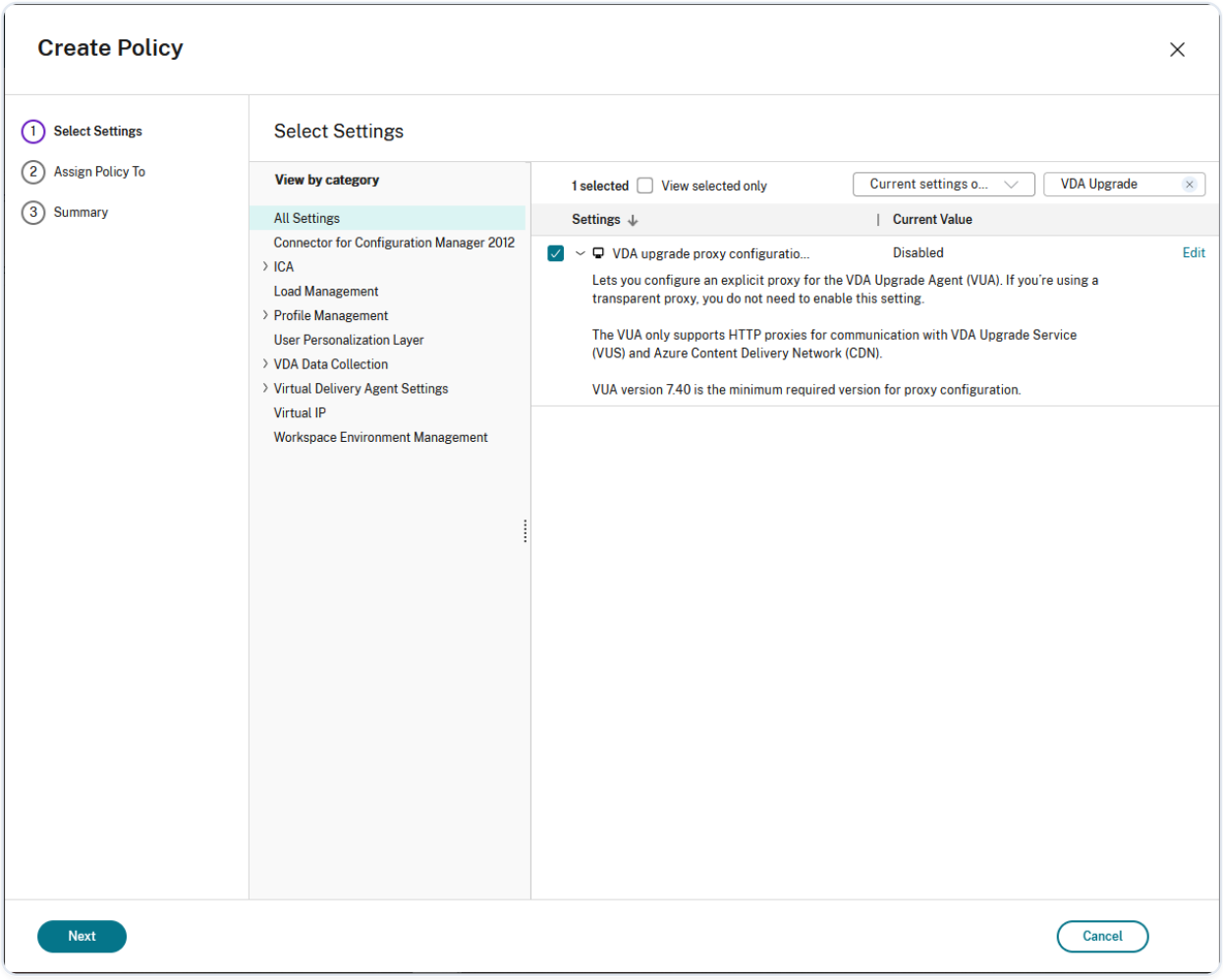
HTTPプロキシのみがサポートされています。 パケットの復号化と検査はサポートされていません。

プロキシ認証はサポートされていません。 SOCKS5はサポートされていません。

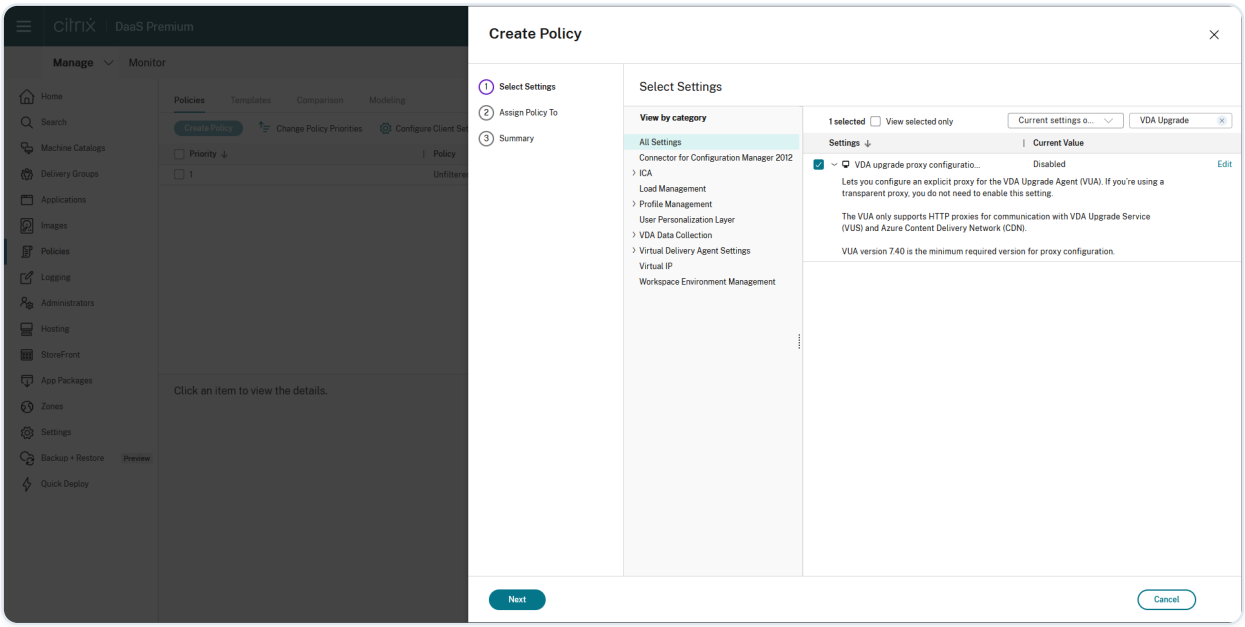
VDAアップグレードエージェントプロキシの構成

VDAアップグレードエージェントプロキシは2つの方法で設定できます

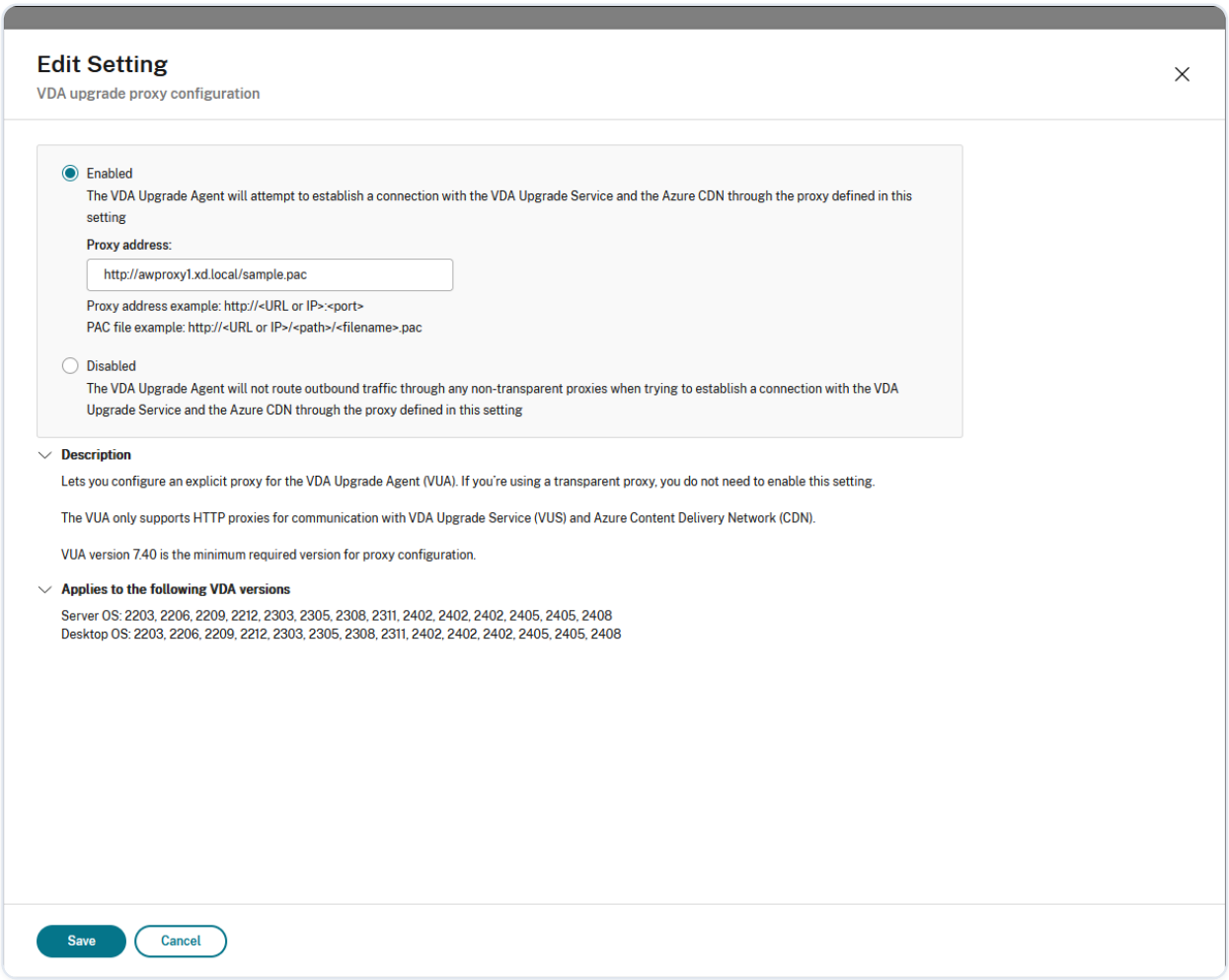
1. **Webstudioポリシー**を使用した**VDAアップグレードエージェントポリシーの構成**。



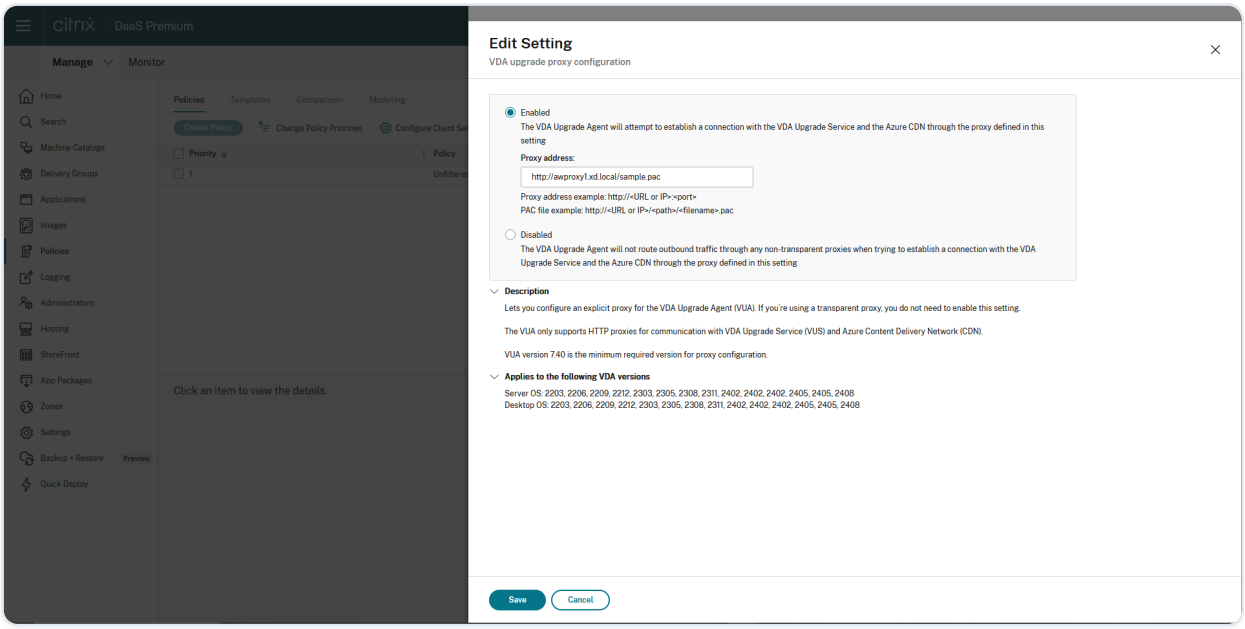
2. **ポリシーの作成**ページで、**設定**から**VDAアップグレードプロキシ構成**を選択します。



3. この設定を有効にします。デフォルトでは、この設定は無効になっています。



4. レジストリキーを使用したVDAアップグレードエージェントの構成。



レジストリキーは、VDAインストール中にMeta-Installerに設定されます。

レジストリ:

キー: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\VirtualDesktopAgent`

値の型: 文字列

値の名前: ProxySettings

値のデータ: プロキシアドレスまたはPACファイルへのパス。

例:

a. プロキシアドレス: `http://<URL or IP>:<port>`
b. PACファイル: `http://<URL or IP>/<path/<filename>.pac`

構成のバックアップまたは移行

この機能は、DaaS構成のバックアップを作成するのに役立ちます。バックアップにより、構成をあるクラウドサイトから別のクラウドサイトへ移行するプロセスが容易になります。また、緊急時にサイトを即座に復旧させることも可能です。 バックアップを作成するには、次の方法を使用できます。

1. バックアップ + 復元
    a. WebStudioと統合されています。
2. 自動構成ツール (ACT)

a. PowerShellベースのツールです。使用するにはツールをインストールしてください。

バックアップは以下の目的で使用できます。

1. 復元
2. 移行

Citrix®は、説明されているシナリオに対して以下のツールを推奨します。

バックアップ

環境	ユースケース	推奨ツール	特別な考慮事項	リンク
DaaS	オンデマンドおよびスケジュールされたバックアップ	バックアップ + 復元	Citrix がバックアップを保持し、必要に応じてユーザーがダウンロードできます	Studio でのバックアップ + 復元
オンプレミス	オンデマンドバックアップ	ACT	ユーザーがバックアップを保持します	Automated Configuration Tool を使用したバックアップと復元

移行

環境	ユースケース	推奨ツール	特別な考慮事項	リンク
オンプレミスからクラウドへ	1つのオンプレミスサイトをDaaSに移行する	ACT		オンプレミスからクラウドへの移行
	複数のオンプレミスサイトを1つのDaaSサイトに統合する	ACT	サイトのマージ	複数のオンプレミスサイトを単一のクラウドサイトにマージする

環境	ユースケース	推奨ツール	特別な考慮事項	リンク
オンプレミスからオンプレミスへ	1つのオンプレミスサイトを別のオンプレミスサイトに移行する	ACT		POCガイド:自動構成ツール - オンプレミスからオンプレミスへの移行
	複数のオンプレミスサイトを別のオンプレミスサイトに統合する	ACT	サイトのマージ	POCガイド:自動構成ツール オンプレミスからオンプレミスへの移行
				複数のオンプレミスサイトを単一のクラウドサイトにマージする
クラウドからクラウドへ	1つのDaaSサイトを別のDaaSサイトに移行する	ACT		クラウドからクラウドへの移行 (/ja-jp/citrix-daas/migrate/migrate-cloud-to-cloud.html#prerequisites-for-migrating-your-configuration)
複数のDaaSサイトを1つのDaaSサイトに統合する	ACT	サイトのマージ		クラウドからクラウドへの移行 (/ja-jp/citrix-daas/migrate/migrate-cloud-to-cloud.html#prerequisites-for-migrating-your-configuration)

環境	ユースケース	推奨ツール	特別な考慮事項	リンク
				複数のオンプレミスサイトを単一のクラウドサイトに移行する (/ja-jp/citrix-daas/migrate/multi-site-merge.html)

セキュリティ

Citrix Virtual Apps and Desktops™ は、セキュリティニーズに合わせて環境を調整できる、設計段階から安全なソリューションを提供します。

モバイルワーカーに関してITが直面するセキュリティ上の懸念の1つは、データの紛失または盗難です。アプリケーションとデスクトップをホストすることで、Citrix Virtual Apps and Desktops は、すべてのデータをデータセンターに保持することにより、機密データと知的財産をエンドポイントデバイスから安全に分離します。データ転送を許可するポリシーが有効になっている場合、すべてのデータは暗号化されます。

Citrix Virtual Apps and Desktops のデータセンターは、一元化された監視および管理サービスにより、インシデント対応も容易にします。Director を使用すると、IT部門はネットワーク全体でアクセスされているデータを監視および分析でき、Studio を使用すると、IT部門は各エンドユーザーデバイスでローカルに問題を修正する代わりに、データセンター内のほとんどの脆弱性をパッチ適用して修復できます。

Citrix Virtual Apps and Desktops は、監査と規制コンプライアンスも簡素化します。調査官は、一元化された監査証跡を使用して、誰がどのアプリケーションとデータにアクセスしたかを判断できるためです。Director は、構成ログと OData API にアクセスすることで、システムへの更新とユーザーデータ使用量に関する履歴データを収集します。

委任管理により、Citrix Virtual Apps and Desktops へのアクセスをきめ細かく制御するための管理者ロールを設定できます。これにより、組織内で特定の管理者にタスク、操作、スコープへのフルアクセスを許可し、他の管理者には制限されたアクセスを許可する柔軟性が得られます。

シトリックス バーチャルアプリ＆デスクトップは、ローカルレベルから組織単位レベルまで、ネットワークのさまざまなレベルでポリシーを適用することにより、管理者にユーザーに対するきめ細かな制御を提供します。このポリシーの制御により、ユーザー、デバイス、またはユーザーとデバイスのグループが接続、印刷、コピー/貼り付け、またはローカルドライブのマッピングができるかどうかが決定され、サードパーティの臨時作業者に関するセキュリティ上の懸念を最小限に抑えることができます。管理者は、デスクトップロック機能も使用でき、エンドユーザーが仮想デスクトップのみを使用できるようにし、エンドユーザーデバイスのローカルオペレーティングシステムへのアクセスを防止します。

管理者は、サイトを構成して、Controller の、またはエンドユーザーと Virtual Delivery Agents (VDA) 間の Transport Layer Security (TLS) プロトコルを使用するようにすることで、Citrix Virtual Apps または Citrix Virtual Desktops のセキュリティを強化できます。このプロトコルは、TCP/IP 接続のサーバー認証、データストリーム暗号化、およびメッセージ整合性チェックを提供するために、サイトで有効にすることもできます。

Citrix Virtual Apps and Desktops は、Windows または特定のアプリケーションの多要素認証もサポートしています。多要素認証は、Citrix Virtual Apps and Desktops によって提供されるすべてのリソースを管理するためにも使用できます。これらの方法には以下が含まれます。

- トークン
- スマートカード
- RADIUS
- ケルベロス
- 生体認証

Citrix Virtual Desktops は、ID管理からウイルス対策ソフトウェアまで、多くのサードパーティ製セキュリティソリューションと統合できます。サポートされている製品のリストは `<http://www.citrix.com/ready>` で確認できます。

Citrix Virtual Apps and Desktops の一部のリリースは、Common Criteria 標準の認定を受けています。これらの標準のリストについては、`<https://www.commoncriteriaportal.org/cc/>` にアクセスしてください。

フェデレーション認証サービス

Citrix フェデレーション認証サービス (FAS) は、Windowsパスワードを提供しないSAMLやOpenID Connect (OIDC) などの最新のIDプロバイダーを介してユーザーが認証する環境で、Citrix仮想デスクトップおよびアプリケーションへのシングルサインオン (SSO) を可能にし、Active Directoryドメインに参加しているセッションホストへのシームレスなアクセスを保証します。

フェデレーション認証サービスを使用して展開を保護する方法の詳細については、別のドキュメントにあるフェデレーション認証サービス ドキュメントを参照してください。

FIDO2およびWebAuthn認証

FIDO2およびWebAuthnを使用したローカル認証と仮想認証

ユーザーは、FIDO2セキュリティキーと、TPM 2.0およびWindows Helloを搭載した統合生体認証デバイスを使用して、仮想セッションでFIDO2またはWebAuthnを活用するアプリケーションに認証できます。

FIDO2の詳細については、「FIDO2: WebAuthn & CTAP」を参照してください。

この機能の使用方法については、「FIDO2リダイレクト」を参照してください。

> **注**
>
> この機能は、WebAuthnまたはFIDO2を使用した仮想セッションへのログオンをサポートしていません。この機能は、仮想セッション内のアプリケーションでこれらの認証方法を使用することのみを許可します。

> この機能は、ダブルホップシナリオではサポートされていません。

サポートマトリックス

セッションホストオペレーティングシステム	WEBアプリケーション認証	UWPアプリケーション認証
Windows サーバー 2016	USBリダイレクト経由でサポート	サポートされていません
Windows サーバー 2019	サポート対象	サポートされていません
ウィンドウズ サーバー 2022	サポート対象	サポート対象
ウィンドウズ 10	サポート対象	サポート対象
ウィンドウズ 11	サポート対象	サポート対象

詳細については、以下の要件を確認してください。

Webアプリケーション認証

要件

WebアプリケーションでFIDO2およびWebAuthn認証を使用するための要件は次のとおりです。

Citrix® コントロールプレーン

- Citrix Virtual Apps and Desktops™ 2009年以降のバージョン

セッションホスト

- オペレーティングシステム
  - Windows 10 1809 以降
  - Windows Server 2019 以降のバージョン
- VDA
  - Windows: バージョン2009以降

クライアントデバイス

- オペレーティングシステム
  - Windows 10 1809 以降
  - Linux: Workspace app for Linuxのシステム要件を参照してください
- Workspaceアプリ
  - Windows: バージョン2009.1以降
  - Linux: 2303以降

Webブラウザの要件

- 64ビットブラウザ
- 32ビットブラウザ (Citrix Virtual Apps and Desktops™ 2402 CU2以降)

> **注**
>
> 仮想アプリまたはデスクトップセッション内でChromiumベースのブラウザを使用している場合、ブラウザがChromiumバージョン147以降を実行していると、FIDO2キーの登録は機能しません。 VDAバージョン2503以降にアップグレードすると、この問題は解決されます。または、回避策として、FIDO2リダイレクトを無効にし、USBリダイレクトを利用して

> FIDO2キーをセッションにリダイレクトできます。詳細については、USBリダイレクトを参照してください。

サポートされる認証方法

- FIDO2セキュリティキー
- ウィンドウズ ハロー
  - TPM 2.0
  - 統合生体認証
    - 顔認識
    - 指紋スキャナー
  - WebAuthn

UWPアプリケーション認証

Citrix Virtual Apps and Desktops 2112のリリースにより、CitrixはUWPアプリケーションでのWebAuthnおよびFIDO2認証をサポートします。

Microsoft Teams、Microsoft Outlook for Office 365、OneDriveなどのアプリケーションは、Azure Active Directoryへのリンクとして認証にUWPアプリケーションを使用します。Citrixは現在、これらのアプリケーションの認証にFIDO2を使用することをサポートしています。

要件

UWPアプリケーションでFIDO2およびWebAuthn認証を使用するための要件は次のとおりです。

Citrixコントロールプレーン

- Citrix Virtual Apps and Desktops 2112 以降のバージョン

セッションホスト

- オペレーティングシステム
  - Windows 10 1809 以降
  - Windows Server 2022 またはそれ以降
- VDA
  - Windows: バージョン2112以降

クライアントデバイス

- オペレーティングシステム
  - Windows 10 1809 以降
  - Linux: Workspace app for Linuxのシステム要件を参照してください
- Workspaceアプリ
  - Windows: バージョン2009.1以降
  - Linux: 2303以降

サポートされる認証方法

- FIDO2 セキュリティキー
- ウィンドウズ ハロー
  - TPM 2.0
  - 統合生体認証
    - 顔認識
    - 指紋スキャナー
  - WebAuthn

> **注：**
>
> クライアント、VDA、またはオペレーティングシステムがこの機能をサポートしていないためFIDO2リダイレクトが利用できないシナリオでは、USBベースのFIDO2キーはUSBリダイレクトを使用してリダイレクトできます。 FIDO2リダイレクトが利用可能なシナリオでも、USBリダイレクトを使用してUSBベースのFIDO2キーをリダイレクトすることが可能です。この場合、FIDO2リダイレクトを無効にし、適切なUSBリダイレクトルールを構成する必要があります。 USBリダイレクトルールを使用してFIDO2キーを構成する方法の詳細については、USBリダイレクトデバイスルールのドキュメントを参照してください。

msedgewebview2.exeベースのアプリケーションの高度な構成

> **注：**

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

> msedgewebview2.exeベースのWebアプリケーションを使用している企業の場合、HDXセッション内でFIDO2リダイレクトが機能するように、VDAに追加のレジストリ値を追加する必要があります。

AllowedProcessesレジストリ値にmsedgewebview2.exeのフルパスを追加します。

- キー: HKLM\SOFTWARE\Citrix\WebAuthnAllowedProcesses
- 値の名前: AllowedProcesses
- 値の型: REG_MULTISZ
- 値のデータ: `<add full path of the msedgewebview2.exe here >`

64ビットアプリケーションの場合、以下の値を設定する必要があります。

- キー: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxHook\AppInit_DLLs\CtxWebAuthnHook\msedgewebview2
- キー: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxHook\AppInit_DLLs\CtxWebAuthnHook
- 値の名前: FilePathName
- 値の型: REG_SZ
- 値のデータ: C:\Program Files\Citrix\HDX\bin\CtxWebAuthnHook.dll
- キー: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxHook\AppInit_DLLs\CtxWebAuthnHook
- 値の名前: Flag
- 値の型: DWORD
- 値のデータ: 00000002

32ビットアプリケーションの場合、以下の値を設定する必要があります。

- キー: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\CtxHook\AppInit_DLLs\CtxWebAuthnHook\
- キー: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\CtxHook\AppInit_DLLs\CtxWebAuthnHook
- 値の名前: FilePathName

- 値の型: REG_SZ
- 値のデータ: C:\Program Files\Citrix\HDX\bin\CtxWebAuthnHook.dll
- キー: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\CtxHook\AppInit_DLLs\CtxWebAuthnHook
- 値の名前: Flag
- 値の型: DWORD
- 値のデータ: 00000002

msedgewebview2.exeベースのアプリケーションでFIDO2リダイレクトを有効にするためのレジストリ値を設定した後、VDAを再起動します。

シトリックス Virtual Apps and Desktops™ と シトリックス ゲートウェイ の統合

StoreFront™ サーバーは、公開されたリソースとデータへのアクセスを管理するために展開および構成されます。リモートアクセスの場合、StoreFront の前に Citrix Gateway を追加することをお勧めします。

> **注：**

> Citrix Virtual Apps and Desktops と Citrix Gateway を統合する方法の詳細な構成手順については、StoreFront のドキュメントを参照してください。

> 以下の図は、Citrix Gateway を含む簡素化された Citrix 展開の例を示しています。Citrix Gateway は StoreFront と通信し、Citrix Virtual Apps and Desktops によって配信されるアプリとデータを保護します。ユーザーデバイスは Citrix Workspace™ アプリを実行して、セキュアな接続を作成し、アプリ、デスクトップ、ファイルにアクセスします。

Citrix Gateway を含む簡素化された Citrix 展開(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/sample-deployment-overview.png)

ユーザーは Citrix Gateway を使用してログオンし、認証します。Citrix Gateway は DMZ に展開され、保護されています。2 要素認証が構成されています。ユーザー資格情報に基づいて、ユーザーには関連するリソースとアプリケーションが提供されます。アプリケーションとデータは適切なサーバー上にあります（図には示されていません）。セキュリティ上機密性の高いアプリケーションとデータには、個別のサーバーが使用されます。

セキュリティに関する考慮事項とベストプラクティス

> **注：**
>
> 組織は規制要件を満たすために特定のセキュリティ標準に準拠する必要がある場合があります。このようなセキュリティ標準は時間とともに変化するため、このドキュメントではこの主題を扱いません。セキュリティ標準とCitrix製品に関する最新情報については、`<http://www.citrix.com/security/>`を参照してください。

セキュリティのベストプラクティス

環境内のすべてのマシンをセキュリティパッチで最新の状態に保ちます。利点の1つは、シンクライアントをターミナルとして使用できるため、このタスクが簡素化されることです。

環境内のすべてのマシンをウイルス対策ソフトウェアで保護します。

プラットフォーム固有のマルウェア対策ソフトウェアの使用を検討してください。

ソフトウェアをインストールする際は、提供されているデフォルトのパスにインストールしてください。

- 提供されているデフォルトのパス以外のファイル場所にソフトウェアをインストールする場合は、制限付きアクセス許可などの追加のセキュリティ対策をそのファイル場所に追加することを検討してください。

すべてのネットワーク通信は、セキュリティポリシーに合わせて適切に保護および暗号化する必要があります。IPSecを使用してMicrosoft Windowsコンピューター間のすべての通信を保護できます。これを行う方法の詳細については、オペレーティングシステムのドキュメントを参照してください。さらに、ユーザーデバイスとデスクトップ間の通信は、デフォルトで128ビット暗号化に構成されているCitrix SecureICAを介して保護されます。SecureICAは、デリバリーグループの作成または更新時に構成できます。

> **注：**
>
> Citrix SecureICAはICA/HDXプロトコルの一部ですが、Transport Layer Security (TLS) のような標準準拠のネットワークセキュリティプロトコルではありません。TLSを使用して、ユーザーデバイスとデスクトップ間のネットワーク通信を保護することもできます。TLSを構成するには、Transport Layer Security (TLS)を参照してください。

アカウント管理にはWindowsのベストプラクティスを適用してください。Machine Creation ServicesまたはProvisioning Servicesによって複製される前に、テンプレートまたはイメージ上にアカウントを作成しないでください。保存された特権ドメインアカウントを使用してタスクをスケジュールしないでください。共有Active Directoryマシンアカウントを手動で作成しないでください。これらの慣行は、マシン攻撃がローカルの永続的なアカウントパスワードを取得し、それらを使用して他のユーザーに属するMCS/PVS共有イメージにログオンするのを防ぐのに役立ちます。

ファイアウォール

環境内のすべてのマシンを、必要に応じてエンクレーブ境界を含め、境界ファイアウォールで保護します。

環境内のすべてのマシンは、パーソナルファイアウォールによって保護されている必要があります。コアコンポーネントとVDAをインストールする際、Windowsファイアウォールサービスが検出された場合（ファイアウォールが有効になっていない場合でも）、コンポーネントと機能の通信に必要なポートを自動的に開くように選択できます。これらのファイアウォールポートを手動で構成することもできます。別のファイアウォールを使用する場合は、手動で構成する必要があります。

従来の環境をこのリリースに移行する場合、既存の境界ファイアウォールの再配置や新しい境界ファイアウォールの追加が必要になる場合があります。たとえば、データセンター内の従来のクライアントとデータベースサーバーの間に境界ファイアウォールがあるとします。このリリースを使用する場合、その境界ファイアウォールは、仮想デスクトップとユーザーデバイスが一方にあり、データセンター内のデータベースサーバーとDelivery Controllerがもう一方にあるように配置する必要があります。したがって、データベースサーバーとControllerを格納するために、データセンター内にエンクレーブを作成することを検討してください。また、ユーザーデバイスと仮想デスクトップの間に保護を設けることも検討してください。

注：

TCPポート1494と2598はICAとCGPに使用されるため、データセンター外のユーザーがアクセスできるようにファイアウォールで開かれている可能性が高いです。Citrixは、管理インターフェイスが意図せず攻撃にさらされる可能性を避けるため、これらのポートを他の目的で使用しないことを推奨します。ポート1494と2598は、Internet Assigned Number Authority (http://www.iana.org/) に正式に登録されています。

アプリケーションセキュリティ

非管理者ユーザーが悪意のある操作を実行するのを防ぐため、VDAホストおよびローカルのWindowsクライアントで、インストーラー、アプリケーション、実行可能ファイル、およびスクリプトに対してWindows AppLockerルールを構成することをお勧めします。

ユーザー権限の管理

ユーザーには必要な機能のみを付与します。Microsoft Windowsの特権は、通常の方法でデスクトップに適用され続けます。特権はユーザー権利の割り当てを通じて、グループメンバーシップはグループポリシーを通じて構成します。このリリースの利点の1つは、デスクトップが保存されているコンピューターに対する物理的な制御を付与することなく、ユーザーにデスクトップへの管理者権限を付与できることです。

デスクトップの特権を計画する際は、以下に注意してください。

- デフォルトでは、非特権ユーザーがデスクトップに接続すると、自身のユーザーデバイスのタイムゾーンではなく、デスクトップを実行しているシステムのタイムゾーンが表示されます。ユーザーがデスクトップを使用する際にローカルタイムを表示できるようにする方法については、「デリバリーグループの管理」の記事を参照してください。
- デスクトップの管理者であるユーザーは、そのデスクトップを完全に制御できます。デスクトップが専用デスクトップではなくプールされたデスクトップである場合、そのユーザーは、将来のユーザーを含む、そのデスクトップの他のすべてのユーザーに関して信頼できる必要があります。デスクトップのすべてのユーザーは、この状況によってデータセキュリティに潜在的に永続的なリスクがあることを認識する必要があります。この考慮事項は、単一ユーザーのみが使用する専用デスクトップには適用されません。そのユーザーは、他のどのデスクトップの管理者であってもなりません。
- デスクトップの管理者であるユーザーは、一般的に、悪意のあるソフトウェアを含むソフトウェアをそのデスクトップにインストールできます。また、そのユーザーは、デスクトップに接続されているネットワーク上のトラフィックを監視または制御できる可能性もあります。

ログオン権限の管理

ログオン権限は、ユーザーアカウントとコンピューターアカウントの両方に必要です。Microsoft Windowsの特権と同様に、ログオン権限は通常の方法でデスクトップに適用され続けます。ログオン権限はユーザー権利の割り当てを通じて、グループメンバーシップはグループポリシーを通じて構成します。

Windowsのログオン権限は、ローカルログオン、リモートデスクトップサービス経由のログオン、ネットワーク経由のログオン（ネットワークからこのコンピューターにアクセス）、バッチジョブとしてログオン、サービスとしてログオンです。

コンピューターアカウントの場合、コンピューターに必要なログオン権限のみを付与します。「ネットワークからこのコンピューターにアクセス」のログオン権限が必要です。

- VDAで、デリバリーコントローラーのコンピューターアカウントに対して
- デリバリーコントローラーで、VDAのコンピューターアカウントに対して。Active Directory OUベースのコントローラー検出を参照してください。
- StoreFront™サーバーで、同じStoreFrontサーバーグループ内の他のサーバーのコンピューターアカウントに対して

ユーザーアカウントの場合、ユーザーには必要なログオン権限のみを付与します。

Microsoftによると、デフォルトでは、Remote Desktop Usersグループには「リモートデスクトップサービス経由でのログオンを許可」のログオン権限が付与されています（ドメインコントローラーを除く）。

組織のセキュリティポリシーによっては、このグループをそのログオン権限から削除するよう明示的に規定している場合があります。次のアプローチを検討してください。

- マルチセッションOS用Virtual Delivery Agent (VDA) は、Microsoft Remote Desktop Servicesを使用します。Remote Desktop Usersグループを制限付きグループとして構成し、Active Directoryグループポリシーを介してグループのメンバーシップを制御できます。詳細については、Microsoftのドキュメントを参照してください。
- シングルセッションOS用VDAを含むCitrix Virtual Apps and Desktops™のその他のコンポーネントでは、Remote Desktop Usersグループは不要です。したがって、これらのコンポーネントの場合、Remote Desktop Usersグループには「リモートデスクトップサービスによるログオンを許可」のログオン権限は不要であり、削除できます。さらに：
  - リモートデスクトップサービスを介してそれらのコンピューターを管理する場合、そのようなすべての管理者がすでにAdministratorsグループのメンバーであることを確認してください。
  - それらのコンピューターをリモートデスクトップサービス経由で管理しない場合は、それらのコンピューターでリモートデスクトップサービス自体を無効にすることを検討してください。

ログイン権限「リモートデスクトップサービス経由でのログオンを拒否」にユーザーとグループを追加することは可能ですが、ログオン拒否権限の使用は一般的に推奨されません。詳細については、Microsoftのドキュメントを参照してください。

ユーザー権限の構成

Delivery Controller™のインストールにより、以下のWindowsサービスが作成されます。

- Citrix AD Identity Service (NT SERVICE\CitrixADIdentityService): VMのMicrosoft Active Directoryコンピューターアカウントを管理します。
- Citrix Analytics (NT SERVICE\CitrixAnalytics): サイト管理者が承認した場合、Citrixが使用するためのサイト構成の使用状況情報を収集します。その後、この情報をCitrixに送信し、製品の改善に役立てます。
- Citrix App Library (NT SERVICE\CitrixAppLibrary): AppDiskの管理とプロビジョニング、AppDNA統合、およびApp-Vの管理をサポートします。
- Citrix Broker Service (NT SERVICE\CitrixBrokerService): ユーザーが利用できる仮想デスクトップまたはアプリケーションを選択します。
- Citrix Configuration Logging Service (NT SERVICE\CitrixConfigurationLogging): 管理者がサイトに対して行ったすべての構成変更およびその他の状態変更を記録します。
- Citrix Configuration Service (NT SERVICE\CitrixConfigurationService): 共有構成のためのサイト全体のリポジトリ。
- Citrix Delegated Administration Service (NT SERVICE\CitrixDelegatedAdmin): 管理者に付与された権限を管理します。
- Citrix Environment Test Service (NT SERVICE\CitrixEnvTest): 他のDelivery Controllerサービスのセルフテストを管理します。
- Citrix Host Service (NT SERVICE\CitrixHostService): Citrix Virtual AppsまたはCitrix Virtual Desktops展開で使用されるハイパーバイザーインフラストラクチャに関する情報を保存し、コンソールがハイパーバイザープール内のリソースを列挙するために使用する機能も提供します。
- Citrix Machine Creation Services (NT SERVICE\CitrixMachineCreationService): デスクトップVMの作成をオーケストレーションします。
- Citrix Monitor Service (NT SERVICE\CitrixMonitor): Citrix Virtual AppsまたはCitrix Virtual Desktopsのメトリックを収集し、履歴情報を保存し、トラブルシューティングおよびレポートツール用のクエリインターフェイスを提供します。
- Citrix Storefront Service (NT SERVICE\ CitrixStorefront): StoreFrontの管理をサポートします。（StoreFrontコンポーネント自体の一部ではありません。）

- Citrix Storefront Privileged Administration Service (NT SERVICE\CitrixPrivilegedService): StoreFrontの特権管理操作をサポートします。（StoreFrontコンポーネント自体の一部ではありません。）
- Citrix Config Synchronizer Service (NT SERVICE\CitrixConfigSyncService): メインサイトデータベースからローカルホストキャッシュに構成データを伝播します。
- Citrix High Availability Service (NT SERVICE\CitrixHighAvailabilityService): メインサイトデータベースが利用できない場合に、ユーザーが利用できる仮想デスクトップまたはアプリケーションを選択します。

Delivery Controllerのインストールでは、以下のWindowsサービスも作成されます。これらは、他のCitrixコンポーネントと一緒にインストールされた場合にも作成されます。

- Citrix Diagnostic Facility COM Server (NT SERVICE\CdfSvc): Citrixサポートが使用するための診断情報の収集をサポートします。
- Citrix Telemetry Service (NT SERVICE\CitrixTelemetryService): Citrixによる分析のために診断情報を収集し、管理者が分析結果と推奨事項を表示してサイトの問題の診断に役立てられるようにします。

Delivery Controllerのインストールでは、以下のWindowsサービスも作成されます。これは現在使用されていません。有効になっている場合は、無効にしてください。

- Citrix リモート ブローカー プロバイダー (NT SERVICE\XaXdCloudProxy)

Delivery Controllerのインストールでは、以下のWindowsサービスも作成されます。これらは現在使用されていませんが、有効にする必要があります。無効にしないでください。

- Citrix オーケストレーション サービス (NT SERVICE\CitrixOrchestration)
- Citrix トラスト サービス (NT SERVICE\CitrixTrust)

Citrix Storefront Privileged Administration Serviceを除き、これらのサービスには「サービスとしてログオン」のログオン権限と、「プロセスのメモリクォータの調整」、「セキュリティ監査の生成」、「プロセスレベルトークンの置き換え」の特権が付与されます。これらのユーザー権限を変更する必要はありません。これらの特権はDelivery Controllerでは使用されず、自動的に無効になります。

サービス設定の構成

Citrix Storefront Privileged AdministrationサービスとCitrix Telemetry Serviceを除き、上記のユーザー権限の構成セクションに記載されているDelivery ControllerのWindowsサービスは、

NETWORK SERVICE IDとしてログオンするように構成されています。これらのサービス設定を変更しないでください。

Citrix Config Synchronizer Service は、Delivery Controller 上のローカル管理者グループに NETWORK SERVICE アカウントが属している必要があります。これにより、ローカルホストキャッシュが正しく機能します。

Citrix Storefront Privileged Administrationサービスは、ローカルシステム (NT AUTHORITY\SYSTEM) としてログオンするように構成されています。これは、通常サービスでは利用できないDelivery ControllerのStoreFront操作（Microsoft IISサイトの作成を含む）に必要です。このサービス設定を変更しないでください。

Citrix Telemetry Service は、サービス固有の ID としてログオンするように構成されています。

Citrix Telemetry Service は無効にできます。このサービスと、すでに無効になっているサービスを除き、これらの Delivery Controller Windows サービスの他のサービスを無効にしないでください。

レジストリ設定の構成

VDAファイルシステムで8.3形式のファイル名とフォルダーの作成を有効にする必要はなくなりました。レジストリキー **NtfsDisable8dot3NameCreation** を構成して、8.3形式のファイル名とフォルダーの作成を無効にできます。これは、**fsutil.exe behavior set disable8dot3** コマンドを使用しても構成できます。

展開シナリオのセキュリティ上の考慮事項

ユーザー環境には、組織によって管理されておらず、完全にユーザーの制御下にあるユーザーデバイス、または組織によって管理および運用されているユーザーデバイスのいずれかが含まれる場合があります。これら2つの環境におけるセキュリティ上の考慮事項は、一般的に異なります。

管理対象ユーザーデバイス

管理対象ユーザーデバイスは管理制御下にあります。これらは、お客様自身の制御下にあるか、信頼する別の組織の制御下にあります。ユーザーデバイスを直接構成してユーザーに提供することも、単一のデスクトップが全画面表示モードでのみ実行されるターミナルを提供することもできます。すべての管理対象ユーザーデバイスについて、上記の一般的なセキュリティベストプラクティスに従ってください。このリリースでは、ユーザーデバイスに必要なソフトウェアが最小限であるという利点があります。

管理対象のユーザーデバイスは、全画面表示モードまたはウィンドウモードで使用するように構成できます。

- 全画面表示モード: ユーザーは通常のWindowsログオン画面でログオンします。その後、同じユーザー資格情報を使用して、このリリースに自動的にログオンします。
- ユーザーはデスクトップをウィンドウで表示します: ユーザーはまずユーザーデバイスにログオンし、次にこのリリースに付属のWebサイトを通じてこのリリースにログオンします。

管理対象外のユーザーデバイス

信頼できる組織によって管理および運用されていないユーザーデバイスは、管理制御下にあるとは見なされません。たとえば、ユーザーが自分のデバイスを入手して構成することを許可する場合がありますが、ユーザーは上記の一般的なセキュリティのベストプラクティスに従わない可能性があります。このリリースには、管理対象外のユーザーデバイスにデスクトップを安全に配信できるという利点があります。これらのデバイスには、キーロガーや同様の入力攻撃を防ぐための基本的なウイルス対策保護が引き続き必要です。

データストレージに関する考慮事項

このリリースを使用する場合、ユーザーが物理的に制御しているユーザーデバイスにデータを保存することを防ぐことができます。ただし、ユーザーがデスクトップにデータを保存することの影響については、引き続き考慮する必要があります。ユーザーがデスクトップにデータを保存することは良い習慣ではありません。データは、ファイルサーバー、データベースサーバー、または適切に保護できるその他のリポジトリに保持する必要があります。

デスクトップ環境は、プールされたデスクトップや専用デスクトップなど、さまざまな種類のデスクトップで構成される場合があります。ユーザーは、プールされたデスクトップなど、ユーザー間で共有されるデスクトップにデータを保存してはなりません。ユーザーが専用デスクトップにデータを保存する場合、そのデスクトップが後で他のユーザーに利用可能になった場合は、そのデータを削除する必要があります。

混在バージョン環境

一部のアップグレードでは、混在バージョン環境は避けられません。ベストプラクティスに従い、異なるバージョンのCitrixコンポーネントが共存する時間を最小限に抑えてください。混在バージョン環境では、たとえばセキュリティポリシーが一律に適用されない場合があります。

> **注：**
>
> これは他のソフトウェア製品にも共通しています。以前のバージョンのActive Directoryを使用すると、後のバージョンのWindowsではグループポリシーが部分的にしか適用されません。

以下のシナリオでは、特定の混在バージョンCitrix環境で発生する可能性のあるセキュリティ問題について説明します。Citrix Receiver 1.7を使用してXenAppおよびXenDesktop 7.6 Feature Pack 2のVDAを実行している仮想デスクトップに接続すると、サイトでポリシー設定 が有効になりますが、XenAppおよびXenDesktop 7.1を実行しているDelivery Controllerでは無効にできません。これは、製品の後のバージョンでリリースされたポリシー設定を認識しないためです。このポリシー設定により、ユーザーはファイルを仮想デスクトップにアップロードおよびダウンロードできるようになり、これがセキュリティ問題となります。この問題を回避するには、Delivery Controller（またはStudioのスタンドアロンインスタンス）をバージョン7.6 Feature Pack 2にアップグレードし、グループポリシーを使用してポリシー設定を無効にします。または、影響を受けるすべての仮想デスクトップでローカルポリシーを使用します。

Remote PC Accessのセキュリティに関する考慮事項

Remote PC Accessは、次のセキュリティ機能を実装しています。

- スマートカードの使用がサポートされています。
- リモートセッションが接続されると、オフィスPCのモニターは空白で表示されます。
- Remote PC Accessは、CTRL+ALT+DEL、USB対応スマートカード、生体認証デバイスを除くすべてのキーボードおよびマウス入力をリモートセッションにリダイレクトします。
- SmoothRoamingは、単一ユーザーのみがサポートされます。
- ユーザーがオフィスPCにリモートセッションを接続している場合、そのユーザーのみがオフィスPCへのローカルアクセスを再開できます。ローカルアクセスを再開するには、ユーザーはローカルPCでCtrl-Alt-Delを押し、リモートセッションで使用したのと同じ資格情報でログオンします。システムに適切なサードパーティの資格情報プロバイダー統合がある場合、ユーザーはスマートカードを挿入するか、生体認証を利用してローカルアクセスを再開することもできます。このデフォルトの動作は、グループポリシーオブジェクト（GPO）を介して高速ユーザー切り替えを有効にするか、レジストリを編集することで上書きできます。

注：

Citrixでは、VDA管理者権限を一般セッションユーザーに割り当てないことをお勧めします。

自動割り当て

デフォルトでは、Remote PC Accessは複数のユーザーのVDAへの自動割り当てをサポートしています。XenDesktop 5.6 Feature Pack 1では、管理者はRemotePCAccess.ps1 PowerShellスクリプトを使用してこの動作を上書きできました。このリリースでは、複数の自動リモートPC割り当てを許可または禁止するためにレジストリエントリを使用します。この設定はサイト全体に適用されます。

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

> 自動割り当てを単一ユーザーに制限するには：

サイト内の各Controllerで、次のレジストリエントリを設定します。

```
HKEY_LOCAL_MACHINE\Software\Citrix|DesktopServer

Name: AllowMultipleRemotePCAssignments

Type: REG_DWORD

Data: 0 = Disable multiple user assignment, 1 = (Default) Enable multiple
user assignment.
```

既存のユーザー割り当てがある場合は、SDKコマンドを使用してそれらを削除し、VDAが単一の自動割り当ての対象となるようにします。

- VDAから割り当てられているすべてのユーザーを削除します: `$machine.AssociatedUserNames | %{ Remove-BrokerUser-Name $_ -Machine $machine`
- デリバリーグループからVDAを削除します: `$machine | Remove-BrokerMachine -DesktopGroup $desktopGroup`

物理的なオフィスPCを再起動します。

XML信頼

XML信頼設定は、以下を使用する展開に適用されます。

- オンプレミスのStoreFront。
- パスワードを必要としないサブスクライバー（ユーザー）認証テクノロジー。このようなテクノロジーの例としては、ドメインパススルー、スマートカード、SAML、Veridiumソリューションなどがあります。

XML信頼設定を有効にすると、ユーザーは正常に認証され、アプリケーションを起動できるようになります。Delivery ControllerはStoreFrontから送信された資格情報を信頼します。この設定は、Delivery ControllerとStoreFront間の通信が保護されている場合（ファイアウォール、IPsec、またはその他のセキュリティ推奨事項を使用している場合）にのみ有効にしてください。

この設定はデフォルトで無効になっています。

XML信頼設定を確認、有効化、または無効化するには、Citrix Virtual Apps and Desktops PowerShell SDKを使用します。

- XML信頼設定の現在の値を確認するには、`Get-BrokerSite` を実行し、`TrustRequestsSentToTheXMLServicePort` の値を調べます。
- XML信頼を有効にするには、`Set-BrokerSite -TrustRequestsSentToTheXmlServicePort $true` を実行します。
- XML信頼を無効にするには、`Set-BrokerSite -TrustRequestsSentToTheXmlServicePort $false` を実行します。

証明書を管理する

TLS は、2 つの当事者間の信頼を確立するために証明書を使用します。サービスを提供する各サーバーに適切な証明書をインストールし、そのサーバーに接続するマシンがその証明書を信頼することを確認する必要があります。証明書に署名するためのオプションは次のとおりです。

- 自己署名証明書。これらは推奨されません。この証明書を信頼する必要がある他のマシンに手動でコピーする必要があるため、管理が困難です。
- エンタープライズ認証局。既存の PKI が導入されている場合、これは通常、内部デバイス間で使用する証明書に署名する最も簡単なオプションです。
- 公開認証局。これには、ドメインの所有権を認証局に証明する必要があります。管理されていないクライアントデバイスは、通常、主要な公開認証局からの証明書を信頼するように事前設定されているという利点があります。

新しい証明書を作成する

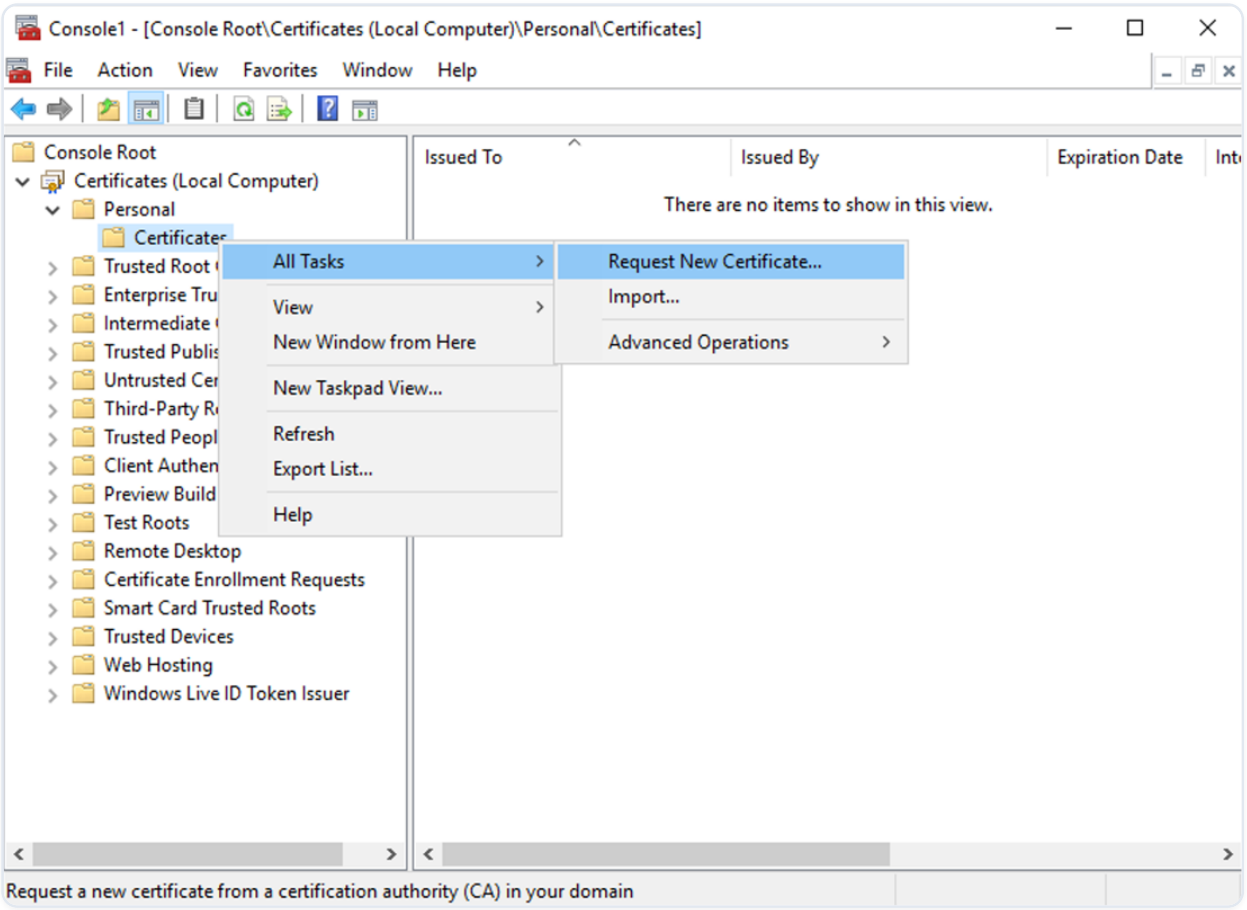
証明書の作成については、組織のポリシーと手順に従ってください。

Microsoft 証明機関を使用して証明書を作成する

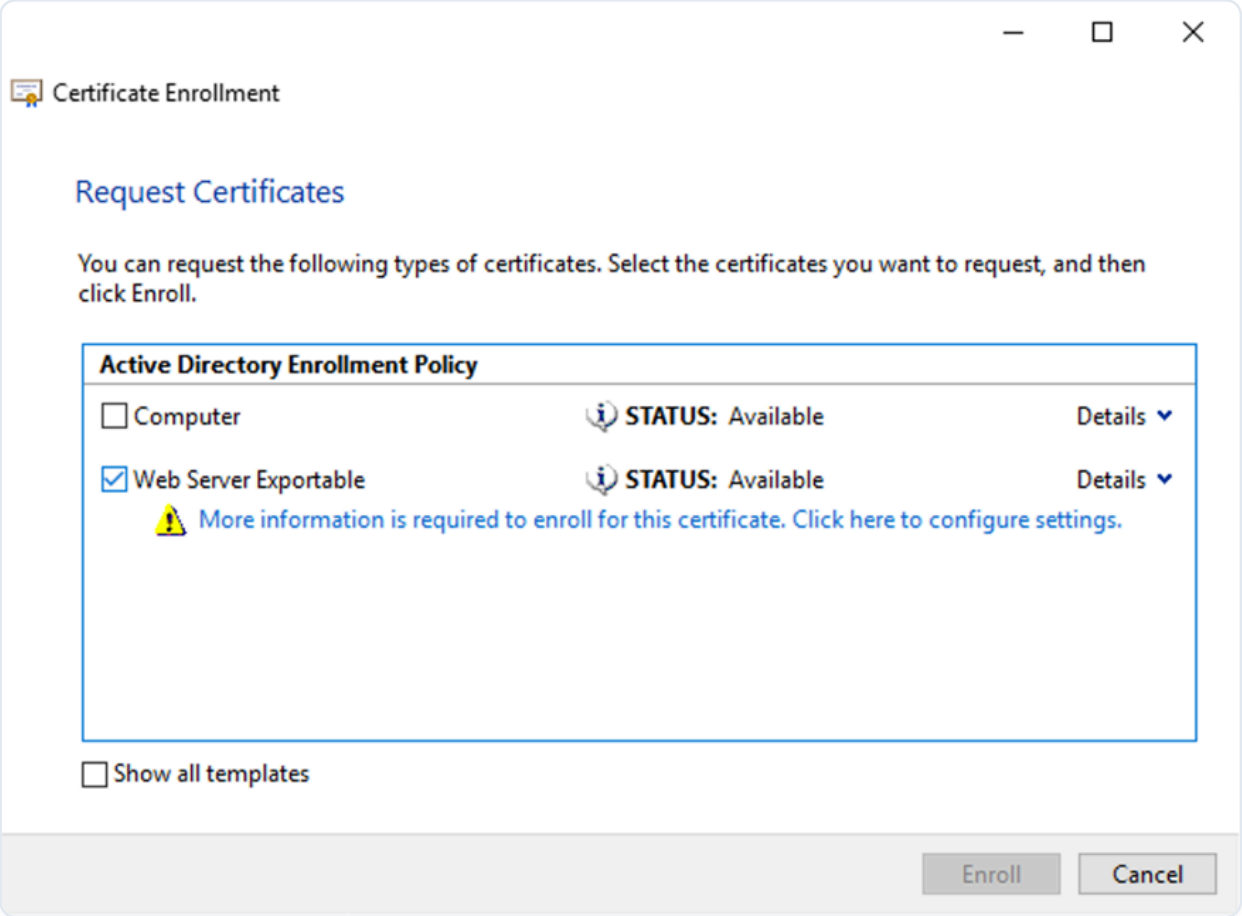
Microsoft 証明機関が Active Directory ドメインまたは Delivery Controller が参加している信頼されたフォレストに統合されている場合、証明書 MMC スナップインの証明書登録ウィザードから証明書を取得できます。Microsoft 証明機関は、Web サーバーでの使用に適した証明書テンプレートを公開している必要があります。

ルート証明書は、グループポリシーを使用してドメイン上の他のマシンに自動的に展開されます。したがって、ドメイン上の他のすべてのマシンは、Microsoft 証明機関を使用して作成された証明書を信頼します。ドメイン上にないマシンがある場合は、ルート認証機関証明書をエクスポートして、それらのマシンにインポートする必要があります。

1. サーバーで、MMC コンソールを開き、証明書スナップインを追加します。プロンプトが表示されたら、 を選択します。
2. **個人 > 証明書**を展開し、**すべてのタスク > 新しい証明書の要求**コンテキストメニューコマンドを使用します。



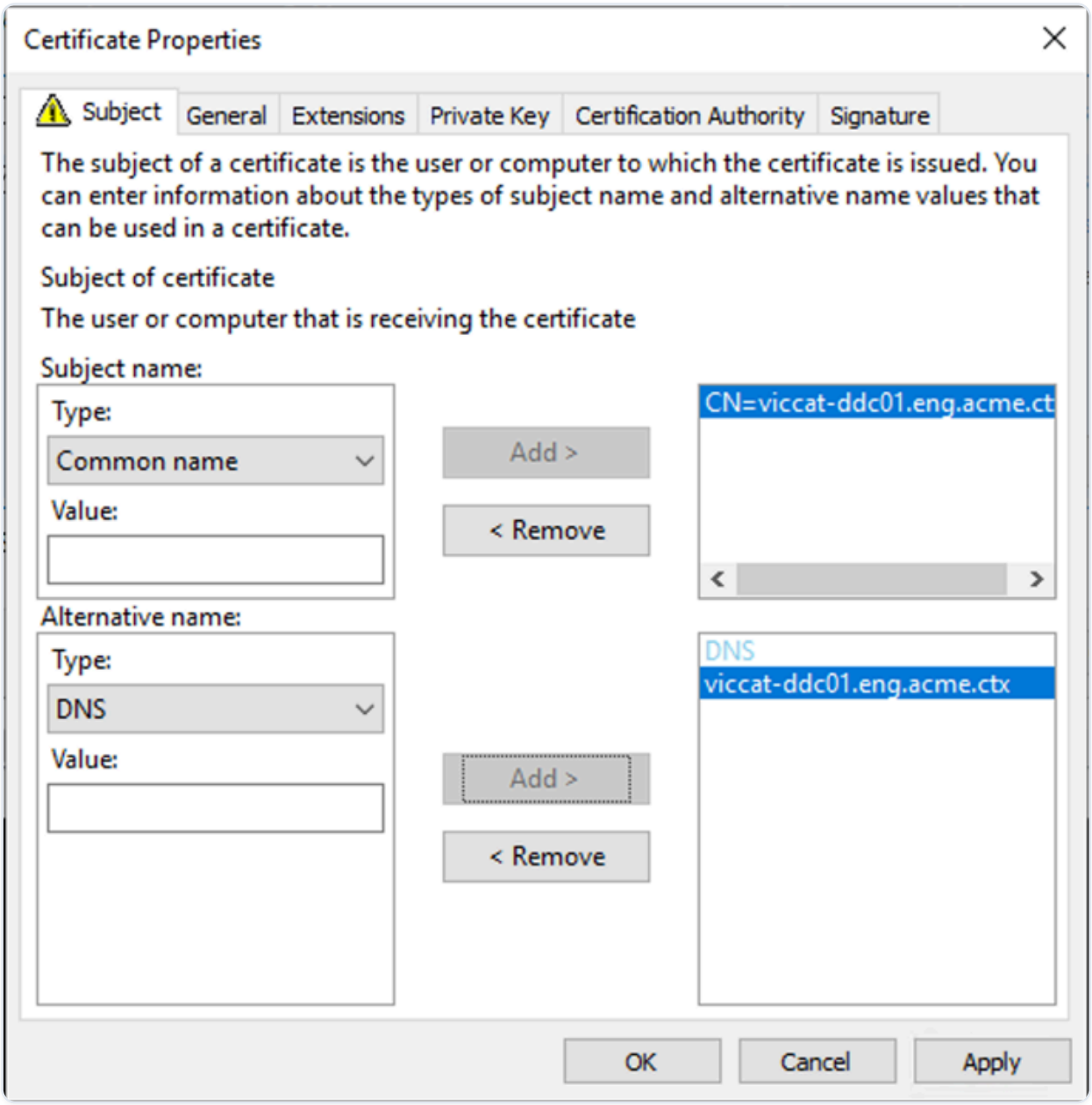
3. **次へ**をクリックして開始し、**次へ**をクリックして Active Directory 登録から証明書を取得することを確認します。
4. **Web Server Exportable** など、適切なテンプレートを選択します。テンプレートが Subject の値を自動的に提供するように設定されている場合は、詳細を指定せずに **Enroll** をクリックできます。それ以外の場合は、**More information is required to enroll for this certificate. Click here to configure settings.** をクリックします。



5. 証明書テンプレートの詳細を指定するには、**詳細**の矢印ボタンをクリックして、以下を構成します。

   サブジェクト名: を選択し、サーバーの FQDN を追加します。

   代替名: を選択し、サーバーの FQDN を追加します。



6. **OK**を押します。
7. **Enroll** を押して証明書を作成します。証明書の一覧に表示されます。

   個人証明書のスクリーンショット(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/personal-certificates.png)

IIS を使用して証明書要求を作成する

IIS がサーバーにインストールされている場合は、次の手順を実行します。

1. **インターネット インフォメーション サービス (IIS) マネージャー**を開きます
2. 接続リストでサーバーノードを選択します。
3. **サーバー証明書**を開きます。 「サーバー証明書」の場所を示すスクリーンショット(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/iis-server-certificates.png)

4. **操作**ペインから、**証明書要求の作成...** を選択します。 「証明書要求の作成」が強調表示された操作メニューのスクリーンショット(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/iis-create-certificate-request.png)
5. **識別名プロパティ**を入力します。 識別名プロパティ画面のスクリーンショット(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/iis-request-certificate-properties.png)
6. **暗号化サービスプロバイダーのプロパティ**画面で、**暗号化サービスプロバイダー**は既定のままにします。キーサイズは**2048**以上に設定します。 暗号化サービスプロバイダーのプロパティ画面のスクリーンショット(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/iis-request-certificate-crypto.png)
7. ファイル名を選択し、**完了**を押します。 ファイル名画面のスクリーンショット(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/iis-request-certificate-file-name.png)
8. CSR を証明機関にアップロードします。
9. 証明書を受け取ったら、**操作**ペインから**証明書要求の完了...** を選択します。 「証明書要求の完了」が強調表示された操作メニューのスクリーンショット(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/iis-complete-certificate-request.png)
10. 証明書を選択し、**フレンドリ名**を指定して**OK**を押します。 証明書応答の完了ウィンドウのスクリーンショット(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/iis-certificate-authority-response.png)

サブジェクトの別名を設定する方法はありません。そのため、証明書は共通名を使用して指定されたサーバーに限定されます。

証明書スナップインから証明書署名要求を作成する

証明書MMCスナップイン内から、証明書署名要求を作成できます。これにより、証明書を提供する認証局に送信できるファイルが生成されます。その後、証明書をインポートして、ローカルの秘密鍵と結合する必要があります。

1. サーバーで、MMCコンソールを開き、証明書スナップインを追加します。プロンプトが表示されたら、を選択します。
2. **個人** > **証明書**を展開します。
3. **すべてのタスク** > **高度な操作** > **カスタム要求の作成**を選択します。
4. **開始する前に**で、**次へ**を選択します。
5. **証明書登録ポリシーの選択**画面で、適切な既存のポリシーを選択するか、**登録ポリシーなしで続行**を選択します。

6. **カスタム要求**画面で、登録ポリシーを使用している場合は、利用可能な場合は**Web Server Exportable**などの適切なテンプレートを選択します。
7. **証明書情報**画面で、**詳細**を展開し、**プロパティ**を選択します。
8. **証明書のプロパティ**ウィンドウの**全般**タブで、適切なフレンドリ名を入力します。
9. **サブジェクト**タブで、次のようにします。
    a. **サブジェクト名**の下で、**共通名**を選択し、サーバーのFQDNを入力します。ワイルドカードを入力できます。**追加**を選択します。
    b. **サブジェクト名**の下で、組織、組織単位、地域、都道府県、国に適切な値を追加します。
    c. **代替名**の下で、**DNS**を選択します。サーバーのFQDNを追加します。複数のサーバーFQDNまたはワイルドカードFQDNを追加できます。
10. **拡張機能**タブで、次のようにします。
    - **キー使用法**の下で、**デジタル署名**と**キーの暗号化**を追加します。
    - 「**拡張キー使用法 (アプリケーションポリシー)**」で、「**サーバー認証**」と「**クライアント認証**」を追加します。
11. 「**秘密キー**」タブで。
    - 「**暗号化サービスプロバイダー (CSP) の選択**」で、適切なプロバイダーを選択します。
    - 「**キーオプション**」で、適切なキーサイズを選択します。RSAプロバイダーの場合、最小で2048のキーサイズを使用します。セキュリティを強化するために4096を選択することもできますが、パフォーマンスにわずかな影響があります。
    - 「**キーオプション**」で、「**秘密キーをエクスポート可能にする**」を選択します。
12. **OK**を選択します。
13. **次へ**を選択します。
14. 「**参照**」を選択し、要求を保存します。
15. 「**完了**」を選択します。
16. CSRを証明機関にアップロードします。
17. 証明書を受け取ったら、秘密キーにリンクされるように、同じサーバーに(#import-existing-certificate)インポートします。

新しい自己署名証明書を作成する

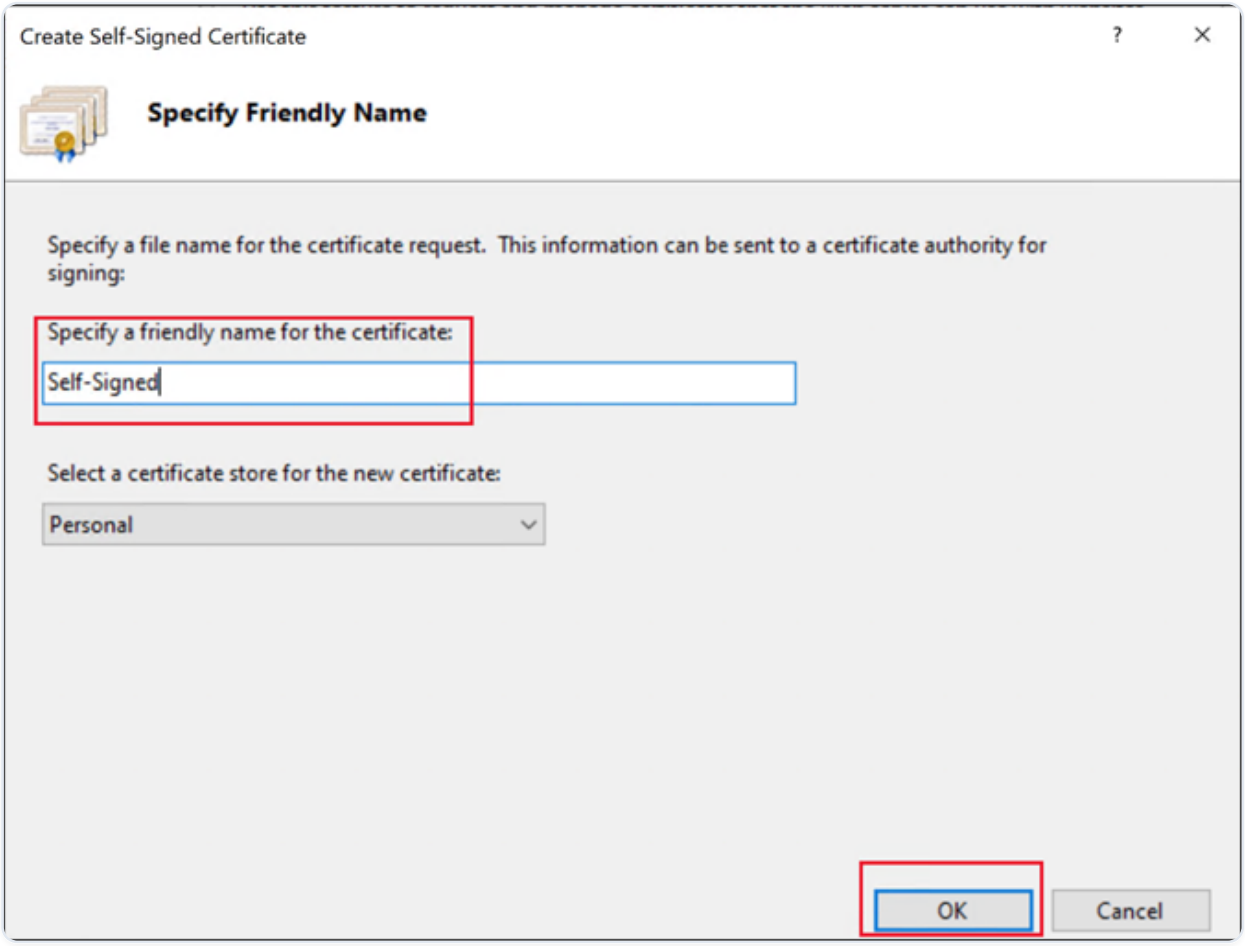
自己署名証明書は、デリバリーコントローラー™とWeb Studioのインストール中に作成されます。新しい自己署名証明書を生成し、既存の証明書を置き換えるために使用できます。

IISマネージャーを使用する

サーバーにIISがインストールされている場合は、次の手順を実行できます。

1. 管理者としてサーバーにログオンします。
2. IISマネージャーを開きます
3. 「**サーバー証明書**」を開きます
4. 「**操作**」ペインで、「**自己署名証明書の作成**」を選択します。

   サーバー証明書(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/server-certificates.png)
5. 「**自己署名証明書の作成**」で、証明書の名前を入力し、「**OK**」をクリックします。自己署名証明書が作成されます。



PowerShellの使用

PowerShellを使用して自己署名証明書を作成できます。

```
$certSubject = "CN=myddc.example.com" # The FQDN of the server.

$friendlyName = "Self-Signed-3"
```

```
$expireYears = 5



## Create new self-signed certificate under LocalMachine\My

$certificate = New-SelfSignedCertificate -Subject $certSubject
-CertStoreLocation "Cert:\LocalMachine\My\" -KeyExportPolicy Exportable
-KeySpec Signature -KeyLength 2048 -KeyAlgorithm RSA -HashAlgorithm SHA256
-FriendlyName $friendlyName -NotAfter $
([System.DateTime]::Now.AddYears($expireYears))



# Add to trusted root certificates

$rootCertStore = Get-Item "Cert:\LocalMachine\Root\"

$rootCertStore.Open([System.Security.Cryptography.X509Certificates.OpenFla
gs]::ReadWrite)

$rootCertStore.Add($certificate)
```

既存の証明書をインポートする

以下のいずれかの方法を使用して、既存の証明書をサーバーにインポートできます。

証明書のインポートウィザード

1. PFXファイルをダブルクリックするか、ファイルを右クリックして「**PFXのインストール**」を選択します。これにより、「**証明書のインポートウィザード**」が開きます。
2. 「**ストアの場所**」で、「**ローカルコンピューター**」を選択します。

   証明書のインポートウィザードのスクリーンショット(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/certificate-import-wizard.png)
3. 必要に応じてパスワードを入力します。

   証明書のインポートウィザード、秘密キーの保護手順のスクリーンショット(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/key-protection.png)

4. 「**証明書ストア**」を選択します。サーバー証明書の場合は、「**個人**」を選択します。このマシンから信頼したいルート証明書または自己署名証明書である場合は、「**信頼されたルート証明機関**」を選択します。

   証明書のインポートウィザード、証明書ストアの手順のスクリーンショット(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/certificate-store.png)

コンピューター証明書の管理コンソールを使用する

1. コンピューター証明書の管理コンソールを開き、適切な証明書ストアに移動します。サーバー証明書の場合、通常は「**個人**」 > 「**証明書**」です。ルート証明書または自己署名証明書を信頼するには、「**信頼されたルート証明機関**」 > 「**証明書**」を選択します。
2. 証明書を右クリックし、「**すべてのタスク**」>「**インポート...**」を選択します。

   コンピューター証明書の管理コンソール(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/manage-computer-certificates-console.png)
3. 「**参照...**」を選択し、ファイルを選択します。
4. 必要に応じてパスワードを入力します。

PowerShell を使用する

証明書をインポートするには、PowerShell コマンドレット Import-PfxCertificate を使用します。たとえば、パスワード `123456` を使用して証明書 `certificate.pfx` を個人証明書ストアにインポートするには、次のコマンドを実行します。

```
Import-PfxCertificate -Password $(ConvertTo-SecureString -String "123456"
-AsPlainText -Force) -CertStoreLocation Cert:\LocalMachine\My\ -FilePath .
\Desktop\certificate.pfx
```

信頼されたルート証明書をインポートするには、`CertStoreLocation` を `Cert:\LocalMachine\Root\` に設定します。

秘密キーなしで証明書をエクスポートする

証明書を他のデバイスにインポートして信頼できるようにエクスポートするには、秘密キーを除外する必要があります。

1. コンピューター証明書の管理を開きます。「**個人**」>「**証明書**」に移動し、エクスポートする証明書を選択します。
2. 「**操作**」メニューから「**すべてのタスク**」を選択し、次に「**エクスポート**」を選択します。

エクスポートメニューのある証明書管理のスクリーンショット(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/certificate-export.png)

3. 「**いいえ、秘密キーをエクスポートしません**」を選択し、「**次へ**」を押します。

   証明書のエクスポート(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/certificate-export-no-private-key.png)

4. 形式「**DER encoded binary X.509 (.CER)**」（デフォルト）を選択し、「**次へ**」を押します。
5. ファイル名を入力し、「**次へ**」を押します。

   「証明書のエクスポートウィザード、ファイル名」のスクリーンショット(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/certificate-export-file.png)

6. 「**完了**」を選択します。

   「証明書のエクスポートウィザード、エクスポート成功」のスクリーンショット(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/certificate-export-complete.png)

秘密キーを含む証明書のエクスポート

証明書を他のサーバーで使用できるようにエクスポートするには、秘密キーを含める必要があります。

1. コンピューター証明書の管理を開きます。「**個人**」>「**証明書**」に移動し、エクスポートする証明書を選択します。
2. 「**操作**」メニューから「**すべてのタスク**」を選択し、次に「**エクスポート**」を選択します。

   「エクスポート」メニューを含む証明書管理のスクリーンショット(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/certificate-export.png)

3. 「**はい、秘密キーをエクスポートします**」を選択し、次に「**次へ**」を選択します。

   「証明書のエクスポート」(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/certificate-export-private-key.png)

4. 「**セキュリティ**」タブでパスワードを入力し、「**次へ**」を選択します。

   「証明書のエクスポートウィザード、セキュリティ手順」のスクリーンショット(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/certificate-export-password.png)

5. ファイル名を入力し、「**次へ**」を選択します。

   「証明書のエクスポートウィザード、ファイル名」のスクリーンショット(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/certificate-export-file.png)

6. 「**完了**」を選択します。

   証明書のエクスポートウィザード、エクスポート成功のスクリーンショット](/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/certificate-export-complete.png)

証明書をPEM形式に変換する

デフォルトでは、Windowsは秘密鍵を含む.pfxファイルとして、PKCS#12形式で証明書をエクスポートします。NetScaler® Gatewayまたはライセンスサーバーで証明書を使用するには、証明書と秘密鍵をPEM形式の別々のファイルに抽出する必要があります。これはopensslを使用して実行できます。

証明書をPEM形式でエクスポートするには、以下を実行します。

```
openssl pkcs12 -in name.pfx -clcerts -nokeys -out name.cer
```

既存のパスワードと新しいパスフレーズの入力を求められます

キーをPEM形式でエクスポートするには、以下を実行します。

```
openssl pkcs12 -in name.pfx -nocerts -out name.key
```

証明書の信頼

- 公開認証局の証明書を使用する場合、デバイスには通常、ルート証明書が事前に構成されています。
- エンタープライズ認証局を使用する場合、その証明書を信頼する必要があるすべてのデバイスにルート証明書を展開する必要があります。Active Directory証明書サービスを使用している場合、ルート証明書はグループポリシーを使用してドメイン上のすべてのマシンにも展開されます。NetScalerゲートウェイや他のドメイン上のマシンなど、ドメインに参加していないマシンには、ルート証明書を手動でインポートする必要があります。
- 自己署名証明書を使用している場合は、その証明書を信頼する必要があるすべてのマシンに手動でインストールする必要があります。

Windowsから自己署名証明書または信頼されたルート証明書をエクスポートするには、秘密鍵なしで証明書をエクスポートするを参照してください。

Windowsが証明書を信頼するようにするには、**信頼されたルート証明機関**ストアに証明書をインポートする必要があります。PowerShellを使用する場合は、ストア**Cert:\\LocalMachine\Root**を入力します。

NetScalerが証明書を信頼するようにするには、まず証明書をPEM形式に変換する、次にルート証明書をインストールする必要があります。

スマートカード

スマートカードおよび同等のテクノロジーは、この記事で説明されているガイドライン内でサポートされています。Citrix Virtual AppsまたはCitrix Virtual Desktops™でスマートカードを使用するには、次の手順を実行します。

- スマートカードの使用に関する組織のセキュリティポリシーを理解します。これらのポリシーには、たとえば、スマートカードの発行方法やユーザーがスマートカードを保護する方法が記載されている場合があります。これらのポリシーの一部は、Citrix Virtual Apps™またはCitrix Virtual Desktops環境で再評価する必要がある場合があります。
- スマートカードで使用するユーザーデバイスの種類、オペレーティングシステム、および公開アプリケーションを決定します。
- スマートカードテクノロジーと、選択したスマートカードベンダーのハードウェアおよびソフトウェアに精通してください。
- 分散環境でデジタル証明書を展開する方法を理解します。

> **注：**
>
> (/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/secure/smart-cards.html#fast-smart-card)ではスマートカードの登録はサポートされていません。スマートカードの登録は、高速スマートカードが無効になっている場合に機能する可能性がありますが、スマートカードとミドルウェアの種類によって異なります。Citrix Virtual Apps and Desktopsとの統合および仮想セッションを介したスマートカード登録のサポートについては、スマートカードおよびミドルウェアベンダーにお問い合わせください。

スマートカードの種類

企業向けスマートカードと消費者向けスマートカードは、同じ寸法、電気コネクタを持ち、同じスマートカードリーダーに適合します。

企業向けスマートカードにはデジタル証明書が含まれています。これらのスマートカードはWindowsログオンをサポートし、ドキュメントやメールのデジタル署名および暗号化のためのアプリケーションでも使用できます。Citrix Virtual Apps and Desktops™はこれらの用途をサポートしています。

消費者向けスマートカードにはデジタル証明書は含まれていません。共有シークレットが含まれています。これらのスマートカードは、支払い（チップアンドサインまたはチップアンドPINクレジットカードなど）をサポートできます。Windowsログオンや一般的なWindowsアプリケーションはサポートしていません。これらのスマートカードを使用するには、特殊なWindowsアプリケーションと適切なソフトウェアインフラストラクチャ（たとえば、決済カードネットワークへの接続を含む）が必要です。これらの特殊なアプリケーションをCitrix Virtual AppsまたはCitrix Virtual Desktopsでサポートする方法については、Citrixの担当者にお問い合わせください。

企業向けスマートカードには、同様の方法で使用できる互換性のある同等品があります。

- スマートカードと同等のUSBトークンは、USBポートに直接接続します。これらのUSBトークンは通常、USBフラッシュドライブと同じサイズですが、携帯電話で使用されるSIMカードと同じくらい小さい場合もあります。これらはスマートカードとUSBスマートカードリーダーの組み合わせとして表示されます。
- Windows Trusted Platform Module (TPM)を使用する仮想スマートカードは、スマートカードとして表示されます。これらの仮想スマートカードは、Citrix Workspace app（最小バージョンCitrix Receiver 4.3）を使用するWindows 8およびWindows 10でサポートされています。
    - XenApp and XenDesktop 7.6 FP3より前のバージョンのCitrix Virtual Apps and Desktops（旧XenApp and XenDesktop）は、仮想スマートカードをサポートしていません。
    - 仮想スマートカードの詳細については、仮想スマートカードの概要を参照してください。

    注記: 「仮想スマートカード」という用語は、ユーザーコンピューターに保存されているデジタル証明書を指すためにも使用されます。これらのデジタル証明書は、厳密にはスマートカードと同等ではありません。

Citrix Virtual Apps and Desktopsのスマートカードサポートは、Microsoft Personal Computer/Smart Card (PC/SC) 標準仕様に基づいています。最低要件として、スマートカードおよびスマートカードデバイスは、基盤となるWindowsオペレーティングシステムによってサポートされ、対象となるWindowsオペレーティングシステムを実行するコンピューターで使用するために、Microsoft Windows Hardware Quality Labs (WHQL) によって承認されている必要があります。ハードウェアのPC/SC準拠に関する追加情報については、Microsoftのドキュメントを参照してください。他の種類のユーザーデバイスもPS/SC標準に準拠している場合があります。詳細については、Citrix Readyプログラムを参照してください。

通常、各ベンダーのスマートカードまたは同等のものには、個別のデバイスドライバーが必要です。ただし、スマートカードがNIST個人識別検証（PIV）標準などの標準に準拠している場合、さまざまなスマートカードに単一のデバイスドライバーを使用できる可能性があります。デバイスドライバーは、ユーザーデバイスとVirtual Delivery Agent (VDA) の両方にインストールする必要があります。デバイスドライバーは、Citrixパートナーから入手できるスマートカードミドルウェア

パッケージの一部として提供されることが多く、スマートカードミドルウェアパッケージは高度な機能を提供します。デバイスドライバーは、暗号化サービスプロバイダー（CSP）、キーストレージプロバイダー（KSP）、またはミニドライバーとも呼ばれる場合があります。

Windowsシステム用の以下のスマートカードとミドルウェアの組み合わせは、Citrixによってそのタイプの代表的な例としてテストされています。ただし、他のスマートカードとミドルウェアも使用できます。Citrix互換のスマートカードとミドルウェアに関する詳細については、`<http://www.citrix.com/ready>`を参照してください。

ミドルウェア	対応カード
Gemalto .NETカード用ミニドライバー	ジェムアルト ドットネット v2以降

他の種類のデバイスでのスマートカードの使用に関する情報については、そのデバイスのCitrix Workspace™アプリのドキュメントを参照してください。

リモートPCアクセス

スマートカードは、Windows 10、Windows 8、またはWindows 7を実行している物理的なオフィスPCへのリモートアクセスでのみサポートされています。

Remote PC Accessでテストされたスマートカードは次のとおりです。

ミドルウェア	対応カード
Gemalto .NETミニドライバー	ジェムアルト ドットネット v2以降

高速スマートカード

高速スマートカードは、既存のHDX PC/SCベースのスマートカードリダイレクトを改善したものです。高遅延のWAN環境でスマートカードを使用する場合にパフォーマンスが向上します。遅延が大きい場合、パフォーマンスの向上は大幅なものになります（例えば、Windowsの高速スマートカードログオンでは15秒、PC/SCベースのスマートカードリダイレクトでは1分以上）。

高速スマートカードは、現在サポートされているWindows VDAを搭載したホストマシンでデフォルトで有効になっています。ホスト側で高速スマートカードを無効にするには（例えば診断目的で）、'Disable Cryptographic Redirection' レジストリ設定をゼロ以外の値に設定します。

```
HKLM\SOFTWARE\Citrix\SmartCard

CryptographicRedirectionDisable (DWORD)
```

クライアント側で高速スマートカードを有効にするには、関連するStoreFrontサイトの*default.ica*ファイルにSmartCardCryptographicRedirection ICAパラメーターを含めます。

```
[WFClient]

SmartCardCryptographicRedirection=On
```

さらに、クライアント側では、以下のレジストリ設定を使用して、高速スマートカードを強制的に有効または無効にできます（例えば診断目的で）。

- HKLM\SOFTWARE\Citrix\ICA Client\SmartCard\ForceEnableCryptographicRedirection (ゼロ以外のDWORDとして)

または

- HKLM\SOFTWARE\Citrix\ICA Client\SmartCard\ForceDisableCryptographicRedirection (ゼロ以外のDWORDとして)

クライアントマシンが64ビットの場合、32ビットレジストリハイブを指定する必要があります（`WOW6432Node`を使用）。

制限事項:

- Windows版Citrix Workspaceアプリのみが高速スマートカードをサポートしています。default.icaファイルで高速スマートカードを設定した場合、Windows版ではないCitrix Workspaceアプリは、既存のPC/SCリダイレクトを依然として使用します。
- 高速スマートカードがサポートする唯一のダブルホップシナリオは、両方のホップで高速スマートカードが有効になっているICA® > ICAです。高速スマートカードはICA > RDPダブルホップシナリオをサポートしていないため、これらのシナリオは機能しません。
- 高速スマートカードはCryptography Next Generationをサポートしていません。したがって、高速スマートカードは楕円曲線暗号 (ECC) スマートカードをサポートしていません。
- 高速スマートカードは読み取り専用のキーコンテナ操作のみをサポートしています。
- 高速スマートカードはスマートカードPINの変更をサポートしていません。

VDAバージョン2203およびWindows版Citrix Workspaceアプリバージョン2202（またはそれ以降）以降、高速スマートカードはCryptography Next Generation (CNG) と互換性があります。さらに、楕円曲線暗号 (ECC) スマートカードは、ECDSAとECDHの両方で、P-256、P-384、P-521ビットの以下の曲線に対応しています。

VDAバージョン2203以降、高速スマートカードは、同じユーザーのログオンセッション内のアプリケーション間でスマートカードPINをキャッシュする機能を追加します。例えば、**セッションPINキャッシュ**が有効になっており、エンドユーザーが以前にOutlookにスマートカードPINを提供している場合、その後Wordを使用してドキュメントに署名すると、Wordはすでにキャッシュされているスマートカード PIN（Outlookに送信されたもの）を使用します。**セッションPINキャッシュ**は、ユーザーがスマートカードPINを入力する回数を減らすことで、ユーザーエクスペリエンスを向上させます。さらに、スマートカードがVDAへのログオンに使用される場合、Windowsスマートカードログオン PINをオプションで**セッションPINキャッシュ**に保存できます。これにより、ユーザーエクスペリエンスがさらに向上します。

セッションPINキャッシュはデフォルトで無効になっています。VDA上の以下のレジストリ設定で有効化および制御できます。

HKLM\SOFTWARE\Citrix\SmartCard: で:

- `EnablePinSessionCache` をDWORDとして (有効にするにはゼロ以外)
- `EnableLogonPinSessionCache` をDWORDとして (有効にするにはゼロ以外)
- `PinSessionCacheEntryStaleTimeout` をDWORDとして (エントリが古くなるまでの秒数、デフォルトは1時間)

スマートカードリーダーの種類

スマートカードリーダーは、ユーザーデバイスに内蔵されている場合や、ユーザーデバイスに別途接続されている場合 (通常はUSBまたはBluetooth経由) があります。USB Chip/Smart Card Interface Devices (CCID) 仕様に準拠した接触型カードリーダーがサポートされています。これらには、ユーザーがスマートカードを挿入するスロットまたはスワイプ部分があります。Deutsche Kreditwirtschaft (DK) 規格では、接触型カードリーダーの4つのクラスが定義されています。

- クラス1スマートカードリーダーは最も一般的で、通常はスロットを備えています。クラス1スマートカードリーダーは、通常、オペレーティングシステムに付属の標準CCIDデバイスドライバーでサポートされます。
- クラス2スマートカードリーダーには、ユーザーデバイスからアクセスできないセキュアキーパッドも搭載されています。クラス2スマートカードリーダーは、セキュアキーパッドが統合されたキーボードに組み込まれている場合があります。クラス2スマートカードリーダーにつ

いては、Citrixの担当者にお問い合わせください。セキュアキーパッド機能を有効にするには、リーダー固有のデバイスドライバーが必要になる場合があります。

- クラス3スマートカードリーダーには、セキュアディスプレイも搭載されています。クラス3スマートカードリーダーはサポートされていません。
- クラス4スマートカードリーダーには、セキュアトランザクションモジュールも搭載されています。クラス4スマートカードリーダーはサポートされていません。

> **注：**
>
> スマートカードリーダーのクラスは、USBデバイスクラスとは関係ありません。

> スマートカードリーダーは、対応するデバイスドライバーをインストールしてユーザーデバイスにインストールする必要があります。

サポートされているスマートカードリーダーについては、使用しているCitrix Workspaceアプリのドキュメントを参照してください。Citrix Workspaceアプリのドキュメントでは、サポートされているバージョンは、スマートカードに関する記事またはシステム要件に関する記事に記載されています。

ユーザーエクスペリエンス

スマートカードのサポートは、Citrix Virtual Apps and Desktopsに統合されており、特定のICA/HDXスマートカード仮想チャネルを使用します。これはデフォルトで有効になっています。

重要: スマートカードリーダーに汎用USBリダイレクトを使用しないでください。これはスマートカードリーダーではデフォルトで無効になっており、有効にしてもサポートされません。

同じユーザーデバイス上で複数のスマートカードと複数のリーダーを使用できますが、パススルー認証が使用されている場合は、ユーザーが仮想デスクトップまたはアプリケーションを起動するときに、スマートカードを1枚だけ挿入する必要があります。アプリケーション内でスマートカードを使用する場合（たとえば、デジタル署名や暗号化機能の場合）、スマートカードの挿入やPINの入力に関する追加のプロンプトが表示されることがあります。これは、複数のスマートカードが同時に挿入されている場合に発生する可能性があります。

- スマートカードがすでにリーダーに挿入されているにもかかわらず、スマートカードの挿入を促すプロンプトが表示された場合は、ユーザーはキャンセルを選択する必要があります。
- PINの入力を求められた場合は、ユーザーはPINを再度入力する必要があります。

カード管理システムまたはベンダーユーティリティを使用してPINをリセットできます。

重要:

Citrix Virtual AppsまたはCitrix Virtual Desktopsセッション内で、Microsoft Remote Desktop Connectionアプリケーションとスマートカードを併用することはサポートされていません。これは「ダブルホップ」使用と呼ばれることがあります。

スマートカードを展開する前に

- スマートカードリーダー用のデバイスドライバーを入手し、ユーザーデバイスにインストールします。多くのスマートカードリーダーは、Microsoftが提供するCCIDデバイスドライバーを使用できます。
- スマートカードベンダーからデバイスドライバーと暗号化サービスプロバイダー（CSP）ソフトウェアを入手し、ユーザーデバイスと仮想デスクトップの両方にインストールします。ドライバーとCSPソフトウェアはCitrix Virtual Apps and Desktopsと互換性がある必要があります。互換性についてはベンダーのドキュメントを確認してください。ミニドライバーモデルをサポートおよび使用するスマートカードを使用する仮想デスクトップの場合、スマートカードミニドライバーは自動的にダウンロードされますが、http://catalog.update.microsoft.comまたはベンダーから入手することもできます。また、PKCS#11ミドルウェアが必要な場合は、カードベンダーから入手してください。
- 重要: Citrixは、Citrixソフトウェアをインストールする前に、物理コンピューターにドライバーとCSPソフトウェアをインストールしてテストすることを推奨します。
- Windows 10でInternet Explorerを使用してスマートカードを使用するユーザーのために、Citrix Receiver™ for WebのURLを信頼済みサイトリストに追加します。Windows 10では、信頼済みサイトの場合、Internet Explorerはデフォルトで保護モードで実行されません。
- 公開鍵インフラストラクチャ（PKI）が適切に構成されていることを確認してください。これには、Active Directory環境向けに証明書とアカウントのマッピングが正しく構成されており、ユーザー証明書の検証が正常に実行できることを確認することが含まれます。
- 展開が、Citrix WorkspaceアプリやStoreFrontなど、スマートカードで使用される他のCitrixコンポーネントのシステム要件を満たしていることを確認してください。
- サイト内の以下のサーバーへのアクセスを確保してください。
    - スマートカード上のログオン証明書に関連付けられているユーザーアカウントのActive Directoryドメインコントローラー

- デリバリーコントローラー™
- シトリックス ストアフロント
- シトリックス ゲートウェイ/シトリックス アクセス ゲートウェイ 10.x
- VDA
- (Remote PC Access の場合、オプション): Microsoft Exchange Server

スマートカードの使用を有効にする

ステップ 1. カード発行ポリシーに従って、ユーザーにスマートカードを発行します。

ステップ 2. (オプション) ユーザーがRemote PC Access を利用できるようにスマートカードを設定します。

ステップ 3. スマートカードのリモート処理のために、Delivery Controller と StoreFront (まだインストールされていない場合) をインストールして構成します。

ステップ 4. スマートカードの使用のためにStoreFront を有効にします。詳細については、StoreFront ドキュメントの「スマートカード認証の構成」を参照してください。

ステップ 5. スマートカードの使用のためにCitrix Gateway/Access Gateway を有効にします。詳細については、NetScaler ドキュメントの「認証と承認の構成」および「Web Interface を使用したスマートカードアクセスの構成」を参照してください。

ステップ 6. スマートカードの使用のためにVDA を有効にします。

- VDA に必要なアプリケーションと更新プログラムがあることを確認します。
- ミドルウェアをインストールします。
- スマートカードのリモート処理を設定し、ユーザーデバイス上のCitrix Workspace アプリと仮想デスクトップセッション間のスマートカードデータの通信を有効にします。

ステップ 7. ユーザーデバイス (ドメイン参加済みまたは非ドメイン参加済みマシンを含む) でスマートカードの使用を有効にします。詳細については、StoreFront ドキュメントの「スマートカード認証の構成」を参照してください。

- 証明機関のルート証明書と発行証明機関の証明書をデバイスのキーストアにインポートします。
- ベンダーのスマートカードミドルウェアをインストールします。

- Windows 用Citrix Workspace アプリをインストールして構成します。その際、グループポリシー管理コンソールを使用してicaclient.adm をインポートし、スマートカード認証を有効にしてください。

ステップ 8. 展開をテストします。テストユーザーのスマートカードを使用して仮想デスクトップを起動し、展開が正しく構成されていることを確認します。可能なすべてのアクセスメカニズム（たとえば、Internet Explorer および Citrix Workspace アプリを介したデスクトップへのアクセス）をテストします。

スマートカードリーダーの挿入回数を追跡する

スマートカードのリモート処理を使用すると、SCardGetStatusChange 関数を使用して、スマートカードがリーダーに挿入または取り外された回数を追跡できます。この関数は、監視するリーダーごとに 1 つの SCARD_READERSTATE データ構造の配列を更新します。各 SCARD_READERSTATE の dwEventState フィールドのハイワード（16 ビット）には、リーダーのカウントが含まれています。詳細については、Microsoft の記事 SCardGetStatusChangeA function および SCARD_READERSTATEA structure を参照してください。

リーダー挿入回数レポート設定は、デフォルトで無効になっています。追跡を有効にするには、次のレジストリキーを追加します。

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartCard

名前: EnableReaderInsertCountReporting

種類: DWORD

値: ゼロ以外の任意の値

セッションが切断されると、カウントはゼロにリセットされます。

リーダー挿入回数レポートは、サードパーティのスマートカードミドルウェアと互換性があります。

スマートカードの展開

この製品バージョンおよびこのバージョンを含む混在環境では、以下の種類のスマートカード展開がサポートされています。その他の構成も動作する可能性がありますが、サポートされていません。

タイプ	STOREFRONT™ 接続
ローカルのドメイン参加済みコンピューター	直接接続
ドメイン参加済みコンピューターからのリモートアクセス	Citrix Gateway 経由で接続
ドメインに参加していないコンピューター	直接接続
ドメインに参加していないコンピューターからのリモートアクセス	Citrix Gateway 経由で接続
ドメインに参加していないコンピューターおよびシンクライアントがDesktop Applianceサイトにアクセス	Desktop Applianceサイト経由で接続
XenApp® Services URL を介してStoreFrontにアクセスするドメイン参加済みコンピューターおよびシンクライアント	XenApp Services URL 経由で接続

展開タイプは、スマートカードリーダーが接続されているユーザーデバイスの特性によって定義されます。

- デバイスがドメイン参加済みか、非ドメイン参加済みか。
- デバイスがStoreFrontにどのように接続されているか。
- 仮想デスクトップとアプリケーションを表示するためにどのソフトウェアが使用されているか。

さらに、Microsoft WordやMicrosoft Excelなどのスマートカード対応アプリケーションをこれらの展開で使用できます。これらのアプリケーションを使用すると、ユーザーはドキュメントにデジタル署名したり、暗号化したりできます。

バイモーダル認証

これらの展開のそれぞれにおいて可能な場合、Receiverはスマートカードの使用とユーザー名およびパスワードの入力の選択肢をユーザーに提供することで、バイモーダル認証をサポートします。これは、スマートカードが使用できない場合（たとえば、ユーザーが自宅に忘れた場合やログオン証明書が期限切れになった場合）に役立ちます。

非ドメイン参加デバイスのユーザーはReceiver for Windowsに直接ログオンするため、ユーザーが明示的な認証にフォールバックできるようにすることができます。バイモーダル認証を構成する

と、ユーザーは最初にスマートカードとPINを使用してログオンするように求められますが、スマートカードに問題が発生した場合は明示的な認証を選択するオプションがあります。

Citrix Gatewayを展開する場合、ユーザーはデバイスにログオンし、Receiver for WindowsによってCitrix Gatewayへの認証を求められます。これは、ドメイン参加済みデバイスと非ドメイン参加済みデバイスの両方に適用されます。ユーザーは、スマートカードとPIN、または明示的な資格情報を使用してCitrix Gatewayにログオンできます。これにより、Citrix Gatewayログオンに対してバイモーダル認証をユーザーに提供できます。Citrix GatewayからStoreFrontへのパススルー認証を構成し、スマートカードユーザーの資格情報検証をCitrix Gatewayに委任することで、ユーザーはStoreFrontにサイレント認証されます。

複数のActive Directoryフォレストに関する考慮事項

Citrix環境では、スマートカードは単一のフォレスト内でサポートされます。フォレストをまたがるスマートカードログオンには、すべてのユーザーアカウントへの直接的な双方向フォレスト信頼が必要です。スマートカードを含むより複雑なマルチフォレスト展開（つまり、信頼が一方通行であるか、異なるタイプである場合）はサポートされていません。

リモートデスクトップを含むCitrix環境でスマートカードを使用できます。この機能は、ローカル（スマートカードが接続されているユーザーデバイス上）またはリモート（ユーザーデバイスが接続するリモートデスクトップ上）にインストールできます。

スマートカード取り外しポリシー

製品に設定されているスマートカード取り外しポリシーは、セッション中にリーダーからスマートカードを取り外した場合に何が起こるかを決定します。スマートカード取り外しポリシーは、Windowsオペレーティングシステムを介して構成および処理されます。

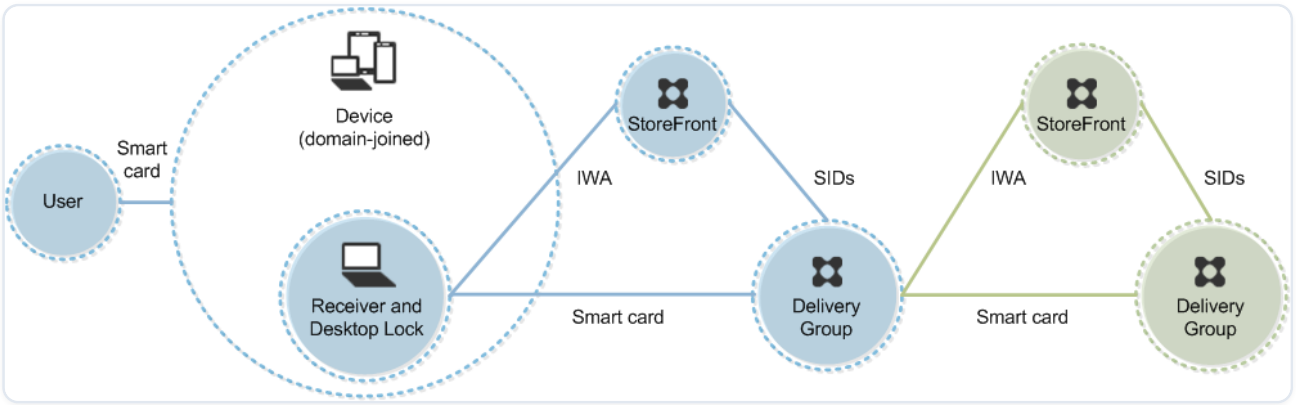
ポリシー設定	デスクトップの動作
何もしない	何もしない。
ワークステーションをロックする	デスクトップセッションが切断され、仮想デスクトップがロックされます。
強制ログオフ	ユーザーは強制的にログオフされます。ネットワーク接続が失われ、この設定が有効になっている場合、セッションがログオフされ、ユーザーはデータを失う可能性があります。
リモートターミナルサービスセッションの場合に切断する	セッションが切断され、仮想デスクトップがロックされます。

証明書失効チェック

証明書失効チェックが有効になっていて、ユーザーが無効な証明書を含むスマートカードをカードリーダーに挿入した場合、ユーザーは認証できず、その証明書に関連するデスクトップまたはアプリケーションにアクセスできません。たとえば、無効な証明書がメールの復号化に使用されている場合、メールは暗号化されたままになります。認証に使用されるものなど、カード上の他の証明書がまだ有効な場合、それらの機能はアクティブなままです。

展開例：ドメイン参加済みコンピューター

この展開では、Desktop Viewer を実行し、StoreFront に直接接続するドメイン参加済みユーザーデバイスを使用します。



ユーザーはスマートカードとPINを使用してデバイスにログオンします。Receiver は、統合Windows認証 (IWA) を使用してユーザーをStoreFrontサーバーに認証します。StoreFront は、ユーザーセキュリティ識別子 (SID) を Citrix Virtual Apps または Citrix Virtual Desktops に渡します。ユーザーが仮想デスクトップまたはアプリケーションを起動すると、Receiver でシングルサインオン機能が構成されているため、PIN の再入力を求められることはありません。

この展開は、2番目のStoreFrontサーバーとアプリケーションをホストするサーバーを追加することで、ダブルホップに拡張できます。仮想デスクトップからのReceiver は、2番目のStoreFrontサーバーに認証します。この2番目の接続には、任意の認証方法を使用できます。最初のホップで示された構成は、2番目のホップで再利用することも、2番目のホップでのみ使用することもできます。

展開例: ドメイン参加済みコンピューターからのリモートアクセス

この展開では、Desktop Viewer を実行し、Citrix Gateway/Access Gateway を介して StoreFront に接続するドメイン参加済みユーザーデバイスが関与します。

展開例: ドメイン参加済みコンピューターからのリモートアクセス(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/smartcard2_1.png)

ユーザーはスマートカードとPINを使用してデバイスにログオンし、その後Citrix Gateway/Access Gatewayに再度ログオンします。この2回目のログオンは、Receiverがこの展開でバイモーダル認証を許可しているため、スマートカードとPIN、またはユーザー名とパスワードのいずれかで行うことができます。

ユーザーはStoreFrontに自動的にログオンし、StoreFrontはユーザーセキュリティ識別子（SID）をCitrix Virtual Apps™またはCitrix Virtual Desktopsに渡します。ユーザーが仮想デスクトップまたはアプリケーションを起動しても、Receiverでシングルサインオン機能が構成されているため、PINの再入力を求められることはありません。

この展開は、2台目のStoreFrontサーバーとアプリケーションをホストするサーバーを追加することで、ダブルホップに拡張できます。仮想デスクトップからのReceiverは、2台目のStoreFrontサーバーに対して認証を行います。この2番目の接続には、任意の認証方法を使用できます。最初のホップで示された構成は、2番目のホップで再利用することも、2番目のホップでのみ使用することもできます。

展開例: ドメイン非参加コンピューター

この展開では、Desktop Viewer を実行し、StoreFront に直接接続するドメイン非参加ユーザーデバイスが関与します。

展開例: ドメイン非参加コンピューター(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/smartcard3_1.png)

ユーザーはデバイスにログオンします。通常、ユーザーはユーザー名とパスワードを入力しますが、デバイスがドメインに参加していないため、このログオンの資格情報はオプションです。この展開ではバイモーダル認証が可能であるため、Receiverはユーザーにスマートカードと PIN、またはユーザー名とパスワードのいずれかを要求します。その後、ReceiverはStorefrontに対して認証を行います。

StoreFrontはユーザーセキュリティ識別子（SID）をCitrix Virtual AppsまたはCitrix Virtual Desktopsに渡します。ユーザーが仮想デスクトップまたはアプリケーションを起動すると、この展開ではシングルサインオン機能が利用できないため、PINの再入力を求められます。

この展開は、2台目のStoreFrontサーバーとアプリケーションをホストするサーバーを追加することで、ダブルホップに拡張できます。仮想デスクトップからのReceiverは、2台目のStoreFrontサーバーに対して認証を行います。この2番目の接続には、任意の認証方法を使用できます。最初のホップで示された構成は、2番目のホップで再利用することも、2番目のホップでのみ使用することもできます。

展開例: ドメイン非参加コンピューターからのリモートアクセス

この展開では、Desktop Viewer を実行し、StoreFront に直接接続するドメイン非参加ユーザーデバイスが関与します。

展開例: ドメイン非参加コンピューターからのリモートアクセス(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/smartcard4_1.png)

ユーザーがデバイスにログオンします。通常、ユーザーはユーザー名とパスワードを入力しますが、デバイスがドメインに参加していないため、このログオンの資格情報はオプションです。この展開ではバイモーダル認証が可能なため、ReceiverはスマートカードとPIN、またはユーザー名とパスワードのいずれかをユーザーに要求します。その後、ReceiverはStorefrontに対して認証を行います。

StoreFrontはユーザーセキュリティ識別子（SID）をCitrix Virtual AppsまたはCitrix Virtual Desktopsに渡します。ユーザーが仮想デスクトップまたはアプリケーションを起動すると、この展開ではシングルサインオン機能が利用できないため、ユーザーは再度PINを要求されます。

この展開は、2番目のStoreFrontサーバーとアプリケーションをホストするサーバーを追加することで、ダブルホップに拡張できます。仮想デスクトップからのReceiverは、2番目のStoreFrontサーバーに対して認証を行います。この2番目の接続には、任意の認証方法を使用できます。最初のホップに示されている構成は、2番目のホップで再利用することも、2番目のホップでのみ使用することもできます。

展開例：ドメインに参加していないコンピューターとシンクライアントがDesktop Applianceサイトにアクセスする場合

この展開には、Desktop Lockを実行し、Desktop Applianceサイトを介してStoreFrontに接続する可能性のある、ドメインに参加していないユーザーデバイスが含まれます。

Desktop Lockは、Citrix Virtual Apps、Citrix Virtual Desktops、およびVDI-in-a-Boxとともにリリースされる個別のコンポーネントです。これはDesktop Viewerの代替であり、主に再利用されたWindowsコンピューターとWindowsシンクライアント向けに設計されています。Desktop Lockは、これらのユーザーデバイスのWindowsシェルとタスクマネージャーを置き換え、ユーザーが基盤となるデバイスにアクセスするのを防ぎます。Desktop Lockを使用すると、ユーザーはWindows Server MachineデスクトップとWindows Desktop Machineデスクトップにアクセスできます。Desktop Lockのインストールはオプションです。

展開例：ドメインに参加していないコンピューターとシンクライアントがDesktop Applianceサイトにアクセスする場合(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/smartcard5_1.png)

ユーザーはスマートカードを使用してデバイスにログオンします。デバイスでDesktop Lockが実行されている場合、デバイスはキオスクモードで実行されているInternet Explorerを介してDesktop Applianceサイトを起動するように構成されています。サイト上のActiveXコントロールがユーザーにPINを要求し、それをStoreFrontに送信します。StoreFrontはユーザーセキュリティ識別子（SID）をCitrix Virtual AppsまたはCitrix Virtual Desktopsに渡します。割り当てられたデスクトップグループのアルファベット順リストで最初に利用可能なデスクトップが起動します。

この展開は、2番目のStoreFrontサーバーとアプリケーションをホストするサーバーを追加することで、ダブルホップに拡張できます。仮想デスクトップからのReceiverは、2番目のStoreFrontサーバーに対して認証を行います。この2番目の接続には、任意の認証方法を使用できます。最初のホップに示されている構成は、2番目のホップで再利用することも、2番目のホップでのみ使用することもできます。

展開例：ドメインに参加しているコンピューターとシンクライアントがXenApp Services URLを介してStoreFrontにアクセスする場合

この展開には、Desktop Lockを実行し、XenApp Services URLを介してStoreFrontに接続するドメインに参加しているユーザーデバイスが含まれます。

Desktop Lockは、Citrix Virtual Apps、Citrix Virtual Desktops、およびVDI-in-a-Boxとともにリリースされる個別のコンポーネントです。これはDesktop Viewerの代替であり、主に再利用されたWindowsコンピューターとWindowsシンクライアント向けに設計されています。Desktop Lockは、これらのユーザーデバイスのWindowsシェルとタスクマネージャーを置き換え、ユーザーが基盤となるデバイスにアクセスするのを防ぎます。Desktop Lockを使用すると、ユーザーはWindows Server MachineデスクトップとWindows Desktop Machineデスクトップにアクセスできます。Desktop Lockのインストールはオプションです。

展開例：ドメインに参加しているコンピューターとシンクライアントがXenApp Services URLを介してStoreFrontにアクセスする場合(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/smartcard6.png)

ユーザーはスマートカードとPINを使用してデバイスにログオンします。デバイスでDesktop Lockが実行されている場合、統合Windows認証（IWA）を使用してユーザーをStorefrontサーバーに認証します。StoreFrontはユーザーセキュリティ識別子（SID）をCitrix Virtual AppsまたはCitrix Virtual Desktopsに渡します。ユーザーが仮想デスクトップを起動すると、Receiverでシングルサインオン機能が構成されているため、ユーザーは再度PINを要求されません。

この展開は、2番目のStoreFrontサーバーとアプリケーションをホストするサーバーを追加することで、ダブルホップに拡張できます。仮想デスクトップからのReceiverは、2番目のStoreFrontサーバーに対して認証を行います。この2番目の接続には、任意の認証方法を使用できます。最初

のホップに示されている構成は、2番目のホップで再利用することも、2番目のホップでのみ使用することもできます。

スマートカードによるパススルー認証とシングルサインオン

パススルー認証

スマートカードによる仮想デスクトップへのパススルー認証は、Windows 10、Windows 8、Windows 7 SP1 EnterpriseおよびProfessional Editionを実行しているユーザーデバイスでサポートされています。

スマートカードによるホストされたアプリケーションへのパススルー認証は、Windows Server 2016、Windows Server 2012 R2、Windows Server 2012、および Windows Server 2008 R2 SP1 を実行しているサーバーでサポートされています。

スマートカードホスト型アプリケーションでパススルー認証を使用するには、サイトの認証方法としてスマートカードによるパススルーを構成する際に、Kerberosの使用を有効にしてください。

注：スマートカードによるパススルー認証の利用可能性は、以下を含む（ただしこれらに限定されない）多くの要因に依存します。

- パススルー認証に関する組織のセキュリティポリシー。
- ミドルウェアの種類と構成。
- スマートカードリーダーの種類。
- ミドルウェアのPINキャッシュポリシー。

スマートカードによるパススルー認証はCitrix StoreFrontで構成されます。詳細については、StoreFrontのドキュメントを参照してください。

シングルサインオン

シングルサインオンは、仮想デスクトップおよびアプリケーションの起動時にパススルー認証を実装するCitrixの機能です。この機能は、ドメイン参加済み、StoreFrontへの直接接続、およびドメイン参加済み、NetScalerからStoreFrontへのスマートカード展開で使用でき、ユーザーがPINを入力する回数を減らすことができます。これらの展開タイプでシングルサインオンを使用するには、StoreFrontサーバーにあるdefault.icaファイルで以下のパラメーターを編集します。

- ドメイン参加済み、StoreFrontへの直接接続スマートカード展開 — DisableCtrlAltDelをOffに設定

- ドメイン参加済み、NetScalerからStoreFrontへのスマートカード展開 — UseLocalUserAndPasswordをOnに設定

これらのパラメーターの設定に関する詳細な手順については、StoreFrontまたはCitrix Gatewayのドキュメントを参照してください。

シングルサインオン機能の利用可否は、以下を含む多くの要因に依存します（ただし、これらに限定されません）。

- シングルサインオンに関する組織のセキュリティポリシー。
- ミドルウェアの種類と構成。
- スマートカードリーダーの種類。
- ミドルウェアのPINキャッシュポリシー。

> **注：**
>
> ユーザーがスマートカードリーダーが接続されたマシン上のVirtual Delivery Agent (VDA) にログオンすると、スマートカードやパスワードなど、以前に成功した認証モードを表すWindowsタイルが表示されることがあります。その結果、シングルサインオンが有効になっている場合、シングルサインオンタイルが表示されることがあります。ログオンするには、シングルサインオンタイルは機能しないため、ユーザーは別のタイルを選択するために**ユーザーの切り替え**を選択する必要があります。

トランスポート層セキュリティ (TLS)

Citrix Virtual Apps and Desktops は、コンポーネント間の TCP ベースの接続にトランスポート層セキュリティ (TLS) プロトコルをサポートしています。Citrix Virtual Apps and Desktops は、(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/hdx-transport/adaptive-transport.html) を使用した UDP ベースの ICA/HDX 接続にデータグラムトランスポート層セキュリティ (DTLS) プロトコルもサポートしています。

TLS と DTLS は類似しており、同じデジタル証明書をサポートしています。Citrix Virtual Apps または Citrix Virtual Desktops™ サイトを TLS を使用するように構成すると、DTLS を使用するようにも構成されます。以下の手順を使用してください。特に記載がない限り、手順は TLS と DTLS の両方に共通です。

- すべての Delivery Controller でサーバー証明書を取得、インストール、登録し、TLS 証明書でポートを構成します。詳細については、「Controller に TLS サーバー証明書をインストールする」を参照してください。

  オプションで、Controller が HTTP および HTTPS トラフィックをリッスンするために使用するポートを変更できます。

- 次のタスクを完了して、Citrix Workspace™ アプリと Virtual Delivery Agent (VDA) 間の TLS 接続を有効にします。

  - VDA がインストールされているマシンで TLS を構成します。(便宜上、VDA がインストールされているマシンは、以降「VDA」と表記します。) 一般的な情報については、「VDA の TLS 設定」を参照してください。TLS/DTLS の構成には、Citrix が提供する PowerShell スクリプトを使用することを強くお勧めします。詳細については、「PowerShell スクリプトを使用して VDA で TLS を構成する」を参照してください。ただし、TLS/DTLS を手動で構成する場合は、「VDA で TLS を手動で構成する」を参照してください。
  - Studio で一連の PowerShell コマンドレットを実行して、VDA を含むデリバリーグループで TLS を構成します。詳細については、「デリバリーグループで TLS を構成する」を参照してください。

    要件と考慮事項:

    - ユーザーと VDA 間の TLS 接続の有効化は、XenApp 7.6 および XenDesktop 7.6 サイト、およびそれ以降のサポート対象リリースでのみ有効です。
    - コンポーネントのインストール、サイトの作成、マシンカタログの作成、およびデリバリーグループの作成後に、デリバリーグループと VDA で TLS を構成します。
    - デリバリーグループで TLS を構成するには、Controller アクセスルールを変更する権限が必要です。フル管理者にはこの権限があります。
    - VDA で TLS を構成するには、VDA がインストールされているマシンで Windows 管理者である必要があります。
    - Machine Creation Services™ または Provisioning Services によってプロビジョニングされたプールされた VDA では、再起動時に VDA マシンイメージがリセットされ、以前の TLS 設定が失われます。VDA が再起動されるたびに PowerShell スクリプトを実行して、TLS 設定を再構成してください。

警告:

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

> サイトデータベースへの TLS の有効化については、「CTX137556」を参照してください。

コントローラーにTLSサーバー証明書をインストールする

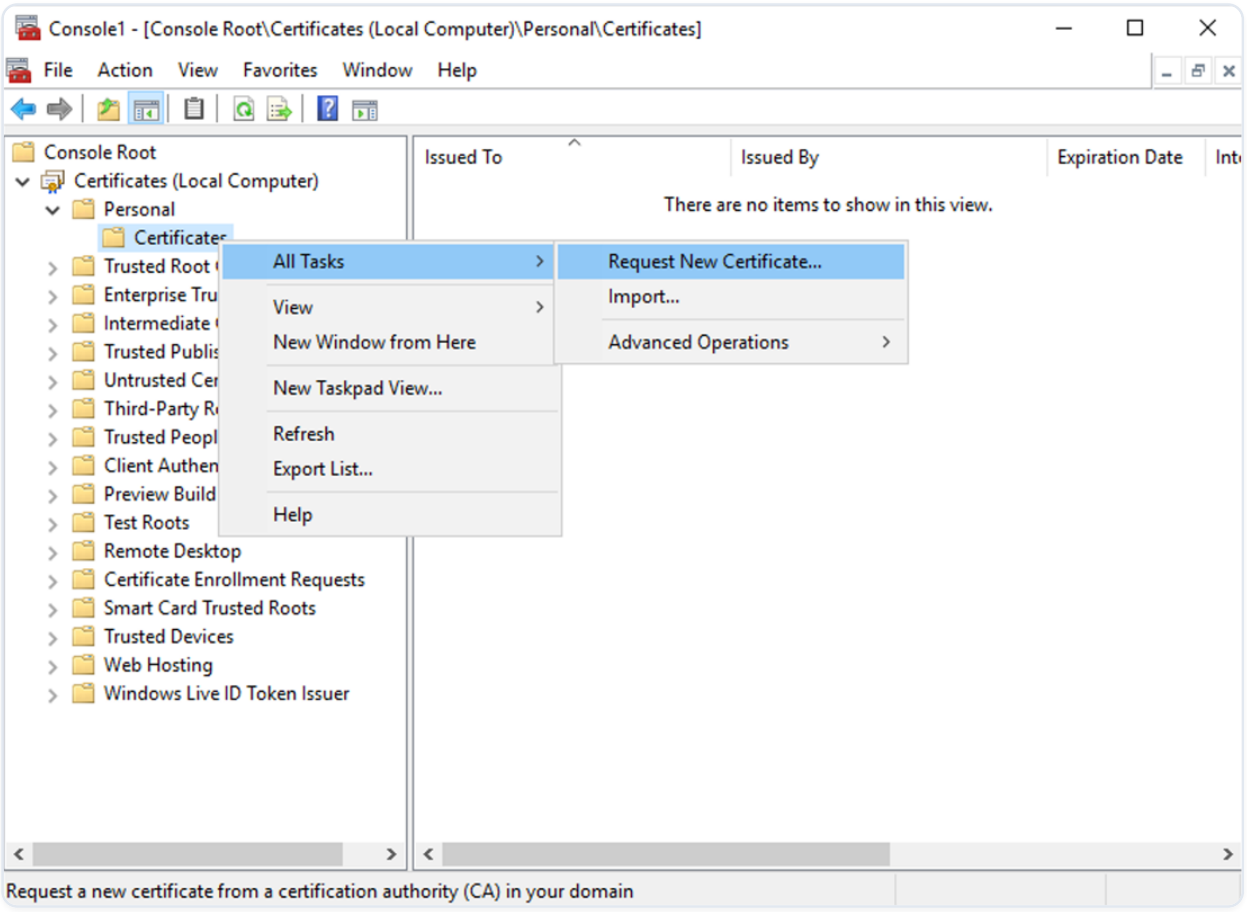
HTTPSの場合、XMLサービスはクライアント証明書ではなくサーバー証明書を使用してTLS機能をサポートします。このセクションでは、Delivery ControllerでのTLS証明書の取得とインストールについて説明します。同じ手順をCloud Connectorに適用して、STAおよびXMLトラフィックを暗号化できます。

さまざまな種類の証明機関と、そこから証明書を要求する方法がありますが、この記事ではMicrosoft証明機関について説明します。Microsoft証明機関は、サーバー認証の目的で公開された証明書テンプレートを持っている必要があります。

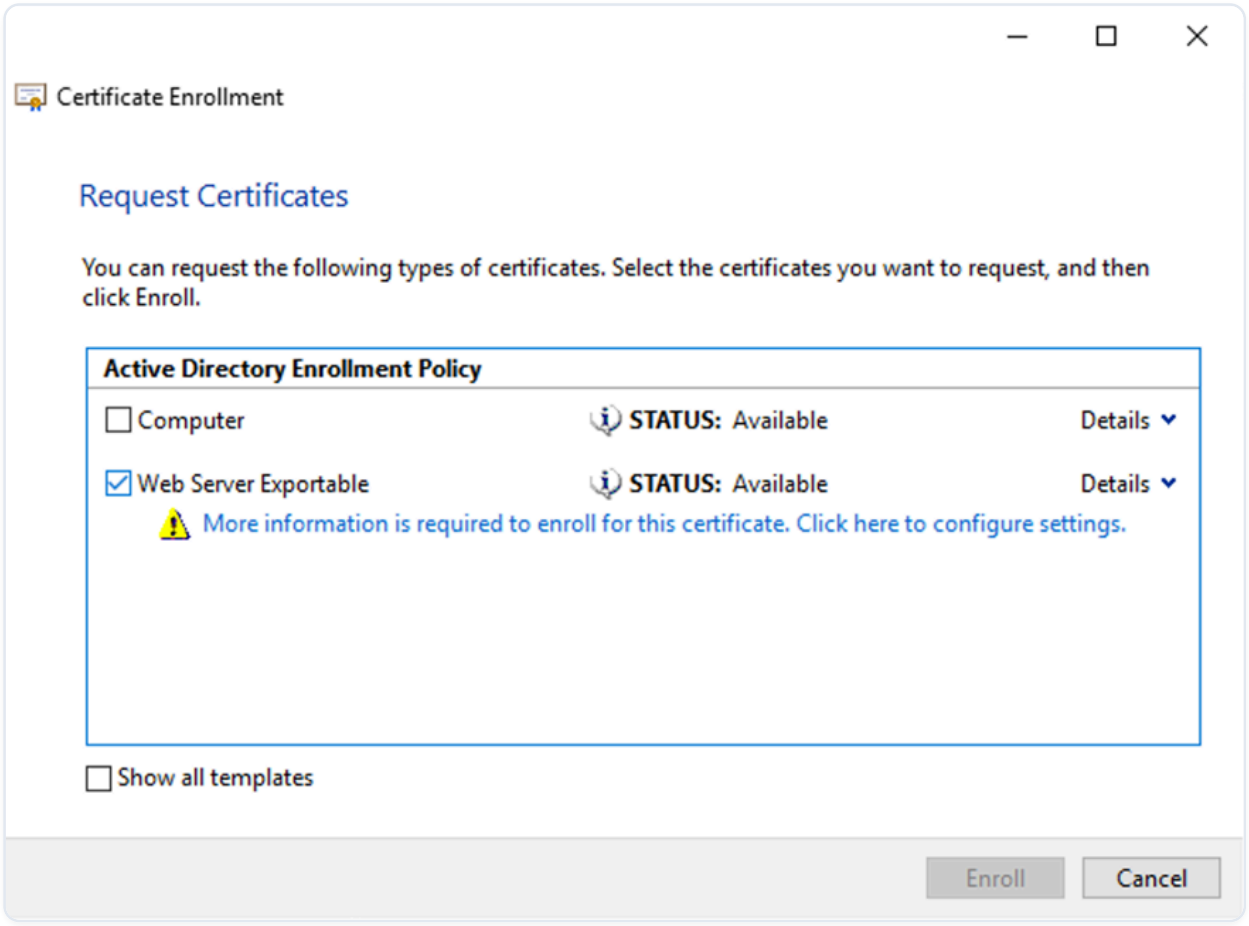
Microsoft証明機関がActive Directoryドメイン、またはDelivery Controllerが参加している信頼されたフォレストに統合されている場合、証明書MMCスナップインの証明書登録ウィザードから証明書を取得できます。

証明書の要求とインストール

1. Delivery Controller™で、MMCコンソールを開き、証明書スナップインを追加します。プロンプトが表示されたら、コンピューターアカウントを選択します。
2. **個人 > 証明書**を展開し、**すべてのタスク > 新しい証明書の要求**コンテキストメニューコマンドを使用します。



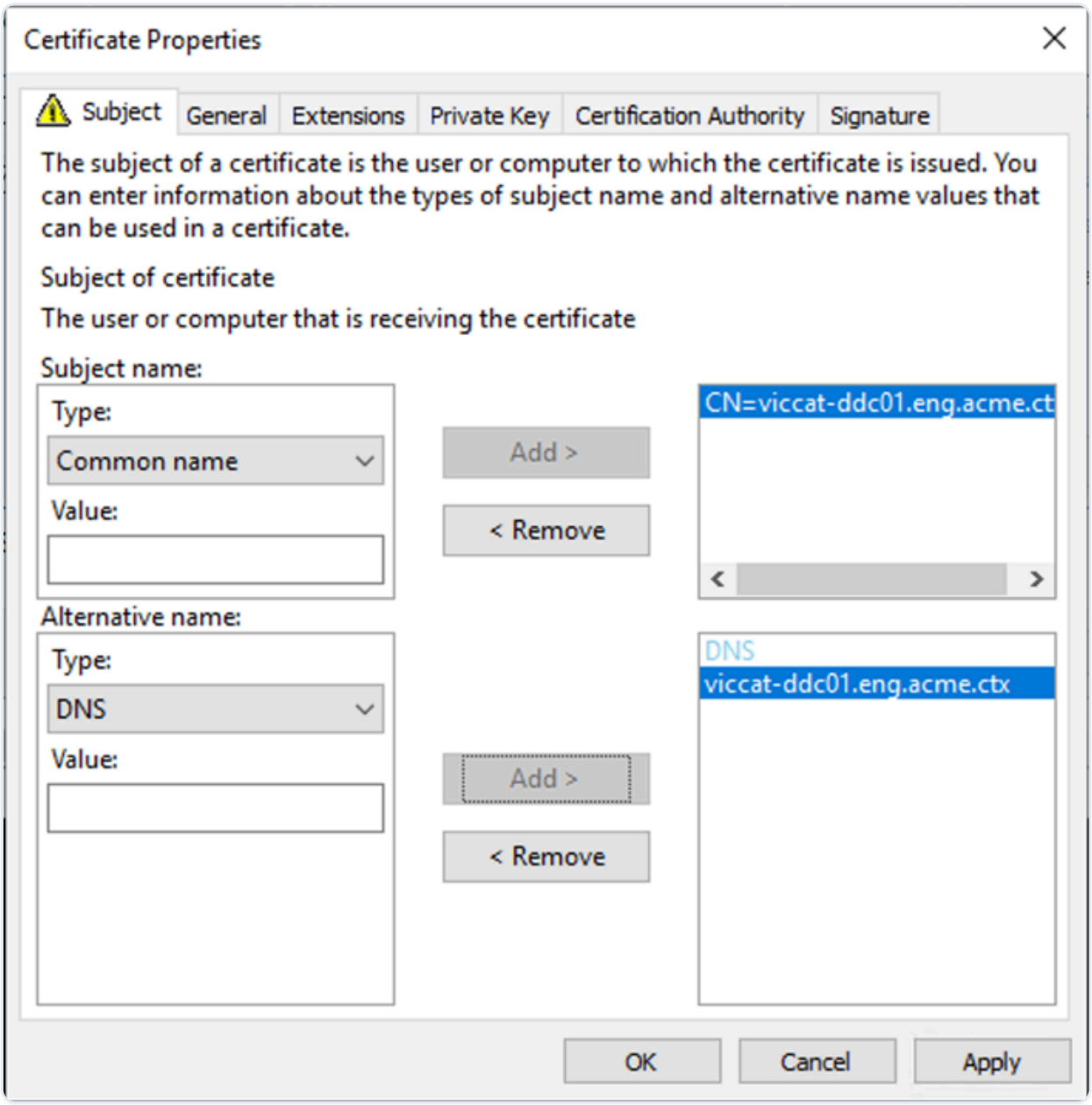
3. 開始するには**次へ**をクリックし、Active Directory登録から証明書を取得することを確認するには**次へ**をクリックします。
4. サーバー認証証明書のテンプレートを選択します。テンプレートがSubjectの値を自動的に提供するように設定されている場合は、詳細を指定せずに**Enroll**をクリックできます。



5. 証明書テンプレートの詳細を指定するには、**詳細**矢印ボタンをクリックして、以下を構成します。

   Subject name: Common Nameを選択し、Delivery ControllerのFQDNを追加します。

   Alternative name: DNSを選択し、Delivery ControllerのFQDNを追加します。



SSL/TLSリスナーポートの構成

1. マシンの管理者としてPowerShellコマンドウィンドウを開きます。
2. Broker ServiceアプリケーションGUIDを取得するには、次のコマンドを実行します。

```
New-PSDrive -Name HKCR -PSProvider Registry -Root HKEY_CLASSES_ROOT



$Service_Guid = Get-ChildItem HKCR:\Installer\Products -Recurse -Ea 0 |
Where-Object { $key = $_; $_.GetValueNames() | ForEach-Object
{ $key.GetValue($_) } | Where-Object { $_ -like 'Citrix Broker
Service' } } | Select-Object Name
```

```
$Service_Guid.Name -match "[A-Z0-9]*$"

$Guid = $Matches[0]

[GUID]$Formatted_Guid = $Guid

Remove-PSDrive -Name HKCR

Write-Host "Broker Service Application GUID: $($Formatted_Guid)"
-ForegroundColor Yellow
```

3. 以前にインストールした証明書のサムプリントを取得するには、同じPowerShellウィンドウで次のコマンドを実行します。

```
$HostName =
([System.Net.Dns]::GetHostByName(($env:computerName))).Hostname

$Thumbprint = (Get-ChildItem -Path Cert:\LocalMachine\My | Where-Object
{$_.Subject -match ("CN=" + $HostName)}).Thumbprint -join ';'

Write-Host -Object "Certificate Thumbprint for $($HostName): $
($Thumbprint)" -Foreground Yellow
```

4. 同じPowerShellウィンドウで、Broker ServiceのSSL/TLSポートを構成し、暗号化に証明書を使用するために、次のコマンドを実行します。

```
$IPV4_Address = Test-Connection -ComputerName $HostName -Count 1  |
Select-Object -ExpandProperty IPV4Address



$IPPort = "$($IPV4_Address):443"



$SSLxml = "http add sslcert ipport=$IPPort certhash=$Thumbprint
appid={$Formatted_Guid}"



$SSLxml | netsh



. netsh http show sslcert
```

正しく構成されている場合、最後のコマンド `.netsh http show sslcert` の出力は、リスナーが正しい `IP:port` を使用しており、`Application ID` がBroker Serviceアプリケーション GUIDと一致していることを示します。

サーバーがDelivery Controllerにインストールされている証明書を信頼している場合、StoreFront™ Delivery ControllerおよびCitrix Gateway STAバインディングをHTTPではなくHTTPSを使用するように構成できます。

注：

ControllerがWindows Server 2016にインストールされており、StoreFrontがWindows Server 2012 R2にインストールされている場合、TLS暗号スイートの順序を変更するためにControllerで構成変更が必要です。この構成変更は、他のWindows Serverバージョンの組み合わせのControllerとStoreFrontでは必要ありません。

暗号スイートの順序リストには、`TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384` または `TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256` の暗号スイート（またはその両方）を含める

> 必要があります。また、これらの暗号スイートは、`TLS_DHE_` の暗号スイートよりも前に配置する必要があります。

1. Microsoftグループポリシーエディターを使用して、**コンピューターの構成 > 管理用テンプレート > ネットワーク > SSL構成設定** に移動します。
2. 「SSL暗号スイートの順序」ポリシーを編集します。デフォルトでは、このポリシーは「未構成」に設定されています。このポリシーを「有効」に設定します。
3. スイートを正しい順序に並べ替えます。使用したくない暗号スイートは削除します。

`TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384` または `TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256` のいずれかが、`TLS_DHE_` の暗号スイートよりも前に配置されていることを確認してください。

Microsoft MSDNで、「Schannel暗号スイートの優先順位付け」も参照してください。

HTTPまたはHTTPSポートの変更

デフォルトでは、Controller 上の XML Service は、HTTP トラフィックにはポート 80 を、HTTPS トラフィックにはポート 443 をリッスンします。デフォルト以外のポートを使用することもできますが、Controller を信頼できないネットワークに公開することによるセキュリティリスクに注意してください。デフォルトを変更するよりも、スタンドアロンの StoreFront サーバーを展開する方が望ましいです。

Controller で使用されるデフォルトの HTTP または HTTPS ポートを変更するには、Studio から次のコマンドを実行します。

```
BrokerService.exe -WIPORT \<http-port> -WISSLPORT \<https-port>
```

ここで、`<http-port>` は HTTP トラフィックのポート番号、`<https-port>` は HTTPS トラフィックのポート番号です。

> **注：**
>
> ポートを変更した後、Studio はライセンスの互換性とアップグレードに関するメッセージを表示する場合があります。この問題を解決するには、次の PowerShell コマンドレットシーケンスを使用してサービスインスタンスを再登録します。

```
Get-ConfigRegisteredServiceInstance -ServiceType Broker -Binding XML_HTTPS
|

Unregister-ConfigRegisteredServiceInstance

Get-BrokerServiceInstance | where Binding -eq "XML_HTTPS" |

Register-ConfigServiceInstance
```

HTTPS トラフィックのみを強制する

XML Service で HTTP トラフィックを無視させたい場合は、Controller 上の HKLM\Software\Citrix\DesktopServer\ に次のレジストリ設定を作成し、Broker Service を再起動します。

HTTP トラフィックを無視するには、DWORD XmlServicesEnableNonSsl を作成し、0 に設定します。

HTTPS トラフィックを無視するために作成できる対応するレジストリ DWORD 値があります: DWORD XmlServicesEnableSsl。これが 0 に設定されていないことを確認してください。

VDA 上の TLS 設定

デリバリーグループには、TLS が構成されている VDA と TLS が構成されていない VDA が混在することはできません。デリバリーグループに TLS を構成する前に、そのデリバリーグループ内のすべての VDA に TLS が構成されていることを確認してください。

VDA で TLS を構成すると、インストールされている TLS 証明書のアクセス許可が変更され、ICA® Service に証明書の秘密キーへの読み取りアクセス権が付与され、ICA Service に次の情報が通知されます。

- **TLS に使用する証明書ストア内の証明書。**
- **TLS 接続に使用する TCP ポート番号。**

  Windows ファイアウォール（有効な場合）は、この TCP ポートでの受信接続を許可するように構成する必要があります。この構成は、PowerShell スクリプトを使用すると自動的に行われます。
- **許可する TLS プロトコルのバージョン。**

> **重要:**

> Citrix は、SSLv3 の使用状況を確認し、必要に応じて SSLv3 のサポートを削除するように展開を再構成することを推奨します。CTX200238を参照してください。

> サポートされている TLS プロトコルバージョンは、階層（最低から最高）に従います: SSL 3.0、TLS 1.0、TLS 1.1、TLS 1.2、および TLS 1.3。許可される最小バージョンを指定します。そのバージョンまたはそれより高いバージョンを使用するすべてのプロトコル接続が許可されます。

たとえば、TLS 1.1 を最小バージョンとして指定した場合、TLS 1.1 および TLS 1.3 プロトコル接続が許可されます。SSL 3.0 を最小バージョンとして指定した場合、サポートされているすべてのバージョンの接続が許可されます。TLS 1.3 を最小バージョンとして指定した場合、TLS 1.3 接続のみが許可されます。

DTLS 1.0 は TLS 1.1 に対応し、DTLS 1.3 は TLS 1.3 に対応します。

- **許可する TLS 暗号スイート。**

  暗号スイートは、接続に使用される暗号化を選択します。クライアントと VDA は、異なる暗号スイートのセットをサポートできます。クライアント（Citrix Workspace アプリまたは StoreFront）が接続し、サポートされている TLS 暗号スイートのリストを送信すると、VDA はクライアントの暗号スイートのいずれかを、自身の構成済み暗号スイートのリストにある暗号スイートのいずれかと照合し、接続を受け入れます。一致する暗号スイートがない場合、VDA は接続を拒否します。

  VDA は、3 つの暗号スイートセット（コンプライアンスモードとも呼ばれます）をサポートしています: GOV（政府）、COM（商用）、および ALL。許容される暗号スイートは、Windows FIPS モードにも依存します。Windows FIPS モードの詳細については、`<http://support.microsoft.com/kb/811833>` を参照してください。次の表に、各セットの暗号スイートを示します。

TLS/DTLS 暗号スイート	ALL	COM	GOV	ALL	COM	GOV
FIPS モード	オフ	オフ	オフ	オン	オン	オン
TLS_ECDHE_RSA_WITH_AES_256_	X		X	X		X

TLS/DTLS 暗号スイート	ALL	COM	GOV	ALL	COM	GOV
GCM_SHA384*						
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	X		X	X		X
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	X	X		X	X	

Windows Server 2012 R2ではサポートされていません。

注：

VDAはDHE暗号スイート（例：TLS_DHE_RSA_WITH_AES_256_GCM_SHA384、TLS_DHE_RSA_WITH_AES_256_CBC_SHA、TLS_DHE_RSA_WITH_AES_128_GCM_SHA256、TLS_DHE_RSA_WITH_AES_128_CBC_SHA）をサポートしていません。Windowsによって選択された場合でも、Receiverでは使用できない場合があります。

Citrix Gatewayを使用している場合は、バックエンド通信の暗号スイートサポートに関する情報について、Citrix ADCのドキュメントを参照してください。TLS暗号スイートのサポートについては、「Citrix ADCアプライアンスで利用可能な暗号」を参照してください。DTLS暗号スイートのサポートについては、「DTLS暗号のサポート」を参照してください。

証明書を要求してインストールする

1. VDAで、MMCコンソールを開き、証明書スナップインを追加します。プロンプトが表示されたら、コンピューターアカウントを選択します。

2. **個人 > 証明書**を展開し、コンテキストメニューコマンド**すべてのタスク > 新しい証明書の要求**を使用します。
3. 「**次へ**」をクリックして開始し、Active Directory登録から証明書を取得することを確認するために「**次へ**」をクリックします。
4. サーバー認証証明書のテンプレートを選択します。デフォルトのWindows **Computer**または**Web Server Exportable**のどちらも使用できます。テンプレートがSubjectの値を自動的に提供するように設定されている場合は、詳細情報を提供せずに「**登録**」をクリックできます。

   「証明書を要求」ダイアログ(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/tls-request-certificates.png)
5. 証明書テンプレートの詳細情報を提供するには、「**詳細**」をクリックして、以下を構成します。

   サブジェクト名 — 種類を「**共通名**」に選択し、VDAのFQDNを追加します

   代替名 — 種類を「**DNS**」に選択し、VDAのFQDNを追加します

   証明書のプロパティ(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/tls-certificate-properties.png)

   > **注：**
   >
   > Active Directory証明書サービス証明書の自動登録を使用して、VDAへの証明書の発行と展開を自動化します。これについては、`<https://support.citrix.com/article/CTX205473>`で説明されています。

   > ワイルドカード証明書を使用して、単一の証明書で複数のVDAを保護できます。

   サブジェクト名 — 種類を「**共通名**」に選択し、VDAの*.primary.domainを入力します

   代替名 — 種類を「**DNS**」に選択し、VDAの*.primary.domainを追加します

   ワイルドカード証明書要求ダイアログ(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/tls-request-certificates-wildcard.png)

   SAN証明書を使用して、単一の証明書で複数の特定のVDAを保護できます。

   サブジェクト名 — 種類を「**共通名**」に選択し、証明書の使用状況を識別するのに役立つ文字列を入力します

代替名 — 種類を「**DNS**」に選択し、各VDAのFQDNのエントリを追加します。最適なTLSネゴシエーションを確保するために、代替名の数を最小限に抑えてください。

「証明書を要求」ダイアログ(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/tls-request-certificates-san.png)

> **注：**
>
> ワイルドカード証明書とSAN証明書の両方で、タブの**秘密キーをエクスポート可能にする**が選択されている必要があります。

> 「証明書を要求」ダイアログ(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/tls-certificate-properties-private-key.png)

PowerShellスクリプトを使用してVDAでTLSを構成する

証明書ストアの > > 領域にTLS証明書をインストールします。その場所に複数の証明書がある場合は、証明書のサムプリントをPowerShellスクリプトに指定します。

> **注：**
>
> XenApp and XenDesktop 7.16 LTSR以降、PowerShellスクリプトはVDAのFQDNに基づいて正しい証明書を検索します。VDAのFQDNに対して単一の証明書のみが存在する場合、サムプリントを指定する必要はありません。

> Enable-VdaSSL.ps1スクリプトは、VDA上のTLSリスナーを有効または無効にします。このスクリプトは、インストールメディアの*Support* > *Tools* > *SslSupport*フォルダーにあります。

TLSを有効にすると、DHE暗号スイートは無効になります。ECDHE暗号スイートは影響を受けません。

TLSを有効にすると、スクリプトは指定されたTCPポートの既存のWindowsファイアウォール規則をすべて無効にします。その後、ICAサービスがTLS TCPポートとUDPポートでのみ受信接続を受け入れることを許可する新しい規則を追加します。また、次のWindowsファイアウォール規則も無効にします。

- Citrix ICA（デフォルト：1494）

- Citrix CGP（デフォルト：2598）
- Citrix WebSocket（デフォルト：8008）

その結果、ユーザーはTLSまたはDTLSを使用してのみ接続できます。TLSまたはDTLSなしでは、ICA/HDX、セッションの信頼性を備えたICA/HDX、またはWebSocket経由のHDXを使用できません。

> **注：**
>
> DTLSは、UDPリアルタイムトランスポート経由のICA/HDXオーディオ、またはICA/HDX Framehawkではサポートされていません。

> ネットワークポートを参照してください。

スクリプトには、以下の構文の説明と追加の例が含まれています。この情報はNotepad++などのツールを使用して確認できます。

> **重要:**
>
> EnableまたはDisableパラメーターと、CertificateThumbPrintパラメーターのいずれかを指定します。その他のパラメーターはオプションです。

構文

```
Enable-VdaSSL {-Enable | -Disable} -CertificateThumbPrint "<thumbprint>" [-SSLPort <port>] [-SSLMinVersion "<min-ssl-version>"] [-SSLCipherSuite"\<suite>"]
```

パラメーター	説明
有効にする	VDAにTLSリスナーをインストールして有効にします。このパラメーターまたはDisableパラメーターのいずれかが必要です。
無効にする	VDA上のTLSリスナーを無効にします。このパラメーターまたはEnableパラメーターのいずれかが必要です。このパラメーターを指定した場合、他のパラメーターは無効になります。

パラメーター	説明
証明書のサムプリント "<thumbprint>"	証明書ストア内のTLS証明書のサムプリントを引用符で囲んで指定します。スクリプトは指定されたサムプリントを使用して、使用する証明書を選択します。このパラメーターを省略すると、誤った証明書が選択されます。
SSLポート <port>	TLSポート。デフォルト: 443
SSLMinVersion "<バージョン>"	引用符で囲まれた最小TLSプロトコルバージョン。有効な値: “TLS_1.0”（デフォルト）、“TLS_1.1”、および“TLS_1.3”。
SSLCipherSuite "<スイート>"	TLS暗号スイート。引用符で囲みます。有効な値: "GOV"、"COM"、および "ALL" (デフォルト)。

例

次のスクリプトは、TLSプロトコルバージョン値をインストールして有効にします。サムプリント（この例では「12345678987654321」として表されます）は、使用する証明書を選択するために使用されます。

```
Enable-VdaSSL -Enable -CertificateThumbPrint "12345678987654321"
```

次のスクリプトは、TLSリスナーをインストールして有効にし、TLSポート400、GOV暗号スイート、および最小TLS 1.2プロトコル値を指定します。サムプリント（この例では「12345678987654321」として表されます）は、使用する証明書を選択するために使用されます。

```
Enable-VdaSSL -Enable

-CertificateThumbPrint "12345678987654321"

-SSLPort 400 -SSLMinVersion "TLS_1.3"

-SSLCipherSuite "All"
```

次のスクリプトは、VDA上のTLSリスナーを無効にします。

```
Enable-VdaSSL -Disable
```

VDAでTLSを手動で構成する

VDAでTLSを手動で構成する場合、各VDAの適切なサービスに対して、TLS証明書の秘密キーへの一般的な読み取りアクセス権を付与します。WindowsシングルセッションOS用VDAの場合はNT SERVICE\PorticaService、WindowsマルチセッションOS用VDAの場合はNT SERVICE\TermServiceです。VDAがインストールされているマシンで、次の手順を実行します。

手順 1. Microsoft管理コンソール（MMC）を起動します: スタート > ファイル名を指定して実行 > mmc.exe。

手順 2. MMCに証明書スナップインを追加します。

1. ファイル > スナップインの追加と削除 を選択します。
2. 証明書 を選択し、追加 をクリックします。
3. 「このスナップインで常に管理する証明書は次のとおりです:」というプロンプトが表示されたら、「コンピューターアカウント」を選択し、次へ をクリックします。
4. 「このスナップインで管理するコンピューターを選択してください」というプロンプトが表示されたら、「ローカルコンピューター」を選択し、完了 をクリックします。

手順 3. 証明書 (ローカルコンピューター) > 個人 > 証明書 の下で、証明書を右クリックし、すべてのタスク > 秘密キーの管理 を選択します。

手順 4. アクセス制御リストエディターに「(FriendlyName) の秘密キーのアクセス許可」が表示されます。(FriendlyName) はTLS証明書の名前です。次のいずれかのサービスを追加し、読み取りアクセス権を付与します。

- WindowsシングルセッションOS用VDAの場合、「PORTICASERVICE」
- WindowsマルチセッションOS用VDAの場合、「TERMSERVICE」

ステップ5. インストールされているTLS証明書をダブルクリックします。証明書ダイアログで、タブを選択し、一番下までスクロールします。をクリックします。

ステップ6. regeditを実行し、HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawdに移動します。

1. SSL Thumbprintキーを編集し、TLS証明書の拇印の値をこのバイナリ値にコピーします。ダイアログボックスの不明な項目（「0000」や特殊文字など）は無視しても問題ありません。

2. SSLEnabledキーを編集し、DWORD値を1に変更します。(後でSSLを無効にするには、DWORD値を0に変更します。)
3. デフォルト設定を変更する場合（オプション）は、同じレジストリパスで以下を使用します。

   SSLPort DWORD – SSLポート番号。デフォルト: 443。

   SSLMinVersion DWORD – 1 = SSL 3.0、2 = TLS 1.0、3 = TLS 1.1、4 = TLS 1.3。デフォルト: 2 (TLS 1.0)。

   SSLCipherSuite DWORD – 1 = GOV、2 = COM、3 = ALL。デフォルト: 3 (ALL)。

ステップ7. TLSのTCPポートとUDPポートがデフォルトの443でない場合、Windowsファイアウォールで開いていることを確認します。(Windowsファイアウォールで受信規則を作成する際は、そのプロパティで「接続を許可する」と「有効」のエントリが選択されていることを確認してください。)

ステップ8. 他のアプリケーションやサービス（IISなど）がTLS TCPポートを使用していないことを確認します。

ステップ9. WindowsマルチセッションOS用VDAの場合、変更を有効にするためにマシンを再起動します。(WindowsシングルセッションOS用VDAを含むマシンを再起動する必要はありません。)

> **重要:**

> VDAがWindows Server 2012 R2、Windows Server 2016、またはWindows 10 Anniversary Edition以降のサポート対象リリースである場合、追加の手順が必要です。これは、Citrix Receiver for Windows (バージョン4.6～4.9)、Citrix Workspace app for HTML5、およびCitrix Workspace app for Chromeからの接続に影響します。Citrix Gatewayを使用する接続も含まれます。

> この手順は、Citrix GatewayとVDA間のTLSが構成されている場合、すべてのVDAバージョンでCitrix Gatewayを使用するすべての接続にも必要です。これは、すべてのCitrix Receiver™ バージョンに影響します。

> VDA (Windows Server 2012 R2、Windows Server 2016、またはWindows 10 Anniversary Edition以降) で、グループポリシーエディターを使用して、 > > > > > に移動します。次の順序を選択します。

```
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384_P384

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384_P256

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P384

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P256

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P384

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P256
```

注：

最初の6つの項目は、楕円曲線P384またはP256も指定します。「curve25519」が選択されていないことを確認してください。FIPSモードは「curve25519」の使用を妨げません。

このグループポリシー設定が構成されている場合、VDAは、グループポリシーリストと、選択されたコンプライアンスモード（COM、GOV、またはALL）のリストの両方に表示される場合にのみ、暗号スイートを選択します。暗号スイートは、クライアント（Citrix WorkspaceアプリまたはStoreFront）から送信されたリストにも表示されている必要があります。

このグループポリシー構成は、VDA上の他のTLSアプリケーションおよびサービスにも影響します。アプリケーションが特定の暗号スイートを必要とする場合、それらをこのグループポリシーリストに追加する必要がある場合があります。

重要:

グループポリシーの変更は適用時に表示されますが、TLS構成のグループポリシーの変更は、オペレーティングシステムの再起動後にのみ有効になります。したがって、プールされたデスクトップの場合、TLS構成のグループポリシーの変更をベースイメージに適用してください。

デリバリーグループでのTLSの構成

TLS接続用に構成したVDAを含む各デリバリーグループに対して、この手順を完了します。

1. StudioからPowerShellコンソールを開きます。
2. Citrix製品のコマンドレットを読み込むには、**asnp Citrix.***を実行します。
3. **Get-BrokerAccessPolicyRule -DesktopGroupName '\<*delivery-group-name*>' \| Set-BrokerAccessPolicyRule -HdxSslEnabled $true**を実行します。
4. **Set-BrokerSite -DnsResolutionEnabled $true**を実行します。

トラブルシューティング

接続エラーが発生した場合は、VDAのシステムイベントログを確認してください。

Windows版Citrix Workspaceアプリを使用しているときに、TLSエラーを示す接続エラーが表示された場合は、Desktop Viewerを無効にしてから、もう一度接続を試してください。接続は引き続き失敗しますが、基になるTLS問題の説明が提供される場合があります。（例：証明機関に証明書を要求する際に、誤ったテンプレートを指定しました。）

HDX™ Adaptive Transportを使用するほとんどの構成は、Citrix Workspaceアプリ、Citrix Gateway、およびVDAの最新バージョンを使用するものを含め、DTLSで正常に動作します。Citrix WorkspaceアプリとCitrix Gateway間、およびCitrix GatewayとVDA間でDTLSを使用する一部の構成では、追加の操作が必要です。

次の場合、追加の操作が必要です。

- Citrix ReceiverのバージョンがHDX Adaptive TransportおよびDTLSをサポートしている場合：Receiver for Windows (4.7, 4.8, 4.9)、Receiver for Mac (12.5, 12.6, 12.7)、Receiver for iOS (7.2, 7.3.x)、またはReceiver for Linux (13.7)

かつ、以下のいずれかに該当する場合も同様です。

- Citrix Gateway のバージョンが VDA への DTLS をサポートしているが、VDA のバージョンが DTLS をサポートしていない場合（バージョン 7.15 以前）、,
- VDA のバージョンが DTLS をサポートしているが（バージョン 7.16 以降）、Citrix Gateway のバージョンが VDA への DTLS をサポートしていない場合。

Citrix Receiver からの接続が失敗するのを避けるには、次のいずれかを実行します。

- Citrix Receiver を、Receiver for Windows バージョン 4.10 以降、Receiver for Mac 12.8 以降、または Receiver for iOS バージョン 7.5 以降に更新する。
- Citrix Gateway を、VDA への DTLS をサポートするバージョンに更新する。
- VDA をバージョン 7.16 以降に更新する。
- VDA で DTLS を無効にする。

- HDX Adaptive Transport を無効にする。

> **注：**
>
> Receiver for Linux の適切な更新はまだ利用できません。Receiver for Android（バージョン 3.12.3）は、HDX Adaptive Transport および Citrix Gateway 経由の DTLS をサポートしていないため、影響を受けません。

> VDA で DTLS を無効にするには、VDA ファイアウォール構成を変更して UDP ポート 443 を無効にします。詳細については、「ネットワークポート」を参照してください。

Controller と VDA 間の通信

Windows Communication Framework (WCF) のメッセージレベル保護により、Controller と VDA 間の通信が保護されます。TLS を使用した追加のトランスポートレベル保護は必要ありません。WCF 構成では、Controller と VDA 間の相互認証に Kerberos を使用します。暗号化には 256 ビットキーの CBC モードで AES を使用します。メッセージの整合性には SHA-1 を使用します。

Microsoft によると、WCF で使用されるセキュリティプロトコルは、WS-SecurityPolicy 1.2 を含む OASIS (Organization for the Advancement of Structured Information Standards) の標準に準拠しています。さらに、Microsoft は、WCF がSecurity Policy 1.2に記載されているすべてのアルゴリズムスイートをサポートしていると述べています。

Controller と VDA 間の通信には basic256 アルゴリズムスイートが使用され、そのアルゴリズムは上記のとおりです。

TLS と HTML5 ビデオリダイレクト、およびブラウザコンテンツリダイレクト

HTML5 ビデオリダイレクトとブラウザコンテンツリダイレクトを使用して、HTTPS Web サイトをリダイレクトできます。これらの Web サイトに挿入された JavaScript は、VDA で実行されている Citrix HDX HTML5 ビデオリダイレクトサービスへの TLS 接続を確立する必要があります。これを実現するために、HTML5 ビデオリダイレクトサービスは、VDA 上の証明書ストアに 2 つのカスタム証明書を生成します。サービスを停止すると、証明書は削除されます。

HTML5 ビデオリダイレクトポリシーは、デフォルトで無効になっています。

ブラウザコンテンツリダイレクトは、デフォルトで有効になっています。

HTML5 ビデオリダイレクトの詳細については、マルチメディアポリシー設定を参照してください。

Delivery Controller で TLS を有効にする

デフォルトでは、HTTP と HTTPS の両方が有効になっています。HTTPS は、サーバーの FQDN を共通名として使用する自己署名証明書を使用しますが、これは StoreFront™ や Web ブラウザーからは信頼されません。

delivery controller™ で TLS を有効にするには、次の操作を行う必要があります。

- すべての Delivery Controller にサーバー証明書を取得、インストール、登録します。詳細については、「証明書の要求とインストール」を参照してください。
- TLS 証明書を使用してポートを構成します。詳細については、「証明書のインストール」を参照してください。
- モニターサービスで HTTPS を有効にする。
- HTTP を無効にして HTTPS トラフィックを強制します。詳細については、「HTTPS トラフィックのみを強制するHTTPS トラフィックのみを強制する」を参照してください。
- 必要に応じて、Controller が HTTP および HTTPS トラフィックをリッスンするために使用するポートを変更できます。詳細については、「HTTP または HTTPS ポートの変更」を参照してください。

証明書の要求とインストール

TLS を使用するには、Common Name または Subject Alternative Name がサーバーの FQDN と一致する証明書をインストールする必要があります。delivery controller の前にロードバランサーを使用している場合は、サーバーとロードバランサーの両方の FQDN を Subject Alternative Name として含めます。詳細については、「証明書」を参照してください。StoreFront が delivery controller に接続するには、RSA デジタル署名アルゴリズムを使用する必要があります。StoreFront は ECDSA アルゴリズムを使用する証明書をサポートしていません。

SSL/TLS リスナーポートの構成

Web Studio および Director の一部としてインストールされる IIS Windows コンポーネントが同じサーバーにインストールされている場合、IIS を使用して TLS を構成できます。詳細については、「Web Studio および Director で TLS を有効にする」を参照してください。それ以外の場合は、PowerShell を使用して証明書を構成するには、次の手順を実行します。

1. 既存の証明書がバインドされているかを確認するには、コマンドプロンプトを開き、`netsh http show sslcert` を実行します。

   ```
   netsh http show sslcert
   ```

2. 既存のバインドがある場合は、それを削除します。

```
netsh http delete sslcert ipport=0.0.0.0:443
```

既存のバインドで特定の IP アドレスとポートが指定されていた場合は、`0.0.0.0:443` をその IP アドレスとポートに置き換えます。

3. 以前にインストールした証明書のサムプリントを見つけます。サムプリントを表示するには、**コンピューター証明書の管理**を開き、証明書を参照して開き、**詳細**タブに移動します。

サムプリントを示す証明書のプロパティのスクリーンショット(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/certificate-thumbprint.png)

または、PowerShellを使用することもできます。たとえば、次のスクリプトは、共通名がサーバーのホスト名と一致する証明書を検索し、サムプリントを出力します。

```
$HostName =
([System.Net.Dns]::GetHostByName(($env:computerName))).Hostname

$Thumbprint = (Get-ChildItem -Path Cert:\LocalMachine\My | Where-Object
{$_.Subject -match ("CN=" + $HostName)}).Thumbprint -join ';'

Write-Host -Object "Certificate Thumbprint for $($HostName): $
($Thumbprint)" -Foreground Yellow
```

証明書の共通名がホスト名と一致しない場合、これは失敗します。ホスト名に対して複数の証明書がある場合、これは連結された複数のサムプリントを返し、適切なサムプリントを選択する必要があります。

次の例では、フレンドリ名で証明書を検索します。

```
$friendlyName = "My certificate name"

$Thumbprint = (Get-ChildItem -Path Cert:\LocalMachine\My | Where-Object
{$_.FriendlyName -eq $friendlyNam}).Thumbprint -join ';'

Write-Host -Object "Certificate Thumbprint for $friendlyName: $
($Thumbprint)" -Foreground Yellow
```

指定されたフレンドリ名を持つ証明書が複数ある場合、これは連結された複数のサムプリントを返し、適切なサムプリントを選択する必要があります。

4. 証明書をポートにバインドするには、`netsh http add sslcert`コマンドを使用します。

```
netsh http add sslcert ipport=[IP address]:443 certhash=[certificate
hash] appid=[application GUID] disablelegacytls=enable
```

- `ipport`: IPアドレスとポート。0.0.0.0:443を使用すると、すべてのIPアドレスに適用されます。代わりに、特定のIPアドレスを指定することもできます。
- `certhash`: 前の手順で特定した証明書のサムプリント。
- `appid`: シトリックス ブローカー サービスのGUID。

> **注：**
>
> 証明書を更新または再バインドする際は、任意のGUIDではなく、Broker Serviceに関連付けられた特定の`appid`を使用してください。
>
> Citrix Broker Serviceの正しい`appid`を見つけるには：

a. 管理者としてPowerShellコマンドウィンドウを開き、次のコマンドを実行します。

```
Get-WmiObject -Class Win32_Product | Select-String -Pattern
"broker"
```

b. 出力でCitrix Broker ServiceのIdentifyingNumber (GUID) を見つけます（例：`{D333C884-187F-447C-8C67-463F33989C8F}`）。このGUIDを`appid`パラメーターに使用します。

- `disablelegacytls=enable`: レガシーバージョンのTLSを無効にします。このパラメーターはWindows 2022以降で利用可能です。Windows 2022ではTLS 1.0と1.1を無効にします。Windows 2025では、TLS 1.0と1.1がデフォルトで無効になっているため、これは不要です。

例えば、すべてのIPアドレスで、サムプリント`bc96f958848639fd101a793b87915d5f2829b0b6`の証明書をポート`443`にバインドするには、次のコマンドを実行します。

```
netsh http add sslcert ipport=0.0.0.0:443
certhash=bc96f958848639fd101a793b87915d5f2829b0b6 appid={91fe7386-
e0c2-471b-a252-1e0a805febac} disablelegacytls=enable
```

HTTPSが有効になったら、デリバリーコントローラーへの接続にHTTPではなくHTTPSを使用するように、StoreFront展開 とNetscaler Gatewayを構成する必要があります。

HTTPS 用のモニターサービス OData API を構成する

モニターサービスは、Citrix® およびサードパーティアプリケーションがデータを照会できるように、OData v3 および v4 API を提供します。Director は OData API V3 を使用して監視サービスに接続します。HTTPS 用のモニター OData API を構成するには、次の手順を完了します。

1. 次のPowerShellを実行します。

```
$serviceGroup = Get-ConfigRegisteredServiceInstance -ServiceType
Monitor | Select -First 1 ServiceGroupUid

Remove-ConfigServiceGroup -ServiceGroupUid
$serviceGroup.ServiceGroupUid

& 'C:\Program Files\Citrix\Monitor\Service\citrix.monitor.exe'
-ConfigureFirewall -RequireODataTls –OdataPort 443 -RequireODataSdkTls
–OdataSdkPort 443

get-MonitorServiceInstance | register-ConfigServiceInstance

Get-ConfigRegisteredServiceInstance -ServiceType Config | Reset-
MonitorServiceGroupMembership
```

2. テキストエディターでファイル `C:\Program Files\Citrix\Monitor\Service\Citrix.Monitor.exe.Config` を開きます。要素 `<add key="owin:baseAddress" value="http://localhost/citrix/monitor/odata/v4" />` を見つけて、`<add key="owin:baseAddress" value="https://localhost/citrix/monitor/odata/v4" />` に変更します。

暗号スイートを構成する

暗号スイートの順序リストには、`TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384` または `TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256` の暗号スイート（またはその両方）を含める必要

があります。また、これらの暗号スイートは、`TLS_DHE_` の暗号スイートよりも前に配置する必要があります。

1. Microsoft グループポリシーエディターを使用して、**コンピューターの構成 > 管理用テンプレート > ネットワーク > SSL 構成設定** に移動します。
2. 「SSL 暗号スイートの順序」ポリシーを編集します。デフォルトでは、このポリシーは「未構成」に設定されています。このポリシーを「有効」に設定します。
3. スイートを正しい順序に並べます。使用しない暗号スイートは削除します。

`TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384` または `TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256` が、`TLS_DHE_` の暗号スイートよりも前に配置されていることを確認してください。

Microsoft Learn で、TLS 暗号スイートの順序の構成 も参照してください。

HTTPS トラフィックのみを強制する

XML Service が HTTP トラフィックを無視するように構成することをお勧めします。

1. `regedit` を実行します。
2. `HKLM\Software\Citrix\DesktopServer\`を開く
3. `XmlServicesEnableNonSsl`という名前の新しいDWORD値を作成し、0に設定します。
4. Broker Serviceを再起動します。

HTTPSトラフィックを無視するために作成できる対応するレジストリDWORD値 `XmlServicesEnableSsl`があります。これが0に設定されていないことを確認してください。

HTTPまたはHTTPSポートを変更する

デフォルトでは、Controller上のXMLサービスは、HTTPトラフィックにはポート80を、HTTPSトラフィックにはポート443をリッスンします。デフォルト以外のポートを使用することもできますが、Controllerを信頼できないネットワークに公開することによるセキュリティリスクに注意してください。デフォルトを変更するよりも、スタンドアロンのStoreFrontサーバーを展開する方が望ましいです。

Controllerで使用されるデフォルトのHTTPまたはHTTPSポートを変更するには、Studioから次のコマンドを実行します。

```
BrokerService.exe -StoreFrontPort <http-port> -StoreFrontTlsPort <https-port>
```

ここで、`<http-port>`はHTTPトラフィックのポート番号、`<https-port>`はHTTPSトラフィックのポート番号です。

> **注:**
>
> ポートを変更した後、Studioはライセンスの互換性とアップグレードに関するメッセージを表示する場合があります。この問題を解決するには、次のPowerShellコマンドレットシーケンスを使用してサービスインスタンスを再登録します。

```
Get-ConfigRegisteredServiceInstance -ServiceType Broker -Binding XML_HTTPS
|

Unregister-ConfigRegisteredServiceInstance

Get-BrokerServiceInstance | where Binding -eq "XML_HTTPS" |

Register-ConfigServiceInstance
```

Web StudioとDirectorでTLSを有効にする

Web StudioおよびDirectorへの接続を保護するために、HTTPSを有効にして常にTLSを使用することをお勧めします。この記事では、Web StudioとDirectorを構成して、信頼された証明書を使用し、HTTPS経由で安全なアクセスを確保する方法について説明します。

デフォルトの動作

Web Studioをインストールすると、インストーラーは自己署名証明書を作成し、現在のサーバーのポート443にバインドします。ローカルサーバー上のWebブラウザーからHTTPS経由でWeb StudioおよびDirectorにアクセスできます。

ただし、別のマシンからHTTPS経由でWeb StudioまたはDirectorにアクセスしようとすると、ブラウザーは証明書を信頼しないため、セキュリティエラーを表示します。

> **注：**
>
> Web StudioなしでDirectorをインストールした場合、インストーラーは自己署名証明書を作成しません。

HTTPS経由で安全なアクセスを有効にする

Web Studioサーバーⅰ以外のマシンからHTTPS経由でWeb StudioまたはDirectorへのアクセスを許可するには、次の手順に従います。

1. 信頼された証明書を作成またはインポートする。
2. IISで証明書をポート443にバインドする。
3. (オプション) HTTP Strict Transport Security (HSTS) を有効にする。
4. Web Studioがプロキシとして構成されていない場合 (クライアントマシンがWeb StudioとDelivery Controllerの両方に接続する場合)、Delivery ControllerでTLSを有効にする。

> **注：**
>
> 自己署名証明書の使用は、各マシンで手動構成が必要なため推奨されません。詳細については、自己署名証明書を使用するを参照してください。

信頼された証明書を作成またはインポートする

サーバーに接続するマシンによって信頼されている、エンタープライズまたはパブリック認証局からの証明書を使用することをお勧めします。

詳細については、新しい証明書の作成 および 既存の証明書のインポート を参照してください。証明書の共通名またはサブジェクトの別名は、ユーザーがWeb StudioまたはDirectorに接続するために使用するFQDNと一致する必要があります。サーバーの前にロードバランサーが展開されている場合は、ロードバランサーのFQDNを使用してください。

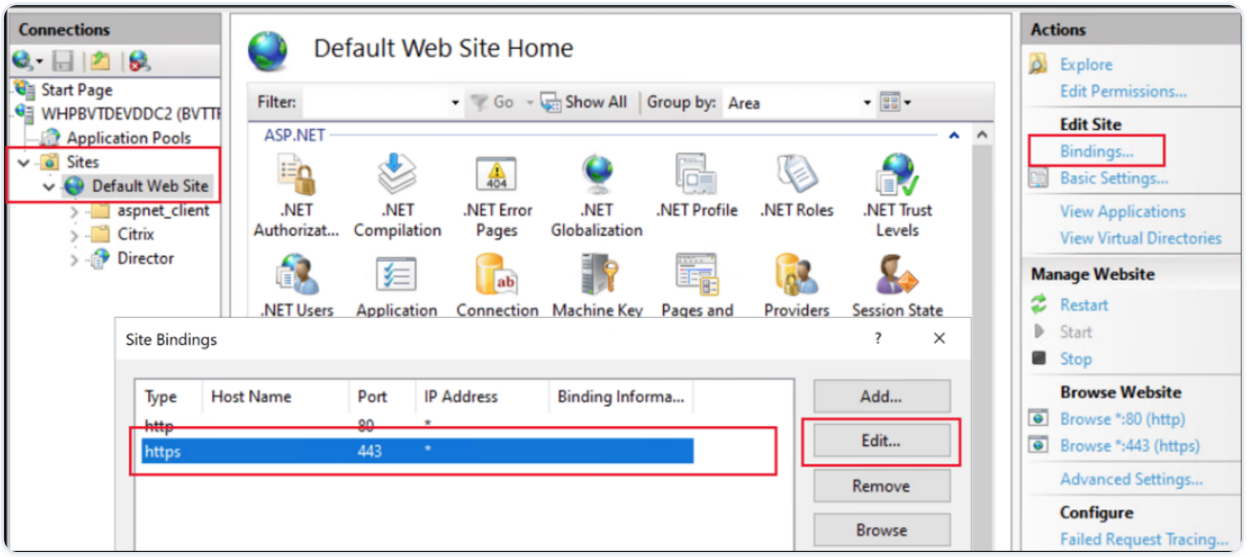
証明書をポート443にバインドする

信頼された証明書を作成またはインポートした後、IISでポート `443` にバインドします。これはインストール前でもインストール後でも実行できます。ポート `443` の証明書バインドがすでに構成されている場合、インストーラーは変更を行いません。

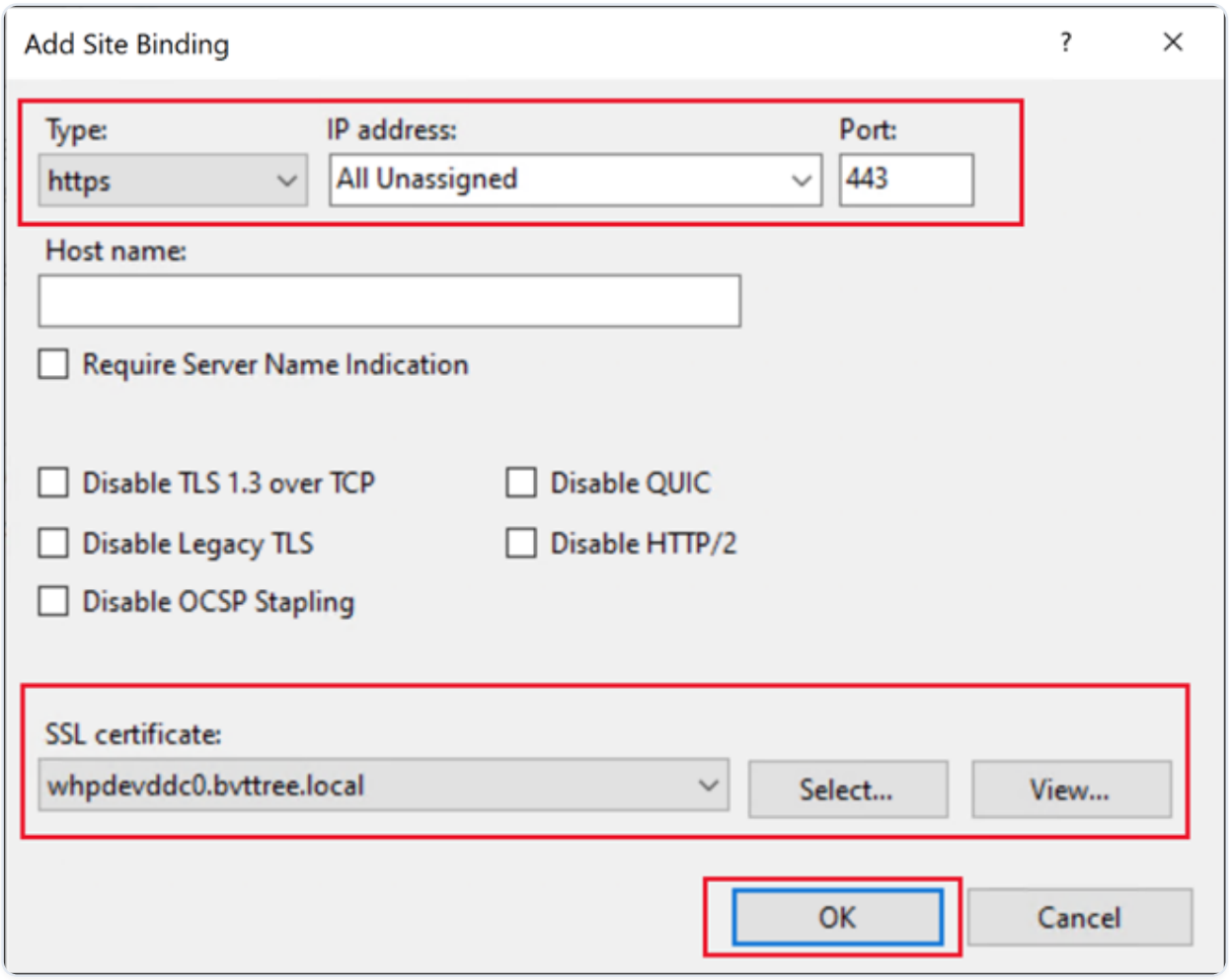
> **注：**
>
> デフォルトでは、Web StudioとDirectorはセキュアなHTTPSアクセスにポート443を使用します。必要に応じてポート番号を変更できます。詳細については、デフォルトのポート番号の変更 を参照してください。

> 証明書をポート `443` にバインドするには、次の手順に従います。

1. 管理者としてサーバーにログオンします。
2. IISマネージャーを開き、**サイト > 既定のWebサイト > バインド** に移動します。
3. 種類が **https** の既存のバインドがある場合は、それを選択して **編集...** をクリックします。**https** バインドがない場合は、**追加** をクリックします。



4. サイトバインドを作成または編集します。
   a. 新しいバインドの場合、種類を **https** に、ポートを `443` に設定します。
   b. 適切なSSL証明書を選択します。
   c. Windows Server 2022以降では、オプションで **レガシーTLSを無効にする** を選択して、ユーザーが最新のTLSバージョンのみを使用して接続できるようにします。
   d. **OK**をクリックします。



または、PowerShellを使用して証明書を変更することもできます。たとえば、次のスクリプトは、指定された共通名を持つ証明書を検索し、それをすべてのIPアドレス、ポート443にバインドし、レガシーTLSバージョンを無効にします。

```
$certSName = 'CN=whpdevddc0.bvttree.local'  # The subject name of the
certificate

$certificate = Get-ChildItem -Path Cert:\LocalMachine\My\ | ? {$_.Subject
-eq $certSName}

netsh http add sslcert ipport=0.0.0.0:443 certhash=$
($certificate.Thumbprint) certstorename=My appid="{91fe7386-e0c2-471b-
a252-1e0a805febac}" disablelegacytls=enable
```

なお、`appid` は、どのアプリケーションが証明書を追加したかを識別するために使用できる任意の GUID です。

自己署名証明書を使用する

既存の自己署名証明書を使用できますが、サーバーにアクセスする各マシンを手動で構成する必要があるため、推奨されません。

Web Studio に接続する必要があるマシンに自己署名証明書をインストールするには、次の手順を実行します。

1. Web Studio および Delivery Controller サーバーから既存の自己署名証明書を(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/secure/certificates.html#export-certificate-without-private-key)します。
2. サーバーにアクセスする必要があるマシンの **信頼されたルート証明書** ストアに証明書を(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/secure/certificates.html#import-existing-certificate)します。

(オプション) HTTP Strict Transport Security (HSTS) を有効にする

HTTP Strict Transport Security (HSTS) は、Web ブラウザーに対し、サイトへのアクセス時に HTTPS のみを使用するよう指示します。ユーザーが HTTP を使用して URL にアクセスしようとすると、ブラウザーは自動的に HTTPS に切り替わります。この設定により、クライアント側とサーバー側の両方で安全な接続検証が保証されます。ブラウザーは、構成された期間、この検証を維持します。

Windows Server 2019 以降では、IIS で HSTS を構成できます。

1. **インターネット インフォメーション サービス (IIS) マネージャー** を開きます。
2. **既定の Web サイト** (または適切な Web サイト) を選択します。
3. 右側の **操作** ペインで、**HSTS...** を選択します。
4. **有効にする** を選択し、最大有効期間を入力します (例: 1 年の場合は 31536000)。
5. **HTTP を HTTPS にリダイレクト** を選択します。

> **注：**
>
> Web Studio は、Studio Web サイトにアクセスする際に HTTP を HTTPS にリダイレクトする **URL 書き換え** ルールを自動的に構成します。ただし、このオプションは Director および IIS サイト上の他のすべてのアプリケーションにも適用されます。

6. **OK**をクリックします。

HSTS設定のスクリーンショット(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/iis-hsts.png)

(オプション) デフォルトのポート番号を変更する

デフォルトでは、Web StudioとDirectorはセキュアなHTTPSアクセスにポート443を使用します。このポート番号を変更するには、`Default Web Site`で目的のポートのサイトバインディングを作成するために、以下の手順に従ってください。

手順:

1. Web Studioをホストしているサーバーで、**インターネットインフォメーションサービス (IIS) マネージャー**を開きます。
2. **接続**ペインで、サーバーノードを展開し、**サイト**の下にある**既定のWebサイト**を選択します。
3. 右側の**操作**ペインで、**バインディング**をクリックします。

   新しいポートを設定する(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/web-studio-new-port.png)
4. **サイトバインディング**ウィンドウで、**追加**をクリックします。
5. サイトバインディングの追加ウィンドウで、新しいバインディングに対して以下を設定します。

   a. **種類**: **https**を選択します。

   b. **IPアドレス**: 適切なIPアドレスを選択するか、該当する場合はすべて未割り当てのままにします。

   c. **ポート**: 目的のポート番号を入力します (例: 444)。

   d. **SSL証明書**: セキュアな通信のために適切なSSL証明書を選択します。

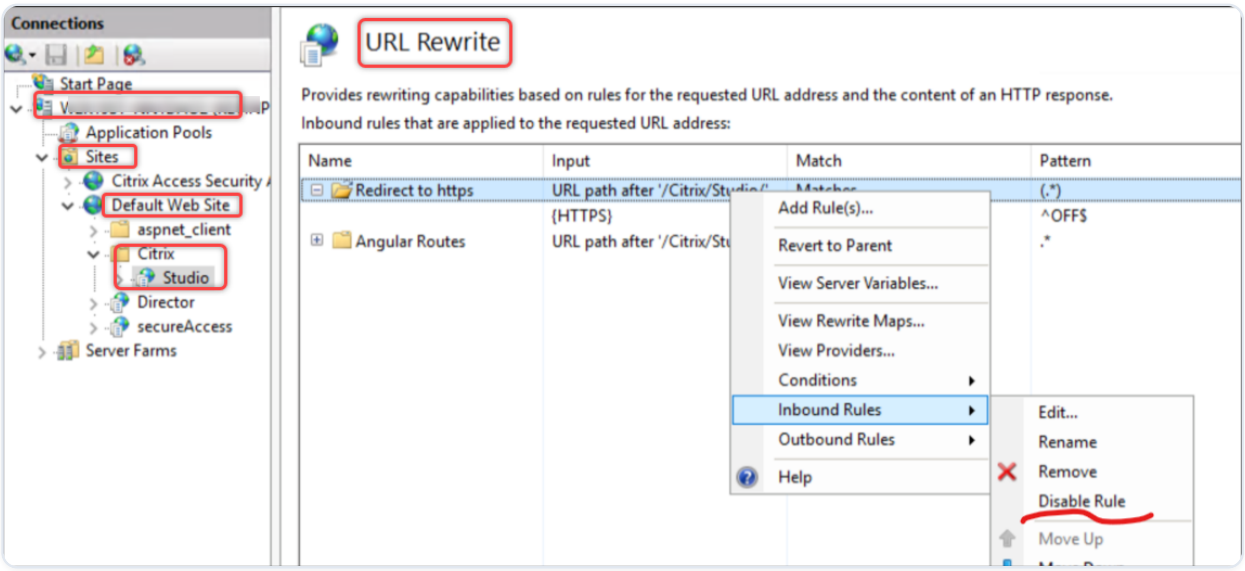
   > **注：**
   >
   > Delivery Controller™とWeb Studioが別々のマシンにインストールされており、サーバーに他のサービスやWebサイトが展開されていない場合は、ポート443を削除できます。そうでない場合は、オーケストレーションサービスや他のFMAサービスとの通信問題を避けるために、このポートを維持してください。
6. 「**OK**」をクリックしてバインディングを保存し、「**サイトバインディング**」ウィンドウを閉じます。

7. **IIS マネージャー**で、サーバーノードをクリックし、**操作**ペインで「**再起動**」をクリックして新しいバインディングを適用します。

（オプション）HTTPS リダイレクトを無効にする

Web Studio をインストールすると、デフォルトで、すべての HTTP アクセスが HTTPS に自動的にリダイレクトされます。このリダイレクトを無効にして HTTP アクセスを許可することも可能です。この方法は、HTTP アクセスをブロックするための他の対策を講じている場合にのみ推奨されます。Web Studio の前に TLS 終端ロードバランサーがある場合でも、ロードバランサーと Web Studio の間で HTTPS を使用することをお勧めします。

1. Web Studio サーバーにログオンします。
2. **インターネットインフォメーションサービス (IIS) マネージャー**を開き、*Server_name* **> サイト > Default Web Site > URL Rewrite** に移動します。
3. 次のスクリーンショットに示すように、**https へのリダイレクト**の**受信規則**を無効にします。



IIS で HSTS を有効にしている場合は、**Redirect Http to Https** もクリアする必要があります。

ユニバーサルプリントサーバーでのトランスポート層セキュリティ (TLS)

Virtual Delivery Agent (VDA) とユニバーサルプリントサーバー間のTCPベースの接続では、トランスポート層セキュリティ (TLS) プロトコルがサポートされています。

> **警告:**

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

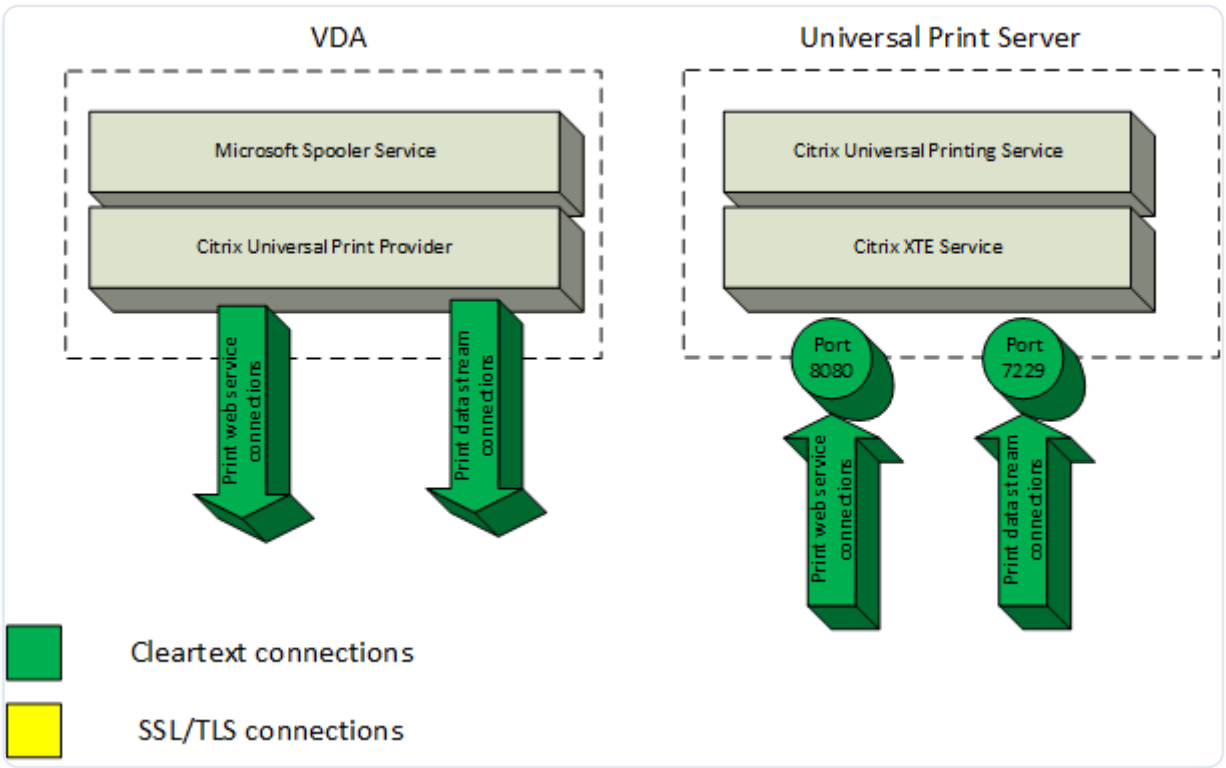
VDAとユニバーサルプリントサーバー間の印刷接続の種類

クリアテキスト接続

印刷に関連する以下の接続は、VDAから発信され、ユニバーサルプリントサーバーのポートに接続します。これらの接続は、**SSL enabled** ポリシー設定が **Disabled** (デフォルト) に設定されている場合にのみ行われます。

- クリアテキスト印刷Webサービス接続 (TCPポート 8080)
- クリアテキスト印刷データストリーム (CGP) 接続 (TCPポート 7229)

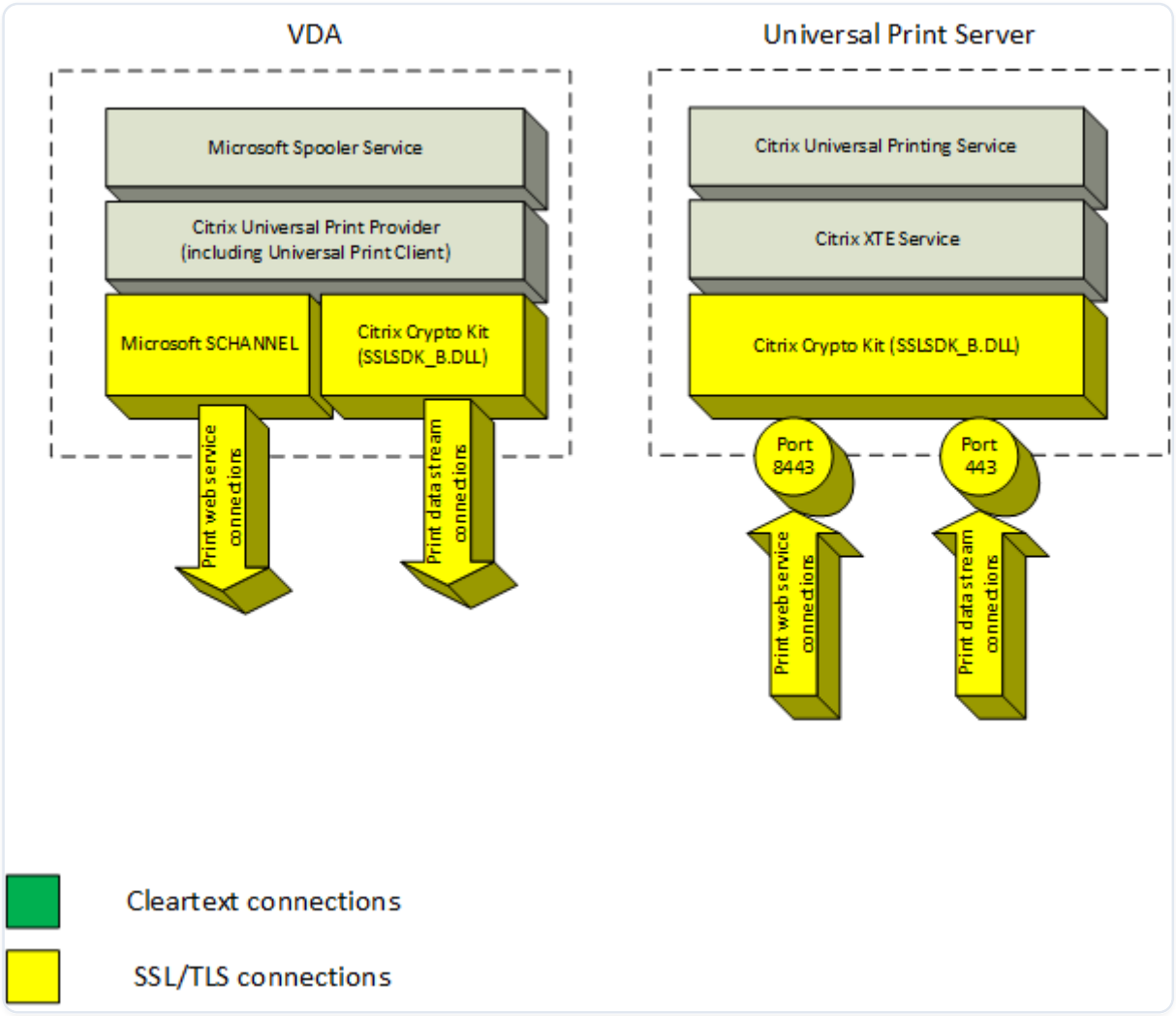
Microsoftサポート記事 Service overview and network port requirements for Windows には、Microsoft Windows Print Spoolerサービスが使用するポートが記載されています。このドキュメントのSSL/TLS設定は、Windows Print Spoolerサービスによって行われるNetBIOSおよびRPC接続には適用されません。**Universal Print Server enable** ポリシー設定が **Enabled with fallback to Windows' native remote printing** に設定されている場合、VDAはフォールバックとしてWindows Network Print Provider (win32spl.dll) を使用します。



暗号化された接続

印刷に関連するこれらのSSL/TLS接続は、VDAから発信され、ユニバーサルプリントサーバーのポートに接続します。これらの接続は、**SSL enabled** ポリシー設定が **Enabled** に設定されている場合にのみ行われます。

- 暗号化された印刷Webサービス接続 (TCPポート 8443)
- 暗号化された印刷データストリーム (CGP) 接続 (TCPポート 443)



SSL/TLS クライアント構成

VDA は SSL/TLS クライアントとして機能します。

Microsoft Group Policy とレジストリを使用して、暗号化された印刷 Web サービス接続 (TCP ポート 8443) 用に Microsoft SCHANNEL SSP を構成します。Microsoft サポート記事の TLS Registry Settings には、Microsoft SCHANNEL SSP のレジストリ設定が記載されています。

VDA 上のグループポリシーエディターを使用して、**コンピューターの構成 > 管理用テンプレート > ネットワーク > SSL 構成設定 > SSL 暗号スイートの順序**に移動します。TLS 1.3 が設定されている場合は、次の順序を選択します。

TLS_AES_256_GCM_SHA384 TLS_AES_128_GCM_SHA256

TLS 1.2 が設定されている場合は、次の順序を選択します。

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384_P384
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384_P256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P384
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P384
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P256

注：

このグループポリシー設定が構成されている場合、VDA は、暗号化された印刷 Web サービス接続 (デフォルトポート: 8443) の暗号スイートを、接続が両方の SSL 暗号スイートリストに表示されている場合にのみ選択します。

- グループポリシー SSL 暗号スイート順序リスト
- 選択した SSL 暗号スイートポリシー設定 (COM、GOV、または ALL) に対応するリスト

このグループポリシー構成は、VDA 上の他の TLS アプリケーションおよびサービスにも影響します。アプリケーションが特定の暗号スイートを必要とする場合、それらをこのグループポリシー暗号スイート順序リストに追加する必要がある場合があります。

重要:

TLS 構成のグループポリシーの変更は、オペレーティングシステムの再起動後にのみ有効になります。

Citrix ポリシーを使用して、暗号化された印刷データストリーム (CGP) 接続 (TCP ポート 443) の SSL/TLS 設定を構成します。

SSL/TLS サーバー構成

Universal Print Server は SSL/TLS サーバーとして機能します。

`Enable-UpsSsl.ps1` PowerShellスクリプトを使用して、SSL/TLS設定を構成します。

Universal Print ServerにTLSサーバー証明書をインストールする

HTTPSの場合、VDAによって信頼されているSSLサーバー証明書をUniversal Print Serverにインストールする必要があります。Microsoft Active Directory証明書サービスまたは別の認証局を使用して、Universal Print Serverの証明書を要求します。

マイクロソフト アクティブ ディレクトリ証明書サービスを使用して証明書を登録/要求する際は、以下の考慮事項に留意してください。

1. 証明書をローカルコンピューターの**個人**証明書ストアに配置します。
2. 証明書のサブジェクト識別名（Subject DN）の**共通名**属性を、Universal Print Serverの完全修飾ドメイン名（FQDN）に設定します。これは証明書テンプレートで指定します。
3. 証明書要求と秘密鍵の生成に使用される暗号化サービスプロバイダー（CSP）を**Microsoft Enhanced RSA and AES Cryptographic Provider (Encryption)**に設定します。これは証明書テンプレートで指定します。
4. キーサイズを2048ビット以上に設定します。これは証明書テンプレートで指定します。

証明書の作成とインストールについて詳しくは、「証明書の管理」を参照してください。

Universal Print ServerでのSSLの構成

Universal Print Server上のXTEサービスは、受信接続をリッスンします。SSLが有効な場合、SSLサーバーとして機能します。受信接続には、印刷コマンドを含む印刷Webサービス接続と、印刷ジョブを含む印刷データストリーム接続の2種類があります。これらの接続でSSLを有効にできます。SSLは、これらの接続の機密性と整合性を保護します。デフォルトでは、SSLは無効になっています。

SSLの構成に使用されるPowerShellスクリプトはインストールメディアにあり、ファイル名は次のとおりです: `\Support\Tools\SslSupport\Enable-UpsSsl.ps1.`.

Universal Print Serverでのリスニングポート番号の構成

XTEサービスのデフォルトポートは次のとおりです。

- クリアテキスト印刷Webサービス（HTTP）TCPポート: 8080
- クリアテキスト印刷データストリーム (CGP) TCPポート: 7229
- 暗号化された印刷Webサービス (HTTPS) TCPポート: 8443
- 暗号化された印刷データストリーム (CGP) TCPポート: 443

Universal Print ServerでXTEサービスが使用するポートを変更するには、管理者としてPowerShellで次のコマンドを実行します (Enable-UpsSsl.ps1 PowerShellスクリプトの使用に関する注意点については、後のセクションを参照してください):

1. `Stop-Service CitrixXTEServer, UpSvc`
2. `Enable-UpsSsl.ps1 -Enable -HTTPSPort <port> -CGPSSLPort <port>` または `Enable-UpsSsl.ps1 -Disable -HTTPPort <port> -CGPPort <port>`
3. `Start-Service CitrixXTEServer`

ユニバーサルプリントサーバーでのTLS設定

負荷分散構成で複数のUniversal Print Serverを使用している場合は、すべてのUniversal Print Serverで**TLS**設定が一貫して構成されていることを確認してください。

Universal Print ServerでTLSを構成すると、インストールされているTLS証明書のアクセス許可が変更され、Universal Printing Serviceに証明書の秘密キーへの読み取りアクセス権が付与されます。また、Universal Printing Serviceに次の情報が通知されます。

- TLSに使用する証明書ストア内の証明書。
- TLS接続に使用するTCPポート番号。

Windowsファイアウォール (有効な場合) は、これらのTCPポートでの受信接続を許可するように構成する必要があります。この構成は、Enable-UpsSsl.ps1 PowerShellスクリプトを使用すると自動的に行われます。

- 許可するTLSプロトコルのバージョン。

Universal Print ServerはTLSプロトコルバージョン1.3および1.2をサポートしています。許可される最小バージョンを指定します。

デフォルトのTLSプロトコルバージョンは1.2です。

> **注：**
>
> TLS 1.1および1.0は、Citrix Virtual Apps and Desktopsバージョン2311以降サポートされなくなりました。

- 許可するTLS暗号スイート。

暗号スイートは、接続に使用される暗号化アルゴリズムを選択します。VDAとUniversal Print Serverは、異なる暗号スイートのセットをサポートできます。VDAが接続し、サポートされているTLS暗号スイートのリストを送信すると、Universal Print Serverはクライアントの暗号スイートの1つを、自身の構成済み暗号スイートのリストにある暗号スイートの1つと照合し、接続を受け入れます。一致する暗号スイートがない場合、Universal Print Serverは接続を拒否します。

Universal Print Serverは、OPEN、FIPS、およびSP800-52ネイティブCrypto Kitモードに対して、GOV(ernment)、COM(mercial)、およびALLという名前の以下の暗号スイートセットをサポートしています。許容される暗号スイートは、**SSL FIPS Mode**ポリシー設定とWindows FIPS Modeにも依存します。Windows FIPSモードの詳細については、このMicrosoftサポート記事を参照してください。

暗号スイート（優先順位の降順）	OPEN ALL	OPEN COM	OPEN GOV	FIPS ALL	FIPS COM	FIPS GOV	SP800-52 ALL	SP800-52 COM	SP800-52 GOV
TLS_ECDHE_RSA_AES256_GCM_SHA384	X		X	X		X	X		X
TLS_ECDHE_RSA_AES256_CBC_	X		X	X		X	X		X

暗号スイート（優先順位の降順）	OPEN ALL	OPEN COM	OPEN GOV	FIPS ALL	FIPS COM	FIPS GOV	SP800-52 ALL	SP800-52 COM	SP800-52 GOV
SHA384									
TLS_ECDHE_RSA_AES256_CBC_SHA	X	X		X	X		X	X	

PowerShellスクリプトを使用してUniversal Print ServerでTLSを構成する

証明書ストアの**ローカルコンピューター > 個人 > 証明書**領域にTLS証明書をインストールします。その場所に複数の証明書がある場合は、証明書のサムプリントを`Enable-UpsSsl.ps1` PowerShellスクリプトに指定します。

注：

PowerShellスクリプトは、Universal Print ServerのFQDNに基づいて正しい証明書を見つけます。Universal Print ServerのFQDNに対して単一の証明書のみが存在する場合、証明書のサムプリントを指定する必要はありません。

`Enable-UpsSsl.ps1`スクリプトは、VDAからUniversal Print ServerへのTLS接続を有効または無効にします。このスクリプトは、インストールメディアの**Support > Tools > SslSupport**フォルダーにあります。

TLSを有効にすると、スクリプトはUniversal Print ServerのTCPポートに対する既存のすべてのWindowsファイアウォールルールを無効にします。その後、XTEサービスがTLS TCPおよびUDPポートでのみ受信接続を受け入れることを許可する新しいルールを追加します。また、以下のWindowsファイアウォールルールも無効にします。

- クリアテキスト印刷Webサービス接続 (デフォルト: 8080)
- クリアテキスト印刷データストリーム (CGP) 接続 (デフォルト: 7229)

その結果、VDAはTLSを使用している場合にのみこれらの接続を行うことができます。

> **注：**
>
> TLSを有効にしても、VDAからUniversal Print ServerへのWindows Print Spooler RPC/SMB接続には影響しません。

> **重要:**
>
> 最初のパラメーターとして**Enable**または**Disable**のいずれかを指定します。ローカルコンピューターの個人証明書ストアにUniversal Print ServerのFQDNを持つ証明書が1つしかない場合、CertificateThumbprintパラメーターはオプションです。その他のパラメーターはオプションです。

構文

```
Enable-UpsSSL.ps1 -Enable [-HTTPPort &lt;port&gt;] [-CGPPort &lt;port&gt;] [-HTTPSPort &lt;port&gt;] [-CGPSSLPort &lt;port&gt;] [-SSLMinVersion &lt;version&gt;] [-SSLCipherSuite &lt;name&gt;] [-CertificateThumbprint &lt;thumbprint&gt;] [-FIPSMode &lt;Boolean&gt;] [-ComplianceMode &lt;mode&gt;]

Enable-UpsSSL.ps1 -Disable [-HTTPPort &lt;portnum&gt;] [-CGPPort &lt;portnum&gt;]
```

パラメーター	説明
有効にする	XTEサーバーでSSL/TLSを有効にします。このパラメーターまたはDisableパラメーターのいずれかが必要です。

パラメーター	説明
無効にする	XTEサーバーでSSL/TLSを無効にします。このパラメーターまたはEnableパラメーターのいずれかが必要です。
CertificateThumbprint `"<thumbprint>"`	ローカルコンピューターの個人証明書ストアにあるTLS証明書のサムプリント。引用符で囲みます。スクリプトは、指定されたサムプリントを使用して、使用する証明書を選択します。
HTTPポート `<port>`	クリアテキスト印刷Webサービス (HTTP/SOAP) ポート。デフォルト: 8080
CGPポート `<port>`	クリアテキスト印刷データストリーム (CGP) ポート。デフォルト: 7229
HTTPSポート `<port>`	暗号化された印刷Webサービス (HTTPS/SOAP) ポート。デフォルト: 8443
CGP SSL ポート `<port>`	暗号化された印刷データストリーム (CGP) ポート。デフォルト: 443
SSLMinVersion `"<version>"`	引用符で囲まれた最小TLSプロトコルバージョン。有効な値: 「TLS_1.2」および「TLS_1.3」。デフォルト: TLS_1.2。
SSLCipherSuite `"<name>"`	引用符で囲まれたTLS暗号スイートパッケージの名前。有効な値: 「GOV」、「COM」、および「ALL」（デフォルト）。
FIPS モード `<Boolean>`	XTEサーバーでFIPS 140モードを有効または無効にします。有効な値: FIPS 140モードを有効にする場合は$true、FIPS 140モードを無効にする場合は$false。

例

次のスクリプトはTLSを有効にします。サムプリント（この例では「12345678987654321」として表されています）は、使用する証明書を選択するために使用されます。

```
Enable-UpsSsl.ps1 –Enable -CertificateThumbprint "12345678987654321"
```

次のスクリプトはTLSを無効にします。

```
Enable-UpsSsl.ps1 –Disable
```

FIPSモードの構成

米国連邦情報処理標準（FIPS）モードを有効にすると、Universal Print Serverの暗号化された接続にはFIPS 140準拠の暗号化のみが使用されるようになります。

クライアントでFIPSモードを構成する前に、サーバーでFIPSモードを構成してください。

Windows FIPSモードの有効化または無効化については、Microsoftのドキュメントサイトをご確認ください。

クライアントでのFIPSモードの有効化

Delivery Controller™でWeb Studioを実行し、**UPS FIPSモード**のCitrixポリシー設定を**有効**に設定します。Citrixポリシーを有効にします。

各VDAで以下を実行します。

1. Windows FIPSモードを有効にします。
2. VDAを再起動します。

サーバーでのFIPSモードの有効化

各Universal Print Serverで以下を実行します。

1. Windows FIPSモードを有効にします。
2. 管理者としてこのPowerShellコマンドを実行します: `stop-service CitrixXTEServer, UpSvc`
3. `-Enable -FIPSMode $true` パラメーターを指定して、`Enable-UpsSsl.ps1` スクリプトを実行します。
4. Universal Print Serverを再起動します。

クライアントでのFIPSモードの無効化

Web Studioで、Citrixポリシー設定の**UPS FIPS Mode**を**Disabled**に設定します。Citrixポリシーを有効にします。**UPS FIPS Mode** Citrixポリシー設定を削除することもできます。

各VDAで以下を実行します:

1. Windows FIPSモードを無効にします。
2. VDAを再起動します。

サーバーでのFIPSモードの無効化

各Universal Print Serverで以下を実行します:

1. Windows FIPSモードを無効にします。
2. 管理者としてこのPowerShellコマンドを実行します: `stop-service CitrixXTEServer, UpSvc`
3. `-Enable -FIPSMode $false` パラメーターを指定して、`Enable-UpsSsl.ps1` スクリプトを実行します。
4. Universal Print Serverを再起動します。

> **注：**
>
> SSLプロトコルバージョンがTLS 1.3に設定されている場合、FIPSモードはサポートされません。

SSL/TLSプロトコルバージョンの構成

デフォルトのSSL/TLSプロトコルバージョンはTLS 1.2です。TLS 1.2とTLS 1.3は、本番環境での使用が推奨されるSSL/TLSプロトコルバージョンです。トラブルシューティングのために、非本番環境でSSL/TLSプロトコルバージョンを一時的に変更する必要がある場合があります。

SSL 2.0およびSSL 3.0は、Universal Print Serverではサポートされていません。

サーバーでのSSL/TLSプロトコルバージョンの設定

Studioで、**SSLプロトコルバージョン**ポリシー設定を目的のプロトコルバージョンに設定し、ポリシーを有効にします。

VDAのオペレーティングシステムが選択したTLSバージョンをサポートしていることを確認してください。Windowsでサポートされ ているTLSバージョンについては、Microsoft Learn - TLSプロトコルバージョンのサポートを参照してください。デフォルトを上書きするようにレジストリを構成するには、Microsoft Learn - TLS、DTLS、およびSSLプロトコルバージョンの設定を参照してください。

クライアントでのSSL/TLSプロトコルバージョンの設定

各VDAで以下を実行します。

1. Delivery Controllerで、**SSLプロトコルバージョン**ポリシー設定を目的のプロトコルバージョンに設定し、ポリシーを有効にします。

2. Microsoftサポート記事TLSレジストリ設定は、Microsoft SCHANNEL SSPのレジストリ設定について説明しています。レジストリ設定を使用して、クライアント側の**TLS 1.2またはTLS 1.3**を有効にします。

   > **重要:**
   >
   > テストが完了したら、レジストリ設定を元の値に戻すことを忘れないでください。

3. VDAを再起動します。

トラブルシューティング

接続エラーが発生した場合は、Universal Print Server上のC:\Program Files (x86)\Citrix\XTE\logs\error.logファイルを確認してください。

SSL/TLSハンドシェイクが失敗した場合、このログファイルにエラーメッセージ**SSL handshake from client failed**が表示されます。このような失敗は、VDAとUniversal Print ServerのSSL/TLSプロトコルバージョンが一致しない場合に発生する可能性があります。

Universal Print Serverのホスト名を含む以下のポリシー設定で、Universal Print ServerのFQDNを使用します。

- セッションプリンター
- プリンターの割り当て
- 負荷分散用のUniversal Print Server

Universal Print ServerとVDAでシステムクロック（日付、時刻、タイムゾーン）が正しいことを確認してください。

仮想チャネル許可リスト

仮想チャネル許可リストは、Citrix以外の仮想チャネルのうち、どのチャネルを環境で許可するかを制御できる機能です。デフォルトでは、仮想チャネル許可リスト機能は有効になっています。その結果、Citrix Virtual Apps and Desktops™セッションでは、Citrix仮想チャネルのみが開くことが許可されます。自社製またはサードパーティ製のカスタム仮想チャネルを使用する必要がある場合は、それらを明示的に許可リストに追加する必要があります。

構成

仮想チャネル許可リストはデフォルトで有効になっています。この機能は、Citrixポリシーの以下の設定を使用して構成できます。

- **仮想チャネル許可リスト**: この機能を有効または無効にし、仮想チャネルをリストに追加します。
- **仮想チャネル許可リストログのスロットリング**: 仮想チャネル許可リストのイベントログのスロットリング期間を設定します。
- **仮想チャネル許可リストのログ記録**: 仮想チャネル許可リストのログレベルを設定します。

仮想チャネルを許可リストに追加する

仮想チャネルを許可リストに追加するには、以下の情報が必要です。

1. コードで定義されている仮想チャネル名。最大7文字です。例: `CTXCVC1`。
2. VDAマシン上で仮想チャネルを開くプロセスのパス。例: `C:\Program Files\Application\run.exe`。

必要な情報が揃ったら、仮想チャネル許可リストポリシー設定を使用して、仮想チャネルを許可リストに追加する必要があります。リストに仮想チャネルを追加するには、仮想チャネル名の後にコンマ、そして仮想チャネルにアクセスするプロセスのパスを入力します。複数のプロセスがある場合は、各プロセスをコンマで区切って追加できます。

単一プロセスの場合

前の例を使用して、以下のエントリをリストに追加します。

```
CTXCVC1,C:\Program Files\Application\run.exe
```

複数のプロセスの場合

複数のプロセスがある場合は、次のエントリをリストに追加します。

```
CTXCVC1,C:\Program Files\Application\run.exe,C:\Program Files\Application\run2.exe
```

ワイルドカードの使用

ワイルドカード (*) の使用がサポートされています。アプリケーションのバージョンに基づいてディレクトリ名または実行可能ファイル名が変更される場合、またはサードパーティコンポーネントがユーザープロファイルにインストールされている場合に、ワイルドカードを使用できます。

次のシナリオでワイルドカードを使用できます。

- 完全なディレクトリ名を置き換える場合。 例: `C:\Program Files\Application*\run1.exe`
- ディレクトリ名の一部を置き換える場合。 例: `C:\Program Files\Application\v*\run1.exe`
- 実行可能ファイル名を置き換える場合。 例: `C:\Program Files\Application\v1.2*.exe`
- 実行可能ファイル名の一部を置き換える場合。 例: `C:\Program Files\Application\v1.2\run*.exe`

次の制限が適用されます。

- ワイルドカードは、単一のディレクトリを置き換えるためにのみ使用できます。たとえば、実行可能ファイルが `C:\Program Files\Application\v1.2\run1.exe` にある場合
  - 許可: `C:\Program Files\Application*\run1.exe`
  - 不許可: `C:\Program Files*\run1.exe`
- エントリにはファイル名拡張子を含める必要があります。
  - 許可: `C:\Program Files\Application\v1.2*.exe`
  - 不許可: `C:\Program Files\Application\v1.2*`
- すべてのパスはローカルである必要があります。

注：

- ネットワークパスは許可されていません。
- ワイルドカードのサポートは、Citrix Virtual Apps and Desktops 2206から利用可能です。
- ワイルドカードのサポートは、Citrix Virtual Apps and Desktops 2203 LTSRのCU2から利用可能です。

システム環境変数の使用

許可リスト内の信頼されたプロセスの定義を簡素化するために、システム環境変数を使用できます。`%programfiles%`、`%programfiles(x86)%`、`%systemdrive%`、`%systemroot%`などの標準変数を使用できます。

システムレベルで定義されている限り、カスタム環境変数も使用できます。

以下の例は、標準の環境変数を示しています。

- `%programfiles%\Application\v1.2\run.exe`
- `%programfiles%\Application*\run.exe`
- `%programfiles(x86)%\Application\v1.*\run.exe`

以下の例は、カスタムシステム環境変数を示しています。

- カスタム変数名: `app`
- カスタム変数値: `%programfiles%\Application\`
- 許可リストエントリ: `CTXCVC1,%app%\run.exe`

> **注：**
>
> ユーザー環境変数はサポートされていません。

> 環境変数のサポートは、Citrix Virtual Apps and Desktopsバージョン2209以降で利用可能です。

仮想チャネル名とプロセスを取得する

VDAマシン上で仮想チャネル名とそれを開くプロセスを取得する最も簡単な方法は、仮想チャネルを提供した開発者またはサードパーティベンダーから情報を入手することです。

または、機能のログを適用し、以下の手順に従って情報を取得することもできます。

1. カスタム仮想チャネルのクライアントおよびサーバーコンポーネントが配置されたら、仮想アプリケーションまたは仮想デスクトップを起動します。
2. VDAマシンのシステムイベントログで、カスタム仮想チャネルの名前と、それを開こうとしたプロセスを探します。利用可能なイベントの詳細については、「イベントログ」を参照してください。

3. セッションからログアウトします。
4. 識別された仮想チャネルとプロセスに対して、仮想チャネル許可リストポリシー設定にエントリを追加します。
5. マシンを再起動します。
6. VDAが登録されたら、仮想アプリケーションまたは仮想デスクトップを実行して、カスタム仮想チャネルが正常に開くことを検証します。

Citrix仮想チャネルに関する考慮事項

すべての組み込みCitrix仮想チャネルは信頼されており、追加設定なしで開くことができます。ただし、以下の2つの機能は、外部依存関係のため、許可リストに明示的なエントリが必要です。

- マルチメディアリダイレクト
- スカイプ フォー ビジネス 用 HDX RealTime Optimization Pack

マルチメディアリダイレクト

Windows Media Player以外のメディアプレーヤーをシステムメディアプレーヤーとして使用する場合、それを信頼されたプロセスとして許可リストに追加する必要があります。許可リストのエントリには、以下の情報が必要です。

- 仮想チャネル名: `CTXMM`
- プロセス: VDAマシンで使用されるメディアプレーヤーへのパス。例: `C:\Program Files (x86)\Windows Media Player\wmplayer.exe`。
- 許可リストエントリ: `CTXMM,C:\Program Files (x86)\Windows Media Player\wmplayer.exe`

スカイプ フォー ビジネス 用 HDX RealTime Optimization Pack

許可リストのエントリには、以下の情報が必要です。

- 仮想チャネル名: `CTXRMEP`
- プロセス: VDAマシン内のSkype for Business実行可能ファイルへのパス。これはSkype for Businessのバージョンやカスタムインストールパスの使用によって異なる場合があります。例: `C:\Program Files\Microsoft Office\root\Office16\lync.exe.`.
- 許可リストエントリ: `CTXRMEP,C:\Program Files\Microsoft Office\root\Office16\lync.exe`

VDA と Delivery Controller™ 間の WebSocket 通信

この記事では、VDA と Delivery Controller 間の通信用に WebSocket 接続を設定する方法について説明します。

概要

WebSocket プロトコルは Citrix Brokering Protocol 上で動作し、Delivery Controller と VDA 間の安定した通信を促進します。 通信に WebSocket プロトコルを使用すると、次の利点があります。

- VDA から Delivery Controller への通信には、TLS ポート 443 のみが必要です。
- VDA と Delivery Controller 間のシームレスで信頼性の高い通信チャネルを提供します。

動作の仕組み

次のセクションでは、Delivery Controller と VDA 間の WebSocket 接続のワークフローについて説明します。

1. Citrix Virtual Apps and Desktops™ 管理者は、Machine Creation Service (MCS) を使用して VDA をプロビジョニングすることでプロセスを開始します。
2. MCS プロビジョニングプロセス中に、MCS は各 VDA の公開鍵と秘密鍵のペアを生成し、公開鍵を Delivery Controller 上の FMA 信頼サービスに登録します。MCS は、公開鍵と秘密鍵のペアを VDA の ID ディスク下のファイルとして保存します。
3. VDA マシンが起動すると、VDA マシンにインストールされている MCS エージェントは、ID ディスクからキーペアを読み取り、この情報を VDA レジストリの場所に書き込みます。
4. VDA にインストールされているブローカーエージェントは、レジストリからキーペアを読み取り、秘密鍵で署名されたサービスキーを使用して、SSL 対応の WebSocket リクエストを Delivery Controller に生成します。
5. Delivery Controller は、FMA 信頼サービスからの公開鍵を使用して、署名されたサービスキー認証ヘッダーを検証します。
6. 検証が完了すると、システムは VDA と Delivery Controller 間の WebSocket 接続を確立します。

AD 参加済み VDA の WebSocket サポート

始める前に

1. サイトを構成します。詳しくは、「サイトの作成」を参照してください。

2. Delivery Controller に TLS 証明書をインストールします。詳しくは、「Controller に TLS サーバー証明書をインストールする」を参照してください。
3. Delivery Controllerを信頼するために、ルートCAと中間CAをVDAにインストールします。

手順

WebSocket接続をセットアップするには、以下の手順に従います。

1. Delivery ControllerでWebSocket接続を有効にします。サイトにある各Delivery Controllerで次のコマンドを実行します。

   ```
   New-ItemProperty "HKLM:\SOFTWARE\Citrix\DesktopServer\WorkerProxy" -Name "WebSocket_Enabled" -PropertyType "DWord" -Value 1 -Force
   ```

   > **注:**
   >
   > WebSocketを有効にした後、必ずDelivery Controllerを再起動してください。

2. MCSプロビジョニングを使用して、AD参加済みVDA用のマシンカタログを作成します。詳しくは、「マシンカタログの作成」を参照してください。
3. デリバリーグループを作成し、VDAを追加します。詳しくは、「デリバリーグループの作成」を参照してください。
4. VDAでWebSocket接続を有効にします。VDAで次のコマンドを実行します。

   ```
   New-ItemProperty "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CitrixBrokerAgent\WebSocket" -Name "Enabled" -PropertyType "DWord" -Value 1 -Force
   ```

   - VDAがWebSocket経由でサーバーに接続されているかどうかを確認するには、次のレジストリキー値を確認します。

     キー:

     ```
     HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CitrixBrokerAgent\WebSocket
     ```

     名前: Connected

     種類: REG_DWORD

値: 1または0

1: VDAがWebSocketを使用してサーバーに接続されています。

0 : VDAがWebSocket経由でサーバーに到達できないか、WebSocketが有効になっていません。

- WebSocketが有効になっているかどうかを確認するには、次のレジストリキー値を確認します。`Enabled`の値は1である必要があります。

  キー:

  ```
  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CitrixBrokerAgent\WebSocket
  ```

  名前: 有効

  種類: REG_DWORD

  値: 1

HDX™ 接続性

Citrix HDXは、あらゆるデバイスおよびあらゆるネットワーク上で、集中型アプリケーションおよびデスクトップのユーザーに高精細なエクスペリエンスを提供する幅広いテクノロジーのセットを表しています。

HDXは、次の3つの技術原則に基づいて設計されています。

- インテリジェントなリダイレクト
- 適応型圧縮
- データ重複排除

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

HDXの提供機能内で、独自のプロプライエタリなトランスポートプロトコルを介して接続し、セッション確立時に最大伝送ユニットを利用し、Citrix SD-WANで接続を最適化できます。

アダプティブトランスポート

アダプティブトランスポートは、Citrix Virtual Apps and Desktops™のメカニズムであり、優先トランスポートプロトコルを使用してHDXセッションの接続を確立し、優先プロトコルでの接続が利用できない場合はTCPへのフォールバックを提供します。

次のトランスポートプロトコルがサポートされています。

- エンライトンド データ トランスポート (EDT)
- 伝送制御プロトコル (TCP)

構成

アダプティブトランスポートはデフォルトで有効になっています。アダプティブトランスポートは、次のモードで動作するように構成できます。

- **優先**: (デフォルト) クライアントは優先プロトコルで接続を試行し、優先プロトコルでの接続が利用できない場合はTCPにフォールバックします。

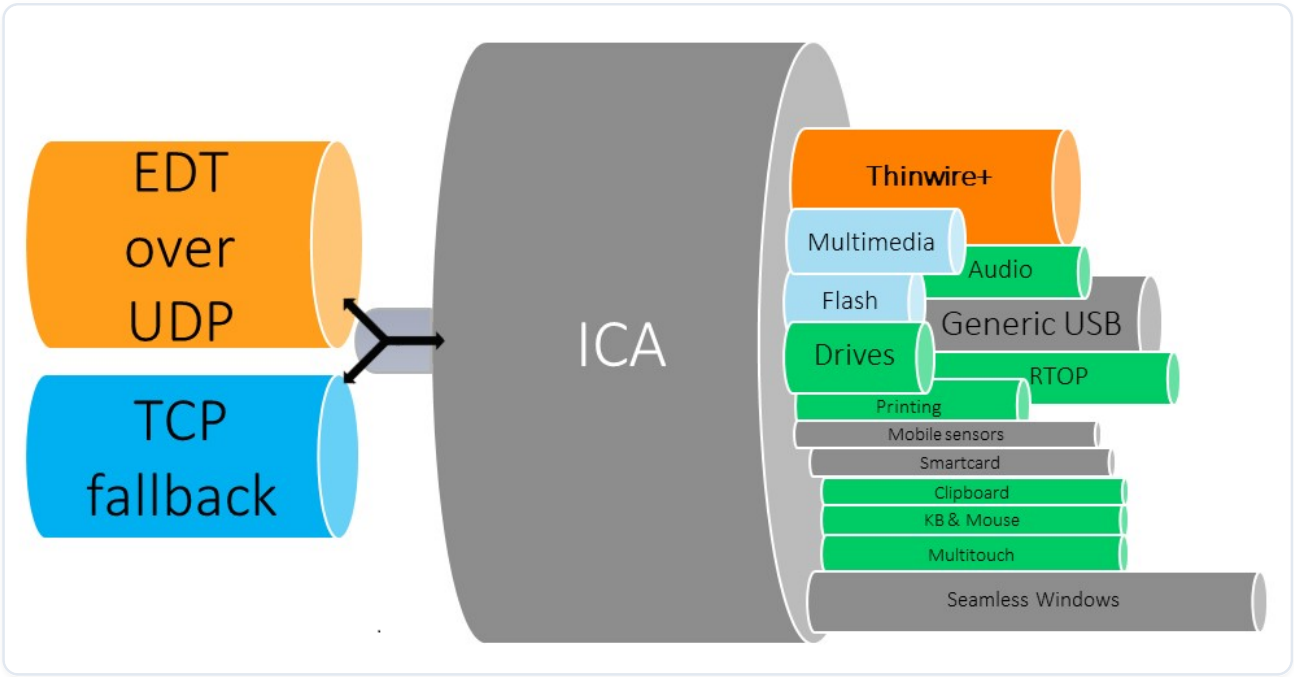
- **診断モード**: クライアントは優先プロトコルのみを使用して接続を試行します。TCPへのフォールバックは無効になります。
- **オフ**: クライアントはTCPのみを使用して接続を試行します。

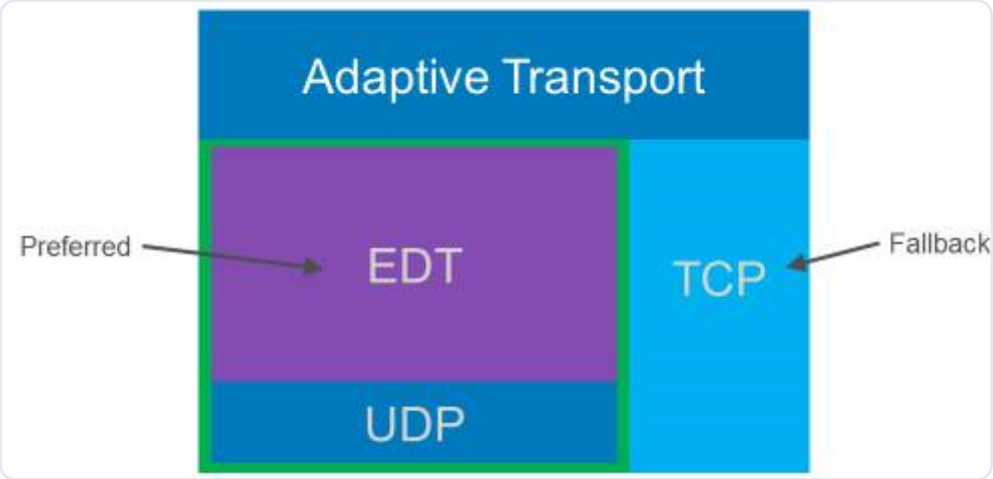
動作の仕組み

アダプティブトランスポートが`Preferred`に設定されている場合、クライアントは優先プロトコルとTCPの両方を使用してセッションに並行して接続を試行します。これにより、優先プロトコルで接続できない場合にクライアントがTCPの使用にフォールバックする必要がある場合でも、接続時間を最適化できます。TCPを使用して接続が確立された場合、クライアントは5分ごとにバックグラウンドで優先プロトコルでの接続を試行します。

アダプティブトランスポートが`Diagnostic mode`に設定されている場合、クライアントは優先プロトコルのみを使用してセッションに接続します。クライアントが優先プロトコルを使用して接続を確立できない場合、TCPへのフォールバックは行われず、接続は失敗します。

アダプティブトランスポートが`Off`に設定されている場合、**アダプティブトランスポート**は無効になり、クライアントはTCPのみを使用してセッションに接続します。





システム要件

アダプティブトランスポートとEDTを使用するための要件は次のとおりです。

- コントロールプレーン
  - シトリックス DaaS (旧称: シトリックス バーチャル アプリケーションズ アンド デスクトップ サービス)
  - Citrix Virtual Apps and Desktops: 現在サポートされているバージョン
- バーチャル デリバリー エージェント
  - Windows: 現在サポートされているバージョン (2402以降を推奨)
  - Linux: 現在サポートされているバージョン (2402以降を推奨)
- シトリックス ワークスペース™ アプリ
  - Windows: 現在サポートされているバージョン (2402以降を推奨)
  - Linux: 現在サポートされているバージョン (2402以降を推奨)
  - Mac: 現在サポートされているバージョン (2402以降を推奨)
  - iOS: Apple App Storeで入手可能な最新バージョン
  - Android: Google Playで入手可能な最新バージョン
- Citrix NetScaler® ゲートウェイ
  - 14.1.12.30以降 (推奨)
  - 13.1.17.42以降 (13.1-52.19以降を推奨)

> **注：**

Linux VDAの詳細については、Linux Virtual Delivery Agentのドキュメントを参照してください。

ネットワーク要件

以下は、アダプティブトランスポートでEDTを使用するためのネットワーク要件です。

セッションホスト

セッションホストにWindows Defender ファイアウォールなどのファイアウォールがある場合、内部接続のために以下のインバウンドトラフィックを許可する必要があります。

説明	送信元	プロトコル	ポート
内部接続 - セッションの信頼性が有効	クライアント	UDP	2598
内部接続 - セッションの信頼性が無効			1494
内部接続 - HDX™ DirectまたはVDA SSL			443

注：

VDAインストーラーは、Windows Defender ファイアウォールに適切な受信規則を追加します。別のファイアウォールを使用している場合は、上記の規則を追加する必要があります。

内部ネットワーク

以下の表は、ネットワークでEDTを使用するために必要なファイアウォール規則を示しています。

説明	プロトコル	送信元	宛先	宛先ポート
直接内部接続 - セッションの信頼性が有効	UDP	クライアントネットワーク	VDAネットワーク	2598

説明	プロトコル	送信元	宛先	宛先ポート
直接内部接続 - セッションの信頼性が無効				1494
直接内部接続 - HDX DirectまたはVDA SSL				443
ネットスケーラー ゲートウェイ		NetScaler SNIP		2598
ネットスケーラー ゲートウェイ - VDA SSL				443

注：

Citrix Gateway Serviceを使用している場合、トランスポートプロトコルとしてEDTを使用するには、**Rendezvous**を有効にする必要があります。システムおよびネットワーク要件については、Rendezvousのドキュメントを参照してください。

クライアントネットワーク

以下の表は、クライアントデバイスの接続要件を示しています。

説明	プロトコル	送信元	宛先	宛先ポート
内部接続 - セッションの信頼性が有効	UDP	クライアントIP	VDAネットワーク	2598
内部接続 - セッションの信頼性が無効				1494

説明	プロトコル	送信元	宛先	宛先ポート
内部接続 - HDX Directまたは SSL VDA				443
外部接続 - NetScaler Gateway			NetScaler GatewayのパブリックIPアドレス	443
外部接続 - Citrix Gateway Service			シトリックスゲートウェイサービス	443

注：

Citrix Gateway Serviceを使用している場合、クライアントは`<https://*.*.nssvc.net>`に到達できる必要があります。`<https://*.*.nssvc.net>`を使用してすべてのサブドメインを許可できない場合は、代わりに`<https://*.c.nssvc.net>`と`<https://*.g.nssvc.net>`を使用できます。詳細については、Knowledge Centerの記事CTX270584を参照してください。

適応型データ転送

Enlightened Data Transport (EDT) は、User Datagram Protocol (UDP) 上に構築されたCitrix独自のトランスポートプロトコルです。これは、困難な長距離接続で優れたユーザーエクスペリエンスを提供し、サーバーのスケーラビリティを維持します。EDTは、信頼性の低いネットワーク上のすべてのICA®仮想チャネルのデータスループットを向上させ、より良く、より一貫したユーザーエクスペリエンスを提供します。

Adaptive Transport が有効になっている場合、EDTが優先プロトコルです。

知っておくべきこと

- NetScaler® GatewayおよびCitrix Gateway Serviceで**MTU Discovery**とEDTを使用するには、**Session Reliability**を有効にする必要があります。
- パケットの断片化は、パフォーマンスの低下や、場合によってはセッションを開くことの失敗を引き起こす可能性があります。これを防ぐには、EDT MTUをネットワークに適した値に調

整する必要があります。EDT MTU Discoveryを使用するか、非標準MTUのネットワークでEDTを使用する場合のMSSの構成方法で説明されている手動の回避策を使用できます。

- NetScaler GatewayでEDTの使用を有効にする方法の詳細については、NetScaler GatewayでEnlightened Data Transportをサポートするように構成するを参照してください。

EDT MTU検出

MTU Discoveryにより、EDTはセッション確立時に最大転送単位 (MTU) を自動的に決定できます。これにより、パフォーマンスの低下やセッション確立の失敗につながる可能性のあるEDTパケットの断片化を防ぎます。

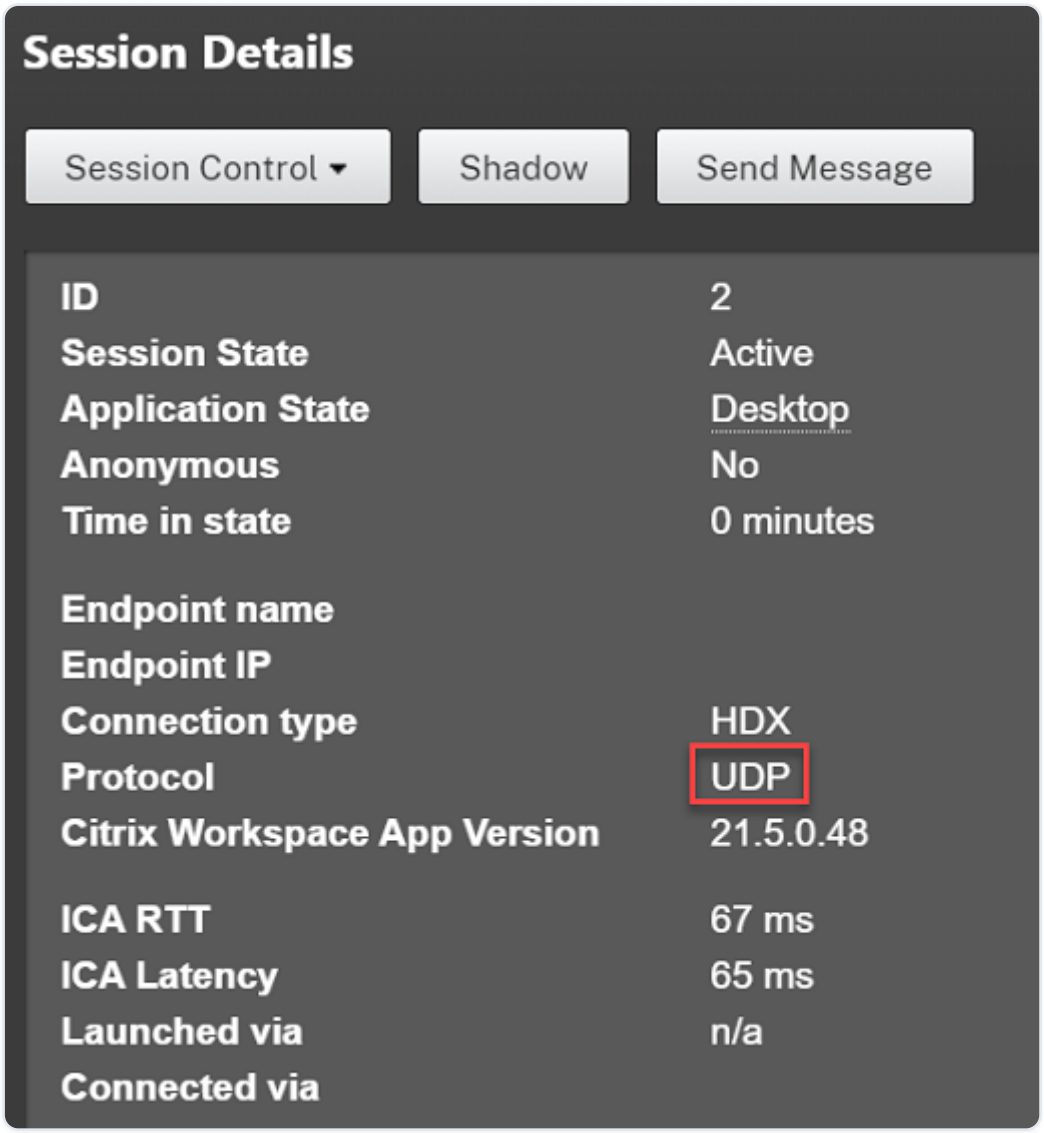
MTU Discoveryはデフォルトで有効になっています。無効にする必要がある場合は、詳細についてレジストリで管理されるHDX機能を参照してください。

> **注：**
>
> - MTU Discoveryが機能するには、**Session Reliability**を有効にする必要があります。
> - Multi-Stream ICAでのMTU Discoveryは、VDAバージョン2209以降で利用可能です。

トラブルシューティング

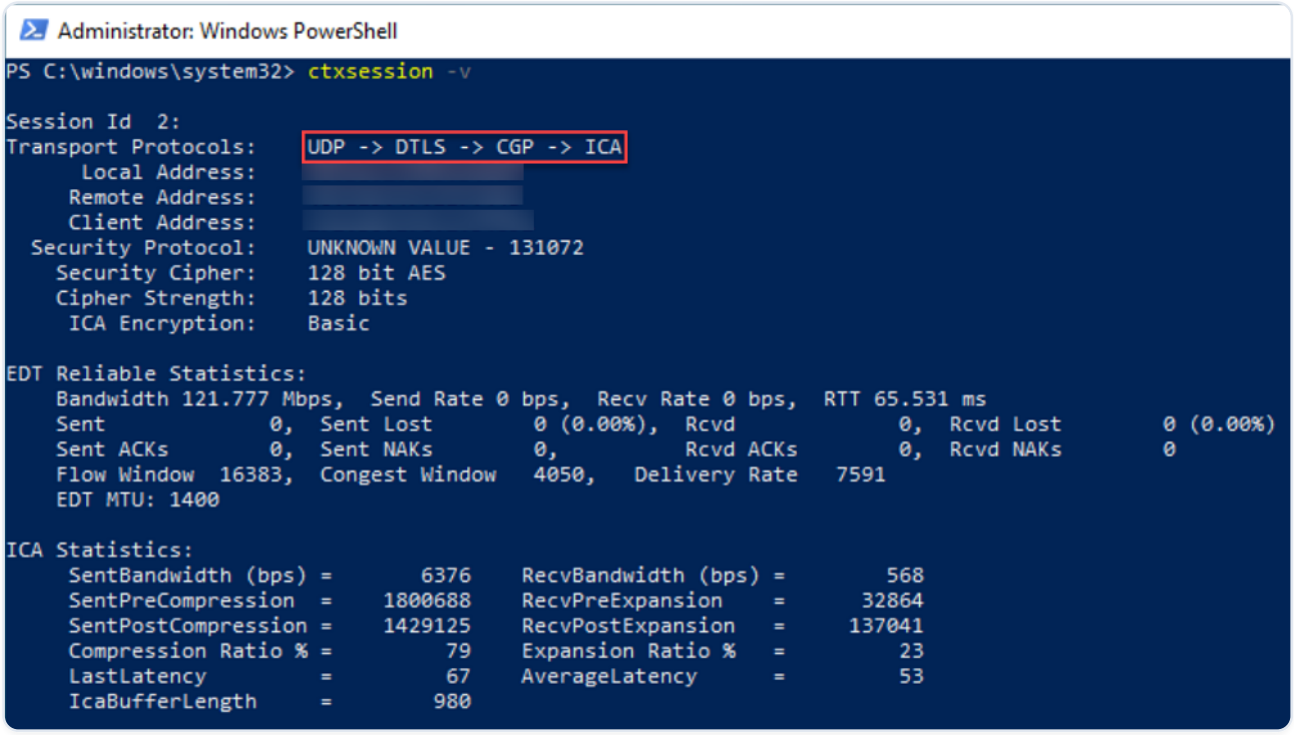
セッションのトランスポートプロトコルとしてEDTが使用されていることを確認するには、DirectorまたはVDA上の`CtxSession.exe`コマンドラインユーティリティを使用できます。

Directorでセッションを検索し、**詳細**を選択します。**接続の種類**が`HDX`で、**プロトコル**が`UDP`の場合、EDTがセッションのトランスポートプロトコルとして使用されています。



CtxSession.exeユーティリティを使用するには、セッション内でコマンドプロンプトまたはPowerShellを起動し、`ctxsession.exe`を実行します。詳細な統計情報を表示するには、`ctxsession.exe -v`を実行します。EDTが使用されている場合、トランスポートプロトコルは次のいずれかを表示します。

- **UDP > ICA®** (セッションの信頼性が無効)
- **UDP > CGP > ICA** (セッションの信頼性が有効)
- **UDP > DTLS > CGP > ICA** (ICAはDTLSでエンドツーエンド暗号化されています)



EDTでセッションが接続に失敗する場合

Adaptive Transportと**EDT**のトラブルシューティングには、以下をお勧めします。

1. システム要件、ネットワーク要件、既知の問題、および留意事項を確認し、すべての項目が対処されていることを確認してください。
2. StudioまたはGPOに、目的の**HDX Adaptive Transport**設定を上書きするCitrix®ポリシーがないか確認します。
3. クライアントに、目的のHDX Adaptive Transport設定を上書きする設定がないか確認します。これは、GPO設定、オプションのWorkspace app管理テンプレートを使用して構成された設定、またはレジストリまたはクライアントの構成ファイルにおける**HDXoverUDP**設定の手動構成である可能性があります。
4. マルチセッションVDAマシンで、UDPリスナーがアクティブであることを確認します。VDAマシンでコマンドプロンプトを開き、`netstat -a -p udp`を実行します。詳細については、「HDX Enlightened Data Transportプロトコルを確認する方法」を参照してください。
5. ネットワークファイアウォールとVDAマシンで実行されているファイアウォールの両方で、適切なファイアウォールルールが構成されているか確認します。
6. NetScaler® GatewayまたはCitrix Gateway Serviceをバイパスして、内部で直接セッションを起動し、使用中のプロトコルを確認します。セッションがEDTを使用している場合、VDAはNetScaler GatewayまたはCitrix Gateway Serviceを介した外部接続にEDTを使用する準備ができています。

7. EDTが直接内部接続では機能するが、NetScaler GatewayまたはCitrix Gateway Serviceを介するセッションでは機能しない場合：
   - **セッションの信頼性**が有効になっていることを確認します。
   - NetScaler Gatewayを使用している場合は、Enlightened Data TransportおよびHDX Insightをサポートするように NetScaler Gatewayを構成するに記載されている必要な構成に準拠していることを確認してください。
8. Citrix Gateway Serviceを使用している場合は、Rendezvousが有効になっていて機能していることを確認します。
9. ユーザーの接続に非標準のMTUが必要かどうかを確認します。実効MTUが1500バイト未満の接続では、EDTパケットの断片化が発生し、パフォーマンスに影響を与えたり、セッション起動の失敗を引き起こしたりする可能性があります。この問題は、VPN、一部のWi-Fiアクセスポイント、および4Gや5Gなどのモバイルネットワークを使用する場合によく発生します。MTU検出が有効になっているか、非標準MTUのネットワークでEDTを使用する場合のMSSの構成方法に記載されているようにカスタムMTUを設定していることを確認してください。

既知の問題

- 非対称ネットワークパスは、NetScaler GatewayまたはCitrix Gateway Serviceを介さない接続でMTU検出が失敗する原因となる可能性があります。この問題に対処するには、VDAバージョン2103以降にアップグレードしてください。
- NetScaler Gatewayを使用している場合、非対称ネットワークパスはMTU検出が失敗する原因となる可能性があります。これは、Gatewayの問題により、EDTパケットヘッダーのDon't Fragment（DF）ビットが伝播されないためです。この問題の修正は、ファームウェアリリース13.1ビルド17.42以降で利用可能です。修正を有効にする方法の詳細については、NetScaler Gatewayのドキュメントを参照してください。
- DS-Liteネットワークを介して接続するユーザーの場合、MTU検出が失敗することがあります。一部のモデムでは、パケット処理が有効になっている場合にDFビットが尊重されず、MTU検出が断片化を検出できなくなります。この状況では、以下のオプションが利用可能です。
  - ユーザーのモデムでパケット処理を無効にします。
  - **MTU検出**を無効にし、非標準MTUのネットワークでEDTを使用する場合のMSSの構成方法に記載されているようにハードコードされたMTUを使用します。
  - セッションにTCPの使用を強制するために**アダプティブトランスポート**を無効にします。ユーザーの一部のみが影響を受ける場合は、他のユーザーがEDTを引き続き使用できるように、クライアント側で無効にすることを検討してください。

HDX™ ダイレクト

Citrixが提供するリソースにアクセスする場合、HDX Directは、直接通信が可能な場合、内部および外部のクライアントデバイスがセッションホストとの安全な直接接続を確立することを可能にします。

システム要件

HDX Directを使用するためのシステム要件は以下のとおりです。

- コントロールプレーン
  - シトリックス DaaS™
  - シトリックス Virtual Apps and Desktops™ 2503 以降
- 仮想配信エージェント (VDA)
  - Windows: バージョン 2503 以降
- Workspaceアプリ
  - Windows: バージョン 2503 以降
  - Linux: バージョン 2411 以降
  - Mac: バージョン 2411 以降
- アクセス層
  - シトリックス ワークスペース™
  - シトリックス ストアフロント™ 2503 以降
  - シトリックス ゲートウェイ サービス
  - Citrix NetScaler® ゲートウェイ

ネットワーク要件

HDX Directを使用するためのネットワーク要件は以下のとおりです。

セッションホスト

セッションホストにWindows Defender ファイアウォールなどのファイアウォールがある場合、内部接続のために以下のインバウンドトラフィックを許可する必要があります。

説明	送信元	プロトコル	ポート
直接内部接続	クライアント	TCP	443
直接内部接続	クライアント	UDP	443

> 注:
>
> VDA インストーラーは、Windows Defender ファイアウォールに適切な受信規則を追加します。別のファイアウォールを使用する場合は、上記の規則を追加する必要があります。

クライアントネットワーク

以下の表は、内部および外部ユーザー向けのクライアントネットワークについて説明しています。

内部ユーザー

説明	プロトコル	送信元	ソースポート	宛先	宛先ポート
直接内部接続	TCP	クライアントネットワーク	1024–65535	VDAネットワーク	443
直接内部接続	UDP	クライアントネットワーク	1024–65535	VDAネットワーク	443

外部ユーザー

説明	プロトコル	送信元	ソースポート	宛先	宛先ポート
STUN (外部ユーザーのみ)	UDP	クライアントネットワーク	1024–65535	インターネット (下記の注記を参照)	3478, 19302
外部ユーザー接続	UDP	クライアントネットワーク	1024–65535	データセンターのパブリックIPアドレス	1024–65535

データセンターネットワーク

以下の表は、内部ユーザーと外部ユーザー向けのデータセンターネットワークについて説明しています。

内部ユーザー

説明	プロトコル	送信元	ソースポート	宛先	宛先ポート
直接内部接続	TCP	クライアントネットワーク	1024–65535	VDAネットワーク	443
直接内部接続	UDP	クライアントネットワーク	1024–65535	VDAネットワーク	443

外部ユーザー

説明	プロトコル	送信元	ソースポート	宛先	宛先ポート
STUN (外部ユーザーのみ)	UDP	VDAネットワーク	1024–65535	インターネット (下記の注記を参照)	3478, 19302
外部ユーザー接続	UDP	DMZ / 内部ネットワーク	1024–65535	VDAネットワーク	55000–55250
外部ユーザー接続	UDP	VDAネットワーク	55000–55250	クライアントのパブリックIP	1024–65535

注：

VDAとWorkspaceアプリの両方が、以下のサーバーに同じ順序でSTUNリクエストを送信しようとします。

- stun.cloud.com:3478

- stun.cloudflare.com:3478
- stun.l.google.com:19302

HDX Directポート範囲ポリシー設定を使用して外部ユーザー接続のデフォルトポート範囲を変更する場合、対応するファイアウォール規則はカスタムポート範囲と一致する必要があります。

構成

HDX Directはデフォルトで無効になっています。この機能は、Citrixポリシーの**HDX Direct**設定を使用して構成できます。

- **HDX Direct**: 機能を有効または無効にする。
- 「**HDX Directモード**」：**HDX Direct**が内部クライアントのみで利用可能か、内部クライアントと外部クライアントの両方で利用可能かを決定します。
- 「**HDX Directポート範囲**」：VDAが外部クライアントからの接続に使用するポート範囲を定義します。

必要に応じて、HDX Directで使用されるSTUNサーバーのリストは、以下のレジストリ値を編集することで変更できます。

- キー：HKLM\SOFTWARE\Citrix\HDX-Direct
- 値の型: REG_MULTI_SZ
- 値の名前：STUNServers
- データ：stun.cloud.com:3478 stun.cloudflare.com:3478 stun.l.google.com:19302

注：

外部ユーザー向けのHDX Directは、トランスポートプロトコルとしてEDT (UDP) を使用する場合にのみ利用可能です。したがって、アダプティブトランスポートを有効にする必要があります。

考慮事項

HDX Directを使用する際の考慮事項は次のとおりです。

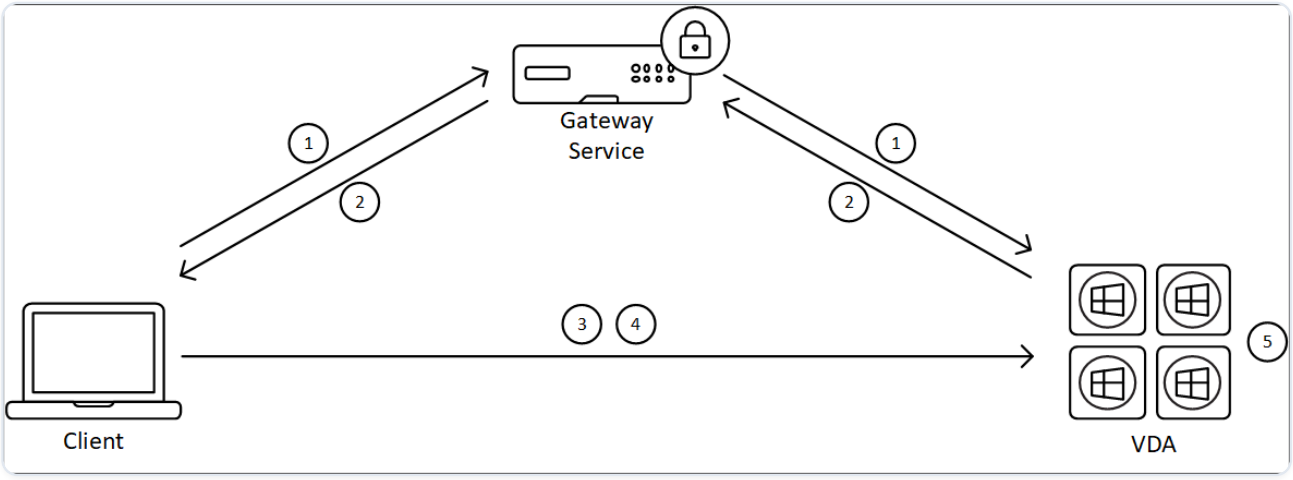
- 外部ユーザー向けのHDX Directは、トランスポートプロトコルとしてEDT (UDP) を使用する場合にのみ利用可能です。したがって、**アダプティブトランスポート**を有効にする必要があります。
- **HDX Insight**を使用している場合、**HDX Direct**を使用すると、セッションがNetScaler Gatewayを介してプロキシされなくなるため、HDX Insightのデータ収集が妨げられることに注意してください。
- マルチセッションセッションホスト環境では、HDX Directはユーザーログオンが1分以内に完了することを要求します。ログオン時間がこのしきい値を超えると、HDX Directはトリガーされず、セッションはGatewayを介して接続されたままになります。より長いログオン時間をサポートするために、HDX Directのタイムアウトを増やすことができます。詳細については、レジストリで管理されるHDX機能を参照してください。

動作の仕組み

HDX Directを使用すると、直接通信が可能な場合にクライアントがセッションホストへの直接接続を確立できます。HDX Directを使用して直接接続が行われる場合、自己署名証明書が使用され、ネットワークレベルの暗号化 (TLS/DTLS) で直接接続を保護します。

内部ユーザー

次の図は、内部ユーザーのHDX Direct接続プロセスの概要を示しています。



1. クライアントはGateway Serviceを介してHDXセッションを確立します。
2. 接続が成功すると、VDAはHDX接続を介して、VDAマシンのFQDN、そのIPアドレスのリスト、およびVDAマシンの証明書をクライアントに送信します。
3. クライアントは、VDAに直接到達できるかどうかを確認するためにIPアドレスをプローブします。

4. クライアントが共有されたいずれかのIPアドレスでVDAに直接到達できる場合、クライアントはVDAとの直接接続を確立します。この接続は、手順(2)で交換された証明書と一致する証明書を使用して(D)TLSで保護されます。
5. 直接接続が正常に確立されると、セッションは新しい接続に転送され、Gateway Serviceへの接続は終了します。

> **注：**
>
> 上記の手順2で接続を確立した後、セッションはアクティブになります。その後の手順は、ユーザーが仮想アプリケーションまたはデスクトップを使用する能力を遅延させたり、妨げたりすることはありません。その後の手順のいずれかが失敗した場合でも、Gatewayを介した接続はユーザーのセッションを中断することなく維持されます。

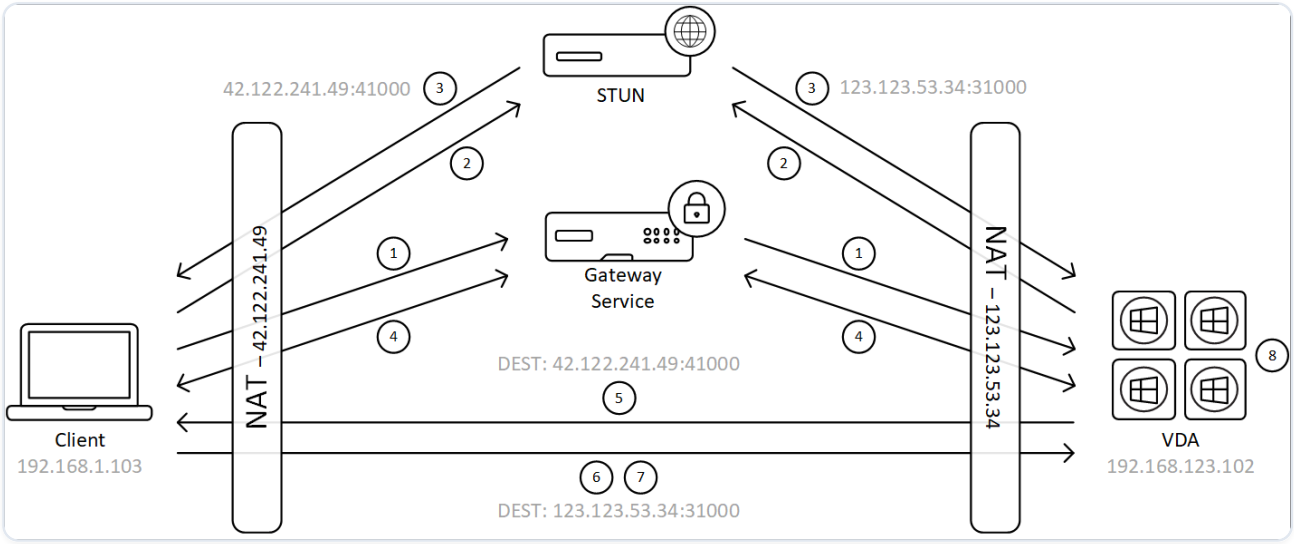
従来の直接接続

Storefront、Direct Workload Connectionを使用するWorkspace、または内部接続専用に構成されたWorkspaceを使用する場合、クライアントとセッションホスト間の直接接続は、最初にGatewayを介してルーティングする必要なく確立されます。

これらの場合、接続は本質的に直接的であるため、HDX Directはトリガーされません。ただし、HDX Directが有効になっている場合、これらの接続はHDX Direct証明書を利用してセッションを保護します。

外部ユーザー

次の図は、外部ユーザー向けのHDX Direct接続プロセスの概要を示しています。



1. クライアントはGateway Serviceを介してHDXセッションを確立します。

2. 接続が成功すると、クライアントとVDAの両方がSTUNリクエストを送信して、それぞれのパブリックIPアドレスとポートを検出します。
3. STUNサーバーは、クライアントとVDAにそれぞれのパブリックIPアドレスとポートで応答します。
4. HDX接続を介して、クライアントとVDAはそれぞれのパブリックIPアドレスとUDPポートを交換し、VDAはクライアントに証明書を送信します。
5. VDAは、クライアントのパブリックIPアドレスとUDPポートにUDPパケットを送信します。クライアントは、VDAのパブリックIPアドレスとUDPポートにUDPパケットを送信します。
6. VDAからのメッセージを受信すると、クライアントはセキュアな接続要求で応答します。
7. DTLSハンドシェイク中に、クライアントは証明書がステップ(4)で交換された証明書と一致することを確認します。検証後、クライアントは認証トークンを送信します。これでセキュアな直接接続が確立されます。
8. 直接接続が正常に確立されると、セッションは新しい接続に転送され、Gateway Serviceへの接続は終了します。

> **注：**
>
> 上記のステップ2で接続を確立した後、セッションはアクティブになります。その後の手順は、ユーザーが仮想アプリケーションまたはデスクトップを使用する能力を遅らせたり、妨げたりすることはありません。その後の手順のいずれかが失敗した場合でも、ユーザーのセッションを中断することなく、Gatewayを介した接続は維持されます。

NAT互換性

外部ユーザーデバイスとセッションホスト間の直接接続を確立するために、HDX™ DirectはNATトラバーサルのためにホールパンチングを利用し、クライアントデバイスとセッションホストのパブリックIPアドレスおよびポートマッピングの交換を容易にするためにSTUNを利用します。これは、VoIP、ユニファイドコミュニケーション、P2Pソリューションの仕組みに似ています。

ファイアウォールやその他のネットワークコンポーネントが、STUNリクエストおよびHDXセッションのUDPトラフィックを許可するように構成されている限り、外部ユーザー向けのHDX Directは機能すると予想されます。ただし、ユーザーおよびセッションホストネットワークのNATタイプが互換性のない組み合わせとなり、HDX Directが失敗する特定のシナリオがあります。

検証

クライアントおよびセッションホスト上のNATタイプとフィルタリングは、STUNTMANのSTUNクライアントユーティリティを使用して検証できます。

1. stunprotocol.orgからターゲットプラットフォームに適したパッケージをダウンロードし、その内容を抽出します。
2. ターミナルプロンプトを開き、内容が抽出されたディレクトリに移動します。
3. NATバインディングおよび動作テストを実行するには、次のコマンドを実行します。
   `stunclient.exe stunserver2025.stunprotocol.org --mode behavior`
4. バインディングテストと動作テストが成功した場合、**バインディングテスト**と**動作テスト**の両方が成功を報告し、NAT動作が指定されます。

   テストが失敗した場合、**バインディングテスト**および/または**動作テスト**が失敗を報告します。

5. NATバインディングおよびフィルタリングテストを実行するには、次のコマンドを実行します。 `stunclient.exe stunserver2025.stunprotocol.org --mode filtering`
6. バインディングテストとフィルタリングテストが成功した場合、**バインディングテスト**と**フィルタリングテスト**の両方が成功を報告し、NATフィルタリングタイプが指定されます。

   テストが失敗した場合、**バインディングテスト**および/または**フィルタリングテスト**が失敗を報告します。

上記のテストを実行した後、NATの動作とフィルタリングの組み合わせに基づいて、外部ユーザー向けのHDX Directが動作すると予想されるかどうかを判断するために、次の表を確認してください。

クライアントNATの動作	クライアントNATのフィルタリング	セッションホストNATの動作	セッションホストNATのフィルタリング	動作が期待されますか？
エンドポイント独立マッピング	任意	エンドポイント独立マッピング	任意	はい
エンドポイント独立マッピング	エンドポイント独立フィルタリング	アドレス依存マッピング	任意	はい
エンドポイント独立マッピング	アドレス依存フィルタリング	アドレス依存マッピング	任意	いいえ
エンドポイント独立マッピング	アドレスおよびポート依存フィルタリング	アドレス依存マッピング	任意	いいえ
エンドポイント独立マッピング	エンドポイント独立フィルタリング	アドレスおよびポート依存マッピング	エンドポイント独立フィルタリング	はい
エンドポイント独立マッピング	アドレス依存フィルタリング	アドレス依存マッピング	任意	いいえ
エンドポイント独立マッピング	アドレスおよびポート依存フィルタリング	アドレス依存マッピング	任意	いいえ
アドレス依存マッピング	任意	エンドポイント独立マッピング	エンドポイント独立フィルタリング	はい
アドレス依存マッピング	任意	エンドポイント独立マッピング	アドレス依存フィルタリング	いいえ
アドレス依存マッピング	任意	エンドポイント独立マッピング	アドレスおよびポート依存フィルタリング	いいえ
アドレス依存マッピング	任意	アドレス依存マッピング	任意	いいえ

クライアントNATの動作	クライアントNATのフィルタリング	セッションホストNATの動作	セッションホストNATのフィルタリング	動作が期待されますか？
アドレス依存マッピング	任意	アドレスおよびポート依存マッピング	任意	いいえ
アドレスおよびポート依存マッピング	任意	エンドポイント独立マッピング	エンドポイント独立フィルタリング	はい
アドレスおよびポート依存マッピング	任意	エンドポイント独立マッピング	アドレス依存フィルタリング	いいえ
アドレスおよびポート依存マッピング	任意	エンドポイント独立マッピング	アドレスおよびポート依存フィルタリング	いいえ
アドレスおよびポート依存マッピング	任意	アドレス依存マッピング	任意	いいえ
アドレスおよびポート依存マッピング	任意	アドレスおよびポート依存マッピング	任意	いいえ
失敗	任意	任意	任意	いいえ
任意	任意	失敗	任意	いいえ
失敗	任意	失敗	任意	いいえ

トラブルシューティング

HDX Direct が直接接続を正常に確立したことを確認するには、VDA マシンで `CtxSession.exe` ユーティリティを使用できます。

`CtxSession.exe` ユーティリティを使用するには、セッション内でコマンドプロンプトまたは PowerShell を起動し、`ctxsession.exe -v` を実行します。**HDX Direct** 接続が正常に確立されている場合、**HDX Direct Status** は `Connected` です。

HDX Direct のトラブルシューティング(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/hdx-direct-troubleshooting.png)

セッションホストのイベントログで、HDX™ Direct 接続が正常に確立されたか、または失敗したかに関する情報を確認することもできます。詳細については、「**イベントログ**」セクションを参照してください。

> 注:
>
> 環境およびセッションホストで利用可能な IP アドレスの数によっては、HDX Direct 接続が確立されるまでに最大 5 分かかる場合があります。

HDX Direct が直接接続を確立できない場合

HDX Direct が直接接続を確立できない場合は、次の手順を確認してください。

1. 使用している VDA バージョンと Workspace アプリバージョンが、システム要件に従ってこの機能をサポートしていることを確認してください。
2. HDX Direct を有効にするポリシーが VDA に適用されており、この機能を無効にする優先度の高い他のポリシーがないことを確認してください。
3. 目的の HDX Direct モードを設定するポリシーが VDA に適用されており、この構成を上書きする優先度の高い他のポリシーがないことを確認してください。
4. Citrix ClxMtp Service がセッションホストで実行されていることを確認してください。
5. Citrix Certificate Manager Service がセッションホストで実行されていることを確認してください。実行されていない場合は、手動で開始してみてください。HDX Direct が無効になっている場合、このサービスは自動的に停止します。
6. セッションホストに自己署名ルート CA 証明書があるかどうかを確認します。
    a. 発行先: `CA-<hostname>` (例: CA-FTLW11-001)
    b. 発行元: `CA-<hostname>` (例: CA-FTLW11-001)
    c. 発行者情報: 組織はCitrix Systems, Inc.です。
7. セッションホストに自己署名サーバー証明書があるか確認します。
    a. 発行先: `<host FQDN>` (例: FTLW11-001.ctxlab.net)
    b. 発行元: `CA-<hostname>` (例: CA-FTLW11-001)
    c. 発行者情報: 組織はCitrix Systems, Inc.です。

8. 証明書が見つからない場合は、Citrixテクニカルサポートにお問い合わせください。
9. 証明書が存在する場合:
    a. セッションホストでCitrix Certificate Manager Serviceを停止します。
    b. 自己署名ルートCA証明書と自己署名サーバー証明書の両方を削除します。
    c. セッションホストでCitrix Certificate Manager Serviceを開始します。サービスは開始されると新しい証明書を作成します。
10. 内部ユーザーの場合:
    a. セッションホストのファイアウォールが、HDX over EDTの場合はUDP 443、HDX over TCPの場合はTCP 443の受信トラフィックをブロックしていないことを確認します。
    b. クライアントネットワークとセッションホストネットワーク間のUDP 443およびTCP 443のトラフィックをネットワークファイアウォールがブロックしていないことを確認します。
11. 外部ユーザーの場合:
    a. クライアントとセッションホストのNATタイプを確認し、その組み合わせが正常に機能することを確認します。詳細については、「NAT互換性」セクションを参照してください。
    b. クライアントまたはセッションホストのいずれかでNATテストが失敗した場合:
        i. システムでファイアウォールが実行されている場合は、UDP 3478での送信トラフィックをブロックしていないことを確認してください。
        ii. ネットワークファイアウォールがUDP 3478での送信トラフィックをブロックしていないことを確認してください。
        iii. ファイアウォールがSTUNサーバーの応答をブロックしていないことを確認してください。
    c. ネットワークファイアウォールに、必要なすべてのトラフィックを許可するための適切なルールが構成されていることを確認してください。詳細については、ネットワーク要件セクションを参照してください。
    d. HDX Directポート範囲ポリシー設定を使用してデフォルトのポート範囲を変更する場合は、ファイアウォールルールがカスタムポート範囲に設定されていることを確認してください。

イベントログ

以下のイベントがVDAマシンのイベントログに記録されます:

ログ	ID	送信元	レベル	説明
アプリケーションとサービスログ > Citrix-HostCore-HDX Direct/操作	1	HDX ダイレクト	情報	内部ユーザー `<username>` のHDX Direct接続が確立されました。
アプリケーションとサービスログ > Citrix-HostCore-HDX Direct/操作	2	HDX ダイレクト	情報	外部ユーザー `<username>` のHDX Direct接続が確立されました。
アプリケーションとサービスログ > Citrix-HostCore-HDX Direct/操作	3	HDX ダイレクト	情報	ユーザー `<username>` のHDX Direct接続に失敗しました。

既知の問題

VDAのインプレースアップグレードを、すでに**HDX Direct**が有効になっているマシンで実行した後、HDX Directが動作しなくなる可能性があります。 この問題を解決するには、次の手順を実行します。

1. セッションホスト上でCitrix Certificate Managerサービスを停止します。
2. 自己署名ルートCA証明書および自己署名サーバー証明書を削除します。
3. レジストリを開きます。
4. `HKLM\Software\Citrix\HDX-Direct` キーを削除します。
5. `HKLM\SYSTEM\CurrentControlSet\Control\TerminalServer\Wds\icawd` にアクセスします。
6. **SSLEnabled** の値を `0` に設定します。
7. **SSLThumbprint** の値の内容を削除します。
8. **Citrix Certificate Managerサービス**を開始します。

セキュアHDX™

セキュアHDXは、トラフィックパス内のネットワーク要素がHDXトラフィックを検査できないようにするアプリケーションレベル暗号化 (ALE) ソリューションです。これは、AES-256-GCM暗号化を使用して、Citrix Workspace™アプリ (クライアント) とVDA (セッションホスト) の間でアプリケーションレベルで真のエンドツーエンド暗号化 (E2EE) を提供することで実現されます。

システム要件

以下の一覧は、セキュアHDXを使用するためのシステム要件を示しています。

- コントロールプレーン
  - シトリックス DaaS™
  - シトリックス Virtual Apps and Desktops™ 2503 以降
- セッションホスト
  - オペレーティングシステム
    - Windows 10 22H2 バージョン
    - Windows 11 22H2以降
    - Windows Server 2019 以降のバージョン
  - 仮想配信エージェント (VDA)
    - Windows: バージョン 2503 以降
    - Linux: バージョン2407以降
- Workspaceアプリ
  - Windows: バージョン 2503 以降
  - Linux: バージョン 2408 以降
  - Mac: バージョン 2409 以降
  - Chrome OS: バージョン 2409 以降
  - HTML5: バージョン 2408 以降
  - Android: バージョン 2503 以降
  - iOS: バージョン 2503 以降
- アクセス層

- シトリックス ワークスペース
- Citrix StoreFront™ 2402 以降

> **注：**
>
> Citrix Virtual Apps and Desktops™ 2402 LTSR のサポートは、**CU3** 以降で利用可能です。

> Linux VDA で Secure HDX を構成する方法の詳細については、Linux VDA のドキュメントを参照してください。

構成

Secure HDX はデフォルトで無効になっています。この機能は、Citrix ポリシーの Secure HDX 設定を使用して構成できます。

Secure HDX: この機能を有効にするか無効にするかを定義します。

> **重要:**
>
> Secure HDX を有効にするデリバリーグループで Secure ICA® が有効になっている場合は、まず Secure ICA を無効にする必要があります (デリバリーグループの編集 > ユーザー設定)。

考慮事項

Secure HDX を使用する際の考慮事項は次のとおりです。

- ユーザーが Secure HDX が有効なセッションホストに、その機能をサポートしないクライアントを使用して接続しようとすると、接続は拒否されます。
- Secure HDXでは、(/ja-jp/citrix-workspace/optimize-cvad/service-continuity.html#configure-service-continuity-for-connectorless-workloads)のみがサポートされています。標準バージョンのService Continuityを使用している場合、クラウドサービスが停止すると、Secure HDXが有効になっているセッションホストに接続できなくなります。
- HDX Insight を使用している場合、Secure HDX を使用すると、NetScaler® が暗号化された HDX トラフィックを検査できないため、HDX Insight のデータ収集が妨げられることに注意し

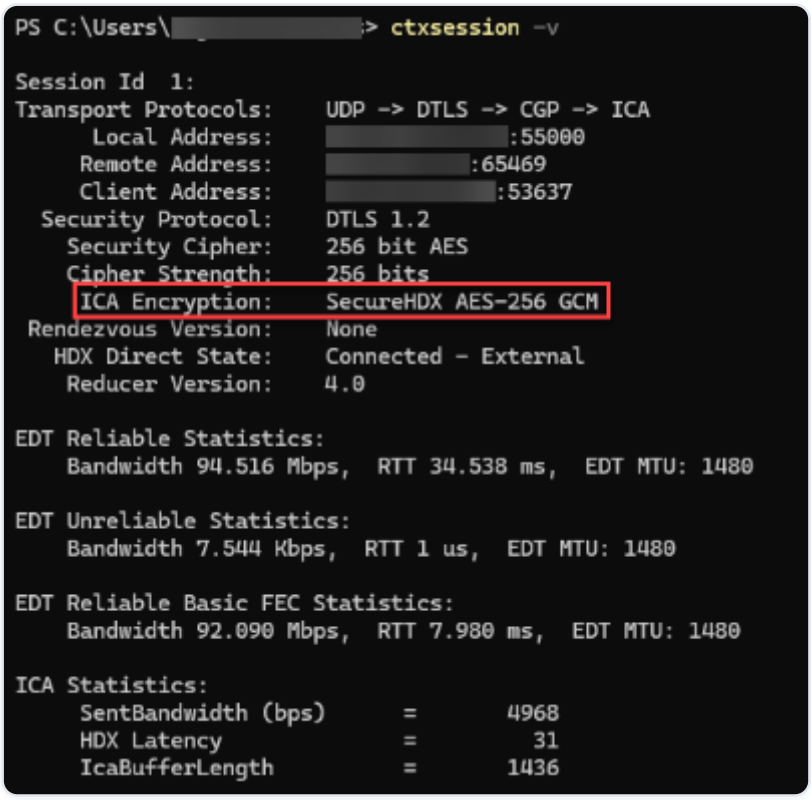
てください。HDX Insight を使用する必要がある場合は、Citrix Virtual Apps and Desktops 2503 以降にアップグレードし、ネットワーク テレメトリ を有効にする必要があります。

- SmartControl を使用している場合、Secure HDX を使用すると、NetScaler が暗号化された HDX トラフィックを検査できないため、SmartControl が機能しなくなることに注意してください。SmartControl を使用する必要がある場合は、Citrix Virtual Apps and Desktops 2503 以降にアップグレードし、ネットワーク テレメトリ を有効にする必要があります。
- Secure HDXが有効になっている場合、Multi-Stream ICAはサポートされません。
- HDXトラフィックの検査に依存するサードパーティソリューションを使用している場合、Secure HDXを有効にするとHDXトラフィックが暗号化されるため、それらのソリューションは機能しなくなります。

トラブルシューティング

Secure HDXがアクティブであることを確認するには、VDAマシンで`ctxsession.exe`ユーティリティを使用できます。

`CtxSession.exe`ユーティリティを使用するには、セッション内でコマンドプロンプトまたはPowerShellを開き、`ctxsession.exe -v`を実行します。Secure HDXが使用されている場合、ICA Encryptionには`SecureHDX AES-256 GCM`と表示されます。



セッションでSecure HDXが有効にならない場合

- 使用中のVDAバージョンがシステム要件に従ってこの機能をサポートしていることを確認してください。
- Secure HDXを有効にするポリシーがVDAに適用されており、この機能を無効にする優先度の高い他のポリシーがないことを確認してください。
- Secure HDXを構成したときにセッションホストがすでに実行されていた場合は、変更を有効にするためにマシンを再起動してください。

仮想チャネル許可リスト

仮想チャネル許可リストは、Citrix以外の仮想チャネルのうち、どのチャネルを環境で許可するかを制御できる機能です。デフォルトでは、仮想チャネル許可リスト機能は有効になっています。その結果、Citrix Virtual Apps and Desktops™セッションでは、Citrix仮想チャネルのみが開くことが許可されます。自社製またはサードパーティ製のカスタム仮想チャネルを使用する必要がある場合は、それらを明示的に許可リストに追加する必要があります。

構成

仮想チャネル許可リストはデフォルトで有効になっています。この機能は、Citrixポリシーの以下の設定を使用して構成できます。

- **仮想チャネル許可リスト**: この機能を有効または無効にし、仮想チャネルをリストに追加します。
- **仮想チャネル許可リストログのスロットリング**: 仮想チャネル許可リストのイベントログのスロットリング期間を設定します。
- **仮想チャネル許可リストのログ記録**: 仮想チャネル許可リストのログレベルを設定します。

仮想チャネルを許可リストに追加する

仮想チャネルを許可リストに追加するには、以下の情報が必要です。

1. コードで定義されている仮想チャネル名。最大7文字です。例: `CTXCVC1`。
2. VDAマシン上で仮想チャネルを開くプロセスのパス。例: `C:\Program Files\Application\run.exe`。

必要な情報が揃ったら、仮想チャネル許可リストポリシー設定を使用して、仮想チャネルを許可リストに追加する必要があります。リストに仮想チャネルを追加するには、仮想チャネル名の後にコンマ、そして仮想チャネルにアクセスするプロセスのパスを入力します。複数のプロセスがある場合は、各プロセスをコンマで区切って追加できます。

単一プロセスの場合

前の例を使用して、以下のエントリをリストに追加します。

```
CTXCVC1,C:\Program Files\Application\run.exe
```

複数のプロセスの場合

複数のプロセスがある場合は、次のエントリをリストに追加します。

```
CTXCVC1,C:\Program Files\Application\run.exe,C:\Program Files\Application\run2.exe
```

ワイルドカードの使用

ワイルドカード (*) の使用がサポートされています。アプリケーションのバージョンに基づいてディレクトリ名または実行可能ファイル名が変更される場合、またはサードパーティコンポーネントがユーザープロファイルにインストールされている場合に、ワイルドカードを使用できます。

次のシナリオでワイルドカードを使用できます。

- 完全なディレクトリ名を置き換える場合。 例: `C:\Program Files\Application*\run1.exe`
- ディレクトリ名の一部を置き換える場合。 例: `C:\Program Files\Application\v*\run1.exe`
- 実行可能ファイル名を置き換える場合。 例: `C:\Program Files\Application\v1.2*.exe`
- 実行可能ファイル名の一部を置き換える場合。 例: `C:\Program Files\Application\v1.2\run*.exe`

次の制限が適用されます。

- ワイルドカードは、単一のディレクトリを置き換えるためにのみ使用できます。たとえば、実行可能ファイルが `C:\Program Files\Application\v1.2\run1.exe` にある場合
  - 許可: `C:\Program Files\Application*\run1.exe`
  - 不許可: `C:\Program Files*\run1.exe`
- エントリにはファイル名拡張子を含める必要があります。
  - 許可: `C:\Program Files\Application\v1.2*.exe`
  - 不許可: `C:\Program Files\Application\v1.2*`

- すべてのパスはローカルである必要があります。

> **注：**
>
> - ネットワークパスは許可されていません。
> - ワイルドカードのサポートは、Citrix Virtual Apps and Desktops 2206から利用可能です。
> - ワイルドカードのサポートは、Citrix Virtual Apps and Desktops 2203 LTSRのCU2から利用可能です。

システム環境変数の使用

許可リスト内の信頼されたプロセスの定義を簡素化するために、システム環境変数を使用できます。`%programfiles%`、`%programfiles(x86)%`、`%systemdrive%`、`%systemroot%`などの標準変数を使用できます。

システムレベルで定義されている限り、カスタム環境変数も使用できます。

以下の例は、標準の環境変数を示しています。

- `%programfiles%\Application\v1.2\run.exe`
- `%programfiles%\Application*\run.exe`
- `%programfiles(x86)%\Application\v1.*\run.exe`

以下の例は、カスタムシステム環境変数を示しています。

- カスタム変数名: `app`
- カスタム変数値: `%programfiles%\Application\`
- 許可リストエントリ: `CTXCVC1,%app%\run.exe`

> **注：**
>
> ユーザー環境変数はサポートされていません。

> 環境変数のサポートは、Citrix Virtual Apps and Desktopsバージョン2209以降で利用可能です。

仮想チャネル名とプロセスを取得する

VDAマシン上で仮想チャネル名とそれを開くプロセスを取得する最も簡単な方法は、仮想チャネルを提供した開発者またはサードパーティベンダーから情報を入手することです。

または、機能のログを適用し、以下の手順に従って情報を取得することもできます。

1. カスタム仮想チャネルのクライアントおよびサーバーコンポーネントが配置されたら、仮想アプリケーションまたは仮想デスクトップを起動します。
2. VDAマシンのシステムイベントログで、カスタム仮想チャネルの名前と、それを開こうとしたプロセスを探します。利用可能なイベントの詳細については、「イベントログ」を参照してください。
3. セッションからログアウトします。
4. 識別された仮想チャネルとプロセスに対して、仮想チャネル許可リストポリシー設定にエントリを追加します。
5. マシンを再起動します。
6. VDAが登録されたら、仮想アプリケーションまたは仮想デスクトップを実行して、カスタム仮想チャネルが正常に開くことを検証します。

Citrix仮想チャネルに関する考慮事項

すべての組み込みCitrix仮想チャネルは信頼されており、追加設定なしで開くことができます。ただし、以下の2つの機能は、外部依存関係のため、許可リストに明示的なエントリが必要です。

- マルチメディアリダイレクト
- スカイプ フォー ビジネス 用 HDX RealTime Optimization Pack

マルチメディアリダイレクト

Windows Media Player以外のメディアプレーヤーをシステムメディアプレーヤーとして使用する場合、それを信頼されたプロセスとして許可リストに追加する必要があります。許可リストのエントリには、以下の情報が必要です。

- 仮想チャネル名: `CTXMM`
- プロセス: VDAマシンで使用されるメディアプレーヤーへのパス。例: `C:\Program Files (x86)\Windows Media Player\wmplayer.exe`。
- 許可リストエントリ: `CTXMM,C:\Program Files (x86)\Windows Media Player\wmplayer.exe`

スカイプ フォー ビジネス 用 HDX RealTime Optimization Pack

許可リストのエントリには、以下の情報が必要です。

- 仮想チャネル名: `CTXRMEP`
- プロセス: VDAマシン内のSkype for Business実行可能ファイルへのパス。これはSkype for Businessのバージョンやカスタムインストールパスの使用によって異なる場合があります。例: `C:\Program Files\Microsoft Office\root\Office16\lync.exe.`.
- 許可リストエントリ: `CTXRMEP,C:\Program Files\Microsoft Office\root\Office16\lync.exe`

トラブルシューティング

カスタム仮想チャネルが開かない場合は、次の手順を確認してください。

1. 正しいVDAバージョンを使用していることを確認してください。
2. 仮想チャネル許可リストにカスタム仮想チャネルを含むポリシーがVDAに適用されており、この構成を上書きする優先度の高い他のポリシーがないことを確認してください。
3. VDAのイベントログを確認し、報告されている仮想チャネル名が許可リストで定義されているものと一致することを確認してください。
    a. 複数のプロセスがある場合は、仮想チャネルを許可リストに追加するで説明されているように、これらが適切に定義されていることを確認してください。
    b. 定義されたプロセスパスでワイルドカードを使用している場合は、ワイルドカードの使用のガイドラインに従っていることを確認してください。
    c. 定義されたプロセスパスで環境変数を使用している場合は、システム環境変数の使用のガイドラインに従っていることを確認してください。

イベントログ

次のイベントがVDAマシンのイベントログに記録されます。

シングルセッションVDA

次のイベントがシングルセッションVDAマシンのイベントログに記録されます。

ログ名	ID	送信元	レベル	説明
システム	2001	`Picadd`	情報	カスタム仮想チャネル `<vcName>` はプロセス

ログ名	ID	送信元	レベル	説明
				`<processName>` によって開かれました
システム	2002	`Picadd`	警告	カスタム仮想チャネル `<vcName>` はプロセス `<processName>` によって開くことができません
システム	2003	`Picadd`	情報	`<username>` がカスタム仮想チャネル `<vcName>` を開きました
システム	2004	`Picadd`	警告	`<username>` がカスタム仮想チャネル `<vcName>` を開こうとしました
システム	2005	`Picadd`	エラー	ポリシー `<pathInPolicy>` で指定されたパスはプロセスパスに解決できません
システム	2007	`Picadd`	情報	ロードされたプロセスパスは `<processPath>` です
システム	2008	`Picadd`	エラー	VCポリシーパス内の環境変数

ログ名	ID	送信元	レベル	説明
				`<varName>` が見つかりません

マルチセッションVDA

マルチセッションVDAマシンのイベントログに次のイベントが記録されます:

ログ名	ID	送信元	レベル	説明
システム	13	`Rpm`	情報	カスタム仮想チャネル `<vcName>` はプロセス `<processName>` によって開かれました
システム	14	`Rpm`	警告	カスタム仮想チャネル `<vcName>` はプロセス `<processName>` によって開くことができません
システム	15	`Rpm`	情報	`<username>` がカスタム仮想チャネル `<vcName>` を開きました
システム	16	`Rpm`	警告	`<username>` がカスタム仮想チャネル `<vcName>` を開こうとしました
システム	17	`Rpm`	エラー	ポリシー `<pathInPolic`

ログ名	ID	送信元	レベル	説明
				`y>` で指定されたパスをプロセスパスに解決できません
システム	18	`Rpm`	情報	ロードされたプロセスパスは `<processPath>` です
システム	19	`Rpm`	エラー	VCポリシーパス内で環境変数 `<varName>` が見つかりません

既知のサードパーティ仮想チャネル

以下は、カスタムCitrix®仮想チャネルを使用する既知のサードパーティソリューションです。このリストには、カスタムCitrix仮想チャネルを使用するすべてのソリューションが含まれているわけではありません。

- カーナー
- ControlUp
- シスコ ウェブエックス チームズ
- シスコ ウェブエックス ミーティングス バーチャルデスクトップ ソフトウェア
- deviceTrust
- エピック ワープドライブ
- エピック スリングショット
- インプリバタ ワンサイン
- ミッドマーク IQPath クライアント拡張機能
- ニュアンス PowerMic クライアント拡張機能
- ニュアンス ドラゴン メディカル ネットワーク エディション 360 vSync
- ズーム ミーティングス for VDI
- アルティマ IA-Connect

関連する仮想チャネルを許可リストに追加するための詳細については、ソリューションのベンダーにお問い合わせください。または、仮想チャネル名とプロセスの取得セクションに記載されている手順に従ってください。

デバイス

HDX™は、あらゆる場所のあらゆるデバイスで高精細なユーザーエクスペリエンスを提供します。デバイスセクションの記事では、以下のデバイスについて説明します。

- スキャン
- 汎用USBデバイス
- クライアントドライブマッピング
- モバイルおよびタッチスクリーンデバイス
- シリアルデバイス
- 特殊キーボード
- Webカメラ

最適化されたUSBデバイスと汎用USBデバイス

最適化されたUSBデバイスとは、Citrix Workspace™アプリが特定のサポートを提供しているデバイスです。たとえば、HDXマルチメディア仮想チャネルを使用してWebカメラをリダイレクトする機能などです。汎用デバイスとは、Citrix Workspaceアプリで特定のサポートがないUSBデバイスです。

デフォルトでは、汎用USBリダイレクトは、汎用モードに設定しない限り、最適化された仮想チャネルサポートを持つUSBデバイスをリダイレクトできません。

一般的に、USBデバイスは汎用モードよりも最適化モードの方が優れたパフォーマンスを発揮します。ただし、最適化モードではUSBデバイスが完全な機能を持たない場合があります。その機能に完全にアクセスするには、汎用モードに切り替える必要があるかもしれません。

USB大容量記憶装置では、Citrix®ポリシーによって制御されるクライアントドライブマッピングまたは汎用USBリダイレクト、あるいはその両方を使用できます。主な違いは次のとおりです。

汎用USBリダイレクトとクライアントドライブマッピングポリシーの両方が有効になっていて、セッション開始前または開始後にマスストレージデバイスが挿入された場合、そのデバイスはクライアントドライブマッピングを使用してリダイレクトされます。

これらの条件が真の場合、マスストレージデバイスは汎用USBリダイレクトを使用してリダイレクトされます。

- 汎用USBリダイレクトとクライアントドライブマッピングポリシーの両方が有効になっている。
- デバイスが自動リダイレクト用に構成されている。
- セッション開始前または開始後にマスストレージデバイスが挿入される。

詳細については、`<http://support.citrix.com/article/CTX123015>`を参照してください。

機能	クライアントドライブマッピング	汎用USBリダイレクト
デフォルトで有効	はい	いいえ
読み取り専用アクセスを構成可能	はい	いいえ
暗号化されたデバイスアクセス	はい、仮想セッションでデバイスにアクセスする前に暗号化が解除されている場合。	シトリックス バーチャル デスクトップ™ のみ

スキャン

スキャナーは、画像、印刷されたテキスト、手書き文字、またはオブジェクトを光学的にスキャンし、デジタル画像に変換するデバイスです。

スキャナーを使用しており、お使いのコンピューターがWindowsを実行している場合、WIAスキャナードライバーを使用している可能性が高いです。このドライバーは、コンピューターとスキャナー間の通信を担当します。

- **Windows Image Acquisition** (WIA) は、ソフトウェアがスキャナーなどのイメージングハードウェアと通信できるようにする、Microsoft のドライバーモデルおよびアプリケーションプログラミングインターフェイス (API) です。
- **TWAIN** (Windows および Mac) は、標準インターフェイスを提供することでスキャナーとアプリケーションを接続する、もう1つのスキャンプロトコルです。TWAIN を使用すると、アプリケーションは TWAIN 準拠デバイス (スキャナー、デジタルカメラなど) から画像を取得できます。

TWAINリダイレクト

はじめに

TWAINは、画像ソフトウェアをスキャナーやデジタルカメラにリンクするために使用されるスキャンプロトコルです。

TWAINの仕組み

- Citrix®セッション内の32ビットアプリケーションを使用してドキュメントをスキャンします。

> **注：**
>
> ローカルに接続されたTWAIN準拠のスキャナーを使用してドキュメントをスキャンします。

- Citrixスキャンモジュールは、TWAINリクエストをクライアントのスキャナーにリダイレクトします。
- スキャンが完了すると、セッションホストに通知されます。

要件

Citrixコントロールプレーン

- シトリックス仮想アプリおよびデスクトップ™ 1912 以降
- シトリックス DaaS™

セッションホスト

- オペレーティングシステム
  - Windows 10 1809 以降
  - ウィンドウズ 11
  - ウィンドウズ サーバー 2022 以降
- VDA
  - バージョン1912以降
- アプリケーション
  - 32ビットアプリケーション

クライアントデバイス

- オペレーティングシステム
  - Windows 10 1809 以降
  - ウィンドウズ 11
- Workspaceアプリ
  - Windows: バージョン1912以降
- スキャナー
  - TWAIN準拠スキャナー

構成

- クライアントエンドポイントにTWAINドライバーをインストールします。
- TWAINとWIAの両方をサポートしている場合、必要なスキャンプロトコルを選択するようにデバイスまたはアプリケーションを設定します。
- スキャナーをクライアントエンドポイントにローカルで（USB経由で）接続します。
- 必要に応じて、USBリダイレクトを介してTWAINデバイスをセッションにリダイレクトします。

> **注：**
>
> TWAINデバイスはUSBリダイレクトとの相性が悪く、スキャン品質が低下します。

ポリシー設定

TWAINリダイレクトを設定し、スキャンを改善するためのポリシー設定。

- **クライアントTWAINデバイスリダイレクト:** TWAINリダイレクトを有効または無効にするには。

> **注：**
>
> デフォルトでは、TWAINリダイレクトは有効になっています。

- **TWAIN圧縮レベル:** クライアントからホストへの画像の圧縮レベルを設定します。

詳細については、TWAINデバイスポリシー設定を参照してください。

トラブルシューティング

公開テストアプリのTwackerでTWAINを試してください。Twackerは、URLからダウンロードできます。

公開デスクトップセッション内でTWAINを検証するには、次の手順に従います。

1. VDAに**Twacker**をインストールします。
2. **Twacker** (32ビット版) を起動します。
3. **File > Select Source**をクリックし、リストからスキャナーを選択します。
4. **File > Acquire**をクリックします。
5. **Scan button**をクリックして、スキャナーをテストします。

Twackerが正常にスキャンできる場合、**Citrix Virtual Apps and Desktops**のセットアップが次のようになっていることを確認できます。

- USBリダイレクト用に構成されている
- TWAINデバイスを使用している
- すべてのローカルクライアントデバイス要件を満たしている

特定のアプリケーション内でスキャンに関する問題が引き続き発生する場合は、ソフトウェアの問題である可能性が高いです。

WIA デバイス

要件

- スキャナーはWIA準拠である必要があります。
- WIAドライバーをローカルデバイスにインストールします。サーバーには必要ありません。
- スキャナーをローカルに接続します（例：USB経由）。
- スキャナーがローカルのWindows Image Acquisitionサービスを使用しており、TWAINドライバーを使用していないことを確認してください。
- テストに使用されるユーザーアカウントに、ICA®セッション内の帯域幅を制限するポリシーが適用されていないことを確認してください。たとえば、クライアントUSBリダイレクト帯域幅制限などです。

Windows イメージ取得アプリケーション許可リスト

許可リストを使用すると、VDA上のどのアプリケーションがWindows Image Acquisitionスキャナーリダイレクトにアクセスできるかを制御できます。レジストリエディターは、Windows Image Acquisitionを含む各VDAの許可リスト設定からの入力を使用します。デフォルトでは、どのアプリケーションもWindows Image Acquisitionにアクセスできません。

VDA上のアプリケーション向けにWindows Image Acquisitionを調整するには、レジストリで管理される機能のリストにあるWindows Image Acquisitionアプリケーション許可リスト設定を参照してください。

ポリシー設定については、「WIAデバイスポリシー設定」を参照してください。

汎用USBデバイス

はじめに

汎用USBリダイレクト機能により、USBデバイスをクライアントマシンからHDX™セッションにリダイレクトでき、エンドユーザーはHDXセッションで幅広い汎用USBデバイスを操作できます。これは、最適化されたサポートがない、または不適切な特殊デバイスを使用する必要があるシナリオで役立ちます。

> **注：**仮想チャネルのサポートに最適化されていないUSBデバイスは、生のUSBリダイレクトを使用して汎用USB仮想チャネルにフォールバックします。

仕組み?

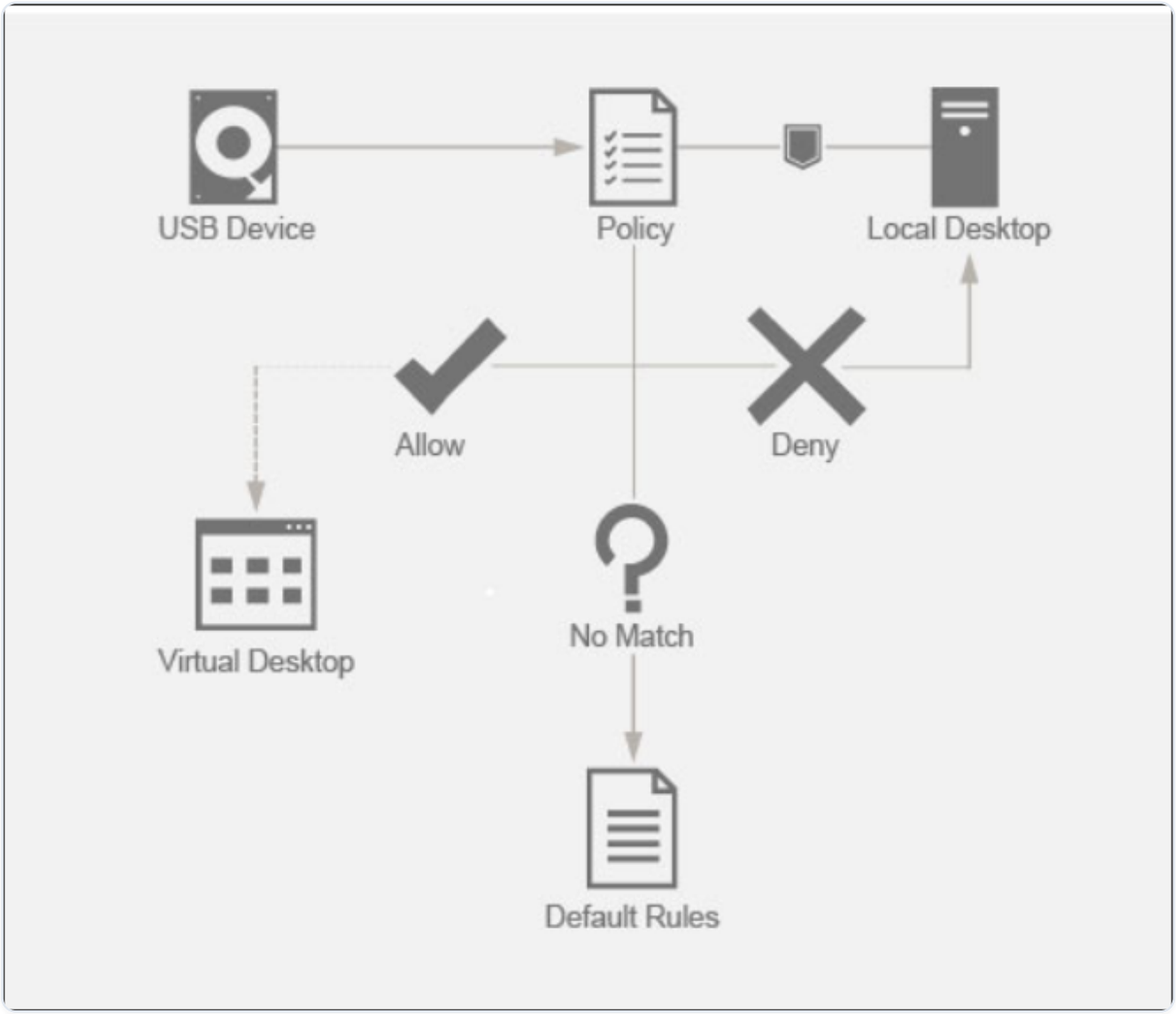
汎用USBリダイレクトは低レベルで機能し、クライアントマシンとXenDesktop®仮想デスクトップ間でUSB要求および応答メッセージをリダイレクトします。

クライアントマシンに互換性のあるデバイスドライバーが必要なくなり、ドライバーは仮想デスクトップでのみサポートされることが期待されます。USBリダイレクトポリシー規則は、DDCポリシー規則が評価および適用された後、クライアント側のポリシーとデフォルト規則が尊重されるように、特定の優先順位に従います。これにより、Citrix管理者は、不正なデバイスや偽装されたデバイスがセッション内にリダイレクトされるのを防ぐことができます。

さらに、リモートセッションへのアクセスを試みる不正なデバイスのイベントログを監査およびフラグ付けでき、管理者はデータ漏洩を防ぐための追加措置を講じることができます。

ユーザーがUSBデバイスを接続すると、セッションホストは一致が見つかるまで各ポリシー規則と連続して照合します。任意のデバイスに対する最初の一致が最終的なものと見なされます。

- 最初の一致が許可規則である場合、デバイスは仮想デスクトップにリダイレクトされます。
- 最初の一致が拒否規則である場合、デバイスはセッションにリダイレクトされず、ローカルユーザーデバイスでのみ使用できます。一致が見つからない場合は、デフォルト規則が使用されます。



構成

USBリダイレクトはデフォルトで無効になっています。Citrix®ポリシーで以下の設定を使用して、汎用USBリダイレクトを構成できます。

- **クライアントUSBデバイスリダイレクト**: USBリダイレクトを有効または無効にする
- **クライアントUSBデバイスリダイレクト規則**: 特定のデバイスアクション、つまり特定のデバイスへのアクセスを許可または拒否するように指定する
- **クライアントUSBデバイスリダイレクト規則（バージョン2）**: USBデバイスのフィルタリング、分割、自動接続の規則を指定する

- **クライアントUSBデバイス最適化規則**: 最適化を無効にするか、最適化モードを変更する
- **既存のUSBデバイスの自動接続を許可する**: HDX™セッションの開始時にクライアントエンドポイントに接続されている既存のUSBデバイスの自動接続を許可または防止する
- **新しく接続されたUSBデバイスの自動検出を許可する**: HDXセッション中にクライアントエンドポイントに接続されるUSBデバイスの自動接続を許可または防止する

詳細については、「USBポリシー設定」を参照してください。

USBリダイレクトの構成方法

デフォルトでは、USBリダイレクト構成は無効になっています。使用するには、USBリダイレクトポリシーと特定のリダイレクト規則をDDCで有効にして構成する必要があります。

> **注：**
>
> バージョン2212より前のコンポーネントを使用している場合、またはLinux/Mac版Workspaceアプリを使用している場合は、USBリダイレクトの構成方法の詳細について「レガシーUSBリダイレクト構成」を参照してください。

汎用USBリダイレクトの有効化

1. **Citrix Web Studio™ポリシー**を開き、**［ポリシー］**タブをクリックします。
2. **［ポリシーの作成］をクリックし、［ICA®］>［USBデバイスポリシー］**を展開します。
3. **クライアントUSBデバイスリダイレクトポリシー**を編集します。
4. 「**許可**」を選択し、「**保存**」をクリックします。

USBリダイレクトポリシー規則の作成

ユーザーがUSBデバイスをVirtual Desktopにリダイレクトしようとすると、一致が見つかるまで各USBポリシー規則に対して順にチェックされます。いずれかのデバイスに対する最初の一致が最終と見なされます。最初の一致が**許可**規則である場合、一致したデバイスは仮想デスクトップにリダイレクトが許可されます。最初の一致が**拒否**規則である場合、一致したデバイスはローカルデスクトップでのみ利用可能です。一致が見つからない場合は、デフォルトの規則が使用されます。

デバイス規則

通常のUSBデバイスと同様に、ポリシーまたはエンドポイント上のクライアントCitrix Workspace™ app構成で設定されたデバイス規則により、転送するデバイスが選択されます。

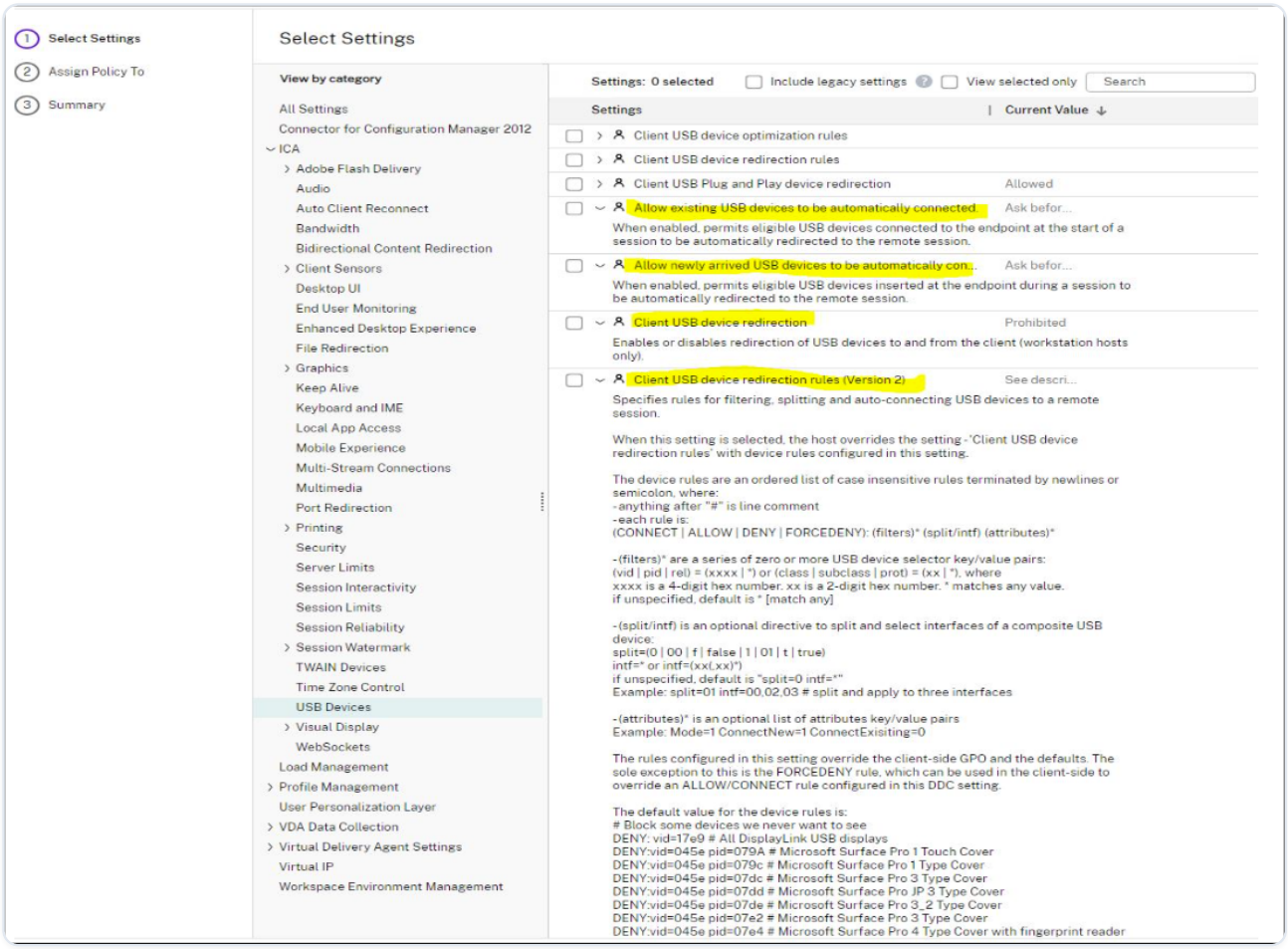
Citrix Workspace appはこれらの規則を使用して、どのUSBデバイスをリモートセッションへの転送を許可または防止するかを決定します。

各規則は、アクションキーワード（**Allow、Connect、またはDeny**）、コロン（:）、およびエンドポイントのUSBサブシステムにある実際のデバイスと一致する0個以上のフィルターパラメーターで構成されます。これらのフィルターパラメーターは、すべてのUSBデバイスが自身を識別するために使用するUSBデバイス記述子メタデータに対応しています。

デバイスルールはクリアテキストであり、各ルールは1行に記述され、#文字の後にオプションのコメントが続きます。ルールは上から下へ（優先順位の降順で）照合されます。デバイスまたは子インターフェイスに一致する最初のルールが適用されます。同じデバイスまたはインターフェイスを選択する後続のルールは無視されます。

例： ALLOW VID=1050 PID=0421 #デバイス1 **例：** CONNECT VID=xxxx PID=yyyy Class=03 #デバイス2

キーワード	説明
CONNECT	このキーワードを使用して、USB仮想チャネル経由でのデバイスのリダイレクトを許可し、セッション起動時および挿入時の自動リダイレクトを有効にします。
ALLOW	このキーワードを使用して、USB仮想チャネル経由でのデバイスのリダイレクトを許可します。
DENY	このキーワードを使用して、USB仮想チャネル経由でのデバイスのリダイレクトを拒否します。



DDC でポリシーを設定する:

1. **Citrix Web Studio ポリシー**」を開き、「**ポリシー**」タブをクリックします。
2. **ポリシーの作成**」をクリックし、「**ICA > USB デバイス ポリシー**」を展開します。
3. **クライアント USB デバイス リダイレクト規則**」を編集します (「**バージョン 2**」)。
4. リダイレクトする必要がある各 USB デバイスの説明に記載されている例に基づいて値を設定し、「保存」をクリックします。

   例: 許可: VID=056A PID=00A4 #STU-430 拒否: Class=08 subclass=05 # マスストレージ

> **注：**
>
> Citrix 管理者が「**既定値を使用**」をオンにして「**保存**」をクリックすると、既定の規則は VDA の次のレジストリにあります。

> **注意!**

> レジストリエディターを使用する前に、この記事の最後にある免責事項を参照してください。

> `HKLM\SOFTWARE\Wow6432Node\Citrix\PortICA\GenericUSB\DeviceRules`

注：

> グループポリシーデバイス規則を使用してクライアントデバイスにポリシーを設定することは引き続き可能ですが、CVAD および CWA の新しいバージョンでは不要になりました。

> USB デバイスのレガシー構成については、「レガシー USB リダイレクト構成」を参照してください。

USB デバイスの自動リダイレクトを構成する (オプション)

USB サポートが有効になっている場合、USB デバイスは自動的にリダイレクトされます。また、USB ユーザー設定は、USB デバイスを自動的に接続するように設定されています。すべての USB デバイスをリダイレクトすることが常に最適であるとは限りません。ユーザーは、自動的にリダイレクトされない USB デバイスリストからデバイスを明示的にリダイレクトできます。USB デバイスが一覧表示されたりリダイレクトされたりするのを防ぐには、クライアントエンドポイントまたは DDC ポリシーのいずれかで DeviceRules を使用します。 このポリシーは、DDC、GPO を使用するクライアント、Citrix Workspace Preferences、または CDViewer の タブのいずれかで設定できます。これらのすべての方法は以下で説明されています。

DDC でポリシーを設定する:

USB デバイスの自動リダイレクトを許可するように設定できる DDC 上のポリシーは 2 つあります。

- 既存のUSBデバイスの自動接続を許可する
- 新しく接続されたUSBデバイスの自動接続を許可する

a. 「**Citrix Web Studioポリシー**」を開き、「**ポリシー**」タブをクリックします。

b. 「**ポリシーの作成**」をクリックし、「**ICA > USBデバイスポリシー**」を展開します。

c. 既存のUSBデバイスを自動的に接続することを**許可**する設定を編集します。

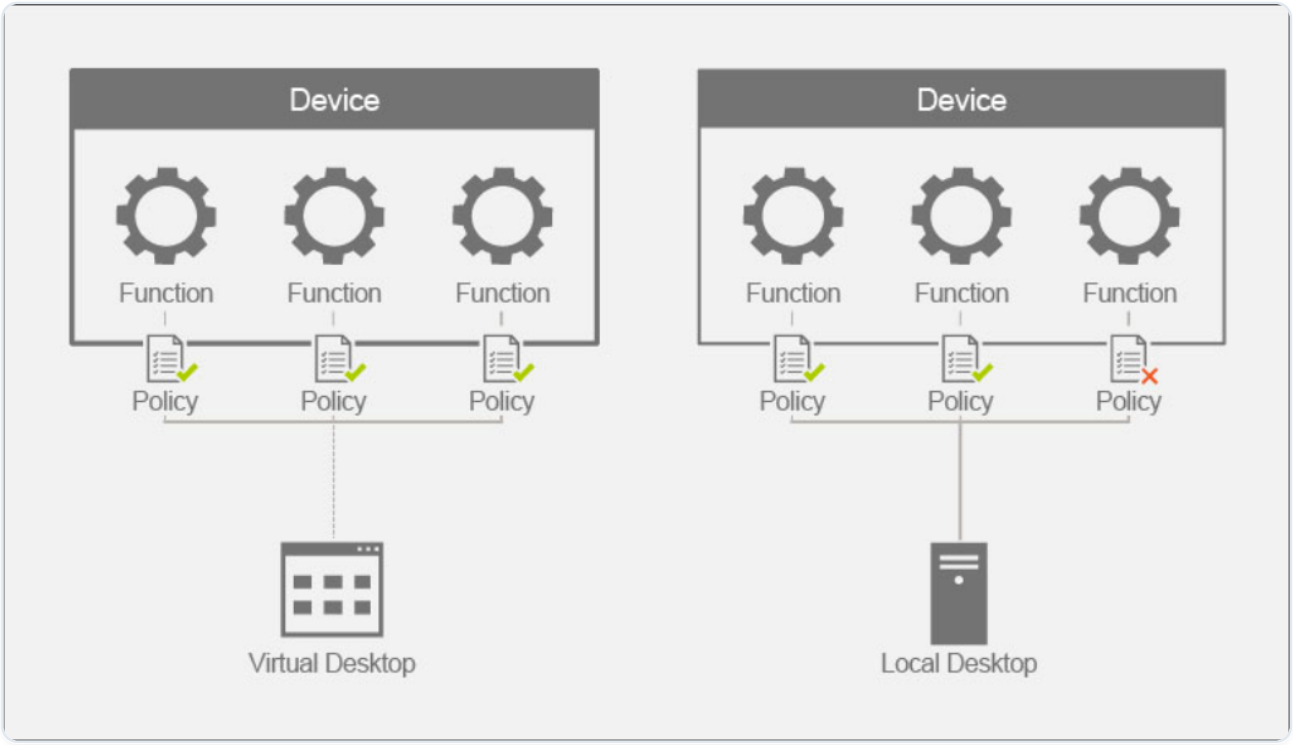
d. 「**デフォルト値を使用**」チェックボックスをオフにし、ドロップダウンメニューから「**利用可能なUSBデバイスを自動的にリダイレクト**」を選択して、「**保存**」をクリックします。

e. 新しく接続されたUSBデバイスを自動的に接続することを**許可**する設定を編集します。

f. 「**デフォルト値を使用**」チェックボックスをオフにし、ドロップダウンメニューから「**利用可能なUSBデバイスを自動的にリダイレクト**」を選択して、「**保存**」をクリックします。

複合デバイスとデバイス分割

複合USBデバイスは、コンピューターに接続された複数の独立したUSBデバイスのように機能する単一のデバイスです。単一のUSBコネクターを持ちますが、それぞれ独自の機能セットを持つ複数のインターフェイスをコンピューターに公開できます。ユーザーが複合USBデバイスを接続すると、ホストデバイスはすべての機能（インターフェイス）を各ポリシー規則と照合します。いずれかの機能（インターフェイス）に対する最初の照合が拒否規則である場合、その規則は複合デバイスに対して最終的なものと見なされ、デバイスは拒否されます。機能（インターフェイス）に対する最初の照合が許可規則である場合、ホストデバイスは次の機能（インターフェイス）に対して規則の照合を続行します。ポリシー規則によってどの機能（インターフェイス）も拒否されない場合、複合デバイスは許可されます。複合デバイスに対する最終的な照合が拒否規則である場合、デバイスはローカルデスクトップでのみ利用可能であり、それ以外の場合は仮想デスクトップにリモート接続されます。一致が見つからない場合は、デフォルト規則が使用されます。



複合デバイスの特定の機能のみを許可するために、デバイスリダイレクト規則（バージョン2）ポリシーで適切な規則を使用して複合デバイスを分割できます。たとえば、FIDO2キーのHID機能のみを使用し、スマートカード機能は使用したくない場合があります。その場合、以下に示すように規則を設定します。

1. Connect: VID=1050 PID=0407 class=03 split=01 intf=00,01 #Yubikeyシリーズ5のFIDO2 HID機能は許可されています。
2. Deny: VID=1050 PID=0407 split=01 intf=02 #Yubikeyシリーズ5のスマートカード機能はブロックされています。

> **ヒント:**
>
> 新しいポリシー規則を作成する際は、USB Webサイトで入手可能なUSBクラスコードを参照してください。

署名パッドの構成

1. VDAホストに適切なデバイスドライバーをインストールします。
2. **Citrix Web Studio™**で**クライアントUSBデバイスリダイレクト**ポリシー設定を有効にします。
3. **クライアントUSBデバイスリダイレクト規則（バージョン2）**ポリシー設定を編集します。
    a. リダイレクトする必要がある署名パッドの**VID**および**PID**情報を設定し、**保存**をクリックします。例：**Connect**: VID=06A8 PID=0057 class=03 #Topaz HSB
4. **クライアントUSBデバイス最適化規則**ポリシー設定を編集します。
    a. モードとその他のデバイス情報を設定します。例：Mode=00000004 VID=06A8 PID=0057 class=03 #キャプチャモードで動作する入力デバイス
5. **既存のUSBデバイスの自動接続を許可する**ポリシー設定を編集します。
6. 「**デフォルト値を使用**」チェックボックスをオフにし、ドロップダウンメニューから「**利用可能なUSBデバイスを自動的にリダイレクト**」を選択し、「**保存**」をクリックします。
7. ポリシー設定「**新しく接続されたUSBデバイスの自動接続を許可**」を編集します。
8. 「**デフォルト値を使用**」チェックボックスをオフにし、ドロップダウンメニューから「**利用可能なUSBデバイスを自動的にリダイレクト**」を選択し、「**保存**」をクリックします。

これらの設定が構成されると、以降のセッション起動では、デバイスが自動的にリダイレクトされ、追加のエンドユーザー操作は不要になります。

> **注：**
>
> VIDとPIDを、リダイレクトするデバイスの実際のVIDとPIDに置き換えます。

USBリダイレクトを使用したBloombergキーボードの構成

1. **Citrix Web Studio**でポリシー設定「**クライアントUSBデバイスリダイレクト**」を有効にします。
2. Bloomberg 5キーボードは、ポリシー設定「**クライアントUSBデバイスリダイレクト規則(バージョン2)**」でデフォルトで設定されており、追加の管理者操作は不要です。
3. ポリシー設定「**既存のUSBデバイスの自動接続を許可**」を編集します。
4. 「**デフォルト値を使用**」チェックボックスをオフにし、ドロップダウンメニューから「**利用可能なUSBデバイスを自動的にリダイレクト**」を選択し、「**保存**」をクリックします。
5. ポリシー設定「**新しく接続されたUSBデバイスの自動接続を許可**」を編集します。
6. 「**デフォルト値を使用**」チェックボックスをオフにし、ドロップダウンメニューから「**利用可能なUSBデバイスを自動的にリダイレクト**」を選択し、「**保存**」をクリックします。

これらの設定が構成されると、Bloombergキーは以降のHDX™セッションで自動的に表示され、追加のエンドユーザー操作は不要になります。

USBリダイレクトを使用したFIDO2キーの構成

Citrixでは、HDXセッションでFIDO2キーを使用するためにFIDO2リダイレクトを使用することをお勧めします。ただし、代わりにUSBリダイレクトを使用してFIDO2キーをリダイレクトする必要がある状況もあります。これには、クライアント、VDA、またはオペレーティングシステム（例: Windows Server 2016）で機能がサポートされていないためにFIDO2リダイレクトが利用できないシナリオが含まれます。

キーに複数のモードが有効になっている場合でも、HDXセッションでその一部のみを許可したい状況もあります。たとえば、FIDO2とOTPは許可したいが、スマートカードはブロックしたい場合などです。

次の手順は、USBリダイレクトを使用してFIDO2キー（Yubikey vid=1050, pid=0407）を構成する方法を示しています。

1. **Citrix Web Studio**で**クライアントUSBデバイスリダイレクト**ポリシー設定を有効にします。
2. **クライアントUSBデバイスリダイレクト規則（バージョン2）**ポリシー設定を編集します。
    a. セッションでリダイレクトするFIDO2キーの**VID**および**PID**情報と、分割デバイス構成を設定し、**保存**をクリックします。
    b. **接続**: VID=1050 PID=0407 class=03 split=01 intf=00,01 #Yubikeyシリーズ5で許可されるFIDO2 HID機能。
    c. **拒否**: VID=1050 PID=0407 split=01 intf=02 # Yubikeyシリーズ5のスマートカード機能はブロックされました。
3. ポリシー設定**既存のUSBデバイスの自動接続を許可する**を編集します。
4. **デフォルト値を使用**チェックボックスをオフにし、ドロップダウンメニューから**利用可能なUSBデバイスを自動的にリダイレクト**を選択して、**保存**をクリックします。
5. ポリシー設定**新しく接続されたUSBデバイスの自動接続を許可する**を編集します。
6. **デフォルト値を使用**チェックボックスをオフにし、ドロップダウンメニューから**利用可能なUSBデバイスを自動的にリダイレクト**を選択して、**保存**をクリックします。

これらの設定が構成されると、FIDO2キーボードは以降のHDXセッションで自動的に表示され、エンドユーザーによる追加の操作は不要になります。

USBリダイレクトを使用した3Dマウスの構成

現在、3dConnexionスペースマウスドライバーはワークステーションOS（Win 10およびWin11）でのみサポートされています。サーバーOSでは動作しません。以下は、ワークステーションOS（vid=046D, pid=C016）でSpaceMouse Enterpriseを構成する手順です。

1. VDAホストに最新のWindowsドライバーをインストールします。
2. 「**Citrix Web Studio**」で「**クライアントUSBデバイスリダイレクト**」ポリシー設定を有効にします。
3. **クライアントUSBデバイスリダイレクト規則（バージョン2）**ポリシー設定を編集します。
    a. リダイレクトする必要がある署名パッドの **VID** と **PID** 情報を設定し、**保存** をクリックします。例: **接続**: VID=046D PID=C016 #SpaceMouse Enterprise
4. 「**クライアントUSBデバイス最適化規則**」ポリシー設定を編集します。
    a. 他のデバイス情報とともにモードを設定します。例：Mode=00000004 VID=046D PID=C016 class=03 #Input device operating in capture mode
5. 「**既存のUSBデバイスの自動接続を許可する**」ポリシー設定を編集します。

6. 「**デフォルト値を使用**」チェックボックスをオフにし、ドロップダウンメニューから「**利用可能なUSBデバイスを自動的にリダイレクトする**」を選択して、**保存**をクリックします。
7. 「**新しく接続されたUSBデバイスの自動接続を許可する**」ポリシー設定を編集します。
8. 「**デフォルト値を使用**」チェックボックスをオフにし、ドロップダウンメニューから「**利用可能なUSBデバイスを自動的にリダイレクトする**」を選択して、**保存**をクリックします。

異なるデバイス規則を使用してUSBリダイレクトで2つ以上のデバイスを構成する

複数のデバイスを、異なるデバイス規則を使用してHDXセッション内でリダイレクトできます。管理者は、一方のデバイスを自動的にリダイレクトし、もう一方のデバイスをエンドユーザーがリダイレクトするオプションを提供したい場合があります。以下に、異なる規則で2つのデバイスを構成する手順を示します。

1. 「**Citrix Web Studio**」で「**クライアントUSBデバイスリダイレクト**」ポリシー設定を有効にします。
2. 「**クライアントUSBデバイスリダイレクト規則**」（**バージョン2**）ポリシー設定を編集します。

    a. セッション内で適切なデバイス規則を使用してリダイレクトする2つのデバイスの**VID**と**PID**情報を追加し、**保存**をクリックします。

    b. **許可**: VID=0911 PID=0c1c #フィリップス製スピーチマイク.

    c. **接続**: VID=06A8 PID=0043 class=03 # Topaz HSB署名パッド

3. ポリシー設定 **既存のUSBデバイスの自動接続を許可する** を編集します。
4. **デフォルト値を使用** チェックボックスをオフにし、ドロップダウンメニューから **利用可能なUSBデバイスを自動的にリダイレクト** を選択し、**保存** をクリックします。
5. ポリシー設定 **新しく接続されたUSBデバイスの自動接続を許可する** を編集します。
6. **デフォルト値を使用** チェックボックスをオフにし、ドロップダウンメニューから **利用可能なUSBデバイスを自動的にリダイレクト** を選択し、**保存** をクリックします。

これらの設定が構成されると、Topaz HSB署名パッドは、その後のHDXセッションで自動的に表示され、追加のエンドユーザー操作は不要になります。一方、Phillipsスピーチマイクは、エンドユーザーがConnection CenterまたはCDViewerのタブでリダイレクトを有効にする必要があります。

トラブルシューティング

USBリダイレクト関連の問題をトリアージするには、次の手順に従ってください。

1. USBリダイレクトのシステム要件が満たされていることを確認します。これには、正しいCVADおよびCWAバージョン、サポートされているデバイス、および検討中のOSプラットフォーム上のデバイスドライバーが含まれます。
2. 環境で使用されているコンポーネントのバージョンとプラットフォームに基づいて、構成が適切であることを確認します。(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/devices/usb-devices/legacy-usb-redirection-configuration.html)を必要とするコンポーネントの詳細については、「レガシーUSBリダイレクト構成」の注記を参照してください。
3. デバイスがクライアントによって列挙されたデバイスの下にリストされていることを確認します。

    a. Workspace Preferencesツールバー: WorkspaceアプリのPreferencesツールバーのタブに列挙されているデバイスを確認します (右クリック **CWAアイコン > 接続センター > 環境設定**... **デバイス**タブをクリック)。

    b. `CtxUsbDiagnostics.exe` (推奨): このツールをコマンドプロンプトウィンドウで実行します。出力には、特定のセッションのデバイス固有の情報が表示されます。デバイスがリダイレクトされているかどうか、またデバイスルールセットがデバイスのリダイレクトを妨げているかどうかがわかります。詳細については、診断ツールを参照してください。

    c. USBViewまたはその他のサードパーティツール: エンドポイント/クライアントマシンでUSBViewのようなサードパーティツールを実行し、デバイスがエンドポイントで検出されていることを確認します。

4. デバイスが列挙されている場合:

    a. 特定のデバイスについてCtxUsbDiagnosticsツールの出力に拒否ルールが表示される場合は、Studioで構成されているポリシーを確認し、バージョン2ポリシーでルールが正しく設定されていることを確認します。拒否ルールがStudioポリシーに表示されない場合は、クライアント側ポリシー、そして最後にクライアント側デフォルトの順に確認して、一致する拒否ルールを見つけます。

    b. CtxUsbDiagnostics出力に拒否ルールがない場合、CWAは設定ウィンドウのタブ (>) で適切なボタンをチェック/クリックすることで、デバイスのリダイレクトを許可します。一度リダイレクトされたデバイスはセッションで利用可能になります。これは、HDXセッションでデバイスマネージャー/USBViewまたは同様のアプリケーションをチェックすることで確認できます。

5. セッション内にデバイスが表示されない場合:

    a. VDAホストに正しいデバイスドライバーが正しくインストールされていない可能性があります。VDAホストに最新バージョンのデバイスドライバーが正しくインストールされてい

ることを確認してください。一部のデバイスドライバーはターミナルサーバーマシンではサポートされていないため、リダイレクトしようとしているデバイスがそうでないことを確認してください。

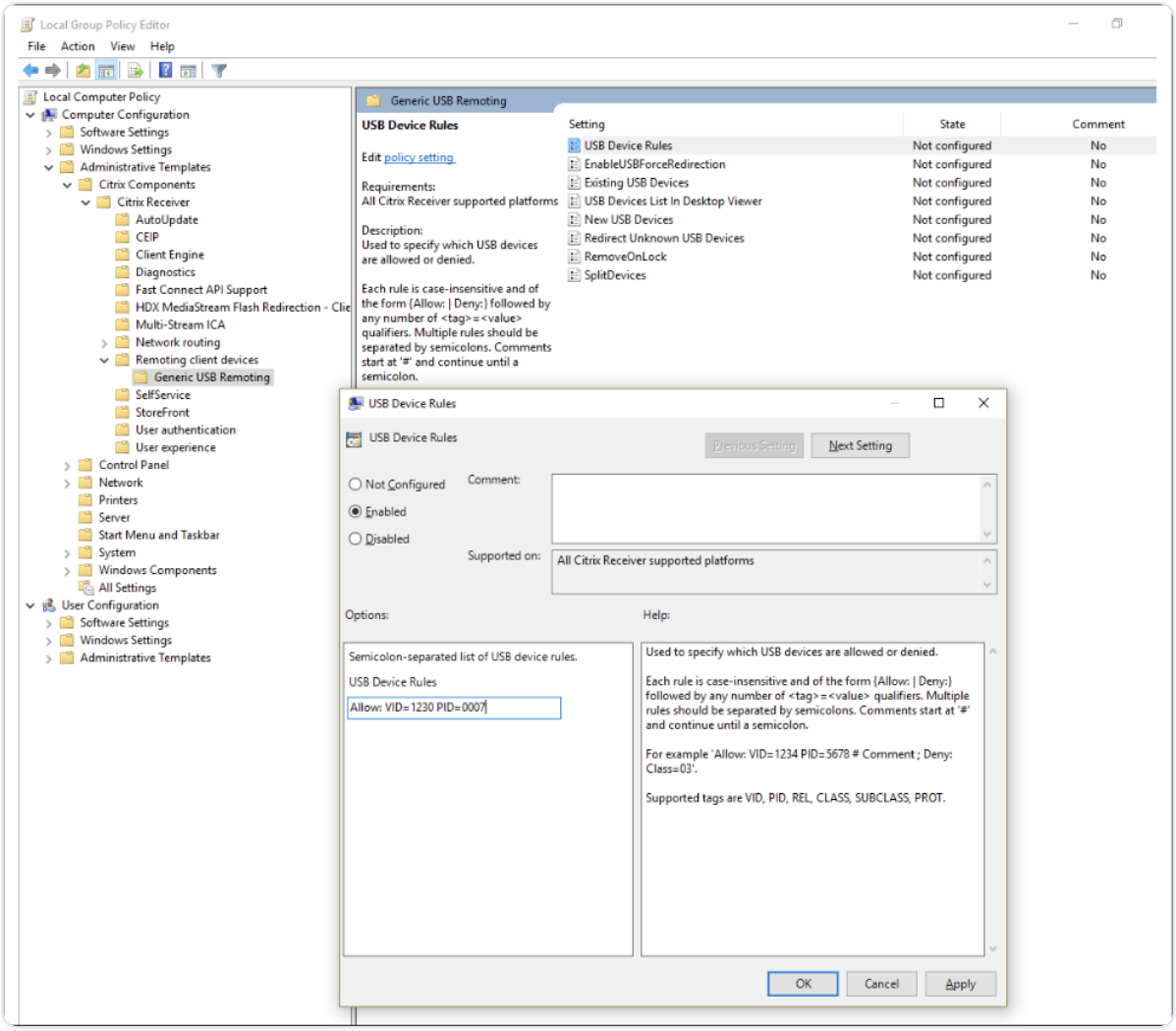
b. デバイスがクライアントエンドポイントで使用されていないことを確認します。一部のデバイスはクライアントエンドポイントにもドライバーのインストールが必要であり、これによりセッションでのリダイレクトが妨げられる可能性があります。

6. クライアントエンドポイントでUSB関連のルールが正しく設定されていることを確認します。

a. **Windows向けCWA：**

i. クライアントのグループポリシー（詳細とSSを追加）が適切に設定されており、Studioで設定されたルールと競合しないことを確認します。

ii. クライアントのレジストリ内のデフォルトルールを検証します。



`(HKLM\SOFTWARE\Wow6432Node\Citrix\PortICA\GenericUSB\DeviceRules) are appropriately set and not in conflict with the rules set in Studio and client group policy.`.

b. CWA for Linux - CWA for Linux の問題のトリアージについては、CWA for Linux の USB ドキュメントを参照してください。

c. CWA for Mac - CWA for Mac の問題のトリアージについては、CWA for Mac を参照してください。

注：

- TSVDA では、オーディオデバイスはデフォルトで USB リダイレクトの使用がブロックされています。これらのデバイスを使用する推奨される方法は、最適化されたオーディオ VC を使用することです。
- デバイスを分割するための正しいデバイスリダイレクトルールが設定されていても、USB 複合デバイスが自動的に分割されない場合があります。この問題は、デバイスが低電力モードになっているために発生します。このような場合、低電力モードになった子デバイスがデバイスリストに表示されないことがあります。この問題を解決するには、次の回避策を使用できます。
  - セッションを切断し、USB デバイスを挿入して、セッションに再接続します。
  - USB デバイスのプラグを抜き、再度差し込みます。この操作により、デバイスは低電力モードから復帰します。
- バッテリー寿命を最適化するために、USB バッテリーセーバー設定が有効になっている場合があります。クライアントエンドポイントがスリープ状態になると、USB デバイスが切断されることがあります。このようなシナリオでは、セッションでデバイスを再度表示するために、デバイスを切断して再接続する必要がある場合があります。

イベントログ

管理者は、ユーザーがリダイレクトしようとする不正なデバイスを監視し、適切な措置を講じることができるようになりました。以下に、リダイレクトが許可されているデバイスと許可されていないデバイスについて、VDA ホストのイベントビューアーに記録されるイベントメッセージの一部を示します。

Id	1000
Name	UsbEventAcceptDevice
Severity	Informational
Facility	System
Text	The Citrix USB Service allows the USB Device with Product ID: %2, Vendor ID: %3, and Device ID: %4 to be remoted.
Comment	This message logs the device info of a device redirected in an HDX session

Id	1001
Name	UsbEventPolicyRejectsDeviceV1
Severity	Warning
Facility	System
Text	The USB device with Product ID: 0x%2, Vendor ID: 0x%3, and Device ID: 0x%4 is not being redirected because the Citrix USB policy, "DENY: ...%5..." is in effect. If you wish to redirect the device, please set an allow rule that matches the device in the "Client USB device redirection rules" policy in Citrix Studio.
Comment	This message displays a message of the device not getting redirected if a DENY rule is being enforced by the legacy “Client USB device redirection rules” policy rule.
Arguments	

Id	1002
Name	UsbEventPolicyRejectsDeviceV2
Severity	Warning
Facility	System
Text	The USB device with Product ID: 0x%2, Vendor ID: 0x%3, and Device ID: 0x%4 is not being redirected because the Citrix USB policy, "DENY: ...%5..." is in effect. If you wish to redirect the device, please set an allow rule that matches the device in the "Client USB device redirection rules (Version 2)" policy in Citrix Studio.
Comment	This message displays a message of the device not getting redirected if a DENY rule is being enforced by the "Client USB device redirection rules (Version 2)" policy rule. For instance, if the studio policy rule allows an approved set of devices and denies all other devices and an end user tries to create a new rule on the client endpoint via group policy, this event will get logged. This message would be indicative of an unauthorized device redirection attempt.
Arguments	

USB診断ツール

`CtxUsbDiagnostics.exe`は、Citrix管理者がクライアントで発生するUSBデバイスリダイレクトの問題を迅速に診断し解決するのに役立つ、VDA上のコマンドラインツールです。このユーティリティツールは、HDXセッション内でリダイレクトに失敗しているクライアントに接続されたUSBデバイスに関連する構成の問題をトリアージするために必要な重要な情報を収集します。

```
> **Note :**

>

> Running Command Prompt or Powershell as an administrator is required to ensure the tool has the necessary permissions to perform system-level operations.
```

要件

セッションホスト

- オペレーティングシステム
  - Windows 10 1809 以降
  - Windows 11 21H2 以降
  - ウィンドウズ サーバー 2016 以降
- VDA
  - Windows版: Citrix Virtual Apps and Desktops™ バージョン 2311 以降

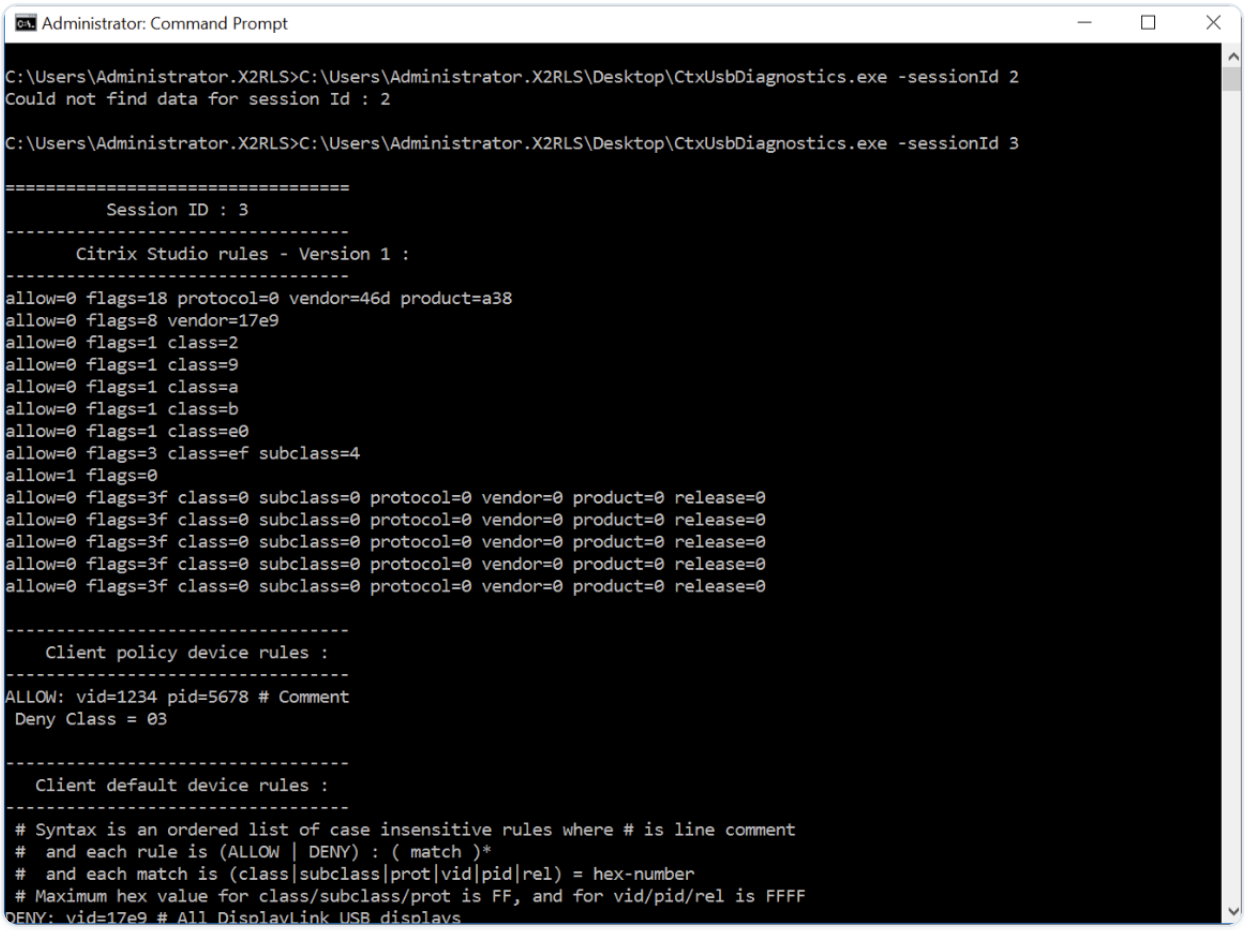
クライアントデバイス

- オペレーティングシステム
  - Windows 10 1809 以降
- ワークスペースアプリ
  - Windows: バージョン 2311 以降

ツールの機能?

このツールは現在、以下を提供します。

- SessionID
- VDAデバイスポリシー（Studioで設定されたデバイスルール）
- クライアントデバイスとクライアントデバイスポリシー（デバイスルール）
- デバイスのリスト、そのリダイレクト状態、および許可または拒否された理由



> **注記：**
>
> 管理者は、すべてのアクティブなセッションのデバイス情報を確認できます。

表示される情報

- **Citrix Studio ルール - バージョン 1/2**
  - DDCルールは、Studioにおけるレガシーな「**クライアントUSBデバイスリダイレクトルール**」または「**クライアントUSBデバイスリダイレクトルール (バージョン 2)**」ポリシーの使用を示します。このセクションに記載されている情報は、Citrix®管理者が構成したすべてのルールを一覧表示します。

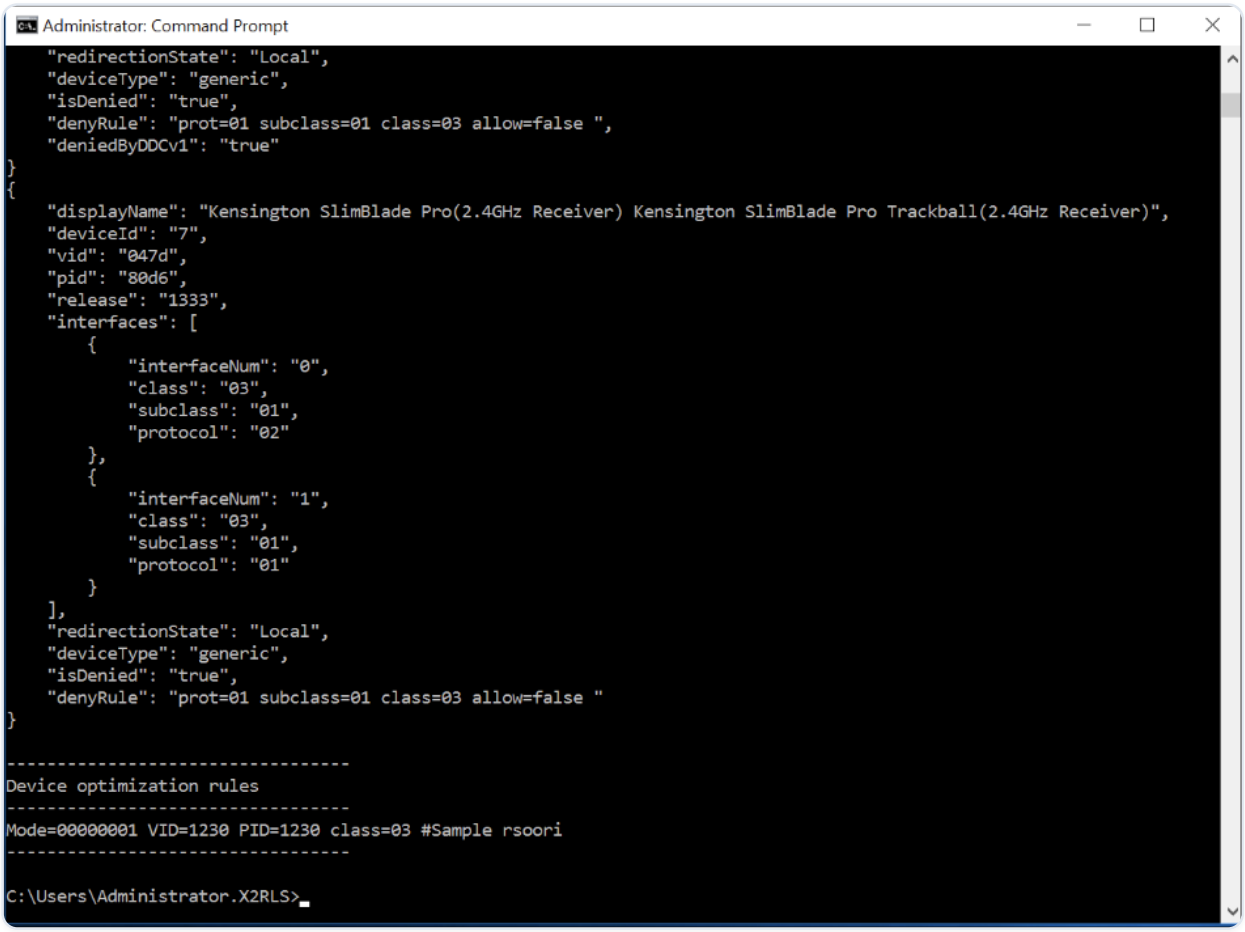
```
C:\Program Files\Citrix\HDX\bin>CtxUsbDiagnostics.exe

---------------------------------
          Session ID : 1
---------------------------------
       Citrix Studio rules - Version 2 :
---------------------------------
DENY: vid=046D pid=0A38
# Block some devices we never want to see
DENY: vid=17e9 # All DisplayLink USB displays
```

- **クライアントのデフォルトデバイスルール**
  - このセクションには、クライアントのレジストリに設定されているルールが一覧表示されます。

```
---------------------------------
   Client default device rules :
---------------------------------
 # Syntax is an ordered list of case insensitive rules where # is line comment
 #   and each rule is (ALLOW | DENY) : ( match )*
 #   and each match is (class|subclass|prot|vid|pid|rel) = hex-number
 # Maximum hex value for class/subclass/prot is FF, and for vid/pid/rel is FFFF
DENY: vid=17e9 # All DisplayLink USB displays
CONNECT: vid=1188 pid=A101 # Bloomberg 5 Biometric module
DENY: vid=1188 pid=A001 split=01 intf=00 # Bloomberg 5 Primary keyboard
CONNECT: vid=1188 pid=A001 split=01 intf=01 # Bloomberg 5 Keyboard HID
DENY: vid=1188 pid=A301 split=01 intf=02 # Bloomberg 5 Keyboard Audio Channel
CONNECT: vid=1188 pid=A301 split=01 intf=00,01 # Bloomberg 5 Keyboard Audio HID
DENY: class=02 # Communications and CDC-Control
DENY: class=09 # Hub devices
DENY:vid=045e pid=079A # Microsoft Surface Pro 1 Touch Cover
DENY:vid=045e pid=079c # Microsoft Surface Pro 1 Type Cover
DENY:vid=045e pid=07dc # Microsoft Surface Pro 3 Type Cover
DENY:vid=045e pid=07dd # Microsoft Surface Pro JP 3 Type Cover
DENY:vid=045e pid=07de # Microsoft Surface Pro 3_2 Type Cover
DENY:vid=045e pid=07e2 # Microsoft Surface Pro 3 Type Cover
DENY:vid=045e pid=07e4 # Microsoft Surface Pro 4 Type Cover with fingerprint reader
DENY:vid=045e pid=07e8 # Microsoft Surface Pro 4_2 Type Cover
DENY:vid=03eb pid=8209 # Surface Pro Atmel maXTouch Digitizer
ALLOW:vid=056a pid=0315 class=03 # Wacom Intuos tablet
ALLOW:vid=056a pid=0314 class=03 # Wacom Intuos tablet
ALLOW:vid=056a pid=00fb class=03 # Wacom DTU tablet
DENY: class=03 subclass=01 prot=01 # HID Boot keyboards
DENY: class=03 subclass=01 prot=02 # HID Boot mice
DENY: class=0a # CDC-Data
DENY: class=0b # Smartcard
DENY: class=e0 # Wireless controller
DENY: class=ef subclass=04 # Miscellaneous network devices
ALLOW: # Otherwise allow everything else
```

- **デバイス最適化ルール**
  - このセクションには、「クライアントUSBデバイス最適化ルール」で設定されているデバイス最適化ルールが一覧表示されます。



デバイスリスト

このセクションには、クライアントエンドポイントに接続されている各デバイスに関する貴重な情報（ハードウェア情報、リダイレクトされているかどうか、正しいデバイスリダイレクトルールが設定されているかどうかなど）が一覧表示されます。

タグ名	説明
displayName	デバイスの一般的な名前を一覧表示します。
ベンダーID	ベンダーID
製品ID	製品ID
インターフェイス	このサブセクションでは、複合デバイスが複数の子デバイスに分割されている場合に、すべてのインターフェイスを一覧表示します。
InterfaceNum	インターフェイス記述子のインデックスを示します
クラス	クラスコード

タグ名	説明
サブクラス	サブクラスコード
プロトコル	プロトコル
リダイレクト状態	**ローカル**は、デバイスがICA®セッションでリダイレクトされていないことを示します。**このセッション**は、デバイスがICAセッションでリダイレクトされていることを示します。**他のセッション**は、デバイスが別のICAセッションでリダイレクトされていることを示します。
optiEnabled	**true** は、デバイスが最適化されていることを示します。**false** は、デバイスが最適化されておらず、データ転送がUSB仮想チャネル経由で行われることを示します。
デバイスタイプ	**汎用**は、デバイスに最適化された仮想チャネルがなく、トラフィックがUSB仮想チャネルを介して流れていることを示します。**最適化済み**は、デバイスに関連付けられたデータ転送が専用の仮想チャネルを介して行われていることを意味します。
拒否済み	**true**は、管理者が設定したポリシー規則によりデバイスがリダイレクトされないことを示します。`false`は、適用されたポリシーによりデバイスがリダイレクトされることを示します。
拒否ルール	このフィールドは、**拒否済み**が`true`に設定されている場合に役立ちます。これは、デバイスがリダイレクトされない原因となっているポリシーで設定された特定のルールを管理者に伝えます。

レガシーUSBリダイレクトの構成

バージョン2212より古いコンポーネントを使用している場合、またはLinux版CWAを使用している場合は、このガイドに従って環境でUSBリダイレクトを構成してください。

汎用USBリダイレクトの有効化

1. **Citrix Web Studio™ポリシー**を開き、**ポリシー**タブをクリックします。
2. **ポリシーの作成**をクリックし、**ICA® > USBデバイスポリシー**を展開します。
3. **クライアントUSBデバイスリダイレクトポリシー**を編集します。
4. **許可**を選択し、**保存**をクリックします。

USBリダイレクトポリシー規則の作成

ユーザーがUSBデバイスを仮想デスクトップにリダイレクトしようとすると、一致が見つかるまで各USBポリシー規則と照合されます。いずれかのデバイスに対する最初の一致が最終と見なされます。最初の一致が許可規則である場合、一致したデバイスは仮想デスクトップにリダイレクトが許可されます。最初の一致が拒否規則である場合、一致したデバイスはローカルデスクトップでのみ利用可能です。一致が見つからない場合は、デフォルト規則が使用されます。

DDC でポリシーを設定する:

1. **Citrix Web Studioポリシー**を開き、**ポリシー**タブをクリックします。
2. **ポリシーの作成**をクリックし、**ICA > USBデバイスポリシー**を展開します。
3. 「**クライアントUSBデバイスリダイレクト規則**」を編集します。
4. リダイレクトする必要がある各USBデバイスについて、説明に記載されている例に基づいて値を設定し、をクリックします。 例： Allow: VID=056A PID=00A4 #STU-430 Deny: Class=08 subclass=05 # Mass Storage

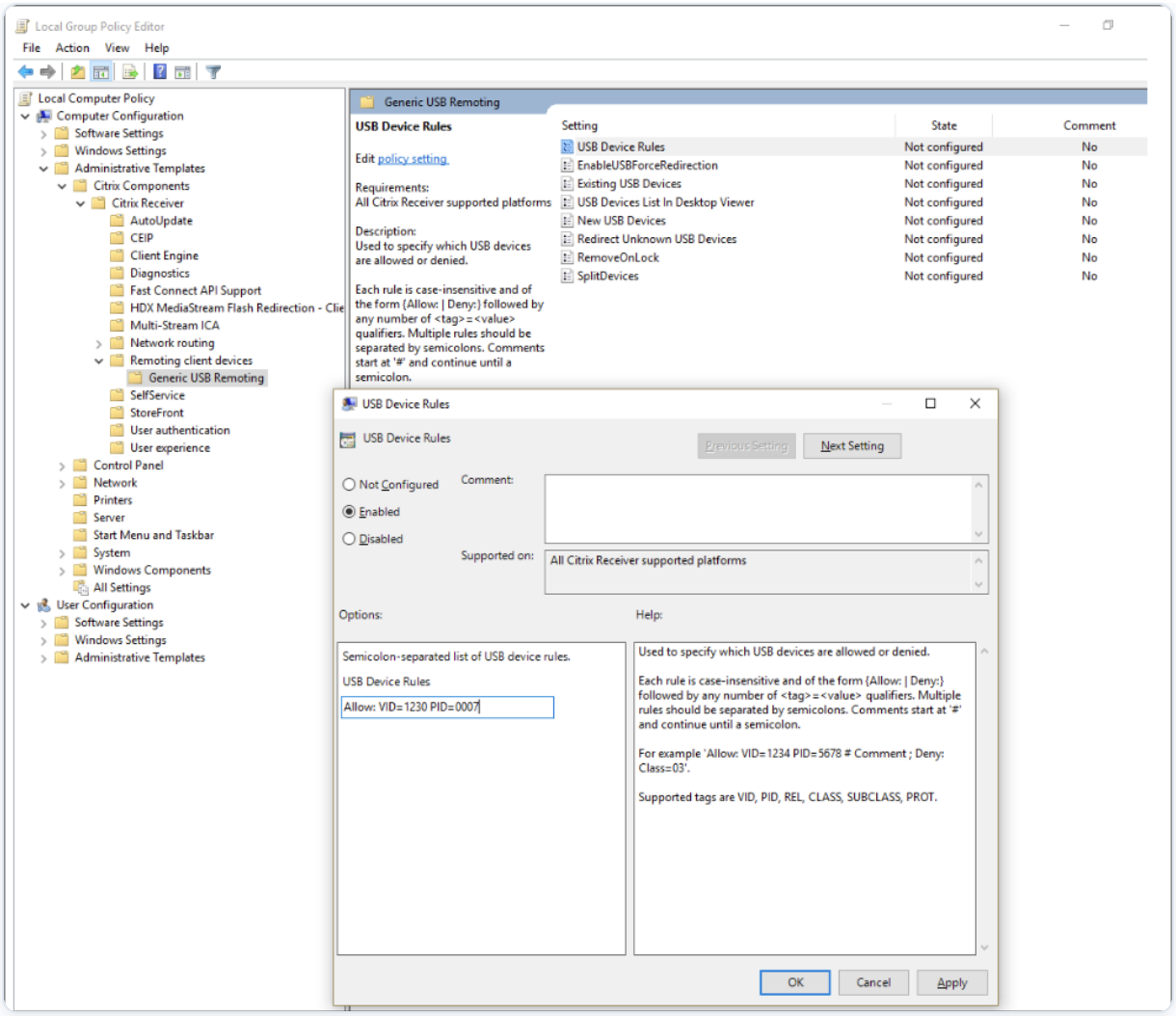
> **注：**
>
> Citrix®管理者が「デフォルト値を使用」をチェックし、「保存」をクリックすると、VDAの以下のレジストリでデフォルト規則が見つかります。
>
> **注意！：**
>
> レジストリエディターを使用する前に、この記事の最後にある免責事項を参照してください。 `HKLM\SOFTWARE\Wow6432Node\Citrix\PortICA\GenericUSB\DeviceRules`

クライアントでGPOを使用する:

1. **ローカル グループ ポリシー エディター**を開き、**管理用テンプレート > Citrix Components > Citrix Receiver™ > Remoting client devices > Generic USB Remoting**に移動します。
2. 「**USBデバイス規則設定**」を開き、その設定を有効にします。この例のようにUSBデバイス規則を追加します。 Allow: VID=1230 PID=0007 規則は、ベンダーID 1230および製品ID 0007のデバイスを許可します。

注：

特定のデバイスをデバイスルールリストの最上位に配置する必要がある場合は、Allow: VID=xxxx PID=xxxxルールを使用します。



注：

> USBViewのようなツール、または接続ツールバーでも、VIDやPIDなどのデバイスの詳細を特定するために使用できます（ここにSSを含めます）。

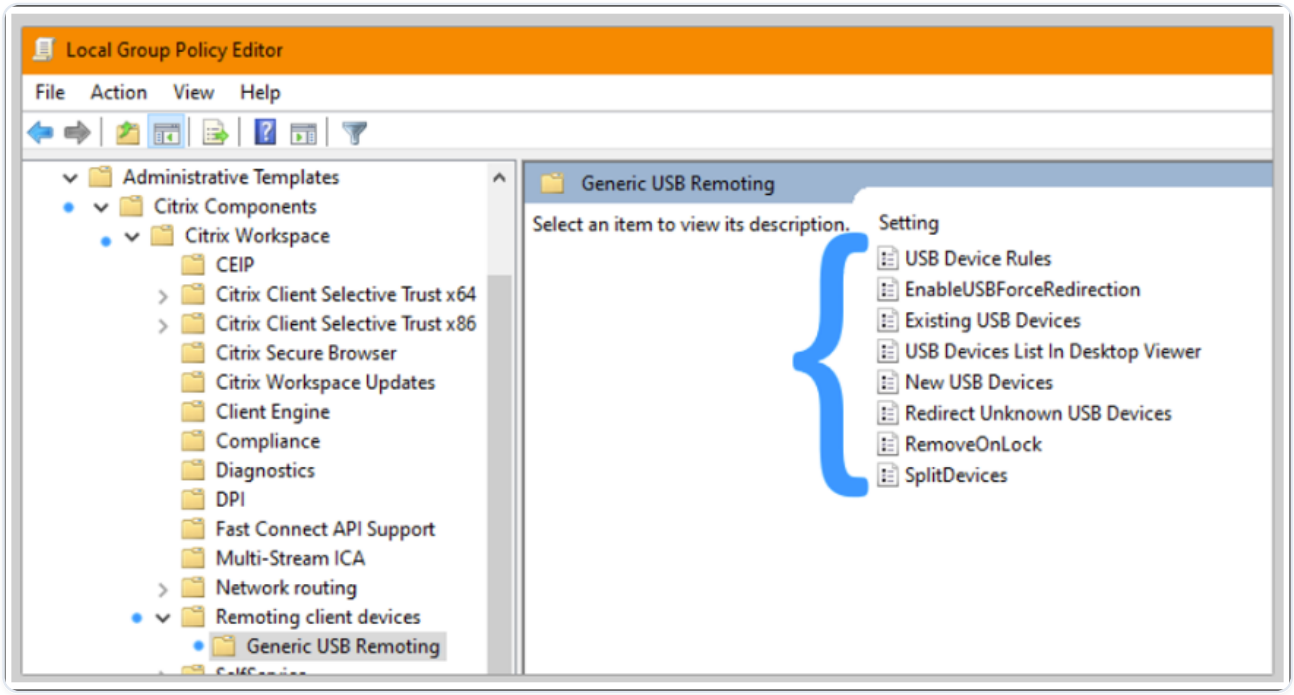
USBデバイスの自動リダイレクトを構成する

USBサポートが有効になっている場合、USBデバイスは自動的にリダイレクトされます。また、USBユーザー設定はUSBデバイスを自動的に接続するように設定されています。すべてのUSBデバイスをリダイレクトすることが常に最適とは限りません。ユーザーは、自動的にリダイレクトされないUSBデバイスリストからデバイスを明示的にリダイレクトできます。USBデバイスが一覧表示されたりリダイレクトされたりするのを防ぐには、クライアントエンドポイントでDeviceRulesポリシー設定を使用します。

このポリシーは、GPO、クライアント側レジストリ、Citrix Workspace™ Preferences、またはCDViewerのConnectionsタブを使用してクライアントで設定できます。これらの方法はすべて以下に説明されています。

クライアントでGPOを使用する:

1. **ローカル グループ ポリシー エディター**を開き、**管理用テンプレート > Citrix Components > Citrix Receiver > Remoting client devices > Generic USB Remoting**に移動します。
2. **新しいUSBデバイス**を開き、**有効**を選択して、**OK**をクリックします。
3. **既存のUSBデバイス**を開き、**有効**を選択して、**OK**をクリックします。



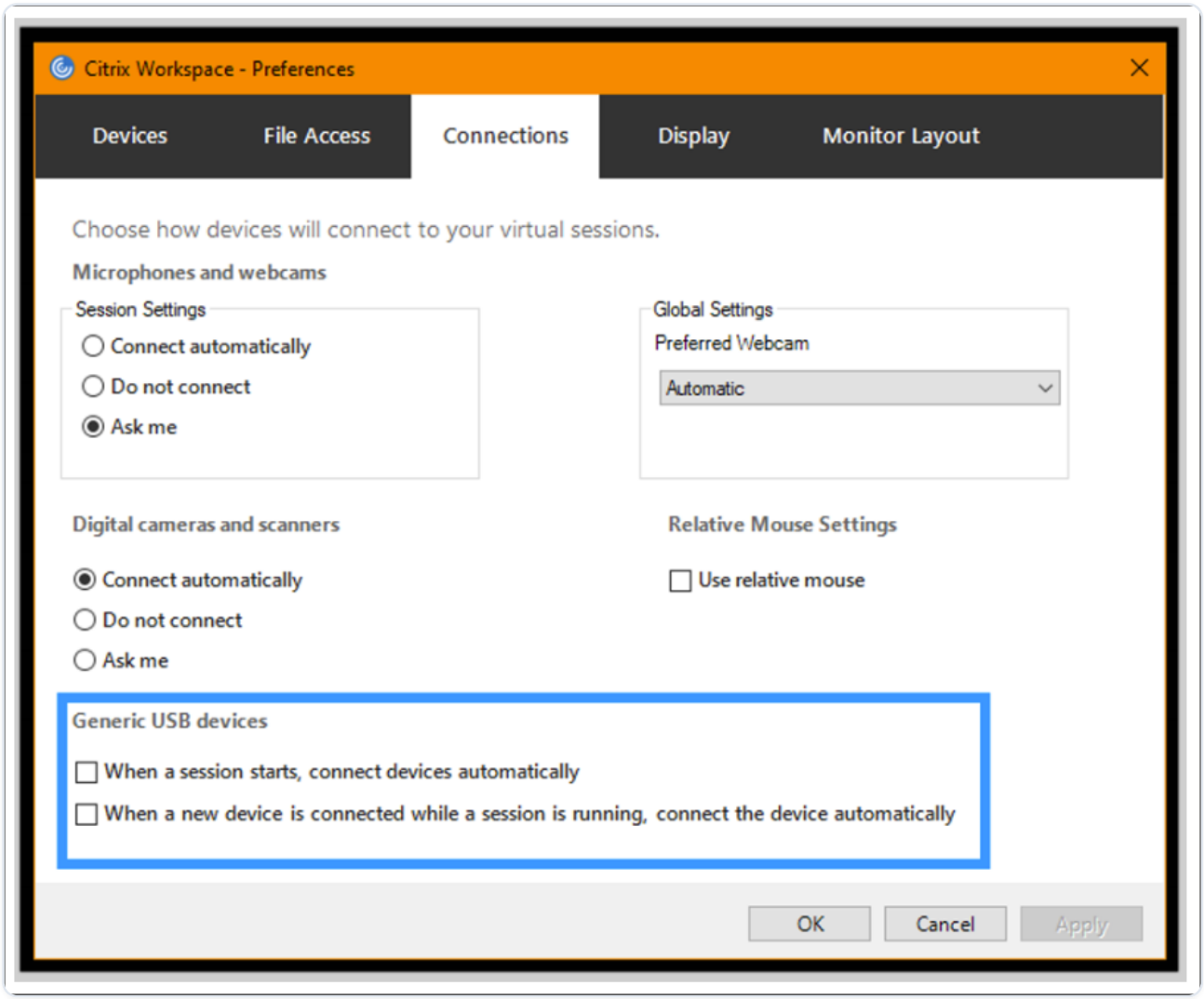
Citrix Connection Center を使用する方法:

1. **Citrix Workspace Preferences > Connections** に移動してください。

2. 次のオプションが選択されていることを確認します。
    a. セッション開始時にデバイスを自動的に接続する
    b. セッション実行中に新しいデバイスが接続された場合、そのデバイスを自動的に接続する。
3. **OK**をクリックします。

CDViewer 接続ツールバーの使用:

1. セッション開始後、「**CDViewer**」ドロップダウンをクリックし、「**Citrix Workspace Preferences > Connections**」タブを選択します。
2. 次のオプションが選択されていることを確認します。
    a. セッション開始時にデバイスを自動的に接続する
    b. セッション実行中に新しいデバイスが接続された場合、そのデバイスを自動的に接続する。
3. ポリシーを保存するには、**適用**と**OK**をクリックします。



クライアントベースの構成の場合、レジストリキーは次の場所にあるクライアントデバイスに設定されます。

> **注意！：**
>
> レジストリエディターを使用する前に、この記事の最後にある免責事項を参照してください。 `HKLM\SOFTWARE\Wow6432Node\Citrix\ICA Client\GenericUSB`

異なるデバイスルールを持つUSBリダイレクトを使用して2つ以上のデバイスを構成する

複数のデバイスを、異なるデバイスルールでHDX™セッション内にリダイレクトできます。管理者は、一方のデバイスを自動的にリダイレクトし、もう一方のデバイスはエンドユーザーにリダイレクトのオプションを提供したい場合があります。以下に、異なるルールで2つのデバイスを構成する手順を示します。

1. **Citrix Web Studio**で**クライアントUSBデバイスリダイレクト**ポリシー設定を有効にします。

2. クライアント側のGPOで**USBデバイスルール**設定を編集します。

    a. **ローカルグループポリシーエディター**を開き、**管理用テンプレート > Citrixコンポーネント > Citrix Receiver > クライアントデバイスのリモート処理 > Generic USB Remoting**に移動します。

    b. **USBデバイスルール設定**を開き、この設定を有効にします。この例のようにUSBデバイスルールを追加します。**Allow: VID=0911 PID=0c1c**ルールは、**ベンダーID 0911**および**製品ID 0c1c**のデバイスを許可しますが、自動的にはリダイレクトされません。**Connect: VID=06A8 PID=0043**ルールは、ステップ3で述べられている自動リダイレクトポリシーが設定されている場合、**ベンダーID 06A8**および**製品ID 0043**のデバイスを自動的にリダイレクトします。

    c. **Allow**: VID=0911 PID=0c1c #Phillips スピーチマイク.

    d. **Connect**: VID=06A8 PID=0043 class=03 # Topaz HSB シグネチャパッド

3. **ローカルグループポリシーエディター**を開き、**管理用テンプレート > Citrixコンポーネント > Citrix Receiver > クライアントデバイスのリモート処理 > Generic USB Remoting**に移動します。
4. **新しいUSBデバイス**を開き、**有効**を選択して**OK**をクリックします。
5. **既存のUSBデバイス**を開き、**有効**を選択して**OK**をクリックします。

これらの設定が構成されると、TopazシグネチャパッドはHDXセッション内に自動的にリダイレクトされ、セッション内でPhillipsスピーチマイクをリダイレクトするには、追加のエンドユーザー操作（接続センターまたはCD Viewerのタブでオプションを選択）が必要になります。

> **注：**
>
> ステップ2と3の上記の設定は、GenericUSBキー（HKLM\SOFTWARE\Wow6432Citrix\ICA Client\GenericUSB）の下にあるクライアント側のレジストリ値**DeviceRules**に直接適用することもできますが、これは推奨される方法ではありません。

クライアントドライブマッピング (CDM)

クライアントドライブマッピングは、クライアントエンドポイント上のストレージドライブをCitrix HDX™セッション内で利用可能にし、ファイルやフォルダーをクライアントからセッションホストへ、またはその逆に転送できるようにします。この機能は、読み取りおよび書き込みの両方の権限でデフォルトで有効になっています。マップされたクライアントデバイス上のファイルや

フォルダーをユーザーが追加または変更できないようにするには、**読み取り専用クライアントドライブアクセス**ポリシー設定を有効にします。この設定をポリシーに追加する際は、**クライアントドライブリダイレクト**設定が**許可**に設定され、ポリシーにも追加されていることを確認してください。

セキュリティ上の予防措置として、エンドポイントドライブはデフォルトで実行権限なしでマップされます。ユーザーがマップされたクライアントドライブから直接実行可能ファイルを実行できるようにするには、セッションホストで**ExecuteFromMappedDrive**レジストリ値を編集します。詳細については、**レジストリで管理されるHDX機能**セクションのマップされたクライアントドライブを参照してください。

要件

CDMを使用するための要件は次のとおりです。

Citrixコントロールプレーン

- シトリックス仮想アプリおよびデスクトップ™ 1912 以降
- シトリックス DaaS™

セッションホスト

- オペレーティングシステム
  - Windows 10 1809 以降
  - ウィンドウズ サーバー 2016 以降
  - Linux: Linux VDAのシステム要件を参照してください
- VDA
  - Windowsの場合、Citrix Virtual Apps and Desktops 1912 以降が必要です。
  - Linux: Linux VDAのドキュメントを参照してください

クライアントデバイス

- オペレーティングシステム
  - Windows 10 1809 以降
  - Linux: Workspace app for Linuxのシステム要件を参照してください。

関連ポリシー

CDM設定については、ポリシー設定リファレンスセクションを参照してください。

ダブルホップシナリオ

CDMはダブルホップシナリオでサポートされています。デフォルトでは、クライアントエンドポイントのドライブはセカンドホップセッションにマップされ、ファーストホップのドライブは利用できません。ただし、クライアントエンドポイントのドライブの代わりに、ファーストホップのドライブがセカンドホップセッションにマップされるように設定することも可能です。

この機能を構成するには、以下のレジストリ値を編集します。

- キー: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ClientDrive\
- 値の名前: NativeDriveMapping
- 値の型: REG_SZ
- 値のデータ:
  - True - 最初のホップセッションのドライブを2番目のホップセッションにマップします
  - False - クライアントエンドポイントのドライブを2番目のホップセッションにマップします

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

モバイルおよびタッチスクリーンクライアントデバイスのサポート

Citrix Virtual Apps and Desktops™ を使用すると、ユーザーは公開されたアプリケーションやデスクトップにモバイルおよびタッチスクリーンクライアントデバイスからアクセスできます。

要件

Citrix® コントロールプレーン

- シトリックス バーチャル アプリケーションズ アンド デスクトップス 1912 以降
- シトリックス DaaS™

セッションホスト

- オペレーティングシステム
  - Windows 10 1903 以降
  - Windows 11 21H2 以降
  - ウィンドウズ サーバー 2016 以降
- VDA
  - ウィンドウズ: シトリックス バーチャル アプリケーションズ アンド デスクトップス バージョン 7.15 以降

クライアントデバイス

- オペレーティングシステム
  - Windows 10 1809 以降
  - Windows 11 21H2 以降
- Windows 用 Citrix Workspace™ アプリ バージョン 1808 以降

Windows Continuum を使用するタッチスクリーンデバイスのタブレットモード

Continuum は、クライアントデバイスの使用方法に適応する Windows 10 の機能です。VDA は、タッチ対応クライアントでキーボードまたはマウスの存在を検出すると、クライアントをデスクトップモードにします。キーボードまたはマウスが存在しない場合、VDA はクライアントをタブレット/モバイルモードにします。この検出は、セッションの接続時および再接続時、ならびにセッション中にキーボードまたはマウスが接続または切断されたときに発生します。

この機能はデフォルトで有効になっています。この機能を無効にするには、ポリシー設定タブレットモード切り替えポリシー設定を構成します。

上記のタッチスクリーンデバイスの要件に加えて、Windows Continuumには以下が必要です。

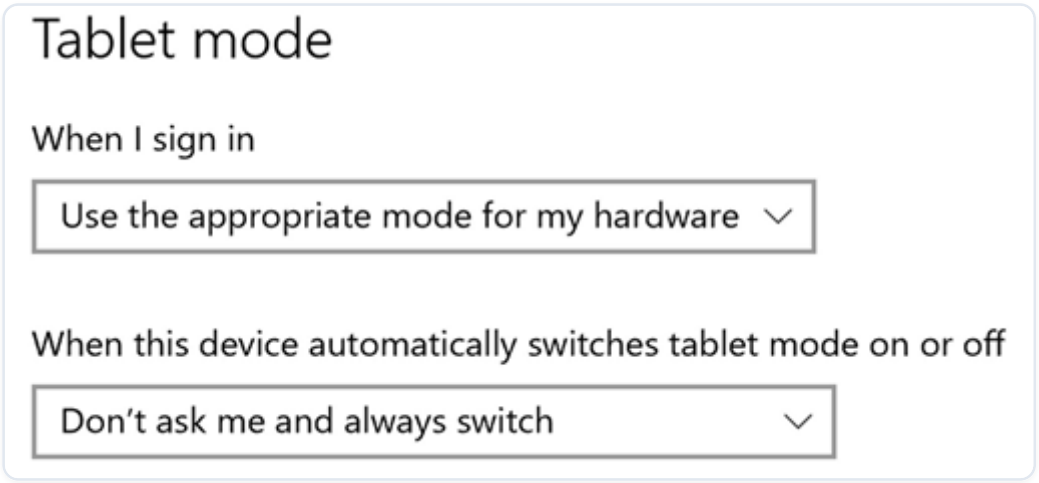
ゼノサーバー (旧 シトリックス ハイパーバイザー™)

- シトリックス ハイパーバイザー 8.2 以降
- ラップトップ/タブレットの切り替えを許可するには、XenServer CLIコマンドを実行します。
  xe vm-param-set uuid=\<VM_UUID\> platform:acpi_laptop_slate=1

> **重要:**
>
> メタデータ設定を変更した後に既存のマシンカタログのベースイメージを更新しても、以前にプロビジョニングされたVMには影響しません。XenServer VMのベースイメージを変更した後、カタログを作成し、ベースイメージを選択して、新しいMachine Creation Services™ (MCS) マシンをプロビジョニングします。

セッションホスト

- オペレーティングシステム
  - Windows 10 1903 以降
  - Windows 11 21H2 以降
- VDA
  - Windows: バージョン 7.16 以降
  - **現在のオペレーティングシステム構成の制限により、ユーザーは最初のICA®セッションを開始してVDAを再起動した後、ドロップダウンメニューから以下のオプションを設定する必要があります。**
    - **設定 > システム > タブレットモード**
      - ハードウェアに適したモードを使用する
      - 常に切り替える（確認しない）



タブレットモードは、タッチスクリーンにより適したユーザーインターフェイスを提供します。

- ボタンが少し大きくなります。
- スタート画面と起動するすべてのアプリが全画面で開きます。
- タスクバーに「戻る」ボタンが含まれます。
- タスクバーからアイコンが削除されます。

ファイルエクスプローラーにアクセスできます。



Windows 10 は、この更新された BIOS に基づいて、ターゲット仮想マシンに GPIO ドライバーをロードします。これは、仮想マシン内でタブレットモードとデスクトップモードを切り替えるために使用されます。

HTML5 用 Citrix Workspace アプリは、Windows Continuum 機能をサポートしていません。

デスクトップモードは、PCとキーボード、マウスを使用するのと同じ方法で操作できる、従来のユーザーインターフェイスを提供します。

マイクロソフト Surface Pro および Surface Book ペン

Windows Inkベースのアプリケーションで標準のペン機能をサポートしています。サポートには、ポインティング、消去、ペン圧、Bluetooth信号、およびオペレーティングシステムのファームウェアとペンモデルに応じたその他の機能が含まれます。例えば、ペン圧は最大4096レベルまで可能です。この機能はデフォルトで有効になっています。

ペン機能のサポートに関する要件は次のとおりです。

Citrixコントロールプレーン

- Citrix Virtual Apps and Desktops のバージョン1903以降
- シトリックス DaaS

セッションホスト

- オペレーティングシステム
  - Windows 10 1809 以降
  - Windows 11 21H2 以降
  - ウィンドウズ サーバー 2016 以降
- VDA
  - Windows: Citrix Virtual Apps and Desktops 1903 以降のバージョン

クライアントデバイス

- オペレーティングシステム
  - Windows 10 1809 以降
  - Windows 11 21H2 以降
- Windows向けCitrix Workspaceアプリ バージョン1902以降

Windows Ink とペンの機能のデモンストレーションについては、このグラフィックをクリックしてください。



この機能を無効または有効にするには、レジストリを介して管理される機能のリストにある Microsoft Surface Pro および Surface Book のペン を参照してください。

既知の問題

ペンサポートに関する既知の問題は次のとおりです。

- Windows Server 2k22 の OS 制限により、2k22 サーバーアプリケーションまたはデスクトップに接続している場合、ユーザーはペンのショートカットを設定したり、コントロールパネルでペン/インクの設定を調整したりすることはできません。
- OS の制限により、ペン対応の Windows 11 クライアントからのペンのショートカットは認識されません。

シリアルポート

ほとんどの新しいPCには、内蔵のシリアル（COM）ポートがありません。USBコンバーターを使用すれば、これらのポートを簡単に追加できます。シリアルポートに適したアプリケーションには、センサー、コントローラー、古いチェックリーダー、パッドなどがよく含まれます。一部のUSB仮想COMポートデバイスは、Windowsが提供するドライバー（usbser.sys）の代わりに、ベンダー固有のドライバーを使用します。これらのドライバーを使用すると、USBデバイスの仮想COMポートを、異なるUSBソケットに接続しても変更されないように強制できます。これは、**デバイスマネージャー > ポート (COM と LPT) > プロパティ**から、またはデバイスを制御するアプリケーションから実行できます。

クライアントCOMポートマッピングを使用すると、ユーザーのエンドポイントのCOMポートに接続されたデバイスを仮想セッション中に使用できます。これらのマッピングは、他のネットワークマッピングと同様に使用できます。

各COMポートに対して、オペレーティングシステムのドライバーはCOM1やCOM2などのシンボリックリンク名を割り当てます。アプリケーションは、そのリンクを使用してポートにアクセスします。

> **重要:**

> デバイスがUSBを直接使用してエンドポイントに接続できるからといって、汎用USBリダイレクトを使用してリダイレクトできるとは限りません。一部のUSBデバイスは仮想COMポートとして機能し、アプリケーションは物理シリアルポートと同じ方法でアクセスできます。オペレーティングシステムはCOMポートを抽象化し、ファイル共有のように扱うことができます。仮想COMの一般的なプロトコルは、CDC ACMまたはMCTの2つです。RS-485ポートを介して接続した場合、アプリケーションがまったく機能しない可能性があります。RS-485をCOMポートとして使用するには、RS-485-to-RS232コンバーターを入手してください。
> **重要:**

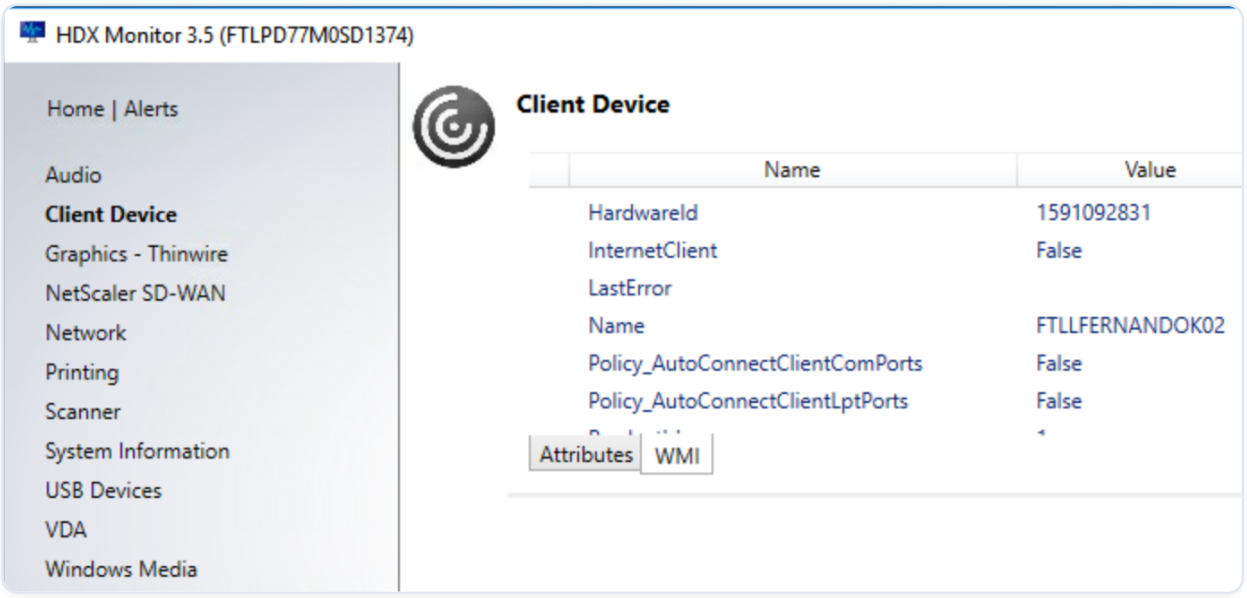
> 一部のアプリケーションは、デバイス（署名パッドなど）がクライアントワークステーションのCOM1またはCOM2に接続されている場合にのみ、一貫して認識します。

クライアントCOMポートをサーバーCOMポートにマッピングする

クライアントCOMポートをCitrix®セッションにマッピングするには、次の3つの方法があります。

- Studioポリシー。ポリシーの詳細については、「ポートリダイレクトポリシー設定」を参照してください。
- VDAコマンドプロンプト。
- リモートデスクトップ（ターミナルサービス）構成ツール。

1. **クライアントCOMポートリダイレクト**ポリシーと**クライアントCOMポートの自動接続Studio**ポリシーを有効にします。適用後、一部の情報はHDX™ Monitorで利用できます。



2. **クライアントCOMポートの自動接続**でポートのマッピングに失敗した場合は、手動でポートをマッピングするか、ログオンスクリプトを使用できます。VDAにログオンし、コマンドプロンプトウィンドウで次のように入力します。

   NET USE COMX: `\\CLIENT\COMZ`:

   または

   NET USE COMX: `\\CLIENT\CLIENTPORT:COMZ`:

   X はVDA上のCOMポートの番号です（ポート1～9がマッピングに利用可能です）。**Z** はマッピングするクライアントCOMポートの番号です。

操作が成功したことを確認するには、VDAのコマンドプロンプトで **NET USE** と入力します。表示されるリストには、マップされたドライブ、LPTポート、およびマップされたCOMポートが含まれます。



3. このCOMポートを仮想デスクトップまたはアプリケーションで使用するには、ユーザーデバイスアプリケーションをインストールし、マップされたCOMポート名を指定します。たとえば、クライアント上のCOM1をサーバー上のCOM3にマップする場合、VDAにCOMポートデバイスアプリケーションをインストールし、セッション中にCOM3を指定します。このマップされたCOMポートは、ユーザーデバイス上のCOMポートと同様に使用します。

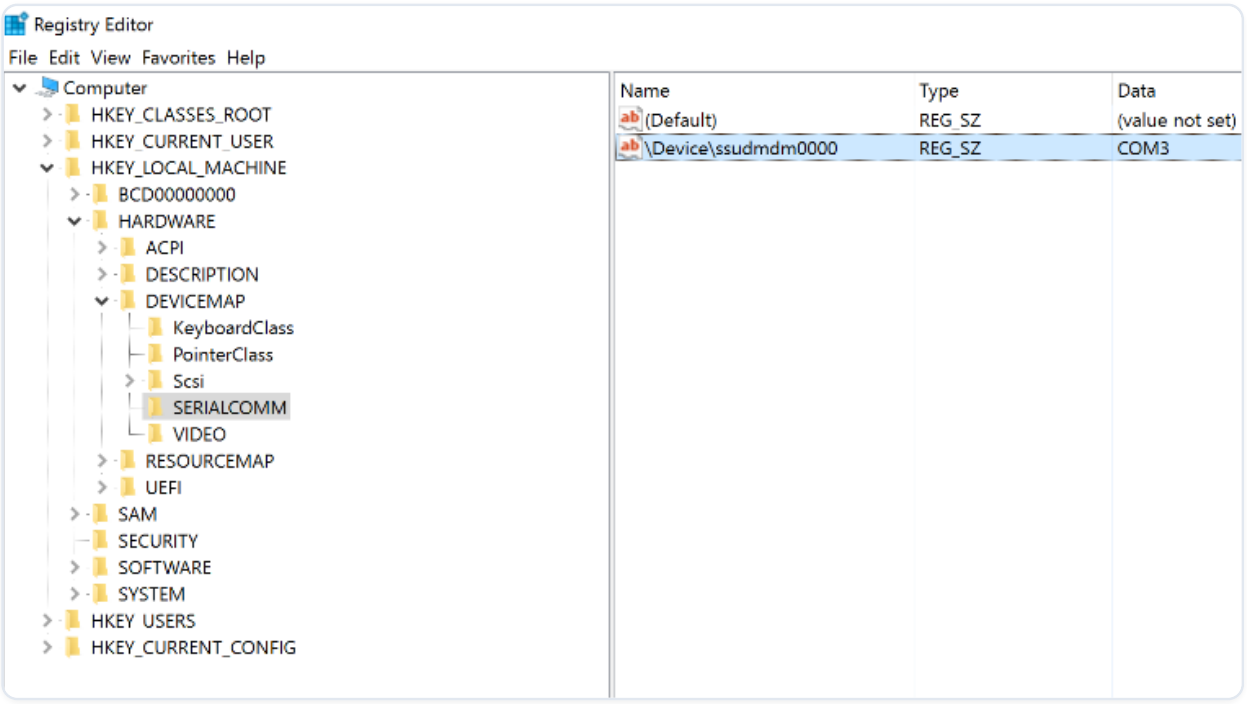
重要:

COMポートマッピングはTAPI互換ではありません。Windows Telephony Application Programming Interface (TAPI) デバイスをクライアントCOMポートにマップすることはできません。TAPIは、アプリケーションがデータ、FAX、音声通話の電話機能を制御するための標準的な方法を定義します。TAPIは、ダイヤル、応答、通話終了などのシグナリングを管理します。また、保留、転送、会議通話などの付加サービスも管理します。

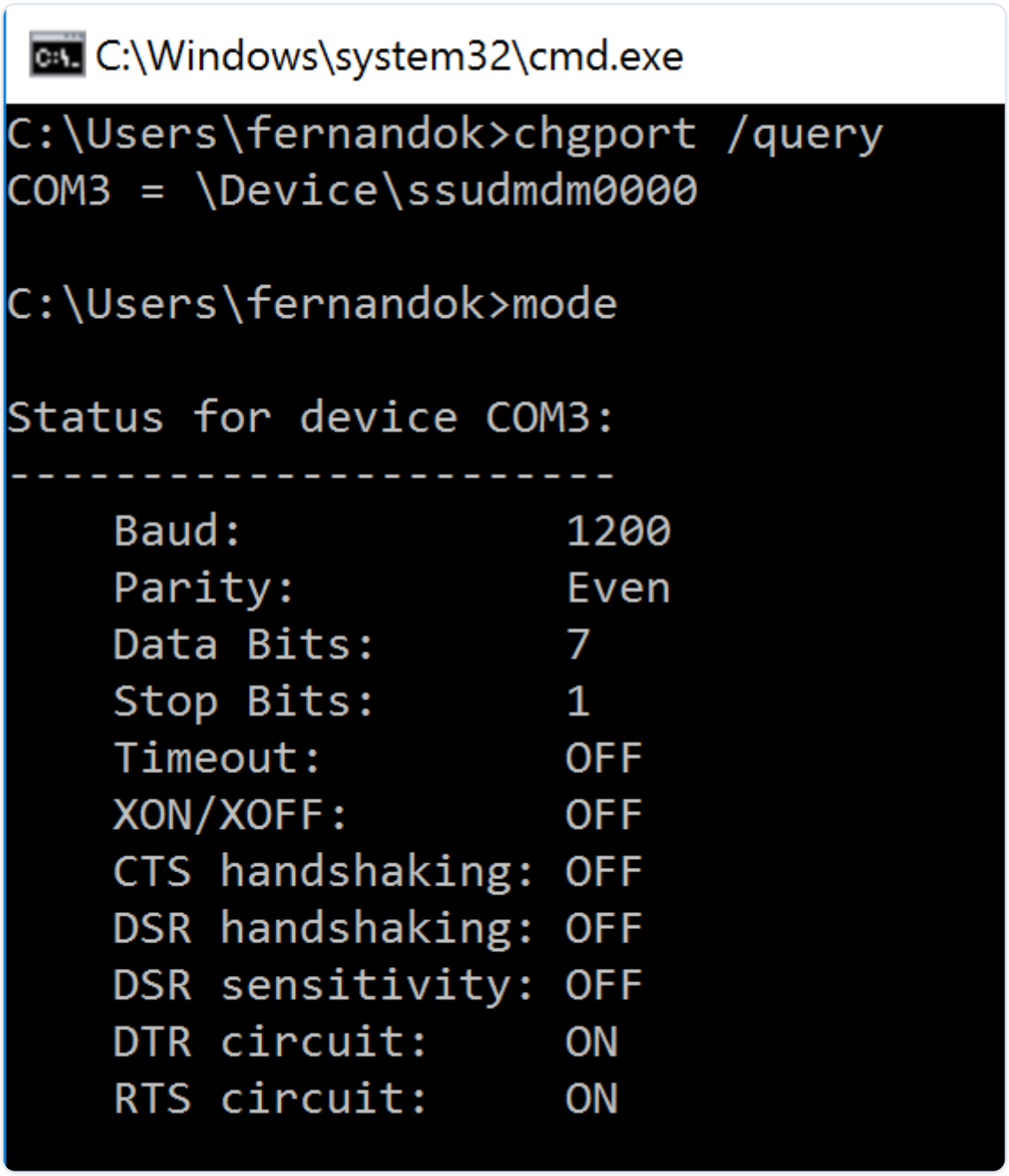
トラブルシューティング

1. Citrixをバイパスして、エンドポイントからデバイスに直接アクセスできることを確認してください。ポートがVDAにマップされていない間は、Citrixセッションに接続されていません。デバイスに付属のトラブルシューティング手順に従い、まずローカルで動作することを確認してください。 シリアルCOMポートにデバイスが接続されると、ここに示されているハイブにレ

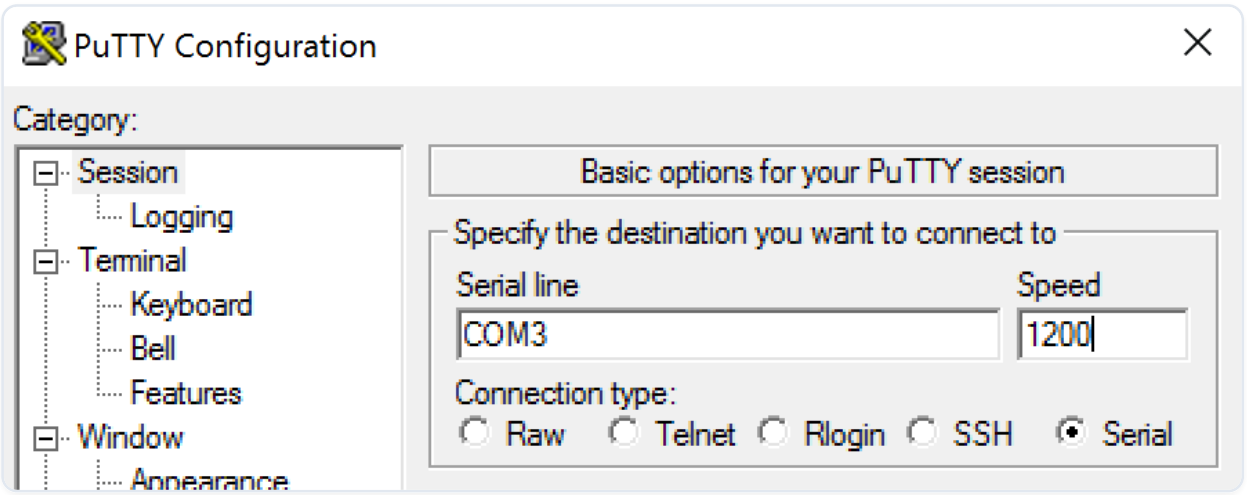
ジストリキーが作成されます。



この情報は、コマンドプロンプトで **chgport /query** を実行することでも確認できます。



デバイスのトラブルシューティング手順が利用できない場合は、PuTTYセッションを開いてみてください。**Session** を選択し、**Serial line** でCOMポートを指定します。



ローカルコマンドウィンドウで**MODE**を実行できます。出力には、使用中のCOMポートと、PuTTYセッションで必要となるボーレート/パリティ/データビット/ストップビットが表示される場合があります。PuTTY接続が成功した場合、**Enter**キーを押してデバイスからのフィードバックを確認します。入力した文字が画面に繰り返されたり、応答されたりする場合があります。この手順が失敗した場合、仮想セッションからデバイスにアクセスすることはできません。

2. ローカルのCOMポートをVDAにマッピングし（ポリシーまたは**NET USE COMX: `\\CLIENT\COMZ`:**を使用）、前のステップと同じPuTTYの手順を繰り返しますが、今回はVDAのPuTTYから実行します。PuTTYが「**Unable to open connection to COM1. Unable to open serial port**」というエラーを表示する場合、別のデバイスがCOM1を使用している可能性があります。

3. **chgport /query**を実行します。VDA上の組み込みWindowsシリアルドライバーが \Device\Serial0をVDAのCOM1ポートに自動割り当てしている場合、次の手順を実行します。
   A. VDAでCMDを開き、**NET USE**と入力します。

   B. VDA上の既存のマッピング（例：COM1）を削除します。

   NET USE COM1 /DELETE

   C. デバイスをVDAにマッピングします。

   NET USE COM1: `\\CLIENT\COM3`:

   D. VDA上のアプリケーションをCOM3にポイントします。

   最後に、ローカルのCOMポート（例：COM3）をVDA上の別のCOMポート（COM1以外、例：COM3）にマッピングしてみてください。アプリケーションがそれを指していることを確認してください。 **NET USE COM3: `\\CLIENT\COM3`**

4. ポートがマッピングされていることが確認でき、PuTTYは動作しているもののデータが通過しない場合、それは競合状態である可能性があります。アプリケーションがマッピングされる前にポートに接続して開いてしまい、マッピングをロックしている可能性があります。次のいずれかを試してください。

   - 同じサーバーで公開されている2番目のアプリケーションを開きます。ポートがマッピングされるまで数秒待ち、その後、ポートを使用しようとする実際のアプリケーションを開きます。
   - Studioではなく、Active Directoryのグループポリシーエディターから**COMポートリダイレクトポリシー**を有効にします。これらのポリシーは「**Client COM port redirection**」と「**Auto connect client COM ports**」です。このように適用されたポリシーは、Studioポリ

シーよりも前に処理され、COMポートが確実にマッピングされるようにする可能性があります。Citrixポリシーは VDAにプッシュされ、次の場所に保存されます。
`HKLN\SOFTWARE\Policies\Citrix \<user session ID\>`

- ユーザーにこのログオンスクリプトを使用するか、アプリケーションを公開する代わりに、まずVDA上のマッピングを削除し、仮想COMポートを再マッピングしてからアプリケーションを起動する.batスクリプトを公開します。

@echo off NET USE COM1 /delete NET USE COM2 /delete NET USE COM1: `\\CLIENT\COM1`: NET USE COM2: `\\CLIENT\COM2`: MODE COM1: BAUD=1200 （または必要な値） MODE COM2: BAUD=9600 PARITY=N Data=8 Stop=1 （または必要な値） START C:\Program Files\\\<Your Software Path>\\\<your_software.exe>

5. SysinternalsのProcess Monitorは、最後の手段となるツールです。VDAでこのツールを実行する際、COM3、picaser.sys、CdmRedirectorなどのオブジェクト、特に\<your_app\>.exeを見つけてフィルターします。エラーは「アクセス拒否」またはそれに類するものとして表示される場合があります。

特殊キーボード

Bloombergキーボード

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

Citrix Virtual Apps and Desktops™は、Bloombergモデル5、モデル4 Starboardキーボード（およびそれ以前のモデル3）をサポートしています。このキーボードにより、金融業界のお客様は、キーボードの特殊機能を使用して金融市場データにアクセスし、迅速な取引を実行できます。

> **重要:**

> Bloombergキーボードは1つのセッションでのみ使用することをお勧めします。複数の同時セッション（1つのクライアントから複数のセッションへ）でキーボードを使用することはお勧めしません。

> Bloombergキーボードは、1つの物理シェルに複数のUSBデバイスを搭載したUSB複合デバイスです。

- キーボード。
- 指紋リーダー。
- 音量を上げ下げするキー、およびスピーカーとマイクをミュートするキーを備えたオーディオデバイス。このデバイスには、オンボードスピーカー、マイク、およびマイクとヘッドセット用のジャックが含まれています。
- これらすべてのデバイスをシステムに接続するためのUSBハブ。

要件:

- Citrix Workspace™ app for Windowsが接続するセッションは、USBデバイスをサポートしている必要があります。
- Bloombergキーボードモデル5をサポートするには、Citrix Workspace app 2207 for Linux以降が必要です。
- Bloombergキーボードモデル5をサポートするには、Citrix Workspace app 2109 for Windows以降が必要です。
- Bloombergキーボードモデル3および4をサポートするには、Citrix Workspace app 1808 for WindowsまたはCitrix Receiver for Windows 4.8以降が必要です。
- モデル4でKVMモード（2本のUSBケーブルのうち1本がKVMを介してルーティングされる）を使用するには、Citrix Workspace app 1808 for WindowsまたはCitrix Receiver for Windows 4.12以降が必要です。

Citrix Workspace app for WindowsでのBloombergキーボードの構成については、Bloombergキーボードの構成を参照してください。

Bloombergキーボードのサポートを有効にするには、レジストリを介して管理される機能のリストでBloombergキーボードを参照してください。

サポートを確認する:

Citrix WorkspaceアプリでBloombergキーボードのサポートが有効になっているかを確認するには、Desktop ViewerがBloombergキーボードのデバイスを正しく報告しているかを確認します。

デスクトップシナリオ:

Desktop Viewerを開きます。Bloombergキーボードのサポートが有効になっている場合、Desktop ViewerにはUSBアイコンの下に3つのデバイスが表示されます。

Bloomberg 5キーボードの場合:

- ブルームバーグLP ブルームバーグ生体認証モジュール
- Bloomberg LP Keyboard (2つのインターフェイスを持つ複合デバイス)
- Bloomberg LP Keyboard Audio (3つのインターフェイスを持つ複合デバイス)

Bloomberg 3および4キーボードの場合:

- ブルームバーグ指紋スキャナー
- ブルームバーグキーボード機能
- ブルームバーグLP キーボード 2013

シームレスアプリケーションのみのシナリオ:

Citrix Workspaceアプリの通知領域アイコンから**接続センター**メニューを開きます。Bloombergキーボードのサポートが有効になっている場合、3つのデバイスが**デバイス**メニューに表示されます。

これらの各デバイスのチェックマークは、それらがセッションにリモート接続されていることを示します。

Webカメラ

高解像度Webカメラストリーミング

Webカメラは、仮想セッション内で実行されているビデオ会議アプリケーションで使用できます。サーバー上のアプリケーションは、サポートされているフォーマットタイプに基づいてWebカメラのフォーマットと解像度を選択します。セッションが開始されると、クライアントはWebカメラ情報をサーバーに送信します。ビデオ会議アプリケーションからWebカメラを選択します。Webカメラとアプリケーションの両方が高解像度レンダリングをサポートしている場合、アプリケーションは高解像度を使用します。Webカメラの解像度は最大1920x1080までサポートしています。

この機能には、Citrix Receiver for Windowsバージョン4.10以降が必要です。HDX Webカメラリダイレクトをサポートするアプリプラットフォームのリストについては、「Citrix Workspace app feature matrix」を参照してください。

高解像度Webカメラストリーミングの詳細については、「HDX video conferencing and webcam video compression」を参照してください。

レジストリキーを使用してこの機能を無効または有効にし、特定の解像度を構成できます。詳細については、レジストリで管理される機能のリストにある「High-definition webcam streaming and High-definition webcam resolution」を参照してください。

グラフィックス

Citrix HDXグラフィックスには、Citrix Virtual Apps and Desktopsからのリッチグラフィックスアプリケーションの配信を最適化する、広範なグラフィックスアクセラレーションおよびエンコーディングテクノロジーが含まれています。これらのグラフィックテクノロジーは、グラフィックスを多用する仮想アプリケーションをリモートで操作する際に、物理デスクトップを使用するのと同じエクスペリエンスを提供します。

グラフィックスレンダリングには、ソフトウェアまたはハードウェアを使用できます。ソフトウェアレンダリングには、ソフトウェアラスタライザーと呼ばれるサードパーティライブラリが必要です。たとえば、WindowsにはDirectXベースのグラフィックス用のWARPラスタライザーが含まれています。場合によっては、代替のソフトウェアレンダラーを使用したいと思うかもしれません。ハードウェアレンダリング（ハードウェアアクセラレーション）には、グラフィックスプロセッサ（GPU）が必要です。

HDX™ Graphicsは、最も一般的なユースケース向けに最適化されたデフォルトのエンコーディング構成を提供します。Citrixポリシーを使用することで、IT管理者はさまざまなグラフィックス関連設定を構成して、さまざまな要件を満たし、望ましいユーザーエクスペリエンスを提供することもできます。

シンワイヤー

Thinwireは、Citrix Virtual Apps and Desktopsで使用されるCitrixのデフォルトのディスプレイリモートテクノロジーです。

ディスプレイリモートテクノロジーにより、あるマシンで生成されたグラフィックスを、通常はネットワーク経由で別のマシンに送信して表示できます。グラフィックスは、キーボード入力やマウス操作などのユーザー入力の結果として生成されます。

エイチディーエックス スリーディー プロ

Citrix Virtual Apps and DesktopsのHDX 3D Pro機能を使用すると、ハードウェアアクセラレーションにグラフィックス処理ユニット（GPU）を使用して最高のパフォーマンスを発揮するデスクトップとアプリケーションを配信できます。これらのアプリケーションには、OpenGLおよびDirectXベースの3Dプロフェッショナルグラフィックスアプリケーションが含まれます。標準VDAはDirectXのGPUアクセラレーションのみをサポートします。

WindowsシングルセッションOS向けGPUアクセラレーション

HDX 3D Proを使用すると、グラフィックスを多用するアプリケーションを、ホストされたデスクトップまたはシングルセッションOSマシン上のアプリケーションの一部として配信できます。HDX 3D Proは、物理ホストコンピューター（デスクトップ、ブレード、ラックワークステーションを含む）と、XenServer®、vSphere、Hyper-V（パススルーのみ）ハイパーバイザーが提供するGPUパススルーおよびGPU仮想化テクノロジーをサポートします。

GPUパススルーを使用すると、専用のグラフィックス処理ハードウェアに排他的にアクセスできるVMを作成できます。ハイパーバイザーに複数のGPUをインストールし、これらのGPUのそれぞれにVMを1対1で割り当てることができます。

GPU仮想化を使用すると、複数の仮想マシンが単一の物理GPUのグラフィックス処理能力に直接アクセスできます。

WindowsマルチセッションOS向けGPUアクセラレーション

HDX 3D Proを使用すると、WindowsマルチセッションOSセッションで実行されているグラフィックス負荷の高いアプリケーションを、サーバーのグラフィックス処理ユニット（GPU）でレンダリングできます。OpenGL、DirectX、Direct3D、およびWindows Presentation Foundation（WPF）のレンダリングをサーバーGPUに移行することで、グラフィックスレンダリングがサーバーCPUの速度を低下させることはありません。また、ワークロードがCPUとGPUに分割されるため、サーバーはより多くのグラフィックスを処理できます。

フレームホーク

> **重要:**
>
> Citrix Virtual Apps and Desktops 7 1903以降、Framehawkはサポートされなくなりました。代わりに、Thinwireをアダプティブトランスポートを有効にして使用してください。

> Framehawkは、ブロードバンドワイヤレス接続（Wi-Fiおよび4G/LTEセルラーネットワーク）を使用するモバイルワーカー向けのディスプレイリモートテクノロジーです。Framehawkは、スペクトル干渉やマルチパス伝播の課題を克服し、仮想アプリおよびデスクトップのユーザーにスムーズでインタラクティブなユーザーエクスペリエンスを提供します。

テキストベースのセッションウォーターマーク

テキストベースのセッションウォーターマークは、データ盗難を抑止し、追跡を可能にするのに役立ちます。この追跡可能な情報は、写真やスクリーンキャプチャを使用してデータを盗む者への抑止力として、セッションデスクトップに表示されます。テキストのレイヤーであるウォーターマークを指定できます。ウォーターマークは、元のドキュメントの内容を変更することなく、セッション画面全体に表示できます。テキストベースのセッションウォーターマークにはVDAのサポートが必要です。

アダプティブ リフレッシュ レート

新しいスケーラビリティの改善により、HDXは仮想モニターのリフレッシュレートをターゲットFPSポリシー設定に合わせます。アダプティブ リフレッシュ レート（ARR）は、シングルセッションVDAとマルチセッションVDAの両方で利用でき、GPUアクセラレーションシナリオと非GPUシナリオの両方で機能します。

ロス許容モード

ロス許容モードは、パケットロスが検出された場合でもセッションがインタラクティブな状態を維持するように徹底的に再設計されています。

関連情報

- HDX 3D プロ
- WindowsシングルセッションOSのGPUアクセラレーション
- WindowsマルチセッションOSのGPUアクセラレーション
- フレームホーク
- シンワイヤー
- テキストベースのセッションウォーターマーク(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/graphics/session-watermark.html)

10ビットハイダイナミックレンジ (HDR)

10ビットハイダイナミックレンジ (HDR) 仮想デスクトップセッションでは、拡張されたエンコードおよびデコード機能を使用して、より広い色域、優れたコントラストと明るさで高品質の画像やビデオをレンダリングできます。また、ユーザーエクスペリエンスを向上させるために、白色輝度レベル、Extended Display Identification Data (EDID)、および視覚品質をカスタマイズできます。

システム要件

エンドポイント:

- NVIDIA GPU 用 Citrix Workspace™ アプリ for Windows 2209 以降
- エンドポイント上で10ビットHEVC (H.265) 444デコードをサポートするNVIDIA GPU
- 10ビットHDR対応モニター。ディスプレイ設定を使用して、すべてのモニターで10ビットHDRを有効にする必要があります。

サーバー:

- NVIDIA GPU 用 Windows シングルセッションOS VDA 2209 以降、およびIntel GPU 用 VDA 2308 以降
- VDA上で10ビットHEVC 444エンコードをサポートするNVIDIA GPU

必要なポリシー

エンドポイント:

- グラフィックのH.265デコードを有効にする

サーバー:

- 3Dグラフィックワークロード向けに最適化
- グラフィックステータスインジケーター (オプション)

サーバー構成

10ビットHDR対応のエンドポイントモニターでCitrix®セッションを起動すると、HDRセッションがデフォルトで有効になります。マルチモニターHDRセッションでは、すべてのエンドポイントモニターで10ビットHDRが有効になっている必要があります。HDRセッションは、ウィンドウモードと全画面モードの両方でサポートされます。

参照白色レベル

この設定は、ニット値によって白色輝度レベルを定義します。セッション内の相対的なHDR画面の明るさを制御します。デフォルト値は80ニットです。異なるニット値を定義するには、次のレジストリキーを設定します。

- HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics
- 種類: REG_DWORD
- 名前: RefWhiteLevel

設定を有効にするには、セッションのサイズを変更するか、セッションを切断して再起動する必要があります。

EDIDのオーバーライド

VDAをHDRセッションでエンドポイントモニターのEDIDを使用するように構成できます。これにより、色域と輝度範囲を一致させることで、モニターの表示機能を最大限に活用できます。デフォルトでは、HDRセッションはHDR1000対応のディスプレイを想定しています。 エンドポイントモニターのEDIDは、NVIDIAまたはその他のツールを使用してエクスポートできます。次のレジストリキーを使用してVDAに適用します。

- HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics
- 種類: REG_BINARY
- 項目名: EDIDOverride

EDIDをレジストリに保存する際、コンマ、スペース、または特殊文字を含めてはなりません。オーバーライドEDIDを有効にするには、サインアウトして新しいセッションを起動します。

視覚的にロスレスなエクスペリエンス

視覚的にロスレスなエクスペリエンスを実現するには、次のポリシーを有効にします。

- 視覚的にロスレス圧縮を許可する
- 視覚品質: 常にロスレスまたはロスレスに構築

ポリシーが設定された後、グラフィックスステータスインジケーターを使用して、イメージ品質スライダーを使用するか、ピクセルパーフェクトモードに切り替えることで、HDRセッションの品質を制御できます。

Windowsの画面ロックを許可する

このポリシーを使用すると、画面ロックを含むすべてのWindowsディスプレイタイムアウトを、ワークステーションOS上のCitrix Virtual Desktopセッションに適用できます。この設定は、Citrix StudioのCitrixグループポリシーオブジェクトを使用して設定できます。

デフォルトでは、この設定が有効になっていない場合、アクティブなセッション中にCitrix Virtual Desktopはセッションロック、スクリーンセーバー、またはディスプレイオフのタイムアウトに応答しません。

ワークステーションVDAでパスワード保護されたスクリーンセーバーが構成されている場合、スクリーンセーバーのタイムアウトに達したときにCitrix Virtual Desktopセッションが自動的にロックされるようにするには、この設定を有効にする必要があります。

VDAでディスプレイオフタイムアウトが構成されているときにこの設定を有効にすると、そのタイムアウトの期限切れにより、ユーザーがセッションとの対話を再開するまで更新されないセッションになります。たとえば、表示されている時間は更新されず、新しい通知も表示されません。

その他の考慮事項

- 仮想GPU上で最大4台のモニターで10ビットHDRセッションを起動できます。
- 次の場合、Citrixセッションは8ビットの非HDRモードに戻ります。
  - いずれかのエンドポイントモニターで10ビットHDRが有効になっていない場合
  - 画面共有を有効にする。
  - VDAで仮想ディスプレイレイアウトを設定する。
  - **視覚的にロスレス圧縮を許可**ポリシーを設定せずにピクセルパーフェクトモードに切り替える。

HDX™ 3D プロ

Citrix Virtual Apps and Desktops™のHDX 3D Pro機能を使用すると、ハードウェアアクセラレーションのためにグラフィック処理ユニット（GPU）を使用すると最高のパフォーマンスを発揮するデスクトップとアプリケーションを提供できます。これらのアプリケーションには、OpenGLおよびDirectXベースの3Dプロフェッショナルグラフィックアプリケーションが含まれます。標準VDAは、DirectXのGPUアクセラレーションのみをサポートします。

HDX 3D Proポリシー設定については、「3Dグラフィックワークロードの最適化」(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/policies/reference/ica-policy-settings/graphics-policy-settings.html#optimize-for-3d-graphics-workload)を参照してください。

サポートされているすべてのCitrix Workspaceアプリは、3Dグラフィックで使用できます。複雑な3Dワークロード、高解像度モニター、マルチモニター構成、高フレームレートアプリケーションで最高のパフォーマンスを得るには、Citrix Workspace app for WindowsおよびCitrix Workspace app for Linuxの最新バージョンをお勧めします。Citrix Workspaceアプリのサポートされているバージョンに関する詳細については、Citrix Workspaceアプリのライフサイクルマイルストーンを参照してください。

3Dプロフェッショナルアプリケーションの例は次のとおりです。

- コンピューター支援設計、製造、エンジニアリング (CAD/CAM/CAE) アプリケーション
- 地理情報システム (GIS) ソフトウェア
- 医用画像処理通信システム (PACS)

- 最新のOpenGL、DirectX、NVIDIA CUDA、OpenCL、およびWebGLバージョンを使用するアプリケーション
- 並列コンピューティングにNVIDIA Compute Unified Device Architecture (CUDA) GPUを使用する計算集約型の非グラフィックアプリケーション

HDX 3D Proは、あらゆる帯域幅で最高のユーザーエクスペリエンスを提供します。

- WAN接続の場合：1.5 Mbpsという低い帯域幅のWAN接続でも、インタラクティブなユーザーエクスペリエンスを提供します。
- LAN接続の場合：LAN接続でローカルデスクトップと同等のユーザーエクスペリエンスを提供します。

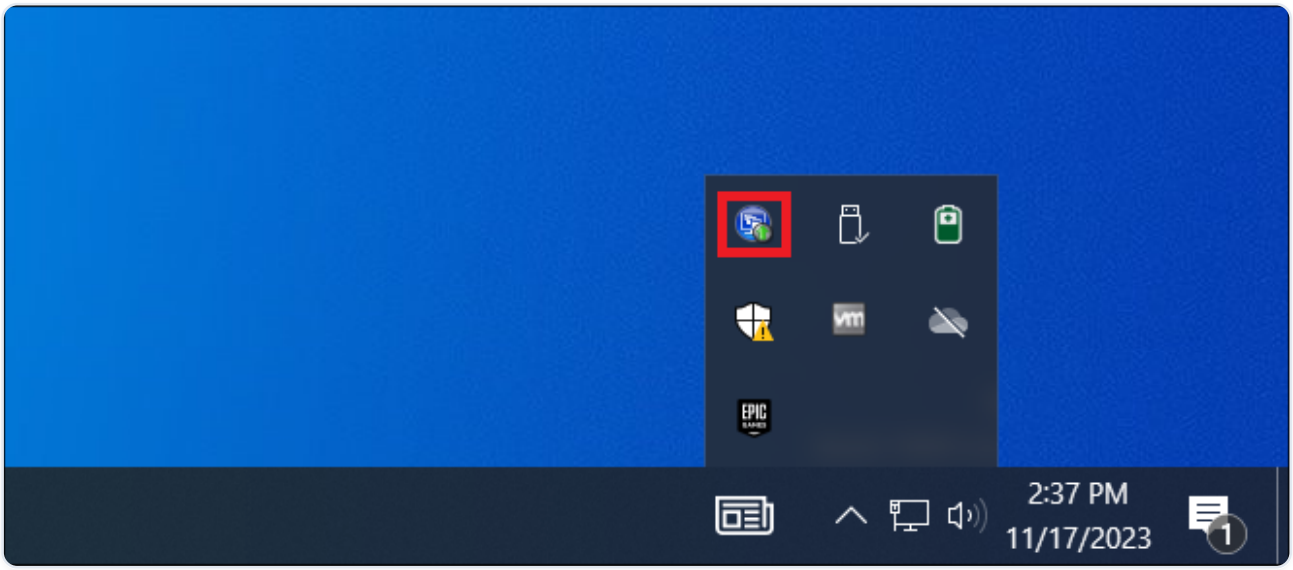
  複雑で高価なワークステーションを、グラフィック処理をデータセンターに移動して一元管理することで、よりシンプルなユーザーデバイスに置き換えることができます。

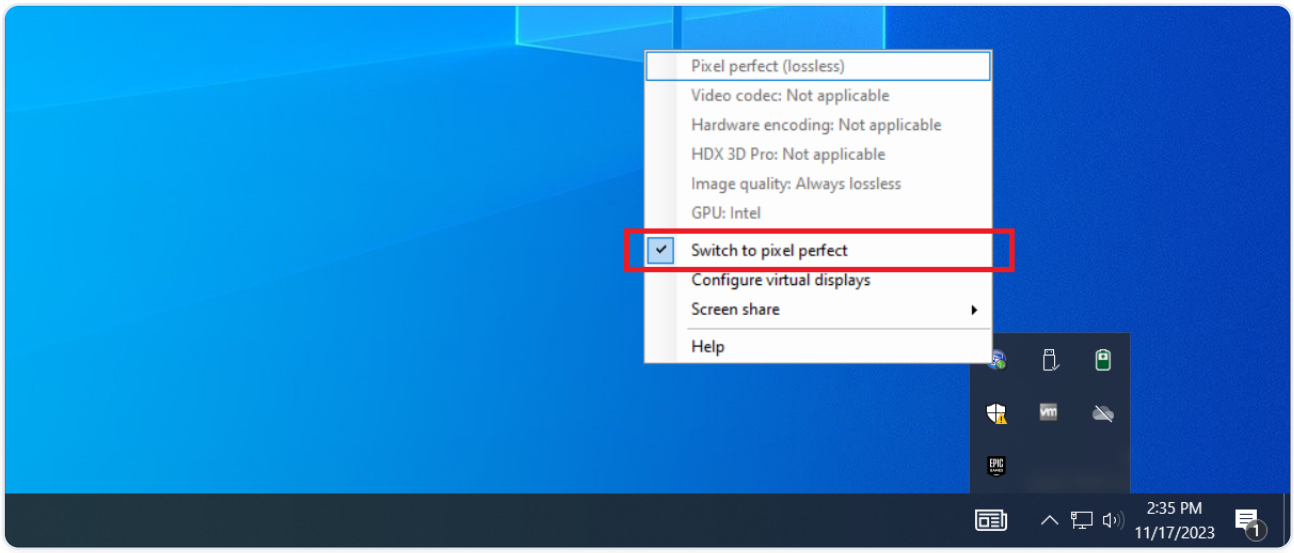
特殊なユースケース向けのロスレス圧縮オプション

HDX 3D Proは、医用画像処理など、ピクセルパーフェクトなグラフィックが必要なアプリケーションをサポートするために、CPUベースのロスレスコーデックも提供します。真のロスレス圧縮は、より多くのネットワークリソースと処理リソースを消費するため、特殊なユースケースでのみ推奨されます。

ロスレス圧縮を使用する場合：

- 通知領域アイコンであるグラフィックステータスインジケーターのロスレスインジケーターは、表示されている画面がロッシーフレームかロスレスフレームかをユーザーに通知します。このアイコンは、**視覚品質**ポリシー設定で**ロスレスにビルド**が指定されている場合に役立ちます。送信されるフレームがロスレスの場合、ロスレスインジケーターは緑色に変わります。





- ロスレススイッチを使用すると、セッション中にいつでも**常にロスレス**モードに変更できます。セッション内で**ロスレス**を選択または解除するには、アイコンを右クリックして**ピクセルパーフェクトに切り替え**をクリックするか、ショートカットALT+SHIFT+1を使用します。
  - ロスレス圧縮の場合：HDX 3D Proは、ポリシーで選択されたコーデックに関係なく、ロスレスコーデックを圧縮に使用します。
  - ロッシー圧縮の場合：HDX 3D Proは、デフォルトまたはポリシーによって選択された元のコーデックを使用します。 ロスレススイッチの設定は、以降のセッションでは保持されません。すべての接続でロスレスコーデックを使用するには、**視覚品質ポリシー**設定で**常にロスレス**を選択します。

セッション内でロスレスを選択または選択解除するためのデフォルトのショートカットALT+SHIFT+1を上書きできます。
`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HDX3D\LLIndicator`で新しいレジストリ設定を構成します。

- 名前: HKEY_LOCAL_MACHINE_HotKey, 種類: String
- ショートカットの組み合わせを設定する形式は、C=0|1, A=0|1, S=0|1, W=0|1, K=val です。キーはコンマ「,」で区切る必要があります。キーの順序は関係ありません。
- A、C、S、W、Kはキーであり、C=Control、A=ALT、S=SHIFT、W=Win、K=有効なキーです。Kに許可される値は、0～9、a～z、および任意の仮想キーコードです。
- 例： F10の場合、K=0x79を設定 Ctrl + F10の場合、C=1, K=0x79を設定 Alt + Aの場合、A=1, K=a または A=1, K=A または K=A, A=1を設定 Ctrl + Alt + 5の場合、C=1, A=1, K=5 または A=1, K=5, C=1を設定 Ctrl + Shift + F5の場合、A=1, S=1, K=0x74を設定

HDX 3D Proのユーザーエクスペリエンスを最適化する

複数のユーザーが帯域幅の制限された接続を共有している場合（たとえば、支店など）、各ユーザーが利用できる帯域幅を制限するために、「セッション全体の帯域幅制限」ポリシー設定を使用することをお勧めします。この設定を使用すると、ユーザーがログオンおよびログオフする際に、利用可能な帯域幅が大きく変動しないようにします。HDX 3D Proは利用可能な帯域幅をすべて使用するように自動的に調整するため、ユーザーセッション全体で利用可能な帯域幅に大きな変動があると、パフォーマンスに悪影響を及ぼす可能性があります。 たとえば、20人のユーザーが60 Mbpsの接続を共有している場合、各ユーザーが利用できる帯域幅は、同時接続ユーザー数に応じて3 Mbpsから60 Mbpsの間で変動する可能性があります。このシナリオでユーザーエクスペリエンスを最適化するには、ピーク時にユーザーごとに必要な帯域幅を決定し、常にこの量にユーザーを制限します。 3Dマウスのユーザーの場合、Generic USB Redirection仮想チャネルの優先度を0に上げることをお勧めします。仮想チャネルの優先度を変更する方法については、Knowledge Centerの記事CTX128190を参照してください。 HDX Monitorツールを使用して、HDX視覚化テクノロジーの動作と構成を検証し、HDXの問題を診断およびトラブルシューティングします。このツールは、Citrix Virtual Apps and DesktopsインストールメディアのSupportフォルダーにあります。

Windows マルチセッション OS 用 GPU アクセラレーション

Citrix Virtual Apps and Desktops™ は、Windows マルチセッション OS セッションで実行されるグラフィックを多用するアプリケーションを、サーバーのグラフィック処理ユニット (GPU) でレンダリングすることをサポートします。OpenGL、DirectX、Direct3D、および Windows Presentation Foundation (WPF) のレンダリングをサーバーの GPU に移動することで、サーバーの CPU をより効率的に使用できます。

Windows Server はマルチユーザーオペレーティングシステムであるため、複数のユーザーが GPU 仮想化 (vGPU) を必要とせずに Citrix Virtual Apps™ によってアクセスされる GPU を共有できます。

レジストリの編集を伴う手順については、注意してください。レジストリを誤って編集すると、オペレーティングシステムの再インストールが必要になるような深刻な問題を引き起こす可能性があります。Citrix® は、レジストリエディターの誤った使用によって生じる問題が解決できることを保証できません。レジストリエディターは自己責任で使用してください。編集する前にレジストリをバックアップしてください。

GPU 共有

GPU 共有により、リモートデスクトップセッションで OpenGL および DirectX アプリケーションの GPU ハードウェアレンダリングが可能になります。次の特性があります。

- アプリケーションのスケーラビリティとパフォーマンスを向上させるために、ベアメタルまたは仮想マシンで使用できます。
- 複数の同時セッションで GPU リソースを共有できます (ほとんどのユーザーは専用 GPU のレンダリングパフォーマンスを必要としません)。
- 特別な設定は必要ありません。

GPU は、ハイパーバイザーおよび GPU ベンダーの要件に従って、フルパススルーモードまたは仮想 GPU (vGPU) モードのいずれかで Windows Server 仮想マシンに割り当てることができます。物理 Windows Server マシンへのベアメタル展開もサポートされています。

GPU 共有は、特定のグラフィックカードに依存しません。

- 仮想マシンについては、使用中のハイパーバイザーと互換性のあるグラフィックカードを選択してください。XenServer のハードウェア互換性リストについては、「Hypervisor Hardware Compatibility List」を参照してください。
- ベアメタルで実行する場合、オペレーティングシステムによって単一のディスプレイアダプターが有効になっていることを推奨します。複数の GPU がハードウェアにインストールされている場合は、デバイスマネージャーを使用して、1 つを除くすべてを無効にしてください。

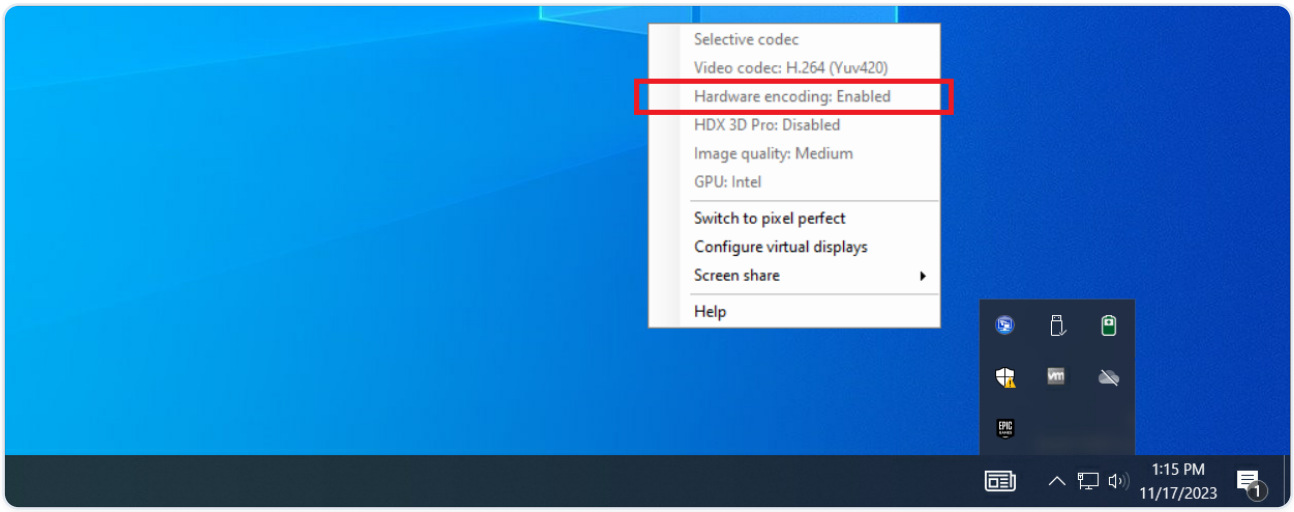
GPU Sharing を使用したスケーラビリティは、いくつかの要因によって異なります。

- 実行されているアプリケーション
- 消費するビデオ RAM の量
- グラフィックカードの処理能力

一部のアプリケーションは、他のアプリケーションよりもビデオ RAM の不足をうまく処理します。ハードウェアが過負荷になると、グラフィックカードドライバーの不安定化やクラッシュが発生する可能性があります。このような問題を回避するには、同時ユーザー数を制限してください。

- NVIDIA GPU および Intel Iris Pro グラフィックプロセッサ用の高性能ビデオエンコーダーへのアクセス。ポリシー設定（デフォルトで有効）がこの機能を制御し、H.264 エンコード（利用可能な場合）にハードウェアエンコードの使用を許可します。このようなハードウェアが利用できない場合、VDA はソフトウェアビデオコーデックを使用した CPU ベースのエンコードにフォールバックします。詳しくは、「グラフィックポリシー設定」を参照してください。

GPU アクセラレーションが機能していることを確認するには、グラフィックステータスインジケーターを使用できます。



DirectX、Direct3D、および WPF レンダリング

DirectX、Direct3D、および WPF レンダリングは、ディスプレイドライバーインターフェイス（DDI）バージョン 9ex、10、または 11 をサポートする GPU を搭載したサーバーでのみ利用できます。

- Windows Server 2016 以降では、RD セッションホストサーバー上の Remote Desktop Services (RDS) セッションは、Microsoft Basic Render Driver をデフォルトのアダプターとして使用します。Windows Server 2016 以降の RDS セッションで GPU を使用するには、グループポリシーの **ローカルコンピューターポリシー** \> **コンピューターの構成** \> **管理用テンプレート** \> **Windows コンポーネント** \> **Remote Desktop Services** \> **リモートデスクトップセッションホスト** \> **リモートセッション環境** で、**すべての Remote Desktop Services セッションにハードウェアの既定のグラフィックアダプターを使用する** 設定を有効にします。
- WPF アプリケーションがサーバーの GPU を使用してレンダリングできるようにするには、Windows マルチセッション OS セッションを実行しているサーバーのレジストリに設定を作成します。レジストリ設定の詳細については、レジストリで管理される機能のリストにある「Windows Presentation Foundation (WPF) レンダリング」を参照してください。

CUDAまたはOpenCLアプリケーションのGPUアクセラレーション

ユーザーセッションで実行されているCUDAおよびOpenCLアプリケーションのGPUアクセラレーションは、デフォルトで無効になっています。

CUDA アクセラレーション機能を使用するには、レジストリ設定を有効にします。詳細については、レジストリで管理される機能のリストにある「CUDA または OpenCL アプリケーションの GPU アクセラレーション」を参照してください。

WindowsシングルセッションOS向けGPUアクセラレーション

HDX 3D Proを使用すると、グラフィックを多用するアプリケーションを、ホストされたデスクトップまたはシングルセッションOSマシン上のアプリケーションとして配信できます。HDX 3D Proは、物理ホストコンピューター（デスクトップ、ブレード、ラックワークステーションを含む）と、XenServer®、vSphere、Nutanix、Hyper-V（パススルーのみ）ハイパーバイザーが提供するGPUパススルーおよびGPU仮想化テクノロジーをサポートします。

HDX™ 3D Pro は以下の機能を提供します:

- WANおよびワイヤレスパフォーマンスを最適化するための、適応型H.264ベースまたはH.265ベースのディープ圧縮。HDX 3D Proは、エンコードのデフォルト圧縮技術としてCPUベースの全画面H.264圧縮を使用します。H.264によるハードウェアエンコードは、NVENCをサポートするNVIDIA、Intel、およびAMDのカードで使用されます。H.265によるハードウェアエンコードは、NVENCをサポートするNVIDIAのカードで使用されます。
- 特殊なユースケース向けのロスレス圧縮オプション。HDX 3D Proは、医療画像処理など、ピクセルパーフェクトなグラフィックが必要なアプリケーションをサポートするために、CPUベースのロスレスコーデックも提供します。真のロスレス圧縮は、より多くのネットワークリソースと処理リソースを消費するため、特殊なユースケースでのみ推奨されます。

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

- 複数および高解像度モニターのサポート。シングルセッションOSマシンでは、最大8台の4Kモニターがサポートされます。ユーザーはモニターを任意の構成で配置でき、異なる解像度と向きのモニターを混在させることができます。モニターの数は、ホストコンピューターのGPU、ユーザーデバイス、および利用可能な帯域幅の機能によって制限されます。HDX 3D Proはすべてのモニター解像度をサポートし、ホストコンピューターのGPUの機能によってのみ制限されます。
- 動的解像度。仮想デスクトップまたはアプリケーションウィンドウを任意の解像度にリサイズできます。**注:** 解像度を変更する唯一のサポートされている方法は、VDAセッションウィンドウのサイズを変更することです。VDAセッション内から解像度を変更すること（**コントロール**

パネル > デザインと**個人設定 > ディスプレイ > 画面の解像度**を使用）はサポートされていません。

- NVIDIA vGPUアーキテクチャのサポート。HDX 3D ProはNVIDIA vGPUカードをサポートしています。詳細については、GPUパススルーおよびGPU共有に関するNVIDIA vGPUを参照してください。NVIDIA vGPUを使用すると、複数のVMが単一の物理GPUに同時に直接アクセスできるようになり、非仮想化オペレーティングシステムに展開されているものと同じNVIDIAグラフィックドライバーが使用されます。
- Virtual Direct Graphics Acceleration (vDGA) を使用したVMware vSphereおよびVMware ESXのサポート - HDX 3D ProをvDGAと組み合わせて、RDSおよびVDIワークロードの両方で使用できます。
- VMware vSphere/ESX のサポート。
- Windows Server 2016のDiscrete Device Assignmentを使用したMicrosoft HyperVのサポート。
- Intel Xeon Processor E3ファミリーおよびIntel Data Center GPU Flexシリーズによるデータセンターグラフィックスのサポート。詳細については、`<https://www.intel.com/content/www/us/en/products/details/discrete-gpus/data-center-gpu/flex-series.html>`を参照してください。
- AMD GPUのサポート。

> 注:
>
> AMD MxGPU（GPU仮想化）のサポートは、VMware vSphere vGPUでのみ機能します。Citrix HypervisorおよびHyper-Vは、GPUパススルーでサポートされています。詳細については、`<https://www.amd.com/en/graphics/workstation-virtual-graphics>`を参照してください。

- NVIDIA GPU、AMD GPU、およびIntel GPU用の高性能ビデオエンコーダーへのアクセス。ポリシー設定（デフォルトで有効）がこの機能を制御します。この機能により、H.264、H.265、またはAV1エンコーディング（利用可能な場合）のハードウェアエンコーディングを使用できます。そのようなハードウェアが利用できない場合、VDAはソフトウェアビデオコーデックを使用したCPUベースのエンコーディングにフォールバックします。詳細については、グラフィックポリシー設定を参照してください。

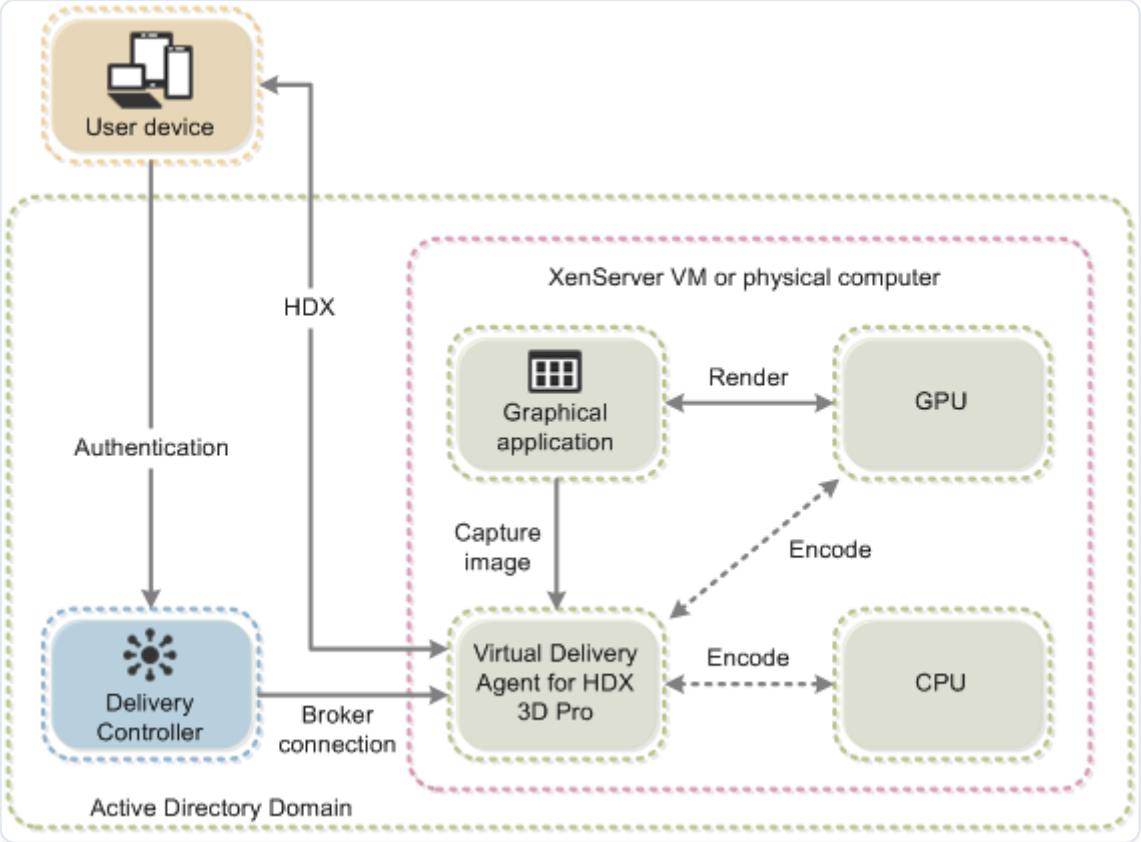
次の図に示すように：

- ユーザーがCitrix Workspace™アプリにログインし、仮想アプリケーションまたはデスクトップにアクセスすると、Controllerがユーザーを認証します。その後、ControllerはHDX 3D Pro用

のVDAに接続し、グラフィックアプリケーションをホストするコンピューターへの接続を仲介します。

HDX 3D Pro用VDAは、ホスト上の適切なハードウェアを使用して、デスクトップ全体またはグラフィックアプリケーションのみのビューを圧縮します。

- デスクトップまたはアプリケーションのビューと、それらに対するユーザーの操作は、ホストコンピューターとユーザーデバイス間で送信されます。この送信は、Citrix WorkspaceアプリとHDX 3D Pro用VDA間の直接HDX接続を介して行われます。



HDX 3D Proのユーザーエクスペリエンスを最適化する

複数のユーザーが帯域幅が制限された接続（たとえば、支店など）を共有している場合、各ユーザーが利用できる帯域幅を制限するために、**セッション全体の帯域幅制限**ポリシー設定を使用することをお勧めします。この設定を使用すると、ユーザーがログオンおよびログオフしても、利用可能な帯域幅が大きく変動しないようにできます。HDX 3D Proは利用可能なすべての帯域幅を使用するように自動的に調整するため、ユーザーセッション中に利用可能な帯域幅が大きく変動すると、パフォーマンスに悪影響を及ぼす可能性があります。

たとえば、20人のユーザーが60 Mbpsの接続を共有している場合、各ユーザーが利用できる帯域幅は、同時ユーザー数に応じて3 Mbpsから60 Mbpsの間で変動する可能性があります。このシナ

リオでユーザーエクスペリエンスを最適化するには、ピーク時のユーザーあたりの必要な帯域幅を決定し、常にこの量にユーザーを制限します。

3Dマウスのユーザーの場合、汎用USBリダイレクト仮想チャネルの優先度を0に上げることをお勧めします。仮想チャネルの優先度を変更する方法については、Knowledge Centerの記事CTX128190を参照してください。

ロスレス圧縮

ロスレス圧縮を使用する場合：

- 通知領域アイコンであるロスレスインジケーターは、表示されている画面がロッシーフレームかロスレスフレームかをユーザーに通知します。このアイコンは、**Visual Quality**ポリシー設定で**Build to lossless**が指定されている場合に役立ちます。送信されるフレームがロスレスの場合、ロスレスインジケーターは緑色に変わります。
- ロスレススイッチを使用すると、ユーザーはセッション内でいつでも**常にロスレス**モードに変更できます。セッション内でいつでもロスレスを選択または選択解除するには、アイコンを右クリックして**ピクセルパーフェクトに切り替え**をクリックするか、ショートカット**ALT+SHIFT+1**を使用します。
- ロスレス圧縮の場合：HDX 3D Proは、ポリシーで選択されたコーデックに関係なく、ロスレスコーデックを圧縮に使用します。
- ロッシー圧縮の場合：HDX 3D Proは、デフォルトまたはポリシーで選択された元のコーデックを使用します。
- ロスレススイッチの設定は、以降のセッションでは保持されません。すべての接続でロスレスコーデックを使用するには、**Visual quality**ポリシー設定で**Always lossless**を選択します。

ロスレスホットキー

セッション内でいつでもホットキーを使用して**ロスレス**を選択またはクリアできます。デフォルトのショートカット**ALT+SHIFT+1**を使用します。

Windowsレジストリでデフォルトのショートカット**ALT+SHIFT+1**を上書きできます。 新しいレジストリ設定を構成するには、次のレジストリ値を設定します:

- **キー**: `HKEY_CURRENT_USER\SOFTWARE\Citrix\Graphics`
- **名前**: `HKLM_HotKey`
- **種類**: `String`

ショートカットの組み合わせを設定する形式は`C=0|1, A=0|1, S=0|1, W=0|1, K=val`です。キーはカンマ「,」で区切り、スペースは入れないでください。キーの順序は関係ありません。

A、C、S、W、Kはキーであり、C=Control、A=ALT、S=SHIFT、W=Win、K=有効なキー（Kに許可される値は0～9、a～z、および任意の仮想キーコード）です。

例:

- **F10**の場合、K=0x79を設定します。
- **Ctrl + F10**の場合、C=1、K=0x79を設定します。
- **Alt + A**の場合、A=1,K=a または A=1,K=A または K=A,A=1 を設定します。
- **Ctrl + Alt + 5**の場合、C=1, A=1,K=5 または A=1,K=5,C=1 を設定します。
- **Ctrl + Shift + F5**の場合、A=1,S=1,K=0x74 を設定します。

次の表は、仮想キーコードの例を示しています。

キー	値
F1	0x70
F2	0x71
F3	0x72
F4	0x73
F5	0x74
F6	0x75
F7	0x76
F8	0x77
F9	0x78
F10	0x79
F11	0x7A
F12	0x7B
ページアップキー	0x21
ページダウンキー	0x22

キー	値
End キー	0x23
Home キー	0x24
左矢印キー	0x25
上矢印キー	0x26
右矢印キー	0x27
下矢印キー	0x28

ショートカットの組み合わせの間にスペースがないことを確認してください。例：

正しい： C=1,K=0x74 誤り： C=1, K=0x74

HDXレジストリエディター(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/hdx-registry-editor.png)

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

シンワイヤー

はじめに

Citrix HDXテクノロジーの一部であるThinwireは、Citrix Virtual Apps and Desktopsで使用されるCitrixのデフォルトのディスプレイリモートテクノロジーです。

ディスプレイリモートテクノロジーにより、あるマシンで生成されたグラフィックを、通常はネットワーク経由で別のマシンに送信して表示できます。

成功したディスプレイリモートソリューションは、ローカルPCと同様の高度にインタラクティブなユーザーエクスペリエンスを提供します。Thinwireは、複雑で効率的な画像分析および圧縮技術を幅広く使用することで、このエクスペリエンスを実現します。Thinwireは、サーバーのスケーラビリティを最大化し、他のディスプレイリモートテクノロジーよりも少ない帯域幅を消費します。

このバランスにより、Thinwireはほとんどの一般的なビジネスユースケースに対応し、Citrix Virtual Apps and Desktopsのデフォルトのディスプレイリモートテクノロジーとして使用されています。

HDX™ 3D プロ

デフォルト構成では、Thinwireは3Dまたは高度にインタラクティブなグラフィックを提供し、GPU（グラフィック処理ユニット）が存在する場合はそれを使用できます。ただし、GPUが存在するシナリオでは、**3Dグラフィックワークロード向けに最適化**または**視覚品質 > ロスレスビルド**ポリシーを使用してHDX 3D Proモードを有効にすることをお勧めします。これらのポリシーは、GPUが存在する場合にハードウェアアクセラレーションを使用して画面全体をエンコードするために、Thinwireがビデオコーデック（H.264、H.265、またはAV1）を使用するように構成します。これにより、3Dプロフェッショナルグラフィックのよりスムーズなエクスペリエンスが提供されます。詳細については、H.264 ロスレスビルド、HDX 3D Pro、およびWindowsシングルセッションOSのGPUアクセラレーションを参照してください。

要件

Thinwireは、Windows Server 2022、Windows Server 2019、Windows Server 2016、Windows Server 2012 R2、Windows 10、Windows 7などの最新のオペレーティングシステム向けに最適化されています。Windows Server 2008 R2では、レガシーグラフィックモードが推奨されます。これらのユースケースにCitrixが推奨するポリシー設定の組み合わせを提供するには、組み込みのCitrixポリシーテンプレート、高サーバー拡張性 - レガシーOS、およびWAN向け最適化 - レガシーOSを使用してください。

- Thinwireの動作を制御するポリシー設定である**ビデオコーデックを圧縮に使用**は、Citrix Virtual Apps and Desktops 7 1808以降およびXenApp and XenDesktop 7.6 FP3以降のVDAバージョンで利用できます。**ビデオコーデックを優先時に使用**オプションは、Citrix Virtual Apps and Desktops 7 1808以降およびXenApp and XenDesktop 7.9以降のVDAバージョンでのデフォルト設定です。
- すべてのCitrix Workspace™アプリはThinwireをサポートしています。一部のCitrix Workspaceアプリは、他のアプリがサポートしないThinwireの機能（例えば、帯域幅使用量を削減するための8ビットまたは16ビットグラフィック）をサポートする場合があります。このような機能のサポートは、Citrix Workspaceアプリによって自動的にネゴシエートされます。

- Thinwireは、マルチモニターおよび高解像度のシナリオで、より多くのサーバーリソース（CPU、メモリ）を使用します。Thinwireが使用するリソースの量を調整することは可能ですが、その結果、帯域幅の使用量が増加する可能性があります。
- 低帯域幅または高遅延のシナリオでは、インタラクティブ性を向上させるために8ビットまたは16ビットグラフィックを有効にすることを検討してください。特に8ビットの色深度では、視覚品質が影響を受ける可能性があります。

エンコード方法

Thinwireは、ポリシーとクライアントの機能に応じて、2つの異なるエンコードモードで動作できます。

- アダプティブJPEGを使用したThinwire **ビデオコーデックを圧縮に使用**ポリシー設定：**ビデオコーデックを使用しない**
- 選択的H.264、H.265、またはAV1を使用したThinwire **ビデオコーデックを圧縮に使用**ポリシー設定：**ビデオコーデックを優先時に使用**または**アクティブに変更される領域の場合**
- フルスクリーンH.264、H.265、またはAV1を使用したThinwire **ビデオコーデックを圧縮に使用**ポリシー設定：**画面全体の場合**

H.265

H.265としても知られる高効率ビデオコーディング (HEVC) は、H.264の後継です。 H.265ビデオコーデックを使用したハードウェアエンコードは、以下のGPUでサポートされています:

- NVIDIA MaxwellベースのGPUおよびそれ以降
- Intel 第6世代GPUおよびそれ以降
- AMD RavenベースのGPUおよびそれ以降

AV1

CitrixはAV1ビデオコーデックのサポートを追加しました。AV1の利点は、H.264およびH.265と比較して、優れた画像圧縮、より良い画質、および低い帯域幅使用量を持つことです。

AV1の以下の要件を満たす必要があります:

- NVIDIA GPUの場合はVDA 2305以降、または
- Intel GPUの場合はVDA 2308以降

以下のGPUはエンコードに対応しています:

- NVIDIA Ada LovelaceベースのGPU

- Intel ARCまたはIntel Data Center GPU Flexシリーズ GPU

NVIDIAのAda Lovelace GPUの詳細については、ADAアーキテクチャを参照してください。

IntelのARCワークステーションおよびデータセンターFlexシリーズGPUの詳細については、Flexシリーズおよび概要を参照してください。

自動ビデオコーデック選択

圧縮ポリシーの**ビデオコーデックを使用**が有効になっているか、VDAで3Dグラフィックワークロードの最適化が有効になっている場合、最適なビデオコーデックを自動的に検出できます。Citrix Workspaceアプリ for Windowsのインストール中に、エンドポイントのデコード機能が評価されます。この情報に基づいて、Citrix Workspaceアプリ for Windowsは接続時にVDAと使用する最適なコーデックをネゴシエートします。以下のリストは、ビデオコーデックが評価される順序を示しています。

- AV1
- H.265
- H.264

自動選択は、これらのコーデックの4:2:0バリアントにのみ適用されます。**視覚品質**設定が「Build-to-Lossless」または「Always Lossless」に設定されており、かつ「Allow Visually Lossless」が「有効」に設定されている場合、ビデオコーデックの自動選択は無効になります。

リソースに接続する際、Citrix WorkspaceアプリはエンドポイントのH.265およびAV1のデコード機能をテストし、その機能をレジストリに保存します。その後、Citrix Workspaceアプリは使用する最適なビデオコーデックを自動的に選択し、VDAとネゴシエートします。VDAとクライアントの両方がH.265とAV1を使用できる場合、AV1がビデオコーデックとして選択されます。VDAまたはクライアントのいずれかでAV1が利用できない場合、H.265がネゴシエートされます。H.265もどちらかで利用できない場合、セッションはH.264をビデオコーデックとして使用します。

> **注：**
>
> この機能はデフォルトで有効になっています。この動作は、新しいクライアント側のレジストリ設定`DisableDecoderCaps`を設定することで変更できます。
>
> ビデオコーデックの自動選択を無効にするには、「DisableDecoderCaps」を`HKLM\Software\WOW6432Node\Policies\Citrix\ICA Client\Graphics Engine DWORD`

> `DisableDecoderCaps = 1`または`HKCU\Software\Policies\Citrix\ICA Client\Graphics Engine DWORD DisableDecoderCaps = 1`として設定します。

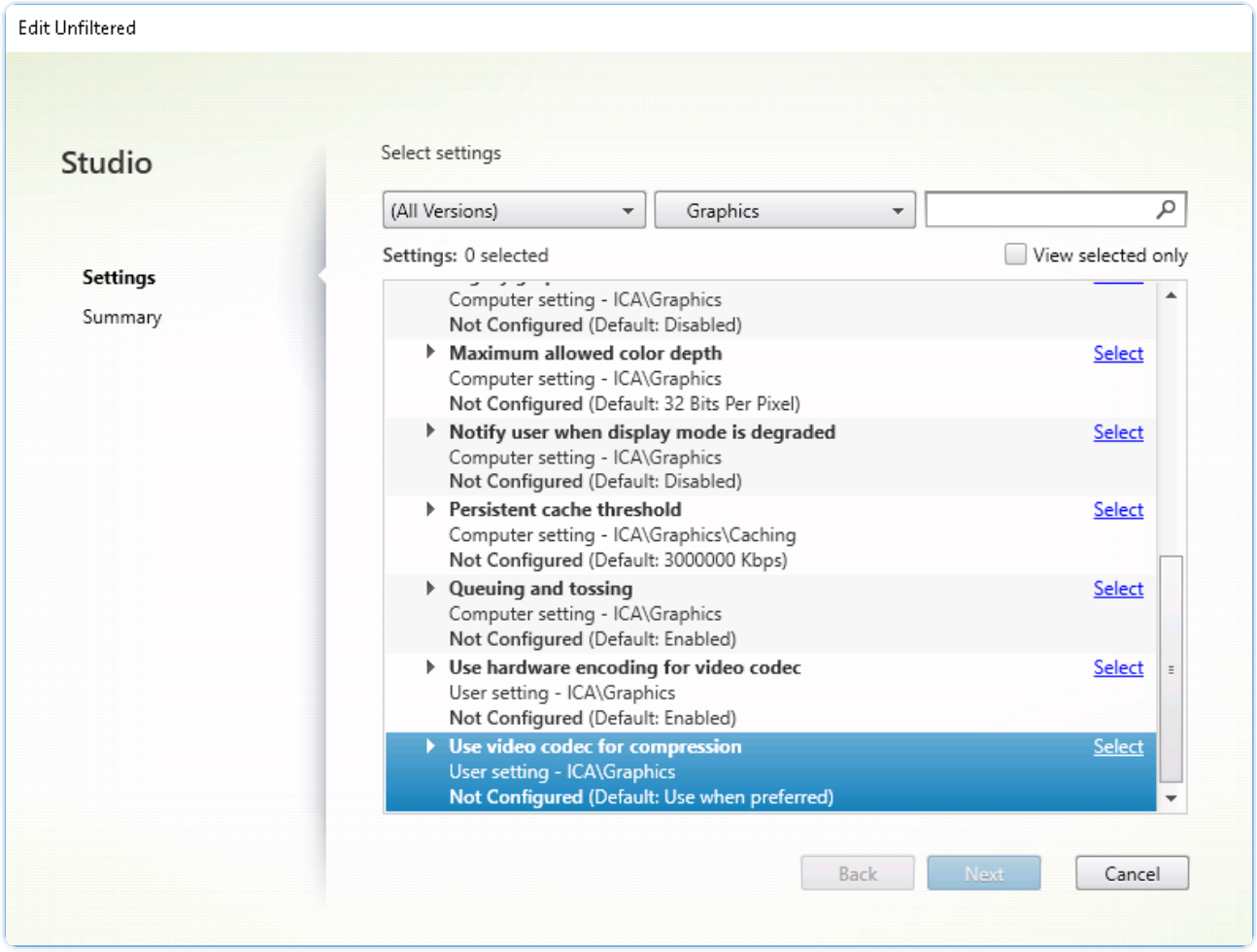
これらの値のいずれかが1に設定されている場合、ビデオコーデックの自動選択は使用されません。 グラフィックステータスインジケーターとHDXモニターでビデオコーデックを監視できます。

構成

Thinwireは、デフォルトのディスプレイリモートテクノロジーです。

以下のグラフィックポリシー設定は、デフォルトを設定し、さまざまなユースケースの代替手段を提供します。

- 圧縮にビデオコーデックを使用
  - **優先時にビデオコーデックを使用**。これがデフォルト設定です。追加の構成は不要です。この設定をデフォルトのままにすることで、すべてのCitrix接続でThinwireが選択され、スケーラビリティ、帯域幅、および一般的なデスクトップワークロードにおける優れた画質のために最適化されます。これは、**アクティブに変化する領域の場合**と機能的に同等です。
- このポリシー設定の他のオプションは、さまざまなユースケースのために他のテクノロジーとThinwireを引き続き使用します。例：
  - **アクティブに変化する領域の場合**。Thinwireのアダプティブディスプレイテクノロジーは、動いている画像（ビデオ、移動中の3D）を識別し、画像が動いている画面の一部でのみH.264、H.265、またはAV1を使用します。
  - **画面全体の場合**。3Dグラフィックを多用するケースで、ユーザーエクスペリエンスと帯域幅を向上させるために、H.264、H.265、またはAV1によるフルスクリーンでThinwireを提供します。H.264 4:2:0の場合（**視覚的にロスレス**ポリシーが無効になっている場合）、最終画像はピクセルパーフェクト（ロスレス）ではなく、特定のシナリオには適さない可能性があります。そのような場合は、代わりにH.264 Build to losslessまたはH.265 Build to losslessの使用を検討してください。



その他のさまざまなポリシー設定（以下の視覚表示ポリシー設定を含む）を使用して、ディスプレイリモート処理テクノロジーのパフォーマンスを微調整できます。Thinwireはこれらすべてをサポートします。

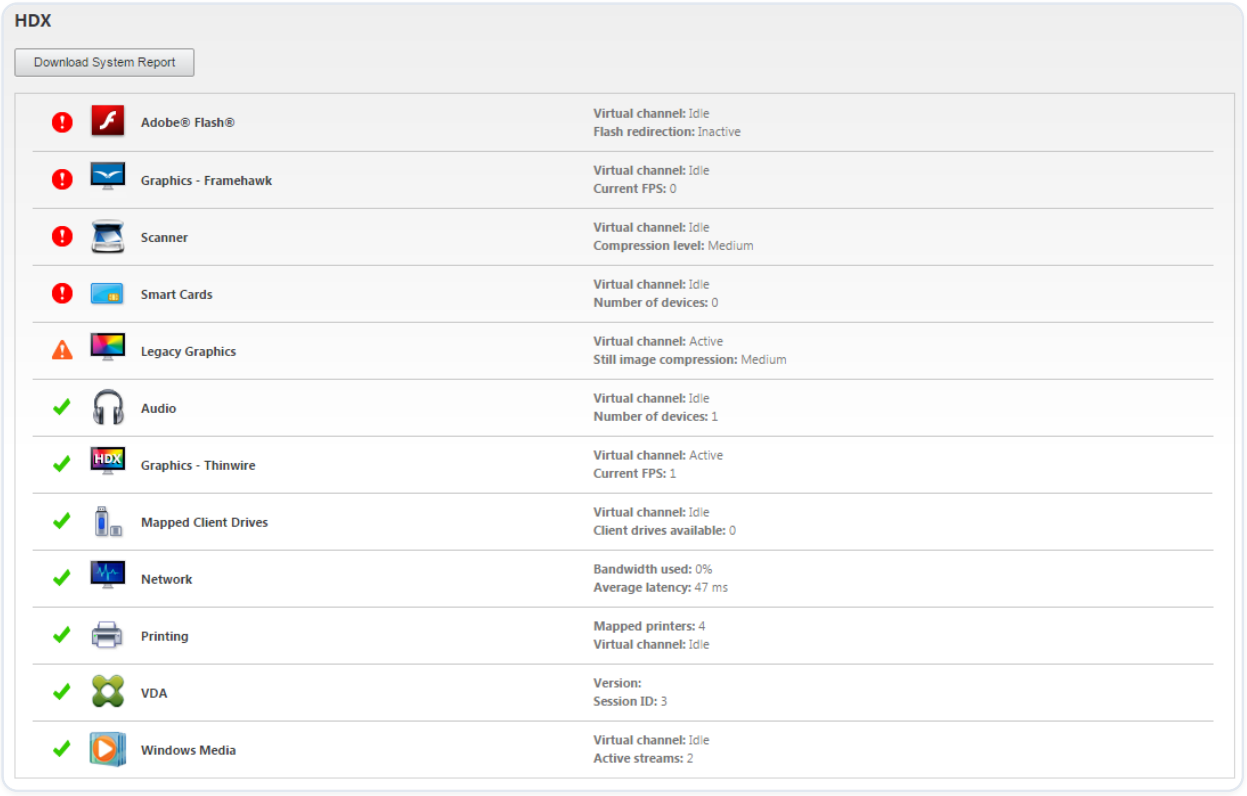
- 単純なグラフィックの優先色深度
- ターゲットフレームレート
- 視覚品質

さまざまなビジネスユースケースに対応するCitrix推奨のポリシー設定の組み合わせを取得するには、組み込みのCitrixポリシーテンプレートを使用します。**高サーバー拡張性**および**超高精細ユーザーエクスペリエンス**テンプレートは、組織の優先順位とユーザーの期待に合わせて最適なポリシー設定の組み合わせでThinwireを使用します。

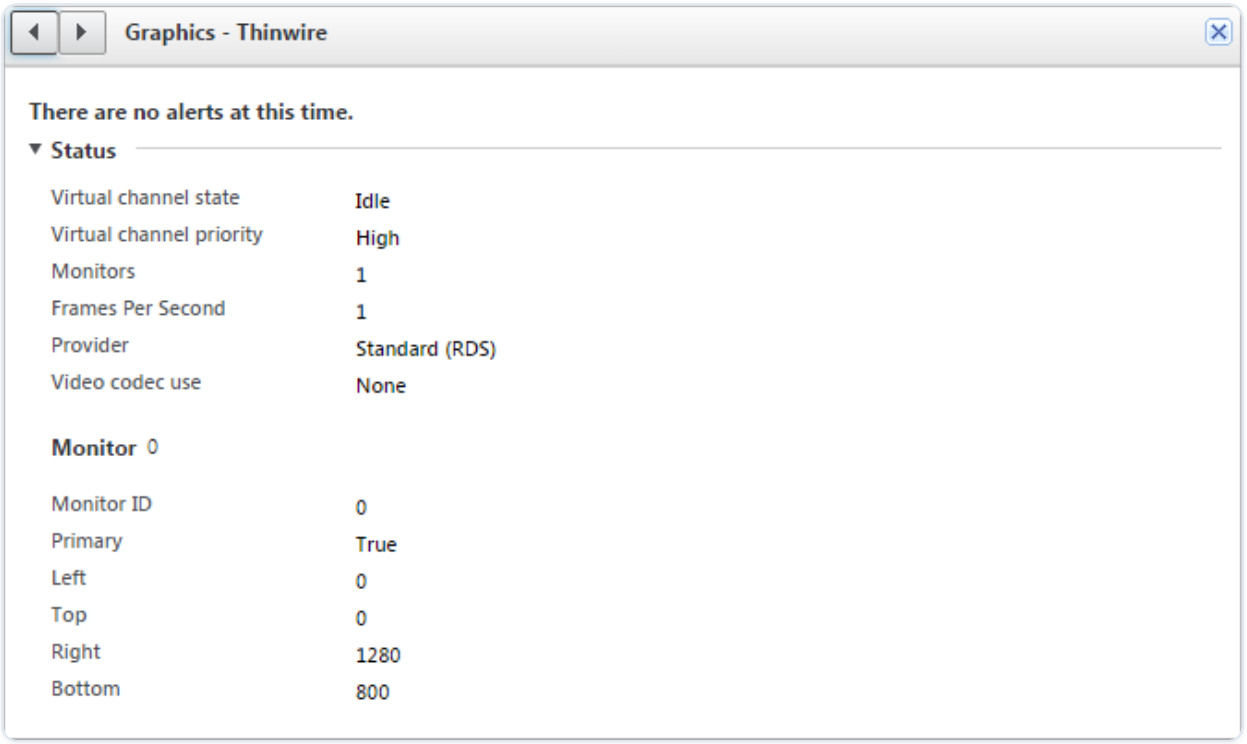
Thinwireの監視

Citrix DirectorからThinwireの使用状況とパフォーマンスを監視できます。HDX仮想チャネルの詳細ビューには、任意のセッションでThinwireのトラブルシューティングと監視に役立つ情報が含まれています。Thinwire関連のメトリックを表示するには：

1. Directorで、ユーザー、マシン、またはエンドポイントを検索し、アクティブなセッションを開いて**詳細**をクリックします。または、**フィルター** > **セッション** > **すべてのセッション**を選択し、アクティブなセッションを開いて**詳細**をクリックすることもできます。
2. **HDX**パネルまでスクロールダウンします。



3. **グラフィック - Thinwire**を選択します。



ロスレス圧縮コーデック (MDRLE)

一般的なデスクトップセッションでは、ほとんどの画像は単純なグラフィックまたはテキスト領域です。Thinwireはこれらの領域がどこにあるかを判断し、2DRLEコーデックを使用してロスレスエンコードのためにこれらの領域を選択します。Citrix Workspaceアプリのクライアント側では、これらの要素はセッション表示のためにCitrix Workspaceアプリ側の2DRLEデコーダーを使用してデコードされます。

XenAppおよびXenDesktop 7.17では、2DRLEコーデックよりも一般的なデスクトップセッションで消費帯域幅が少ない、より高い圧縮率のMDRLEコーデックを追加しました。この新しいコーデックはサーバーのスケーラビリティに影響を与えません。

帯域幅が低いと、通常、セッションの対話性が向上し（特に共有リンクや制約のあるリンクの場合）、コストが削減されます。

MDRLEコーデックの構成は不要です。Citrix WorkspaceアプリがMDRLEデコードをサポートしている場合、VDAはVDA MDRLEエンコードとCitrix WorkspaceアプリMDRLEデコードを使用します。Citrix WorkspaceアプリがMDRLEデコードをサポートしていない場合、VDAは自動的に2DRLEエンコードにフォールバックします。

MDRLEの要件:

- Citrix Virtual Apps and Desktopsの最小バージョン7 1808 VDA
- XenAppおよびXenDesktopの最小バージョン7.17 VDA
- Windows向けCitrix Workspaceアプリの最小バージョン1808
- Windows向けCitrix Receiverの最小バージョン4.11

プログレッシブモード

Citrix Virtual Apps and Desktops 1808では、プログレッシブモードが導入され、デフォルトで有効になりました。ネットワーク条件が制約されている場合（デフォルト：帯域幅 < 2 Mbps、または遅延 > 200 ms）、Thinwireはテキストと静止画像の圧縮を強化し、画面アクティビティ中の対話性を向上させました。高圧縮されたテキストと画像は、画面アクティビティが停止すると、ランダムなブロック方式で段階的にシャープ化されます。このように圧縮とシャープ化を行うことで、全体的な対話性は向上しますが、キャッシュ効率が低下し、帯域幅の使用量が増加します。

Citrix Virtual Apps and Desktops 1906以降、プログレッシブモードはデフォルトで無効になっています。現在、異なるアプローチを使用しています。静止画の品質はネットワーク条件に基づいており、各**視覚品質**設定の事前定義された最小値と最大値の間で変動します。明示的なシャープ化ステップがないため、Thinwireは画像配信を最適化し、キャッシュ効率を維持しながら、プログレッシブモードのほぼすべての利点を提供します。

プログレッシブモードの動作の変更

レジストリキーを使用してプログレッシブモードの状態を変更できます。詳しくは、レジストリで管理される機能の一覧にあるプログレッシブモードを参照してください。

ロスレスビルド

ロスレスビルドは、対話性と最終的な画質のためにグラフィック配信を最適化する特別なThinwire構成です。この設定は、**視覚品質**ポリシーを**ロスレスビルド**に設定することで有効にできます。

Build to losslessは、画面アクティビティ中にH.264、H.265、またはAV1を使用して画面を圧縮し、アクティビティが停止するとピクセルパーフェクト（ロスレス）にシャープ化します。非可逆の画質は、利用可能なリソースに合わせて調整され、可能な限り最高のフレームレートを維持します。シャープ化のステップは段階的に実行されます。たとえば、モデルを選択して回転させる場合などです。

Build to lossless は、ハードウェアアクセラレーションを含む画面全体にビデオコーデックを使用するすべての利点を提供しますが、最終的にロスレスが保証された画面という追加の利点があります。これは、最終的なピクセルパーフェクトな画像を必要とする3Dタイプのワークロードにとって重要です。たとえば、医療画像の操作などです。また、H.264 **Build to lossless** は、フルスクリーンH.264 4:4:4よりも少ないリソースを使用します。その結果、**Build to lossless** を使用すると、通常、Visually lossless H.264 4:4:4よりも高いフレームレートが得られます。

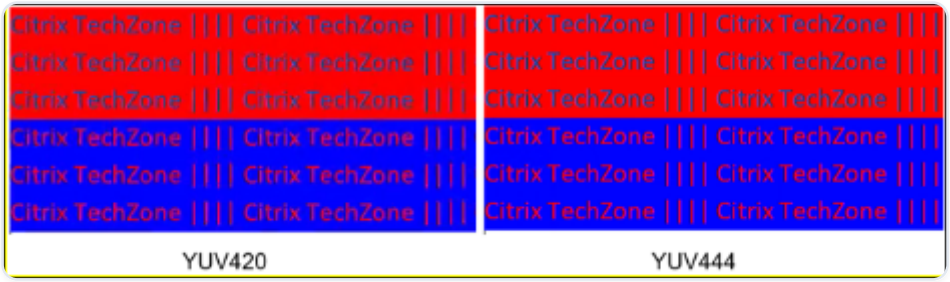
> **注：**
>
> ビルドトゥロスレスを使用している場合、ビデオコーデックの使用を無効にできます。**Use video codec** ポリシーを `Do not use video codec` に設定するだけです。これにより、動画は代わりにAdaptive JPEGでエンコードされます。

視覚的にロスレスなエンコード

視覚的にロスレスなエンコードは、ビデオコーデック圧縮にクロマサブサンプリングされたYUV 4:2:0カラースペースではなく、YUV 4:4:4カラースペースを使用します。これにより、カラースペース変換中に色情報が失われることがなく、デコード後には元のRGB画像と視覚的に区別できなくなります。

次の例を考えてみましょう。ビデオコーデックを使用して画面全体を圧縮する場合、4:2:0の色圧縮は、テキストのような高コントラストの詳細を劣化させ、ぼやけて読みにくくする可能性があ

ります。対照的に、4:4:4はほぼすべての色情報を保持し、視覚的に認識できる劣化を示しません。



ピクセルパーフェクトな品質や正確な色表示を必要とするワークロードは、視覚的にロスレスなエンコードの恩恵を受けることができます。

視覚的にロスレスなエンコードは、H.264とH.265の両方で利用できます。H.264 4:4:4エンコードは純粋にソフトウェアベースのソリューションであるため、VDAとクライアントの両方でCPU使用率に大きな影響を与える可能性があります。これにより、フレームレートにも影響が出る場合があります。

Citrix Workspaceアプリ2305のリリースによりH.265 4:4:4のサポートが追加され、ThinwireがVDAとクライアントの両方のGPUをH.265 4:4:4エンコードに使用できるようになり、パフォーマンスが大幅に向上しました。

視覚的にロスレスな4:4:4エンコードを許可するには、2つのポリシーを有効にする必要があります。

- **視覚品質**: `Build to Lossless` または `Always Lossless` に設定します
- **視覚的にロスレスを許可**: `Enabled` に設定します

> **注：**
>
> **視覚的にロスレスを許可** が有効になっていない場合、Thinwireエンコーダーは `Build to lossless` または `Always Lossless` のいずれかに切り替わります。

> H.265 4:4:4視覚的にロスレスには、追加の要件があります。

- NVIDIA GPUにはVDAバージョン2209以降が必要です
- Intel GPUにはVDAバージョン2308以降が必要です

H.265 4:4:4でサポートされているGPUは次のとおりです。

- NVIDIA Pascal世代以降のGPU

- Intel第10世代以降のGPU

クライアントには、Citrix Workspaceアプリ for Windowsバージョン2305が必要です（バージョン2309.1を推奨）。

H.265 4:4:4のハードウェアデコードは、以下のクライアントデバイスGPUで可能です。

- NVIDIA Turing世代以降のGPU
- Intel第10世代以降のGPU

テキストベースのセッションウォーターマーク

テキストベースのセッションウォーターマークは、データ盗難を抑止し、追跡を可能にするのに役立ちます。この追跡可能な情報は、写真やスクリーンキャプチャを使用してデータを盗む者への抑止力として、セッションデスクトップに表示されます。元のドキュメントの内容を変更することなく、セッション画面全体に表示されるテキストのレイヤーであるウォーターマークを指定できます。テキストベースのセッションウォーターマークにはVDAサポートが必要です。

> **重要:**

> テキストベースのセッションウォーターマークは、セキュリティ機能ではありません。このソリューションはデータ盗難を完全に防ぐものではありませんが、ある程度の抑止力と追跡可能性を提供します。この機能を使用した場合の完全な情報追跡可能性は保証しませんが、必要に応じて他のセキュリティソリューションと組み合わせて使用することをお勧めします。

> セッションウォーターマークはテキストであり、ユーザーに配信されるセッションに適用されます。セッションウォーターマークには、データ盗難を追跡するための情報が含まれています。最も重要なデータは、スクリーンイメージが取得された現在のセッションのログオンユーザーのIDです。データ漏洩をより効果的に追跡するために、サーバーまたはクライアントのインターネットプロトコルアドレスや接続時間などの他の情報を含めます。

ユーザーエクスペリエンスを調整するには、セッションウォーターマークポリシー設定 を使用して、画面上の配置とウォーターマークの外観を構成します。

要件:

仮想配信エージェント:

マルチセッションOS 7.17 シングルセッションOS 7.17

制限事項:

- セッションウォーターマークは、ローカルアプリアクセス、Windowsメディアリダイレクト、MediaStream、ブラウザコンテンツリダイレクト、およびHTML5ビデオリダイレクトが使用されているセッションではサポートされていません。セッションウォーターマークを使用するには、これらの機能が無効になっていることを確認してください。
- セッションが全画面ハードウェアアクセラレーションモード（全画面H.264またはH.265エンコーディング）で実行されている場合、セッションウォーターマークはサポートされず、表示されません。
- これらのHDX™ポリシーを設定すると、ウォーターマーク設定は有効にならず、セッション表示にウォーターマークは表示されません。

ビデオコーデックにハードウェアエンコーディングを使用 を **有効 圧縮にビデオコーデックを使用** を **画面全体**

- これらのHDXポリシーを設定すると、動作は未定義となり、ウォーターマークが表示されない場合があります。

  ビデオコーデックにハードウェアエンコーディングを使用 を **有効 圧縮にビデオコーデックを使用** を **優先する場合にビデオコーデックを使用**

  ウォーターマークが表示されるようにするには、**ビデオコーデックにハードウェアエンコーディングを使用** を **無効** に設定するか、**圧縮にビデオコーデックを使用** を **アクティブに変更される領域** または **ビデオコーデックを使用しない** に設定します。
- セッションウォーターマークは、Thinwireグラフィックモードのみをサポートします。
- セッションレコーディングを使用している場合、記録されたセッションにはウォーターマークは含まれません。
- Windowsリモートアシスタンスを使用している場合、ウォーターマークは表示されません。
- ユーザーが画面をキャプチャするために **Print Screen** キーを押した場合、VDA側でキャプチャされた画面にはウォーターマークは含まれません。キャプチャされた画像がコピーされるのを防ぐための対策を講じることをお勧めします。

画面共有

画面共有により、ユーザーは画面の内容、キーボード、マウスの制御を含め、Citrix Virtual Desktopセッションを他のユーザーと共有できます。

システム要件

- Windows: シングルセッションまたはマルチセッションOS VDA
- Linux: Linuxセッションの共有に関する詳細については、Linux VDAドキュメントを参照してください。
- デスクトップセッションのみ共有できます。
- セッションをホストしているVDAと、共有セッションに接続するマシンの間にネットワーク接続が必要です。ネットワークポートの要件は、使用中のICAポート（TCP/UDP 1494または2598）と、画面共有ポリシーの構成（デフォルトではTCP 52525～52625）に基づいています。

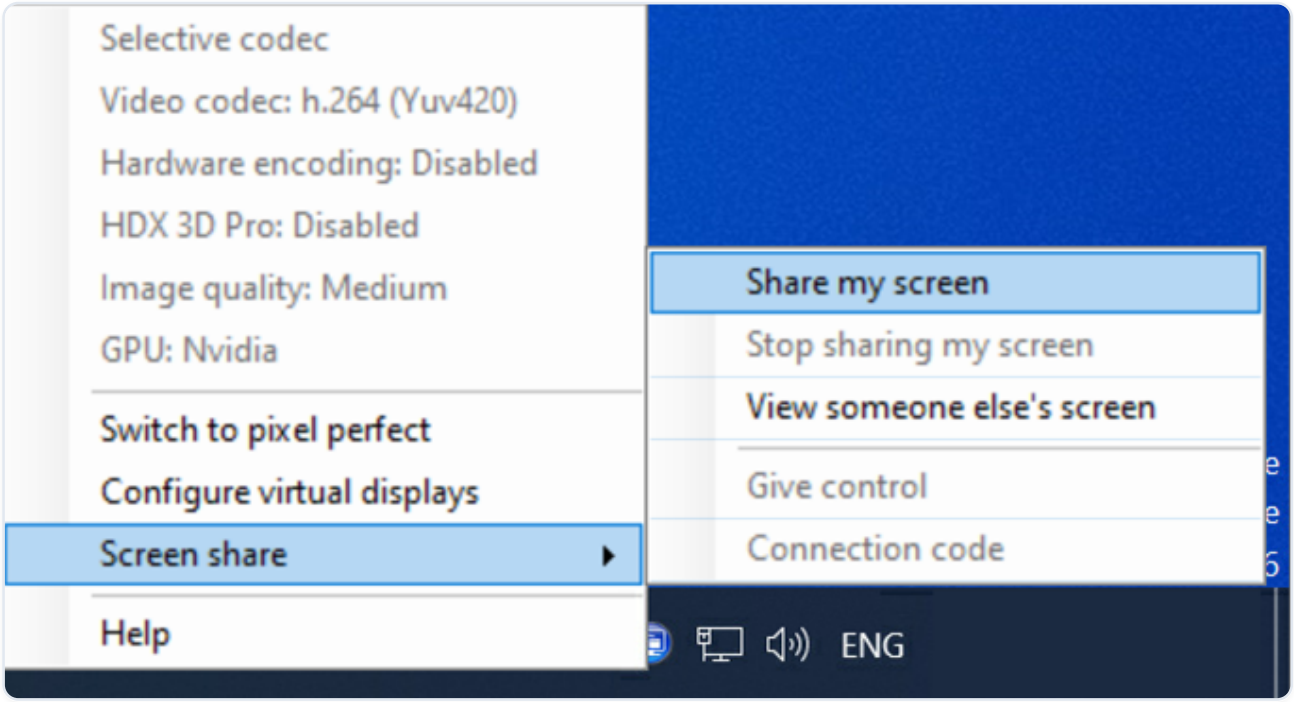
構成

画面共有はCitrixポリシーを使用して有効にする必要があります。画面共有はデフォルトで無効になっています。機能を有効または無効にし、使用可能なネットワークポート範囲を割り当てるには、画面共有ポリシーを構成します。

セッションの共有と接続のためのコントロールを含むユーザーインターフェイスを表示するには、グラフィックステータスインジケーターポリシーを有効にします。

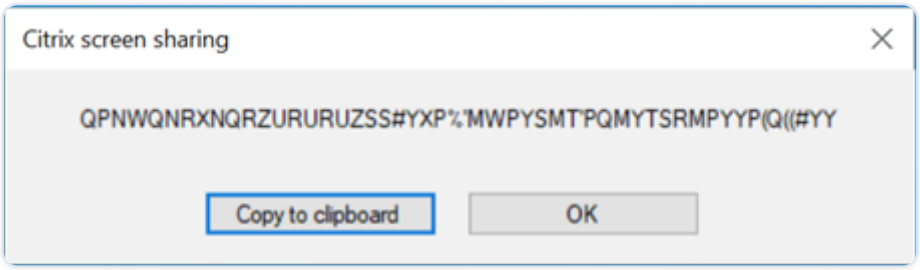
セッションの共有

セッションを共有するには、Windowsの通知領域にあるHDX™グラフィックステータスインジケーターアイコンを探します。それを右クリックしてメニューを表示し、**画面共有 > 自分の画面を共有**を選択します。



クリップボードにコピーをクリックするか、ダイアログボックスに表示されている文字列全体を手動で選択してコピーします。その文字列は、電子メールやIMクライアントなど、選択したアプリケーションに貼り付けて、他のユーザーに配布できます。

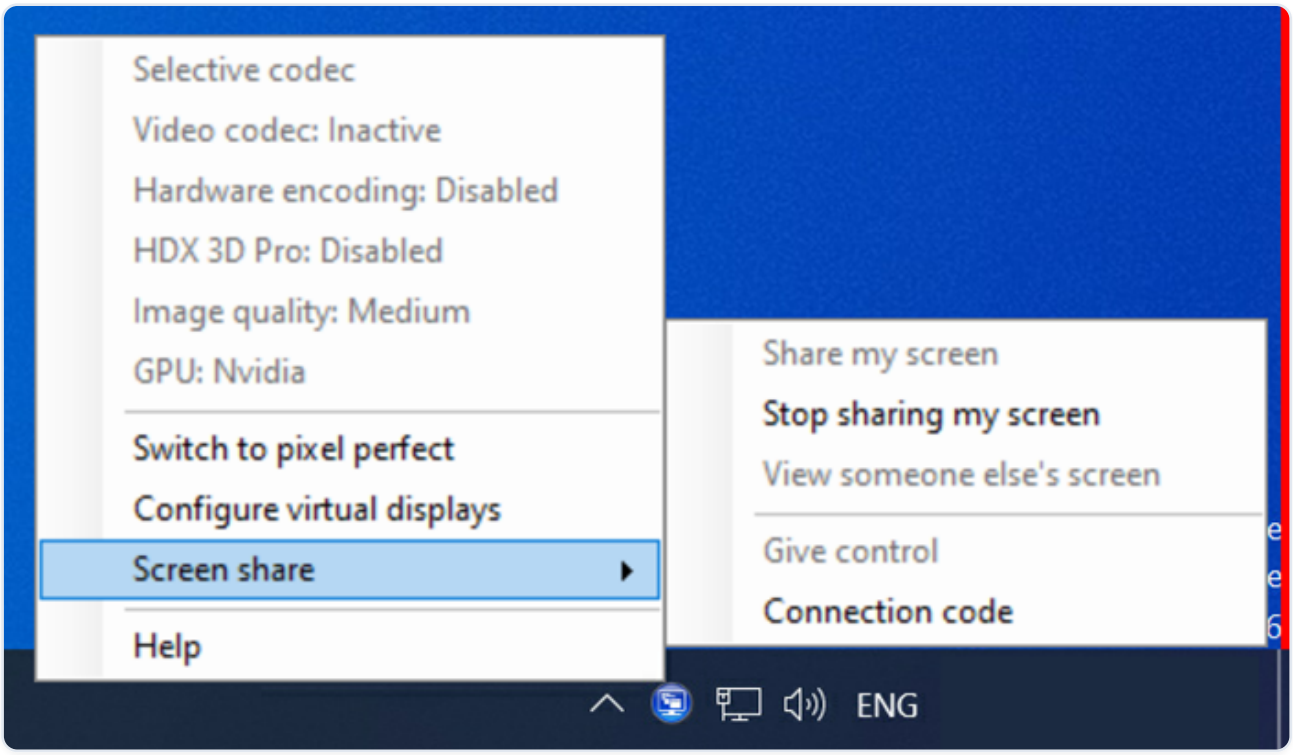
ダイアログボックスを閉じるには、**OK**または**x**をクリックします。セッションが共有されている間はいつでも、**画面共有 > 接続コード**メニューオプションから接続コードを取得できます。



画面の周囲に赤い枠線が表示されます。これは、セッションが現在共有されており、他のユーザーから見えることを示すインジケーターです。

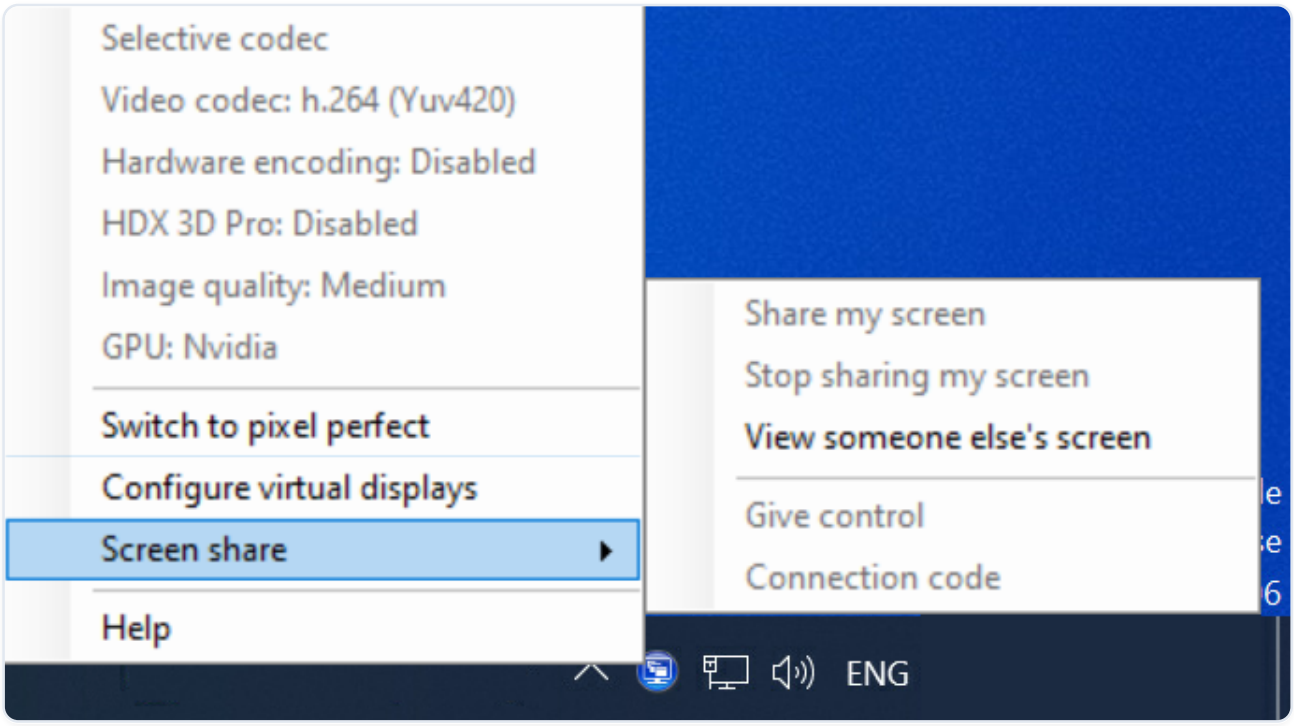
キーボードとマウスの制御も、**画面共有 > 制御を付与**メニューオプションを使用して他のユーザーと共有できます。

セッションの共有を停止し、すべてのユーザーを切断するには、**画面共有 > 自分の画面の共有を停止**メニューオプションを使用します。

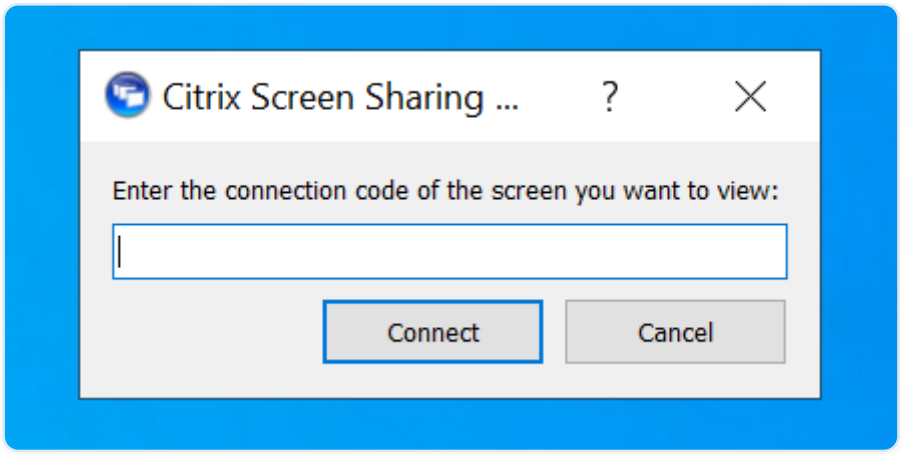


共有セッションへの接続

他のユーザーのセッションに接続するには、Windows の通知領域にある HDX グラフィックステータスインジケーターアイコンを探します。それを右クリックしてメニューを表示し、**画面共有 > 他のユーザーの画面を表示**を選択します。

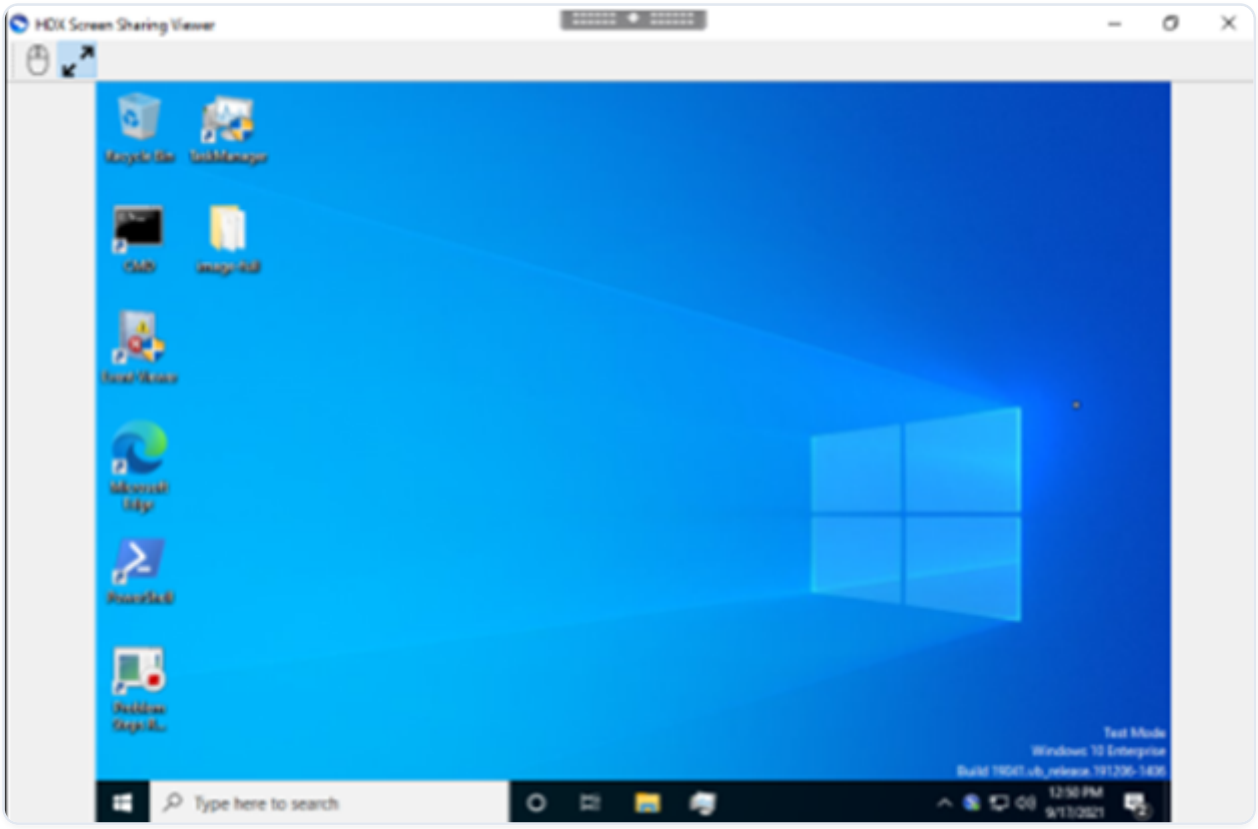


セッションを共有しているユーザーから提供された接続文字列をテキストボックスに入力または貼り付けます。**接続**をクリックして接続を確立します。



HDX 画面共有ビューアウィンドウの左上隅にあるマウスアイコンをクリックすると、キーボードとマウスの制御を要求できます。

共有セッションからいつでも切断するには、**HDX 画面共有ビューア**ウィンドウを閉じます。



その他の考慮事項

- 画面共有ビューアアプリケーションは、VDA に *C:\Program Files\Citrix\HDX\bin\TwPlayer.exe* として含まれており、Virtual Apps Server を使用して公開アプリケーションとして展開される場合があります。この代替展開モデルにより、仮想デスクトップにアクセスできないユーザーとのコラボレーションが可能になります。
- 共有セッションに接続できるユーザー数は、画面共有ポリシーのネットワークポート範囲を使用して制限できます。ユーザーごとに1つのポートが必要です。デフォルトの範囲では、最大100人のユーザーが許可されます。
- セッションに接続されているすべてのモニターが共有されます。個々のモニターを選択することはできません。
- H.265 ビデオコーデックはサポートされていません。

仮想ディスプレイレイアウト

仮想ディスプレイ構成UIを使用すると、ライブセッション内でVDA上のセッションモニターごとに仮想ディスプレイレイアウトを定義できます。この機能により、各セッションモニターを個別に複数の仮想モニターに分割できます。リモートデスクトップでは、合計8つの仮想モニターに分割できます。また、ディスプレイのセッションプライマリモニターとDPI設定を更新することもできます。

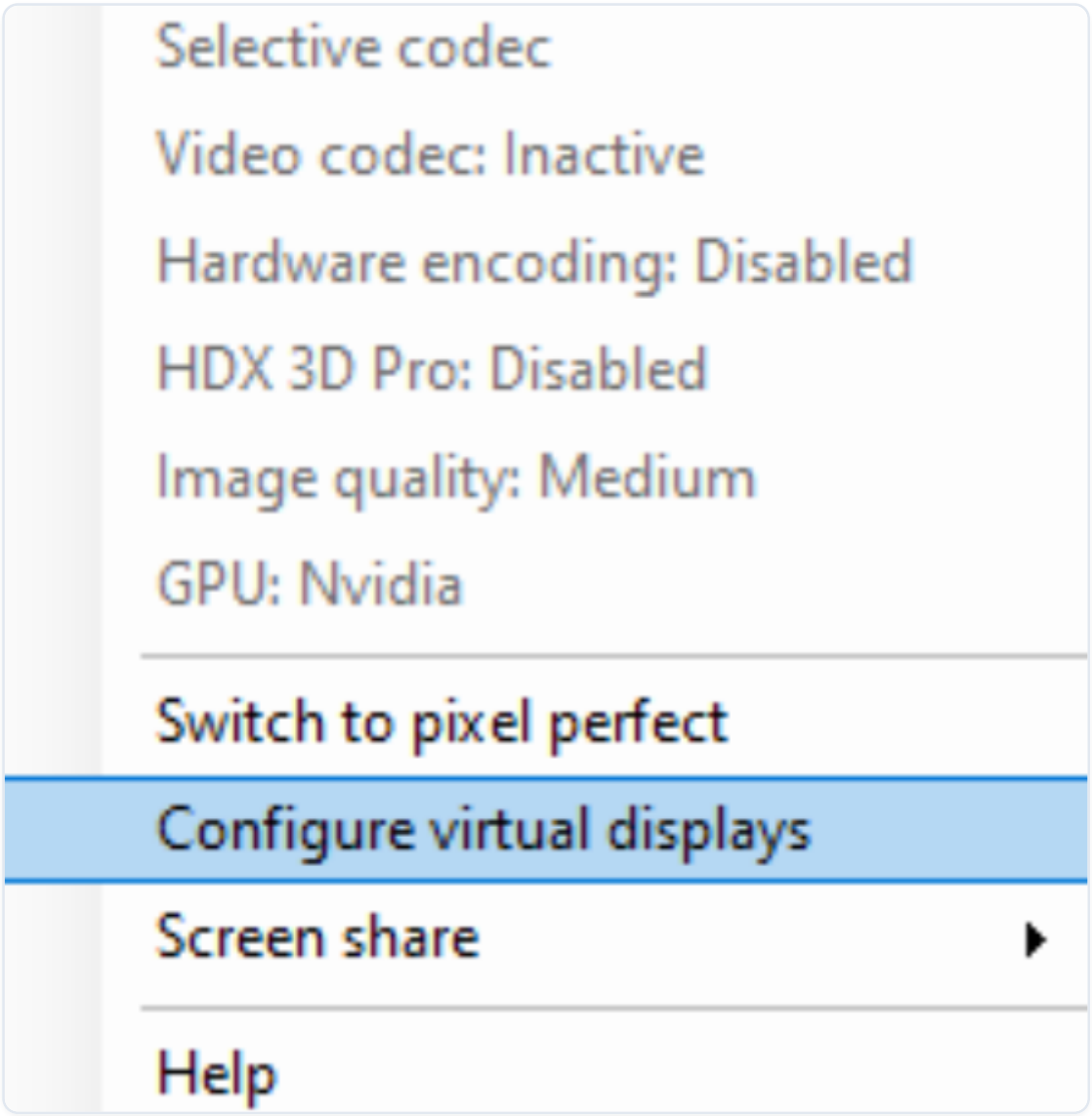
仮想ディスプレイ構成は、ユーザーごと、クライアントデバイスごとに保存されます。この構成は、特定のユーザーからの特定のクライアントからの以降のすべての接続に適用されます。セッションのリサイズ、セッションの切断または再接続、およびセッションのログオフまたはログオンをまたいで保持されます。構成された仮想ディスプレイレイアウトのリセットは、セッションのリサイズとセッションモニター数の変更時に発生します。

システム要件

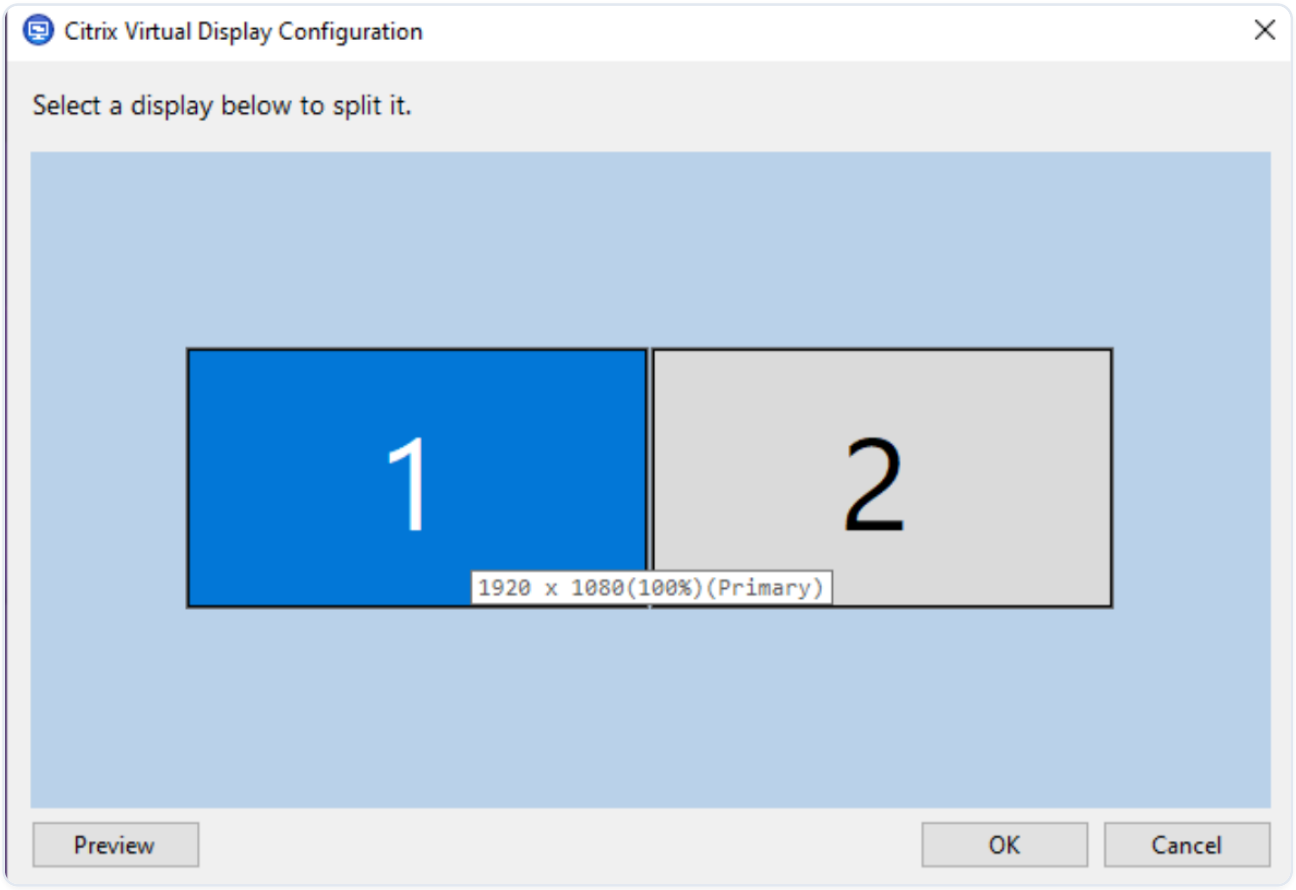
- Windows: シングルセッションまたはマルチセッションOS VDA
- グラフィックステータスインジケーターポリシーを有効にする必要があります
- デスクトップセッションのみ構成できます。

構成

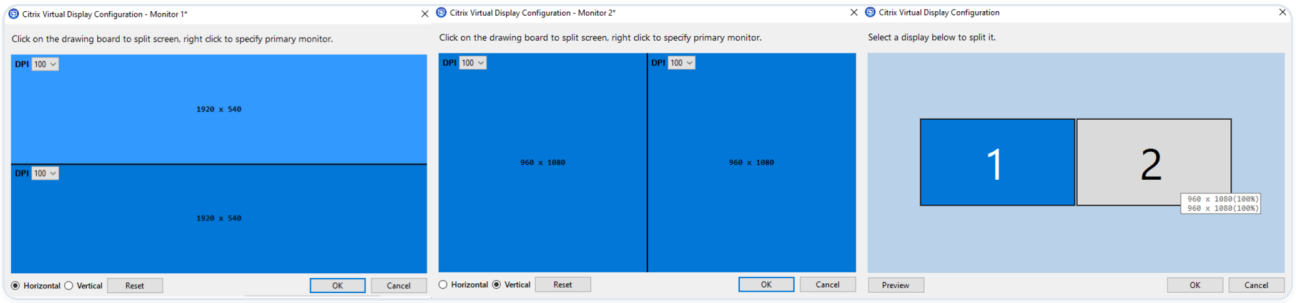
仮想ディスプレイレイアウトを構成するには、グラフィックステータスインジケーターアイコンを右クリックし、「仮想ディスプレイの構成」オプションを選択します。仮想ディスプレイ構成UIが起動します。



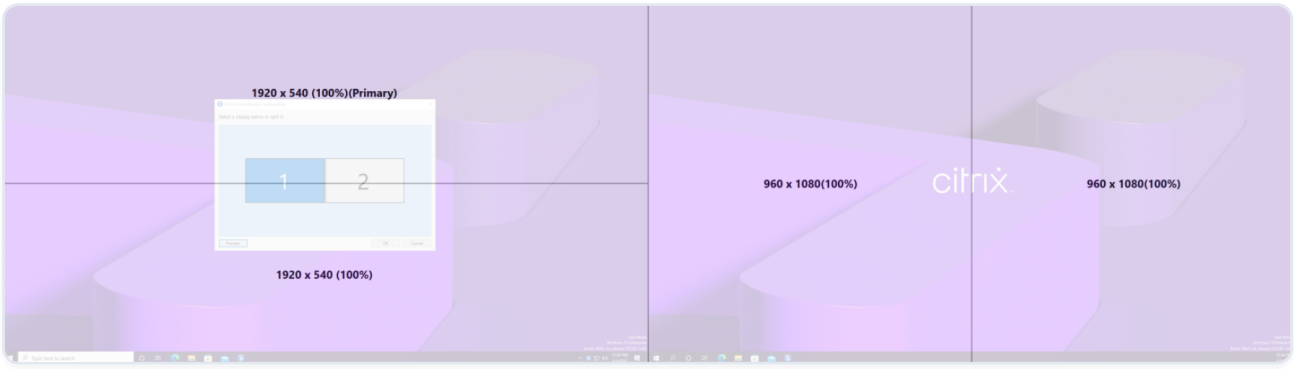
UIには現在のセッションディスプレイレイアウトが表示され、青色はセッションのプライマリモニターを示します。ディスプレイにカーソルを合わせると、ディスプレイ設定のツールヒントが表示されます。このツールヒントには、特定のセッションモニターで定義されている現在の仮想ディスプレイレイアウトに関する情報が表示されます。



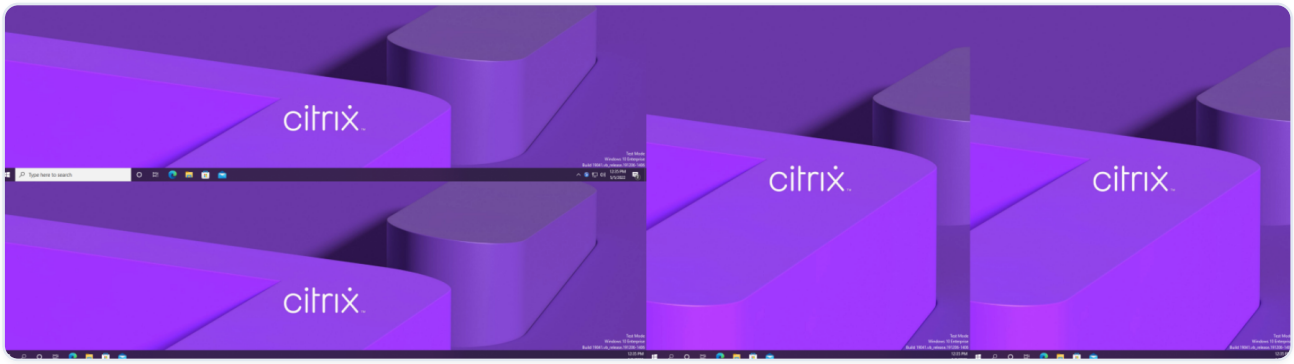
ディスプレイを選択すると、対話型UIに移行し、選択したセッションモニターの仮想ディスプレイを構成できます。水平線または垂直線を描画して、画面を仮想モニターに分割できます。画面は、セッションモニターの解像度の指定されたパーセンテージに従って分割されます。仮想ディスプレイを右クリックしてプライマリモニターとしてマークし、DPIドロップダウンリストを使用して仮想ディスプレイの優先スケーリング係数を設定します。仮想ディスプレイレイアウトを定義したら、**OK**をクリックしてレイアウトを一時的に保存するか、**キャンセル**をクリックして変更を破棄します。**リセット**を使用して構成を元に戻し、セッションモニターの元のレイアウトを復元できます。



現在構成されている仮想ディスプレイレイアウトをプレビューするには、**プレビュー**ボタンをクリックします。セッション内の仮想ディスプレイの予想される位置と解像度を強調表示するウィンドウが表示されます。



OKをクリックして、仮想ディスプレイレイアウトをすぐに適用して保存します。**キャンセル**をクリックしてUIを閉じ、すべての変更を破棄します。



その他の考慮事項

- 必要な最小仮想ディスプレイ解像度は640 x 480です。
- UIで定義された仮想ディスプレイDPIは、指定されたディスプレイ解像度に対するOSのスケーリングサポートに依存します。
- Citrix Workspace™アプリの既存の仮想ディスプレイ機能と同時にこの機能を使用しないでください。
- プレビュー機能はServer 2016ではサポートされていません。

適応型リフレッシュレート

新しいスケーラビリティの改善により、HDX™ は、仮想モニターのリフレッシュレートを、設定されたターゲット FPS ポリシーに一致させます。適応型リフレッシュレート (ARR) は、シングルセッション VDA とマルチセッション VDA の両方で利用でき、GPU アクセラレーションシナリオと非 GPU シナリオの両方で機能します。

ターゲットフレームレート(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/targetframerate_60.png)

DirectX診断ツール(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/directx-diagnostic-tool.png)

> **注**
>
> アダプティブ リフレッシュレートは、Citrix Indirect DisplayまたはIDDが使用されている場合（Citrix Virtual Apps and Desktops™のデフォルトによる）にのみ利用可能であり、ベンダー提供のディスプレイアダプターを使用している場合は利用できません。

グラフィック用ロス許容モード

グラフィックのロス耐性モードは、パケットロスが検出されたときにセッションがインタラクティブな状態を維持するように徹底的に再設計されました。ネットワークの状態が、事前に定義された帯域幅、遅延、パケットロスのしきい値を超えて悪化すると、Citrix®グラフィックエンコーダーは、パケットロスの影響を克服するために、より積極的なパケット配信モードに自動的に切り替わります。その結果、帯域幅の使用量はパケットロスの量に比例して増加します。その後、状況が改善すると、Citrixグラフィックエンコーダーはシームレスに元の状態に戻ります。しきい値はポリシーを介して構成でき、デフォルトは300ミリ秒の遅延と5%のパケットロスです。

現在、Windows 2311 用のCitrix Workspace™アプリがサポートされています。他のプラットフォームのサポートは、今後のCitrix Workspaceアプリのリリースで追加される予定です。この機能の以前のバージョンと同様に、この機能が動作するにはHDX™ Adaptive Transport (EDT) を有効にする必要があります。さらに、Citrix Gateway Service を介して接続する場合、グラフィックの損失許容モードもGatewayで有効にする必要があります。

マルチメディア

HDX™ テクノロジースタックは、2つの補完的なアプローチを通じてマルチメディアアプリケーションの配信をサポートします。

- サーバー側レンダリングによるマルチメディア配信
- クライアント側レンダリングによるマルチメディアリダイレクト

この戦略により、優れたユーザーエクスペリエンスで幅広いマルチメディア形式を配信できると同時に、サーバーのスケーラビリティを最大化してユーザーあたりのコストを削減できます。

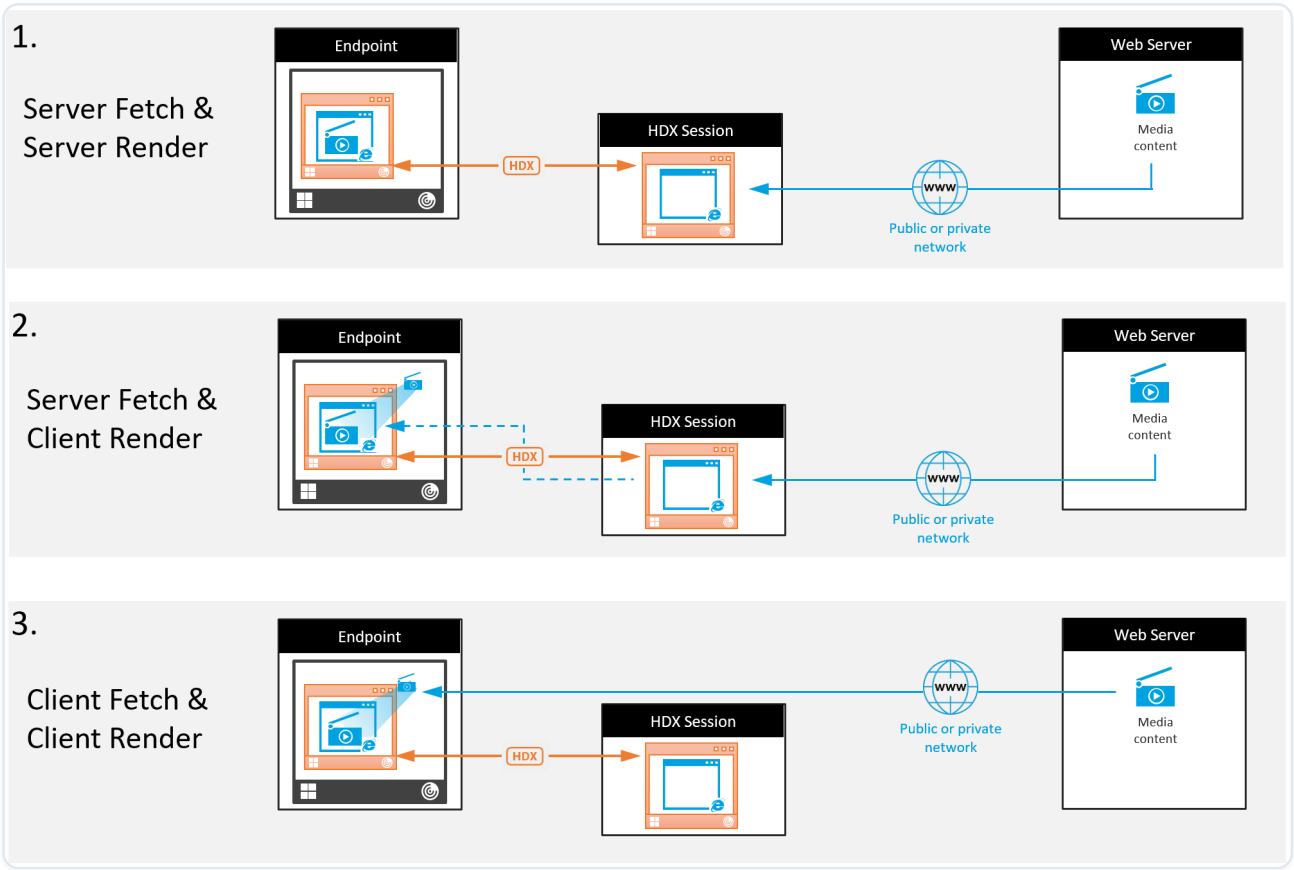
サーバー側でレンダリングされるマルチメディア配信では、オーディオおよびビデオコンテンツはアプリケーションによってCitrix Virtual Apps and Desktopsサーバー上でデコードおよびレンダリングされます。その後、コンテンツは圧縮され、ICAプロトコルを使用してユーザーデバイス上のCitrix Workspaceアプリに配信されます。この方法は、さまざまなアプリケーションおよびメディア形式との互換性を最大限に高めます。ビデオ処理は計算負荷が高いため、サーバー側でレンダリングされるマルチメディア配信は、オンボードのハードウェアアクセラレーションから大きな恩恵を受けます。たとえば、DirectX Video Acceleration (DXVA) のサポートにより、H.264デコードを個別のハードウェアで実行することでCPUの負荷を軽減します。Intel Quick Sync、AMD RapidFire、NVIDIA NVENCテクノロジーは、ハードウェアアクセラレーションによるH.264エンコーディングを提供します。

ほとんどのサーバーはビデオ圧縮のためのハードウェアアクセラレーションを提供しないため、すべてのビデオ処理がサーバーCPUで行われる場合、サーバーのスケーラビリティは悪影響を受けます。多くのマルチメディア形式をローカルレンダリングのためにユーザーデバイスにリダイレクトすることで、高いサーバーのスケーラビリティを維持できます。

- Windows Mediaリダイレクトは、通常Windows Media Playerに関連付けられているさまざまなメディア形式について、サーバーの負荷を軽減します。
- HTML5ビデオは普及しており、Citrix®はこの種のコンテンツ向けにリダイレクトテクノロジーを導入しました。HTML5、HLS、DASH、またはWebRTCを使用するWebサイトには、ブラウザコンテンツリダイレクトをお勧めします。
- 一般的なコンテンツリダイレクトテクノロジーであるホストからクライアントへのリダイレクトとローカルアプリアクセスをマルチメディアコンテンツに適用できます。

これらのテクノロジーを組み合わせると、リダイレクトを設定しない場合、HDXはサーバー側レンダリングを実行します。 リダイレクトを設定した場合、HDXはサーバーフェッチとクライアントレンダリング、またはクライアントフェッチとクライアントレンダリングのいずれかを使用します。これらの方法が失敗した場合、HDXは必要に応じてサーバー側レンダリングにフォールバックし、フォールバック防止ポリシーの対象となります。

シナリオ例



シナリオ1. (サーバーフェッチとサーバーレンダリング):

1. サーバーはソースからメディアファイルを取得し、デコードしてから、オーディオデバイスまたはディスプレイデバイスにコンテンツを提示します。
2. サーバーは、提示された画像またはサウンドをそれぞれディスプレイデバイスまたはオーディオデバイスから抽出します。
3. サーバーはオプションでそれを圧縮し、その後クライアントに送信します。

このアプローチでは、高いCPUコスト、高い帯域幅コスト（抽出された画像/音声が効率的に圧縮されていない場合）、および低いサーバー拡張性が発生します。

Thinwireおよびオーディオ仮想チャネルがこのアプローチを処理します。このアプローチの利点は、クライアントのハードウェアおよびソフトウェア要件を削減できることです。このアプローチ

を使用すると、デコードはサーバーで行われ、より幅広い種類のデバイスとフォーマットで動作します。

シナリオ2。（サーバーフェッチとクライアントレンダリング）：

このアプローチは、メディアコンテンツがデコードされ、オーディオまたはディスプレイデバイスに提示される前に傍受できることに依存しています。圧縮されたオーディオ/ビデオコンテンツは代わりにクライアントに送信され、そこでローカルでデコードおよび提示されます。このアプローチの利点は、クライアントデバイスにオフロードされ、サーバーのCPUサイクルを節約できることです。

しかし、これはクライアントに追加のハードウェアおよびソフトウェア要件ももたらします。クライアントは、受信する可能性のある各フォーマットをデコードできる必要があります。

シナリオ3。（クライアントフェッチとクライアントレンダリング）：

このアプローチは、メディアコンテンツのURLがソースからフェッチされる前に傍受できることに依存しています。URLはクライアントに送信され、そこでメディアコンテンツがフェッチ、デコード、およびローカルで提示されます。このアプローチは概念的にシンプルです。その利点は、サーバーが制御コマンドのみを送信するため、サーバーのCPUサイクルと帯域幅の両方を節約できることです。ただし、メディアコンテンツが常にクライアントからアクセスできるとは限りません。

フレームワークとプラットフォーム：

シングルセッションオペレーティングシステム（Windows、Mac OS X、Linux）は、マルチメディアアプリケーションのより迅速な開発を可能にするマルチメディアフレームワークを提供します。この表は、より一般的なマルチメディアフレームワークの一部をリストしています。各フレームワークは、メディア処理をいくつかの段階に分け、パイプラインベースのアーキテクチャを使用します。

フレームワーク	プラットフォーム
DirectShow	Windows (98以降)
メディア ファンデーション	ウィンドウズ (ビスタ以降)
Gストリーマー	リナックス
クイックタイム	マック オーエス テン

メディアリダイレクト技術によるダブルホップサポート

オーディオリダイレクト	いいえ
ブラウザコンテンツリダイレクト	いいえ
HDX Webカメラリダイレクト	はい
HTML5ビデオのリダイレクト	はい
Windows Mediaリダイレクト	はい

オーディオ機能

HDXオーディオ機能を最適化するポリシーに、以下のCitrixポリシー設定を構成して追加できます。使用方法の詳細、および他のポリシー設定との関係と依存関係については、「オーディオポリシー設定」、「帯域幅ポリシー設定」、および「マルチストリーム接続ポリシー設定」を参照してください。

アダプティブオーディオ

アダプティブオーディオを使用すると、VDAでオーディオ品質ポリシーを手動で構成する必要がありません。アダプティブオーディオは、環境に合わせて設定を最適化し、古いオーディオ圧縮形式を置き換えて、優れたユーザーエクスペリエンスを提供します。

アダプティブオーディオはデフォルトで有効になっています。アダプティブオーディオを無効にするには、「オーディオポリシー設定」を参照してください。

重要:

リアルタイムオーディオアプリケーションが必要な場合、Citrix®はTCPではなくUser Datagram Protocol（UDP）を使用してオーディオを配信することを推奨します。UDP経由で利用できるオーディオトランスポートオプションは次のとおりです。

- UDP経由のオーディオ
- HDX™ アダプティブ トランスポート (エンライトンド データ トランスポート)

DTLSを使用したUDPオーディオ暗号化は、Citrix GatewayとCitrix Workspace™ appの間でのみ利用可能です。そのため、TCPトランスポートを使用する方が望ましい場合があります。TCPは、VDAからCitrix Workspace appへのエンドツーエンドのTLS暗号化をサポートします。

アダプティブオーディオとUDPオーディオの詳細については、「UDPリアルタイムトランスポート経由のオーディオとオーディオUDPポート範囲」を参照してください。

オーディオのロストレラントモード

損失許容モードはオーディオをサポートします。この機能は、リアルタイムストリーミングのユーザーエクスペリエンスを向上させ、高遅延およびパケット損失のあるネットワーク経由でユーザーが接続している場合に、EDTを介したオーディオ品質を改善します。この機能はデフォルトで無効になっています。

注：

この機能が動作するには、**HDX Adaptive Transport (EDT)** ポリシーと**オーディオの損失許容モード**ポリシーの両方を有効にする必要があります。

システム要件

損失許容モードをサポートする以下の製品が最小バージョンであることを確認してください。

- シトリックス バーチャル デリバリー エージェント (VDA) 2308
- Windows向けCitrix Workspaceアプリ 2309

さらに、以下の機能を有効にする必要があります。

- HDX Adaptive Transportポリシー。
- (オプション) リモート接続の場合、Citrix Gateway Serviceが必要です。

注：

上記の条件が満たされない場合、オーディオはEDT Reliableトランスポート経由で送信されます。

追加情報

損失許容モードは、マルチメディアコンテンツを再送信することなく伝送中のパケット損失を許容する損失許容トランスポートプロトコルであり、ユーザーによりリアルタイムなエクスペリエンスをもたらします。

Enlightened Data Transport (EDT) は、Citrix独自のトランスポートプロトコルであり、サーバーのスケーラビリティを維持しながら、困難な長距離接続で優れたユーザーエクスペリエンスを提供します。損失許容モードは、ネットワーク輻輳に直面しても安定した接続を維持するために、損失許容モードをトランスポートプロトコルとして使用するCitrix Gatewayサービスの機能です。これにより、リモートワーカーに一貫した安定したエクスペリエンスが保証されます。通常の状況では、EDTと損失許容モードの両方が同様の結果を提供します。ただし、パケット損失のあるネットワーク状況では、損失許容モードはEDTと比較してより優れたオーディオエクスペリエンスを提供します。これにより、リアルタイムマルチメディアに依存するリモートワーカーにとって不可欠な機能となります。

オーディオ品質

一般的に、音質が高いほど、より多くのオーディオデータをユーザーデバイスに送信するため、より多くの帯域幅とサーバーCPU使用率を消費します。サウンド圧縮を使用すると、音質とセッション全体のパフォーマンスのバランスを取ることができます。Citrixポリシー設定を使用して、サウンドファイルに適用する圧縮レベルを構成します。

デフォルトでは、TCPトランスポートが使用されている場合、**オーディオ品質ポリシー**設定は「高 - 高精細オーディオ」に設定されています。UDPトランスポート（推奨）が使用されている場合、ポリシーは「中 - 音声に最適化」に設定されます。**高精細オーディオ**設定は、高忠実度のステレオオーディオを提供しますが、他の品質設定よりも多くの帯域幅を消費します。最適化されていない音声チャットまたはビデオチャットアプリケーション（ソフトフォンなど）には、このオーディオ品質を使用しないでください。その理由は、リアルタイム通信に適さない遅延をオーディオパスに導入する可能性があるためです。選択されたトランスポートプロトコルに関係なく、リアルタイムオーディオには音声に最適化されたポリシー設定を推奨します。

帯域幅が制限されている場合（衛星接続やダイヤルアップ接続など）は、オーディオ品質を**Low**に下げると、消費される帯域幅が最小限になります。この状況では、低帯域幅接続のユーザー向けに個別のポリシーを作成し、高帯域幅接続のユーザーが悪影響を受けないようにします。

設定の詳細については、「オーディオポリシー設定」を参照してください。ユーザーデバイスでClient audio settingsを有効にすることを忘れないでください。

オーディオ再生と録音の帯域幅ガイドライン：

- アダプティブオーディオ（デフォルト）
  - ビットレート: 可変アダプティブ
  - チャンネル数: 再生用2（ステレオ）、マイクキャプチャ用1（モノラル）
  - 周波数: 48000 Hz
  - ビット深度: 16ビット
- 高音質
  - ビットレート：再生で約100 kbps（最小75、最大175 kbps）/マイクキャプチャで約70 kbps
  - チャンネル数：再生で2（ステレオ）、マイクキャプチャで1（モノラル）
  - 周波数：44100 Hz
  - ビット深度: 16ビット
- 中品質 (VoIPに推奨)
  - ビットレート: 再生時 ~16 kbps (最小20 kbps、最大40 kbps)、マイクキャプチャ時 ~16 kbps
  - チャンネル数: 再生とキャプチャの両方で1 (モノラル)
  - 周波数: 16000 Hz (広帯域)
  - ビット深度: 16ビット
- 低品質
  - ビットレート: 再生時 ~11 kbps (最小10 kbps、最大25 kbps)、マイクキャプチャ時 ~11 kbps
  - チャンネル数: 再生とキャプチャの両方で1 (モノラル)
  - 周波数: 8000 Hz (狭帯域)
  - ビット深度: 16ビット

クライアントオーディオリダイレクト

ユーザーデバイス上のスピーカーまたはその他のサウンドデバイスを介して、サーバー上のアプリケーションからオーディオを受信できるようにするには、**クライアントオーディオリダイレクト**設定を**許可**のままにします。これはデフォルトです。

クライアントオーディオマッピングは、サーバーとネットワークに余分な負荷をかけます。ただし、クライアントオーディオリダイレクトを禁止すると、すべてのHDXオーディオ機能が無効になります。

設定の詳細については、「オーディオポリシー設定」を参照してください。ユーザーデバイスでクライアントオーディオ設定を有効にすることを忘れないでください。

クライアントマイクのリダイレクト

ユーザーデバイス上のマイクなどの入力デバイスを使用してユーザーがオーディオを録音できるようにするには、**クライアントマイクのリダイレクト**設定をデフォルト（許可）のままにします。

セキュリティのため、ユーザーデバイスは、信頼できないサーバーがマイクへのアクセスを試みた場合に、ユーザーに警告します。ユーザーはマイクを使用する前に、アクセスを許可するか拒否するかを選択できます。ユーザーはCitrix Workspaceアプリでこの警告を無効にできます。

設定の詳細については、「オーディオポリシー設定」を参照してください。ユーザーデバイスでClient audio settingsを有効にすることを忘れないでください。

オーディオプラグアンドプレイ

オーディオプラグアンドプレイポリシー設定は、複数のオーディオデバイスを使用してサウンドを録音および再生することを許可または禁止します。この設定は、デフォルトで**有効**になっています。オーディオプラグアンドプレイにより、オーディオデバイスが認識されるようになります。ユーザーセッションが開始されるまで接続されていなくても、デバイスは認識されます。

この設定は、WindowsマルチセッションOSマシンにのみ適用されます。

設定の詳細については、「オーディオポリシー設定」を参照してください。

オーディオリダイレクト帯域幅制限とオーディオリダイレクト帯域幅制限の割合

オーディオリダイレクト帯域幅制限ポリシー設定は、セッションでのオーディオの再生と録音の最大帯域幅（キロビット/秒）を指定します。

オーディオリダイレクト帯域幅制限の割合設定は、オーディオリダイレクトの最大帯域幅を、利用可能な総帯域幅の割合として指定します。

デフォルトでは、両方の設定でゼロ（最大なし）が指定されています。両方の設定が構成されている場合、帯域幅制限が最も低い方が使用されます。

設定の詳細については、「帯域幅ポリシー設定」を参照してください。ユーザーデバイスでクライアントオーディオ設定を有効にすることを忘れないでください。

UDPリアルタイムトランスポート経由のオーディオとオーディオUDPポート範囲

デフォルトでは、ユーザーデータグラムプロトコル（UDP）リアルタイムトランスポート経由のオーディオは許可されています（インストール時に選択した場合）。これは、UDPリアルタイムトランスポート経由のオーディオを使用する接続のために、サーバー上にUDPポートを開きます。ネットワークの輻輳やパケット損失がある場合は、可能な限り最高のユーザーエクスペリエンスを確保するために、オーディオにUDP/RTPを構成することをお勧めします。ソフトフォンアプリケーションなどのリアルタイムオーディオの場合、EDTよりもUDPオーディオが推奨されます。UDPは再送信なしでパケット損失を許容するため、パケット損失が多い接続で遅延が追加されることはありません。

重要:

Citrix Gatewayが経路にない場合、UDPで送信されるオーディオデータは暗号化されません。Citrix GatewayがCitrix Virtual Apps and Desktops™リソースにアクセスするように構成されている場合、エンドポイントデバイスとCitrix Gateway間のオーディオトラフィックはDTLSプロトコルを使用して保護されます。

オーディオUDPポート範囲は、Windows VDAがユーザーデバイスとオーディオパケットデータを交換するために使用するポート番号の範囲を指定します。

デフォルトでは、範囲は16500から16509です。

注：

適応型オーディオにUDPリアルタイムトランスポート経由のオーディオが必要ない場合、Citrixはポリシー設定を「無効」に構成することを推奨します。これにより、Citrix WorkspaceアプリクライアントがUDP接続のオープンを要求したり、不要なCitrix Workspaceアプリクライアントのファイアウォール構成ダイアログウィンドウが表示されたりするのを防ぐことができます。

> UDPリアルタイムトランスポート経由のオーディオに関する設定の詳細については、オーディオポリシー設定を参照してください。オーディオUDPポート範囲の詳細については、マルチストリーム接続ポリシー設定を参照してください。ユーザーデバイスでクライアントオーディオ設定を有効にすることを忘れないでください。

UDP経由のオーディオにはWindows VDAが必要です。Linux VDAでサポートされているポリシーについては、ポリシーサポートリストを参照してください。

ユーザーデバイスのオーディオ設定ポリシー

1. グループポリシーオブジェクト管理用テンプレートの構成に従って、グループポリシーテンプレートをロードします。
2. グループポリシーエディターで、**管理用テンプレート > Citrixコンポーネント > Citrix Workspace > ユーザーエクスペリエンス**を展開します。
3. **クライアントオーディオ設定**で、**未構成**、**有効**、または**無効**を選択します。
   - **未構成**。デフォルトでは、オーディオリダイレクトは高品質オーディオまたは以前に構成されたカスタムオーディオ設定を使用して有効になっています。
   - **有効**。選択したオプションを使用してオーディオリダイレクトを有効にします。
   - **無効**。オーディオリダイレクトを無効にします。
4. **有効**を選択した場合、音質を選択します。UDPオーディオの場合は、**中**（デフォルト）を使用します。
5. UDPオーディオの場合のみ、**リアルタイムトランスポートを有効にする**を選択し、ローカルのWindowsファイアウォールで開く受信ポートの範囲を設定します。
6. Citrix Gateway で UDP Audio を使用するには、**Allow Real-Time Transport Through gateway** を選択します。Citrix Gateway を DTLS で構成します。詳細については、こちらの記事を参照してください。

管理者として、これらの変更を行うためのエンドポイントデバイスを制御できない場合は、StoreFront の default.ica 属性を使用して UDP Audio を有効にします。たとえば、BYOD (個人所有デバイス) や自宅のコンピューターの場合などです。

1. StoreFront マシンで、メモ帳などのエディターを使用して C:\inetpub\wwwroot\Citrix\\\<Store Name>\App_Data\default.ica を開きます。
2. セクションに以下のエントリを作成します。

   ; このテキストはリアルタイムトランスポートを有効にします

RTPオーディオを有効にする=true

; このテキストはゲートウェイ経由のリアルタイムトランスポートを許可します

ゲートウェイ経由のUDPを有効にする=true

; このテキストはオーディオ品質を「中」に設定します

AudioBandwidthLimit=1

; UDP ポート範囲

RtpAudioLowestPort=16500

RtpAudioHighestPort=16509

default.ica を編集してユーザーデータグラムプロトコル (UDP) オーディオを有効にすると、そのストアを使用しているすべてのユーザーに対して UDP オーディオが有効になります。

マルチメディア会議中のエコーを回避する

オーディオまたはビデオ会議のユーザーはエコーを聞くことがあります。エコーは通常、スピーカーとマイクが互いに近すぎるときに発生します。そのため、オーディオおよびビデオ会議にはヘッドセットの使用をお勧めします。

HDXは、エコーを最小限に抑えるエコーキャンセレーションオプション（デフォルトで有効）を提供します。エコーキャンセレーションの有効性は、スピーカーとマイクの間の距離に影響されます。デバイスが互いに近すぎたり遠すぎたりしないようにしてください。

レジストリ設定を変更して、エコーキャンセレーションを無効にできます。詳細については、レジストリを介して管理される機能のリストにあるマルチメディア会議中のエコーを回避するを参照してください。

ソフトフォン

ソフトフォンは、電話インターフェースとして機能するソフトウェアです。ソフトフォンを使用して、コンピューターやその他のスマートデバイスからインターネット経由で電話をかけます。ソフトフォンを使用すると、画面を使って電話番号をダイヤルしたり、その他の電話関連機能を実行したりできます。

Citrix Virtual Apps and Desktopsは、ソフトフォンを配信するためのいくつかの代替手段をサポートしています。

- **制御モード**。ホストされているソフトフォンが物理的な電話機を制御します。このモードでは、Citrix Virtual Apps and Desktopsサーバーを介してオーディオトラフィックは流れません。
- **HDX RealTime最適化ソフトフォンサポート（推奨）**。メディアエンジンはユーザーデバイス上で実行され、Voice over Internet Protocolトラフィックはピアツーピアで流れます。例については、以下を参照してください。
  - Microsoft Teams向けHDX最適化
  - HDX RealTime Optimization Pack（Microsoft Skype for Businessの配信を最適化します）
  - Cisco Jabber Softphone for VDI (シスコ ジャバー ソフトフォン フォー VDI)（旧称VXME）
  - VDI向け シスコ Webex ミーティング
  - Avaya VDI Equinox (アバイア VDI エクイノックス)（旧称VDI Communicator）
  - Zoom VDI Plugin (ズーム VDI プラグイン)
  - Genesys PureEngage クラウド
  - Nuance Dragon PowerMic ディクテーションデバイス
- **ローカルアプリアクセス**。Citrix Virtual Apps and Desktopsの機能で、ソフトフォンなどのアプリケーションをWindowsユーザーデバイス上でローカルに実行しながら、仮想/公開デスクトップとシームレスに統合されているように見せることができます。この機能は、すべてのオーディオ処理をユーザーデバイスにオフロードします。詳細については、「ローカルアプリアクセスとURLリダイレクト」を参照してください。
- **HDX RealTime汎用ソフトフォンサポート**。ICA経由のVoice over Internet Protocol。

汎用ソフトフォンサポート

汎用ソフトフォンサポートにより、データセンターのXenAppまたはXenDesktopで、変更されていないソフトフォンをホストできます。オーディオトラフィックは、Citrix ICAプロトコル（できればUDP/RTPを使用）を介して、Citrix Workspaceアプリを実行しているユーザーデバイスに送信されます。

汎用ソフトフォンサポートは、HDX RealTimeの機能です。このソフトフォン配信アプローチは、特に次の場合に役立ちます。

- ソフトフォンを配信するための最適化されたソリューションが利用できず、ユーザーがLocal App Accessを使用できるWindowsデバイスを使用していない場合。
- ソフトフォンの最適化された配信に必要なメディアエンジンがユーザーデバイスにインストールされていないか、ユーザーデバイスで実行されているオペレーティングシステムのバージョ

ンで利用できない場合。このシナリオでは、汎用HDX RealTimeが貴重なフォールバックソリューションを提供します。

Citrix Virtual Apps and Desktopsを使用する際のソフトフォン配信には、次の2つの考慮事項があります。

- ソフトフォンアプリケーションが仮想/公開デスクトップにどのように配信されるか。
- ユーザーのヘッドセット、マイク、スピーカー、またはUSB電話機にオーディオがどのように配信されるか。

Citrix Virtual Apps and Desktopsには、汎用ソフトフォン配信をサポートするための多数のテクノロジーが含まれています。

- リアルタイムオーディオの高速エンコードと帯域幅効率のためのOptimized-for-Speechコーデック。
- 低遅延オーディオスタック。
- ネットワーク遅延が変動したときにオーディオをスムーズにするサーバー側ジッターバッファ。
- サービス品質のためのパケットタグ付け (DSCP および WMM)。
  - RTPパケットのDSCPタグ付け (レイヤー3)
  - Wi-FiのWMMタグ付け

Windows、Linux、Chrome、Mac版のCitrix Workspaceアプリも、Voice over Internet Protocolに対応しています。Windows版Citrix Workspaceアプリは、以下の機能を提供します。

- クライアント側のジッターバッファ - ネットワーク遅延が変動しても、スムーズなオーディオを保証します。
- エコーキャンセル - ヘッドセットを使用しない作業者向けに、マイクとスピーカー間の距離の変動を大きく許容します。
- オーディオプラグアンドプレイ - オーディオデバイスは、セッションを開始する前に接続する必要はありません。いつでも接続できます。
- オーディオデバイスルーティング - ユーザーは着信音をスピーカーに、音声パスをヘッドセットにルーティングできます。
- マルチストリームICA - ネットワーク上で柔軟なサービス品質ベースのルーティングを可能にします。
- ICAは4つのTCPストリームと2つのUDPストリームをサポートします。UDPストリームの1つは、RTPを介したリアルタイムオーディオをサポートします。

Citrix Workspaceアプリの機能の概要については、Citrix Receiver Feature Matrixを参照してください。

システム構成の推奨事項

クライアントハードウェアとソフトウェア: 最適なオーディオ品質を得るには、最新バージョンのCitrix Workspaceアプリと、音響エコーキャンセル (AEC) 機能を備えた高品質のヘッドセットをお勧めします。Windows、Linux、Mac版のCitrix Workspaceアプリは、Voice over Internet Protocolをサポートしています。また、Dell WyseはThinOS (WTOS) 向けにVoice over Internet Protocolをサポートしています。

CPUに関する考慮事項: VDAのCPU使用率を監視して、各仮想マシンに2つの仮想CPUを割り当てる必要があるかどうかを判断します。リアルタイムの音声とビデオはデータ集約型です。2つの仮想CPUを構成すると、スレッド切り替えの遅延が減少します。したがって、Citrix Virtual Desktops™ VDI環境では2つのvCPUを構成することをお勧めします。

2つの仮想CPUを持つことは、物理CPUの数を2倍にすることを必ずしも意味しません。物理CPUはセッション間で共有できるためです。

Citrix Gateway Protocol (CGP) は、セッション信頼性機能に使用され、CPU 消費も増加させます。高品質のネットワーク接続では、VDA の CPU 消費を削減するためにこの機能を無効にできます。強力なサーバーでは、上記のいずれのステップも不要な場合があります。

UDPオーディオ: UDP経由のオーディオは、ネットワークの輻輳とパケット損失に対して優れた耐性を提供します。利用可能な場合は、TCPの代わりにこれをお勧めします。

LAN/WAN構成: 良好なリアルタイムオーディオ品質のためには、ネットワークの適切な構成が不可欠です。通常、過剰なブロードキャストパケットはジッターを引き起こす可能性があるため、仮想LAN (VLAN) を構成する必要があります。IPv6対応デバイスは多くのブロードキャストパケットを生成する可能性があります。IPv6サポートが不要な場合は、それらのデバイスでIPv6を無効にできます。Quality of Serviceをサポートするように構成してください。

WAN接続の使用設定: LANおよびWAN接続を介してボイスチャットを使用できます。WAN接続では、オーディオ品質は接続の遅延、パケット損失、およびジッターに依存します。WAN接続のユーザーにソフトフォンを配信する場合、データセンターとリモートオフィス間でNetScaler® SD-WANを使用することをお勧めします。これにより、高いQuality of Serviceが維持されます。NetScaler SD-WANは、UDPを含むMulti-Stream ICAをサポートしています。また、単一のTCPストリームの場合、さまざまなICA仮想チャネルの優先順位を区別して、高優先度のリアルタイムオーディオデータが優先的に処理されるようにすることが可能です。

DirectorまたはHDX Monitorを使用して、HDX構成を検証します。

リモートユーザー接続: Citrix Gatewayは、UDP/RTPトラフィックをネイティブに（TCPでのカプセル化なしで）配信するためにDTLSをサポートしています。 ポート443経由のUDPトラフィックに対してファイアウォールを双方向に開きます。

コーデックの選択と帯域幅の消費: ユーザーデバイスとデータセンター内のVDAの間では、**Optimized-for-Speech**コーデック設定（中品質オーディオとも呼ばれます）を使用することをお勧めします。VDAプラットフォームとIP-PBXの間では、ソフトフォンは構成またはネゴシエートされたコーデックを使用します。例：

- G711は良好な音声品質を提供しますが、1コールあたり80キロビット/秒から100キロビット/秒の帯域幅要件があります（ネットワークレイヤー2のオーバーヘッドに依存）。
- G729は良好な音声品質を提供し、1コールあたり30キロビット/秒から40キロビット/秒の低い帯域幅要件があります（ネットワークレイヤー2のオーバーヘッドに依存）。

仮想デスクトップへのソフトフォンアプリケーションの配信

XenDesktop®仮想デスクトップにソフトフォンを配信するには、2つの方法があります。

- アプリケーションは仮想デスクトップイメージにインストールできます。
- アプリケーションはMicrosoft App-Vを使用して仮想デスクトップにストリーミングできます。このアプローチには、仮想デスクトップイメージが整理された状態に保たれるため、管理上の利点があります。仮想デスクトップにストリーミングされた後、アプリケーションは通常の方法でインストールされたかのようにその環境で実行されます。すべてのアプリケーションがApp-Vと互換性があるわけではありません。

ユーザーデバイスとの間のオーディオ配信

汎用HDX RealTimeは、ユーザーデバイスとの間でオーディオを配信する2つの方法をサポートしています。

- **Citrix Audio Virtual Channel**。Citrix Audio Virtual Channelはオーディオ転送専用に設計されているため、一般的に推奨されます。
- **Generic USB Redirection**。ユーザーデバイスがCitrix Virtual Apps and Desktopsサーバーへの LANまたはLANに似た接続上にある場合、ボタンまたはディスプレイ（あるいはその両方）を備えたオーディオデバイス、ヒューマンインターフェースデバイス（HID）をサポートします。

Citrix オーディオ仮想チャネル

双方向のCitrixオーディオ仮想チャネル（CTXCAM）により、オーディオをネットワーク経由で効率的に配信できます。汎用HDX RealTimeは、ユーザーのヘッドセットまたはマイクからのオーディオを取得して圧縮します。その後、ICAを介して仮想デスクトップ上のソフトフォンアプリケーションに送信します。同様に、ソフトフォンのオーディオ出力は圧縮され、逆方向にユーザーのヘッドセットまたはスピーカーに送信されます。この圧縮は、ソフトフォン自体が使用する圧縮（G.729やG.711など）とは独立しています。これは、Optimized-for-Speechコーデック（中品質）を使用して行われます。その特性は、Voice over Internet Protocolに最適です。エンコード時間が短く、ネットワーク帯域幅はピーク時で約56キロビット/秒（各方向28 Kbps）しか消費しません。このコーデックは、デフォルトのオーディオコーデックではないため、Studioコンソールで明示的に選択する必要があります。デフォルトはHDオーディオコーデック（高品質）です。このコーデックは高忠実度のステレオサウンドトラックに優れていますが、Optimized-for-Speechコーデックと比較してエンコードが遅いです。

汎用 USB リダイレクト

Citrix Generic USB Redirectionテクノロジー（CTXGUSB仮想チャネル）は、複合デバイス（オーディオとHID）およびアイソクロナスUSBデバイスを含むUSBデバイスをリモートで利用するための汎用的な手段を提供します。このアプローチは、LAN接続されたユーザーに限定されます。その理由は、USBプロトコルがネットワーク遅延に敏感であり、かなりのネットワーク帯域幅を必要とする傾向があるためです。アイソクロナスUSBリダイレクトは、一部のソフトフォンを使用する場合にうまく機能します。このリダイレクトは、優れた音声品質と低遅延を提供します。ただし、Citrix Audio Virtual Channelはオーディオトラフィックに最適化されているため、こちらが推奨されます。主な例外は、ボタン付きのオーディオデバイスを使用している場合です。たとえば、データセンターにLAN接続されたユーザーデバイスに接続されたUSB電話などです。この場合、Generic USB Redirectionは、ソフトフォンに信号を送り返すことで機能を制御する、電話機またはヘッドセットのボタンをサポートします。デバイス上でローカルに機能するボタンには問題ありません。

オーディオ診断コマンドラインツール

VDA上のオーディオ診断コマンドラインツールは、オーディオポリシー、構成、データ転送に関連するセッションデータを照会するために使用できます。

使用方法

コマンドプロンプトを開き、`C:\Program Files\Citrix\HDX\bin`フォルダーから`CtxAudio.exe`を実行します。

- 管理者としてツールを実行すると、すべてのアクティブなICAセッションのオーディオ情報が表示されます。

- 非管理者としてツールを実行すると、現在ユーザーのICAセッションオーディオ情報が表示されます。

出力

このツールは、セッション内のオーディオ関連の問題の診断に役立つさまざまな構成設定を出力します。

セクション	説明
ポリシー情報	現在のセッションに適用されているオーディオポリシー。
設定情報	レジストリに保存されているオーディオ関連の構成設定。
状態情報	現在のセッションに適用されているオーディオの状態、バージョン、コーデック、およびトランスポート。
デバイス情報	セッションで使用されているデバイス名、その役割、およびステータス。

注：

出力は、マルチセッション (TS) VDA またはシングルセッション VDA (WSVDA) のどちらでツールを実行するかによって異なります。

制限事項

クライアントにオーディオデバイスをインストールし、オーディオリダイレクトを有効にして、RDSセッションを開始します。オーディオファイルが再生に失敗し、エラーメッセージが表示されることがあります。

回避策として、RDSマシンにレジストリキーを追加し、マシンを再起動します。詳細については、レジストリで管理される機能のリストにあるオーディオの制限を参照してください。

ブラウザコンテンツリダイレクト

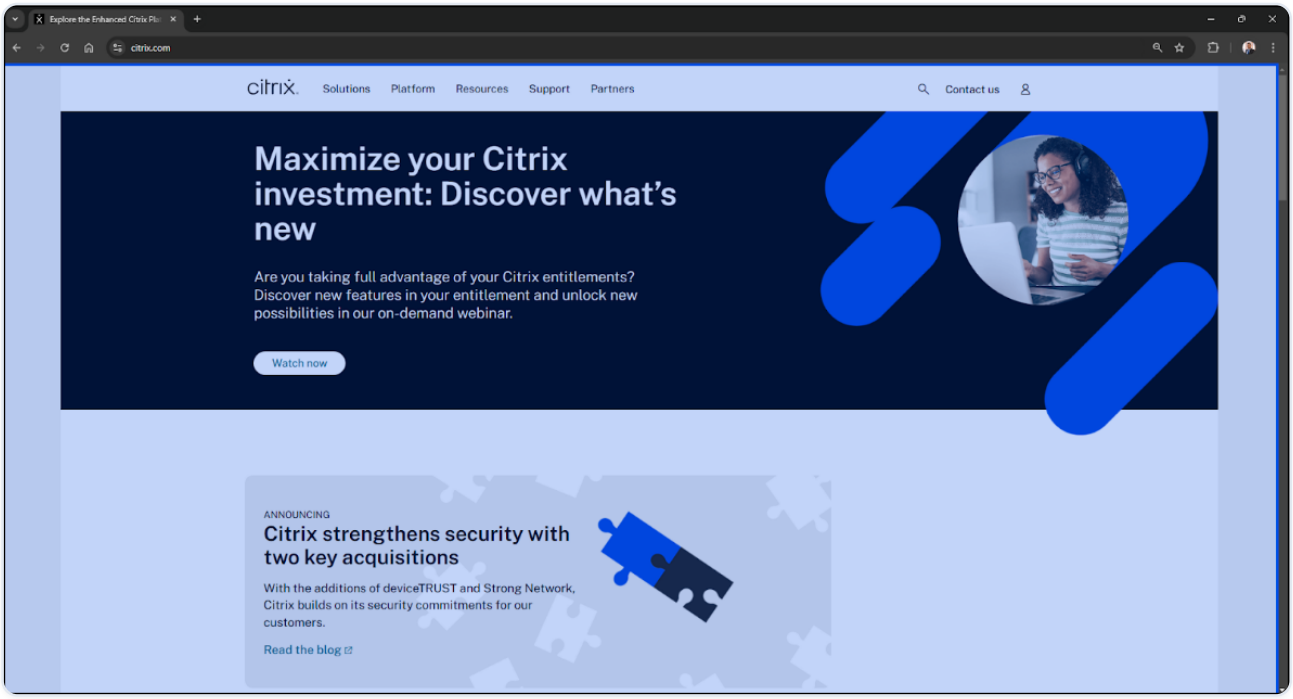
はじめに

Browser Content Redirection (BCR) は、Citrix Virtual Apps and Desktops™ 環境におけるウェブブラウジングのユーザーエクスペリエンスを向上させます。ウェブページのレンダリングをユーザーのローカルマシンにオフロードすることで、BCR はサーバーの負荷を軽減し、特に複雑なウェブサイトやリソースを大量に消費するウェブサイトのパフォーマンスを向上させます。

動作の仕組み

BCR は Citrix Workspace™ アプリを利用して、ユーザーデバイス上にセキュアなブラウジング環境を作成します。ユーザーが許可されたウェブページにアクセスすると、ブラウザウィンドウのビューポートがクライアントにリダイレクトされます。その後、クライアント側のブラウザエンジンはローカルマシンのリソースを活用してページをレンダリングし、読み込み時間の短縮とよりスムーズなインタラクションを実現します。

ブラウザのビューポートのみがリダイレクトされることに注意してください。ビューポートとは、ブラウザでコンテンツが表示される長方形の領域です。ビューポートには、アドレスバー、お気に入りツールバー、ステータスバーなどは含まれません。これらの項目はユーザーインターフェイスにあり、VDA のブラウザで引き続き実行されます。



主な利点

Browser Content Redirection はウェブトラフィックをインテリジェントに管理し、インフラストラクチャへの負担を軽減しながら、ユーザーに優れたエクスペリエンスを提供します。

組織にとってのメリットは次のとおりです。

- **コスト削減:** リソースを大量に消費するウェブページをユーザーデバイスにオフロードすることで、貴重なサーバーリソースを解放し、帯域幅の消費を削減します。これにより、ハードウェアコストとネットワークコストが削減されます。
- **ユーザーエクスペリエンスの向上:** グラフィックを多用するウェブサイトでも、よりスムーズで応答性の高いブラウジングエクスペリエンスをユーザーに提供します。ネイティブのようなパフォーマンスを提供し、遅延をなくし、生産性を向上させます。
- **セキュリティの向上:** 内部および外部リソースへのアクセスを許可しながら、セキュアな環境を維持します。
- **柔軟性の向上:** 基本的なウェブブラウジングから、プロキシトラバーサルや SSO 認証を必要とする複雑なウェブアプリケーションまで、幅広いユースケースをサポートします。Citrix Web Studio™ で詳細なポリシー制御を使用して、リダイレクト設定を簡単に管理できます。

システム要件

サーバー側コンポーネント

シトリックス バーチャル アプリ アンド デスクトップ

- 長期サービスリリース
  - 最小要件 - サポート終了していない LTSR Citrix Virtual Apps and Desktops リリース
  - 推奨されるバージョン - Citrix Virtual Apps and Desktops 2402 以降
- 現在のリリース
  - 最小要件 - サポート終了していない CR Citrix Virtual Apps and Desktops リリース
  - 推奨 - 最新のCitrix Virtual Apps and Desktopsリリース

ブラウザコンポーネント

- ブラウザ
  - マイクロソフト エッジ
  - グーグル クローム
- ブラウザリダイレクト拡張機能: ChromeとEdgeの両方のウェブストアで公開されています
- 最高のパフォーマンスを得るために、ブラウザの最新バージョンを使用することをお勧めします。

注：

- 上記で提供されている拡張機能リンクは一般提供 (GA) されており、本番レベルの展開に関連しています。GA拡張機能に加えて、CitrixはGoogle Chromeストアで特にベータ版 (GA + 1) 拡張機能も公開しています。
- Citrixは、今後のアップデートがテストされ、問題が早期に報告されるように、お客様がベータ版でテストユーザーを持つことを推奨しています。これにより、GA拡張機能が正式に展開される際にスムーズなプロセスが保証されます。
- 拡張機能のリリースは通常、Citrix Workspaceアプリのリリースと一致します

クライアント側コンポーネント

ウィンドウズ

- Windows 10 または 11
- Citrix Workspaceアプリ
  - 最小要件 - サポート終了していないCitrix Workspaceアプリ
  - 推奨
    - 長期サービスリリース - Citrix Workspaceアプリ 2402 最新CU
    - 現在のリリース - Citrix Workspaceアプリ 2405 以降

注：

- ブラウザコンテンツリダイレクトは、Citrix Workspace App Windows LTSRリリース1912および2203.1ではサポートされていません。
- ブラウザコンテンツリダイレクトに必要なクライアント側ブラウザエンジンは、Citrix Workspace Appの現行リリースではデフォルトでインストールされます。
- ブラウザコンテンツリダイレクトに必要なクライアント側ブラウザエンジンは、Citrix Workspace App 2402 LTSRリリースではデフォルトでインストールされません。管理者は、ADDLOCALスイッチを利用して、Citrix Workspace AppにBCRブラウザコンポーネントをインストールできます。

- Windows向けCitrix Workspaceアプリ2507以降、ブラウザコンテンツリダイレクト（BCR）はモジュールコンポーネントとして管理されますが、引き続きCitrix Workspaceアプリにパッケージ化されています。BCRコンポーネントはLTSRバージョンでもデフォルトでインストールされるようになり、CRとLTSRの間の一貫性が確保されます。さらに、通常のCitrix Workspaceアプリのリリースサイクル外で独立したアップデートや暫定的なパッチが必要な状況のために、スタンドアロンのBCRパッケージが公開されます。詳細については、Citrix Workspace App Windows documentationを参照してください。

詳細については、Citrix Workspaceアプリ Windowsドキュメントを参照してください。

リナックス

- Citrix Workspace アプリ
  - 最小要件 - サポート終了していないCitrix Workspace App
  - 推奨 - Citrix Workspaceアプリ 2408 以降 詳細については、Citrix Workspaceアプリ Linuxドキュメントを参照してください

注：

- Linux向けCitrix Workspaceアプリ2601以降、ブラウザコンテンツリダイレクト（BCR）はモジュールコンポーネントとして管理されます。BCRコンポーネントは引き続きLinux向けCitrix Workspaceアプリにデフォルトでパッケージ化およびインストールされ、一貫したユーザーエクスペリエンスを保証します。さらに、通常のCitrix Workspaceアプリのリリースサイクル外で独立したアップデートや暫定的なパッチが必要な状況のために、スタンドアロンのBCRパッケージが公開されます。詳細については、Citrix Workspace App Linux documentationを参照してください。

ChromeOS

- Citrix Workspace アプリ
  - Chromeウェブストアの最新バージョン

MacOS

- macOS 11 Big Sur (ビッグサー)

- macOS 12 Monterey (モントレー)
- macOS 13 Ventura (ベンチュラ)
- macOS 14 Sonoma (14.2.1まで)
- Citrix Workspace アプリ
  - 最小要件 - Citrix Workspaceアプリ 2411 以降

注：

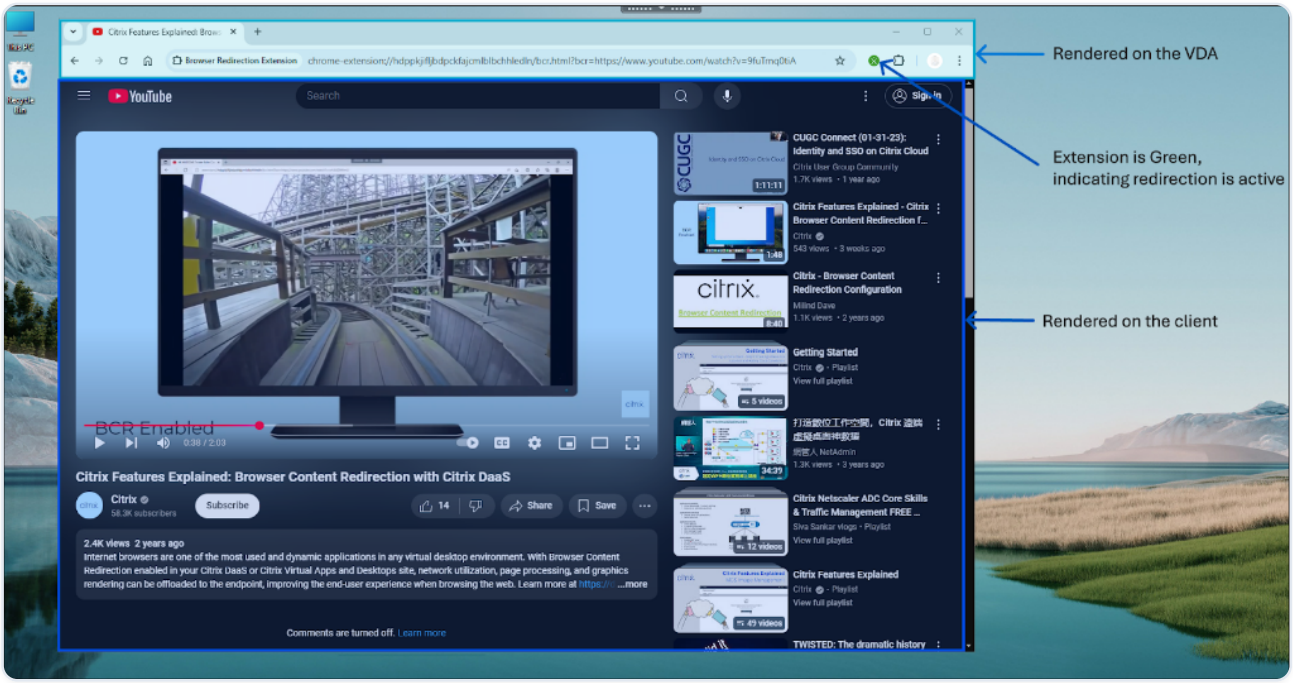
- macOSの場合、ブラウザコンテンツリダイレクトパッケージはCitrix Workspaceアプリとは独立しており、常に最新バージョンです。したがって、このパッケージは、指定された最小バージョンよりも新しい複数のCWAバージョンと互換性があります。
- Citrix Workspaceアプリ for Macへの依存がないため、ブラウザコンテンツリダイレクトのバージョン番号はCitrix Workspaceアプリ for Macのバージョンとは一致しません。
- クライアント側のブラウザエンジンはCitrix Workspaceアプリ for Macにはパッケージされていません。Mac用のクライアント側をCitrixダウンロードからダウンロードしてインストールしてください。
- IntelおよびARMパッケージは別々です。したがって、macOSエンドポイントに適したバージョンをインストールする必要があります。
- Mac版Citrix Workspaceアプリ 2511.1以降、モジュラーBCRコンポーネントはデフォルトでインストールされますが、Citrix Workspaceアプリにはパッケージ化されていません。これにより、Citrix Downloadsからコンポーネントを手動でダウンロードしてインストールする必要がなくなります。スタンドアロンのBCRパッケージは、通常のCitrix Workspaceアプリのリリースサイクル外で独立した更新や暫定パッチが必要な状況のために公開されます。詳細については、Citrix Workspaceアプリ Macドキュメントを参照してください。

設定手順

1. システム要件に従って、クライアント側およびサーバー側のコンポーネントをインストールします
   - 拡張機能の展開の詳細については、「拡張機能の展開」セクションを参照してください
2. Studioポリシーを構成します

- Web Studioポリシーは、さまざまなユースケースに合わせてブラウザコンテンツリダイレクトを構成するためのきめ細かな方法を提供します
- 基本ポリシーにより、管理者はブラウザコンテンツリダイレクトで許可/不許可にする必要があるURLを構成できます
- URLはワイルドカードを使用して構成できます

3. サポートされているWebブラウザを開き、許可されたURLに移動します
   - 許可リストで一致が見つかった場合、ウェブサイトはクライアントにリダイレクトされます
   - Citrix Workspaceアプリは、シームレスなエクスペリエンスのために、ビューポートをVDA側のブラウザにブレンドします。
4. 拡張機能のロゴの色は、コンテンツリダイレクトのステータスを示します。
   - 緑：アクティブで接続済み
   - 灰色：現在タブで非アクティブ/アイドル状態
   - 赤：破損/動作していません



> **注：**
>
> - HTML5ビデオリダイレクトとブラウザコンテンツリダイレクトは独立した機能です。この機能が動作するためにHTML5ビデオリダイレクトポリシーは必要ありません。ただ

し、Citrix HDX™ HTML5ビデオリダイレクトサービスはブラウザコンテンツリダイレクトに使用されます。

- すべての設定はWeb Studioを介して行い、レジストリキーを使用しないことをお勧めします。

構成オプション

ブラウザコンテンツリダイレクトは、さまざまな顧客環境のユースケースに合わせて構成するためのさまざまな方法を提供します。ポリシー設定の詳細については、ブラウザコンテンツリダイレクトポリシー設定を参照してください。

リダイレクトメカニズム

クライアントフェッチクライアントレンダー

デフォルトでは、ブラウザコンテンツリダイレクトはこのモードで動作します。つまり、クライアント側のブラウザエンジンがWebページに直接アクセスします。これには、クライアントネットワークからWebページへの必要なアクセスが必要です。クライアントフェッチクライアントレンダーのシナリオでは、Citrix VDAからクライアントへのネットワーク、CPU、およびRAMの使用量をすべてオフロードし、ブラウザコンテンツリダイレクトを構成する最も最適な方法です。

ポリシー構成オプション

- ブラウザコンテンツリダイレクト：許可
- ブラウザコンテンツリダイレクトACL構成
  - リダイレクトする必要があるURLを指定します。デフォルトでは、YouTubeのみがリダイレクト用に構成されているWebサイトです。
- ブラウザコンテンツリダイレクトブロックリスト構成
  - 特定URL/サブURLのリダイレクトをブロックするためのオプションの構成オプション。最大限のカスタマイズを行うには、上記のオプションと組み合わせてこのオプションを活用してください。

サーバーフェッチクライアントレンダリング

この場合、クライアント側のブラウザエンジンは、仮想チャネルを使用してVDAを介してWebサーバーからコンテンツにアクセスし、フェッチします。このオプションは、クライアントがインターネットにアクセスできない場合（シンクライアントなど）に役立ちます。VDAでのCPUとRAMの消費は少ないですが、ICA®仮想チャネルで帯域幅が消費されます。

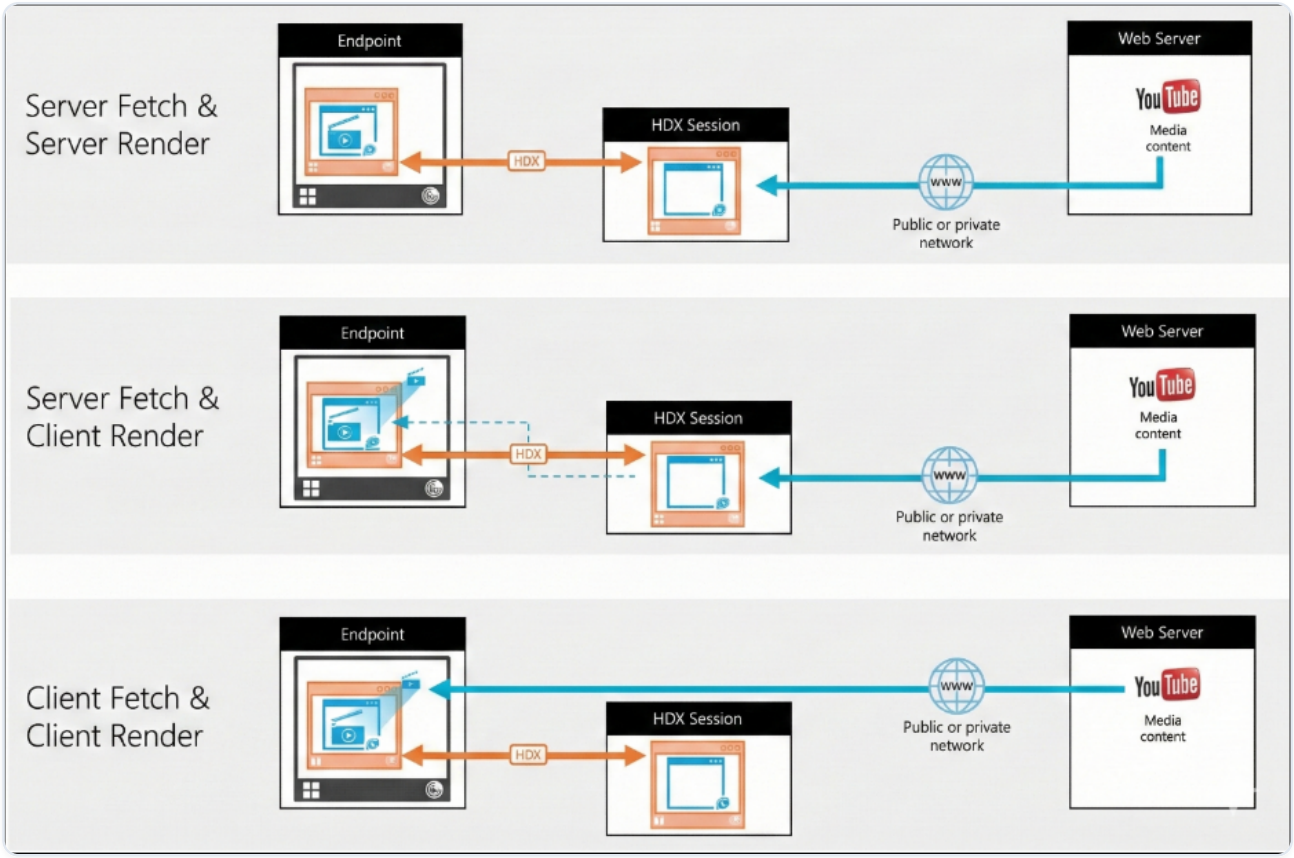
このシナリオには3つの動作モードがあります。「プロキシ」という用語は、VDAがインターネットアクセスを取得するためにアクセスするプロキシデバイスを指します。

ポリシー構成オプション

- 「クライアントフェッチクライアントレンダリング」セクションで指定されたポリシーに加えて、以下を構成します
- ブラウザコンテンツリダイレクトプロキシ構成
  - **直接または透過:** サーバーフェッチクライアントレンダリングを活用し、VDAからWebページへの直接アクセスまたは透過プロキシアクセスがある場合は、これを構成します。ポリシーにはキーワード「DIRECT」を構成する必要があります。
  - **明示的プロキシ:** サーバーフェッチクライアントレンダリングを活用し、VDAからWebページへの明示的プロキシアクセスがある場合は、これを構成します。
  - **PACファイル:** VDA内のブラウザが指定されたURLをフェッチするための適切なプロキシサーバーを自動的に選択できるPACファイルに依存している場合は、これを構成します。

フォールバックモード

クライアントリダイレクトが失敗する場合があります。たとえば、クライアントマシンがインターネットに直接アクセスできない場合、エラー応答がVDAに戻されることがあります。そのような場合、VDA上のブラウザはページを再読み込みし、サーバー上でレンダリングできます。



認証の処理

認証サイト

現在のBrowser Content Redirectionの実装では、リダイレクトメカニズムに関わらず、Browser Content Redirectionがウェブサイトへのログインを処理できるように、認証サイトを構成する必要があります。

例:

1. ブラウザコンテンツリダイレクトACL構成で`<https://www.youtube.com/>`*のみが構成されており、認証サイトが構成されていない場合、BCRはウェブサイトにサインインする際にサーバーサイドレンダリングにフォールバックし、そこで続行されます。
2. この場合、BCRが認証サイトを処理できるようにするには、`<https://www.accounts.google.com/>`* および必要に応じてIdPウェブサイトなどの他の認証サイトを構成します。各ウェブサイトのサインインは異なるため、リストに含めるようにしてください。
3. 構成されている場合、BCRは認証を処理します。例えば、クライアントフェッチクライアントレンダリングでは、シームレスなサインインエクスペリエンスのために、認証もクライアント側ブラウザエンジンから行われます。

ポリシー構成オプション

リダイレクトメカニズムのセクションで言及されているポリシーに加えて、Browser Content Redirection認証サイトポリシーを構成します。

> **注：**
>
> - BCRクライアント側ブラウザは、リダイレクトされたウィンドウが閉じられた後、クッキー（認証を含む）を永続化しません。これは、BCRウィンドウが完全に閉じられて再度開かれたときに、ウェブサイトに再ログインする必要があるという形で現れます。
> - BCRクライアント側ブラウザは、VDA側ブラウザからクッキーを読み取りません。そのため、ユーザーのパーソナライゼーションと設定はVDAブラウザと同期しません。

統合Windows認証

Browser Content Redirectionは、VDAと同じドメイン内で統合Windows認証 (IWA) とともに構成されている場合、ウェブサイトへのシームレスな認証方法を提供できます。

ポリシー構成オプション

- Browser Content Redirection統合Windows認証サポートポリシーを構成します。

シングルサインオンを有効にする前に、以下を完了してください。

- Kerberosインフラストラクチャを構成して、ホスト名から構築されたサービスプリンシパル名 (SPN) のチケットを発行します。例: HTTP/serverhostname.com。
- サーバーフェッチクライアントレンダリングの場合: サーバーフェッチモードでブラウザコンテンツリダイレクトを使用する場合は、VDAでDNSが適切に構成されていることを確認してください。
- クライアントフェッチクライアントレンダリングの場合: クライアントフェッチモードでブラウザコンテンツリダイレクトを使用する場合は、クライアントデバイスでDNSが適切に構成されており、オーバーレイからWebサーバーのIPアドレスへのTCP接続を許可していることを確認してください。

プロキシ認証

ブラウザコンテンツリダイレクトは、サーバーからコンテンツをフェッチする際に、Webプロキシへのシームレスな認証方法を提供できます。有効にすると、ブラウザコンテンツリダイレクトはKerberosサービスチケットを自動的に取得して使用し、プロキシで認証します。

ポリシー構成オプション

- ブラウザコンテンツリダイレクトのサーバーフェッチプロキシ認証ポリシーを構成します。

サーバーフェッチプロキシ認証ポリシーを有効にする前に、以下を完了してください。

- PACファイルを構成して、ダウンストリームWebプロキシ経由でトラフィックをルーティングし、プロキシがKerberos認証を使用するように設定する必要があります。

ユースケース

ブラウザコンテンツリダイレクト（BCR）は、特にリソースを大量に消費し、企業が頻繁にアクセスする幅広いWebサイトで利用できます。これには、YouTubeのようなビデオストリーミングプラットフォームが含まれ、レンダリングをエンドポイントデバイスにオフロードすることで、サーバー負荷を大幅に軽減し、コストを節約できます。さらに、BCRは、ビデオ会議やコラボレーションツール（Google Meet、Teams Web、Zoom Web）などのユニファイドコミュニケーションアプリケーションや、コンタクトセンターアプリケーション（Genesys Cloud）に最適であり、スムーズなパフォーマンスと強化されたユーザーエクスペリエンスを保証します。BCRを活用することで、企業はリソースを最適化し、さまざまなWebベースのアプリケーションで効率を向上させることができます。特定のWebサイトの設定方法については、CTX238236を参照してください。

拡張機能の展開

手動で展開

ブラウザリダイレクト拡張機能は、ChromeおよびEdgeのWebストアで公開されています。この拡張機能はVDA上のブラウザにのみ必要であり、クライアント側には必要ありません。拡張機能をインストールするには、Chrome / Edge Webストアに移動し、ブラウザリダイレクト拡張機能を検索して、それぞれのブラウザに追加します。この方法は個々のユーザーに有効です。多数のユーザーに拡張機能を展開するには、グループポリシーを使用して拡張機能を展開します。

(/en-us/citrix-daas/media/deploy-manually-bcr.png)

グループポリシーを使用した展開

前提条件

- **アクセス:** グループポリシーを構成するマシンまたはActive Directory環境で管理者権限が必要です。
- **ADMXファイル:** お使いのChromeのバージョンに対応するGoogle Chrome ADMXファイル（管理用テンプレート）をダウンロードします。これらはGoogle Chrome Enterprise Helpページで見つけることができます。
- **Edgeテンプレート:** Microsoft Edge Enterprise landingページからMicrosoft Edgeの管理用テンプレート（ADMXファイル）をダウンロードします。
- **拡張機能IDと更新URL:** Citrix Browser Content Redirection拡張機能の拡張機能IDと更新URL。

GOOGLE CHROMEの手順

1. ADMXファイルのインポート:
    - Chrome ADMX ファイルを管理用テンプレートの中央ストアにコピーします。これは通常、ドメインコントローラー上の %SystemRoot%\PolicyDefinitions です。
2. グループポリシー管理を開く:
    - グループポリシー管理コンソール (gpmc.msc) を起動します。
3. GPOを作成または編集します。
    - 新しいグループポリシーオブジェクト (GPO) を作成するか、拡張機能を展開するユーザーまたはコンピューターに適用される既存のGPOを編集します。
4. 拡張機能の設定に移動します。
    - GPOエディターで、以下に移動します。

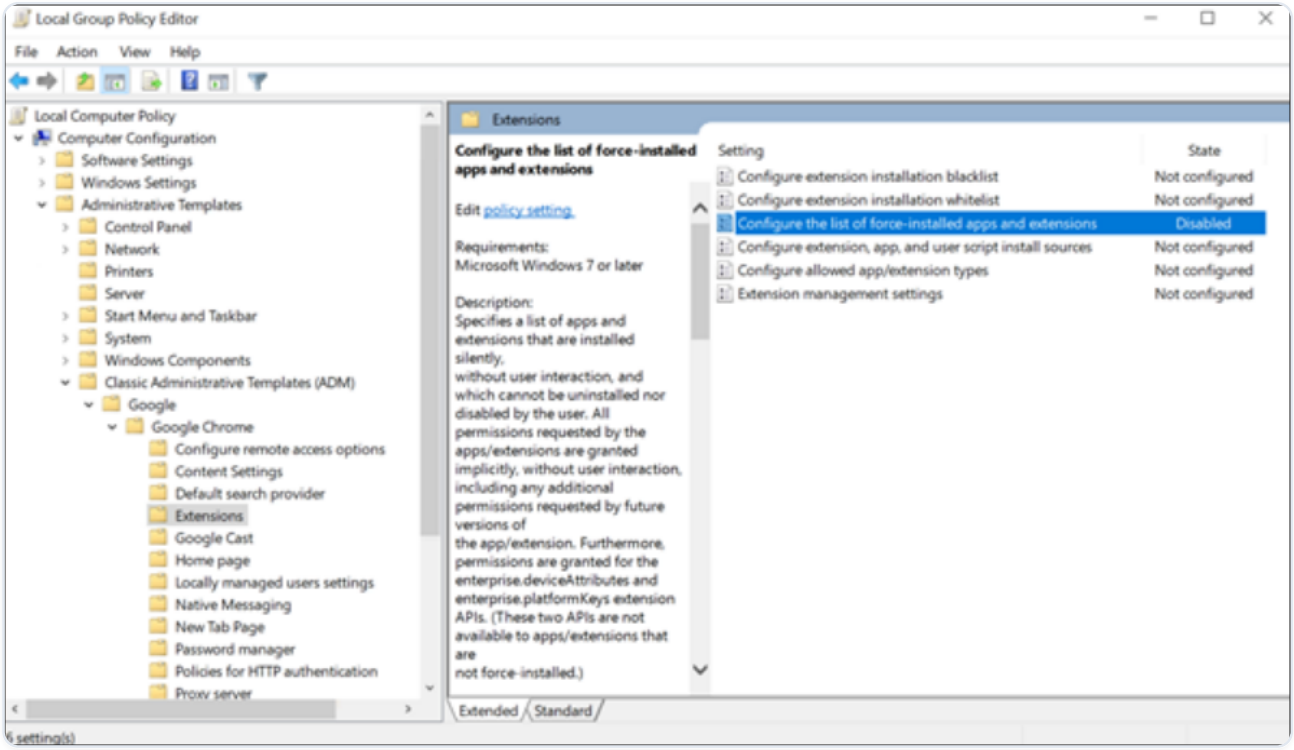
    - ユーザーの構成 > 管理用テンプレート > 従来の管理用テンプレート (ADM) > Google > Google Chrome > 拡張機能

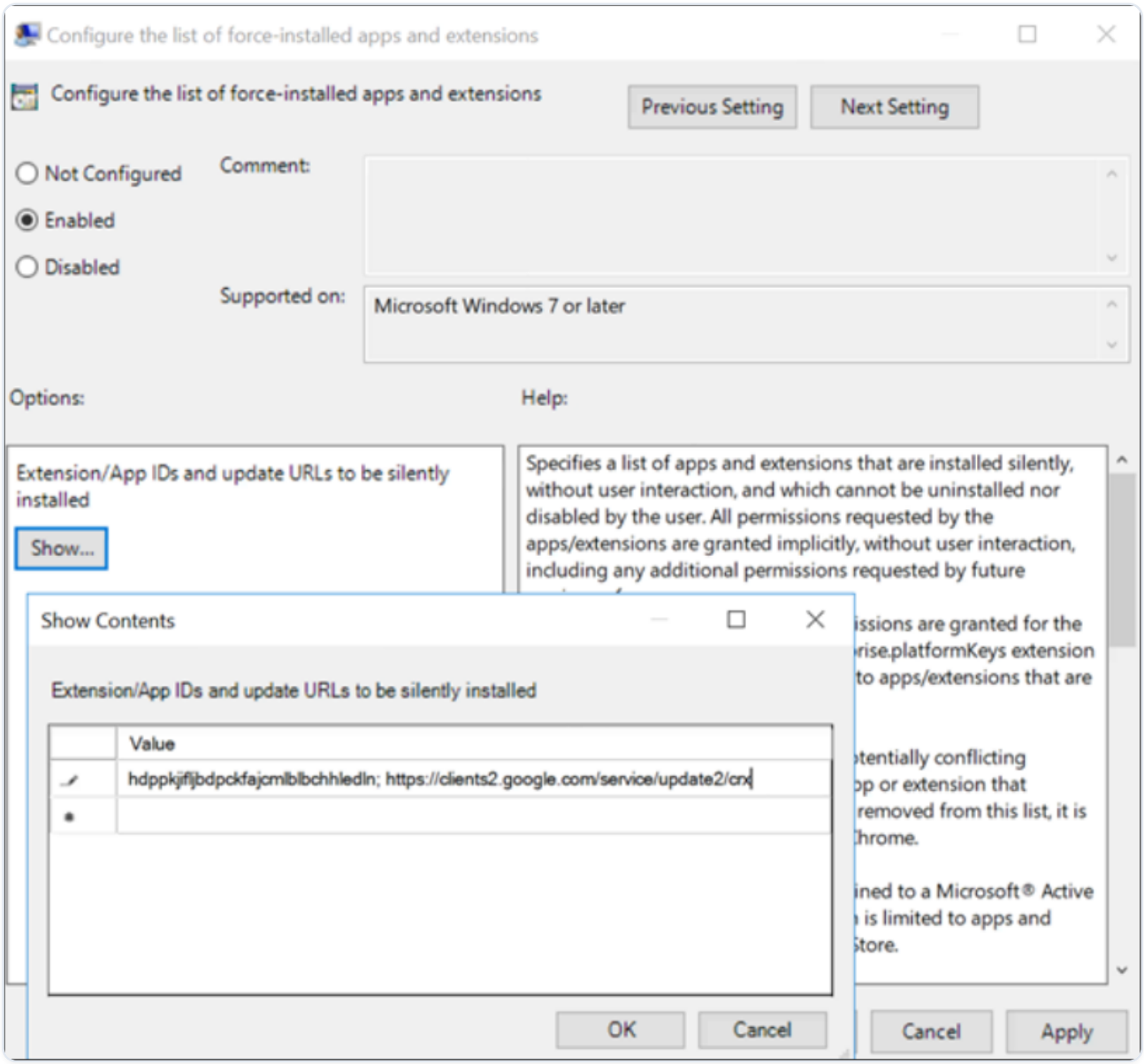
5. 「強制インストールするアプリと拡張機能のリストを構成する」を有効にします。
    - このポリシー設定をダブルクリックし、「有効」を選択します。
    - 「強制インストールするアプリと拡張機能のリストを構成する」設定が無効に設定されている場合、拡張機能はすべてのユーザーのChromeから自動的に削除されます。
6. 拡張機能IDと更新URLを追加します。
    - 「表示」ボタンをクリックします。
    - 拡張機能IDと更新URLを次の形式で入力します: <extension_id>;<update_url>
    - 値: hdppkjifljbdpckfajcmlblbchhledln; https://clients2.google.com/service/update2/crx (更新URL)
7. GPOを適用します。
    - Active Directory構造内の適切な組織単位 (OU) にGPOをリンクします。
8. グループポリシーを更新:
    - ターゲットマシンで、gpupdate /force を実行してポリシーをすぐに適用するか、ポリシーが自動的に更新されるのを待ちます。

MICROSOFT EDGE の手順

1. ADMXファイルのインポート:
    - Edge ADMXファイルを、管理用テンプレートの中央ストア (%SystemRoot%\PolicyDefinitions) にコピーします。
2. グループポリシー管理を開く:
    - グループポリシー管理コンソール (gpmc.msc) を起動します。
3. GPOを作成または編集します。
    - 新しいGPOを作成するか、既存のGPOを編集します。
4. 拡張機能の設定に移動します。
    - GPOエディターで、以下に移動します。
        - コンピューターの構成 > ポリシー > 管理用テンプレート > Microsoft Edge > 拡張機能

5. 「サイレントインストールされる拡張機能を制御する」を有効にする:
    - このポリシー設定をダブルクリックし、「有効」を選択します。
6. 拡張機能IDと更新URLを追加します。
    - 「表示」ボタンをクリックします。
    - 拡張機能IDと更新URLを次の形式で入力します: <extension_id>;<update_url>
    - 値: hdppkjifljbdpckfajcmlblbchhledln; https://clients2.google.com/service/update2/crx (更新URL)
7. GPOを適用します。
    - Active Directory構造内の適切な組織単位 (OU) にGPOをリンクします。
8. グループポリシーを更新:
    - ターゲットマシンで、gpupdate /forceを実行するか、自動更新を待ちます。





トラブルシューティング

トラブルシューティング情報については、ナレッジセンターの記事「ブラウザコンテンツリダイレクトのトラブルシューティング方法」を参照してください。

ブラウザコンテンツリダイレクトの制限事項

サーバー側の制限事項 (VDA)

ブラウザコンテンツリダイレクトは、以下のユースケースをサポートできません。記載されているシナリオまたは新しいシナリオで機能強化が必要な場合は、Citrix製品チームにお問い合わせください。

- ポップアップウィンドウは、ブラウザコンテンツリダイレクトではサポートされていません。
- セッションクッキーの永続性はサポートされていません。

- ブラウザコンテンツリダイレクトを使用している場合、HTML5ビデオのリダイレクトポリシーは無効にする必要があります。
- セッションの切断/再接続のシナリオでは、BCRを再度有効にするためにVDAブラウザウィンドウを更新する必要があります。
- BCRでリダイレクトされたウィンドウからの印刷およびファイルのダウンロードはサポートされていません。
- シークレットモードまたはプライベートブラウジングモードは、ブラウザコンテンツリダイレクトではサポートされていません。

クライアント側の制限 (CWA)

- ブラウザコンテンツリダイレクトは、ARMhfフレームワークではサポートされていません。
- BCRは、1つのブラウザで最大25個のリダイレクトされたタブ、および2つのブラウザで合計30個のリダイレクトされたタブをサポートします。

HDX™ ビデオ会議とWebカメラビデオ圧縮

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

> 仮想セッション内で実行されているアプリケーションは、HDXウェブカメラビデオ圧縮またはHDXプラグアンドプレイ汎用USBリダイレクトを使用してウェブカメラを利用できます。モードを切り替えるには、**Citrix Workspace™アプリ > 環境設定 > デバイス**を使用します。可能であれば、常にHDXウェブカメラビデオ圧縮を使用することをお勧めします。HDX汎用USBリダイレクトは、HDXビデオ圧縮とのアプリケーション互換性の問題がある場合、またはウェブカメラの高度なネイティブ機能が必要な場合にのみ推奨されます。パフォーマンスを向上させるため、CitrixはVirtual Delivery Agentに少なくとも2つの仮想CPUを搭載することを推奨します。

ユーザーがHDXウェブカメラビデオ圧縮から切り替えるのを防ぐには、**ICA®ポリシー設定 > USBデバイスポリシー**設定の下にあるポリシー設定を使用してUSBデバイスリダイレクトを無効にし

ます。Citrix Workspaceアプリのユーザーは、Desktop Viewerのマイクとウェブカメラの設定で**マイクまたはウェブカメラを使用しない**を選択することにより、デフォルトの動作を上書きできます。

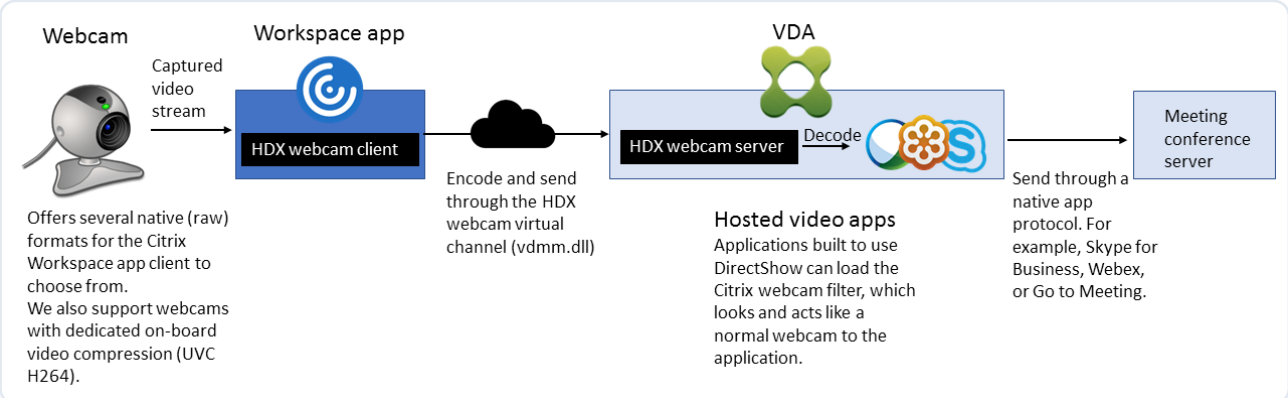
HDXウェブカメラビデオ圧縮

HDXウェブカメラビデオ圧縮は、**最適化された**ウェブカメラモードとも呼ばれます。この種類のウェブカメラビデオ圧縮は、H.264ビデオを仮想セッションで実行されているビデオ会議アプリケーションに直接送信します。VDAリソースを最適化するため、HDXウェブカメラ圧縮はウェブカメラビデオのエンコード、トランスコード、デコードを行いません。この機能はデフォルトで有効になっています。

サーバーからビデオ会議アプリへの直接ビデオストリーミングを無効にするには、VDAでレジストリキーを0に設定します。詳しくは、レジストリで管理される機能の一覧にあるウェブカメラビデオ圧縮を参照してください。

ビデオリソースをストリーミングするためのデフォルト機能を無効にすると、HDXウェブカメラビデオ圧縮は、クライアントオペレーティングシステムの一部であるマルチメディアフレームワークテクノロジーを使用して、キャプチャデバイスからのビデオをインターセプトし、トランスコードして圧縮します。キャプチャデバイスの製造元は、OSカーネルストリーミングアーキテクチャに接続するドライバーを提供します。

クライアントはウェブカメラとの通信を処理します。その後、クライアントはビデオを適切に表示できるサーバーにのみ送信します。サーバーはウェブカメラを直接処理しませんが、その統合によりデスクトップで同じエクスペリエンスが得られます。Workspaceアプリは、帯域幅を節約し、WANシナリオでの回復性を向上させるためにビデオを圧縮します。



HDXウェブカメラビデオ圧縮には、**マルチメディア会議**ポリシーを有効にする必要があります。このポリシーはデフォルトで有効になっています。

ウェブカメラがハードウェアエンコードをサポートしている場合、HDXビデオ圧縮はデフォルトでハードウェアエンコードを使用します。ハードウェアエンコードは、ソフトウェアエンコード

よりも多くの帯域幅を消費する可能性があります。ソフトウェア圧縮を強制するには、クライアントでレジストリキーを編集します。詳しくは、レジストリで管理される機能の一覧にあるウェブカメラソフトウェア圧縮を参照してください。

HDXウェブカメラビデオ圧縮の要件

HDXウェブカメラビデオ圧縮は、Citrix Workspaceアプリの次のバージョンをサポートしています。

プラットフォーム	プロセッサ
Windows版 Citrix Workspaceアプリ	Windows向けCitrix Workspaceアプリは、XenAppおよびXenDesktop 7.17以降で32ビットおよび64ビットアプリのWebカメラビデオ圧縮をサポートしています。それ以前のバージョンでは、Windows向けCitrix Workspaceアプリは32ビットアプリのみをサポートしています。
Mac向けCitrix Workspaceアプリ	Mac向けCitrix Workspaceアプリ2006以降は、XenAppおよびXenDesktop 7.17以降で64ビットアプリのWebカメラビデオ圧縮をサポートしています。それ以前のバージョンでは、Mac向けCitrix Workspaceアプリは32ビットアプリのみをサポートしています。
Linux向け Citrix Workspace アプリ	Linux向けCitrix Workspaceアプリは、仮想デスクトップ上で32ビットおよび64ビットの両方のアプリをサポートしています。
Chrome向けCitrix Workspaceアプリ	一部のARM ChromebookはH.264エンコーディングをサポートしていないため、32ビットアプリのみが最適化されたHDX Webカメラビデオ圧縮を使用できます。

Media Foundationベースのビデオアプリケーションは、Windows 8.x以降およびWindows Server 2012 R2以降でHDX Webカメラビデオ圧縮をサポートしています。詳細については、Knowledge Centerの記事CTX132764を参照してください。

その他のユーザーデバイス要件:

- サウンドを生成するための適切なハードウェア。

- DirectShow互換のWebカメラ（Webカメラのデフォルト設定を使用してください）。ハードウェアエンコーディング対応のWebカメラは、クライアント側のCPU使用率を低減します。
- HDX Webカメラビデオ圧縮の場合、可能であれば、カメラメーカーから入手したWebカメラドライバーをクライアントにインストールしてください。デバイスドライバーのインストールはサーバー上では不要です。

Webカメラによってフレームレート、明るさ、コントラストのレベルが異なります。Webカメラのコントラストを調整すると、アップストリームトラフィックを大幅に削減できます。Citrixは、初期機能検証のために以下のWebカメラを使用しています:

- Microsoft LifeCam VXモデル（2000、3000、5000、7000）
- クリエイティブ ライブ！カム オプティア プロ
- ロジクール クイックカム メッセンジャー
- ロジクール C600、C920
- HP デラックス ウェブカメラ

優先ビデオフレームレートを調整するには、クライアントでレジストリキーを編集します。詳細については、レジストリで管理される機能のリストにあるWebcam video compression frame rateを参照してください。

高解像度Webカメラストリーミング

サーバー上のビデオ会議アプリケーションは、サポートされているフォーマットタイプに基づいてWebカメラのフォーマットと解像度を選択します。セッションが開始されると、クライアントはWebカメラ情報をサーバーに送信します。アプリケーションからWebカメラを選択します。Webカメラとビデオ会議アプリケーションが高解像度レンダリングをサポートしている場合、アプリケーションは高解像度を使用します。すべてのWebカメラ解像度をサポートしています。

この機能には、Citrix Workspaceアプリ for Windows バージョン1808以降、またはCitrix Receiver for Windows バージョン4.10以降が必要です。

レジストリキーを使用して、この機能を無効または有効にできます。詳細については、レジストリで管理される機能のリストにあるHigh-definition webcam streamingを参照してください。

メディアタイプのネゴシエーションが失敗した場合、HDXはデフォルトのVGA解像度（640 x 480 ピクセル）にフォールバックします。クライアントのレジストリキーを使用して、デフォルトの解像度を構成できます。カメラが指定された解像度をサポートしていることを確認してください。詳細については、レジストリで管理される機能のリストにあるHigh-definition webcam resolutionを参照してください。

HDX Webカメラビデオ圧縮は、プラグアンドプレイの汎用USBリダイレクトと比較して帯域幅を大幅に削減し、WAN接続でも良好に機能します。帯域幅を調整するには、クライアントでレジストリキーを設定します。詳細については、レジストリで管理される機能のリストにあるHigh-definition webcam bandwidthを参照してください。

ビット/秒単位で値を入力します。帯域幅を指定しない場合、ビデオ会議アプリケーションはデフォルトで350000 bpsを使用します。

HDXプラグアンドプレイ汎用USBリダイレクト

HDXプラグアンドプレイ汎用USBリダイレクト（アイソクロナス）は、**汎用**Webカメラモードとも呼ばれます。HDXプラグアンドプレイ汎用USBリダイレクトの利点は、シンクライアント/エンドポイントにドライバーをインストールする必要がないことです。USBスタックは仮想化されており、ローカルクライアントに接続したものはすべてリモートVMに送信されます。リモートデスクトップは、ネイティブに接続したかのように動作します。Windowsデスクトップは、ハードウェアとのすべてのやり取りを処理し、プラグアンドプレイロジックを実行して正しいドライバーを見つけます。ほとんどのWebカメラは、ドライバーがサーバーに存在し、ICA経由で動作する場合に機能します。汎用Webカメラモードは、USBプロトコルで非圧縮ビデオをネットワーク経由で送信するため、大幅に多くの帯域幅（毎秒数メガビット）を使用します。

HTML5 マルチメディアリダイレクト

HTML5 マルチメディアリダイレクトは、HDX™ MediaStream のマルチメディアリダイレクト機能を拡張し、HTML5 オーディオとビデオを含みます。特にモバイルデバイスへのマルチメディアコンテンツのオンライン配信の増加により、ブラウザ業界はオーディオとビデオを提示するためのより効率的な方法を開発しました。

Flash は標準でしたが、プラグインが必要で、すべてのデバイスで動作せず、モバイルデバイスではバッテリー消費量が多くなります。YouTube、Netflix、および Mozilla、Google、Microsoft の新しいブラウザバージョンなどの企業は、HTML5 に移行しており、これが新しい標準となっています。

HTML5 ベースのマルチメディアには、独自のプラグインに比べて多くの利点があります。

- 企業に依存しない標準 (W3C)
- 簡素化されたデジタル著作権管理 (DRM) ワークフロー
- プラグインによって引き起こされるセキュリティ問題なしにパフォーマンスの向上

HTTP プログレッシブダウンロード

HTTP プログレッシブダウンロードは、HTML5 をサポートする HTTP ベースの疑似ストリーミング方式です。プログレッシブダウンロードでは、ブラウザは HTTP Web サーバーからダウンロード中に単一のファイル（単一の品質でエンコードされたもの）を再生します。ビデオは受信時にドライブに保存され、ドライブから再生されます。ビデオを再視聴する場合、ブラウザはキャッシュからビデオを読み込むことができます。

プログレッシブダウンロードの例については、HTML5 ビデオ リダイレクト テスト ページ を参照してください。ウェブページ内のビデオ要素を検査し、HTML5 ビデオタグ内のソース (mp4 コンテナ形式) を見つけるには、ブラウザの開発者ツールを使用します。

HTML5 と Flash の比較

機能	HTML5	フラッシュ
独自のプレーヤーが必要	いいえ	はい
モバイルデバイスで実行	はい	一部
さまざまなプラットフォームでの実行速度	高	低速
iOSでサポート	はい	いいえ
リソース使用量	少ない	多い
より速くロード	はい	いいえ

要件

mp4形式のプログレッシブダウンロードのリダイレクトのみをサポートしています。WebMおよびDASH/HLSのようなアダプティブビットレートストリーミング技術はサポートしていません。

以下をサポートしており、ポリシーを使用してこれらを制御します。詳細については、「マルチメディアポリシー設定」を参照してください。

- サーバー側レンダリング
- サーバーフェッチクライアントレンダリング
- クライアント側フェッチとレンダリング

Citrix Workspace™アプリおよびCitrix Receiver™の最小バージョン:

- Windows向けCitrix Workspaceアプリ1808
- シトリックス レシーバー for Windows 4.5
- シトリックス ワークスペース アプリ 1808 for Linux
- シトリックス レシーバー for Linux 13.5

最小VDAブラウザバージョン	WINDOWS オペレーティングシステム バージョン/ビルド/サービスパック
インターネット エクスプローラー 11.0	ウィンドウズ 10 x86 (1607 RS1) および x64 (1607 RS1); ウィンドウズ 7 x86 および x64; ウィンドウズ サーバー 2016 RTM 14393 (1607); ウィンドウズ サーバー 2012 R2
Firefox 47 証明書を手動でFirefoxの証明書ストアに追加するか、Windowsの信頼された証明書ストアから証明書を検索するようにFirefoxを構成します。詳細については、`https://wiki.mozilla.org/CA:AddRootToFirefox`を参照してください。	ウィンドウズ 10 x86 (1607 RS1) および x64 (1607 RS1); ウィンドウズ 7 x86 および x64; ウィンドウズ サーバー 2016 RTM 14393 (1607); ウィンドウズ サーバー 2012 R2
クローム 51	ウィンドウズ 10 x86 (1607 RS1) および x64 (1607 RS1); ウィンドウズ 7 x86 および x64; ウィンドウズ サーバー 2016 RTM 14393 (1607); ウィンドウズ サーバー 2012 R2

HTML5ビデオリダイレクトソリューションのコンポーネント

- **HdxVideo.js** - Webサイト上のビデオコマンドをインターセプトするJavaScriptフック。HdxVideo.jsは、セキュアWebSocket (SSL/TLS) を使用してWebSocketServiceと通信します。
- **WebSocket SSL証明書**
  - CA (ルート) の場合: **Citrix XenApp/XenDesktop HDX In-Product CA** (C = US; S = Florida; L = Fort Lauderdale; O = Citrix Systems, Inc.; OU = XenApp and XenDesktop Engineering; CN = Citrix XenApp and XenDesktop HDX In-Product CA) 場所: **証明書 (ローカルコンピューター) > 信頼されたルート証明機関 > 証明書**。
  - エンドエンティティ (リーフ) の場合: **Citrix XenApp/XenDesktop HDX Service** (C = US; S = Florida; L = Fort Lauderdale; O = Citrix Systems, Inc.; OU = XenApp and XenDesktop Engineering; CN = Citrix XenApp and XenDesktop HDX Service) 場所: **証明書 (ローカルコンピューター) > 個人 > 証明書**。

- **WebSocketService.exe** - ローカルシステムで実行され、SSL終端とユーザーセッションマッピングを実行します。TLS Secure WebSocketは127.0.0.1ポート9001でリッスンしています。
- **WebSocketAgent.exe** - ユーザーセッションで実行され、WebSocketServiceコマンドの指示に従ってビデオをレンダリングします。

HTML5ビデオのリダイレクトを有効にするにはどうすればよいですか?

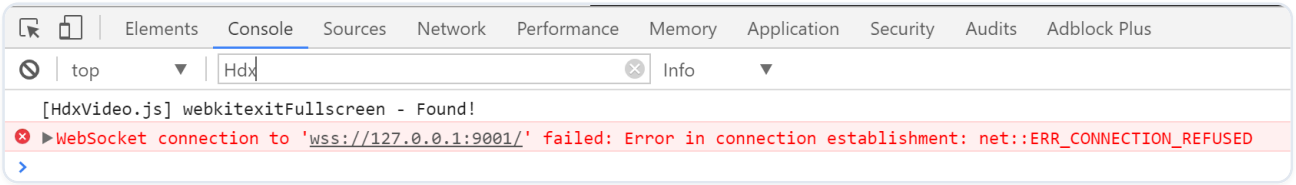
このリリースでは、この機能は制御されたWebページでのみ利用可能です。HTML5マルチメディアコンテンツが利用可能なWebページに、HdxVideo.js JavaScript（Citrix Virtual Apps and Desktopsインストールメディアに含まれています）を追加する必要があります。たとえば、社内トレーニングサイトのビデオなどです。

youtube.comのような、アダプティブビットレート技術（例: HTTP Live Streaming (HLS) および Dynamic Adaptive Streaming over HTTP (DASH)）に基づいたウェブサイトはサポートされていません。

詳細については、「*マルチメディアポリシー設定*」を参照してください。

トラブルシューティングのヒント

WebページがHdxVideo.jsを実行しようとすると、エラーが発生する可能性があります。JavaScriptの読み込みに失敗すると、HTML5リダイレクトメカニズムも失敗します。ブラウザの開発者ツールウィンドウでコンソールを検査し、HdxVideo.jsに関連するエラーがないことを確認してください。例:



Microsoft Teams の最適化 (新規)

Citrix® は、VDI 環境で Microsoft Teams のオーディオとビデオを最適化する 2 つの方法をサポートしています。Citrix HDX™ Optimization と、Microsoft が提供する Teams 用の新しい VDI ソリューションです。Classic Teams はサポート終了に達したため、このページで説明されている最適化アプローチは現在の Microsoft Teams クライアントに適用されます。

> **注：**

Microsoft は、Windows エンドポイントにおける WebRTC ベースの Citrix HDX Optimization for Microsoft Teams の非推奨化を発表しました。以下の 2 つのマイルストーンが適用されます。

- October 1, 2026 - サポート終了: Microsoft または Citrix による公式サポートは終了します。
- April 1, 2027 - 提供終了: WebRTC ベースの最適化は機能しなくなります。レガシー最適化のための Citrix Studio ポリシーは適用されなくなります。

お客様は、Teams 用の新しい VDI ソリューションへの移行をお勧めします。この変更は Windows エンドポイントのみに影響します。macOS、Linux、ChromeOS、および HTML5 エンドポイントは影響を受けません。詳細については、Microsoft Blog を参照してください。

最適化アプローチ

- **Citrix HDX Optimization (MTOP)**: Citrix と Microsoft の組み合わせソリューションで、Citrix が所有する仮想チャネル (CTXMTOP) を使用します。メディアオフロードは、Citrix Workspace™ アプリの `HdxRtcEngine` によって処理されます。このソリューションは、従来 MTOP と呼ばれています。
- **Teams 用の新しい VDI ソリューション**: Microsoft が所有および管理する新しい最適化で、Microsoft が所有する仮想チャネル (MSTEAMS、MSTEAM1、MSTEAM2) を使用します。Windows および Mac エンドポイントで利用できます。詳細については、Microsoft ドキュメントの Teams 用の新しい VDI ソリューション を参照してください。

主な違い

CITRIX HDX 最適化	TEAMS 用の新しい VDI ソリューション
最適化は、Citrix と Microsoft の組み合わせソリューションであり、Citrix が所有する仮想チャネル (CTXMTOP) を使用します。	最適化ソリューションは Microsoft が所有および管理しており、Microsoft が所有する仮想チャネル (MSTEAMS、MSTEAM1、MSTEAM2) を使用します。
メディアオフロードは、Citrix Workspaceアプリにある`HdxRtcEngine`によって処理されます。	メディアオフロードは、WindowsおよびMacエンドポイント上のSlimCoreメディアエンジンによって処理されます。

CITRIX HDX 最適化	TEAMS 用の新しい VDI ソリューション
Citrix Workspaceアプリのインストールを除き、エンドポイントに追加のコンポーネントは不要です。	追加コンポーネント - **Teams VDIプラグイン**は、さまざまな方法でエンドポイントに展開する必要があります。このプラグインは、SlimCoreメディアエンジンのダウンロードと更新を管理します。
エンドポイントプラットフォーム (Windows、macOS、Linux、ChromeOS) で利用可能です。	エンドポイントプラットフォーム (WindowsおよびMac) で利用可能です。
新機能はCitrixとMicrosoftの連携により管理されます。	新機能はMicrosoftによって管理されます。ユーザーは、Citrix HDX最適化では利用できない一部の新機能にアクセスできます。
関連するコンポーネントに応じて、CitrixとMicrosoftの両方によってサポートされます。お客様はCitrixまたはMicrosoftのいずれかにケースをオープンでき、必要に応じて適切なチームにリダイレクトされます。	Microsoftが所有し、サポートしています。Citrixは、Citrix Workspaceアプリ、仮想チャネル許可リスト、プラグイン展開メカニズムなど、関連するCitrixコンポーネントをサポートします。

相互運用性とローミング

Citrix HDX最適化とTeams向けの新VDIソリューションは並行して存在できますが、Teamsクライアントは一度にいずれか一方のみを使用します。

- Teamsアプリの起動時に、次の順序で最適化が選択されます。Teams向けの新VDIソリューション、次にCitrix HDX最適化 (WebRTC)、次に標準のオーディオ/ビデオリダイレクト。
- Teams向けの新VDIソリューションが失敗した場合、TeamsはWebRTCではなく、標準のオーディオ/ビデオリダイレクトに直接フォールバックします。選択を再実行し、適切な最適化を選択するには、Teamsアプリの再起動が必要です。
- エンドポイント間のローミングはシームレスであり、Teamsアプリの再起動は不要です。これには、Teams向けの新VDIソリューションをサポートするエンドポイントとサポートしないエンドポイントの間でユーザーがローミングする場合も含まれます。

Citrix HDX™ 最適化

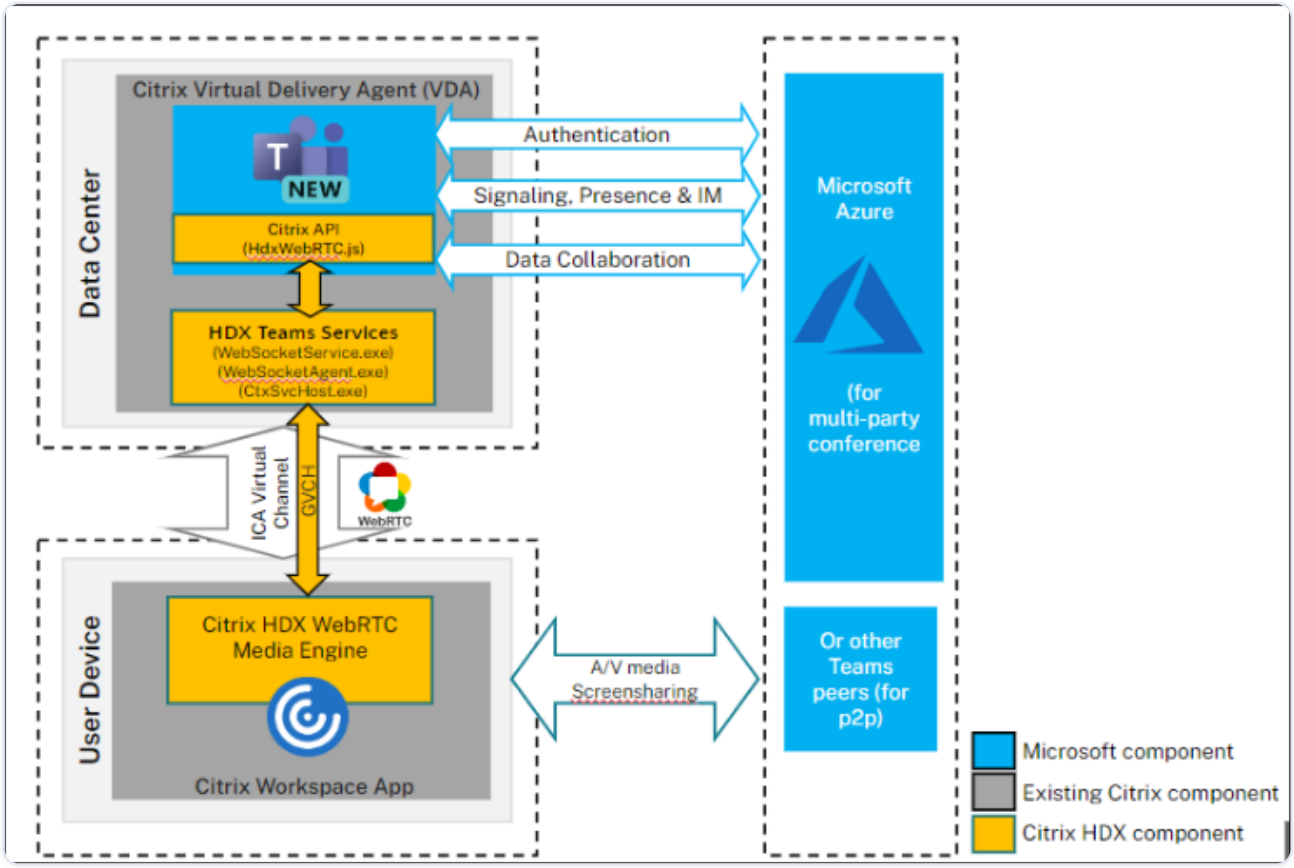
> **注：**

Microsoft は、Windows エンドポイントにおける Microsoft Teams 向け WebRTC ベースの HDX 最適化の非推奨を発表しました。2つのマイルストーンが適用されます。

- October 1, 2026 - サポート終了: Microsoft または Citrix による公式サポートは終了します
- April 1, 2027 - 提供終了: Microsoft は、Windows エンドポイント向け HDX WebRTC 最適化の非推奨を発表しました。WebRTC ベースの最適化は機能しなくなります。レガシー最適化のための Citrix Studio ポリシーは適用されなくなります。

お客様は、Microsoft Teams 向けの新 VDI ソリューション (SlimCore) への移行が推奨されます。この変更は Windows エンドポイントのみに影響し、macOS、Linux、ChromeOS、および HTML5 エンドポイントには影響しません。詳細については、Microsoft Blog を参照してください。

Citrix HDX (WebRTC 最適化) では、オフロードされたメディアの処理を担当するエンドポイント上のメディアエンジン (HdxRtcEngine) は Citrix Workspace™ アプリに組み込まれており、Citrix Workspace アプリをインストールすると、エンジンも自動的にインストールされます。



システム要件

このセクションでは、新しい Teams クライアントをサポートするために必要な最小バージョンと推奨バージョンを示します。最小バージョンでは、一部の重要なバグ修正や最新機能が利用できない場合があることに注意してください。最新の修正と機能で最高の体験を得るには、推奨バージョンを展開してください。

VDI オペレーティングシステム

詳細については、Microsoft ドキュメントに記載されている推奨事項を参照してください。

注：

- Windows Server 2016 はサポートされていません。Citrix は、それに応じてアップグレードを計画することをお勧めします。
- バージョンは頻繁に更新されるため、ここで言及されているバージョンはサポート終了となる可能性があります。したがって、さまざまなコンポーネントのサポートされているバージョンを使用していることを確認するために、Citrix Workspace app および Citrix Virtual Apps and Desktops の製品ライフサイクルページを参照してください。
- Citrix Virtual Apps and Desktops™ 1912 LTSR をご利用の場合、2024年12月にサポート終了となるため、Citrix はアップグレードを計画することをお勧めします。

仮想配信エージェント (VDA)

最小バージョン	推奨バージョン
1912 LTSR CU8+; 2203 LTSR (任意のCU); 2212 CR	2203 LTSR CU5+ (または) 2402 LTSR およびそれ以降のCRバージョン

シトリックス ワークスペース アプリ

最小バージョン	推奨バージョン
Windows 2203 LTSR (最新の累積更新プログラム); Windows 2302 CR; Linux 2207; Mac 2302; Chrome/HTML5 2301	ウィンドウズ 2402 LTSR; ウィンドウズ 2405 CR; リナックス 2405; マック 2405; クローム OS/HTML5 2405

展開

1. VDIに新しいTeamsクライアントをインストールします。詳細については、VDI向け新しいTeamsの展開を参照してください。
2. 新しいTeamsを最適化するために、VDAで以下のレジストリキーを構成します。
   - **場所**: `HKLM\SOFTWARE\WOW6432Node\Citrix\WebSocketService`
   - **キー (REG_Multi_SZ)**: `ProcessWhitelist`
   - **値**: `msedgewebview2.exe`

   > **注：**
   >
   > Citrix Virtual Apps and Desktops 2402 LTSR (または) Citrix Virtual Apps and Desktops 2203 LTSR CU5+ 以降では、`msedgewebview2.exe` レジストリエントリはデフォルトで許可リストに含まれているため、手動で構成する必要はありません。

3. Microsoft Teamsリダイレクト ポリシーが有効になっていることを確認してください。このポリシーはデフォルトで有効になっています。
4. クライアント側で追加の構成は必要ありません。ウィザードの指示に従ってCitrix Workspaceアプリをインストールしてください。

App レイヤリング

新しいMicrosoft Teamsはインストール方法が変更され、C:\Program Files\WindowsApps にインストールされるようになりました。この変更をサポートするには、App Layeringバージョン2403.2以降を実行する必要があります。この修正を含むアップグレードディスクは、App Layeringダウンロード ページからダウンロードできます。

詳細については、App Layering ドキュメントを参照してください。

Citrix プロファイル管理

New Microsoft Teams のローミングを有効にする方法については、Citrix Profile Management のドキュメントを参照してください。Citrix Profile Management の現在の最小バージョンガイダンスは 2402 LTSR (または) 2203 LTSR CU5+ です。

ネットワークに関する考慮事項

New Teams のネットワーク要件は Classic Teams と変わりません。したがって、Classic Teams ドキュメントのネットワーク要件セクションを参照してください。

機能マトリックスとバージョンサポート

バージョンは頻繁に更新されるため、ここで言及されている一部の古いバージョンはサポート終了となる可能性があります。したがって、さまざまなコンポーネントのサポートされているバージョンを使用していることを確認するために、Citrix Workspace App および Citrix Virtual Apps and Desktops の製品ライフサイクルページを参照してください。

注：

- ここで言及されているバージョンは、特定の機能がサポートされる最小バージョン、または New Teams がサポートされる最小バージョンのうち、いずれか高い方です。
- 最小バージョンセクションに記載されている Citrix Virtual Apps and Desktops 1912 LTSR CU8+ は、2024年12月にサポート終了となるため、以下の表には記載されていません。ただし、それまでは引き続きサポート対象バージョンです。
- Citrix Virtual Apps and Desktops の最小バージョンが `N/A` となっている機能は、VDA側で変更がなかったことを意味します。

機能	VDA (最小バージョン)	CITRIX WORKSPACE APP FOR WINDOWS (最小バージョン)	CITRIX WORKSPACE APP FOR MAC (最小バージョン)	CITRIX WORKSPACE APP FOR LINUX (最小バージョン)	CITRIX WORKSPACE APP FOR CHROMEOS (最小バージョン)
オーディオ/ビデオ (p2p および会議)	2203 LTSR (任意の CU)、2212 CR	2203 LTSR 最新 CU、2302 CR	2302	2207	2301
画面共有	2203 LTSR (任意の CU)、2212 CR	2203 LTSR 最新 CU、2302 CR	2302	2207	2301
i. 画面インジケーターの赤い枠線	2203 LTSR (任意の	2203 LTSR 最新 CU、2302 CR	2302	2207	いいえ

機能	VDA (最小バージョン)	CITRIX WORKSPACE APP FOR WINDOWS (最小バージョン)	CITRIX WORKSPACE APP FOR MAC (最小バージョン)	CITRIX WORKSPACE APP FOR LINUX (最小バージョン)	CITRIX WORKSPACE APP FOR CHROMEOS (最小バージョン)
	CU)、2212 CR				
ii. キャプチャを Desktop Viewerに制限	2203 LTSR (任意の CU)、2212 CR	2203 LTSR 最新 CU、2302 CR	2302	2207	いいえ
iii. マルチモニター	2203 LTSR (任意の CU)、2212 CR	2203 LTSR 最新 CU、2302 CR	2302	2207	いいえ
DTMF	該当なし	2203 LTSR 最新 CU、2302 CR	2302	2207	2301
プロキシサーバーのサポート	該当なし	2203 LTSR 最新 CU、2302 CR	2302	2207	2305
アプリ共有	2203 LTSR (任意の CU)、2212 CR	2203 LTSR 最新 CU、2302 CR	2302	2209	いいえ
ライブキャプション	該当なし	2203 LTSR 最新 CU、2302 CR	2302	2207	2303
動的e911	該当なし	2203 LTSR 最新 CU、2302 CR	2302	2207	2301

機能	VDA (最小バージョン)	CITRIX WORKSPACE APP FOR WINDOWS (最小バージョン)	CITRIX WORKSPACE APP FOR MAC (最小バージョン)	CITRIX WORKSPACE APP FOR LINUX (最小バージョン)	CITRIX WORKSPACE APP FOR CHROMEOS (最小バージョン)
制御を付与	該当なし	2203 LTSR 最新 CU、2302 CR	2302	2207	いいえ
制御を要求	該当なし	2203 LTSR 最新 CU、2302 CR	2302	2207	2303
マルチウィンドウ	2203 LTSR (任意の CU)、2212 CR	2203 LTSR 最新 CU、2302 CR	2302	2207	2303
会議の文字起こし	2203 LTSR (任意の CU)、2212 CR	2203 LTSR 最新 CU、2302 CR	2302	2207	2303
背景のぼかし	2203 LTSR (任意の CU)、2212 CR	2203 LTSR 最新 CU、2302 CR	2302	2212	2303
画面共有 (App Protection 使用時)	2203 LTSR (任意の CU)、2212 CR	2402 LTSR、2309.1 CR	2308	2311	いいえ
サイマルキャスト	2203 LTSR (任意の CU)、2212 CR	2402 LTSR、2305 CR	2305	2305	2312

機能	VDA (最小バージョン)	CITRIX WORKSPACE APP FOR WINDOWS (最小バージョン)	CITRIX WORKSPACE APP FOR MAC (最小バージョン)	CITRIX WORKSPACE APP FOR LINUX (最小バージョン)	CITRIX WORKSPACE APP FOR CHROMEOS (最小バージョン)
セカンダリリンガー	2203 LTSR (任意の CU)、2212 CR	2402 LTSR、2307.1 CR	2308	2308	2312
システムオーディオの共有	2203 LTSR (任意の CU)、2212 CR	2402 LTSR、2403 CR	2405	2402	いいえ

トラブルシューティングとその他の考慮事項

新しいTeamsについては、CTX253754、Microsoft Teamsのトラブルシューティングを参照してください。新しいTeamsに関連する最新情報については、CTX585013を参照してください。

既知の制限事項

Citrix Workspaceアプリの制限事項

- HIDサポート - 通話の応答と終了はサポートされていません。音量の上げ下げはサポートされています。
- ユーザーは、VDAでSnipping Toolを使用している間、Microsoft Teamsのコンテンツのスクリーンショットを撮ることはできません。ただし、クライアント側でSnipping Toolを使用した場合、コンテンツをキャプチャできます。
- システムオーディオ共有の制限
  - RAVEおよびBCRリダイレクトされたアプリまたはタブで画面を共有している場合、この機能を使用してオーディオを共有することはできません。
  - この機能は、公開デスクトップでのみサポートされています。

VDAに関する制限事項

- 公開された（シームレスな）アプリケーションとしての新しいTeamsはサポートされていません。
    - CVAD 2402 LTSR、2203 LTSR CU5以降で修正済み
- Citrix WorkspaceアプリのHigh DPI設定を「はい」に構成すると、リダイレクトされたビデオウィンドウがずれて表示されます。この制限は、モニターのDPIスケーリング係数が100%を超えて設定されている場合に発生します。
- Microsoft Teams 2.1は、一度に1つのWebカメラのリダイレクトのみをサポートします。ただし、シングルセッションVDAでは、複数のWebカメラのリダイレクトやプラグアンドプレイ（PnP）Webカメラのリダイレクトはサポートしていません。

Citrix WorkspaceアプリおよびVDAに関する制限

- 最適化された通話の音量は、クライアントマシンの音量バーを使用してのみ制御できます。VDA上では制御できません。

Microsoftからの制限事項の詳細については、「VDIでサポートされていない機能」を参照してください。

Teams向け新しいVDIソリューション

> **注：**
>
> Teams向け新しいVDIソリューションは、現在、Citrix®上のWindowsおよびMacエンドポイント向けに一般提供されています。このソリューションには、最小バージョンのMicrosoft Teamsが必要です。「システム要件」(#system-requirements)を参照してください。

> Teams向け新しいVDIソリューションでは、MicrosoftはCitrix Virtual Channel SDKを使用してカスタム仮想チャネルを構築します。エンドポイントでは、メディアは`HdxRtcEngine`ではなく、Microsoftメディアエンジン (SlimCore) にオフロードされます。カスタム仮想チャネルは、VDA上のTeamsとエンドポイント上のメディアエンジン間の通信を伝送します。

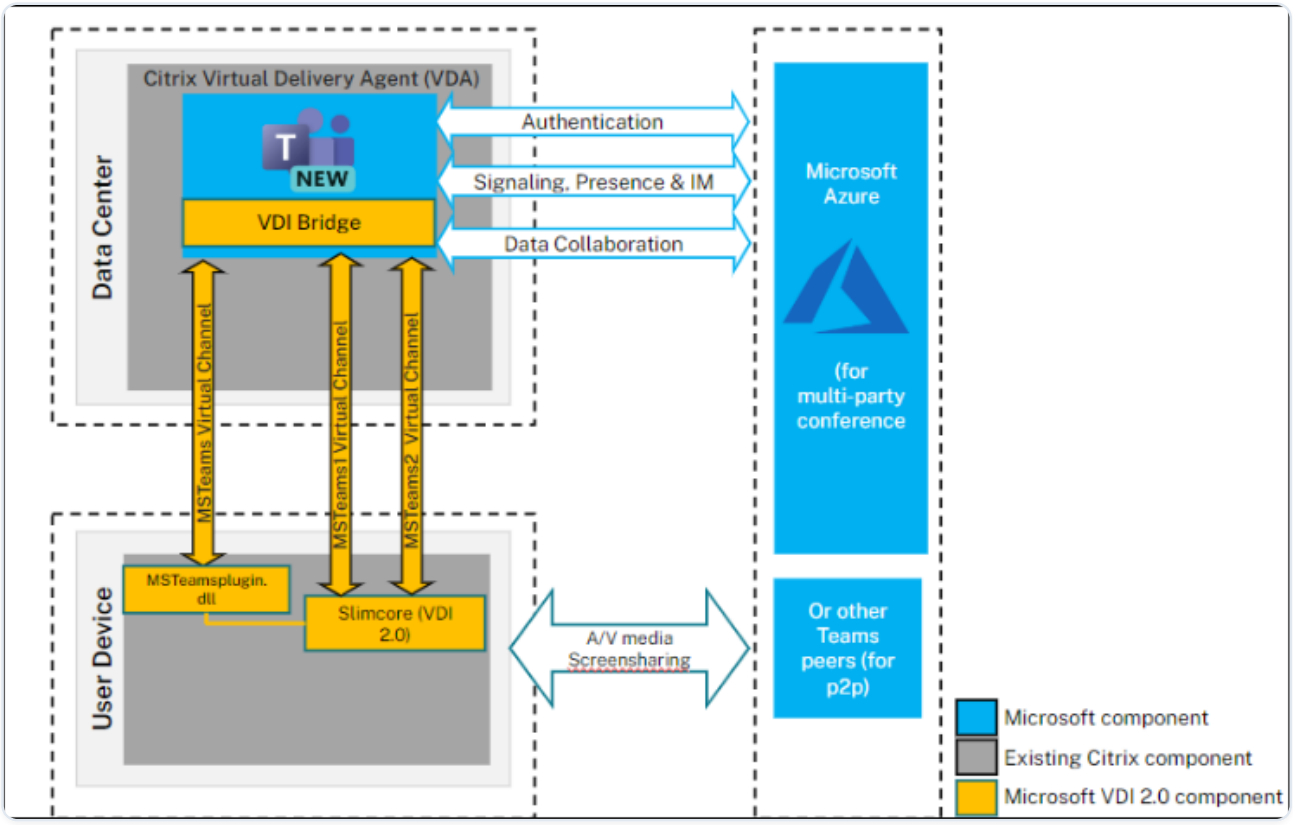
> **注：**

Microsoftは、WindowsエンドポイントにおけるWebRTCベースのCitrix HDX™ Optimization for Microsoft Teamsの廃止を発表しました。2つのマイルストーンが適用されます。

- October 1, 2026 - サポート終了: MicrosoftまたはCitrixによって公式にサポートされなくなります。
- April 1, 2027 - 提供終了: WebRTCベースの最適化は機能しなくなります。レガシー最適化用のCitrix Studioポリシーは適用されなくなります。

お客様は、Teams向け新しいVDIソリューションへの移行をお勧めします。この変更はWindowsエンドポイントのみに影響します。macOS、Linux、ChromeOS、およびHTML5エンドポイントは影響を受けません。詳細については、Microsoftブログを参照してください。

このソリューションはMicrosoftが所有および管理しています。Citrixは、関連するCitrixコンポーネント（Citrix Workspace™アプリ、仮想チャネル許可リスト、およびこのページで説明されているプラグイン展開メカニズム）をサポートします。Microsoftが所有するアーキテクチャと詳細については、MicrosoftドキュメントのTeams向け新しいVDIソリューションを参照してください。



システム要件

このセクションでは、Teams向け新しいVDIソリューションをサポートするために必要な最小バージョンと推奨バージョンを一覧表示します。最小バージョンでは、一部の重要なバグ修正や最新機能が利用できない場合があります。最良のエクスペリエンスを得るには、推奨バージョンを展開してください。

仮想配信エージェント (VDA)

> **注：**
>
> 2203 LTSR CU2以前、または2303 CR以前をご利用の場合は、これらのバージョンの制限を理解し、アップグレードを計画するためにCTX682593を参照してください。

最小バージョン	推奨バージョン
2203 LTSR CU3; 2305 CR	2203 LTSR CU5+; 2402 LTSR およびそれ以降のCR

Windows版 Citrix Workspaceアプリ

最小バージョン	推奨バージョン
2203 LTSR (最新 CU); 2302 CR	2402 LTSR; 2405 CR またはそれ以降

Mac向けCitrix Workspaceアプリ

最小バージョン	推奨バージョン
2508.10	2607 またはそれ以降

MacエンドポイントにはmacOS 14、15、または26が必要です。macOS 26では、Citrix Workspaceアプリ2511以降が必要です。Citrix Workspaceアプリ for Mac 2508.10では、プラグインを手動でインストールする必要があります。Citrix Workspaceアプリ、クライアントアプリ管理、または仮想チャネルプラグインマネージャーを介してプラグインをインストールするオプションは、Citrix Workspaceアプリ for Mac 2603以降で利用可能です。

最小Microsoft Teamsバージョン、エンドポイントOS要件、およびハードウェア要件については、Microsoftドキュメントを参照してください。

コンポーネント

- 新しいTeams `vdiBridge`: Teamsにバンドルされているサーバー側仮想チャネルモジュール。
- カスタム仮想チャネル (VC): Microsoft Teamsが所有するカスタムVC。
- プラグイン: クライアント側VC DLL。メディアエンジンのダウンロードとクリーンアップを担当します。
- メディアエンジン (SlimCore): MicrosoftによってMSIXパッケージとして提供される、オペレーティングシステム固有のメディアエンジン。

展開

1. 前提条件に記載されているMicrosoft Teamsのバージョンがあることを確認してください。
2. Microsoft Teamsの仮想チャネルを許可するように、**仮想チャネル許可リスト**ポリシーを構成します。これらのチャネルにより、Teamsクライアントはクライアント側プラグインに接続できます。詳細については、仮想チャネルセキュリティを参照してください。

   このソリューションには、3つのカスタム仮想チャネルが必要です。ワイルドカードを使用して、`ms-teams.exe`実行可能ファイルとカスタム仮想チャネルを許可します。

```
MSTEAMS,C:\Program Files\WindowsApps\MSTeams*8wekyb3d8bbwe\ms-teams.exe

MSTEAM1,C:\Program Files\WindowsApps\MSTeams*8wekyb3d8bbwe\ms-teams.exe

MSTEAM2,C:\Program Files\WindowsApps\MSTeams*8wekyb3d8bbwe\ms-teams.exe
```

注：

- VDA 2603以降では、これら3つの仮想チャネルがデフォルトで許可されます。これらのバージョンでは、Studioポリシーの構成は不要です。
- 仮想チャネル許可リストポリシーのワイルドカードは、CVAD 2203 LTSR CU2以降、またはCitrix Virtual Apps and Desktops™ 2206 CR以降で利用できます。
- ポリシーを有効にするには、VDAマシンを再起動する必要があります。
- MSTeamsのインストールパスはMSIXアプリケーションであるため変更されるため、ワイルドカードが必要です。上記に示されている正確な行を許可します。

3. このソリューションは、Citrixポリシーではなく、Microsoft Teams側のポリシーによって制御されます。デフォルトで有効になっています。特定のユーザーグループに対して有効または無効にするには、Microsoftドキュメントを参照してください。
4. エンドポイントにTeamsプラグインを展開します。Teamsプラグインをインストールするオプションを参照してください。
5. メディアエンジンのステージングと登録、およびMSIXのインストールをブロックする可能性のあるグループポリシーについては、Microsoftのドキュメントを参照してください。

Teamsプラグインをインストールするオプション

インストール方法に関わらず、プラグインはエンドポイントのCitrix Workspaceアプリの場所に配置されます。

- Windows (`MsTeamsPluginCitrix.dll`): 64ビット `C:\Program Files (x86)\Citrix\ICA Client`; 32ビット `C:\Program Files\Citrix\ICA Client`
- Mac: `/Applications/Utilities/MsTeamsVdi.Plugin.app`

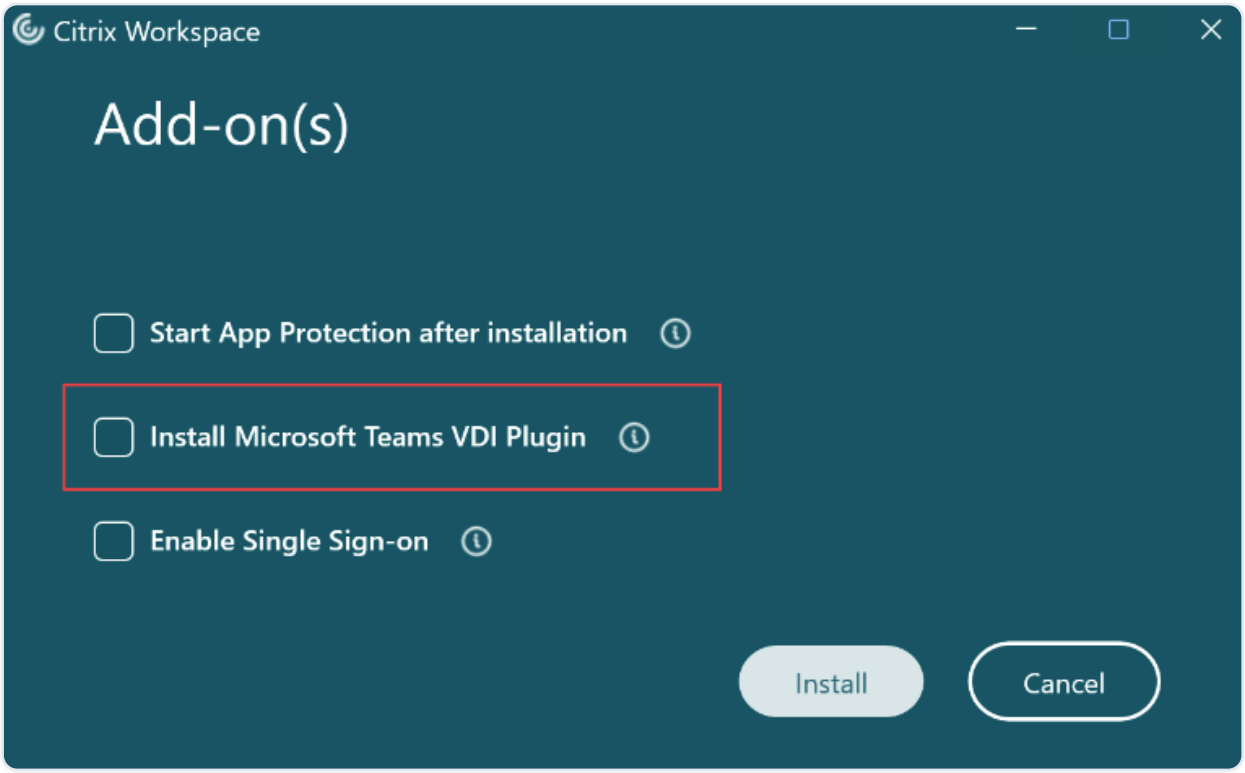
注：

- Windowsでは、仮想チャネルが正しく開くように、Citrix Workspaceアプリを管理者モードでインストールしてください。Citrix Workspaceアプリのユーザーごとのインストールはサポートされていません。
- Microsoft StoreからCitrix Workspaceアプリをインストールした場合、Microsoft Teams VDIプラグインはサポートされません。
- エンドポイントにCitrix Workspaceアプリが見つからない場合、プラグインのインストールは停止します。
- Windowsでは、プラグインとCitrix Workspaceアプリは同じアーキテクチャである必要があります。32ビットのCitrix Workspaceアプリは64ビットのプラグインをロードできません。
- プラグインはアップグレードまたは修復できますが、ダウングレードはできません。また、アクティブなセッションがない場合にのみ可能です。

オプション1: Citrix Workspaceアプリのインストールによる方法

- **Windows:** 新規インストールまたは手動アップグレード中に、**アドオン**ページで**Microsoft Teams VDIプラグインのインストール**を選択します。Citrix Workspaceアプリ for Windows

2508以降では、このオプションはデフォルトで選択されています。インストールをスキップするには、このチェックを外してください。アップグレード時には、以前の選択が記憶されます。



コマンドラインから `/InstallMSTeamsPlugin` スイッチを使用してインストールすることもできます。例えば、`CitrixWorkspaceApp.exe /InstallMSTeamsPlugin=Y` はプラグインをインストールし、`/InstallMSTeamsPlugin=N` はそれを阻止します。

新規インストールの場合、最小要件はCitrix Workspaceアプリ for Windows 2402 LTSRです。インプレースアップグレードの場合、最小要件はCitrix Workspaceアプリ for Windows 2405 CRです。最新の詳細については、サードパーティ製プラグインのインストールを参照してください。

- **Mac:** Citrix Workspaceアプリのインストール中にプラグインをインストールするオプションは、Citrix Workspaceアプリ for Mac 2603以降で利用可能であり、ユーザーによる操作が必要です。Citrix Workspaceアプリ for Mac 2607では、プラグインがデフォルトで自動的にインストールされます。Citrix Workspaceアプリ for Mac 2508.10では、プラグインを手動でインストールしてください。オプション2: プラグインを直接ダウンロードするを参照してください。

オプション2: プラグインを直接ダウンロードする

- **Windows:** MSIをダウンロードし、サポートされている任意のCitrix Workspaceアプリのバージョンに、SCCMやIntuneなどのツールを使用して展開します。
    - 32ビット版Citrix Workspaceアプリ: aka.ms/plugin

  - 64ビット版Citrix Workspaceアプリ: aka.ms/plugin_x64
  - ArmベースのCitrix Workspaceアプリ: aka.ms/plugin_arm64

- **Mac:** aka.ms/macpluginからプラグインをダウンロードし、JAMFなどのツールを使用して展開します。

オプション3: クライアントアプリ管理 (旧Global App Configurationサービス)

クライアントアプリ管理 (旧Global App Configurationサービス、またはGACS) は、管理対象および非管理対象のエンドポイントのアプリ設定を管理し、Teamsプラグインをエンドポイント全体に展開できます。Macでは、Citrix Workspaceアプリ for Mac 2603以降が必要です。Microsoft Teams VDIプラグイン管理を参照してください。

オプション4: 仮想チャネルプラグインマネージャー

仮想チャネルプラグインマネージャーは、Teams向けの新VDIソリューションを含む、エンドポイントコンポーネントを必要とするアプリケーションのために、クライアントエンドポイント全体にプラグインを展開します。VDAで実行されているアプリケーションを検出し、ユーザーにエンドポイントへのプラグインのインストールを促します。管理者はBYODシナリオでこれを使用できます。Macでは、Citrix Workspaceアプリ for Mac 2603以降が必要です。仮想チャネルプラグインマネージャーを参照してください。

プラグインの更新シナリオ

プラグインがオプション1、3、または4を通じてインストールされている場合、CitrixはTeamsプラグインの更新をシームレスに処理します。プラグインが手動でインストールされている場合 (オプション2)、Citrixは更新を処理しません。

- プラグインの自動更新のために、Citrix Workspaceアプリの自動更新がオンになっていることを確認してください。
- Citrix Workspaceアプリ for Windows 2405以降であることを確認してください。Citrix Workspaceアプリ for Windows 2508以降では、Citrix Workspaceアプリが自動更新される際にプラグインが自動的にインストールされます。
- Citrixはプラグインのアンインストールを処理しません。必要に応じて、プラグインを個別にアンインストールしてください。

> **注：**
>
> CitrixはTeamsプラグインの更新を処理しますが、メディアエンジンは処理しません。Microsoftがメディアエンジンを提供し、更新します。

Citrix公開アプリとしてのTeams

Citrix Virtual Appsアプリケーションとして公開されたTeamsは、必要なすべてのコンポーネントが最小バージョンを満たしている場合、このソリューションで最適化できます。必要なバージョンと既知の制限については、Microsoftドキュメントを参照してください。

相互運用性とローミング

Teams向けNew VDIソリューションとCitrix HDX最適化がどのように相互運用され、ローミングがどのように動作するかについては、Microsoft Teamsの最適化を参照してください。

ネットワークに関する考慮事項

Microsoftドキュメントのネットワークに関する考慮事項を参照してください。

機能サポート

機能セットと実装はMicrosoftが所有しています。Microsoftドキュメントの機能リストを参照してください。

トラブルシューティング

Microsoft Teamsクライアントは最適化ステータスを報告し、最適化が失敗した場合はエラーコードを報告します。これらのステータスインジケーターとエラーコードはMicrosoftによって定義されています。完全なリストとエンドツーエンドのトラブルシューティングについては、MicrosoftドキュメントのTeams向けNew VDIソリューションのトラブルシューティングを参照してください。

Citrix Monitorは、このソリューションの最適化状態を可視化します。セッションの詳細では、セッショントポロジビューに、アプリケーションが最適化されているかどうか、およびプラグインマネージャー、プラグインとそのバージョン、仮想チャネルの状態、仮想チャネル許可リストのステータスなど、不足しているコンポーネントが示されます。詳細については、リアルタイム通信最適化の可視性を参照してください。

一部のMicrosoftエラーコードは、Citrix側の構成を示しています。一般的なCitrixの確認事項：

- Teamsクライアントがカスタム仮想チャネルがブロックされていると報告した場合（Microsoftエラー2003）、仮想チャネル許可リストにMSTEAMS、MSTEAM1、およびMSTEAM2が含まれていることを確認してください。
- Teamsクライアントがプラグインが検出されないと報告した場合（Microsoftエラー2000）、プラグインがインストールされ、ロードされていることを確認してください。Process Explorerで`wfica32.exe`を選択し、下部ペインを表示して、DLLタブで`MsTeamsPluginCitrix.dll`を確認してください。

- Teamsクライアントがサポートされていないバージョンを報告した場合（Microsoftエラー2004）、サポートされているバージョンにアップグレードしてください。システム要件を参照してください。

既知の制限事項

機能と実装はMicrosoftが所有しています。Microsoftのドキュメントで既知の問題を参照してください。

Microsoft Teams (Classic) の最適化

> **注：**

> 新しいMicrosoft Teams 2.1がVDAで一般提供されるようになりました。このMicrosoft Teamsバージョンは、WebRTCを使用したCitrix Microsoft Teams最適化と互換性があります。新しいTeamsの最適化の詳細については、MS Teams Newを参照してください。

> Citrix Virtual Apps and Desktops 2402以降では、`msedgewebview2.exe`レジストリエントリはデフォルトで許可リストに含まれているため、手動で構成する必要はありません。

> 公開アプリケーションは、新しいMicrosoft Teamsでサポートされるようになりました。

> Citrixは、Citrix Virtual Apps and Desktops™およびCitrix Workspace™アプリを使用して、デスクトップベースのMicrosoft Teams向けに最適化を提供します。デフォルトでは、必要なすべてのコンポーネントをCitrix WorkspaceアプリとVirtual Delivery Agent (VDA) にバンドルしています。

Microsoft Teams向けのCitrixの最適化には、VDA側のHDX™サービスと、Microsoft Teamsホスト型アプリと連携してコマンドを受信するAPIが含まれています。これらのコンポーネントは、Citrix Workspaceアプリ側のメディアエンジンへの制御仮想チャネル (CTXMTOP) を開きます。エンドポイントはマルチメディアをローカルでデコードして提供し、Citrix Workspaceアプリのウィンドウをホスト型Microsoft Teamsアプリに戻します。

認証とシグナリングは、他のMicrosoft Teamsサービス (チャットやコラボレーションなど) と同様に、Microsoft Teamsホスト型アプリでネイティブに発生します。オーディオ/ビデオのリダイレクトはこれらに影響しません。

`CTXMTOP`はコマンドおよび制御仮想チャネルです。これは、Citrix WorkspaceアプリとVDAの間でメディアが交換されないことを意味します。

クライアントフェッチ/クライアントレンダリングのみが利用可能です。

このビデオデモンストレーションでは、Citrix仮想環境でMicrosoft Teamsがどのように機能するかを理解できます。

Microsoft Teamsのインストール

CitrixとMicrosoftは、Microsoft Teamsの最新バージョンを使用し、常に最新の状態に保つことを推奨しています。 現在のバージョンのリリース日から90日以上古いリリース日のMicrosoft Teamsデスクトップアプリのバージョンはサポートされていません。 サポートされていないMicrosoft Teamsデスクトップアプリのバージョンでは、ユーザーにブロックページが表示され、アプリの更新が要求されます。

最新の利用可能なバージョンについては、Microsoft Teamsアプリ（デスクトップおよびMac）の更新履歴を参照してください。

Microsoft Teamsの全ユーザー向けインストールガイドラインに従うことをお勧めします。Microsoft Teamsを`AppData`にインストールする.exeインストーラーの使用は避けてください。代わりに、コマンドラインから`ALLUSER=1`フラグを使用して`C:\Program Files (x86)\Microsoft\Teams`にインストールしてください。

```
msiexec /i <path_to_msi> /l*v <install_logfile_name> ALLUSER=1 ALLUSERS=1
```

この例では、`ALLUSERS=1`パラメーターも使用しています。このパラメーターを設定すると、Microsoft Teams Machine-Wide Installerが**コントロールパネル**の**プログラムと機能**に表示されます。また、コンピューターのすべてのユーザーのWindows設定の**アプリと機能**にも表示されます。これにより、管理者資格情報を持つすべてのユーザーがMicrosoft Teamsをアンインストールできます。

`ALLUSERS=1`と`ALLUSER=1`の違いを理解することが重要です。`ALLUSERS=1`パラメーターは、非VDI環境とVDI環境の両方で使用できます。`ALLUSER=1`パラメーターは、マシンごとのインストールを指定するためにVDI環境でのみ使用してください。

`ALLUSER=1`モードでは、新しいバージョンがリリースされてもMicrosoft Teamsアプリケーションは自動更新されません。このモードは、Windows ServerまたはWindows 10のランダム/プールされたカタログからのホスト型共有アプリやデスクトップなど、非永続的な環境に推奨されま

す。詳細については、「MSIを使用してMicrosoft Teamsをインストールする」（VDIインストールセクション）を参照してください。

Windows 10専用の永続VDI環境があるとします。Microsoft Teamsアプリケーションを自動更新し、Microsoft Teamsを`Appdata/Local`の下にユーザーごとにインストールすることを希望する場合、`.exe`インストーラーまたは`ALLUSER=1`なしのMSIを使用してください。

注：

Citrixでは、ゴールデンイメージにMicrosoft Teamsをインストールする前にVDAをインストールすることを推奨しています。このインストール順序は、`ALLUSER=1`フラグを有効にするために必要です。VDAをインストールする前に仮想マシンにMicrosoft Teamsをインストールした場合は、Microsoft Teamsをアンインストールして再インストールしてください。

Remote PC Accessの場合

Citrixでは、VDAのインストール後にMicrosoft Teamsバージョン1.4.00.22472以降をインストールすることを推奨しています。そうしないと、Microsoft TeamsがVDAを正しく検出するために、一度サインアウトして再度サインインする必要があります。バージョン1.4.00.22472以降には、VDA検出のためにMicrosoft Teamsの起動時およびサインイン時に実行される拡張ロジックが含まれています。これらのバージョンには、アクティブなセッションタイプ識別（HDX、RDP、またはクライアントマシンにローカル接続）も含まれています。ローカル接続の場合、以前のバージョンのMicrosoft Teamsでは、特定の機能やUI要素（ブレイクアウトルーム、会議やチャットのポップアウトウィンドウ、会議のリアクションなど）の検出と無効化に失敗する可能性があります。

重要:

ローカルセッションからHDXセッションにローミングし、Microsoft Teamsがバックグラウンドで開いたまま実行されている場合、HDXで正しく最適化するには、Microsoft Teamsを終了して再起動する必要があります。 逆に、最適化されたHDXセッションを介してMicrosoft Teamsをリモートで使用している場合は、HDXセッションを切断し、デバイスで同じWindowsセッションにローカルで再接続します。オフィスで作業している場合は、Microsoft TeamsがリモートPCアクセス状態（HDXまたはローカル）を正しく検出できるように、Microsoft Teamsを再起動する必要があります。これは、Microsoft TeamsがVDIモードを評価できるのはアプリ起動時のみであり、バックグラウンドで既に実行されている間は評価できないためです。再起動しないと、Microsoft Teamsはポップアウトウィンドウ、ブレイクアウトルーム、会議のリアクションなどの機能を読み込めない可能性があります。

App Layeringの場合

Citrix App Layeringを使用してVDAとMicrosoft Teamsのインストールを異なるレイヤーで管理する場合、コマンドラインから`ALLUSER=1`フラグを使用してMicrosoft Teamsをインストールする前に、Windows VDA上にレジストリキーを作成する必要があります。詳細については、「」(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/policies/reference/hdx-registry-settings.html#multimedia)の「*Citrix App Layeringを使用したMicrosoft Teamsの最適化*」セクションを参照してください。

プロファイル管理の推奨事項

Windows ServerおよびプールされたVDI Windows 10環境には、マシン全体のインストーラーを使用することをお勧めします。

コマンドラインからMSIに**ALLUSER=1**フラグ（全ユーザー向けインストーラー）が渡されると、Microsoft Teamsアプリは`C:\Program Files (x86)`（約300 MB）にインストールされます。このアプリは、ログに`AppData\Local\Microsoft\TeamsMeetingAddin`を、ユーザー固有の構成、ユーザーインターフェイス要素のキャッシュなどに`AppData\Roaming\Microsoft\Teams`（約600～700 MB）を使用します。

> **重要:**

> **ALLUSER=1**フラグを渡さない場合、MSIはTeams.exeインストーラーと`setup.json`を`C:\Program Files (x86)\Teams Installer`に配置します。レジストリキー（TeamsMachineInstaller）は`HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run`の下に追加されます。

> その後のユーザーログオンにより、代わりに**AppData**に最終インストールがトリガーされます。

マシン全体のインストーラー

以下は、Windows Server 2016 64ビットVMにMicrosoft Teamsマシンワイドインストーラーをインストールすることによって作成されるフォルダー、デスクトップショートカット、およびレジストリの例です。

フォルダー:

- `C:\Program Files (x86)\Microsoft\Teams`
- `C:\Users\<username>\AppData\Roaming\Microsoft\Teams`

デスクトップショートカット:

`C:\Program Files (x86)\Microsoft\Teams\current\Teams.exe`

レジストリ:

- `HKEY_LOCAL_MACHINE \SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run`
- `HKEY_LOCAL_MACHINE \SOFTWARE\Microsoft\Windows\CurrentVersion\Run`
- `HKEY_CURRENT_USER \SOFTWARE\Microsoft\Windows\CurrentVersion\Run`
- 名前: `Teams`
- 種類: `REG_SZ`
- 値: `C:\Program Files (x86)\Microsoft\Teams\current\Teams.exe`

> **注：**
>
> レジストリの場所は、基盤となるオペレーティングシステムとビット数によって異なります。

推奨事項

- Microsoft Teams のレジストリキーを削除して自動起動を無効にすることをお勧めします。これにより、同時に発生する多数のログオン（たとえば、勤務開始時など）によって VM の CPU 使用率が急上昇するのを防ぎます。
- 仮想デスクトップにGPU/vGPUがない場合、パフォーマンスを向上させるために、Microsoft Teamsの**設定**で**GPUハードウェアアクセラレーションを無効にする**ことをお勧めします。この設定（`"disableGpu":true`）は、`desktop-config.json`の`%Appdata%\Microsoft\Teams`に保存されます。ログオンスクリプトを使用してそのファイルを編集し、値を`true`に設定できます。
- Citrix Workspace Environment Management™ (WEM) を使用している場合は、Microsoft Teams のプロセッサ消費を管理するために **CPU スパイク保護**を有効にしてください。

ユーザーごとのインストーラー

`.exe`インストーラーを使用する場合、インストールプロセスは異なります。すべてのファイルはAppDataに配置されます。

フォルダー:

- `C:\Users\<username>\AppData\Local\Microsoft\Teams`
- `C:\Users\<username>\AppData\Local\Microsoft\TeamsPresenceAddin`
- `C:\Users\<username>\AppData\Local\Microsoft\TeamsMeetingAddin`
- `C:\Users\<username>\AppData\Local\SquirrelTemp`
- `C:\Users\<username>\AppData\Roaming\Microsoft\Teams`

デスクトップショートカット:

`C:\Users\<username>\AppData\Local\Microsoft\Teams\Update.exe --processStart "Teams.exe"`

レジストリ:

`HKEY_CURRENT_USER \SOFTWARE\Microsoft\Windows\CurrentVersion\Run`

ベストプラクティス

ベストプラクティスの推奨事項は、ユースケースシナリオに基づいています。 非永続的な設定でMicrosoft Teamsを使用する場合、効率的なMicrosoft Teamsランタイムデータ同期のためにプロファイルキャッシュマネージャーが必要です。プロファイルキャッシュマネージャーを使用すると、ユーザーセッション中に適切なユーザー固有の情報がキャッシュされます。たとえば、ユーザー固有の情報には、ユーザーデータ、プロファイル、設定が含まれます。これら2つのフォルダーのデータを同期します。

- `C:\Users\<username>\AppData\Local\Microsoft\IdentityCache`
- `C:\Users\<username>\AppData\Roaming\Microsoft\Teams`

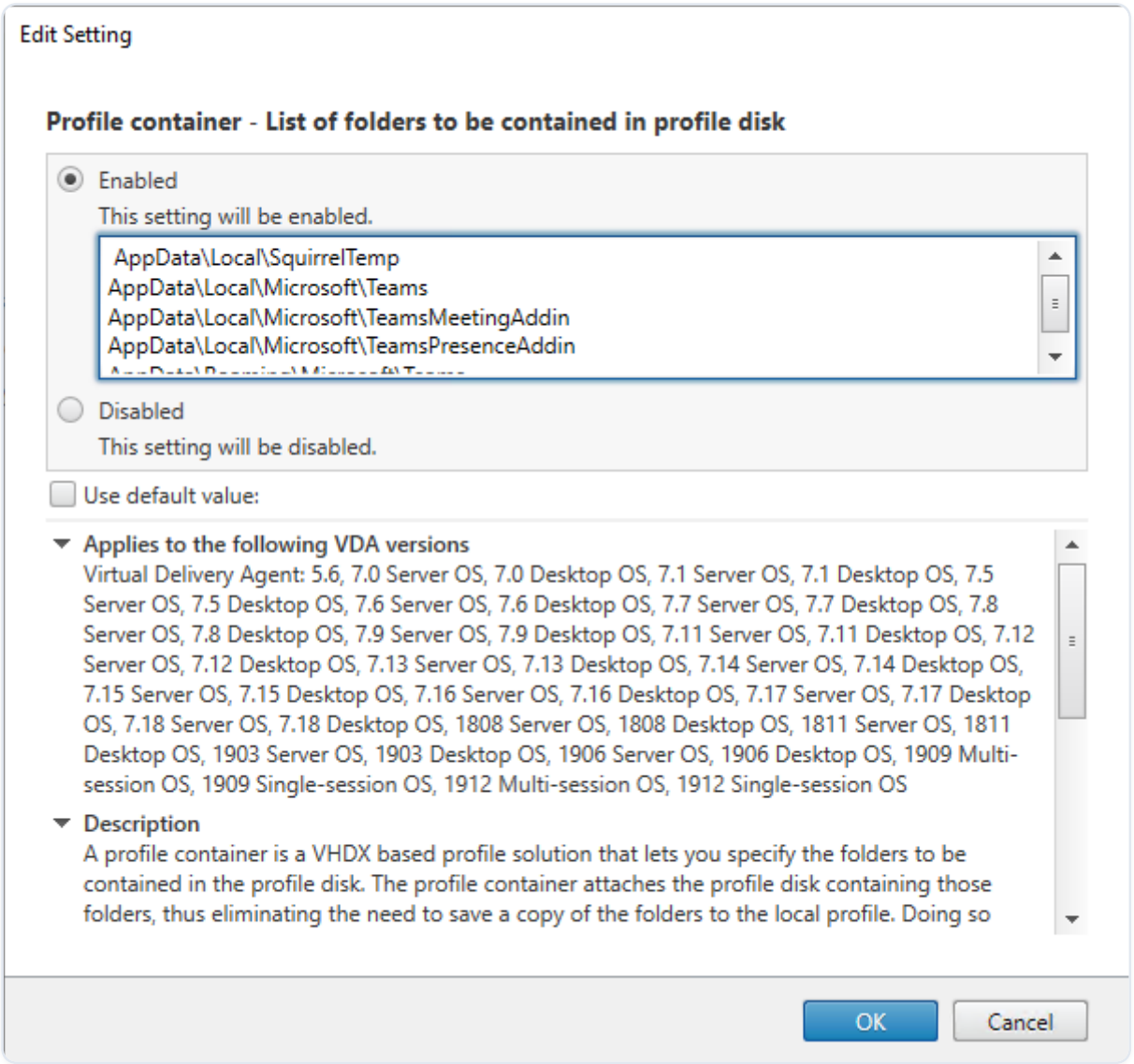
非永続的セットアップ向けの Microsoft Teams キャッシュコンテンツ除外リスト

Microsoft ドキュメントに記載されているように、Microsoft Teams のキャッシュフォルダーからファイルとディレクトリを除外します。この操作により、ユーザーのキャッシュサイズを削減し、非永続的セットアップをさらに最適化できます。

ユースケース: シングルセッションシナリオ

このシナリオでは、エンドユーザーは一度に1つの場所でMicrosoft Teamsを使用します。同時に2つのWindowsセッションでMicrosoft Teamsを実行する必要はありません。一般的な仮想デスクトップ展開では、各ユーザーに1つのデスクトップが割り当てられ、Microsoft Teamsは仮想デスクトップに1つのアプリケーションとして展開されます。 Citrix Profileコンテナを有効にし、ユーザーごとのインストーラーにリストされているユーザーごとのディレクトリをコンテナにリダイレクトすることをお勧めします。

1. ゴールデンイメージにMicrosoft Teamsのコンピューター全体インストーラー (**ALLUSER=1**) を展開します。
2. Citrix Profile Managementを有効にし、適切な権限でユーザープロファイルストアを設定します。
3. 次のProfile Managementポリシー設定を有効にします: **ファイルシステム > 同期 > プロファイルコンテナ – プロファイルディスクに含めるフォルダーのリスト。**



この構成内のすべてのユーザーごとのディレクトリをリストします。これらの設定は、Citrix Workspace Environment Management（WEM）サービスを使用して構成することもできます。

4. 設定を適切なデリバリーグループに適用します。
5. ログインして展開を検証します。

システム要件

推奨される最小バージョン - Delivery Controller (DDCs) 1906.2

以前のバージョンを使用している場合は、Microsoft Teamsの最適化を有効にするを参照してください:

サポートされているオペレーティングシステム:

- Windows Server 2022、2019、2016、2012R2 StandardおよびDatacenterエディション、ならびにServer Coreオプション

最小バージョン - Virtual Delivery Agents (VDA) 1906.2

サポートされているオペレーティングシステム:

- ウィンドウズ 11
- Windows 10 64ビット、バージョン1607以降。VMホスト型アプリは、Citrix Workspaceアプリ for Windows 2109.1以降でサポートされています。
- Windows Server 2022, 2019, 2016, および 2012 R2 (Standard および Datacenter エディション)

要件:

- BCR_x64.msi - Microsoft Teamsの最適化コードを含み、GUIから自動的に起動するMSI。VDAインストールのコマンドラインインターフェイスを使用している場合は、除外しないでください。

推奨バージョン – Citrix Workspaceアプリ for Windows最新CRおよび最小バージョン - Citrix Workspaceアプリ 1907 for Windows

- ウィンドウズ 11。
- Windows 10 (32ビットおよび64ビットエディション、Embeddedエディションを含む) (Windows 7のサポートはバージョン2006で終了しました) (Windows 8.1のサポートはバージョン2204.1で終了しました)。

- Windows 10 IoT Enterprise 2016 LTSB (v1607) および 2019 LTSC (v1809) に対応しています。
- サポートされているプロセッサ（CPU）アーキテクチャ: x86およびx64（ARMはサポートされていません）。
- エンドポイント要件: ピアツーピアのビデオ会議中に720p HD解像度をサポートできる、約2.2～2.4 GHzのデュアルコアCPU。
- デュアルコアまたはクアッドコアCPUで、ベース速度が低く（約1.5 GHz）、Intel Turbo BoostまたはAMD Turbo Coreを搭載し、少なくとも2.4 GHzまでブーストできるもの。
- 動作確認済みHPシンクライアント: t630/t640、t730/t740、mt44/mt45。
- 動作確認済みDellシンクライアント: 5070、5470 Mobile TCおよびAIO。
- 動作確認済み10ZiGシンクライアント: 4510および5810q。
- 動作確認済みエンドポイントの完全なリストについては、「シンクライアント」を参照してください。
- Citrix Workspaceアプリには、最低600 MBの空きディスク容量と1 GBのRAMが必要です。
- Microsoft .NET Frameworkの最小要件はバージョン4.8です。Citrix Workspaceアプリは、システムに.NET Frameworkが存在しない場合、自動的にダウンロードしてインストールします。

管理者は、Microsoft Teams最適化ポリシーを変更することで、最適化モードでMicrosoft Teamsを有効/無効にできます。Citrix Workspaceアプリで最適化モードで起動するユーザーは、Microsoft Teamsを無効にできません。

最小バージョン - Linux用Citrix Workspaceアプリ2006

詳しくは、Citrix WorkspaceアプリfoLinuxのドキュメントにあるMicrosoft Teamsの最適化を参照してください。

ソフトウェア:

- `GStreamer` 1.0以降またはCairo 2
- `libc++-9.0` 以降
- `libgdk` 3.22 以降
- OpenSSL 1.1.1d
- `libnsl`
- Ubuntu 20.04 以降

認証の強化:

- Libsecretライブラリ
- libunwind-12ライブラリ。詳しくは、llvm-12のlibunwind-12ライブラリ依存関係の追加を参照してください。

ハードウェア:

- ピアツーピアのビデオ会議通話中に720p HD解像度をサポートできる最小1.8 GHzデュアルコアCPU
- ベース速度1.8 GHz、Intel Turbo Boostの高速化が少なくとも2.9 GHzのデュアルコアまたはクアッドコアCPU

検証済みエンドポイントの完全なリストについては、Thin Clientsを参照してください。

詳細については、Citrix Workspaceアプリをインストールするための前提条件を参照してください。

`/opt/Citrix/ICAClient/config/module.ini`ファイルで**VDWEBRTC**フィールドの値をOffに更新することで、Microsoft Teamsの最適化を無効にできます。デフォルトはVDWEBRTC=Onです。更新が完了したら、セッションを再起動してください。(ルート権限が必要です)。

最小バージョン - Mac用Citrix Workspaceアプリ2012

サポートされているオペレーティングシステム:

- macOS カタリナ (10.15)。
- macOS Big Sur 11.0.1以降。
- macOS モントレー。

サポートされている機能:

- オーディオ
- ビデオ
- 画面共有の最適化 (送受信)

> **注：**
>
> Citrix Viewerアプリが画面共有を機能させるには、macOSの「セキュリティとプライバシー」設定へのアクセスが必要です。ユーザーは、**Appleメニュー > システム環境設定 > セキュリティとプライバシー > プライバシータブ > 画面収録**でこの設定を構成し、**Citrix Viewer**を選択します。

> Microsoft Teamsの最適化は、Citrix Workspaceアプリ2012以降およびmacOS 10.15でデフォルトで機能します。

Microsoft Teamsの最適化を無効にするには、ターミナルでこのコマンドを実行し、Citrix Workspaceアプリを再起動します。

```
defaults write com.citrix.receiver.nomas mtopEnabled -bool NO
```

最小バージョン - 最新バージョンのChromeOSで実行されているCitrix Workspaceアプリfor ChromeOSの最新バージョン

ハードウェア:

- Intel i3、クアッドコア2.4 GHzと同等以上の性能を持つプロセッサ。

サポートされている機能:

- オーディオ
- ビデオ
- 画面共有の最適化（送受信） - デフォルトでは無効になっています。有効にする方法については、これらの設定を参照してください。

シングルサーバーのスケーラビリティ

このセクションでは、単一の物理ホストでサポートできるユーザー数または仮想マシン（VM）数を推定するための推奨事項とガイダンスを提供します。これは一般にCitrix Virtual Apps and Desktopsのシングルサーバーのスケーラビリティ（SSS）と呼ばれます。Citrix Virtual Apps（CVA）またはセッション仮想化のコンテキストでは、ユーザー密度とも呼ばれます。その目的は、主要なハイパーバイザーを実行している単一のハードウェアで、いくつのユーザーまたはVMを実行できるかを明らかにすることです。

> **注：**

> このセクションには、SSSを推定するためのガイダンスが含まれています。このガイダンスは大まかなものであり、お客様固有の状況や環境に必ずしも当てはまらない場合があります。Citrix Virtual Apps and DesktopsのSSSを真に理解する唯一の方法は、Login VSIなどのスケーラビリティまたは負荷テストツールを使用することです。Citrixは、SSSを迅速に推定するためだけに、このガイダンスとこれらの簡単なルールを使用することを推奨します。た

> だし、特にハードウェアを購入したり、財務上の決定を下したりする前に、結果を検証するためにLogin VSIまたは選択した負荷テストツールを使用することをCitrixは推奨します。

ハードウェア (テスト対象システム)

- デル パワーエッジ R740
- Intel Xeon (Gold) 6126 @ 2.60 GHz (最大ターボ 3.70 GHz)、ソケットあたり 12 コア、ハイパースレッディング有効のデュアルソケット
- 382 GB の RAM
- ローカル SSD RAID 0 ストレージ (11 ディスク) 6 TB

ソフトウェア

Citrix Virtual Apps and Desktops 2106 を実行する Windows 2019 (TSVDA) を搭載した単一の仮想マシン (40 論理プロセッサ) VMware ESXi 6.7

用語

- ナレッジワーカーのワークロード: Acrobat Reader、Freemind/Java、フォトビューアー、Edge、および Excel、Outlook、PowerPoint、Word などの MS Office アプリが含まれます。
- ベースライン: ナレッジワーカーのワークロード (Microsoft Teams なし) で実行されるサーバーのスケーラビリティテスト。
- Microsoft Teams ワークロード: ナレッジワーカーの一般的なワークロード + Microsoft Teams。

Microsoft Teams のストレステスト方法

- Microsoft Teams は HDX で最適化されています。そのため、すべてのマルチメディア処理はエンドポイントまたはクライアントにオフロードされ、測定には含まれません。
- ワークロードが開始される前に、すべてのMicrosoft Teamsプロセスが停止または終了されます。
- Microsoft Teams を開く（コールドスタート）。
- Microsoft Teams がロードされ、Microsoft Teams のプライマリウィンドウがフォーカスを取得するまでにかかる時間を測定します。
- キーボードショートカットを使用してチャットウィンドウに切り替える。
- キーボードショートカットを使用してカレンダーウィンドウに切り替える。
- キーボードショートカットを使用して、特定のユーザーにチャットメッセージを送信します。

- キーボードショートカットを使用してMicrosoft Teamsウィンドウに切り替える。

結果

- ベースライン（137ユーザー）と比較して、Microsoft Teams ワークロード（81ユーザー）ではスケーラビリティに40%の影響があります。
- サーバー容量を約40%（CPUで）増やすと、ベースラインワークロードの場合と同じユーザー数に戻ります。
- ベースラインと比較して、Microsoft Teams ワークロードでは20%の追加メモリが必要です。
- ユーザーあたりのストレージサイズを512～1024 MB増やします。
- IOPS書き込みが約50%増加、IOPS読み取りが約100%増加。Microsoft Teamsは、ストレージが遅い環境では大きな影響を与える可能性があります。

機能マトリックスとバージョンサポート

機能	MICROSOFT TEAMS (最小バージョン)	VDA (最小バージョン)	WINDOWS CR 向け CITRIX WORKSPACE アプリ (最小バージョン)	CITRIX WORKSPACEアプリ FOR MAC（最小バージョン）	CITRIX WORKSPACEアプリ FOR LINUX（最小バージョン）	CITRIX WORKSPACEアプリ FOR CHROME OS（最小バージョン）
オーディオ/ビデオ (P2P および会議)	現在のバージョンから90日前	1906	1907	2009	2004	2105.5
画面共有	現在のバージョンから90日遡ったもの	1906	1907	2012	2006	2105.5
i. 画面インジケーターの赤い枠線	現在のバージョンから90日遡ったもの	1906	2002	2012	2006	いいえ

機能	MICROSOFT TEAMS (最小バージョン)	VDA (最小バージョン)	WINDOWS CR 向け CITRIX WORKSPACE アプリ (最小バージョン)	CITRIX WORKSPACEアプリ FOR MAC（最小バージョン）	CITRIX WORKSPACEアプリ FOR LINUX（最小バージョン）	CITRIX WORKSPACEアプリ FOR CHROME OS（最小バージョン）
ii. キャプチャを Desktop Viewerに制限	現在のバージョンから90日遡ったもの	1906	2009.5	2012	2006	いいえ
iii. マルチモニター	現在のバージョンから90日遡ったもの	1912 CU6+	2106 (1)	2106	2106	いいえ
DTMF	現在のバージョンから90日遡ったもの	該当なし	2102	2101	2101	2111.1
プロキシサーバーのサポート	現在のバージョンから90日遡ったもの	該当なし	2012 (2)	2104 (3)	2101 (3)	2305
アプリ共有	現在のバージョンから90日遡ったもの	2109	2109.1	2203.1	2209	いいえ
ライブキャプション	現在のバージョンから90	N/A (4)	2109.1	2109	2109	2303

機能	MICROSOFT TEAMS (最小バージョン)	VDA (最小バージョン)	WINDOWS CR 向け CITRIX WORKSPACE アプリ (最小バージョン)	CITRIX WORKSPACEアプリ FOR MAC（最小バージョン）	CITRIX WORKSPACEアプリ FOR LINUX（最小バージョン）	CITRIX WORKSPACEアプリ FOR CHROME OS（最小バージョン）
	日遡ったもの					
動的e911	現在のバージョンから90日遡ったもの	該当なし	2112.1	2112	2112	2112
制御を付与	現在のバージョンから90日遡ったもの	該当なし	2112.1	2203.1	いいえ	いいえ
制御を要求	現在のバージョンから90日遡ったもの	該当なし	2112.1	2203.1	2203	2303
マルチウィンドウ	1.5.00.11865	2112, 1912 CU6 (5)	2112.1	2203.1	2203	2303
会議の文字起こし	現在のバージョンから90日遡ったもの	2112.1, 1912 CU6+	2112	2203.1	2203	2303
背景ぼかし	現在のバージョンから90	2112, 1912 CU6+	2207	2301	2212	2303

機能	MICROSOFT TEAMS (最小バージョン)	VDA (最小バージョン)	WINDOWS CR 向け CITRIX WORKSPACE アプリ (最小バージョン)	CITRIX WORKSPACEアプリ FOR MAC（最小バージョン）	CITRIX WORKSPACEアプリ FOR LINUX（最小バージョン）	CITRIX WORKSPACEアプリ FOR CHROME OS（最小バージョン）
	日遡ったもの					

1. CD Viewerは全画面モードのみ。SHIFT+F2はサポートされていません。
2. Negotiate/Kerberos、NTLM、Basic、およびDigest。`Pac`ファイルもサポートされています。
3. 匿名のみ。
4. VDAが2112以降の場合、ライブキャプションは、Citrix WorkspaceアプリのバージョンがMac用2203.1、Linux用2203、またはWindows用2112の場合にのみ機能します。これは、Microsoft Teamsがシングルウィンドウ UIモードまたはマルチウィンドウモードの場合、ライブキャプションの動作が異なるためです。
5. マルチウィンドウは2112 VDAで導入されましたが、VDA 1912 LTSR CU6リリースにバックポートされました。

注：

- **Citrix Workspace app for Windows 1912 CU6 (またはそれ以降)**に記載されているすべての機能は、Citrix Workspace app for Windows 2203.1 LTSR CU1に適用されます。
- Microsoftは、Microsoft Teamsにおけるシングルウィンドウモードのサポートを非推奨としました。これに対応するため、VDAを1912 CU6+ LTSRに、Citrix Workspaceアプリを2203 CU2+以降にアップグレードする必要があります。これらはマルチウィンドウモードをサポートしています。

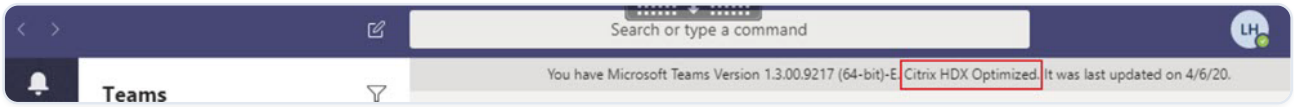
Microsoft Teamsの最適化を有効にする

Microsoft Teamsの最適化を有効にするには、Microsoft Teams redirectionポリシーで説明されている管理コンソールポリシーを使用します。このポリシーはデフォルトで**ON**になっています。このポリシーが有効になっていることに加えて、HDXはCitrix Workspaceアプリのバージョンが少なくとも必要な最小バージョンであることを確認します。ポリシーを有効にし、Citrix Workspaceアプ

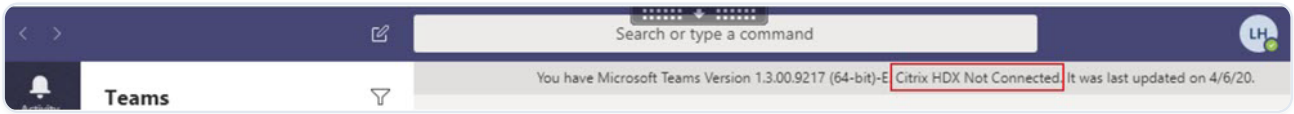
リのバージョンがサポートされている場合、VDAで**HKEY_CURRENT_USER\Software\Citrix\HDXMediaStream\MSTeamsRedirSupport**が自動的に**1**に設定されます。Microsoft Teamsは、VDIモードでロードするためにこのキーを読み取ります。

> **注：**
>
> バージョン1906.2以降のVDA、またはManageコンソール（Studio）でポリシーが利用できない古いコントローラーバージョン（バージョン7.15など）を使用している場合でも、VDAを最適化できます。Microsoft TeamsのHDX最適化は、VDAでデフォルトで有効になっています。

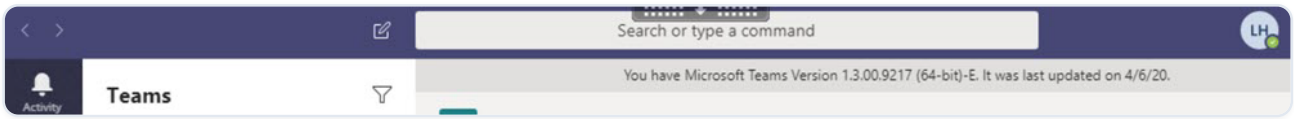
About > Versionをクリックすると、**Citrix HDX Optimized**の凡例が表示されます。



Citrix HDX Not Connectedと表示される場合、Citrix APIはMicrosoft Teamsにロードされています。APIのロードはリダイレクトへの最初のステップです。しかし、スタックの後続の部分でエラーが発生しています。このエラーは、VDAサービスまたはCitrix Workspaceアプリにある可能性が最も高いです。



凡例が表示されない場合、Microsoft TeamsはCitrix APIの読み込みに失敗しました。通知領域のアイコンを右クリックしてMicrosoft Teamsを終了し、再起動してください。管理コンソールポリシーが**Prohibited**に設定されておらず、Citrix Workspaceアプリのバージョンがサポートされていることを確認してください。



> **重要: セッションの再接続**

- 接続性が変更された場合、HDX最適化セッションを取得するためにMicrosoft Teamsを再起動する必要がある場合があります。たとえば、サポートされていないエンドポイント（iOS、Android、またはWindows/Linux/Macの古いバージョンのWorkspaceアプリ）か

らサポートされているエンドポイント（Windows/Linux/Mac/ChromeOS/HTML5のWorkspaceアプリ）にローミングする場合、またはその逆の場合です。

- VDAにMicrosoft Teamsの.exeインストーラーを使用してアプリをインストールした場合も、Microsoft Teamsの再起動が必要です。.exeインストーラーは、永続的なVDI展開に推奨されます。このような場合、HDXセッションが切断状態にある間にMicrosoft Teamsが自動更新されることがあります。そのため、HDXセッションに再接続するユーザーは、Microsoft Teamsが最適化されて実行されていないことに気づくでしょう。
- ローカルセッションからHDXセッションにローミングする場合、HDXで最適化するためにMicrosoft Teamsを再起動する必要があります。この操作は、Remote PC Accessシナリオで必要です。

ネットワーク要件

Microsoft Teamsは、会議や多人数通話のためにMicrosoft 365のメディアプロセッササーバーに依存しています。また、Microsoft Teamsは、以下のシナリオでMicrosoft 365トランスポートリレーに依存しています。

- ポイントツーポイント通話の2つのピアが直接接続されていない
- 参加者がメディアプロセッサに直接接続されていない。

したがって、ピアとMicrosoft 365クラウド間のネットワークの状態が通話のパフォーマンスを決定します。ネットワーク計画に関する詳細なガイドラインについては、Microsoft 365 network connectivity principlesを参照してください。

クラウド音声およびビデオの全体的な展開に影響を与える可能性のあるリスクと要件を特定するために、環境を評価することをお勧めします。 ネットワークがMicrosoft Teamsに対応しているかテストするには、Skype for Business Network Assessment Toolを使用してください。サポート情報については、Supportを参照してください。

Real Time Protocol (RTP) トラフィックに関する主要なネットワーク推奨事項の概要

- 支社からMicrosoft 365ネットワークにできるだけ直接接続します。
- 支社で十分な帯域幅を計画し、提供します。
- 各支社のネットワーク接続と品質を確認します。
- 支店で以下のいずれかを使用する必要がある場合は、RTP/UDPトラフィック（Citrix WorkspaceアプリのHdxRtcEngine.exeによって処理される）が妨げられないことを確認してください。

- プロキシサーバーをバイパスする
- ネットワークSSLインターセプト
- ディープパケットインスペクションデバイス
- VPNヘアピン（可能であればスプリットトンネリングを使用）

重要: VPNスプリットトンネル構成

HdxRtcEngine.exeのトラフィックはVPNトンネルから迂回させ、ユーザーのローカルインターネット接続を使用してサービスに直接接続できるようにする必要があります。これを実現する方法は、使用するVPN製品とマシンプラットフォームによって異なりますが、ほとんどのVPNソリューションでは、このロジックを適用するための簡単なポリシー設定が可能です。VPNプラットフォーム固有の分割トンネルガイダンスの詳細については、このMicrosoftの記事を参照してください。

WorkspaceアプリのWebRTCメディアエンジン（HdxRtcEngine.exe）は、クライアントにオフロードされるマルチメディアストリームにSecure Real-time Transport Protocol (SRTP) を使用します。SRTPはRTPに機密性と認証を提供します。この機能では、AES暗号化方式を使用してメディアおよび制御メッセージを暗号化するために、対称鍵（DTLSとネゴシエートされる）が使用されます。

良好なユーザーエクスペリエンスのために、以下のメトリックが推奨されます。

メトリック	エンドポイントからMICROSOFT 365まで
遅延 (片道)	< 50 ミリ秒
遅延 (RTT)	< 100 ミリ秒
パケット損失	15秒間隔で1%未満
パケット到着間隔ジッター	15秒間隔で30ミリ秒未満

詳細については、Microsoft Teams 用に組織のネットワークを準備するを参照してください。

帯域幅要件については、Microsoft Teams の最適化では、オーディオ (OPUS/G.722/PCM G711) およびビデオ (H264) 用にさまざまなコーデックを使用できます。

ピアは、セッション記述プロトコル (SDP) Offer/Answer を使用して、通話確立プロセス中にこれらのコーデックをネゴシエートします。 Citrix のユーザーあたりの最小推奨事項は次のとおりです。

タイプ	帯域幅	コーデック
音声 (双方向)	約 90 kbps	G.722
音声 (双方向)	約 60 kbps	オーパス*
ビデオ (双方向)	約 700 kbps	H264 360p で 30 fps 16:9
画面共有	約 300 kbps	H264 1080p、15フレーム/秒

* Opusは、6 kbpsから510 kbpsまでの定ビットレートおよび可変ビットレートエンコーディングをサポートしています。

OpusとH264は、ピアツーピアおよび電話会議に推奨されるコーデックです。

> **重要:**

> パフォーマンスについてですが、クライアントマシンでのCPU使用量に関して、エンコードはデコードよりもコストがかかります。LinuxおよびWindows版Citrix Workspaceアプリで、最大エンコード解像度をハードコードできます。「エンコーダーパフォーマンス見積もり」および「Microsoft Teamsの最適化」を参照してください。

プロキシサーバー

プロキシの場所に応じて、以下を考慮してください。

- VDAでのプロキシ構成:

  VDAで明示的なプロキシサーバーを構成し、localhostへの接続をプロキシ経由でルーティングすると、リダイレクトは失敗します。プロキシを正しく構成するには、 **> > >** で 設定を選択し、 `127.0.0.1:9002` をバイパスする必要があります。

  PACファイルを使用する場合、PACファイルからのVDAプロキシ構成スクリプトは、 `wss://127.0.0.1:9002` に対して **DIRECT** を返す必要があります。そうでない場合、最適化は失敗します。スクリプトが **DIRECT** を返すことを確認するには、 `shExpMatch(url, "wss://127.0.0.1:9002/*")` を使用します。

- Citrix Workspaceアプリでのプロキシ構成:

  支社がプロキシ経由でインターネットにアクセスするように構成されている場合、以下のバージョンがプロキシサーバーをサポートします。

  - Citrix Workspaceアプリ for Windowsバージョン2012 (Negotiate/Kerberos、NTLM、Basic、Digest。`Pac`ファイルもサポートされています)
  - Citrix Workspaceアプリ for Windowsバージョン1912 CU5 (Negotiate/Kerberos、NTLM、Basic、Digest。`Pac`ファイルもサポートされています)
  - Citrix Workspaceアプリ for Linuxバージョン2101 (匿名認証)
  - Citrix Workspaceアプリ for Macバージョン2104 (匿名認証)

以前のバージョンのCitrix Workspaceアプリを搭載したクライアントデバイスは、プロキシ構成を読み取ることができません。これらのデバイスは、トラフィックをMicrosoft 365 TURNサーバーに直接送信します。

重要:

- クライアントデバイスがDNS解決を行うためにDNSサーバーに接続できることを確認してください。クライアントデバイスは、以下のMicrosoft Teamsリレーサーバーの FQDNを解決できる必要があります。
  - `worldaz.relay.teams.microsoft.com`
  - `inaz.relay.teams.microsoft.com`
  - `uaeaz.relay.teams.microsoft.com`
  - `euaz.relay.teams.microsoft.com`
  - `usaz.relay.teams.microsoft.com`
  - `turn.dod.teams.microsoft.us`
  - `turn.gov.teams.microsoft.us`

DNS要求が失敗した場合、外部ユーザーとのP2P通話およびメディア確立を伴う会議通話は失敗します。

- 会議サーバーの場所は、最初の参加者の仮想デスクトップの場所に基づいて選択されます（クライアントではありません）。

通話の確立とメディアフローパス

可能な場合、Citrix WorkspaceアプリのHDX WebRTCメディアエンジン（HdxRtcEngine.exe）は、ピアツーピア通話でユーザーデータグラムプロトコル（UDP）を介した直接ネットワークのセキュアリアルタイムトランスポートプロトコル（SRTP）接続を確立しようとします。UDPハイポートがブロックされている場合、メディアエンジンはTCP/TLS 443にフォールバックします。

HDXメディアエンジンは、候補の検出と接続の確立のために、ICE、NAT用セッショントラバーサルユーティリティ（STUN）、およびNAT周辺リレーを使用したトラバーサル（TURN）をサポートしています。このサポートは、エンドポイントがDNS解決を実行できる必要があることを意味します。

2つのピア間、またはピアと会議サーバー間に直接パスがなく、多人数通話または会議に参加しているシナリオを考えてみましょう。HdxRtcEngine.exeは、Microsoft 365のMicrosoft Teamsトランスポートリレーサーバーを使用して、他のピアまたは会議がホストされているメディアプロセッサに到達します。クライアントマシンは、3つのMicrosoft 365サブネットIPアドレス範囲と4つのUDPポート（UDPがブロックされている場合はフォールバックとしてTCP/TLS 443）にアクセスできる必要があります。詳細については、通話設定 および Office 365 URLとIPアドレス範囲 ID 11 のアーキテクチャ図を参照してください。

ID	カテゴリ	アドレス	宛先ポート
11	最適化が必要	13.107.64.0/18, 52.112.0.0/14, 52.122.0.0/15	**UDP:** 3478, 3479, 3480, 3481, **TCP:** 443 (フォールバック)

これらの範囲には、トランスポートリレーとメディアプロセッサの両方が含まれており、Azure Load Balancerによってフロントエンドされています。 Microsoft Teamsトランスポートリレーは STUNおよびTURN機能を提供しますが、ICEエンドポイントではありません。また、Microsoft Teamsトランスポートリレーはメディア、TLSを終端したり、トランスコーディングを行ったりしません。他のピアまたはメディアプロセッサにトラフィックを転送する際に、TCP（HdxRtcEngine.exeがTCPを使用する場合）をUDPにブリッジできます。

WorkspaceアプリのWebRTCメディアエンジンは、Microsoft 365クラウド内で最も近いMicrosoft Teamsトランスポートリレーに接続します。メディアエンジンは、エニーキャストIPとポート3478～3481 UDP（ワークロードごとに異なるUDPポートですが、多重化が発生する可能性があります）、またはフォールバックとして443 TCP/TLSを使用します。通話品質は基盤となるネットワークプロトコルに依存します。UDPは常にTCPよりも推奨されるため、ブランチオフィスでUDPトラフィックに対応できるようにネットワークを設計することをお勧めします。

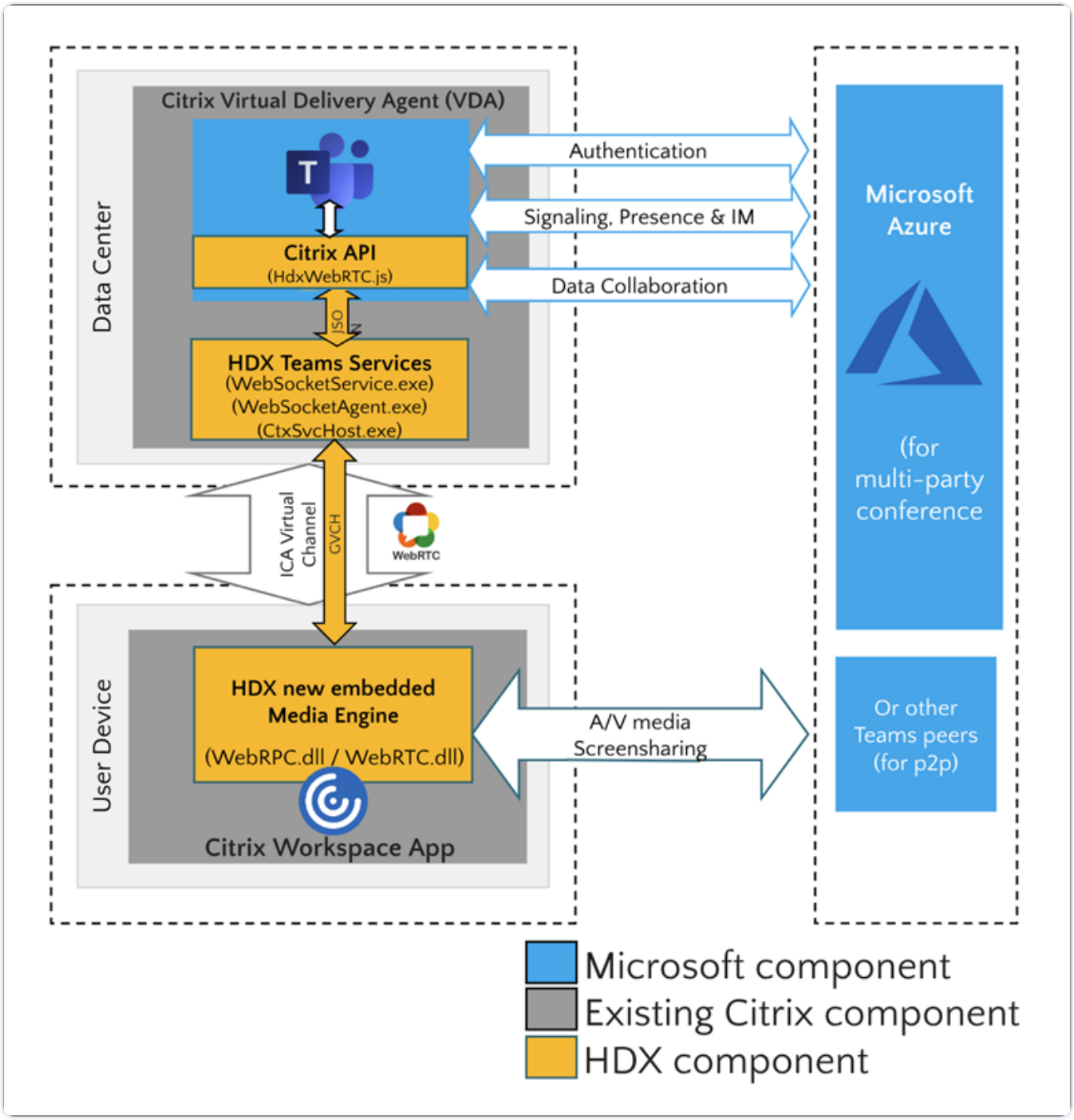
Microsoft Teamsが最適化モードでロードされ、HdxRtcEngine.exeがエンドポイントで実行されている場合、ICEの障害により通話設定の失敗や、音声/ビデオが片方向のみになる可能性があります。通話が完了できない場合やメディアストリームが全二重でない場合は、まずエンドポイントの**Wiresharkトレース**を確認してください。ICE候補収集プロセスに関する詳細については、サポートセクションの「ログの収集」を参照してください。

> **注：**
>
> エンドポイントにインターネットアクセスがない場合でも、両方のユーザーが同じLAN上にいれば、ピアツーピア通話を行うことができる場合があります。会議は失敗します。この場合、通話設定が開始されるまでに30秒のタイムアウトが発生します。

通話設定

このアーキテクチャ図を、通話フローシーケンスの視覚的な参照として使用してください。対応する手順は図に示されています。

アーキテクチャ



1. Microsoft Teams を起動します。
2. Microsoft Teams は O365 に対して認証を行います。テナントポリシーは Microsoft Teams クライアントにプッシュされ、関連する TURN およびシグナリングチャネル情報がアプリに中継されます。
3. Microsoft Teams は VDA で実行されていることを検出し、Citrix JavaScript API に API 呼び出しを行います。
4. Microsoft Teams 内の Citrix JavaScript は、VDA で実行されている WebSocketService.exe に対してセキュアな WebSocket 接続を開き、これによりユーザーセッション内で WebSocketAgent.exe が生成されます。

5. WebSocketAgent.exe は、Citrix HDX Microsoft Teams Redirection Service (CtxSvcHost.exe) を呼び出すことによって、汎用仮想チャネルをインスタンス化します。
6. Citrix Workspace アプリの wfica32.exe (HDX エンジン) は、HdxRtcEngine.exe と呼ばれる新しいプロセスを生成します。これは、Microsoft Teams の最適化に使用される新しい WebRTC エンジンです。
7. Citrix メディアエンジンと Teams.exe は双方向仮想チャネルパスを持ち、マルチメディア要求の処理を開始できます。

   -----ユーザー通話------

8. **ピア A** が **通話** ボタンをクリックします。Teams.exe は Microsoft 365 の Microsoft Teams サービスと通信し、**ピア B** とのエンドツーエンドのシグナリングパスを確立します。Microsoft Teams は HdxRtcEngine に、サポートされている一連の通話パラメーター (コーデック、解像度など。これはセッション記述プロトコル (SDP) オファーとして知られています) を要求します。これらの通話パラメーターは、シグナリングパスを使用して Microsoft 365 の Microsoft Teams サービスに中継され、そこからもう一方のピアに中継されます。
9. SDPオファー/アンサー（シングルパスネゴシエーション）はシグナリングチャネルを介して行われ、ICE接続チェック（STUNバインド要求を使用したNATおよびファイアウォールトラバーサル）が完了します。その後、Secure Real-time Transport Protocol (SRTP)メディアは、HdxRtcEngine.exeと他のピア間（会議の場合はMicrosoft 365会議サーバー）で直接流れます。

マイクロソフト 電話システム

Phone Systemは、Microsoft Teamsを使用してMicrosoft 365クラウドで通話制御とPBXを可能にするMicrosoftのテクノロジーです。Microsoft Teamsの最適化は、Microsoft 365 Calling PlansまたはDirect Routingを使用してPhone Systemをサポートします。Direct Routingを使用すると、追加のオンプレミスソフトウェアなしで、サポートされている独自のセッションボーダーコントローラーをMicrosoft Phone Systemに直接接続できます。 通話キュー、転送、フォワード、保留、ミュート、通話再開がサポートされています。

DTMF

デュアルトーン多周波（DTMF）機能は、以下のバージョンのCitrix Workspaceアプリ（およびそれ以降）でサポートされています。

- Citrix Workspace アプリ for Windows バージョン 2102
- Citrix Workspaceアプリ Windows版 LTSR 1912 CU5 (Windows 10 OSのみ)
- Citrix Workspaceアプリ for Linux バージョン 2101
- Citrix Workspaceアプリ for Mac バージョン 2101

- ChromeOS向けCitrix Workspaceアプリ バージョン2111.1

動的e911のサポート

バージョン2112以降、Citrix Workspaceアプリは動的緊急通報をサポートしています。Microsoft Calling Plans、Operator Connect、およびDirect Routingで使用する場合、以下のことが可能になります。

- 緊急通報の設定とルーティング。
- セキュリティ担当者への通知。

通知は、VDAで実行されているMicrosoft Teamsクライアントではなく、エンドポイントで実行されているCitrix Workspaceアプリの現在の場所に基づいて提供されます。

Ray Baum法では、911通報者の派遣可能な位置情報を適切な公共安全応答拠点（PSAP）に送信することが義務付けられています。HDXによるMicrosoft Teamsの最適化は、以下のバージョンのCitrix Workspaceアプリで使用する場合、Ray Baum法に準拠しています。

- Citrix Workspaceアプリ for Windows バージョン 2112.1 以降
- Citrix Workspaceアプリ for Linux バージョン 2112 以降
- Citrix Workspaceアプリ for Mac バージョン 2112 以降
- Citrix Workspaceアプリ for ChromeOS バージョン 2112 以降

動的な緊急通報を有効にするには、管理者はMicrosoft Teams管理センターを使用して、ネットワークまたは緊急ロケーションマップを作成するために以下を構成する必要があります。

- ネットワーク設定
- ロケーション情報サービス (LIS)

動的緊急通報の詳細については、Microsoft のドキュメントを参照してください。

Citrix WorkspaceアプリがMicrosoft Teamsに中継するディスパッチ可能な位置情報は次のとおりです。

- イーサネット/スイッチ接続用のリンク層検出プロトコル (LLDP) を使用したシャーシ ID / ポート ID。イーサネット/スイッチ (LLDP) は以下でサポートされています。
  - Windows バージョン 8.1 および 10
  - LLDP 有効化ソフトウェアを必要とする macOS。LLDP 有効化ソフトウェアをダウンロードするには、`www.microsoft.com`にアクセスして「LLDP enablement software」を検索してください。

    - Linux。シンクライアントのオペレーティングシステム (OS) ディストリビューションに LLDP ライブラリを含める必要があります。

- Citrix Workspace アプリがインストールされているエンドポイントの WLAN BBSID および {IPv4-IPv6; サブネット; MAC アドレス}。

    - サブネットおよび WiFi ベースのロケーションは、Windows、Linux、Mac 用 Workspace アプリでサポートされています。

- Citrix Workspaceアプリがインストールされ ているOSレベルでユーザーの許可が与えられている場合（権限がHDX RTC Engineに設定されている場合）の緯度と経度

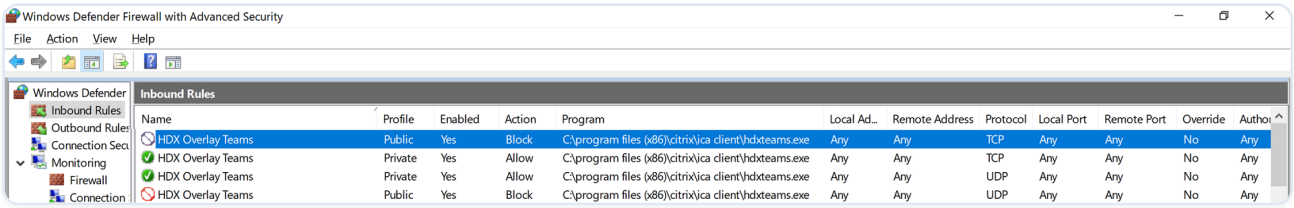
    - すべてのWorkspaceアプリプラットフォームでサポートされています。ただし、Citrix Workspace for Linuxの場合、シンクライアントのOSディストリビューションに`libgps`ライブラリを含める必要があります（>sudo apt-get install libgps23 gpsd lldpd）。

ファイアウォールの考慮事項

ユーザーが Microsoft Teams クライアントを使用して最適化された通話を初めて開始すると、**Windows ファイアウォール**設定に関する警告が表示されることがあります。この警告は、HdxTeams.exe または HdxRtcEngine.exe (HDX Overlay Microsoft Teams) の通信を許可するようユーザーに求めます。

ファイアウォールの警告](/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/firewall1.png)

「**Windows Defender ファイアウォール > セキュリティが強化されたWindows Defender ファイアウォール**」コンソールの**受信の規則**に、次の4つのエントリが追加されます。必要に応じて、より制限の厳しい規則を適用できます。



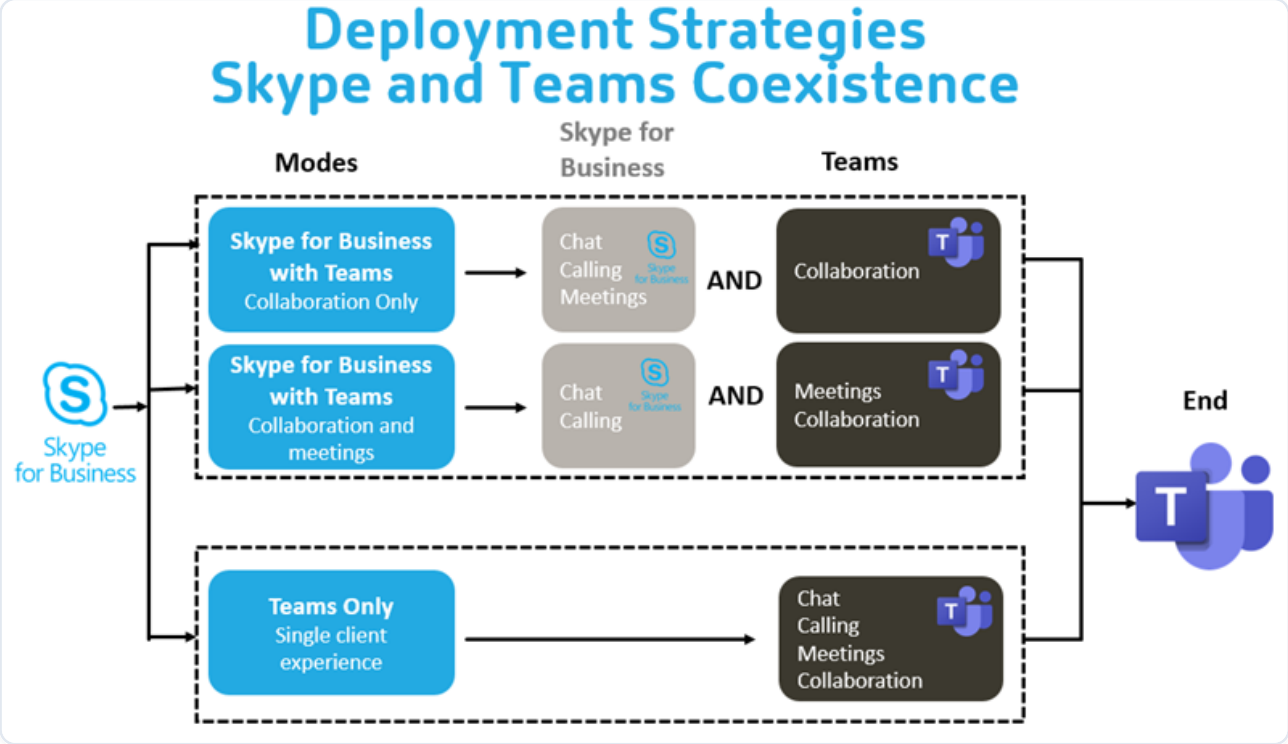
Microsoft Teams と Skype for Business の共存について

Microsoft TeamsとSkype for Businessは、機能が重複する2つの個別のソリューションとして並行して展開できます。 詳細については、「Microsoft TeamsとSkype for Businessの共存と相互運用性を理解する」を参照してください。

Citrix RealTime Optimization PackとMicrosoft Teamsマルチメディアエンジン用のHDX最適化は、環境で設定された構成を尊重します。例としては、アイランドモードや、Microsoft Teamsとの

Skype for Businessコラボレーションなどがあります。また、Microsoft TeamsとのSkype for Businessコラボレーションと会議も含まれます。

周辺機器へのアクセスは、一度に1つのアプリケーションにのみ許可されます。たとえば、通話中にRealTime Media EngineがWebカメラにアクセスすると、通話中はイメージングデバイスがロックされます。デバイスが解放されると、Microsoft Teamsで利用できるようになります。



Citrix SD-WAN™: Microsoft Teams向けに最適化されたネットワーク接続

最適なオーディオおよびビデオ品質には、低遅延、低ジッター、低パケット損失のMicrosoft 365クラウドへのネットワーク接続が必要です。支社のCitrix Workspaceアプリユーザーからデータセンターを経由してインターネットに接続する前に、Microsoft Teamsのオーディオ/ビデオRTPトラフィックをバックホールすると、過剰な遅延が発生する可能性があります。また、WANリンクで輻輳を引き起こす可能性もあります。Citrix SD-WANは、Microsoft 365のネットワーク接続原則に従って、Microsoft Teamsの接続を最適化します。Citrix SD-WANは、Microsoft RESTベースのMicrosoft 365 IPアドレスとWebサービス、および近接DNSを使用します。これは、Microsoft Teamsトラフィックを識別、分類、および誘導するために使用されます。

多くの地域で、ビジネスブロードバンドインターネット接続は、断続的なパケット損失、過剰なジッター期間、および停止に悩まされています。

Citrix SD-WANは、ネットワークの状態が不安定または劣化している場合に、Microsoft Teamsのオーディオ/ビデオ品質を維持するための2つのソリューションを提供します。

- Microsoft Azureを使用している場合、Azure VNETに展開されたCitrix SD-WAN仮想アプライアンス（VPX）は、高度な接続最適化を提供します。これらの最適化には、シームレスなリンクフェイルオーバーとオーディオパケットレーシングが含まれます。
- Citrix SD-WANのお客様は、Citrix Cloud™ Directサービスを介してMicrosoft 365に接続できます。このサービスは、すべてのインターネット向けトラフィックに対して信頼性の高い安全な配信を提供します。

支社のインターネット接続の品質が問題にならない場合は、遅延を最小限に抑えるだけで十分かもしれません。遅延を最小限に抑えるために、Microsoft TeamsトラフィックをCitrix SD-WANブランチアプライアンスから最寄りのMicrosoft 365フロントドアに直接誘導します。詳細については、「Citrix SD-WAN Office 365の最適化」を参照してください。

シトリックス SD-WAN](/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/sd-wan.png)

マルチウィンドウ会議とチャット

Windows版Microsoft Teamsでは、複数の会議またはチャットウィンドウを使用できます。ポップアウト機能の詳細については、Microsoft 365サイトのMicrosoft Teams Pop-Out Windows for Chats and Meetingsを参照してください。

> **注：**
>
> この機能は、Citrix Workspaceアプリ for Windows 2112.1、Mac 2203、Linux 2203、ChromeOS 2303でサポートされています。VDA 2112以降が必要で、1912 CU6+ LTSRにバックポートされました。

背景のぼかしと背景効果

Windows、Mac、Linux、ChromeOS/HTML5 用 Citrix Workspace アプリは、HDX を使用した Microsoft Teams の最適化において、背景のぼかしと背景効果をサポートしています。

背景をぼかしたり、デフォルトの画像に置き換えたりすることで、会話がシルエット（体と顔）に集中できるようにし、予期せぬ邪魔を避けることができます。この機能は、P2P または電話会議で使用できます。

> **注：**

> この機能は、Microsoft Teams の UI/ボタンと統合されています。マルチウィンドウのサポートは、VDA を 2112 以降に更新する必要がある前提条件です。詳細については、「マルチウィンドウ会議とチャット」を参照してください。

> 背景のぼかしと効果に関する Microsoft Teams UI コントロールには、以下の最小バージョンが必要です。

- Windows 2207 用 Citrix Workspace アプリ
- Mac 2301 用 Citrix Workspace アプリ
- Citrix Workspaceアプリ Linux向け 2307
- ChromeOS 2303 用 Citrix Workspace アプリ

制限事項:

- クライアントは、背景画像をMicrosoft Teamsのデフォルト画像に置き換える間、インターネットに接続されている必要があります。
- 管理者およびユーザー定義の背景画像の置き換えは、Microsoft Teams UIではサポートされていません。カスタム背景画像は、画像がクライアントにも保存されている場合、クライアント上の構成設定を使用して構成できます。

カスタム背景画像の設定

以下のレジストリキーは、Microsoft Teams UIを使用してこの機能を制御する予定がない場合、または管理者がデフォルトの動作を上書きしたい場合にのみ必要です。たとえば、エンドポイントの性能が十分でないため、背景のぼかしを無効にする場合などです。

Windowsの場合

カスタム背景画像を設定するには、管理者またはエンドユーザーがクライアントまたはエンドポイントで以下のレジストリキーを構成する必要があります。

場所: `HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXMediaStream`

- 名前: VideoBackgroundEffect
- 種類: DWORD
- 値: 0 (無効), 1 (有効), 2 (背景画像の置き換え)

1に設定された値は背景をぼかします。この値はエンドユーザーまたは管理者が設定できます。

値を2に設定した場合、**VideoBackgroundImage** キーも存在する必要があります。この値は管理者のみが設定できます。以下のキーは、背景画像を置き換えたい場合のみ必要であり、ぼかしには必要ありません。

- 名前: VideoBackgroundImage
- 種類: REG_SZ
- 値: my_image_name.jpeg

ビデオの背景画像は`C:\Program Files (x86)\Citrix\ICA Client`ディレクトリに存在する必要があります。

このレジストリ構成は、Microsoft Teams UIセレクターなしでCitrix Workspaceアプリ2206での背景ぼかしまたは画像置換を有効にするためにも使用できます。言い換えれば、環境またはVDAがマルチウィンドウをサポートしていない場合でも、Citrix Workspaceアプリ2206以降でHKCUレジストリの回避策を適用して同様の結果を得ることができます。ただし、ユーザーはHDXセッション中またはMicrosoft Teams通話中に機能を制御することはできません。

レジストリキーの変更は、HDXセッションが接続したときにのみ有効になります。

Macの場合

ユーザーがダウンロードした画像の場所: */Users/username/Downloads/any_image.png*

カスタム画像をデフォルト画像として設定するには、次のコマンドを実行します。

```
defaults write com.citrix.HdxRtcEngine VideoBackgroundEffect -int 2
```

```
defaults write com.citrix.HdxRtcEngine VideoBackgroundImage -string "/Users/username/Downloads/any_image.png"
```

Linuxの場合

ユーザーがダウンロードした画像の場所: */home/username/Downloads/any_image.jpg*

ファイル */var/.config/citrix/hdx_rtc_engine/config.json* を作成し、以下の構成キーをJSON形式で追加します。例：

```
{



"VideoBackgroundEffect":2,


```

```
"VideoBackgroundImage":"/home/username/Downloads/any_image.jpg"



}
```

HTML5の場合

1. **HTML5Client** フォルダー内の **configuration.js** ファイルに移動します。
2. 属性 **backgroundEffects** を追加し、属性を **true** に設定します。例:

```
'features' : {

    'msTeamsOptimization' :

    {

        'backgroundEffects' : true

    }

}
```

3. 変更を保存します。

クライアントCPU消費に関する考慮事項

ぼかし機能はCPUへの負荷が低いですが、消費量の増加が予想されます。たとえば、4コア、1.5 GHz Intel® Pentium® Silverチップ（TurboBoostで最大2.8 GHz）を搭載したシンクライアントでは、背景のぼかしによりCPU使用率が約2%増加します。平均CPU使用率は20%未満です。

Microsoft Teamsのギャラリービューとアクティブスピーカー

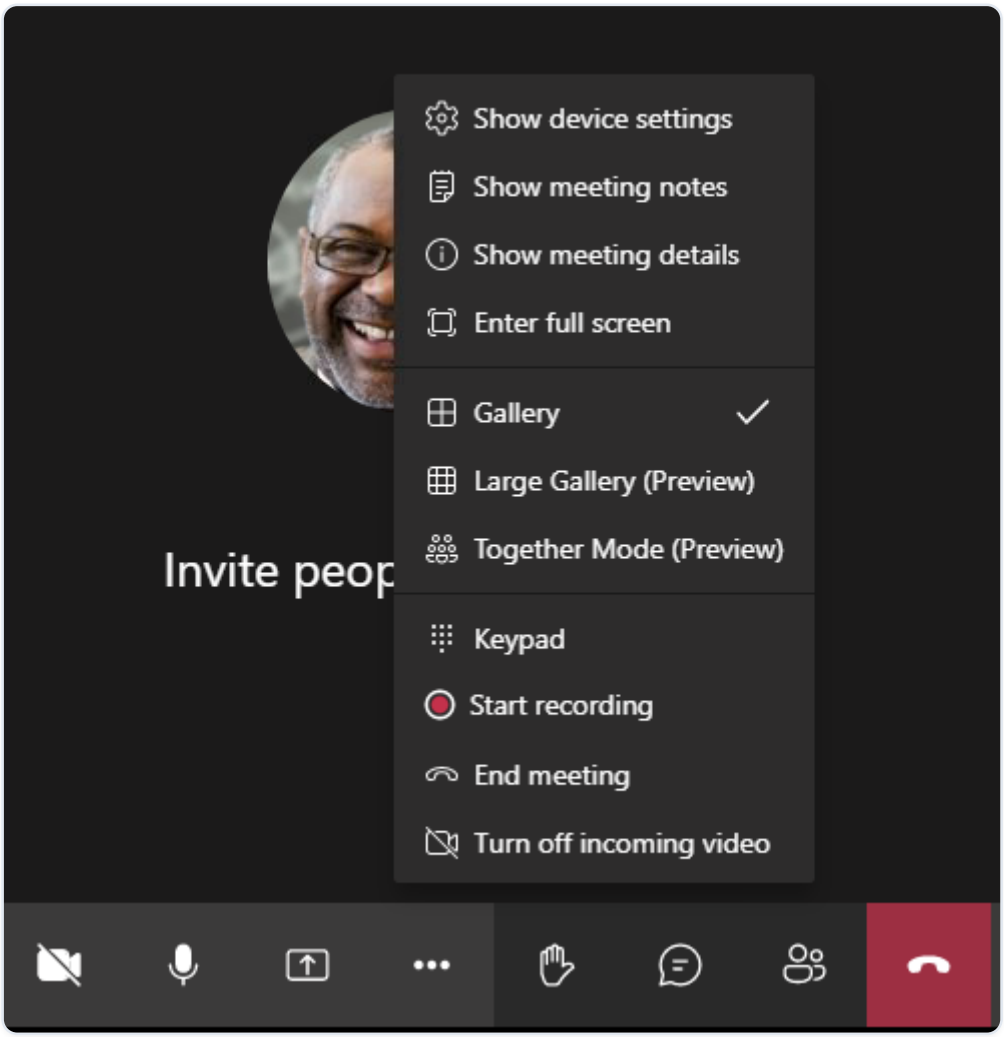
Microsoft Teamsは、**ギャラリー**、**大規模ギャラリー**、および**Together**モードのレイアウトをサポートしています。

Microsoft Teamsは、4人の参加者のビデオストリームを2x2のグリッドで表示します（**ギャラリー**として知られています）。この場合、Microsoft Teamsは4つのビデオストリームをクライアントデバイスに送信してデコードします。4人を超える参加者がビデオを共有している場合、画面には最後に最もアクティブだった4人の話者のみが表示されます。

Microsoft Teamsは、最大7x7のグリッドを持つ大規模ギャラリービューも提供します。その結果、Microsoft Teams会議サーバーは単一のビデオフィードを合成し、それをクライアントデバイスに送信してデコードするため、CPU消費量が低減されます。この単一のマトリックス形式のフィードには、ユーザーのセルフプレビュービデオも含まれる場合があります。

最後に、Microsoft Teamsは新しい会議エクスペリエンスの一部である**Togetherモード**をサポートしています。AIセグメンテーション技術を使用して参加者を共有背景にデジタル配置することで、Microsoft Teamsはすべての参加者を同じ講堂に配置します。

ユーザーは、会議中に省略記号メニューで**ギャラリー**、**大規模ギャラリー**、または**Togetherモード**のレイアウトを選択することで、これらのモードを制御できます。



ビデオアスペクト比の制約のサポート（Citrix Workspaceアプリ for Windows 2102、Citrix Workspaceアプリ for Linux 2106、Citrix Workspaceアプリ for MAC 2106以降）：

- **フレームに合わせる**オプションは、ギャラリー/大規模ギャラリービューで利用できます。このオプションは、サブウィンドウに収まるようにビデオサイズをトリミングします。一方、**フレームにフィット**は、ビデオの側面に黒いバー（レターボックス）を表示するため、トリミングは行われません。

次の表は、ギャラリーレイアウトと大規模ギャラリーレイアウトの比較を示しています。

	ギャラリービュー 2X2 (デフォルト)	ラージギャラリービュー
レイアウト/グリッド	4人の参加者のビデオストリームを含む2x2のグリッドを表示します。画面には直近の最もアクティブな4人のスピーカーのみが表示され、他の参加者はグリッドに表示されません。	49人の参加者のビデオストリームを含む7x7のグリッドを表示します。
ミキシング技術	メディアルーターは、各参加者からの個々のストリームをすべてのユーザーに転送します。	中央の会議サーバーがすべてのオーディオまたはビデオをミキシングおよびトランスコードし、各参加者向けにカスタマイズされた複合レイアウトを作成します。この処理により、追加の遅延が発生します。
アクティブスピーカー	新しいアクティブスピーカーは、グリッド内で最もアクティブでないスピーカーと置き換わります。	アクティブか非アクティブかに関わらず、すべての参加者を表示します。
エンドポイントでのエンコード	Simulcastが有効になっている場合、1つ以上のビデオストリームがエンドポイントでエンコードされることがあります。Simulcastのサポートの詳細については、「Simulcast」を参照してください。	Simulcastが有効になっている場合、1つ以上のビデオストリームがエンドポイントでエンコードされることがあります。Simulcastのサポートの詳細については、「Simulcast」を参照してください。
エンドポイントでのデコード	各参加者は最大4つの個別のメディアストリームを受信します。これにより、HdxRtcEngine.exeによるエンドポイントでのCPU消費量が増加します（デコード/レンダリングのため）。	各参加者は、オーディオとビデオの単一ストリームのみを取得します。この設定により、エンドポイントでのCPU消費が削減されます。

	ギャラリービュー 2X2 (デフォルト)	ラージギャラリービュー
最大解像度	720p。4人の参加者がビデオを共有している場合、ビデオフィードあたりの最大解像度は360pです。4人未満の参加者がビデオを共有している場合、ビデオフィードあたりの解像度は高くなる可能性があります。	複合レイアウトまたはミキシングの場合は720p。複合レイアウトでは、参加者ごとに高品質のビデオストリームは必要ありません。この条件のため、各送信者は解像度またはアップロードビットレートを削減します。
「低速ユーザー」の問題	送信者は、各モダリティ（オーディオ/ビデオ/画面共有）の品質を、参加者間の最低共通ネットワーク品質に調整します。このマルチメディアストリームは、他のすべての参加者に転送されます。その結果、ネットワーク状態の悪い参加者が、通話中の他の全員の品質に影響を与えます。	最低共通ネットワーク品質のシナリオの影響を受けにくい。会議サーバーは、個々の参加者のネットワーク状態に基づいて異なる品質を提供します。
セルフプレビュー	自分自身を小さなサムネイルでリアルタイムに表示します。	自分自身をサムネイルで表示し、他のビデオフィードと混合します。その結果、メインのビデオレイアウトに自分自身が追加の遅延とともに含まれて表示されることがあります。

Microsoft Teamsでの画面共有

Microsoft Teamsは、ビデオベースの画面共有（VBSS）に依存しており、共有されているデスクトップをH264などのビデオコーデックで効率的にエンコードし、高精細ストリームを作成します。HDX最適化を使用すると、受信する画面共有はビデオストリームとして扱われます。

Windows、Linux、Mac向けのCitrix Workspaceアプリ2109以降、およびChromeOS向けのCitrix Workspaceアプリ2303以降では、ユーザーは画面とビデオカメラを同時に共有できます。

以前のバージョンでは、ビデオ通話中に相手がデスクトップの共有を開始すると、元のカメラビデオフィードは一時停止されます。代わりに、画面共有ビデオフィードが表示されます。その後、相手は手動でカメラ共有を再開する必要があります。

PowerPoint Liveに関する注意

PowerPoint Liveからコンテンツを共有している場合、この制限は存在しません。その場合、他のピアは引き続きあなたのウェブカメラとコンテンツを見ることができ、他のスライドを確認するために前後に移動できます。このシナリオでは、スライドはVDA上でレンダリングされます。PowerPoint Liveのスライドデッキにアクセスするには、「Share tray」ボタンをクリックし、提案されたPowerPointスライドのいずれかを選択するか、「Browse」をクリックしてコンピューターまたはOneDrive上のPowerPointファイルを見つけます。

送信画面共有も最適化され、Citrix Workspaceアプリにオフロードされます。この場合、メディアエンジンはCitrix Desktop Viewer (CDViewer.exe) ウィンドウのみをキャプチャして送信し、その周囲には赤い枠線が描画されます。Desktop Viewerと重なるローカルアプリケーションはキャプチャされません。

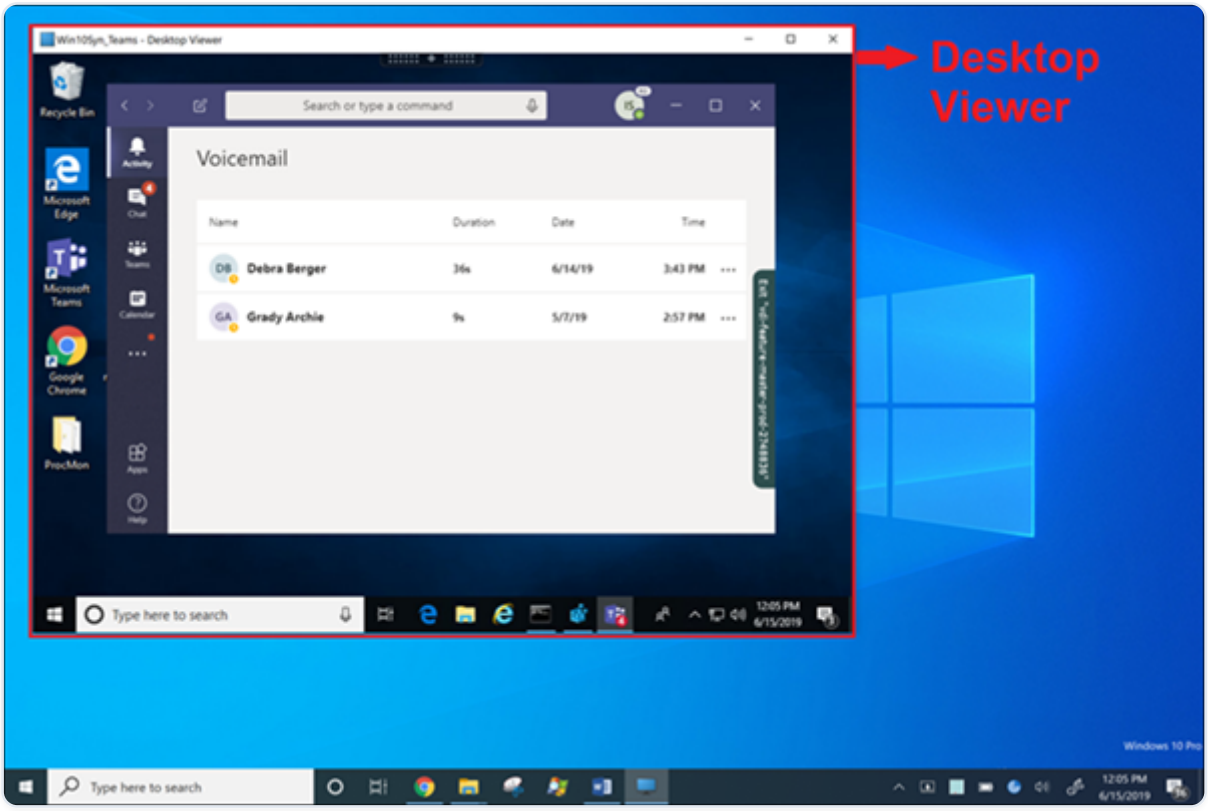
注

Mac版Citrix Workspaceアプリで画面共有を有効にするには、特定の権限を設定してください。詳細については、システム要件を参照してください。

既知の制限:

- Desktop Viewerが無効になっている場合、またはDesktop Lockが使用されている場合、Microsoft Teamsの画面ピッカーではマルチモニター選択は利用できません。Desktop Viewerは、`.ICA`ファイルテンプレートを編集するか、`StoreFront web.config`によって無効にすることができます。SHIFT+F2ホットキーはマルチモニター画面共有と互換性がありません。
- Workspaceアプリのバージョン2106より前では、プライマリモニターのみが共有されます。仮想デスクトップ内のアプリケーションをプライマリモニターにドラッグすると、通話中の他のピアがそれを見ることができます。
- Citrix Workspaceアプリを仮想モニターレイアウト機能（単一の物理モニターの論理パーティション）で構成した場合、マルチモニター画面共有が機能しない可能性があります。この場合、すべての仮想モニターは複合画像として共有されます。

- Citrix Workspaceアプリ for Windowsの古いバージョン（1907から2008まで）では、クライアントマシンで実行されているローカルアプリケーションも共有されます。この共有は、ローカルアプリがDesktop Viewerの上にオーバーレイされている場合にのみ可能です。この動作は、2009.6以降および1912 CU5以降で削除されました。
- 画面共有中にウィンドウモードからフルスクリーンに変更すると、画面共有が停止します。画面共有を機能させるには、一度停止して再度共有する必要があります。
- 最適化されたMicrosoft Teamsでは、共有コントロールを特定の場所にピン留めすることはできません。
- 最小化されたアプリを共有すると、アプリのタイトルバーも共有される場合があります。



シームレスアプリケーションからの画面共有:

Microsoft Teamsをスタンドアロンのシームレスアプリケーションとして公開している場合、画面共有は物理エンドポイントのローカルデスクトップをキャプチャします。Citrix Workspaceアプリの最小バージョン1909が必要です。

アプリ共有

Citrix Workspaceアプリ for Windows 2112.1およびVDA 2112以降、Microsoft Teamsはアプリ共有をサポートしています。

Citrix Workspaceアプリ for Windows 2109、Mac 2203、Linux 2209、およびVDA 2109以降、Microsoft Teamsは仮想セッションで実行されている特定のアプリの画面共有をサポートしていま

す。最適化されたMicrosoft Teamsを使用して、Javaなどのカスタム社内アプリケーションを共有することもできます。特定のアプリを共有するには：

1. リモートセッション内でMicrosoft Teamsアプリに移動します。
2. Microsoft Teams UIで**コンテンツを共有**をクリックします。
3. 会議で共有するアプリを選択します。選択したアプリの周囲に赤い枠が表示され、通話中のピアは共有されたアプリを見ることができます。

別のアプリを共有するには、もう一度**コンテンツを共有**をクリックして、新しいアプリを選択します。

アプリ共有を無効にする場合は、VDAの`HKLM\SOFTWARE\Citrix\Graphics`に次のレジストリキーを作成します。 名前: `UseWsProvider` 種類: `DWORD` 値: 0

> **注：**
>
> - アプリを最小化すると、Microsoft Teamsは共有アプリの最後の画像を表示します。画面共有を再開するには、ウィンドウを最大化できます。
> - 画面共有は、VDA側でのウィンドウのキャプチャに依存します。コンテンツは最大レートでCitrix Workspaceアプリに中継されます。最大レートは1秒あたり30フレームです。Citrix Workspaceアプリは、コンテンツをピアまたは会議サーバーに転送します。

> Microsoft Teamsのアプリ共有](/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/ms-teams-app-sharing.png)

特定のアプリの画面共有に関する既知の制限：

- アプリを画面共有しているとき、マウスカーソルは表示されません。
- アプリを共有中に最小化すると、スクリーンピッカーにはアプリのアイコンのみが表示されます。アプリのサムネイルはスクリーンピッカーでプレビューされません。アプリを最大化するまで、コンテンツを共有できず、赤い枠も表示されません。
- LAAアプリは、VDAの最適化されたMicrosoft Teamsでデスクトップアプリと共有できるアプリのリストを表示します。ただし、リストからアプリを選択しても、期待どおりの結果にならない場合があります。

アプリ保護との互換性 特定のアプリの画面共有は、HDX最適化されたMicrosoft Teamsのアプリ保護機能と互換性があります。アプリ保護が有効になっているデリバリーグループからアプリまたはデスクトップを起動した場合、特定のアプリを画面共有できます。

Microsoft Teams UIで**コンテンツを共有**をクリックすると、スクリーンピッカーから**デスクトップ**オプションが削除されます。開いているアプリを共有するには、**ウィンドウ**オプションのみを選択できます。

> **注：**
>
> アプリ保護が有効になっているデリバリーグループからアプリまたはデスクトップを起動する場合、Citrix Workspaceアプリ for Windows 2202以前を使用していると、受信ビデオまたは画面共有を表示できません。

Microsoft Teamsで制御を付与および要求する

この機能は、Citrix Workspaceアプリの以下のバージョンでサポートされています（VDAバージョンやオペレーティングシステム、シングルセッションまたはマルチセッションには依存しません）。

- Citrix Workspaceアプリ for Windows バージョン2112.1以降
- Citrix Workspaceアプリ for Mac バージョン2203.1以降
- Citrix Workspaceアプリ for Linux バージョン2203以降
- ChromeOS 版 Citrix Workspace アプリ バージョン 2303 以降

Microsoft Teams通話中に参加者が画面を共有している場合、制御を要求できます。制御を取得すると、共有画面に対して選択、編集、その他のキーボードおよびマウス操作を行うことができます。

画面が共有されているときに制御するには、Microsoft Teams UI の ボタンをクリックします。画面を共有している会議参加者は、要求を許可または拒否できます。

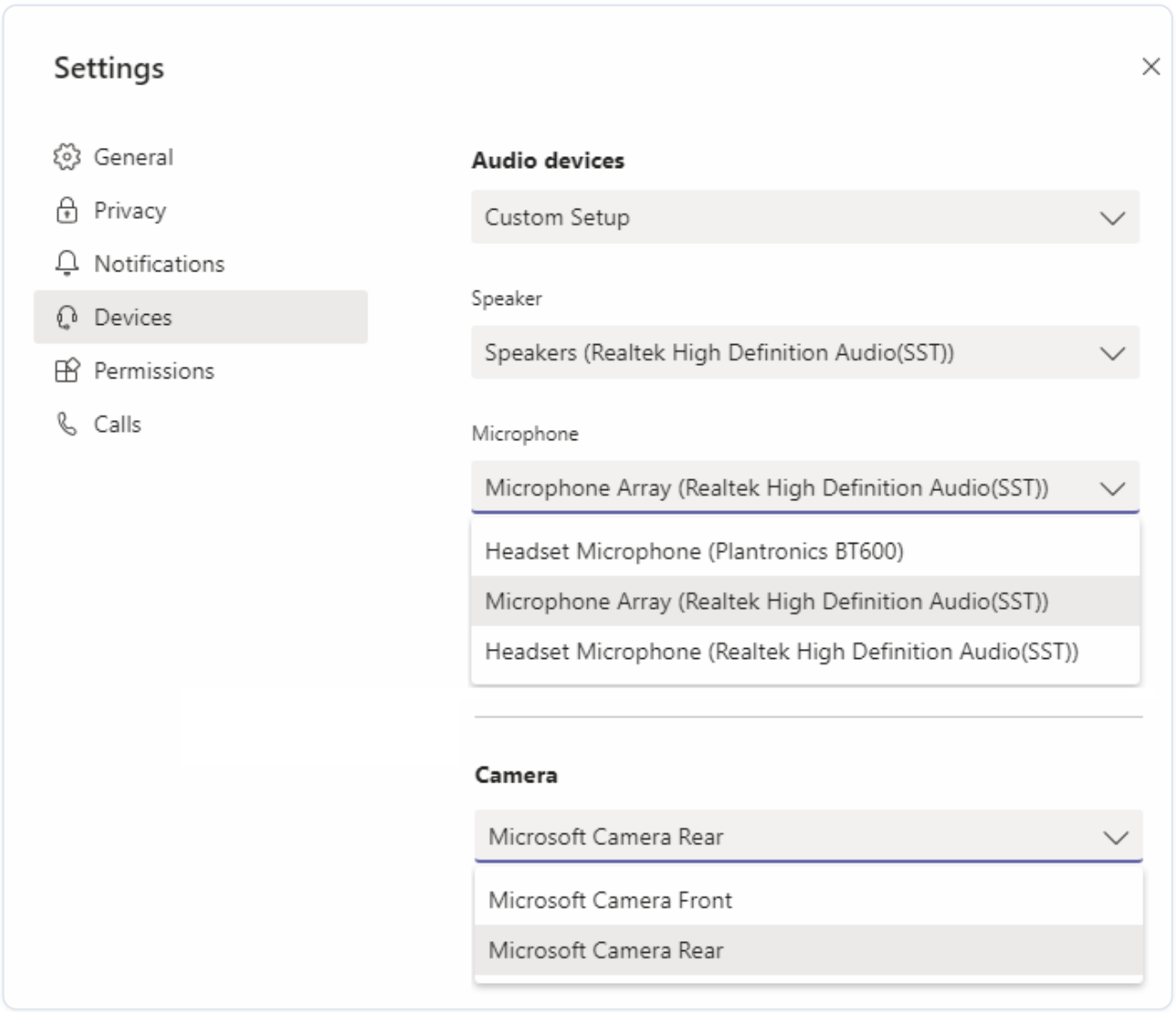
制御中は、共有画面の選択、編集、その他の変更を行うことができます。これらの操作には、キーボードとマウスの両方を使用できます。完了したら、 をクリックします。

> **制限事項:**

- ユーザーが単一のアプリを共有している場合 (アプリ共有とも呼ばれます)、制御の付与と要求は利用できません。デスクトップ全体またはモニターを共有する必要があります。
- コントロールバーを特定の場所に固定する機能は利用できません。

Microsoft Teamsでの周辺機器

Microsoft Teamsの最適化が有効な場合、Citrix Workspaceアプリは周辺機器（ヘッドセット、マイク、カメラ、スピーカーなど）にアクセスします。その後、周辺機器はMicrosoft Teams UIの（**設定 > デバイス**）に適切に一覧表示されます。



Microsoft Teamsはデバイスに直接アクセスしません。代わりに、メディアの取得、キャプチャ、処理のためにWorkspaceアプリのWebRTCメディアエンジンに依存します。Microsoft Teamsは、ユーザーが選択できるようにデバイスを一覧表示します。

Microsoft Teams のアクティブ中に挿入された周辺機器は、デフォルトでは選択されません。Microsoft Teams UI の > 画面から周辺機器を手動で選択する必要があります。周辺機器が選択されると、Microsoft Teams は周辺機器の情報をキャッシュします。その結果、同じエンドポイントからセッションに再接続すると、周辺機器が自動的に選択されます。

推奨事項:

- エコーキャンセレーション機能が内蔵された Microsoft Teams 認定ヘッドセット。マイクとスピーカーが別々のデバイスにある追加の周辺機器を使用するセットアップでは、エコーが発生する可能性があります。例としては、内蔵マイク付きのウェブカメラとスピーカー付きのモニターがあります。外部スピーカーを使用する場合は、マイクからできるだけ離して配置してください。また、音をマイクに屈折させる可能性のある表面からも離して配置してください。詳細については、`www.microsoft.com` にアクセスし、Microsoft Teams 認定ヘッドセットを検索してください。
- Microsoft Teams 認定カメラ。ただし、Skype for Business 認定周辺機器は Microsoft Teams と互換性があります。詳細については、<www.microsoft.com> にアクセスし、Microsoft Teams 認定カメラと Skype for Business 認定周辺機器を検索してください。
- Citrix Workspaceアプリのメディアエンジンは、オンボードH.264エンコーディング（UVC 1.1および1.5）を実行するWebカメラではCPUオフロードを利用できません。

> **注：**

> Windows用Workspaceアプリ2009.6は、24ビットまたは96 kHzを超える周波数のオーディオ形式に対応した周辺機器を取得できるようになりました。

> HdxTeams.exe（Windows用Citrix Workspaceアプリ2009以前の場合）は、これらの特定のオーディオデバイス形式（チャンネル、ビット深度、サンプルレート）のみをサポートします。

> - 再生デバイス: 最大2チャンネル、16ビット、最大96,000 Hzの周波数
> - 録音デバイス: 最大4チャンネル、16ビット、最大96,000 Hzの周波数

> スピーカーまたはマイクのいずれかが予期される設定と一致しない場合でも、Microsoft Teamsでのデバイス列挙は失敗し、**設定 > デバイス**の下に**なし**と表示されます。

HdxTeams.exeの**Webrpc**ログには、この種類の情報が表示されます。

`Mar 27 20:58:22.885 webrtcapi.WebRTCEngine Info: init. initializing...`.

`Mar 27 20:58:23.190 webrtcapi.WebRTCEngine Error: init. couldn't create audio module!` !

回避策として、特定のデバイスを無効にするか、次のいずれかを実行します。

1. **サウンドコントロールパネル** (mmsys.cpl) を開きます。
2. 再生デバイスまたは録音デバイスを選択します。
3. **プロパティ > 詳細設定**に移動し、設定をサポートされているモードに変更します。

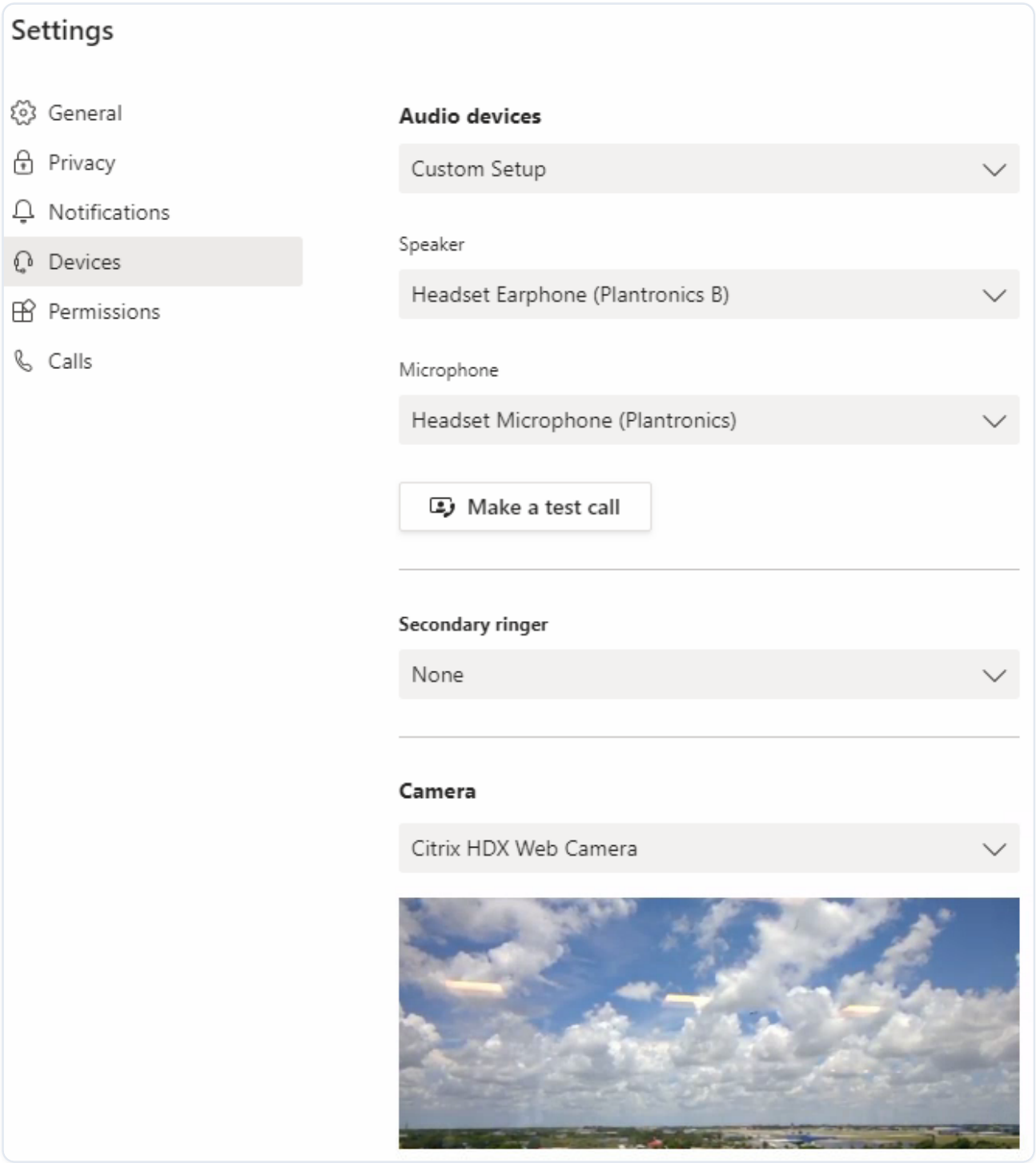
フォールバックモード

Microsoft Teams が最適化された VDI モードでロードに失敗した場合 (Microsoft Teams/バージョン情報/バージョンで「Citrix HDX Not Connected」と表示される場合)、VDA はレガシー HDX テクノロジーにフォールバックします。レガシー HDX テクノロジーには、Web カメラのリダイレクト、クライアントのオーディオとマイクのリダイレクトが含まれる場合があります。Microsoft Teams の最適化をサポートしない Workspace アプリのバージョン/プラットフォーム OS を使用している場合、フォールバックレジストリキーは適用されません。 フォールバックモードでは、周辺機器は VDA にマッピングされます。周辺機器は、仮想デスクトップにローカルで接続されているかのように Microsoft Teams アプリに表示されます。

VDA でレジストリキーを設定することで、フォールバックメカニズムをきめ細かく制御できるようになりました。詳細については、レジストリで管理される機能のリストにある Microsoft Teams フォールバックモード を参照してください。

この機能には、Microsoft Teamsバージョン1.3.0.13565以降が必要です。

Microsoft Teams アプリの **>** タブで、最適化モードか非最適化モードかを判断するには、カメラ名が主な違いとなります。Microsoft Teams が非最適化モードでロードされると、レガシー HDX テクノロジーが起動します。Web カメラ名には、次の図に示すように **Citrix HDX** のサフィックスが付いています。スピーカーとマイクのデバイス名は、最適化モードと比較してわずかに異なる (または切り詰められる) 場合があります。



レガシー HDX テクノロジーが使用されている場合、Microsoft Teams はオーディオ、ビデオ、画面共有の処理をエンドポイントの Citrix Workspace アプリ WebRTC メディアエンジンにオフロードしません。代わりに、HDX テクノロジーはサーバー側レンダリングを使用します。ビデオをオンにすると、VDA で高い CPU 消費が予想されます。リアルタイムオーディオのパフォーマンスは最適ではない可能性があります。

既知の制限事項

Citrixの制限事項

Citrix Workspaceアプリの制限事項：

- HID ボタン - 通話の応答と終了はサポートされていません。音量アップとダウンはサポートされています。
- Microsoft Teamsの管理センターでのQoS設定は、VDIユーザーには適用されません。
- ユーザーは、VDA でスニッピングツールを使用している間は、Microsoft Teams のコンテンツのスクリーンショットを撮ることができません。ただし、クライアント側でスニッピングツールを使用すると、コンテンツをキャプチャできます。

VDAの制限事項：

- **Citrix Workspace アプリの高 DPI** 設定を `Yes` に構成すると、リダイレクトされたビデオウィンドウがずれて表示されます。この制限は、モニターの DPI スケーリング係数が 100% を超える値に設定されている場合に発生します。

Citrix Workspace アプリと VDA の制限事項:

- 最適化された通話の音量は、VDAではなく、クライアントマシンの音量バーを使用してのみ制御できます。

サイマルキャスト

最適化されたMicrosoft Teamsビデオ会議通話のサイマルキャストサポートは、WindowsおよびMacで有効になっています。Linuxについては、シンクライアントベンダーにご確認ください。 サイマルキャストを使用すると、すべての通話者にとって最適な通話体験のために適切な解像度に調整することで、異なるエンドポイント間でのビデオ会議通話の品質とエクスペリエンスが向上します。

この改善されたエクスペリエンスにより、各ユーザーは、エンドポイントの機能、ネットワークの状態など、いくつかの要因に応じて、異なる解像度（たとえば、720p、360pなど）で複数のビデオストリームを配信できます。受信側のエンドポイントは、処理できる最大品質の解像度を要求し、すべてのユーザーに最適なビデオエクスペリエンスを提供します。

> **注：**
>
> この機能は、Microsoft Teamsからのアップデートが展開された後にのみ利用可能です。ETAについては、`<https://www.microsoft.com/>` にアクセスし、Microsoft 365ロードマップ

を検索してください。Microsoftによってアップデートが展開されたら、ドキュメントの更新と発表についてはCTX253754 を確認してください。

Microsoftの制限事項

- 3x3ギャラリービューはサポートされていません。Microsoft Teamsの依存関係 – 3x3グリッドがいつ提供されるかについてはMicrosoftにお問い合わせください。
- Skype for Businessとの相互運用性は音声通話に限定されており、ビデオモダリティはありません。
- 送受信ビデオストリームの最大解像度は720pです。
- PSTN通話の呼び出し音はサポートされていません。
- ダイレクトルーティングのメディアバイパスはサポートされていません。
- ブロードキャストおよびライブイベントのプロデューサーおよびプレゼンターの役割はサポートされていません。出席者の役割はサポートされていますが、最適化されていません（代わりにVDAでレンダリングされます）。
- Microsoft Teamsのズームインおよびズームアウト機能はサポートされていません。
- ロケーションベースルーティングとメディアバイパスはサポートされていません。
- 通話のマージはサポートされていません（ユーザーインターフェイスにオプションが表示されません）。

CitrixとMicrosoftの制限事項

- 画面共有を行う際、**システムオーディオを含める**オプションは利用できません。
- サイマルキャストはChromeOSではサポートされていません。

今後のMicrosoft Teamsシングルウィンドウの EOL

January 31, 2024に、MicrosoftはVDI Microsoft Teams最適化を使用している場合、シングルウィンドウUIに対するMicrosoft Teamsのサポートを終了し、マルチウィンドウエクスペリエンスのみをサポートします。Microsoftは、この非推奨化について9/8/2023にM365管理者センター（投稿ID: MC674419）で通知しました。 マルチウィンドウ機能に関する公開されている詳細は、Tech Communityの記事：New Meeting and Calling Experience in Microsoft Teamsで確認できます。

注：

Citrixは、ビデオおよび画面共有のためにMicrosoft Teamsを最適化モードで引き続き使用するには、VDAとCitrix Workspaceアプリをサポートされているバージョンにアップグレードすることを推奨します。インフラストラクチャとエンドポイントをアップグレードしてマルチウィンドウをサポートしない場合、通話、ビデオ通話、および画面共有は最適化されなくなります。これにより、通話品質の問題、レイテンシーの増加、およびサーバーへの負荷の増加が発生する可能性があります。

次の表は、Citrix VDIでMicrosoft Teamsの最適化された通話を継続して使用するために必要なVDAおよびCitrix Workspaceアプリの最小バージョン、LTSRバージョン、推奨バージョンを示しています。

コンポーネント	最小バージョン (1)	LTSRサポートバージョン (2)	推奨バージョン (3)
マイクロソフト チームズ	1.5.00.11865	該当なし	最新
VDA	1912 CU6 LTSR, 2109 CR, 2203 LTSR	1912 CU8+, 2203 LTSR CU2+ (4)	2308 CR+
Windows版 Citrix Workspaceアプリ	2112.1 CR	2203 CU2+ (4)	2309 CR以降
Mac版 Citrix Workspaceアプリ	2203 CR	該当なし	2308 CR+
Linux向け Citrix Workspace アプリ	2202 CR	該当なし	2308 CR+
ChromeOSまたはHTML5版 Citrix Workspaceアプリ	2303 CR	該当なし	2309 CR以降

注:

1. 最小バージョン: これはマルチウィンドウが最初に導入されたバージョンです。ここに記載されている最小バージョンの一部は、サポート終了となっている場合があります。

2. LTSRサポート対象バージョン: これは、Citrixがマルチウィンドウ向けにサポートしているLTSRバージョンです。これらのLTSRリリースの古いバージョンは動作する可能性がありますが、新しいLTSR CUバージョンがリリースされると、それらのバージョンに対するサポートは利用できなくなります。LTSRサポートポリシーの詳細については、`<https://support.citrix.com/article/CTX205549/faq-citrix-virtual-apps-and-desktops-and-citrix-hypervisor-long-term-service-release-ltsr>`を参照してください。
3. 推奨バージョン: これは、ユーザー/顧客がソフトウェアのアップグレードを選択した場合にCitrixが推奨するソフトウェアのバージョンです。これらはすべてCRバージョンです。
4. VDAおよびCWAベースバージョンのバージョン2203 LTSRには、マルチウィンドウ機能が含まれています。これらのバージョンは、公式にサポートされている最新のCUに置き換えられています。お客様は、これらのサポート対象外のバージョンを自己責任で引き続き使用できます。Citrixは、LTSRリリースをご利用のお客様に最新のCUへのアップグレードを推奨しています。

WebRTCからのSDP形式（プランB）の非推奨のお知らせ

Citrixは、将来のリリースでWebRTCからの現在のSDP形式 (プランB) のサポートを廃止する予定です。最適化されたMicrosoft Teamsの機能に対応するには、WebRTCでUnified Planを使用する必要があります。

影響を受ける製品

Citrix Workspaceアプリケーションの将来のリリースにおいて、Citrix Workspaceアプリの今後のリリースを使用するエンドポイントと、Citrix Workspaceアプリ2108以前のバージョンを使用するエンドポイント間の通話はサポートされません。この通話の非互換性には、1912 LTSR Citrix Workspaceアプリクライアント (CWA) が含まれます。以下のCWAクライアントが影響を受けます。

- Windows向けCitrix Workspaceアプリ
- Linux向け Citrix Workspace アプリ
- Mac向けCitrix Workspaceアプリ
- Chrome向けCitrix Workspaceアプリ

プランBの代替

Citrix Workspaceアプリのバージョン2109より古いバージョンを実行している場合は、サポートされているバージョン（できれば最新のCRリリース）にアップグレードする必要があります。そうしないと、将来のリリースまたは新しいエンドポイントとの通話は接続に失敗します。将来のリリースとフェデレーション通信パートナー間の通話も、フェデレーションパートナーがCitrix Workspaceをアップグレードしていない場合、完了に失敗する可能性があります。

Citrix Workspaceアプリバージョン2108は2023年3月にサポート期限が終了しており、新しいバージョンにアップグレードする必要があります。詳細については、Citrix Workspaceアプリのバージョンサポートに関するWorkspace Appを参照してください。

プランBの廃止に関する詳細については、WebRTCドキュメントを参照してください。

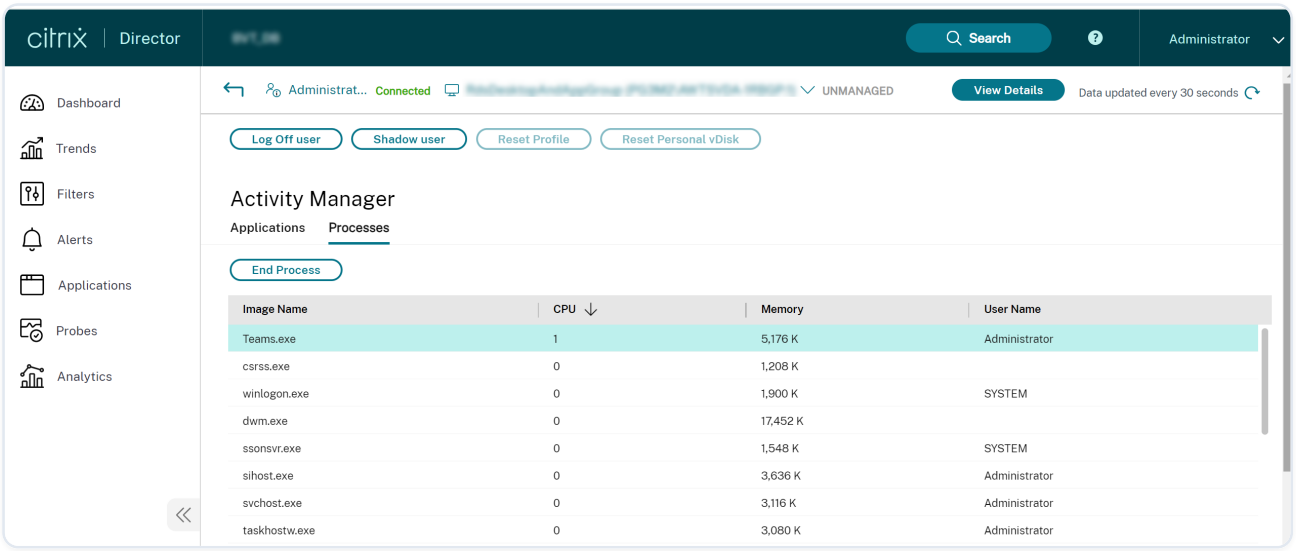
追加情報

- Microsoft Teams の監視、トラブルシューティング、サポート
- VM への Microsoft Teams デスクトップアプリの展開
- MSI を使用した Microsoft Teams のインストール (VDI インストールセクション)
- シンクライアント
- Skype for Business ネットワーク評価ツール
- Microsoft Teams と Skype for Business の共存と相互運用性を理解する

Microsoft Teamsの監視、トラブルシューティング、サポート

Teamsの監視

このセクションでは、HDXによるMicrosoft Teamsの最適化を監視するためのガイドラインを提供します。 最適化モードで実行中で、`HdxRtcEngine.exe`がクライアントマシンで実行されている場合、VDA上の`WebSocketAgent.exe`というプロセスがセッションで実行されています。Directorの**アクティビティマネージャー**を使用してアプリケーションを確認します。



Microsoft Teamsの最適化ステータスは、Director > **ユーザー詳細**ページ > **セッション詳細**パネル > **MS Teams最適化**フィールドで確認できます。Microsoft Teamsが最適化されていることは、クリアなオーディオやビデオなど、より良いユーザーエクスペリエンスのために重要です。この機能はVDAバージョン2311以降で利用可能です。サポートされているCitrix Workspace™アプリのバージョンは、「Microsoft Teamsの最適化」に記載されています。Directorは、Microsoft Teamsが公開アプリケーションとして、または公開デスクトップ内で実行されている場合にのみ、Microsoft Teamsの最適化ステータスを表示します。 詳しくは、「Microsoft Teamsの最適化ステータス」を参照してください。

VDAの最小バージョン1912では、Citrix HDX Monitor（最小バージョン3.11）を使用してアクティブなTeams通話を監視できます。Citrix Virtual Apps and Desktops製品ISOには、フォルダー `layout\image-full\Support\HDX Monitor` に最新の `hdxmonitor.msi` が含まれています。VDAの最小バージョン1912では、Citrix HDX Monitor（最小バージョン3.11）を使用してアクティブなMicrosoft Teams通話を監視できます。Citrix Virtual Apps and Desktops製品ISOには、フォルダー `layout\image-full\Support\HDX Monitor` に最新の `hdxmonitor.msi` が含まれています。

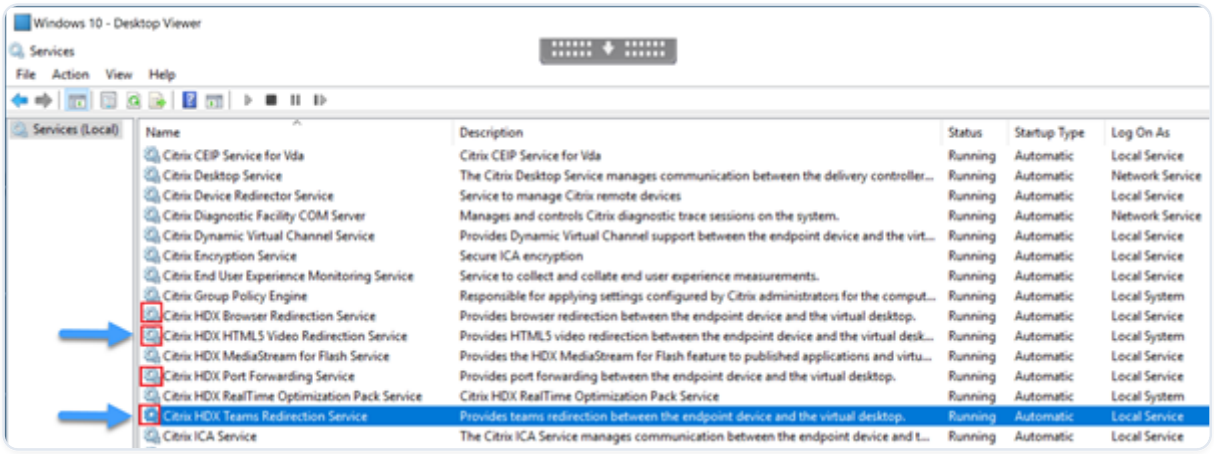
詳しくは、Knowledge Centerの記事「CTX253754」の「*監視*」を参照してください。

トラブルシューティング

このセクションでは、Microsoft Teamsの最適化を使用する際に発生する可能性のある問題のトラブルシューティングのヒントを提供します。詳しくは、「CTX253754」を参照してください。

バーチャル デリバリー エージェント上で

BCR_x64.msiによって4つのサービスがインストールされます。このうち2つだけがVDAでのMicrosoft Teamsリダイレクトを担当します。



- **Citrix HDX Teams Redirection Service**は、Microsoft Teamsで使用される仮想チャネルを確立します。このサービスはCtxSvcHost.exeに依存しています。
- **Citrix HDX HTML5 Video Redirection Service**は、WebSocketService.exeとして実行され、127.0.0.1:9002 TCPでリッスンします。WebSocketService.exeは主に2つの機能を実行します。

  i. **セキュアWebSocketのTLS終端**は、Microsoft Teamsアプリ内のコンポーネントであるvdiCitrixPeerConnection.jsからセキュアWebSocket接続を受信します。これはProcess Monitorで追跡できます。証明書について詳しくは、「ControllerとVDA間の通信」の「TLSとHTML5ビデオのリダイレクト、およびブラウザコンテンツのリダイレクト」セクションを参照してください。

  一部のアンチウイルスソフトウェアやデスクトップセキュリティソフトウェアは、`WebSocketService.exe`とその証明書の適切な機能に干渉します。Citrix HDX HTML5 Video Redirectionサービスが`services.msc`コンソールで実行されている場合でも、netstatで確認すると、localhost `127.0.0.1:9002` TCPソケットはリッスンモードになりません。サービスを再起動しようとすると、ハングアップします（「停止中...」）。`WebSocketService.exe`プロセスに適切な除外を適用してください。

  「プロセスモニター」(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/team-process-monitor.png)

  ii. **ユーザーセッションマッピング。** Microsoft Teamsアプリケーションが起動すると、WebSocketService.exeはVDAのユーザーセッションでWebSocketAgent.exeプロセスを開始します。WebSocketService.exeはLocalSystemアカウントとしてセッション0で実行されます。

  「WebSocketAgent.exeサービス」(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/websocketservice-websocketagent.png)

  VDAでWebSocketService.exeサービスがアクティブなリッスン状態にあるかどうかを確認するには、`netstat`を使用できます。

昇格されたコマンドプロンプトウィンドウから`netstat -anob -p tcp`を実行します。

「netstatの例を実行」(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/teams-netstat.png)

接続が成功すると、状態はESTABLISHEDに変わります。

「netstatの成功例」(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/teams-netstat-success.png)

重要:

WebSocketService.exeは、2つのTCPソケット（127.0.0.1:9001と127.0.0.1:9002）でリッスンします。ポート9001は、ブラウザコンテンツリダイレクトとHTML5ビデオのリダイレクトに使用されます。ポート9002は、Microsoft Teamsのリダイレクトに使用されます。Teams.exeとWebSocketService.exe間の直接通信を妨げる可能性のあるプロキシ構成がVDAのWindows OSにないことを確認してください。Internet Explorer 11で明示的なプロキシ（**インターネットオプション > 接続 > LANの設定 > プロキシサーバー**）を構成すると、接続が割り当てられたプロキシサーバーを経由する場合があります。手動および明示的なプロキシ設定を使用する場合は、**ローカルアドレスにはプロキシサーバーを使用しない**がチェックされていることを確認してください。

サービスの位置と説明

サービス	WINDOWS SERVER OSの実行可能ファイルへのパス	ログオンアカウント	説明
Citrix HTML5ビデオリダイレクトサービス	"C:\Program Files (x86)\Citrix\System32\WebSocketService.exe" /service	ローカルシステムアカウント	仮想デスクトップとエンドポイントデバイス間でメディアリダイレクトを実行するために必要な初期フレームワークを、複数のHDXマルチメディアサービスに提供します。
Citrix HDXブラウザリダイレクトサービス	"C:\Program Files (x86)\Citrix\System32\CtxSvcHost.exe" -g BrowserRedirSvcs	このアカウント（ローカルサービス）	エンドポイントデバイスと仮想デスクトップ間でブラウザ

サービス	WINDOWS SERVER OSの実行可能ファイルへのパス	ログオンアカウント	説明
			コンテンツリダイレクトを提供します。
Citrixポート転送サービス	"C:\Program Files (x86)\Citrix\System32\CtxSvcHost.exe" -g PortFwdSvcs	このアカウント（ローカルサービス）	ブラウザコンテンツリダイレクトのために、エンドポイントデバイスと仮想デスクトップ間でポート転送を提供します。
Citrix HDX Teamsリダイレクトサービス	"C:\Program Files (x86)\Citrix\System32\CtxSvcHost.exe" -g TeamsSvcs	ローカルシステムアカウント	エンドポイントデバイスと仮想デスクトップ間でMicrosoft Teamsリダイレクトを提供します。

シトリックス ワークスペース アプリ

ユーザーのエンドポイントでは、Windows用Citrix WorkspaceアプリがHdxTeams.exeまたはHdxRtcEngine.exeという新しいサービスをインスタンス化します。これは、VDAでMicrosoft Teamsが起動し、ユーザーがセルフプレビューで通話しようとしたり、周辺機器にアクセスしようとしたりするときに行われます。このサービスが表示されない場合は、以下を確認してください。

1. Windows 用 Workspace アプリ バージョン 1905 以降がインストールされていることを確認します。Workspace アプリのインストールパスに HdxTeams.exe または HdxRtcEngine.exe と webrpc.dll バイナリが表示されますか？
2. 手順1を確認したら、HdxTeams.exe または HdxRtcEngine.exe が起動しているかどうかを確認するために、次の操作を行います。
    a. VDA 上の Microsoft Teams を終了します。
    b. VDA で services.msc を起動します。
    c. Citrix HDX Teams Redirection Service を停止します。
    d. ICA® セッションを切断します。
    e. ICA セッションを接続します。
    f. Citrix HDX Teams Redirection Service を開始します。
    g. Citrix HDX HTML5 Video Redirection Service を再起動します。

h. VDA 上で Microsoft Teams を起動します。

3. クライアントエンドポイントで HdxTeams.exe または HdxRtcEngine.exe が起動しない場合は、次の操作を行います。

   a. VDA を再起動します。

   b. クライアントエンドポイントを再起動します。

サポート

Citrix と Microsoft は、Microsoft Teams の最適化を使用して、Citrix Virtual Apps and Desktops™ からの Microsoft Teams の配信を共同でサポートしています。この共同サポートは、両社の緊密な連携の成果です。有効なサポート契約があり、このソリューションで問題が発生した場合は、問題の原因となっていると思われるコードのベンダーにサポートチケットをオープンしてください。つまり、Teams の場合は Microsoft、最適化コンポーネントの場合は Citrix です。 Citrix または Microsoft がチケットを受け取り、問題をトリアージし、必要に応じてエスカレートします。各社のサポートチームに連絡する必要はありません。

問題が発生した場合は、Teams UI で **>** をクリックすることをお勧めします。VDA 側のログは、技術的な問題をより迅速に解決するために、Citrix と Microsoft の間で自動的に共有されます。

ログの収集

HDXメディアエンジンログはユーザーのマシン上（VDA上ではない）にあります。問題が発生した場合は、サポートケースにログを添付してください。

Windowsログ：

Windowsログは、**HDXTeams**フォルダー内の%TEMP%にあります（AppData/Local/Temp/HDXTeamsまたはAppData/Local/Temp/HdxRtcEngine）。webrpc_Day_Month_timestamp_Year.txtという名前の.txtファイルを探してください。Citrix Workspaceアプリの新しいバージョン（Citrix Workspaceアプリ2009.5以降など）を使用している場合は、ログをAppData\Local\Temp\HdxRtcEngineに保存します。

各セッションはログ用の個別のフォルダーを作成します。

Macログ：

1. VDWEBRTCログ - 仮想チャネルの実行を記録します。

   場所：`/Users/<User Name>/Library/Logs/Citrix Workspace/CitrixViewer_<Y_M_D_H_M_S>.txt`

2. HdxRtcEngineログ - HdxRtcEngine上のプロセスの実行を記録します。

場所: `$TMPDIR/hdxrtcengine/<W_M_D_H_M_S_Y>/hdxrtcengine.log`

HdxRtcEngineログはデフォルトで有効になっています。

3. Webrpcログ - webrtcライブラリのラップアップの実行を記録する最も重要なログです。

場所: `/Users/<USERNAME>/Library/Logs/HdxRtcEngine/<W_M_D_H_M_S_Y>/webrpc.log`

Linuxログ：

Linuxログは`/tmp/webrpc/<current date>/ and /tmp/hdxrtcengine/<current date>/`フォルダーにあります。 Webrtcログ：`/tmp/webrpc/<current date>/webrtc.log` カーネルログ：`/var/log/syslog`

ICE/STUN/TURN/ログ：

通話を確立する際には、次の4つのICEフェーズが必要です。

- 候補収集
- 候補交換
- 接続チェック (STUNバインド要求)
- 候補昇格

HdxRtcEngine.exeログでは、以下のエントリが関連するInteractive Connectivity Establishment (ICE) エントリです。これらのエントリは、通話設定が成功するために必要です。収集段階のサンプルスニペットを以下に示します。

```
RPCStubs Info: -> device id = \\?
\display#int3470#4&1835d135&0&uid13424#{65e8773d-8f56-11d0-
a3b9-00a0c9223196}\{bf89b5a5-61f7-4127-a279-e187013d7caf} label =
Microsoft Camera Front groupId =



webrtcapi.RTCPeerConnection Info: createOffer. audio = 1 video = 1

webrtcapi.RTCPeerConnection Info: setLocalDescription.

>>> begin:sdp

[…]
```

```
webrtcapi.RTCPeerConnection Info: OnSignalingChange. signaling state =
HaveLocalOffer



webrtcapi.RTCPeerConnection Info: OnIceGatheringChange. state = Gathering



[…]

>>> begin:sdp

candidate:840548147 1 udp 2122194687 10.108.124.215 56927 typ host
generation 0 ufrag oVk6 network-id 1

<<< end:sdp

[…]

>>> begin:sdp

candidate:1938109490 1 udp 24911871 52.114.xxx.xxx 52786 typ relay raddr
73.205.xxx.x rport 25651 generation 0 ufrag dDML network-id 1 network-cost
10

<<< end:sdp

[…]

>>> begin:sdp

candidate:4271145120 1 udp 1685987071 66.xxx.xxx.xxx 55839 typ srflx raddr
10.108.124.215 rport 55839 generation 0 ufrag uAVH network-id 1

<<< end:sdp

[…]



webrtcapi.RTCPeerConnection Info: OnIceGatheringChange. state = Complete
webrtcapi.RTCPeerConnection Info: setRemoteDescription.
```

```
>>> begin:sdp

[…]



webrtcapi.RTCPeerConnection Info: OnSignalingChange. signaling state =
HaveRemotelOffer
```

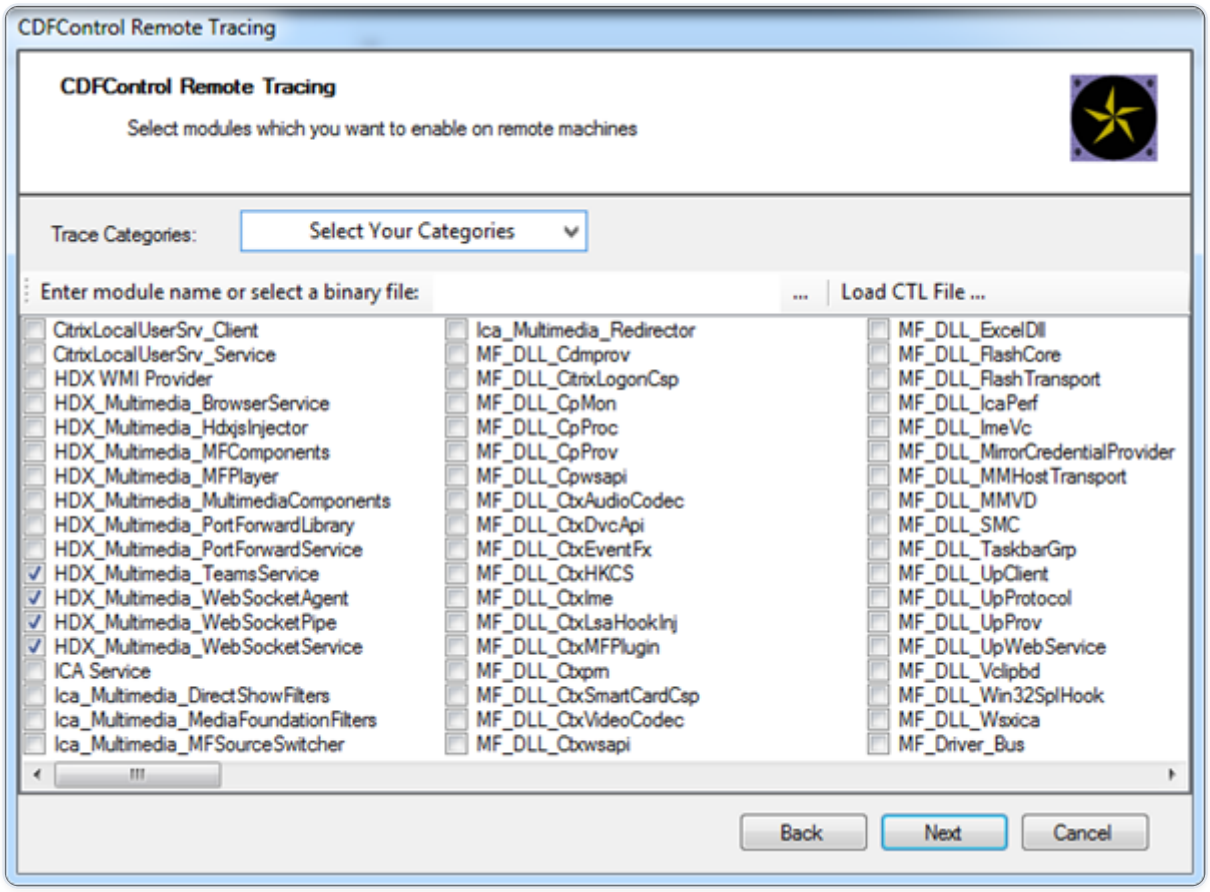
複数のICE候補がある場合、優先順位は次のとおりです。

1. ホスト
2. ピア反射型
3. サーバー反射型
4. トランスポートリレー

問題が発生し、それを一貫して再現できる場合は、Microsoft Teamsで**ヘルプ > 問題の報告**をクリックすることをお勧めします。Microsoftにケースをオープンした場合、技術的な問題を解決するためにログがCitrixとMicrosoftの間で共有されます。 Citrixサポートに連絡する前にCDFトレースをキャプチャすることも有益です。詳細については、Knowledge Centerの記事CDFcontrolを参照してください。

CDFトレース収集の推奨事項については、Knowledge Centerの記事Recommendations for Collecting the CDF Tracesを参照してください。

VDA側CDFトレース - 次のCDFトレースプロバイダーを有効にします。



Workspaceアプリ側CDFトレース - 次のCDFトレースプロバイダーを有効にします。

Workspace App 側の CDF トレース(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/team-cwa-cdf-traces.png)

- IcaClient_DriversVd_TeamsRedir (オプション)
- IcaClient_Multimedia_HdxTeams (Citrix Workspace app 2012 以降が必要)

Windows Media リダイレクト

Windows Media リダイレクトは、サーバーがストリーミングオーディオとビデオをユーザーに配信する方法を制御し、最適化します。メディアのランタイムファイルをサーバーではなくクライアントデバイスで再生することで、Windows Media リダイレクトは、マルチメディアファイルの再生に必要な帯域幅を削減します。Windows Media リダイレクトは、仮想Windowsデスクトップで実行されているWindows Media Playerおよび互換性のあるプレーヤーのパフォーマンスを向上させます。

Windows Media クライアント側コンテンツフェッチの要件が満たされない場合、メディア配信は自動的にサーバー側フェッチを使用します。この方法はユーザーには透過的です。使用されている方法を特定するには、Citrix Scoutを使用してHostMMTransport.dllからCitrix Diagnosis Facility

(CDF) トレースを実行できます。詳しくは、「Citrix Scout」(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/manage-deployment/cis/scout.html)を参照してください。

Windows Media リダイレクトは、ホストサーバーでメディアパイプラインをインターセプトし、メディアデータをネイティブの圧縮形式でキャプチャし、コンテンツをクライアントデバイスにリダイレクトします。クライアントデバイスは、ホストサーバーから受信したメディアデータを解凍してレンダリングするために、メディアパイプラインを再構築します。Windows Media リダイレクトは、Windowsオペレーティングシステムを実行しているクライアントデバイスでうまく機能します。これらのデバイスには、ホストサーバーに存在していたメディアパイプラインを再構築するために必要なマルチメディアフレームワークがあります。Linuxクライアントは、同様のオープンソースメディアフレームワークを使用してメディアパイプラインを再構築します。

ポリシー設定の**Windows Media リダイレクト**は、この機能を制御し、デフォルトで**許可**されています。通常、この設定により、サーバーからレンダリングされるオーディオおよびビデオの品質が、クライアントデバイスでローカルに再生されるコンテンツに匹敵するレベルに向上します。まれに、Windows Media リダイレクトを使用して再生されるメディアが、基本的なICA®圧縮と通常のオーディオを使用してレンダリングされるメディアよりも悪く見えることがあります。この機能を無効にするには、**Windows Media リダイレクト**設定をポリシーに追加し、その値を**禁止**に設定します。

ポリシー設定について詳しくは、「マルチメディアポリシー設定」(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/policies/reference/ica-policy-settings/multimedia-policy-settings.html)を参照してください。

制限事項:

セッション内でWindows Media PlayerとRemote Audio & Video Extensions (RAVE) を有効にしている場合、黒い画面が表示されることがあります。この黒い画面は、ビデオコンテンツを右クリックして**常に「再生中」を最前面に表示**を選択した場合に表示されることがあります。

仮想チャネルプラグインマネージャー

はじめに

仮想チャネルプラグインマネージャーは、指定されたアプリケーション向けにクライアントエンドポイント全体にプラグインを展開するように設計されています。プラグインマネージャーは、VDAで実行されている特定のアプリケーションを検出し、アプリケーションの実行時に最高の体験を得るために、エンドポイントにプラグインをインストールするようユーザーに促します。

ユーザーは、プラグインをインストールするか、スキップするか、またはインストールを拒否するかを選択できます。プラグインマネージャーは、管理対象か非管理対象かを問わず、すべてのエンドポイントでプラグインを管理する柔軟性を提供します。

例: Microsoft Teams は新しいアーキテクチャ (SlimCore Optimization) を採用しており、最適化を機能させるにはエンドポイントにプラグインをインストールする必要があります。仮想チャネルプラグインマネージャーは、エンドポイント全体にプラグインを展開できます。詳細については、Teams の新しい VDI ソリューション を参照してください。

システム要件

仮想チャネルプラグインマネージャーの最小要件は次のとおりです。

- 仮想デスクトップエージェント (VDA)
  - 2411
  - 2402 LTSR CU2
- DDC
  - Cloud 121 リリース
  - 2407 CR
  - 2402 LTSR CU1
- Citrix Workspace™ アプリ (Citrix Workspace アプリ)
  - Windows 2409 用 Citrix Workspace アプリ

> **注：**
>
> この機能は現在、Windowsエンドポイントに適用されます。

サポートされるアプリケーション

- 現在サポートされているアプリケーションは以下のとおりです。
  - Microsoft Teams - Teams の新しい VDI ソリューション を参照してください。

仮想チャネルプラグインマネージャー

機能の理解

Citrix® は、お客様の環境が複雑になる可能性があり、管理対象および管理対象外のエンドポイント全体にプラグインを展開するにはかなりの労力が必要であることを理解しています。この機能は、そのプロセスを簡素化するように設計されています。

この機能には2つのコンポーネントが含まれています。1つはVDA側（検出プロセス）、もう1つはCitrix Workspace™ App側（インストーラープロセス）です。管理者が、ポリシーの有効化、レジストリエントリの作成、監視するアプリケーションの指定など、上記の前提条件を満たすと、次のようになります。

- VDA側の検出プロセスは、エンドユーザーが仮想デスクトップにログオンすると、アプリケーションの起動を監視します
- 検出プロセスはCitrix Workspace App側に通知し、指定されたアプリケーションを最適化するために必要なプラグインをインストールするようユーザーに促します
- ユーザーは画面にプラグインに関する簡単な詳細情報が表示されたポップアップを受け取ります。ユーザーはプラグインをインストールするか、スキップするか、またはインストールしないことを選択できます。
    - ユーザーがインストールプロセスをスキップした場合、そのセッションではポップアップが再度表示されません。インストールプロンプトはセッションの再接続時に表示されます。
    - ユーザーがプラグインをインストールしないことを選択した場合、その選択はユーザープロファイルに記録され、管理者が確認できるようになります。
- ユーザーがプラグインをインストールすることを選択した場合、Citrix Workspace App側がエンドポイントにプラグインをダウンロードしてインストールします。
    - インストールが成功すると、プラグインを有効にするためにセッションを再接続するようユーザーにメッセージが表示されます。ユーザーはすぐに再接続するか、成功メッセージを閉じて後で再接続するかを選択できます。
    - インストールが失敗した場合、ユーザーにはエラーメッセージが表示され、失敗は管理者が確認できるように記録されます。

仮想チャネルプラグインマネージャー

展開

1. Microsoft Teamsリダイレクトポリシーが有効になっているか確認します。詳細については、Microsoft Teamsリダイレクトポリシーを参照してください。

   このポリシーは、監視対象のアプリケーションに関わらず有効にする必要があります。将来、より多くのアプリケーションがサポートされ、Microsoft Teamsの代わりにそれらのアプリケーションを監視したい場合でも、このポリシーは有効にしておく必要があります。このポリシーはデフォルトで有効になっています。

2. 仮想チャネルプラグインマネージャーポリシーを有効にする必要があります。ポリシーを有効にする方法の詳細については、仮想チャネルプラグインマネージャーポリシー設定を参照してください。

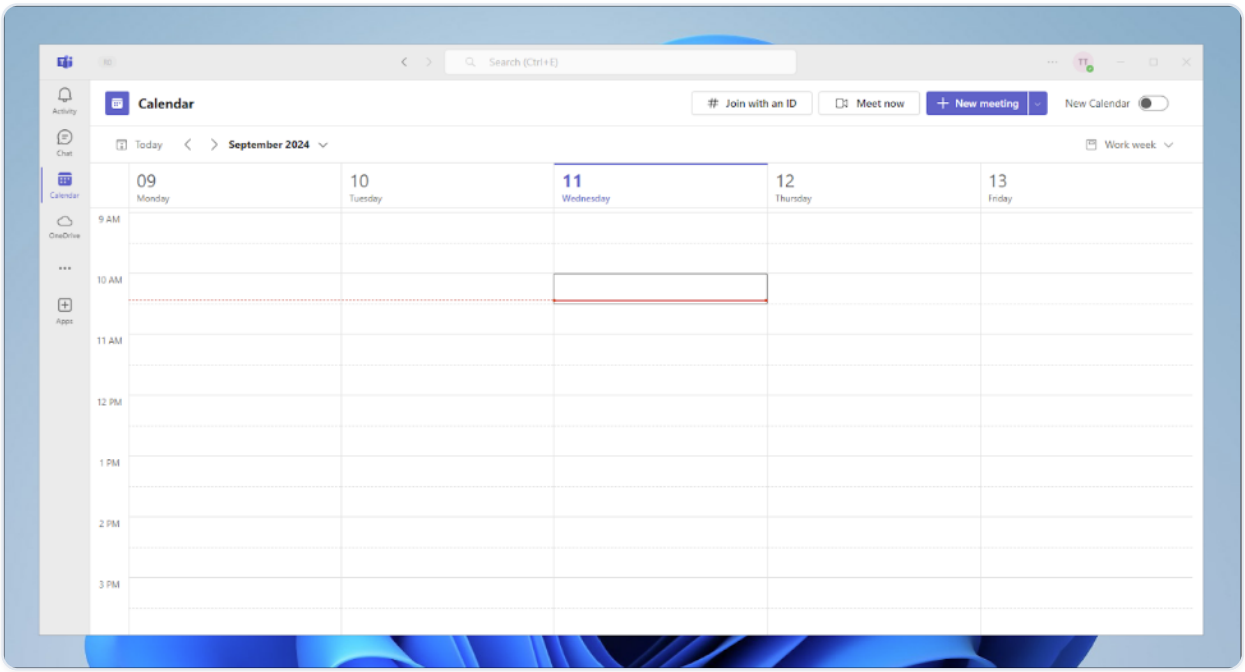
   このポリシーは、Citrix Studioのマルチメディアポリシー設定で利用できます。このポリシーを有効にすると、監視するアプリケーション名（例: 「Microsoft Teams」）を指定できます。このポリシーはデフォルトで無効になっています。

3. Citrix Workspace™アプリはシステムワイドモードでインストールする必要があります。

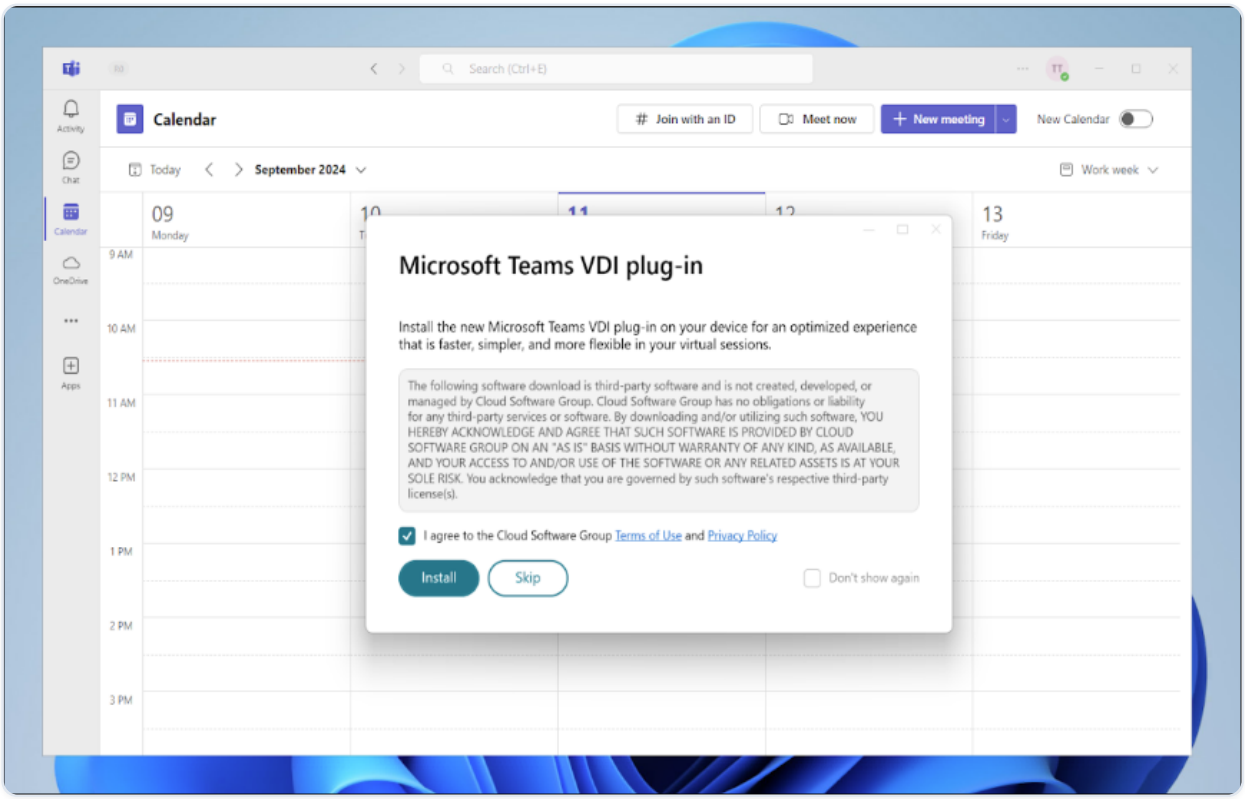
> **注：**
>
> プラグインは、サードパーティのCDNからエンドポイントにダウンロードされます。たとえば、Microsoft Teamsを選択した場合、プラグインはMicrosoft CDNからダウンロードされます。したがって、エンドポイントはサードパーティのCDNにアクセスできる必要があります。そうでない場合、プラグインのインストールは失敗します。

手順

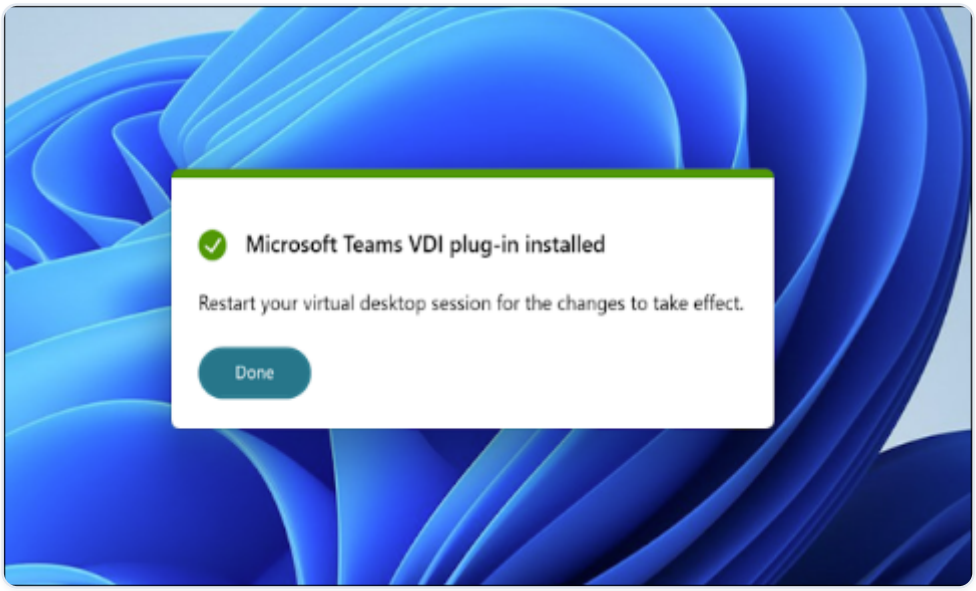
1. ユーザーはCitrixセッションでアプリケーションを起動します。例: Microsoft Teams。



2. ユーザーは、より良いエクスペリエンスのためにエンドポイントにTeams VDIプラグインをインストールするためのポップアップを受け取ります。プラグインはエンドポイントにインストールされるため、ポップアップはセッション内ではなくセッションの上に表示されます。



3. ユーザーがインストールボタンをクリックすると、プラグインがインストールされます。変更を有効にするには、仮想デスクトップセッションを再起動する必要があります。



既知の問題と制限事項

- 2407 VDAでは、機能をアクティブ化するためにポリシーに加えて、以下のレジストリ設定をVDA上で1に設定する必要があります。このレジストリ設定は、2411 VDA以降では自動的に許可され、構成する必要はありません。

  `HKLM\SOFTWARE\Citrix\HDXMediaStream

  Name: EnableAppDetector Type: DWORD`

- 今後、制限事項が追加される予定です

ユニファイドコミュニケーションSDKの最適化

はじめに

Citrix Virtual Apps and Desktopsを使用すると、さまざまなエンドポイントデバイス上のユーザーにアプリケーションを配信できます。これらのアプリケーションの多くには、音声会議やビデオ会議などのリアルタイム通信 (RTC) 機能が含まれています。しかし、仮想化環境でこれらのアプリケーションを配信する際には課題が生じることがあります。従来の配信方法では、メディアストリーム (オーディオ/ビデオ) をクライアントデバイスからデータセンター内のVDIサーバーにルーティングし、その後エンドポイントに送り返します。この「ヘアピン化」は、特に帯域幅を大量に消費するオーディオおよびビデオ通話において、サーバーに不要なトラフィックと処理オーバーヘッドをもたらします。

Citrix Unified Communications SDK (UCSDK) は、テクノロジーベンダーがこれらのRTCアプリケーションをCitrix環境で使用するために最適化できるようにするテクノロジーです。アプリケーションが最適化されると、ローカルデスクトップで実行されているアプリケーションと同等か、

それ以上のユーザーエクスペリエンスを提供できます。今日の世の中では、シームレスなリアルタイム通信は生産性とコラボレーションに不可欠です。仮想環境内でアプリケーションを使用する場合、音声通話やビデオ通話、画面共有、その他の通信機能がローカルデスクトップと同じくらいスムーズに動作することが重要です。最適化されたアプリケーションは、このエクスペリエンスを提供します。

この製品ドキュメントでは、Citrixのお客様がUCSDK最適化アプリケーションを学習し、展開するために必要なすべてを詳しく説明します。

動作の仕組み

Citrixは、VDI内のリアルタイム通信アプリケーション向けに最適化された配信方法を提供しています。このアプローチでは、Unified Communications SDK (UCSDK) を活用して、仮想化されたアプリケーションを次の2つの部分に分割します。

- **ユーザーインターフェイス (UI):** ユーザーインターフェイスは仮想ホスト内に残り、仮想デスクトップまたはアプリケーションウィンドウ内にシームレスに表示されます。
- **メディアエンジン:** メディア処理タスク (オーディオとビデオのエンコード/デコード) は、ユーザーのローカルデバイスにオフロードされます。これにより、サーバーの負荷が最小限に抑えられ、ネットワーク使用量が最適化されます。

通常、Citrixはリアルタイム通信分野のテクノロジーベンダーにUCSDKを提供し、それらのアプリケーションにUCSDKを統合するために協力しています。統合されると、UCSDK最適化アプリケーションを使用するCitrixのお客様は、強化されたエクスペリエンスを得ることができます。Citrix UCSDKは、カスタムの社内アプリケーションが構築されている場合にも、Citrixのお客様が利用できます。ただし、ほとんどの場合、お客様はUCSDKを利用して開発する必要はなく、最適化されたエクスペリエンスを実現するためにCitrix環境とアプリケーションを構成するだけで済みます。

> **注：**
>
> Citrix WebRTC SDK (または) HDX™最適化アプリケーションへの言及は、Citrix UCSDKとの統合を示しており、互換的に使用できます。

主な利点

Citrix UCSDKで最適化されたアプリケーションを使用する場合、次のことが期待できます。

- プロセッサ負荷の高いメディアエンコード/デコードをCitrix Virtual Delivery Agent (VDA) からクライアントエンドポイントにオフロードすることで、メディア処理パフォーマンスが向上し、エンドユーザーの全体的な応答性が高まります。
- Citrix VDAでのCPUおよび帯域幅使用量が削減され、IT部門はホストあたりの同時ユーザー数を増やし、企業はCitrix仮想デスクトップの展開を費用対効果の高い方法で拡張できます。
- 最適化されたエンドポイントがレガシー仮想デスクトップの寿命を延ばし、ホストインフラストラクチャの必要性を減らすため、企業の総所有コストが削減され、時間の経過とともに設備投資と運用コストが削減されます。
- Windows、Mac、Linux、ChromeOS、およびHTML5エンドポイントプラットフォームのサポート。

ユースケース

UCSDKは、WebRTC標準に準拠したリアルタイム通信アプリケーションを最適化するために特別に構築されています。以下に、UCSDKを使用できる/すでに使用しているWebRTCベースのアプリケーションの主要なシナリオと種類を示します。

- **サービスとしてのコンタクトセンター (CCaaS) / クラウドコンタクトセンタープラットフォーム:** 主に複数のチャネルにわたる顧客とのやり取りを管理し、エージェントのワークフローを最適化します。
    - 例: アマゾン コネクト、トゥイリオ、アバイア エクスペリエンス プラットフォーム、トークデスク、コンテンツ グル
- **サービスとしてのユニファイドコミュニケーション (UCaaS) / クラウドビジネスコミュニケーション:** 音声、ビデオ、チームメッセージング、プレゼンスを統合し、包括的なビジネスコミュニケーションを実現します。
    - 例: リング セントラル、8x8、インターメディア、アルカテル・ルーセント レインボー
- **サービスとしてのコミュニケーションプラットフォーム (CPaaS):** リアルタイム通信機能をカスタムアプリケーションに直接組み込むためのAPIを提供します。
    - 例: トゥイリオ、リボン コミュニケーションズ
- **エンタープライズビデオ会議およびコラボレーション:** 高品質なビデオ会議、カンファレンス、高度なコラボレーション機能のための専用プラットフォームです。
    - 例: Pexip

- **金融取引通信:** 金融市場の独自の、高性能でコンプライアンスに準拠した通信ニーズのために設計されています。
    - 例: IPC Unigy
- **仮想学習およびトレーニングプラットフォーム:** インタラクティブで高品質な仮想教室およびトレーニング体験のために設計されています。
    - 例: ヴィテロ

Citrix UCSDKの基盤となるWebRTCは、その最適化機能がWebRTCベースのあらゆる通信アプリケーションに拡張できることを意味します。これにより、現在UCSDKで最適化されているとリストされていないアプリケーションであっても、リアルタイムインタラクションにWebRTCを利用する幅広いアプリケーションを最適化する道が開かれます。お客様には、最適化を希望するユースケースやアプリケーションについてCitrixにお問い合わせいただくことをお勧めします。

UCSDK アーキテクチャ

UCSDK アーキテクチャ (/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/ucsdk-architecture.png)

- ベンダーアプリケーション: これは、UCSDK を統合した、デスクトップベースまたはブラウザベースのサードパーティ製リアルタイム通信アプリケーションです。
- UCSDK JS: UCSDK JS は、ベンダーアプリケーションがオーディオ/ビデオをエンドポイントにオフロードするために利用する API を提供します。
- HdxRtcEngine: これは、Citrix Workspace アプリに組み込まれている WebRTC メディアエンジンで、オフロードされたオーディオ/ビデオ通話を処理および管理します。

SDK がロードされて使用されると、リダイレクトが成功した場合、クライアントエンドポイントで `HdxRtcEngine.exe` プロセスが起動されます。クライアントエンドポイントで `HdxRtcEngine.exe` が起動されると、すべてのシグナリングおよびペイロードデータは Citrix VDA からクライアントエンドポイントに流れ、クラウドに到達し、クライアントエンドポイントに戻ってから VDA に転送されます。たとえば、フローの完全な往復は次のようになります。

`Vendor App -> CitrxWebrtc.js SDK -> Citrix VDA components -> Citrix Client Endpoint components -> Cloud -> Citrix Client Endpoint components -> Citrix VDA components -> CitrxWebrtc.js SDK -> Vendor App`

システム要件

システム要件は、UCSDK の最新バージョン (5.0.0) で必要となる Citrix コンポーネントのさまざまなバージョンを示しています。SDK の古いバージョンおよび特定の機能要件に関する互換性の詳細については、以下の バージョンと機能マトリックス の表を参照してください。

注：

お客様が UCSDK に追加された機能を使用するには、ベンダーアプリケーションが適切な UCSDK バージョンを統合し、その機能を有効にしていること、および環境で適切な VDA および CWA バージョンを使用していることを確認してください。

完全互換バージョン

完全互換バージョンとは、これらのバージョンの Citrix コンポーネントを UCSDK の最新バージョンと組み合わせて使用することで、お客様が利用可能なすべての機能を活用できることを示します。UCSDK の現在の最新バージョン (5.0.0) の場合、Citrix コンポーネントの完全互換バージョンは以下のとおりです。

- **Citrix 仮想アプリおよびデスクトップ:** 2603
- **Citrix Workspace アプリ ウィンドウズ:** 2603
- **Citrix Workspace App Mac:** リリース予定
- **Citrix Workspace アプリ リナックス:** 2603
- **Citrix Workspace App ChromeOS/HTML5:** リリース予定

注：

UCSDK最適化は、Windows、Mac、Linux、ChromeOS、HTML5のすべてのエンドポイントプラットフォームでサポートされています。上記のリストで特定のEndpoint Platformに「リリース予定」と表示されている場合、それは最新のUCSDK機能と完全に互換性のあるバージョンがまだリリースされていないことを意味します。したがって、お客様は、新しいUCSDKを使用している場合でも、Citrix Workspaceアプリの古いバージョンを使用して既存の機能を継続して使用できます。

構成

UCSDKの機能は、ベンダーが統合したUCSDKのバージョンとベンダーが有効にした機能、Citrix Virtual Apps and Desktops、および使用中のCitrix Workspaceアプリのバージョンの3つの要因に依存します。

Citrix側では、最適化されたアプリケーションが最適化されるように、以下が構成されていることを確認してください。

1. Microsoft Teamsリダイレクトポリシーがオンになっていることを確認します。詳細については、マルチメディアポリシー設定を参照してください。このポリシーはデフォルトでオンになっています。
2. `CitrixWebrtc.js` SDKを利用するサードパーティのElectronまたはブラウザベースのアプリケーションは、デフォルトではサポートされていません。`CtxHdxWebSocketService` (`WebSocketService.exe`) は、許可リストにないアプリケーションからの接続を許可しません。目的のアプリケーションバイナリ実行可能ファイル名をホワイトリストレジストリキーに追加する必要があります。

> **注：**
>
> CVAD 2603以降、Citrix Unified Communications SDK (UCSDK) を使用するアプリケーションの最適化は、「Microsoft Teamsリダイレクト」ポリシーに依存しなくなりました。管理者は、他のUCSDK統合アプリケーションに影響を与えることなく、Microsoft Teamsの最適化を無効にできるようになりました。この分離を使用するには、ベンダーアプリケーションがCVAD 2603と並行してBootstrapメソッド（UCSDK 4.0で初めて導入）を利用する必要があることに注意してください。詳細については、UCSDKとHDX Microsoft Teams最適化の分離を参照してください。

VDA上

- キーパスを作成します: `HKLM\Software\WOW6432Node\Citrix\WebSocketService`
- キー名: `ProcessWhitelist`
- 種類: `MULTISZ`
- キー値: `Mytestapp.exe`

複数のアプリケーションがある場合は、各アプリケーションを新しい行に入力します。テキストファイルからコピー＆ペーストしたり、コンマを挿入したりしないでください。指定された名前

がアプリケーションの実行可能ファイル名と一致していることを確認してください。このレジストリ値は大文字と小文字を区別しません。

アプリケーションが本格的なデスクトップアプリケーションではなくブラウザ経由でアクセスされる場合、レジストリ値で例えば`chrome.exe`を許可する必要があります。

上記のレジストリが正常に構成されたら、VDAを再起動するか、`CtxHdxWebSocketService`を再起動してホワイトリストの設定を完了します。

クライアント上

設定は不要です。Citrix Workspaceアプリをインストールするだけです。

各ベンダーは非常に具体的なアプリケーション名を持っている場合があります。したがって、WebSocketServiceで許可する必要があるアプリケーション名を決定するには、現在のベンダーサポートセクションにリンクされているベンダーのドキュメントを参照してください。

機能リファレンス

Smart Syncによる通話接続時間の短縮

UCSDK 5.0.0で導入されたSmart Sync機能は、VDAとクライアントエンドポイント間の通信を効率化することで、通話接続時間を短縮します。この機能強化により、全体的に通話設定が高速化され、特に高遅延ネットワーク環境で最も顕著なパフォーマンス向上が実現されます。

Citrixは、この機能を活用するために、お客様がアプリケーションベンダーに連絡してUCSDK 5.0.0にアップグレードすることを推奨します。

> **注：**
>
> この機能は、UCSDK 5.0.0とCitrix Workspaceアプリのみに依存します。正確なクライアントバージョンについては、バージョンと機能マトリックスを参照してください。VDAのバージョン依存性はないため、以前のサポートされているVDAも引き続き使用できます。

バージョンと機能マトリックス

バージョン更新は頻繁に行われるため、特定のバージョンがサポートされていることを確認するには、Citrix Virtual Apps and DesktopsおよびCitrix Workspace appの製品ライフサイクルページを参照してください。多くの古い機能については、表に記載されているバージョンは、このドキュメントの作成時点での最終サポート対象のCurrent Release (CR) バージョンです。

機能	UCSDK バージョン	VDA	CWA ウィンドウズ	CWA MAC	CWA リナックス	CWA CHROME OS/ HTML5
オーディオ/ビデオ (p2p & 会議)	3.1.0	2203 LTSR 最新 CU / 2311 CR	2402 LTSR 最新CU / 2311 CR	2311	2311	2312
画面共有	3.1.0	2203 LTSR 最新 CU / 2311 CR	2402 LTSR 最新CU / 2311 CR	2311	2311	2312
DTMF	3.1.0	2203 LTSR 最新 CU / 2311 CR	2402 LTSR 最新CU / 2311 CR	2311	2311	2312
プロキシサーバーのサポート	3.1.0	2203 LTSR 最新 CU / 2311 CR	2402 LTSR 最新CU / 2311 CR	2311	2311	2312
アプリ共有	3.1.0	2203 LTSR 最新 CU / 2311 CR	2402 LTSR 最新CU / 2311 CR	2311	2311	該当なし
動的e911	3.1.0	2203 LTSR 最新 CU / 2311 CR	2402 LTSR 最新CU / 2311 CR	2311	2311	2312
マルチウィンドウ	3.1.0	2203 LTSR 最新 CU / 2311 CR	2402 LTSR 最新CU / 2311 CR	2311	2311	2312
SDP統合プランのサポート	3.1.0	2203 LTSR 最	2402 LTSR 最	2311	2311	2312

機能	UCSDK バージョン	VDA	CWA ウィンドウズ	CWA MAC	CWA リナックス	CWA CHROME OS/ HTML5
		新 CU / 2311 CR	新CU / 2311 CR			
ストリーム解像度 / シマルキャスト	3.1.0	2203 LTSR 最新 CU / 2311 CR	2402 LTSR 最新CU / 2311 CR	2311	2311	2312
リモートオーディオ (ループあり)	3.1.0	2203 LTSR 最新 CU / 2311 CR	2402 LTSR 最新CU / 2311 CR	2311	2311	2405
ブラウザベースの UCSDK (ブートストラップサポート)	4.0.2	2407 CR	2402 LTSR 最新CU / 2311 CR	2311	2311	2312
Web HID API	4.0.2	2203 LTSR 最新 CU / 2311 CR	2409.10	2411	2411	2505
ウェブオーディオAPI	4.0.2	2203 LTSR 最新 CU / 2311 CR	2405	2405	2405	該当なし
ICE の再起動	4.1.0	2203 LTSR 最新 CU / 2311 CR	2503.2	2503	2503	2502.10
画面録画 (プレビュー)[1]	4.1.0	2503	2503.2	該当なし	該当なし	該当なし

機能	UCSDK バージョン	VDA	CWA ウィンドウズ	CWA MAC	CWA リナックス	CWA CHROME OS/ HTML5
スマートシンク	5.0.0	2203 LTSR 最新 CU / 2311 CR	2603	該当なし	2604	該当なし

注：

画面録画用の新しいポリシーを導入したため、CVAD 2503に付属するdelivery controller™のバージョン2503が必要です。

現在のベンダーサポート

複数のサードパーティベンダーが、Unified Communications SDKを自社製品に統合しています。ベンダーとそのサポートドキュメントの現在のリストは以下のとおりです。

ベンダー	ドキュメント
スプリンクラー	Citrix 音声通話用メディアオフロード - スプリンクラー
アマゾンコネクト	Citrix Cloud Desktops 向け Amazon Connect オーディオの最適化
リングセントラル	Citrix VDI 環境での RingCentral の使用
ファイブナイン	Citrix 環境での Five9 WebRTC
トゥイリオ	Citrix VDIにおけるTwilio Flex
アバイア	「Citrix向けAvaya Experience Platform Public Cloud VDIソリューション」(https://documentation.avaya.com/bundle/ExperiencePlatform_Administering_10/page/Avaya__Experience_Platform_VDI_solution_for_Citrix_1.html)

ベンダー	ドキュメント
8x8	Citrix VDIとデスクトップおよびウェブ向け8x8 Workの統合
コンテンツ・グル	カンテン・グル Citrix統合
リボン・コミュニケーションズ	リボン・コミュニケーションズ Citrix WebRTC SDK
インターメディア	「Citrix Virtual Apps and DesktopsへのIntermedia Uniteのインストール」(https://support.intermedia.com/app/articles/detail/a_id/24355)
アルカテル・ルーセント・レインボー	「Rainbowデスクトップアプリケーション向けCitrix最適化」(https://help.openrainbow.com/hc/ja-jp/articles/23752823816850-CITRIX-Optimization-for-Rainbow-Desktop-application)
トークデスク	Talkdesk Agent Workspace VDI コネクト
IPC	IPC Unigy ソフトクライアント Citrix VDI
ヴィテロ	Citrix VDI 向けヴィテロ インスパイア
ペクシプ	Citrix Pexip Infinity Docs で Connect デスクトップアプリを展開する
ズーム ウェブアプリ	Zoom Web App の WebRTC リダイレクトを構成する

トラブルシューティング

トラブルシューティング情報については、Citrix Unified Communications SDK で最適化されたアプリのトラブルシューティングガイダンスを参照してください。

既知の問題と制限事項

このセクションでは、現在認識されている既知の問題と制限事項について説明します。

一般的なコンテンツリダイレクト

コンテンツリダイレクトを使用すると、ユーザーがサーバーで公開されているアプリケーションを使用するか、ユーザーデバイスでローカルに実行されているアプリケーションを使用するかによって、情報にアクセスする方法を制御できます。

クライアントフォルダーリダイレクト(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/general-content-redirection/client-folder-redirection.html)

クライアントフォルダーリダイレクトは、クライアント側のファイルがホスト側のセッションでアクセス可能になる方法を変更します。

- サーバーでクライアントドライブマッピングのみを有効にすると、クライアント側のフルボリュームは、Universal Naming Convention (UNC) リンクとしてセッションに自動的にマッピングされます。
- サーバーでクライアントフォルダーリダイレクトを有効にし、ユーザーがWindowsデスクトップデバイスでそれを構成すると、ユーザーが指定したローカルボリュームの一部がリダイレクトされます。

ホストからクライアントへのリダイレクト(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/general-content-redirection/host-to-client-redirection.html)

特定のまれなユースケースでは、ホストからクライアントへのリダイレクトの使用を検討してください。通常、他の形式のコンテンツリダイレクトの方が優れている場合があります。このタイプのリダイレクトは、マルチセッションOS VDAでのみサポートされており、シングルセッションOS VDAではサポートされていません。

ローカルアプリアクセスとURLリダイレクト(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/general-content-redirection/laa-url-redirect.html)

ローカルアプリアクセスは、ローカルにインストールされたWindowsアプリケーションをホストされたデスクトップ環境にシームレスに統合します。これは、あるコンピューターから別のコンピューターに切り替えることなく行われます。

HDX™テクノロジーは、最適化されたサポートがない、または不適切な特殊デバイス向けに**汎用USBリダイレクト**を提供します。

クライアントフォルダーリダイレクト

クライアントフォルダーリダイレクトは、クライアント側のファイルがホスト側のセッションでアクセスされる方法を変更します。サーバーでクライアントドライブマッピングのみを有効にすると、クライアント側の完全なボリュームは、Universal Naming Convention (UNC) リンクとしてセッションに自動的にマッピングされます。サーバーでクライアントフォルダーリダイレクトを有効にし、ユーザーがユーザーデバイスでそれを構成すると、ユーザーが指定したローカルボリュームの一部がリダイレクトされます。

ユーザーが指定したフォルダーのみが、セッション内でUNCリンクとして表示されます。つまり、ユーザーデバイス上の完全なファイルシステムではなく、指定されたフォルダーのみが表示されます。レジストリを介してUNCリンクを無効にすると、クライアントフォルダーはセッション内でマップされたドライブとして表示されます。

クライアントフォルダーリダイレクトは、WindowsシングルセッションOSマシンでのみサポートされています。

外部USBドライブのクライアントフォルダーリダイレクトは、デバイスの取り外しと再接続時に保存されません。

サーバーでクライアントフォルダーリダイレクトを有効にします。次に、クライアントデバイスで、リダイレクトするフォルダーを指定します。クライアントフォルダーオプションを指定するために使用するアプリケーションは、このリリースに付属のCitrix Workspace™アプリに含まれています。

要件:

サーバーの場合:

- ウィンドウズ サーバー 2022
- Windows Server 2019、StandardおよびDatacenterエディション
- Windows Server 2016、StandardおよびDatacenterエディション
- Windows Server 2012 R2、Standard および Datacenter エディション

クライアントの場合:

- Windows 10、32ビットおよび64ビットエディション（最小バージョン1607）
- Windows 8.1、32ビットおよび64ビットエディション（Embedded Editionを含む）
- Windows 7、32ビットおよび64ビットエディション（Embedded Editionを含む）

サーバーでクライアントフォルダーリダイレクトを有効にするには、レジストリを介して管理される機能のリストにあるクライアントフォルダーリダイレクトを参照してください。

ユーザーデバイスで、リダイレクトするフォルダーを指定します:

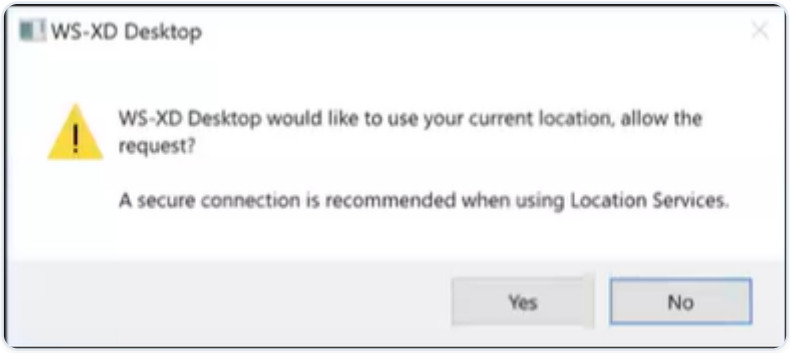
1. Citrix Workspaceアプリの最新バージョンがインストールされていることを確認します。
2. Citrix WorkspaceアプリのインストールディレクトリからCtxCFRUI.exeを起動します。
3. **Custom** ラジオボタンを選択し、フォルダーを追加、編集、または削除します。
4. 設定を有効にするには、セッションを切断して再接続します。

クライアント位置情報リダイレクト

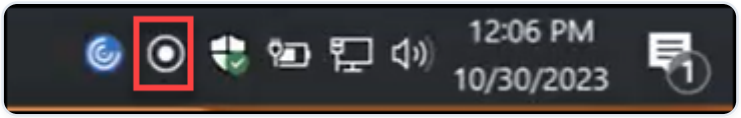
クライアント位置情報リダイレクトを有効にすると、VDAでホストされているアプリとデスクトップセッションが、クライアントの現在の位置情報にシームレスにアクセスできるようになります。マルチセッションオペレーティングシステム（TS VDAまたはマルチセッションWS VDA）では、各セッションは接続されたクライアントによって提供される独自の場所を持ちます。この機能を使用すると、位置情報に依存するVDA上のアプリケーションは、クライアントの正確な位置情報を取得できます。

詳細については、Microsoftドキュメントを参照してください。

クライアント位置情報リダイレクトが有効になり、サーバー側とクライアント側の両方で位置情報へのアクセスが許可されると、位置情報にアクセスするアプリケーションまたはデスクトップを起動したときに、クライアントは次のダイアログボックスで現在の位置情報を共有するように求めます。



クライアント位置情報リダイレクトを有効にすると、VDAでホストされているアプリまたはデスクトップが現在の位置情報を照会したときに、クライアントのタスクバーに次のアイコンが表示されます。



システム要件

サーバーの場合：

- シングルセッション（Win10/11）またはマルチセッション（Win 11 22H2およびServer 2022 23H2以降）OS VDA
- Windows、iOS、またはAndroid用Citrix Workspace™アプリ

構成

この機能が動作するには、Citrix®ポリシーを使用してクライアント位置情報リダイレクトを有効にする必要があります。クライアント位置情報リダイレクトはデフォルトで無効になっています。

クライアント位置情報リダイレクトを有効にするには、次の手順を実行します。

Windows VDAおよびクライアント側で：

1. **設定 > プライバシー > 位置情報**で、次のオプションを有効にします。
    - **このデバイスの位置情報へのアクセスを許可する**
    - **アプリが位置情報にアクセスできるようにする**
    - **デスクトップアプリに位置情報へのアクセスを許可する**
2. マルチセッションOSの場合、**Location Override**設定を有効にします。

Controller/DDC側で:

Studio > ポリシー > 位置情報 > 設定 > アプリケーションがクライアントデバイスの物理的な位置情報を使用することを許可するポリシーを有効にします。 詳細については、クライアントセンサーポリシー設定を参照してください。

双方向コンテンツリダイレクト

双方向コンテンツリダイレクトにより、Webブラウザー内のHTTPまたはHTTPS URL、あるいはアプリケーションに埋め込まれたURLを、Citrix VDAセッションとクライアントエンドポイント間で双方向に転送できます。Citrixセッションで実行されているブラウザーに入力されたURLは、クライアントのデフォルトブラウザーを使用して開くことができます。逆に、クライアントで実行されているブラウザーに入力されたURLは、公開アプリケーションまたはデスクトップのいずれかを使用して、Citrixセッションで開くことができます。双方向コンテンツリダイレクトの一般的なユースケースには、次のようなものがあります。

- 開始ブラウザーがソースへのネットワークアクセスを持たない場合のWeb URLのリダイレクト。
- ブラウザーの互換性およびセキュリティ上の理由によるWeb URLのリダイレクト。
- Citrixセッションまたはクライアントでブラウザーを実行したくない場合に、アプリケーションに埋め込まれたWeb URLのリダイレクト。

システム要件

- シングルセッションまたはマルチセッションOS VDA
- Citrix Workspace™ アプリ for Windows 2311 以降
- Citrix Workspace™ アプリ for Linux 2503 以降
- Citrix Workspace™ アプリ for Mac 2607 以降

ブラウザー：

- Citrix ブラウザリダイレクト拡張機能を使用する Google Chrome
  - Google Chrome 拡張機能
- Citrix ブラウザリダイレクト拡張機能を使用する Microsoft Edge
  - Microsoft Edge 拡張機能

構成

Citrix Virtual Apps and Desktops™ バージョン 2311 以降、双方向コンテンツリダイレクトは Citrix Studio を介してのみ構成されます。以前のリリースでは、クライアントエンドポイントと Studio の両方でポリシー設定が構成されていました。双方向コンテンツリダイレクトはデフォルトで無効になっています。

VDA の構成については、**ICA ポリシー**設定の 双方向コンテンツリダイレクト を参照してください。

ブラウザーリダイレクトを機能させるには、表示されているコマンドを使用して、元のブラウザー（URL のリダイレクト元）にブラウザー拡張機能を登録する必要があります。使用しているブラウザーに基づいて、必要に応じて VDA とクライアントでコマンドを実行します。

ブラウザ	VDA	クライアント
グーグル クローム	"%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe" /regChrome	"%ProgramFiles(x86)%\Citrix\ICA Client\redirector.exe" /regChrome
マイクロソフト エッジ	"%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe" /regEdge	"%ProgramFiles(x86)%\Citrix\ICA Client\redirector.exe" /regEdge
利用可能なすべてのブラウザ	コマンド: "%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe" /regall	コマンド: "%ProgramFiles(x86)%\Citrix\ICA Client\redirector.exe" /regall

ブラウザ拡張機能を登録解除するには：

ブラウザ	VDA	クライアント
グーグル クローム	"%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe" /unregChrome	"%ProgramFiles(x86)%\Citrix\ICA Client\redirector.exe" /unregChrome
マイクロソフト エッジ	"%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe" /unregEdge	"%ProgramFiles(x86)%\Citrix\ICA Client\redirector.exe" /unregEdge
利用可能なすべてのブラウザ	"%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe" /unregall	"%ProgramFiles(x86)%\Citrix\ICA Client\redirector.exe" /unregall

注：

- これらのコマンドを管理者権限でコマンドプロンプト（CMD）ウィンドウで実行します。

- 登録コマンドを実行すると、ChromeおよびEdgeブラウザは、初回起動時にCitrix Browser Redirection Extensionを有効にするようユーザーに促します。
- 登録コマンドは、Browser Redirection Extensionをネイティブメッセージングホストにリンクさせ、拡張機能がネイティブコードと通信できるようにします。これがなければ、ブラウザは通信をブロックします。
- Google Chromeウェブストアからブラウザ拡張機能を手動でインストールすることもできます。Microsoft Edgeアドオンストアから Browser Redirection Extensionを使用するには、Virtual Delivery Agent (VDA) バージョン2503以降が必要です。古いVDAバージョンの場合は、Microsoft Edgeブラウザ内でGoogle Chromeウェブストアから拡張機能をインストールしてください（ChromeウェブストアからMicrosoft Edgeに拡張機能を追加するを参照）。
- システム要件に記載されているCitrix Workspaceアプリのバージョンは、双方向コンテンツリダイレクトとOAuthリダイレクトの両方をサポートするために必要な最小バージョンです。
- Macの場合：公証済みアプリケーションに対するmacOSのセキュリティ要件のため、カスタムOAuthコールバックURLスキームはCitrixに事前登録されている必要があり、インストール後に動的に変更することはできません。デフォルトでは`citrix-oauth-redir`のみがサポートされています。URLスキームを登録するには、Citrix製品チームにお問い合わせください。

Citrix VDAからクライアントへのワイルドカードリダイレクト

双方向コンテンツリダイレクトは、リダイレクトするURLを定義する際にワイルドカードの使用をサポートします。双方向コンテンツリダイレクトを構成するには、構成の手順を参照してください。

VDAからクライアントへのカスタムプロトコルリダイレクト

双方向コンテンツリダイレクトは、Citrix VDAからクライアントへのカスタムプロトコルのリダイレクトをサポートします。HTTPまたはHTTPS以外のプロトコルがサポートされています。双方向コンテンツリダイレクトを構成するには、構成の手順を参照してください。

Web Studioで、**双方向コンテンツリダイレクト**のカスタムプロトコルを設定します。

注：

- これらのコマンドを実行するには、管理者権限が必要です。
- クライアントには、プロトコルを処理するために登録されたアプリケーションが必要です。そうでない場合、URLはクライアントにリダイレクトされますが、起動に失敗します。
- ChromeおよびEdgeブラウザーで入力または起動するカスタムプロトコルURLはサポートされておらず、リダイレクトされません。
- 次のプロトコルはサポートされていません: `rtsp://, rtspu://, pnm://, mms://`。

その他の考慮事項

- ブラウザの要件と構成は、リダイレクトを開始するブラウザにのみ適用されます。リダイレクトが成功した後にURLが開かれる宛先ブラウザは、サポートの対象外です。VDAからクライアントにURLをリダイレクトする場合、サポートされるブラウザ構成はVDA上でのみ必要です。逆に、クライアントからVDAにURLをリダイレクトする場合、サポートされるブラウザ構成はクライアント上でのみ必要です。リダイレクトされたURLは、方向に応じて、クライアントまたはVDAのいずれかの宛先マシンで構成されているデフォルトのブラウザに渡されます。VDAとクライアントで同じブラウザタイプを使用する必要はありません。
- リダイレクトルールがループ構成にならないことを確認してください。たとえば、VDAポリシーが `https://www.citrix.com` をリダイレクトするように設定され、クライアントポリシーが同じURLをリダイレクトするように設定されている場合、無限ループが発生します。
- URL短縮サービスはサポートされていません。
- クライアントからVDAへのリダイレクトには、Windowsクライアントが管理者権限でインストールされている必要があります。
- 宛先ブラウザがすでに開いている場合、リダイレクトされたURLは新しいタブで開きます。そうでない場合、URLは新しいブラウザウィンドウで開きます。
- 双方向コンテンツリダイレクトは、ローカルアプリアクセス (LAA) が有効になっている場合は機能しません。

ホストからクライアントへのリダイレクト

ホストからクライアントへのリダイレクトにより、Citrix®セッションで実行されているアプリケーションにハイパーリンクとして埋め込まれたURLを、ユーザーのエンドポイントデバイス上の対応するアプリケーションを使用して開くことができます。ホストからクライアントへのリダイレクトの一般的なユースケースには、次のようなものがあります。

- Citrixサーバーがソースへのインターネットまたはネットワークアクセスを持たない場合のWebサイトのリダイレクト。
- セキュリティ、パフォーマンス、互換性、またはスケーラビリティの理由から、Citrixセッション内でWebブラウザを実行することが望ましくない場合のWebサイトのリダイレクト。
- URLを開くために必要なアプリケーションがCitrixサーバーにインストールされていない場合の特定のURLタイプのリダイレクト。

ホストからクライアントへのリダイレクトは、Webページでアクセスしたり、Citrixセッションで実行されているWebブラウザのアドレスバーに入力したりするURLを対象としていません。Webブラウザでのリダイレクトについては、「双方向URLリダイレクト」または「ブラウザコンテンツリダイレクト」を参照してください。

システム要件

- マルチセッションOS VDA
- サポートされているクライアント：
  - Windows向けCitrix Workspace™アプリ
  - Mac向けCitrix Workspaceアプリ
  - Linux向け Citrix Workspace アプリ
  - HTML5向けCitrix Workspaceアプリ
  - Chrome向けCitrix Workspaceアプリ

クライアントデバイスには、URLタイプのリダイレクトを処理するためのアプリケーションがインストールされ、構成されている必要があります。

構成

この機能を有効にするには、ホストからクライアントへのリダイレクト Citrixポリシーを使用します。**ホストからクライアントへのリダイレクト**は、デフォルトで無効になっています。ホストからクライアントへのリダイレクトポリシーを有効にすると、Citrix Launcherアプリケーションは Windowsサーバーに登録され、URLをインターセプトしてクライアントデバイスに送信できるようになります。

次に、必要なURLタイプのデフォルトアプリケーションとしてCitrix Launcherを使用するように Windowsグループポリシーを構成する必要があります。CitrixサーバーVDAで、ServerFTAdefaultPolicy.xmlファイルを作成し、次のXMLコードを挿入します。

```
<?xml version="1.0" encoding="UTF-8"?>



<DefaultAssociations>



<Association Identifier="http" ProgId="ServerFTAHTML"
ApplicationName="ServerFTA" />



<Association Identifier="https" ProgId="ServerFTAHTML"
ApplicationName="ServerFTA" />



</DefaultAssociations>
```

グループポリシー管理コンソールから、**コンピューターの構成 > 管理用テンプレート > Windows コンポーネント > エクスプローラー > 既定の関連付け構成ファイルを設定する** に移動し、ServerFTAdefaultPolicy.xmlファイルを保存します。

注：

Citrixサーバーにグループポリシー設定がない場合、WindowsはURLを開くためのアプリケーションを選択するようユーザーに促します。

デフォルトでは、次のURLタイプのリダイレクトをサポートしています。

- HTTP
- HTTPS
- RTSP
- RTSPU
- PNM
- MMS

リダイレクト用のリストに、追加の標準またはカスタムURLタイプを含めるには、以前に参照したServerFTAdefaultPolicy.xmlファイルに新しい**Association Identifier**行を作成します。例：

```
<Association Identifier="ftp" ProgId="ServerFTAHTML"
ApplicationName="ServerFTA" />

<Association Identifier="mailto" ProgId="ServerFTAHTML"
ApplicationName="ServerFTA" />

<Association Identifier="customtype1" ProgId="ServerFTAHTML"
ApplicationName="ServerFTA" />

<Association Identifier="customtype2" ProgId="ServerFTAHTML"
ApplicationName="ServerFTA" />
```

リストにURLタイプを追加するには、クライアント構成も必要です。Windowsクライアントで以下のレジストリキーと値を作成します。

注：

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

- キー: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Policies\Citrix\ICA Client\SFTA
- 値の名前: ExtraURLProtocols
- 値の型: REG_SZ
- 値のデータ: 必要なURLタイプをセミコロンで区切って指定します。URLのオーソリティ部分より前のすべてを含めます。例： `ftp://;mailto:;customtype1://;custometype2://`

URLの種類はWindowsクライアントにのみ追加できます。上記のレジストリ設定がないクライアントは、Citrixセッションへのリダイレクトを拒否します。クライアントには、指定されたURLの種類を処理するようにインストールおよび構成されたアプリケーションが必要です。

デフォルトのリダイレクトリストからURLタイプを削除するには、サーバーVDAで以下のレジストリキーと値を作成します。

- キー: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\SFTA
- 値の名前: DisableServerFTA
- 値の型: DWORD
- 値のデータ: 1
- 値の名前: NoRedirectClasses
- 値の型: REG_MULTI_SZ
- 値のデータ: 次の値の任意の組み合わせを指定します: `http`、`https`、`rtsp`、`rtspu`、`pnm`、または `mms`。複数の値を別々の行に入力します。例:

`http`

`https`

`rtsp`

特定のWebサイトセットに対してホストからクライアントへのリダイレクトを有効にするには、サーバーVDAでレジストリキーと値を作成します。

- キー: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\SFTA
- 値の名前: ValidSites
- 値の型: REG_MULTI_SZ
- 値のデータ: 完全修飾ドメイン名 (FQDN) の任意の組み合わせを指定します。複数のFQDNを別々の行に入力します。プロトコル (`http://` または `https://`) を含めず、FQDNのみを含めます。FQDNには、アスタリスク (`*`) をワイルドカード文字として左端の位置にのみ含めることができます。このワイルドカードは、RFC 6125のルールに準拠した単一レベルのドメインに一致します。例:

`www.exmaple.com`

`*.example.com`

> **注：**
>
> **ValidSites**キーを**DisableServerFTA**キーおよび**NoRedirectClasses**キーと組み合わせて使用することはできません。

サーバーVDAのデフォルトブラウザ構成

このセクションで参照されているホストからクライアントへのリダイレクトを有効にすると、サーバーVDA上の以前のデフォルトブラウザ構成はすべて上書きされます。Web URLがリダイレクトされない場合、Citrix Launcherは、`command_backup` レジストリキーで構成されているブラウザにURLを渡します。このキーはデフォルトでInternet Explorerを指していますが、別のブラウザへのパスを含むように変更できます。詳細については、レジストリを介して管理される機能のリストにある サーバーVDAのデフォルトブラウザ構成 を参照してください。

ローカルアプリアクセスとURLリダイレクト

はじめに

Local App Accessは、ローカルにインストールされたWindowsアプリケーションを、デスクトップを切り替えることなくホストされたデスクトップ環境にシームレスに統合します。Local App Accessを使用すると、次のことが可能になります。

- 物理的なラップトップ、PC、またはその他のデバイスにローカルにインストールされているアプリケーションに、仮想デスクトップから直接アクセスできます。
- 柔軟なアプリケーション配信ソリューションを提供します。仮想化できない、またはIT部門が保守していないローカルアプリケーションをユーザーが持っている場合でも、それらのアプリケーションは仮想デスクトップにインストールされているかのように動作します。
- アプリケーションが仮想デスクトップとは別にホストされている場合のダブルホップの遅延を解消します。これを行うには、公開されたアプリケーションへのショートカットをユーザーのWindowsデバイスに配置します。
- 次のようなアプリケーションを使用します。
    - GoToMeetingなどのビデオ会議ソフトウェア。
    - まだ仮想化されていない特殊なアプリケーションまたはニッチなアプリケーション。
    - そうでなければ、ユーザーデバイスからサーバーへ、そしてサーバーからユーザーデバイスへと大量のデータを転送するようなアプリケーションと周辺機器。たとえば、DVDバーナーやTVチューナーなど。

Citrix Virtual Apps and Desktops™では、ホストされたデスクトップセッションは、URLリダイレクトを使用してLocal App Accessアプリケーションを起動します。URLリダイレクトにより、アプリケーションは複数のURLアドレスで利用可能になります。デスクトップセッション内のブラウザで埋め込みリンクを選択することにより、ローカルブラウザ（ブラウザのURLブロックリスト

に基づく）を起動します。ブロックリストにないURLに移動すると、そのURLはデスクトップセッションで再度開かれます。

URLリダイレクトはデスクトップセッションでのみ機能し、アプリケーションセッションでは機能しません。アプリケーションセッションで使用できる唯一のリダイレクト機能は、ホストからクライアントへのコンテンツリダイレクトです。これは、サーバーFTA（ファイルタイプ関連付け）リダイレクトの一種です。このFTAは、HTTP、HTTPS、RTSP、MMSなどの特定のプロトコルをクライアントにリダイレクトします。たとえば、HTTPで埋め込みリンクのみを開く場合、リンクはクライアントアプリケーションで直接開かれます。URLブロックリストまたは許可リストのサポートはありません。

Local App Accessが有効になっている場合、ローカルで実行されているアプリケーション、ユーザーがホストするアプリケーションからのリンクとして、またはデスクトップ上のショートカットとしてユーザーに表示されるURLは、次のいずれかの方法でリダイレクトされます。

- ユーザーのコンピューターからホストされたデスクトップへ
- Citrix Virtual Apps and Desktopsサーバーからユーザーのコンピューターへ
- 起動された環境でレンダリングされる（リダイレクトされない）

特定のWebサイトからのコンテンツのリダイレクトパスを指定するには、Virtual Delivery AgentでURL許可リストとURLブロックリストを構成します。これらのリストには、URLリダイレクトポリシー設定を指定する複数文字列のレジストリキーが含まれています。詳細については、「ローカルアプリアクセス ポリシー設定」を参照してください。

URLは、以下の例外を除き、VDAでレンダリングできます。

- 地域/ロケール情報 — msn.comやnews.google.comなど、ロケール情報を必要とするWebサイト（地域に基づいて国固有のページを開きます）。たとえば、VDAが英国のデータセンターからプロビジョニングされ、クライアントがインドから接続している場合、ユーザーはin.msn.comが表示されることを期待しますが、実際にはuk.msn.comが表示されます。
- マルチメディアコンテンツ — リッチメディアコンテンツを含むWebサイトは、クライアントデバイスでレンダリングされると、エンドユーザーにネイティブなエクスペリエンスを提供し、高遅延ネットワークでも帯域幅を節約します。この機能は、Silverlightなどの他のメディアタイプを含むサイトをリダイレクトします。このプロセスは安全な環境で行われます。つまり、管理者が承認したURLはクライアントで実行され、残りのURLはVDAにリダイレクトされます。

URLリダイレクトに加えて、FTAリダイレクトを使用できます。FTAは、セッション内でファイルが検出されたときにローカルアプリケーションを起動します。ローカルアプリが起動された場合、そのローカルアプリはファイルを開くためにファイルへのアクセス権を持っている必要があ

ります。したがって、ローカルアプリケーションを使用して開くことができるファイルは、ネットワーク共有上またはクライアントドライブ上（クライアントドライブマッピングを使用）にあるファイルのみです。たとえば、PDFファイルを開く際に、PDFリーダーがローカルアプリである場合、そのPDFリーダーを使用してファイルが開かれます。ローカルアプリはファイルに直接アクセスできるため、ファイルを開くためのICA®を介したネットワーク転送は発生しません。

要件、考慮事項、および制限事項

WindowsマルチセッションOS用VDAおよびWindowsシングルセッションOS用VDAの有効なオペレーティングシステムで、ローカルアプリアクセスをサポートしています。ローカルアプリアクセスには、Citrix Workspaceアプリ for Windowsバージョン4.1（最小）が必要です。以下のブラウザーがサポートされています。

- Edge、最新バージョン
- Firefox、最新バージョンおよび延長サポートリリース
- Chrome、最新バージョン

ローカルアプリアクセスとURLリダイレクトを使用する際の以下の考慮事項と制限事項を確認してください。

- ローカルアプリアクセスは、すべてのモニターにまたがる全画面の仮想デスクトップ向けに設計されています。
    - ウィンドウモードで実行される仮想デスクトップや、すべてのモニターをカバーしない仮想デスクトップでローカルアプリアクセスを使用すると、ユーザーエクスペリエンスが混乱する可能性があります。
    - 複数モニター — 1つのモニターが最大化されると、そのセッションで起動されたすべてのアプリケーションのデフォルトデスクトップになります。このデフォルトは、後続のアプリケーションが通常別のモニターで起動される場合でも発生します。
    - この機能は1つのVDAをサポートします。複数の同時VDAとの統合はありません。
- 一部のアプリケーションは予期しない動作をし、ユーザーに影響を与える可能性があります。
    - ドライブ文字は、仮想デスクトップのC:ドライブではなくローカルのC:ドライブのように表示されるため、ユーザーを混乱させる可能性があります。
    - 仮想デスクトップで利用可能なプリンターは、ローカルアプリケーションでは利用できません。
    - 昇格された権限を必要とするアプリケーションは、クライアントホスト型アプリケーションとして起動できません。

  - シングルインスタンスアプリケーション（Windows Media Playerなど）に対する特別な処理はありません。
  - ローカルアプリケーションは、ローカルマシンのWindowsテーマで表示されます。
  - 全画面表示アプリケーションはサポートされていません。これには、PowerPointのスライドショーやデスクトップ全体を覆うフォトビューアーなど、全画面で開くアプリケーションが含まれます。
  - ローカルアプリアクセスは、ローカルアプリケーションのプロパティ（クライアントのデスクトップやスタートメニューのショートカットなど）をVDAにコピーします。ただし、ショートカットキーや読み取り専用属性などの他のプロパティはコピーしません。
  - 重なり合うウィンドウの順序の処理方法をカスタマイズするアプリケーションは、予期しない結果をもたらす可能性があります。たとえば、一部のウィンドウが非表示になることがあります。
  - マイコンピューター、ごみ箱、コントロールパネル、ネットワークドライブのショートカット、フォルダーのショートカットなど、ショートカットはサポートされていません。
  - 次のファイルの種類とファイルはサポートされていません：カスタムファイルの種類、関連付けられたプログラムがないファイル、zipファイル、隠しファイル。
  - 32ビットと64ビットのクライアントホスト型またはVDAアプリケーションが混在している場合、タスクバーのグループ化はサポートされていません。つまり、32ビットのローカルアプリケーションと64ビットのVDAアプリケーションをグループ化することはできません。
  - COMを使用してアプリケーションを起動することはできません。たとえば、Officeアプリケーション内から埋め込みOfficeドキュメントをクリックした場合、プロセスの起動が検出されず、ローカルアプリケーションの統合は失敗します。

- ユーザーが別の仮想デスクトップセッション内から仮想デスクトップを起動するダブルホップシナリオはサポートされていません。
- URLリダイレクトは明示的なURL（つまり、ブラウザのアドレスバーに表示されるURL、またはブラウザに応じてブラウザ内ナビゲーションを使用して見つかるURL）のみをサポートします。
- URLリダイレクトはデスクトップセッションでのみ機能し、アプリケーションセッションでは機能しません。
- VDAセッションのローカルデスクトップフォルダーでは、ユーザーはファイルを作成できません。
- ローカルで実行されているアプリケーションの複数のインスタンスは、仮想デスクトップ用に設定されたタスクバー設定に従って動作します。ただし、ローカルで実行されているアプリ

ケーションへのショートカットは、それらのアプリケーションの実行中のインスタンスとグループ化されません。また、ホストされたアプリケーションの実行中のインスタンスや、ホストされたアプリケーションへのピン留めされたショートカットともグループ化されません。ユーザーは、タスクバーからローカルで実行されているアプリケーションのウィンドウのみを閉じることができます。ユーザーはローカルアプリケーションウィンドウをデスクトップのタスクバーやスタートメニューにピン留めできますが、これらのショートカットを使用するとアプリケーションが常に起動するとは限りません。

- **ローカルアプリアクセスを許可**ポリシー設定を**有効**に設定した場合、ブラウザーコンテンツリダイレクトはサポートされません。デフォルトでは、ローカルアプリアクセスは禁止されています。

Windowsとの連携

ローカルアプリアクセスとWindowsとの連携には、次の動作が含まれます。

- Windows 8およびWindows Server 2012のショートカットの動作
  - クライアントにインストールされているWindowsストアアプリケーションは、ローカルアプリアクセスのショートカットの一部として列挙されません。
  - 画像ファイルとビデオファイルは、デフォルトでWindowsストアアプリケーションを使用して開かれます。ただし、ローカルアプリアクセスはWindowsストアアプリケーションを列挙し、デスクトップアプリケーションでショートカットを開きます。
- ローカルプログラム
  - Windows 7の場合、フォルダーはスタートメニューで利用できます。
  - Windows 8の場合、ローカルプログラムは、ユーザーがスタート画面からカテゴリとして**すべてのアプリ**を選択した場合にのみ利用できます。すべてのサブフォルダーがローカルプログラムに表示されるわけではありません。
- アプリケーション向けのWindows 8グラフィック機能
  - デスクトップアプリケーションはデスクトップ領域に制限されており、スタート画面およびWindows 8スタイルのアプリケーションによって覆われます。
  - ローカルアプリアクセスアプリケーションは、マルチモニターモードではデスクトップアプリケーションのように動作しません。マルチモニターモードでは、スタート画面とデスクトップが異なるモニターに表示されます。
- Windows 8とローカルアプリアクセスURLリダイレクト

- Windows 8のInternet Explorerではアドオンが有効になっていないため、URLリダイレクトを有効にするにはデスクトップ版Internet Explorerを使用してください。
- Windows Server 2012では、Internet Explorerはデフォルトでアドオンを無効にします。URLリダイレクトを実装するには、Internet Explorerの拡張構成を無効にします。その後、Internet Explorerのオプションをリセットして再起動し、標準ユーザー向けにアドオンが有効になっていることを確認します。

ローカルアプリアクセスとURLリダイレクトの構成

Citrix Workspace™アプリでローカルアプリアクセスとURLリダイレクトを使用するには：

- ローカルクライアントマシンにCitrix Workspaceアプリをインストールします。Citrix Workspaceアプリのインストール中に両方の機能を有効にするか、グループポリシーエディターを使用してローカルアプリアクセステンプレートを有効にすることができます。
- **ローカルアプリアクセスを許可**ポリシー設定を**有効**に設定します。URLリダイレクトのURL許可リストおよびブロックリストポリシー設定も構成できます。詳しくは、「ローカルアプリアクセス ポリシー設定」を参照してください。

ローカルアプリアクセスとURLリダイレクトを有効にする

すべてのローカルアプリケーションでローカルアプリアクセスを有効にするには、次の手順に従います。

1. Web Studioにサインインし、左側のペインで**ポリシー**をクリックします。
2. アクションバーで、**ポリシーの作成**をクリックします。
3. ［ポリシーの作成］ウィンドウで、検索ボックスに「Allow Local App Access」と入力し、**選択**をクリックします。
4. 設定の編集ウィンドウで、**許可**を選択します。デフォルトでは、**ローカルアプリアクセスを許可**ポリシーは禁止されています。この設定が許可されている場合、VDAは、公開アプリケーションとローカルアプリアクセスのショートカットをセッションで有効にするかどうかをエンドユーザーが決定できるようにします。（この設定が禁止されている場合、公開アプリケーションとローカルアプリアクセスのショートカットの両方がVDAで機能しません。）このポリシー設定は、マシン全体とURLリダイレクトポリシーに適用されます。
5. ［ポリシーの作成］ウィンドウで、検索ボックスに「URL redirection allow list」と入力し、**選択**をクリックします。URLリダイレクト許可リストは、リモートセッションのデフォルトブラウザーで開くURLを指定します。
6. 「設定の編集」ウィンドウで、「**追加**」をクリックしてURLを追加し、「**OK**」をクリックします。

7. ［ポリシーの作成］ウィンドウで、検索ボックスに「URL redirection block list」と入力し、**選択**をクリックします。URLリダイレクトブロックリストは、エンドポイントで実行されているデフォルトブラウザーにリダイレクトされるURLを指定します。
8. 「設定の編集」ウィンドウで、「**追加**」をクリックしてURLを追加し、「**OK**」をクリックします。
9. 「設定」ページで、「**次へ**」をクリックします。
10. 「ユーザーとマシン」ページで、該当するデリバリーグループにポリシーを割り当て、「**次へ**」をクリックします。
11. 「概要」ページで設定を確認し、「**完了**」をクリックします。

Citrix Workspaceアプリのインストール中にすべてのローカルアプリケーションでURLリダイレクトを有効にするには、次の手順に従います。

1. マシン上のすべてのユーザーに対してCitrix Workspaceアプリをインストールするときに、URLリダイレクトを有効にします。これにより、URLリダイレクトに必要なブラウザーアドオンも登録されます。
2. コマンドプロンプトから、以下のいずれかのオプションを使用してCitrix Workspaceアプリをインストールするための適切なコマンドを実行します。
   - CitrixReceiver.exeの場合は、`/ALLOW_CLIENTHOSTEDAPPSURL=1`を使用します。
   - CitrixReceiverWeb.exeの場合は、`/ALLOW_CLIENTHOSTEDAPPSURL=1`を使用します。

グループポリシーエディターを使用してローカルアプリアクセス テンプレートを有効にする

注：

- グループポリシーエディターを使用してローカルアプリアクセステンプレートを有効にする前に、receiver.admx/admlテンプレートファイルをローカルGPOに追加します。
- Windows向けCitrix Workspaceアプリのテンプレートファイルは、CitrixBase.admx/CitrixBase.admlを%systemroot%\policyDefinitionsフォルダーに追加した場合にのみ、ローカルGPOの**管理用テンプレート > Citrixコンポーネント > Citrix Workspace**フォルダーで利用できます。

> グループポリシーエディターを使用してローカルアプリアクセス テンプレートを有効にするには、次の手順に従います。

1. **gpedit.msc**を実行します。
2. **コンピューターの構成 > 管理用テンプレート > クラシック管理用テンプレート (ADM) > Citrix Components > Citrix Workspace > ユーザーエクスペリエンス**に移動します。
3. **ローカルアプリアクセス設定**をクリックします。
4. **有効**を選択し、**URLリダイレクトを許可**を選択します。URLリダイレクトの場合、この記事の後半にある「*ブラウザーアドオンの登録*」セクションで説明されているコマンドラインを使用して、ブラウザーアドオンを登録します。

公開アプリケーションのみにアクセスを提供する

レジストリエディターまたはPowerShell SDKを使用して、公開アプリケーションへのアクセスを提供できます。

レジストリエディターについては、レジストリを介して管理される機能のリストにある「公開アプリケーションのローカルアプリアクセス」を参照してください。

PowerShell SDKを使用するには：

1. Delivery Controller™が実行されているマシンでPowerShellを開きます。
2. 次のコマンドを入力します: `set-configsitemetadata -name "studio_clientHostedAppsEnabled" -value "true"`。

クラウドサービス展開で**ローカルアプリアクセスアプリケーションの追加**にアクセスするには、Citrix DaaS Remote PowerShell SDKを使用します。詳しくは、「Citrix DaaS Remote PowerShell SDK」を参照してください。

1. インストーラーをダウンロードします:

   `<https://download.apps.cloud.com/CitrixPoshSdk.exe>`

2. 次のコマンドを実行します:

   a. `asnp citrix.*`.

   b. `Get-XdAuthentication`

3. 次のコマンドを入力します: `set-configsitemetadata -name "studio_clientHostedAppsEnabled" -value "true"`。

該当する前の手順を完了したら、以下の手順に従って続行します。

1. Web Studioにサインインし、左側のペインで**アプリケーション**を選択します。
2. 上部中央ペインで、空白領域を右クリックし、コンテキストメニューから**Add Local App Access Application**を選択します。アクションバーの**Add Local App Access Application**をクリックすることもできます。アクションバーにAdd Local App Access Applicationオプションを表示するには、**Refresh**をクリックします。
3. ローカルアプリアクセスアプリケーションを公開します。

    - ローカルアプリケーションアクセスウィザードが起動し、紹介ページが表示されます。このページは、今後のウィザードの起動時に表示しないように設定できます。
    - ウィザードは、以下で説明するグループ、場所、識別、配信、および概要の各ページを案内します。各ページの作業が完了したら、概要ページに到達するまで**次へ**をクリックします。
    - グループページで、新しいアプリケーションを追加するデリバリーグループを1つ以上選択し、**次へ**をクリックします。
    - ページで、ユーザーのローカルマシン上のアプリケーションの完全な実行可能パスを入力し、アプリケーションが配置されているフォルダーへのパスを入力します。Citrixでは、システム環境変数パスを使用することをお勧めします。例: %ProgramFiles(x86)%\Internet Explorer\iexplore.exe。
    - 識別ページで、デフォルト値を受け入れるか、必要な情報を入力してから**次へ**をクリックします。
    - ページで、このアプリケーションをユーザーに配信する方法を構成し、**次へ**をクリックします。選択したアプリケーションのアイコンを指定できます。また、仮想デスクトップ上のローカルアプリケーションへのショートカットを、スタートメニュー、デスクトップ、またはその両方に表示するかどうかを指定できます。
    - 概要ページで設定を確認し、**完了**をクリックしてローカルアプリケーションアクセスウィザードを終了します。

ブラウザアドオンを登録する

> **注：**
>
> URLリダイレクトに必要なブラウザーアドオンは、コマンドラインから / ALLOW_CLIENTHOSTEDAPPSURL=1 オプションを使用してCitrix Workspaceアプリをインストールすると、自動的に登録されます。

> 1つまたはすべてのアドオンを登録および登録解除するには、次のコマンドを使用します。

- クライアントデバイスにアドオンを登録するには: \<*client-installation-folder*>\redirector.exe /reg\<*browser*>
- クライアントデバイスのアドオンを登録解除するには: \<*client-installation-folder*>\redirector.exe /unreg\<*browser*>
- VDAにアドオンを登録するには: \<*VDAinstallation-folder*>\VDARedirector.exe /reg\<*browser*>
- VDAのアドオンを登録解除するには: \<*VDAinstallation-folder*>\VDARedirector.exe /unreg\<*browser*>

ここで、\<*browser*>はInternet Explorer、Firefox、Chrome、またはAllです。

たとえば、次のコマンドは、Citrix Workspaceアプリを実行しているデバイスにInternet Explorerアドオンを登録します。

C:\Program Files\Citrix\ICA Client\redirector.exe/regIE

次のコマンドは、WindowsマルチセッションOS VDA上のすべてのアドオンを登録します。

C:\Program Files (x86)\Citrix\HDX\bin\VDARedirector.exe /regAll

ブラウザ間のURLインターセプト

- デフォルトでは、Internet Explorerは指定されたURLをリダイレクトします。URLがブロックリストにないが、ブラウザまたはWebサイトが別のURLにリダイレクトする場合、最終的なURLはリダイレクトされません。ブロックリストにある場合でもリダイレクトされません。

URLリダイレクトが正しく機能するように、ブラウザからプロンプトが表示されたらアドオンを有効にしてください。インターネットオプションを使用しているアドオン、またはプロンプト内のアドオンが無効になっている場合、URLリダイレクトは正しく機能しません。

- Firefoxのアドオンは常にURLをリダイレクトします。

アドオンがインストールされると、Firefoxは新しいタブページにアドオンのインストールを許可するか、または防止するかを促します。機能が動作するようにアドオンを許可してください。

- Chromeのアドオンは、入力されたURLではなく、常にナビゲートされた最終URLをリダイレクトします。

拡張機能は外部からインストールされています。拡張機能を無効にすると、ChromeでURLリダイレクト機能が動作しません。シークレットモードでURLリダイレクトが必要な場合は、ブラウザの設定でそのモードでの拡張機能の実行を許可してください。

ログオフ時および切断時のローカルアプリケーションの動作を構成する

注：

これらの手順に従って設定を構成しない場合、デフォルトでは、ユーザーが仮想デスクトップからログオフまたは切断しても、ローカルアプリケーションは実行を継続します。再接続後、ローカルアプリケーションが仮想デスクトップで利用可能な場合、それらは再統合されます。

ログオフ時および切断時のローカルアプリケーションの動作を構成するには、レジストリを介して管理される機能のリストにあるログオフ時および切断時のローカルアプリケーションの動作を参照してください。

汎用USBリダイレクトとクライアントドライブに関する考慮事項

HDX™テクノロジーは、ほとんどの一般的なUSBデバイスに対して**最適化されたサポート**を提供します。最適化されたサポートは、WAN経由でパフォーマンスと帯域幅の効率を向上させ、ユーザーエクスペリエンスを改善します。特に高遅延またはセキュリティに敏感な環境では、最適化されたサポートが通常最良の選択肢です。

HDXテクノロジーは、最適化されたサポートがない、または不適切な特殊なデバイスに対して**汎用USBリダイレクト**を提供します。例を次に示します。

- USBデバイスに、マウスやWebカメラのボタンの増加など、最適化されたサポートに含まれない高度な機能がある場合。
- ユーザーが最適化されたサポートに含まれない機能を必要とする場合。
- USBデバイスが、テストおよび測定機器や産業用コントローラーなどの特殊なデバイスである場合。
- アプリケーションがUSBデバイスとしてデバイスに直接アクセスする必要がある場合。
- USBデバイスにWindowsドライバーしか利用できない場合。たとえば、スマートカードリーダーには、Citrix Workspace™ app for Android用のドライバーが利用できない場合があります。
- Citrix Workspace appのバージョンが、この種類のUSBデバイスに対して最適化されたサポートを提供していない場合。

汎用USBリダイレクトでは、次のようになります。

- ユーザーはユーザーデバイスにデバイスドライバーをインストールする必要がありません。
- USBクライアントドライバーはVDAマシンにインストールされます。

重要:

- 汎用USBリダイレクトは、最適化されたサポートと組み合わせて使用できます。汎用USBリダイレクトを有効にする場合は、汎用USBリダイレクトと最適化されたサポートの両方について、CitrixのUSBデバイスポリシー設定を構成してください。
- クライアントUSBデバイスの最適化ルールのCitrixポリシー設定は、特定のUSBデバイスに対する汎用USBリダイレクトの特定のポリシー設定です。ここで説明する最適化されたサポートには適用されません。

USBデバイスのパフォーマンスに関する考慮事項

ネットワークの遅延と帯域幅は、一部の種類のUSBデバイスで汎用USBリダイレクトを使用する場合、ユーザーエクスペリエンスとUSBデバイスの動作に影響を与える可能性があります。たとえば、タイミングに敏感なデバイスは、高遅延で低帯域幅のリンクでは正しく動作しない場合があります。可能な場合は、代わりに最適化されたサポートを使用してください。

一部のUSBデバイスは、使用可能にするために高帯域幅を必要とします。たとえば、3Dマウス（通常、高帯域幅を必要とする3Dアプリで使用）などです。帯域幅を増やすことができない場合は、帯域幅ポリシー設定を使用して他のコンポーネントの帯域幅使用量を調整することで、問題を軽減できる場合があります。詳細については、「クライアントUSBデバイスリダイレクトの帯域幅ポリシー設定」および「マルチストリーム接続ポリシー設定」を参照してください。

USBデバイスのセキュリティに関する考慮事項

一部のUSBデバイスは、スマートカードリーダー、指紋リーダー、署名パッドなど、本質的にセキュリティに敏感です。USBストレージデバイスなどの他のUSBデバイスは、機密データである可能性のあるデータを送信するために使用できます。

USBデバイスは、マルウェアを配布するためによく使用されます。Citrix Workspace appとCitrix Virtual Apps and Desktops™の設定により、これらのUSBデバイスからのリスクを軽減できますが、排除することはできません。この状況は、汎用USBリダイレクトを使用する場合でも、最適化されたサポートを使用する場合でも当てはまります。

重要:

セキュリティに配慮が必要なデバイスやデータについては、常にTLSまたはIPsecのいずれかを使用してHDX接続を保護してください。

必要なUSBデバイスのサポートのみを有効にしてください。このニーズを満たすように、汎用USBリダイレクトと最適化されたサポートの両方を構成してください。

USBデバイスを安全に使用するためのガイダンスをユーザーに提供してください。

- 信頼できる情報源から入手したUSBデバイスのみを使用してください。
- インターネットカフェなど、開かれた環境でUSBデバイスを放置しないでください。
- 複数のコンピューターでUSBデバイスを使用するリスクを説明してください。

汎用USBリダイレクトとの互換性

汎用USBリダイレクトは、USB 2.0以前のデバイスでサポートされています。汎用USBリダイレクトは、USB 2.0またはUSB 3.0ポートに接続されたUSB 3.0デバイスでもサポートされています。汎用USBリダイレクトは、スーパースピードなど、USB 3.0で導入されたUSB機能はサポートしていません。

以下のCitrix Workspaceアプリは、汎用USBリダイレクトをサポートしています。

- Windows向けCitrix Workspaceアプリについては、「アプリケーション配信の構成」を参照してください。
- Citrix Workspaceアプリ for Mac。詳しくは、Citrix Workspaceアプリ for Macを参照してください。
- Linux向けCitrix Workspaceアプリについては、「最適化」を参照してください。
- Chrome OS 向け Citrix Workspace アプリについては、Citrix Workspace app for Chromeを参照してください。

Citrix Workspace アプリのバージョンについては、Citrix Workspace app feature matrixを参照してください。

以前のバージョンのCitrix Workspaceアプリを使用している場合は、Citrix Workspaceアプリのドキュメントを参照して、汎用USBリダイレクトがサポートされていることを確認してください。サポートされているUSBデバイスの種類に関する制限については、Citrix Workspaceアプリのドキュメントを参照してください。

汎用USBリダイレクトは、VDA for Single-session OSバージョン7.6以降のデスクトップセッションでサポートされています。

汎用USBリダイレクトは、VDA for Multi-session OSバージョン7.6以降のデスクトップセッションでサポートされていますが、以下の制限があります。

- VDAは、Windows Server 2012 R2、Windows Server 2016、Windows Server 2019、またはWindows Server 2022を実行している必要があります。
- USBデバイスドライバーは、完全な仮想化サポートを含め、VDA OS（Windows 2012 R2）のRemote Desktop Session Host（RDSH）と完全に互換性がある必要があります。

一部の種類のUSBデバイスは、リダイレクトしても有用ではないため、汎用USBリダイレクトではサポートされていません。

- USBモデム。
- USBネットワークアダプター。
- USBハブ。USBハブに接続されたUSBデバイスは個別に処理されます。
- USB仮想COMポート。汎用USBリダイレクトではなく、COMポートリダイレクトを使用してください。

汎用USBリダイレクトでテスト済みのUSBデバイスについては、Citrix Ready Marketplaceを参照してください。一部のUSBデバイスは、汎用USBリダイレクトで正しく動作しません。

汎用USBリダイレクトの構成

汎用USBリダイレクトを使用するUSBデバイスの種類を制御し、個別に構成できます。

- VDAで、Citrixポリシー設定を使用します。詳しくは、ポリシー設定リファレンスのクライアントドライブとユーザーデバイスのリダイレクトおよびUSBデバイスポリシー設定を参照してください。
- Citrix Workspaceアプリで、Citrix Workspaceアプリに依存するメカニズムを使用します。たとえば、管理用テンプレートは、Windows向けCitrix Workspaceアプリを構成するレジストリ設定を制御します。デフォルトでは、特定のクラスのUSBデバイスに対してUSBリダイレクトが許可され、他のデバイスに対しては拒否されます。詳しくは、Windows向けCitrix Workspaceアプリのドキュメントの構成を参照してください。

この個別の構成により、柔軟性が向上します。例：

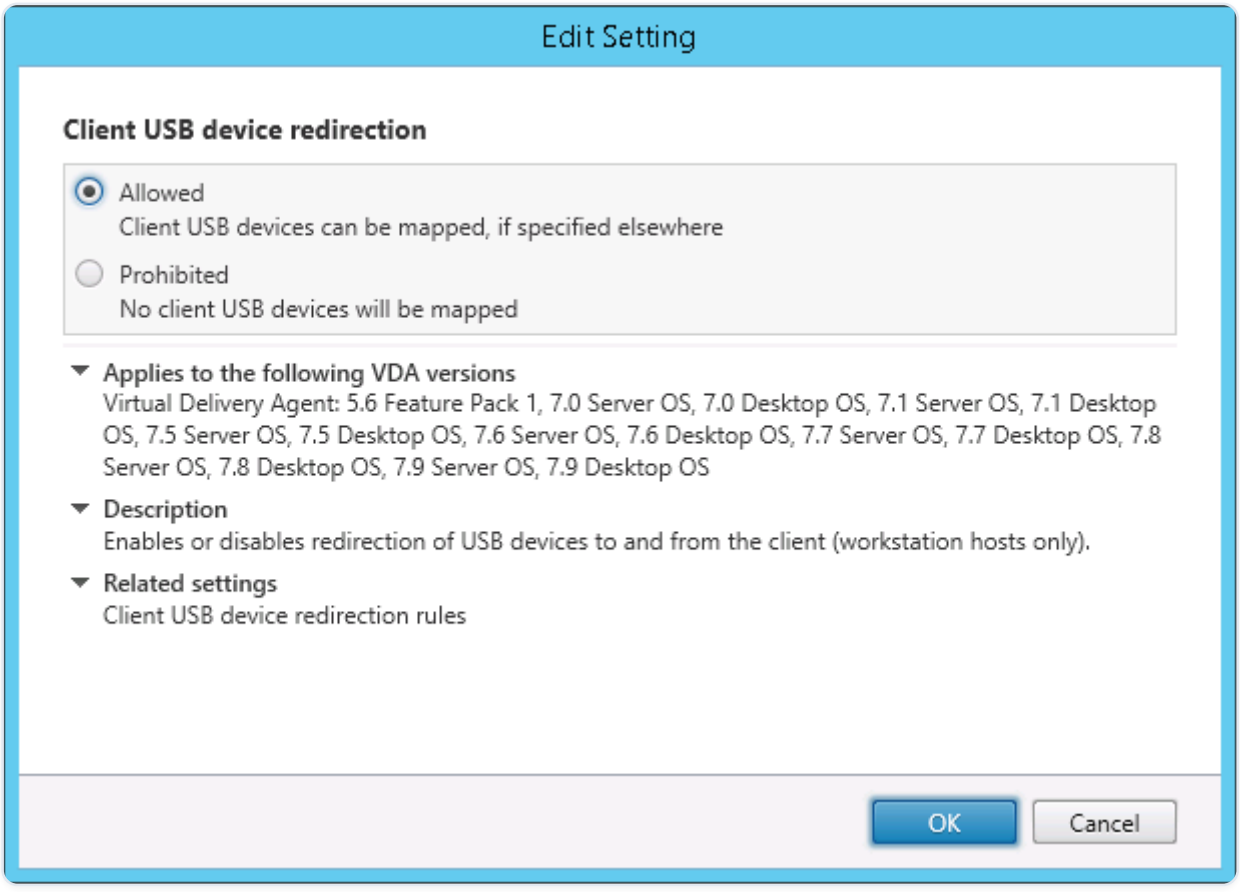
- 2つの異なる組織または部門がCitrix WorkspaceアプリとVDAを担当している場合、それぞれが個別に制御を適用できます。この構成は、ある組織のユーザーが別の組織のアプリケーションにアクセスする場合に適用されます。
- Citrixポリシー設定は、特定のユーザーのみ、またはLAN経由でのみ接続するユーザー（Citrix Gatewayを使用しない場合）に許可されるUSBデバイスを制御できます。

汎用USBリダイレクトを有効にする

汎用USBリダイレクトを有効にし、ユーザーによる手動リダイレクトを不要にするには、Citrixポリシー設定とCitrix Workspaceアプリの接続設定の両方を構成します。

Citrixポリシー設定で：

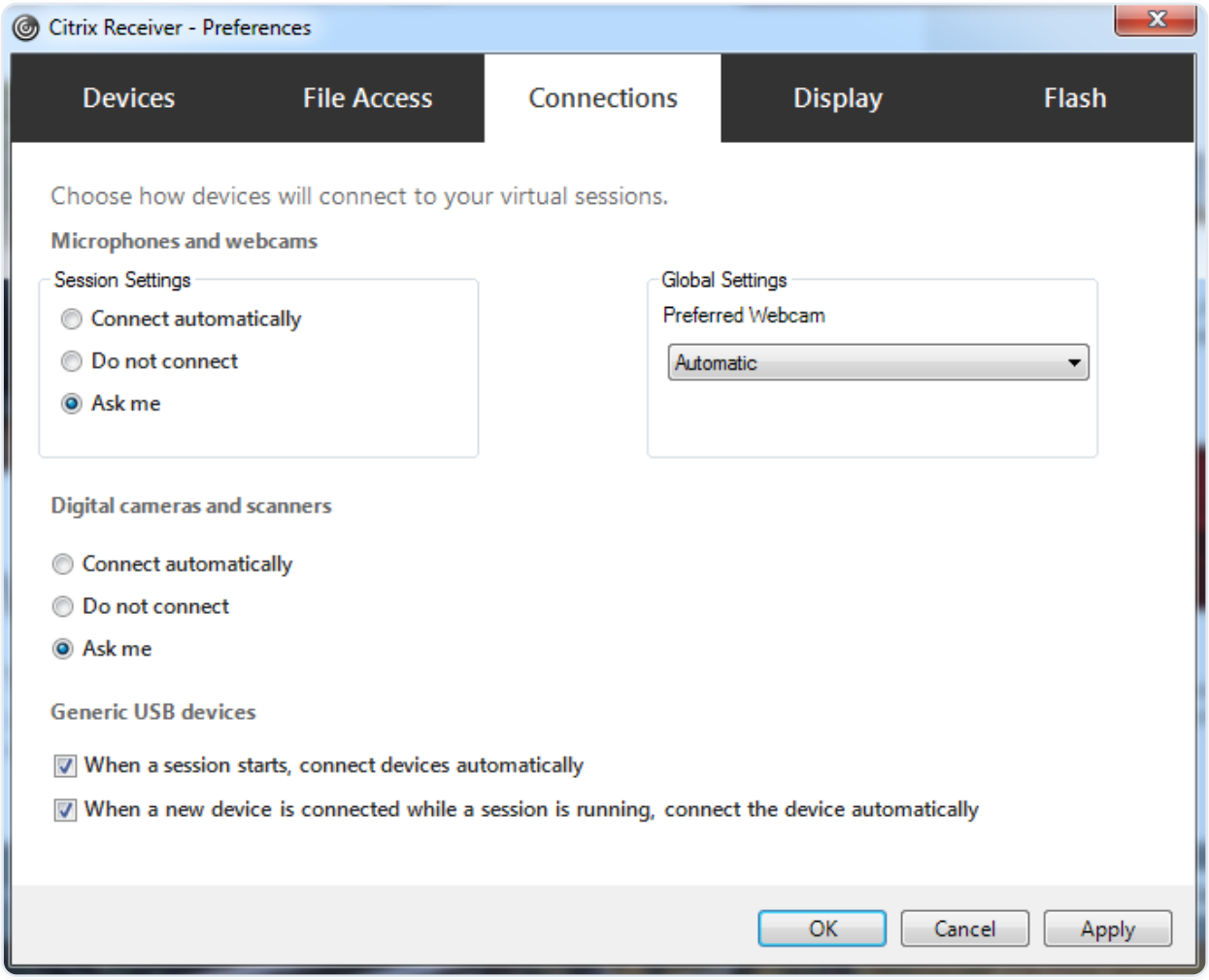
1. クライアントUSBデバイスリダイレクトをポリシーに追加し、その値を**許可**に設定します。



2. （オプション）リダイレクトに利用可能なUSBデバイスのリストを更新するには、クライアントUSBデバイスリダイレクト規則設定をポリシーに追加し、USBポリシー規則を指定します。

   ポリシー設定が完了したら、Citrix Workspaceアプリで：

3. 手動リダイレクトなしでデバイスが自動的に接続されるように指定します。これは、管理テンプレートを使用するか、Citrix Workspaceアプリの**Windows > Preferences > Connections**で実行できます。



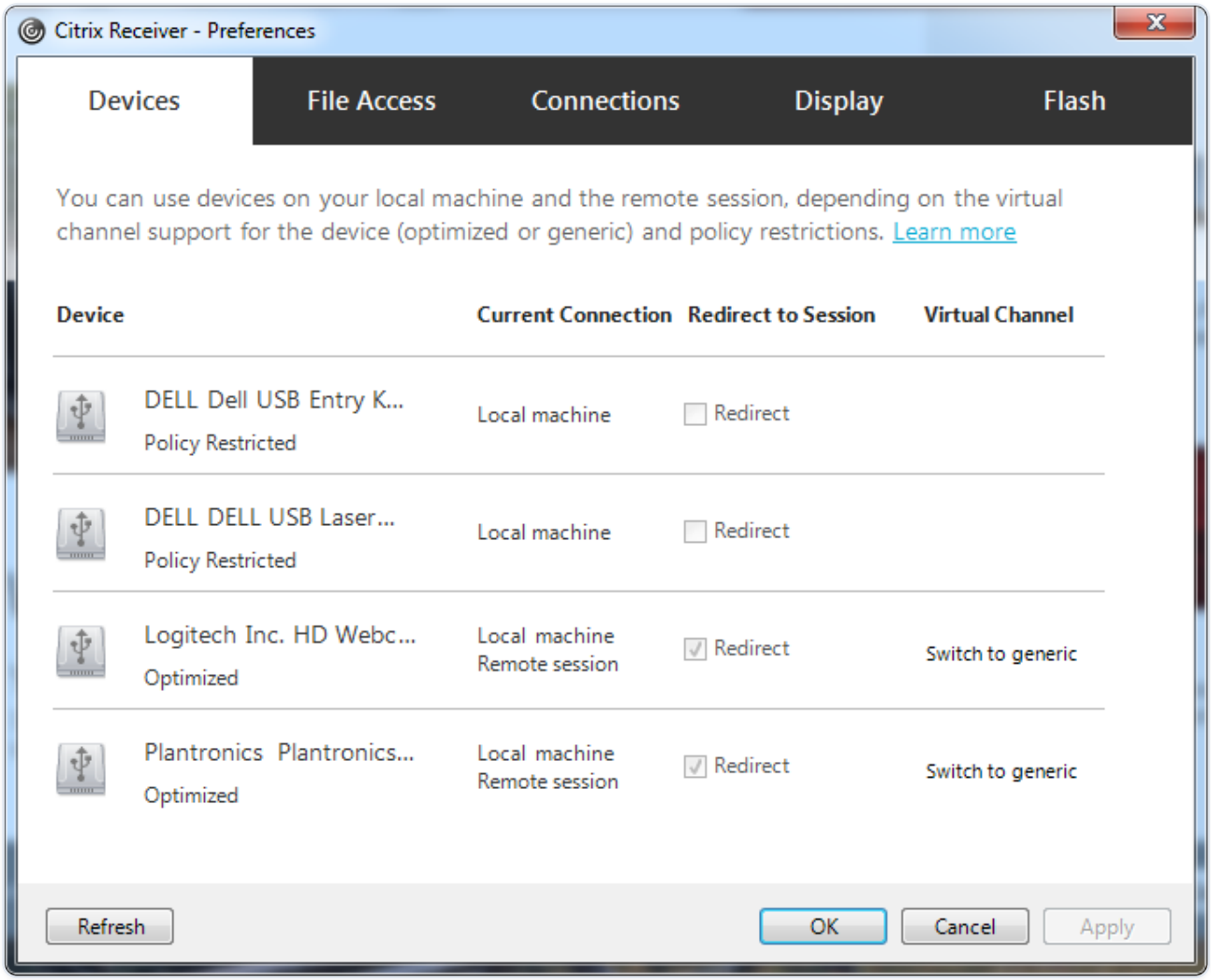
前の手順でVDAのUSBポリシー規則を指定した場合は、Citrix Workspaceアプリにも同じポリシー規則を指定します。

シンクライアントについては、USBサポートの詳細と必要な構成について製造元にお問い合わせください。

汎用USBリダイレクトで利用可能なUSBデバイスの種類を構成する

USBサポートが有効で、USBユーザー設定がUSBデバイスを自動的に接続するように設定されている場合、USBデバイスは自動的にリダイレクトされます。接続バーがない場合も、USBデバイスは自動的にリダイレクトされます。

ユーザーは、USBデバイスリストからデバイスを選択することで、自動的にリダイレクトされないデバイスを明示的にリダイレクトできます。詳細については、Citrix Workspaceアプリ for Windowsのユーザーヘルプ記事「Desktop Viewerにデバイスを表示する」を参照してください。



最適化されたサポートではなく、汎用USBリダイレクトを使用するには、次のいずれかの方法があります。

- Citrix Workspaceアプリで、汎用USBリダイレクトを使用するUSBデバイスを手動で選択し、［環境設定］ダイアログボックスの［デバイス］タブから**［汎用に切り替える］**を選択します。
- USBデバイスタイプ（例: AutoRedirectStorage=1）の自動リダイレクトを構成し、USBユーザー設定をUSBデバイスを自動的に接続するように設定することで、汎用USBリダイレクトを使用するUSBデバイスを自動的に選択します。詳細については、「USBデバイスの自動リダイレクトを構成する」を参照してください。

> **注：**
>
> Webカメラが HDX マルチメディアリダイレクトと互換性がないと判明した場合にのみ、Webカメラで使用する汎用USBリダイレクトを構成してください。

> USBデバイスがリストされたりリダイレクトされたりするのを完全に防ぐには、Citrix WorkspaceアプリとVDAのデバイス規則を指定できます。

汎用USBリダイレクトの場合、少なくともUSBデバイスクラスとサブクラスを知っている必要があります。すべてのUSBデバイスが、その明白なUSBデバイスクラスとサブクラスを使用するわけではありません。例：

- ペンはマウスデバイスクラスを使用します。
- スマートカードリーダーは、ベンダー定義またはHIDデバイスクラスを使用できます。

より正確な制御を行うには、ベンダーID、製品ID、およびリリースIDを知る必要があります。この情報はデバイスベンダーから入手できます。

> **重要:**
>
> 悪意のあるUSBデバイスは、意図された用途と一致しないUSBデバイス特性を示す場合があります。デバイスルールは、この動作を防ぐことを目的としていません。

> デフォルトのUSBポリシー規則を上書きするために、USBデバイスリダイレクト規則を指定することで、汎用USBリダイレクトで利用可能なUSBデバイスを制御します。

シトリックス DaaS（旧シトリックス バーチャル アプリケーションズ アンド デスクトップ サービス）：

- ほとんどの場合、Citrix Group Policy Management Console MSI（`CitrixGroupPolicyManagement_x64.msi`）をダウンロードしてActive Directoryシステムにインストールし、ADグループポリシーを管理します。（VDAにはMSIをインストールしないでください。）
- Citrix Workspaceアプリ for Windowsの場合、ユーザーデバイスのレジストリを編集します。インストールメディアには管理用テンプレート（ADMファイル）が含まれているため、Active Directoryグループポリシーを通じてユーザーデバイスを変更できます: dvd root `\os\lang\Support\Configuration\icaclient_usb.adm`

オンプレミス版Citrix Virtual Apps and Desktops：

- VDAの場合、グループポリシー規則を通じてマルチセッションOSマシンの管理者上書き規則を編集します。Group Policy Management Consoleはインストールメディアに含まれています:

  - x64: DVDルート `\os\lang\x64\Citrix Policy\CitrixGroupPolicyManagement_x64.msi`
  - x86: DVDルート `\os\lang\x86\Citrix Policy\CitrixGroupPolicyManagement_x86.msi`

- Citrix Workspaceアプリ for Windowsの場合、ユーザーデバイスのレジストリを編集します。インストールメディアには管理用テンプレート（ADMファイル）が含まれているため、Active Directoryグループポリシーを通じてユーザーデバイスを変更できます: dvd root `\os\lang\Support\Configuration\icaclient_usb.adm`

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

> 製品のデフォルト規則は、HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ICA Client\GenericUSB に保存されています。これらの製品のデフォルト規則は編集しないでください。代わりに、この記事の後半で説明する管理者上書き規則を作成するためのガイドとして使用してください。GPOの上書きは、製品のデフォルト規則よりも前に評価されます。

管理者上書き規則は、HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\PortICA\GenericUSB\DeviceRules に保存されています。GPOポリシー規則は、**{Allow: | Deny:}** の形式で、その後に空白で区切られた *tag=value* 式のセットが続きます。

次のタグがサポートされています:

タグ	説明
VID	デバイス記述子からのベンダーID
PID	デバイス記述子からの製品ID
REL	デバイス記述子からのリリースID

タグ	説明
クラス	デバイス記述子またはインターフェイス記述子のいずれかからのクラス。利用可能なUSBクラスコードについては、`<http://www.usb.org/>`のUSBウェブサイトを参照してください。
サブクラス	デバイス記述子またはインターフェース記述子のいずれかからのサブクラス
保護	デバイス記述子またはインターフェイス記述子のいずれかからのプロトコル

ポリシールールを作成する際は、次の点に注意してください。

- 規則では大文字と小文字は区別されません。
- ルールには、`#`で始まるオプションのコメントを末尾に含めることができます。区切り文字は不要で、コメントは照合目的では無視されます。
- 空行と純粋なコメント行は無視されます。
- 空白は区切り文字として使用されますが、数値または識別子の途中に含めることはできません。たとえば、「Deny: Class = 08 SubClass=05」は有効なルールですが、「Deny: Class=0 Sub Class=05」は無効です。
- タグは一致演算子「=」を使用する必要があります。例: VID=1230。
- 各ルールは新しい行で開始するか、セミコロンで区切られたリストの一部である必要があります。

注：

- Citrix Virtual Apps and Desktopsバージョン2212以降、一部のUSBデバイスは汎用USBリダイレクト機能の使用が無効になっています。これらのデバイスは、それぞれのベンダーID (VID) と製品ID (PID) を使用して明示的に追加する必要があります。
- ADMテンプレートファイルを使用している場合は、ルールをセミコロン区切りのリストとして1行で作成する必要があります。

例:

- 次の例は、ベンダーおよび製品識別子に対する管理者定義のUSBポリシールールを示しています。

  ```
  Allow: VID=046D PID=C626 # Allow Logitech SpaceNavigator 3D Mouse Deny: VID=046D # Deny all Logitech products
  ```

- 次の例は、定義されたクラス、サブクラス、およびプロトコルに対する管理者定義のUSBポリシールールを示しています。

  ```
  Deny: Class=EF SubClass=01 Prot=01 # Deny MS Active Sync devices Allow: Class=EF SubClass=01 # Allow Sync devices Allow: Class=EF # Allow all USB-Miscellaneous devices
  ```

USBデバイスの使用と削除

ユーザーは、仮想セッションを開始する前または後にUSBデバイスを接続できます。

Windows版Citrix Workspaceアプリを使用する場合、以下が適用されます。

- セッション開始後に接続されたデバイスは、Desktop ViewerのUSBメニューにすぐに表示されます。
- USBデバイスが適切にリダイレクトされない場合は、仮想セッションが開始されるまでデバイスの接続を待つことで問題を解決できる場合があります。
- データ損失を避けるため、USBデバイスを取り外す前にWindowsの「ハードウェアを安全に取り外す」アイコンを使用してください。

USBマスストレージデバイスのセキュリティ制御

USBマスストレージデバイスには、最適化されたサポートが提供されます。このサポートは、Citrix Virtual Apps and Desktopsのクライアントドライブマッピングの一部です。ユーザーがログオンすると、ユーザーデバイス上のドライブが仮想デスクトップ上のドライブ文字に自動的にマッピングされます。ドライブは、マッピングされたドライブ文字を持つ共有フォルダーとして表示されます。クライアントドライブマッピングを構成するには、**クライアントリムーバブルドライブ**設定を使用します。この設定は、ICAポリシー設定のファイルリダイレクトポリシー設定セクションにあります。

USBマスストレージデバイスでは、クライアントドライブマッピングまたは汎用USBリダイレクト、あるいはその両方を使用できます。これらはCitrixポリシーを使用して制御します。主な違いは次のとおりです。

機能	クライアントドライブマッピング	汎用USBリダイレクト
デフォルトで有効	はい	いいえ
読み取り専用アクセスを構成可能	はい	いいえ
暗号化されたデバイスアクセス	はい、デバイスにアクセスする前に暗号化が解除されている場合	はい
BitLocker To Goデバイス	いいえ	いいえ
セッション中にデバイスを安全に削除できる	いいえ	はい、ユーザーが安全な取り外しに関するオペレーティングシステムの推奨事項に従う場合

汎用USBリダイレクトとクライアントドライブマッピングの両方のポリシーが有効になっており、セッションの開始前または開始後にマスストレージデバイスが挿入された場合、クライアントドライブマッピングを使用してリダイレクトされます。汎用USBリダイレクトとクライアントドライブマッピングの両方のポリシーが有効になっており、デバイスが自動リダイレクト用に構成されていて、セッションの開始前または開始後にマスストレージデバイスが挿入された場合、汎用USBリダイレクトを使用してリダイレクトされます。詳しくは、Knowledge Centerの記事CTX123015を参照してください。

注：

USBリダイレクトは、50 Kbpsなどの低帯域幅接続でもサポートされます。ただし、大きなファイルのコピーは機能しません。

印刷

環境でのプリンターの管理は、多段階のプロセスです。

1. まだ印刷の概念に慣れていない場合は、慣れてください。
2. 印刷アーキテクチャを計画します。これには、ビジネスニーズ、既存の印刷インフラストラクチャ、ユーザーとアプリケーションが現在印刷とどのようにやり取りしているか、およびどの印刷管理モデルが環境に最適かを分析することが含まれます。
3. プリンタープロビジョニング方法を選択し、印刷設計を展開するためのポリシーを作成して、印刷環境を構成します。新しい従業員やサーバーが追加されたときにポリシーを更新します。
4. ユーザーに展開する前に、パイロット印刷構成をテストします。
5. プリンタードライバーを管理し、印刷パフォーマンスを最適化することで、Citrix® 印刷環境を維持します。
6. 発生する可能性のある問題をトラブルシューティングします。

印刷の概念

展開の計画を開始する前に、印刷に関する以下の主要な概念を理解していることを確認してください。

- 利用可能なプリンタープロビジョニングの種類
- 印刷ジョブのルーティング方法
- プリンタードライバー管理の基本

印刷の概念は、Windows の印刷の概念に基づいています。環境で印刷を構成し、正常に管理するには、Windows のネットワーク印刷とクライアント印刷がどのように機能するか、そしてそれがこの環境での印刷動作にどのように変換されるかを理解する必要があります。

印刷プロセス

この環境では、すべての印刷はアプリケーションをホストするマシン上で（ユーザーによって）開始されます。印刷ジョブは、ネットワークプリントサーバーまたはユーザーデバイスを介して印刷デバイスにリダイレクトされます。

仮想デスクトップおよびアプリケーションのユーザーには、永続的なワークスペースはありません。セッションが終了するとユーザーのワークスペースは削除されるため、すべての設定は各セッションの開始時に再構築する必要があります。その結果、ユーザーが新しいセッションを開始するたびに、システムはユーザーのワークスペースを再構築する必要があります。

ユーザーが印刷する場合：

- ユーザーに提供するプリンターを決定します。これはプリンタープロビジョニングとして知られています。
- ユーザーの印刷設定を復元します。
- セッションのデフォルトプリンターを決定します。

プリンタープロビジョニング、印刷ジョブルーティング、プリンタープロパティ保持、およびドライバー管理のオプションを構成することで、これらのタスクの実行方法をカスタマイズできます。さまざまなオプション設定が、環境での印刷パフォーマンスとユーザーエクスペリエンスにどのように影響するかを必ず評価してください。

プリンタープロビジョニング

セッションでプリンターを利用可能にするプロセスは、プロビジョニングとして知られています。プリンタープロビジョニングは通常、動的に処理されます。つまり、セッションに表示されるプリンターは、事前に決定されて保存されるわけではありません。代わりに、ログオン時および再接続時にセッションが構築される際に、ポリシーに基づいてプリンターが組み立てられます。その結果、ポリシーに反映されていれば、プリンターはポリシー、ユーザーの場所、およびネットワークの変更に応じて変化する可能性があります。したがって、別の場所に移動するユーザーは、ワークスペースの変更を確認する場合があります。

システムは、クライアント側のプリンターも監視し、クライアント側のプリンターへの追加、削除、変更に基づいて、セッション内の自動作成プリンターを動的に調整します。この動的なプリンター検出は、さまざまなデバイスから接続するモバイルユーザーにメリットをもたらします。

プリンタープロビジョニングの最も一般的な方法は次のとおりです。

- **ユニバーサルプリントサーバー** - Citrix Universal Print Server は、ネットワークプリンターのユニバーサル印刷をサポートします。ユニバーサルプリントサーバーは、ユニバーサル印刷ドライバーを使用します。このソリューションにより、マルチセッションOSマシンで単一のドライバーを使用して、任意のデバイスからネットワーク印刷を行うことができます。

Citrixは、リモートプリントサーバーのシナリオにCitrix Universal™ Print Serverを推奨します。ユニバーサルプリントサーバーは、最適化され圧縮された形式で印刷ジョブをネットワーク経由で

転送するため、ネットワークの使用量を最小限に抑え、ユーザーエクスペリエンスを向上させます。

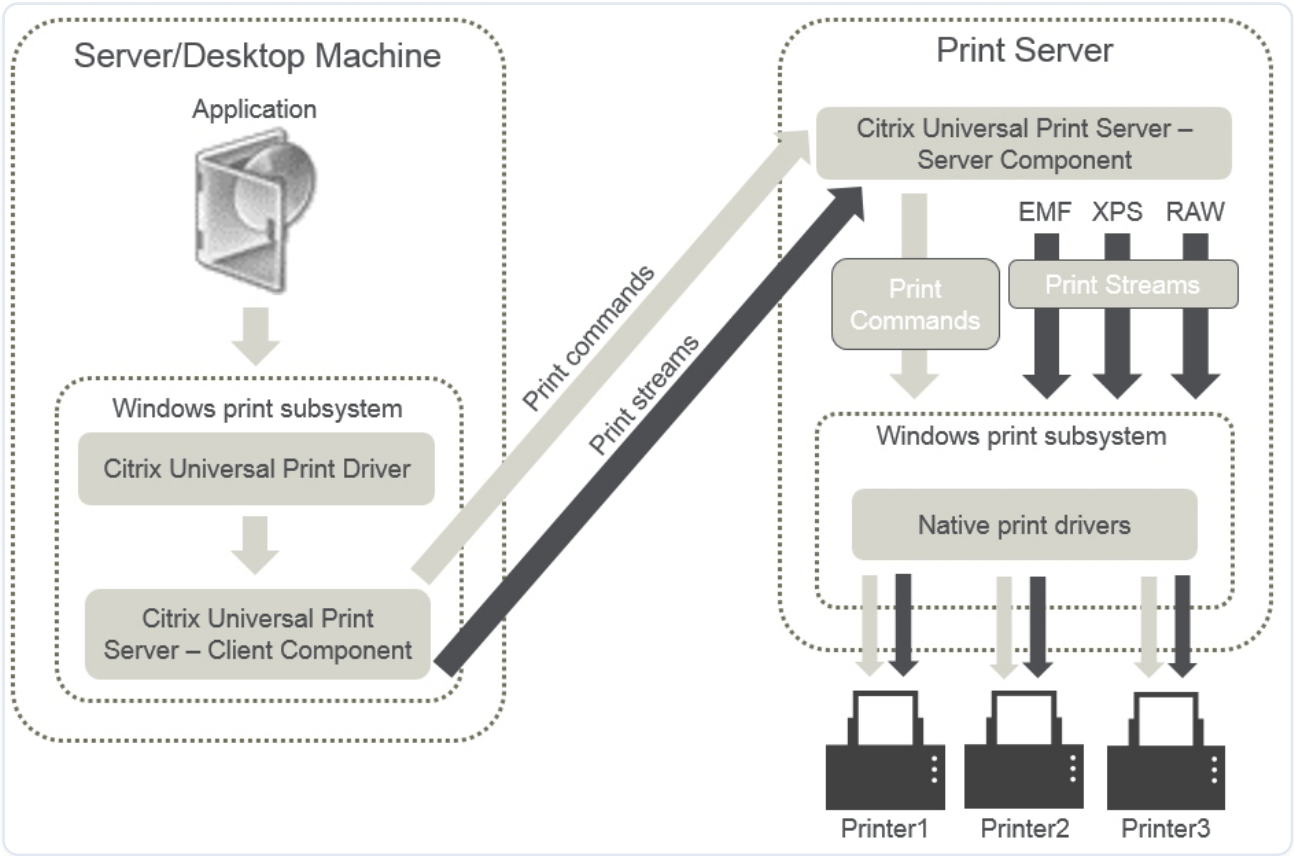
ユニバーサルプリントサーバーの機能は次のとおりです。

クライアントコンポーネント、**UPClient** - セッションネットワークプリンターをプロビジョニングし、ユニバーサル印刷ドライバーを使用する各マルチセッションOSマシンでUPClientを有効にします。

サーバーコンポーネント、**UPServer** - セッションネットワークプリンターをプロビジョニングし、セッションプリンターにユニバーサル印刷ドライバーを使用する各プリントサーバーにUPServerをインストールします（セッションプリンターが集中管理されているかどうかにかかわらず）。

Universal Print Serverの要件とセットアップの詳細については、システム要件およびインストールの記事を参照してください。

次の図は、Universal Print Serverを使用する環境におけるネットワークベースのプリンターの一般的なワークフローを示しています。



Citrix Universal Print Serverを有効にすると、接続されているすべてのネットワークプリンターが自動検出によって自動的に利用されます。

- **自動作成** - *自動作成*とは、各セッションの開始時に自動的に作成されるプリンターを指します。リモートネットワークプリンターとローカルに接続されたクライアントプリンターの両方を自動作成できます。ユーザーあたりのプリンター数が多い環境では、デフォルトのクライアントプリンターのみを自動作成することを検討してください。自動作成するプリンターの数を減らすと、Multi-session OSマシンでのオーバーヘッド（メモリとCPU）が少なくなります。自動作成されるプリンターを最小限に抑えることで、ユーザーのログオン時間を短縮することもできます。

  自動作成されるプリンターは、以下に基づいています。

  - ユーザーデバイスにインストールされているプリンター。
  - セッションに適用されるポリシー。

    自動作成ポリシー設定を使用すると、自動作成されるプリンターの数や種類を制限できます。デフォルトでは、ローカルに接続されたプリンターとネットワークプリンターを含む、ユーザーデバイス上のすべてのプリンターを自動的に構成すると、プリンターはセッションで利用可能になります。

  ユーザーがセッションを終了すると、そのセッションのプリンターは削除されます。

  クライアントおよびネットワークプリンターの自動作成には、関連するメンテナンスが必要です。たとえば、プリンターを追加するには、次の操作が必要です。

  - セッションプリンターポリシー設定を更新する。
  - プリンタードライバーマッピングおよび互換性ポリシー設定を使用して、すべてのMulti-session OSマシンにドライバーを追加する。

印刷ジョブのルーティング

「印刷経路」という用語は、印刷ジョブがルーティングされる経路と、印刷ジョブがスプールされる場所の両方を包含します。この概念の両方の側面が重要です。ルーティングはネットワークトラフィックに影響を与えます。スプールは、ジョブを処理するデバイス上のローカルリソースの利用に影響を与えます。

この環境では、印刷ジョブは印刷デバイスへの2つのパスを取ることができます。クライアント経由またはネットワーク印刷サーバー経由です。これらのパスは、クライアント印刷経路およびネットワーク印刷経路と呼ばれます。デフォルトでどちらのパスが選択されるかは、使用されるプリンターの種類によって異なります。

ローカル接続プリンター

システムは、マルチセッションOSマシンからクライアントを介して、ローカル接続プリンターにジョブをルーティングし、その後印刷デバイスにルーティングします。ICA®プロトコルは、印刷ジョブのトラフィックを最適化し、圧縮します。印刷デバイスがユーザーデバイスにローカルに接続されている場合、印刷ジョブはICA仮想チャネル経由でルーティングされます。

ローカル接続プリンターへの印刷ジョブのルーティング図(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/cds-print-local-attached.png)

ネットワークベースのプリンター

デフォルトでは、ネットワークプリンター宛てのすべての印刷ジョブは、マルチセッションOSマシンからネットワーク経由で直接印刷サーバーにルーティングされます。ただし、次の場合には、印刷ジョブはICA接続経由で自動的にルーティングされます。

- 仮想デスクトップまたはアプリケーションが印刷サーバーに接続できない場合。
- マルチセッションOSマシンでネイティブプリンタードライバーが利用できない場合。

Universal Print Serverが有効になっていない場合、ネットワーク印刷用にクライアント印刷経路を構成することは、ICA接続経由でジョブを送信することによって得られる最適化とトラフィック圧縮の恩恵を受けることができる、広域ネットワークなどの低帯域幅接続に役立ちます。

クライアント印刷経路を使用すると、トラフィックを制限したり、印刷ジョブに割り当てられる帯域幅を制限したりすることもできます。印刷機能のないシンクライアントのように、ユーザーデバイスを介したジョブのルーティングが不可能な場合は、ICA/HDXトラフィックを優先し、良好なセッション内ユーザーエクスペリエンスを確保するために、Quality of Serviceを構成する必要があります。

ネットワーク接続プリンターへの印刷ジョブのルーティング図(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/cds-print-network-attached.png)

印刷ドライバーの管理

Citrix Universal Printer Driver (UPD) は、ほとんどのプリンターと互換性のあるデバイス非依存の印刷ドライバーです。Citrix UPDは、次の2つのコンポーネントで構成されています。

サーバーコンポーネント。Citrix UPDは、Citrix Virtual Apps and Desktops™ VDAのインストールの一部としてインストールされます。VDAは、Citrix UPDとともに次のドライバーをインストールします。「Citrix Universal Printer」（EMFドライバー）および「Citrix XPS Universal Printer」（XPSドライバー）。

印刷ドライバー(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/print-drivers.png)

VDAインストーラーは、ユニバーサルプリントサーバーPDFプリンタードライバーのインストールを制御するオプションを提供しなくなりました。PDFプリンタードライバーは常に自動的にインストールされるようになりました。7.17 VDA（またはそれ以降のサポートされているバージョン）にアップグレードすると、以前にインストールされていたCitrix PDFプリンタードライバーは自動的に削除され、最新バージョンに置き換えられます。

印刷ジョブが開始されると、ドライバーはアプリケーションの出力を記録し、変更せずにエンドポイントデバイスに送信します。

クライアントコンポーネント。Citrix UPDは、Citrix Workspace™アプリのインストールの一部としてインストールされます。Citrix Virtual Apps and Desktopsセッションの受信印刷ストリームを取得します。その後、印刷ストリームをローカル印刷サブシステムに転送し、そこでデバイス固有のプリンタードライバーを使用して印刷ジョブがレンダリングされます。

Citrix UPDは、以下の印刷形式をサポートしています。

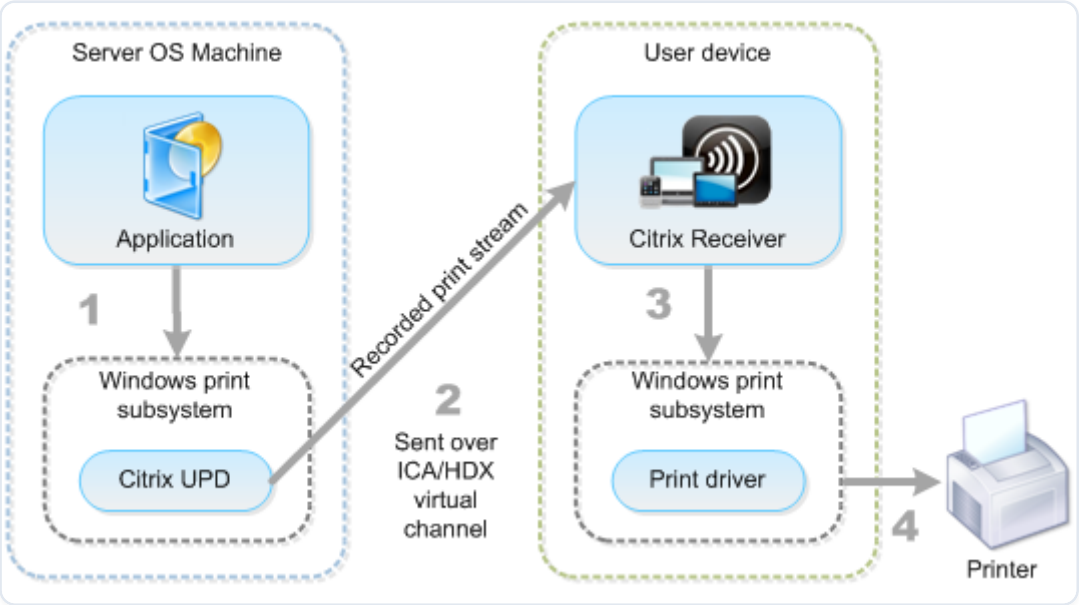
- 拡張メタファイル形式（**EMF**）。デフォルト。EMFは、Windowsメタファイル（WMF）形式の32ビットバージョンです。EMFドライバーは、Windowsベースのクライアントのみが使用できます。
- XML Paper Specification（**XPS**）。XPSドライバーは、XMLを使用してAdobe PDF形式に似たプラットフォームに依存しない「電子ペーパー」を作成します。
- Printer Command Language（**PCL5c**および**PCL4**）。PCLは、元々Hewlett-Packardがインクジェットプリンター用に開発した印刷プロトコルです。基本的なテキストとグラフィックの印刷に使用され、HP LaserJetおよび多機能周辺機器で広くサポートされています。
- PostScript（**PS**）。PostScriptは、テキストとベクターグラフィックの印刷に使用できるコンピューター言語です。このドライバーは、低コストのプリンターや多機能周辺機器で広く使用されています。

PCLおよびPSドライバーは、MacやUNIXクライアントなどのWindows以外のデバイスを使用する場合に最適です。Citrix UPDがドライバーを使用しようとする順序は、Universal driver preferenceポリシー設定を使用して変更できます。

Citrix UPD（EMFおよびXPSドライバー）は、ステープルや用紙トレイ選択などの高度な印刷機能をサポートしています。これらの機能は、ネイティブドライバーがMicrosoft Print Capabilityテクノロジーを使用して利用可能にしている場合に利用できます。ネイティブドライバーは、Print Capabilities XMLで標準化されたPrint Schema Keywordsを使用する必要があります。非標準の

キーワードが使用されている場合、Citrix Universal Print Driverでは高度な印刷機能は利用できません。

次の図は、ユニバーサルプリントドライバーのコンポーネントと、デバイスにローカルに接続されたプリンターの一般的なワークフローを示しています。



ドライバー管理戦略を計画する際には、ユニバーサルプリントドライバー、デバイス固有のドライバー、またはその両方をサポートするかどうかを決定します。標準ドライバーをサポートする場合、以下を決定する必要があります。

プリンターの自動作成中に、システムがユーザーデバイスに接続された新しいローカルプリンターを検出すると、必要なプリンタードライバーについてマルチセッションOSマシンをチェックします。デフォルトでは、Windowsネイティブドライバーが利用できない場合、システムはユニバーサルプリントドライバーを使用します。

印刷を成功させるには、マルチセッションOSマシン上のプリンタードライバーとユーザーデバイス上のドライバーが一致している必要があります。次の図は、クライアント印刷でプリンタードライバーが2か所でどのように使用されるかを示しています。

クライアントがローカルプリンターに印刷する図(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/cds-print-client-routing.png)

- サポートするドライバーの種類。
- マルチセッションOSマシンにプリンタードライバーがない場合に、自動的にインストールするかどうか。
- ドライバー互換性リストを作成するかどうか。

関連コンテンツ

- 印刷構成の例(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/printing/printing-configuration-example.html)
- ベストプラクティス、セキュリティに関する考慮事項、およびデフォルトの操作(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/printing/printing-best-practices.html)
- 印刷ポリシーと設定(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/printing/printing-policies-preferences.html)
- プリンターのプロビジョニング(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/printing/printing-provision-printers.html)
- 印刷環境の維持(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/printing/printing-maintain-environment.html)

印刷構成の例

ニーズと環境に最も適した印刷構成オプションを選択することで、管理を簡素化できます。デフォルトの印刷構成では、ほとんどの環境でユーザーが印刷できますが、デフォルトでは、期待されるユーザーエクスペリエンスや、環境に最適なネットワーク使用量と管理オーバーヘッドが提供されない場合があります。

印刷構成は、以下によって異なります。

- ビジネスニーズと既存の印刷インフラストラクチャ。

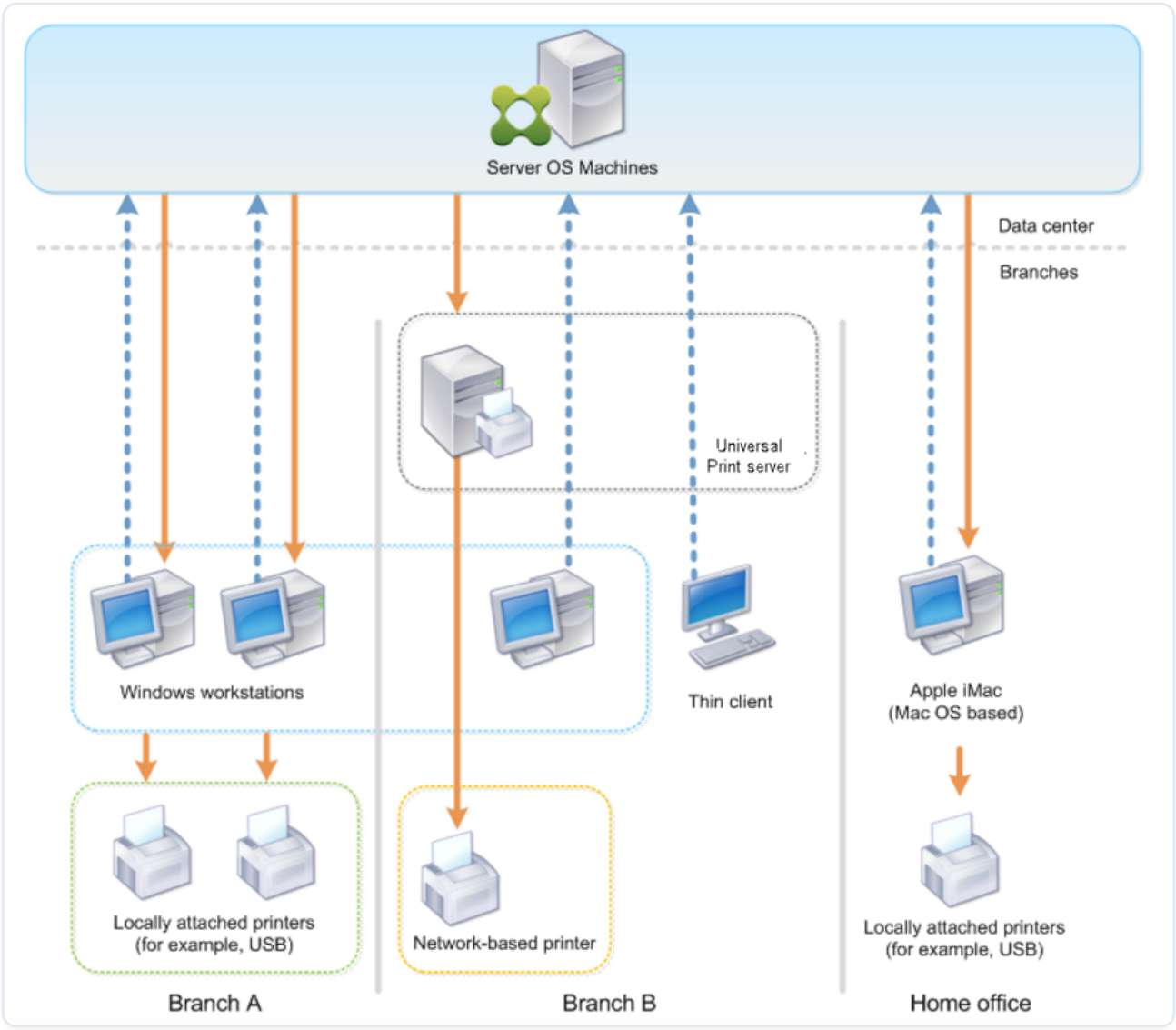
  組織のニーズに合わせて印刷構成を設計します。既存の印刷実装（ユーザーがプリンターを追加できるかどうか、どのユーザーがどのプリンターにアクセスできるかなど）は、印刷構成を定義する際に役立つガイドとなる場合があります。
- 組織に、特定のユーザー（人事部や給与計算部門のプリンターなど）のためにプリンターを予約するセキュリティポリシーがあるかどうか。
- ユーザーが主要な作業場所から離れているときに印刷する必要があるかどうか（ワークステーション間を移動する従業員や出張中の従業員など）。

印刷構成を設計する際は、ローカルユーザーデバイスから印刷する場合と同じエクスペリエンスをセッション内でユーザーに提供するように努めてください。

印刷展開の例

次の図は、これらのユースケースの印刷展開を示しています。

- **支店A** - 数台のWindowsワークステーションがある小規模な海外支店。各ユーザーワークステーションには、ローカルに接続されたプライベートプリンターがあります。
- **支店B** - シンクライアントとWindowsベースのワークステーションがある大規模な支店。効率を高めるため、この支店のユーザーはネットワークベースのプリンター（フロアごとに1台）を共有しています。支店内に設置されたWindowsベースのプリントサーバーが印刷キューを管理します。
- **ホームオフィス** - 会社のCitrix®インフラストラクチャにアクセスするMac OSベースのユーザーデバイスがあるホームオフィス。ユーザーデバイスには、ローカルに接続されたプリンターがあります。



以下のセクションでは、環境の複雑さを最小限に抑え、管理を簡素化する構成について説明します。

自動作成されたクライアントプリンターとCitrix Universal™プリンタードライバー

支店Aでは、すべてのユーザーがWindowsベースのワークステーションで作業するため、自動作成されたクライアントプリンターとユニバーサルプリンタードライバーが使用されます。これらのテクノロジーは、以下の利点を提供します。

- パフォーマンス - 印刷ジョブはICA®印刷チャネルを介して配信されるため、印刷データを圧縮して帯域幅を節約できます。

  大容量のドキュメントを印刷する単一のユーザーが他のユーザーのセッションパフォーマンスを低下させないように、Citrixポリシーが構成され、最大印刷帯域幅が指定されます。

  代替ソリューションとして、マルチストリームICA接続を活用する方法があります。この接続では、印刷トラフィックは別の低優先度TCP接続内で転送されます。マルチストリームICAは、WAN接続でQuality of Service (QoS) が実装されていない場合のオプションです。
- 柔軟性 - Citrix Universalプリンタードライバーを使用することで、クライアントに接続されたすべてのプリンターを、データセンターに新しいプリンタードライバーを統合することなく、仮想デスクトップまたはアプリケーションセッションから使用できます。

Citrix ユニバーサルプリントサーバー

支店Bでは、すべてのプリンターがネットワークベースであり、そのキューはWindowsプリントサーバーで管理されているため、Citrix Universal Print Serverが最も効率的な構成となります。

必要なすべてのプリンタードライバーは、ローカル管理者によってプリントサーバーにインストールおよび管理されます。仮想デスクトップまたはアプリケーションセッションへのプリンターのマッピングは、次のとおりです。

- Windowsベースのワークステーションの場合 - ローカルITチームは、ユーザーが適切なネットワークベースのプリンターをWindowsワークステーションに接続するのを支援します。これにより、ユーザーはローカルにインストールされたアプリケーションから印刷できるようになります。

  仮想デスクトップまたはアプリケーションセッション中、ローカルで構成されたプリンターは自動作成によって列挙されます。その後、仮想デスクトップまたはアプリケーションは、可能であれば直接ネットワーク接続としてプリントサーバーに接続します。

  Citrix Universal Print Serverコンポーネントがインストールされ有効になっているため、ネイティブプリンタードライバーは不要です。ドライバーが更新されたり、プリンターキューが変更されたりしても、データセンターでの追加構成は必要ありません。

- シンクライアントの場合 - シンクライアントユーザーの場合、プリンターは仮想デスクトップまたはアプリケーションセッション内で接続する必要があります。ユーザーに最もシンプルな印刷エクスペリエンスを提供するために、管理者はフロアごとに単一のCitrixセッションプリンターポリシーを構成し、そのフロアのプリンターをデフォルトプリンターとして接続します。

  ユーザーがフロア間を移動しても正しいプリンターが接続されるように、ポリシーはサブネットまたはシンクライアントの名前に基づいてフィルタリングされます。この構成は近接印刷と呼ばれ、ローカルプリンタードライバーのメンテナンス（委任された管理モデルに従って）を可能にします。

  プリンターキューを変更または追加する必要がある場合、Citrix管理者は環境内の該当するセッションプリンターポリシーを変更する必要があります。

ネットワーク印刷トラフィックはICA仮想チャネルの外部で送信されるため、QoSが実装されます。ICA/HDXトラフィックで使用されるポートのインバウンドおよびアウトバウンドネットワークトラフィックは、他のすべてのネットワークトラフィックよりも優先されます。この構成により、大規模な印刷ジョブによってユーザーセッションが影響を受けることはありません。

自動作成されたクライアントプリンターとCitrix Universal Printer Driver

ユーザーが非標準のワークステーションで作業し、管理されていない印刷デバイスを使用するホームオフィスの場合、最も簡単なアプローチは、自動作成されたクライアントプリンターとUniversal Printer Driverを使用することです。

展開の概要

まとめると、サンプル展開は次のように構成されています。

- Multi-session OSマシンにはプリンタードライバーはインストールされていません。Citrix Universal Printer Driverのみが使用されます。ネイティブ印刷へのフォールバックとプリンタードライバーの自動インストールは無効になっています。
- すべてのユーザーに対してすべてのクライアントプリンターを自動作成するようにポリシーが構成されています。Multi-session OSマシンは、デフォルトで印刷サーバーに直接接続します。必要な構成は、Universal Print Serverコンポーネントを有効にすることだけです。
- ブランチBの各フロアに対してセッションプリンターポリシーが構成され、それぞれのフロアのすべてのシンクライアントに適用されます。
- 優れたユーザーエクスペリエンスを確保するために、ブランチBにQoSが実装されています。

ベストプラクティス、セキュリティに関する考慮事項、およびデフォルトの操作

ベストプラクティス

特定の環境に最適な印刷ソリューションを決定する要因は多数あります。これらのベストプラクティスの一部は、お客様のサイトには適用されない場合があります。

- Citrix Universal™ Print Serverを使用します。
- UniversalプリンタードライバーまたはWindowsネイティブドライバーを使用します。
- マルチセッションOSマシンにインストールするプリンタードライバーの数を最小限に抑えます。
- ネイティブドライバーへのドライバーマッピングを使用します。
- テストされていないプリンタードライバーを実稼働サイトにインストールしないでください。
- ドライバーの更新は避けてください。常にドライバーをアンインストールし、プリントサーバーを再起動してから、交換用ドライバーをインストールするようにしてください。
- 使用されていないドライバーをアンインストールするか、プリンタードライバーマッピングおよび互換性ポリシーを使用して、そのドライバーでプリンターが作成されないようにします。
- バージョン2のカーネルモードドライバーの使用は避けてください。
- プリンターモデルがサポートされているかどうかを確認するには、製造元に問い合わせるか、www.citrix.com/readyでCitrix Ready製品ガイドを参照してください。

  一般的に、Microsoftが提供するすべてのプリンタードライバーはTerminal Servicesでテストされており、Citrixで動作することが保証されています。ただし、サードパーティ製プリンタードライバーを使用する前に、Windows Hardware Quality Labs（WHQL）プログラムによってTerminal Services向けに認定されていることをプリンタードライバーベンダーに確認してください。Citrixはプリンタードライバーを認定していません。

セキュリティに関する考慮事項

Citrixの印刷ソリューションは、設計上安全です。

- Citrix Print Manager Serviceは、ログオンとログオフ、切断、再接続、セッション終了などのセッションイベントを常に監視し、対応します。実際のセッションユーザーを偽装してサービス要求を処理します。
- Citrix Printing は、各プリンターにセッション内で一意の名前空間を割り当てます。

- Citrix Printing は、自動作成されたプリンターのデフォルトのセキュリティ記述子を設定し、あるセッションで自動作成されたクライアントプリンターが他のセッションで実行中のユーザーからアクセスできないようにします。デフォルトでは、管理ユーザーは、任意のクライアントプリンターの権限を表示および手動で調整できる場合でも、誤って他のセッションのクライアントプリンターに印刷することはできません。

デフォルトの印刷操作

デフォルトでは、ポリシー規則を構成しない場合、印刷動作は次のとおりです。

- ユニバーサルプリントサーバーは無効になっています。
- ユーザーデバイスで構成されたすべてのプリンターは、各セッションの開始時に自動的に作成されます。

  この動作は、Citrix ポリシー設定「クライアントプリンターの自動作成」を「すべてのクライアントプリンターを自動作成」オプションで構成することと同じです。
- システムは、ユーザーデバイスにローカルに接続されたプリンターにキューに入れられたすべての印刷ジョブを、クライアント印刷ジョブとして（つまり、ICA® チャネル経由でユーザーデバイスを介して）ルーティングします。
- システムは、ネットワークプリンターにキューに入れられたすべての印刷ジョブを、Multi-session OS マシンから直接ルーティングします。システムがネットワーク経由でジョブをルーティングできない場合、それらをリダイレクトされたクライアント印刷ジョブとしてユーザーデバイスを介してルーティングします。

  この動作は、Citrix ポリシー設定「印刷サーバーへの直接接続」を無効にすることと同じです。
- システムは、ユーザーの印刷設定と印刷デバイス固有の設定の組み合わせである印刷プロパティを、ユーザーデバイスに保存しようとします。クライアントがこの操作をサポートしない場合、システムは印刷プロパティをMulti-session OS マシンのユーザープロファイルに保存します。

  この動作は、Citrix ポリシー設定「プリンタープロパティの保持」を「クライアントに保存されていない場合のみプロファイルに保持」オプションで構成することと同じです。
- VDA バージョン 7.16 以降では、V3 インボックスプリンタードライバーがオペレーティングシステムに含まれていないため、Citrix ポリシー設定「インボックスプリンタードライバーの自動インストール」は Windows 8 以降の Windows オペレーティングシステムバージョンには影響しません。

- 7.16 より前の VDA では、Multi-session OS マシンで利用可能な場合、システムはプリンタードライバーの Windows バージョンを使用します。プリンタードライバーが利用できない場合、システムは Windows オペレーティングシステムからドライバーをインストールしようとします。ドライバーが Windows で利用できない場合、Citrix Universal Print Driver を使用します。

  この動作は、Citrix ポリシー設定「インボックスプリンタードライバーの自動インストール」を有効にし、ユニバーサル印刷設定を「要求されたドライバーが利用できない場合にのみユニバーサル印刷を使用する」で構成することと同じです。

  「インボックスプリンタードライバーの自動インストール」を有効にすると、多数のネイティブプリンタードライバーがインストールされる可能性があります。

> **注：**
>
> 印刷の出荷時デフォルト設定が不明な場合は、新しいポリシーを作成し、すべての印刷ポリシー規則を「有効」に設定することで、それらを表示できます。表示されるオプションがデフォルトです。

常時オンのログ記録

VDA上のプリントサーバーと印刷サブシステムで、常時オンのログ記録機能が利用可能です。

ログをZIP形式でまとめてメール送信するため、またはCitrix Insight Servicesにログを自動的にアップロードするためには、**Start-TelemetryUpload** PowerShellコマンドレットを使用します。

印刷ポリシーと設定

ユーザーが公開アプリケーションからプリンターにアクセスする際、Citrix®ポリシーを設定して以下を指定できます。

- プリンターのプロビジョニング方法（またはセッションへの追加方法）
- 印刷ジョブのルーティング方法
- プリンタードライバーの管理方法

ユーザーデバイス、ユーザー、またはポリシーがフィルターされるその他のオブジェクトごとに、異なる印刷構成を設定できます。

ほとんどの印刷機能は、Citrixの印刷ポリシー設定を通じて構成されます。印刷設定は、標準のCitrixポリシーの動作に従います。

ユーザーのネットワークアカウントに十分な権限がある場合、システムはセッションの終了時にプリンター設定をプリンターオブジェクトまたはクライアント印刷デバイスに書き込むことができます。デフォルトでは、Citrix Workspace™アプリは、設定や環境設定を他の場所で探す前に、セッション内のプリンターオブジェクトに保存されている設定を使用します。

デフォルトでは、システムはプリンタープロパティをユーザーデバイス上（デバイスがサポートしている場合）またはMulti-session OSマシンのユーザープロファイルに保存または保持します。ユーザーがセッション中にプリンタープロパティを変更すると、それらの変更はマシンのユーザープロファイルに更新されます。ユーザーが次回ログオンまたは再接続すると、ユーザーデバイスは保持されているそれらの設定を継承します。つまり、ユーザーデバイスでのプリンタープロパティの変更は、ユーザーがログオフして再度ログオンするまで、現在のセッションには影響しません。

印刷設定の場所

Windowsの印刷環境では、印刷設定への変更はローカルコンピューターまたはドキュメントに保存できます。この環境では、ユーザーが印刷設定を変更すると、設定は以下の場所に保存されます。

- **ユーザーデバイス自体** - Windowsユーザーは、コントロールパネルでプリンターを右クリックし、「印刷設定」を選択することで、ユーザーデバイス上のデバイス設定を変更できます。たとえば、ページ方向として「横」が選択された場合、そのプリンターのデフォルトのページ方向設定として「横」が保存されます。
- **ドキュメント内** - ワープロやデスクトップパブリッシングプログラムでは、ページ方向などのドキュメント設定がドキュメント内に保存されることがよくあります。たとえば、ドキュメントを印刷キューに入れると、Microsoft Wordは通常、指定した印刷設定（ページ方向やプリンター名など）をドキュメント内に保存します。これらの設定は、次回そのドキュメントを印刷する際にデフォルトで表示されます。
- **ユーザーがセッション中に行った変更から** - システムは、自動作成されたプリンターの印刷設定への変更がセッション内のコントロールパネル（つまり、Multi-session OSマシン上）で行われた場合にのみ、その変更を保持します。
- **Multi-session OSマシン上** - これらは、マシン上の特定のプリンタードライバーに関連付けられたデフォルト設定です。

Windowsベースの環境で保持される設定は、ユーザーが変更を行った場所によって異なります。これは、スプレッドシートプログラムなど、ある場所に表示される印刷設定が、ドキュメントなど

他の場所の設定とは異なる場合があることも意味します。結果として、特定のプリンターに適用される印刷設定は、セッション中に変更される可能性があります。

ユーザーの印刷設定の階層

印刷設定は複数の場所に保存できるため、システムは特定の優先順位に従ってそれらを処理します。また、デバイス設定はドキュメント設定とは別に扱われ、通常はドキュメント設定よりも優先されることに注意することが重要です。

デフォルトでは、システムは常に、ユーザーがセッション中に変更した印刷設定（つまり、保持された設定）を、他の設定を考慮する前に適用します。ユーザーが印刷すると、システムはMulti-session OSマシンに保存されているデフォルトのプリンター設定と、保持されているクライアントプリンター設定を結合して適用します。

ユーザーの印刷設定の保存

Citrixでは、プリンタープロパティの保存場所を変更しないことをお勧めします。ユーザーデバイスにプリンタープロパティを保存するデフォルト設定は、一貫した印刷プロパティを確保する最も簡単な方法です。システムがユーザーデバイスにプロパティを保存できない場合、自動的にMulti-session OSマシンのユーザープロファイルにフォールバックします。

次のシナリオに該当する場合は、プリンタープロパティ保持ポリシー設定を確認してください。

- ユーザーがユーザーデバイスにプリンタープロパティを保存できないレガシープラグインを使用している場合。
- Windowsネットワークで強制プロファイルを使用しており、ユーザーのプリンタープロパティを保持したい場合。

プリンターのプロビジョニング

Citrix Universal™ プリントサーバー

環境に最適な印刷ソリューションを決定する際には、次の点を考慮してください。

- Universal Print Server は、Windows Print Provider では利用できない機能（イメージとフォントのキャッシュ、高度な圧縮、最適化、QoS サポート）を提供します。
- Universal Print Driver は、Microsoft が定義するパブリックなデバイス非依存設定をサポートします。ユーザーが特定のプリンタードライバーメーカーに固有のデバイス設定にアクセスする必要がある場合、Universal Print Server と Windows ネイティブドライバーの組み合わせが最適なソリューションとなる可能性があります。この構成により、Universal Print Server の利点

を維持しつつ、ユーザーに特殊なプリンター機能へのアクセスを提供できます。考慮すべきトレードオフとして、Windows ネイティブドライバーにはメンテナンスが必要です。

- Citrix Universal Print Server は、ネットワークプリンターのユニバーサル印刷をサポートします。Universal Print Server は、Multi-session OS マシン上の単一ドライバーである Universal Print Driver を使用して、シンクライアントやタブレットを含むあらゆるデバイスからのローカルまたはネットワーク印刷を可能にします。

Windows ネイティブドライバーで Universal Print Server を使用するには、Universal Print Server を有効にします。デフォルトでは、Windows ネイティブドライバーが利用可能な場合はそれが使用されます。そうでない場合は、Universal Print Driver が使用されます。その動作を変更する（Windows ネイティブドライバーのみを使用する、または Universal Print Driver のみを使用するなど）には、Universal Print Driver の使用ポリシー設定を更新します。

Universal Print Server のインストール

Universal Print Server を使用するには、インストールドキュメントに記載されているとおりに、UpsServer コンポーネントをプリントサーバーにインストールして構成します。詳細については、「コアコンポーネントのインストール」および「コマンドラインを使用したインストール」を参照してください。

UPClient コンポーネントを個別に展開したい環境（例: **XenApp 6.5** を使用する場合）の場合：

1. Windows Single-session OS または Windows Multi-session OS 用の Citrix Virtual Apps and Desktops™ Virtual Delivery Agent (VDA) スタンドアロンパッケージをダウンロードします。
2. 「コマンドラインを使用したインストール」に記載されているコマンドライン手順を使用して VDA を抽出します。
3. `\Image-Full\Support\VcRedist_2013_RTM` から前提条件をインストールします。
    - Vcredist_x64 / vcredist_x86
        - 32 ビット展開の場合は x86 を実行し、64 ビット展開の場合は両方を実行します。
4. `\Image-Full\x64\Virtual Desktop Components` または `\Image-Full\x86\Virtual Desktop Components` からcdfの前提条件をインストールします。
    - Cdf_x64 / Cdf_x86
        - 32ビットの場合はx86、64ビットの場合はx64
5. `\Image-Full\x64\Virtual Desktop Components` または `\Image-Full\x86\Virtual Desktop Components` でUPClientコンポーネントを見つけます。

6. UPClientコンポーネントを抽出し、そのMSIを起動してインストールします。
7. UPClientコンポーネントのインストール後、再起動が必要です。

Universal Print ServerのCEIPをオプトアウトする

Universal Print Serverをインストールすると、Citrixカスタマーエクスペリエンス向上プログラム（CEIP）に自動的に登録されます。データの初回アップロードは、インストール日時から7日後に行われます。

CEIPをオプトアウトするには、レジストリキー**`HKLM\Software\Citrix\Universal Print Server\CEIPEnabled`を編集し、DWORD値を**0**に設定します。

再度オプトインするには、DWORD値を1に設定します。

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

詳細については、Citrix Insight Servicesを参照してください。

Universal Print Serverを構成する

Universal Print Serverを構成するには、以下のCitrixポリシー設定を使用します。詳細については、画面上のポリシー設定ヘルプを参照してください。

- **Universal Print Serverを有効にする**。Universal Print Serverはデフォルトで無効になっています。Universal Print Serverを有効にすると、Universal Print Serverが利用できない場合にWindows Print Providerを使用するかどうかを選択します。Universal Print Serverを有効にすると、ユーザーはWindows Print ProviderおよびCitrix Providerインターフェイスを介してネットワークプリンターを追加および列挙できます。
- **Universal Print Server印刷データストリーム (CGP) ポート**。Universal Print Server印刷データストリームCGP (Common Gateway Protocol) リスナーが使用するTCPポート番号を指定します。デフォルトは**7229**です。
- **ユニバーサルプリントサーバー Webサービス (HTTP/SOAP) ポート**。ユニバーサルプリントサーバーリスナーが受信HTTP/SOAP要求に使用するTCPポート番号を指定します。デフォルトは**8080**です。

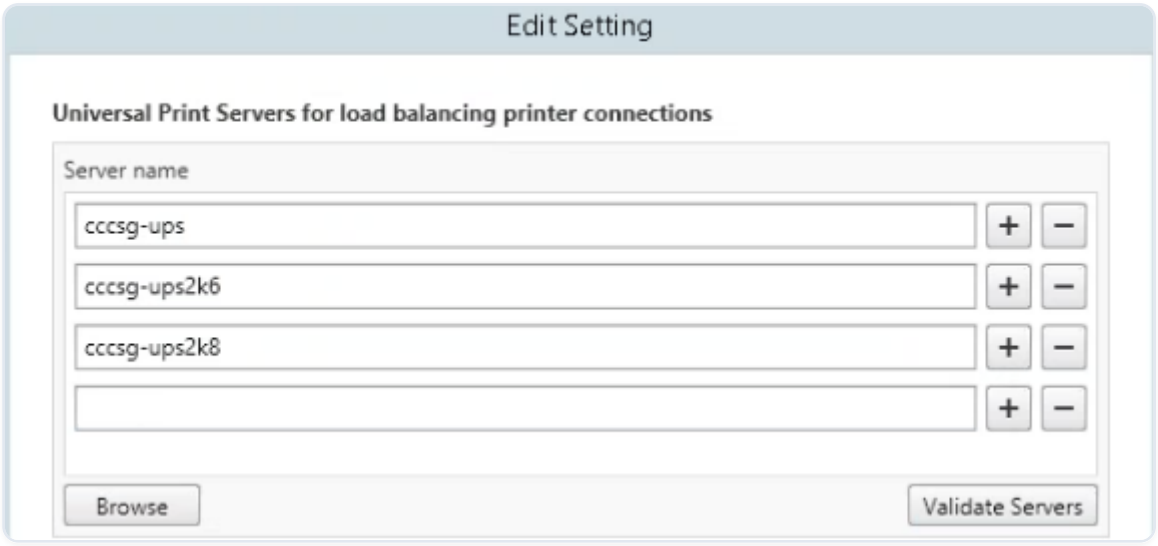
Citrix Virtual Apps and Desktops VDAへのUniversal Print Server通信のデフォルトポートであるHTTP 8080を変更するには、Universal Print Serverコンピューターで以下のレジストリを作成し、ポート番号の値を変更する必要があります。

`HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\PrintingPolicies`

"UpsHttpPort"=DWORD:\<portnumber\>

このポート番号は、StudioのHDXポリシー、Universal Print Server Webサービス (HTTP/SOAP) ポートと一致している必要があります。

- **Universal Print Server印刷ストリーム入力帯域幅制限 (kbps)**。CGPを使用して各印刷ジョブからUniversal Print Serverに配信される印刷データの転送速度の上限 (キロビット/秒) を指定します。デフォルトは0 (無制限) です。
- **負荷分散用のUniversal Print Server**。この設定は、他のCitrix印刷ポリシー設定を評価した後、セッション起動時に確立されたプリンター接続の負荷分散に使用されるUniversal Print Serverを一覧表示します。プリンター作成時間を最適化するために、Citrixはすべての印刷サーバーが同じ共有プリンターのセットを持つことを推奨します。



- **Universal Print Serverのサービス停止しきい値**。ロードバランサーが、利用できない印刷サーバーが回復するまで待機する時間を指定します。この時間を過ぎると、サーバーは永続的にオフラインであると判断され、その負荷は他の利用可能な印刷サーバーに再分散されます。デフォルトは180 (秒) です。

Delivery Controller™で印刷ポリシーが変更されると、ポリシーの変更がVDAに適用されるまでに数分かかる場合があります。

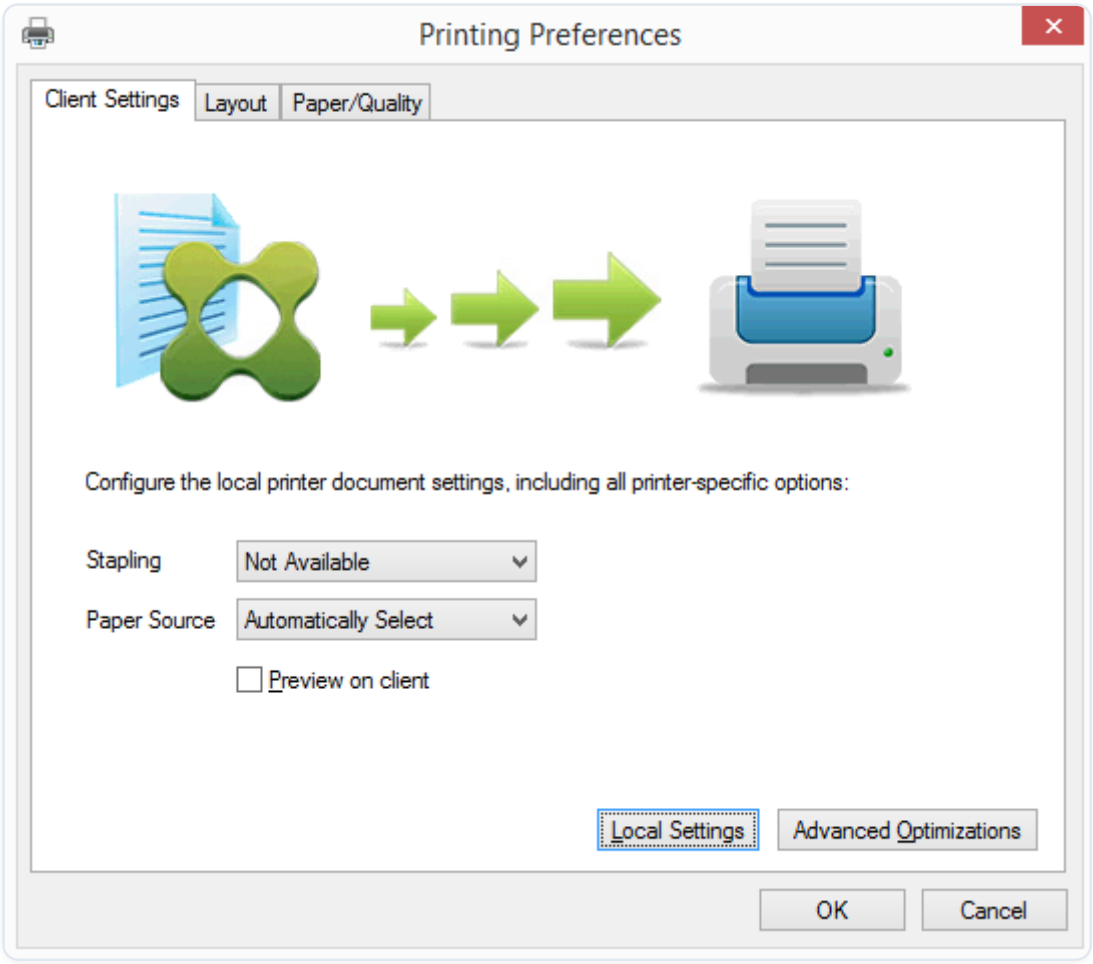
他のポリシー設定との相互作用 - Universal Print Serverは、他のCitrix印刷ポリシー設定を尊重し、以下の表に示すようにそれらと相互作用します。提供される情報は、Universal Print Serverポリシー設定が有効になっており、Universal Print Serverコンポーネントがインストールされ、ポリシー設定が適用されていることを前提としています。

ポリシー設定	**相互作用**
クライアントプリンターのリダイレクト、クライアントプリンターの自動作成	Universal Print Serverが有効になると、クライアントネットワークプリンターはネイティブドライバーではなくUniversal Print Driverを使用して作成されます。ユーザーは以前と同じプリンター名を確認できます。
セッションプリンター	Citrix Universal Print Serverソリューションを使用する場合、ユニバーサルプリントドライバーのポリシー設定が適用されます。
プリントサーバーへの直接接続	Universal Print Serverが有効で、ユニバーサルプリントドライバーの使用ポリシー設定がユニバーサル印刷のみを使用するように構成されている場合、ユニバーサルプリントドライバーを使用して、プリントサーバーへの直接ネットワークプリンター接続を作成できます。
UPDの優先設定	EMFおよびXPSドライバーをサポートします。

ユーザーインターフェイスへの影響 - Universal Print Serverで使用されるCitrix Universal Print Driverは、以下のユーザーインターフェイスコントロールを無効にします。

- プリンターのプロパティダイアログボックスの「ローカルプリンター設定」ボタン
- ドキュメントのプロパティダイアログボックスの「ローカルプリンター設定」および「クライアントでプレビュー」ボタン

Citrix Universal Print Driver（EMFおよびXPSドライバー）は、ステープルや給紙元などの高度な印刷機能をサポートしています。セッション内でUPDにマップされているクライアントまたはネットワークプリンターがこれらの機能をサポートしている場合、ユーザーはカスタムUPD印刷ダイアログから「ステープル」または「給紙元」オプションを選択できます。



ステープルやセキュアPINなどの非標準のプリンター設定を行うには、Citrix UPD EMFまたはXPSドライバーを使用するクライアントマッププリンターのカスタムUPD印刷ダイアログで**ローカル設定**を選択します。マップされたプリンターの**印刷設定**ダイアログがセッション外のクライアントに表示され、ユーザーは任意のプリンターオプションを変更できます。変更されたプリンター設定は、そのドキュメントを印刷する際にアクティブなセッションで使用されます。

これらの機能は、ネイティブドライバーがMicrosoft Print Capabilityテクノロジーを使用して利用可能にしている場合に利用できます。ネイティブドライバーは、Print Capabilities XMLで標準化されたPrint Schema Keywordsを使用する必要があります。非標準のキーワードが使用されている場合、Citrix Universal Print Driverを使用しても高度な印刷機能は利用できません。

Universal Print Serverを使用する場合、Citrix Print Providerのプリンターの追加ウィザードは、Windows Print Providerのプリンターの追加ウィザードと同じですが、以下の例外があります。

- 名前またはアドレスでプリンターを追加する場合、プリントサーバーのHTTP/SOAPポート番号を指定できます。そのポート番号はプリンター名の一部となり、表示されます。
- Citrix Universal print driver usageポリシー設定でユニバーサル印刷を使用する必要があると指定されている場合、プリンターの選択時にUniversal print driver名が表示されます。Windows Print ProviderはUniversal print driverを使用できません。

Citrix Print Providerは、クライアント側レンダリングをサポートしていません。

Universal Print Serverの詳細については、CTX200328を参照してください。

自動作成されたクライアントプリンター

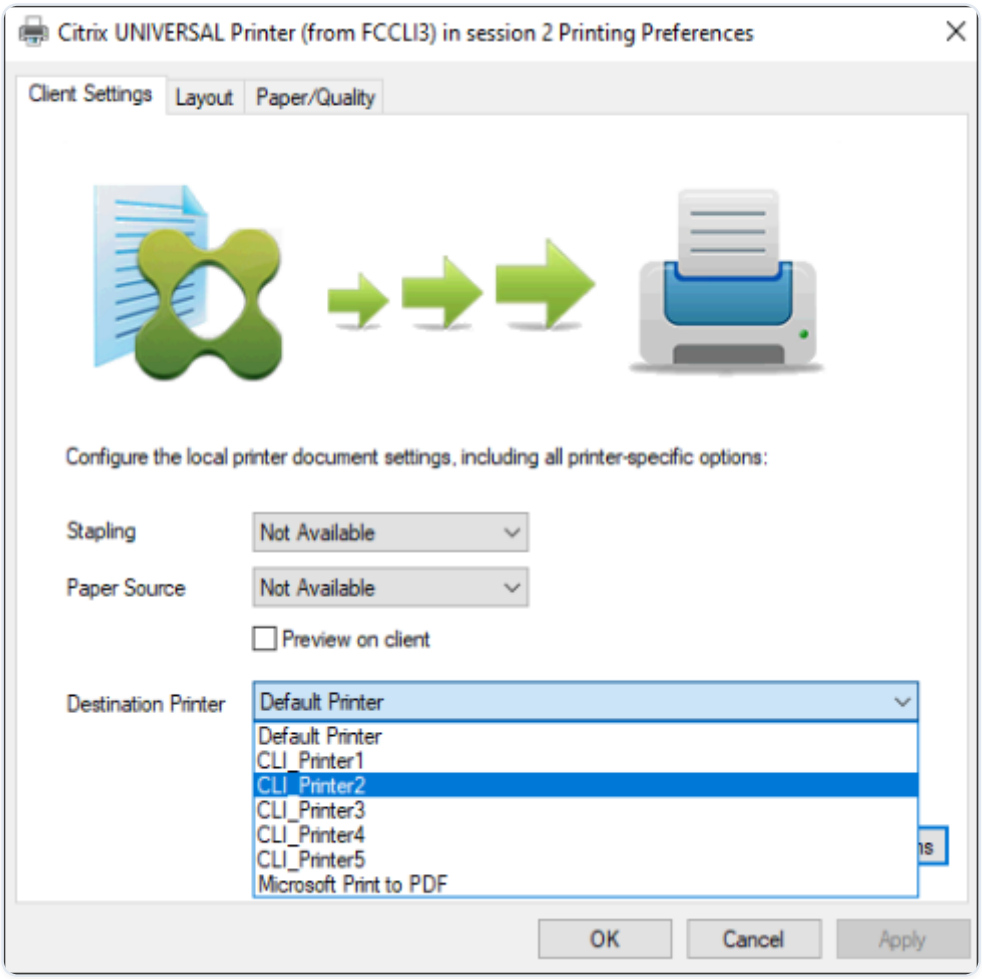
クライアントプリンターには、次のユニバーサル印刷ソリューションが提供されます。

- **Citrix Universal Printer** - セッションの開始時に作成される汎用プリンターで、印刷デバイスに接続されていません。Citrix Universal Printerのみを自動作成して使用すると、リソース使用量が減少し、ユーザーのサインイン時間が短縮される可能性があります。Universal Printerは、任意のクライアント側印刷デバイスに印刷できます。

  Citrix Universal Printerは、お使いの環境のすべてのユーザーデバイスまたはCitrix Workspace™アプリで動作しない場合があります。Citrix Universal PrinterにはWindows環境が必要であり、Citrix Offline Plug-inやクライアントにストリーミングされるアプリケーションはサポートしていません。このような環境では、自動作成されたクライアントプリンターとUniversal print driverの使用を検討してください。

  Windows以外のCitrix Workspaceアプリでユニバーサル印刷ソリューションを使用するには、PostscriptまたはPCLベースの他のUniversal print driverのいずれかを使用します。

  Citrix Universal Printerでは、クライアントのデフォルトプリンターまたは特定のクライアントプリンターを印刷先として選択できます。印刷ジョブの特定のプリンターを選択するには、**［印刷設定］**ダイアログボックスを開きます。**［宛先プリンター］**ドロップダウンを選択します。**［デフォルトプリンター］**オプションは、印刷ジョブをクライアントのデフォルトプリンターに送信します。セッションを実行しているエンドポイントに接続されているクライアントリダイレクトプリンターも一覧表示されます。選択したプリンターは、今後の印刷ジョブの宛先プリンターとして保存されます。



- **Citrix Universal print drivers** - デバイスに依存しないプリンタードライバー。Citrix Universal print driverを構成すると、システムはデフォルトでEMFベースのUniversal print driverを使用します。

  Citrix Universal print driverは、古いまたは高度でないプリンタードライバーよりも小さい印刷ジョブを作成する場合があります。ただし、特殊なプリンターの印刷ジョブを最適化するには、デバイス固有のドライバーが必要になる場合があります。

ユニバーサル印刷の構成 - 次のCitrixポリシー設定を使用して、ユニバーサル印刷を構成します。詳細については、画面上のポリシー設定ヘルプを参照してください。

- Universal print driverの使用。ユニバーサル印刷を使用するタイミングを指定します。
- 汎用ユニバーサルプリンターの自動作成。ユニバーサル印刷と互換性のあるユーザーデバイスが使用されている場合に、セッション用の汎用Citrix Universal Printerオブジェクトの自動作成を有効または無効にします。デフォルトでは、汎用Universal Printerオブジェクトは自動作成されません。
- ユニバーサルドライバーの優先順位。システムがユニバーサルプリントドライバーを使用しようとする順序を、リストの最初のエントリから指定します。ドライバーの追加、編集、削除、およびリスト内のドライバーの順序変更が可能です。

- ユニバーサル印刷プレビューの優先順位。自動作成されたプリンターまたは汎用ユニバーサルプリンターに対して、印刷プレビュー機能を使用するかどうかを指定します。
- ユニバーサル印刷EMF処理モード。Windowsユーザーデバイス上のEMFスプールファイルの処理方法を制御します。デフォルトでは、EMFレコードはプリンターに直接スプールされます。プリンターに直接スプールすることで、スプーラーはレコードをより速く処理でき、CPUリソースの使用量も少なくなります。

その他のポリシーについては、「印刷パフォーマンスの最適化」を参照してください。用紙サイズ、印刷品質、色、両面印刷、部数などの設定のデフォルトを変更するには、「CTX113148」を参照してください。

ユーザーデバイスからプリンターを自動作成 - セッションの開始時に、システムはデフォルトですべてのユーザーデバイス上のプリンターを自動作成します。ユーザーにプロビジョニングされるプリンターの種類（もしあれば）を制御し、自動作成を防止できます。

Citrixポリシー設定 「クライアントプリンターの自動作成」を使用して、自動作成を制御します。以下を指定できます。

- ネットワークプリンターおよびローカル接続プリンターを含む、ユーザーデバイスから見えるすべてのプリンターが、各セッションの開始時に自動的に作成される（デフォルト）
- ユーザーデバイスに物理的に接続されているすべてのローカルプリンターが自動的に作成される
- ユーザーデバイスのデフォルトプリンターのみが自動的に作成される
- すべてのクライアントプリンターで自動作成が無効になる

「クライアントプリンターの自動作成」設定には、「クライアントプリンターのリダイレクト」設定が「許可」（デフォルト）である必要があります。

ユーザーにネットワークプリンターを割り当てる

デフォルトでは、ユーザーデバイス上のネットワークプリンターはセッションの開始時に自動的に作成されます。システムでは、各セッション内で作成するネットワークプリンターを指定することで、列挙およびマップされるネットワークプリンターの数を減らすことができます。このようなプリンターはセッションプリンターと呼ばれます。

IPアドレスでセッションプリンターポリシーをフィルター処理して、近接印刷を提供できます。近接印刷により、指定されたIPアドレス範囲内のユーザーは、同じ範囲内に存在するネットワーク印刷デバイスに自動的にアクセスできます。近接印刷はCitrix Universal Print Serverによって提供され、このセクションで説明されている構成は必要ありません。

近接印刷には、次のシナリオが考えられます。

- 会社の内部ネットワークは、ユーザーにIPアドレスを自動的に割り当てるDHCPサーバーで運用されています。
- 社内のすべての部署には、一意に割り当てられたIPアドレス範囲があります。
- ネットワークプリンターは、各部署のIPアドレス範囲内に存在します。

近接印刷が構成されており、従業員がある部署から別の部署に移動した場合、追加の印刷デバイス構成は不要です。ユーザーデバイスが新しい部署のIPアドレス範囲内で認識されると、その範囲内のすべてのネットワークプリンターにアクセスできるようになります。

セッションでリダイレクトする特定のプリンターを構成する - 管理者割り当てプリンターを作成するには、Citrixポリシー設定の「セッションプリンター」を構成します。次のいずれかの方法を使用して、そのポリシーにネットワークプリンターを追加します。

- `\\servername\printername`の形式を使用して、プリンターのUNCパスを入力します。
- ネットワーク上のプリンターの場所を参照します。
- 特定のサーバー上のプリンターを参照します。`\\servername`の形式を使用してサーバー名を入力し、「参照」をクリックします。

重要：サーバーは、適用されているすべてのポリシーの有効なセッションプリンター設定を、優先度の高いものから低いものの順にマージします。プリンターが複数のポリシーオブジェクトで構成されている場合、カスタムのデフォルト設定は、そのプリンターが構成されている最も優先度の高いポリシーオブジェクトからのみ取得されます。

「セッションプリンター」設定で作成されたネットワークプリンターは、サブネットなどのオブジェクトでフィルタリングすることにより、セッションが開始された場所に応じて異なる場合があります。

セッションのデフォルトネットワークプリンターを指定する - デフォルトでは、ユーザーのメインプリンターがセッションのデフォルトプリンターとして使用されます。Citrixポリシー設定の「デフォルトプリンター」を使用して、セッションでユーザーデバイスのデフォルトプリンターがどのように確立されるかを変更します。

1. 「デフォルトプリンター設定」ページで、「クライアントのデフォルトプリンターを選択」の設定を選択します。
    - ネットワークプリンター名。「セッションプリンター」ポリシー設定で追加されたプリンターがこのメニューに表示されます。このポリシーのデフォルトとして使用するネットワークプリンターを選択します。

- ユーザーのデフォルトプリンターを調整しない。デフォルトプリンターには、現在のターミナルサービスまたはWindowsユーザープロファイル設定を使用します。詳細については、画面上のポリシー設定ヘルプを参照してください。

2. 影響を与えたいユーザーグループ（またはその他のフィルターされたオブジェクト）にポリシーを適用します。

近接印刷を構成する - 近接印刷はCitrix Universal Print Serverによっても提供され、ここで説明する構成は必要ありません。

1. 各サブネット（またはプリンターの場所に対応する）に個別のポリシーを作成します。
2. 各ポリシーで、そのサブネットの地理的な場所にあるプリンターをセッションプリンター設定に追加します。
3. デフォルトプリンター設定を「ユーザーのデフォルトプリンターを調整しない」に設定します。
4. クライアントIPアドレスでポリシーをフィルターします。DHCP IPアドレス範囲の変更を反映するように、これらのポリシーを必ず更新してください。

印刷環境の維持

印刷環境の維持には、以下が含まれます。

- プリンタードライバーの管理
- 印刷パフォーマンスの最適化
- プリンターの表示と印刷キューの管理

プリンタードライバーの管理

管理オーバーヘッドとプリンタードライバーの問題の可能性を最小限に抑えるため、Citrix は Citrix Universal™ プリンタードライバーの使用を推奨します。

自動作成が失敗した場合、デフォルトでは、システムは Windows に付属の Windows ネイティブプリンタードライバーをインストールします。ドライバーが利用できない場合、システムはユニバーサルプリンタードライバーにフォールバックします。プリンタードライバーのデフォルトの詳細については、「ベストプラクティス、セキュリティに関する考慮事項、およびデフォルトの操作」を参照してください。

Citrix Universal プリンタードライバーがすべてのシナリオで選択肢とならない場合は、プリンタードライバーをマップして、マルチセッション OS マシンにインストールされるドライバーの

数を最小限に抑えます。さらに、プリンタードライバーをマップすると、次のことが可能になります。

- 指定されたプリンターが Citrix Universal プリンタードライバーのみを使用できるようにする
- 指定されたドライバーでプリンターが作成されることを許可または防止する
- 古いドライバーや破損したドライバーを適切なプリンタードライバーに置き換える
- クライアントドライバー名に対して、Windows サーバーで利用可能なドライバーを代用する

プリンタードライバーの自動インストールを防止する - マルチセッション OS マシン全体で一貫性を確保するために、プリンタードライバーの自動インストールは無効にする必要があります。これは、Citrix® ポリシー、Microsoft ポリシー、またはその両方を通じて実現できます。Windows ネイティブプリンタードライバーの自動インストールを防止するには、Citrix ポリシー設定の「インボックスプリンタードライバーの自動インストール」を無効にします。

クライアントプリンタードライバーをマップする - 各クライアントは、ログオン時にプリンタードライバー名を含むクライアント側プリンターに関する情報を提供します。クライアントプリンターの自動作成中に、クライアントから提供されたプリンターモデル名に対応する Windows サーバープリンタードライバー名が選択されます。その後、自動作成プロセスは、識別された利用可能なプリンタードライバーを使用して、リダイレクトされたクライアント印刷キューを構築します。

ドライバー置換ルールを定義し、マップされたクライアントプリンタードライバーの印刷設定を編集するための一般的なプロセスは次のとおりです。

1. 自動作成されたクライアントプリンターのドライバー置換ルールを指定するには、Citrixポリシー設定「Printer driver mapping and compatibility」を構成し、クライアントプリンタードライバー名を追加して、「Find printer driver」メニューからクライアントプリンタードライバーの代わりに置換するサーバードライバーを選択します。この設定ではワイルドカードを使用できます。たとえば、すべてのHPプリンターに特定のドライバーを使用させるには、ポリシー設定で「HP*」を指定します。
2. プリンタードライバーを禁止するには、ドライバー名を選択し、「Do not create」設定を選択します。
3. 必要に応じて、既存のマッピングを編集したり、マッピングを削除したり、リスト内のドライバーエントリの順序を変更したりします。
4. マップされたクライアントプリンタードライバーの印刷設定を編集するには、プリンタードライバーを選択し、「Settings」をクリックして、印刷品質、向き、色などの設定を指定します。プリンタードライバーがサポートしていない印刷オプションを指定した場合、そのオプションは無効になります。この設定は、ユーザーが以前のセッションで設定した保持されているプリンター設定を上書きします。

5. 一部のプリンター機能は特定のドライバーでのみ利用可能であるため、Citrixではドライバーをマッピングした後、プリンターの動作を詳細にテストすることをお勧めします。

ユーザーがログオンすると、システムはクライアントプリンターを設定する前に、クライアントプリンタードライバーの互換性リストをチェックします。

印刷パフォーマンスの最適化

印刷パフォーマンスを最適化するには、Universal Print ServerとUniversal Print Driverを使用します。以下のポリシーは、印刷の最適化と圧縮を制御します。

- Universal printing optimization defaults。セッション用にUniversal Printerが作成される際のデフォルト設定を指定します。
  - 希望する画質は、ユニバーサル印刷に適用されるデフォルトの画像圧縮制限を指定します。デフォルトでは、標準品質が有効になっており、ユーザーは標準または低品質の圧縮を使用してのみ画像を印刷できます。
  - ヘビーウェイト圧縮を有効にするは、希望する画質で設定された圧縮レベルを超えて帯域幅を削減するかどうかを有効または無効にします。画質は低下しません。デフォルトでは、ヘビーウェイト圧縮は無効になっています。
  - Image and Font Caching settingsは、印刷ストリームに複数回出現する画像とフォントをキャッシュするかどうかを指定し、各固有の画像またはフォントがプリンターに一度だけ送信されるようにします。デフォルトでは、埋め込み画像とフォントはキャッシュされます。
  - Allow non-administrators to modify these settingsは、ユーザーがセッション内でデフォルトの印刷最適化設定を変更できるかどうかを指定します。デフォルトでは、ユーザーはデフォルトの印刷最適化設定を変更できません。
- Universal printing image compression limit。Universal Print Driverで印刷される画像の最大品質と最小圧縮レベルを定義します。デフォルトでは、画像圧縮制限は「Best Quality」（ロスレス圧縮）に設定されています。
- ユニバーサル印刷の印刷品質制限。セッションで印刷出力を生成するために利用可能な最大ドット/インチ (dpi) を指定します。デフォルトでは、制限は指定されていません。

デフォルトでは、ネットワークプリンター宛てのすべての印刷ジョブは、マルチセッションOSマシンからネットワーク経由で直接プリントサーバーにルーティングされます。ネットワークの遅延が大きい場合や帯域幅が限られている場合は、ICA®接続経由で印刷ジョブをルーティングすることを検討してください。そのためには、Citrixポリシー設定「Direct connections to print servers」

を無効にします。ICA接続経由で送信されるデータは圧縮されるため、WANを介してデータが移動する際の帯域幅消費が少なくなります。

印刷帯域幅を制限してセッションパフォーマンスを向上させる - Multi-session OSマシンからユーザープリンターにファイルを印刷する際、特にユーザーが低速ネットワーク経由でサーバーにアクセスする場合、帯域幅の競合により、他の仮想チャネル（ビデオなど）のパフォーマンスが低下する可能性があります。このような劣化を防ぐため、ユーザー印刷で使用される帯域幅を制限できます。印刷のデータ転送速度を制限することで、HDX™データストリームでビデオ、キーストローク、マウスデータの転送により多くの帯域幅を利用できるようになります。

> **重要:**
>
> プリンターの帯域幅制限は、他のチャネルが使用されていない場合でも常に適用されます。

> 印刷帯域幅のセッション制限を構成するには、以下のCitrixポリシーの帯域幅プリンター設定を使用します。サイトの制限を設定するには、Studioを使用してこのタスクを実行します。個々のサーバーの制限を設定するには、各Multi-session OSマシンでローカルにグループポリシー管理コンソールを使用してこのタスクを実行します。

- 「プリンターリダイレクト帯域幅制限」設定は、印刷に利用できる帯域幅をキロビット/秒（kbps）で指定します。
- 「プリンターリダイレクト帯域幅制限（パーセント）」設定は、印刷に利用できる帯域幅を、利用可能な全体帯域幅の割合に制限します。

  注：「プリンターリダイレクト帯域幅制限（パーセント）」設定を使用して帯域幅をパーセンテージで指定するには、「セッション全体の帯域幅制限」も有効にする必要があります。

  両方の設定に値を入力した場合、最も制限の厳しい設定（小さい方の値）が適用されます。

印刷帯域幅に関するリアルタイム情報を取得するには、Citrix Directorを使用します。

ユニバーサルプリントサーバーの負荷分散

ユニバーサルプリントサーバーソリューションは、負荷分散ソリューションにプリントサーバーを追加することで拡張できます。各VDAには、印刷負荷をすべてのプリントサーバーに分散するための独自のロードバランサーがあるため、単一障害点はありません。

ポリシー設定のUniversal Print Servers for load balancingとUniversal Print Servers out-of-service thresholdを使用して、負荷分散ソリューション内のすべてのプリントサーバーに印刷負荷を分散します。

プリントサーバーに予期せぬ障害が発生した場合、各VDAのロードバランサーのフェイルオーバーメカニズムは、障害が発生したプリントサーバーに割り当てられていたプリンター接続を、他の利用可能なプリントサーバーに自動的に再分散します。これにより、既存および新規のすべてのセッションがユーザーエクスペリエンスに影響を与えることなく、また管理者の即時介入を必要とせずに正常に機能します。

管理者は、一連のパフォーマンスカウンターを使用して、VDA上の負荷分散されたプリントサーバーのアクティビティを監視し、以下を追跡できます。

- VDA上の負荷分散されたプリントサーバーのリストとその状態（利用可能、利用不可）
- 各プリントサーバーが受け入れたプリンター接続の数
- 各プリントサーバーで失敗したプリンター接続の数
- 各プリントサーバーでのアクティブなプリンター接続の数
- 各プリントサーバーでの保留中のプリンター接続の数

印刷キューの表示と管理

次の表は、環境内でプリンターを表示し、印刷キューを管理できる場所をまとめたものです。

	印刷経路	場所
クライアントプリンター (ユーザーデバイスに接続されたプリンター)	クライアント印刷経路	UAC有効時: Microsoft Management Console にある印刷の管理スナップイン; UAC無効時: Windows 8 以前: コントロールパネル, Windows 8: 印刷の管理スナップイン
ネットワークプリンター (ネットワークプリントサーバー上のプリンター)	ネットワーク印刷経路	UAC有効時: プリントサーバー \> Microsoft Management Console にある印刷の管理スナップイン; UAC無効時: プリントサーバー \> コントロールパネル

	印刷経路	場所
ネットワークプリンター (ネットワークプリントサーバー上のプリンター)	クライアント印刷経路	UAC有効時: プリントサーバー \> Microsoft Management Console にある印刷の管理スナップイン; UAC無効時: Windows 8 以前: コントロールパネル, Windows 8: 印刷の管理スナップイン
ローカルネットワークサーバープリンター（マルチセッションOSマシンに追加されたネットワークプリントサーバーからのプリンター）	ネットワーク印刷経路	UAC有効時: プリントサーバー \> コントロールパネル; UAC無効時: プリントサーバー \> コントロールパネル

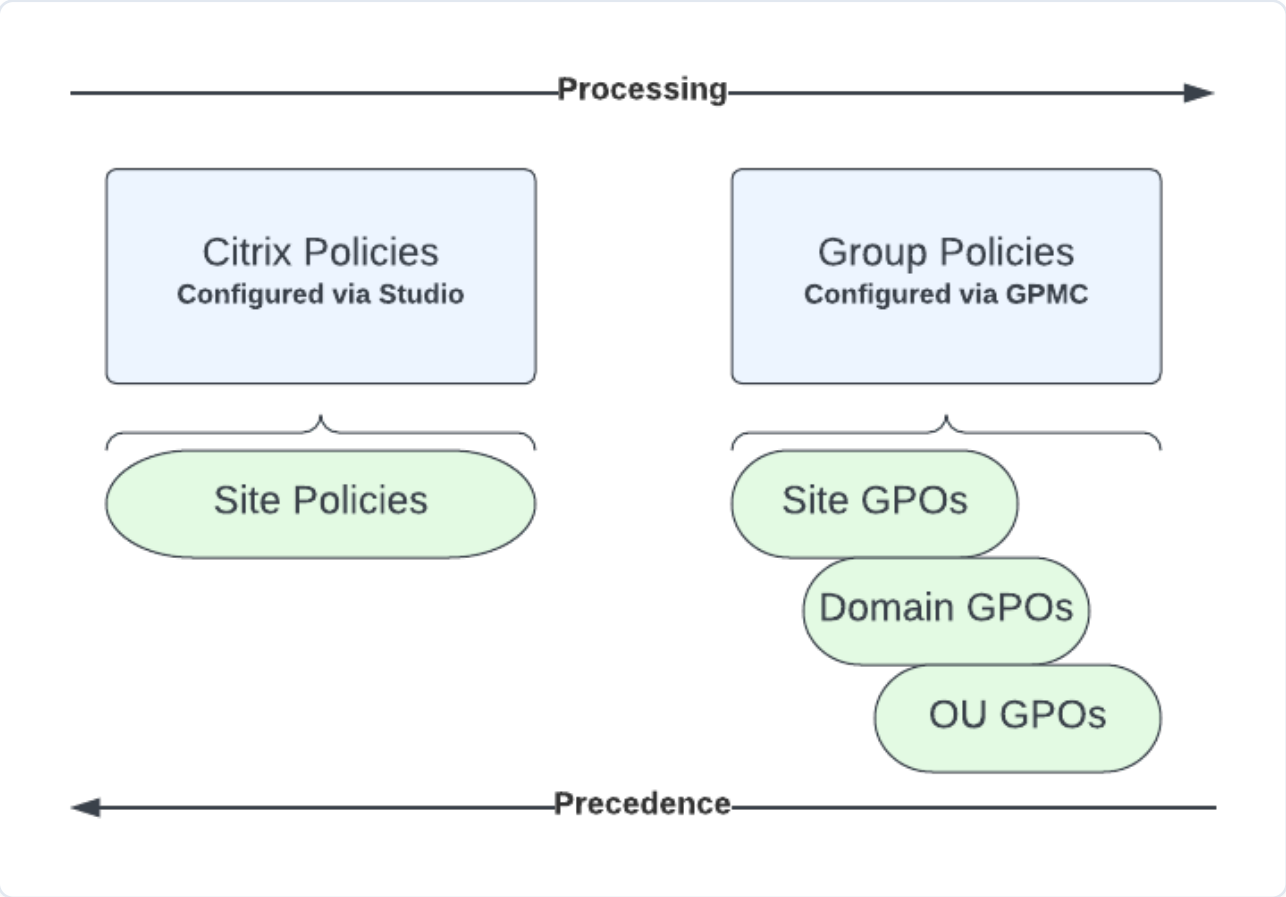
注：

ネットワーク印刷経路を使用するネットワークプリンターの印刷キューはプライベートであり、システムを通じて管理することはできません。

ポリシー

ポリシーは、ユーザー、デバイス、または接続タイプのグループに対して、セッション、帯域幅、およびセキュリティがどのように管理されるかを定義する設定の集合です。

ポリシー設定は、物理マシンおよび仮想マシン、またはユーザーに適用できます。設定は、ローカルレベルの個々のユーザー、またはActive Directoryのセキュリティグループに適用できます。構成は特定の基準とルールを定義します。ポリシーを明示的に割り当てない場合、設定はすべての接続に適用されます。



ポリシーはネットワークのさまざまなレベルに適用できます。組織単位GPOレベルに配置されたポリシー設定は、ネットワーク上で最も高い優先順位を持ちます。ドメインGPOレベルのポリシーは、サイトグループポリシーオブジェクトレベルのポリシーを上書きします。サイトグループポリシーオブジェクトレベルは、MicrosoftおよびCitrixローカルポリシーレベルの両方における競合するポリシーを上書きします。

すべてのCitrixローカルポリシーは、Web Studioコンソールで作成および管理され、サイトデータベースに保存されます。グループポリシーは、Microsoftグループポリシー管理コンソール（GPMC）を使用して作成および管理され、Active Directoryに保存されます。Microsoftローカルポリシーは、Windowsオペレーティングシステムで作成され、レジストリに保存されます。

Studioは、モデリングウィザードを使用して、管理者がテンプレートとポリシー内の構成設定を比較し、競合する設定や冗長な設定を排除するのに役立ちます。管理者はGPMCを使用してGPOを設定し、設定を構成できます。また、それらをネットワークのさまざまなレベルのターゲットユーザーセットに適用することもできます。

これらのGPOはActive Directoryに保存されます。これらの設定の管理へのアクセスは、セキュリティ上の理由からほとんどのIT担当者に対して制限されています。

設定は、優先順位とその条件に従ってマージされます。無効な設定は、下位の有効な設定を上書きします。未構成のポリシー設定は無視され、下位の設定を上書きしません。

ローカルポリシーは、Active Directory内のグループポリシーと競合することもあり、状況によっては互いに上書きし合う可能性があります。

すべてのポリシーは次の順序で処理されます。

1. エンドユーザーはドメイン資格情報を使用してマシンにログオンします。
2. 資格情報はドメインコントローラーに送信されます。
3. Active Directoryはすべてのポリシー（エンドユーザー、エンドポイント、組織単位、およびドメイン）を適用します。
4. エンドユーザーはCitrix Workspace™アプリにログオンし、アプリケーションまたはデスクトップにアクセスします。
5. CitrixおよびMicrosoftのポリシーは、エンドユーザーとリソースをホストするマシンに対して処理されます。
6. Active Directoryはポリシー設定の優先順位を決定します。その後、それらをエンドポイントデバイスのレジストリと、リソースをホストするマシンに適用します。
7. エンドユーザーがリソースからログオフします。エンドユーザーおよびエンドポイントデバイスに対するCitrixポリシーは、アクティブではなくなります。
8. エンドユーザーがユーザーデバイスからログオフすると、GPOユーザーポリシーが解放されます。
9. エンドユーザーがデバイスの電源を切ると、GPOマシンポリシーが解放されます。

ユーザー、デバイス、マシンのグループに対してポリシーを作成する場合、一部のメンバーは異なる要件を持つ可能性があり、一部のポリシー設定に例外が必要になる場合があります。例外は、ポリシーが誰または何に影響するかを決定するStudioおよびGPMCのフィルターによって作成されます。

> **注：**
>
> 同じGPO内でWindowsポリシーとCitrixポリシーを混在させることはサポートされていません。

ポリシーの操作

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

ユーザーアクセスとセッション環境を制御するためにCitrixポリシーを構成します。Citrixポリシーは、接続、セキュリティ、および帯域幅の設定を制御する最も効率的な方法です。特定のユーザーグループ、デバイス、または接続タイプに対してポリシーを作成できます。各ポリシーには複数の設定を含めることができます。

Citrixポリシーを操作するためのツール

Citrixポリシーでは、以下のツールを使用できます。

- **Web Studio。** グループポリシーを管理する権限がないCitrix管理者である場合は、Web Studioを使用してサイトのポリシーを作成します。Web Studioを使用して作成されたポリシーはサイトデータベースに保存され、更新はVDAがブローカーに登録されたとき、またはユーザーがそのVDAに接続したときにVDAにプッシュされます。
- **ローカルグループポリシーエディター** (Microsoft Management Consoleスナップイン)。ネットワーク環境でActive Directoryを使用しており、グループポリシーを管理する権限がある場合は、ローカルグループポリシーエディターを使用してサイトのポリシーを作成できます。構成

する設定は、グループポリシー管理コンソールで指定するグループポリシーオブジェクト (GPO) に影響します。

> **重要:**
>
> 一部のポリシー設定を構成するには、ローカルグループポリシーエディターを使用することをお勧めします。例としては、VDAをコントローラーに登録する設定や、Microsoft App-V サーバーに関連する設定などがあります。 追加のポリシー検証が追加されます。その結果、無効なポリシー設定が存在する場合、インプレースアップグレードを行うとポリシーデータが失われる可能性があります。Web Studio以外の方法でポリシーを作成または編集する場合は、最新バージョンのSDKとスナップインを使用することをCitrixは推奨します。

ポリシーの処理順序と優先順位

グループポリシー設定は、次の順序で処理されます。

1. ローカルGPO
2. Virtual Apps and DesktopsサイトGPO (サイトデータベースに保存)
3. サイトレベルのGPO
4. ドメインレベルのGPO
5. 組織単位

ただし、競合が発生した場合、最後に処理されたポリシー設定が以前に処理された設定を上書きします。ポリシー設定の優先順位は次のとおりです。

1. 組織単位
2. ドメインレベルのGPO
3. サイトレベルのGPO
4. Virtual Apps and Desktops サイト GPO (サイトデータベースに保存)
5. ローカル GPO

例えば、Citrix管理者はWeb Studioを使用して、会社の営業担当者向けにクライアントファイルリダイレクトを有効にするポリシー（ポリシーA）を作成します。一方、別の管理者はグループポリシーエディターを使用して、営業担当者向けにクライアントファイルリダイレクトを無効にするポリシー（ポリシーB）を作成します。営業担当者が仮想デスクトップにログオンすると、ポリシー

Bが適用され、ポリシーAは無視されます。その理由は、ポリシーBがドメインレベルで処理され、ポリシーAがVirtual Apps and DesktopsサイトGPOレベルで処理されたためです。

ただし、ユーザーがICA®またはリモートデスクトッププロトコル（RDP）セッションを起動すると、Citrixセッション設定は、Active Directoryポリシーまたはリモートデスクトップセッションホスト構成を使用して構成された同じ設定を上書きします。この設定には、一般的なRDPクライアント接続設定に関連する設定が含まれます。RDPクライアント接続設定の例としては、デスクトップの壁紙、メニューアニメーション、ドラッグ中のウィンドウコンテンツの表示などがあります。

複数のポリシーを使用する場合、競合する設定を含むポリシーに優先順位を付けることができます。詳細については、「ポリシーの比較、優先順位付け、モデル化、およびトラブルシューティング」を参照してください。

Citrixポリシーのワークフロー

ポリシーを構成するプロセスは次のとおりです。

1. ポリシーを作成します。
2. ポリシー設定を構成します。
3. ポリシーをマシンオブジェクトとユーザーオブジェクトに割り当てます。
4. ポリシーに優先順位を付けます。
5. Citrixグループポリシーモデリングウィザードを実行して、有効なポリシーを確認します。

> **注：**
>
> Citrixグループポリシーモデリングウィザードを開くには、**ポリシー > モデリング**タブに移動し、アクションバーで**モデリングウィザードの起動**をクリックします。**モデリング**タブは、お客様の要望に応じてWeb Studioで利用できます。

Citrixポリシーと設定のナビゲート

ローカルグループポリシーエディターでは、ポリシーと設定は「コンピューターの構成」と「ユーザーの構成」の2つのカテゴリに表示されます。各カテゴリにはCitrixポリシーノードがあります。このスナップインのナビゲートと使用方法の詳細については、Microsoftのドキュメントを参照してください。

Web Studioでは、ポリシー設定は、影響を与える機能または特徴に基づいてカテゴリに分類されます。例えば、**プロファイル管理**セクションには、プロファイル管理のポリシー設定が含まれています。

- コンピューター設定（マシンに適用されるポリシー設定）は、仮想デスクトップの動作を定義し、仮想デスクトップの起動時に適用されます。これらの設定は、仮想デスクトップでアクティブなユーザーセッションがない場合でも適用されます。
- ユーザー設定は、ICAを使用して接続する際のユーザーエクスペリエンスを定義します。ユーザーポリシーは、ユーザーがICAを使用して接続または再接続するときに適用されます。ユーザーがRDPを使用して接続したり、コンソールに直接ログオンしたりする場合は、ユーザーポリシーは適用されません。

  ポリシー、設定、またはテンプレートにアクセスするには、Web Studioの左ペインで を選択します。

  - タブには、すべてのポリシーが一覧表示されます。ポリシーを選択すると、下部に次のタブが表示されます。
    - 概要 - 名前、優先度、有効/無効の状態、および説明を一覧表示します
    - 設定 - 構成されているすべての設定を一覧表示します
    - 割り当て先 - ポリシーが割り当てられているユーザーおよびマシンオブジェクトを一覧表示します。 詳しくは、「ポリシーの作成」を参照してください。
  - タブには、Citrixが提供するテンプレートと、作成したカスタムテンプレートが一覧表示されます。テンプレートを選択すると、下部に次のタブが表示されます。
    - 説明（テンプレートを使用する理由）
    - 設定（構成された設定のリスト）。詳しくは、「ポリシーテンプレート」を参照してください。
  - タブでは、ポリシーまたはテンプレートの設定を、他のポリシーまたはテンプレートの設定と比較できます。たとえば、ベストプラクティスへの準拠を確実にするために、設定値を検証したい場合があります。詳しくは、「ポリシーの比較、優先順位付け、モデル化、およびトラブルシューティング」を参照してください。

  ポリシーまたはテンプレートで設定を検索するには：

  a. ポリシーまたはテンプレートを選択します。
  b. アクションバーで または を選択します。
  c. ページで、 フィールドに設定の名前を入力します。

検索を絞り込むには、以下を選択します。

- 特定の製品バージョン
- カテゴリ（例：帯域幅）
- 設定名に含まれるキーワード
- **選択済みのみ表示**チェックボックス
- 選択したポリシーに追加された設定のみを検索する場合。

フィルタリングされていない検索の場合は、**すべての設定**を選択します。

- ポリシー内の設定を検索するには：

a. ポリシーを選択します。

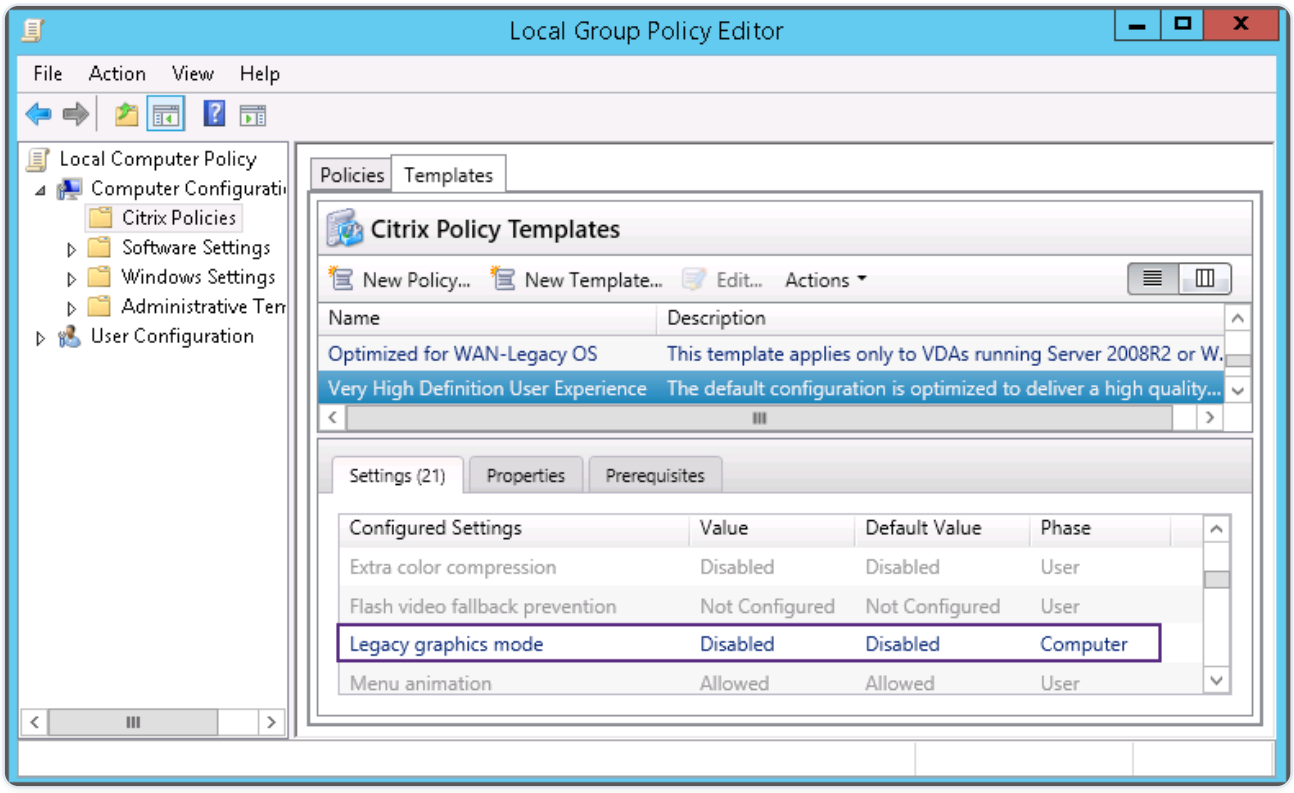
b. **設定**タブを選択し、設定の名前を入力します。

特定の製品バージョンを選択するか、カテゴリを選択して検索を絞り込むことができます。フィルタリングされていない検索の場合は、**すべての設定**を選択します。

ポリシーは、一度作成されると、使用されたテンプレートとは独立します。新しいポリシーの**説明**フィールドを使用して、使用されたソーステンプレートを追跡できます。

グループポリシーエディターでは、コンピューター設定とユーザー設定は、両方の種類の設定を含むテンプレートから作成された場合でも、個別に適用する必要があります。この例では、コンピューターの構成で「非常に高精細なユーザーエクスペリエンス」を使用することを選択しています。

- レガシーグラフィックモードは、このテンプレートから作成されたポリシーで使用されるコンピューター設定です。
- グレー表示されているユーザー設定は、このテンプレートから作成されたポリシーでは使用されません。



ポリシーテンプレート

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

> テンプレートは、特定の目的を達成するためのポリシーを作成する際に推奨される設定のコレクションです。たとえば、エンドユーザーに高精細なユーザーエクスペリエンスを提供するためのポリシーを作成する場合、「非常に高精細なユーザーエクスペリエンス」テンプレートで定義されている設定を、そのようなポリシーを作成するための参照および開始点として使用できます。

テンプレートはポリシーではありません。テンプレートは、Citrixポリシー設定の補足ドキュメントです。これらは、特定のユーザー関連設定の集合的な機能を示します。

テンプレートの使用は任意です。管理者はテンプレートを使用せずにポリシーを作成できます。テンプレートは、サイトをどのように構成すべきかについて大まかなアイデアを持っているものの、目的の構成を達成するためにどの設定を使用すべきか確信が持てない管理者にとって役立ちます。

管理者は、既存のテンプレート、既存のポリシー、またはゼロからテンプレートを作成できます。

ADMX/ADML

ここで説明するCitrixグループポリシーテンプレートは、Windowsポリシーテンプレートとは関係ありません。ここで説明するテンプレートとWindowsポリシーテンプレートは、2つの異なる概念です。CitrixグループポリシーテンプレートはADMXファイルではありません。

組み込みのCitrixテンプレート

以下のポリシーテンプレートが利用可能です。

- **非常に高精細なユーザーエクスペリエンス**。このテンプレートは、ユーザーエクスペリエンスを最大化するデフォルト設定を適用します。複数のポリシーが優先順位に従って処理されるシナリオでこのテンプレートを使用します。
- **高いサーバー拡張性**。このテンプレートを適用して、サーバーリソースを節約します。このテンプレートは、ユーザーエクスペリエンスとサーバーの拡張性のバランスを取ります。優れたユーザーエクスペリエンスを提供しつつ、単一サーバーでホストできるユーザー数を増やします。このテンプレートは、グラフィックの圧縮にビデオコーデックを使用せず、サーバー側のマルチメディアレンダリングを防止します。
- **高いサーバー拡張性 - レガシーOS**。この高いサーバー拡張性テンプレートは、Windows Server 2008 R2またはWindows 7以前を実行しているVDAにのみ適用されます。このテンプレートは、これらのオペレーティングシステムにより効率的なレガシーグラフィックモードに依存しています。
- **NetScaler SD-WANに最適化**。Citrix Virtual Desktopsの配信を最適化するためにNetScaler SD-WANを使用している支社のユーザーにこのテンプレートを適用します。(NetScaler SD-WANはCloudBridgeの新しい名称です)。
- **WAN向けに最適化**。このテンプレートは、共有WAN接続を使用する支社のタスクワーカーや、帯域幅の低いリモートロケーションで、グラフィックがシンプルでマルチメディアコンテンツが少ないユーザーインターフェイスを持つアプリケーションにアクセスする場合を想定しています。このテンプレートは、ビデオ再生エクスペリエンスと一部のサーバー拡張性を犠牲にして、帯域幅効率を最適化します。
- **WAN向けに最適化 - レガシーOS**。この*WAN向けに最適化*テンプレートは、Windows Server 2008 R2またはWindows 7以前を実行しているVDAにのみ適用されます。このテンプレートは、これらのオペレーティングシステムにより効率的なレガシーグラフィックモードに依存しています。
- **セキュリティと制御**。リスク許容度が低い環境でこのテンプレートを使用し、Citrix Virtual Apps and Desktopsでデフォルトで有効になっている機能を最小限に抑えます。このテンプ

レートには、ユーザーデバイスでの印刷、クリップボード、周辺機器、ドライブマッピング、ポートリダイレクト、Flashアクセラレーションへのアクセスを無効にする設定が含まれています。このテンプレートを適用すると、帯域幅が増加し、サーバーあたりのユーザー密度が減少する可能性があります。

組み込みのCitrixテンプレートをデフォルト設定で使用することをお勧めしますが、特定の推奨値がない設定もあります。たとえば、WAN向けに最適化されたテンプレートに含まれる**セッション全体の帯域幅制限**などです。この場合、テンプレートは設定を公開し、管理者がこの設定がシナリオに適用される可能性が高いことを理解できるようにします。

テンプレートのデフォルト設定画像(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/template-default-settings.png)

XenApp and XenDesktop 7.6 FP3より前の展開（ポリシー管理とVDA）を使用しており、High Server ScalabilityおよびOptimized for WANテンプレートが必要な場合は、該当するレガシーOSバージョンのこれらのテンプレートを使用してください。

> **注：**
>
> Citrixは組み込みテンプレートを作成および更新します。これらのテンプレートは変更または削除できません。

Web Studioを使用してテンプレートを作成および管理する

テンプレートに基づいてテンプレートを作成するには：

1. Web Studioにサインインし、左ペインで**ポリシー**を選択します。
2. **テンプレート**タブを選択し、テンプレートを作成する元のテンプレートを選択します。
3. **テンプレートの作成**タブを選択します。**設定の選択**画面が表示されます。
4. テンプレートに含めるポリシー設定を選択して構成します。
5. 「**次へ**」をクリックします。「**概要**」画面が表示されます。
6. テンプレートの名前を入力します。
7. **完了**をクリックします。新しいテンプレートが**テンプレート**タブに表示されます。

ポリシーに基づいてテンプレートを作成するには：

1. Web Studioにサインインし、左ペインで**ポリシー**を選択します。
2. **ポリシー**タブを選択し、テンプレートを作成する元のポリシーを選択します。

3. **その他**タブをクリックします。
4. 「**テンプレートとして保存**」を選択します。「**設定の選択**」画面が表示されます。
5. テンプレートに含める新しいポリシー設定を選択して構成します。
6. 「**次へ**」をクリックします。「**概要**」画面が表示されます。
7. テンプレートの名前と説明を入力し、「**完了**」をクリックします。

テンプレートと委任管理

Web Studioのテンプレートはサイトデータベースに保存されますが、Citrix Studioのテンプレートは、現在の管理者のユーザープロファイルフォルダーに`.gpt`拡張子を持つファイルとして保存されます。ある管理者が作成したCitrix Studioテンプレートは、他の管理者や、別のマシン上の同じ管理者には表示されません。Web Studioテンプレートは、権限と委任管理の対象となるすべての管理者に表示されます。

ポリシーの作成

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

> ポリシーを作成する前に、それが影響を与える可能性のあるユーザーまたはデバイスのグループを決定します。ユーザーの職務、接続タイプ、ユーザーデバイス、または地理的な場所に基づいてポリシーを作成することもできます。Windows Active Directoryグループポリシーで使用するのと同じ基準を使用することもできます。

すでにグループに適用されるポリシーを作成している場合は、別のポリシーを作成するのではなく、そのポリシーを編集することを検討してください。ポリシーを編集した後、適切な設定を構成します。特定の機能を有効にするためだけ、または特定のユーザーにポリシーが適用されないようにするためだけにポリシーを作成することは避けてください。

ポリシーを作成する際、ポリシーテンプレートの設定に基づいて作成し、必要に応じて設定をカスタマイズできます。テンプレートを使用せずに、必要なすべての設定を追加して作成することもできます。

Web Studioでは、**ポリシーを有効にする**チェックボックスが明示的にオンにされていない限り、新しく作成されたポリシーは無効に設定されます。

ポリシー作成時および設定構成時に、システムは設定タイプを表示するオプションを提供します。次の設定タイプを表示できます。

- すべての設定 - すべてのVDAバージョンに適用されるすべての設定を表示
- 現在の設定のみ - 現在のVDAバージョンに固有の設定を表示
- レガシー設定のみ - 非推奨のVDAバージョンにのみ適用される設定を表示

設定を構成しながら設定を表示するには：

1. Web Studioにサインインし、左ペインで**ポリシー**を選択します。
2. **ポリシー**タブで、**ポリシーの作成**をクリックします。
3. **設定の選択**テーブルで、**設定**の横にあるドロップダウンをクリックします。
4. ドロップダウンから次のいずれかのオプションを選択します。

- すべての設定 - すべてのVDAバージョンのすべての設定を表示
- 現在の設定のみ - 現在のVDAバージョンのみの設定を表示します
- レガシー設定のみ - 非推奨のVDAバージョンのみの設定を表示します

1. 「**設定**」テーブルには、前の手順に基づいて利用可能な設定が一覧表示されます。

ポリシー設定

ポリシー設定は、有効、無効、または未構成にできます。デフォルトでは、ポリシー設定は構成されていません。つまり、ポリシーに追加されていません。設定は、ポリシーに追加された場合にのみ適用されます。

一部のポリシー設定は、次のいずれかの状態になります。

- 「許可」または「禁止」は、設定によって制御されるアクションを許可または防止します。セッション内でユーザーが設定のアクションを管理することを許可または防止する場合があります。たとえば、メニューアニメーション設定が「許可」に設定されている場合、ユーザーはクライアント環境でメニューアニメーションを制御できます。
- 「有効」または「無効」は、設定をオンまたはオフにします。設定を無効にすると、下位ランクのポリシーでは有効になりません。

さらに、一部の設定は、依存する設定の有効性を制御します。たとえば、クライアントドライブリダイレクトは、ユーザーがデバイス上のドライブにアクセスできるかどうかを制御します。ユー

ザーがネットワークドライブにアクセスできるようにするには、この設定と「**クライアントネットワークドライブ**」設定の両方をポリシーに追加する必要があります。「**クライアントドライブリダイレクト**」設定が無効になっている場合、「**クライアントネットワークドライブ**」設定が有効になっていても、ユーザーはネットワークドライブにアクセスできません。

一般に、マシンに影響を与えるポリシー設定の変更は、仮想デスクトップが再起動したとき、またはユーザーがログオンしたときに有効になります。ユーザーに影響を与えるポリシー設定の変更は、ユーザーが次回ログオンしたときに有効になります。Active Directoryを使用している場合、ポリシー設定はActive Directoryが90分間隔でポリシーを再評価するときに更新されます。そして、ポリシー設定は、仮想デスクトップが再起動したとき、またはユーザーがログオンしたときに適用されます。

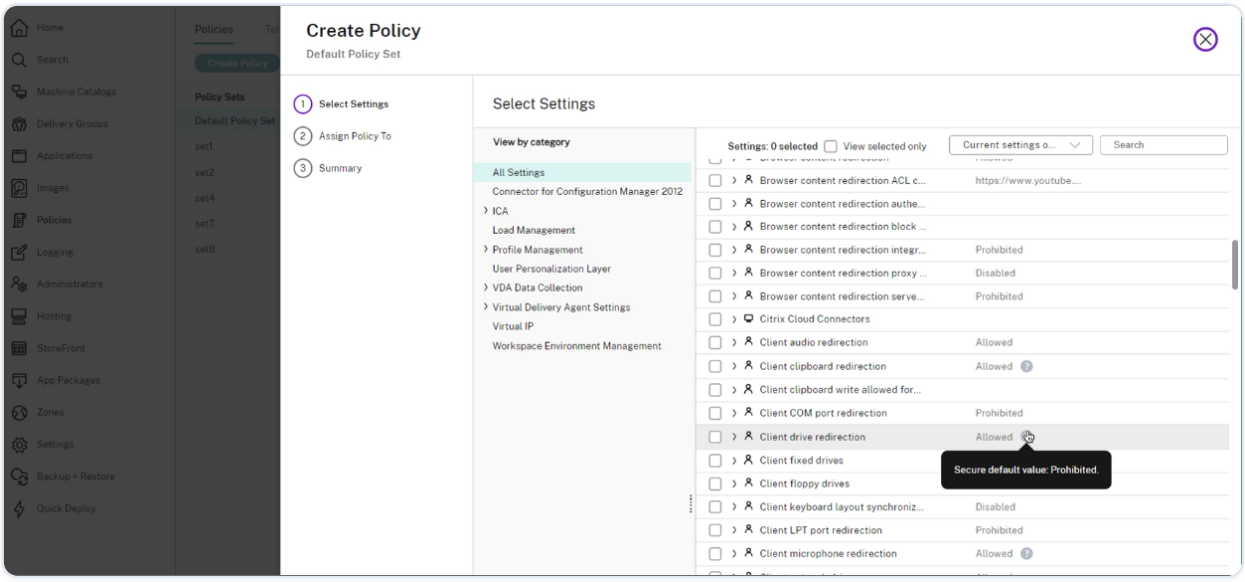
一部のポリシー設定では、設定をポリシーに追加するときに値を入力または選択できます。「デフォルト値を使用」を選択することで、設定の構成を制限できます。この選択により、設定の構成が無効になり、ポリシーが適用されるときに設定のデフォルト値のみが使用されるようになります。この選択は、「デフォルト値を使用」を選択する前に入力された値とは関係ありません。

セキュアデフォルト設定が有効になっている場合、VDAインストール中に、ポリシー設定の優先順位は次のように影響を受けます。

- カスタマイズされた設定が最優先されます
- セキュアなデフォルト設定が2番目の優先順位になります
- デフォルト設定が最も低い優先順位になります

ポリシーのセキュアデフォルト設定を表示するには：

1. Web Studioにログオンします。
2. 左側のナビゲーションで、「**ポリシー**」をクリックします。
3. 「**ポリシー**」タブで、「**ポリシーの作成**」をクリックします。
4. 「**設定の選択**」テーブルで、現在の値が「**許可済み ?**」である設定にマウスカーソルを合わせると、「**セキュリティ保護されたデフォルト値: 禁止**」が表示されます。



ベストプラクティスとして：

- ポリシーは個々のユーザーではなく、グループに割り当ててください。グループにポリシーを割り当てると、グループにユーザーを追加または削除したときに、割り当てが自動的に更新されます。
- リモートデスクトップセッションホスト構成で、競合する設定や重複する設定を有効にしないでください。リモートデスクトップセッションホスト構成は、Citrixポリシー設定と同様の機能を提供することがあります。トラブルシューティングを容易にするため、可能な限りすべての設定を一貫性のある状態（有効または無効）に保ってください。
- 使用されていないポリシーは無効にしてください。設定が追加されていないポリシーは、不要な処理を生成します。

ポリシーの割り当て

ポリシーを作成する際、特定のユーザーおよびマシンオブジェクトに割り当てます。そのポリシーは、特定の基準またはルールに従って接続に適用されます。一般的に、基準の組み合わせに基づいて、ポリシーに好きなだけ割り当てを追加できます。

割り当てを指定しない場合、または割り当てを指定しても無効にする場合、ポリシーは**すべて**の接続に適用されます。

> **注:**
>
> ポリシーの割り当ては、ポリシーフィルターとも呼ばれます。詳細については、以下のトピックを参照してください。

- ポリシーのフィルターを作成、変更、または削除する
- フィルターはどのように適用されますか？

次の表に、利用可能な割り当てを示します。

割り当て名	ポリシーの適用基準
アクセスコントロール	クライアントが接続しているアクセス制御条件。*接続の種類* - NetScaler® Gatewayを使用する接続と使用しない接続のどちらにポリシーを適用するか。*NetScaler Gatewayファーム名* - NetScaler Gateway仮想サーバーの名前。*アクセス条件* - 使用するエンドポイント分析ポリシーまたはセッションポリシーの名前。
NetScaler SD-WAN	ユーザーセッションがNetScaler SD-WANを介して起動されるかどうか。**注:** 1つのポリシーにNetScaler SD-WANの割り当てを1つだけ追加できます。
クライアントIPアドレス	セッションへの接続に使用されるユーザーデバイスのIPアドレス: IPv4の例: 12.0.0.0, 12.0.0.*, 12.0.0.1-12.0.0.70, 12.0.0.1/24; IPv6の例: 2001:0db8:3c4d:0015:0:0:abcd:ef12, 2001:0db8:3c4d:0015::/54
クライアント名	ユーザーデバイスの名前。完全一致: ClientABCName。ワイルドカードの使用: Client*Name。
デリバリーグループ	デリバリーグループのメンバーシップ。
デリバリーグループの種類	デスクトップまたはアプリケーションの種類: プライベートデスクトップ、共有デスクトップ、プライベートアプリケーション、または共有アプリケーション。**注:** プライベートデスクトップと共有デスクトップのフィルターオプションは、Citrix Virtual Apps and Desktops 7.xでのみ利用可能です。詳細については、CTX219153を参照してください。

割り当て名	ポリシーの適用基準
組織単位 (OU)	組織単位。
タグ	タグ。**注:** このポリシーをすべてのタグ付きマシンに適用します。アプリケーションタグは含まれません。
ユーザーまたはグループ	ユーザーまたはグループ名。

ユーザーがログオンすると、接続の割り当てに一致するすべてのポリシーが特定されます。これらのポリシーは優先順位順に並べ替えられ、設定の複数のインスタンスが比較されます。各設定は、ポリシーの優先順位に従って適用されます。無効になっているポリシー設定は、有効になっている下位ランクの設定よりも優先されます。構成されていないポリシー設定は無視されます。

重要:

Group Policy Management Console を使用して Active Directory ポリシーと Citrix ポリシーの両方を構成する場合、割り当てと設定が期待どおりに適用されないことがあります。詳細については、CTX127461を参照してください。

「Unfiltered」という名前のポリシーがデフォルトで提供されます。

- Web Studio を使用して Citrix ポリシーを管理する場合、Unfiltered ポリシーに追加した設定は、サイト内のすべてのサーバー、デスクトップ、および接続に適用されます。
- ローカルグループポリシーエディターを使用して Citrix ポリシーを管理する場合、Unfiltered ポリシーに追加した設定は、すべてのサイトと接続に適用されます。サイトと接続は、ポリシーを含むグループポリシーオブジェクト (GPO) のスコープ内にある必要があります。たとえば、Sales OU には、米国の営業チームのすべてのメンバーを含む Sales-US という GPO が含まれています。Sales-US GPO は、いくつかのユーザーポリシー設定を含む Unfiltered ポリシーで構成されています。米国の営業マネージャーがサイトにログオンすると、Unfiltered ポリシーの設定がセッションに自動的に適用されます。この構成は、ユーザーが Sales-US GPO のメンバーであるためです。

割り当てのモードは、ポリシーがすべての割り当て基準に一致する接続にのみ適用されるかどうかを決定します。モードが (デフォルト) に設定されている場合、ポリシーは割り当て基準に一致する接続にのみ適用されます。モードが に設定されている場合、接続が割り当て基準に一致しな

い場合にポリシーが適用されます。以下の例は、複数の割り当てが存在する場合に割り当てモードが Citrix ポリシーにどのように影響するかを示しています。

- **例: モードが異なる同種の割り当て** - 同じ種類の2つの割り当てがあり、一方が に設定され、もう一方が に設定されているポリシーでは、接続が両方の割り当てを満たす場合、 に設定された割り当てが優先されます。例:

  ポリシー 1 には次の割り当てが含まれます。

  - 割り当て A は Sales グループを指定します。モードは に設定されています。
  - 割り当て B は営業マネージャーのアカウントを指定します。モードは に設定されています。

  割り当て B のモードが に設定されているため、ユーザーが Sales グループのメンバーであっても、営業マネージャーがサイトにログオンしたときにポリシーは適用されません。

- **例: モードが同じでタイプが異なる割り当て** - タイプが異なる2つ以上の割り当てがあり、 に設定されているポリシーでは、ポリシーが適用されるためには、接続が各タイプの少なくとも1つの割り当てを満たす必要があります。例:

  ポリシー 2 には次の割り当てが含まれます。

  - 割り当て C は、Sales グループを指定するユーザー割り当てです。モードは に設定されています。
  - 割り当て D は、10.8.169.* (企業ネットワーク) を指定するクライアント IP アドレス割り当てです。モードは に設定されています。

  営業マネージャーがオフィスからサイトにログオンすると、接続が両方の割り当てを満たすため、ポリシーが適用されます。

  ポリシー3には、次の割り当てが含まれます。

  - 割り当てEは、営業グループを指定するユーザー割り当てです。モードは「許可」に設定されています。
  - 割り当てFは、NetScaler Gatewayの接続条件を指定するアクセスコントロール割り当てです。モードは「許可」に設定されています。

  営業マネージャーがオフィスからサイトにログオンしても、接続が割り当てFを満たさないため、ポリシーは適用されません。

Web Studioを使用して、テンプレートに基づいてポリシーを作成する

1. Web Studioにサインインし、左側のペインで**［ポリシー］**を選択します。
2. **［テンプレート］**タブを選択し、テンプレートを選択します。
3. アクションバーで**［テンプレートからポリシーを作成］**を選択します。
4. デフォルトでは、新しいポリシーはテンプレートのすべてのデフォルト設定を使用します。この場合、**［テンプレートのデフォルト設定（推奨）］が選択されています。設定を変更する場合は、**［デフォルト設定を変更して追加］**を選択し、設定を追加または削除します。
5. 次のいずれかを選択して、ポリシーの適用方法を指定します。

   - **［選択したユーザーおよびマシンオブジェクト］**。選択したユーザーおよびマシンオブジェクトにポリシーを適用するには、**［割り当て］**をクリックして、ポリシーを適用するユーザーおよびマシンオブジェクトを選択します。
   - **［サイト内のすべてのオブジェクト］**。サイト内のすべてのユーザーおよびマシンオブジェクトにポリシーを適用します。

6. ポリシーの名前を入力します。ポリシーが影響する対象（例：経理部、リモートユーザーなど）に基づいてポリシーに名前を付けることを検討してください。必要に応じて、説明を追加します。

   ポリシーはデフォルトで無効になっています。有効にすることができます。ポリシーを有効にすると、ログオンするユーザーにすぐに適用されます。無効にすると、ポリシーは適用されません。ポリシーの優先順位を付けたり、後で設定を追加したりする必要がある場合は、適用する準備ができるまでポリシーを無効にしておくことを検討してください。

Web Studioを使用してポリシーを作成する

1. Web Studioにサインインし、左ペインで**ポリシー**を選択します。
2. **ポリシー**タブを選択します。
3. アクションバーで**ポリシーの作成**を選択します。
4. ポリシー設定を追加および構成します。
5. 次のいずれかを選択して、ポリシーを適用する方法を指定します。

   - 選択したユーザーオブジェクトとマシンオブジェクトに割り当て、ポリシーを適用する必要があるユーザーオブジェクトとマシンオブジェクトを選択します。
   - サイト内のすべてのオブジェクトに割り当てて、サイト内のすべてのユーザーオブジェクトとマシンオブジェクトにポリシーを適用します。

6. ポリシーの名前を入力するか、デフォルトを受け入れます。ポリシーが影響する対象（例: 経理部、リモートユーザーなど）に基づいてポリシーに名前を付けることを検討してください。必要に応じて、説明を追加します。

   ポリシーはデフォルトで有効になっていますが、無効にすることもできます。ポリシーを有効にすると、ログオンするユーザーにすぐに適用されます。無効にすると、ポリシーは適用されません。ポリシーの優先順位を付けたり、後で設定を追加したりする必要がある場合は、適用する準備ができるまでポリシーを無効にしておくことを検討してください。

グループポリシーエディターを使用してポリシーを作成および管理する

グループポリシーエディターで、**コンピューターの構成**または**ユーザーの構成**を展開します。**ポリシー**ノードを展開し、**Citrixポリシー**を選択します。適切なアクションを選択します。

タスク	手順
ポリシーを作成する	**ポリシー**タブで、**新規**をクリックします。
既存のポリシーを編集する	**ポリシー**タブで、ポリシーを選択し、**編集**をクリックします。
既存のポリシーの優先度を変更する	**ポリシー**タブでポリシーを選択し、**上位**または**下位**をクリックします。
ポリシーの概要情報を表示する	**ポリシー**タブでポリシーを選択し、**概要**タブをクリックします。
ポリシー設定を表示および修正する	**ポリシー**タブでポリシーを選択し、**設定**タブをクリックします。
ポリシーフィルターを表示および修正する	**ポリシー**タブでポリシーを選択し、**フィルター**タブをクリックします。ポリシーに複数のフィルターを追加する場合、ポリシーが適用されるには、すべてのフィルター条件が満たされている必要があります。
ポリシーを有効または無効にする	**ポリシー**タブでポリシーを選択し、**アクション > 有効**または**アクション > 無効**を選択します。
既存のテンプレートからポリシーを作成する	**テンプレート**タブでテンプレートを選択し、**新しいポリシー**をクリックします。

ポリシーセット

ポリシーセットは、Citrix Virtual Apps and Desktops™ のオブジェクトであり、ポリシーを集約して、簡素化されたロールベースのアクセスと容易な管理を可能にします。管理者チームや会社の論理的な区分を反映するようにポリシーセットを作成できます。たとえば、地理的な地域ごと、事業部門ごと、または特定のユースケースごとにポリシーセットを作成できます。作成後、スコープとデリバリーグループがポリシーセットに割り当てられ、承認された管理者のみが関連するユーザーとマシンに適用されるポリシーを管理できるようになります。

注：

ポリシーセットを有効にする前に、Citrix® は以下の点に注意することを推奨します。

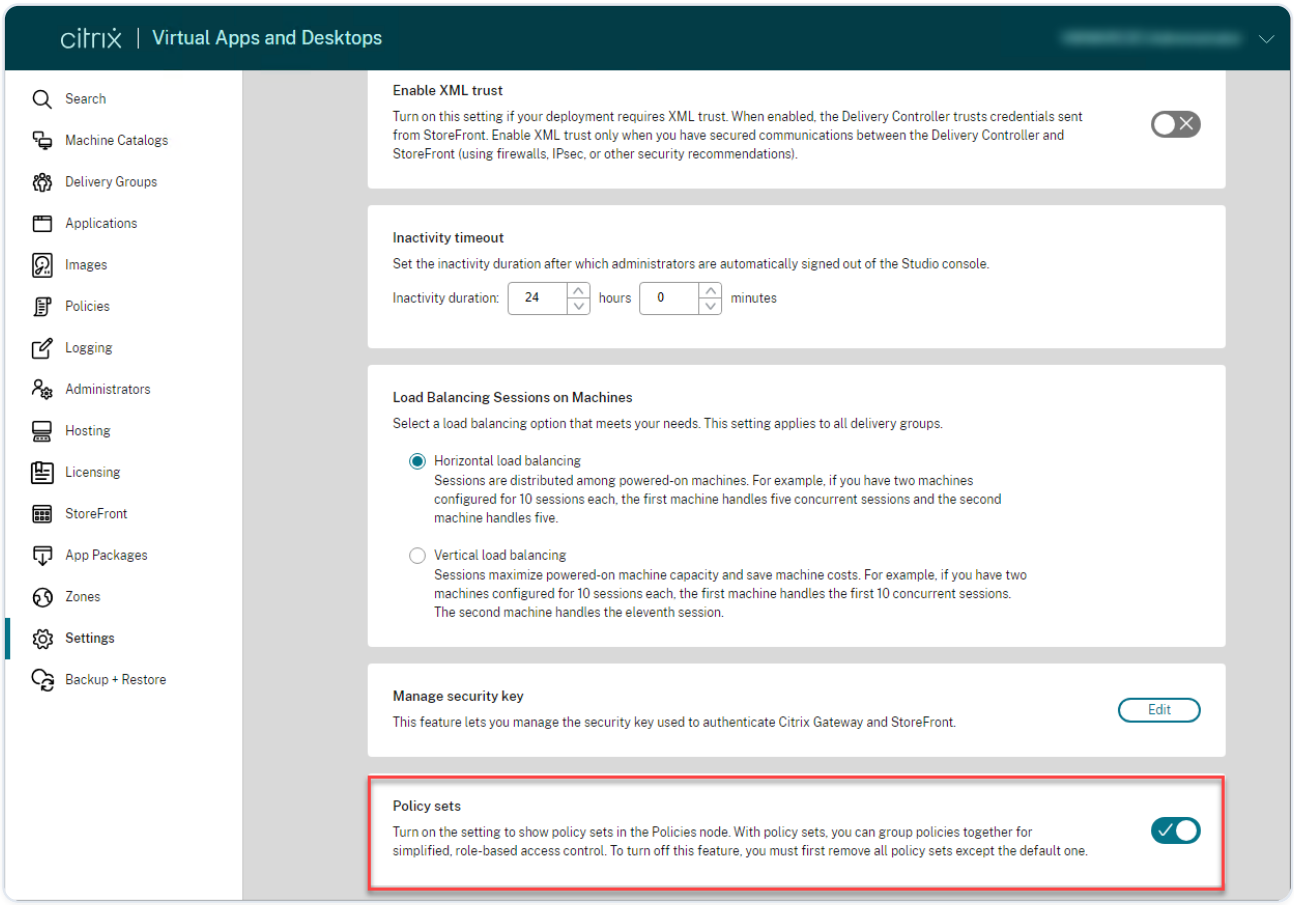
- 追加のポリシー検証が追加されます。その結果、無効なポリシー設定が存在する場合、インプレースアップグレードを行うとポリシーデータが失われる可能性があります。
- 無効なデータを検出するには、GPOスキャナーツール を使用し、アップグレードする前に必要な編集を行ってください。詳細については、CTX676686 を参照してください。
- 今後のすべてのアップグレードでは、Citrix は最新のSDKを使用することを推奨します。古いSDKを使用してポリシーを更新すると、無効なデータがポリシー設定に追加される可能性があり、ポリシーデータが失われるリスクにつながる可能性があります。

利点

- 分散型管理者チーム向けのロールベースのアクセス制御
- 合併、買収、および統合の簡素化
- 制限された障害ドメイン
- ポリシーのマルチテナントサポート

ポリシーセットを有効にする

Virtual Apps and Desktops の ［**管理**］ タブから、 ［**設定**］ に移動し、 ［**ポリシーセット**］ 設定をオンにします。



> **注：**
>
> ポリシーセットを作成する前に、ポリシーセットを有効にする必要があります。

機能の比較

ポリシーセット適用前	ポリシーセット適用後
サイト全体のポリシー、設定、フィルター、およびポリシーの優先順位は、Citrix Studio 内の1か所で構成されます。	ポリシー、設定、フィルター、およびポリシーの優先順位は、各ポリシーセットで個別に構成されます。
1つのポリシーを管理する場合、すべてのポリシーを管理する必要があります。	フル管理者は、特定のポリシーセットを個別に管理する機能を下位レベルの管理者に委任できます。
大規模で分散された環境のポリシーは、複雑になり管理が困難になります。	大規模で分散された環境のポリシーは、簡単に分割して管理できます。

ポリシーセットの仕組み?

概要

- ポリシーセットはデリバリーグループに割り当てられます
- ポリシーセットには、1つまたは複数のスコープがあります。
- ポリシーセットが割り当てられていないデリバリーグループは、デフォルトのポリシーセットを受け取ります。
- デリバリーグループには、1つのポリシーセットのみを割り当てることができます。
- 複数のデリバリーグループで同じポリシーセットを使用できます。
- ポリシーセットがデリバリーグループに割り当てられていても、ポリシーはフィルターを維持します。

詳細については、「フィルターはどのように適用されますか？」を参照してください。ポリシーセットのポリシー割り当てまたはポリシーフィルターの動作方法に変更はありません。つまり、ポリシーの場合と同じように機能します。

デフォルトのポリシーセット

- ポリシーセット設定がオンの場合、既存のすべてのポリシーはデフォルトのポリシーセット内にグループ化されます。
- 管理者チームがポリシーセットを作成してデリバリーグループに割り当てない限り、すべてのデリバリーグループはデフォルトのポリシーセットを受け取ります。
- デリバリーグループに別のポリシーセットが割り当てられると、デフォルトのポリシーセットからポリシーを受け取らなくなります。

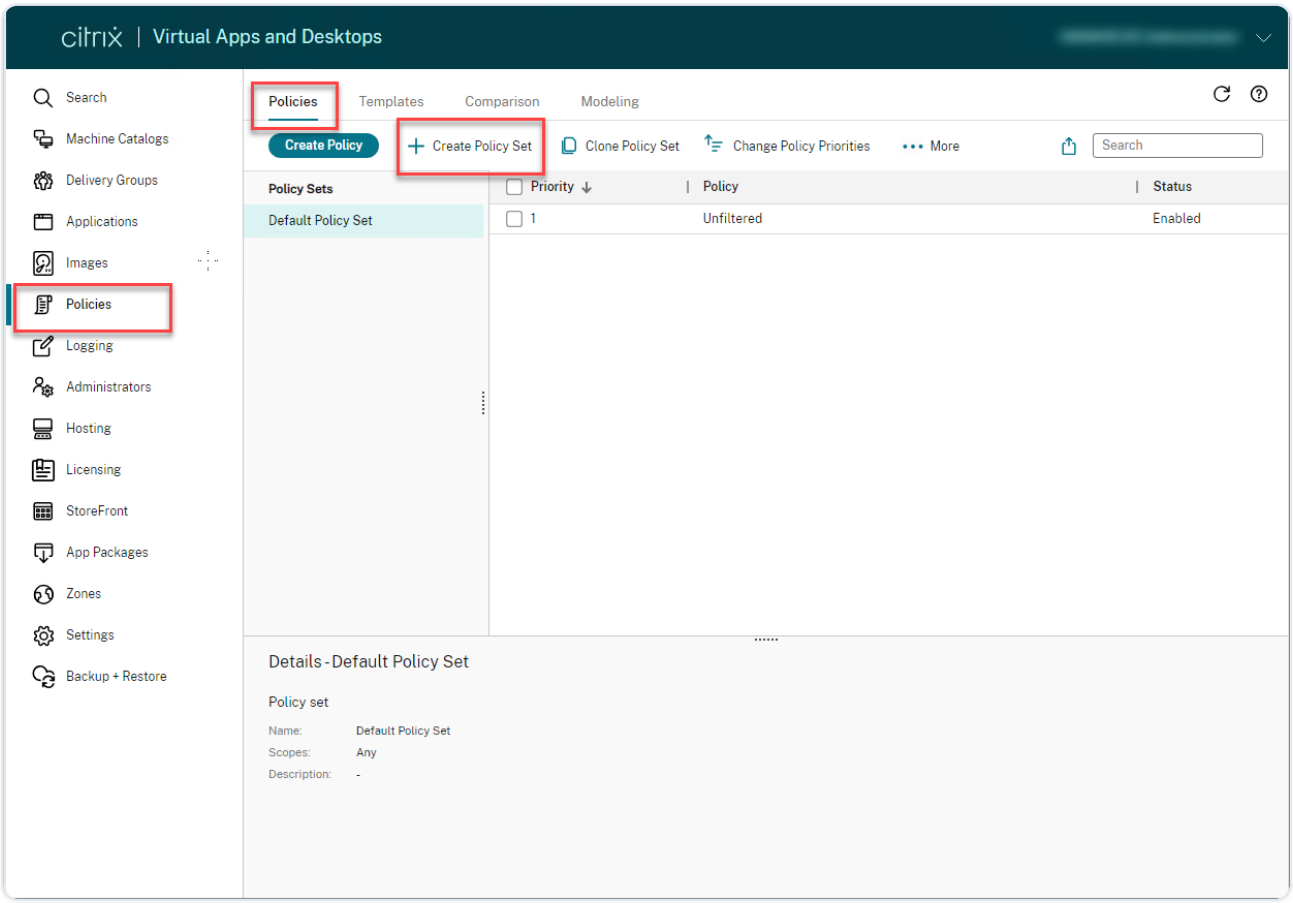
ポリシーセットの作成

ポリシーセットは、次の2つの方法で作成できます。

- ポリシーセットの作成 - このアクションにより、空のポリシーセットが作成されます。
- ポリシーセットのクローン作成 - このアクションにより、既存のポリシーセットに基づいてポリシーセットが作成されます。

ポリシーセットの作成

1. Web Studioにサインインし、左ペインで**ポリシー**を選択します。



1. 「**ポリシーセットの作成**」を選択します。「**はじめに**」タブが表示されます。
2. 「**次へ**」をクリックするか、「**名前と説明**」タブをクリックします。
3. ポリシーセットの名前と説明を入力します。
4. 「**次へ**」をクリックするか、「**割り当て**」タブをクリックします。
5. ポリシーセットを割り当てるデリバリーグループを1つ以上選択します。
6. 「**次へ**」をクリックするか、「**スコープ**」タブをクリックします。
7. ポリシーセットのスコープを選択します。
8. 「**作成**」をクリックします。定義された割り当てとスコープでポリシーセットが作成されます。

ポリシーセットの複製

1. Web Studioにサインインし、左ペインで**ポリシー**を選択します。
2. 「**ポリシーセットの複製**」を選択します。
3. ポリシーセットの名前を変更します。
4. ポリシーセットの割り当てを変更または作成し、「**次へ**」をクリックします。
5. クローンされたポリシーセットに含めるポリシーを選択または選択解除します。

6. ポリシーのスコープを変更します。
7. 「**作成**」をクリックします。ポリシーセットが作成されます。

ポリシーセットの編集

1. Web Studioにサインインし、左ペインで**ポリシー**を選択します。
2. 「**ポリシーセットの編集**」を選択します。
3. ポリシーセットの名前を変更し、**次へ**をクリックします。
4. ポリシーセットの割り当てを変更または作成し、**次へ**をクリックします。
5. ポリシーのスコープを変更します。
6. **Create** をクリックします。

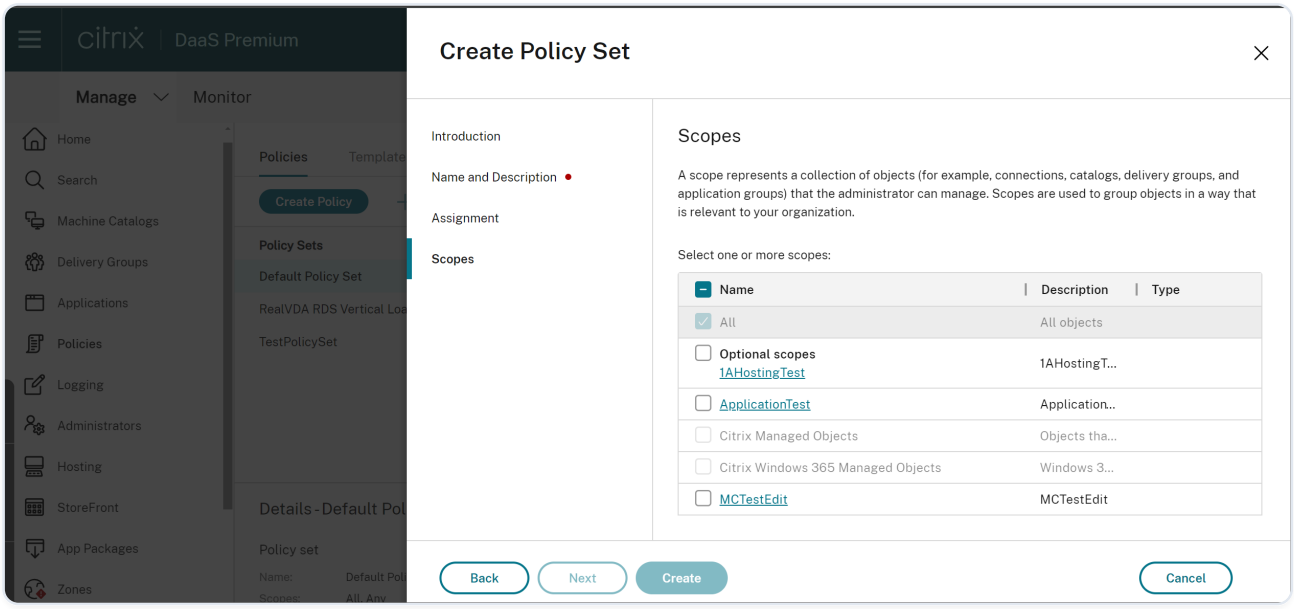
ポリシーセットの割り当て

ポリシーセットはデリバリーグループに割り当てられます。ポリシーセットの作成時または編集時に割り当てを構成できます。デリバリーグループの作成時または編集時にも割り当てを構成できます。

ポリシーセットのスコープ

管理者は、承認された管理者のみがポリシーセットを表示または編集できるように、ポリシーセットのスコープを定義できます。ポリシーセットの作成時または編集時にスコープを構成できます。

ポリシーセットの導入により、API を使用して Citrix Policy を作成および管理することもできます。詳しくは、「Citrix DaaS でポリシーセットを作成する方法」を参照してください。



ポリシーの比較、優先順位付け、トラブルシューティング

注：

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

複数のポリシーを使用して、ユーザーの職務、地理的な場所、または接続の種類に基づいて、ユーザーのニーズに合わせて環境をカスタマイズできます。たとえば、セキュリティを強化するために、機密データを定期的に扱うユーザーグループに制限を設けることができます。

また、ユーザーが機密ファイルをローカルクライアントドライブに保存できないようにするポリシーを作成することもできます。ただし、ユーザーグループ内の一部のユーザーがローカルドライブへのアクセスを必要とする場合は、それらのユーザー専用の別のポリシーを作成できます。その後、どちらが優先されるかを制御するために、2つのポリシーをランク付けまたは優先順位付けします。複数のポリシーを使用する場合、次のことを決定する必要があります。

- ポリシーの優先順位付け方法
- 例外の作成方法
- ポリシーが競合する場合に有効なポリシーを表示する方法。

一般に、ポリシーは、サイト全体、特定のDelivery Controller、またはユーザーデバイス用に構成された同様の設定を上書きします。この原則の例外はセキュリティです。環境内で最も高い暗号化設定は、常に他の設定やポリシーを上書きします。最も高い暗号化設定には、オペレーティングシステムと最も制限の厳しいシャドウイング設定が含まれます。

Citrixポリシーは、オペレーティングシステムで設定したポリシーと相互作用します。Citrix環境では、Citrix設定は、Active Directoryポリシーで構成された、またはリモートデスクトップセッションホスト構成を使用して構成された同じ設定を上書きします。この設定には、一般的なリモートデスクトッププロトコル（RDP）クライアント接続設定に関連する設定が含まれます。一般的なRDP設定には、デスクトップの壁紙、メニューアニメーション、ドラッグ中のウィンドウコンテンツの表示などの設定が含まれます。

Secure ICA®などの一部のポリシー設定は、オペレーティングシステムの設定と一致している必要があります。より高い優先順位の暗号化レベルが別の場所で設定されている場合、ポリシーで指定した、またはアプリケーションとデスクトップを配信するときに指定した**Secure ICAポリシー**設定は上書きされる可能性があります。

たとえば、デリバリーグループを作成するときに指定する暗号化設定は、環境全体で指定した暗号化設定と同じレベルである必要があります。

> **注：**
>
> ダブルホップシナリオの2番目のホップでは、シングルセッションOS VDAがマルチセッションOS VDAに接続することを考慮してください。この場合、Citrixポリシーは、シングルセッションOS VDAをユーザーデバイスであるかのように扱います。たとえば、ポリシーがユーザーデバイスに画像をキャッシュするように設定されているとします。この例では、ダブルホップシナリオの2番目のホップ用にキャッシュされた画像は、シングルセッションOS VDAマシンにキャッシュされます。

ポリシーモデリングウィザードを使用する

ポリシーモデリングは、計画およびテスト目的で、フィルターが適用された有効なポリシーをシミュレートするのに役立ちます。フィルターが適用された有効なポリシーのみがモデル化されます。無効なポリシーは適用されず、フィルターが適用されていない有効なポリシーは常に適用されます。

ポリシーモデリングウィザードを開くには、次の手順を実行します。

1. 左側のナビゲーションから**ポリシー**を選択します。
2. 「**モデリング**」タブを選択します。
3. アクションバーで「**ポリシーモデリング**」を選択します。
4. 「**はじめに**」ページを読み、「**次へ**」をクリックします。
5. ユーザーまたはコンピューターを選択します。コンテナーまたは特定のユーザーやコンピューターを参照できます。**次へ**をクリックします。
6. フィルターの証拠を選択します。必要に応じて、**デリバリーグループ**、**タグ**、**クライアントIPアドレス**などの詳細情報を入力して、シミュレーションをより詳細にすることもできます。**次へ**をクリックします。
7. 選択内容の概要を確認し、**実行**をクリックします。

実行をクリックすると、ウィザードはモデリング結果のレポートを生成します。このレポートを表示している間、次のことができます。

- ドロップダウンメニューで、**すべての設定**、**コンピューター設定**、または**ユーザー設定**のいずれを表示するかを選択します。
- 検索バーを使用して、特定の設定を検索します。
- 特定の設定をクリックして、その設定の詳細を表示します。たとえば、特定のポリシーに対してすべてのユーザー設定が適用されなかった場合、**詳細**ペインには設定が適用されなかった理由が表示されます。
- モデリング結果をJSON形式、HTML形式、またはその両方でエクスポートするには、**エクスポート**をクリックします。

ポリシーモデリングを実行すると、さらに多くのオプションが利用可能になります。次のことができます。

- **モデリングレポートの表示**：これにより、上記のモデリングレポートが開き、再度表示したりエクスポートしたりできます。
- **ポリシーモデリングの再実行**：これにより、以前に選択したのと同じ基準セットでポリシーモデリングを再実行し、新しいモデリング結果を生成できます。これは、一部のポリシーが変更され、それらの変更が現在のモデルにどのように影響するかを確認したい場合に役立ちます。
- **モデリングレポートの削除**：現在のモデリングレポートを削除します。

ポリシーとテンプレートの比較

ポリシーまたはテンプレートの設定を、他のポリシーまたはテンプレートの設定と比較できます。たとえば、ベストプラクティスへの準拠を維持するために、設定値を確認する必要がある場合があります。また、ポリシーまたはテンプレートの設定を、Citrixが提供するデフォルト設定と比較することもできます。

1. Web Studioにサインインし、左ペインで**ポリシー**を選択します。
2. **比較**タブをクリックし、**選択**をクリックします。
3. 比較するポリシーまたはテンプレートを選択します。比較にデフォルト値を含めるには、**デフォルト設定と比較**チェックボックスをオンにします。
4. **比較**をクリックすると、構成された設定が列に表示されます。
5. すべての設定を表示するには、「**すべての設定を表示**」を選択します。デフォルトビューに戻るには、「**共通設定を表示**」を選択します。

ポリシーの優先順位付け

ポリシーに競合する設定が含まれている場合、ポリシーの優先順位を付けることで、その優先順位を定義できます。ユーザーがログオンすると、接続の割り当てに一致するすべてのポリシーが識別されます。これらのポリシーは優先順位順に並べ替えられ、任意の設定の複数のインスタンスが比較されます。各設定は、ポリシーの優先順位に従って適用されます。

ポリシーには異なる優先順位番号を付与することで、優先順位を付けます。デフォルトでは、新しいポリシーには最も低い優先順位が与えられます。ポリシー設定が競合する場合、優先順位が高いポリシー（優先順位番号1が最も高い）が、優先順位が低いポリシーを上書きします。設定は、優先順位と設定の条件に従ってマージされます。たとえば、設定が無効になっているか有効になっているかなどです。無効になっている設定は、有効になっている下位ランクの設定を上書きします。構成されていないポリシー設定は無視され、下位ランクの設定を上書きしません。

1. 左側のペインで「**ポリシー**」を選択します。「**ポリシー**」タブが選択されていることを確認してください。
2. 「**ポリシー**」タブで、アクションバーの「**ポリシーの優先順位を変更**」を選択します。「**ポリシーの優先順位を変更**」ページが表示されます。
3. 優先順位リストで、ポリシーの優先順位を変更するには、次のいずれかの方法を使用します。
    - ポリシーを目的の位置にドラッグします。
    - 1つ上または下に移動するには、それぞれ上または下矢印アイコンをクリックします。
    - リストの先頭または末尾に移動するには、それぞれ先頭または末尾矢印アイコンをクリックします。
    - 優先順位番号を変更するには、「**編集**」アイコンをクリックし、必要に応じて番号を入力し、「**保存**」をクリックします。
4. 「**保存**」をクリックします。

例外

ユーザー、ユーザーデバイス、またはマシンのグループに対してポリシーを作成する場合、グループの一部のメンバーが特定のポリシー設定の例外を必要とすることがあります。例外を作成するには、次の方法があります。

- 例外を必要とするグループメンバーのみにポリシーを作成し、そのポリシーをグループ全体のポリシーよりも上位にランク付けする
- ポリシーに追加された割り当てに拒否モードを使用する

モードが「拒否」に設定された割り当ては、割り当て条件に一致しない接続にのみポリシーを適用します。たとえば、ポリシーには次の割り当てが含まれます。

- 割り当てAは、範囲208.77.88.*を指定するクライアントIPアドレス割り当てです。モードは「許可」に設定されています。
- 割り当て B は、特定のユーザーアカウントを指定するユーザー割り当てです。モードは拒否に設定されています。

このポリシーは、割り当て A で指定された範囲の IP アドレスを使用してサイトにログオンするすべてのユーザーに適用されます。ただし、割り当て B で指定されたユーザーアカウントを使用してサイトにログオンするユーザーには適用されません。

接続に適用されるポリシーを決定する

複数のポリシーが適用されるため、接続が期待どおりに応答しない場合があります。優先度の高いポリシーが接続に適用される場合、元のポリシーで構成した設定が上書きされる可能性があります。ポリシーの結果セットを計算し、接続に対して最終的なポリシー設定がどのようにマージされるかを判断できます。

ポリシーの結果セットは、次の方法で計算できます。

- **Citrix Group Policy Modeling** ウィザードを使用して、接続シナリオをシミュレートし、Citrix ポリシーがどのように適用されるかを把握します。接続シナリオの条件として、次のようなものを指定できます。
  - ドメインコントローラー
  - ユーザー
  - Citrix ポリシー割り当ての証拠値
  - 低速ネットワーク接続などのシミュレートされた環境設定 ウィザードが生成するレポートには、シナリオで有効になる Citrix ポリシーが一覧表示されます。ドメインユーザーとしてコントローラーにログオンするため、ウィザードはサイトポリシー設定と Active Directory グループポリシーオブジェクト (GPO) の両方を使用して結果を計算します。
- **グループポリシーの結果**を使用して、特定のユーザーとコントローラーに有効な Citrix ポリシーを記述したレポートを作成します。グループポリシーの結果ツールは、環境内の GPO の現在の状態を評価し、レポートを生成するのに役立ちます。生成されたレポートには、Citrix ポリシーを含むこれらのオブジェクトが、特定のユーザーとコントローラーに現在どのように適用されているかが記述されています。

Citrix Group Policy Modeling ウィザードは Web Studio で起動できます。または、Windows のグループポリシー管理コンソールからグループポリシーの結果ツールを起動することもできます。

Web Studio を使用して作成されたサイトポリシー設定は、次の場合、ポリシーの結果セットに含まれません。

- グループポリシー管理コンソールから Citrix Group Policy Modeling ウィザードを実行する場合
- グループポリシー管理コンソールからグループポリシーの結果ツールを実行する場合

最も包括的なポリシーの結果セットが得られることを確認するには、グループポリシー管理コンソールのみを使用してポリシーを作成する場合を除き、Web Studio から Citrix Group Policy Modeling ウィザードを起動することをお勧めします。

ポリシーのトラブルシューティング

ユーザー、IPアドレス、およびその他の割り当てられたオブジェクトには、複数のポリシーが同時に適用される場合があります。このシナリオでは、ポリシーが期待どおりに動作しない競合が発生する可能性があります。Citrixグループポリシーモデリングウィザードまたはグループポリシー結果ツールを実行すると、ユーザー接続にポリシーが適用されていないことが判明する場合があります。このようなシナリオでは、ポリシー評価基準に一致する条件下でアプリケーションやデスクトップに接続するユーザーには、ポリシー設定が適用されません。この状況は、次の場合に発生します。

- ポリシー評価基準に一致する割り当てを持つポリシーがない場合。
- 割り当てに一致するポリシーに設定が構成されていない場合。
- 割り当てに一致するポリシーが無効になっている。

指定された基準を満たす接続にポリシー設定を適用する場合は、次のことを確認してください。

- それらの接続に適用したいポリシーが有効になっていること。
- 適用したいポリシーに適切な設定が構成されていること。

デフォルトのポリシー設定

以下の表に、ポリシー設定、そのデフォルト値、およびそれらが適用されるVirtual Delivery Agent (VDA) のバージョンを示します。

ICA®

名前	デフォルト設定	VDA
アダプティブトランスポート	オフ。優先される場合に使用します	VDA 7.13～7.15、VDA 7.16以降
クライアントクリップボードリダイレクト	許可	すべてのVDAバージョン
クライアントクリップボード書き込み許可形式	形式は指定されていません	VDA 7.6 以降
デスクトップの起動	禁止	マルチセッションOS用VDA 7以降
ICAリスナーポート番号	1494	すべてのVDAバージョン
クライアント接続中の非公開プログラムの起動	禁止	マルチセッションOS用VDA 7以降
クリップボードのクライアントからセッションへの転送サイズを制限する	無効	VDA 2009
クリップボードのセッションからクライアントへの転送サイズを制限する	無効	VDA 2009
ロス許容モード	許可	VDA 2003。注: 損失許容モードはまだ利用できません。VDA のこのバージョンは、利用可能になった時点でこれをサポートします。
ロス許容しきい値	損失許容モードが利用可能な場合: パケット損失: 5%、遅延: 300 ms (RTT)	VDA 2003 以降
Rendezvous プロトコル	無効	Citrix Cloud を介して確立された HDX セッションにのみ適用されます。

名前	デフォルト設定	VDA
クライアントクリップボードへの書き込みを制限する	禁止	VDA 7.6 以降
セッションクリップボードへの書き込みを制限する	禁止	VDA 7.6 以降
セッションクリップボード書き込み許可形式	形式は指定されていません	VDA 7.6 以降
タブレットモードの切り替え	有効	VDA 7.16 以降; VDA 7.14 および 7.15 LTSR の場合、この設定はレジストリを使用して構成します。
仮想チャネル許可リスト	有効	VDA 2109 以降

ICA/Adobe Flash 配信/Flash リダイレクト

名前	デフォルト設定	VDA
Flashビデオのフォールバック防止	未構成	VDA 7.6 FP3 から現在まで
Flashビデオのフォールバック防止エラー *.swf	VDA 7.6 FP3 から現在まで	

ICA/オーディオ

名前	デフォルト設定	VDA
アダプティブオーディオ	有効	Citrix Virtual Apps and Desktops™ 2109以降を使用するVDAの、シングルセッションOSおよびマルチセッションOSの両方のセッションに適用されます。
UDPリアルタイムトランスポート経由のオーディオ	許可	すべてのVDAバージョン

名前	デフォルト設定	VDA
オーディオプラグアンドプレイ	許可	マルチセッションOS用VDA 7 から現在まで
オーディオ品質	高 - 高精細オーディオ	すべてのVDAバージョン
クライアントオーディオリダイレクト	許可	すべてのVDAバージョン
クライアントマイクのリダイレクト	許可	すべてのVDAバージョン
オーディオのロストレラントモード	禁止	VDAバージョン2402以降

ICA/自動クライアント再接続

名前	デフォルト設定	VDA
自動クライアント再接続	許可	すべてのVDAバージョン
自動クライアント再接続認証	認証を要求しない	すべてのVDAバージョン
自動クライアント再接続ログ	自動再接続イベントをログに記録しない	すべてのVDAバージョン
自動クライアント再接続タイムアウト	120秒	VDA 7.13 から現在まで
再接続UIの透過レベル	80%	VDA 7.13 から現在まで

ICA/帯域幅

名前	デフォルト設定	VDA
オーディオリダイレクトの帯域幅制限	0 キロビット/秒	すべてのVDAバージョン
オーディオリダイレクトの帯域幅制限（パーセント）	0	すべてのVDAバージョン

名前	デフォルト設定	VDA
クライアントUSBデバイスリダイレクトの帯域幅制限	0 キロビット/秒	VDA 5.5、5.6 FP1、Multi-session OS 用 VDA 7 以降、Single-session OS 用 VDA 7 以降
クライアントUSBデバイスリダイレクトの帯域幅制限（パーセント）	0	VDA 5.5、5.6 FP1、Multi-session OS 用 VDA 7 以降、Single-session OS 用 VDA 7 以降
クリップボードリダイレクトの帯域幅制限	0 キロビット/秒	すべてのVDAバージョン
クリップボードリダイレクトの帯域幅制限（パーセント）	0	すべてのVDAバージョン
COMポートリダイレクトの帯域幅制限	0 キロビット/秒	すべてのVDAバージョン。VDA 7.0から7.8までは、レジストリを使用してこの設定を構成します。
COMポートリダイレクトの帯域幅制限（パーセント）	0	すべてのVDAバージョン。VDA 7.0から7.8までは、レジストリを使用してこの設定を構成します。
ファイルリダイレクト帯域幅制限	0 キロビット/秒	すべてのVDAバージョン
ファイルリダイレクトの帯域幅制限（パーセント）	0	すべてのVDAバージョン
HDX MediaStreamマルチメディアアクセラレーション帯域幅制限	0 キロビット/秒	VDA 5.5、5.6 FP1、Multi-session OS用VDA 7およびSingle-session OS用VDA 7から現在のMulti-session OS用VDAおよびSingle-session OS用VDA

名前	デフォルト設定	VDA
HDX MediaStreamマルチメディアアクセラレーション帯域幅制限パーセント	0	VDA 5.5、5.6 FP1、Multi-session OS 用 VDA 7 以降、Single-session OS 用 VDA 7 以降
LPTポートリダイレクト帯域幅制限	0 キロビット/秒	すべてのVDAバージョン。VDA 7.0から7.8までは、レジストリを使用してこの設定を構成します。
LPTポートリダイレクトの帯域幅制限（パーセント）	0	すべてのVDAバージョン。VDA 7.0から7.8までは、レジストリを使用してこの設定を構成します。
セッション全体の帯域幅制限	0 キロビット/秒	すべてのVDAバージョン
プリンターリダイレクト帯域幅制限	0 キロビット/秒	すべてのVDAバージョン
プリンターリダイレクトの帯域幅制限（パーセント）	0	すべてのVDAバージョン
TWAINデバイスリダイレクト帯域幅制限	0 キロビット/秒	VDA 5.5、5.6 FP1、Multi-session OS 用 VDA 7 以降、Single-session OS 用 VDA 7 以降
TWAINデバイスリダイレクト帯域幅制限の割合	0	VDA 5.5、5.6 FP1、Multi-session OS 用 VDA 7 以降、Single-session OS 用 VDA 7 以降

ICA/双方向コンテンツリダイレクト

名前	デフォルト設定	VDA
双方向コンテンツリダイレクトを許可する	禁止	VDA 7.13 から現在まで

名前	デフォルト設定	VDA
クライアントにリダイレクトを許可するURL	空	VDA 7.13 から現在まで
VDAにリダイレクトされる許可されたURL	空	VDA 7.13 から現在まで
双方向コンテンツリダイレクトの構成	無効	VDA 2311 から現在まで

ICA/ブラウザコンテンツリダイレクト

名前	デフォルト設定	VDA
ブラウザコンテンツリダイレクト	許可	VDA 7.16 から現在まで
ブラウザコンテンツリダイレクトACL構成	`https://www.youtube.com/*`	VDA 7.16 から現在まで
ブラウザコンテンツリダイレクト統合Windows認証のサポート	禁止	VDA 2106 から現在まで
ブラウザコンテンツリダイレクトプロキシ構成	空	VDA 7.16 から現在まで
ブラウザコンテンツリダイレクトサーバーフェッチWebプロキシ認証	禁止	VDA 2012から現在まで

ICA/クライアントセンサー

名前	デフォルト設定	VDA
アプリケーションによるクライアントデバイスの物理的な場所の使用を許可する	禁止	VDA 5.6 FP1、マルチセッションOS用VDA 7から現在まで、シングルセッションOS用VDA 7から現在まで

ICA/デスクトップUI

名前	デフォルト設定	VDA
デスクトップコンポジションリダイレクト	無効 (7.6 FP3から現在まで); 有効 (5.6から7.6 FP2まで)	VDA 5.6、シングルセッションOS用VDA 7から7.15まで
デスクトップコンポジションリダイレクトのグラフィック品質	中	VDA 5.6、シングルセッションOS用VDA 7から7.15まで
デスクトップの壁紙	許可	すべてのVDAバージョン
メニューアニメーション	許可	すべてのVDAバージョン
ドラッグ中にウィンドウの内容を表示	許可	すべてのVDAバージョン

ICA/エンドユーザー監視

名前	デフォルト設定	VDA
ICAラウンドトリップ計算	有効	すべてのVDAバージョン
ICAラウンドトリップ計算間隔	15秒	すべてのVDAバージョン
アイドル接続のICAラウンドトリップ計算	無効	すべてのVDAバージョン

ICA/強化されたデスクトップエクスペリエンス

名前	デフォルト設定	VDA
強化されたデスクトップエクスペリエンス	許可	マルチセッションOS 7以降のVDA

ICA/ファイルリダイレクト

名前	デフォルト設定	VDA
クライアントドライブの自動接続	許可	すべてのVDAバージョン
クライアントドライブのリダイレクト	許可	すべてのVDAバージョン
クライアント固定ドライブ	許可	すべてのVDAバージョン
クライアントフロッピードライブ	許可	すべてのVDAバージョン
クライアントネットワークドライブ	許可	すべてのVDAバージョン
クライアント光学ドライブ	許可	すべてのVDAバージョン
クライアントリムーバブルドライブ	許可	すべてのVDAバージョン
ホストからクライアントへのリダイレクト	無効	マルチセッションOS向けVDA 7以降
クライアントドライブ文字を保持する	無効	VDA 5、5.5、5.6 FP1、シングルセッションOS向けVDA 7以降
読み取り専用クライアントドライブアクセス	無効	VDA 5.5、5.6 FP1、マルチセッションOS向けVDA 7以降、シングルセッションOS向けVDA 7以降
特殊フォルダーのリダイレクト	許可	Web Interface展開のみ。マルチセッションOS向けVDA 7以降
非同期書き込みを使用する	無効	すべてのVDAバージョン

ICA/グラフィック

名前	デフォルト設定	VDA
視覚的にロスレスな圧縮を許可する	無効	VDA 7.6以降
表示メモリ制限	65,536 Kb	VDA 5、5.5、5.6 FP1、シングルセッションOS向けVDA 7以降
ディスプレイモードの劣化設定	最初に色深度を劣化させる	すべてのVDAバージョン
動的ウィンドウプレビュー	有効	VDA 5.5、5.6 FP1、マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
グラフィックステータスインジケーター	無効	VDA 7.16以降
イメージキャッシュ	有効	VDA 5.5、5.6 FP1、マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
レガシーグラフィックモード	無効	マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
許可される最大色深度	32ビット/ピクセル	すべてのVDAバージョン
ディスプレイモードが劣化した場合にユーザーに通知する	無効	マルチセッションOS用VDA 7以降
3Dグラフィックワークロード向けに最適化	無効	VDA 7.17から現在まで
キューイングとトッシング	有効	すべてのVDAバージョン
画面共有	無効	VDA 2112

名前	デフォルト設定	VDA
圧縮にビデオコーデックを使用	優先される場合にビデオコーデックを使用	VDA 7.6 FP3から現在まで
ビデオコーデックにハードウェアエンコードを使用	有効	VDA 7.11から現在まで

ICA/グラフィック/キャッシュ

名前	デフォルト設定	VDA
永続キャッシュしきい値	3,000,000 ビット/秒	マルチセッションOS用VDA 7から現在まで

ICA/グラフィック/Framehawk

名前	デフォルト設定	VDA
Framehawkディスプレイチャネル	無効	VDA 7.6 FP2 以降
Framehawkディスプレイチャネルのポート範囲	3224,3324	VDA 7.6 FP2 以降

ICA/キープアライブ

名前	デフォルト設定	VDA
ICAキープアライブタイムアウト	60秒	すべてのVDAバージョン
ICAキープアライブ	ICAキープアライブメッセージを送信しない	すべてのVDAバージョン

ICA/キーボードおよびIME

名前	デフォルト設定	VDA
クライアントキーボードレイアウト同期およびIMEの改善	無効	1912 LTSR CU2以降にのみ適用されます。

名前	デフォルト設定	VDA
Unicodeキーボードレイアウトマッピングを有効にする	禁止	1912 LTSR CU2以降にのみ適用されます。
キーボードレイアウト切り替えポップアップメッセージボックスを非表示にする	禁止	1912 LTSR CU2以降にのみ適用されます。

ICA/ローカルアプリアクセス

名前	デフォルト設定	VDA
ローカルアプリアクセスを許可	禁止	マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
URLリダイレクトブロックリスト	サイトは指定されていません	マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
URLリダイレクト許可リスト	サイトは指定されていません	マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降

ICA/モバイルエクスペリエンス

名前	デフォルト設定	VDA
自動キーボード表示	禁止	VDA 5.6 FP1、マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
タッチ最適化デスクトップの起動	許可	VDA 5.6 FP1、マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降。この設定は無効になっており、Windows 10およびWindows Server 2016マシンでは利用できません。

名前	デフォルト設定	VDA
コンボボックスのリモート処理	禁止	VDA 5.6 FP1、マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降

ICA/マルチメディア

名前	デフォルト設定	VDA
HTML5ビデオリダイレクト	禁止	VDA 7.12以降
ビデオ品質の制限	未構成	マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
Microsoft Teamsリダイレクト	許可	マルチセッションOS用VDA 1906以降、シングルセッションOS用VDA 1906以降。
マルチメディア会議	許可	すべてのVDAバージョン
WAN経由のWindows Media マルチメディアリダイレクトの最適化	許可	マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
WAN経由のWindows Media マルチメディアリダイレクトの最適化にGPUを使用	禁止	マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
Windows Mediaフォールバックの防止	未構成	VDA 7.6 FP3以降
Windows Mediaクライアント側コンテンツフェッチ	許可	マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
Windows Mediaリダイレクト	許可	すべてのVDAバージョン
Windows Mediaリダイレクトバッファサイズ	5秒	VDA 5、5.5、5.6 FP1から現在まで

名前	デフォルト設定	VDA
Windows Mediaリダイレクトバッファサイズの使用	無効	VDA 5、5.5、5.6 FP1から現在まで

ICA/マルチストリーム接続

名前	デフォルト設定	VDA
UDP経由のオーディオ	許可	VDA for Multi-session OS 7から現在まで
オーディオUDPポート範囲	16500、16509	VDA 5.5、5.6 FP1、VDA for Multi-session OS 7から現在まで、VDA for Single-session OS 7から現在まで
マルチポートポリシー	プライマリポート (2598) は高優先度	VDA 5.5、5.6 FP1、VDA for Multi-session OS 7から現在まで、VDA for Single-session OS 7から現在まで
マルチストリーム コンピューター設定	無効	VDA 5.5、5.6 FP1、VDA for Multi-session OS 7から現在まで、VDA for Single-session OS 7から現在まで
マルチストリーム ユーザー設定	無効	VDA 5.5、5.6 FP1、VDA for Multi-session OS 7から現在まで、VDA for Single-session OS 7から現在まで
マルチストリーム仮想チャネルストリーム割り当て設定	デフォルトのストリーム割り当てについては、マルチストリーム仮想チャネル割り当て設定を参照してください。	VDA 2003

ICA/ポートリダイレクト

名前	デフォルト設定	VDA
クライアントCOMポートの自動接続	無効	すべてのVDAバージョン。VDA 7.0から7.8までは、レジストリを使用してこの設定を構成します
クライアントLPTポートの自動接続	無効	すべてのVDAバージョン。VDA 7.0から7.8までは、レジストリを使用してこの設定を構成します
クライアントCOMポートリダイレクト	禁止	すべてのVDAバージョン。VDA 7.0から7.8までは、レジストリを使用してこの設定を構成します
クライアントLPTポートリダイレクト	禁止	すべてのVDAバージョン。VDA 7.0から7.8までは、レジストリを使用してこの設定を構成します

ICA/印刷

名前	デフォルト設定	VDA
クライアントプリンターリダイレクト	許可	すべてのVDAバージョン
デフォルトプリンター	デフォルトプリンターをクライアントのメインプリンターに設定する	すべてのVDAバージョン
プリンターの割り当て	ユーザーの現在のプリンターがセッションのデフォルトプリンターとして使用されます	すべてのVDAバージョン
プリンターの自動作成イベントログの優先順位	エラーと警告をログに記録	すべてのVDAバージョン

名前	デフォルト設定	VDA
セッションプリンター	プリンターが指定されていません	すべてのVDAバージョン
プリンターが作成されるまで待機する (デスクトップ)	無効	すべてのVDAバージョン

ICA/印刷/クライアントプリンター

名前	デフォルト設定	VDA
クライアントプリンターを自動作成	すべてのクライアントプリンターを自動作成	すべてのVDAバージョン
汎用ユニバーサルプリンターを自動作成	無効	すべてのVDAバージョン
クライアントプリンター名	標準プリンター名	VDA 5.6
印刷サーバーへの直接接続	有効	すべてのVDAバージョン
プリンタードライバーのマッピングと互換性	ルールは指定されていません	すべてのVDAバージョン
プリンタープロパティの保持	クライアントに保存されていない場合にのみプロファイルに保持	すべてのVDAバージョン
保持および復元されたクライアントプリンター	許可	VDA 5、5,5、5.6 FP1

ICA/Printing/Drivers

名前	デフォルト設定	VDA
インボックスプリンタードライバーの自動インストール	有効	すべてのVDAバージョン
ユニバーサルドライバーの優先順位	イーエムエフ; エックスピーエス; ピーシーエルファイブ	すべてのVDAバージョン

名前	デフォルト設定	VDA
	シー; ピーシーエルフォー; ピーエス	
ユニバーサル印刷ドライバーの使用	要求されたドライバーが利用できない場合にのみユニバーサル印刷を使用する	すべてのVDAバージョン

ICA/印刷/ユニバーサルプリントサーバー

名前	デフォルト設定	VDA
ユニバーサルプリントサーバーを有効にする	無効	すべてのVDAバージョン
ユニバーサルプリントサーバー印刷データストリーム (CGP) ポート	7229	すべてのVDAバージョン
ユニバーサルプリントサーバー印刷ストリーム入力帯域幅制限 (kbps)	0	すべてのVDAバージョン
ユニバーサルプリントサーバーWebサービス (HTTP/SOAP) ポート	8080	すべてのVDAバージョン
負荷分散用のUniversal Print Server	VDA バージョン 7.9 から現在まで	
ユニバーサルプリントサーバーのサービス停止しきい値	180 (秒)	VDA バージョン 7.9 から現在まで

ICA/印刷/ユニバーサル印刷

名前	デフォルト設定	VDA
ユニバーサル印刷 EMF 処理モード	プリンターに直接スプールする	すべてのVDAバージョン
ユニバーサル印刷画像圧縮制限	最高品質 (ロスレス圧縮)	すべてのVDAバージョン

名前	デフォルト設定	VDA
ユニバーサル印刷最適化のデフォルト	画像圧縮: 希望する画質 = 標準品質, ヘビーウェイト圧縮を有効にする = 無効; 画像とフォントのキャッシュ: 埋め込み画像のキャッシュを許可する = 有効; 管理者以外のユーザーがこれらの設定を変更することを許可する = 無効;	すべてのVDAバージョン
ユニバーサル印刷プレビュー設定	自動作成されたプリンターまたは汎用ユニバーサルプリンターには印刷プレビューを使用しない	すべてのVDAバージョン
ユニバーサル印刷の印刷品質制限	制限なし	すべてのVDAバージョン

ICA/セキュリティ

名前	デフォルト設定	VDA
SecureICAの最小暗号化レベル	基本	マルチセッションOS用VDA 7以降

ICA/サーバー制限

名前	デフォルト設定	VDA
サーバーアイドルタイマー間隔	0ミリ秒	マルチセッションOS用VDA 7以降

ICA/セッション制限

名前	デフォルト設定	VDA
切断されたセッションタイマー	無効	VDA 5、5.5、5.6 FP1、シングルセッションOS用VDA 7以降

名前	デフォルト設定	VDA
リモートPCアクセス切断セッションタイマー	無効	シングルセッションOS用VDA 7以降
切断セッションタイマー間隔	1,440分	VDA 5、5.5、5.6 FP1、シングルセッションOS用VDA 7以降
セッション接続タイマー	無効	VDA 5、5.5、5.6 FP1、シングルセッションOS用VDA 7以降
セッション接続タイマー間隔	1,440分	VDA 5、5.5、5.6 FP1、シングルセッションOS用VDA 7以降
セッションアイドルタイマー	有効	VDA 5、5.5、5.6 FP1、シングルセッションOS用VDA 7以降
セッションアイドルタイマー間隔	1,440分	VDA 5、5.5、5.6 FP1、シングルセッションOS用VDA 7以降

ICA/セッションの信頼性

名前	デフォルト設定	VDA
セッションの信頼性接続	許可	すべてのVDAバージョン
セッションの信頼性ポート番号	2598	すべてのVDAバージョン
セッションの信頼性タイムアウト	180秒	すべてのVDAバージョン

ICA/タイムゾーン制御

名前	デフォルト設定	VDA
レガシークライアントのローカル時刻を推定する	有効	マルチセッションOS 7以降のVDA
セッション切断またはログオフ時にシングルセッションOSのタイムゾーンを復元する	有効	現在のVDAバージョン
クライアントのローカル時刻を使用する	サーバーのタイムゾーンを使用する	すべてのVDAバージョン

ICA/TWAINデバイス

名前	デフォルト設定	VDA
クライアントTWAINデバイスリダイレクト	許可	VDA 5.5、5.6 FP1、マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
TWAIN圧縮レベル	中	VDA 5.5、5.6 FP1、マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降

ICA/USBデバイス

名前	デフォルト設定	VDA
クライアントUSBデバイス最適化ルール	有効 (VDA 7.6 FP3以降); 無効 (VDA 7.11以降); デフォルトでは、ルールは指定されていません	VDA 7.6 FP3以降
クライアントUSBデバイスのリダイレクト	禁止	すべてのVDAバージョン

名前	デフォルト設定	VDA
クライアントUSBデバイスリダイレクト規則	ルールは指定されていません	すべてのVDAバージョン
クライアントUSBプラグアンドプレイデバイスリダイレクト	許可	マルチセッションOS 用 VDA 7 以降、シングルセッション OS 用 VDA 7 以降

ICA/ビジュアルディスプレイ

名前	デフォルト設定	VDA
単純なグラフィックの優先色深度	24ビット/ピクセル	VDA 7.6 FP3 以降
ターゲットフレームレート	30 フレーム/秒	すべてのVDAバージョン
画質	中	マルチセッションOS 用 VDA 7 以降、シングルセッション OS 用 VDA 7 以降

ICA/ビジュアルディスプレイ/動画

名前	デフォルト設定	VDA
最小画質	標準	VDA 5.5、5.6 FP1、マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
動画圧縮	有効	VDA 5.5、5.6 FP1、マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
プログレッシブ圧縮レベル	なし	VDA 5.5、5.6 FP1、マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降

名前	デフォルト設定	VDA
プログレッシブ圧縮のしきい値	2,147,483,647 キロビット/秒	VDA 5.5、5.6 FP1、マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
目標最小フレームレート	10 フレーム/秒	VDA 5.5、5.6 FP1、マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降

注：

「**目標最小フレームレート**」ポリシーは廃止されました。

ICA/視覚表示/静止画像

名前	デフォルト設定	VDA
追加の色圧縮	無効	すべてのVDAバージョン
追加の色圧縮のしきい値	8,192 キロビット/秒	すべてのVDAバージョン
高負荷圧縮	無効	すべてのVDAバージョン
非可逆圧縮レベル	中	すべてのVDAバージョン
非可逆圧縮しきい値	2,147,483,647 ケービーピーエス	すべてのVDAバージョン

ICA/WebSockets

名前	デフォルト設定	VDA
WebSockets接続	禁止	マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降

名前	デフォルト設定	VDA
WebSocketsポート番号	8008	マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
WebSockets信頼済みオリジンサーバーリスト	ワイルドカード「*」は、すべてのReceiver for Web URLを信頼するために使用されます	マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降

負荷管理

名前	デフォルト設定	VDA
同時ログオン許容数	2	マルチセッションOS用VDA 7以降
CPU使用率	無効	マルチセッションOS用VDA 7以降
CPU使用率から除外されるプロセスの優先度	標準以下または低	マルチセッションOS用VDA 7以降
ディスク使用量	無効	マルチセッションOS用VDA 7以降
最大セッション数	250	マルチセッションOS用VDA 7以降
メモリ使用量	無効	マルチセッションOS用VDA 7以降
メモリ使用量のベース負荷	ゼロ負荷: 768 MB	マルチセッションOS用VDA 7以降

プロファイル管理/詳細設定

名前	デフォルト設定	VDA
自動構成を無効にする	無効	すべてのVDAバージョン

名前	デフォルト設定	VDA
問題が発生した場合にユーザーをログオフする	無効	すべてのVDAバージョン
ロックされたファイルへのアクセス時の再試行回数	5	すべてのVDAバージョン
ログオフ時にインターネットCookieファイルを処理する	無効	すべてのVDAバージョン

プロファイル管理/基本設定

名前	デフォルト設定	VDA
アクティブライトバック	無効	すべてのVDAバージョン
Profile Management を有効にする	無効	すべてのVDAバージョン
除外されるグループ	無効。すべてのユーザーグループのメンバーが処理されます。	すべてのVDAバージョン
オフラインプロファイルのサポート	無効	すべてのVDAバージョン
ユーザーストアへのパス	ウィンドウズ	すべてのVDAバージョン
ローカル管理者によるログオンの処理	無効	すべてのVDAバージョン
処理されるグループ	無効。すべてのユーザーグループのメンバーが処理されます。	すべてのVDAバージョン

プロファイル管理/クロスプラットフォーム設定

名前	デフォルト設定	VDA
クロスプラットフォーム設定ユーザーグループ	無効。処理済みグループで指定されたすべてのユーザーグループが処理されます	すべてのVDAバージョン
クロスプラットフォーム設定を有効にする	無効	すべてのVDAバージョン
クロスプラットフォーム定義へのパス	無効。パスは指定されていません。	すべてのVDAバージョン
クロスプラットフォーム設定ストアへのパス	無効。Windows\PM_CMが使用されます。	すべてのVDAバージョン
クロスプラットフォーム設定の作成元	無効	すべてのVDAバージョン

プロファイル管理/ファイルシステム/除外

名前	デフォルト設定	VDA
除外リスト - ディレクトリ	無効。ユーザープロファイル内のすべてのフォルダーが同期されます。	すべてのVDAバージョン
除外リスト - ファイル	無効。ユーザープロファイル内のすべてのファイルが同期されます。	すべてのVDAバージョン

プロファイル管理/ファイルシステム/同期

名前	デフォルト設定	VDA
同期するディレクトリ	無効。除外されていないフォルダーのみが同期されます。	すべてのVDAバージョン
同期するファイル	無効。除外されていないファイルのみが同期されます。	すべてのVDAバージョン

名前	デフォルト設定	VDA
ミラーリングするフォルダー	無効。フォルダーはミラーリングされません。	すべてのVDAバージョン

プロファイル管理/フォルダーリダイレクト

名前	デフォルト設定	VDA
管理者アクセスを許可する	無効	すべてのVDAバージョン
ドメイン名を含める	無効	すべてのVDAバージョン

プロファイル管理/フォルダーリダイレクト/AppData(Roaming)

名前	デフォルト設定	VDA
AppData(Roaming)パス	無効。場所は指定されていません。	すべてのVDAバージョン
AppData(Roaming)のリダイレクト設定	コンテンツは、AppData(Roaming)パスのポリシー設定で指定されたUNCパスにリダイレクトされます	すべてのVDAバージョン

プロファイル管理/フォルダーリダイレクト/連絡先

名前	デフォルト設定	VDA
連絡先パス	無効。場所は指定されていません。	すべてのVDAバージョン
連絡先のリダイレクト設定	コンテンツは、**連絡先パスポリシー**設定で指定されたUNCパスにリダイレクトされます	すべてのVDAバージョン

プロファイル管理/フォルダーリダイレクト/デスクトップ

名前	デフォルト設定	VDA
デスクトップパス	無効。場所は指定されていません。	すべてのVDAバージョン
デスクトップのリダイレクト設定	コンテンツは、**デスクトップパスポリシー**設定で指定されたUNCパスにリダイレクトされます	すべてのVDAバージョン

プロファイル管理/フォルダーリダイレクト/ドキュメント

名前	デフォルト設定	VDA
ドキュメントパス	無効。場所は指定されていません。	すべてのVDAバージョン
ドキュメントのリダイレクト設定	コンテンツは、**ドキュメントパスポリシー**設定で指定されたUNCパスにリダイレクトされます	すべてのVDAバージョン

プロファイル管理/フォルダーリダイレクト/ダウンロード

名前	デフォルト設定	VDA
ダウンロードパス	無効。場所は指定されていません。	すべてのVDAバージョン
ダウンロードのリダイレクト設定	コンテンツは、**ダウンロードパスポリシー**設定で指定されたUNCパスにリダイレクトされます	すべてのVDAバージョン

プロファイル管理/フォルダーリダイレクト/お気に入り

名前	デフォルト設定	VDA
お気に入りパス	無効。場所は指定されていません。	すべてのVDAバージョン

名前	デフォルト設定	VDA
お気に入りのリダイレクト設定	コンテンツは、**お気に入りパスポリシー**設定で指定されたUNCパスにリダイレクトされます	すべてのVDAバージョン

プロファイル管理/フォルダーリダイレクト/リンク

名前	デフォルト設定	VDA
リンクパス	無効。場所は指定されていません。	すべてのVDAバージョン
リンクのリダイレクト設定	コンテンツは、**リンクパスポリシー**設定で指定されたUNCパスにリダイレクトされます	すべてのVDAバージョン

プロファイル管理/フォルダーリダイレクト/ミュージック

名前	デフォルト設定	VDA
ミュージックパス	無効。場所は指定されていません。	すべてのVDAバージョン
ミュージックのリダイレクト設定	コンテンツは、「**ミュージックパスポリシー**」設定で指定されたUNCパスにリダイレクトされます	すべてのVDAバージョン

プロファイル管理/フォルダーリダイレクト/ピクチャ

名前	デフォルト設定	VDA
ピクチャパス	無効。場所は指定されていません。	すべてのVDAバージョン
ピクチャのリダイレクト設定	コンテンツは、「**ピクチャパスポリシー**」設定で指定されたUNCパスにリダイレクトされます	すべてのVDAバージョン

プロファイル管理/フォルダーリダイレクト/保存されたゲーム

名前	デフォルト設定	VDA
保存されたゲームパス	無効。場所は指定されていません。	すべてのVDAバージョン
保存されたゲームのリダイレクト設定	コンテンツは、「**保存されたゲームパスポリシー**」設定で指定されたUNCパスにリダイレクトされます	すべてのVDAバージョン

プロファイル管理/フォルダーリダイレクト/検索

名前	デフォルト設定	VDA
検索パス	無効。場所は指定されていません。	すべてのVDAバージョン
検索のリダイレクト設定	コンテンツは、**検索パスポリシー**設定で指定されたUNCパスにリダイレクトされます。	すべてのVDAバージョン

プロファイル管理/フォルダーリダイレクト/スタートメニュー

名前	デフォルト設定	VDA
スタートメニューパス	無効。場所は指定されていません。	すべてのVDAバージョン
スタートメニューのリダイレクト設定	コンテンツは、スタートメニューパスポリシー設定で指定されたUNCパスにリダイレクトされます。	すべてのVDAバージョン

プロファイル管理/フォルダーリダイレクト/ビデオ

名前	デフォルト設定	VDA
ビデオパス	無効。場所は指定されていません。	すべてのVDAバージョン

名前	デフォルト設定	VDA
ビデオのリダイレクト設定	コンテンツは、**ビデオパスポリシー**設定で指定されたUNCパスにリダイレクトされます	すべてのVDAバージョン

プロファイル管理/ログ設定

名前	デフォルト設定	VDA
Active Directory のアクション	無効	すべてのVDAバージョン
一般情報	無効	すべてのVDAバージョン
一般的な警告	無効	すべてのVDAバージョン
ログの有効化	無効	すべてのVDAバージョン
ファイルシステムのアクション	無効	すべてのVDAバージョン
ファイルシステム通知	無効	すべてのVDAバージョン
ログオフ	無効	すべてのVDAバージョン
ログオン	無効	すべてのVDAバージョン
ログファイルの最大サイズ	1048576	すべてのVDAバージョン
ログファイルへのパス	無効。ログファイルはデフォルトの場所 (%SystemRoot%\System32\Logfiles\UserProfileManager) に保存されます。	すべてのVDAバージョン
パーソナライズされたユーザー情報	無効	すべてのVDAバージョン
ログオン時とログオフ時のポリシー値	無効	すべてのVDAバージョン
レジストリアクション	無効	すべてのVDAバージョン

名前	デフォルト設定	VDA
ログオフ時のレジストリの相違点	無効	すべてのVDAバージョン

プロファイル管理/プロファイルの処理

名前	デフォルト設定	VDA
キャッシュされたプロファイルを削除するまでの遅延	0	すべてのVDAバージョン
ログオフ時にローカルにキャッシュされたプロファイルを削除する	無効	すべてのVDAバージョン
ローカルプロファイルの競合処理	ローカルプロファイルを使用する	すべてのVDAバージョン
既存プロファイルの移行	ローカルとローミング	すべてのVDAバージョン
テンプレートプロファイルへのパス	無効。新しいユーザープロファイルは、ユーザーが最初にログオンしたデバイスのデフォルトユーザープロファイルから作成されます。	すべてのVDAバージョン
テンプレートプロファイルがローカルプロファイルを上書きする	無効	すべてのVDAバージョン
テンプレートプロファイルが移動プロファイルを上書きする	無効	すべてのVDAバージョン
すべてのログオンでCitrix®必須プロファイルとして使用されるテンプレートプロファイル	無効	すべてのVDAバージョン

プロファイル管理/レジストリ

名前	デフォルト設定	VDA
除外リスト	無効。ユーザーがログオフすると、HKCUハイブ内のすべてのレジストリキーが処理されます。	すべてのVDAバージョン
包含リスト	無効。ユーザーがログオフすると、HKCUハイブ内のすべてのレジストリキーが処理されます。	すべてのVDAバージョン

プロファイル管理/ストリーム配信ユーザープロファイル

名前	デフォルト設定	VDA
常にキャッシュ	無効	すべてのVDAバージョン
常にキャッシュサイズ	0 MB	すべてのVDAバージョン
プロファイルストリーミング	無効	すべてのVDAバージョン
ストリーミングされたユーザープロファイルグループ	無効。OU内のすべてのユーザープロファイルは通常どおり処理されます。	すべてのVDAバージョン
保留中のエリアロックファイルのタイムアウト (日数)	1日	すべてのVDAバージョン

レシーバー

名前	デフォルト設定	VDA
StoreFront™アカウントリスト	ストアは指定されていません	マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降

ユーザーパーソナライゼーションレイヤー

名前	デフォルト設定	VDA
ユーザーレイヤーリポジトリパス	無効。パスは指定されていません。	VDA 19.12以降のバージョン
ユーザーレイヤーサイズ(GB)	10 GB。ユーザーレイヤーは、設定されたサイズまで拡張するシンプロビジョニングディスクです。ユーザーレイヤーのサイズが小さくなることはありません。	VDA 19.12以降のバージョン

バーチャル デリバリー エージェント

名前	デフォルト設定	VDA
コントローラー登録IPv6ネットマスク	ネットマスクは指定されていません	マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
コントローラー登録ポート	80	すべてのVDAバージョン
コントローラーSID	SIDは指定されていません	すべてのVDAバージョン
コントローラー	コントローラーは指定されていません	すべてのVDAバージョン
コントローラーの自動更新を有効にする	有効	マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
IPv6コントローラー登録のみを使用する	無効	マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
サイトGUID	GUIDは指定されていません	すべてのVDAバージョン

バーチャル デリバリー エージェント/HDX 3D Pro

名前	デフォルト設定	VDA
ロスレスを有効にする	有効	VDA 5.5、5.6 FP1
HDX 3D Pro品質設定	VDA 5.5、5.6 FP1	

バーチャル デリバリー エージェント/監視

名前	デフォルト設定	VDA
プロセス監視を有効にする	無効	VDA 7.11以降
リソース監視を有効にする	有効	VDA 7.11以降

仮想IP

名前	デフォルト設定	VDA
仮想IPループバックサポート	無効	VDA 7.6 以降
仮想IP仮想ループバックプログラムリスト	なし	VDA 7.6 以降

ポリシー設定リファレンス

ポリシーには、ポリシーが適用されるときに適用される設定が含まれます。このセクションの説明では、機能を有効にするためにより多くの設定が必要かどうか、または設定に類似しているかどうかも示します。

クイックリファレンス

以下の表に、ポリシー内で構成できる設定を示します。左の列で完了したいタスクを見つけ、右の列で対応する設定を見つけてください。

.CHM (コンパイル済みHTML) 形式および .CSV 形式で、すべてのポリシー設定の完全なリストが利用可能です。これらのファイルは、ブローカー (デリバリーコントローラー) がインストールされているサーバーの `\program files\citrix\grouppolicy` フォルダーにあります。ポリシー設定の最新バージョンは、こちらをクリックしてダウンロードすることもできます。

オーディオ

このタスクの場合	このポリシー設定を使用
複数のオーディオデバイスの使用を許可するかどうかを制御する	オーディオプラグアンドプレイ
ユーザーデバイスのマイクからのオーディオ入力を許可するかどうかを制御する	クライアントマイクのリダイレクト
ユーザーデバイスのオーディオ品質を制御する	オーディオ品質
ユーザーデバイスのスピーカーへのオーディオマッピングを制御する	クライアントオーディオリダイレクト

ユーザーデバイスの帯域幅

使用される帯域幅を制限するには	このポリシー設定を使用
クライアントオーディオマッピング	オーディオリダイレクト帯域幅制限またはオーディオリダイレクト帯域幅制限率
ローカルクリップボードを使用した切り取りと貼り付け	クリップボードリダイレクト帯域幅制限またはクリップボードリダイレクト帯域幅制限率
セッションでのローカルクライアントドライブへのアクセス	ファイルリダイレクト帯域幅制限またはファイルリダイレクト帯域幅制限率
HDX™ MediaStream マルチメディアアクセラレーション	HDX MediaStream マルチメディアアクセラレーション帯域幅制限またはHDX MediaStream マルチメディアアクセラレーション帯域幅制限率
クライアントセッション	セッション全体の帯域幅制限
印刷	プリンターリダイレクト帯域幅制限またはプリンターリダイレクト帯域幅制限率
TWAINデバイス（カメラやスキャナーなど）	TWAINデバイスリダイレクト帯域幅制限またはTWAINデバイスリダイレクト帯域幅制限率

使用される帯域幅を制限するには	このポリシー設定を使用
USBデバイス	クライアントUSBデバイスリダイレクト帯域幅制限またはクライアントUSBデバイスリダイレクト帯域幅制限率

クライアントドライブとユーザーデバイスのリダイレクト

このタスクの場合	このポリシー設定を使用する
ユーザーがサーバーにログオンしたときに、ユーザーデバイス上のドライブを接続するかどうかを制御します	クライアントドライブの自動接続
サーバーとローカルクリップボード間のカットアンドペーストデータ転送を制御します	クライアントクリップボードリダイレクト
ユーザーデバイスからドライブがどのようにマップされるかを制御します	クライアントドライブのリダイレクト
ユーザーのローカルハードドライブがセッションで利用可能かどうかを制御します	クライアント固定ドライブとクライアントドライブのリダイレクト
ユーザーのローカルフロッピーディスクドライブがセッションで利用可能かどうかを制御します	クライアントフロッピーディスクドライブとクライアントドライブのリダイレクト
ユーザーのネットワークドライブがセッションで利用可能かどうかを制御します	クライアントネットワークドライブとクライアントドライブのリダイレクト
ユーザーのローカルCD、DVD、またはBlu-rayドライブがセッションで利用可能かどうかを制御します	クライアント光学ドライブとクライアントドライブのリダイレクト
ユーザーのローカルリムーバブルドライブがセッションで利用可能かどうかを制御します	クライアントリムーバブルドライブとクライアントドライブリダイレクト
スキャナーやカメラなどのユーザーのTWAINデバイスがセッションで利用可能かどうかを制御し、画像データ転送の圧縮を制御します	クライアントTWAINデバイスリダイレクト; TWAIN圧縮リダイレクト
USBデバイスがセッションで利用可能かどうかを制御します	クライアントUSBデバイスリダイレクトとクライアントUSBデバイスリダイレクト規則

このタスクの場合	このポリシー設定を使用する
WAN経由でクライアントディスクへのファイルの書き込みおよびコピーの速度を向上させます	非同期書き込みを使用する

コンテンツリダイレクト

このタスクの場合	このポリシー設定を使用する
サーバーからユーザーデバイスへのコンテンツリダイレクトを使用するかどうかを制御します	ホストからクライアントへのリダイレクト

デスクトップUI

このタスクの場合	このポリシー設定を使用する
ユーザーセッションでデスクトップの壁紙を使用するかどうかを制御します	デスクトップの壁紙
ウィンドウのドラッグ中にウィンドウの内容を表示します	ドラッグ中のウィンドウの内容を表示

グラフィックとマルチメディア

重要:

Flashポリシーは、古いVDAを使用している顧客が新しいコントローラー（たとえば、バージョン1912コントローラー）を使用し、引き続きFlashを使用できるようにするためにのみ残されています。このVDAバージョンはFlashをサポートしていません。

このタスクの場合	このポリシー設定を使用します
仮想デスクトップからユーザーデバイスに送信される1秒あたりの最大フレーム数を制御します。	ターゲットフレームレート

このタスクの場合	このポリシー設定を使用します
ユーザーデバイスに表示される画像の視覚的な品質を制御します。	視覚的な品質
セッションでアクセスされたときに、Webサイトがフラッシュコンテンツを表示できるかどうかを制御します。	Flashサーバー側コンテンツ取得URLリスト; Flash URL互換性リスト; Flashビデオフォールバック防止ポリシー設定; Flashビデオフォールバック防止エラー *.swf
サーバーでレンダリングされたビデオの圧縮を制御します。	圧縮にビデオコーデックを使用。ビデオコーデックにハードウェアエンコードを使用。
ユーザーへのHTML5マルチメディアWebコンテンツの配信を制御します。	HTML5ビデオリダイレクト

マルチストリームネットワークトラフィックの優先順位付け

このタスクの場合	このポリシー設定を使用
複数の接続にわたるICA®トラフィックのポートを指定し、ネットワークの優先順位を確立します。	マルチポートポリシー
サーバーとユーザーデバイス間のマルチストリーム接続のサポートを有効にします。	マルチストリーム (コンピューターとユーザーの設定)

印刷

このタスクの場合	このポリシー設定を使用
ユーザーデバイス上のクライアントプリンターの作成を制御します。	クライアントプリンターの自動作成とクライアントプリンターのリダイレクト
プリンタープロパティが保存される場所を制御します。	プリンタープロパティの保持
クライアントまたはサーバーが印刷要求を処理するかどうかを制御する	印刷サーバーへの直接接続

このタスクの場合	このポリシー設定を使用
ユーザーが自分のユーザーデバイスに接続されているプリンターにアクセスできるかどうかを制御する	クライアントプリンターリダイレクト
クライアントおよびネットワークプリンターを自動的に作成する際のネイティブWindowsドライバーのインストールを制御する	インボックスプリンタードライバーの自動インストール
ユニバーサルプリンタードライバーをいつ使用するかを制御する	ユニバーサルプリンタードライバーの使用
ローミングユーザーセッション情報に基づいてプリンターを選択する	既定のプリンター
ユニバーサルプリントサーバーの負荷分散とフェールオーバースレッショルドの設定	負荷分散のためのユニバーサルプリントサーバー。サービス停止しきい値のユニバーサルプリントサーバー

注：

ポリシーを使用して、デスクトップまたはアプリケーションセッションでスクリーンセーバーを有効にすることはできません。スクリーンセーバーを必要とするユーザーの場合、スクリーンセーバーはユーザーデバイスに実装できます。

ICA® ポリシー設定

注：

このページでは、ICAポリシー設定の説明とサポートされている構成値を提供します。ポリシーの操作の詳細については、「ポリシーの操作」セクションを参照してください。

アダプティブトランスポート

この設定により、EDTをプライマリとして、TCPをフォールバックとしてデータ転送を行うことを許可または禁止します。

デフォルトでは、アダプティブトランスポートは有効（**優先**）になっており、可能な場合はEDTが使用され、TCPにフォールバックします。必要に応じて設定を変更できます。

- **優先**。可能な場合はEDT経由のアダプティブトランスポートが使用され、TCPにフォールバックします。
- **診断モード**。EDTが強制的にオンになり、TCPへのフォールバックは無効になります。この設定はトラブルシューティングの場合にのみ推奨されます。
- **オフ**。TCPが強制的にオンになり、EDTは無効になります。

詳細については、「アダプティブトランスポート」を参照してください。

ドラッグアンドドロップ設定

この設定により、クライアントと仮想アプリケーションまたはデスクトップの間でファイルをドラッグすることを許可または禁止します。デフォルトでは、ドラッグアンドドロップポリシーは無効になっています。必要に応じて、このポリシーを有効にできます。

アプリケーション起動待機タイムアウト

この設定は、セッションが最初のアプリケーションの起動を待機するミリ秒単位の待機タイムアウト値を指定します。アプリケーションの起動がこの期間を超えると、セッションは終了します。

デフォルトの時間（10,000ミリ秒）を選択するか、ミリ秒単位の数値を指定できます。

クライアントクリップボードリダイレクト

この設定は、ユーザーデバイスのクリップボードがサーバー上のクリップボードにマップされることを許可または禁止します。

デフォルトでは、クリップボードのリダイレクトは許可されています。

セッションとローカルクリップボード間のコピー＆ペーストデータ転送を禁止するには、**禁止**を選択します。ユーザーは、セッション内で実行されているアプリケーション間では引き続きデータをコピー＆ペーストできます。

この設定を許可した後、クライアント接続でクリップボードが消費できる最大許容帯域幅を構成します。**クリップボードリダイレクト帯域幅制限**または**クリップボードリダイレクト帯域幅制限率**の設定を使用します。

クライアントクリップボード書き込み許可形式

クライアントクリップボード書き込みの制限設定が**有効**の場合、ホストクリップボードデータはクライアントエンドポイントと共有できません。この設定を使用して、特定のデータ形式をクラ

イアントエンドポイントのクリップボードと共有することを許可できます。この設定を使用するには、有効にして、許可する特定の形式を追加します。

次のクリップボード形式はシステム定義です。

- CF_TEXT
- CF_BITMAP
- CF_METAFILEPICT
- CF_SYLK
- CF_DIF
- CF_TIFF
- CF_OEMTEXT
- CF_DIB
- CF_PALETTE
- CF_PENDATA
- CF_RIFF
- CF_WAVE
- CF_UNICODETEXT
- CF_ENHMETAFILE
- CF_HDROP
- CF_LOCALE
- CF_DIBV5
- CF_OWNERDISPLAY
- CF_DSPTEXT
- CF_DSPBITMAP
- CF_DSPMETAFILEPICT
- CF_DISPENHMETAFILE
- CF_HTML

XenAppおよびXenDesktopとCitrix Virtual Apps and Desktops™には、以下のカスタム形式が事前定義されています。

- CFX_RICHTEXT

- CFX_OfficeDrawingShape
- CFX_BIFF8
- CFX_FILE

HTML形式はデフォルトで無効になっています。この機能を有効にするには:

- **クライアントクリップボードリダイレクト**が**許可**に設定されていることを確認します。
- **クライアントクリップボード書き込みの制限**が**有効**に設定されていることを確認します。
- **クライアントクリップボード書き込み許可形式**に**CF_HTML**（およびサポートしたいその他の形式）のエントリを追加します。

カスタム形式をさらに追加できます。カスタム形式名は、システムに登録される形式と一致している必要があります。形式名は大文字と小文字を区別します。

この設定は、**クライアントクリップボードリダイレクト**ポリシーが**禁止**に設定されている場合、または**クライアントクリップボード書き込みの制限**ポリシーが**無効**に設定されている場合には適用されません。

> **注:**
>
> HTML形式のクリップボードコピーサポート（CF_HTML）を有効にすると、コピーされたコンテンツのソースから宛先にスクリプトがコピーされます。コピーを進める前に、ソースを信頼できることを確認してください。スクリプトを含むコンテンツをコピーした場合、それらは宛先ファイルをHTMLファイルとして保存して実行した場合にのみ有効になります。

クリップボードのクライアントからセッションへの転送サイズを制限する

この設定は、ユーザーが単一のコピー＆ペースト操作中にクライアントエンドポイントから仮想セッションに転送できるクリップボードデータの最大サイズを指定します。

クリップボードの転送サイズを制限するには、**クリップボードのクライアントからセッションへの転送サイズを制限する**設定を有効にします。次に、**サイズ制限**フィールドにキロバイト単位の値を入力して、ローカルクリップボードとセッション間のデータ転送サイズを定義します。

既定では、この設定は無効になっており、クライアントからセッションへの転送に制限はありません。

HDX™ ダイレクト

HDX Direct を使用すると、直接通信が可能な場合に、クライアントがセッションホストとの直接接続を自動的に確立できます。接続は、ネットワークレベルの暗号化を使用して安全に確立されます。

HDX Direct モード

HDX Direct は、内部クライアントと外部クライアントの両方でセッションホストとの直接接続を確立するために使用できます。この設定は、HDX Direct が内部クライアントのみに利用可能か、内部クライアントと外部クライアントの両方に利用可能かを決定します。

内部のみに設定されている場合、HDX Direct は内部ネットワーク内のクライアントに対してのみ直接接続を確立しようとします。

内部および**外部**に設定されている場合、HDX Direct は内部クライアントと外部クライアントの両方に対して直接接続を確立しようとします。

既定では、HDX Direct は内部クライアントのみに設定されています。

HDX Direct ポート範囲

外部ユーザーからの接続に HDX Direct が使用するポートの範囲です。 既定では、HDX Direct はポート範囲 55000～55250 を使用します。

クリップボードのセッションからクライアントへの転送サイズを制限する

この設定は、ユーザーが単一のコピー＆ペースト操作中に仮想セッションからクライアントエンドポイントに転送できるクリップボードデータの最大サイズを指定します。

クリップボードの転送サイズを制限するには、**クリップボードのセッションからクライアントへの転送サイズを制限する**設定を有効にします。次に、**サイズ制限**フィールドにキロバイト単位の値を入力して、セッションとローカルクリップボード間のデータ転送サイズを定義します。

既定では、この設定は無効になっており、セッションからクライアントへの転送に制限はありません。

クライアントクリップボードへの書き込みを制限する

この設定が**有効**な場合、ホストのクリップボードデータはクライアントエンドポイントと共有できません。**クライアントクリップボード書き込み許可形式**設定を有効にすることで、特定の形式を許可できます。

デフォルトでは、この設定は**無効**です。

セッションクリップボードへの書き込みを制限する

この設定が**有効**な場合、クライアントのクリップボードデータはセッションアプリケーションと共有できません。**セッションクリップボード書き込み許可形式**設定を有効にすることで、特定の形式を許可できます。

デフォルトでは、この設定は**無効**です。

セッションクリップボード書き込み許可形式

セッションクリップボードへの書き込みを制限する設定が**有効**な場合、クライアントのクリップボードデータはセッションアプリケーションと共有できません。この設定を使用して、特定のデータ形式をセッションクリップボードと共有することを許可できます。

以下のクリップボード形式はシステム定義です。

- CF_TEXT
- CF_BITMAP
- CF_METAFILEPICT
- CF_SYLK
- CF_DIF
- CF_TIFF
- CF_OEMTEXT
- CF_DIB
- CF_PALETTE
- CF_PENDATA
- CF_RIFF
- CF_WAVE
- CF_UNICODETEXT
- CF_ENHMETAFILE
- CF_HDROP
- CF_LOCALE
- CF_DIBV5
- CF_OWNERDISPLAY
- CF_DSPTEXT
- CF_DSPBITMAP

- CF_DSPMETAFILEPICT
- CF_DISPENHMETAFILE
- CF_HTML

XenApp and XenDesktopおよびCitrix Virtual Apps and Desktopsでは、以下のカスタム形式が事前定義されています。

- CFX_RICHTEXT
- CFX_OfficeDrawingShape
- CFX_BIFF8

HTML形式はデフォルトで無効になっています。この機能を有効にするには：

- **クライアントクリップボードリダイレクト**が**許可**に設定されていることを確認します。
- **セッションクリップボード書き込みの制限**が**有効**に設定されていることを確認します。
- **セッションクリップボード書き込み許可形式**に**CF_HTML**（およびサポートしたいその他の形式）のエントリを追加します。

カスタム形式を追加できます。カスタム形式名は、システムに登録される形式と一致する必要があります。形式名は大文字と小文字を区別します。

この設定は、**クライアントクリップボードリダイレクト**ポリシーが**禁止**に設定されている場合、または**セッションクリップボード書き込みの制限**ポリシーが**無効**に設定されている場合には適用されません。

> **注:**
>
> HTML形式のクリップボードコピーサポート (CF_HTML) を有効にすると、コピーされたコンテンツのソースから宛先にスクリプトがコピーされます。コピーを進める前に、ソースを信頼できることを確認してください。スクリプトを含むコンテンツをコピーした場合、それらは宛先ファイルをHTMLファイルとして保存して実行した場合にのみ有効になります。

デスクトップの起動

この設定は、VDA Direct Access Usersグループの非管理者ユーザーがICA接続を使用してそのVDA上のセッションに接続することを許可または禁止します。

デフォルトでは、非管理者ユーザーはこれらのセッションに接続できません。

この設定は、RDP接続を使用しているVDAダイレクトアクセスユーザーグループ内の非管理者ユーザーには影響しません。これらのユーザーは、この設定が有効または無効になっている場合でもVDAに接続できます。この設定は、VDAダイレクトアクセスユーザーグループに属していない非管理者ユーザーには影響しません。これらのユーザーは、この設定が有効または無効になっている場合、VDAに接続できません。

FIDO2リダイレクト

この設定は、FIDO2リダイレクトを有効または無効にします。FIDO2リダイレクトにより、ユーザーは仮想マシン内のローカルエンドポイントFIDO2コンポーネントを活用できます。ユーザーは、TPM 2.0とWindows Helloを搭載したデバイスで、FIDO2セキュリティキーまたは統合生体認証を介して仮想セッションを認証できます。

この設定が**許可**されている場合、ユーザーはローカルエンドポイント機能を使用してFIDO2認証を行うことができます。デフォルトでは、この設定は**許可**されています。

ICAリスナー接続タイムアウト

この設定は、ICAプロトコルを使用した接続が完了するまでの最大待機時間を指定します。

デフォルトでは、最大待機時間は120,000ミリ秒、つまり2分です。

ICAリスナーポート番号

この設定は、サーバー上のICAプロトコルによって使用されるTCP/IPポート番号を指定します。

デフォルトでは、ポート番号は1494に設定されています。

有効なポート番号は0～65535の範囲内である必要があり、他のよく知られているポート番号と競合してはなりません。ポート番号を変更した場合は、新しい値を有効にするためにサーバーを再起動してください。サーバーのポート番号を変更した場合は、サーバーに接続するすべてのCitrix Workspace™アプリまたはプラグインでも変更する必要があります。

キーボードと入力方式エディター (IME)

この設定は、次の項目を有効または無効にします。

- 動的キーボードレイアウト同期
- 入力方式エディター (IME)
- Unicode キーボードレイアウトマッピング
- キーボードレイアウト切り替え通知ダイアログメッセージを非表示または表示します

1. Web Studioで、**キーボードとIME**を選択します。

2. VDAでの動的なキーボードレイアウト同期と汎用クライアント入力方式エディター (IME) 機能を制御するには、**クライアントキーボードレイアウトの同期とIMEの改善**を選択します。設定できる項目は次のとおりです。

   無効 - 動的なキーボードレイアウト同期と汎用クライアント入力方式エディター (IME)。

   動的なクライアントキーボードレイアウト同期をサポート - 動的なキーボードレイアウト同期を有効にします。

   動的なクライアントキーボードレイアウト同期とIMEの改善をサポート - 動的なキーボードレイアウト同期と汎用クライアント入力方式エディター (IME) の両方を有効にします。

3. Unicodeキーボードマッピングを有効または無効にするには、**Unicodeキーボードレイアウトマッピングを有効にする**を選択します。
4. ユーザーがクライアントキーボードレイアウトを変更したときに、キーボードレイアウトが同期中であることを示すメッセージを表示するかどうかを制御するには、**キーボードレイアウト切り替えポップアップメッセージボックスを非表示にする**を選択します。メッセージが表示されないようにすると、ユーザーは誤った文字入力にならないように、入力する前に数秒待つ必要があります。

デフォルト設定：

- **クライアントキーボードレイアウトの同期とIMEの改善**
  - Windows Server 2016およびWindows Server 2019では無効。
  - Windows Server 2012およびWindows 2010では、動的なクライアントキーボードレイアウト同期とIMEの改善をサポート。
- **Unicodeキーボードレイアウトマッピングを無効にする**
- **キーボードレイアウト切り替えポップアップメッセージボックスを表示する**

このポリシーは、ポリシー設定の**説明**セクションに記載されているレジストリ設定を置き換えます。

ログオフチェッカーの起動遅延

この設定は、ログオフチェッカーの起動を遅延させる期間を指定します。このポリシーを使用して、クライアントセッションがセッションを切断するまでに待機する時間（秒単位）を設定します。

この設定は、ユーザーがサーバーからログオフするのにかかる時間も増加させます。

ロス許容モード

重要:

- この機能には、Windows 用 Citrix Workspace アプリ 2002 以降が必要です。VDA のこのバージョンは、利用可能になった時点でこれをサポートします。
- グラフィックのロス許容モードは、Citrix Gateway または Citrix Gateway Service ではサポートされていません。このモードは、直接接続でのみ利用可能です。

この設定は、グラフィックのロス許容モードを有効または無効にします。

デフォルトでは、グラフィックのロス許容モードは**許可**されています。

許可されている場合、パケット損失と遅延がしきい値を超えると、このモードに入ります。しきい値は、ロス許容しきい値ポリシーを使用して設定できます。

ロス許容しきい値

ロス許容モードが利用可能な場合、この設定は、セッションがグラフィックのロス許容モードに切り替わるネットワークメトリックのしきい値を指定します。

デフォルトのしきい値は次のとおりです。

- パケット損失: 5%
- 遅延: 300 ms (RTT)

詳細については、損失許容モードを参照してください。

オーディオのロス許容モード

この設定は、オーディオの損失許容モードを有効または無効にします。

有効にすると、オーディオは損失許容モードで送信されます。

デフォルトでは、オーディオの損失許容モードは**禁止**されています。

ポリシーを有効にするには、オーディオポリシーの損失許容モードのレジストリを**許可**に編集します。

オーディオの損失許容モードを有効にするには、EDTトランスポートが必要です。

Rendezvous プロトコル

この設定は、Citrix Gateway Serviceを使用する際のHDXセッションのプロキシ方法を変更します。有効にすると、HDXトラフィックはCitrix Cloud Connectorを経由しなくなります。代わりに、VDAはCitrix Gateway Serviceに直接アウトバウンド接続を確立します（Cloud Connectorのスケーラビリティが向上します）。

> **重要:**
>
> Citrix Cloud™の機能トグルとHDXポリシー設定がこの機能を制御します。Citrix Cloudの機能トグルはデフォルトで有効になっていますが、HDX設定はデフォルトで無効になっています。HDX設定は、Citrix Gateway Serviceを介して確立されたHDXセッションにのみ影響します。この設定は、クライアントとVDA間で直接確立されたセッションや、オンプレミスのCitrix Gatewayを介して確立されたセッションには影響しません。

> 詳細については、Rendezvousプロトコルを参照してください。

Rendezvousプロキシ構成

この設定により、Rendezvousプロトコルで使用する明示的なプロキシを構成できます。透過型プロキシを使用している場合、この設定を有効にする必要はありません。

デフォルトでは、この設定は無効になっています。

無効にすると、VDAはGateway ServiceとのRendezvous接続を確立しようとするときに、非透過型プロキシを介してアウトバウンドトラフィックをルーティングしません。

有効にすると、VDAはこの設定で定義されたプロキシを介してGateway ServiceとのRendezvous接続を確立しようとします。

VDAは、Rendezvous接続にHTTPおよびSOCKS5プロキシの使用をサポートしています。Rendezvous接続にプロキシを使用するようにVDAを構成するには、この設定を有効にする必要があります。また、プロキシのアドレスまたはPACファイルへのパスを指定します。例：

- プロキシアドレス: `http://<URL or IP>:<port>` または `socks5://<URL or IP>:<port>`
- PACファイル: `http://<URL or IP>/<path>/<filename>.pac`

  VDAバージョン2103は、PACファイルを使用したプロキシ構成でサポートされる最小バージョンです。SOCKS5プロキシのPACファイルスキーマの詳細については、「プロキシ構成」を参照してください。

> **注：**
>
> SOCKS5プロキシのみがEDTを介したデータ転送をサポートします。HTTPプロキシの場合は、ICAのトランスポートプロトコルとしてTCPを使用してください。

> 詳細については、「Rendezvousプロトコル」を参照してください。

クライアント接続中の非公開プログラムの起動

この設定は、サーバー上でRDPを介して初期アプリケーションの起動を許可するかどうかを指定します。

デフォルトでは、サーバー上でRDPを介して初期アプリケーションの起動は許可されていません。

タブレットモード切り替えポリシー設定

タブレットモードの切り替えは、VDA上のストアアプリ、Win32アプリ、およびWindowsシェルを最適化します。これは、電話やタブレットなどの小型デバイス、またはタッチ対応デバイスから接続する際に、仮想デスクトップを自動的にタブレットモードに切り替えることで実現されます。

このポリシーが無効になっている場合、VDAはユーザーが設定したモードになり、クライアントの種類に関係なく、そのモードを維持します。

自動クライアント再接続ポリシー設定

自動クライアント再接続セクションには、セッションの自動再接続を制御するためのポリシー設定が含まれています。

自動クライアント再接続

この設定は、接続が中断された後に同じクライアントによる自動再接続を許可または禁止します。

Citrix Receiver for Windows 4.7以降およびCitrix Workspaceアプリ1808以降では、自動クライアント再接続はCitrix Studioからのポリシー設定のみを使用します。Studioでこれらのポリシーを更新すると、自動クライアント再接続がサーバーからクライアントに同期されます。以前のバージョンのCitrix Receiver for Windowsで自動クライアント再接続を構成するには、Studioポリシーを使用し、レジストリまたはdefault.icaファイルを変更します。

自動クライアント再接続を許可すると、接続が切断されたときに中断された場所からユーザーが作業を再開できるようになります。自動再接続は、切断された接続を検出し、ユーザーをセッションに再接続します。

セッションIDと資格情報へのキーを含むCitrix Workspace™アプリのCookieが使用されない場合、自動再接続によって新しいセッションが開始される可能性があります。つまり、既存のセッションに再接続するのではなく、新しいセッションが開始されます。Cookieは、有効期限が切れている場合は使用されません。たとえば、再接続の遅延や、資格情報の再入力が必要な場合などにCookieの有効期限が切れることがあります。ユーザーが意図的に切断した場合、自動クライアント再接続はトリガーされません。

再接続が進行中の場合、セッションウィンドウはグレー表示されます。カウントダウンタイマーは、セッションが再接続されるまでの残り時間を表示します。セッションがタイムアウトすると、切断されます。

アプリケーションセッションの場合、自動再接続が許可されていると、通知領域にカウントダウンタイマーが表示されます。このタイマーは、セッションが再接続されるまでの残り時間を指定します。Citrix Workspaceアプリは、再接続が成功するか、ユーザーが再接続の試行をキャンセルするまで、セッションへの再接続を試みます。

ユーザーセッションの場合、自動再接続が許可されていると、Citrix Workspaceアプリは、再接続が成功するか、ユーザーが再接続の試行をキャンセルしない限り、指定された期間セッションへの再接続を試みます。デフォルトでは、この期間は2分です。この期間を変更するには、ポリシーを編集します。

デフォルトでは、自動クライアント再接続は許可されています。ポリシーを**禁止**に設定することで無効にできます。

自動クライアント再接続認証

この設定は、自動クライアント再接続に認証が必要かどうかを指定します。

ユーザーが最初にログオンすると、資格情報は暗号化され、メモリに保存され、暗号化キーを含むCookieが作成されます。このCookieはCitrix Workspaceアプリに送信されます。この設定が構成されている場合、Cookieは使用されません。代わりに、Citrix Workspaceアプリが自動的に再接続を試みるときに、資格情報を要求するダイアログボックスがユーザーに表示されます。

デフォルトでは、認証は不要です。

自動クライアント再接続ログ

この設定は、イベントログへの自動クライアント再接続の記録を有効または無効にします。

ログ記録が有効な場合、サーバーのシステムログは、成功および失敗した自動再接続イベントに関する情報をキャプチャします。サイトは、すべてのサーバーの再接続イベントの結合されたログを提供しません。

デフォルトでは、ログ記録は無効です。

自動クライアント再接続のタイムアウト

デフォルトでは、自動クライアント再接続のタイムアウトは120秒に設定されており、自動クライアント再接続のタイムアウトの最大設定可能値は300秒です。このポリシーを使用してタイムアウト値を設定します。

再接続UIの透明度レベル

この設定により、セッションの信頼性再接続中にXenAppまたはXenDesktop®セッションウィンドウに適用される不透明度レベルを指定できます。

デフォルトでは、再接続UIの透明度は80%に設定されています。

オーディオポリシー設定

オーディオセクションには、パフォーマンスを低下させることなく、ユーザーデバイスがセッションでオーディオを送受信できるようにするポリシー設定が含まれています。

アダプティブオーディオ

この設定は、アダプティブオーディオを有効または無効にします。このポリシーを有効にすると、最高のユーザーエクスペリエンスを提供するためにオーディオ品質設定が動的に調整されます。この設定は、Citrix Virtual Apps and Desktops™ 2109以降を使用するVDAのシングルセッションOSおよびマルチセッションOSセッションの両方に適用されます。

この設定が禁止されている場合、オーディオ品質ポリシーが適用されます。詳細については、「オーディオ品質」を参照してください。

デフォルトでは、アダプティブオーディオポリシーは有効になっています。

UDPリアルタイムトランスポート経由のオーディオ

この設定は、User Datagram Protocol (UDP) を使用してRTP経由でVDAとユーザーデバイス間でオーディオを送受信することを許可または禁止します。この設定が無効になっている場合、オーディオはTCP経由で送受信されます。

デフォルトでは、UDP経由のオーディオは許可されています。

オーディオプラグアンドプレイ

この設定は、複数のオーディオデバイスを使用してサウンドを録音および再生することを許可または禁止します。

デフォルトでは、複数のオーディオデバイスの使用は許可されています。

この設定は、WindowsマルチセッションOSマシンにのみ適用されます。

オーディオ品質

この設定は、ユーザーセッションで受信されるサウンドの品質レベルを指定します。

デフォルトでは、サウンド品質は「高 - 高精細オーディオ」に設定されています。

サウンド品質を制御するには、次のいずれかのオプションを選択します。

- 低帯域幅接続の場合は、「低 - 低速接続用」を選択します。ユーザーデバイスに送信されるサウンドは最大16 Kbpsに圧縮されます。この圧縮により、サウンドの品質は大幅に低下しますが、低帯域幅接続でも適切なパフォーマンスが得られます。
- 「中」を選択 - 音声に最適化されており、Voice over Internet Protocolアプリケーションを提供します。この設定は、512 Kbps未満の回線、または著しい輻輳やパケット損失があるような、困難なネットワーク接続でメディアアプリケーションを提供します。このコーデックはエンコード時間が速いため、サーバー側のメディア処理が必要な場合に、ソフトフォンやユニファイドコミュニケーションアプリケーションでの使用に最適です。

  ユーザーデバイスに送信されるオーディオは、最大64 Kbpsに圧縮されます。この圧縮により、ユーザーデバイスで再生されるオーディオの品質は中程度に低下しますが、低遅延で低帯域幅の消費を実現します。Voice over Internet Protocolの品質が不十分な場合は、「Audio over UDP Real-time Transport」ポリシー設定が「許可」に設定されていることを確認してください。

  現在、UDP経由のリアルタイムトランスポート（RTP）は、このオーディオ品質が選択されている場合にのみサポートされます。低速（512 Kbps未満）回線のような困難なネットワーク接続でメディアアプリケーションを配信する場合でも、このオーディオ品質を使用してください。また、ネットワークに輻輳やパケット損失がある場合も同様です。
- 「高」を選択 - 帯域幅が豊富で音質が重要な接続には、高精細オーディオを使用します。クライアントはネイティブレートでサウンドを再生できます。サウンドはCD品質まで維持される高音質レベルで圧縮され、最大112 Kbpsの帯域幅を使用します。この量のデータを送信すると、CPU使用率が増加し、ネットワークが輻輳する可能性があります。

帯域幅は、オーディオの録音中または再生中にのみ消費されます。両方が同時に発生する場合、帯域幅の消費量は2倍になります。

最大帯域幅を指定するには、**オーディオリダイレクト帯域幅制限**または**オーディオリダイレクト帯域幅制限率**の設定を構成します。

クライアントオーディオリダイレクト

この設定は、サーバーでホストされているアプリケーションが、ユーザーデバイスにインストールされているサウンドデバイスを介してサウンドを再生できるかどうかを指定します。この設定は、ユーザーがオーディオ入力を録音できるかどうかも指定します。

デフォルトでは、オーディオリダイレクトは許可されています。

この設定を許可した後、オーディオの再生または録音によって消費される帯域幅を制限できます。オーディオによって消費される帯域幅の量を制限すると、アプリケーションのパフォーマンスが向上する可能性がありますが、オーディオ品質が低下する可能性もあります。帯域幅は、オーディオの録音中または再生中にのみ消費されます。両方が同時に発生する場合、帯域幅の消費量は2倍になります。最大帯域幅を指定するには、**オーディオリダイレクト帯域幅制限**または**オーディオリダイレクト帯域幅制限率**の設定を構成します。

WindowsマルチセッションOSマシンでは、複数のオーディオデバイスをサポートするために、**オーディオプラグアンドプレイ**設定が有効になっていることを確認してください。

重要：クライアントオーディオリダイレクトを禁止すると、すべてのHDX™オーディオ機能が無効になります。

クライアントマイクのリダイレクト

この設定は、クライアントマイクのリダイレクトを有効または無効にします。有効にすると、ユーザーはセッションでマイクを使用してオーディオ入力を録音できます。

デフォルトでは、マイクのリダイレクトは許可されています。

セキュリティのため、デバイスによって信頼されていないサーバーがマイクにアクセスしようとすると、ユーザーに警告が表示されます。ユーザーはアクセスを許可するかどうかを選択できます。ユーザーはCitrix Workspace™アプリで警告を無効にできます。

WindowsマルチセッションOSマシンでは、複数のオーディオデバイスをサポートするために、オーディオプラグアンドプレイ設定が有効になっていることを確認してください。

ユーザーデバイスで**クライアントオーディオリダイレクト**設定が無効になっている場合、このルールは無効になります。

帯域幅ポリシー設定

「**帯域幅**」セクションには、クライアントセッションの帯域幅使用に関連するパフォーマンスの問題を回避するためのポリシー設定が含まれています。

重要: これらのポリシー設定を**マルチストリームポリシー**設定と併用すると、予期しない結果が生じる可能性があります。ポリシーでマルチストリーム設定を使用する場合は、これらの帯域幅制限ポリシー設定が含まれていないことを確認してください。

オーディオリダイレクト帯域幅制限

この設定は、ユーザーセッションでオーディオを再生または録音するために許可される最大帯域幅を指定します。許可される最大帯域幅は、1秒あたりのキロビット単位で指定されます。

デフォルトでは、最大値（ゼロ）は指定されていません。

この設定に値を入力し、**オーディオリダイレクト帯域幅制限の割合**設定に値を入力した場合、最も制限の厳しい設定（小さい方の値）が適用されます。

オーディオリダイレクトの帯域幅制限（パーセント）

この設定は、オーディオの再生または録音に許可される最大帯域幅制限を、セッションの総帯域幅に対する割合として指定します。

デフォルトでは、最大値（ゼロ）は指定されていません。

この設定に値を入力し、**オーディオリダイレクト帯域幅制限**設定に値を入力した場合、最も制限の厳しい設定（小さい方の値）が適用されます。

この設定を構成する場合、クライアントセッションで利用可能な帯域幅の総量を指定する**セッション全体の帯域幅制限**設定も構成する必要があります。

クライアントUSBデバイスリダイレクト帯域幅制限

この設定は、USBデバイスのクライアントとの間のリダイレクトに許可される最大帯域幅を指定します。許可される最大帯域幅は、1秒あたりのキロビット単位で指定されます。

デフォルトでは、最大値（ゼロ）は指定されていません。

この設定に値を入力し、**クライアントUSBデバイスリダイレクト帯域幅制限の割合**設定に値を入力した場合、最も制限の厳しい設定（小さい方の値）が適用されます。

クライアントUSBデバイスリダイレクトの帯域幅制限（パーセント）

この設定は、クライアントとの間でUSBデバイスをリダイレクトするために許可される最大帯域幅を、セッションの総帯域幅に対する割合として指定します。

デフォルトでは、最大値（ゼロ）は指定されていません。

この設定に値を入力し、**クライアントUSBデバイスリダイレクト帯域幅制限**設定にも値を入力した場合、最も制限の厳しい設定（小さい方の値）が適用されます。

この設定を構成する場合、クライアントセッションで利用可能な帯域幅の総量を指定する**セッション全体の帯域幅制限**設定も構成する必要があります。

クリップボードリダイレクト帯域幅制限

この設定は、セッションとローカルクリップボード間のデータ転送に許可される最大帯域幅を指定します。許可される最大帯域幅は、キロビット/秒で指定されます。

デフォルトでは、最大値（ゼロ）は指定されていません。

この設定に値を入力し、**クリップボードリダイレクト帯域幅制限（パーセント）**設定にも値を入力した場合、最も制限の厳しい設定（小さい方の値）が適用されます。

クリップボードリダイレクトの帯域幅制限（パーセント）

この設定は、セッションとローカルクリップボード間のデータ転送に許可される最大帯域幅を、セッションの総帯域幅に対する割合として指定します。

デフォルトでは、最大値（ゼロ）は指定されていません。

この設定に値を入力し、**クリップボードリダイレクト帯域幅制限**設定にも値を入力した場合、最も制限の厳しい設定（小さい方の値）が適用されます。

この設定を構成する場合、クライアントセッションで利用可能な帯域幅の総量を指定する**セッション全体の帯域幅制限**設定も構成する必要があります。

COMポートリダイレクトの帯域幅制限

注：Virtual Delivery Agent 7.0から7.8の場合、この設定はレジストリを使用して構成します。詳細については、「レジストリを使用したCOMポートおよびLPTポートリダイレクト設定の構成」を参照してください。

この設定は、クライアント接続でCOMポートにアクセスするために許可される最大帯域幅をキロビット/秒で指定します。この設定に値を入力し、**COMポートリダイレクト帯域幅制限（パーセント）**設定にも値を入力した場合、最も制限の厳しい設定（小さい方の値）が適用されます。

COMポートリダイレクトの帯域幅制限（パーセント）

注：Virtual Delivery Agent 7.0から7.8の場合、この設定はレジストリを使用して構成します。詳細については、「レジストリを使用したCOMポートおよびLPTポートリダイレクト設定の構成」を参照してください。

この設定は、クライアント接続でCOMポートにアクセスするために許可される最大帯域幅を、セッションの総帯域幅に対する割合として指定します。

デフォルトでは、最大値（ゼロ）は指定されていません。

この設定に値を入力し、**COMポートリダイレクト帯域幅制限**設定に値を入力した場合、最も制限の厳しい設定（小さい方の値）が適用されます。

この設定を構成する場合、クライアントセッションで利用可能な総帯域幅を指定する**セッション全体の帯域幅制限**設定も構成する必要があります。

ファイルリダイレクト帯域幅制限

この設定は、ユーザーセッションでクライアントドライブにアクセスするために許可される最大帯域幅を指定します。許可される最大帯域幅は、キロビット/秒で指定されます。

デフォルトでは、最大値（ゼロ）は指定されていません。

この設定に値を入力し、**ファイルリダイレクト帯域幅制限の割合**設定に値を入力した場合、最も制限の厳しい設定（小さい方の値）が適用されます。

ファイルリダイレクトの帯域幅制限（パーセント）

この設定は、クライアントドライブにアクセスするために許可される最大帯域幅制限を、セッションの総帯域幅に対する割合として指定します。

デフォルトでは、最大値（ゼロ）は指定されていません。

この設定に値を入力し、**ファイルリダイレクト帯域幅制限**設定に値を入力した場合、最も制限の厳しい設定（小さい方の値）が適用されます。

この設定を構成する場合、クライアントセッションで利用可能な総帯域幅を指定する**セッション全体の帯域幅制限**設定も構成する必要があります。

HDX™ MediaStream マルチメディアアクセラレーション帯域幅制限

この設定は、HDX MediaStream マルチメディアアクセラレーションを使用してストリーミングオーディオおよびビデオを配信するために許可される最大帯域幅制限を指定します。許可される最大帯域幅は、キロビット/秒で指定されます。

デフォルトでは、最大値（ゼロ）は指定されていません。

この設定と**HDX MediaStream Multimedia Acceleration帯域幅制限パーセント**設定の両方に値を入力した場合、最も制限の厳しい設定（小さい方の値）が適用されます。

HDX MediaStream Multimedia Acceleration帯域幅制限パーセント

この設定は、HDX MediaStream Multimedia Accelerationを使用してストリーミングオーディオおよびビデオを配信するために許可される最大帯域幅を、セッションの総帯域幅に対する割合として指定します。

デフォルトでは、最大値（ゼロ）は指定されていません。

この設定と**HDX MediaStream Multimedia Acceleration帯域幅制限**設定の両方に値を入力した場合、最も制限の厳しい設定（小さい方の値）が適用されます。

この設定を構成する場合、クライアントセッションで利用可能な帯域幅の総量を指定する**セッション全体の帯域幅制限**設定も構成する必要があります。

LPTポートリダイレクト帯域幅制限

注：Virtual Delivery Agent 7.0から7.8の場合、この設定はレジストリを使用して構成します。詳細については、「レジストリを使用したCOMポートおよびLPTポートリダイレクト設定の構成」を参照してください。

この設定は、単一ユーザーセッションでLPTポートを使用する印刷ジョブに許可される最大帯域幅を指定します。許可される最大帯域幅は、キロビット/秒で指定されます。

デフォルトでは、最大値（ゼロ）は指定されていません。

この設定と**LPTポートリダイレクト帯域幅制限パーセント**設定の両方に値を入力した場合、最も制限の厳しい設定（小さい方の値）が適用されます。

LPTポートリダイレクトの帯域幅制限（パーセント）

注：Virtual Delivery Agent 7.0から7.8の場合、この設定はレジストリを使用して構成します。詳細については、「レジストリを使用したCOMポートおよびLPTポートリダイレクト設定の構成」を参照してください。

この設定は、単一クライアントセッションでLPTポートを使用する印刷ジョブの帯域幅制限を、セッションの総帯域幅に対する割合として指定します。

デフォルトでは、最大値（ゼロ）は指定されていません。

この設定と**LPTポートリダイレクト帯域幅制限**設定の両方に値を入力した場合、最も制限の厳しい設定（小さい方の値）が適用されます。

この設定を構成する場合、クライアントセッションで利用可能な帯域幅の総量を指定する**セッション全体の帯域幅制限**設定も構成する必要があります。

セッション全体の帯域幅制限

この設定は、ユーザーセッションで利用可能な総帯域幅を、1秒あたりのキロビット単位で指定します。

適用可能な最大帯域幅の上限は20 Mbps (20,000 Kbps)です。デフォルトでは、最大値（ゼロ）は指定されていません。

クライアント接続によって消費される帯域幅の量を制限すると、クライアント接続外の他のアプリケーションが限られた帯域幅を競合している場合に、パフォーマンスが向上する可能性があります。

プリンターリダイレクト帯域幅制限

この設定は、ユーザーセッションでクライアントプリンターにアクセスするために許可される最大帯域幅を指定します。許可される最大帯域幅は、1秒あたりのキロビット単位で指定されます。

デフォルトでは、最大値（ゼロ）は指定されていません。

この設定に値を入力し、**Printer redirection bandwidth limit percent** 設定に値を入力した場合、最も制限の厳しい設定（小さい方の値）が適用されます。

プリンターリダイレクトの帯域幅制限（パーセント）

この設定は、クライアントプリンターにアクセスするために許可される最大帯域幅を、総セッション帯域幅の割合として指定します。

デフォルトでは、最大値（ゼロ）は指定されていません。

この設定に値を入力し、**Printer redirection bandwidth limit** 設定に値を入力した場合、最も制限の厳しい設定（小さい方の値）が適用されます。

この設定を構成する場合、クライアントセッションで利用可能な総帯域幅を指定する**Overall session bandwidth limit** 設定も構成する必要があります。

TWAINデバイスリダイレクト帯域幅制限

この設定は、公開アプリケーションからTWAINイメージングデバイスを制御するために許可される最大帯域幅を指定します。許可される最大帯域幅は、1秒あたりのキロビット単位で指定されます。

デフォルトでは、最大値（ゼロ）は指定されていません。

この設定に値を入力し、**TWAIN device redirection bandwidth limit percent** 設定に値を入力した場合、最も制限の厳しい設定（小さい方の値）が適用されます。

TWAINデバイスリダイレクト帯域幅制限の割合

この設定は、公開アプリケーションからTWAINイメージングデバイスを制御するために許可される最大帯域幅を、セッションの総帯域幅に対する割合として指定します。

デフォルトでは、最大値（ゼロ）は指定されていません。

この設定に値を入力し、**TWAIN device redirection bandwidth limit** 設定にも値を入力した場合、最も制限の厳しい設定（値が小さい方）が適用されます。

この設定を構成する場合、クライアントセッションで利用可能な帯域幅の総量を指定する**Overall session bandwidth limit** 設定も構成する必要があります。

双方向コンテンツリダイレクトポリシー設定

「**双方向コンテンツリダイレクト**」セクションには、クライアントからVDAへのURLリダイレクトとVDAからクライアントへのURLリダイレクトを有効または無効にするポリシー設定があります。

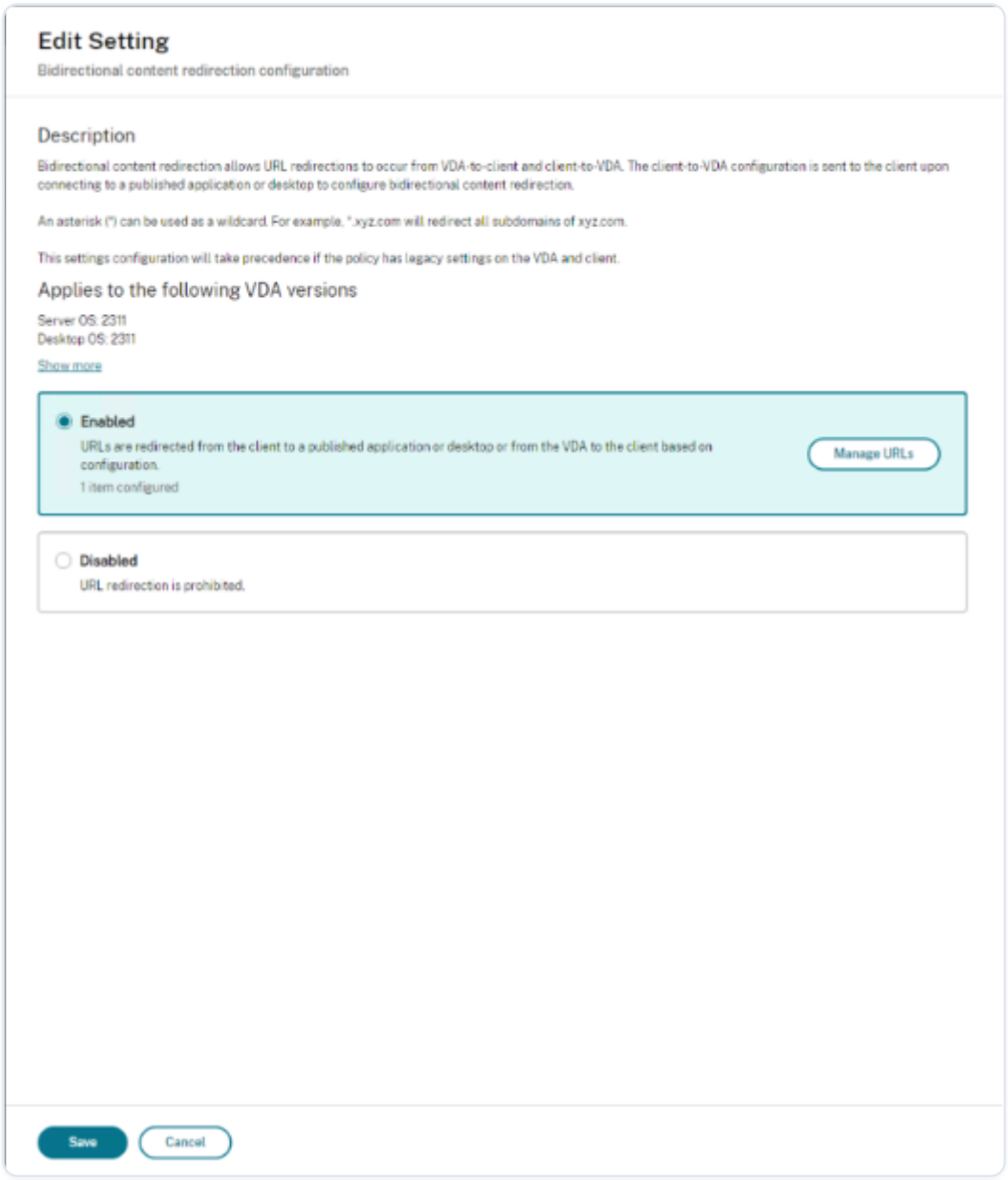
サーバーポリシーはWeb Studioで設定されます。Citrix Workspace™アプリバージョン2311以降、この設定は、Web Studioで非推奨となった以下の3つのレガシー設定に代わるものです。

- 双方向コンテンツリダイレクトを許可する
- VDAにリダイレクトされる許可されたURL
- クライアントにリダイレクトされる許可されたURL

また、Windowsクライアント上の以下の3つのローカルGroup Policy Object (GPO) 設定も置き換えます。

- 双方向コンテンツリダイレクト
- 双方向コンテンツリダイレクトのオーバーライド
- OAuthリダイレクト

この設定が有効になっている場合、公開されたアプリまたはデスクトップに接続すると、双方向コンテンツリダイレクトを構成するためのクライアントからVDAへの設定がクライアントに送信されます。



この設定が構成されている場合、Web Studioおよびクライアントのレガシー設定よりも優先されます。Citrix®は、予期しない動作を避けるために、新しいポリシー設定のみを使用し、レガシー設定を削除することを推奨します。

VDAとDDCがバージョン2311以降を実行している場合、クライアントポリシーを設定してはなりません。そうでない場合、クライアントポリシーはCitrix WorkspaceアプリのGroup Policy Object管理テンプレートから設定されます。

Citrixは、ホストからクライアントへのリダイレクトと、クライアントからURLへのリダイレクトのためのLocal App Accessを提供しています。ただし、Citrixは、ドメイン参加済みWindowsクライアントには双方向コンテンツリダイレクトを使用することを推奨しています。

Citrixは、Desktop Studioではなく、Web Studioの新しいUIを使用してこの機能を構成することを推奨しています。

ワイルドカードリダイレクト

双方向コンテンツリダイレクトは、リダイレクトするURLを定義する際にワイルドカードの使用をサポートしています。詳細および双方向コンテンツリダイレクトの構成については、構成の手順を参照してください。 Web Studioで、`hostToClientUrls`配列または`clientToHostUrls`配列内の`url`キーの値としてJSON文字列を編集して、ワイルドカードURLを設定します。

> **注:**
>
> - 無限ループを避けるため、`hostToClientUrls`と`clientToHostUrls`に同じURLを設定しないでください。
> - トップレベルドメインはサポートされていません。たとえば、`<https://www.citrix.*>`や`<http://www.citrix.co*>`はリダイレクトされません。

双方向コンテンツリダイレクトの構成

このポリシーを`Enabled`に設定して機能の構成を開始し、**Manage URLs**をクリックします。次の構成を設定します。

- **VDAからクライアントへのリダイレクト**
- **クライアントからVDAへのリダイレクト**

VDAからクライアントへのリダイレクト

VDAからクライアントにURLをリダイレクトするには、1行に1つのURLを入力します。ワイルドカードを使用できます。 OAuthリダイレクトを使用すると、クライアントエンドポイントのブラウザーを使用して認証を実行し、トークンをVDAに送り返すことができます。

利点:

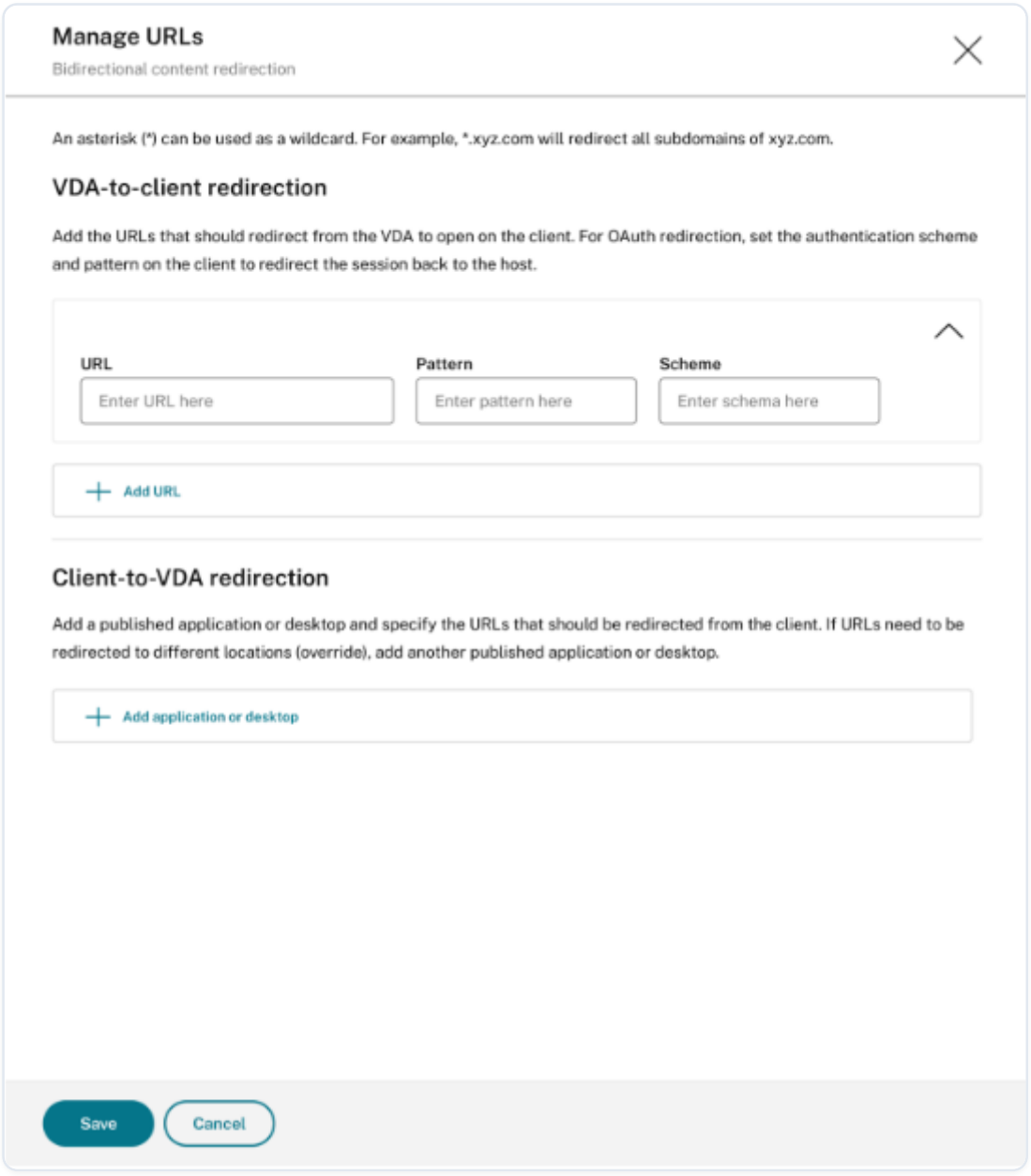
- これらの資格情報をホスト環境に保存しないようにできます。
- エンドポイントで利用可能で、VDAでは利用できない生体認証機能を使用できます。

構成：

URLのVDAからクライアントへのリダイレクトを構成するには、以下を指定します。

- **URL**（必須）VDAからリダイレクトしてクライアントで開く必要があるURLを追加します。**OAuthリダイレクト**の場合、セッションをホストにリダイレクトするように、クライアントで認証スキームとパターンを設定します。

- **パターン**：（オプション）VDAからクライアントへのURLリダイレクトを介してクライアントにリダイレクトされたときに、OAuth認証フローが開始されたかのように追跡され、フローが完了したとき（結果のスキームまたはリダイレクトURLパターンが開かれたことによって検出される）、その結果のURLがそのフローを開始したホストVDAにリダイレクトされるURL正規表現。
- **スキーム**：（オプション）**スキーム**が指定されている場合、終了URLは`<scheme>`://`<something>`の形式であると想定されます。スキームが指定されていない（空である）とします。その場合、元の結果のURLパターンは、正規表現キャプチャグループ（パターンで指定する必要がある）を介してパターンから抽出され、元のURLは`citrix-oauth-redir://`リダイレクトURLを使用するように書き換えられます。フローが完了すると、元のリダイレクトURLはホスト（VDA）にリダイレクトされます。この場合、OAuth認証サーバーは`citrix-oauth-redir://byIndex/1 (2, 3, ... N)`リダイレクトURLを許可するように構成する必要があります。



注：

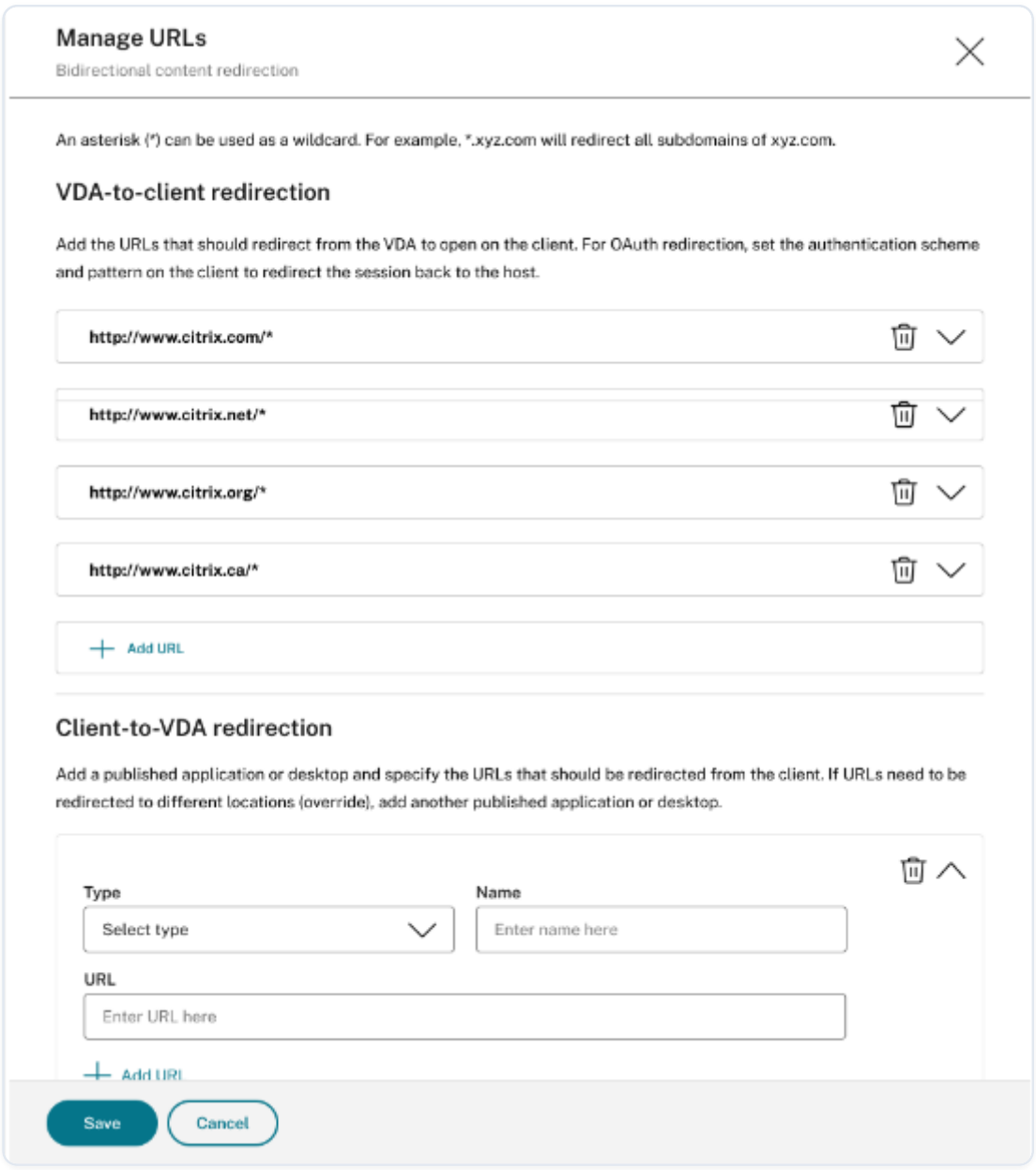
パターンと**スキーム**はどちらもオプションですが、**パターン**が指定されている場合は、**スキーム**も指定する必要があります。

クライアントからVDAへのリダイレクト

クライアントからVDAにURLをリダイレクトするには、次の手順を実行します。

1. クライアントURLの宛先を構成します。
2. 公開アプリケーションまたは公開デスクトップのいずれかを選択します。
3. そのリソースの名前を指定します。

4. そのリソースにリダイレクトする必要があるすべてのURLを追加します。 新しいアプリケーションまたはデスクトップを追加し、そのリソースにリダイレクトするURLを指定することで、このデフォルトのリソースを上書きできます。



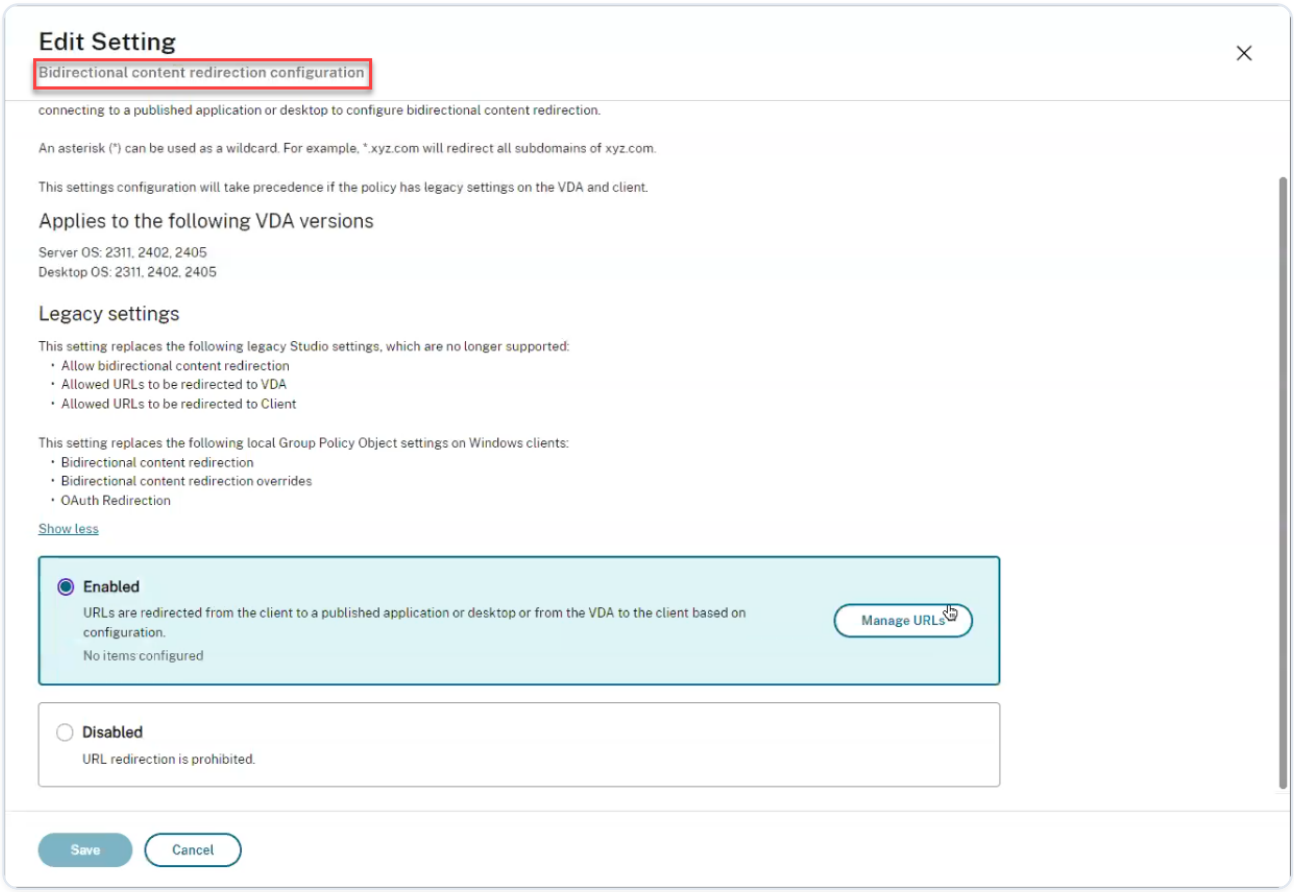
デスクトップスタジオ

> **注：**
>
> Citrixは、Citrix Virtual Apps and Desktops™バージョン2402以降、この機能を構成するためにWeb Studioを使用することを推奨します。

2311の双方向コンテンツリダイレクトを構成するには、次の形式でJSON文字列を作成します。

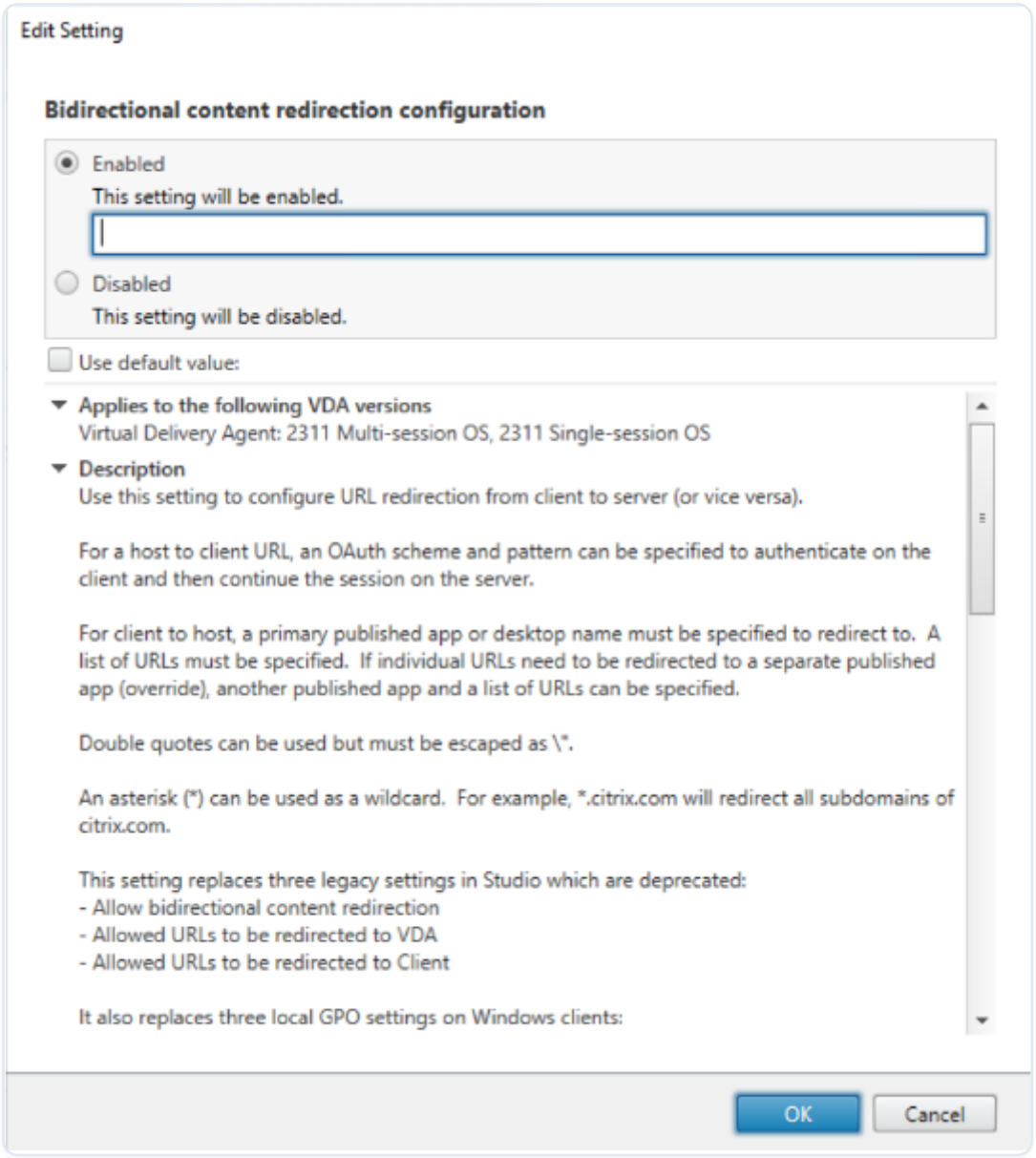
```
{
  "version": 1,
  "hostToClientConfig": [
    {
      "hostToClientUrls": [
        {
          "url": "http://www.citrix.com/*"
        },
        {
          "url": "www.example.com"
        },
        {
          "url": "https://login.example.org/*",
          "oAuthRedirectionPattern": "https://login.example.org/
oauth2?.*",
          "oAuthScheme": "idm.desktop-authentication"
        }
      ]
    }
  ],
  "clientToHostConfig": [
```

```
    {
      "publishedAppOrDesktopNameType": "Desktop",
      "publishedAppOrDesktopName": "Win11Desktop",
      "clientToHostUrls": [
        "https://www.example.net",
        "https://*.citrix.example"
      ]
    },
    {
      "publishedAppOrDesktopNameType": "Application",
      "publishedAppOrDesktopName": "Chrome",
      "clientToHostUrls": [
        "https://tibco.example"
      ]
    }
  ]
}
```



次のパラメーターを設定する必要があります。

- **version**: (必須) 1に設定します。
- VDAからクライアントへのURLリダイレクトの場合、単一の`hostToClientConfig`を作成します。
- `hostToClientUrls`: (必須) ホスト（VDA）からクライアントにリダイレクトされるURLのリスト。ワイルドカードが許可されます。`hostToClientConfig`が指定されているが、クライアントからホストVDAへのリダイレクトが不要な場合、`clientToHostConfig`は`publishedAppOrDesktopNameType`、空の`publishedAppOrDesktopName`、および空の`clientToHostUrls`とともに指定する必要があります。



OAuthリダイレクト

OAuthリダイレクトを使用すると、クライアントエンドポイントブラウザを使用して認証し、トークンをVDAに送り返すことができます。

利点：

- これらの資格情報をホストされた環境に保存することを回避できます。
- エンドポイントで利用可能で、VDAでは利用できない生体認証機能を使用できます。

URLのOAuthリダイレクトを構成するには、次のパラメーターを指定します。

- **oAuthRedirectionPattern**: (オプション) VDAからクライアントへのURLリダイレクトを介してクライアントにリダイレクトされたときに、OAuth認証フローが開始されたかのように追跡されるURL正規表現。フローが完了したとき（結果のスキームまたはリダイレクトURLパター

ンが開かれたことによって検出される）、その結果のURLは、そのフローを開始したホストVDAにリダイレクトされます。

- **oAuthScheme**: (オプション) スキームが指定されている場合、終了URLは`<scheme>`://`<something>`の形式であると想定されます。スキームが指定されていない（空である）とします。その場合、元の結果URLパターンは、正規表現キャプチャグループ（パターンで指定する必要がある）を介してパターンから抽出され、元のURLは`citrix-oauth-redir://`リダイレクトURLを使用するように書き換えられます。フローが完了すると、元のリダイレクトURLはホスト（VDA）にリダイレクトされます。この場合、任意のOAuth認証サーバーは、`citrix-oauth-redir://byIndex/1 (2, 3, ... N)`リダイレクトURLを許可するように構成されている必要があります。

クライアントからVDAへのリダイレクトの場合、リダイレクトする各リソースに対して**clientToHostConfig**を作成します。 各リソースには、次のパラメーターを含めます。

- **publishedAppOrDesktopNameType**: (必須) Web Studioで構成された公開デスクトップ（「Desktop」）または公開アプリケーション（「Application」）のいずれか。リソースが無効な場合、リダイレクトは正しく機能しません。
- **publishedAppOrDesktopName**: (必須) Web Studioで構成されたリソース名。
- **clientToHostUrls**: (必須) クライアントからホスト（VDA）にリダイレクトされるURLのリスト。ワイルドカードが許可されます。

既知の制限

PowerShellを使用してカスタムURLスキーム（HTTPまたはHTTPSではない）でブラウザを起動すると、カスタムURLはクライアントにリダイレクトされません。

ブラウザコンテンツリダイレクトポリシー設定

ブラウザコンテンツリダイレクトセクションには、この機能を構成するためのポリシー設定が含まれています。

Browser content redirection controls and optimizes the way Citrix Virtual Apps and Desktops™ deliver any web browser content (for example, HTML5) to users. Only the visible area of the browser where content is displayed is redirected.

HTML5ビデオのリダイレクトとブラウザコンテンツリダイレクトは、独立した機能です。この機能が動作するためにHTML5ビデオのリダイレクトポリシーは必要ありません。ただし、Citrix HDX HTML5 Video Redirection Serviceはブラウザコンテンツリダイレクトに使用されます。詳細については、「ブラウザコンテンツリダイレクト」を参照してください。

> **注：**
>
> Web Studioで利用可能なポリシー設定は、VDA上のレジストリキーで上書きできますが、レジストリキーはオプションです。

TLSとブラウザコンテンツリダイレクト

ブラウザコンテンツリダイレクトを使用して、HTTPS Webサイトをリダイレクトできます。これらのWebサイトに挿入されるJavaScriptは、VDAで実行されているCitrix HDX HTML5 Video Redirection Service（WebSocketService.exe）へのTLS接続を確立する必要があります。このリダイレクトを実現し、WebページのTLS整合性を維持するために、Citrix HDX HTML5 Video Redirection ServiceはVDA上の証明書ストアに2つのカスタム証明書を生成します。

HdxVideo.jsは、セキュアWebソケットを使用して、VDAで実行されているWebSocketService.exeと通信します。このプロセスはローカルシステムで実行され、SSL終端とユーザーセッションマッピングを実行します。

WebSocketService.exeは、127.0.0.1ポート9001でリッスンしています。

ブラウザコンテンツリダイレクト

By default, Citrix Workspace™ app tries client fetch and client render. The server-side rendering is tried when client fetch and client render fail. If you also enable the browser content redirection proxy configuration policy, Citrix Workspace app tries only server fetch and client render.

デフォルトでは、この設定は「許可」です。

ブラウザコンテンツリダイレクトの統合Windows認証サポート設定

ブラウザコンテンツリダイレクトは、認証にNegotiateスキームを使用するオーバーレイを有効にします。この機能強化により、VDAと同じドメイン内で統合Windows認証（IWA）が構成されたWebサーバーへのシングルサインオンが提供されます。

許可に設定すると、ブラウザコンテンツリダイレクトオーバーレイはユーザーのVDA資格情報を使用してNegotiateチケットを取得します。その後、ユーザーはシングルサインオンでWebサーバーに認証されます。

禁止に設定すると、ブラウザコンテンツリダイレクトオーバーレイはVDAからNegotiateチケットを要求しません。ユーザーは基本認証方法を使用してWebサーバーに認証されます。この認証方法では、ユーザーはWebサーバーにアクセスするたびにVDA資格情報を入力する必要があります。

デフォルトでは、この設定は「禁止」です。

ブラウザコンテンツリダイレクトのサーバーフェッチWebプロキシ認証設定

この設定は、オーバーレイで発生するHTTPトラフィックをダウンストリームWebプロキシ経由でルーティングします。ダウンストリームWebプロキシは、VDAユーザーのドメイン資格情報を使用して、Negotiate認証スキームを介してHTTPトラフィックを承認および認証します。

PACファイルで、ブラウザコンテンツリダイレクトプロキシ構成ポリシーを使用して、サーバーフェッチモードのブラウザコンテンツリダイレクトを構成する必要があります。PACスクリプトで、オーバーレイのトラフィックをダウンストリームWebプロキシ経由でルーティングする手順を指定します。その後、ダウンストリームWebプロキシを構成して、Negotiate認証スキームを介してVDAユーザーを認証します。

許可に設定すると、Webプロキシは**Proxy-Authenticate: Negotiate**ヘッダーを含む407 Negotiateチャレンジで応答します。その後、ブラウザコンテンツリダイレクトは、VDAユーザーのドメイン資格情報を使用してKerberosサービスチケットを取得します。また、そのサービスチケットをWebプロキシへの後続のリクエストに含めます。

禁止に設定すると、ブラウザコンテンツリダイレクトは、オーバーレイとWebプロキシ間のすべてのTCPトラフィックを干渉することなくプロキシします。オーバーレイは、基本認証資格情報またはその他の利用可能な資格情報を使用してWebプロキシに認証します。

デフォルトでは、この設定は禁止されています。

ブラウザコンテンツリダイレクトACL（アクセス制御リスト）構成ポリシー設定

この設定を使用して、ブラウザコンテンツリダイレクトを使用できるURL、またはブラウザコンテンツリダイレクトへのアクセスが拒否されるURLのアクセス制御リスト（ACL）を構成します。

承認されたURLとは、コンテンツがクライアントにリダイレクトされる許可リスト内のURLです。

ワイルドカード`*`は許可されていますが、URLのプロトコルまたはドメインアドレス部分では許可されていません。ただし、Citrix Virtual Apps and Desktops 7 2206以降では、ワイルドカード`*`はURLのサブドメインアドレス部分で許可されています。

許可: `http://www.xyz.com/index.html`, `https://www.xyz.com/*`, `http://www.xyz.com/*videos*`, `http://*.xyz.com/`

不許可: `http://*.*.com/`

URLでパスを指定することで、より詳細な制御が可能です。たとえば、`https://www.xyz.com/sports/index.html`を指定した場合、index.htmlページのみがリダイレクトされます。

デフォルトでは、この設定は`https://www.youtube.com/*`に設定されています。

詳細については、Knowledge Centerの記事CTX238236を参照してください。

> **注：**
>
> ACLを構成して、BCRがWebサイトをエンドポイントにリダイレクトすることを許可できます。また、認証サイトは、構成されたURLで使用される認証のために、OktaやDuoなどのIDプロバイダー（IdP）を許可するように構成できます。

ブラウザーコンテンツリダイレクト認証サイト

この設定を使用して、URLのリストを構成します。ブラウザコンテンツリダイレクトを使用してリダイレクトされたサイトは、このリストを使用してユーザーを認証します。この設定は、許可リスト内のURLから移動した場合でも、ブラウザコンテンツリダイレクトがアクティブ（リダイレクトされた状態）のままになるURLを指定します。

典型的なシナリオは、認証に認証プロバイダー (IdP) を利用するWebサイトです。たとえば、Webサイト `www.xyz.com` はエンドポイントにリダイレクトされる必要がありますが、Okta (`www.xyz.okta.com`) のようなサードパーティのIdPが認証部分を処理します。管理者は、ブラウザコンテンツリダイレクトACL構成ポリシーを使用して `www.xyz.com` を許可リストに追加します。次に、ブラウザコンテンツリダイレクト認証サイトを使用して `www.xyz.okta.com` を許可リストに追加します。

詳細については、Knowledge Centerの記事 CTX238236 を参照してください。

ブラウザコンテンツリダイレクトブロックリスト設定

この設定は、ブラウザコンテンツリダイレクトACL構成設定と連携して機能します。ブラウザコンテンツリダイレクトACL構成設定とブロックリスト構成設定の両方にURLが存在する場合を考えます。この場合、ブロックリスト構成が優先され、URLのブラウザコンテンツはリダイレクトされません。

未承認URL: ブラウザコンテンツがクライアントにリダイレクトされず、サーバーでレンダリングされるブロックリスト内のURLを指定します。

ワイルドカード * は許可されていますが、URLのプロトコルまたはドメインアドレス部分内では許可されていません。

許可されるもの: `http://www.xyz.com/index.html`, `https://www.xyz.com/*`, `http://www.xyz.com/*videos*`

不許可: `http://*.xyz.com/`

URLでパスを指定することで、より詳細な粒度を実現できます。たとえば、`https://www.xyz.com/sports/index.html` を指定した場合、index.htmlのみがブロックリストに含まれます。

ブラウザコンテンツリダイレクトプロキシ設定

この設定は、ブラウザコンテンツリダイレクト用のVDA上のプロキシ設定の構成オプションを提供します。有効なプロキシアドレスとポート番号、PAC / WPAD URL、または直接/透過設定で有効になっている場合、Citrix Workspaceアプリはサーバーフェッチとクライアントレンダリングのみを試行します。

無効になっているか、構成されておらず、デフォルト値を使用している場合、Citrix Workspaceアプリはクライアントフェッチとクライアントレンダリングを試行します。

デフォルトでは、この設定は禁止されています。

明示的なプロキシの許可パターン:

`http://<hostname/ip address\>:\<port\>`

例:

`http://proxy.example.citrix.com:80` `http://10.10.10.10:8080`

PAC/WPADファイルの許可パターン:

`http://<hostname/ip address>:<port>/<path>/<Proxy.pac>`

例: `http://wpad.myproxy.com:30/configuration/pac/Proxy.pac`

`https://<hostname/ip address>:<port>/<path>/<wpad.dat>`

例: `http://10.10.10.10/configuration/pac/wpad.dat`

直接プロキシまたは透過プロキシで許可されるパターン:

ポリシーのテキストボックスに「**DIRECT**」と入力します。

ブラウザコンテンツリダイレクトのレジストリキーのオーバーライド

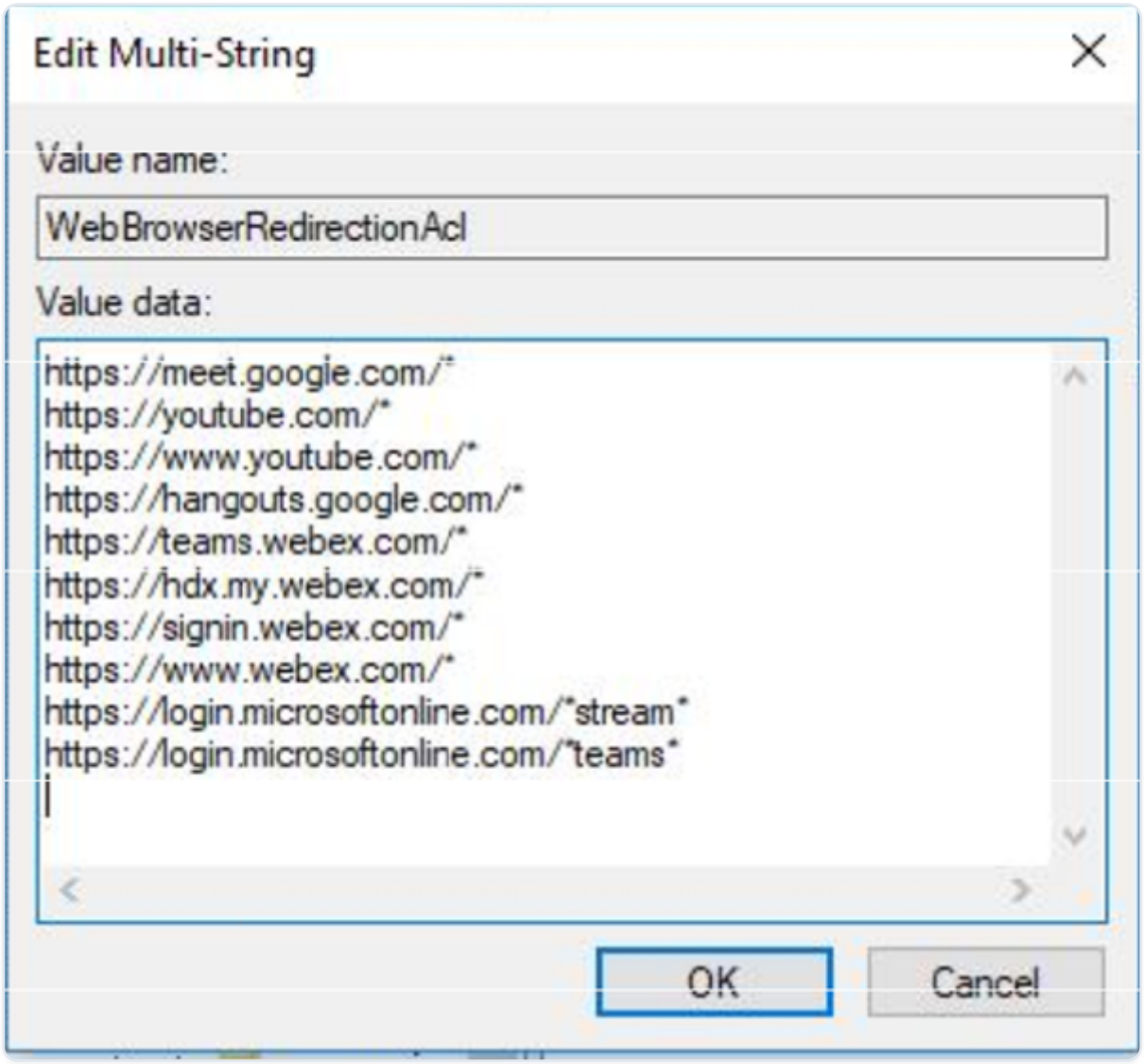
> **警告:**
>
> レジストリを誤って編集すると、オペレーティングシステムの再インストールが必要になるような深刻な問題が発生する可能性があります。Citrix®は、レジストリエディターの誤った

> 使用によって生じる問題が解決できることを保証できません。レジストリエディターの使用は自己責任で行ってください。編集する前に必ずレジストリをバックアップしてください。

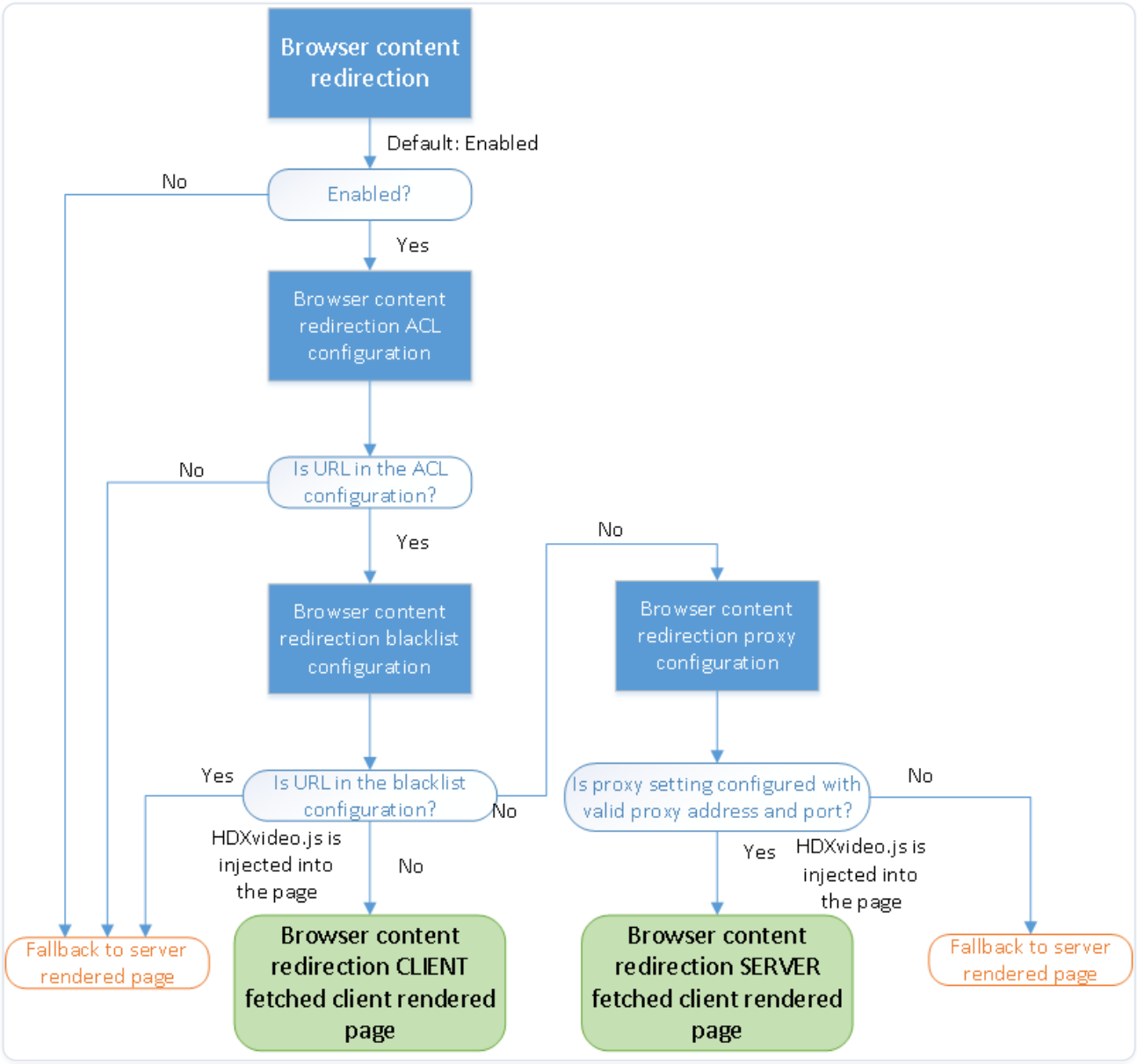
> ポリシー設定のレジストリオーバーライドオプション:

`\HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxMediastream`

名前	タイプ	値
WebBrowserRedirection	DWORD	1=許可, 0=禁止
WebBrowserRedirectionAcl	REG_MULTI_SZ	
WebBrowserRedirectionAuthenticationSites	REG_MULTI_SZ	
WebBrowserRedirectionProxyAddress	REG_SZ	`http://myproxy.citrix.com:8080` または `http://10.10.10.10:8888`
WebBrowserRedirectionBlacklist	REG_MULTI_SZ	


Edit Multi-String
Value name:
WebBrowserRedirectionAcl
Value data:
https://meet.google.com/*
https://youtube.com/*
https://www.youtube.com/*
https://hangouts.google.com/*
https://teams.webex.com/*
https://hdx.my.webex.com/*
https://signin.webex.com/*
https://www.webex.com/*
https://login.microsoftonline.com/*stream*
https://login.microsoftonline.com/*teams*
OK
Cancel

ブラウザコンテンツリダイレクトのためのHDXVideo.jsの挿入



HdxVideo.js は、ブラウザコンテンツリダイレクト Chrome 拡張機能または Internet Explorer Browser Helper Object (BHO) を使用してウェブページに挿入されます。BHO は Internet Explorer 用のプラグインモデルです。これはブラウザ API のフックを提供し、プラグインがページの Document Object Model (DOM) にアクセスしてナビゲーションを制御できるようにします。

BHO は、特定のページに HdxVideo.js を挿入するかどうかを決定します。この決定は、前のフローチャートに示されている管理ポリシーに基づいています。

JavaScript を挿入し、ブラウザコンテンツをクライアントにリダイレクトすることを決定した後、VDA 上の Internet Explorer ブラウザではウェブページが空白になります。**document.body.innerHTML** を空に設定すると、VDA 上のウェブページの本文全体が削除されます。ページは、クライアント上のオーバーレイブラウザ (Hdxbrowser.exe) に表示するために、クライアントに送信される準備ができています。

クライアントセンサーポリシー設定

クライアントセンサーセクションには、ユーザーセッションでモバイルデバイスのセンサー情報がどのように処理されるかを制御するためのポリシー設定が含まれています。

アプリケーションによるクライアントデバイスの物理的な位置情報の使用を許可する

この設定は、モバイルデバイス上のセッションで実行されているアプリケーションが、ユーザーデバイスの物理的な位置情報を使用できるかどうかを決定します。

デフォルトでは、位置情報の使用は禁止されています。

この設定が禁止されている場合、アプリケーションが位置情報を取得しようとすると、「アクセス拒否」の値が返されます。

この設定が許可されている場合、ユーザーはCitrix Workspace™アプリの位置情報へのアクセス要求を拒否することで、位置情報の使用を禁止できます。AndroidおよびiOSデバイスでは、各セッションで位置情報が最初に要求されたときにプロンプトが表示されます。

「アプリケーションによるクライアントデバイスの物理的な位置情報の使用を許可する」設定を使用するホスト型アプリケーションを開発する際は、以下を考慮してください。

- 位置情報が有効なアプリケーションが位置情報の利用可能性に依存しないようにしてください。その理由は次のとおりです。
  - ユーザーが位置情報へのアクセスを許可しない可能性があります。
  - アプリケーションの実行中に位置情報が利用できない、または変更される可能性があります。
  - ユーザーが位置情報をサポートしていない別のデバイスからアプリケーションセッションに接続する可能性があります。
- 位置情報が有効なアプリケーションは、次の条件を満たす必要があります。
  - 位置情報機能をデフォルトでオフにする。
  - アプリケーションの実行中に、ユーザーがその機能を許可または禁止するオプションを提供する。
  - アプリケーションがキャッシュする位置データをクリアするオプションをユーザーに提供します。(Citrix Workspaceアプリは位置データをキャッシュしません。)
- 位置情報対応アプリケーションは、位置情報の粒度を管理する必要があります。この管理により、取得されたデータがアプリケーションの目的に適切であることが保証されます。また、関連するすべての法域の規制に準拠します。

- 位置情報サービスを使用する場合は、安全な接続 (TLS または VPN の使用など) を強制します。Citrix Workspaceアプリを信頼できるサーバーに接続します。
- 位置情報サービスの使用に関して、法的助言を得ることを検討してください。

デスクトップUIポリシー設定

デスクトップUIセクションには、デスクトップの壁紙、メニューアニメーション、ドラッグイメージなどの視覚効果を制御するポリシー設定が含まれています。これらのポリシー設定は、クライアント接続で使用される帯域幅の管理に役立ちます。帯域幅の使用量を制限することで、WANでのアプリケーションパフォーマンスを向上させることができます。

> **重要:**
>
> このリリースでは、レガシーグラフィックモードとデスクトップコンポジションリダイレクト（DCR）はサポートされていません。このポリシーは、以下を使用する場合の旧バージョンとの互換性のためだけに含められています。
>
> - XenApp 7.15 LTSR
> - XenDesktop 7.15 LTSR
> - Windows 7およびWindows 2008 R2を使用している以前のVDAリリース。

デスクトップコンポジションリダイレクト

この設定は、ユーザーによりスムーズなWindowsデスクトップエクスペリエンスを提供するために、ローカルのDirectXグラフィックレンダリングに以下の処理能力を使用するかどうかを指定します。

- ユーザーデバイス上のグラフィック処理ユニット（GPU）
- または、,
- ユーザーデバイス上の統合グラフィックプロセッサ（IGP）

有効にすると、**デスクトップコンポジションリダイレクト**は、サーバーの高いスケーラビリティを維持しながら、応答性の高いWindowsエクスペリエンスを提供します。

デフォルトでは、**デスクトップコンポジションリダイレクト**は無効になっています。

デスクトップコンポジションリダイレクトの選択を解除し、ユーザーセッションで必要な帯域幅を削減するには、この設定をポリシーに追加するときに、**無効**を選択します。

デスクトップコンポジションリダイレクトのグラフィック品質

この設定は、デスクトップコンポジションリダイレクトに使用されるグラフィックの品質を指定します。

デフォルトは「高」です。

「高」、「中」、「低」、または「ロスレス」品質から選択します。

デスクトップの壁紙

この設定は、ユーザーセッションでの壁紙の表示を許可または禁止します。

デフォルトでは、ユーザーセッションで壁紙を表示できます。

デスクトップの壁紙を選択解除し、ユーザーセッションで必要な帯域幅を削減するには、この設定をポリシーに追加する際に「**禁止**」を選択します。

メニューアニメーション

この設定は、ユーザーセッションでのメニューアニメーションを許可または禁止します。

デフォルトでは、メニューアニメーションは許可されています。

メニューアニメーションは、アクセシビリティのためのMicrosoftの個人設定です。有効にすると、短い遅延の後、スクロールまたはフェードインによってメニューが表示されます。メニューの下部には矢印アイコンが表示されます。その矢印をポイントするとメニューが表示されます。

このポリシー設定が「**許可**」に設定されており、メニューアニメーションのMicrosoft個人設定が有効になっている場合、デスクトップでメニューアニメーションが有効になります。

> **注：**
>
> メニューアニメーションのMicrosoft個人設定への変更は、デスクトップに影響を与えます。セッション終了時に変更を破棄するようにデスクトップを設定している場合を考慮してください。この場合、メニューアニメーションを有効にしているユーザーは、その後のセッションでメニューアニメーションを利用できない可能性があります。メニューアニメーションを必要とするユーザーに対しては、デスクトップのメインイメージでMicrosoft設定を有効にするか、デスクトップがユーザーの変更を保持するようにしてください。

ドラッグ中のウィンドウコンテンツの表示

この設定は、画面上でウィンドウをドラッグする際にウィンドウコンテンツの表示を許可または禁止します。

デフォルトでは、ウィンドウコンテンツの表示は許可されています。

「**許可**」に設定すると、ウィンドウをドラッグしたときにウィンドウ全体が移動するように見えます。「**禁止**」に設定すると、ドロップするまでウィンドウのアウトラインのみが移動するように見えます。

エンドユーザー監視ポリシー設定

「**エンドユーザー監視**」セクションには、セッションのトラフィックを測定するためのポリシー設定が含まれています。

ICA®ラウンドトリップ計算

この設定は、アクティブな接続に対してICAラウンドトリップ計算が実行されるかどうかを決定します。

デフォルトでは、アクティブな接続に対する計算は有効になっています。

デフォルトでは、各ICAラウンドトリップ測定の開始は遅延されます。この遅延は、ユーザーインタラクションを示すトラフィックが発生するまで続きます。この遅延は無期限に続く可能性があり、ICAラウンドトリップ測定がICAトラフィックの唯一の原因となるのを防ぐように設計されています。

ICAラウンドトリップ計算間隔

この設定は、ICAラウンドトリップ計算が実行される頻度を秒単位で指定します。

デフォルトでは、ICAラウンドトリップは15秒ごとに計算されます。

アイドル接続のICAラウンドトリップ計算

この設定は、アイドル接続に対してICAラウンドトリップ計算が実行されるかどうかを決定します。

デフォルトでは、アイドル接続に対して計算は実行されません。

デフォルトでは、各ICAラウンドトリップ測定の開始は遅延されます。この遅延は、ユーザーインタラクションを示すトラフィックが発生するまで続きます。この遅延は無期限に続く可能性があり、ICAラウンドトリップ測定がICAトラフィックの唯一の原因となるのを防ぐように設計されています。

強化されたデスクトップエクスペリエンスポリシー設定

強化されたデスクトップエクスペリエンスポリシー設定は、ローカルのWindows 7デスクトップのように見えるサーバーオペレーティングシステム上でセッションを実行します。

デフォルトでは、この設定は許可されています。

仮想デスクトップ上にWindowsクラシックテーマのユーザープロファイルが存在する場合、このポリシーはそのユーザーに強化されたデスクトップエクスペリエンスを提供しません。Windows 7テーマのユーザープロファイルを持つユーザーが、Windows Server 2012を実行している仮想デスクトップにログオンする場合を考えます。また、このポリシーが構成されていないか、無効になっている場合、そのユーザーはテーマの適用に失敗したことを示すエラーメッセージを目にします。

どちらの場合も、ユーザープロファイルをリセットすることで問題が解決します。

アクティブなユーザーセッションを持つ仮想デスクトップでポリシーを無効にすると、それらのセッションのインターフェイスは、Windows 7およびWindows Classicデスクトップで一貫性がなくなります。この不整合を避けるために、このポリシー設定を変更した後、仮想デスクトップを再起動してください。その後、仮想デスクトップ上のすべてのローミングプロファイルを削除します。Citrix®は、プロファイル間の不整合を避けるために、仮想デスクトップ上の他のユーザープロファイルも削除することを推奨します。

環境でローミングユーザープロファイルを使用しているとします。この場合、プロファイルを共有するすべての仮想デスクトップで、強化されたデスクトップエクスペリエンス機能が有効または無効になっていることを確認してください。

Citrixは、サーバーオペレーティングシステムとクライアントオペレーティングシステムを実行している仮想デスクトップ間でローミングプロファイルを共有することを推奨しません。クライアントおよびサーバーオペレーティングシステムのプロファイルは異なります。両方のタイプ間でローミングプロファイルを共有すると、ユーザーが両者の間を移動する際にプロファイルプロパティに不整合が生じる可能性があります。

ファイルリダイレクトポリシー設定

ファイルリダイレクトセクションには、クライアントドライブマッピングおよびクライアントドライブ最適化に関連するポリシー設定が含まれています。

クライアントドライブの自動接続

この設定は、ユーザーがログオンしたときのクライアントドライブの自動接続を許可または禁止します。

デフォルトでは、自動接続は許可されています。

この設定をポリシーに追加するときは、自動接続するドライブの種類の設定を必ず有効にしてください。たとえば、ユーザーのCD-ROMドライブの自動接続を許可するには、この設定と**クライアント光学ドライブ**設定を構成します。

関連するポリシー設定は次のとおりです。

- **クライアントドライブリダイレクト**
- **クライアントフロッピーディスクドライブ**
- **クライアント光学ドライブ**
- **クライアント固定ドライブ**
- **クライアントネットワークドライブ**
- **クライアントリムーバブルドライブ**

クライアントドライブリダイレクト

この設定は、ユーザーデバイス上のドライブとの間でファイルリダイレクトを有効または無効にします。

デフォルトでは、ファイルリダイレクトは有効になっています。

> **注：**
>
> クライアントドライブリダイレクトポリシー設定は、汎用USBリダイレクトを使用してセッションにマップされたドライブには適用されません。

> 有効にすると、ユーザーはすべてのクライアントドライブにファイルを保存できます。無効にすると、すべてのファイルリダイレクトが防止されます。この構成は、個々のファイルリダイレクト設定の状態に関係なく適用されます。個々のファイルリダイレクト設定には、クライアントフロッピードライブとクライアントネットワークドライブが含まれます。

関連するポリシー設定は次のとおりです。

- **クライアントフロッピードライブ**
- **クライアント光学ドライブ**
- **クライアント固定ドライブ**
- **クライアントネットワークドライブ**
- **クライアントリムーバブルドライブ**

クライアント固定ドライブ

この設定により、ユーザーはユーザーデバイス上の固定ドライブにアクセスしたりファイルを保存したりできるようになります。

デフォルトでは、クライアント固定ドライブへのアクセスは許可されています。

この設定をポリシーに追加する場合は、**クライアントドライブリダイレクト**設定が存在し、許可に設定されていることを確認してください。これらの設定が無効になっている場合、クライアント固定ドライブはマップされず、**クライアント固定ドライブ**設定の状態に関係なく、ユーザーはこれらのドライブに手動でアクセスできません。

ユーザーがログオンしたときに固定ドライブが自動的に接続されるように、**クライアントドライブの自動接続**設定を構成します。

クライアントフロッピードライブ

この設定により、ユーザーはユーザーデバイス上のフロッピードライブにアクセスしたりファイルを保存したりできるようになります。

デフォルトでは、クライアントフロッピードライブへのアクセスは許可されています。

この設定をポリシーに追加する場合、「**クライアントドライブのリダイレクト**」設定が存在し、「許可」に設定されていることを確認してください。これらの設定が無効になっている場合、クライアントフロッピーディスクドライブはマップされず、ユーザーは「**クライアントフロッピーディスクドライブ**」設定の状態にかかわらず、これらのドライブに手動でアクセスできません。

ユーザーがログオンしたときにフロッピーディスクドライブが自動的に接続されるようにするには、「**クライアントドライブの自動接続**」設定を構成します。

クライアントネットワークドライブ

この設定は、ユーザーがユーザーデバイスを介してネットワーク（リモート）ドライブにファイルにアクセスしたり保存したりすることを許可または禁止します。

デフォルトでは、クライアントネットワークドライブへのアクセスは許可されています。

この設定をポリシーに追加する場合、「**クライアントドライブのリダイレクト**」設定が存在し、「許可」に設定されていることを確認してください。これらの設定が無効になっている場合、クライアントネットワークドライブはマップされず、ユーザーはこれらのドライブに手動でアクセスできません。この構成は、「**クライアントネットワークドライブ**」設定の状態にかかわらず適用されます。

ユーザーがログオンしたときにネットワークドライブが自動的に接続されるようにするには、「**クライアントドライブの自動接続**」設定を構成します。

クライアント光学ドライブ

この設定は、ユーザーが以下の場所にファイルにアクセスしたり保存したりすることを許可または禁止します。

- ユーザーデバイス上のCD-ROM
- ユーザーデバイス上のDVD-ROM
- ユーザーデバイス上のBD-ROMドライブ。

デフォルトでは、クライアント光学ドライブへのアクセスは許可されています。

この設定をポリシーに追加する場合、「**クライアントドライブのリダイレクト**」設定が存在し、「**許可**」に設定されていることを確認してください。これらの設定が無効になっている場合、クライアント光学ドライブはマップされず、ユーザーはこれらのドライブに手動でアクセスできません。この構成は、「**クライアント光学ドライブ**」設定の状態にかかわらず適用されます。

ユーザーがログオンしたときに光学ドライブが自動的に接続されるようにするには、「**クライアントドライブの自動接続**」設定を構成します。

クライアントリムーバブルドライブ

この設定により、ユーザーはユーザーデバイス上のUSBドライブへのファイルアクセスまたは保存を許可または禁止されます。

デフォルトでは、クライアントリムーバブルドライブへのアクセスは許可されています。

この設定をポリシーに追加する際は、**クライアントドライブのリダイレクト**設定が存在し、「許可」に設定されていることを確認してください。これらの設定が無効になっている場合、クライアントリムーバブルドライブはマップされず、ユーザーはこれらのドライブに手動でアクセスできません。この構成は、**クライアントリムーバブルドライブ**設定の状態に関係なく適用されます。

ユーザーがログオンしたときにリムーバブルドライブが自動的に接続されるように、**クライアントドライブの自動接続**設定を構成します。

ホストからクライアントへのリダイレクト

この設定により、URLおよび一部のメディアコンテンツのファイルタイプ関連付けを有効または無効にし、ユーザーデバイスで開くことができます。無効にすると、コンテンツはサーバーで開かれます。

デフォルトでは、ファイルタイプ関連付けは無効になっています。

この設定を有効にすると、以下のURLタイプがローカルで開かれます。

- HTTP
- HTTPS
- リアルプレーヤーおよびQuickTime (RTSP)
- リアルプレーヤーおよびQuickTime (RTSPU)
- レガシーReal Player (PNM)
- マイクロソフト メディア サーバー (MMS)

クライアントドライブ文字の保持

この設定により、クライアントドライブをセッション内で同じドライブ文字にマップすることを有効または無効にします。

デフォルトでは、クライアントドライブ文字は保持されません。

この設定をポリシーに追加する場合は、**クライアントドライブのリダイレクト**設定が存在し、許可に設定されていることを確認してください。

読み取り専用クライアントドライブアクセス

この設定は、ユーザーとアプリケーションが以下の操作を行うことを許可または禁止します。

- マップされたクライアントドライブ上にファイルを作成する
- マップされたクライアントドライブ上のファイルを変更する
- マップされたクライアントドライブ上のフォルダーを変更する

デフォルトでは、マップされたクライアントドライブ上のファイルとフォルダーは変更できます。

有効に設定されている場合、ファイルとフォルダーは読み取り専用権限でアクセスできます。

この設定をポリシーに追加する場合は、**クライアントドライブのリダイレクト**設定が存在し、許可に設定されていることを確認してください。

特殊フォルダーのリダイレクト

この設定は、Citrix Workspace™アプリおよびWeb Interfaceのユーザーが、セッションからローカルのドキュメントおよびデスクトップの特殊フォルダーを表示することを許可または禁止します。

デフォルトでは、特殊フォルダーのリダイレクトは許可されています。

この設定は、ポリシーによってフィルター処理されたオブジェクトが特殊フォルダーのリダイレクトを持つことを防ぎます。これは、他の場所に存在する設定に関係なく適用されます。この設定が禁止されている場合、StoreFront™、Web Interface、またはCitrix Workspaceアプリに指定された関連設定はすべて無視されます。

どのユーザーが特殊フォルダーのリダイレクトを使用できるかを定義するには、**許可**を選択し、この機能を適用したいユーザーでフィルター処理されたポリシーにこの設定を含めます。この設定は、他のすべての特殊フォルダーのリダイレクト設定を上書きします。

ユーザーがローカルハードドライブ上のファイルにアクセスしたり保存したりするのを防ぐポリシー設定は、特殊フォルダーリダイレクトの動作も妨げます。この状況は、特殊フォルダーリダイレクトがユーザーデバイスと対話する必要があるために発生します。

この設定をポリシーに追加する際は、**クライアント固定ドライブ**設定が存在し、「許可」に設定されていることを確認してください。

ファイル転送ポリシー

デフォルトでは、ファイル転送は有効になっています。これらのポリシーは、**ユーザー設定 - ICA\ファイルリダイレクト**の下にあります。Web Studioを使用して変更してください。ファイル転送ポリシーを使用する際は、以下を考慮してください。

- **Chrome OS/HTML5向けCitrix Workspaceアプリのファイル転送** - ユーザーがCitrix Virtual Apps and Desktopsセッションとデバイス間でファイルを転送することを許可または禁止します。
- **Chrome OS/HTML5向けCitrix Workspaceアプリのファイルアップロード** - ユーザーがデバイスからCitrix Virtual Apps and Desktopsセッションにファイルをアップロードすることを許可または禁止します。
- **Chrome OS/HTML5向けCitrix Workspaceアプリのファイルダウンロード** - ユーザーがCitrix Virtual Apps and Desktopsセッションからデバイスにファイルをダウンロードすることを許可または禁止します。

> **注：**
>
> ファイル転送ポリシーは、HTML5向けCitrix WorkspaceアプリおよびChrome OS向けCitrix Workspaceアプリにのみ適用されます。

非同期書き込みの使用

この設定は、非同期ディスク書き込みを有効または無効にします。

デフォルトでは、非同期書き込みは無効になっています。

非同期ディスク書き込みは、比較的高い帯域幅と高い遅延が特徴であるWAN経由でのファイル転送速度とクライアントディスクへの書き込み速度を向上させることができます。ただし、接続またはディスクに障害が発生した場合、書き込み中のクライアントファイルが未定義の状態になる可能性があります。この未定義の状態が発生した場合、ポップアップウィンドウで影響を受けるファイルがユーザーに通知されます。ユーザーは、再接続時またはディスク障害が修正されたときに中断されたファイル転送を再開するなどの是正措置を講じることができます。

Citrix®は、リモート接続が必要で、良好なファイルアクセス速度を持ち、接続またはディスク障害が発生した場合に失われたファイルやデータを容易に回復できるユーザーに対してのみ、非同期ディスク書き込みを有効にすることを推奨します。

この設定をポリシーに追加する際は、**クライアントドライブリダイレクト**設定が存在し、「許可」に設定されていることを確認してください。この設定が無効になっている場合、非同期書き込みは行われません。

グラフィックポリシー設定

グラフィックセクションには、ユーザーセッションで画像がどのように処理されるかを制御するためのポリシー設定が含まれています。

視覚的にロスレスな圧縮を許可する

この設定により、グラフィックに対して、真のロスレス圧縮の代わりに視覚的にロスレスな圧縮を使用できます。視覚的にロスレスな圧縮は、真のロスレス圧縮よりもパフォーマンスが向上しますが、目視では気づかない程度のわずかな損失があります。この設定は、視覚品質設定の値の使用方法を変更します。

デフォルトでは、この設定は無効になっています。

グラフィックステータスインジケーター

この設定は、グラフィックステータスインジケーターをユーザーセッションで実行するように構成します。このツールを使用すると、ユーザーはアクティブなグラフィックモードに関する情報を確認できます。この情報には、ビデオコーデック、ハードウェアエンコード、画質、セッションで使用中のモニターに関する詳細が含まれます。グラフィックステータスインジケーターを使用すると、ユーザーはピクセルパーフェクトモードを有効または無効にすることもできます。

Citrix Virtual Apps and Desktops™ 2103以降のリリースには、画質とインタラクティブ性の適切なバランスをユーザーが見つけるのに役立つ画質スライダーが含まれています。

Citrix Virtual Apps and Desktops 2109以降のリリースには、グラフィックステータスインジケーターを使用して起動されるユーザーインターフェイスを介して仮想ディスプレイレイアウトを構成する機能が含まれています。

グラフィックステータスインジケーターは、以前のバージョンのロスレスインジケーターツールを置き換えます。このポリシーは、Citrix Virtual Apps and Desktopsバージョン7.16から1809までロスレスインジケーターを有効にします。

画面共有

この設定により、ユーザーは画面コンテンツ、キーボード、マウスを含むセッションを他のユーザーと共有できます。

デフォルトでは、この設定は無効になっています。

VDAは、TCPポート範囲のポートを使用してデータを交換しようとします。これは、最も低いポートから始まり、その後の接続ごとに増分されます。このポートは、インバウンドトラフィックとアウトバウンドトラフィックの両方を処理します。

既定では、TCPポート範囲は52525～52625に設定されています。

画面共有に使用されるポートは、ファイアウォールの例外リストに追加する必要があります。このオプションは、VDAのインストール時にチェックボックスとして表示されます。既定では、このオプションはチェックされていません。

ディスプレイメモリ制限

この設定は、セッションの最大ビデオバッファサイズをキロバイト単位で指定します。

デフォルトでは、ディスプレイメモリ制限は65,536キロバイトです。

セッションの最大ビデオバッファサイズをキロバイト単位で指定します。128から4,194,303までのキロバイト単位の量を指定します。最大値4,194,303はディスプレイメモリを制限しません。デフォルトでは、ディスプレイメモリは65,536キロバイトです。接続でより多くの色深度と高解像度を使用するには、より多くのメモリが必要です。レガシーグラフィックモードでは、メモリ制限に達すると、「ディスプレイモードの劣化設定」に従ってディスプレイが劣化します。

より多くの色深度と高解像度を必要とする接続の場合、制限を増やします。次の式を使用して、必要な最大メモリを計算します。

メモリ深度（バイト）=（色深度（ビット/ピクセル）/ 8）x（垂直解像度（ピクセル））x（水平解像度（ピクセル））.

例えば、色深度32、垂直解像度600、水平解像度800のシナリオを考えます。この場合、必要な最大メモリは（32 / 8）x（600）x（800）= 1920000バイトとなり、ディスプレイメモリ制限は1920 KBになります。

32ビット以外の色深度は、レガシーグラフィックモードポリシー設定が有効になっている場合にのみ利用可能です。

HDX™は、各セッションに必要なディスプレイメモリの量のみを割り当てます。したがって、一部のユーザーのみがデフォルトよりも多くを必要とする場合でも、ディスプレイメモリ制限を増やすことによるスケーラビリティへの悪影響はありません。

ディスプレイモードの劣化設定

> **注：**
>
> Virtual Delivery Agent 7.xの場合、このポリシー設定は、レガシーグラフィックモードポリシー設定が有効になっている場合にのみ適用されます。

> セッションの表示メモリ制限に達した場合、この設定は、色深度と解像度のどちらが先に劣化するかを指定します。

デフォルトでは、色深度が先に劣化します。

セッションメモリ制限に達すると、表示される画像の品質を低下させることができます。この品質は、色深度と解像度のどちらを先に劣化させるかを選択することで低下させることができます。色深度が先に劣化する場合、表示される画像はより少ない色を使用します。解像度が先に劣化する場合、表示される画像は1インチあたりのピクセル数が少なくなります。

色深度または解像度が劣化した場合にユーザーに通知するには、「表示モードが劣化した場合にユーザーに通知」設定を構成します。

動的ウィンドウプレビュー

この設定は、シームレスウィンドウの表示を有効または無効にします。

- フリップ-
- フリップ 3D
- タスクバープレビュー
- Windows ピーク

WINDOWS AERO プレビューオプション	説明
タスクバープレビュー	ユーザーがウィンドウのタスクバーアイコンにマウスカーソルを合わせると、そのウィンドウの画像がタスクバーの上に表示されます。
Windows ピーク	ユーザーがタスクバーのプレビュー画像にマウスカーソルを合わせると、ウィンドウのフルサイズの画像が画面に表示されます。
フリップ	ユーザーが ALT+TAB を押すと、開いている各ウィンドウの小さなプレビューアイコンが表示されます。
フリップ 3D	ユーザーが TAB+Windows ロゴキーを押すと、開いているウィンドウの大きな画像が画面にカスケード表示されます。

デフォルトでは、この設定は有効になっています。

イメージキャッシュ

> **注：**

> Virtual Delivery Agent 7.x の場合、このポリシー設定は、レガシーグラフィックモードのポリシー設定が有効になっている場合にのみ適用されます。

> この設定は、セッション内の画像のセクションのキャッシュと取得を有効または無効にします。画像をセクションにキャッシュし、必要に応じてこれらのセクションを取得すると、次のことが可能になります。

- ユーザーデバイスでのスクロールがよりスムーズになる
- ユーザーデバイスでのネットワーク経由で送信されるデータ量を削減する
- ユーザーデバイスで必要な処理を削減する

デフォルトでは、画像キャッシュ設定は有効になっています。

> **注：**

画像キャッシュ設定は、画像がどのようにキャッシュされ、取得されるかを制御します。この設定は、画像がキャッシュされるかどうかを制御するものではありません。画像は、レガシーグラフィックモード設定が有効になっている場合にキャッシュされます。

レガシーグラフィックモード - サポートされていません。下位互換性のためのみ

重要:

このリリースでは、レガシーグラフィックモードとデスクトップコンポジションリダイレクト (DCR) はサポートしていません。このポリシーは、XenApp 7.15 LTSR、XenDesktop 7.15 LTSR、およびWindows 7とWindows 2008 R2を使用する以前のVDAリリースとの下位互換性のためのみに含まれています。

この設定は、リッチグラフィックエクスペリエンスを無効にします。この設定を使用して、レガシーグラフィックエクスペリエンスに戻し、WANまたはモバイル接続での帯域幅消費を削減します。XenAppおよびXenDesktop 7.13で導入された帯域幅削減により、このモードは廃止されました。

デフォルトでは、この設定は無効になっており、ユーザーにはリッチグラフィックエクスペリエンスが提供されます。

レガシーグラフィックモードは以下でサポートされています。

- ウィンドウズ 7
- ウィンドウズ サーバー 2008 R2 VDA。

レガシーグラフィックモードは以下ではサポートされていません。

- Windows 8.xおよび10
- Windows Server 2012、2012 R2、および2016。

XenAppおよびXenDesktop 7.6 FP3以降でのグラフィックモードとポリシーの最適化について詳しくは、CTX202687を参照してください。

最大許容色深度

注：

> Virtual Delivery Agent 7.xの場合、このポリシー設定は、レガシーグラフィックモードポリシー設定が有効になっている場合にのみ適用されます。

> この設定は、セッションで許可される最大色深度を指定します。

デフォルトでは、最大許容色深度は32ビット/ピクセルです。

この設定は、Thinwireドライバーと接続にのみ適用されます。プライマリディスプレイドライバーとしてThinWire以外のドライバーを使用するVDAには適用されません。これらのVDAは、プライマリディスプレイドライバーとしてWindows Display Driver Model (WDDM) ドライバーを使用するVDAです。Windows 8などのWDDMドライバーをプライマリディスプレイドライバーとして使用するシングルセッションOS VDAの場合、この設定は効果がありません。Windows Server 2012 R2などのWDDMドライバーを使用するWindowsマルチセッションOS VDAの場合、この設定によりユーザーがVDAに接続できなくなる可能性があります。

高い色深度を設定すると、より多くのメモリが必要になります。メモリ制限に達したときに色深度を低下させるには、**表示モードの低下設定**を構成します。色深度が低下すると、表示される画像はより少ない色を使用します。

表示モードが低下したときにユーザーに通知する

> **注：**

> Virtual Delivery Agent 7.xの場合、このポリシー設定は、レガシーグラフィックモードポリシー設定が有効になっている場合にのみ適用されます。

> この設定は、色深度または解像度が低下したときに、ユーザーに簡単な説明を表示します。

デフォルトでは、ユーザーへの通知は無効になっています。

3Dグラフィックワークロード向けに最適化

この設定は、グラフィックを多用するワークロードに最適なデフォルト設定を構成します。グラフィックを多用するアプリケーションに重点を置くユーザーに対して、この設定を有効にします。このポリシーは、セッションでGPUが利用可能な場合にのみ適用してください。このポリシーによって設定されたデフォルト設定を明示的に上書きするその他の設定が優先されます。

デフォルトでは、3Dグラフィックワークロード向けに最適化は無効になっています。

キューイングとトッシング

> **注：**
>
> Virtual Delivery Agent 7.xの場合、このポリシー設定は、レガシーグラフィックモードポリシー設定が有効になっている場合にのみ適用されます。

> この設定は、別の画像に置き換えられたキュー内の画像を破棄します。

デフォルトでは、キューイングとトッシングは有効になっています。

この設定は、グラフィックがユーザーデバイスに送信される際の応答を改善します。この設定を構成すると、フレームがドロップされるため、アニメーションが途切れることがあります。

圧縮にビデオコーデックを使用する

エンドポイントでビデオデコードが利用可能な場合、グラフィックの圧縮にビデオコーデックの使用を許可します。「**画面全体**」が選択されている場合、ビデオコーデックはすべてのデフォルトコーデックとして適用されます。「**アクティブに変化する領域**」が選択されている場合、ビデオコーデックは画面上で常に変化する領域に使用され、その他のデータは静止画圧縮とビットマップキャッシュを使用します。エンドポイントでビデオデコードが利用できない場合、または「**ビデオコーデックを使用しない**」を指定した場合、静止画圧縮とビットマップキャッシュの組み合わせが使用されます。「**推奨時に使用**」が選択されている場合、システムはさまざまな要因に基づいて選択します。選択方法が強化されるにつれて、バージョン間で結果が異なる場合があります。

現在のシナリオに適切な設定をシステムが最善を尽くして選択できるようにするには、「**推奨時に使用**」を選択します。

特にサーバーレンダリングされたビデオや3Dグラフィックを多用する場合に、ユーザーエクスペリエンスと帯域幅の向上を最適化するには、「**画面全体**」を選択します。

特に低帯域幅でビデオパフォーマンスを向上させ、静的およびゆっくりと変化するコンテンツのスケーラビリティを維持するために最適化するには、「**アクティブに変化する領域**」を選択します。この設定はマルチモニター展開でサポートされています。

サーバーのCPU負荷を最適化し、多数のサーバーレンダリングされたビデオやその他のグラフィックを多用するアプリケーションがない場合に最適化するには、「**ビデオコーデックを使用しない**」を選択します。

デフォルトは「**推奨時に使用**」です。

ビデオにハードウェアエンコーディングを使用する

この設定により、利用可能な場合、グラフィックハードウェアを使用してビデオコーデックで画面要素を圧縮できます。そのようなハードウェアが利用できない場合、VDAはソフトウェアビデオコーデックを使用したCPUベースのエンコーディングにフォールバックします。

このポリシー設定のデフォルトオプションは「**有効**」です。

複数のモニターがサポートされています。

ビデオデコードをサポートするCitrix Workspace™アプリは、ハードウェアエンコードで使用できます。

NVIDIA

NVIDIA GRID GPUの場合、ハードウェアエンコードはマルチセッションOSおよびシングルセッションOS用のVDAでサポートされています。

NVIDIA GPUはNVENCハードウェアエンコードをサポートしている必要があります。サポートされているGPUのリストについては、NVIDIA video codec SDKを参照してください。

NVIDIA GRIDにはドライバーバージョン3.1以降が必要です。NVIDIA Quadroにはドライバーバージョン362.56以降が必要です。CitrixはNVIDIA Release R361ブランチのドライバーを推奨しています。

ロスレステキストはNVENCハードウェアエンコードと互換性がありません。ロスレステキストを有効にした場合、ロスレステキストがNVENCハードウェアエンコードよりも優先されます。

アクティブに変化する領域に対するH.264ハードウェアコーデックの選択的な使用がサポートされています。

視覚的にロスレス（YUV 4:4:4）圧縮がサポートされています。視覚的にロスレス（グラフィックポリシー設定、視覚的にロスレス圧縮を許可）には、Citrix Workspaceアプリ1808以降またはCitrix Receiver for Windows 4.5以降が必要です。

インテル

Intel Iris Proグラフィックプロセッサの場合、ハードウェアエンコードはシングルセッションOSおよびマルチセッションOS用のVDAでサポートされています。

Intel Broadwellプロセッサファミリー以降のIntel Iris Proグラフィックプロセッサがサポートされています。Intel Remote Displays SDKバージョン1.0が必要であり、IntelのWebサイトからダウンロードできます: Remote Displays SDK。

ロスレステキストは、ビデオコーデックポリシーが画面全体に設定され、**3Dグラフィックワークロード向けに最適化**ポリシーが無効になっている場合にのみサポートされます。

視覚的にロスレス（YUV 4:4:4）はサポートされていません。

Intelエンコーダーは、最大8つのエンコードセッション（たとえば、1人のユーザーが8台のモニターを使用する場合、または8人のユーザーがそれぞれ1台のモニターを使用する場合）で良好なユーザーエクスペリエンスを提供します。8つ以上のエンコードセッションが必要な場合は、仮想マシンが接続するモニターの数を確認してください。管理者は、良好なユーザーエクスペリエンスを維持するために、このポリシー設定をユーザーごとまたはマシンごとに構成するかどうかを決定します。

AMD

AMDの場合、シングルセッションOS用VDAでハードウェアエンコードがサポートされています。

AMD GPUはRapidFire SDKをサポートする必要があります。例えば、AMD Radeon ProまたはFirePro GPUなどです。

エンコードを機能させるには、最新のAMDドライバーをインストールしてください。これらのドライバーは`<https://www.amd.com/en/support>`からダウンロードできます。

ロスレステキストはAMDハードウェアエンコードと互換性がありません。ロスレステキストを有効にした場合、ロスレステキストがAMDハードウェアエンコードよりも優先されます。

活発に変化する領域向けのH.264ハードウェアコーデックの選択的な使用がサポートされています。

キャッシュポリシー設定

このセクションには、クライアント接続の帯域幅が制限されている場合に、ユーザーデバイスで画像データをキャッシュすることを可能にするポリシー設定が含まれています。

永続キャッシュしきい値

注: Virtual Delivery Agent 7.xの場合、このポリシー設定は、**レガシーグラフィックモード**ポリシー設定が有効になっている場合にのみ適用されます。

この設定は、ユーザーデバイスのハードドライブにビットマップをキャッシュし、それにより、以前のセッションからの大きく頻繁に使用される画像の再利用を可能にします。

デフォルトでは、しきい値は1秒あたり3000000ビットです。

しきい値は、永続キャッシュ機能が有効になる下限を表します。たとえば、デフォルト値を使用すると、帯域幅が3000000 bpsを下回った場合、ビットマップはユーザーデバイスのハードドライブにキャッシュされます。

Framehawkポリシー設定

> **重要:**
>
> Citrix Virtual Apps and Desktops 7 1903以降、Framehawkはサポートされなくなりました。代わりに、Thinwireをアダプティブトランスポートを有効にして使用してください。

> **Framehawk**セクションには、サーバー上のFramehawkディスプレイチャネルを有効にして構成するポリシー設定が含まれています。

FRAMEHAWKディスプレイチャネル

有効にすると、サーバーはユーザーのグラフィックと入力のリモート処理にFramehawkディスプレイチャネルを使用しようとします。このディスプレイチャネルはUDPを使用して、損失と遅延の特性が高いネットワークでより良いユーザーエクスペリエンスを提供します。ただし、他のグラフィックモードよりも多くのサーバーリソースと帯域幅を使用する可能性もあります。

デフォルトでは、Framehawkディスプレイチャネルは無効になっています。

FRAMEHAWKディスプレイチャネルのポート範囲

このポリシー設定は、VDAがユーザーデバイスとFramehawkディスプレイチャネルデータを交換するために使用するUDPポート番号の範囲を指定します。ポート番号は*最小ポート番号*または*最大ポート番号*の形式です。VDAは、最小ポート番号から開始し、その後の試行ごとにインクリメントして、各ポートを使用しようとします。このポートはインバウンドおよびアウトバウンドトラフィックを処理します。

デフォルトでは、ポート範囲は3224,3324です。

キープアライブ ポリシー設定

Keep Alive セクションには、ICA® キープアライブメッセージを管理するためのポリシー設定が含まれています。

ICA キープアライブ タイムアウト

この設定は、連続するICAキープアライブメッセージ間の秒数を指定します。

デフォルトでは、キープアライブメッセージ間の間隔は60秒です。

ICAキープアライブメッセージを送信する1～3600秒の間隔を指定します。ネットワーク監視ソフトウェアが非アクティブな接続を閉じる役割を担っている場合は、この設定を構成しないでください。

ICA キープアライブメッセージ

この設定は、定期的なICAキープアライブメッセージの送信を有効または無効にします。

デフォルトでは、キープアライブメッセージは送信されません。

この設定を有効にすると、切断された接続が切断されるのを防ぎます。サーバーがアクティビティを検出しない場合、この設定により、Remote Desktop Services (RDS) がセッションを切断するのを防ぎます。サーバーは数秒ごとにキープアライブメッセージを送信し、セッションがアクティブであるかどうかを検出します。セッションがアクティブでなくなった場合、サーバーはそのセッションを切断済みとしてマークします。

セッションの信頼性を使用している場合、ICAキープアライブは機能しません。セッションの信頼性を使用していない接続に対してのみ、ICAキープアライブを構成してください。

関連するポリシー設定: セッションの信頼性接続。

ローカルアプリアクセス ポリシー設定

ローカルアプリアクセスセクションには、ユーザーのローカルにインストールされたアプリケーションとホストされたアプリケーションを管理するポリシー設定が含まれています。これらのポリシー設定は、ホストされたデスクトップ環境での統合を管理します。

ローカルアプリアクセスを許可

この設定は、ユーザーのローカルにインストールされたアプリケーションとホストされたアプリケーションの統合を許可または禁止します。これらのポリシー設定は、ホストされたデスクトップ環境での統合を管理します。

ユーザーがローカルにインストールされたアプリケーションを起動すると、そのアプリケーションは実際にはローカルで実行されているにもかかわらず、仮想デスクトップ内で実行されているように見えます。

ローカルアプリアクセスを許可ポリシー設定を**有効**にすると、ブラウザコンテンツリダイレクトはサポートされず、デスクトップセッションにクライアント側の通知領域のバッテリーステータスは表示されません。

デフォルトでは、**ローカルアプリアクセスを許可**は禁止されています。

URLリダイレクトブロックリスト

この設定は、ローカルのWebブラウザにリダイレクトされて起動されるWebサイトを指定します。これらのWebサイトには、次のものが含まれる場合があります。

- msn.comやnewsgoogle.comなど、ロケール情報を必要とするWebサイト
- ユーザーデバイスでより適切にレンダリングされるリッチメディアコンテンツを含むWebサイト。

デフォルトでは、サイトは指定されていません。

URLリダイレクト許可リスト

この設定は、起動された環境でレンダリングされるWebサイトを指定します。

デフォルトでは、サイトは指定されていません。

モバイルエクスペリエンスポリシー設定

「**モバイルエクスペリエンス**」セクションには、Citrix Mobility Packを処理するためのポリシー設定が含まれています。

キーボードの自動表示

この設定は、モバイルデバイスの画面でのキーボードの自動表示を有効または無効にします。

デフォルトでは、キーボードの自動表示は無効になっています。

タッチ最適化デスクトップの起動

この設定は無効になっており、Windows 10またはWindows Server 2016マシンでは使用できません。

この設定は、Citrix Workspace™アプリの全体的なインターフェイス動作を決定します。この設定により、タブレットデバイス向けに最適化されたタッチフレンドリーなインターフェイスの使用が許可または禁止されます。

デフォルトでは、タッチフレンドリーなインターフェイスが使用されます。

Windowsインターフェイスのみを使用するには、このポリシー設定を「禁止」に設定します。

コンボボックスのリモート化

この設定は、モバイルデバイスのセッションで表示できるコンボボックスの種類を決定します。このポリシー設定を「許可」に設定すると、デバイスネイティブのコンボボックスコントロールが表

示されます。この設定が許可されている場合、ユーザーはCitrix Workspace app for iOSセッション設定を変更して、Windowsコンボボックスを使用できます。

デフォルトでは、**コンボボックスのリモート化**機能は禁止されています。

マルチメディアポリシー設定

「**マルチメディア**」セクションには、ユーザーセッションにおけるストリーミングHTML5およびWindowsのオーディオとビデオを管理するためのポリシー設定が含まれています。

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

マルチメディアポリシー

デフォルトでは、Delivery Controller™で設定されたすべてのマルチメディアポリシーは、以下のレジストリに保存されます。

マシンポリシー:

HKEY_LOCAL_MACHINE\Software\Policies\Citrix\MultimediaPolicies

ユーザーポリシー:

HKEY_LOCAL_MACHINE\Software\Policies\Citrix{ユーザーセッションID}\User\MultimediaPolicies

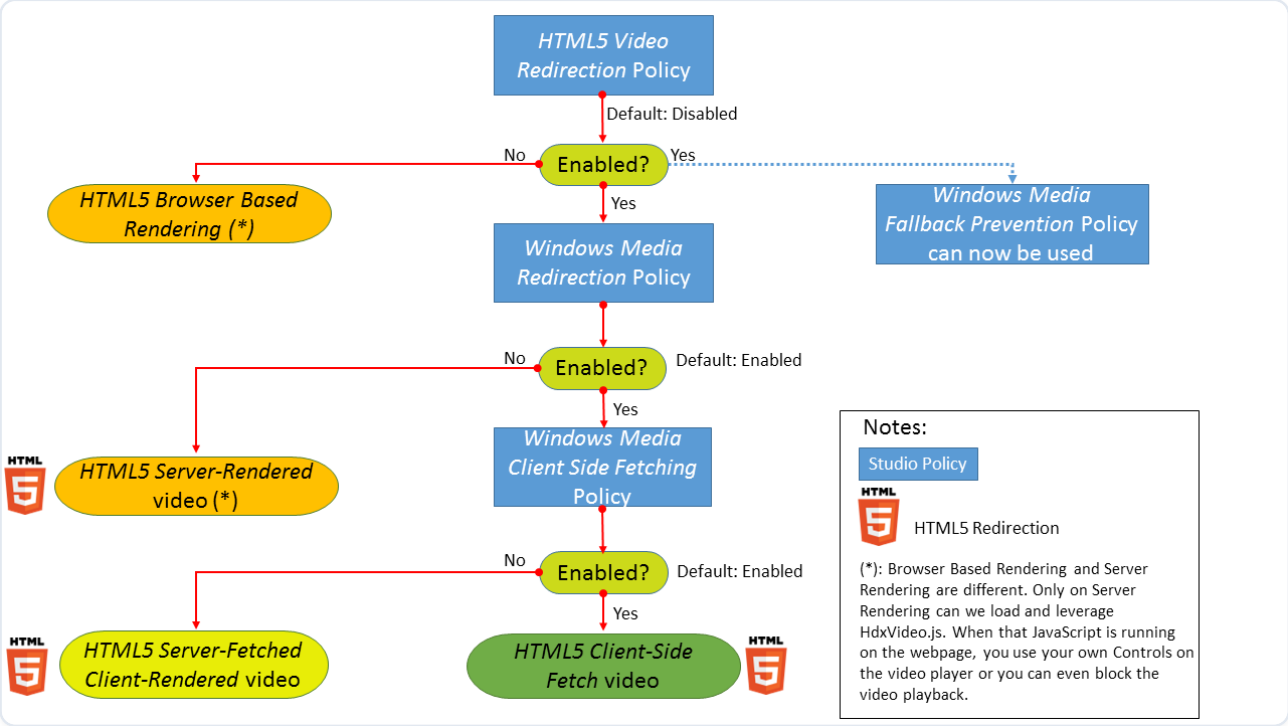
現在のユーザーセッションIDを見つけるには、Windowsコマンドラインで**qwinsta**コマンドを発行します。

HTML5ビデオリダイレクト

Citrix Virtual Apps and Desktops™サーバーがHTML5マルチメディアWebコンテンツをユーザーに配信する方法を制御し、最適化します。

デフォルトでは、この設定は無効になっています。

HTML5リダイレクトのグラフィックイメージ



このリリースでは、この機能は制御されたWebページでのみ利用可能です。HTML5マルチメディアコンテンツが利用可能なWebページ（例: 社内トレーニングサイトのビデオ）にJavaScriptを追加する必要があります。

HTML5ビデオリダイレクトを構成するには:

1. VDAインストール時の%Program Files%/Citrix/ICA Service/HTML5 Video Redirectionから、ファイル**HdxVideo.js**を社内Webページの場所にコピーします。
2. この行をWebページに挿入します（Webページに他のスクリプトがある場合は、それらのスクリプトの前に**HdxVideo.js**を含めます）。 `<script src="HdxVideo.js" type="text/javascript"\></script>`

注：HdxVideo.jsがWebページと同じ場所にない場合は、**src**属性を使用してそのフルパスを指定します。

JavaScript が管理対象のウェブページに追加されておらず、ユーザーが HTML5 ビデオを再生する場合を考えてみましょう。この場合、Citrix Virtual Apps and Desktops はサーバー側レンダリングにデフォルト設定されます。

HTML5ビデオのリダイレクトを機能させるには、***Windows Media Redirection***を許可します。このポリシーは、Server Fetch Client Renderには必須であり、Client Side Fetchingには必要です。Client Side Fetchingは、*Windows Media client-side content fetching*も許可されている必要があります。

Microsoft Edgeはこの機能をサポートしていません。

HdxVideo.jsは、ブラウザのHTML5プレーヤーコントロールを独自のコントロールに置き換えます。特定のWebサイトでHTML5ビデオリダイレクトポリシーが有効になっていることを確認するには、プレーヤーコントロールを、**HTML5ビデオリダイレクト**ポリシーが禁止されているシナリオと比較します。

（ポリシーが許可されている場合のCitrixカスタムコントロール）



（ポリシーが禁止されているか、構成されていない場合のネイティブWebページコントロール）



以下のビデオコントロールがサポートされています。

- 再生
- 一時停止
- シーク
- 繰り返し
- オーディオ
- 全画面表示

HTML5ビデオリダイレクトテストページを表示できます。

TLS、HTML5ビデオリダイレクト、およびブラウザーコンテンツリダイレクト

HTML5ビデオリダイレクトは、次の目的で使用できます。

- HTTPS Webサイトからのビデオのリダイレクト
- または
- Webサイト全体をリダイレクトするためのブラウザーコンテンツリダイレクト

これらのWebサイトに挿入されたJavaScriptは、VDAで実行されているCitrix HDX HTML5 Video Redirection Service (WebSocketService.exe) へのTLS接続を確立する必要があります。VDAの証明書ストアにあるCitrix HDX HTML5 Video Redirection Serviceは、次の目的で2つのカスタム証明書を生成します。

- ビデオのリダイレクトを実現する
- WebページのTLS整合性を維持する

HdxVideo.jsは、Secure WebSocketsを使用して、VDAで実行されているWebSocketService.exeと通信します。このプロセスはローカルシステムアカウントとして実行され、SSL終端とユーザーセッションマッピングを行います。

WebSocketService.exeは、127.0.0.1ポート9001でリッスンしています。

ビデオ品質の制限

この設定は、Windows Mediaにのみ適用され、HTML5には適用されません。**WAN経由のWindows Mediaマルチメディアリダイレクトの最適化**を有効にする必要があります。

この設定は、HDX™接続で許可される最大ビデオ品質レベルを指定します。設定すると、最大ビデオ品質は指定された値に制限され、環境内でマルチメディアのサービス品質 (QoS) が維持されます。

デフォルトでは、この設定は構成されていません。

許可される最大ビデオ品質レベルを制限するには、次のいずれかのオプションを選択します。

- 1080p/8.5Mbps
- 720p/4.0Mbps
- 480p/720Kbps
- 380p/400Kbps
- 240p/200Kbps

同じサーバーで複数のビデオを同時に再生すると、大量のリソースが消費され、サーバーのスケーラビリティに影響を与える可能性があります。

Microsoft Teamsのリダイレクト

この設定は、HDXテクノロジーに基づいてMicrosoft Teamsの最適化を有効にします。

このポリシーが有効で、サポートされているバージョンのCitrix Workspace™アプリを使用している場合、このレジストリキーはVDAで**1**に設定されます。Microsoft Teamsアプリケーションは、VDIモードでロードするためにこのキーを読み取ります。 レジストリキーを手動で設定する必要はありません。

HKEY_CURRENT_USER\Software\Citrix\HDXMediaStream

名前: MSTeamsRedirSupport

値: DWORD (1 - オン, 0 - オフ)

> **注：**

> Web Studioでポリシーが利用できない古いバージョンのController（例: バージョン7.15）で、バージョン1906.2以降のVDAを使用しているとします。この場合、HDX最適化はVDAでデフォルトで有効になっています。Workspaceアプリのバージョンが1907以降の場合、Microsoft Teamsは最適化モードで起動します。7.15 LTSR ControllerとCR VDAを混在させる場合の注意点については、Knowledge Centerの記事CTX205549を参照してください。

> この場合、特定のユーザーに対して機能を無効にするには、レジストリ設定を上書きできます。ユーザーの組織単位にログオンスクリプトを適用するグループポリシーを使用して、レジストリ設定を上書きします。

> デフォルトでは、Microsoft Teamsリダイレクトは有効になっています。

マルチメディア会議

この設定により、ビデオ会議アプリケーションによる最適化されたWebカメラリダイレクトテクノロジーの使用を許可または禁止します。

デフォルトでは、ビデオ会議のサポートは許可されています。

この設定をポリシーに追加する際は、**Windows Mediaリダイレクト**設定が存在し、**許可**（デフォルト）に設定されていることを確認してください。

マルチメディア会議を使用する場合は、次の条件が満たされていることを確認してください。

- マルチメディア会議に使用するWebカメラのメーカー提供ドライバーがクライアントにインストールされていること。
- ビデオ会議セッションを開始する前に、Webカメラをユーザーデバイスに接続します。サーバーは、一度に1つのインストールされたWebカメラのみを使用します。複数のWebカメラがユーザーデバイスにインストールされている場合、サーバーは各Webカメラを順番に試行します。この試行は、ビデオ会議セッションが正常に作成されるまで続行されます。

汎用USBリダイレクトを使用してWebカメラをリダイレクトする場合、このポリシーは必要ありません。その場合は、WebカメラドライバーをVDAにインストールしてください。

WAN経由のWindows Mediaマルチメディアリダイレクトの最適化

この設定はWindows Mediaにのみ適用され、HTML5には適用されません。この設定により、以下が可能になります。

- リアルタイムマルチメディアトランスコーディング
- 劣化したネットワーク経由でのモバイルデバイスへのオーディオおよびビデオメディアストリーミングを許可
- WAN経由でWindows Mediaコンテンツが配信される方法を改善することで、ユーザーエクスペリエンスを向上させます。

デフォルトでは、WAN経由でのWindows Mediaコンテンツの配信は最適化されています。

この設定をポリシーに追加する際は、**Windows Media Redirection**設定が存在し、**Allowed**に設定されていることを確認してください。

この設定が有効になっている場合、メディアストリーミングを可能にするために、必要に応じてリアルタイムのマルチメディアトランスコーディングが自動的に展開されます。また、極端なネットワーク条件下でもシームレスなユーザーエクスペリエンスを提供します。

WAN経由でのWindows Mediaマルチメディアリダイレクトの最適化にGPUを使用する

この設定はWindows Mediaにのみ適用され、リアルタイムのマルチメディアトランスコーディングをVirtual Delivery Agent (VDA) のグラフィックス処理ユニット (GPU) で実行できるようにします。これにより、サーバーのスケーラビリティが向上します。GPUトランスコーディングは、VDAがハードウェアアクセラレーションをサポートするGPUを搭載している場合にのみ利用可能です。そうでない場合、トランスコーディングはCPUにフォールバックします。

注: GPUトランスコーディングはNVIDIA GPUでのみサポートされています。

デフォルトでは、WAN経由でのWindows Mediaコンテンツの配信を最適化するためにVDA上のGPUを使用することは禁止されています。

この設定をポリシーに追加する際は、以下の設定が存在し、Allowedに設定されていることを確認してください。

- **Windows Mediaリダイレクト**
- **WAN経由でのWindows Mediaマルチメディアリダイレクト設定の最適化**

Windows Mediaフォールバック防止

この設定は、ブラウザコンテンツリダイレクト、HTML5、およびWindows Mediaに適用されます。HTML5をサポートするには、**HTML5 video redirection**ポリシーを**Allowed**に設定します。

管理者は、**Windows Media fallback prevention**ポリシー設定を使用して、ストリーミングコンテンツをユーザーに配信するために試行される方法を指定できます。

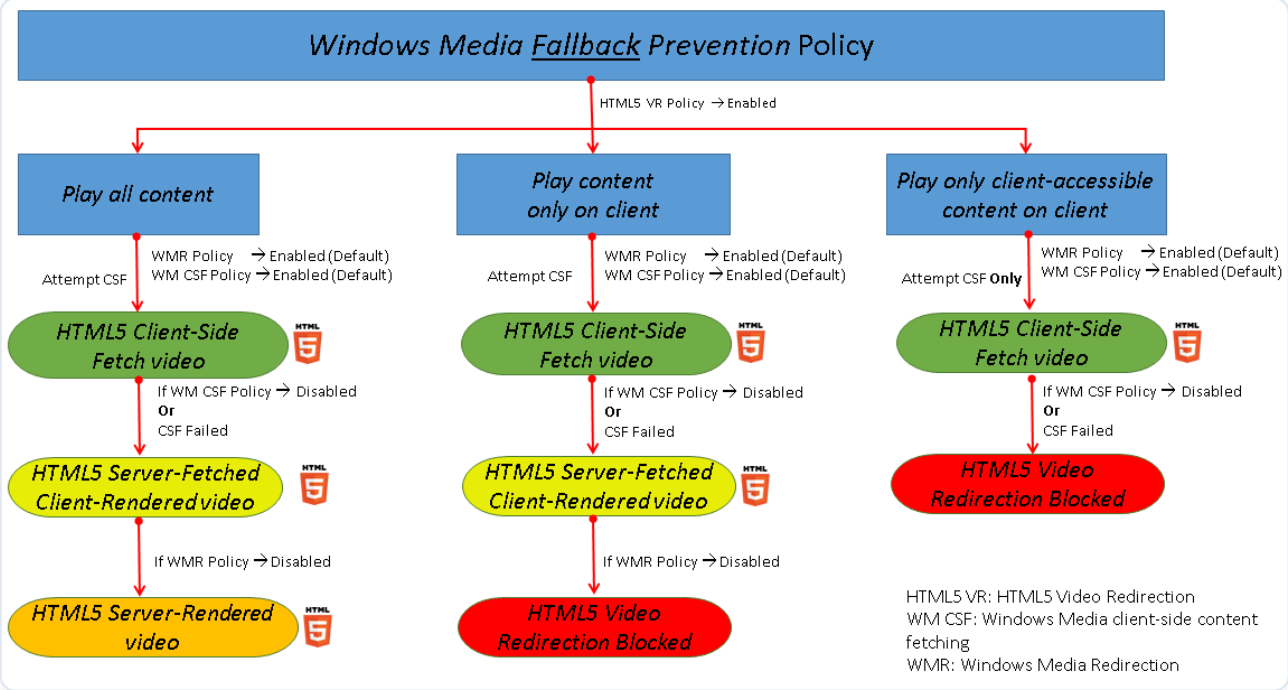
デフォルトでは、この設定は構成されていません。設定が「構成されていません」に設定されている場合、動作は**すべてのコンテンツを再生**と同じになります。

この設定を構成するには、次のいずれかのオプションを選択します。

- **すべてのコンテンツを再生する**。クライアント側でのコンテンツ取得を試行し、次にWindows Mediaリダイレクトを試行します。失敗した場合は、サーバーでコンテンツを再生します。
- **すべてのコンテンツをクライアントでのみ再生する**。クライアント側での取得を試行し、次にWindows Mediaリダイレクトを試行します。失敗した場合、コンテンツは再生されません。
- **クライアントでクライアントがアクセス可能なコンテンツのみを再生する**。クライアント側での取得のみを試行します。失敗した場合、コンテンツは再生されません。

コンテンツが再生されない場合、プレーヤーウィンドウに次のエラーメッセージが表示されます（デフォルトの表示時間は5秒）。

```
"Company has blocked video because of lack of resources"
```



このエラーメッセージの表示時間は、VDA上の次のレジストリキーでカスタマイズできます。レジストリエントリが存在しない場合、表示時間はデフォルトで5秒になります。

レジストリパスは、VDAのアーキテクチャによって異なります。

\HKLM\SOFTWARE\Wow6432Node\Citrix\HdxMediastream

または

\HKLM\SOFTWARE\Citrix\HdxMediastream

レジストリキー：

名前: VideoLoadManagementErrDuration

種類: DWORD

範囲: 1 - DWORD制限まで（デフォルト = 5）

単位: 秒

Windows Mediaクライアント側コンテンツ取得

この設定はHTML5とWindows Mediaの両方に適用されます。この設定により、ユーザーデバイスは、XenAppまたはXenDesktop®ホストサーバーを介さずに、インターネットまたはイントラネット上のソースプロバイダーからマルチメディアファイルを直接ストリーミングできるようになります。

デフォルトでは、この設定は**許可**されています。この設定を許可すると、ネットワーク使用率とサーバーのスケーラビリティが向上します。この改善は、メディアに関するあらゆる処理をホストサーバーからユーザーデバイスに移動することで実現されます。また、Microsoft DirectShowやMedia Foundationなどの高度なマルチメディアフレームワークをユーザーデバイスにインストールする必要がなくなります。ユーザーデバイスには、URLからファイルを再生する機能のみが必要です。

この設定をポリシーに追加するときは、**Windows Mediaリダイレクト**設定が存在し、**許可**に設定されていることを確認してください。**Windows Mediaリダイレクト**が無効になっている場合、ソースプロバイダーからユーザーデバイスへのマルチメディアファイルの直接ストリーミングも無効になります。

Windows Mediaリダイレクト

この設定はHTML5とWindows Mediaの両方に適用され、サーバーがストリーミングオーディオとビデオをユーザーに配信する方法を制御および最適化します。

デフォルトでは、この設定は**許可**されています。HTML5の場合、ポリシー**HTML5ビデオのリダイレクト**が**禁止**されている場合、この設定は有効になりません。

この設定が有効になっている場合、サーバーからレンダリングされるオーディオとビデオの品質は、ユーザーデバイスでローカルに再生されるオーディオとビデオに匹敵するレベルに向上します。サーバーはマルチメディアを元の圧縮形式でクライアントにストリーミングし、ユーザーデバイスがメディアを解凍してレンダリングできるようにします。

Windows Mediaリダイレクトは、Microsoft DirectShow、DirectX Media Objects (DMO)、およびMedia Foundationの標準に準拠するコーデックでエンコードされたマルチメディアファイルを最適化します。特定のマルチメディアファイルを再生するには、そのマルチメディアファイルのエンコード形式と互換性のあるコーデックがユーザーデバイスに存在する必要があります。

デフォルトでは、Citrix Workspaceアプリでオーディオは無効になっています。ユーザーがICA®セッションでマルチメディアアプリケーションを実行できるようにするには、オーディオをオンにするか、Citrix Workspaceアプリインターフェイスでオーディオをオンにする権限をユーザーに付与します。

Windows Mediaリダイレクトを使用してメディアを再生したときの品質が、基本的なICA圧縮と通常のオーディオを使用してレンダリングした場合よりも悪い場合にのみ、**禁止**を選択してください。このような状況はまれですが、たとえばキーフレームの頻度が低いメディアの場合など、低帯域幅の条件下で発生する可能性があります。

Windows Mediaリダイレクトのバッファサイズ

この設定はレガシーであり、HTML5には適用されません。

この設定は、マルチメディアアクセラレーションのバッファサイズを1～10秒で指定します。

デフォルトでは、バッファサイズは5秒です。

Windows Mediaリダイレクトのバッファサイズの使用

この設定はレガシーであり、HTML5には適用されません。

この設定は、**Windows Media Redirection buffer size** 設定で指定されたバッファサイズの使用を有効または無効にします。

デフォルトでは、指定されたバッファサイズは使用されません。

この設定が無効になっている場合、または**Windows Media Redirection buffer size** 設定が構成されていない場合、サーバーはデフォルトのバッファサイズ値（5秒）を使用します。

マルチストリーム接続ポリシー設定

「**マルチストリーム接続**」セクションには、セッション内の複数のICA®接続のサービス品質の優先順位付けを管理するためのポリシー設定が含まれています。

> **注：**
>
> マルチストリーム接続ポリシーが有効になっている場合、MTU検出はサポートされません。

UDP経由のオーディオ

この設定は、サーバー上でのUDP経由のオーディオを許可または禁止します。

デフォルトでは、サーバー上でのUDP経由のオーディオは許可されています。

有効にすると、この設定はサーバー上でUDPポートを開き、UDP経由のオーディオリアルタイムトランスポートを使用するように構成されたすべての接続をサポートします。

オーディオUDPポート範囲

この設定は、Virtual Delivery Agent (VDA) によって使用されるポート番号の範囲（最小ポート番号、最大ポート番号）を指定します。この指定は、ユーザーデバイスとの間でオーディオパケットデータを交換するのに役立ちます。VDAは、ユーザーデバイスとデータを交換するために各UDPポートペアを使用しようとします。最小値から開始し、その後の試行ごとに2ずつ増やします。各ポートは、インバウンドトラフィックとアウトバウンドトラフィックの両方を処理します。

デフォルトでは、この範囲は16500,16509に設定されています。

マルチポートポリシー

この設定は、ICAトラフィックに使用するTCPポートを指定し、各ポートのネットワーク優先順位を確立します。

デフォルトでは、プライマリポート (2598) は高優先度です。

ポートを構成するとき、次の優先順位を割り当てることができます。

- **非常に高い:** ウェブカメラ会議などのリアルタイムアクティビティ用
- **高:** 画面、キーボード、マウスなどの対話型要素用
- **中:** クライアントドライブマッピングなどのバルク処理用
- **低:** 印刷などのバックグラウンドアクティビティ用

各ポートには一意の優先順位が必要です。たとえば、CGPポート1とCGPポート3の両方に「非常に高」の優先順位を割り当てることはできません。

ポートを優先順位付けから削除するには、ポート番号を0に設定します。プライマリポートを削除したり、その優先順位レベルを変更したりすることはできません。

この設定を構成するときは、サーバーを再起動してください。この設定は、**Multi-Stream computer**設定ポリシー設定が有効になっている場合にのみ有効になります。

マルチストリーム コンピューター設定

この設定は、サーバー上でMulti-Streamを有効または無効にします。

デフォルトでは、Multi-Streamは無効になっています。Citrix SD-WAN™またはサードパーティ製ルーターを使用して目的のQuality of Serviceを実現する場合は、Multi-Stream computerポリシー設定を構成してください。

Multi-Streamが有効になっている場合、Adaptive Transportの機能であるMTU Discoveryはサポートされません。

この設定を構成するときは、変更が有効になるようにサーバーを再起動してください。

> **重要:**
>
> このポリシー設定を、セッション全体の帯域幅制限などの帯域幅制限ポリシー設定と組み合わせて使用すると、予期しない結果が生じる可能性があります。この設定をポリシーに含める場合は、帯域幅制限設定が含まれていないことを確認してください。

マルチストリーム ユーザー設定

この設定は、ユーザーデバイス上でMulti-Streamを有効または無効にします。

デフォルトでは、Multi-Streamはすべてのユーザーに対して無効になっています。Citrix SD-WANまたはサードパーティ製ルーターを使用して目的のQuality of Serviceを実現する場合は、Multi-Stream user設定を構成してください。

この設定は、**マルチストリームコンピューター**設定ポリシー設定が有効になっているホストでのみ有効になります。

> **重要:**
>
> このポリシー設定を、全体的なセッション帯域幅制限などの帯域幅制限ポリシー設定と併用すると、予期しない結果が生じる可能性があります。この設定をポリシーに含める場合は、帯域幅制限設定を含めないようにしてください。

マルチストリーム仮想チャネル割り当て設定

この設定は、マルチストリームが使用されている場合に仮想チャネルが割り当てられるICAストリームを指定します。

これらの設定を構成しない場合、仮想チャネルはデフォルトのストリームに保持されます。仮想チャネルをICAストリームに割り当てるには、仮想チャネル名の横にある**ストリーム番号**リストから目的のストリーム番号（0、1、2、3）を選択します。

環境でカスタム仮想チャネルが使用されている場合は、**追加**をクリックし、**仮想チャネル**の下のテキストボックスに仮想チャネル名を指定し、その横にある**ストリーム番号**リストから目的のストリーム番号を選択します。指定する名前は、フレンドリ名ではなく、実際の仮想チャネル名である必要があります。たとえば、Citrix Browser AccelerationではなくCTXSBRです。

これらの設定は、マルチストリームコンピューター設定を有効にした場合にのみ有効になります。

デフォルトでは、仮想チャネルとそのストリーム割り当ては次のとおりです。

- AppFlow®: 2
- オーディオ: 0
- ブラウザコンテンツリダイレクト: 2
- クライアントCOMポートマッピング: 3
- クライアントドライブマッピング: 2
- クライアントプリンターマッピング: 3
- クリップボード: 2
- CTXDND: 1 (**注:** これは、Citrixセッションとローカルエンドポイント間でファイルをドラッグアンドドロップする機能をサポートします。)
- DVCプラグイン (DVCプラグインのフレンドリ名から自動生成された静的VC名、または管理者によって割り当てられたもの): 2
- エンドユーザーエクスペリエンス監視: 1
- ファイル転送 (HTML5 Receiver): 2
- 汎用データ転送: 2
- ICA制御: 1
- 入力メソッドエディター: 1
- レガシー クライアント プリンター マッピング (COM1): 1, 3
- レガシー クライアント プリンター マッピング (COM2): 2, 3
- レガシー クライアント プリンター マッピング (LPT1): 1, 3
- レガシー クライアント プリンター マッピング (LPT2): 2, 3

- ライセンス管理: 1
- Microsoft Teams/WebRTC リダイレクト: 1
- モバイルレシーバー: 1
- マルチタッチ: 1
- ポートフォワーディング: 2
- リモートオーディオおよびビデオ拡張機能 (RAVE): 2
- シームレス (透過ウィンドウ統合): 1
- センサーと位置情報: 1
- スマートカード: 1
- Thinwire グラフィック: 1
- 透過UI統合/ログオンステータス: 2
- TWAIN リダイレクト: 2
- USB: 2
- ゼロ遅延フォントおよびキーボード: 2
- ゼロ遅延データチャネル: 2

仮想チャネルの割り当てと優先度について詳しくは、Knowledge Center の記事 CTX131001 を参照してください。

ポートリダイレクトポリシー設定

「**ポートリダイレクト**」セクションには、クライアントLPTおよびCOMポートマッピングのポリシー設定が含まれています。

Virtual Delivery Agentのバージョン**7.0より前**の場合、ポートリダイレクトを構成するには、以下のポリシー設定を使用します。VDAバージョン**7.0から7.8まで**の場合、これらの設定はレジストリを使用して構成します。「レジストリを使用したCOMポートおよびLPTポートリダイレクト設定の構成」を参照してください。VDAバージョン**7.9**の場合、以下のポリシー設定を使用します。

クライアントCOMポートの自動接続

この設定は、ユーザーがサイトにログオンしたときに、ユーザーデバイス上のCOMポートの自動接続を有効または無効にします。

デフォルトでは、クライアントCOMポートは自動的に接続されません。

クライアントLPTポートの自動接続

この設定は、ユーザーがサイトにログオンしたときに、ユーザーデバイス上のLPTポートの自動接続を有効または無効にします。

デフォルトでは、クライアントLPTポートは自動的に接続されません。

クライアントCOMポートリダイレクト

この設定は、ユーザーデバイス上のCOMポートへのアクセスを許可または禁止します。

デフォルトでは、COMポートリダイレクトは禁止されています。

以下のポリシー設定が関連しています。

- COMポートリダイレクト帯域幅制限
- COMポートリダイレクトの帯域幅制限（パーセント）

クライアントLPTポートリダイレクト

この設定は、ユーザーデバイス上のLPTポートへのアクセスを許可または禁止します。

デフォルトでは、LPTポートリダイレクトは禁止されています。

LPTポートは、LPTポートに印刷ジョブを送信するレガシーアプリケーションのみが使用します。これらのポートは、ユーザーデバイス上の印刷オブジェクトに印刷ジョブを送信するレガシーアプリケーションでは使用されません。今日のほとんどのアプリケーションは、プリンターオブジェクトに印刷ジョブを送信できます。このポリシー設定は、LPTポートに印刷するレガシーアプリケーションをホストするサーバーにのみ必要です。

なお、クライアントCOMポートリダイレクトは双方向ですが、LPTポートリダイレクトは出力のみであり、ICAセッション内では`\\client\LPT1`および`\\client\LPT2`に制限されます。

関連するポリシー設定は次のとおりです。

- LPTポートリダイレクト帯域幅制限
- LPTポートリダイレクトの帯域幅制限（パーセント）

印刷ポリシー設定

印刷セクションには、クライアント印刷を管理するためのポリシー設定が含まれています。

クライアントプリンターリダイレクト

この設定は、ユーザーがセッションにログオンしたときに、クライアントプリンターがサーバーにマップされるかどうかを制御します。

デフォルトでは、クライアントプリンターのマッピングは許可されています。この設定が無効になっている場合、セッション用のPDFプリンターは自動作成されません。

関連するポリシー設定: クライアントプリンターの自動作成

デフォルトプリンター

この設定は、ユーザーデバイス上のデフォルトプリンターがセッションでどのように確立されるかを指定します。

デフォルトでは、ユーザーの現在のプリンターがセッションのデフォルトプリンターとして使用されます。

デフォルトプリンターに現在のRemote Desktop ServicesまたはWindowsユーザープロファイル設定を使用するには、「ユーザーのデフォルトプリンターを調整しない」を選択します。このオプションを選択した場合、デフォルトプリンターはプロファイルに保存されず、他のセッションまたはクライアントプロパティに従って変更されることもありません。セッション内のデフォルトプリンターは、セッションで最初に自動作成されたプリンターであり、次のいずれかです。

- **コントロールパネル > デバイス**と**プリンター**でWindowsサーバーにローカルに追加された最初のプリンター。
- サーバーにローカルに追加されたプリンターがない場合、最初に自動作成されたプリンター。

このオプションを使用すると、プロファイル設定を通じてユーザーに最も近いプリンターを提示できます（近接印刷として知られています）。

プリンターの割り当て

この設定は、デフォルトプリンターとセッションプリンターの設定の代替手段を提供します。個別のデフォルトプリンターとセッションプリンターの設定を使用して、サイト、大規模グループ、または組織単位の動作を構成します。**プリンター割り当て**設定を使用して、多数のプリンターを複数のユーザーに割り当てます。

この設定は、リストされたユーザーデバイス上のデフォルトプリンターがセッションでどのように確立されるかを指定します。

デフォルトでは、ユーザーの現在のプリンターがセッションのデフォルトプリンターとして使用されます。

各ユーザーデバイスのセッションで自動作成されるネットワークプリンターも指定します。デフォルトでは、プリンターは指定されていません。

- デフォルトプリンターの値を設定する場合：

ユーザーデバイスの現在のデフォルトプリンターを使用するには、「Do not adjust」を選択します。

デフォルトプリンターに現在のRemote Desktop ServicesまたはWindowsユーザープロファイル設定を使用するには、「Do no adjust」を選択します。このオプションを選択すると、デフォルトプリンターはプロファイルに保存されず、他のセッションまたはクライアントのプロパティに応じて変更されません。セッション内のデフォルトプリンターは、セッションで最初に自動作成されたプリンターであり、次のいずれかです。

- Windowsサーバーにローカルで追加された最初のプリンター（**コントロールパネル > デバイス**とプリンター）。
- サーバーにローカルで追加されたプリンターがない場合、最初に自動作成されたプリンター。

- セッションプリンターの値を設定する場合：プリンターを追加するには、自動作成するプリンターのUNCパスを入力します。プリンターを追加した後、ログオンするたびに現在のセッションにカスタマイズされた設定を適用できます。

プリンターの自動作成イベントログ設定

この設定は、プリンターの自動作成プロセス中にログに記録されるイベントを指定します。エラーや警告をログに記録しない、エラーのみをログに記録する、またはエラーと警告をログに記録する、のいずれかを選択できます。

デフォルトでは、エラーと警告がログに記録されます。

警告の例としては、プリンターのネイティブドライバーをインストールできず、代わりにUniversal print driverがインストールされるイベントがあります。このシナリオでUniversal print driverを使用するには、Universal print driverの使用設定を「Use universal printing only」または「Use universal printing only if the requested driver is unavailable」に構成します。

セッションプリンター

この設定は、セッションで自動作成されるネットワークプリンターを指定します。ICA/HDXセッション内では、Citrix Print Managerサービス（CpSvc.exe）が、**セッションプリンター**ポリシー設定で指定された各ネットワークプリンターに対して、セッションログオン中にネットワークプリンター接続を作成します。セッションログオフ中にプリンターを削除します。デフォルトでは、プリンターは指定されていません。

セッションプリンターポリシー設定では、ネットワークプリンターはWindows Print ServerまたはCitrix Universal™ Print Server上に存在できます。

- **Windows Print Server:** 1つ以上のネットワークプリンターを共有します。また、ネットワークプリンターを使用するために必要なネイティブプリンタードライバーも備えています。
- **Universal Print Server:** Citrix Universal Print Serverソフトウェアがインストールされている Windows Print Server。

Windows Print Server を使用する場合、Citrix Print Manager サービスはネイティブプリンタードライバーを使用してネットワークプリンター接続を作成します。Citrix Virtual Apps™ サーバーには、ネイティブプリンタードライバーがインストールされている必要があります。

Citrix Universal Print Server を使用する場合、Citrix Print Manager サービスは、ネイティブプリンタードライバー、Citrix Universal Printer Driver、または Citrix Universal XPS Printer Driver のいずれかを使用してネットワークプリンター接続を作成します。使用するドライバーは、Universal Print Driver の使用ポリシー設定によって制御されます。

すべての Windows プリンタードライバーは現在、v3 または v4 ドライバーバージョンのいずれかに分類されます。詳細については、「Support for the Microsoft V3 and V4 Printer Driver Architectures」を参照してください。

セッションプリンターを追加し、それらがセッションに表示されることを確認するには、次の手順を実行します。

1. Web Studio にサインインし、左ペインで を選択し、 タブをクリックします。
2. **セッションプリンター**ポリシーを有効にします。
3. ポリシーで、セッションプリンターを追加します。プリンターを追加するには、自動作成するプリンターのUNCパスを入力します。プリンターを追加した後、ログオンするたびに現在のセッションにカスタマイズされた設定を適用できます。セッションプリンターがリストに表示されている必要があります。
4. ポリシーが設定された後、公開されたアプリケーションにセッションプリンターが表示されない場合があります。この問題は、Citrix Virtual Apps サーバーにプリンタードライバーがないか、ポリシーが作成されたものの有効になっていないために発生する可能性があります。

   > **注：**
   >
   > セッションプリンターにネイティブプリンタードライバーが必要で、そのネイティブプリンタードライバーが VDA にインストールされていない場合、セッションプリンターはセッションに作成されない可能性があります。

5. 公開されたデスクトップを起動し、 > でセッションプリンターを手動で追加します。

6. これが失敗した場合は、Citrix Virtual Apps サーバーとプリントサーバー間の通信を調査します。RDP を使用してテストを実行することを検討してください。

プリンターが作成されるのを待つ

Delivery Controller のポリシーを使用して、Citrix Virtual Desktops でこの機能を有効にします。

プリンターの作成を待機する (サーバーデスクトップ):

この設定により、セッションへの接続を遅延させ、クライアントリダイレクトされたプリンターを自動作成できます。

デフォルトでは、接続遅延は発生しません。

プリンターの作成を待機する (Citrix Virtual Apps):

次の PowerShell コマンドレットを実行すると、マルチセッションホストで実行されている仮想アプリへの接続を遅延させ、アプリケーションが開かれる前にクライアントリダイレクトされたプリンターを自動作成できます。

```
Set-BrokerApplication -Name <VirtualAppName> -WaitForPrinterCreation $true
```

デフォルトでは、接続遅延は発生しません。

クライアントプリンターポリシー設定

クライアントプリンターセクションには、クライアントプリンターのポリシー設定が含まれています。これには、クライアントプリンターの自動作成、プリンタープロパティの保持、プリントサーバーへの接続に関する設定が含まれます。

クライアントプリンターの自動作成

この設定は、自動作成されるクライアントプリンターを指定します。この設定は、デフォルトのクライアントプリンター自動作成設定を上書きします。

デフォルトでは、すべてのクライアントプリンターが自動作成されます。

この設定は、**クライアントプリンターリダイレクト**設定が存在し、**許可**に設定されている場合にのみ有効になります。

この設定をポリシーに追加する際は、オプションを選択してください。

- **すべてのクライアントプリンターを自動作成**すると、ユーザーデバイス上のすべてのプリンターが自動的に作成されます。
- **クライアントのデフォルトプリンターのみを自動作成**すると、ユーザーデバイスでデフォルトプリンターとして選択されているプリンターのみが自動的に作成されます。

- **ローカル（非ネットワーク）クライアントプリンターのみを自動作成**すると、LPT、COM、USB、TCP/IP、またはその他のローカルポートを介してユーザーデバイスに直接接続されているプリンターのみが自動的に作成されます。
- **クライアントプリンターを自動作成しない**を選択すると、ユーザーがログオンしたときにすべてのクライアントプリンターの自動作成が無効になります。このオプションを選択すると、クライアントプリンターの自動作成に関するRemote Desktop Services (RDS) の設定が、優先度の低いポリシーのこの設定を上書きします。

汎用ユニバーサルプリンターの自動作成

この設定は、セッション用の汎用Citrix Universal™ Printerオブジェクトの自動作成を有効または無効にします。これらのセッションには、ユニバーサル印刷と互換性のあるユーザーデバイスが使用されているセッションのみが含まれます。

デフォルトでは、汎用ユニバーサルプリンターオブジェクトは自動作成されません。

関連するポリシー設定は次のとおりです。

- ユニバーサルプリントドライバーの使用状況
- ユニバーサルドライバーの優先順位

PDFユニバーサルプリンターの自動作成

この設定は、以下のセッションでCitrix PDFプリンターの自動作成を有効または無効にします。

- Windows向けCitrix Workspaceアプリ（VDA 7.19以降）
- HTML5 用 Citrix Workspace™ アプリ
- Chrome向けCitrix Workspaceアプリ

デフォルトでは、Citrix PDFプリンターは自動作成されません。

クライアントプリンター名

この設定は、自動作成されたクライアントプリンターの命名規則を選択します。

デフォルトでは、標準のプリンター名が使用されます。

「**標準プリンター名**」を選択すると、「HPLaserJet 4 from client name in session 3」のようなプリンター名が使用されます。

「**レガシープリンター名**」を選択すると、旧式のクライアントプリンター名が使用され、製品のXenDesktopバージョンに存在したレガシープリンター名との下位互換性が維持されます。このオプションは、現在のCitrix Virtual Apps and Desktopsバージョンの製品でも使用できます。レガ

シープリンター名の例は「Client/clientname#/HPLaserJet 4」です。このオプションはセキュリティが低下します。

Citrix Workspaceアプリ for HTML5から起動したセッションでCitrix PDFプリンターを使用する場合、「**クライアントプリンター名**」設定をデフォルトにするか、「**標準プリンター名**」を選択してください。「**レガシープリンター名**」を選択すると、Citrix Workspaceアプリ for HTML5はCitrix PDFプリンターオプションをサポートしません。

印刷サーバーへの直接接続

この設定は、仮想デスクトップまたはサーバーホスティングアプリケーションからクライアントプリンター用の印刷サーバーへの直接接続を有効または無効にします。ここで、クライアントプリンターはアクセス可能なネットワーク共有でホストされます。

デフォルトでは、直接接続が有効になっています。

ネットワークプリントサーバーが仮想デスクトップまたはサーバーホスティングアプリケーションからWANを介していない場合は、直接接続を有効にします。ネットワークプリントサーバーと仮想デスクトップまたはサーバーホスティングアプリケーションが同じLAN上にある場合、直接通信により印刷が高速化されます。

ネットワークがWANを介している場合、または大幅な遅延や帯域幅の制限がある場合は、直接接続を無効にします。印刷ジョブはユーザーデバイスを介してルーティングされ、そこでネットワークプリントサーバーにリダイレクトされます。ユーザーデバイスに送信されるデータは圧縮されるため、WANを介してデータが転送される際の帯域幅の消費が少なくなります。

2つのネットワークプリンターが同じ名前を持つ場合、ユーザーデバイスと同じネットワーク上のプリンターが使用されます。

プリンタードライバーのマッピングと互換性

この設定は、自動作成されたクライアントプリンターのドライバー置換ルールを指定します。

この設定は、Microsoft OneNoteおよびXPS Document Writerを自動作成されたクライアントプリンターリストから除外するように構成されています。

ドライバー置換ルールを定義する際、指定されたドライバーでプリンターが作成されることを許可または禁止できます。また、作成されたプリンターがユニバーサルプリントドライバーのみを使用することを許可することもできます。ドライバー置換は、ユーザーデバイスが提供するプリンタードライバー名を上書きまたはマッピングし、サーバー上の同等のドライバーに置き換えます。これらのルールにより、サーバーアプリケーションは、サーバーと同じドライバーを持つがドライバー名が異なるクライアントプリンターにアクセスできるようになります。

次のことができます。

- ドライバーマッピングを追加する
- 既存のマッピングを編集する
- マッピングのカスタム設定を上書きする
- マッピングを削除する
- リスト内のドライバーエントリの順序を変更する

マッピングを追加する際は、クライアントプリンタードライバー名を入力し、置き換えたいサーバードライバーを選択します。

プリンタープロパティの保持

この設定は、プリンターのプロパティを保存するかどうか、およびどこに保存するかを指定します。

デフォルトでは、システムはプリンターのプロパティがユーザーデバイスに保存されるか（利用可能な場合）、またはユーザープロファイルに保存されるかを決定します。

この設定をポリシーに追加するときは、オプションを選択してください。

- クライアントデバイスのみに保存は、保存されない必須プロファイルまたは移動プロファイルを持つユーザーデバイス向けです。
- ユーザープロファイルのみに保持は、帯域幅によって制約されるユーザーデバイス（このオプションはネットワークトラフィックを削減します）およびログオン速度、またはレガシープラグインを使用するユーザー向けです。このオプションは、プリンターのプロパティをサーバー上のユーザープロファイルに保存し、ユーザーデバイスとのプロパティ交換を防ぎます。このオプションは、Remote Desktop Services (RDS) の移動プロファイルが使用されている場合にのみ適用されます。
- クライアントに保存されていない場合のみプロファイルに保持は、システムがプリンターのプロパティをどこに保存するかを決定できるようにします。プリンターのプロパティは、利用可能な場合はユーザーデバイスに、またはユーザープロファイルに保存されます。このオプションは最も柔軟ですが、ログオン時間を遅くしたり、システムチェックのために余分な帯域幅を使用したりする可能性があります。
- プリンターのプロパティを保持しないは、プリンターのプロパティの保存を防ぎます。

保持および復元されたクライアントプリンター

この設定は、ユーザーデバイス上のプリンターの保持と再作成を有効または無効にします。デフォルトでは、クライアントプリンターは自動的に保持および復元されます。

保持されたプリンターとは、次回のセッション開始時に再度作成される、または記憶されるユーザー作成のプリンターです。Citrix Virtual Apps™ が保持されたプリンターを再作成する場合、**クライアントプリンターの自動作成**設定を除くすべてのポリシー設定が考慮されます。

復元されたプリンターとは、管理者が完全にカスタマイズし、クライアントポートに永続的にアタッチされた保存状態を持つプリンターです。

CITRIX PDFユニバーサルプリンタードライバー

Citrix PDFユニバーサルプリンタードライバーを使用すると、Citrix Virtual Apps and Desktopsによって提供されるホスト型アプリケーションまたは仮想デスクトップで実行されているアプリケーションで開かれたドキュメントをユーザーが印刷できます。ユーザーが**Citrix PDFプリンター**オプションを選択すると、ドライバーはファイルをPDFに変換し、そのPDFをローカルデバイスに転送します。その後、PDFはローカルに接続されたプリンターから表示および印刷するために開かれます。PDFは、Citrixユニバーサルプリンティングでサポートされている形式の1つです（EMFおよびXPSに加えて）。 PDFプリンターは、Citrixポリシーを使用して有効化、構成、およびデフォルトとして設定できます。**Citrix PDFプリンター**オプションは、Windows、Chrome、およびHTML5向けのCitrix Workspaceアプリのユーザーが利用できます。

> **注：**
>
> Windowsエンドポイントには PDFビューアーが必要です。クライアントには、PDFファイルを開くためにWindowsにファイルタイプ関連付けが登録されているアプリケーションが必要です。

ドライバーポリシー設定

「**ドライバー**」セクションには、プリンタードライバーに関連するポリシー設定が含まれています。

インボックスプリンタードライバーの自動インストール

> **注**
>
> このリリースでは、このポリシーはVDAをサポートしていません。

> この設定は、以下のプリンタードライバーの自動インストールを有効または無効にします。

- Windowsインボックスドライバーセット

- `pnputil.exe /a`を使用してホストにステージングされたドライバーパッケージ

デフォルトでは、これらのドライバーは必要に応じてインストールされます。

ユニバーサルドライバーの優先順位

この設定は、リストの最初のエントリから始まる、ユニバーサルプリンタードライバーが使用される順序を指定します。

デフォルトでは、優先順位は次のとおりです。

- EMF
- XPS
- PCL5c (ピーシーエルファイブシー)
- PCL4
- PS

ドライバーの追加、編集、削除、およびリスト内のドライバーの順序変更が可能です。

ユニバーサルプリントドライバーの使用

この設定は、ユニバーサル印刷を使用するタイミングを指定します。

既定では、要求されたドライバーが利用できない場合にのみ、ユニバーサル印刷が使用されます。

ユニバーサル印刷では、標準のモデル固有ドライバーの代わりに汎用プリンタードライバーが使用されるため、ホストコンピューターでのドライバー管理の負担が軽減される可能性があります。ユニバーサル印刷ドライバーの可用性は、ユーザーデバイス、ホスト、および印刷サーバーソフトウェアの機能によって異なります。特定の構成では、ユニバーサル印刷が利用できない場合があります。

この設定をポリシーに追加するときは、次の表からオプションを選択します。

オプション	説明
プリンターモデル固有のドライバーのみを使用する	クライアントプリンターが、サインイン時に自動作成される標準のモデル固有ドライバーのみを使用することを指定します。要求されたドライバーが利用できない場合、クライアントプリンターは自動作成できません。

オプション	説明
ユニバーサル印刷のみを使用する	標準のモデル固有ドライバーは使用されないことを指定します。プリンターの作成には、ユニバーサル印刷ドライバーのみが使用されます。
要求されたドライバーが利用できない場合にのみユニバーサル印刷を使用する	利用可能な場合は、プリンター作成に標準のモデル固有ドライバーを使用します。ドライバーがサーバーで利用できない場合、クライアントプリンターは適切なユニバーサルドライバーで自動的に作成されます。
ユニバーサル印刷が利用できない場合にのみプリンターモデル固有のドライバーを使用する	利用可能な場合は、ユニバーサル印刷ドライバーを使用します。ドライバーがサーバーで利用できない場合、クライアントプリンターは適切なモデル固有のプリンタードライバーで自動的に作成されます。

ユニバーサルプリントサーバーのポリシー設定

ユニバーサルプリントサーバーセクションには、ユニバーサルプリントサーバーを処理するためのポリシー設定が含まれています。

SSL暗号スイート

この設定は、暗号化された印刷データストリーム (CGP) 接続のためにUniversal Print Clientで使用されるSSL/TLS暗号スイートのセットを指定します。

暗号化された印刷Webサービス (HTTPS/SOAP) 接続のためにUniversal Print Clientで使用される暗号スイートパッケージを制御するには、を参照してください。

デフォルト値: ALL

この設定には次の値があります: ALL、COM、またはGOV。

各値に対応する暗号スイートは次のとおりです:

ALL:

TLS_ECDHE_RSA_AES256_GCM_SHA384

TLS_ECDHE_RSA_AES256_CBC_SHA384

TLS_ECDHE_RSA_AES128_CBC_SHA

COM:

TLS_ECDHE_RSA_AES128_CBC_SHA

GOV:

TLS_ECDHE_RSA_AES256_GCM_SHA384

TLS_ECDHE_RSA_AES256_CBC_SHA384

SSL準拠モード

この設定は、Universal Print Clientが暗号化された印刷データストリーム (CGP) 接続に使用するNIST Special Publication 800-52への準拠レベルを指定します。

デフォルト値: なし。

この設定には次の値があります:

なし。

暗号化された印刷データストリーム (CGP) 接続は、デフォルトの準拠モードを使用します。

SP800-52。

暗号化された印刷データストリーム (CGP) 接続は、NIST Special Publication 800-52準拠モードを使用します。

SSL有効

この設定は、Universal Print Clientが以下の目的でSSL/TLSを使用するかどうかを指定します:

- 印刷データストリーム (CGP) 接続
- Webサービス (HTTP/SOAP) 接続

Universal Print Server enable を **Enabled with fallback to Windows' native remote printing** に設定すると、Microsoft Windows Network Print Providerによってフォールバック接続が行われます。この設定は、これらのフォールバック接続には影響しません。

既定値: 無効

この設定は次の値をとります。

有効。

ユニバーサルプリントクライアントは、Universal Print Serverへの接続にSSL/TLSを使用します。

無効。

ユニバーサルプリントクライアントは、Universal Print Serverへの接続にSSL/TLSを使用します。

SSL FIPSモード

この設定は、Universal Print Clientが印刷データストリーム（CGP）接続のために使用するSSL/TLS暗号化モジュールがFIPSモードで実行されるかどうかを指定します。

既定値: 無効

この設定は次の値をとります。

有効。

FIPSモードがオンになります。

無効。

FIPSモードがオフになります。

SSLプロトコルバージョン

この設定は、Universal Print Client が使用する SSL/TLS プロトコルバージョンを指定します。

デフォルト値: ALL

この設定には次の値があります。

ALL。

TLS バージョン 1.0、1.1、または 1.2 を使用します。

ティーエルエスv1.

TLS バージョン 1.0 を使用します。

TLSv1.1。

TLS バージョン 1.1 を使用します。

TLSv1.2。

TLS バージョン 1.2 を使用します。

SSL UNIVERSAL PRINT SERVER 暗号化印刷データストリーム (CGP) ポート

この設定は、Universal Print Server 暗号化印刷データストリーム (CGP) ポートの TCP ポート番号を指定します。このポートは、印刷ジョブのデータを受信します。

デフォルト値: 443

SSL UNIVERSAL PRINT SERVER 暗号化 WEB サービス (HTTPS/SOAP) ポート

この設定は、Universal Print Serverの暗号化されたWebサービス（HTTPS/SOAP）ポートのTCPポート番号を指定します。このポートは、印刷コマンドのデータを受信します。

デフォルト値: 8443

UNIVERSAL PRINT SERVERの有効化

このポリシーは、Citrix Universal Print Server (UPS) の使用を有効または無効にします。このポリシー設定は、仮想デスクトップまたはサーバーホスティングアプリケーションを含む組織単位 (OU) に適用します。このポリシー設定には、Citrix UPSコンポーネントが要求されたプリントサーバーにインストールされていないか、利用できない場合に、ネイティブのWindowsリモート印刷サービスを使用してプリントサーバーへの接続を許可するフォールバックオプションが含まれています。このポリシーへの変更は、VDAが再起動された後にのみ適用されます。

デフォルトでは、Universal Print Serverは無効になっています。

この設定をポリシーに追加するときは、次のいずれかのオプションを選択します。

- **Windowsネイティブのリモート印刷へのフォールバックを有効にする**: 可能な場合、Universal Print Serverはネットワークプリンター接続を処理します。Universal Print Serverが利用できない場合、Windows Print Providerが使用されます。Windows Print Providerは、以前にWindows Print Providerで作成されたすべてのプリンターを引き続き処理します。
- **Windowsネイティブのリモート印刷へのフォールバックなしで有効にする**: Universal Print Serverは、ネットワークプリンター接続を排他的に処理します。Universal Print Serverが利用できない場合、ネットワークプリンター接続は失敗します。この設定は、Windows Print Providerを介したネットワーク印刷を実質的に無効にします。この設定を含むポリシーがアクティブな間は、以前にWindows Print Providerで作成されたプリンターは作成されません。
- **無効**: Universal Print Server機能は無効です。UNC名を持つネットワークプリンターに接続する際、Universal Print Serverへの接続は試行されません。リモートプリンターへの接続は、引き続きWindowsネイティブのリモート印刷機能を使用します。

UNIVERSAL PRINT SERVER印刷データストリーム (CGP) ポート

この設定は、Universal Print Server印刷データストリームのCommon Gateway Protocol (CGP) リスナーが使用するTCPポート番号を指定します。このポリシー設定は、プリントサーバーを含むOUにのみ適用します。

デフォルトでは、ポート番号は7229に設定されています。

有効なポート番号は1～65535の範囲である必要があります。

UNIVERSAL PRINT SERVER印刷ストリーム入力帯域幅制限 (KBPS)

この設定は、印刷データの転送速度の上限（キロビット/秒）を指定します。転送速度は、各印刷ジョブからCGPを使用してUniversal Print Serverに配信される印刷データに対して計算されます。このポリシー設定は、仮想デスクトップまたはサーバーホスティングアプリケーションを含むOUに適用します。

デフォルトでは、値は0であり、上限がないことを指定します。

UNIVERSAL PRINT SERVER WEBサービス (HTTP/SOAP) ポート

この設定は、Universal Print ServerのWebサービス (HTTP/SOAP) リスナーが使用するTCPポート番号を指定します。Universal Print Serverは、ネットワーク印刷シナリオでCitrixユニバーサル印刷ドライバーの使用を可能にするオプションコンポーネントです。

Universal Print Serverが使用される場合、印刷コマンドはCitrix Virtual Apps and Desktopsホストから SOAP over HTTPを介してUniversal Print Serverに送信されます。この設定は、Universal Print Serverが受信HTTP/SOAPリクエストをリッスンするデフォルトのTCPポートを変更します。

ホストと印刷サーバーのHTTPポートは両方とも同じように構成する必要があります。ポートを同じように構成しない場合、ホストソフトウェアはUniversal Print Serverに接続しません。この設定は、Citrix Virtual Apps and Desktops上のVDAを変更します。さらに、Universal Print Serverのデフォルトポートも変更する必要があります。

デフォルトでは、ポート番号は8080に設定されています。

有効なポート番号は0～65535の範囲である必要があります。

負荷分散用のUNIVERSAL PRINT SERVER

この設定は、他のCitrix®印刷ポリシー設定を評価した後、セッション起動時に確立されたプリンター接続の負荷分散に使用されるUniversal Print Serverを一覧表示します。プリンター作成時間を最適化するために、Citrixはすべての印刷サーバーが同じ共有プリンターのセットを持つことを推奨します。負荷分散のために追加できる印刷サーバーの数に上限はありません。

この設定は、印刷サーバーのフェイルオーバー検出とプリンター接続の回復も実装します。印刷サーバーは定期的に可用性がチェックされます。サーバー障害が検出された場合、そのサーバーは負荷分散スキームから削除されます。また、そのサーバー上のプリンター接続は、他の利用可能な印刷サーバーに再配布されます。障害が発生した印刷サーバーが回復すると、負荷分散スキームに戻されます。

Validate Servers をクリックして、各サーバーが印刷サーバーであること、サーバーリストに重複するサーバー名が含まれていないこと、およびすべてのサーバーに同一の共有プリンターセットがインストールされていることを確認します。この操作には時間がかかる場合があります。

UNIVERSAL PRINT SERVERサービス停止しきい値

この設定は、ロードバランサーが利用できない印刷サーバーが回復するのをどれくらいの期間待つかを指定します。この期間が過ぎると、サーバーは永続的にオフラインであると判断され、その負荷は他の利用可能な印刷サーバーに再配布されます。

デフォルトでは、しきい値は180（秒）に設定されています。

UNIVERSAL PRINT SERVER WEBサービス (HTTP/SOAP) 接続タイムアウト

この設定は、Universal Print ClientがUniversal Print Server Webサービスのconnect()操作がタイムアウトするまで待機する秒数を指定します。この設定には以下の値があります。これらの値はすべて数値であり、単位（時間）は秒です。

- 最小値は0です。
- 最大値は60です。
- デフォルト値は10です。

タイムアウトが1から60（両端を含む）の場合、Universal Print Clientは、操作が完了するまで指定された時間待機します。この操作は、TCPソケット接続操作です。ソケットは、TCP/IPネットワークを介したプロセス間通信を可能にするWindowsオペレーティングシステムの機能です。

タイムアウトが0の場合、Universal Print Clientは、オペレーティングシステムによって定義されたデフォルトのタイムアウトを使用します。この構成は、この変更前のUniversal Print Clientの以前のバージョンで利用可能だった構成です。

Universal Print Clientは、Universal Print Serverと通信するVirtual Delivery Agent (VDA) のコンポーネントです。

> **注：**
>
> このポリシー設定は、VDAバージョン7.35以降に適用されます。

UNIVERSAL PRINT SERVER WEBサービス (HTTP/SOAP) 受信タイムアウト

この設定は、Universal Print ClientがUniversal Print Server Webサービスのrecv()操作がタイムアウトするまで待機する秒数を指定します。この設定には次の値があり、これらの値はすべて数値で、単位（時間）は秒です。

- 最小値は0です。
- 最大値は60です。
- デフォルト値は10です。

タイムアウトが1から60（両端を含む）の場合、Universal Print Clientは、操作が完了するまで指定された時間待機します。この操作は、TCPソケット受信操作です。ソケットは、TCP/IPネットワークを介したプロセス間通信を可能にするWindowsオペレーティングシステムの機能です。

タイムアウトが0の場合、Universal Print Clientは、オペレーティングシステムによって定義されたデフォルトのタイムアウトを使用します。この構成は、この変更前のUniversal Print Clientの以前のバージョンで利用可能だった構成です。

Universal Print Clientは、Universal Print Serverと通信するVirtual Delivery Agent (VDA) のコンポーネントです。

> **注：**
>
> このポリシー設定は、VDAバージョン7.35以降で適用されます。

UNIVERSAL PRINT SERVER WEBサービス (HTTP/SOAP) 送信タイムアウト

この設定は、Universal Print Client が Universal Print Server Webサービスの send() 操作がタイムアウトするまで待機する秒数を指定します。この設定には次の値があります。これらの値はすべて数値であり、単位（時間）は秒です。

- 最小値は0です。
- 最大値は60です。
- デフォルト値は10です。

タイムアウトが1から60（両端を含む）の場合、Universal Print Client は操作が完了するまで指定された時間待機します。この操作はTCPソケット送信操作です。ソケットは、TCP/IPネットワークを介したプロセス間通信を可能にするWindowsオペレーティングシステムの機能です。

タイムアウトが0の場合、Universal Print Client はオペレーティングシステムによって定義されたデフォルトのタイムアウトを使用します。この構成は、この変更前のUniversal Print Clientの以前のバージョンで利用可能だった構成です。

Universal Print Client は、Universal Print Server と通信するVDAのコンポーネントです。

> **注：**
>
> このポリシー設定は、VDAバージョン7.35以降で適用されます。

ユニバーサル印刷ポリシー設定

ユニバーサル印刷セクションには、ユニバーサル印刷を管理するためのポリシー設定が含まれています。

ユニバーサル印刷EMF処理モード

この設定は、Windowsユーザーデバイス上のEMFスプールファイルの処理方法を制御します。

デフォルトでは、EMFレコードはプリンターに直接スプールされます。

この設定をポリシーに追加するときは、オプションを選択します。

- プリンター用のEMFを再処理すると、EMFスプールファイルが再処理され、ユーザーデバイス上のGDIサブシステムを介して送信されます。この設定は、EMFの再処理を必要とするが、セッションで自動的に選択されない可能性のあるドライバーに使用できます。
- Citrix Universal™プリンタードライバーで使用する場合、プリンターに直接スプールすると、EMFレコードがスプールされ、処理のためにユーザーデバイスに配信されます。通常、これらのEMFスプールファイルはクライアントのスプールキューに直接挿入されます。EMF形式と互換性のあるプリンターおよびドライバーの場合、これが最速の印刷方法です。

ユニバーサル印刷画像圧縮制限

この設定は以下を指定します:

- Citrix Universal Print Driverで印刷される画像に利用可能な最大品質
- Citrix Universal Print Driverで印刷される画像に利用可能な最小圧縮レベル

デフォルトでは、画像圧縮制限は「最高品質（ロスレス圧縮）」に設定されています。

「圧縮なし」が選択されている場合、EMF印刷のみ圧縮が無効になります。

この設定をポリシーに追加するときは、オプションを選択します。

- 圧縮なし
- 最高品質 (ロスレス圧縮)
- 高音質
- 標準品質

- 低品質 (最大圧縮)

この設定を**ユニバーサル印刷最適化のデフォルト**設定を含むポリシーに追加する場合は、次の点に注意してください。

- **ユニバーサル印刷画像圧縮制限**設定の圧縮レベルが、**ユニバーサル印刷最適化のデフォルト**設定で定義されているレベルよりも低い場合を考慮してください。この場合、画像はユニバーサル印刷画像圧縮制限設定で定義されているレベルで圧縮されます。
- 圧縮が無効になっている場合、ユニバーサル印刷最適化のデフォルト設定の「希望する画質」および「ヘビーウェイト圧縮を有効にする」オプションは、ポリシーに影響を与えません。

ユニバーサル印刷最適化のデフォルト

この設定は、セッション用にユニバーサル印刷ドライバーが作成される際の印刷最適化のデフォルト値を指定します。

- 希望する画質は、ユニバーサル印刷に適用されるデフォルトの画像圧縮制限を指定します。デフォルトでは、標準品質が有効になっており、ユーザーは標準または低品質の圧縮を使用してのみ画像を印刷できます。
- ヘビーウェイト圧縮を有効にするは、希望する画質で設定された圧縮レベルを超えて帯域幅を削減するかどうかを有効または無効にします。画質は低下しません。デフォルトでは、ヘビーウェイト圧縮は無効になっています。
- 画像とフォントのキャッシュ設定は、印刷ストリームに複数回出現する画像とフォントをキャッシュするかどうかを指定します。この設定により、各固有の画像またはフォントがプリンターに一度だけ送信されることが保証されます。デフォルトでは、埋め込み画像とフォントはキャッシュされます。これらの設定は、ユーザーデバイスがこの動作をサポートしている場合にのみ適用されます。
- 非管理者によるこれらの設定の変更を許可するは、ユーザーがセッション内でデフォルトの印刷最適化設定を変更できるかどうかを指定します。デフォルトでは、ユーザーはデフォルトの印刷最適化設定を変更できません。

注: これらのオプションはすべてEMF印刷でサポートされています。XPS印刷では、「希望する画質」オプションのみがサポートされています。

この設定を**ユニバーサル印刷画像圧縮制限**設定を含むポリシーに追加する場合は、次の点に注意してください。

- **ユニバーサル印刷画像圧縮制限**設定の圧縮レベルが、**ユニバーサル印刷最適化のデフォルト**設定で定義されているレベルよりも低い場合を考慮してください。この場合、画像はユニバーサル印刷画像圧縮制限設定で定義されているレベルで圧縮されます。

- 圧縮が無効になっている場合、ポリシーでは、ユニバーサル印刷最適化のデフォルト設定の「希望する画質」と「ヘビーウェイト圧縮を有効にする」オプションは無効になります。

ユニバーサル印刷プレビューの優先設定

この設定は、自動作成されたプリンターまたは汎用ユニバーサルプリンターに対して印刷プレビュー機能を使用するかどうかを指定します。

デフォルトでは、自動作成されたプリンターまたは汎用ユニバーサルプリンターに対して印刷プレビューは使用されません。

この設定をポリシーに追加するときは、オプションを選択します。

- 自動作成されたプリンターまたは汎用ユニバーサルプリンターに対して印刷プレビューを使用しない
- 自動作成されたプリンターに対してのみ印刷プレビューを使用する
- 汎用ユニバーサルプリンターに対してのみ印刷プレビューを使用する
- 自動作成されたプリンターと汎用ユニバーサルプリンターの両方に対して印刷プレビューを使用する

ユニバーサル印刷の印刷品質制限

この設定は、セッションで印刷出力を生成するために利用できる最大ドット/インチ (dpi) を指定します。

デフォルトでは、「制限なし」が有効になっており、ユーザーは接続先のプリンターで許可されている最高の印刷品質を選択できます。

この設定が構成されている場合、出力解像度の観点から、ユーザーが利用できる最大印刷品質が制限されます。印刷品質自体と、ユーザーが接続するプリンターの印刷品質機能の両方が、構成された設定に制限されます。

たとえば、中解像度 (600 DPI) に構成されている場合、ユーザーは最大 600 DPI の品質でしか出力を印刷できません。また、**ユニバーサルプリンター**ダイアログボックスの**詳細設定**タブにある**印刷品質**設定には、中品質 (600 DPI) までの解像度設定のみが表示されます。

この設定をポリシーに追加するときは、オプションを選択します。

- 下書き (150 DPI)
- 低解像度 (300 DPI)
- 中解像度 (600 DPI)
- 高解像度 (1200 DPI)

- 制限なし

セキュリティポリシー設定

セキュリティセクションには、セッション暗号化とログオンデータの暗号化を構成するためのポリシー設定が含まれています。

SecureICAの最小暗号化レベル

この設定は、サーバーとユーザーデバイス間で送信されるセッションデータを暗号化する最小レベルを指定します。

重要: Virtual Delivery Agent 7.xの場合、このポリシー設定は、RC5 128ビット暗号化によるログオンデータの暗号化を有効にするためにのみ使用できます。その他の設定は、Citrix Virtual Apps and Desktopsのレガシーバージョンとの下位互換性のためにのみ提供されています。

VDA 7.xの場合、セッションデータの暗号化はVDAのDelivery Groupの基本設定を使用して行われます。Delivery GroupでEnable Secure ICAが選択されている場合、セッションデータはRC5 (128ビット) 暗号化を使用して暗号化されます。Delivery GroupでEnable Secure ICAが選択されていない場合、セッションデータは基本暗号化で暗号化されます。

この設定をポリシーに追加するときは、オプションを選択してください。

- Basicは、非RC5アルゴリズムを使用してクライアント接続を暗号化します。これにより、データストリームが直接読み取られるのを防ぎますが、復号化は可能です。デフォルトでは、サーバーはクライアント-サーバー間のトラフィックにBasic暗号化を使用します。
- RC5 (128ビット) ログオンは、RC5 128ビット暗号化を使用してログオンデータのみを暗号化し、クライアント接続にはBasic暗号化を使用します。
- RC5 (40ビット) は、RC5 40ビット暗号化を使用してクライアント接続を暗号化します。
- RC5 (56ビット) は、RC5 56ビット暗号化を使用してクライアント接続を暗号化します。
- RC5 (128ビット) は、RC5 128ビット暗号化を使用してクライアント接続を暗号化します。

クライアント-サーバー暗号化に指定する設定は、環境内の他の暗号化設定やWindowsオペレーティングシステムと相互作用する可能性があります。サーバーまたはユーザーデバイスのいずれかで、より高い優先度の暗号化レベルが設定されている場合を考慮してください。この場合、公開リソースに指定した設定が上書きされる可能性があります。

特定のユーザーの通信とメッセージの整合性をさらに保護するために、暗号化レベルを上げることができます。ポリシーでより高い暗号化レベルが必要な場合、より低い暗号化レベルを使用しているCitrix Receiversは接続を拒否されます。

SecureICAは認証やデータ整合性のチェックを行いません。サイトにエンドツーエンドの暗号化を提供するには、SecureICAをTLS暗号化と組み合わせて使用してください。

SecureICAはFIPS準拠のアルゴリズムを使用しません。この設定が問題となる場合は、SecureICAを使用しないようにサーバーとCitrix Receiverを構成してください。

SecureICAは、機密保持のためにRFC 2040で説明されているRC5ブロック暗号を使用します。ブロックサイズは64ビット（32ビットワード単位の倍数）です。キー長は128ビットです。ラウンド数は12です。

RC5ブロック暗号のキーは、セッションが作成されるときにネゴシエートされます。ネゴシエーションはDiffie-Hellmanアルゴリズムを使用して実行されます。このネゴシエーションでは、Diffie-Hellman公開パラメーターが使用されます。これらのパラメーターは、Virtual Delivery Agentのインストール時にWindowsレジストリに保存されます。公開パラメーターは秘密ではありません。Diffie-Hellmanネゴシエーションの結果は秘密キーであり、そこからRC5ブロック暗号のセッションキーが導出されます。ユーザーログオン用とデータ転送用に個別のセッションキーが使用されます。また、Virtual Delivery Agentとの間のトラフィックにも個別のセッションキーが使用されます。したがって、各セッションには4つのセッションキーがあります。秘密キーとセッションキーは保存されません。RC5ブロック暗号の初期化ベクトルも秘密キーから導出されます。

サーバー制限ポリシー設定

サーバー制限セクションには、アイドル接続を制御するためのポリシー設定が含まれています。

サーバーアイドルタイマー間隔

この設定は、ユーザーからの入力がない場合に、中断されないユーザーセッションがどのくらいの期間維持されるかを決定します。データはミリ秒で計算されます。

デフォルトでは、アイドル接続は切断されません（サーバーアイドルタイマー間隔 = 0）。Citrix®は、この値を最低60000ミリ秒（60秒）に設定することを推奨します。

ポリシーを表示するには、**複数のバージョン**を選択し、シングルセッションOSのバージョンをクリアしてから、**サーバー制限**を選択します。

> **注**
>
> このポリシー設定が使用されている場合、セッションが指定された時間アイドル状態であったときに、ユーザーに「アイドルタイマーの期限切れ」ダイアログボックスが表示されることがあります。Citrixポリシー設定は、このMicrosoftダイアログボックスメッセージを制御し

> ません。詳細については、`<http://support.citrix.com/article/CTX118618>`を参照してください。

セッション制限ポリシー設定

セッション制限セクションには、セッションが強制的にログオフされるまでに接続を維持する期間を制御するポリシー設定が含まれています。

切断されたセッションタイマー

この設定は、切断されロックされたデスクトップが、セッションがログオフされるまでにロックされたままになる期間を指定するタイマーを有効または無効にします。

このタイマーが有効になっている場合、タイマーの期限が切れると、切断されたセッションはログオフされます。

デフォルトでは、切断されたセッションはログオフされません。

Remote PC Accessの切断されたセッションタイマー

この設定は、タイマーの期限が切れた後に切断されたユーザーセッションをログオフするタイマーを有効または無効にします。この設定を有効にする場合は、**切断されたセッションタイマー間隔**設定を使用して、ユーザーセッションがログオフされるまでに切断されたデスクトップがロックされたままになる期間を分単位で指定します。

デフォルトでは、この設定は無効になっています。

切断されたセッションタイマー間隔

この設定は、切断されロックされたデスクトップが、セッションがログオフされるまでにロックされたままになる期間を分単位で指定します。

デフォルトでは、期間は1,440分（24時間）です。

切断されたセッションタイマー – マルチセッション

この設定は、切断されたRDSセッションがログオフされるまでにどのくらいの期間持続できるかを決定するタイマーを有効または無効にします。デフォルトでは、このタイマーは無効になっており、切断されたセッションはログオフされません。

切断されたセッションタイマー間隔 – マルチセッション

この設定は、切断されたRDSセッションがログオフされるまでにどのくらいの期間（分単位）持続できるかを決定します。デフォルトでは、期間は1440分（24時間）です。

セッション接続タイマー

この設定は、ユーザーデバイスとデスクトップ間の途切れない接続の最大継続時間を指定するタイマーを有効または無効にします。このタイマーが有効になっている場合、タイマーの期限が切れるとセッションは切断されるか、ログオフされます。Microsoft の「**時間制限に達したときにセッションを終了する**」設定が、セッションの次の状態を決定します。

デフォルトでは、このタイマーは無効になっています。

セッション接続タイマー間隔

この設定は、ユーザーデバイスとデスクトップ間の途切れない接続の最大分数（時間）を指定します。

デフォルトでは、最大継続時間は1,440分（24時間）です。

セッション接続タイマー – マルチセッション

この設定は、ユーザーデバイスとターミナルサーバー間の途切れない接続の最大継続時間を指定するタイマーを有効または無効にします。デフォルトでは、このタイマーは無効になっています。

セッション接続タイマー間隔 – マルチセッション

この設定は、ユーザーデバイスとRDSセッション間の途切れない接続の最大分数（時間）を指定します。デフォルトでは、最大継続時間は1440分（24時間）です。

セッションアイドルタイマー

ユーザーが何も入力しない場合、この設定は以下を有効または無効にするために使用されます。

- デスクトップへの途切れないユーザーデバイス接続が維持される期間を指定するタイマー。

このタイマーの期限が切れると、セッションは切断状態になり、「**切断されたセッションタイマー**」が適用されます。「**切断されたセッションタイマー**」が無効になっている場合、セッションはログオフされません。

デフォルトでは、このタイマーは有効になっています。

セッションアイドルタイマー間隔

ユーザーからの入力がない場合、この設定は以下を指定するために使用されます。

- デスクトップへのユーザーデバイスの途切れない接続が維持される分数。

デフォルトでは、アイドル状態の接続は1,440分（24時間）維持されます。

セッションアイドルタイマー – マルチセッション

この設定は、ユーザーデバイスとターミナルサーバー間のアイドル接続の最大期間を決定するタイマーを有効または無効にします。デフォルトでは、このタイマーは無効になっています。

セッションアイドルタイマー間隔 – マルチセッション

この設定は、ユーザーデバイスとRDSセッション間のアイドル接続が何分間維持されるかを指定します。デフォルトでは、最大期間は1440分（24時間）です。

> **注：**
>
> Citrix®ポリシーを使用して構成されたマルチセッションマシンのタイマー設定は、Microsoftグループポリシーを通じて構成されたタイマー設定を上書きすることが想定されています。予期しない動作を避けるため、いずれかの方法を使用してタイマー設定を構成することをお勧めします。

セッションの信頼性ポリシー設定

セッションの信頼性セクションには、セッションの信頼性接続を管理するためのポリシー設定が含まれています。

セッションの信頼性接続

この設定により、ネットワーク接続が失われたときにセッションを開いたままにするかどうかが決まります。セッションの信頼性は、自動クライアント再接続と連携して、ネットワーク障害から回復した後にユーザーがCitrix Workspace™アプリセッションに自動的に再接続できるようにします。デフォルトでは、セッションの信頼性は許可されています。

Web Studioの設定は、以下のクライアントに適用されます。

- Citrix Workspaceアプリ1808以降
- Citrix Receiver for Windows 4.7以降のバージョン。

Web Studioポリシーは、クライアント上のCitrix Receiver™グループポリシーオブジェクトを上書きします。Web Studioでこれらのポリシーを更新すると、セッションの信頼性がサーバーからクライアントに同期されます。

> **注：**

- Citrix Receiver for Windows 4.7以降およびCitrix Workspaceアプリ for Windows - Web Studioでポリシーを設定します。
- Citrix Receivers for Windows 4.7より前のバージョン - Web Studioでポリシーを設定します。また、一貫した動作のために、クライアントでCitrix Receiverグループポリシーオブジェクトテンプレートを設定します。

ネットワーク接続が中断された場合、セッションの信頼性によりセッションがアクティブな状態に保たれ、ユーザーの画面に表示されます。ユーザーは、ネットワーク接続が再開されるまで、使用しているアプリケーションを引き続き見ることができます。

セッションの信頼性を使用して、サーバー上でセッションをアクティブな状態に保ちます。接続が失われたことを示すために、ユーザーのディスプレイは不透明になります。ユーザーは中断中にフリーズしたセッションを見る可能性があります。ネットワーク接続が復元されると、ユーザーはアプリケーションとの対話を再開できます。セッションの信頼性により、再認証のプロンプトなしでユーザーが再接続されます。

セッションの信頼性と自動クライアント再接続の両方を使用する場合、これら2つの機能は順番に動作します。セッションの信頼性は、セッションの信頼性タイムアウト設定で指定された時間の経過後にユーザーセッションを閉じ（または切断し）ます。その後、自動クライアント再接続設定が有効になり、切断されたセッションにユーザーを再接続しようとします。

デフォルトでは、セッションの信頼性は許可されています。

注：

Citrix ADCを使用している場合、ICA接続をプロキシするには、Citrix StoreFront > **Manage Citrix Gateways / Secure Ticket Authority**で**セッションの信頼性を有効にする**を選択する必要があります。

セッションの信頼性ポート番号

この設定は、受信セッションの信頼性接続に使用するTCPポート番号を指定します。

デフォルトでは、ポート番号は2598に設定されています。

セッションの信頼性タイムアウト

この設定は、セッションの信頼性プロキシがユーザーの再接続を待機し、セッションが切断されるまでの時間を秒単位で指定します。

セッションが開いている時間を延長することはできますが、この機能は利便性のためであり、ユーザーに再認証を促すものではありません。セッションが開いている時間が長くなるほど、ユーザーがデバイスを放置し、不正なユーザーがアクセスする可能性が高まります。

デフォルトでは、タイムアウトは180秒（3分）に設定されています。

セッションウォーターマークポリシー設定

セッションウォーターマークセクションには、この機能を構成するためのポリシー設定が含まれています。 この機能を有効にすると、VDAマシンのネットワーク帯域幅とCPU使用率が大幅に増加します。利用可能なハードウェアリソースに基づいて、選択したVDAマシンにセッションウォーターマークを構成することをお勧めします。

> **重要**
>
> 他のウォーターマークポリシー設定を有効にするには、セッションウォーターマークを有効にします。より良いユーザーエクスペリエンスを実現するために、2つを超えるウォーターマークテキスト項目を有効にしないでください。

セッションウォーターマークを有効にする

この設定を有効にすると、セッションディスプレイには、セッション固有の情報を表示する不透明なテキストウォーターマークが表示されます。他のウォーターマーク設定は、この設定が有効になっているかどうかに依存します。

デフォルトでは、セッションウォーターマークは無効になっています。

クライアントIPアドレスを含める

この設定を有効にすると、セッションは現在のクライアントIPアドレスをウォーターマークとして表示します。

デフォルトでは、クライアントIPアドレスを含めるは無効になっています。

接続時間を含める

この設定を有効にすると、セッションウォーターマークに接続時間が表示されます。形式はyyyy/mm/dd hh:mmです。表示される時刻は、システムクロックとタイムゾーンに基づいています。

デフォルトでは、接続時間を含めるは無効になっています。

ログオンユーザー名を含める

この設定を有効にすると、セッションは現在のログオンユーザー名をウォーターマークとして表示します。表示形式はUSERNAME@DOMAINNAMEです。ユーザー名は最大20文字にすることをお勧めします。ユーザー名が20文字を超えると、文字フォントが過度に小さくなったり、切り捨てられたりして、ウォーターマークの効果が低下する可能性があります。

デフォルトでは、ログオンユーザー名を含めるは有効になっています。

VDAホスト名を含める

この設定を有効にすると、セッションは現在のICA®セッションのVDAホスト名をウォーターマークとして表示します。

デフォルトでは、VDAホスト名を含める設定が有効になっています。

VDA IPアドレスを含める

この設定を有効にすると、セッションは現在のICAセッションのVDA IPアドレスをウォーターマークとして表示します。

デフォルトでは、VDA IPアドレスは無効になっています。

セッションウォーターマークのスタイル

この設定は、単一のウォーターマークテキストラベルを表示するか、複数のラベルを表示するかを制御します。「**値**」ドロップダウンメニューから「**複数**」または「**単一**」を選択します。

「**複数**」は、セッションに5つのウォーターマークラベルを表示します。中央に1つ、四隅に4つです。

「**単一**」は、セッションの中央に単一のウォーターマークラベルを表示します。

デフォルトでは、セッションウォーターマークスタイルは「複数」です。

ウォーターマークのカスタムテキスト

この設定を使用すると、カスタムテキスト（たとえば、会社名）をセッションウォーターマークに表示できます。空でない文字列を設定すると、ウォーターマークで有効になっている他の情報に加えて、新しい行にテキストが表示されます。ウォーターマークのカスタムテキストは25 Unicode文字に制限されています。より長い文字列を設定した場合、25文字に切り詰められます。

デフォルトのテキストはありません。

Citrix Virtual Apps and Desktops™ 7 2206以降、テキストにカスタムタグを使用してさらにカスタマイズを追加できます。その結果、カスタムテキストの最大文字数は1024に増加しました。

ウォーターマーク設定で利用可能なタグは、次の表に記載されています。

タグ	説明	例
`<font=value>`	ウォーターマークテキストのフォントを変更できます。値は、VDAで利用可能なフォントの名前です。	`<font=Courier New>`
`<fontzoom=value>`	フォントのズーム率を設定できます。ウォーターマークテキストの200%ズームの場合、値は200です。	`<fontzoom=200>`
`<position=value>`	ウォーターマークテキストの位置を変更できます。値は `center`、`topleft`、`topright`、`bottomleft`、および `bottomright` です。このタグはシングルスタイルでのみ適用可能です。	`<position=topright>`
`<rotation=value>`	ウォーターマークテキストを回転できます。値は度数で指定され、範囲は-360から360です。	`<rotation=45>`
`<style=value>`	表示スタイルを変更できます。このタグはセッションウォーターマークスタイルポリシーを上書きします。	`<style=single>`

利用可能なウォーターマークスタイルは次のとおりです。

- シングルスタイル - セッションの中央に単一のウォーターマークテキストラベルが表示されます。位置タグを使用して場所を変更できます。
- xスタイルまたは複数 - セッションに5つのウォーターマークラベルが表示されます。中央に1つ、各コーナーに1つずつです。
- タイル - セッションに複数のラベルが表示されます。ウォーターマークテキストは画面全体に均等に配置されます。

ウォーターマークテキストを変更するために利用可能なタグは、次の表に記載されています。

タグ	説明
`<clientip>`	エンドポイントのIPアドレス。
`<date>`	セッションが確立された日付。
`<domain>`	ログインしているユーザーアカウントのドメイン名。
`<hostname>`	VDAのマシン名。
`<newline>`	追加の行を作成します。
`<serverip>`	VDAのIPアドレス。
`<time>`	セッションが確立された時刻。
`<username>`	ユーザーの名前。

注：

- **ウォーターマークカスタムテキスト**ポリシーは、**セッションウォーターマークを有効にする**ポリシーが有効になっている場合にのみ適用されます。デフォルト値は*無効*です。
- ウォーターマークテキストを変更するためにタグを使用する場合、**セッションウォーターマークを有効にする**を除く他のすべてのセッションウォーターマークポリシーは無視されます。ウォーターマークテキスト設定にタグを使用する場合、他のすべてのウォーターマークポリシーを使用できます。

透かしの透明度

ウォーターマークの不透明度を0から100まで指定できます。指定する値が大きいほど、ウォーターマークは不透明になります。

デフォルトでは、値は17です。

タイムゾーン制御ポリシー設定

タイムゾーン制御セクションには、セッションでのローカル時間の使用に関連するポリシー設定が含まれています。

レガシークライアントのローカル時間を推定する

この設定は、ユーザーデバイスのローカルタイムゾーンの推定を有効または無効にします。これらのデバイスには、サーバーに不正確なタイムゾーン情報を送信するユーザーデバイスが含まれます。

デフォルトでは、サーバーは必要に応じてローカルタイムゾーンを推定します。

この設定は、サーバーに詳細なタイムゾーン情報を送信しないレガシーなCitrix ReceiverまたはICAクライアントでの使用を目的としています。この設定が、サーバーに詳細なタイムゾーン情報を送信するCitrix Receiver（例: Windows版Citrix Receiver™のサポート対象バージョン）で使用される場合を考慮してください。この場合、この設定は効果がありません。

セッション切断またはログオフ時にデスクトップOSのタイムゾーンを復元する

ユーザーがセッションを切断またはログオフした場合を考慮してください。この場合、この設定は、シングルセッションOS VDAのタイムゾーン設定がマシンの元のタイムゾーンに復元されるかどうかを決定します。この設定を有効にすると、ユーザーが切断またはログオフしたときに、VDAはマシンのタイムゾーンを元の設定に復元します。この設定を有効にするには、**クライアントのローカル時間を使用**を**クライアントのタイムゾーンを使用**に設定します。

デフォルトでは、この設定は有効になっています。

クライアントのローカル時間を使用

この設定は、ユーザーセッションのタイムゾーン設定を決定します。選択肢は、ユーザーセッションのタイムゾーン（サーバータイムゾーン）またはユーザーデバイスのタイムゾーン（クライアントタイムゾーン）です。

デフォルトでは、ユーザーセッションのタイムゾーンが使用されます。

この設定を有効にするには、グループポリシーエディターで 設定を有効にします。この設定は、 > > > > > > にあります。

サーバーOSを実行しているマシンでシングルセッションVDA（以前のWorkstation VDA）を使用している場合は、ローカルユーザー権限 を に構成します。このユーザー権限は、 > > > > > にあります。

> **注：**
>
> シングルセッションOSでは、 はユーザー権利の割り当て に含まれますが、マルチセッションOSでは含まれません。マルチセッションOSでは、タイムゾーンは次のグループポリシーを使用して同期されます: Computer Configuration\Administrative Templates\Windows

> Components\Remote Desktop Services\Remote Desktop Session Host\Device and Resource Redirection\Allow timezone redirection。このポリシーは、サーバーがマルチセッションOS VDA（`/ServerVDI` コマンドでインストール）のリモートデスクトップセッションホストである場合に適用されます。マルチセッションOSでは、デフォルトで、また設計上、ユーザーはタイムゾーンを変更するローカル権限を持っていません。

TWAINデバイスのポリシー設定

TWAINデバイスセクションには、以下のポリシー設定が含まれています。

- デジタルカメラやスキャナーなどのクライアントTWAINデバイスのマッピング
- サーバーからクライアントへの画像転送の最適化

> **注：**
>
> Citrix Receiver for Windows 4.5では、TWAIN 2.0がサポートされています。

クライアントTWAINデバイスのリダイレクト

TWAINデバイスは、TWAINプロトコルを使用して、サーバーでホストされている画像処理アプリケーションと通信します。

この設定は、ユーザーがユーザーデバイス上のTWAINデバイスにアクセスすることを許可または禁止します。デフォルトでは、TWAINデバイスのリダイレクトは許可されています。

関連するポリシー設定は次のとおりです。

- TWAIN圧縮レベル
- TWAINデバイスのリダイレクト帯域幅制限
- TWAINデバイスリダイレクト帯域幅制限の割合

TWAIN圧縮レベル

この設定は、クライアントからサーバーへの画像転送の圧縮レベルを指定します。最良の画質には「低」、良好な画質には「中」、低い画質には「高」を使用します。デフォルトでは、中程度の圧縮が適用されます。

USBデバイスポリシー設定

USBデバイスセクションには、USBデバイスのファイルリダイレクトを管理するためのポリシー設定が含まれています。

クライアントUSBデバイス最適化ルール

クライアントUSBデバイス最適化ルールは、最適化を無効にするか、最適化モードを変更するためにデバイスに適用できます。

ユーザーがUSB入力デバイスを接続すると、ホストは**USBポリシー**設定がそのデバイスを許可するかどうかを確認します。デバイスが許可されている場合、ホストはデバイスの**クライアントUSBデバイス最適化ルール**を確認します。ルールが指定されていない場合、デバイスは最適化されません。キャプチャモード (04) は、署名デバイスに推奨されるモードです。高遅延によってパフォーマンスが低下する他のデバイスの場合、管理者はインタラクティブモード (02) を有効にできます。この記事の表で利用可能なモードの説明を参照してください。

知っておくとよいこと

- Wacomの署名パッドおよびタブレットを使用する場合は、スクリーンセーバーを無効にすることをお勧めします。スクリーンセーバーを無効にする手順は、このセクションの最後にあります。
- Wacom STU署名パッドおよびタブレットシリーズ製品の最適化のサポートは、Citrix Virtual Apps and Desktops™ポリシーのインストール時に事前設定されています。
- 署名デバイスはCitrix Virtual Apps and Desktops全体で動作し、署名デバイスとして使用するためにドライバーを必要としません。Wacomには、デバイスをさらにカスタマイズするためにインストールできる追加のソフトウェアがあります。`<http://www.wacom.com/>`を参照してください。
- 描画タブレット。特定の描画入力デバイスは、PCI/ACPIバス上でHIDデバイスとして表示される場合があり、サポートされていません。これらのデバイスは、Citrix Virtual Desktopsセッション内でリダイレクトされるように、クライアント上のUSBホストコントローラーに接続してください。

ポリシールールは、空白で区切られたtag=value形式の式を取ります。以下のタグがサポートされています。

タグ名	説明
モード	最適化モードは、class=**03**の入力デバイスでサポートされています。サポートされているモードは次のとおりです。最適化なし - 値**01**。インタラクティブモード - 値**02**。ペンタブレットや3D Proマウスなどのデバイスに推奨されます。キャプチャモード - 値**04**。署名パッドなどのデバイスに推奨されます。

タグ名	説明
VID	デバイス記述子からのベンダーID（4桁の16進数）。
PID	デバイス記述子からの製品ID（4桁の16進数）。
REV	デバイス記述子からのリビジョンID（4桁の16進数）。
クラス	デバイス記述子またはインターフェース記述子のいずれかからのクラス。
サブクラス	デバイス記述子またはインターフェース記述子のいずれかからのサブクラス。
保護	デバイス記述子またはインターフェース記述子のいずれかからのプロトコル。

例

Mode=00000004 VID=067B PID=1230 class=03 #キャプチャモードで動作する入力デバイス

Mode=00000002 VID=067B PID=1230 class=03 #インタラクティブモードで動作する入力デバイス（デフォルト）

Mode=00000001 VID=067B PID=1230 class=03 #最適化なしで動作する入力デバイス

Mode=00000100 VID=067B PID=1230 #デバイスセットアップの最適化が無効（デフォルト）

Mode=00000200 VID=067B PID=1230 #デバイスセットアップの最適化が有効

Wacom署名パッドデバイスのスクリーンセーバーを無効にする

Wacom署名パッドおよびタブレットを使用するには、Citrix®はスクリーンセーバーを次のように無効にすることをお勧めします。

1. デバイスをリダイレクトした後、**Wacom-STU-Driver**をインストールします。
2. 署名パッドのコントロールパネルにアクセスするには、**Wacom-STU-Display MSI**をインストールします。
3. **コントロールパネル > Wacom STU Display > STU430** または **STU530** に移動し、お使いのモデルのタブを選択します。

4. 「**変更**」を選択し、UACセキュリティウィンドウが表示されたら「**はい**」を選択します。
5. 「**スライドショーを無効にする**」を選択し、「**適用**」を選択します。

1つの署名パッドモデルに対して設定が行われると、その設定はすべてのモデルに適用されます。

クライアントUSBデバイスのリダイレクト

この設定は、USBデバイスのユーザーデバイスとの間のリダイレクトを許可または禁止します。

デフォルトでは、USBデバイスはリダイレクトされません。

クライアントUSBデバイスリダイレクト規則

この設定は、USBデバイスのリダイレクトルールを指定します。

デフォルトでは、ルールは指定されていません。

ユーザーがUSBデバイスを接続すると、ホストデバイスは一致が見つかるまで各ポリシー規則と照合して確認します。いずれかのデバイスに対する最初の一致が最終的なものと見なされます。最初の一致が許可ルールである場合、そのデバイスは仮想デスクトップにリモート接続されます。最初の一致が拒否ルールである場合、そのデバイスはローカルデスクトップでのみ利用可能です。一致が見つからない場合、デフォルトのルールが使用されます。

ポリシー規則は{Allow:|Deny:}の形式をとり、その後に空白で区切られたtag=value式のセットが続きます。次のタグがサポートされています。

タグ名	説明
VID	デバイス記述子からのベンダーID
PID	デバイス記述子からの製品ID
REL	デバイス記述子からのリリースID
クラス	デバイス記述子またはインターフェイス記述子のいずれかからのクラス
サブクラス	デバイス記述子またはインターフェース記述子のいずれかからのサブクラス
プロトコル	デバイス記述子またはインターフェイス記述子のいずれかからのプロトコル

ポリシー規則を作成する際は、次の点に注意してください。

- 規則では大文字と小文字は区別されません。
- 規則の末尾にはオプションのコメントを付けることができます。コメントは#で始まります。
- 空行と純粋なコメント行は無視されます。
- タグは一致演算子 = を使用する必要があります (例: VID=067B_。
- 各ルールは新しい行で開始するか、セミコロンで区切られたリストの一部である必要があります。
- USB Implementers Forum, Inc. の Web サイトで入手可能な USB クラスコードを参照してください。

管理者定義の USB ポリシールールの例:

- 許可: VID=067B PID=0007 # 別の産業、別のフラッシュドライブ
- 拒否: Class=08 subclass=05 # マスストレージ
- すべての USB デバイスを拒否するルールを作成するには、他のタグなしで「DENY:」を使用します。

クライアント USB プラグアンドプレイデバイスのリダイレクト

この設定により、カメラや販売時点情報管理 (POS) デバイスなどのプラグアンドプレイデバイスをクライアントセッションで使用することを許可または禁止します。

デフォルトでは、プラグアンドプレイデバイスのリダイレクトは許可されています。「許可」に設定すると、特定のユーザーまたはグループのすべてのプラグアンドプレイデバイスがリダイレクトされます。「禁止」に設定すると、デバイスはリダイレクトされません。

USB デバイスの自動リダイレクトを構成する

USB サポートが有効になっている場合、USB デバイスは自動的にリダイレクトされます。また、USB ユーザー設定は USB デバイスを自動的に接続するように設定されています。

> **注：**

> Receiver for Windows 4.2 では、デスクトップアプライアンスモードで動作している場合も USB デバイスは自動的にリダイレクトされます。また、接続バーは表示されません。以前のバージョンの Citrix Receiver for Windows では、USB デバイスは以下のモードで動作している場合も自動的にリダイレクトされます。

- デスクトップアプライアンスモード
- 仮想マシン (VM) ホスト型アプリケーション

すべてのUSBデバイスをリダイレクトすることが常に最適であるとは限りません。ユーザーは、自動的にリダイレクトされないUSBデバイスリストからデバイスを明示的にリダイレクトできます。USBデバイスがリストに表示されたり、リダイレクトされたりするのを防ぐには、クライアントエンドポイントまたはDDCポリシーのいずれかでDeviceRulesを使用します。詳細については、管理者ガイドを参照してください。

注意:

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

USBデバイスの自動リダイレクトに関するユーザー設定

ポリシー:

1. **ローカルグループポリシーエディター**を開き、**管理用テンプレート > Citrixコンポーネント > Citrix Receiver™ > クライアントデバイスのリモート処理 > 汎用USBリモーティング**に移動します。
2. **新しいUSBデバイス**を開き、**有効**を選択し、**OK**をクリックします。
3. **既存のUSBデバイス**を開き、**有効**を選択し、**OK**をクリックします。

シトリックス レシーバー:

1. **Citrix Receiverの環境設定 > 接続**に移動します。
2. 以下に示すオプションが選択されていることを確認します。
   - セッションの開始時に、デバイスを自動的に接続する
   - セッションの実行中に新しいデバイスが接続された場合、デバイスを自動的に接続する。
3. **OK**をクリックします。

すべてのレジストリキーとポリシーの変更は、Windowsクライアントデバイスに適用されます。

通常のUSBプリンターのリダイレクト

通常のUSBプリンターに最適なソリューションは、専用のユニバーサルプリンタードライバーと仮想チャネルを使用して印刷を実行することです。デフォルトでは、通常のUSBプリンターは自動的にリダイレクトされません。

通常のプリンターはヒューリスティックを使用して検出されます。また、例えばスキャン機能を備えた高度なプリンターは、完全に機能させるにはUSBサポートを使用してリダイレクトする必要がある場合があります。

通常のプリンターが自動的にリダイレクトされるかどうかを構成するには、このレジストリを使用します。

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB\Devices

名前: AutoRedirectPrinters

種類: DWORD

データ: 00000000

デフォルト値は0です（自動的にリダイレクトしません）。値を0より大きい任意の数値に変更すると、通常のUSBプリンターをリダイレクトするためのUSBサポートが有効になります。

Active Directoryポリシーをこのレジストリキーに展開し、両方が存在する場合は非ポリシー値を上書きすることもできます。

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB\Devices

名前: AutoRedirectAudio

種類: DWORD

データ: 00000000

通常のオーディオデバイスのリダイレクト

通常のプリンターと同様に、通常のオーディオデバイスからオーディオデータを送信するには、ICA®の専用オーディオ仮想チャネルを使用することで最高のユーザーエクスペリエンスが実現されます。ただし、一部の特殊なデバイスはUSBサポートを使用してリダイレクトする必要がある場合があります。どのデバイスが通常のオーディオデバイスであるかを判断するためにヒューリスティックが使用されます。

通常のオーディオデバイスが自動的にリダイレクトされるかどうかを構成するには、クライアントエンドポイントでこのレジストリを使用します。

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB\Devices

名前: AutoRedirectAudio

種類: DWORD

データ: 00000000

デフォルトは0に設定されています (自動的にリダイレクトしません)。値を0以外に変更すると、USBサポート付きのプレーンなUSBオーディオデバイスがリダイレクトされます。

Active Directoryポリシーを使用して、この値をレジストリキーに展開し、両方が存在する場合は非ポリシー値を上書きできます。

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB\Devices

名前: AutoRedirectVideo

種類: DWORD

データ: 00000000

プレーンなストレージデバイス (マスストレージデバイス) のリダイレクト

プレーンなストレージデバイスの場合、最適化も行うクライアントドライブマッピングなど、専用の仮想チャネルを使用することで、最高のユーザーエクスペリエンスを実現できます。ファイルの単純な読み書きに加えて、CD/DVDの書き込みや暗号化されたファイルシステムデバイスへのアクセスなど、特定の特殊なタスクを実行するには、ジェネリックUSBサポートを使用してデバイスをリダイレクトする必要がある場合があります。

どのデバイスがプレーンなストレージデバイスであるかを判断するために、ヒューリスティックが使用されます。プレーンなストレージデバイスを自動的にリダイレクトするかどうかを設定するには、このレジストリキーを使用します。

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB\Devices

名前: AutoRedirectStorage

種類: DWORD

データ: 00000000

デフォルトは0に設定されています (自動的にリダイレクトしません)。値を0以外に変更すると、ジェネリックUSBサポートを使用してプレーンなUSBストレージデバイスがリダイレクトされます。

Active Directoryポリシーを使用して、この値を以下のレジストリキーに展開し、両方が存在する場合は非ポリシー値を上書きすることもできます。

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB\Devices

名前: AutoRedirectStorage

種類: DWORD

データ: 00000000

> **注：**
>
> 汎用USBサポートを使用している場合、プレーンストレージデバイスへの読み取り専用アクセスは構成できませんが、CDMを使用している場合は構成できます。

ハードウェア暗号化機能付きUSBフラッシュドライブのリダイレクト

ハードウェア暗号化機能付きUSBフラッシュドライブは、通常、暗号化されたストレージパーティションと、暗号化されたパーティションをロック解除するためのユーティリティが含まれる2番目のユーティリティパーティションで構成されています。USBフラッシュドライブデバイスの場合、最適化も実行する専用のクライアントドライブマッピング/動的サムドライブマッピングHDX仮想チャネルを使用することで、最高のユーザーエクスペリエンスを実現できます。

汎用USBリダイレクトは、以下の場合に必要です。

- Windows以外のクライアント (例: Linuxクライアント)
- 顧客がクライアント上のローカル機能へのユーザーアクセスを制限 (ロックダウン) しているクライアント

汎用USBリダイレクトは、ハードウェア暗号化なしで任意のUSBストレージデバイスをシングルセッションOSおよびマルチセッションOS VDAセッションの両方にリダイレクトできます。

Citrix Virtual Apps and Desktops 7 1808より前は、ハードウェア暗号化されたUSBフラッシュドライブは、シングルセッションOSまたはマルチセッションOS VDAセッションに有用な方法でリダイレクトできませんでした。Citrix Virtual Apps and Desktops 7 1808で導入された新しい機能強化により、ハードウェア暗号化されたUSBフラッシュドライブの汎用USBリダイレクトがシングル

セッションOSおよびマルチセッションOS VDAセッションでサポートされます。 デバイスがリダイレクトされた後、そのドライブはローカルクライアントに表示されません。したがって、ドライブのロック解除が必要な場合は、セッション内で実行してください。この機能には、Windows Update KB4074590が必要です。

プレーン静止画デバイス (スキャナーおよびデジタルカメラ)

プレーン静止画デバイスの場合、最適化も実行する専用の仮想チャネル (TWAIN仮想チャネルなど) を使用することで、最高のユーザーエクスペリエンスを実現できます。これらのデバイスは業界標準に準拠している必要があります。デバイスが非準拠であるか、元の意図に従って使用されていないと見なされる場合、汎用USBリダイレクトがデバイスを使用する唯一の方法となる可能性があります。どのデバイスがプレーン静止画デバイスであるかを判断するためにヒューリスティックが使用されます。

このレジストリキーを使用して、プレーン静止画デバイスが自動的にリダイレクトされるかどうかを構成します。

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB\Devices

名前: AutoRedirectImage

種類: DWORD

データ: 00000000

デフォルトは0に設定されています（自動的にリダイレクトされません）。値を0以外に変更すると、汎用USBのプレーンなUSB静止画デバイスがリダイレクトされます。

Active Directoryポリシーを使用して、この値をこのレジストリキーに展開することもでき、両方が存在する場合は非ポリシー値を上書きします。

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB\Devices

名前: AutoRedirectImage

種類: DWORD

データ: 00000000

デバイス固有の設定

Citrix最適化可能デバイスを選択するために使用されるヒューリスティックは、必ずしもユーザーの希望と一致するとは限りません。Citrix最適化可能デバイスの例としては、プリンター、オーディオ、ビデオ、ストレージ、静止画デバイスなどがあります。上記にリストされていないデバイ

スの自動リダイレクトを制御したい場合があります。デバイス固有の基準で自動リダイレクトを制御できます。

例として、DemoTech 2,000バーコードリーダーはUSBサポートを使用してリダイレクトする必要はありません。ベンダー識別子は12AB、製品識別子は5678です。これらの16進数はデバイスマネージャーで確認できます。

これが自動的にリダイレクトされるのを防ぐには、このデバイス固有のレジストリキーを作成します。

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB\Devices\VID12AB PID5678

名前: AutoRedirect

種類: DWORD

データ: 00000000

値が0の場合、デバイスは自動的にリダイレクトされません。0以外の値は、デバイスが自動リダイレクトの対象となることを示します（ユーザー設定による）。ベンダー識別子と製品識別子の間には単一のスペース文字があります。

Active Directoryポリシーを使用して、この値をこのレジストリキーに展開することもできます。両方が存在する場合、非ポリシー値を上書きします。

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB\Devices\VID12AB PID5678

名前: AutoRedirect

種類: DWORD

データ: 00000000

デバイス固有のAutoRedirect設定は、上記で説明したより一般的なAutoRedirectXXX値よりも優先されます。Citrix最適化デバイスのデフォルトのヒューリスティックは、デバイスを汎用として誤って解釈する可能性があります。したがって、デバイス固有のAutoRedirect値を1に設定して、自動的にリダイレクトします。

既存のUSBデバイスの自動接続を許可する

この設定は、セッション開始時にエンドポイントに接続されている既存のUSBデバイスをリモートセッションに自動接続することを許可または防止します。

この設定をポリシーに追加するときは、次のいずれかのオプションを選択します。

- 利用可能なUSBデバイスをリダイレクトする前に確認する。
- 利用可能なUSBデバイスを自動的にリダイレクトしない。
- 利用可能なUSBデバイスを自動的にリダイレクトする。

デフォルトでは、**利用可能なUSBデバイスをリダイレクトする前に確認する**オプションが選択されています。選択されたポリシーに基づいて、クライアントの**環境設定** > **デバイス**セクションで選択されたオプションを上書きできます。

> **注：**
>
> 現在、**既存のUSBデバイスの自動接続を許可する**ポリシーは、Citrix Workspace™ app for Windowsにのみ適用されます。

新しく接続されたUSBデバイスの自動接続を許可する

この設定は、セッション中にエンドポイントに挿入されたUSBデバイスをリモートセッションに自動接続することを許可または防止します。

この設定をポリシーに追加するときは、次のいずれかのオプションを選択します。

- 利用可能なUSBデバイスをリダイレクトする前に確認する。
- 利用可能なUSBデバイスを自動的にリダイレクトしない。
- 利用可能なUSBデバイスを自動的にリダイレクトします。

デフォルトでは、**利用可能なUSBデバイスをリダイレクトする前に確認する**オプションが選択されています。選択されたポリシーに基づいて、クライアントの**基本設定** > **デバイス**セクションで選択されたオプションが上書きされる場合があります。

> **注：**
>
> 現在、**新しく接続されたUSBデバイスの自動接続を許可する**ポリシーは、Citrix Workspace アプリ for Windowsにのみ適用されます。

クライアントUSBデバイスリダイレクト規則 (バージョン2)

この設定は、USBデバイスをリモートセッションにフィルタリング、分割、および自動接続するためのルールを指定します。

この設定が選択されている場合、ホストは*クライアントUSBデバイスリダイレクトルール*設定を、この設定で構成されたデバイスルールで上書きします。

詳しくは、「複合USBデバイスリダイレクトの構成」を参照してください。

仮想チャネル許可リストポリシー設定

仮想チャネル許可リストポリシー設定は、ICA®セッションで開くことが許可されている仮想チャネルを指定する許可リストの使用を有効にします。

無効にすると、すべての仮想チャネルが許可されます。

有効にすると、Citrix®仮想チャネルのみが許可されます。

カスタムまたはサードパーティの仮想チャネルを使用するには、仮想チャネルをリストに追加します。仮想チャネルをリストに追加するには：

1. 仮想チャネル名の後にコンマを入力します。
2. 仮想チャネルにアクセスするプロセスのパスを入力します。

複数の実行可能パスをリストでき、パスはコンマで区切られます。

例:

```
CTXCVC1,C:\VC1\vchost.exe
```

```
CTXCVC2,C:\VC2\vchost.exe,C:\Program Files\Third Party\vcaccess.exe
```

Citrix Virtual Apps and Desktops 7 2109以降、仮想チャネル許可リストはデフォルトで有効になっています。許可リストに仮想チャネルを追加する方法の詳細については、「許可リストへの仮想チャネルの追加」を参照してください。

Skype for Business 用の HDX RealTime Optimization Pack を使用している場合は、仮想チャネルを許可リストに追加します。詳細については、「HDX RealTime Optimization Pack のドキュメント」を参照してください。

> **重要:**
>
> 設定を有効にするには、VDAマシンを再起動する必要があります。

> 仮想チャネルの詳細については、「ICA仮想チャネル」を参照してください。

仮想チャネル許可リストのログ記録

このポリシー設定を使用して、仮想チャネル許可リストのログ記録レベルを構成できます。

次のオプションが利用可能です。

オプション	説明
無効	すべてのログイベントを無効にします。
警告のみをログに記録	許可リストに含まれていない、開こうとするカスタム仮想チャネルに対してのみイベントがログに記録されます。
すべてのイベントをログに記録	すべてのイベントがログに記録されます

仮想チャネル許可リストのログスロットリング

このポリシー設定を使用して、アクティブなセッションのイベントログ記録の頻度を構成できます。

各仮想チャネルのすべてのイベントは、最初に発生したときにログに記録されます。セッションがアクティブな間、スロットリング期間中は繰り返し発生するイベントは抑制されます。セッションが切断された場合、スロットリング期間はリセットされます。

視覚表示ポリシー設定

視覚表示セクションには、仮想デスクトップからユーザーデバイスに送信される画像の品質を制御するためのポリシー設定が含まれています。

シンプルなグラフィックの優先色深度

このポリシー設定は、VDAバージョン7.6 FP3以降で利用可能です。8ビットオプションは、VDAバージョン7.12以降で利用可能です。

この設定により、シンプルなグラフィックがネットワーク経由で送信される際の色深度を下げることができます。ピクセルあたり8ビットまたは16ビットに下げることで、低帯域幅接続での応答性が向上する可能性があります。ただし、この操作は画質のわずかな劣化を招く可能性があります。(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/policies/reference/ica-policy-settings/graphics-policy-settings.html)ポリシー設定が**画面全体**に設定されている場合、8ビットの色深度はサポートされません。

デフォルトの優先色深度はピクセルあたり24ビットです。

8ビット設定がVDAバージョン7.11以前に適用された場合、VDAは24ビット（デフォルト）の色深度にフォールバックします。

ターゲットフレームレート

この設定は、仮想デスクトップからユーザーデバイスに送信される1秒あたりの最大フレーム数を指定します。

デフォルトでは、最大は1秒あたり30フレームです。

1秒あたりのフレーム数を高く設定する（例：30）と、ユーザーエクスペリエンスは向上しますが、より多くの帯域幅が必要になります。1秒あたりのフレーム数を減らす（例：10）と、ユーザーエクスペリエンスを犠牲にしてサーバーのスケーラビリティが最大化されます。CPUが遅いユーザーデバイスの場合、ユーザーエクスペリエンスを向上させるために低い値を指定してください。

1秒あたりの最大サポートフレームレートは60です。

視覚品質

この設定は、ユーザーデバイスに表示される画像の希望する視覚品質を指定します。

デフォルトでは、この設定は「中」です。

画像の品質を指定するには、次のいずれかのオプションを選択します。

- **低** - 帯域幅が制限されたネットワークで、対話性のために視覚的な品質を犠牲にできる場合に推奨されます。
- **中** - ほとんどのユースケースで最高のパフォーマンスと帯域幅効率を提供します。
- **高** - 視覚的にロスレスな画質が必要な場合に推奨されます。
- **ロスレスにビルド** - ネットワークアクティビティが高い期間はロッシー画像をユーザーデバイスに送信し、ネットワークアクティビティが低下した後はロスレス画像を送信します。この設定により、帯域幅が制限されたネットワーク接続でのパフォーマンスが向上します。
- **常にロスレス** - 画像データの保持が不可欠な場合は、「**常にロスレス**」を選択して、ロッシーデータがユーザーデバイスに送信されないようにします。たとえば、画質の低下が許されないX線画像を表示する場合などです。

動きのある画像ポリシー設定

動きのある画像セクションには、動的な画像の圧縮を削除または変更できる設定が含まれています。

最小画像品質

注：Virtual Delivery Agent 7.xの場合、このポリシー設定は、レガシーグラフィックモードポリシー設定が有効になっている場合にのみ適用されます。

この設定は、アダプティブディスプレイの許容される最小画像品質を指定します。圧縮が少ないほど、表示される画像の品質は高くなります。超高、非常に高、高、標準、低のいずれかの圧縮を選択します。

デフォルトでは、これは標準に設定されています。

動きのある画像の圧縮

この設定は、アダプティブディスプレイが有効になっているかどうかを指定します。アダプティブディスプレイは、利用可能な帯域幅に基づいて、スライドショー内のビデオやトランジションスライドの画像品質を自動的に調整します。アダプティブディスプレイが有効になっている場合、ユーザーは品質の低下なしにスムーズなプレゼンテーションを見ることができます。

デフォルトでは、アダプティブディスプレイは有効になっています。

VDAバージョン7.0から7.6の場合、この設定はレガシーグラフィックモードが有効になっている場合にのみ適用されます。VDAバージョン7.6 FP1以降の場合、この設定はレガシーグラフィックモードが有効になっている場合、またはレガシーグラフィックモードが無効でビデオコーデックがグラフィックの圧縮に使用されていない場合に適用されます。

レガシーグラフィックモードが有効になっている場合、ポリシーの変更を有効にするにはセッションを再起動する必要があります。アダプティブディスプレイはプログレッシブディスプレイと相互排他的です。アダプティブディスプレイを有効にするとプログレッシブディスプレイが無効になり、その逆も同様です。ただし、プログレッシブディスプレイとアダプティブディスプレイの両方を同時に無効にすることができます。プログレッシブディスプレイはレガシー機能であるため、XenAppまたはXenDesktopでは推奨されません。プログレッシブしきい値レベルを設定すると、アダプティブディスプレイが無効になります。

プログレッシブ圧縮レベル

注：Virtual Delivery Agent 7.xの場合、このポリシー設定は、レガシーグラフィックモードポリシー設定が有効になっている場合にのみ適用されます。

この設定は、詳細度は低いものの、より高速な画像の初期表示を提供します。

デフォルトでは、プログレッシブ圧縮は適用されません。

通常の非可逆圧縮設定で定義された、より詳細な画像は、利用可能になったときに表示されます。写真などの帯域幅を多く消費するグラフィックの表示を改善するには、非常に高または超高圧縮を使用します。

プログレッシブ圧縮を有効にするには、その圧縮レベルが「ロッシー圧縮レベル」設定よりも高くする必要があります。

注：プログレッシブ圧縮に関連する圧縮レベルの増加は、クライアント接続を介した動的画像の対話性も向上させます。回転する3Dモデルなどの動的画像の品質は、画像が動きを停止するまで一時的に低下し、その時点で通常のロッシー圧縮設定が適用されます。

関連するポリシー設定は次のとおりです。

- プログレッシブ圧縮しきい値
- プログレッシブヘビーウェイト圧縮

プログレッシブ圧縮しきい値

注：Virtual Delivery Agent 7.xの場合、このポリシー設定は、レガシーグラフィックモードポリシー設定が有効になっている場合にのみ適用されます。

この設定は、プログレッシブ圧縮が適用される接続の最大帯域幅を1秒あたりのキロビットで表します。これは、この帯域幅以下のクライアント接続にのみ適用されます。

デフォルトでは、しきい値は1秒あたり2147483647キロビットです。

関連するポリシー設定は次のとおりです。

- プログレッシブ圧縮しきい値
- プログレッシブヘビーウェイト圧縮

目標最小フレームレート

この設定は、低帯域幅の条件下で、動的画像に対してシステムが維持しようとする1秒あたりの最小フレームレートを指定します。

デフォルトでは、これは10fpsに設定されています。

VDAバージョン7.0から7.6の場合、この設定はレガシーグラフィックモードが有効になっている場合にのみ適用されます。VDAバージョン7.6 FP1以降の場合、この設定はレガシーグラフィックモードが無効または有効になっている場合に適用されます。

> **注：**
>
> 目標最小フレームレートポリシーは非推奨となり、10 fpsに設定されています。これは、グラフィックステータスインジケーターの品質スライダーを使用してエンドユーザーが変更できます。

静止画像ポリシー設定

静止画像セクションには、静止画像の圧縮を削除または変更できる設定が含まれています。

追加の色圧縮

この設定は、帯域幅が制限されているクライアント接続を介して配信される画像に対する追加の色圧縮の使用を有効または無効にし、表示される画像の品質を低下させることで応答性を向上させます。

デフォルトでは、追加の色圧縮は無効になっています。

有効にすると、追加の色圧縮は、クライアント接続の帯域幅が「追加の色圧縮しきい値」を下回っている場合にのみ適用されます。クライアント接続の帯域幅がしきい値を超えている場合、または「無効」が選択されている場合、追加の色圧縮は適用されません。

追加の色圧縮しきい値

注：Virtual Delivery Agent 7.xの場合、このポリシー設定は、レガシーグラフィックモードポリシー設定が有効になっている場合にのみ適用されます。

この設定は、追加の色圧縮が適用される接続の最大帯域幅をキロビット/秒で表します。クライアント接続の帯域幅が設定値を下回ると、有効になっている場合、追加の色圧縮が適用されます。

デフォルトでは、しきい値は8192キロビット/秒です。

ヘビーウェイト圧縮

注：Virtual Delivery Agent 7.xの場合、このポリシー設定は、レガシーグラフィックモードポリシー設定が有効になっている場合にのみ適用されます。

この設定は、より高度でCPU負荷の高いグラフィックアルゴリズムを使用することで、画質を損なうことなくプログレッシブ圧縮を超えて帯域幅を削減することを有効または無効にします。

デフォルトでは、ヘビーウェイト圧縮は無効になっています。

有効にすると、ヘビーウェイト圧縮はすべての非可逆圧縮設定に適用されます。Citrix Workspace™アプリでサポートされていますが、他のプラグインには影響しません。

関連するポリシー設定は次のとおりです。

- プログレッシブ圧縮レベル
- プログレッシブ圧縮しきい値

非可逆圧縮レベル

注：Virtual Delivery Agent 7.xの場合、このポリシー設定は、レガシーグラフィックモードポリシー設定が有効になっている場合にのみ適用されます。

この設定は、帯域幅が制限されているクライアント接続を介して配信される画像に使用される非可逆圧縮の度合いを制御します。このような場合、圧縮なしで画像を表示すると遅くなることがあります。

デフォルトでは、中程度の圧縮が選択されています。

帯域幅を多く消費する画像の応答性を向上させるには、高圧縮を使用します。画質の劣化が許容されないX線画像を表示する場合など、画像データの保持が不可欠な場合は、非可逆圧縮を使用しない方がよいでしょう。

関連ポリシー設定：非可逆圧縮しきい値

非可逆圧縮しきい値

注：Virtual Delivery Agent 7.xの場合、このポリシー設定は、レガシーグラフィックモードポリシー設定が有効になっている場合にのみ適用されます。

この設定は、非可逆圧縮が適用される接続の最大帯域幅を1秒あたりのキロビット数で表します。

デフォルトでは、しきい値は1秒あたり2147483647キロビットです。

ポリシーに非可逆圧縮レベル設定を追加し、しきい値を指定しないことで、LAN経由での写真などの高精細ビットマップの表示速度を向上させることができます。

関連ポリシー設定：非可逆圧縮レベル

WebSocketsポリシー設定

WebSocketsセクションには、HTML5向けCitrix Workspace™アプリを使用して仮想デスクトップおよびホスト型アプリケーションにアクセスするためのポリシー設定が含まれています。WebSockets機能は、ブラウザベースのアプリケーションとサーバー間の双方向通信を行うことで、セキュリティを向上させ、オーバーヘッドを削減します。この機能は、複数のHTTP接続を開くことなくこれを実現します。

WebSockets接続

この設定では、WebSockets接続を許可または禁止します。

デフォルトでは、WebSocket接続は禁止されています。

WebSocketsポート番号

この設定では、受信WebSocket接続のポートを識別します。

デフォルトでは、値は8008です。

WebSockets信頼済みオリジンサーバーリスト

この設定では、通常はWeb向けCitrix Workspaceアプリである、URLとして表現された信頼済みオリジンサーバーのコンマ区切りリストを提供します。サーバーは、これらのアドレスのいずれかから発信されたWebSockets接続のみを受け入れます。

既定では、ワイルドカード「*」は、すべてのCitrix Workspaceアプリ for WebのURLを信頼するために使用されます。

リストにアドレスを入力する場合は、次の構文を使用します。

\<protocol>://\<ホストの完全修飾ドメイン名>:

プロトコルはHTTPまたはHTTPSである必要があります。ポートが指定されていない場合、HTTPにはポート80が、HTTPSにはポート443が使用されます。

ワイルドカード `*` は、IPアドレスの一部として使用する場合を除き (`10.105.*.*`)、URL内で使用できます。

WIA デバイスのポリシー設定

WIA デバイスセクションには、Windows Image Acquisition (WIA) を使用したスキャナーリダイレクトを管理するためのポリシー設定が含まれています。

WIA リダイレクト

デジタルカメラやスキャナーなどの WIA デバイスは、WIA フレームワークを使用して、サーバーでホストされている画像処理アプリケーションと通信します。この設定により、ユーザーがユーザーデバイス上の WIA デバイスにアクセスすることを許可または禁止します。デフォルトでは、WIA リダイレクトは禁止されています。

WIA 準拠デバイスの詳細については、「WIA デバイス」を参照してください。

レジストリで管理されるHDX™機能

> **注：**

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

> レジストリエディターを開くには、サーバーで `regedit.exe` を実行します。次に、設定を追加または編集するレジストリキーに移動します。

デバイス

Bloombergキーボード

Citrix Virtual Apps and Desktops™は、Bloombergモデル4およびモデル3のスターボードキーボードをサポートしています。デフォルトでは、拡張Bloombergキーボードのサポートは無効になっています。

Bloombergキーボードのサポートを有効にするには、接続を開始する前にクライアントマシンで次のレジストリ値を設定します。

- **キー**: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICAClient\GenericUSB`
- **値の名前**: `EnableBloombergHID`
- **値の型**: `DWORD`
- **値のデータ**:
  - `0` - 無効
  - `1` - 有効

詳しくは、「Bloombergキーボード」を参照してください。

マップされたクライアントドライブ

セキュリティ上の予防措置として、ユーザーがCitrix Virtual Apps and Desktopsにログオンすると、デフォルトでは、サーバーはユーザーの実行権限なしでクライアントドライブをマップします。ユーザーがマップされたクライアントドライブにある実行可能ファイルを実行できるようにするには、サーバーのレジストリを編集してこのデフォルトを上書きします。

アクセスを許可するには、次のレジストリ値を編集します (**CDMSettings**が存在しない場合は作成します)。

- **キー**: `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\CDMSettings`

- **値の名前**: `ExecuteFromMappedDrive`
- **値の型**: `DWORD`
- **値のデータ**:
  - `1` - 許可
  - `0` - マップされたドライブでのアクセスを拒否

この変更は、レジストリを編集した後に接続されたセッションに適用されます。

Citrix Virtual Apps and Desktops 7 2006は、このレジストリの場所を含む最初のバージョンです。以前のバージョンのCitrix Virtual Apps and Desktopsでは、異なるレジストリの場所が使用されていました。

詳しくは、「クライアントドライブマッピング」を参照してください。

マイクロソフト Surface Pro および Surface Book ペン

Citrix Virtual Apps and Desktopsは、Windows Inkベースのアプリケーションで標準のペン機能をサポートしています。デフォルトでは、この機能は有効になっています。

この機能を無効または有効にするには、次のレジストリ値を設定します。

- **キー**: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Citrix Virtual Desktop Agent\PenApi`
- **値の名前**: `DisablePen`
- **値の型**: `DWORD`
- **値のデータ**:
  - `1` - 無効
  - `0` - 有効

詳細については、「Microsoft Surface Pro および Surface Book のペン」を参照してください。

Windows Image Acquisitionアプリケーションの許可リスト

この設定により、VDA 上のどのアプリケーションが Windows イメージ取得スキャナーリダイレクトにアクセスできるかを制御できます。

デフォルトでは、どのアプリケーションも Windows イメージ取得にアクセスできません。

VDA 上のアプリケーションに対して Windows イメージ取得を調整するには、次のレジストリ設定を作成します。

- **キー**: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix`

- **値の名前**: `WIAAllowedProcesses`

  WIAAllowedProcesses を選択して右クリックします。「**新規 > 複数行文字列値**」を選択し、新しい値の名前を **AllowProcesses** に変更します。

- 値のデータ: Windows イメージ取得にアクセスできる各アプリケーションの完全なパスとプロセス名を入力します。各アプリケーションは新しい行に入力してください。

この設定への変更は、次回 VDA でセッションを起動したときに有効になります。

全般

HDX ダイレクト

マルチセッションセッションホストにおける HDX Direct のデフォルトのタイムアウトは 60 秒です。タイムアウトを変更するには、次のレジストリ値を変更します。

- **キー**: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd\HdxDirect`
- **値の名前**: `HdxDirectInitiateTimeoutInSeconds`
- **値の型**: `DWORD`
- **値のデータ**: `60` (10進数)

HDX リデューサー

セッションホストで使用するHDX圧縮アルゴリズム（Reducer）のバージョンを構成できます。

シングルセッションVDAでReducer V4を有効にするには、次のレジストリ値を設定します。

キー: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\GroupPolicy\Defaults\WDSettings` **値の名前**: `ReducerOverrideMask` **値の型**: `DWORD` **値のデータ**: `23` (10進数)

マルチセッションVDAでReducer V4を有効にするには、次のレジストリ値を設定します。

- **キー**: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd`
- **値の名前**: `ReducerOverrideMask`
- **値の型**: `DWORD`
- **値のデータ**: `23` (10進数)

EDTタイムアウトの構成

VDAでEDTタイムアウトを5秒から25秒の任意の値に構成できます。デフォルトのEDTタイムアウト値は25秒です。

- **キー**: `HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd\Tds\udp\UDPStackParameters`
- **値の型**: `DWORD`
- **値の名前**: `edtConnectionTimeout`
- **値のデータ**: 5〜25秒の時間 (10進数)

Windows向けCitrix Workspace™アプリのタイムアウトも構成できます:

- **キー**: `HKLM\SOFTWARE\WOW6432Node\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\EDT`
- **値の型**: `String / REG_SZ`
- **値の名前**: `edtConnectionTimeout`
- **値のデータ**: 5〜25秒の時間 (10進数)

Rendezvousバージョンの構成

使用するRendezvousのバージョンを構成するには、次のレジストリ値を設定します:

- **キー**: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\VirtualDesktopAgent`
- **値の型**: `DWORD`
- **値の名前**: `GctRegistration`
- **値のデータ**:
  - `1` - V2を有効にするには
  - `0` - V1を有効にするには

VDAへの自動ログオンを構成する

この設定により、Windows 10シングルセッションOSおよびマルチセッションOSのVDAで、Microsoftポリシー設定の**常にパスワードを要求する**を有効または無効にできます。

もし**常にパスワードを要求する**が有効になっている場合、ユーザーはリモートセッションを開始するときにVDAで資格情報を入力する必要があります。この設定が無効になっている場合、ユーザーはVDAで資格情報を提供することなく、自動的にリモートセッションに接続します。

デフォルトでは、Microsoftポリシー設定は無効になっています。**常にパスワードを要求する**設定を有効または無効にするには、VDAで次のレジストリ値を設定します。

- **キー**: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Portica`
- **値の名前**: `AutoLogon`
- **値の型**: `DWORD`
- **値のデータ**:
  - `1` - Microsoftポリシー設定を無効にし、ユーザーがリモートセッションに自動的にサインインできるようにします。
  - `0` – Microsoftポリシー設定を有効にし、ユーザーがリモートセッションを起動するときに資格情報の入力を求めます。

タイムアウト警告を無効にする

デフォルトでは、非アクティブまたはアイドル状態のセッションを持つユーザーは、セッションが自動的に切断される2分前に警告メッセージを受け取ります。

この設定は、以下のアイドルセッションタイムアウト制限に達したユーザーに対する警告メッセージを無効にし、削除します。

- ウィンドウズ サーバー 2004
- Windows 10マルチセッション2004以降のマルチセッションOS

警告を削除するには、VDAで以下のレジストリ値を設定します。

- **キー**: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Winstations\ICA-CGP`
- **値の名前**: `fEnableTimeoutWarning`
- **値の型**: `DWORD`
- **値のデータ**:
  - `1` - 警告メッセージを無効にする
  - `0` - 警告メッセージを有効にする

警告メッセージを表示するには、レジストリ値を削除するか、`0`に設定します。

EDT MTU検出

MTU検出により、EDTはセッション確立時に最大転送単位（MTU）を自動的に決定できます。これにより、パフォーマンスの低下やセッション確立の失敗につながる可能性のあるEDTパケットの断片化を防ぎます。

この設定はデフォルトで有効になっています。EDT MTU検出を無効にするには、以下のレジストリ値を構成し、VDAを再起動します。

- **キー**: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd`
- **値の名前**: `MtuDiscovery`
- **値の型**: `DWORD`
- **値のデータ**: `0`

この設定はマシン全体に適用され、サポートされているクライアントから接続するすべてのセッションに影響します。

ロス許容モードを有効にする

Citrix Workspaceアプリ for Windows、マルチユーザーVDA、およびデスクトップVDAの双方向オーディオサービスで、ロス許容モードを使用してアダプティブオーディオにアクセスできます。この設定はデフォルトで無効になっています。ロス許容モードを有効にするには、使用しているマシンに応じて、以下のレジストリ値を構成し、それぞれのマシンを再起動します。

Citrix Workspaceアプリ for Windowsクライアントの場合、,

- **キー**: `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ClientAudio`
- **値の名前**: `EdtUnreliableAllowed`
- **値の型**: `REG_SZ`
- **値のデータ**: `1`

TS VDAの場合、,

- **キー**: `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\Audio`
- **値の名前**: `EdtUnreliableAllowed`
- **値の型**: `DWORD`
- **値のデータ**: `1`

WS VDAの場合、,

- **キー**: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Audio`
- **値の名前**: `EdtUnreliableAllowed`
- **値の型**: `DWORD`
- **値のデータ**: `1`

一般的なコンテンツリダイレクト

ホストからクライアントへのリダイレクトにURLタイプを追加する

デフォルトでは、HTTP、HTTPS、RTSP、RTSPU、PNM、MMSのURLタイプのリダイレクトをサポートしています。Windowsクライアントで以下のレジストリキーと値を作成することで、URLタイプをリストに追加できます。

- **キー**: `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Policies\Citrix\ICA Client\SFTA`
- **値の名前**: `ExtraURLProtocols`
- **値の型**: `REG_SZ`
- **値のデータ**: 必要なURLタイプをセミコロンで区切って指定します。URLの権限部分より前のすべてを含めます。例: `ftp://;mailto:;customtype1://;custometype2://`

URLタイプはWindowsクライアントにのみ追加できます。このレジストリ設定がないクライアントは、Citrixセッションへのリダイレクトを拒否します。クライアントには、指定されたURLタイプを処理するようにインストールおよび構成されたアプリケーションが必要です。

詳細については、「ホストからクライアントへのリダイレクト」を参照してください。

クライアントフォルダーリダイレクト

クライアントフォルダーリダイレクトは、クライアント側のファイルがホスト側のセッションでアクセス可能になる方法を変更します。サーバーでクライアントフォルダーリダイレクトを有効にし、ユーザーがユーザーデバイスでそれを構成するとします。この場合、ユーザーが指定したローカルボリュームの一部がリダイレクトされます。

サーバーでクライアントフォルダーリダイレクトを有効にするには、次のレジストリ値を設定します。

- **キー**: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\Client Folder Redirection`
- **値の名前**: `CFROnlyModeAvailable`

- **値の型**: `DWORD`
- **値のデータ**: `1`

詳細については、クライアントフォルダーリダイレクトを参照してください。

特定のWebサイトセットに対するホストからクライアントへのリダイレクト

特定のWebサイトセットに対してホストからクライアントへのリダイレクトを有効にするには、サーバーVDAで次のレジストリ値を設定します。

- **キー**: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\SFTA`
- **値の名前**: `ValidSites`
- **値の型**: `REG_MULTI_SZ`
- **値のデータ**: 完全修飾ドメイン名（FQDN）の任意の組み合わせを指定します。複数のFQDNを別々の行に入力します。プロトコル（`http://`または`https://`）なしで、FQDNのみを含めます。FQDNには、最も左の位置にのみワイルドカード文字としてアスタリスク（`*`）を含めることができます。このワイルドカードは、RFC 6125の規則と一致する単一レベルのドメインに一致します。例:

`www.example.com`

`*.example.com`

詳細については、ホストからクライアントへのリダイレクトを参照してください。

ログオフ時および切断時のローカルアプリケーションの動作

デフォルトでは、ユーザーが仮想デスクトップからログオフまたは切断しても、ローカルアプリケーションは実行を継続します。再接続後、ローカルアプリケーションが仮想デスクトップで利用可能な場合、それらは再統合されます。ログオフ時および切断時のローカルアプリケーションの動作を構成するには、ホストされたデスクトップで次のレジストリ値を設定します。

- **キー**: `HKEY_LOCAL_MACHINE\SOFTWARE\wow6432node\Citrix\Client Hosted Apps\Policies`
- **値の名前**: `Session State`
- **値の型**: `DWORD`
- **値のデータ**:
  - `1` - ユーザーが仮想デスクトップからログオフまたは切断しても、ローカルアプリケーションは引き続き実行されます。再接続すると、ローカルアプリケーションが仮想デスクトップで利用可能な場合、再統合されます。

- `3` - ユーザーが仮想デスクトップからログオフまたは切断すると、ローカルアプリケーションは閉じます。

詳しくは、「Local App Access and URL redirection」を参照してください。

ホストからクライアントへのリダイレクトのデフォルトリストからURLタイプを削除する

デフォルトのリダイレクトリストからURLタイプを削除するには、サーバーVDAで以下のレジストリキーと値を作成します。

- **キー**: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\SFTA`
- **値の名前**: `DisableServerFTA`
- **値の型**: `DWORD`
- **値のデータ**: `1`
- **値の名前**: `NoRedirectClasses`
- **値の型**: `REG_MULTI_SZ`
- **値のデータ**: `http`、`https`、`rtsp`、`rtspu`、`pnm`、または`mms`のいずれかの値を組み合わせて指定します。複数の値を指定する場合は、別々の行に入力します。例:

`http`

`https`

`rtsp`

詳しくは、「Host to client redirection」を参照してください。

サーバーVDAのデフォルトブラウザ構成

ホストからクライアントへのリダイレクトを有効にすると、Server VDA のデフォルトのブラウザ設定を上書きできます。Web URL がリダイレクトされない場合、Citrix ランチャーは `command_backup` レジストリキーで構成されているブラウザに URL を渡します。このキーはデフォルトで Internet Explorer を指していますが、別のブラウザへのパスを含むように変更できます。

- Internet Explorer (デフォルト)
  - **キー**: `HKEY_CLASSES_ROOT\http\shell\open\command_backup`
  - **値の名前**: `Default`
  - **値の型**: `REG_SZ`
  - **値のデータ**: `"c:\program files\internet explorer\iexplore.exe" "%1"`

  - **キー**: `HKEY_CLASSES_ROOT\https\shell\open\command_backup`
  - **値の名前**: `Default`
  - **値の型**: `REG_SZ`
  - **値のデータ**: `"c:\program files\internet explorer\iexplore.exe" "%1"`

- グーグル クローム
  - **キー**: `HKEY_CLASSES_ROOT\http\shell\open\command_backup`
  - **値の名前**: `Default`
  - **値の型**: `REG_SZ`
  - **値のデータ**: `"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" "%1"`
  - **キー**: `HKEY_CLASSES_ROOT\https\shell\open\command_backup`
  - **値の名前**: `Default`
  - **値の型**: `REG_SZ`
  - **値のデータ**: `"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" "%1"`

- マイクロソフト エッジ
  - **キー**: `HKEY_CLASSES_ROOT\http\shell\open\command_backup`
  - **値の名前**: `Default`
  - **値の型**: `REG_SZ`
  - **値のデータ**: `"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" "%1"`
  - **キー**: `HKEY_CLASSES_ROOT\https\shell\open\command_backup`
  - **値の名前**: `Default`
  - **値の型**: `REG_SZ`
  - **値のデータ**: `"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" "%1"`

公開アプリケーションのローカルアプリアクセス

ローカルアプリアクセスは、ローカルにインストールされたWindowsアプリケーションを、デスクトップを切り替えることなくホストされたデスクトップ環境にシームレスに統合します。公開アプリケーションへのアクセスを提供するには、サーバーで次のレジストリ値を設定します。

- **キー**: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\DesktopStudio`
- **値の名前**: `ClientHostedAppsEnabled`
- **値の型**: `DWORD`
- **値のデータ**:
  - `1` - 有効
  - `0` - 無効

詳細については、ローカルアプリアクセスとURLリダイレクトを参照してください。

グラフィック

CUDAまたはOpenCLアプリケーションのGPUアクセラレーション

ユーザーセッションで実行されているCUDAおよびOpenCLアプリケーションのGPUアクセラレーションは、デフォルトで無効になっています。

CUDAアクセラレーションのPOC機能を使用するには、次のレジストリ設定を有効にします。

- **キー**: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\CtxHook\AppInit_Dlls\Graphics Helper`
- **値の名前**: `CUDA`
- **値の型**: `DWORD`
- **値のデータ**: `00000001`

OpenCLアクセラレーションのPOC機能を使用するには、次のレジストリ設定を有効にします。

- **キー**: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\CtxHook\AppInit_Dlls\Graphics Helper`
- **値の名前**: `OpenCL`
- **値の型**: `DWORD`
- **値のデータ**: `00000001`

詳細については、WindowsマルチセッションOSのGPUアクセラレーションを参照してください。

プログレッシブモード

プログレッシブモードはデフォルトで無効になっています。以下のレジストリ値でプログレッシブモードの状態を変更できます:

- **キー**: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics`
- **値の型**: `REG_DWORD`
- **値の名前**: `ProgressiveDisplay`
- **値のデータ**:
  - `0` - 常にオフ (プログレッシブモードを無効にします。この値がデフォルトです。)
  - `1` - 自動 (ネットワークの状態に基づいて切り替えます。)
  - 2 = 常にオン

詳細については、プログレッシブモードを参照してください。

> **注：**
>
> プログレッシブモードは非推奨になりました。Thinwireは、画像の配信を最適化し、キャッシュ効率を維持しながら、プログレッシブモードのほぼすべての利点を提供する代替オプションです。

Windows Presentation Foundation (WPF) レンダリング

HDX 3D Proを使用すると、WindowsマルチセッションOSセッションで実行されているグラフィック負荷の高いアプリケーションを、サーバーのグラフィック処理ユニット (GPU) でレンダリングできます。Windows Presentation Foundation (WPF) のレンダリングをサーバーのGPUに移行することで、グラフィックレンダリングがサーバーのCPUを遅くすることはありません。

サーバーのGPUを使用してWPFアプリケーションのレンダリングを有効にするには、WindowsマルチセッションOSを実行しているサーバーのレジストリに次の設定を作成します。

1. VDAでレジストリエディターを開き、次のキーに移動します。

   `HKLM\Software\Citrix\CtxHook\AppInit_DLLs\Graphics Helper`

2. 次のレジストリ値を作成または編集します。

   - AdapterHandle = 0x00000001

- DevicePath = 0x00000001
- フラグ = 0x00000412
- WPF = 0x00000001

3. WPFアプリの実行可能ファイル名でサブキーを作成します。たとえば、アプリが「mywpfapp.exe」という名前の場合、次のキーを作成します。

```
HKLM\Software\Citrix\CtxHook\AppInit_DLLs\Graphics Helper\mywpfapp.exe
```

4. 設定を有効にするには、サーバーを再起動します。

詳細については、WindowsマルチセッションOSのGPUアクセラレーションおよびWindowsマルチセッションOSでWPFアプリを最大限に活用するのブログを参照してください。

マルチメディア

マルチメディア会議中のエコーを回避する

Citrix Virtual Apps and Desktopsは、エコーを最小限に抑えるエコーキャンセルオプションを提供します。この機能はデフォルトで有効になっています。エコーキャンセルを無効にするには、次のいずれかのレジストリ設定を変更できます。

- **キー**:
  - 32ビット: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ClientAudio`
  - 64ビット: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ClientAudio`
- **値の名前**: `EchoCancellation`
- **値の型**: `String/REG_SZ`
- **値のデータ**: `False`

詳細については、オーディオ機能を参照してください。

オーディオの制限

クライアントにオーディオデバイスをインストールし、オーディオリダイレクトを有効にしてRDSセッションを開始した後、オーディオファイルが再生されない場合があります。回避策として、RDSマシンに以下のレジストリキーを追加し、マシンを再起動してください。

- **キー**: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SCMConfig`
- **値の名前**: `EnableSvchostMitigationPolicy`

- **値の型**: `DWORD`
- **値のデータ**: `0`

詳細については、オーディオ機能を参照してください。

高解像度Webカメラの解像度

メディアタイプのネゴシエーションが失敗した場合、HDXはデフォルトのVGA解像度（640 x 480 ピクセル）にフォールバックします。クライアントのレジストリキーを使用して、デフォルトの解像度を構成できます。以下のレジストリキーを設定する前に、カメラが指定された解像度をサポートしていることを確認してください。

- **キー**: `HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXRealTime`
- 幅
  - **値の名前**: `DefaultWidth`
  - **値の型**: `DWORD`
  - **値のデータ**: 10進数で指定する幅 (例: 1280)
- 高さ
  - **値の名前**: `DefaultHeight`
  - **値の型**: `DWORD`
  - **値のデータ**: 10進数で指定する高さ (例: 720)

Microsoft Teamsのフォールバックモード

Microsoft Teamsが最適化されたVDIモードでロードに失敗した場合 (Teams/About/Versionで「Citrix HDX Not Connected」と表示される場合)、VDAはウェブカメラのリダイレクトやクライアントオーディオおよびマイクのリダイレクトなど、従来のHDXテクノロジーにフォールバックします。Microsoft Teamsの最適化をサポートしないWorkspaceアプリのバージョン/プラットフォームOSを使用している場合、フォールバックレジストリキーは適用されません。

フォールバックメカニズムを制御するには、VDA上で以下のいずれかのレジストリ値を設定します。

- **キー** (いずれか1つのみ必要):
  - **コンピューター設定:** `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Teams`
  - **ユーザー設定:** `HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\Teams`
- **値の名前**: `DisableFallback`

- **値の型**: `DWORD`
- 値のデータ:
  - `1` - フォールバックモードを無効にする
  - `2` - オーディオのみを有効にする

値が存在しないか0に設定されている場合、フォールバックモードが有効になります。この機能には、Microsoft Teamsバージョン1.3.0.13565以降が必要です。詳細については、「Microsoft Teamsの最適化」を参照してください。

Citrix App Layering™を使用したMicrosoft Teamsの最適化

Citrix App Layeringを使用してVDAとMicrosoft Teamsのインストールを異なるレイヤーで管理している場合は、コマンドラインから`ALLUSER=1`フラグを使用してMicrosoft Teamsをインストールする前に、Windows上に**PortICA**という名前の空のレジストリキーを作成します。既定の値の名前、種類、データはそのままにします。

- レジストリエディターの32ビット版のキー:
  `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\PortICA`
- レジストリエディターの64ビット版のキー:
  `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`

詳細については、「Microsoft Teamsの最適化」を参照してください。

Webカメラのソフトウェア圧縮

Webカメラがハードウェアエンコードをサポートしている場合、HDXビデオ圧縮はデフォルトでハードウェアエンコードを使用します。ハードウェアエンコードは、ソフトウェアエンコードよりも多くの帯域幅を消費する可能性があります。ソフトウェア圧縮を強制するには、クライアントに次の値を追加します。

- **キー**: `HKEY_CURRENT_USER\SOFTWARE\Citrix\HdxRealTime`
- **値の名前**: `DeepCompress_ForceSWEncode`
- **値の型**: `DWORD`
- **値のデータ**: `1`

詳細については、HDX webcam video compressionを参照してください。

Webカメラビデオ圧縮

HDX Webカメラビデオ圧縮は、H.264ビデオを仮想セッションで実行されているビデオ会議アプリケーションに直接送信します。VDAリソースを最適化するために、HDX Webカメラ圧縮はWebカメラビデオのエンコード、トランスコード、デコードを行いません。この機能はデフォルトで有効になっています。

サーバーからビデオ会議アプリへの直接ビデオストリーミングを無効にするには、VDAで次のレジストリ値を設定します。

- **キー**: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxRealTime`
- **値の名前**: `OfferH264ToApp`
- **値の型**: `DWORD`
- **値のデータ**: `0`

詳細については、HDX webcam video compressionを参照してください。

Webカメラビデオ圧縮フレームレート

優先ビデオフレームレートを調整するには、クライアントで次のレジストリ値を編集します。

- **キー**: `HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXRealTime`
- **値の名前**: `FramesPerSecond`
- **値の型**: `DWORD`
- **値のデータ**: `15`

ウェブカメラが指定されたフレームレートをサポートしていない場合、アプリケーションはデフォルトで15 FPSを使用します。

詳細については、HDXウェブカメラビデオ圧縮を参照してください。

ロード管理ポリシー設定

ロード管理セクションには、Windowsマルチセッション OSマシンを提供するサーバー間のロード管理を有効化および構成するためのポリシー設定が含まれています。

ロード評価インデックスの計算については、CTX202150を参照してください。

同時ログオン許容数

この設定は、サーバーが受け入れ可能な同時ログオンの最大数を指定します。

デフォルトでは、この値は2に設定されています。

この設定が有効な場合、負荷分散は、指定された数を超えるログオンが同時にサーバーVDAでアクティブにならないように試みます。ただし、この制限は厳密には適用されません。制限を適用し（指定された数を超える同時ログオンを失敗させる）、次のレジストリキーを作成します。

> HKLM\Software\Citrix\DesktopServer\LogonToleranceIsHardLimit 種類: DWORD 値: 1

CPU使用率

この設定は、サーバーがフルロードを報告するCPU使用率のレベルをパーセンテージで指定します。有効にすると、サーバーがフルロードを報告するデフォルト値は90%です。

デフォルトでは、この設定は無効になっており、CPU使用率は負荷計算から除外されます。

CPU使用率から除外されるプロセスの優先度

> **注：**

> Workspace Environment Managementがマシンを管理するシナリオでは、この設定をCPU Priority設定と併用すると、意図しない結果が生じる可能性があります。CPU Priority設定を使用する場合は、この設定を無効にすることをお勧めします。

> この設定は、プロセスのCPU使用率がCPU使用率負荷インデックスから除外される優先度レベルを指定します。

デフォルトでは、この値は**標準以下**または**低**に設定されています。

ディスク使用量

この設定は、サーバーが75%のフルロードを報告するディスクキューの長さを指定します。有効にすると、ディスクキューのデフォルト値は8です。

デフォルトでは、この設定は無効になっており、ディスク使用率は負荷計算から除外されます。

セッションの最大数

この設定は、サーバーがホストできるセッションの最大数を指定します。有効にすると、サーバーがホストできるセッションの最大数のデフォルト設定は250になります。

デフォルトでは、この設定は有効になっています。

メモリ使用量

この設定は、サーバーがフルロードを報告するメモリ使用量のレベルをパーセンテージで指定します。有効にすると、サーバーがフルロードを報告するデフォルト値は90%になります。

デフォルトでは、この設定は無効になっており、メモリ使用量は負荷計算から除外されます。

メモリ使用量のベースロード

この設定は、ベースオペレーティングシステムのメモリ使用量の近似値を指定します。また、サーバーがゼロロードと見なされるメモリ使用量をMB単位で定義します。

デフォルトでは、この値は768 MBに設定されています。

プロファイル管理ポリシー設定

このセクションには、プロファイル管理を有効化および構成するためのポリシー設定が含まれています。

以下のようなその他の情報については、プロファイル管理ポリシーを参照してください。

- 対応する.iniファイル設定の名前
- ポリシー設定に必要なプロファイル管理のバージョン

高度なポリシー設定

ロックされたファイルへのアクセス時の再試行回数

ロックされたファイルへのアクセス時の再試行回数を設定します。

このポリシーが無効になっている場合、5回の再試行のデフォルト値が使用されます。このポリシーがここで構成されていない場合、.iniファイルの値が使用されます。このポリシーがここでも.iniファイルでも構成されていない場合、デフォルト値が使用されます。

ログオフ時にインターネットCookieファイルを処理する

一部の展開では、`Index.dat`が参照しない余分なインターネットCookieが残されます。継続的なブラウジングの後、ファイルシステムに残された余分なCookieは、プロファイルの肥大化につながる可能性があります。このポリシーを使用すると、Profile Managementを有効にしてIndex.datの処理を強制し、余分なCookieを削除できます。このポリシーはログオフ時間を増加させるため、この問題が発生した場合にのみ有効にしてください。

このポリシーがここで構成されていない場合、.iniファイルの値が使用されます。このポリシーがここでも.iniファイルでも構成されていない場合、Index.datの処理は行われません。

自動構成を無効にする

Profile Managementは、Citrix Virtual Desktops™環境（パーソナルvDiskの有無など）を検査し、それに応じてグループポリシーを構成します。「未構成」状態のProfile Managementポリシーのみが調整されるため、行ったカスタマイズはすべて保持されます。

このポリシーにより、展開を高速化し、最適化を簡素化できます。このポリシーを構成する必要はありません。ただし、次のいずれかの操作を行う場合は、自動構成を無効にできます。

- 以前のバージョンからの設定を保持するためにアップグレードする
- トラブルシューティング

自動構成は、実行時に環境に応じてデフォルトのポリシー設定を自動的に構成する動的な構成チェッカーと見なすことができます。これにより、設定を手動で構成する必要がなくなります。実行時環境には以下が含まれます。

- ウィンドウズ OS
- Windows OS のバージョン
- シトリックス バーチャル デスクトップの有無
- パーソナル vDisk の有無

環境が変更された場合、自動構成によって以下のポリシーが変更される可能性があります。

- アクティブライトバック
- 常にキャッシュ
- ログオフ時にローカルにキャッシュされたプロファイルを削除
- キャッシュされたプロファイルを削除するまでの遅延
- プロファイルストリーミング

異なる OS でのポリシーのデフォルトの状態については、次の表を参照してください。

	マルチセッションOS	シングルセッションOS
アクティブライトバック	有効	Personal vDiskが使用されている場合は*無効*。それ以外の場合は、有効。
常にキャッシュ	無効	Personal vDiskが使用されている場合は*無効*。それ以外の場合は、有効。

	マルチセッションOS	シングルセッションOS
ログオフ時にローカルにキャッシュされたプロファイルを削除	有効	次のいずれかの状況が発生した場合、*無効*になります: Personal vDiskが使用されている、Citrix Virtual Desktopsが割り当てられている、またはCitrix Virtual Desktopsがインストールされていない場合。それ以外の場合は有効です。
キャッシュされたプロファイルを削除するまでの遅延	0秒	ユーザーの変更が永続的でない場合は60秒。それ以外の場合は0秒。
プロファイルストリーミング	有効	Personal vDiskが使用されている場合は*無効*。それ以外の場合は、有効。

ただし、自動構成が無効になっている場合、上記のすべてのポリシーはデフォルトで**無効**になります。

> **重要:**

> Personal vDiskは非推奨です。詳細については、PVD、AppDisk、およびサポートされていないホストの削除を参照してください。

> Profile Management 1909以降、Windows 10 (バージョン1607以降) およびWindows Server 2016以降のスタートメニューで、改善されたエクスペリエンスを得ることができます。この改善は、以下のポリシーの自動構成によって実現されます。

- `Appdata\Local\Microsoft\Windows\Caches`と`Appdata\Local\Packages`を**ミラーリングするフォルダー**に追加します。
- `Appdata\Local\Microsoft\Windows\UsrClass.Dat*`を**同期するファイル**に追加します。

ここでこの設定が構成されていない場合、.iniファイルの値が使用されます。

この設定がここでも.iniファイルでも構成されていない場合、自動構成が有効になります。この場合、環境が変更されると、Profile Managementの設定が変更される可能性があります。

問題が発生した場合にユーザーをログオフする

問題が発生した場合に Profile Management がユーザーをログオフさせるかどうかを指定できます。

このポリシーが無効になっているか、構成されていない場合、問題が発生すると Profile Management はユーザーに一時プロファイルを提供します。たとえば、ユーザー ストアが利用できない場合などです。

有効になっている場合、エラーメッセージが表示され、ユーザーはログオフされます。この設定により、問題のトラブルシューティングが簡素化されます。

ここでこの設定が構成されていない場合、.iniファイルの値が使用されます。

この設定がここでも.iniファイルでも構成されていない場合、一時プロファイルが提供されます。

カスタマー エクスペリエンス向上プログラム

デフォルトでは、カスタマー エクスペリエンス向上プログラムが有効になっており、匿名統計と使用状況データを収集することで、Citrix® 製品の品質とパフォーマンスの向上に役立てています。

ここでこの設定が構成されていない場合、.iniファイルの値が使用されます。

Outlook の検索インデックス ローミングを有効にする

ユーザープロファイルとともに Outlook 検索データを自動的にローミングすることで、ユーザーベースの Outlook 検索エクスペリエンスを許可します。この機能には、Outlook の検索インデックスを保存するために、ユーザー ストアに追加のスペースが必要です。

このポリシーを有効にするには、ログオフしてから再度ログオンしてください。

Outlook 検索インデックス データベース – バックアップと復元

Outlook の検索インデックス ローミングを有効にするポリシーが有効になっている場合に、ログオン中に Profile Management が何を行うかを指定できます。

このポリシーが有効になっている場合、Profile Management は、ログオン時に検索インデックス データベースが正常にマウントされるたびに、そのデータベースをバックアップします。Profile Management は、そのバックアップを検索インデックス データベースの良好なコピーとして扱います。データベースの破損により検索インデックス データベースのマウントが失敗した場合、Profile Management は検索インデックス データベースを最後に確認された良好なコピーに戻します。

> 注:

> 新しいバックアップが正常に保存されると、Profile Managementは以前に保存されたバックアップを削除します。バックアップは利用可能なVHDXストレージを消費します。

OUTLOOK検索データローミングの同時セッションサポートを有効にする

Profile Managementにより、同じユーザーの同時セッションでネイティブのOutlook検索エクスペリエンスが提供されます。このポリシーは、Outlookの検索インデックスローミングポリシーと併用してください。

このポリシーが有効な場合、各同時セッションは個別のOutlook OSTファイルを使用します。

デフォルトでは、Outlook OSTファイルを保存するために使用できるVHDXディスクは2つだけです（ディスクごとに1ファイル）。ユーザーがさらにセッションを開始した場合、そのOutlook OSTファイルはローカルユーザープロファイルに保存されます。Outlook OSTファイルを保存するためのVHDXディスクの最大数を指定できます。

ONEDRIVEコンテナを有効にする

OneDriveフォルダーをユーザーとともにローミングできるようにします。

OneDriveコンテナは、VHDXベースのフォルダーローミングソリューションです。Profile Managementは、ファイル共有上にユーザーごとにVHDXファイルを作成し、ユーザーのOneDriveフォルダーをVHDXファイルに保存します。VHDXファイルは、ユーザーがログオンするときにアタッチされ、ログオフするときにデタッチされます。

UWPアプリのローミング

UWP (Universal Windows Platform) アプリをユーザーとともにローミングできるようにします。その結果、ユーザーは異なるデバイスから同じUWPアプリにアクセスできます。

このポリシーが有効な場合、Profile ManagementはUWPアプリを個別のVHDXディスクに保存することで、ユーザーとともにローミングできるようにします。これらのディスクは、ユーザーのログオン中にアタッチされ、ログオフ中にデタッチされます。

構成の優先順位:

この設定がここで構成されていない場合、.iniファイルの値が使用されます。 この設定がここでも.iniファイルでも構成されていない場合、この機能は無効になります。

ログオン時のユーザーグループポリシーの非同期処理を有効にする

Windowsは、ユーザーグループポリシーに同期モードと非同期モードの2つの処理モードを提供します。Windowsは、次のユーザーログオンの処理モードを決定するためにレジストリ値を使用し

ます。レジストリ値が存在しない場合、同期モードが適用されます。レジストリ値はマシンレベルの設定であり、ユーザーとともにローミングされません。したがって、ユーザーが次の場合、非同期モードは期待どおりに適用されません。

- 異なるマシンにログオンする。
- ログオフ時にローカルにキャッシュされたプロファイルを削除するポリシーが有効になっている同じマシンにログオンする。

このポリシーを有効にすると、レジストリ値はユーザーとともにローミングされます。その結果、ユーザーがログオンするたびに処理モードが適用されます。

VHDディスクの圧縮をトリガーする空き領域の比率

VHDディスクの圧縮を有効にする が有効な場合に適用されます。VHDディスクの圧縮をトリガーする空き領域の比率を指定できます。ユーザーログオフ時に空き領域の比率が指定された値を超えると、ディスクの圧縮がトリガーされます。

空き領域の比率 = (現在のVHDファイルサイズ – 必要な最小VHDファイルサイズ*) ÷ 現在のVHDファイルサイズ

* Microsoft Windowsオペレーティングシステムの `MSFT_Partition` クラスのGetSupportedSizeメソッドを使用して取得されます。

VHDディスクの圧縮をトリガーするログオフ回数

VHDディスクの圧縮を有効にする が有効な場合に適用されます。VHDディスクの圧縮をトリガーするユーザーログオフ回数を指定できます。

最後の圧縮以降のログオフ回数が指定された値に達すると、ディスク圧縮が再度トリガーされます。

VHDディスク圧縮のデフラグを無効にする

VHDディスク圧縮を有効にする が有効な場合に適用されます。VHDディスク圧縮のファイルデフラグを無効にするかどうかを指定できます。

VHDディスク圧縮が有効な場合、VHDディスクファイルはまずWindowsに組み込まれている `defrag` ツールを使用して自動的にデフラグされ、その後圧縮されます。VHDディスクのデフラグはより良い圧縮結果をもたらしますが、無効にするとシステムリソースを節約できます。

プロファイルコンテナのマルチセッションライトバックを有効にする

マルチセッションシナリオでプロファイルコンテナのライトバックを有効にします。有効にすると、すべてのセッションでの変更がプロファイルコンテナに書き戻されます。そうでない場合、プロファイルコンテナでは最初のセッションのみが読み取り/書き込みモードであるため、最初の

セッションでの変更のみが保存されます。Citrix Profile Managementプロファイルコンテナは Citrix Profile Management 2103以降でサポートされています。FSLogix Profile ContainerはCitrix Profile Management 2003以降でサポートされています。

FSLogix Profile Containerでこのポリシーを使用するには、以下の前提条件が満たされていることを確認してください。

- FSLogix Profile Container機能がインストールされ、有効になっていること。
- FSLogixでプロファイルタイプが **読み取り/書き込みプロファイルを試行し、読み取り専用にフォールバックする** に設定されていること。

ユーザーストアをレプリケートする

リモートユーザープロファイルストアを、ログオンおよびログオフごとに複数のパスにレプリケートできます。これにより、Profile Managementはユーザーログオンのプロファイル冗長性を提供できます。

このポリシーを有効にすると、システムI/Oが増加し、ログオフが長くなる可能性があります。

> **注：**
>
> - この機能は、ユーザーストアとフルプロファイルコンテナの両方で利用できます。
> - レプリケートされたプロファイルコンテナは、ユーザーログオンのプロファイル冗長性を提供しますが、セッション内フェールオーバーには対応していません。

ユーザーストアへの資格情報ベースのアクセスを有効にする

デフォルトでは、Citrix Profile Managementは現在のユーザーを偽装してユーザーストアにアクセスします。ユーザーストアへのアクセス時にProfile Managementが現在のユーザーを偽装しないようにする場合は、この機能を有効にしてください。現在のユーザーがアクセス権を持たないストレージリポジトリ（Azure Filesなど）にユーザーストアを配置できます。

Profile Management がユーザー ストアにアクセスできるようにするには、プロファイル ストレージ サーバーの資格情報を Workspace Environment Management™ (WEM) または Windows 資格情報マネージャーに保存します。Profile Management が実行される各マシンで同じ資格情報を構成する必要をなくすために、Workspace Environment Management を使用することをお勧めします。Windows 資格情報マネージャーを使用する場合は、ローカル システム アカウントを使用して資格情報を安全に保存してください。

> **注：**
>
> このポリシーは、ファイルベースと VHDX ベースの両方のユーザー ストアで利用できます。Profile Management のバージョン 2212 より前では、このポリシーは VHDX ベースのユーザー ストアでのみ利用できます。
>
> この設定がここで構成されていない場合、.iniファイルの値が使用されます。この設定がここでも.iniファイルでも構成されていない場合、デフォルトで無効になります。

VHDX ファイルのストレージ パスをカスタマイズする

Profile Management は、プロファイル コンテナー、Outlook の検索インデックス ローミング、フォルダー ミラーリングの高速化といった VHDX ベースのポリシーを提供します。デフォルトでは、VHDX ファイルはユーザー ストアに保存されます。このポリシーを使用すると、それらを保存する別のパスを指定できます。

VHD コンテナーのデフォルト容量

VHD コンテナーのデフォルトのストレージ容量 (GB 単位) を指定できます。

構成の優先順位:

1. ここでこのポリシーが構成されていない場合、.iniファイルの値が使用されます。
2. このポリシーがここでも.iniファイルでも構成されていない場合、デフォルトは50 (GB) です。

セッションで VHDX ディスクを自動的に再アタッチする

このポリシーを有効にすると、Profile Management は VHDX ベースのポリシーの高い安定性を確保します。デフォルトでは、このポリシーは有効になっています。

このポリシーが有効になっている場合、Profile Management は VHDX ベースのポリシーで使用されている VHDX ディスクを監視します。いずれかのディスクがデタッチされた場合、Profile Management はそのディスクを自動的に再アタッチします。

プロファイルコンテナの自動拡張しきい値

プロファイルコンテナが自動拡張をトリガーするストレージ容量の使用率を指定できます。

構成の優先順位:

- ここでこのポリシーが構成されていない場合、.iniファイルの値が使用されます。
- このポリシーがここでも.iniファイルでも構成されていない場合、デフォルトはストレージ容量の90 (%) です。

プロファイルコンテナの自動拡張増分

自動拡張がトリガーされたときに、プロファイルコンテナが自動的に拡張するストレージ容量（GB単位）を指定できます。

構成の優先順位:

- ここでこのポリシーが構成されていない場合、.iniファイルの値が使用されます。
- このポリシーがここでも.iniファイルでも構成されていない場合、デフォルトは10 (GB) です。

プロファイルコンテナの自動拡張制限

自動拡張がトリガーされたときに、プロファイルコンテナが自動的に拡張できる最大ストレージ容量（GB単位）を指定できます。

構成の優先順位:

- ここでこのポリシーが構成されていない場合、.iniファイルの値が使用されます。
- このポリシーがここでも.iniファイルでも構成されていない場合、デフォルトは80 (GB) です。

ユーザーレベルのポリシー設定を有効にする

このポリシーを有効にすると、マシンレベルのポリシー設定がユーザーレベルで機能し、ユーザーレベルの設定がマシンレベルの設定を上書きします。

構成の優先順位:

1. ここでこのポリシーが構成されていない場合、.iniファイルの値が使用されます。
2. このポリシーがここでも.iniファイルでも構成されていない場合、無効になります。

ユーザーグループの優先順位を設定する

ユーザーグループの優先順位を指定できます。この順序は、ユーザーが異なるポリシー設定を持つ複数のグループに属している場合に、どのグループが優先されるかを決定します。

ユーザーが競合するポリシー設定を持つ複数のグループに属している場合、以下を考慮してください:

- ユーザーがこのポリシーで定義されている1つ以上のグループに属している場合、最も優先順位の高いグループが優先されます。
- ユーザーがこのポリシーで定義されているどのグループにも属していない場合、アルファベット順で最も早くリストされているSIDを持つグループが優先されます。

ユーザーストアの選択方法

複数のユーザーストアが利用可能な場合に、ユーザーストアの選択方法を指定できます。オプションは次のとおりです:

- **構成順序。** Profile Managementは、最初に構成されたストアを選択します。
- **アクセスパフォーマンス。** Profile Managementは、最高のアクセスパフォーマンスを持つストアを選択します。

構成の優先順位:

1. ここでこの設定が構成されていない場合、.ini ファイルの値が使用されます。
2. ここでも .ini ファイルでもこの設定が構成されていない場合、**構成順序**が使用されます。

基本ポリシー設定

このセクションには、Profile Management の基本構成に関連するポリシー設定が含まれています。

Profile Management を有効にする

デフォルトでは、展開を容易にするため、Profile Management はログオンまたはログオフを処理しません。Profile Management は、他のすべてのセットアップタスクを実行し、Citrix® ユーザープロファイルが環境でどのように動作するかをテストした後にのみ有効にしてください。

このポリシーがここで構成されていない場合、.ini ファイルの値が使用されます。このポリシーがここでも .ini ファイルでも構成されていない場合、Profile Management は Windows ユーザープロファイルを一切処理しません。

処理されるグループ

コンピューターローカルグループとドメイングループ（ローカル、グローバル、ユニバーサル）の両方を使用できます。ドメイングループは、DOMAIN NAME\GROUP NAME の形式で指定する必要があります。

このポリシーがここで構成されている場合、Profile Management はこれらのユーザーグループのメンバーのみを処理します。このポリシーが無効になっている場合、Profile Management はすべてのユーザーを処理します。このポリシーがここで構成されていない場合、.ini ファイルの値が使用されます。このポリシーがここでも .ini ファイルでも構成されていない場合、すべてのユーザーグループのメンバーが処理されます。

除外されるグループ

コンピューターローカルグループとドメイングループ（ローカル、グローバル、ユニバーサル）を使用して、特定のユーザープロファイルが処理されないようにすることができます。ドメイングループは、DOMAIN NAME\ GROUP NAME の形式で指定します。

この設定がここで構成されている場合、Profile Management はこれらのユーザーグループのメンバーを除外します。この設定が無効になっている場合、Profile Management はどのユーザーも除外しません。この設定がここで構成されていない場合、.ini ファイルの値が使用されます。この設定がここでも .ini ファイルでも構成されていない場合、どのグループのメンバーも除外されません。

ローカル管理者のログオンを処理する

BUILTIN\Administrators グループのメンバーのログオンを処理するかどうかを指定します。Citrix Virtual Apps 環境などのマルチセッションオペレーティングシステムでは、このポリシーが無効になっているか、構成されていないと見なされます。この場合、Profile Management は、ドメインユーザーによるログオンは処理されるが、ローカル管理者によるログオンは処理されないと想定します。シングルセッションオペレーティングシステム（Citrix Virtual Desktops 環境など）では、ローカル管理者のログオンが処理されます。このポリシーにより、ローカル管理者権限を持つドメインユーザー（通常は仮想デスクトップが割り当てられた Citrix Virtual Desktops ユーザー）は、次のことが可能になります。

- 処理をバイパスする
- ログオンする
- Profile Managementで問題が発生しているデスクトップのトラブルシューティング

注：ドメインユーザーのログオンは、通常、製品ライセンスへの準拠を確実にするために、グループメンバーシップによって課される制限の対象となる場合があります。 このポリシーが無効になっている場合、Profile Managementはローカル管理者によるログオンを処理しません。このポリシーがここで構成されていない場合、.iniファイルの値が使用されます。このポリシーがここでも.iniファイルでも構成されていない場合、管理者は処理されません。

ユーザーストアへのパス

ユーザー設定（レジストリの変更と同期されたファイル）が保存されるディレクトリ（ユーザーストア）へのパスを設定します。

パスは次のいずれかです。

- 相対パス。ホームディレクトリ（通常、Active Directoryのユーザーの#homeDirectory#属性として構成されます）に対する相対パスである必要があります。

- UNCパス。通常、サーバー共有またはDFS名前空間を指定します。
- 無効または未構成。この場合、#homeDirectory#\Windowsの値が想定されます。

このポリシーには、次の種類の変数が使用できます。

- パーセント記号で囲まれたシステム環境変数（例: %ProfVer%）。システム環境変数は通常、追加の設定が必要です。
- ハッシュで囲まれたActive Directoryユーザーオブジェクトの属性（例: #sAMAccountName#）。
- Profile Management変数。詳細については、Profile Management変数の製品ドキュメントを参照してください。

`%username%`と`%userdomain%`を除き、ユーザー環境変数は使用できません。場所やユーザーなどの組織変数を完全に定義するために、カスタム属性を作成することもできます。属性は大文字と小文字を区別します。

例:

- `\\server\share#sAMAccountName#`は、ユーザー設定をUNCパス`\\server\share\JohnSmith`に保存します（現在のユーザーに対して#sAMAccountName#がJohnSmithに解決される場合）。
- `\\server\profiles$\%USERNAME%.%USERDOMAIN%\!CTX_OSNAME!!CTX_OSBITNESS!`は`\\server\profiles$\JohnSmith.DOMAINCONTROLLER1\Win8x64`に展開される可能性があります。

重要: どの属性または変数を使用する場合でも、このポリシーがNTUSER.DATを含むフォルダーの1つ上のレベルのフォルダーに展開されることを確認してください。たとえば、このファイルが`\\server\profiles$\JohnSmith.Finance\Win8x64\UPM_Profile`に含まれている場合、ユーザー ストアへのパスを`\\server\profiles$\JohnSmith.Finance\Win8x64`に設定します（\UPM_Profileサブフォルダーではありません）。

ユーザー ストアへのパスを指定する際の変数の使用方法の詳細については、次のトピックを参照してください。

- 複数のファイルサーバーでCitrixユーザープロファイルを共有する
- OU内およびOU間でプロファイルを管理する
- Profile Managementによる高可用性と災害復旧

が無効になっている場合、ユーザー設定はホームディレクトリのWindowsサブディレクトリに保存されます。

このポリシーが無効になっている場合、ユーザー設定はホームディレクトリのWindowsサブディレクトリに保存されます。このポリシーがここで構成されていない場合、.iniファイルの値が使用されます。このポリシーがここでも.iniファイルでも構成されていない場合、ホームドライブのWindowsディレクトリが使用されます。

ユーザー ストアの移行

ユーザー設定（レジストリの変更と同期されたファイル）が以前に保存されていたフォルダーへのパス（以前使用していたユーザー ストアのパス）を指定します。

この設定が構成されている場合、以前のユーザー ストアに保存されているユーザー設定は、「ユーザー ストアへのパス」ポリシーで指定された現在のユーザー ストアに移行されます。

パスは、絶対UNCパスまたはホームディレクトリからの相対パスのいずれかです。

どちらの場合も、次の種類の変数を使用できます。

- パーセント記号で囲まれたシステム環境変数
- ハッシュ記号で囲まれたActive Directoryユーザーオブジェクトの属性

例:

- フォルダー `Windows\%ProfileVer%` は、ユーザー設定をユーザー ストアの `Windows\W2K3` というサブフォルダーに保存します（%ProfileVer%がW2K3に解決されるシステム環境変数である場合）。
- `\\server\share#SAMAccountName#` はユーザー設定を UNC パス `\\server\share\<JohnSmith>` に保存します (`#SAMAccountName#` が現在のユーザーに対して JohnSmith に解決される場合)。

パスでは、 `%username%` と `%userdomain%` を除くユーザー環境変数を使用できます。

この設定が無効になっている場合、ユーザー設定は現在のユーザー ストアに保存されます。

この設定がここで構成されていない場合、.ini ファイルの対応する設定が使用されます。

この設定がここで、または .ini ファイルで構成されていない場合、ユーザー設定は現在のユーザー ストアに保存されます。

アクティブなライトバック

変更されたファイルとフォルダー (レジストリ エントリは除く) は、セッション中にログオフする前にユーザー ストアに同期できます。

このポリシーがここで構成されていない場合、.ini ファイルの値が使用されます。このポリシーがここで、または .ini ファイルで構成されていない場合、有効になります。

オフラインプロファイルのサポート

このポリシーにより、プロファイルは可能な限り早い機会にユーザー ストアと同期できます。これは、ローミングするラップトップまたはモバイルデバイスのユーザーを対象としています。ネットワーク接続が切断された場合でも、再起動または休止状態の後でも、プロファイルはラップトップまたはデバイス上でそのまま維持されます。モバイルユーザーが作業すると、プロファイルはローカルで更新されます。また、ネットワーク接続が再確立されると、最終的にユーザー ストアと同期されます。

このポリシーがここで構成されていない場合、.ini ファイルの値が使用されます。このポリシーがここで、または .ini ファイルで構成されていない場合、オフラインプロファイルは無効になります。

アクティブなライトバックレジストリ

このポリシーを「アクティブなライトバック」と併用してください。変更されたレジストリ エントリは、セッション中にユーザー ストアに同期できます。

この設定をここで構成しない場合、.ini ファイルの値が使用されます。

この設定をここで、または .ini ファイルで構成しない場合、アクティブなライトバックレジストリは無効になります。

セッションロックおよび切断時のアクティブライトバック

このポリシーと**アクティブライトバック**ポリシーの両方が有効になっている場合、プロファイルファイルとフォルダーは、セッションがロックまたは切断されたときにのみ書き戻されます。

このポリシーと**アクティブライトバック**および**アクティブライトバックレジストリ**ポリシーの両方が有効になっている場合、レジストリエントリは、セッションがロックまたは切断されたときにのみ書き戻されます。

オフラインプロファイルのサポート

オフラインプロファイル機能を有効にします。この機能は、ネットワークから頻繁に切断されるコンピューター向けです。たとえば、サーバーやデスクトップではなく、ラップトップやモバイルデバイスなどです。

ここでこの設定が構成されていない場合、.iniファイルの値が使用されます。

ここまたは.iniファイルでこの設定が構成されていない場合、オフラインプロファイルのサポートは無効になります。

クロスプラットフォームポリシー設定

このセクションには、**Profile Management cross-platform** 設定機能の構成に関連するポリシー設定が含まれています。

クロスプラットフォーム設定を有効にする

既定では、展開を容易にするため、クロスプラットフォーム設定は無効になっています。この機能を十分に計画しテストした後にのみ、このポリシーを有効にして処理をオンにしてください。

ここでこのポリシーが構成されていない場合、.iniファイルの値が使用されます。ここで、または.iniファイルでこのポリシーが構成されていない場合、クロスプラットフォーム設定は適用されません。

クロスプラットフォーム設定ユーザーグループ

1つ以上のWindowsユーザーグループを入力します。たとえば、このポリシーを使用して、テストユーザーグループのプロファイルのみを処理できます。このポリシーが構成されている場合、Profile Managementのクロスプラットフォーム設定機能は、これらのユーザーグループのメンバーのみを処理します。このポリシーが無効になっている場合、この機能は、処理済みグループポリシーで指定されたすべてのユーザーを処理します。

ここでこのポリシーが構成されていない場合、.iniファイルの値が使用されます。ここで、または.iniファイルでこのポリシーが構成されていない場合、すべてのユーザーグループが処理されます。

クロスプラットフォーム定義へのパス

ダウンロードパッケージからコピーした定義ファイルのネットワーク上の場所を識別します。このパスはUNCパスである必要があります。ユーザーはこの場所への読み取りアクセス権を持ち、管理者は書き込みアクセス権を持っている必要があります。この場所は、Server Message Block (SMB) またはCommon Internet File System (CIFS) ファイル共有である必要があります。

ここでこのポリシーが構成されていない場合、.iniファイルの値が使用されます。ここで、または.iniファイルでこのポリシーが構成されていない場合、クロスプラットフォーム設定は適用されません。

クロスプラットフォーム設定ストアへのパス

ユーザーのクロスプラットフォーム設定が保存されるフォルダーであるクロスプラットフォーム設定ストアへのパスを設定します。ユーザーはこの領域への書き込みアクセス権を持っている必要があります。パスは絶対UNCパスまたはホームディレクトリに対する相対パスにすることができます。

この領域は、複数のプラットフォームで共有されるプロファイルデータが配置されるユーザーストアの共通領域です。ユーザーはこの領域への書き込みアクセス権を持っている必要があります。パスは絶対UNCパスまたはホームディレクトリに対する相対パスにすることができます。**Path to user store** と同じ変数を使用できます。

このポリシーが無効になっている場合、パス Windows\PM_CP が使用されます。ここでこのポリシーが構成されていない場合、.iniファイルの値が使用されます。ここで、または.iniファイルでこのポリシーが構成されていない場合、既定値が使用されます。

クロスプラットフォーム設定を作成するためのソース

このポリシーがそのプラットフォームのOUで有効になっている場合、プラットフォームをベースプラットフォームとして指定します。このポリシーは、ベースプラットフォームのプロファイルからクロスプラットフォーム設定ストアにデータを移行します。

各プラットフォーム独自のプロファイルセットは、別々のOUに保存されます。クロスプラットフォーム設定ストアをシードするために、どのプラットフォームのプロファイルデータを使用するかを決定する必要があります。これはベースプラットフォームと呼ばれます。クロスプラットフォーム設定ストアにデータのない定義ファイルが含まれている場合、または単一プラットフォームプロファイルのキャッシュデータがストア内の定義データよりも新しい場合を考慮してください。この場合、このポリシーを無効にしない限り、プロファイル管理は単一プラットフォームプロファイルからストアにデータを移行します。

> **重要:**
>
> このポリシーが複数のOU、または複数のユーザーオブジェクトやマシンオブジェクトで有効になっている場合、最初にユーザーがログオンしたプラットフォームがベースプロファイルになります。 デフォルトでは、このポリシーは有効になっています。

ファイルシステム ポリシー設定

このセクションには、以下の設定を行うポリシーが含まれています。

- ユーザープロファイル内のどのファイルが、プロファイルがインストールされているシステムとユーザー ストアの間で同期されるか
- ユーザープロファイル内のどのディレクトリが、プロファイルがインストールされているシステムとユーザー ストアの間で同期されるか

除外ポリシー設定

このセクションでは、ユーザープロファイル内のどのファイルとディレクトリを同期プロセスから除外するかを設定するためのポリシー設定について説明します。

除外リスト - ファイル

同期中に無視されるファイルのリスト。ファイル名はユーザープロファイル (%USERPROFILE%) に対する相対パスである必要があります。ワイルドカードはファイル名とフォルダー名でサポートされていますが、ファイル名のワイルドカードのみが再帰的に適用されます。

例:

- `Desktop\Desktop.ini` は `Desktop` フォルダー内のファイル `Desktop.ini` を無視します。
- `%USERPROFILE%*.tmp` はプロファイル全体で拡張子 `.tmp` を持つすべてのファイルを無視します。
- `AppData\Roaming\MyApp*.tmp` はプロファイルの一部で拡張子 `.tmp` を持つすべてのファイルを無視します。
- `Downloads*\a.txt` は `Downloads` フォルダーの直下のサブフォルダーにある `a.txt` を無視します。

このポリシーが無効になっている場合、ファイルは除外されません。このポリシーがここで構成されていない場合、.ini ファイルの値が使用されます。このポリシーがここでも .ini ファイルでも構成されていない場合、ファイルは除外されません。

デフォルトの除外リストを有効にする - ディレクトリ

同期中に無視されるディレクトリのデフォルトリスト。このポリシーを使用して、GPO 除外ディレクトリを手動で入力することなく指定できます。

このポリシーを無効にすると、Profile Management はデフォルトでどのディレクトリも除外しません。

このポリシーをここで構成しない場合、Profile Management は .ini ファイルの値を使用します。このポリシーをここでも .ini ファイルでも構成しない場合、Profile Management はデフォルトでどのディレクトリも除外しません。

除外リスト - ディレクトリ

同期中に無視されるフォルダーのリスト。フォルダー名はユーザープロファイル (%USERPROFILE%) に対する相対パスとして指定する必要があります。フォルダー名でのワイルドカードはサポートされていますが、再帰的には適用されません。

例:

- `Desktop` はユーザープロファイル内の `Desktop` フォルダーを無視します

このポリシーが無効になっている場合、フォルダーは除外されません。このポリシーがここで構成されていない場合、.iniファイルの値が使用されます。このポリシーがここでも.iniファイルでも構成されていない場合、フォルダーは除外されません。

ログオン除外チェック

この設定は、ユーザーストア内のプロファイルに除外されたファイルまたはフォルダーが含まれている場合に、Profile Managementが何を行うかを構成します。可能なポリシー設定と対応するアクションを次の表に示します。

ポリシー設定	アクション
設定が無効になっているか、「ログオン時に除外されたファイルまたはフォルダーを同期する」の値がデフォルトに設定されている	ユーザーがログオンすると、Profile Managementはユーザーストアからローカルプロファイルに除外されたファイルまたはフォルダーを同期します。
設定が「ログオン時に除外されたファイルまたはフォルダーを無視する」に設定されている	ユーザーがログオンすると、Profile Managementはユーザーストア内の除外されたファイルまたはフォルダーを無視します。
設定が「ログオン時に除外されたファイルまたはフォルダーを削除する」に設定されている	ユーザーがログオンすると、Profile Managementはユーザーストア内の除外されたファイルまたはフォルダーを削除します。
Web Studioで設定が構成されていない	.iniファイルの値が使用されます
Web Studioまたは.iniファイルで設定が構成されていない	ユーザーがログオンすると、除外されたファイルまたはフォルダーはユーザーストアからローカルプロファイルに同期されます。

大容量ファイルの処理 - シンボリックリンクとして作成されるファイル

ログオンパフォーマンスを向上させ、サイズの大きいファイルを処理するために、Profile Management はこのリスト内のファイルをコピーする代わりにシンボリックリンクを作成します。

ファイルを参照するポリシーではワイルドカードを使用できます。例: `!ctx_localappdata!\Microsoft\Outlook*.OST`。

Microsoft Outlook のオフラインフォルダーファイル (`*.ost`) を処理するには、**Outlook** フォルダーが Profile Management の対象から除外されていないことを確認してください。

これらのファイルは、複数のセッションで同時にアクセスすることはできません。

同期ポリシー設定

同期セクションでは、ユーザープロファイル内のどのファイルとフォルダーを、プロファイルがインストールされているシステムとユーザー ストアの間で同期するかを指定するためのポリシー設定について説明します。

同期するディレクトリ

デフォルトでは、Profile Management は、ユーザープロファイルがインストールされているシステムとユーザー ストアの間でユーザープロファイルを同期します。同期からフォルダーを除外した場合、このポリシーを使用すると、除外されたフォルダーのサブフォルダーを同期に含めることができます。

このリストのパスは、ユーザープロファイルに対する相対パスである必要があります。フォルダー名でのワイルドカードはサポートされていますが、再帰的には適用されません。

このポリシーがここで構成されていない場合、.ini ファイルの値が使用されます。このポリシーがここでも .ini ファイルでも構成されていない場合、ユーザープロファイル内の除外されていないフォルダーのみが同期されます。

同期するファイル

デフォルトでは、Profile Management は、ユーザープロファイルがインストールされているシステムとユーザー ストアの間でユーザープロファイルを同期します。同期からフォルダーを除外した場合、このポリシーを使用すると、除外されたフォルダー内のファイルを同期に含めることができます。

このリストのパスは、ユーザープロファイルに対する相対パスである必要があります。ファイル名とフォルダー名でワイルドカードがサポートされていますが、ファイル名のワイルドカードのみが再帰的に適用されます。ワイルドカードをネストすることはできません。

例:

- `AppData\Local\Microsoft\Office\Access.qat` は、デフォルト構成で除外されているフォルダーの下にあるファイルを指定します。
- `AppData\Local\MyApp*.cfg` は、プロファイルフォルダー `AppData\Local\MyApp` およびそのサブフォルダー内の拡張子 `.cfg` を持つすべてのファイルを指定します。

このポリシーを無効にすると、有効にして空のリストを構成した場合と同じ効果があります。

このポリシーがここで構成されていない場合、.ini ファイルの値が使用されます。このポリシーがここでも .ini ファイルでも構成されていない場合、ユーザープロファイル内の除外されていないファイルのみが同期されます。

ミラーリングするフォルダー

このポリシーを使用すると、トランザクションフォルダー（参照フォルダーとも呼ばれる）に関連する問題を解決できます。このフォルダーには、相互に依存するファイルが含まれており、あるファイルが別のファイルを参照しています。

フォルダーのミラーリングにより、プロファイル管理はトランザクションフォルダーとその内容を単一のエンティティとして処理し、プロファイルの肥大化を防ぐことができます。たとえば、**Internet Explorer の Cookie** フォルダーをミラーリングして、Index.dat がインデックス化する Cookie と同期されるようにすることができます。このような状況では、「最後の書き込みが優先されます」。そのため、複数のセッションで変更されたミラーリングされたフォルダー内のファイルは、最後の更新によって上書きされ、プロファイル変更が失われます。

たとえば、次の表は、ユーザーがインターネットを閲覧している間に Index.dat が Cookie をどのように参照するかを示しています。

シナリオ	INDEX.DAT が COOKIE を参照する方法	
ユーザーは2つの Internet Explorer セッションを持っており、それぞれ異なるサーバー上にあり、各セッションで異なるサイトを訪れます。	各サイトからの Cookie は、適切なサーバーに追加されます。	各サイトからの Cookie は、適切なサーバーに追加されます。
ユーザーは最初のセッションからログオフするか、セッションの途中でログオフします（アクティブなライトバック機能が構成されている場合）。	2番目のセッションからの Cookie は、最初のセッションからの Cookie を置き換える必要があります。	
最初のセッションと2番目のセッションがマージされ、Index.dat 内の Cookie への参照が古くなります。	新しいセッションでのその後の閲覧は、繰り返しのマージと肥大化した Cookie フォルダーにつながります。	

Cookie フォルダーをミラーリングすることで、この問題が解決されます。この場合、ユーザーがログオフするたびに、Cookie は最後のセッションからの Cookie で上書きされます。これにより、Index.dat は常に最新の状態に保たれます。

ここでこのポリシーが構成されていない場合、.ini ファイルの値が使用されます。ここで、または .ini ファイルでこのポリシーが構成されていない場合、フォルダーはミラーリングされません。

フォルダーのミラーリングを高速化する

このポリシーと**ミラーリングするフォルダー**ポリシーの両方が有効になっている場合、**プロファイル管理はミラーリングされた**フォルダーを VHDX ベースの仮想ディスクに保存します。ログオン中に仮想ディスクをアタッチし、ログオフ中にデタッチします。このポリシーを有効にすると、ユーザー ストアとローカル プロファイルの間でフォルダーをコピーする必要がなくなり、フォルダーのミラーリングが高速化されます。

ファイル重複排除ポリシー設定

ユーザーストア内のさまざまなユーザープロファイルに同一のファイルが存在する場合があります。ユーザーストアにファイルの重複インスタンスが保存されていると、ストレージコストが増加します。

ファイル重複排除ポリシーにより、Profile Management はユーザーストアから重複ファイルを削除し、それらの単一インスタンスを中央の場所 (*共有ストア* と呼ばれる) に保存できます。これにより、ユーザーストアでのファイルの重複が回避され、ストレージコストが節約されます。

重複排除のために共有ストアに含めるファイル

ファイル重複排除を有効にし、重複排除のために共有ストアに含めるファイルを指定できます。

共有ストアから除外するファイル

共有ストアから除外するファイルを指定できます。このポリシーは、*重複排除のために共有ストアに含めるファイル* ポリシーと併用してください。

プロファイルコンテナから重複排除するファイルの最小サイズ

プロファイルコンテナから重複排除するファイルの最小サイズを指定できます。サイズは 256 MB 以上である必要があります。

構成の優先順位:

1. ここでこの設定が構成されていない場合、.iniファイルの値が使用されます。
2. この設定がここまたは .ini ファイルのいずれかで構成されていない場合、値は 256 です。

フォルダーリダイレクトのポリシー設定

このセクションには、プロファイルに一般的に表示されるフォルダーを共有ネットワークの場所にリダイレクトするかどうかを指定するポリシー設定が含まれています。

管理者アクセスの許可

この設定により、管理者はユーザーのリダイレクトされたフォルダーの内容にアクセスできるようになります。

> **注：**
>
> この設定は、ドメインへの完全かつ無制限のアクセス権を持つ管理者に対して権限を付与します。

デフォルトでは、この設定は無効になっており、ユーザーにはリダイレクトされたフォルダーの内容への排他的なアクセス権が付与されます。

ドメイン名を含める

この設定により、`%userdomain%` 環境変数を UNC パスの一部として組み込むことができます。この UNC パスは、リダイレクトされたフォルダーに対して指定されます。

デフォルトでは、この設定は無効になっています。そして、リダイレクトされたフォルダーに対して指定される UNC パスの一部として、`%userdomain%` 環境変数は含まれません。

AppData(Roaming) ポリシー設定

このセクションには、**AppData(Roaming)** フォルダーのコンテンツを共有ネットワークの場所にリダイレクトするためのポリシー設定が含まれています。

APPDATA(ROAMING) パス

この設定は、**AppData(Roaming)** フォルダーのコンテンツがリダイレクトされるネットワークの場所を指定します。

デフォルトでは、この設定は無効になっており、場所は指定されていません。

ここでこの設定が構成されていない場合、Profile Management は指定されたフォルダーをリダイレクトしません。

APPDATA(ROAMING) のリダイレクト設定

この設定は、**AppData(Roaming)** フォルダーのコンテンツをリダイレクトする方法を指定します。

デフォルトでは、コンテンツは UNC パスにリダイレクトされます。詳細については、ユーザー ストアへのパス セクションを参照してください。

ここでこの設定が構成されていない場合、Profile Management は指定されたフォルダーをリダイレクトしません。

デスクトップポリシー設定

このセクションには、`Desktop` フォルダーのコンテンツを共有ネットワークの場所にリダイレクトするためのポリシー設定が含まれています。

デスクトップパス

この設定は、**デスクトップ**フォルダーのコンテンツがリダイレクトされるネットワークの場所を指定します。

デフォルトでは、この設定は無効になっており、場所は指定されていません。

ここでこの設定が構成されていない場合、Profile Management は指定されたフォルダーをリダイレクトしません。

デスクトップのリダイレクト設定

この設定は、**デスクトップ**フォルダーのコンテンツをリダイレクトする方法を指定します。

デフォルトでは、コンテンツは UNC パスにリダイレクトされます。

ここでこの設定が構成されていない場合、Profile Management は指定されたフォルダーをリダイレクトしません。

ドキュメントポリシー設定

このセクションには、**ドキュメント**フォルダーの内容を共有ネットワークの場所にリダイレクトするためのポリシー設定が含まれています。

ドキュメントパス

この設定は、**ドキュメント**フォルダー内のファイルがリダイレクトされるネットワークの場所を指定します。

デフォルトでは、この設定は無効になっており、場所は指定されていません。

ここでこの設定が構成されていない場合、Profile Management は指定されたフォルダーをリダイレクトしません。

ドキュメントパス設定は、**ドキュメント**フォルダーへのファイルのリダイレクトだけでなく、**ミュージック**、**ピクチャ**、**ビデオ**フォルダーへのファイルのリダイレクトのためにも有効にする必要があります。

ドキュメントのリダイレクト設定

この設定は、**ドキュメント**フォルダーの内容をリダイレクトする方法を指定します。

デフォルトでは、内容は UNC パスにリダイレクトされます。

ドキュメントフォルダーの内容をリダイレクトする方法を制御するには、次のいずれかのオプションを選択します。

- 次の UNC パスにリダイレクトします。ドキュメントパスポリシー設定で指定された UNC パスにコンテンツをリダイレクトします。
- ユーザーのホームディレクトリにリダイレクトします。コンテンツをユーザーのホームディレクトリにリダイレクトします。これは通常、Active Directory のユーザーの #homeDirectory# 属性として構成されます。

ここでこの設定が構成されていない場合、Profile Management は指定されたフォルダーをリダイレクトしません。

ダウンロードのポリシー設定

このセクションには、**ダウンロード**フォルダーのコンテンツを共有ネットワークの場所にリダイレクトするためのポリシー設定が含まれています。

ダウンロードパス

この設定は、**ダウンロード**フォルダー内のファイルがリダイレクトされるネットワークの場所を指定します。

デフォルトでは、この設定は無効になっており、場所は指定されていません。

ここでこの設定が構成されていない場合、Profile Management は指定されたフォルダーをリダイレクトしません。

ダウンロードのリダイレクト設定

この設定は、**ダウンロード**フォルダーのコンテンツをリダイレクトする方法を指定します。

デフォルトでは、コンテンツはUNCパスにリダイレクトされます。

ここでこの設定が構成されていない場合、Profile Management は指定されたフォルダーをリダイレクトしません。

お気に入りポリシー設定

このセクションには、「**お気に入り**」フォルダーのコンテンツを共有ネットワークの場所にリダイレクトするためのポリシー設定が含まれています。

お気に入りパス

この設定は、「**お気に入り**」フォルダーのコンテンツがリダイレクトされるネットワークの場所を指定します。

デフォルトでは、この設定は無効になっており、場所は指定されていません。

この設定がここで構成されていない場合、Profile Management は指定されたフォルダーをリダイレクトしません。

お気に入りのリダイレクト設定

この設定は、「**お気に入り**」フォルダーのコンテンツをリダイレクトする方法を指定します。

デフォルトでは、コンテンツは UNC パスにリダイレクトされます。

この設定がここで構成されていない場合、Profile Management は指定されたフォルダーをリダイレクトしません。

リンクポリシー設定

このセクションには、**リンク**フォルダーのコンテンツを共有ネットワークの場所にリダイレクトするためのポリシー設定が含まれています。

リンクパス

この設定は、**リンク**フォルダーのコンテンツがリダイレクトされるネットワークの場所を指定します。

デフォルトでは、この設定は無効になっており、場所は指定されていません。

ここでこの設定が構成されていない場合、Profile Management は指定されたフォルダーをリダイレクトしません。

リンクのリダイレクト設定

この設定は、**リンク**フォルダーのコンテンツをリダイレクトする方法を指定します。

デフォルトでは、コンテンツは UNC パスにリダイレクトされます。

ここでこの設定が構成されていない場合、Profile Management は指定されたフォルダーをリダイレクトしません。

音楽ポリシー設定

このセクションには、**Music**フォルダーのコンテンツを共有ネットワークの場所にリダイレクトするためのポリシー設定が含まれています。

音楽パス

この設定は、**Music**フォルダーのコンテンツがリダイレクトされるネットワークの場所を指定します。

デフォルトでは、この設定は無効になっており、場所は指定されていません。

ここでこの設定が構成されていない場合、Profile Managementは指定されたフォルダーをリダイレクトしません。

音楽のリダイレクト設定

この設定は、**Music**フォルダーのコンテンツをリダイレクトする方法を指定します。

デフォルトでは、コンテンツはUNCパスにリダイレクトされます。

Musicフォルダーのコンテンツをリダイレクトする方法を制御するには、次のいずれかのオプションを選択します。

- 次のUNCパスにリダイレクトします。Musicパスポリシー設定で指定されたUNCパスにコンテンツをリダイレクトします。
- ドキュメントフォルダーを基準にリダイレクトします。ドキュメントフォルダーを基準としたフォルダーにコンテンツをリダイレクトします。

Documentsフォルダーを基準としたフォルダーにコンテンツをリダイレクトするには、**Documents path**設定を有効にする必要があります。

ここでこの設定が構成されていない場合、Profile Managementは指定されたフォルダーをリダイレクトしません。

画像ポリシー設定

このセクションには、**画像**フォルダーのコンテンツを共有ネットワークの場所にリダイレクトするためのポリシー設定が含まれています。

画像パス

この設定は、**画像**フォルダーのコンテンツがリダイレクトされるネットワークの場所を指定します。

デフォルトでは、この設定は無効になっており、場所は指定されていません。

ここでこの設定が構成されていない場合、Profile Management は指定されたフォルダーをリダイレクトしません。

画像のリダイレクト設定

この設定は、**画像**フォルダーのコンテンツをリダイレクトする方法を指定します。

デフォルトでは、コンテンツは UNC パスにリダイレクトされます。

画像フォルダーのコンテンツをリダイレクトする方法を制御するには、次のいずれかのオプションを選択します。

- 次の UNC パスにリダイレクトします。コンテンツを「画像パス」ポリシー設定で指定された UNC パスにリダイレクトします。
- ドキュメントフォルダーを基準にリダイレクトします。コンテンツをドキュメントフォルダーを基準としたフォルダーにリダイレクトします。

コンテンツを**ドキュメント**フォルダーを基準としたフォルダーにリダイレクトするには、**ドキュメントパス**設定を有効にする必要があります。

ここでこの設定が構成されていない場合、Profile Management は指定されたフォルダーをリダイレクトしません。

Searchesポリシー設定

このセクションには、**Searches**フォルダーのコンテンツを共有ネットワークの場所にリダイレクトするためのポリシー設定が含まれています。

SEARCHESのリダイレクト設定

この設定は、**Searches**フォルダーのコンテンツをリダイレクトする方法を指定します。

デフォルトでは、コンテンツはUNCパスにリダイレクトされます。

ここでこの設定が構成されていない場合、Profile Managementは指定されたフォルダーをリダイレクトしません。

SEARCHESパス

この設定は、**Searches**フォルダーのコンテンツがリダイレクトされるネットワークの場所を指定します。

デフォルトでは、この設定は無効になっており、場所は指定されていません。

ここでこの設定が構成されていない場合、Profile Managementは指定されたフォルダーをリダイレクトしません。

スタートメニューのポリシー設定

このセクションには、**スタートメニュー**フォルダーのコンテンツを共有ネットワークの場所にリダイレクトするためのポリシー設定が含まれています。

スタートメニューのリダイレクト設定

この設定は、**スタートメニュー**フォルダーのコンテンツをリダイレクトする方法を指定します。

デフォルトでは、コンテンツはUNCパスにリダイレクトされます。

ここでこの設定が構成されていない場合、Profile Managementは指定されたフォルダーをリダイレクトしません。

スタートメニューのパス

この設定は、**スタートメニュー**フォルダーのコンテンツがリダイレクトされるネットワークの場所を指定します。

デフォルトでは、この設定は無効になっており、場所は指定されていません。

ここでこの設定が構成されていない場合、Profile Managementは指定されたフォルダーをリダイレクトしません。

ビデオポリシー設定

このセクションには、**ビデオ**フォルダーのコンテンツを共有ネットワークの場所にリダイレクトするためのポリシー設定が含まれています。

ビデオのリダイレクト設定

この設定は、**ビデオ**フォルダーのコンテンツをリダイレクトする方法を指定します。

デフォルトでは、コンテンツはUNCパスにリダイレクトされます。

ビデオフォルダーのコンテンツをリダイレクトする方法を制御するには、次のいずれかのオプションを選択します。

- 次のUNCパスにリダイレクトします。コンテンツを、ビデオパスポリシー設定で指定されたUNCパスにリダイレクトします。
- ドキュメントフォルダーを基準にリダイレクトします。コンテンツを、ドキュメントフォルダーを基準としたフォルダーにリダイレクトします。

コンテンツを**ドキュメント**フォルダーを基準としたフォルダーにリダイレクトするには、**ドキュメントパス**設定を有効にする必要があります。

この設定がここで構成されていない場合、Profile Managementは指定されたフォルダーをリダイレクトしません。

ビデオパス

この設定は、**ビデオ**フォルダーのコンテンツがリダイレクトされるネットワークの場所を指定します。

デフォルトでは、この設定は無効になっており、場所は指定されていません。

この設定がここで構成されていない場合、Profile Managementは指定されたフォルダーをリダイレクトしません。

ログポリシー設定

このセクションには、Profile Management のログ記録を構成するポリシー設定が含まれています。

Active Directory のアクション

この設定は、Active Directory で実行されるアクションの詳細ログを有効または無効にします。

デフォルトでは、この設定は無効になっています。

この設定を有効にする場合は、**ログ記録を有効にする**設定も有効になっていることを確認してください。

この設定が Web Studio で構成されていない場合、.ini ファイルの値が使用されます。

この設定が Web Studio または .ini ファイルで構成されていない場合、以下がログに記録されます。

- エラー
- 一般情報

一般情報

この設定は、一般情報の詳細ログを有効または無効にします。

デフォルトでは、この設定は無効になっています。

この設定を有効にする場合は、**ログ記録を有効にする**設定も有効になっていることを確認してください。

この設定がここで構成されていない場合、.ini ファイルの値が使用されます。

この設定がWeb Studioまたは.iniファイルで構成されていない場合、以下がログに記録されます。

- エラー
- 一般情報

一般的な警告

この設定は、一般的な警告の詳細ログを有効または無効にします。

デフォルトでは、この設定は無効になっています。

この設定を有効にする際は、**ログの有効化**設定も有効になっていることを確認してください。

この設定がここで構成されていない場合、.iniファイルの値が使用されます。

この設定がWeb Studioまたは.iniファイルで構成されていない場合、以下がログに記録されます。

- エラー
- 一般情報

ログの有効化

この設定は、デバッグ（詳細ログ）モードでのProfile Managementのログ記録を有効または無効にします。デバッグモードでは、"%SystemRoot%\System32\Logfiles\UserProfileManager" にあるログファイルに詳細なステータス情報が記録されます。

デフォルトでは、この設定は無効になっており、エラーのみがログに記録されます。

Citrix®は、Profile Managementのトラブルシューティングを行う場合にのみ、この設定を有効にすることをお勧めします。

この設定がここで構成されていない場合、.iniファイルの値が使用されます。

この設定がここまたは.iniファイルで構成されていない場合、エラーのみがログに記録されます。

ファイルシステムアクション

この設定は、ファイルシステムで実行されるアクションの詳細ログを有効または無効にします。

デフォルトでは、この設定は無効になっています。

この設定を有効にする場合は、**ログの有効化**設定も有効になっていることを確認してください。

この設定がここで構成されていない場合、.iniファイルの値が使用されます。

この設定がWeb Studioまたは.iniファイルで構成されていない場合、以下がログに記録されます。

- エラー

- 一般情報

ファイルシステム通知

この設定は、ファイルシステム通知の詳細ログを有効または無効にします。

デフォルトでは、この設定は無効になっています。

この設定を有効にする場合は、**ログの有効化**設定も有効になっていることを確認してください。

この設定がここで構成されていない場合、.iniファイルの値が使用されます。

この設定がWeb Studioまたは.iniファイルで構成されていない場合、以下がログに記録されます。

- エラー
- 一般情報

ログオフ

この設定は、ユーザーのログオフの詳細ログを有効または無効にします。

デフォルトでは、この設定は無効になっています。

この設定を有効にする際は、**ログ記録を有効にする**設定も有効になっていることを確認してください。

ここでこの設定が構成されていない場合、.iniファイルの値が使用されます。

この設定がWeb Studioまたは.iniファイルで構成されていない場合、以下がログに記録されます。

- エラー
- 一般情報

ログオン

この設定は、ユーザーのログオンの詳細ログを有効または無効にします。

デフォルトでは、この設定は無効になっています。

この設定を有効にする際は、**ログ記録を有効にする**設定も有効になっていることを確認してください。

この設定がここで構成されていない場合、.iniファイルの値が使用されます。

この設定がWeb Studioまたは.iniファイルで構成されていない場合、以下がログに記録されます。

- エラー

- 一般情報

ログファイルの最大サイズ

この設定は、Profile Managementログファイルの最大許容サイズをバイト単位で指定します。

デフォルトでは、この値は1048576バイト（1 MB）に設定されています。

十分なディスク容量がある場合、Citrixはこのファイルのサイズを5 MB以上に増やすことを推奨します。ログファイルが最大サイズを超えて増加した場合：

- 既存のファイルのバックアップ（.bak）が削除されます
- ログファイルは.bakに名前が変更されます
- 新しいログファイルが作成されます

ログファイルは`%SystemRoot%\System32\Logfiles\UserProfileManager`に作成されます。

この設定がここで構成されていない場合、.iniファイルの値が使用されます。

この設定がここで、または.iniファイルで構成されていない場合、デフォルト値が使用されます。

ログファイルへのパス

この設定は、Profile Managementログファイルを保存するための代替パスを指定します。

デフォルトでは、この設定は無効になっており、ログファイルはデフォルトの場所 (%SystemRoot%\System32\Logfiles\UserProfileManager) に保存されます。

パスは、ローカルドライブまたはリモートのネットワークベースドライブ (UNCパス) を指すことができます。リモートパスは大規模な分散環境で役立つ場合がありますが、大量のネットワークトラフィックを生成する可能性があり、ログファイルには不適切かもしれません。永続的なハードドライブを持つプロビジョニングされた仮想マシンの場合は、そのドライブへのローカルパスを設定します。この設定により、マシンの再起動時にログファイルが保持されます。永続的なハードドライブを持たない仮想マシンの場合は、UNCパスを設定することでログファイルを保持できます。ただし、マシンのシステムアカウントはUNC共有への書き込みアクセス権を持っている必要があります。オフラインプロファイル機能によって管理されるラップトップには、ローカルパスを使用してください。

ログファイルにUNCパスを使用する場合、Citrixはログファイルフォルダーに適切なアクセス制御リストを適用することを推奨します。この設定により、承認されたユーザーまたはコンピューターアカウントのみが保存されたファイルにアクセスできるようになります。

この設定がここで構成されていない場合、.iniファイルの値が使用されます。

この設定がここでも.iniファイルでも構成されていない場合、デフォルトの場所 %SystemRoot%\System32\Logfiles\UserProfileManager が使用されます。

パーソナライズされたユーザー情報

この設定は、パーソナライズされたユーザー情報の詳細ログを有効または無効にします。

デフォルトでは、この設定は無効になっています。

この設定を有効にする際は、**ログの有効化** 設定も有効になっていることを確認してください。

この設定がここで構成されていない場合、.iniファイルの値が使用されます。

この設定がWeb Studioまたは.iniファイルで構成されていない場合、以下がログに記録されます。

- エラー
- 一般情報

ログオン時およびログオフ時のポリシー値

この設定は、ユーザーがログオンおよびログオフする際のポリシー値の詳細ログを有効または無効にします。

デフォルトでは、この設定は無効になっています。

この設定を有効にする場合は、**ログ記録を有効にする**設定も有効になっていることを確認してください。

この設定がここで構成されていない場合、.iniファイルの値が使用されます。

この設定がWeb Studioまたは.iniファイルで構成されていない場合、以下がログに記録されます。

- エラー
- 一般情報

レジストリアクション

この設定は、レジストリで実行されたアクションの詳細ログを有効または無効にします。

デフォルトでは、この設定は無効になっています。

この設定を有効にする場合は、**ログ記録を有効にする**設定も有効になっていることを確認してください。

この設定がここで構成されていない場合、.iniファイルの値が使用されます。

この設定がWeb Studioまたは.iniファイルで構成されていない場合、以下がログに記録されます。

- エラー
- 一般情報

ログオフ時のレジストリの差異

この設定は、ユーザーがログオフしたときにレジストリ内の差異を詳細にログ記録するかどうかを有効または無効にします。

デフォルトでは、この設定は無効になっています。

この設定を有効にする場合は、**ログ記録を有効にする**設定も有効になっていることを確認してください。

この設定がここで構成されていない場合、.iniファイルの値が使用されます。

この設定がWeb Studioまたは.iniファイルで構成されていない場合、以下がログに記録されます。

- エラー
- 一般情報

プロファイル処理ポリシー設定

このセクションには、Profile Management がユーザープロファイルを処理する方法を指定するポリシー設定が含まれています。

キャッシュされたプロファイルを削除するまでの遅延

この設定は、Profile Management がログオフ時にローカルにキャッシュされたプロファイルを削除するまでの遅延を、分単位でオプションで延長する時間を指定します。

値が 0 の場合、ログオフプロセスの終了時にプロファイルがすぐに削除されます。Profile Management は 1 分ごとにログオフをチェックします。その結果、値が 60 の場合、ユーザーがログオフしてから 1 ～ 2 分の間にプロファイルが削除されることが保証されます。このアクションは、最後のチェックがいつ行われたかによって異なります。ログオフ中にプロセスがファイルまたはユーザーレジストリハイブを開いたままにしていることがわかっている場合、遅延を延長すると便利です。大規模なプロファイルの場合、このプロセスはログオフを高速化することもできます。

デフォルトでは、この値は 0 に設定されており、Profile Management はローカルにキャッシュされたプロファイルをすぐに削除します。

この設定を有効にする場合は、「ログオフ時にローカルにキャッシュされたプロファイルを削除する」も有効になっていることを確認してください。

この設定がここで構成されていない場合、.ini ファイルの値が使用されます。

この設定がここでも .ini ファイルでも構成されていない場合、プロファイルはすぐに削除されます。

ログオフ時にローカルにキャッシュされたプロファイルを削除する

この設定は、ユーザーがログオフした後にローカルにキャッシュされたプロファイルが削除されるかどうかを指定します。

この設定が有効になっている場合、ユーザーのローカルプロファイルキャッシュはログオフ後に削除されます。Citrix® は、ターミナルサーバーでこの設定を有効にすることをお勧めします。

デフォルトでは、この設定は無効になっており、ユーザーのローカルプロファイルキャッシュはログオフ後も保持されます。

この設定がここで構成されていない場合、.ini ファイルの値が使用されます。

この設定がここでも .ini ファイルでも構成されていない場合、キャッシュされたプロファイルは削除されません。

ローカルプロファイルの競合処理

この設定は、ユーザープロファイルが以下の両方に存在する場合のProfile Managementの動作を構成します。

- ユーザーストア
- ローカルWindowsユーザープロファイル（Citrixユーザープロファイルではない）

デフォルトでは、Profile ManagementはローカルWindowsプロファイルを使用しますが、それを変更することはありません。

Profile Managementの動作を制御するには、以下のいずれかのオプションを選択します。

- ローカルプロファイルを使用する。Profile Managementはローカルプロファイルを使用しますが、それを変更することはありません。
- ローカルプロファイルを削除する。Profile ManagementはローカルWindowsユーザープロファイルを削除し、その後、ユーザーストアからCitrixユーザープロファイルをインポートします。

- ローカルプロファイルの名前を変更する。Profile ManagementはローカルWindowsユーザープロファイルの名前を変更し（バックアップ目的で）、その後、ユーザーストアからCitrixユーザープロファイルをインポートします。

この設定がここで構成されていない場合、.iniファイルの値が使用されます。

この設定がここでも.iniファイルでも構成されていない場合、既存のローカルプロファイルが使用されます。

既存プロファイルの移行

この設定は、ユーザーがユーザーストアに現在のプロファイルを持っていない場合に、ログオン中にユーザーストアに移行されるプロファイルの種類を指定します。

ユーザーがユーザーストアにプロファイルを持っていない場合、Profile Managementはログオン中に既存のプロファイルを「その場で」移行できます。その後、以下の両方でユーザーストアプロファイルがProfile Managementによって使用されます。

- 現在のセッション
- 同じユーザー ストアへのパスで構成されたその他のセッション

デフォルトでは、ログオン時にローカルプロファイルと移動プロファイルの両方がユーザー ストアに移行されます。

ログオン時にユーザー ストアに移行されるプロファイルの種類を指定するには、次のいずれかのオプションを選択します。

- ローカルプロファイルと移動プロファイル
- ローカル
- 移動
- なし（無効）

なしを選択すると、システムは、Profile Managementがインストールされていない環境であるかのように、既存のWindowsメカニズムを使用してプロファイルを作成します。

この設定がここで構成されていない場合、.iniファイルの値が使用されます。

この設定がここでも.iniファイルでも構成されていない場合、既存のローカルプロファイルと移動プロファイルが移行されます。

既存のアプリケーションプロファイルの自動移行

この設定は、異なるオペレーティングシステム間での既存のアプリケーションプロファイルの自動移行を有効または無効にします。アプリケーションプロファイルには、`AppData`フォルダー内のアプリケーションデータと、`HKEY_CURRENT_USER\SOFTWARE`の下のレジストリエントリの両方が含まれます。この設定は、異なるオペレーティングシステム間でアプリケーションプロファイルを移行したい場合に役立ちます。

たとえば、オペレーティングシステム（OS）をWindows 10バージョン1803からWindows 10バージョン1809にアップグレードするとします。この設定が有効になっている場合、各ユーザーが最初にログオンしたときに、Profile Managementは既存のアプリケーション設定をWindows 10バージョン1809に自動的に移行します。その結果、`AppData`フォルダー内のアプリケーションデータと、HKEY_CURRENT_USER\SOFTWAREの下のレジストリエントリが移行されます。

複数の既存のアプリケーションプロファイルがある場合、Profile Managementは次の優先順位で移行を実行します。

1. 同じOSタイプのプロファイル（シングルセッションOSからシングルセッションOSへ、マルチセッションOSからマルチセッションOSへ）。
2. 同じWindows OSファミリーのプロファイル。例: Windows 10からWindows 10、またはWindows Server 2016からWindows Server 2016。
3. 以前のバージョンのOSのプロファイル。例: Windows 7からWindows 10、またはWindows Server 2012からWindows 2016。
4. 最も近いOSのプロファイル。

注: ユーザーストアパスに変数「!CTX_OSNAME!」を含めることで、OSの短い名前を指定する必要があります。これにより、Profile Managementは既存のアプリケーションプロファイルを特定できます。

ここでこの設定が構成されていない場合、.iniファイルの設定が使用されます。

ここでも.iniファイルでもこの設定が構成されていない場合、デフォルトで無効になります。

テンプレートプロファイルへのパス

この設定は、Profile Managementがユーザープロファイルを作成するためのテンプレートとして使用するプロファイルへのパスを指定します。

指定されたパスは、NTUSER.DATレジストリファイル、およびテンプレートプロファイルに必要なその他のフォルダーとファイルを含むフォルダーへの完全なパスである必要があります。

注: パスにNTUSER.DATを含めないでください。たとえば、ファイル`\\myservername\myprofiles\template\ntuser.dat`の場合、場所を`\\myservername\myprofiles\template`として設定します。

絶対パスを使用します。絶対パスは、UNCパスまたはローカルマシン上のパスのいずれかです。後者を使用すると、たとえば、Citrix Provisioning™ Servicesイメージ上にテンプレートプロファイルを永続的に指定できます。相対パスはサポートされていません。

注: この設定は、Active Directory属性、システム環境変数、または`%USERNAME%`および`%USERDOMAIN%`変数の展開をサポートしていません。

デフォルトでは、この設定は無効になっており、新しいユーザープロファイルは、ユーザーが最初にログオンするデバイスのデフォルトユーザープロファイルから作成されます。

ここでこの設定が構成されていない場合、.iniファイルの値が使用されます。

ここでも.iniファイルでもこの設定が構成されていない場合、テンプレートは使用されません。

テンプレートプロファイルがローカルプロファイルを上書きする

この設定により、ユーザープロファイルの作成時にテンプレートプロファイルがローカルプロファイルを上書きできるようになります。

ユーザーがCitrixユーザープロファイルを持たず、ローカルのWindowsユーザープロファイルを持っているとします。この場合、この値が有効になっていると、デフォルトでローカルプロファイルが使用され、ユーザーストアに移行されます。このポリシー設定を有効にすると、ユーザープロファイルの作成時に使用されるローカルプロファイルをテンプレートプロファイルが上書きできるようになります。

ここでこの設定が構成されていない場合、.iniファイルの値が使用されます。

ここでも.iniファイルでもこの設定が構成されていない場合、テンプレートは使用されません。

テンプレートプロファイルが移動プロファイルを上書きする

この設定により、ユーザープロファイルの作成時にテンプレートプロファイルが移動プロファイルを上書きできるようになります。

ユーザーがCitrixユーザープロファイルを持たず、移動Windowsユーザープロファイルを持っているとします。この場合、この値が有効になっていると、デフォルトで移動プロファイルが使用され、ユーザーストアに移行されます。このポリシー設定を有効にすると、ユーザープロファイルの作成時に使用される移動プロファイルをテンプレートプロファイルが上書きできるようになります。

ここでこの設定が構成されていない場合、.iniファイルの値が使用されます。

ここでも.iniファイルでもこの設定が構成されていない場合、テンプレートは使用されません。

すべてのログオンでCitrix必須プロファイルとして使用されるテンプレートプロファイル

この設定により、Profile Managementはテンプレートプロファイルをすべてのユーザープロファイルを作成するためのデフォルトプロファイルとして使用できるようになります。

デフォルトでは、この設定は無効になっており、新しいユーザープロファイルは、ユーザーが最初にログオンしたデバイスのデフォルトユーザープロファイルから作成されます。

ここでこの設定が構成されていない場合、.iniファイルの値が使用されます。

ここでも.iniファイルでもこの設定が構成されていない場合、テンプレートは使用されません。

プロファイルコンテナのポリシー設定

プロファイルコンテナ

ユーザープロファイルに関連付けられた大きなフォルダーは、ログオンの遅延を引き起こします。Citrix Profile Managementは、プロファイルディスク（VHDXファイル）に含めるフォルダーを指定できるVHDXベースのプロファイルソリューションを提供します。このソリューションは、指定されたフォルダーをネットワークに保存されているプロファイルディスクにマッピングすることで、ログオン時間を短縮します。プロファイルコンテナは、ログオン時にこれらのフォルダーを含むプロファイルディスクをアタッチするため、フォルダーのコピーをローカルプロファイルに保存する必要がなくなります。これにより、ログオン時間が短縮されます。

プロファイルコンテナのローカルキャッシュを有効にする

このポリシーは、Citrix Profile Managementプロファイルコンテナのローカルキャッシュサポートを有効にします。ポリシーが**有効**に設定されている場合、各ローカルプロファイルは、そのCitrix Profile Managementプロファイルコンテナのローカルキャッシュとして機能します。プロファイルストリーミングが使用されている場合、ローカルにキャッシュされたファイルはオンデマンドで作成されます。それ以外の場合は、ユーザーログオン時に作成されます。ローカルキャッシュ機能を使用するには、ユーザープロファイル全体をCitrix Profile Managementプロファイルコンテナに配置します。

プロファイルコンテナから除外するフォルダー

Citrix Profile Managementプロファイルコンテナから除外するフォルダーのリスト。

プロファイルコンテナに含めるフォルダー

親フォルダーが除外されている場合に、Citrix Profile Managementプロファイルコンテナに保持するフォルダーのリスト。

このリストのフォルダーは、除外されたフォルダーのサブフォルダーである必要があります。そうでない場合、この設定は機能しません。

プロファイルコンテナに含めるファイル

Citrix Profile Managementプロファイルコンテナに含めるファイルのリスト。

このリストのファイルは、除外されたフォルダー内にある必要があります。そうでない場合、この設定は機能しません。

プロファイルコンテナから除外するファイル

Citrix Profile Managementプロファイルコンテナから除外するファイルのリスト。

VHDディスクの圧縮を有効にする

Profile ManagementのVHDディスク圧縮を有効にできます。有効にすると、特定の条件が満たされたときに、ユーザーのログオフ時にVHDディスクが自動的に圧縮されます。このポリシーにより、プロファイルコンテナ、OneDriveコンテナ、およびミラーフォルダコンテナによって消費されるストレージスペースを節約できます。

必要性と利用可能なリソースに応じて、詳細設定にある「**VHDディスク圧縮をトリガーする空き領域の比率**」、「**VHDディスク圧縮をトリガーするログオフ回数**」、「**VHDディスク圧縮のデフラグを無効にする**」の各ポリシーを使用して、デフォルトのVHD圧縮設定と動作を調整できます。

プロファイルコンテナのVHD自動拡張を有効にする

プロファイルコンテナのVHD自動拡張を有効にするかどうかを指定できます。有効にすると、すべてのVHD自動拡張設定がプロファイルコンテナに適用されます。

構成の優先順位:

- ここでこのポリシーが構成されていない場合、.iniファイルの値が使用されます。
- ここでも.iniファイルでもこのポリシーが構成されていない場合、無効になります。

VHDコンテナへの排他的アクセスを有効にする

デフォルトでは、VHDコンテナは同時アクセスを許可します。この設定を有効にすると、一度に1つのアクセスのみが許可されます。この機能は、プロファイルコンテナとOneDriveコンテナに適用されます。

> **注：**
>
> コンテナベースのプロファイルソリューションでプロファイルコンテナに対してこの設定を有効にすると、「*プロファイルコンテナのマルチセッションライトバックを有効にする*」設定が自動的に無効になります。
>
> 構成の優先順位:

1. ここでこのポリシーが構成されていない場合、.iniファイルの値が使用されます。
2. ここでも.iniファイルでもこのポリシーが構成されていない場合、設定は無効になります。

ログオン時にプロファイルコンテナが利用できない場合にユーザーをログオフする

ユーザーログオン時にプロファイルコンテナが利用できない場合にユーザーを強制的にログオフさせ、(オプションで)ユーザーに表示されるエラーメッセージをカスタマイズできます。

構成の優先順位:

1. ここでこのポリシーが構成されていない場合、.iniファイルの値が使用されます。
2. ここでも.iniファイルでもこのポリシーが構成されていない場合、設定は無効になります。

プロファイルコンテナにアクセスするユーザーとグループ

プロファイルコンテナに対する`Read & Execute`権限を持つADドメインユーザーとグループを指定できます。デフォルトでは、プロファイルコンテナはその所有者のみがアクセスできます。

構成の優先順位:

1. このポリシーがここで構成されていない場合、.iniファイルの設定が使用されます。
2. このポリシーがここでも.iniファイルでも構成されていない場合、プロファイルコンテナはその所有者のみがアクセスできます。

レジストリポリシー設定

このセクションには、Profile Management の処理から含める、または除外するレジストリキーを指定するポリシー設定が含まれています。

除外リスト

ログオフ時に無視されるHKCUハイブ内のレジストリキーのリスト。

例: Software\Policies

このポリシーが無効になっている場合、レジストリキーは除外されません。ここでこのポリシーが構成されていない場合、.iniファイルの値が使用されます。ここで、または.iniファイルでこのポリシーが構成されていない場合、レジストリキーは除外されません。

包含リスト

ログオフ時に処理されるHKCUハイブ内のレジストリキーのリスト。

例: Software\Adobe。

このポリシーが有効になっている場合、このリストにあるキーのみが処理されます。このポリシーが無効になっている場合、HKCUハイブ全体が処理されます。ここでこのポリシーが構成されていない場合、.iniファイルの値が使用されます。ここで、または.iniファイルでこのポリシーが構成されていない場合、HKCUのすべてが処理されます。

デフォルトの除外リストを有効にする - Profile Management 5.5

ユーザープロファイルに同期されないHKCUハイブ内のレジストリキーのデフォルトリスト。このポリシーを使用して、GPO除外ファイルを手動で入力することなく指定できます。

このポリシーを無効にすると、Profile Management はデフォルトでレジストリキーを除外しません。ここでこのポリシーを構成しない場合、Profile Management は .ini ファイルの値を使用します。ここで、または .ini ファイルでこのポリシーを構成しない場合、Profile Management はデフォルトでレジストリキーを除外しません。

NTUSER.DATのバックアップ

NTUSER.DATの最後に正常だったコピーのバックアップを有効にし、破損がある場合にロールバックします。

ここでこのポリシーを構成しない場合、Profile Management は .ini ファイルの値を使用します。ここで、または .ini ファイルでこのポリシーを構成しない場合、Profile Management は NTUSER.DAT をバックアップしません。

アプリケーションアクセス制御

このポリシーは、ファイル、フォルダー、およびレジストリへのユーザーアクセスを制御します。一般的なユースケースは、関連するユーザーにアプリを表示するかどうかを制御するために、マシンにインストールされているアプリへのユーザーアクセスを制御するルールを適用することです。

アプリのアクセス制御を有効にする。有効にすると、Profile Management は、指定したルールに基づいて、項目（ファイル、フォルダー、レジストリなど）へのユーザーアクセスを制御します。

アプリケーションルールを作成するには、次の2つの方法があります。

- GUIベースのツール – **WEM Tool Hub > アプリケーションアクセス制御用ルールジェネレーター**
- PowerShellツール – Profile Managementインストールパッケージで利用可能

ストリーム配信ユーザープロファイルポリシー設定

このセクションには、Profile Management がストリーム配信ユーザープロファイルを処理する方法を指定するポリシー設定が含まれています。

常にキャッシュ

この設定は、ユーザーのログオン後、Profile Management がストリーム配信ファイルをできるだけ早くキャッシュするかどうかを指定します。ユーザーのログオン後にファイルをキャッシュすると、ネットワーク帯域幅が節約され、ユーザーエクスペリエンスが向上します。

この設定は、**プロファイルストリーミング**設定と組み合わせて使用します。

デフォルトでは、この設定は無効になっており、ユーザーのログオン後、ストリーム配信ファイルはできるだけ早くキャッシュされません。

この設定がここで構成されていない場合、.iniファイルの値が使用されます。

この設定がここでも .ini ファイルでも構成されていない場合、無効になります。

常にキャッシュするサイズ

この設定は、ストリーム配信されるファイルのサイズの下限を MB 単位で指定します。Profile Management は、このサイズ以上のファイルを、ユーザーのログオン後できるだけ早くキャッシュします。

デフォルトでは、値は 0 (ゼロ) に設定されており、プロファイル全体をキャッシュする機能が使用されます。プロファイル全体をキャッシュする機能が有効になっている場合、Profile Management は、ユーザーのログオン後、ユーザーストア内のすべてのプロファイルコンテンツをバックグラウンドタスクとしてフェッチします。

この設定がここで構成されていない場合、.iniファイルの値が使用されます。

この設定がここでも .ini ファイルでも構成されていない場合、無効になります。

プロファイルストリーミング

この設定は、Citrix® ストリーム配信ユーザープロファイル機能を有効または無効にします。有効にすると、プロファイルファイルとフォルダーは、ユーザーがログオン後にアクセスした場合に

のみ、ユーザーストアからローカルコンピューターにフェッチされます。レジストリエントリと保留領域のファイルはすぐにフェッチされます。

デフォルトでは、プロファイルストリーミングは無効になっています。

この設定がここで構成されていない場合、.iniファイルの値が使用されます。

この設定がここでも .ini ファイルでも構成されていない場合、無効になります。

ストリーム配信ユーザープロファイルグループ

この設定は、Windows ユーザーグループに基づいて、OU 内のどのユーザープロファイルをストリーム配信するかを指定します。

有効にすると、指定されたユーザーグループ内のユーザープロファイルのみがストリーミングされます。その他のすべてのユーザープロファイルは通常どおり処理されます。

デフォルトでは、この設定は無効になっており、OU内のすべてのユーザープロファイルは通常どおり処理されます。

この設定がここで構成されていない場合、.iniファイルの値が使用されます。

この設定がここでも.iniファイルでも構成されていない場合、すべてのユーザープロファイルが処理されます。

プロファイルストリーミング除外を有効にする

プロファイルストリーミング除外が有効な場合：

- Profile Managementは、除外リスト内のフォルダーをストリーミングしません
- ユーザーがログオンすると、すべてのフォルダーがユーザーストアからローカルコンピューターに即座にフェッチされます

詳細については、「ユーザープロファイルのストリーム」を参照してください。

ペンディングエリアロックファイルのタイムアウト

この設定は、ストレージサーバーが応答しなくなったときにユーザーストアがロックされたままの場合、ペンディングエリアからユーザーストアにユーザーファイルが書き戻されるまでの日数を指定します。この動作により、ペンディングエリアの肥大化が防止され、ユーザーストアに常に最新のファイルが含まれることが保証されます。

デフォルトでは、この設定は1日（1）に設定されています。

この設定がここで構成されていない場合、.iniファイルの値が使用されます。

この設定がここでも.iniファイルでも構成されていない場合、デフォルト値が使用されます。

ペンディングエリアのプロファイルストリーミングを有効にする

ペンディングエリア内のファイルとフォルダーに対してプロファイルストリーミング機能を有効にできます。

ペンディングエリアは、プロファイルストリーミングが有効になっている間、プロファイルの一貫性を確保するために使用されます。これは、同時セッションで変更されたプロファイルファイルとフォルダーを一時的に保存します。

既定では、このポリシーは無効になっており、ログオン時に保留領域内のすべてのファイルとフォルダーがローカルプロファイルにフェッチされます。このポリシーを有効にすると、保留領域内のファイルは要求されたときにのみローカルプロファイルにフェッチされます。このポリシーをプロファイルストリーミングポリシーと組み合わせて使用すると、同時セッションシナリオで最適なログオンエクスペリエンスを確保できます。

このポリシーは、フォルダーのプロファイルストリーミングを有効にするポリシーが有効になっている場合に、保留領域内のフォルダーに適用されます。

ユーザーパーソナライゼーションレイヤーポリシー設定

Virtual Delivery Agent内でユーザーレイヤーのマウントを有効にするには、構成パラメータを使用して以下を指定します。

- ネットワーク上のどこでユーザーレイヤーにアクセスするか。
- 新しいユーザーレイヤーディスクがどのくらい大きくなるか。

そのため、利用可能なポリシーのリストには、次の2つのポリシーが表示されます。

- ユーザーレイヤーリポジトリパス - 「値」フィールドに「\\サーバー名またはアドレス\フォルダー名」の形式でパスを入力します。
- ユーザーレイヤーサイズGB - デフォルトのユーザーレイヤーサイズである10 GBは、Citrix®が推奨する最小値です。ユーザーレイヤーは、使用されるスペースに応じて設定されたサイズまで拡張されるシンプロビジョニングディスクです。ユーザーレイヤーのサイズが小さくなることはありません。

> **注：**

> ユーザーレイヤーサイズを増やすと、新しいユーザーレイヤーに影響を与え、既存のユーザーレイヤーを拡張します。レイヤーサイズを減らすと、新しいユーザーレイヤーにのみ影響します。既存のユーザーレイヤーのサイズが小さくなることはありません。

> 詳細については、「ユーザーパーソナライゼーションレイヤー」を参照してください。

Virtual Delivery Agent ポリシー設定

Virtual Delivery Agent (VDA) セクションには、VDA とサイトのコントローラー間の通信を制御するポリシー設定が含まれています。

重要: 自動更新機能を使用しない場合、VDA は Delivery Controller™ に登録するために、これらの設定によって提供される情報を必要とします。この情報は登録に必要であるため、VDA のインストール中にこの情報を提供しない限り、グループポリシーエディターを使用して以下の設定を構成する必要があります。

- コントローラー登録 IPv6 ネットマスク
- コントローラー登録ポート
- コントローラー SID
- コントローラー
- IPv6 コントローラー登録のみを使用
- サイト GUID

コントローラー登録 IPv6 ネットマスク

このポリシー設定により、管理者は VDA を優先サブネットのみに制限できます（グローバル IP が登録されている場合でも）。この設定は、VDA が登録する IPv6 アドレスとネットワークを指定します。VDA は、指定されたネットマスクに一致する最初のアドレスにのみ登録します。この設定は、「IPv6 コントローラー登録のみを使用」ポリシー設定が有効になっている場合にのみ有効です。

デフォルトでは、この設定は空白です。

コントローラー登録ポート

この設定は、**コントローラーの自動更新を有効にする** 設定が無効になっている場合にのみ使用してください。

この設定は、レジストリベースの登録を使用する際に、VDA がコントローラーに登録するために使用する TCP/IP ポート番号を指定します。

デフォルトでは、ポート番号は80に設定されています。

コントローラーSID

この設定は、**コントローラーの自動更新を有効にする**設定が無効になっている場合にのみ使用してください。

この設定は、VDAがレジストリベースの登録を使用する際にコントローラーに登録するために使用する、スペース区切りのコントローラーセキュリティ識別子（SID）のリストを指定します。この設定はオプションであり、登録に使用されるコントローラーのリストを制限するために**コントローラー**設定と組み合わせて使用される場合があります。

デフォルトでは、この設定は空白です。

コントローラー

この設定は、**コントローラーの自動更新を有効にする**設定が無効になっている場合にのみ使用してください。

この設定は、VDAがレジストリベースの登録を使用する際にコントローラーに登録するために使用する、スペース区切りのコントローラー完全修飾ドメイン名（FQDN）のリストを指定します。この設定はオプションであり、**コントローラーSID**設定と組み合わせて使用される場合があります。

デフォルトでは、この設定は空白です。

コントローラーの自動更新を有効にする

この設定により、VDAはインストール後にコントローラーに自動的に登録できるようになります。

VDAが登録されると、登録先のコントローラーは現在のコントローラーFQDNとSIDのリストをVDAに送信します。VDAはこのリストを永続ストレージに書き込みます。各コントローラーは、90分ごとにサイトデータベースをチェックしてコントローラー情報を確認します。以下のいずれかの状況が発生した場合、コントローラーは登録済みのVDAに更新されたリストを送信します。

- 前回のチェック以降にコントローラーが追加または削除された場合
- ポリシーの変更が発生した場合

VDAは、受信した最新のリストにあるすべてのコントローラーからの接続を受け入れます。

デフォルトでは、この設定は有効になっています。

IPv6コントローラー登録のみを使用

この設定は、VDAがControllerに登録するために使用するアドレス形式を制御します。

- 有効にすると、VDAはマシンのIPv6アドレスを使用してControllerに登録します。VDAがControllerと通信する場合、次のアドレス順序を使用します: グローバルIPアドレス、ユニークローカルアドレス (ULA)、リンクローカルアドレス (他のIPv6アドレスが利用できない場合)。
- 無効にすると、VDAはマシンのIPv4アドレスを使用してControllerに登録し、通信します。

デフォルトでは、この設定は無効になっています。

サイトGUID

この設定は、**コントローラーの自動更新を有効にする**設定が無効になっている場合にのみ使用してください。

この設定は、Active Directoryベースの登録を使用する際に、VDAがControllerに登録するために使用するサイトのグローバル一意識別子 (GUID) を指定します。

デフォルトでは、この設定は空白です。

HDX™ 3D Pro ポリシー設定

HDX 3D Proセクションには、ユーザー向けの画質構成ツールを有効化および構成するためのポリシー設定が含まれています。このツールを使用すると、ユーザーは利用可能な帯域幅の使用を最適化できます。この最適化のために、画質と応答性のバランスがリアルタイムで調整されます。

ロスレスを有効にする

この設定は、ユーザーが画質構成ツールを使用してロスレス圧縮を有効または無効にできるかどうかを指定します。デフォルトでは、ユーザーにロスレス圧縮を有効にするオプションは提供されません。

ユーザーがロスレス圧縮を有効にしたとします。この場合、画質は画質構成ツールで利用可能な最大値に自動的に設定されます。デフォルトでは、ユーザーデバイスとホストコンピューターの機能に応じて、GPUベースまたはCPUベースの圧縮のいずれかを使用できます。

HDX 3D Pro 品質設定

この設定は、画質構成ツールでユーザーが利用できる最小値と最大値を指定します。これらの値を使用すると、画質構成ツールで画質調整の範囲を定義できます。

画質の値は0から100（両端を含む）の間で指定します。最大値は最小値以上である必要があります。

監視ポリシー設定

「**監視**」セクションには、プロセス、リソース監視、およびアプリケーション障害監視のポリシー設定が含まれています。

これらのポリシーのスコープは、以下に基づいて定義できます。

- サイト
- デリバリーグループ
- デリバリーグループの種類
- 組織単位
- タグ

プロセスおよびリソース監視のポリシー

CPU、メモリ、およびプロセスの各データポイントはVDAから収集され、監視データベースに保存されます。VDAからデータポイントを送信するとネットワーク帯域幅を消費し、それらを保存すると監視データベースの相当なスペースを消費します。特定のスコープ（たとえば、特定のデリバリーグループまたは組織単位）に対して、リソースデータまたはプロセスデータ、あるいはその両方を監視したくない場合を考慮してください。この場合、ポリシーを無効にすることをお勧めします。

プロセス監視を有効にする

この設定を有効にすると、VDAがインストールされているマシンで実行されているプロセスを監視できます。CPU使用率やメモリ使用量などの統計情報は、監視サービスに送信されます。これらの統計情報は、Directorでのリアルタイム通知および履歴レポートに使用されます。

この設定のデフォルトは無効です。

リソース監視を有効にする

この設定を有効にすると、VDAがインストールされているマシンで重要なパフォーマンスカウンターを監視できます。統計情報（CPU使用率、メモリ使用量、IOPS、ディスク待機時間データなど）は監視サービスに送信されます。これらの統計情報は、Directorでのリアルタイム通知および履歴レポートに使用されます。

この設定のデフォルトは有効です。

スケーラビリティ

CPUおよびメモリデータは、各VDAから5分間隔でデータベースにプッシュされます。プロセスデータ（有効な場合）は10分間隔でデータベースにプッシュされます。IOPSおよびディスク待機時間データは1時間間隔でデータベースにプッシュされます。

CPUとメモリデータ

CPUとメモリデータは、デフォルトで**有効**です。データ保持期間の値は次のとおりです (Platinumライセンス):

データ粒度	日数
5分データ	1日
10分データ	7日
時間データ	30日
日次データ	90日

IOPSとディスク待機時間データ

IOPSとディスク待機時間データは、デフォルトで**有効**です。データ保持期間の値は次のとおりです (Platinumライセンス):

データ粒度	日数
時間データ	3日間
日次データ	90日間

データ保持設定では、1つのVDAに対して1年間、以下を保存するために約276 KBのディスク容量が必要です。

- CPU
- メモリ
- IOPS
- ディスク遅延データ

マシン数	必要なストレージ容量（概算）
1	276 KB
1K	270 MB
40K	10.6 GB

プロセスデータ

プロセスデータはデフォルトで**無効**です。必要に応じて、一部のマシンでプロセスデータを有効にすることをお勧めします。プロセスデータのデフォルトのデータ保持設定は次のとおりです。

データ粒度	日数
10分データ	1日
1時間データ	7日

プロセスデータがデフォルトの保持設定で有効になっている場合、プロセスデータは1年間でVDAあたり約1.5 MB、ターミナルサービスVDA (TS VDA) あたり3 MBを消費します。

マシン数	必要なストレージの目安 VDA	必要なストレージの目安 TS VDA
1	1.5 MB	3 MB
1K	1.5 GB	3 GB

> **注：**
>
> 以前に提示された数値には、インデックス領域は含まれていません。また、すべての計算は概算であり、展開によって異なります。

オプションの構成

必要に応じて、デフォルトの保持設定を変更できます。ただし、この構成は追加のストレージを消費します。以下の設定を有効にすることで、プロセス使用率データの精度を高めることができます。有効にできる構成は次のとおりです。

ENABLEMINUTELEVELGRANULARITYPROCESSUTILIZATION

ENABLEDAYLEVELGRANULARITYPROCESSUTILIZATION

これらの構成は、監視PowerShellコマンドレットから有効にできます: Set-MonitorConfiguration

アプリケーション障害監視のポリシー

デフォルトでは、**アプリケーション障害**タブには、マルチセッションOS VDAからのアプリケーション障害のみが表示されます。アプリケーション障害監視の設定は、以下の監視ポリシーで変更できます。

アプリケーション障害の監視を有効にする

この設定を使用して、アプリケーション障害監視を構成し、アプリケーションエラーまたは障害（クラッシュおよび未処理の例外）、あるいはその両方を監視します。 **値**を**None**に設定すると、アプリケーション障害監視が無効になります。 この設定のデフォルトは「アプリケーション障害のみ」です。

シングルセッションOS VDAでのアプリケーション障害の監視を有効にする

デフォルトでは、マルチセッションOS VDAでホストされているアプリケーションからの障害のみが監視されます。シングルセッションOS VDAを監視するには、ポリシーを**Allowed**に設定します。 この設定のデフォルトは**Prohibited**です。

障害監視から除外されるアプリケーションのリスト

障害監視の対象としないアプリケーションのリストを指定します。 デフォルトでは、このリストは空です。

Analytics 用データ収集のポリシー

ANALYTICS 用 VDA データ収集

このポリシーを使用して、パフォーマンスおよびセキュリティ分析のために、Monitor サービスが VDA のパフォーマンスおよびセキュリティ関連のメトリックを収集するかどうかを有効または無効にします。デフォルトでは、このポリシーは**許可**されています。VDA からのデータ収集を停止するには、ポリシーを**禁止**に設定します。

セキュリティ監視のためのクリップボード場所メタデータ収集

このポリシーを使用して、セキュリティ監視、監査、およびコンプライアンスのために、Broker サービスによるクリップボード場所メタデータ収集を有効または無効にします。デフォルトでは、このポリシーは**有効**です。VDA からのデータ収集を停止するには、ポリシーを**無効**に設定します。

パフォーマンス監視のための診断データ収集

このポリシーを使用して、監視サービスがセッション情報、UPM/EUEM サービスの状態、Microsoft Teams の最適化、接続プロトコルなどの診断データを収集できるようにします。デフォルトでは、このポリシーは**有効**です。VDA からのデータ収集を停止するには、ポリシーを**無効**に設定します。

ストレージ計画のヒント

グループポリシー。リソースデータまたはプロセスデータの監視に関心がない場合は、グループポリシーを使用して、いずれかまたは両方をオフにすることができます。詳しくは、「ポリシーの作成」の**「グループポリシー」**セクションを参照してください。

データグルーミング。デフォルトのデータ保持設定を変更して、データを早期にグルーミングし、ストレージスペースを解放できます。グルーミング設定について詳しくは、「API を使用したデータアクセス」の「データの粒度と保持」を参照してください。

仮想IPポリシー設定

> **重要:**
>
> - Windows 10 Enterprise multi-session は Remote Desktop IP Virtualization (Virtual IP) をサポートしていません。また、Windows 10 Enterprise multi-session では Remote Desktop IP Virtualization または仮想ループバックをサポートしていません。
> - リモートデスクトップIP仮想化 (仮想IP) は、クラウドホスト型マシンではサポートされていません。詳細については、Microsoftドキュメントを参照してください。

仮想IPセクションには、セッションが独自の仮想ループバックアドレスを持つかどうかを制御するポリシー設定が含まれています。

仮想IPループバックのサポート

この設定が有効な場合、各セッションは独自の仮想ループバックアドレスを持ちます。無効な場合、セッションは個別のループバックアドレスを持ちません。

デフォルトでは、この設定は無効になっています。

仮想IP仮想ループバックプログラムリスト

この設定は、仮想ループバックアドレスを使用できるアプリケーション実行可能ファイルを指定します。プログラムをリストに追加する際は、実行可能ファイル名のみを指定してください。完全なパスを指定する必要はありません。

デフォルトでは、実行可能ファイルは指定されていません。

レジストリを使用してCOMポートおよびLPTポートリダイレクト設定を構成する

VDAバージョン7.0から7.8では、**COMポートおよびLPTポート**設定は、レジストリを使用してのみ構成できます。VDAバージョン7.0より前、およびVDAバージョン7.9以降では、これらの設定はWeb Studioで構成できます。詳しくは、「ポートリダイレクトポリシー設定」および「帯域幅ポリシー設定」を参照してください。

COMポートおよびLPTポートリダイレクトのポリシー設定は、VDAイメージまたはマシン上のHKLM\Software\Citrix\GroupPolicy\Defaults\Deprecatedにあります。

COMポートおよびLPTポートリダイレクトを有効にするには、次のようにREG_DWORD型の新しいレジストリキーを追加します。

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

レジストリキー	説明	許可される値
AllowComPortRedirection	COMポートリダイレクトを許可または禁止する	1 (許可) または 0 (禁止)
LimitComBw	COMポートリダイレクトチャネルの帯域幅制限	数値
LimitComBWPercent	COMポートリダイレクトチャネルの帯域幅制限（セッションの総帯域幅に対する割合）	0から100までの数値
AutoConnectClientComPorts	ユーザーデバイスからCOMポートを自動的に接続する	1 (許可) または 0 (禁止)
AllowLptPortRedirection	LPTポートリダイレクトを許可または禁止する	1 (許可) または 0 (禁止)
LimitLptBw	LPTポートリダイレクトチャネルの帯域幅制限	数値
LimitLptBwPercent	LPTポートリダイレクトチャネルの帯域幅制限（セッション全体の帯域幅に対する割合）	0から100までの数値
AutoConnectClientLptPorts	ユーザーデバイスからLPTポートを自動的に接続する	1 (許可) または 0 (禁止)

これらの設定を構成した後、マシンカタログを変更して、新しいマスターイメージまたは更新された物理マシンを使用するようにします。デスクトップは、ユーザーが次回ログオフしたときに新しい設定で更新されます。

Configuration Manager 2012用コネクタのポリシー設定

Configuration Manager 2012用コネクタセクションには、Citrix Connector 7.5エージェントを構成するためのポリシー設定が含まれています。

> **重要:**

> 警告、ログオフ、および再起動メッセージポリシーは、手動で管理されているか、Provisioning Servicesによって管理されているマルチセッションOSマシンカタログへの展開にのみ適用されます。これらのマシンカタログの場合、保留中のアプリケーションのインストールまたはソフトウェアアップデートがある場合に、コネクタサービスはユーザーに警告します。

> MCSによって管理されるカタログの場合、Web Studioを使用してユーザーに通知します。手動で管理されるシングルセッションOSカタログの場合、Configuration Managerを使用してユーザーに通知します。Provisioning Servicesによって管理されるシングルセッションOSカタログの場合、Provisioning Servicesを使用してユーザーに通知します。

警告頻度間隔

この設定は、ユーザーへの警告メッセージの表示間隔を定義します。

間隔はddd.hh:mm:ssの形式で設定されます。ここで、:

- dddは日数で、オプションのパラメーターであり、0〜999の範囲です。
- hhは時間で、0〜23の範囲です。
- mmは分で、0〜59の範囲です。
- ssは秒で、0〜59の範囲です。

デフォルトでは、間隔設定は1時間（01:00:00）です。

警告メッセージボックスの本文テキスト

この設定には、今後のソフトウェアアップデートまたはログオフを必要とするメンテナンスをユーザーに通知するメッセージの編集可能なテキストが含まれています。

デフォルトでは、メッセージは次のとおりです: {TIMESTAMP} 作業を保存してください。サーバーは{TIMELEFT}後にメンテナンスのためオフラインになります。

警告メッセージボックスのタイトル

この設定には、ユーザーへの警告メッセージのタイトルバーの編集可能なテキストが含まれています。

デフォルトでは、タイトルは「Upcoming Maintenance」です。

警告期間

この設定は、メンテナンスのどれくらい前に警告メッセージが最初に表示されるかを定義します。

時刻はddd.hh:mm:ssの形式で設定されます。ここで、:

- dddは日数で、オプションのパラメーターであり、範囲は0〜999です。
- hhは時間で、範囲は0〜23です。
- mmは分で、範囲は0〜59です。
- ssは秒で、範囲は0〜59です。

デフォルトでは、設定は16時間（16:00:00）であり、最初の警告メッセージがメンテナンスの約16時間前に表示されることを示します。

最終強制ログオフメッセージボックスの本文

この設定には、強制ログオフが開始されたことをユーザーに警告するメッセージの編集可能なテキストが含まれています。

デフォルトでは、メッセージは「The server is currently going offline for maintenance」です。

最終強制ログオフメッセージボックスのタイトル

この設定には、最終的な強制ログオフメッセージのタイトルバーの編集可能なテキストが含まれています。

デフォルトでは、タイトルは「ITスタッフからの通知」です。

強制ログオフ猶予期間

この設定は、ユーザーにログオフを通知してから、保留中のメンテナンスを処理するための強制ログオフが実行されるまでの期間を定義します。

時間はddd.hh:mm:ssの形式で設定され、ここで:

- dddは日数で、オプションのパラメーターであり、0〜999の範囲です。
- hhは時間で、0〜23の範囲です。
- mmは分で、0〜59の範囲です。
- ssは秒で、0〜59の範囲です。

デフォルトでは、強制ログオフ猶予期間の設定は5分（00:05:00）です。

強制ログオフメッセージボックスの本文

この設定には、強制ログオフが開始される前に、作業を保存してログオフするようユーザーに伝えるメッセージの編集可能なテキストが含まれています。

デフォルトでは、メッセージには次の内容が含まれています: {TIMESTAMP} 作業を保存してログオフしてください。サーバーは{TIMELEFT}後にメンテナンスのためオフラインになります。

強制ログオフメッセージボックスのタイトル

この設定には、強制ログオフメッセージのタイトルバーの編集可能なテキストが含まれています。

既定では、タイトルは「Notification From IT Staff」です。

イメージ管理モード

Connectorエージェントは、Provisioning ServicesまたはMCSによって管理されているマシンのクローン上で実行されているかどうかを自動的に検出します。エージェントは、イメージ管理されたクローンでのConfiguration Managerの更新をブロックし、カタログのマスターイメージに更新を自動的にインストールします。

マスターイメージが更新された後、WEb Studioを使用してMCSカタログクローンの再起動をオーケストレーションします。Connector Agentは、Configuration Managerのメンテナンスウィンドウ中にPVSカタログクローンの再起動を自動的にオーケストレーションします。この動作を上書きして、Configuration Managerによってカタログクローンにソフトウェアがインストールされるようにするには、をに変更します。

再起動メッセージボックスの本文

この設定には、サーバーが再起動されるときにユーザーに通知するメッセージの編集可能なテキストが含まれています。

既定では、メッセージは「The server is currently going offline for maintenance.」です。

エージェントタスクが実行される定期的な時間間隔

この設定は、Citrix Connector™エージェントタスクが実行される頻度を決定します。

時間はddd.hh:mm:ssの形式で設定されます。ここで、:

- dddは日数で、オプションのパラメーターであり、0〜999の範囲です。
- hhは時間で、0〜23の範囲です。
- mmは分で、0〜59の範囲です。
- ssは秒で、0〜59の範囲です。

既定では、定期的な時間間隔の設定は5分（00:05:00）です。

ポリシーの変更

次の表に、Citrix Virtual Apps and Desktops™ 7 2402でのポリシーの更新（追加、削除、名前の変更、デフォルト状態の変更など）を示します。

ポリシー設定	変更点
クライアントプリンターポリシー設定 > 保持および復元されたクライアントプリンター	2402で非推奨

注：

アップグレードする前に、すべての非推奨設定を削除してください。非推奨設定が使用されたままになっている場合、アップグレードはエラーで失敗する可能性があります。

管理

Citrix Virtual Apps and Desktops™ サイトの管理には、さまざまな項目とタスクが含まれます。

ライセンス

サイトを作成するときは、Citrix License Server への有効な接続が必要です。後で、Studio から、ライセンスの追加、ライセンスの種類やモデルの変更、ライセンス管理者の管理など、いくつかのライセンス関連タスクを実行できます。Studio から License Administration Console にアクセスすることもできます。

アプリケーション

デリバリーグループ、およびオプションでアプリケーショングループ内のアプリケーションを管理します。

ゾーン

地理的に分散した展開では、ゾーンを使用してアプリケーションとデスクトップをエンドユーザーの近くに配置し、パフォーマンスを向上させることができます。サイトをインストールして構成すると、すべてのコントローラー、マシンカタログ、およびホスト接続は1つのプライマリゾーンに配置されます。後で、Studio を使用して、これらの項目を含むサテライトゾーンを作成できます。サイトに複数のゾーンがある場合、新しく作成されたマシンカタログ、ホスト接続、または追加されたコントローラーをどのゾーンに配置するかを指定できます。ゾーン間で項目を移動することもできます。

接続とリソース

アプリケーションとデスクトップをユーザーに提供するマシンをホストするためにハイパーバイザーまたはその他のサービスを使用している場合、サイトを作成するときに、そのハイパーバイザーまたはその他のサービスへの最初の接続を作成します。その接続のストレージとネットワークの詳細は、そのリソースを構成します。後で、その接続とそのリソースを変更したり、さらに接続を作成したりできます。構成済みの接続を使用するマシンを管理することもできます。

ローカルホストキャッシュ

ローカルホストキャッシュにより、Delivery Controller™ とサイトデータベース間の接続が失敗した場合でも、サイトでの接続ブローカー操作を続行できます。

仮想IPと仮想ループバック

Microsoft の仮想IPアドレス機能は、公開アプリケーションにセッションごとに一意の動的に割り当てられたIPアドレスを提供します。Citrix の仮想ループバック機能を使用すると、localhost との通信に依存するアプリケーションを、localhost 範囲内の一意の仮想ループバックアドレスを使用するように構成できます。

デリバリーコントローラー

この記事では、サイトへのControllerの追加と削除に関する考慮事項と手順について説明します。また、Controllerを別のゾーンまたはサイトに移動する方法、およびVDAを別のサイトに移動する方法についても説明します。

ControllerへのVDA登録

VDAがアプリケーションとデスクトップの配信を支援するには、Controllerに登録（通信を確立）する必要があります。Controllerのアドレスはいくつかの方法で指定でき、それについてはこの記事で説明します。サイトでControllerが追加、移動、削除される際に、VDAが最新の情報を持っていることが重要です。

セッション

セッションアクティビティを維持することは、最高のユーザーエクスペリエンスを提供するために不可欠です。いくつかの機能により、セッションの信頼性を最適化し、不便さ、ダウンタイム、生産性の損失を軽減できます。

- セッションの信頼性
- クライアントの自動再接続
- ICA®キープアライブ
- ワークスペースコントロール
- セッションローミング

Studioでの検索の使用

Studioでマシン、セッション、マシンカタログ、アプリケーション、またはデリバリーグループに関する情報を表示したい場合は、柔軟な検索機能を使用します。

タグ

タグを使用して、マシン、アプリケーション、グループ、ポリシーなどのアイテムを識別します。その後、特定のタグを持つアイテムに適用されるように特定の操作を調整できます。

IPv4/IPv6

Citrix Virtual Apps and Desktops は、純粋な IPv4、純粋な IPv6、および IPv4 と IPv6 の重複するネットワークを使用するデュアルスタック展開をサポートしています。この記事では、これらの展開について説明し、図解します。また、IPv4 または IPv6 の使用を制御する Citrix ポリシー設定についても説明します。

ユーザープロファイル

デフォルトでは、VDA をインストールすると Citrix Profile Management が自動的にインストールされます。このプロファイルソリューションを使用する場合は、一般的な情報についてこの記事を確認してください。詳細については、Profile Management のドキュメントを参照してください。

Citrix Diagnostic Facility (CDF) トレースの収集

CDFControl ユーティリティは、さまざまな Citrix トレースプロバイダーから表示される Citrix Diagnostic Facility (CDF) トレースメッセージをキャプチャするためのイベントトレースコントローラーまたはコンシューマーです。これは、複雑な Citrix 関連の問題のトラブルシューティング、フィルターサポートの解析、およびパフォーマンスデータの収集のために作成されています。

シトリックス インサイト サービス

Citrix Insight Services (CIS) は、計測、テレメトリ、およびビジネスインサイト生成のための Citrix プラットフォームです。

シトリックス スカウト

Citrix Scout は、診断情報を収集し、ヘルスチェックを実行します。結果は、Citrix Virtual Apps and Desktops 展開におけるプロアクティブなメンテナンスに利用できます。Citrix は、Citrix Insight Services を通じて、診断コレクションの包括的な自動分析を提供します。また、Scout を使用して、単独で、または Citrix サポートのガイダンスを受けて問題をトラブルシューティングすることもできます。

アプリケーション

> **注：**

> Citrix Virtual Apps and Desktops™展開は、Web Studio（Webベース）とCitrix Studio（Windowsベース）の2つの管理コンソールを使用して管理できます。この記事ではWeb

> Studioのみを扱います。Citrix Studioについては、Citrix Virtual Apps and Desktops 7 2212以前の同等の記事を参照してください。

はじめに

展開でデリバリーグループのみを使用している場合（アプリケーショングループは使用しない場合）、アプリケーションはデリバリーグループに追加します。アプリケーショングループも使用している場合は、通常、代わりにアプリケーショングループにアプリケーションを追加します。このガイダンスにより、管理が容易になります。アプリケーションは常に少なくとも1つのデリバリーグループまたはアプリケーショングループに属している必要があります。

アプリケーションの追加ウィザードでは、1つ以上のデリバリーグループ、または1つ以上のアプリケーショングループを選択できますが、両方は選択できません。後でアプリケーションのグループ関連付けを変更することはできますが（たとえば、アプリケーショングループからデリバリーグループにアプリケーションを移動するなど）、ベストプラクティスでは、そのような複雑さを追加することは推奨されません。アプリケーションは1種類のグループに保持してください。

アプリケーションを複数のグループに関連付ける場合、それらのすべてのグループでアプリケーションを表示するのに十分な権限がないと、可視性の問題が発生する可能性があります。そのような場合は、より高い権限を持つ管理者に相談するか、アプリケーションが関連付けられているすべてのグループを含むようにスコープを拡張してください。

同じ名前の2つのアプリケーション（異なるグループからのものなど）を同じユーザーに公開する場合、Web Studioで `Application name (for user)` プロパティを変更します。そうしないと、ユーザーはCitrix Workspace™アプリで重複する名前を目にすることになります。

アプリケーションのプロパティ（設定）は、追加時または後で変更できます。アプリケーションが配置されているアプリケーションフォルダーも、アプリケーションの追加時または後で変更できます。

詳細については、以下を参照してください。

- デリバリーグループの作成
- アプリケーショングループの作成
- タグ

アプリケーションの追加

デリバリーグループまたはアプリケーショングループを作成するときにアプリケーションを追加できます。これらの手順については、デリバリーグループの作成およびアプリケーショングループ

の作成で詳しく説明されています。次の手順では、グループ作成後にアプリケーションを追加する方法について説明します。

知っておくと良いこと:

- Remote PC Accessデリバリーグループにアプリケーションを追加することはできません。
- アプリケーションの追加ウィザードを使用して、デリバリーグループまたはアプリケーショングループからアプリケーションを削除することはできません。これは別の操作です。

1つ以上のアプリケーションを追加するには：

1. 左ペインで**アプリケーション**を選択し、アクションバーで**アプリケーションの追加**を選択します。
2. アプリケーションの追加ウィザードが**はじめに**ページとともに起動します。このページは、今後のウィザードの起動時に表示しないように設定できます。
3. ウィザードは、**グループ**、**アプリケーション**、**概要**の各ページを案内します。各ページの作業が完了したら、**概要**ページに到達するまで**次へ**をクリックします。

単一のデリバリーグループまたはアプリケーショングループにアプリケーションを追加する場合の、手順1の代替方法：

- **1つのデリバリーグループにのみアプリケーションを追加するには：** 手順1で、Web Studioの左ペインで**デリバリーグループ**を選択し、中央ペインでデリバリーグループを選択してから、アクションバーで**アプリケーションの追加**を選択します。ウィザードには**グループ**ページが表示されません。
- **1つのアプリケーショングループにのみアプリケーションを追加するには：** 手順1で、Web Studioの左ペインで**アプリケーション**を選択し、中央ペインでアプリケーショングループを選択してから、アクションバーでアプリケーショングループ名の下にある**アプリケーションの追加**エントリを選択します。ウィザードには**グループ**ページが表示されません。

グループページ

このページには、サイト内のすべてのデリバリーグループが一覧表示されます。アプリケーショングループも作成している場合は、アプリケーショングループとデリバリーグループが一覧表示されます。どちらかのグループを選択できますが、両方のグループを選択することはできません。つまり、アプリケーショングループとデリバリーグループに同時にアプリケーションを追加することはできません。通常、アプリケーショングループを使用している場合は、デリバリーグループではなくアプリケーショングループにアプリケーションを追加します。

アプリケーションを追加するときは、少なくとも1つのデリバリーグループ（または、利用可能な場合はアプリケーショングループ）の横にあるチェックボックスをオンにします。すべてのアプリケーションは、常に少なくとも1つのグループに関連付けられている必要があります。

アプリケーションページ

追加をクリックして、アプリケーションソースを表示します。

- **スタートメニューから：** 選択したデリバリーグループ内のマシンで検出されたアプリケーション。このソースを選択すると、検出されたアプリケーションのリストを含む新しいページが起動します。追加するアプリケーションのチェックボックスをオンにして、**OK**をクリックします。

  このソースは、(1)関連付けられたデリバリーグループがないアプリケーショングループを選択した場合、(2)関連付けられたデリバリーグループにマシンが含まれていないアプリケーショングループを選択した場合、または(3)マシンが含まれていないデリバリーグループを選択した場合は、選択できません。
- **手動：** デリバリーグループ内のVDAまたはネットワーク上の別の場所にあるアプリケーション。このソースを選択すると、新しいページが開き、次の方法で追加するアプリケーションを指定できます。
  - 実行可能ファイルへのパス、作業ディレクトリ、オプションのコマンドライン引数、および管理者とユーザーの表示名を入力します。
  - デリバリーグループ内のVDAからアプリケーションを選択します。これを行うには、**参照**をクリックし、VDAにアクセスするための資格情報を入力し、VDAに接続されるまで待機してから、VDAからアプリケーションを選択します。選択したアプリケーションのプロパティが、ページのフィールドに自動的に入力されます。
- **既存:** 以前サイトに追加されたアプリケーション。このソースを選択すると、検出されたアプリケーションのリストを含む新しいページが起動します。追加するアプリケーションのチェックボックスを選択し、**OK**をクリックします。

  サイトにアプリケーションがない場合、このソースは選択できません。
- **アプリケーションパッケージ:** App-V、MSIX、MSIX app attach、またはFlexAppアプリケーションパッケージ内のアプリケーション。このソースを選択すると、**パッケージからのアプリケーションの追加**ページが起動します。アプリケーションパッケージソースを選択し、表示された結果から追加するアプリケーションを選択して、**OK**を選択します。詳しくは、「Appパッケージの展開と配信」を参照してください。

- **アプリケーショングループ**: アプリケーショングループ。このソースを選択すると、アプリケーショングループのリストを含む新しいページが起動します。（表示には各グループ内のアプリケーションもリストされますが、個々のアプリケーションではなくグループのみを選択できます。）選択したグループ内の現在および将来のすべてのアプリケーションが追加されます。追加するアプリケーショングループのチェックボックスを選択し、**OK**をクリックします。

  このソースは、(1) アプリケーショングループがない場合、または (2) 選択したデリバリーグループがアプリケーショングループをサポートしていない場合（たとえば、静的に割り当てられたマシンを持つデリバリーグループ）には選択できません。

表に示されているように、**追加**リストの一部のソースは、そのタイプの有効なソースがない場合、選択できません。互換性のないソース（たとえば、アプリケーショングループにアプリケーショングループを追加できないなど）はリストに含まれません。選択したグループに既に追加されているアプリケーションは選択できません。

このページまたは後で、アプリケーションのプロパティ（設定）を変更できます。

デフォルトでは、追加されたアプリケーションは`Applications`という名前のアプリケーションフォルダーに配置されます。このページまたは後で、アプリケーションを変更できます。アプリケーションを追加しようとして、同じ名前のアプリケーションが同じフォルダーに存在する場合、追加しようとしているアプリケーションの名前を変更するよう求められます。提示された新しい名前を受け入れるか、拒否してアプリケーションの名前を変更するか、別のフォルダーを選択できます。たとえば、**Applications**フォルダーに`app`が既に存在し、そのフォルダーに`app`という名前の別のアプリケーションを追加しようとすると、新しい名前`app_1`が提示されます。

概要ページ

10個以下のアプリケーションを追加する場合、その名前は**追加するアプリケーション**にリストされます。10個を超えるアプリケーションを追加する場合、合計数が指定されます。

概要情報を確認し、**「完了」**をクリックします。

アプリケーションのグループ関連付けを変更する

アプリケーションを追加した後、そのアプリケーションが関連付けられているデリバリーグループとアプリケーショングループを変更できます。

アプリケーションを別のグループにドラッグできます。これは、アクションバーのコマンドを使用する代替手段です。

アプリケーションが複数のデリバリーグループまたはアプリケーショングループに関連付けられている場合、グループの優先順位を使用して、複数のグループがアプリケーションを検索するためにチェックされる順序を指定できます。デフォルトでは、すべてのグループの優先順位は0（最高）です。同じ優先順位のグループは負荷分散されます。

アプリケーションは、アプリケーションを配信できる共有（プライベートではない）マシンを含むデリバリーグループに関連付けることができます。また、共有マシンを含むデリバリーグループがデスクトップのみを配信する場合でも、(1) デリバリーグループに共有マシンが含まれており、XenDesktop 7.xバージョン7.9より前に作成された場合、および (2) `Edit delivery group` 権限がある場合は、そのデリバリーグループを選択できます。プロパティダイアログがコミットされると、デリバリーグループの種類は自動的に `desktops and applications` に変換されます。

1. Web Studioにサインインし、左ペインで**Applications**を選択し、アプリケーションを選択します。
2. アクションバーで**「プロパティ」**を選択します。
3. **「グループ」**ページを選択します。
   - グループを追加するには、**「追加」をクリックし、「アプリケーショングループ」または「デリバリーグループ」を選択します。（アプリケーショングループを作成していない場合、唯一の項目は**「デリバリーグループ」**です。）次に、1つ以上の利用可能なグループを選択します。アプリケーションと互換性のないグループ、またはすでにアプリケーションに関連付けられているグループは選択できません。
   - グループを削除するには、1つ以上のグループを選択し、**「削除」**をクリックします。グループの関連付けを削除した結果、アプリケーションがどのグループとも関連付けられなくなる場合、アプリケーションが削除されることを警告されます。
   - グループの優先度を変更するには、グループを選択し、**「優先度の編集」をクリックします。優先度値を選択し、**「OK」**をクリックします。
4. 完了したら、**「適用」をクリックして変更を適用し、ウィンドウを開いたままにするか、**「OK」**をクリックして変更を適用し、ウィンドウを閉じます。

アプリケーションの複製、有効化または無効化、名前の変更、または削除

次のアクションが利用可能です。

- **複製：** 異なるパラメーターまたはプロパティを持つ別のバージョンを作成するために、アプリケーションを複製したい場合があります。アプリケーションを複製すると、一意のサフィックスで自動的に名前が変更され、元のアプリケーションの隣に配置されます。また、アプリケー

ションを複製してから、別のグループに追加したい場合もあります。（複製後、アプリケーションを移動する最も簡単な方法はドラッグすることです。）

- **有効化または無効化：** アプリケーションの有効化と無効化は、デリバリーグループまたはアプリケーショングループの有効化と無効化とは異なるアクションです。
- **名前の変更：** 一度に1つのアプリケーションのみ名前を変更できます。アプリケーションの名前を変更しようとして、同じ名前のアプリケーションが同じフォルダーまたはグループに存在する場合、別の名前を指定するように求められます。
- **削除：** アプリケーションを削除すると、関連付けられていたデリバリーグループおよびアプリケーショングループから削除されますが、元々アプリケーションを追加するために使用されたソースからは削除されません。アプリケーションの削除は、デリバリーグループまたはアプリケーショングループから削除するのとは異なるアクションです。

アプリケーションを複製、有効化、無効化、名前変更、または削除するには：

1. 左ペインで**「アプリケーション」**を選択します。
2. 中央ペインで1つ以上のアプリケーションを選択し、アクションバーで適切なタスクを選択します。
3. プロンプトが表示されたら、アクションを確認します。

デリバリーグループからアプリケーションを削除する

アプリケーションは、少なくとも1つのデリバリーグループまたはアプリケーショングループに関連付けられている（属している）必要があります。アプリケーションをデリバリーグループから削除しようとしたときに、そのアプリケーションがどのデリバリーグループまたはアプリケーショングループとも関連付けがなくなる場合、続行するとアプリケーションが削除されるという通知が表示されます。その場合、そのアプリケーションを配信したい場合は、有効なソースから再度追加する必要があります。

1. 左側のペインで、 を選択します。
2. デリバリーグループを選択します。中央下のペインの タブで、削除するアプリケーションを選択します。
3. アクションバーから を選択します。
4. 削除を確認します。

アプリケーショングループからアプリケーションを削除する

アプリケーションは、少なくとも1つのデリバリーグループまたはアプリケーショングループに属している必要があります。アプリケーションをアプリケーショングループから削除しようとしたと

きに、そのアプリケーションがどのグループにも属さなくなる場合、続行するとアプリケーションが削除されるという通知が表示されます。その場合、そのアプリケーションを配信したい場合は、有効なソースから再度追加する必要があります。

1. 左側のペインで、 を選択します。
2. 中央のペインでアプリケーショングループを選択し、1つまたは複数のアプリケーションを選択します。
3. アクションバーで を選択します。
4. 削除を確認します。

アプリケーションのプロパティを変更する

アプリケーションのプロパティは、一度に1つしか変更できません。

アプリケーションのプロパティを変更するには：

1. 左側のペインで を選択します。
2. アプリケーションを選択し、アクションバーで を選択します。
3. 変更するプロパティが含まれるページを選択します。
4. 完了したら、 をクリックして変更を適用し、ウィンドウを開いたままにするか、 をクリックして変更を適用してウィンドウを閉じます。

次のリストでは、ページが括弧内に表示されます。

プロパティ	ページ
Citrix Workspaceアプリにアプリケーションが表示されるカテゴリまたはフォルダー	配信
コマンドライン引数。「公開アプリケーションへのパラメーターの受け渡し」を参照してください。	場所
アプリケーションが利用可能なデリバリーグループとアプリケーショングループ	グループ
説明	識別
ファイル名拡張子とファイルの種類関連付け：アプリケーションが自動的に開く拡張子	ファイルの種類関連付け

プロパティ	ページ
アイコン	配信
StoreFront™のキーワード	識別
制限; アプリケーション制限の構成を参照	配信
名前: ユーザーおよび管理者に表示される名前	識別
実行可能ファイルへのパス; 公開アプリケーションへのパラメーターの受け渡しを参照	場所
ユーザーのデスクトップ上のショートカット: 有効または無効	配信
可視性: Citrix Workspaceアプリでアプリケーションを表示できるユーザーを制限します。非表示のアプリケーションでも起動できます。利用不可かつ非表示にするには、別のグループに追加します。	可視性の制限
作業ディレクトリ	場所

アプリケーションの変更は、現在のアプリケーションユーザーがセッションからログオフするまで有効にならない場合があります。

アプリケーション制限を構成する

アプリケーションの使用状況を管理するために、アプリケーション制限を構成します。たとえば、アプリケーション制限を使用して、アプリケーションに同時にアクセスするユーザーの数を管理できます。同様に、アプリケーション制限は、リソースを大量に消費するアプリケーションの同時インスタンス数を管理するためにも使用できます。この制限は、サーバーのパフォーマンスを維持し、サービスの劣化を防ぐのに役立ちます。

この機能は、Controller によって仲介されるアプリケーションの起動数（Citrix Workspace アプリや StoreFront からの起動など）を制限するものであり、他の方法で起動できる実行中のアプリケーションの数を制限するものではありません。これは、アプリケーション制限が同時使用を管理する際に管理者を支援するものの、すべてのシナリオで強制力を持つわけではないことを意味します。たとえば、Controller が停止モードの場合、アプリケーション制限は適用できません。

デフォルトでは、同時に実行できるアプリケーションインスタンスの数に制限はありません。アプリケーション制限の設定はいくつかあります。それらのいずれか、またはすべてを構成できます。

- デリバリーグループ内のすべてのユーザーによるアプリケーションの同時インスタンスの最大数。
- デリバリーグループ内のユーザーごとのアプリケーションのインスタンス数（1つ）。
- マシンごとのアプリケーションの同時インスタンスの最大数（PowerShell のみ）。

制限が構成されている場合、ユーザーが構成された制限を超えるアプリケーションインスタンスを起動しようとすると、エラーメッセージが生成されます。複数の制限が構成されている場合、最初に到達した制限でエラーが報告されます。

アプリケーション制限の使用例：

- **同時インスタンス数の最大制限:** デリバリーグループで、アプリケーション `Alpha` の同時インスタンスの最大数を 15 に構成します。その後、そのデリバリーグループのユーザーは、そのアプリケーションのインスタンスを 15 個同時に実行しています。そのデリバリーグループのいずれかのユーザーが `Alpha` を起動しようとすると、エラーメッセージが生成されます。`Alpha` は、構成された同時アプリケーションインスタンス制限（15）を超えるため、起動されません。
- **ユーザーごとのインスタンス数制限:** 別のデリバリーグループで、アプリケーション `Beta` のユーザーごとのインスタンス数オプションを有効にします。ユーザー Tony はアプリケーション `Beta` を正常に起動します。その日の後半、そのアプリケーションが Tony のセッションでまだ実行されている間に、彼は `Beta` の別のインスタンスを起動しようとします。エラーメッセージが生成され、`Beta` はユーザーごとのインスタンス数制限を超えるため、起動されません。
- **同時インスタンス数の最大制限とユーザーごとのインスタンス数制限:** 別のデリバリーグループで、同時インスタンスの最大数を 10 に構成し、アプリケーション `Delta` のユーザーごとのインスタンス数オプションを有効にします。その後、そのデリバリーグループの 10 人のユーザーがそれぞれ `Delta` のインスタンスを実行している場合、そのデリバリーグループの他のユーザーが `Delta` を起動しようとすると、エラーメッセージが表示されます。`Delta` は起動されません。現在の 10 人の `Delta` ユーザーのいずれかがそのアプリケーションの 2 番目のインスタンスを起動しようとすると、エラーメッセージが表示され、2 番目のインスタンスは起動されません。
- **マシンごとの同時インスタンス数の最大制限とタグ制限の使用:** アプリケーション `Charlie` には、特定のサーバーで同時に実行できるインスタンスの数を規定するライセンスおよびパ

フォーマンス要件があります。これらの要件は、サイト内のすべてのサーバーで同時に実行できるインスタンスの数も規定します。

アプリケーションのインスタンス数/マシン制限は、サイト内のすべてのサーバーに影響します（特定のデリバリーグループ内のマシンだけでなく）。サイトに 3 台のサーバーがあるとします。アプリケーション `Charlie` の場合、マシンあたりのアプリインスタンス制限を 2 に構成します。したがって、サイト全体でアプリケーション `Charlie` のインスタンスは 6 つまでしか起動できません。（これは、3 台のサーバーそれぞれで Charlie のインスタンスが 2 つという制限です。）

アプリケーションの使用をデリバリーグループ内の特定のコンピューターのみに制限するには（サイト全体のすべてのコンピューターでのインスタンス制限に加えて）：

- それらのマシンにタグ付け機能を使用します。
- そのアプリケーションのマシンごとの最大インスタンス数を構成します。

アプリケーションがControllerの仲介以外の方法（たとえば、Controllerが停止モードの場合など）で起動され、構成された制限を超過した場合、ユーザーは制限を超過しないように十分な数のインスタンスを閉じるまで、それ以上のインスタンスを起動できません。制限を超過したインスタンスは強制的にシャットダウンされません。ユーザーが閉じるまで継続して実行が許可されます。

セッションローミングを無効にする場合は、ユーザーごとのアプリケーションインスタンス数制限を無効にします。ユーザーごとのアプリケーションインスタンス数制限を有効にする場合は、新しいデバイスでの新しいセッションを許可する2つの値のいずれも構成しないでください。ローミングについて詳しくは、「セッション」を参照してください。

デリバリーグループごとの最大インスタンス数制限と、ユーザーごとのインスタンス数制限を構成するには：

1. 左側のペインで **［アプリケーション］** を選択し、アプリケーションを選択します。
2. アクションバーで **［アプリケーションプロパティの編集］** を選択します。
3. **［配信］** ページで、次のいずれかのオプションを選択します。

   - **アプリケーションの無制限の使用を許可する**。同時に実行されるインスタンスの数に制限はありません。これがデフォルトです。
   - **アプリケーションの制限を設定する**。制限の種類は2つあります。いずれかまたは両方を指定します。

     - マシンごとに同時に実行できるインスタンスの最大数を指定します
     - ユーザーごとにアプリケーションのインスタンスを1つに制限する

4. ［**OK**］ をクリックして変更を適用し、ダイアログボックスを閉じます。または、 ［**適用**］ をクリックして変更を適用し、ダイアログボックスを開いたままにします。

マシンごとの最大インスタンス数制限を構成するには（PowerShellのみ）：

- PowerShellで（Citrix Cloud™展開の場合はRemote PowerShell SDKを、オンプレミス展開の場合はPowerShell SDKを使用して）、適切な `BrokerApplication` コマンドレットを `MaxPerMachineInstances` パラメーターとともに指定します。
- ガイダンスについては、`Get-Help` コマンドレットを使用してください。例:

  ```
  Get-Help Set-BrokerApplication –Parameter MaxPerMachineInstances
  ```

公開アプリケーションにパラメーターを渡す

アプリケーションのプロパティの**場所**ページを使用して、コマンドラインを入力し、公開アプリケーションにパラメーターを渡します。

公開アプリケーションをファイルの種類に関連付けると、`"%*"` (二重引用符で囲まれたパーセント記号とアスタリスク記号) がアプリケーションのコマンドラインの末尾に追加されます。これらの記号は、ユーザーデバイスに渡されるパラメーターのプレースホルダーとして機能します。

公開アプリケーションが期待どおりに起動しない場合は、そのコマンドラインに正しい記号が含まれていることを確認してください。デフォルトでは、`"%*"` 記号が追加されると、ユーザーデバイスから提供されるパラメーターが検証されます。ユーザーデバイスから提供されるカスタマイズされたパラメーターを使用する公開アプリケーションの場合、コマンドライン検証をバイパスするために、`"%**"` 記号がコマンドラインに追加されます。アプリケーションのコマンドラインにこれらの記号が表示されない場合は、手動で追加してください。

実行可能ファイルへのパスにスペースを含むディレクトリ名が含まれている場合 (例: `"C:\Program Files"`)、スペースがコマンドラインの一部であることを示すために、アプリケーションのコマンドラインを二重引用符で囲みます。これを行うには、パスを二重引用符で囲み、`%*` 記号を別の二重引用符で囲みます。パスの閉じ引用符と `%*` 記号の開始引用符の間にスペースを含めるようにしてください。

たとえば、公開アプリケーションであるWindows Media Playerのコマンドラインは次のとおりです。

```
"C:\Program Files\Windows Media Player\mplayer1.exe" "%*"
```

> **注：**

> 公開アプリケーションを起動するためのコマンドラインの最大文字数 (引数を含む) は203文字です。

アプリケーションフォルダーの管理

デフォルトでは、デリバリーグループに追加する新しいアプリケーションは、**Applications**という名前のフォルダーに配置されます。デリバリーグループの作成時、アプリケーションの追加時、または後で別のフォルダーを指定できます。

知っておくと良いこと:

- Applicationsフォルダーの名前を変更したり削除したりすることはできませんが、その中に含まれるすべてのアプリケーションを、作成した他のフォルダーに移動することはできます。
- フォルダー名には1〜64文字を含めることができます。スペースも使用できます。
- フォルダーは最大5レベルまでネストできます。
- フォルダーにアプリケーションを含める必要はありません。空のフォルダーも許可されます。
- フォルダーは、移動したり、作成時に別の場所を指定したりしない限り、Web Studioでアルファベット順に表示されます。
- 同じ名前のフォルダーを複数持つことができますが、それぞれ異なる親フォルダーを持つ必要があります。同様に、同じ名前のアプリケーションを複数持つことができますが、それぞれ異なるフォルダーに存在する必要があります。
- フォルダー内のアプリケーションを表示するには`View Applications`権限が必要です。また、アプリケーションを含むフォルダーを削除、名前変更、または削除するには、そのフォルダー内のすべてのアプリケーションに対して`Edit Application Properties`権限が必要です。
- 以下のほとんどの手順では、Web Studio のアクションバーを使用してアクションを要求します。または、右クリックメニューを使用するか、項目をドラッグすることもできます。たとえば、意図しない場所にフォルダーを作成または移動した場合、ドラッグアンドドロップで正しい場所に移動できます。
- Web Studio のすべてのノード（**マシンカタログ**、**デリバリーグループ**、**アプリケーション**、**アプリケーショングループ**など）は、バックエンドで同じフォルダーツリーを共有します。フォルダーの名前変更や移動の際に名前の競合を避けるため、異なるノード間で最上位フォルダーには一意の名前を使用してください。

`New-BrokerAdminFolder` SDK コマンドレットを使用してフォルダーを作成し、それを**アプリケーション**ノードの下に表示させたい場合は、`Set-BrokerAdminFolderMetadata` コマンドレットを使用して`ContainsApplications`メタデータを追加する必要があります。

例:

```
Set-BrokerAdminFolderMetadata -AdminFolderId {adminFolderUid} -Name
ContainsApplications -Value true
```

アプリケーションフォルダーを管理するには、左ペインで**アプリケーション**を選択します。以下のリストを参考にしてください。

- **すべてのフォルダー（ネストされたフォルダーを除く）を表示するには：** フォルダーリストの上にある**すべて表示**をクリックします。
- **最上位レベル（ネストされていない）にフォルダーを作成するには：** **アプリケーション**フォルダーを選択します。新しいフォルダーを**アプリケーション**以外の既存のフォルダーの下に配置するには、そのフォルダーを選択します。次に、アクションバーで**フォルダーの作成**を選択します。名前を入力します。
- **フォルダーを移動するには：** フォルダーを選択し、アクションバーで**フォルダーの移動**を選択します。ネストされたフォルダーが含まれていない限り、一度に1つのフォルダーしか移動できません。（フォルダーを移動する最も簡単な方法は、ドラッグすることです。）
- **フォルダーの名前を変更するには：** フォルダーを選択し、アクションバーで**フォルダー名の変更**を選択します。名前を入力します。
- **フォルダーを削除するには：** フォルダーを選択し、アクションバーで**フォルダーの削除**を選択します。アプリケーションや他のフォルダーを含むフォルダーを削除すると、それらのオブジェクトも削除されます。アプリケーションを削除すると、デリバリーグループからのアプリケーション割り当てが削除されます。マシンからは削除されません。
- **アプリケーションをフォルダーに移動するには：** 1つまたは複数のアプリケーションを選択します。次に、アクションバーで**アプリケーションの移動**を選択します。フォルダーを選択します。

デリバリーグループまたはアプリケーショングループを作成する際に、**アプリケーション**ページで追加するアプリケーションをフォルダーに配置することもできます。デフォルトでは、追加されたアプリケーションは**アプリケーション**フォルダーに入ります。**変更**をクリックしてフォルダーを選択または作成します。

公開デスクトップでのアプリケーションのローカル起動を制御する

ユーザーが公開デスクトップ内から公開アプリケーションを起動する際、そのデスクトップセッションでアプリケーションを起動するか、公開アプリケーションとして起動するかを制御できます。Citrix Workspaceアプリは、VDA上のWindowsレジストリでアプリケーションのインストールパスを検索し、存在する場合はアプリケーションのローカルインスタンスを起動します。それ以外の場合は、ホストされたアプリケーションのインスタンスが起動されます。VDAにインストールされていないアプリケーションを起動すると、ホストされたアプリケーションが起動されます。詳細については、「vPrefer起動」を参照してください。

PowerShell（Citrix Cloud展開環境ではRemote PowerShell SDK、オンプレミス展開環境ではPowerShell SDKを使用）で、このアクションを変更できます。

`New-Broker` Applicationまたは`Set-BrokerApplication` コマンドレットで、`LocalLaunchDisabled` オプションを使用します。例：

```
Set-BrokerApplication -LocalLaunchDisabled <Boolean>
```

デフォルトでは、このオプションの値はfalse（`-LocalLaunchDisabled $false`）です。公開デスクトップ内から公開アプリケーションを起動すると、そのデスクトップセッション内でアプリケーションが起動されます。

オプションの値をtrue（`-LocalLaunchDisabled $true`）に設定すると、公開アプリケーションが起動されます。これにより、公開デスクトップから公開アプリケーションへの個別の追加セッションが（Citrix Workspaceアプリ for Windowsを使用して）作成されます。

要件と制限：

- アプリケーションの`ApplicationType` の値は`HostedOnDesktop` である必要があります。
- このオプションは、適切なPowerShell SDKを介してのみ利用可能です。現在、Web Studioのグラフィカルインターフェイスでは利用できません。
- このオプションには、StoreFront 3.14、Citrix Receiver for Windows 4.11、およびDelivery Controller 7.17が最低限必要です。

アプリパッケージ

> **注：**
>
> Citrix Virtual Apps and Desktops™の展開は、Web Studio (ウェブベース) と Citrix Studio (Windowsベース) の2つの管理コンソールを使用して管理できます。この記事ではWeb

> Studioのみを扱います。Citrix Studioの詳細については、Citrix Virtual Apps and Desktops 7 2212以前の同等の記事を参照してください。

> Microsoftは、アプリケーションをユーザーに配信するための3つのパッケージングテクノロジーを提供しています: App-V、MSIX、およびMSIX app attach。この記事では、**Web Studio > App Packages**を使用してこれらのパッケージ化されたアプリケーションを展開および配信する方法について説明します。

- App-Vアプリケーションの展開と配信
- MSIXおよびMSIX app attachアプリケーションの展開と配信

App-Vアプリケーションの展開と配信

このセクションでは、次の情報について説明します。

- 概要。App-Vパッケージを配信および管理するための管理方法について説明します。
- 手順。これらのパッケージを展開および配信するための手順を説明します。

概要

このセクションでは、App-Vパッケージを配信および管理するための管理方法について説明します。App-Vパッケージアプリケーションを配信する際に操作するコンポーネントと概念の詳細については、Microsoftのドキュメントを参照してください: `<https://docs.microsoft.com/ja-jp/windows/application-management/app-v/appv-for-windows>`。

App-Vパッケージを配信および管理するには、次の方法を使用できます:

- **Dual Admin**。アプリケーションパッケージはApp-Vサーバーで構成および管理されます。Citrix Virtual Apps and DesktopsとApp-Vサーバーが連携してパッケージを配信および管理します。

  この方法では、Citrix Virtual Apps and DesktopsがApp-Vサーバーの状態のスナップショットビューを定期的に更新する必要があります。これには、ハードウェア、インフラストラクチャ、および管理のオーバーヘッドが発生します。Citrix Virtual Apps and DesktopsとApp-Vサーバーは、特にユーザー権限に関して同期を維持する必要があります。

  Dual Adminは、App-Vと環境が密接に連携している展開で最適に機能します。

  - **App-V管理サーバー**。App-Vパッケージと動的構成ファイルのライフサイクルを公開および管理します。

- VDAマシンにインストールされている**Citrix Personalization component**。アプリケーションの起動に必要な適切なApp-V公開サーバーの登録を管理します。

この方法により、App-V公開サーバーが適切なタイミングでユーザーと同期されます。公開サーバーは、ログオン時の更新や接続グループなど、パッケージライフサイクルの他の側面を維持します。

- **シングル管理者**。アプリケーションパッケージはネットワーク共有に保存されます。Citrix Virtual Apps and Desktops は、パッケージを個別に配信および管理します。

  この方法により、展開において App-V サーバーとデータベースインフラストラクチャが不要になるため、オーバーヘッドが削減されます。

  この方法では、App-V パッケージをネットワーク共有に保存し、その場所からメタデータを環境にアップロードします。その後、VDA マシンにインストールされている Citrix Personalization コンポーネントが、次のようにアプリケーションを管理および配信します。

  - アプリケーションが起動されたときに、展開構成ファイルとユーザー構成ファイルを処理します。
  - ホストマシン上のパッケージのライフサイクルのすべての側面を管理します。

両方の管理方法を同時に使用できます。つまり、デリバリーグループにアプリケーションを追加するときに、アプリケーションは App-V サーバーまたはネットワーク共有に存在する App-V パッケージから取得できます。

> **注：**
>
> 両方の管理方法を同時に使用していて、App-V パッケージが両方の場所に動的構成ファイルを持っている場合、App-V サーバー上のファイル（デュアル管理者）が使用されます。

手順

App-V アプリケーションの配信をサポートするには、VDA マシンに Citrix Personalization コンポーネントをインストールする必要があります。詳細については、「VDA マシンへの Citrix Personalization コンポーネントのインストール」を参照してください。

App-V パッケージ化されたアプリケーションをユーザーに配信するには、次の手順に従います。

1. アプリケーションパッケージをネットワーク共有に保存する。
2. アプリケーションパッケージを環境にアップロードする。

3. アプリケーションをデリバリーグループに追加する。
4. 相互依存するApp-Vパッケージの自動配信を有効にするには、分離グループを作成します。

シングル管理者方式で Citrix Virtual Apps and Desktops が App-V 動的構成ファイルを認識して適用するようにするには、このCitrix ブログを参照してください。

MSIX および MSIX app attach アプリケーションの展開と配信

このセクションでは、次の情報について説明します。

- 概要。MSIX および MSIX app attach パッケージがどのように配信および管理されるかについて説明します。
- 手順。これらのパッケージを展開および配信するための手順を提供します。

概要

Citrix Virtual Apps and Desktops は、VDA マシンにインストールされている Citrix Personalization コンポーネントを介して、MSIX および MSIX app attach アプリケーションをユーザーに配信します。このコンポーネントは、ホストマシン上のパッケージのライフサイクルのすべての側面を管理します。

MSIX および MSIX app attach の詳細については、Microsoft ドキュメントの `<https://docs.microsoft.com/ja-jp/windows/msix/>` と `<https://docs.microsoft.com/ja-jp/azure/virtual-desktop/what-is-app-attach>` をそれぞれ参照してください。

手順

MSIXおよびMSIX app attachパッケージの配信をサポートするには、VDAマシンにCitrix Personalizationコンポーネントをインストールする必要があります。詳細については、「VDAマシンへのCitrix Personalizationコンポーネントのインストール」を参照してください。

MSIXおよびMSIX app attachパッケージ化されたアプリケーションをユーザーに配信するには、次の手順に従います。

1. アプリケーションパッケージをネットワーク共有に保存する。
2. アプリケーションパッケージを環境にアップロードする。
3. アプリケーションをデリバリーグループに追加する。

VDAマシンにCitrix Personalizationコンポーネントをインストールする

Citrix Personalizationコンポーネントは、App-V、MSIX、およびMSIX app attach形式のアプリケーションパッケージの公開プロセスを管理します。このコンポーネントは、VDAをインストー

ルする際にデフォルトではインストールされません。コンポーネントはVDAのインストール中またはインストール後にインストールできます。

VDAのインストール中にコンポーネントをインストールするには、次のいずれかの方法を使用します。

- インストールウィザードで、**［追加コンポーネント］**ページに移動し、**［Citrix Personalization for App-V - VDA］**チェックボックスをオンにします。
- コマンドラインインターフェイスでは、**/includeadditional "Citrix Personalization for App-V – VDA"** オプションを使用します。

VDAのインストール後にコンポーネントをインストールするには、次の手順に従います。

1. VDAマシンで、**コントロールパネル > プログラム > プログラムと機能**に移動し、**Citrix Virtual Delivery Agent**を右クリックして、**変更**を選択します。
2. 表示されるウィザードで、**［追加コンポーネント］**ページに進み、**［Citrix Personalization for App-V - VDA］**チェックボックスを有効にします。

> **注：**
>
> Microsoft App-V Desktop Clientは、ユーザーデバイスでApp-Vパッケージから仮想アプリケーションを実行するコンポーネントです。Windows 10（1607以降）、Windows Server 2016、およびWindows Server 2019には、このApp-Vクライアントソフトウェアがすでに含まれています。VDAマシンで有効にするだけで済みます。詳細については、このMicrosoftドキュメント記事を参照してください: `<https://docs.microsoft.com/ja-jp/windows/application-management/app-v/appv-enable-the-app-v-desktop-client>`。

アプリケーションパッケージをネットワーク共有に保存する

インフラストラクチャをセットアップしたら、アプリケーションパッケージを生成し、UNCまたはSMBネットワーク共有、あるいはAzureファイル共有などのネットワークロケーションに保存します。

詳細な手順は次のとおりです。

1. アプリケーションパッケージを生成します。詳細については、Microsoftのドキュメントを参照してください。
2. アプリケーションパッケージをネットワークロケーションに保存します。

- **App-V Single Admin**の場合：パッケージと対応する動的構成ファイル（App-V）をUNCまたはSMBネットワーク共有、あるいはAzureファイル共有に保存します。
- **App-V Dual Admin**の場合：UNCパスからApp-V管理サーバーにパッケージを公開します。（HTTP URLからの公開はサポートされていません。）
- **MSIXまたはMSIX app attach**の場合：パッケージをUNCまたはSMBネットワーク共有、あるいはAzureファイル共有に保存します。

3. VDAがパッケージストレージパスに対する読み取り権限を持っていることを確認してください。

   - ADドメイン内のUNCまたはSMBネットワーク共有にパッケージを保存する場合は、VDAマシンにストレージパスへの読み取り権限を付与します。これを行うには、マシンのADアカウントに共有への読み取り権限を明示的に付与するか、その権限を持つADグループにアカウントを含めます。
   - Azureファイル共有にパッケージを保存する場合は、まずAzureのストレージパスへの読み取り権限をユーザーアカウントに付与します。次に、VDAマシンで実行されている `ctxAppVService` を構成して、そのユーザーアカウントを使用してパッケージストレージパスにアクセスするようにします。詳細な手順については、次のセクションを参照してください。

ユーザーログオンアカウントの変更

VDAは、パッケージストレージパスにアクセスするために `ctxAppVService` を呼び出します。デフォルトでは、 `ctxAppVService` はマシンの**ローカルシステムアカウント**を使用してパッケージストレージパスにアクセスします。このタイプのマシン認証はADドメインで機能します。ただし、ユーザーアカウントベースの認証が必要なADとAzure ADの統合シナリオでは機能しません。

Azureファイル共有にパッケージを保存する場合は、 `ctxAppVService` のログオンアカウントを、パッケージストレージパスへの読み取り権限を持つユーザーアカウントに変更します。詳細な手順は次のとおりです。

1. **サービス**を開始し、**ctxAppVService**を右クリックし、**プロパティ**を選択します。
2. **［ログオン］タブで、［このアカウント］**を選択し、パッケージストレージパスへの読み取り権限を持つユーザーアカウントを入力し、ユーザーのパスワードを2回入力します。
3. **OK**をクリックします。

アプリケーションパッケージを環境にアップロードする

必要に応じてアプリケーションパッケージをネットワークの場所に保存した後、配信のために環境にアップロードします。必要に応じて、以下のいずれかの方法を使用します。

- 一括アップロード
- 1つずつアップロード

準備

Citrix Virtual Apps and Desktops は、パッケージ検出のためのネットワークロケーションへの接続をセットアップするために VDA マシンを使用します。そのため、事前に (/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/install-configure/delivery-groups-create.html) を作成し、グループ内の少なくとも1つの VDA が以下の要件を満たしていることを確認してください。

- VDAバージョン:
  - App-Vパッケージを検出する場合: 2203以降
  - MSIXおよびMSIXアプリ添付パッケージを検出する場合: 2209以降
- Citrix Personalization for App-V コンポーネント: インストール済み
- パッケージの場所に対するアクセス許可: 読み取り (詳細については、(#store-application-packages-on-network-shares) を参照してください。)
- 電源: オン
- 状態: 登録済み

アプリケーションパッケージを一括でアップロードする

ネットワーク上の場所にあるパッケージを環境にアップロードします。アップロードする前に、次の項目が準備されていることを確認してください。

- (#preparations) の要件を満たすデリバリーグループ
- ネットワークの場所のパス

パッケージを一括でアップロードするには、次の手順に従います。

1. 左側のペインで、**アプリパッケージ**を選択します。
2. **ソース**タブで、**ソースの追加**ボタンをクリックします。**ソースの追加**ページが表示されます。
3. **名前**フィールドに、パッケージソースのわかりやすい名前を入力します。
4. **デリバリーグループ**フィールドで、**デリバリーグループの選択**をクリックします。次に、(#preparations) で述べられている要件を満たすデリバリーグループを選択し、**OK**をクリックします。
5. **場所の種類**フィールドで、パッケージを保存する場所に基づいて**Microsoft App-Vサーバー**または**ネットワーク共有**を選択し、対応する設定を完了します。

- **Microsoft App-Vサーバー**を選択した場合は、次の情報を入力します。
  - 管理サーバーのURL。例: `http://appv-server.example.com`
  - 管理サーバー管理者のログイン資格情報。
  - 公開サーバーのURLとポート番号。例: `http://appv-server.example.com:3330`
- **ネットワーク共有**を選択した場合は、次の情報を指定します。
  - ネットワーク共有の UNC パスを入力します。例: `\\Package-Server\apps\`
  - アップロードするパッケージの種類を選択します。オプションには、App-V、MSIX、MSIX app attach があります。
  - パッケージのサブフォルダーを検索するかどうかを指定します。

6. **ソースの追加**をクリックします。

   ソースの追加ページが閉じ、新しく追加されたソースがソースリストに表示されます。Citrix Virtual Apps and Desktops は、デリバリーグループ内の VDA を使用してパッケージを環境にアップロードします。アップロードが完了すると、ステータスフィールドに*インポート成功*と表示されます。対応するパッケージは**パッケージ**タブに表示されます。

> **注：**
>
> ソースの場所でパッケージの更新を確認し、環境にインポートするには、ソースリストで場所を選択し、**パッケージの更新を確認**をクリックします。

アプリケーションパッケージを1つずつアップロードする

ネットワーク共有から環境にアプリケーションパッケージをアップロードします。アップロードする前に、次の項目が準備されていることを確認してください。

- (#preparations) で述べられている要件を満たすデリバリーグループ
- ネットワークの場所のパス。

パッケージを環境にアップロードするには、次の手順に従います。

1. 左側のペインで、**アプリパッケージ**を選択します。
2. **パッケージ**タブで、**パッケージの追加**ボタンをクリックします。**パッケージの追加**ページが表示されます。

3. 「**デリバリーグループ**」フィールドで、「**デリバリーグループの選択**」をクリックします。次に、準備に記載されている要件を満たすデリバリーグループを選択し、「**OK**」をクリックします。
4. 「**パッケージのフルパス**」フィールドに、必要に応じてパスを入力します。
   - 複数のパッケージを一度にアップロードするには、セミコロン (`;`) で区切って、それらのフルパスを入力します。例: `\\Package-Server\apps\office365.appv;\\Package-Server\apps\skype.msix;\\Package-Server\apps\slack.vhd`
   - ネットワーク共有にあるすべてのパッケージをアップロードするには、ストレージパスを入力します。例: `\\package-Server\apps\`
5. 「**パッケージの追加**」をクリックします。

   アプリケーションパッケージが「**パッケージ**」タブに表示されます。

アプリケーションをデリバリーグループに追加する

アプリケーションパッケージが完全にアップロードされたら、必要に応じてそのアプリケーションを1つ以上のデリバリーグループに追加します。その結果、それらのデリバリーグループに関連付けられているユーザーは、アプリケーションにアクセスできるようになります。

パッケージ内の1つ以上のアプリケーションを複数のデリバリーグループに追加するには、次の手順に従います。

1. 左側のペインで、**アプリパッケージ**を選択します。
2. **Packages**タブで、必要に応じてパッケージを選択します。
3. アクションバーで、**［デリバリーグループの追加］** をクリックします。「デリバリーグループの追加」ページが表示されます。
4. 必要に応じてパッケージ内の1つ以上のアプリケーションを選択し、**［次へ］** をクリックします。*アプリケーション*配信タイプのデリバリーグループが表示されます。
5. デリバリーグループの一覧で、アプリケーションを割り当てるグループを選択し、**［次へ］** をクリックします。 **注：** MSIXまたはMSIX app attachパッケージを選択した場合、機能レベルが2106以降のデリバリーグループのみが一覧に表示されます。
6. **完了**をクリックします。

次の場合に、パッケージ化されたアプリケーションをデリバリーグループに追加することもできます。

- デリバリーグループを作成する場合。詳細については、「デリバリーグループの作成」を参照してください。

- 既存のデリバリーグループまたはアプリケーショングループを編集する場合。詳細については、「アプリケーションの追加」を参照してください。

（オプション）App-Vパッケージの分離グループを作成する

相互依存するApp-Vパッケージを自動的に配信できるように、分離グループを作成できます。

> **注：**
>
> 分離グループは、App-Vシングル管理者方式でサポートされています。App-Vデュアル管理者方式を使用している場合は、Microsoft App-Vインフラストラクチャで*接続グループ*を作成することで、同じ目標を達成できます。詳しくは、次のMicrosoftドキュメント記事を参照してください：`<https://docs.microsoft.com/ja-jp/windows/application-management/app-v/appv-connection-group-file>`。

分離グループについて

分離グループとは、仮想環境を作成するために同じWindows Sandboxで実行する必要がある、相互依存するアプリケーションパッケージの集合です。Citrix App-V分離グループは、App-V接続グループに似ていますが、同一ではありません。分離グループには、次の2種類のパッケージが含まれます。

- **明示的**アプリケーションパッケージ。特定のライセンス要件を持つアプリケーション。これらのアプリケーションをデリバリーグループに追加することで、特定の範囲のユーザーに制限できます。
- **自動**アプリケーションパッケージ。デリバリーグループに追加されているかどうかに関係なく、常にすべてのユーザーが利用できるアプリケーション。

たとえば、アプリケーション`app-a`を実行するにはJRE 1.7が必要です。app-a（*明示的*としてマーク）とJRE 1.7（*自動*としてマーク）を含む分離グループを作成できます。次に、`app-a`のApp-Vパッケージを1つ以上のデリバリーグループに追加します。ユーザーがapp-aを起動すると、JRE 1.7が自動的に展開されます。

ユーザーが分離グループ内で*明示的*とマークされたApp-Vアプリケーションを起動すると、Citrix Virtual Apps and Desktopsはデリバリーグループ内のアプリケーションに対するユーザーのアクセス許可を確認します。ユーザーがアプリケーションにアクセスする権限を持っている場合、同じ分離グループ内の*自動*アプリケーションパッケージがユーザーに利用可能になります。

*自動*パッケージをデリバリーグループに追加する必要はありません。分離グループに別の*明示的*アプリケーションパッケージがある場合、そのパッケージは同じデリバリーグループにある場合にのみユーザーが利用できます。

分離グループについて詳しくは、このCitrixブログを参照してください。

APP-V分離グループを作成する

分離グループを作成し、相互依存するアプリケーションパッケージを追加します。詳細な手順は次のとおりです。

1. **「分離グループ」**タブで、**「分離グループの追加」**をクリックします。
2. 分離グループの名前と説明を入力します。環境内のすべてのアプリケーションパッケージが、**［利用可能なパッケージ］** の一覧に表示されます。
3. **「利用可能なパッケージ」**リストから、必要に応じてアプリケーションを選択し、右矢印をクリックします。選択したアプリケーションが**「分離グループ内のパッケージ」**リストに表示されます。
4. **「展開」**フィールドで、アプリケーションに対して**「明示的」**または**「自動」**を選択します。
5. さらにパッケージを追加するには、手順2～3を繰り返します。
6. リスト内のパッケージの順序を調整するには、上矢印または下矢印をクリックします。
7. **「保存」**をクリックします。

> **注：**
>
> 隔離グループ構成により、VDA上にApp-V接続グループが作成されます。展開シナリオは複雑になる可能性があり、App-Vクライアントは一度に1つのアクティブな接続グループにのみ存在するパッケージをサポートします。同じパッケージを、同じデリバリーグループに追加された2つの異なる隔離グループに追加することは避けることをお勧めします。

パッケージ化されたアプリケーションをシングルセッションまたは共有デスクトップVDAに公開する

App-V、MSIX、およびMSIX app attachパッケージを、デリバリーグループを介してシングルセッションまたは共有デスクトップVDAセッションに直接配信できるようになりました。アプリケーションに設定されているアクセス許可に基づいて、サインイン時にデスクトップVDAでパッケージ化されたアプリケーションにアクセスできます。

利点

- サインイン時にVDAで利用可能で、WorkspaceまたはStoreFrontを介してオンデマンドでステージングされないアプリケーション。
- パッケージ化されたアプリケーションにアクセスする際の起動時間の改善。
- VDAのベースイメージとは別に、パッケージ化されたアプリケーションの独立したメンテナンスを容易にします。

考慮事項

- このオプションは、適切なPowerShell SDKを介してシングルセッションVDAでのみ利用できます。Web Studioワークフローでは現在利用できません。共有デスクトップへの公開は、PowerShell SDKを使用するか、Web Studioワークフローを介した既存の方法で行うことができます。既存の手順について詳しくは、「デリバリーグループへのアプリケーションの追加」を参照してください。
- アプリケーションはデリバリーグループの一部である必要があります。

始める前に

- パッケージ化されたアプリケーションが署名されており、ファイル共有またはUNCの場所に存在することを確認してください。詳細については、「ネットワーク共有にアプリケーションパッケージを保存する」を参照してください。
- VDAマシンにCitrix Personalizationコンポーネントをインストールします。

手順

パッケージ化されたアプリケーションをデスクトップVDAに配信するには、次の手順に従います。

1. Web Studioにアプリケーションパッケージをインポートします。
2. パッケージ化されたBrokerApplicationを公開します。
3. Web Studioでのアプリケーションの可視性を制限します。

Web Studioにアプリケーションパッケージをインポートする

1. Webブラウザを開きます。`https://<address of the server hosting Web Studio>/Citrix/Studio`と入力します。
2. デリバリーグループを作成します。詳細については、「デリバリーグループを作成する」を参照してください。
3. アプリケーションパッケージをWeb Studioにインポートします。詳細については、「アプリケーションパッケージを一括アップロードする」を参照してください。

BrokerApplicationでパッケージ化されたアプリケーションを公開する

マルチセッション（共有）VDAまたはシングルセッションアプリケーションVDAに公開する場合、公開手順は変更されません。詳細については、「デリバリーグループにアプリケーションを追加する」を参照してください。 シングルセッションデスクトップVDAに公開する場合は、次の操作を行います。

Delivery Controller™上で、以下のPowerShellコマンドを実行します:

1. パッケージ内に存在するコマンドを取得するには：

   ```
   Import-Module "D:\Support\Tools\Scripts\Citrix.Cloud.AppLibrary.Admin.v1.psm1"
   ```

   > **注：**
   >
   > この機能をサポートする `App-V package discovery module` のバージョンは、上記のパスにあるCitrix Virtual Apps and Desktops ISO（2311以降のバージョン）で確認できます。

2. 関連するデリバリーグループIDとパッケージ化されたアプリケーションIDを取得するには:

   `Get-BrokerDesktopGroup | Format-Table Uid, Name` `Get-AppLibAppVApplication | Format-Table Uid, Name`

3. パッケージを公開し、適切なBrokerMachineConfigurationを作成するには:

   ```
   Publish-PackagedApplication -AppLibararyApplicationUid <AppLibararyApplication.Uid > -DesktopGroupUid <DesktopGroup.Uid>
   ```

4. Broker構成を同期するには、これは後でVDA上のBrokerエージェントに送信されます:

   ```
   Update-DesktopGroupMachineConfigurations -DesktopGroupUid <DesktopGroup.Uid>
   ```

   > **注：**
   >
   > VDA からパッケージ化されたアプリケーションを公開または削除した後、PowerShell コマンド `Update-DesktopGroupMachineConfigurations` を実行してください。

Web Studio でのアプリケーションの可視性を制限する

デフォルトでは、ユーザーは自分の VDA を提供するデリバリーグループに割り当てられているすべてのパッケージ化されたアプリケーションをデスクトップセッションで利用できます。Web Studio で特定のユーザーまたはグループにアプリケーションの可視性を設定することで、デスクトップ VDA 上のパッケージ化されたアプリケーションの可視性を制御できます。パッケージ化されたアプリケーションの可視性を管理するには、「アプリケーションプロパティの変更」を参照してください。

ユニバーサル Windows プラットフォームアプリ

ユニバーサル Windows プラットフォーム (UWP) アプリについては、以下の Microsoft ドキュメントを参照してください。

- ユニバーサル Windows プラットフォーム (UWP) アプリとは
- Windows パッケージマネージャー

要件と制限

Citrix Virtual Apps and Desktops™ は、以下の Windows マシン上の VDA で UWP アプリを使用することをサポートしています。

- Windows 10 以降のバージョン
- Windows Server 2016 以降のバージョン

VDA はバージョン 7.11 以降である必要があります。

UWP アプリを使用する場合、以下の Citrix Virtual Apps and Desktops の機能はサポートされていないか、制限されています。

- ファイルタイプの関連付けはサポートされていません。
- ローカルアプリアクセスはサポートされていません。
- 動的プレビュー：セッションで実行中のアプリが重なっている場合、プレビューにはデフォルトのアイコンが表示されます。動的プレビューに使用される Win32 API は、UWP アプリではサポートされていません。
- アクションセンターのリモート処理：UWP アプリは、セッション内のメッセージを表示するためにアクションセンターを使用できます。これらのメッセージは現在、ユーザーに表示するためにエンドポイントにリダイレクトされません。

同じサーバーから UWP アプリと非 UWP アプリを起動することはサポートされていません。代わりに、UWP アプリと非 UWP アプリを別々のデリバリーグループまたはアプリケーショングループに配置してください。

マシンにインストールされているすべてのUWPアプリが列挙されるため、Citrix®はWindowsストアへのユーザーアクセスを無効にすることを推奨します。これにより、あるユーザーがインストールしたUWPアプリが別のユーザーによってアクセスされるのを防ぎます。

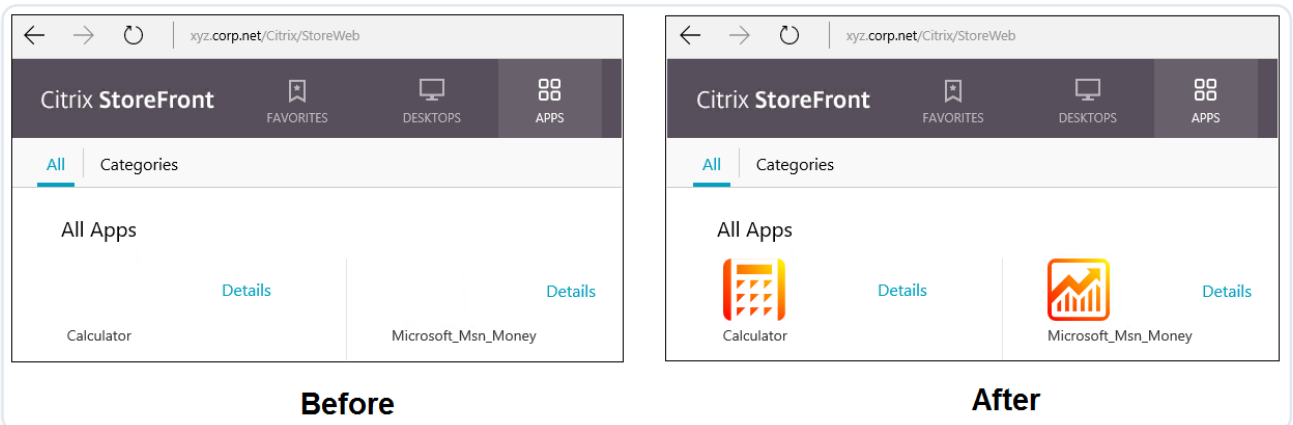
サイドローディング中、UWPアプリはマシンにインストールされ、他のユーザーが使用できるようになります。別のユーザーがアプリを起動すると、アプリがインストールされ、OSはそのAppXデータベースを更新して、そのユーザーによって「インストール済み」であることを示します。

固定ウィンドウまたはシームレスウィンドウで起動された公開UWPアプリから開始された正常なログオフにより、VDAセッションが閉じなくなり、ユーザーが強制的にログオフされる可能性があります。この場合、VDAセッションに残っているいくつかのプロセスが、セッションが適切に閉じられるのを妨げます。これを解決するには、VDAセッションが閉じない原因となっているプロセスを特定し、CTX891671のガイダンスに従って、「LogoffCheckSysModules」レジストリキー値に追加します。

UWPアプリのアプリケーション表示名と説明が正しくない場合があります。アプリケーションをデリバリーグループに追加する際に、これらのプロパティを編集して修正してください。

その他の問題については、既知の問題を確認してください。

現在、いくつかのUWPアプリは透明度が有効な白いアイコンを使用しており、StoreFront表示の白い背景に対してアイコンが見えなくなることがあります。この問題を回避するには、背景を変更できます。たとえば、StoreFrontマシンでファイル `C:\inetpub\wwwroot\Citrix\StoreWeb\custom\style.css` を編集します。ファイルの最後に `.storeapp-icon {background-image: radial-gradient( circle at top right, yellow, red ); }` を追加します。次の図は、この例の変更前と変更後を示しています。



Windows Server 2016以降のバージョンでは、UWPアプリの起動時にサーバーマネージャーも起動する場合があります。これを防ぐには、`HKLM\Software\Microsoft\ServerManager\DoNotOpenServerManagerAtLogon`レジストリキーを使用して、ログオン時にサーバーマネージャーが自動起動しないように無効にできます。詳細については、`<https://blogs.technet.microsoft.com/rmilne/2014/05/30/how-to-hide-server-manager-at-logon/>`を参照してください。

UWPアプリのインストールと公開

UWPアプリのサポートはデフォルトで有効になっています。

VDA（またはマスターイメージ）に1つ以上のUWPアプリをインストールするには、次のいずれかの方法を使用します。

- Windows Store for Businessからオフラインインストールを完了し、Deployment Image Servicing and Management (DISM) などのツールを使用してアプリをデスクトップイメージに展開します。詳細については、Windows Package Managerを参照してください。
- アプリをサイドロードします。詳細については、Windows クライアントデバイスで基幹業務 (LOB) アプリをサイドロードするを参照してください。
- 各対象ユーザー向けに、Windows Store for Businessから直接UWPアプリをインストールします。

Citrix Virtual AppsまたはCitrix Virtual Desktops™で1つ以上のUWPアプリを追加（公開）するには：

1. マシンにUWPアプリがインストールされたら、UWPアプリをデリバリーグループまたはアプリケーショングループに追加します。これは、グループの作成時または後で行うことができます。**アプリケーション**ページで、**追加**メニューから**スタートメニューから**を選択します。
2. アプリケーションリストが表示されたら、公開するUWPアプリを選択します。
3. ウィザードを続行するか、編集ダイアログを閉じます。

VDAでユニバーサルアプリの使用を無効にするには、`HKLM\Software\Citrix\VirtualDesktopAgent\FeatureToggle`にレジストリ設定**EnableUWASeamlessSupport**を追加し、**0**に設定します。

UWPアプリのアンインストール

`Remove-AppXPackage`のようなコマンドでUWPアプリをアンインストールすると、その項目は管理者に対してのみアンインストールされます。アプリを起動して使用した可能性のあるユーザー

のマシンからアプリを削除するには、各マシンで削除コマンドを実行します。1つのコマンドですべてのユーザーのマシンからAppXパッケージをアンインストールすることはできません。

オートスケール™

> **注：**
>
> Citrix Virtual Apps and Desktops™ の展開は、Web Studio (Webベース) と Citrix Studio (Windowsベース) の2つの管理コンソールを使用して管理できます。この機能は Web Studio でのみ利用可能です。

> Autoscaleは、マシンをプロアクティブに電力管理するための、一貫性のある高性能なソリューションを提供する機能です。コストとユーザーエクスペリエンスのバランスを取ることを目的としています。

Autoscaleは、デリバリーグループ内の登録されているすべてのシングルセッションおよびマルチセッションOSマシンのプロアクティブな電源管理を可能にします。

Autoscaleの機能は次のとおりです。

- スケジュールベースおよび負荷ベースの設定(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/manage-deployment/autoscale/schedule-based-and-load-based-settings.html)
- 動的セッションタイムアウト(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/manage-deployment/autoscale/dynamic-session-timeout.html)
- Autoscaleタグ付きマシン（クラウドバースト）(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/manage-deployment/autoscale/autoscale-tagged-machines.html)
- ユーザーログオフ通知(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/manage-deployment/autoscale/force-user-logoff.html)

サポートされているVDAホスティングプラットフォーム

Autoscaleは、Citrix Virtual Apps and Desktopsがサポートするすべてのプラットフォームをサポートしています。これには、XenServer、Amazon Web Services、Google Cloud Platform、Microsoft Azure Resource Manager、VMware vSphereなど、さまざまなインフラストラクチャプラットフォームが含まれます。サポートされているプラットフォームの完全なリストについては、Citrix Virtual Apps and Desktopsのシステム要件を参照してください。

> **注：**
>
> パブリッククラウドホスト接続をデプロイに追加する場合、Hybrid Rights Licenseが必要です。Hybrid Rights Licenseの詳細については、Transition and Trade-Up (TTU) with Hybrid Rightsを参照してください。ライセンスの追加については、サイトの作成を参照してください。

サポートされているワークロード

Autoscaleは、マルチセッションOSとシングルセッションOSの両方のデリバリーグループをサポートしています。注意すべきユーザーインターフェイスは3つあります。

- マルチセッションOSデリバリーグループ（旧RDSデリバリーグループ）用のAutoscaleユーザーインターフェイス
- シングルセッションOSランダム（プール型）デリバリーグループ（旧プール型VDIデリバリーグループ）用のAutoscaleユーザーインターフェイス
- シングルセッションOS静的デリバリーグループ（旧静的VDIデリバリーグループ）用のAutoscaleユーザーインターフェイス

さまざまなデリバリーグループのユーザーインターフェイスの詳細については、Autoscaleユーザーインターフェイスを参照してください。

利点

Autoscale機能には、次の利点があります。

- デリバリーグループ内のマシンを電源管理するための、単一で一貫したメカニズムを提供します。
- 負荷ベースまたはスケジュールベースの電源管理、あるいはその両方の組み合わせでマシンに電力を供給することにより、可用性を確保し、コストを管理します。
- コスト削減やキャパシティ使用率などのメトリックを監視し、通知を有効にするには、Directorを使用します。

2分間のビデオを見る

次のビデオでは、Autoscaleの簡単なツアーを提供します。

<iframe src="https://www.youtube.com/embed/5yxERrFZQ68" width="720px" height="480px" frameborder="0" title="YouTube video player" allowfullscreen=""> </iframe>

Autoscale™ の概要

Autoscale はデリバリーグループレベルで動作します。設定したスケジュールに基づいて、デリバリーグループ内のマシンをプロアクティブに電源管理します。

Autoscale は、すべての種類のデリバリーグループに適用されます。

- シングルセッション静的OS
- シングルセッションランダムOS
- マルチセッションランダムOS

> **注：**
>
> MMCベースのStudioを使用してデリバリーグループを作成またはアップグレードする場合、Autoscale はデフォルトで有効になっています。

> この記事では、Autoscale に関連する基本的な概念について説明し、デリバリーグループで Autoscale を有効にして構成する方法に関するガイダンスを提供します。

基本的な概念

開始する前に、Autoscale の次の基本的な概念について学習してください。

- スケジュール
- 容量バッファ
- 負荷インデックス

スケジュール

Autoscaleは、設定したスケジュールに基づいて、デリバリーグループ内のマシンの電源をオン/オフします。

スケジュールには、各タイムスロットのアクティブなマシンの数と、ピーク時およびオフピーク時が定義されています。

スケジュールの設定は、デリバリーグループの種類によって異なります。詳細については、以下を参照してください。

- マルチセッションOSデリバリーグループ
- シングルセッションOSランダムデリバリーグループ

- シングルセッションOS静的デリバリーグループ

容量バッファ

容量バッファは、動的な負荷増加に対応するために、現在の需要に予備容量を追加するために使用されます。注意すべき2つのシナリオがあります。

- マルチセッションOSデリバリーグループの場合、容量バッファは、ロードインデックスの観点から、デリバリーグループの総容量のパーセンテージとして定義されます。
- シングルセッションOSデリバリーグループの場合、容量バッファは、デリバリーグループ内のマシンの総数のパーセンテージとして定義されます。

ロードインデックス

> **重要:**
>
> ロードインデックスは、マルチセッションデリバリーグループにのみ適用されます。

> ロードインデックスメトリックは、マシンがユーザーログオン要求を受信する可能性を決定します。これは、同時ログオン、セッション、CPU、ディスク、メモリの使用量に対して構成された**Citrix Load Management policy**設定を使用して計算されます。

ロードインデックスは0から10,000の範囲です。デフォルトでは、マシンが250セッションをホストしている場合、完全にロードされていると見なされます。

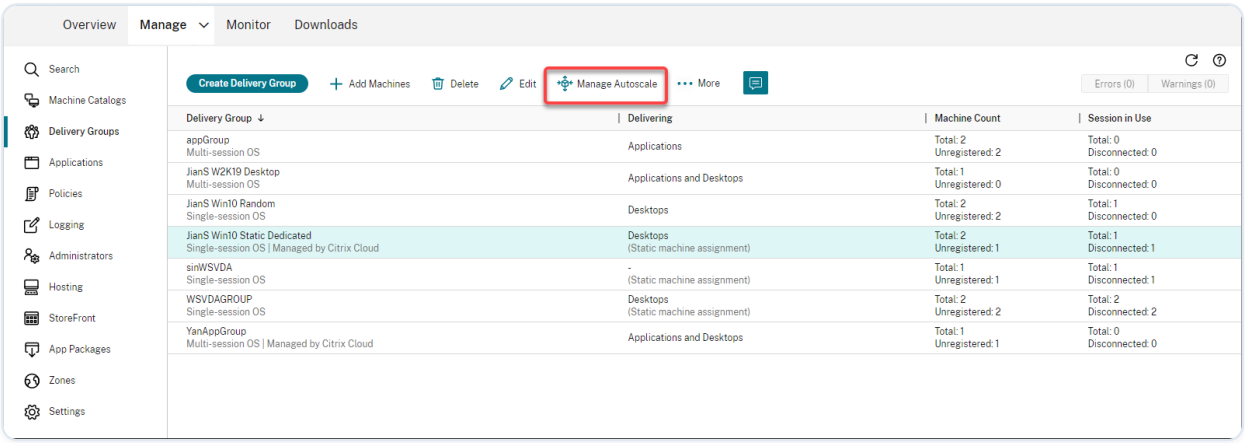
- 「0」はアンロードされたマシンを示します。ロードインデックス値が0のマシンは、ベースライン負荷状態です。
- 「10,000」は、これ以上セッションを実行できない完全にロードされたマシンを示します。

デリバリーグループのAutoscaleを有効にする

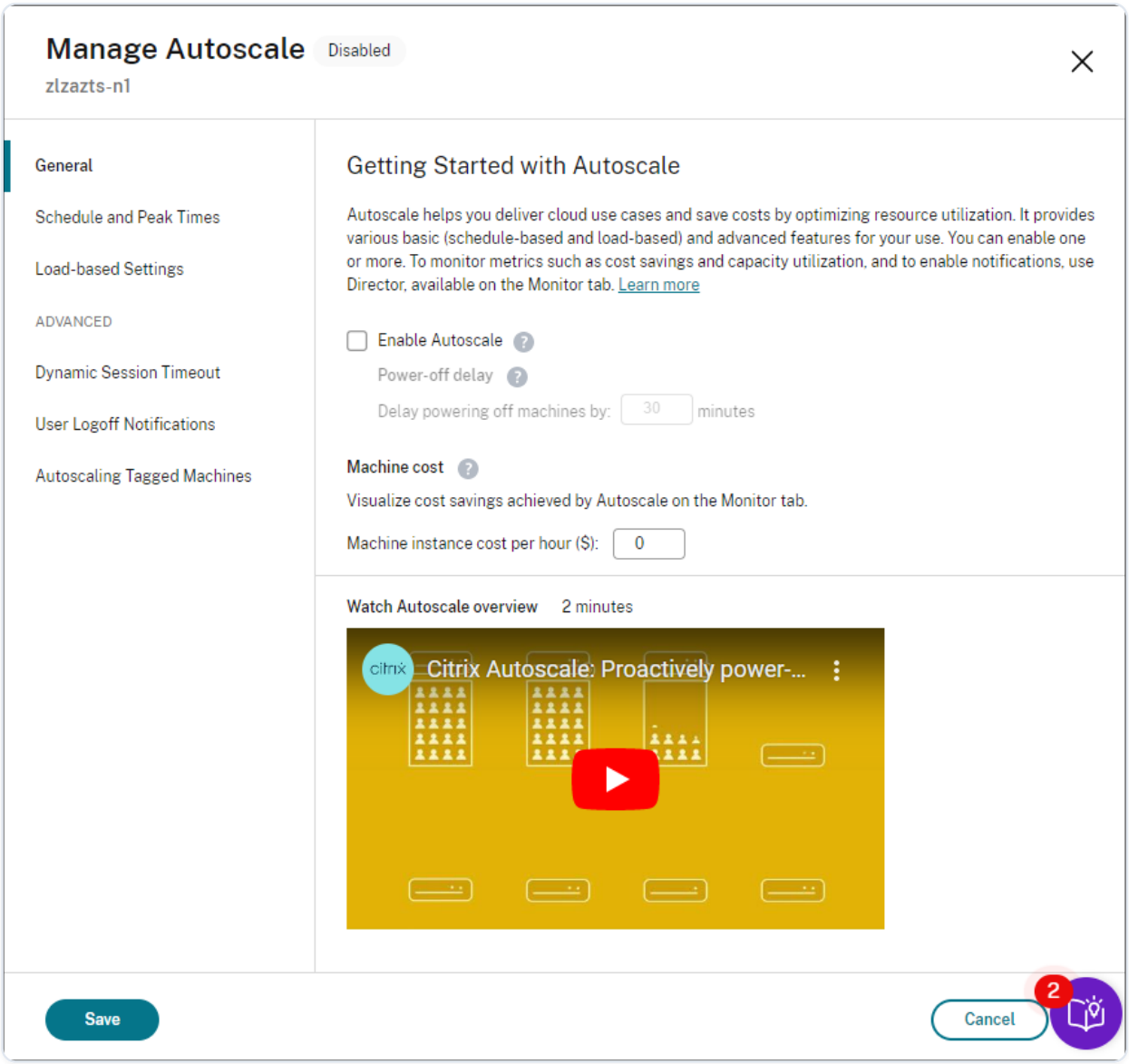
デリバリーグループを作成すると、Autoscaleはデフォルトで無効になります。Web Studioを使用してデリバリーグループのAutoscaleを有効にして構成するには、次の手順に従います。

PowerShellコマンドを使用して、デリバリーグループのAutoscaleを有効にして構成することもできます。詳細については、Broker PowerShell SDKコマンドを参照してください。

1. 左側のペインで、**［デリバリーグループ］**を選択します。
2. 管理するデリバリーグループを選択し、**Autoscaleの管理**をクリックします。



3. ページで、 チェックボックスをオンにしてAutoscaleを有効にします。Autoscaleを有効にすると、ページ上のオプションが有効になります。



4. 組織のニーズに基づいてデフォルト設定を変更するには、次の設定を完了します。

   - スケジュールを設定する

- 非アクティブなマシンをより効率的に電源オフにするには、動的セッションタイムアウトとユーザーログオフ通知を使用します。
- デリバリーグループ内のマシンの一部を電源管理するには、タグ付きマシンのAutoscaleを使用します。

Autoscaleを無効にするには、 チェックボックスをオフにします。ページ上のオプションがグレー表示され、選択したデリバリーグループでAutoscaleが無効になっていることを示します。

重要:

- Autoscaleを無効にすると、Autoscaleによって管理されているすべてのマシンは、無効化時の状態のままになります。
- Autoscaleを無効にすると、ドレイン状態のマシンはドレイン状態から解除されます。ドレイン状態の詳細については、ドレイン状態を参照してください。

メトリックの監視

デリバリーグループでAutoscaleを有効にすると、DirectorからAutoscaleで管理されているマシンの以下のメトリックを監視できます。

- マシンの使用状況
- 推定節約額
- マシンとセッションのアラート通知
- マシンのステータス
- 負荷評価の傾向

注：

デリバリーグループでAutoscaleを最初に有効にした後、そのデリバリーグループの監視データが表示されるまでに数分かかる場合があります。 Autoscaleが有効になり、その後デリバリーグループで無効になった場合でも、監視データは引き続き利用可能です。Autoscaleは5分間隔で監視データを収集します。

メトリックの詳細については、「Autoscaleで管理されるマシンの監視」を参照してください。

知っておくとよいこと

Autoscale はデリバリーグループレベルで動作します。デリバリーグループごとに構成されます。選択したデリバリーグループ内のマシンのみを電源管理します。

容量とマシンの登録

Autoscaleは、容量を決定する際に、サイトに登録されているマシンのみを含めます。登録されていない電源オンのマシンはセッション要求を受け入れることができません。その結果、それらはデリバリーグループの全体的な容量には含まれません。

複数のマシンカタログにわたるスケーリング

一部のサイトでは、複数のマシンカタログが単一のデリバリーグループに関連付けられている場合があります。Autoscaleは、スケジュールまたはセッションの需要要件を満たすために、各カタログからマシンをランダムに電源オンにします。

たとえば、あるデリバリーグループには2つのマシンカタログがあります。カタログAには3台のマシンが電源オンになっており、カタログBには1台のマシンが電源オンになっています。Autoscaleが追加のマシンを電源オンにする必要がある場合、カタログAまたはカタログBのいずれかのマシンを電源オンにする可能性があります。

マシンのプロビジョニングとセッションの需要

デリバリーグループに関連付けられているマシンカタログには、需要の増減に応じて電源をオン/オフするのに十分なマシンが必要です。セッション需要がデリバリーグループ内の登録済みマシンの総数を超えた場合、Autoscaleはすべての登録済みマシンの電源がオンになっていることを保証します。ただし、**Autoscaleは追加のマシンをプロビジョニングしません。**

インスタンスサイズの考慮事項

パブリッククラウドでインスタンスを適切にサイジングすると、コストを最適化できます。ワークロードのパフォーマンスと容量要件に合致する限り、より小さなインスタンスをプロビジョニングすることをお勧めします。

小規模なインスタンスは、大規模なインスタンスよりも少ないユーザーセッションをホストします。そのため、最後のユーザーセッションがログオフされるまでの時間が短いため、Autoscale はマシンをより速くドレイン状態にします。結果として、Autoscale は小規模なインスタンスをより早く電源オフにし、コストを削減します。

ドレイン状態

Autoscale は、デリバリーグループ内の電源オン状態のマシンの数を、構成されたプールサイズと容量バッファにまでスケールダウンしようとします。

この目標を達成するために、Autoscale はセッション数が最も少ない余分なマシンを「ドレイン状態」にし、すべてのセッションがログオフされたときにそれらの電源をオフにします。この動作は、セッションの需要が減少し、スケジュールで電源オンになっているマシンよりも少ないマシンが必要な場合に発生します。

Autoscale は、余分なマシンを「ドレイン状態」に1台ずつ移行します。

- 2台以上のマシンが同じ数のアクティブセッションを持っている場合、Autoscale は、指定された電源オフ遅延の間電源がオンになっていたマシンをドレインします。

  そうすることで、最近電源がオンになったマシンがドレイン状態になるのを避けることができます。なぜなら、それらのマシンはセッション数が最も少ない可能性が高いからです。
- 2台以上のマシンが指定された電源オフ遅延の間電源がオンになっていた場合、Autoscale はそれらのマシンをランダムに1台ずつドレインします。

ドレイン状態のマシンは、新しいセッションの起動をホストしなくなり、既存のセッションがログオフされるのを待っています。マシンは、すべてのセッションがログオフされた場合にのみシャットダウンの候補になります。ただし、セッション起動にすぐに利用できるマシンがない場合、Autoscale は、マシンの電源をオンにするよりも、ドレイン状態のマシンにセッション起動を誘導することを優先します。

次のいずれかの条件が満たされると、マシンはドレイン状態から解除されます。

- マシンの電源がオフになる。
- マシンが属するデリバリーグループで Autoscale が無効になっている。
- Autoscale は、スケジュールまたは負荷需要の要件を満たすためにマシンを使用します。このケースは、スケジュール（スケジュールベースのスケーリング）または現在の需要（負荷ベースのスケーリング）が、現在電源がオンになっているマシンの数よりも多くのマシンを必要とする場合に発生します。

> **重要:**

> セッション起動に利用できるマシンがすぐにない場合、Autoscale は、マシンの電源をオンにするよりも、ドレイン状態のマシンにセッション起動を誘導することを優先します。セッション起動をホストするドレイン状態のマシンは、ドレイン状態のままになります。

> どのマシンがドレイン状態にあるかを確認するには、`Get-BrokerMachine` PowerShell コマンドを使用します。例: `Get-BrokerMachine -DrainingUntilShutdown $true`。また

は、管理コンソールを使用することもできます。「ドレイン状態のマシンを表示する」を参照してください。

ドレイン状態のマシンを表示する

注：

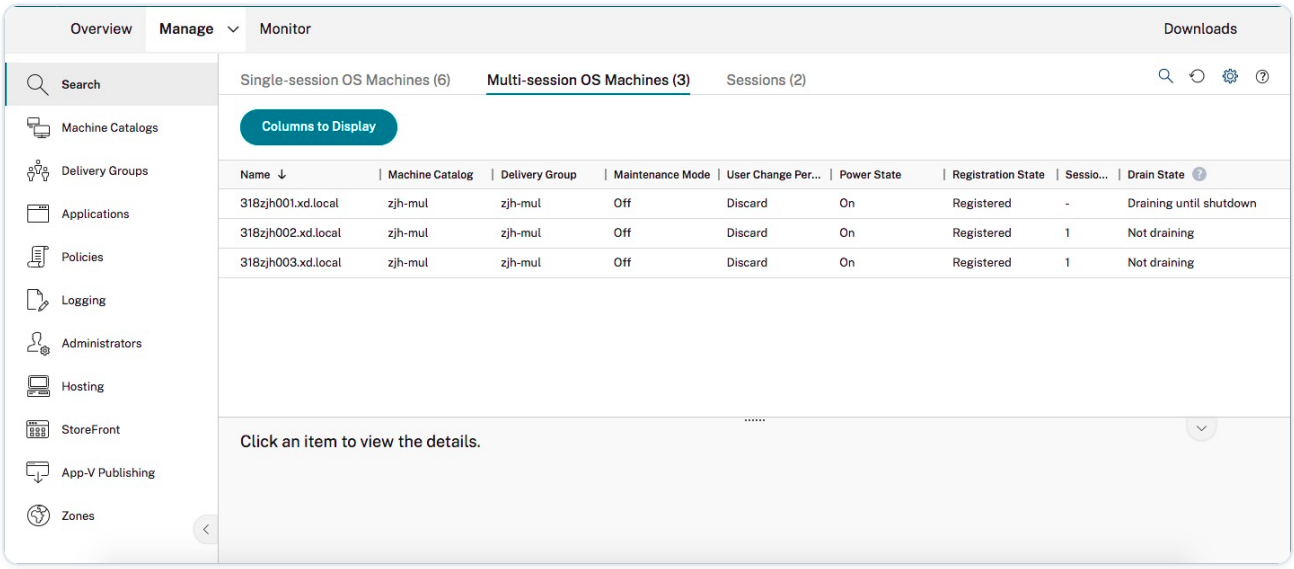
この機能は、マルチセッションマシンにのみ適用されます。

Web Studio では、ドレイン状態のマシンを表示できます。これにより、どのマシンがシャットダウンしようとしているかを知ることができます。次の手順を完了します。

1. **検索**ノードに移動し、**表示する列**をクリックします。
2. 「**表示する列**」ウィンドウで、「**ドレイン状態**」の横にあるチェックボックスをオンにします。
3. **保存**をクリックして、**表示する列**ウィンドウを終了します。

ドレイン状態列には、次の情報が表示されます。

- **シャットダウンまでドレイン中。** マシンがシャットダウンされるまでドレイン状態にある場合に表示されます。
- **ドレイン中ではありません。** マシンがまだドレイン状態ではない場合に表示されます。



詳細情報

Autoscaleの詳細については、Tech ZoneのCitrix Autoscaleを参照してください。

スケジュールベースおよび負荷ベースの設定

Autoscale™によるマシンの電源管理方法

Autoscaleは、選択されたスケジュールに基づいてマシンの電源をオン/オフします。Autoscaleを使用すると、特定の曜日を含む複数のスケジュールを設定し、その時間帯に利用可能なマシンの数を調整できます。特定の曜日の特定の時間に一連のユーザーがマシンリソースを消費すると予想される場合、Autoscaleは最適化されたエクスペリエンスの提供に役立ちます。これらのマシンは、セッションが実行されているかどうかにかかわらず、スケジュール中に電源がオンになることに注意してください。

> **注：**
>
> Autoscaleは、電源管理されているすべてのマシンをサポートします。

> スケジュールは、デリバリーグループの**タイムゾーン**に基づいています。タイムゾーンを変更するには、デリバリーグループのユーザー設定を変更します。詳しくは、「デリバリーグループの管理」を参照してください。

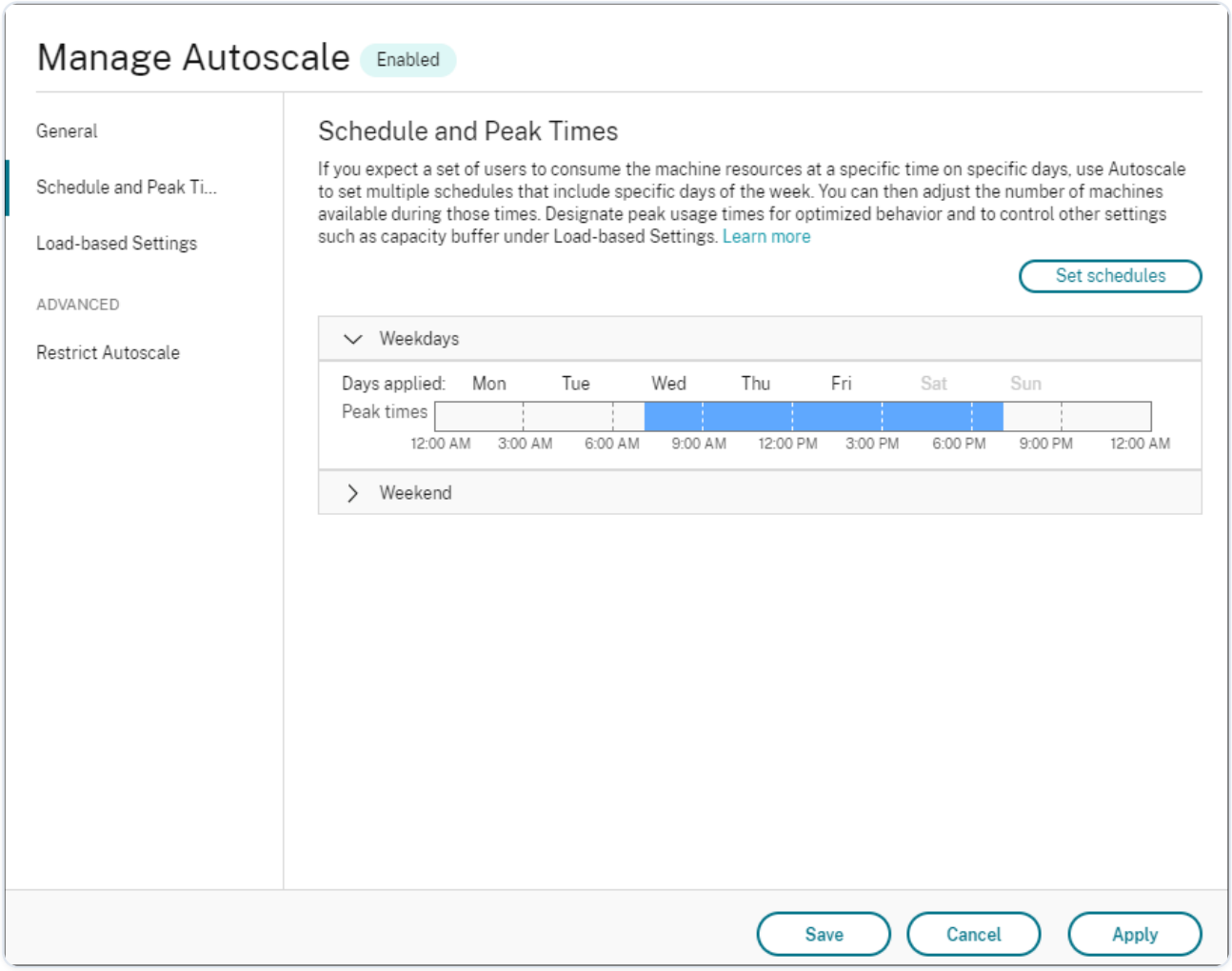
Autoscaleには、*平日*（月曜日から金曜日）と*週末*（土曜日と日曜日）の2つのデフォルトスケジュールがあります。デフォルトでは、**平日**スケジュールでは、ピーク時に午前7時から午後6時30分まで1台のマシンの電源がオンになり、オフピーク時には電源がオンになりません。デフォルトの容量バッファは、ピーク時とオフピーク時ともに10%に設定されています。デフォルトでは、**週末**スケジュールでは、マシンの電源はオンになりません。

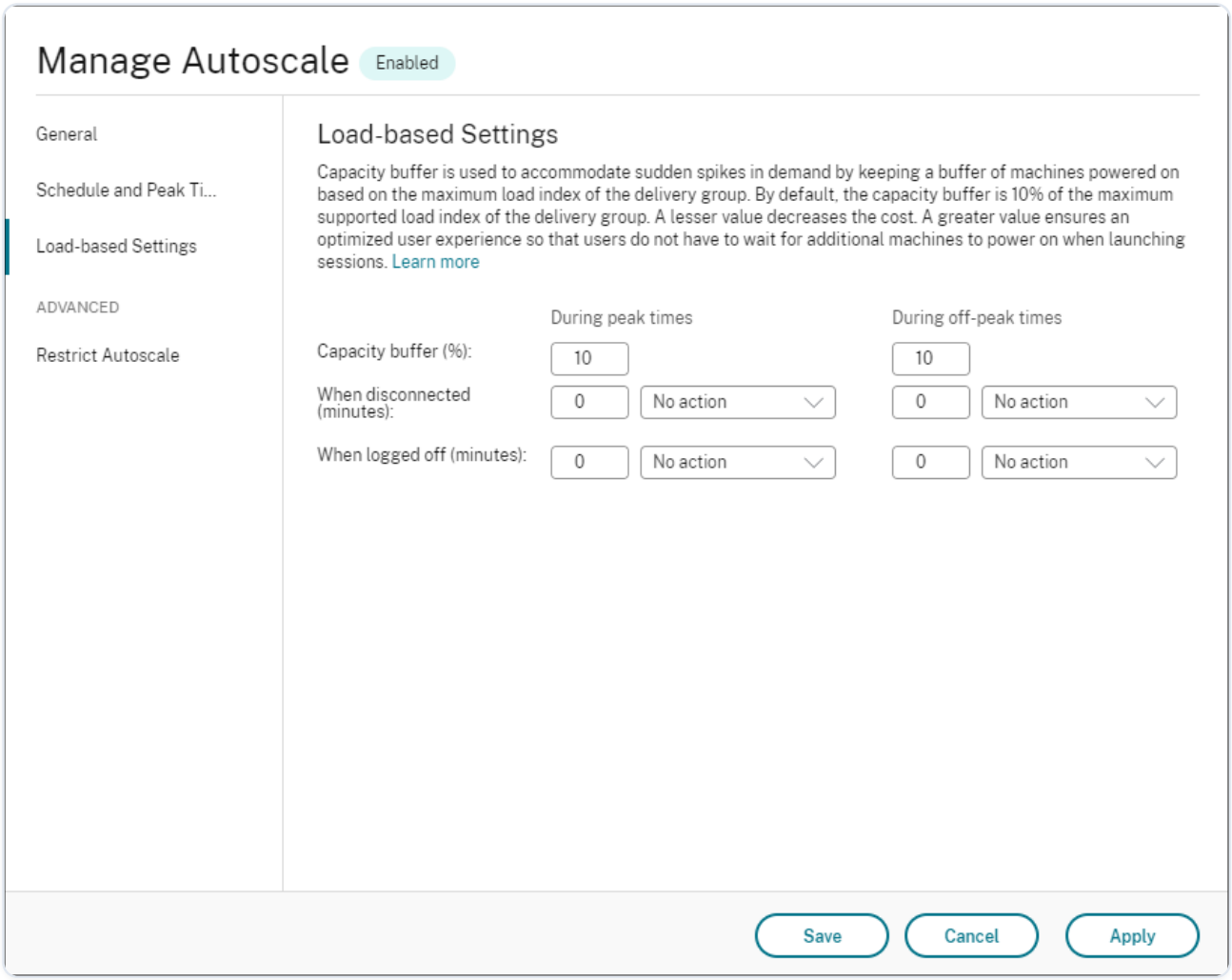
> **注：**
>
> Autoscaleは、サイトに登録されているマシンのみを、計算における利用可能な容量の一部として扱います。「登録済み」とは、マシンが使用可能であるか、すでに使用中であることを意味します。これにより、ユーザーセッションを受け入れられるマシンのみがデリバリーグループの容量に含まれるようになります。

ユーザーインターフェイス

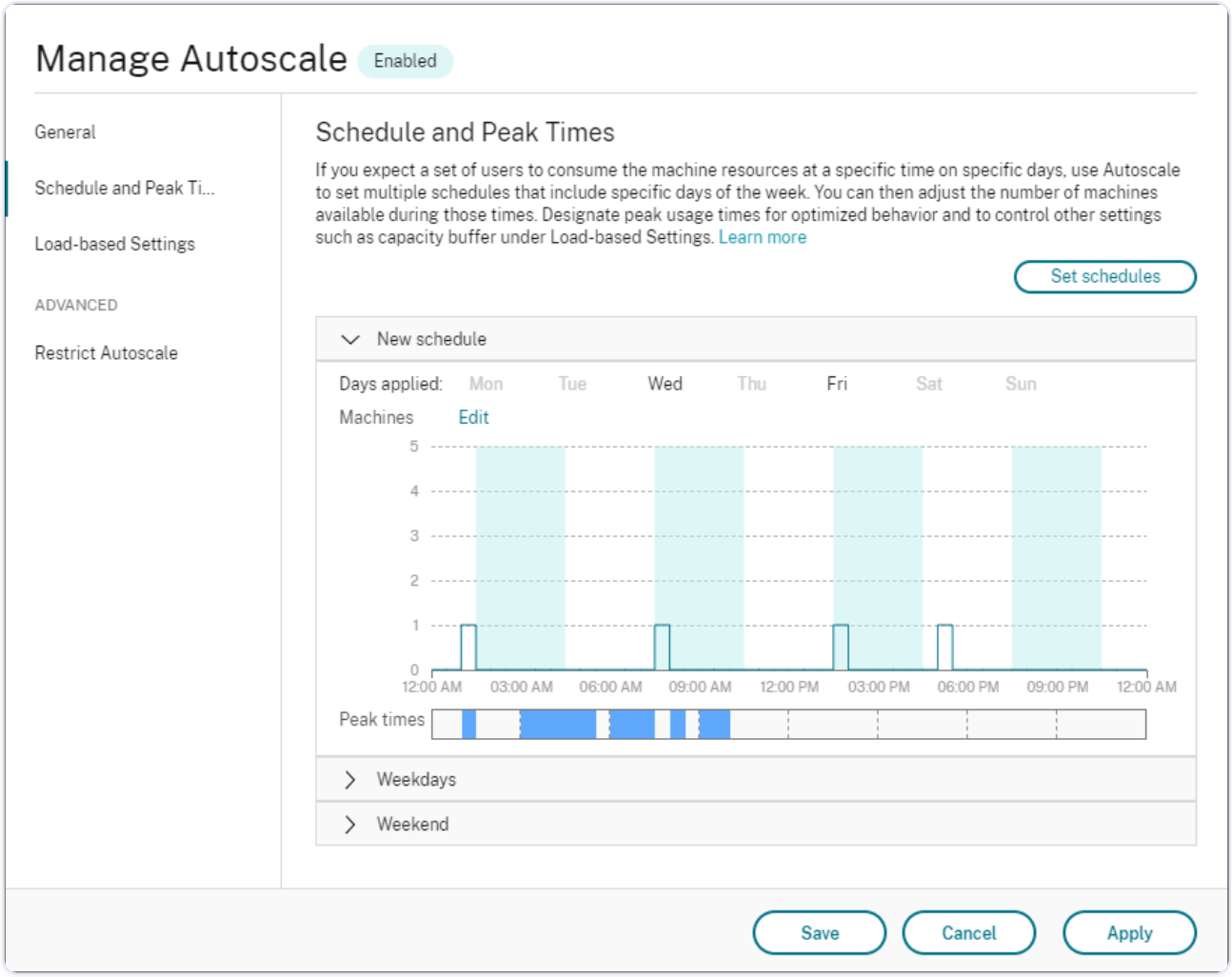
留意すべきユーザーインターフェイスは3種類あります。

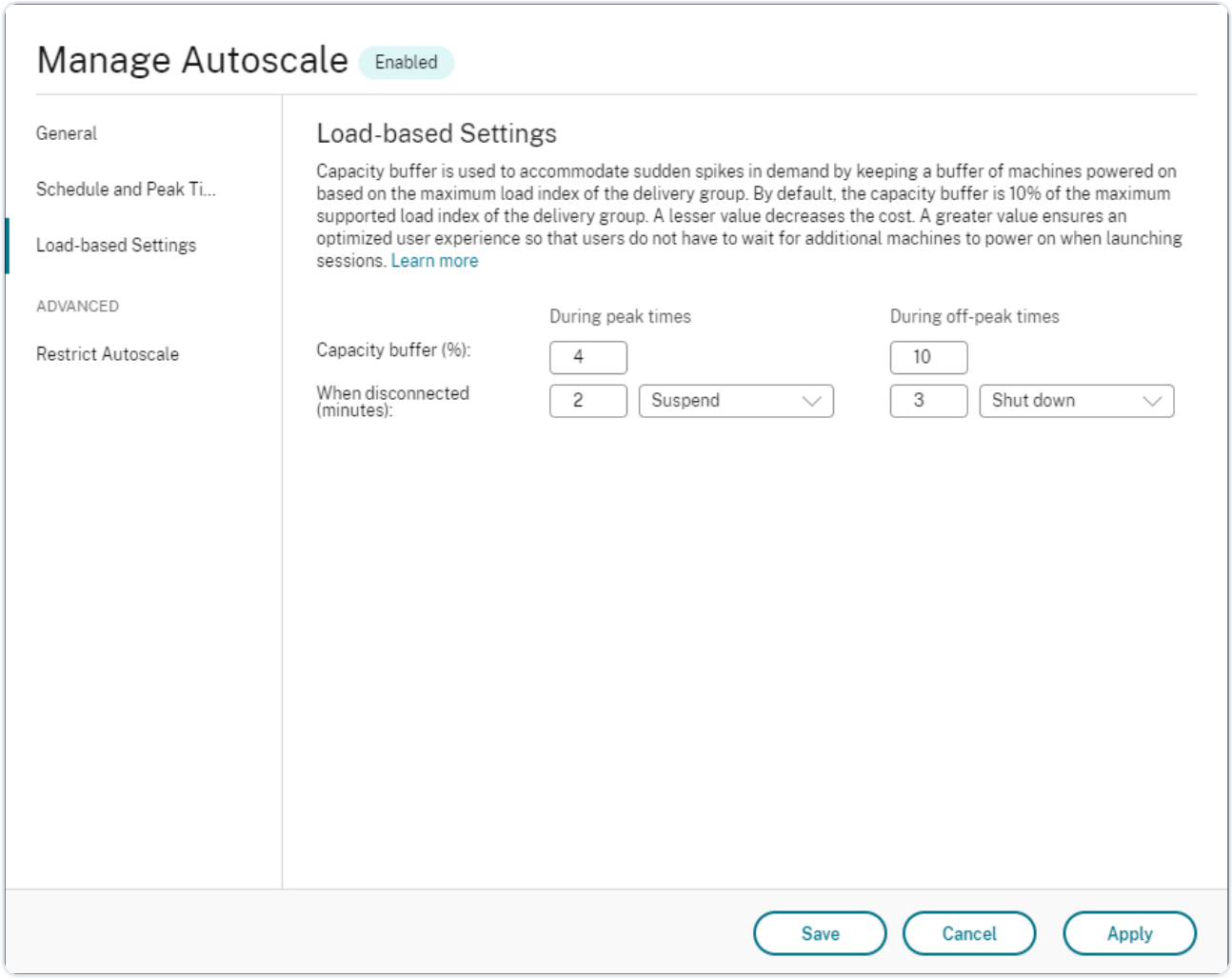
*シングルセッションOS静的デリバリーグループ*のユーザーインターフェイス：


Manage Autoscale
Enabled
General
Schedule and Peak Ti...
Load-based Settings
ADVANCED
Restrict Autoscale
Schedule and Peak Times
If you expect a set of users to consume the machine resources at a specific time on specific days, use Autoscale to set multiple schedules that include specific days of the week. You can then adjust the number of machines available during those times. Designate peak usage times for optimized behavior and to control other settings such as capacity buffer under Load-based Settings. Learn more
Set schedules
Weekdays
Days applied: Mon Tue Wed Thu Fri Sat Sun
Peak times
12:00 AM 3:00 AM 6:00 AM 9:00 AM 12:00 PM 3:00 PM 6:00 PM 9:00 PM 12:00 AM
Weekend
Save
Cancel
Apply

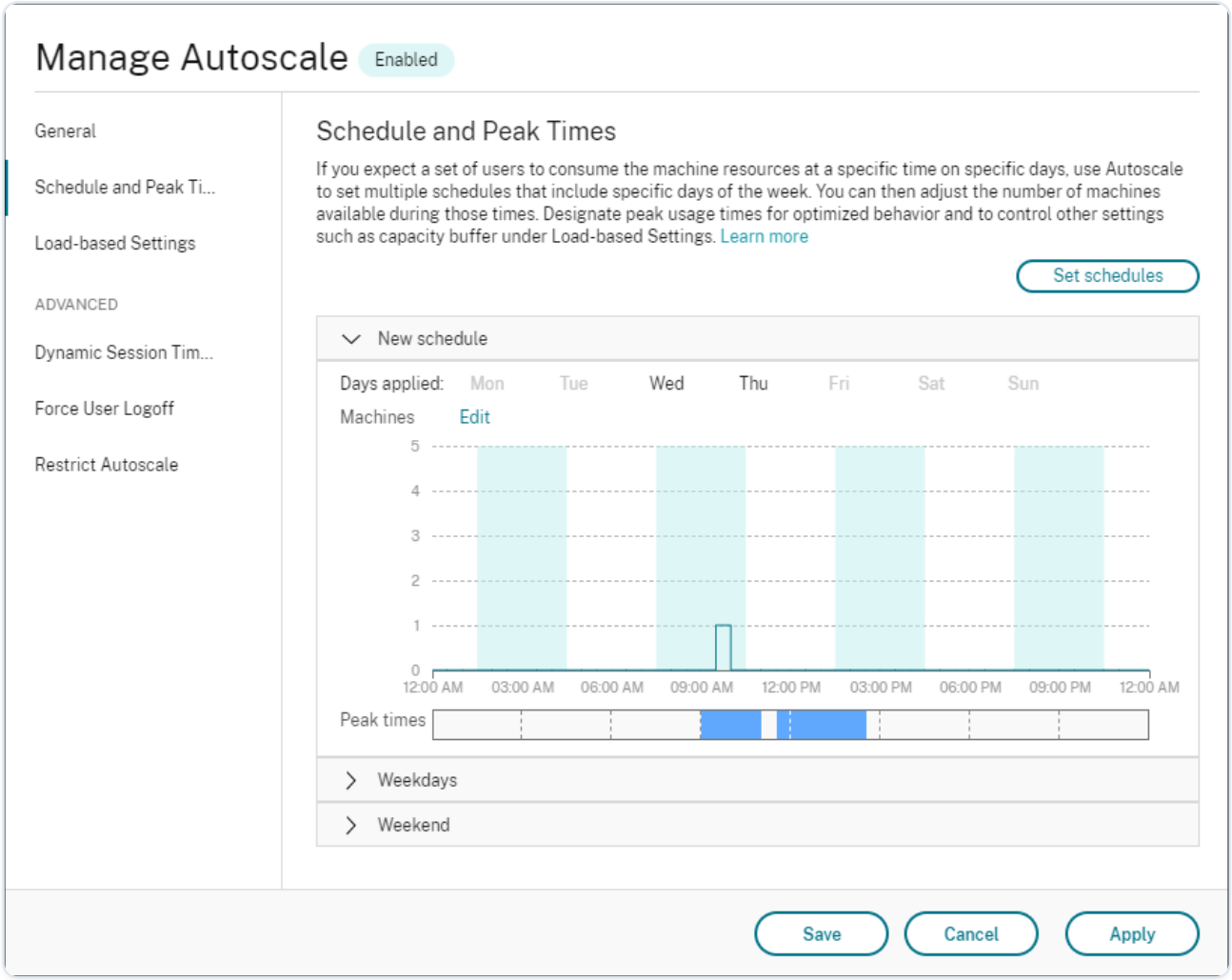


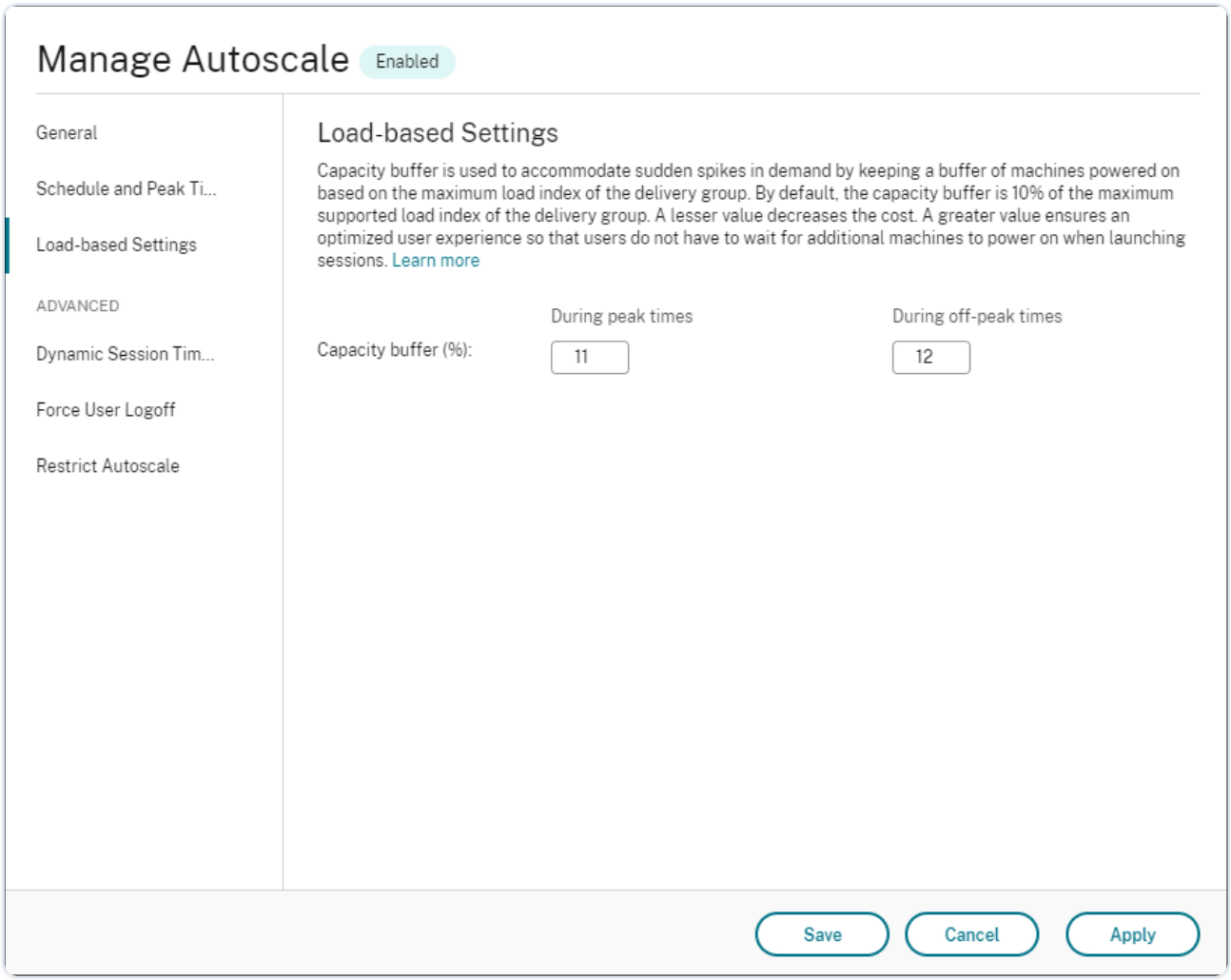
シングルセッションOSランダムデリバリーグループのAutoscaleユーザーインターフェイス：


Manage Autoscale
Enabled
General
Schedule and Peak Ti...
Load-based Settings
ADVANCED
Restrict Autoscale
Schedule and Peak Times
If you expect a set of users to consume the machine resources at a specific time on specific days, use Autoscale to set multiple schedules that include specific days of the week. You can then adjust the number of machines available during those times. Designate peak usage times for optimized behavior and to control other settings such as capacity buffer under Load-based Settings. Learn more
Set schedules
New schedule
Days applied: Mon Tue Wed Thu Fri Sat Sun
Machines Edit
5
4
3
2
1
0
12:00 AM 03:00 AM 06:00 AM 09:00 AM 12:00 PM 03:00 PM 06:00 PM 09:00 PM 12:00 AM
Peak times
Weekdays
Weekend
Save
Cancel
Apply



マルチセッションOSデリバリーグループのAutoscaleユーザーインターフェイス:


Manage Autoscale
Enabled
General
Schedule and Peak Ti...
Load-based Settings
ADVANCED
Dynamic Session Tim...
Force User Logoff
Restrict Autoscale
Schedule and Peak Times
If you expect a set of users to consume the machine resources at a specific time on specific days, use Autoscale to set multiple schedules that include specific days of the week. You can then adjust the number of machines available during those times. Designate peak usage times for optimized behavior and to control other settings such as capacity buffer under Load-based Settings. Learn more
Set schedules
New schedule
Days applied: Mon Tue Wed Thu Fri Sat Sun
Machines Edit
5
4
3
2
1
0
12:00 AM 03:00 AM 06:00 AM 09:00 AM 12:00 PM 03:00 PM 06:00 PM 09:00 PM 12:00 AM
Peak times
Weekdays
Weekend
Save
Cancel
Apply



スケジュールベースの設定

Autoscaleスケジュール。スケジュールの追加、編集、選択、削除が可能です。

適用日。選択したスケジュールに適用した日を強調表示します。残りの日はグレー表示されます。

編集。マシンを1時間ごとまたは30分ごとに割り当てることができます。マシンは数値またはパーセンテージで割り当てることができます。

> **注：**
>
> - このオプションは、マルチセッションOSおよびシングルセッションOSのランダムデリバリーグループ用のAutoscaleユーザーインターフェイスでのみ利用可能です。
> - **編集**の横にあるヒストグラムは、異なるタイムスロットで実行されているマシンの数または割合を示します。

- **ピーク時間**の上にある**編集**をクリックして、各タイムスロットに**マシンを割り当てる**ことができます。**起動するマシン**ウィンドウのメニューから選択したオプションに応じて、マシンを数値またはパーセンテージで割り当てることができます。
- マルチセッションOSデリバリーグループの場合、各日において30分単位で実行中のマシンの最小数を個別に設定できます。シングルセッションOSランダムデリバリーグループの場合、各日において60分単位で実行中のマシンの最小数を個別に設定できます。

独自のスケジュールを定義するには、次の手順に従います。

1. **Autoscaleの管理**ウィンドウの**スケジュールとピーク時間**ページで、**スケジュールを設定**をクリックします。
2. **Autoscaleスケジュールの編集**ウィンドウで、各スケジュールに適用する日を選択します。必要に応じてスケジュールを削除することもできます。
3. **完了**をクリックしてスケジュールを保存し、**スケジュールとピーク時間**ページに戻ります。
4. 該当するスケジュールを選択し、必要に応じて構成します。
5. **適用**をクリックして、**Autoscaleの管理**ウィンドウを終了するか、他のページで設定を構成します。

重要:

- Autoscaleでは、異なるスケジュールで同じ曜日が重複することはできません。たとえば、schedule1で月曜日を選択した後、schedule2で月曜日を選択すると、schedule1の月曜日は自動的にクリアされます。
- スケジュール名は大文字と小文字を区別しません。
- スケジュール名は空白にしたり、スペースのみを含めたりすることはできません。
- Autoscaleでは、文字間に空白スペースを入れることができます。
- スケジュール名には、次の文字を含めることはできません: \ / ; : # . * ? = < > \| ( ) { } " ' `。
- Autoscaleは重複するスケジュール名をサポートしていません。各スケジュールに異なる名前を入力してください。
- Autoscaleは空のスケジュールをサポートしていません。つまり、曜日が選択されていないスケジュールは保存されません。

> **注：**
>
> 選択したスケジュールに含まれる曜日は強調表示され、含まれない曜日はグレー表示されます。

負荷ベースの設定

ピーク時間。選択したスケジュールに適用した日のピーク時間を定義できます。これを行うには、横棒グラフを右クリックします。ピーク時間を定義すると、残りの未定義の時間はデフォルトでオフピーク時間になります。**デフォルト**では、選択したスケジュールに含まれる日のピーク時間として、午前7時から午後7時までの時間帯が定義されています。

> **重要:**
>
> - マルチセッションOSデリバリーグループの場合、ピーク時間の棒グラフは容量バッファに使用されます。
> - シングルセッションOSデリバリーグループの場合、ピーク時間の棒グラフは容量バッファに使用され、ログオフ後または切断後にトリガーされるアクションを制御します。
> - マルチセッションOSおよびシングルセッションOSデリバリーグループの両方で、スケジュールに含まれる日のピーク時間を30分単位で細かく定義できます。または、代わりに`New-BrokerPowerTimeScheme PowerShell`コマンドを使用することもできます。詳細については、「Broker PowerShell SDKコマンド」を参照してください。

キャパシティバッファー。稼働中のマシンのバッファーを維持できます。値が小さいほどコストが削減されます。値が大きいほど、セッション起動時にユーザーが追加のマシンの電源がオンになるのを待つ必要がなくなり、最適化されたユーザーエクスペリエンスが保証されます。デフォルトでは、ピーク時とオフピーク時のキャパシティバッファーは10%です。キャパシティバッファーを0に設定すると、セッション起動時にユーザーが追加のマシンの電源がオンになるのを待つ必要がある場合があります。Autoscaleでは、ピーク時とオフピーク時でキャパシティバッファーを個別に決定できます。

その他の設定

> **ヒント:**

- Broker PowerShell SDKを使用して、その他の設定を構成できます。詳しくは、「Broker PowerShell SDKコマンド」を参照してください。
- 切断時およびログオフ時の設定に関連するSDKコマンドについては、`<https://citrix.github.io/delivery-controller-sdk/Broker/about_Broker_PowerManagement/#power-policy>`を参照してください。

切断時。セッション切断後、切断されロックされたマシンが、中断またはシャットダウンされるまでにどのくらいの時間電源がオンのままになるかを指定できます。時間値を指定すると、構成したアクションに応じて、指定された切断時間が経過したときにマシンが中断またはシャットダウンされます。デフォルトでは、切断されたマシンにはアクションが割り当てられません。ピーク時とオフピーク時でアクションを個別に定義できます。そのためには、下矢印をクリックし、メニューから次のいずれかのオプションを選択します。

- **アクションなし**。選択すると、セッション切断後もマシンは電源がオンのままになります。Autoscaleはそれに対してアクションを実行しません。
- **中断**。選択すると、指定された切断時間が経過したときに、Autoscaleはマシンをシャットダウンせずに一時停止します。**中断**を選択すると、次のオプションが使用可能になります。
  - **再接続なしの場合（分）**。中断されたマシンは、切断されたユーザーが再接続する際には利用可能ですが、新しいユーザーには利用できません。すべてのワークロードを処理するためにマシンを再度利用可能にするには、シャットダウンします。Autoscaleがマシンをシャットダウンするまでのタイムアウトを分単位で指定します。
- **シャットダウン**。選択すると、指定された切断時間が経過したときに、Autoscaleはマシンをシャットダウンします。

注：

このオプションは、シングルセッションOSのランダムおよび静的デリバリーグループ用のAutoscaleユーザーインターフェイスでのみ使用できます。

ログオフ時。セッションログオフ後、マシンが中断またはシャットダウンされるまでにどのくらいの時間電源がオンのままになるかを指定できます。時間値を指定すると、構成したアクションに応じて、指定されたログオフ時間が経過したときにマシンが中断またはシャットダウンされます。デフォルトでは、ログオフされたマシンにはアクションが割り当てられま

せん。ピーク時とオフピーク時でアクションを個別に定義できます。そのためには、下矢印をクリックし、メニューから次のいずれかのオプションを選択します。

- **アクションなし**。選択すると、セッションログオフ後もマシンは電源がオンのままになります。Autoscaleはそれに対してアクションを実行しません。
- **中断**。選択すると、指定されたログオフ時間が経過したときに、Autoscaleはマシンをシャットダウンせずに一時停止します。
- **シャットダウン**。選択すると、指定されたログオフ時間が経過したときに、Autoscaleはマシンをシャットダウンします。

注：

このオプションは、シングルセッションOSの静的デリバリーグループ用のAutoscaleユーザーインターフェイスでのみ使用できます。

切断されたセッションを持つ、異なる時間帯に移行するシングルセッションOSマシンの電源管理

重要:

- この機能強化は、切断されたセッションを持つシングルセッションOSマシンにのみ適用されます。ログオフされたセッションを持つシングルセッションOSマシンには適用されません。
- この機能強化を有効にするには、該当するデリバリーグループでAutoscaleを有効にする必要があります。そうしないと、期間移行時に切断電源ポリシーアクションはトリガーされません。

以前のリリースでは、アクション（切断アクション = 「**一時停止**」または「**シャットダウン**」）が必要な時間帯に移行するシングルセッションOSマシンは、電源が入ったままでした。このシナリオは、マシンがアクション（切断アクション = 「**何もしない**」）が不要な時間帯（ピーク時またはオフピーク時）に切断された場合に発生しました。

このリリース以降、Autoscaleは、指定された切断時間が経過すると、移行先の時間帯に設定されている切断アクションに応じて、マシンを一時停止またはシャットダウンします。

例えば、シングルセッションOSデリバリーグループに対して、以下の電源ポリシーを設定します。

- `PeakDisconnectAction`を「Nothing」に設定します
- `OffPeakDisconnectAction`を「Shutdown」に設定します
- 「OffPeakDisconnectTimeout」を「10」に設定します

> **注：**
>
> 切断アクション電源ポリシーの詳細については、`<https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/about_Broker_PowerManagement/#power-policy>`および`<https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/Get-BrokerDesktopGroup/>`を参照してください。

> 以前のリリースでは、ピーク時にセッションが切断されたシングルセッションOSマシンは、ピークからオフピークに移行しても電源が入ったままでした。このリリース以降、期間移行時に`OffPeakDisconnectAction`および`OffPeakDisconnectTimeout`ポリシーアクションがシングルセッションOSマシンに適用されます。その結果、マシンはオフピークに移行してから10分後に電源がオフになります。

以前の動作（つまり、切断されたセッションを持つマシンがピークからオフピークへ、またはオフピークからピークへ移行しても何もしない）に戻したい場合は、次のいずれかを実行します。

- 「LegacyPeakTransitionDisconnectedBehaviour」レジストリ値を1（true; 以前の動作を有効にする）に設定します。デフォルトでは、値は0（false; 期間移行時に切断電源ポリシーアクションをトリガーする）です。
  - パス: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\DesktopServer
  - 名前: LegacyPeakTransitionDisconnectedBehaviour
  - 種類: REG_DWORD
  - データ: 0x00000001 (1)
- `Set-BrokerServiceConfigurationData` PowerShellコマンドを使用して設定を構成します。例:

- `PS C:\> Set-BrokerServiceConfigurationData HostingManagement.LegacyPeakTransitionDisconnectedBehaviour -SettingValue $true`

期間移行時に電源ポリシーアクションを適用する前に、マシンは次の基準を満たす必要があります。

- 切断されたセッションがあります。
- 保留中の電源操作がない。
- 異なる時間帯に移行するシングルセッションOSデリバリーグループに属している。
- 特定時間帯（ピーク時またはオフピーク時）にセッションが切断され、電源操作が割り当てられている期間に移行する。

容量バッファの仕組み

容量バッファは、動的な負荷増加に対応するために、現在の需要に予備容量を追加するために使用されます。注意すべき2つのシナリオがあります。

- マルチセッションOSデリバリーグループの場合、容量バッファは、ロードインデックスの観点からデリバリーグループの総容量の割合として定義されます。ロードインデックスの詳細については、「ロードインデックス」を参照してください。
- シングルセッションOSデリバリーグループの場合、容量バッファは、マシンの数の観点からデリバリーグループの総容量の割合として定義されます。

> **注：**

> Autoscaleをタグ付きマシンに制限するシナリオでは、容量バッファは、ロードインデックスの観点からデリバリーグループ内のタグ付きマシンの総容量の割合として定義されます。

> Autoscaleでは、ピーク時とオフピーク時で容量バッファを個別に設定できます。容量バッファフィールドの値が小さいほど、Autoscaleが起動する予備容量が少なくなるため、コストが削減されます。値が大きいほど、ユーザーはセッション起動時により多くのマシンが起動するのを待つ必要がなくなり、最適化されたユーザーエクスペリエンスが保証されます。デフォルトでは、容量バッファは10%です。

> **重要:**

容量バッファにより、総予備容量がデリバリーグループの総容量の「X」パーセントを下回るレベルに低下した場合にマシンが起動されます。これにより、必要な割合の予備容量が確保されます。

マルチセッションOSデリバリーグループ

マシンはいつ起動されますか?

重要:

スケジュールが選択されている場合、Autoscaleはスケジュールで起動するように構成されているすべてのマシンを起動します。Autoscaleは、負荷に関係なく、スケジュール中に指定された数のマシンを起動したままにします。

デリバリーグループ内の起動済みマシンの数が、ロードインデックスの観点からバッファ容量を維持するために必要なバッファを満たせなくなった場合、Autoscaleは追加のマシンを起動します。たとえば、デリバリーグループに20台のマシンがあり、スケジュールベースのスケーリングの一部として、容量バッファ20%で3台のマシンが起動するようにスケジュールされているとします。最終的に、負荷がない場合でも4台のマシンが起動されます。これは、バッファとして4 x 10kのロードインデックスが必要なため、少なくとも4台のマシンが起動される必要があるためです。このケースは、ピーク時、マシンの負荷増加、新しいセッションの起動、およびデリバリーグループに新しいマシンを追加する際に発生する可能性があります。Autoscaleは、次の条件を満たすマシンのみを起動することに注意してください。

- マシンがメンテナンスモードではない。
- マシンが実行されているハイパーバイザーがメンテナンスモードではない。
- マシンは現在電源オフの状態です。
- マシンに保留中の電源操作はありません。

マシンはいつ電源オフになりますか?

重要:

- スケジュールが選択されている場合、Autoscale はスケジュールに基づいてマシンの電源をオフにします。

- Autoscale は、スケジュール中に電源オンになるようにスケジュールで構成されたマシンの電源をオフにしません。

デリバリーグループのターゲットとなる電源オン状態のマシン数（バッファを含む）をサポートするのに十分すぎるほどのマシンがある場合、Autoscale は余分なマシンの電源をオフにします。このケースは、オフピーク時、マシンの負荷が減少したとき、セッションログオフ時、およびデリバリーグループからマシンを削除したときに発生する可能性があります。Autoscale は、以下の条件を満たすマシンのみ電源をオフにします。

- マシンと、マシンが実行されているハイパーバイザーがメンテナンスモードではありません。
- マシンは現在電源オンの状態です。
- マシンは利用可能として登録されているか、起動後に登録を待機しています。
- マシンにアクティブなセッションはありません。
- マシンに保留中の電源操作はありません。
- マシンは指定された電源オフ遅延を満たしています。これは、マシンが少なくとも「X」分間電源オンの状態であったことを意味します。「X」はデリバリーグループに指定された電源オフ遅延です。

例のシナリオ

次のシナリオを想定します。

- **デリバリーグループの構成**。Autoscale で電源管理するデリバリーグループには、10台のマシン（M1～M10）が含まれています。
- **Autoscale の構成**
  - キャパシティバッファは10%に設定されています。
  - 選択されたスケジュールにはマシンが含まれていません。

シナリオは次の順序で実行されます。

1. ユーザーはログオンしません。
2. ユーザーセッションが増加します。
3. より多くのユーザーセッションが開始されます。
4. セッション終了により、ユーザーセッションの負荷が減少します。
5. セッション負荷がオンプレミスリソースのみで処理されるまで、ユーザーセッションの負荷はさらに減少します。

上記のシナリオでAutoscaleがどのように機能するかについては、以下を参照してください。

- ユーザー負荷なし（初期状態）
  - 1台のマシン（例: M1）が電源オンになります。このマシンは、構成されたキャパシティバッファのために電源オンになります。この場合、10（マシン数）x 10,000（負荷インデックス）x 10%（構成されたキャパシティバッファ）は10,000に等しくなります。したがって、1台のマシンが電源オンになります。
  - 電源オンになったマシン（M1）の負荷インデックス値は、ベースライン負荷（負荷インデックスは0）です。
- 最初のユーザーがログオンします
  - セッションはマシンM1でホストされるように指示されます。
  - 電源オンになったマシンM1の負荷インデックスが増加し、マシンM1はベースライン負荷ではなくなります。
  - 構成されたキャパシティバッファにより、Autoscale は需要を満たすために追加のマシン (M2) の電源をオンにし始めます。
  - マシン M2 の負荷インデックス値はベースライン負荷にあります。
- ユーザーが負荷を増加させます
  - セッションはマシン M1 と M2 の間で負荷分散されます。その結果、起動中のマシン (M1 と M2) の負荷インデックスが増加します。
  - 総予備容量は、負荷インデックスの観点から依然として 10,000 を超えるレベルにあります。
  - マシン M2 の負荷インデックス値はもはやベースライン負荷ではありません。
- より多くのユーザーセッションが開始されます
  - セッションはマシン (M1 と M2) の間で負荷分散されます。その結果、起動中のマシン (M1 と M2) の負荷インデックスがさらに増加します。
  - 負荷インデックスの観点から総予備容量が 10,000 を下回るレベルに低下すると、Autoscale は構成されたキャパシティバッファにより、需要を満たすために追加のマシン (M3) の電源をオンにし始めます。
  - マシン M3 の負荷インデックス値はベースライン負荷にあります。
- さらに多くのユーザーセッションが開始されます

    - セッションはマシン (M1 から M3) の間で負荷分散されます。その結果、起動中のマシン (M1 から M3) の負荷インデックスが増加します。
    - 総予備容量は、負荷インデックスの観点から 10,000 を超えるレベルにあります。
    - マシン M3 の負荷インデックス値はもはやベースライン負荷ではありません。

- セッション終了によりユーザーセッションの負荷が減少します
    - ユーザーがセッションからログオフするか、アイドルセッションがタイムアウトすると、M1からM3までのマシンで解放された容量が、他のユーザーが開始したセッションをホストするために再利用されます。
    - ロードインデックスの観点から総予備容量が10,000を超えるレベルに増加すると、Autoscaleはマシンの1つ（たとえばM3）をドレイン状態にします。その結果、新しい変更が発生しない限り、他のユーザーが開始したセッションはそのマシンに転送されなくなります。たとえば、エンドユーザーの負荷が再び増加したり、他のマシンの負荷が最も低くなったりした場合です。
- ユーザーセッションの負荷は減少し続けます
    - マシンM3上のすべてのセッションが終了し、指定された電源オフ遅延がタイムアウトすると、AutoscaleはマシンM3の電源をオフにします。
    - さらに多くのユーザーがセッションを終了すると、電源がオンになっているマシン（M1とM2）で解放された容量が、他のユーザーが開始したセッションをホストするために再利用されます。
    - ロードインデックスの観点から総予備容量が10,000を超えるレベルに増加すると、Autoscaleはマシンの1つ（たとえばM2）をドレイン状態にします。その結果、他のユーザーが開始したセッションはそのマシンに転送されなくなります。
- セッションがなくなるまでユーザーセッションの負荷は減少し続けます
    - マシンM2上のすべてのセッションが終了し、指定された電源オフ遅延がタイムアウトすると、AutoscaleはマシンM2の電源をオフにします。
    - 電源がオンになっているマシン（M1）のロードインデックス値はベースライン負荷です。構成された容量バッファーのため、AutoscaleはマシンM1をドレイン状態にしません。

> **注：**

> マルチセッションOSデリバリーグループの場合、ユーザーがセッションからログオフすると、デスクトップへのすべての変更は失われます。ただし、構成されている場合、ユーザー固有の設定はユーザープロファイルとともにローミングされます。

シングルセッションOSランダムデリバリーグループ

容量バッファーは、デリバリーグループ内のマシンの総数に基づいて、電源がオンになっているマシンのバッファーを維持することで、需要の急増に対応するために使用されます。デフォルトでは、容量バッファーはデリバリーグループ内のマシンの総数の10%です。

マシンの数（容量バッファーを含む）が現在電源がオンになっているマシンの総数を超える場合、需要を満たすために追加のマシンの電源がオンになります。マシンの数（容量バッファーを含む）が現在電源がオンになっているマシンの総数よりも少ない場合、余分なマシンは、構成したアクションに応じてシャットダウンまたは中断されます。

例のシナリオ

次のシナリオを想定します。

- **デリバリーグループの構成**。Autoscaleで電源管理するデリバリーグループには、10台のマシン（M1～M10）が含まれています。
- **Autoscaleの構成**
  - 容量バッファは10%に設定されています。
  - 選択されたスケジュールにはマシンが含まれていません。

シナリオは次の順序で実行されます。

1. ユーザーはログオンしません。
2. ユーザーセッションが増加します。
3. さらに多くのユーザーセッションが開始されます。
4. セッション終了により、ユーザーセッションの負荷が減少します。
5. オンプレミスリソースのみでセッション負荷が処理されるまで、ユーザーセッションの負荷はさらに減少します。

上記のシナリオでAutoscaleがどのように機能するかについては、以下を参照してください。

- ユーザー負荷なし（初期状態）

    - 1台のマシン（M1）が電源オンになります。このマシンは、構成された容量バッファのために電源オンになります。この場合、10（マシンの数）x 10%（構成された容量バッファ）は1に等しくなります。したがって、1台のマシンが電源オンになります。

- 最初のユーザーがログオンします
    - ユーザーがデスクトップを使用するために初めてログオンすると、電源オンになっているマシンでホストされているデスクトップのプールからデスクトップが割り当てられます。この場合、ユーザーにはマシンM1からデスクトップが割り当てられます。
    - Autoscaleは、構成された容量バッファのために需要を満たすために、追加のマシン（M2）の電源をオンにし始めます。
- 2番目のユーザーがログオンします
    - ユーザーにはM2マシンからデスクトップが割り当てられます。
    - 設定されたキャパシティバッファにより需要を満たすため、Autoscaleは追加のマシン（M3）の電源をオンにし始めます。
- 3人目のユーザーがログオンします
    - ユーザーにはM3マシンからデスクトップが割り当てられます。
    - 設定されたキャパシティバッファにより需要を満たすため、Autoscaleは追加のマシン（M4）の電源をオンにし始めます。
- ユーザーがログオフします
    - ユーザーがログオフするか、ユーザーのデスクトップがタイムアウトすると、解放された容量（例：M3）がバッファとして利用可能になります。その結果、キャパシティバッファが10%に設定されているため、AutoscaleはM4マシンの電源をオフにし始めます。
- ユーザーがいなくなるまで、さらに多くのユーザーがログオフします
    - さらに多くのユーザーがログオフした後、Autoscaleはマシン（例：M2またはM3）の電源をオフにします。
    - ユーザーが残っていなくても、そのマシンは予備容量として予約されているため、Autoscaleは残りの1台のマシン（例：M1）の電源をオフにしません。

> **注：**

> シングルセッションOSのランダムデリバリーグループの場合、ユーザーがセッションをログオフすると、デスクトップへのすべての変更は失われます。ただし、設定されている場合、ユーザー固有の設定はユーザープロファイルとともにローミングされます。

シングルセッションOSの静的デリバリーグループ

キャパシティバッファは、デリバリーグループ内の未割り当てマシンの総数に基づいて、未割り当てマシンのバッファの電源をオンに保つことで、急な需要の急増に対応するために使用されます。デフォルトでは、キャパシティバッファはデリバリーグループ内の未割り当てマシンの総数の10%です。

> **重要:**
>
> デリバリーグループ内のすべてのマシンが割り当てられた後、キャパシティバッファはマシンの電源オン/オフには関与しません。

> マシンの数（キャパシティバッファを含む）が現在電源がオンになっているマシンの総数を超える場合、需要を満たすために追加の未割り当てマシンが電源オンになります。マシンの数（キャパシティバッファを含む）が現在電源がオンになっているマシンの総数よりも少ない場合、設定したアクションに応じて、余分なマシンは電源オフまたは一時停止されます。

シングルセッションOS静的デリバリーグループの場合、Autoscaleは次のようになります。

- 適用されるシングルセッションOSデリバリーグループの`AutomaticPowerOnForAssigned`プロパティがtrueに設定されている場合にのみ、ピーク時に割り当てられたマシンをオンにし、オフピーク時にオフにします。
- マシンがオフになっていて、そのマシンが属するデリバリーグループの`AutomaticPowerOnForAssignedDuringPeak`プロパティがtrueに設定されている場合、ピーク時に自動的にマシンをオンにします。

割り当てられたマシンで容量バッファがどのように機能するかを理解するには、以下を考慮してください。

- 容量バッファは、デリバリーグループに1台以上の未割り当てのマシンがある場合にのみ機能します。
- デリバリーグループに未割り当てのマシンがない場合（デリバリーグループ内のすべてのマシンが割り当てられている場合）、容量バッファはマシンの電源オン/オフには関与しません。

- `AutomaticPowerOnForAssignedDuringPeak`プロパティは、ピーク時に割り当てられたマシンの電源がオンになるかどうかを決定します。trueに設定されている場合、Autoscaleはピーク時にマシンの電源をオンのままにします。Autoscaleは、電源がオフになっている場合でも、それらの電源をオンにします。

例のシナリオ

次のシナリオを想定します。

- **デリバリーグループの構成**。Autoscaleで電源管理したいデリバリーグループには、10台のマシン（M1～M10）が含まれています。
- **Autoscaleの構成**
  - M1からM3までのマシンは割り当て済みで、M4からM10までのマシンは未割り当てです。
  - ピーク時およびオフピーク時のキャパシティバッファは10%に設定されています。
  - 選択されたスケジュールに従って、Autoscaleは午前9時から午後6時までマシンの電源を管理します。

上記のシナリオでAutoscaleがどのように機能するかについては、以下を参照してください。

- スケジュールの開始 – 午前9時
  - AutoscaleはマシンM1からM3の電源をオンにします。
  - 設定されたキャパシティバッファのため、Autoscaleは追加のマシン（例：M4）の電源をオンにします。マシンM4は未割り当てです。
- 最初のユーザーがログオンします
  - ユーザーがデスクトップを使用するために初めてログオンすると、未割り当ての電源オン状態のマシンでホストされているデスクトップのプールからデスクトップが割り当てられます。この場合、ユーザーにはマシンM4からデスクトップが割り当てられます。そのユーザーによるその後のログオンは、初回使用時に割り当てられた同じデスクトップに接続されます。
  - 設定されたキャパシティバッファのため、Autoscaleは需要を満たすために追加のマシン（例：M5）の電源をオンにし始めます。
- 2番目のユーザーがログオンします
  - ユーザーには、未割り当ての電源オン状態のマシンからデスクトップが割り当てられます。この場合、ユーザーにはマシンM5からデスクトップが割り当てられます。そのユー

ザーによるその後のログオンは、初回使用時に割り当てられた同じデスクトップに接続されます。

- 設定されたキャパシティバッファのため、Autoscaleは需要を満たすために追加のマシン（例：M6）の電源をオンにし始めます。

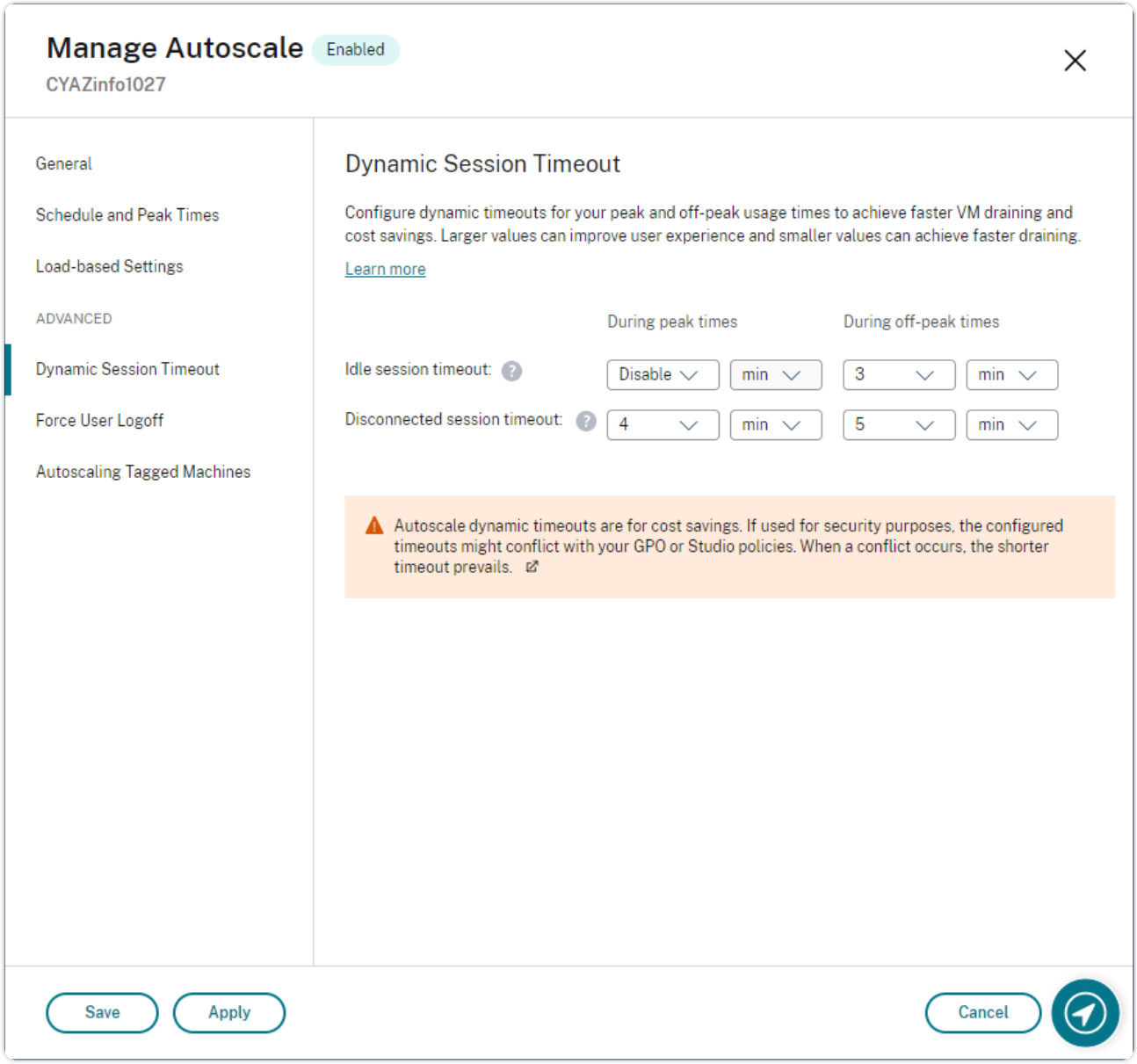
- ユーザーがログオフします
  - ユーザーがデスクトップからログオフするか、デスクトップがタイムアウトすると、Autoscaleは午前9時から午後6時までマシンM1からM5の電源をオンのままにします。それらのユーザーが次回ログオンするときは、初回使用時に割り当てられた同じデスクトップに接続されます。
  - 割り当てられていないマシン M6 は、新しく割り当てられていないユーザーにデスクトップを提供するのを待機しています。
- スケジュールの終了 – 午後 6 時
  - 午後 6 時に、Autoscale はマシン M1 から M5 の電源をオフにします。
  - Autoscale は、構成された容量バッファのため、割り当てられていないマシン M6 の電源をオンのままにします。そのマシンは、新しく割り当てられていないユーザーにデスクトップを提供するのを待機しています。
  - デリバリーグループでは、マシン M6 から M10 は割り当てられていないマシンです。

動的セッションタイムアウト

この機能を使用すると、ピーク時とオフピーク時の使用時間に合わせて切断セッションとアイドルセッションのタイムアウトを設定し、マシンのドレインを高速化してコストを削減できます。この機能は以下に適用されます。

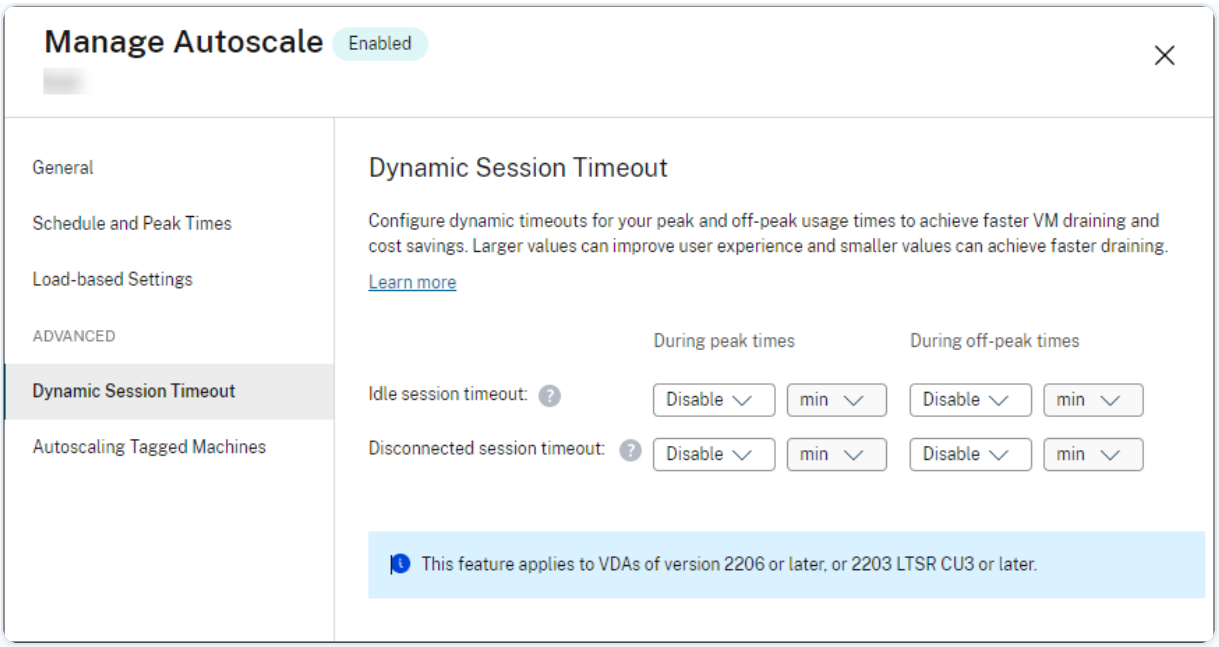
- シングルセッションおよびマルチセッションOSマシン。
- オートスケール用にタグ付けされているかどうかにかかわらず、デリバリーグループ内のすべてのマシン。

VDAは、10分以上アイドル状態のセッションのアイドル時間を報告するため、動的セッションタイムアウトは、アイドル状態になってから10分以内にアイドルセッションを切断することはできません。値を小さくすると、残存するセッションがより早く削除され、コストが削減されます。



注：

- この機能は、マルチセッションOSデリバリーグループで常に利用可能です。
- シングルセッションOSデリバリーグループの場合、この機能はバージョン2206 CR以降、または2203 LTSR CU3以降のVDAに適用されます。これらのVDAがCitrix Cloud™に少なくとも1回登録されていることを確認してください。利用できない場合、次のユーザーインターフェイスが表示されます。



- Autoscale™の動的タイムアウトはコスト削減を目的としています。セキュリティ目的で使用する場合、設定されたタイムアウトがGPOまたは管理コンソールポリシーと競合する可能性があります。競合が発生した場合、短い方のタイムアウトが優先されます。

アイドルセッションタイムアウト。ユーザー入力がない場合に、中断されていないユーザー接続が維持される時間を指定するタイマーを有効または無効にします。タイマーが期限切れになると、セッションは切断状態になり、**切断セッションタイムアウト**が適用されます。**切断セッションタイムアウト**が無効になっている場合、セッションはログオフされません。

重要:

- 10分（600秒）以下の値を指定した場合、Autoscaleは関連するセッションが10分間アイドル状態になった後に切断します。これは、AutoscaleがVDAが報告するセッションのアイドル時間に依存しているためです。VDAは、10分以上アイドル状態のセッションに対してのみアイドル時間を報告します。
- アイドルセッションは、アイドルセッションタイムアウトに達するまでの最後の5分以内にユーザーが操作した場合でも、切断状態になることがあります。

> **切断セッションタイムアウト**。切断されたデスクトップがログオフされるまでロックされたままになる時間を指定するタイマーを有効または無効にします。有効になっている場合、タイマーが期限切れになると切断されたセッションはログオフされます。

よくある質問

動的セッションタイムアウト機能は、オートスケール用にタグ付けされたマシンにのみ適用されます?

動的セッションタイムアウト機能は、オートスケール用にタグ付けされているかどうかにかかわらず、デリバリーグループ内のすべてのマシンに適用されます。

動的セッションタイムアウトによりセッションがログオフされた場合、タグ付けされていないマシンも、タグ付けされたマシンのオートスケールターゲットに含まれます?

動的セッションタイムアウト機能は、オートスケールのタグ付け機能とは関係ありません。動的セッションタイムアウトによってセッションが終了した場合、マシンがシャットダウンまでドレインされている限り、タグ付けされていないマシンもその過程でシャットダウンされる可能性があります。

タグ付けされたマシンのオートスケール (クラウドバースト)

> **注：**
>
> この機能は以前、Restrict Autoscale と呼ばれていました。

はじめに

Autoscaleは、デリバリーグループ内のマシンの一部のみを電源管理する柔軟性を提供します。これを実現するには、1つ以上のマシンにタグを適用し、その後、Autoscaleを構成してタグ付きマシンのみを電源管理します。

この機能は、クラウドベースのリソースが追加の需要 (つまり、バーストワークロード) に対応する前に、オンプレミスリソース (または予約済みのパブリッククラウドインスタンス) を使用してワークロードを処理したいクラウドバーストのユースケースで役立ちます。オンプレミスのマシン (または予約済みインスタンス) に最初にワークロードを処理させるには、タグ制限とゾーン優先度を併用する必要があります。

タグ制限は、Autoscale によって電源管理されるマシンを指定します。ゾーン優先度は、ユーザー起動要求を処理する優先ゾーン内のマシンを指定します。詳細については、「タグ」および「ゾーン優先度」を参照してください。

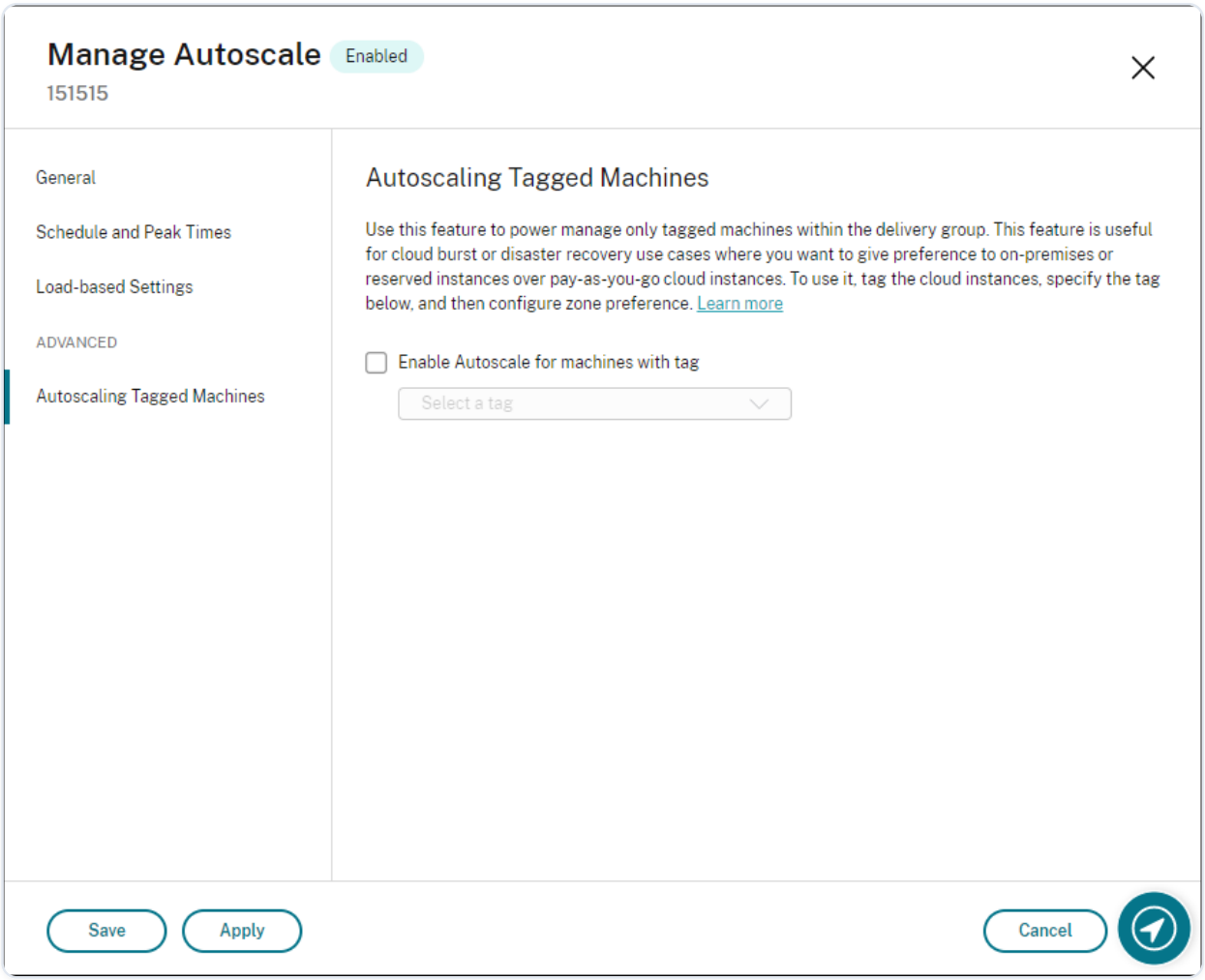
特定のタグ付きマシンをオートスケールするには、Manage コンソールまたは PowerShell を使用できます。

Manage コンソールを使用して特定のタグ付きマシンをオートスケールする

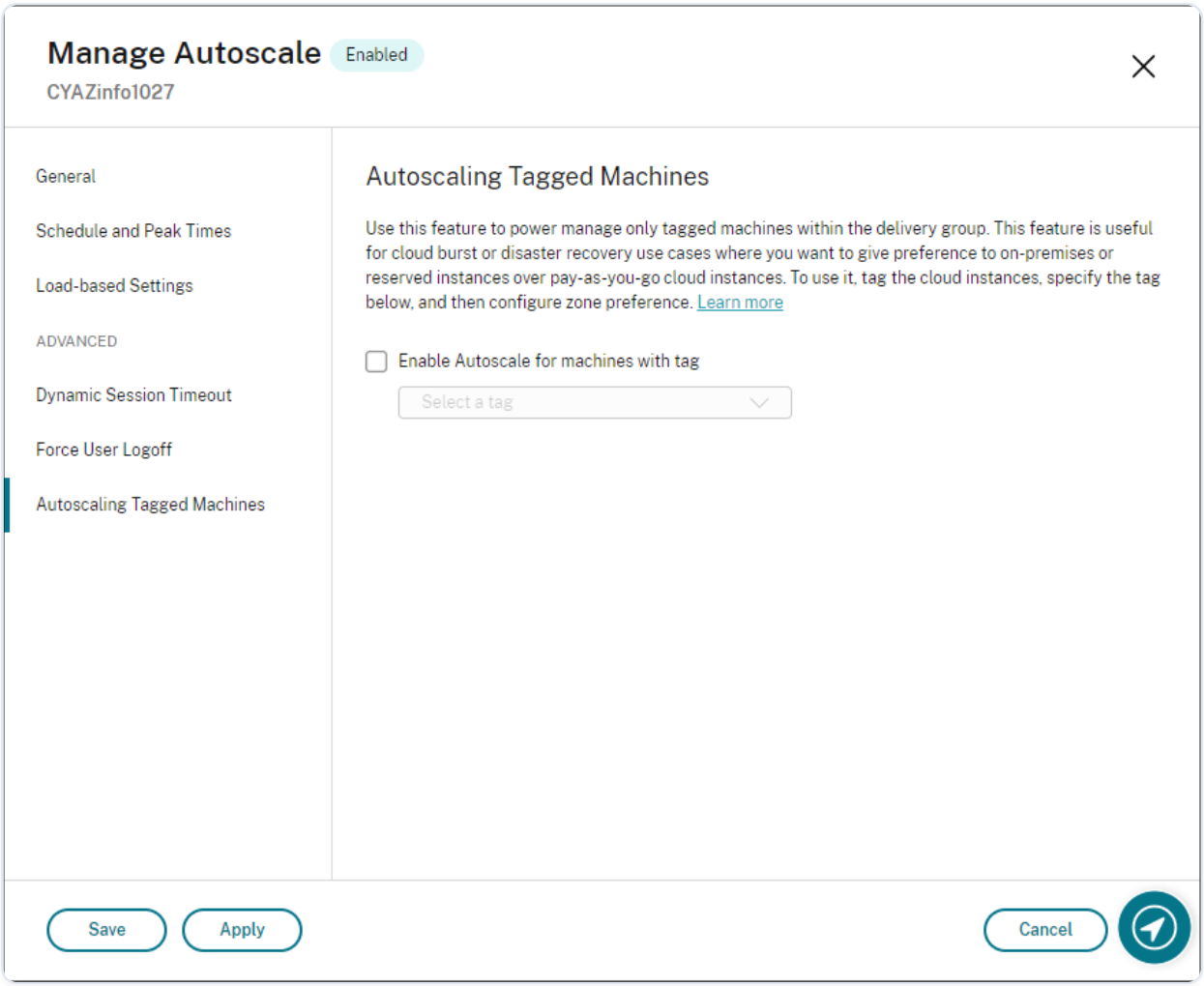
特定のタグ付きマシンをオートスケールするには、次の手順を実行します。

1. タグを作成し、そのタグをデリバリーグループ内の該当するマシンに適用します。詳細については、「タグとタグ制限の管理」を参照してください。
2. デリバリーグループを選択し、**Manage Autoscale** ウィザードを開きます。
3. **タグ付きマシンのオートスケール**ページで、**タグ付きマシンのオートスケールを有効にする**を選択し、リストからタグを選択して、**適用**をクリックして変更を保存します。

   シングルセッションOSの*静的*および*ランダム*なデリバリーグループのユーザーインターフェイス:



マルチセッションOSデリバリーグループのユーザーインターフェイス:



警告:

- 特定のタグを持つマシンをオートスケールすると、ヒストグラムが自動的に更新され、タグごとのマシンの数が反映される場合があります。**スケジュールとピーク時間**ページで、必要に応じて、各時間帯にマシンを手動で割り当てることができます。
- タグ付けされたマシンで使用されているタグは削除できません。タグを削除するには、まずタグの制限を解除する必要があります。

タグの制限を適用した後、後でデリバリーグループから削除したい場合があります。そのためには、**Autoscaleの管理 > タグ付けされたマシンのAutoscale**ページに移動し、**タグ付きマシンのAutoscaleを有効にする**のチェックを外します。

警告:

- **タグ付きマシンのAutoscaleを有効にする**のチェックを外さずに、該当するマシンからタグを削除すると、**Autoscaleの管理**ウィザードを開いたときに警告が表示されることがあります。マシンからタグを削除すると、Autoscaleで指定したタグが無効になるため、Autoscaleが管理するマシンがなくなる可能性があります。この警告を解決するには、**タグ付けされたマシンのAutoscale**ページに移動し、無効なタグを削除してから、**適用**をクリックして変更を保存します。

Autoscaleがリソースの電源をオンにするタイミングを制御する

タグ付けされていないマシンの使用状況に基づいて、Autoscaleがタグ付けされたマシンの電源をオンにし始めるタイミングを制御することもできます。これにより、タグ付けされたワークロードまたはパブリッククラウドワークロードの消費をさらに最適化できます。

これを行うには、次の手順を完了します。

1. **タグ付けされたマシンのAutoscale**ページで、**Autoscaleがタグ付けされたマシンの電源をオンにし始めるタイミングを制御する**を選択します。
2. ピーク時とオフピーク時の両方で到達させたいタグ付けされていないマシンの使用率をパーセンテージで入力し、**適用**をクリックします。サポートされる値: 0〜100。

Autoscaleがタグ付けされたマシンの電源をオンにし始めるタイミングを制御する(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/autoscale-powers-on-tagged-machines.png)

ヒント:

このパーセンテージは、Autoscaleがタグ付けされたマシンの電源をオンにし始めるタイミングを制御します。パーセンテージがしきい値（デフォルトは10%）を下回ると、Autoscaleはタグ付けされたマシンの電源をオンにし始めます。パーセンテージがしきい値を超えると、Autoscaleは電源オフモードになります。パーセンテージを入力する際は、次の2つのシナリオを考慮してください。

- シングルセッションOSデリバリーグループの場合: この値は、アイドル状態のタグ付けされていないマシンの総数に対するパーセンテージとして定義されます。例: タグ付けさ

れていないシングルセッションOSマシンが10台あります。セッションがないマシンが1台だけになったときに、Autoscaleはタグ付けされたマシンの電源をオンにし始めます。

- マルチセッションOSデリバリーグループの場合: この値は、利用可能なタグ付けされていないマシンの総容量（負荷インデックスの観点から）に対するパーセンテージとして定義されます。例: タグ付けされていないマルチセッションOSマシンが10台あります。それらが90%ロードされたときに、Autoscaleはタグ付けされたマシンの電源をオンにし始めます。

PowerShellを使用して特定のタグ付けされたマシンをAutoscaleする

PowerShell SDKを直接使用するには、次の手順を完了します。

1. **タグを作成します。** New-Brokertag PowerShellコマンドを使用してタグを作成します。
   - 例: `$managed = New-BrokerTag Managed`。この場合、タグ名は「Managed」です。New-Brokertag PowerShellコマンドの詳細については、`<https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/New-BrokerTag/>`を参照してください。
2. **タグをマシンに適用します。**Get-Brokermachine PowerShellコマンドを使用して、Autoscaleで電源管理するカタログ内のマシンにタグを適用します。
   - 例: `Get-BrokerMachine -CatalogName "cloud" | Add-BrokerTag $managed.Name`。この場合、カタログ名は「cloud」です。
   - Get-Brokermachine PowerShellコマンドの詳細については、`<https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/Get-BrokerMachine/>`を参照してください。

注：

タグを適用した後で、新しいマシンをカタログに追加する場合があります。その場合、タグは新しいマシンに自動的に適用*されません*。

3. **タグ付けされたマシンを、Autoscaleで電源管理するデリバリーグループに追加します。** Get-BrokerDesktopGroup PowerShellコマンドを使用して、マシンを含むデリバリーグループにタグ制限を追加します（つまり、「タグXを持つマシンへの起動を制限する」）。

- 例: `Get-BrokerDesktopGroup -Uid 1 | Set-BrokerDesktopGroup -RestrictAutoscaleTagUid $managed.Uid`。この場合、デリバリーグループのUIDは1です。
- Get-BrokerDesktopGroup PowerShellコマンドの詳細については、`<https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/Get-BrokerDesktopGroup/>`を参照してください。

タグ制限を適用した後、後でデリバリーグループから削除したい場合があります。その場合は、Get-BrokerDesktopGroup PowerShellコマンドを使用します。

例: `Get-BrokerDesktopGroup –Uid 1 | Set-BrokerDesktopGroup –RestrictAutoscaleTagUid $null`。この場合、デリバリーグループのUIDは1です。

> **注：**
>
> タグ付けされていないマシンは、ユーザーが電源を切った後に自動的に再起動します。この動作により、ワークロードをより早く処理できるようになります。これは、`Set-BrokerDesktopGroup`の`AutomaticRestartForUntaggedMachines`プロパティを使用して、デスクトップグループごとに有効または無効にできます。詳細については、`<https://citrix.github.io/delivery-controller-sdk/Broker/Set-BrokerDesktopGroup/>`を参照してください。

例のシナリオ

次のシナリオを想定します。

- **マシンカタログの構成**。2つのマシンカタログ（C1とC2）があります。
  - カタログC1には、オンプレミス展開でローカルにある5台のマシン（M1～M5）が含まれています。
  - カタログC2には、クラウド展開でリモートにある5台のマシン（M6～M10）が含まれています。
- **タグの制限**。「Cloud」という名前のタグが作成され、カタログC2内のマシンM6からM10に適用されます。
- **ゾーン構成**。2つのゾーン（Z1とZ2）が作成されます。
  - カタログC1を含むゾーンZ1は、オンプレミス展開に対応します。

- カタログC2を含むゾーンZ2は、クラウド展開に対応します。

- **デリバリーグループ構成**
  - デリバリーグループには10台のマシン（M1～M10）が含まれており、そのうち5台はカタログC1（M1～M5）から、残りの5台はカタログC2（M6～M10）からのものです。
  - マシンM1からM5は手動で電源がオンにされ、スケジュール期間中ずっと電源がオンのままになります。

- **Autoscale構成**
  - 容量バッファは10%に設定されています。
  - Autoscaleは、「Cloud」タグが付いたマシンのみを電源管理します。この場合、Autoscaleはクラウドマシン M6からM10を電源管理します。

- **公開アプリケーションまたはデスクトップ構成**。公開デスクトップ（例）にはゾーン設定が構成されており、ユーザー起動要求ではゾーンZ2よりもゾーンZ1が優先されます。
  - ゾーンZ1は、公開デスクトップの優先ゾーン（ホームゾーン）として構成されています。

このシナリオは、次の順序で実行されます。

1. ユーザーはログオンしません。
2. ユーザーセッションが増加します。
3. ユーザーセッションは、利用可能なすべてのオンプレミス マシンが消費されるまでさらに増加します。
4. さらに多くのユーザーセッションが開始されます。
5. セッション終了により、ユーザーセッションが減少します。
6. セッション負荷がオンプレミス マシンのみで処理されるまで、ユーザーセッションはさらに減少します。

上記のシナリオでAutoscaleがどのように機能するかについては、以下を参照してください。

- ユーザー負荷なし（初期状態）
  - オンプレミス マシン M1～M5 はすべて電源がオンになっています。
  - クラウド内の1台のマシン（例: M6）の電源がオンになります。このマシンは、構成された容量バッファのために電源がオンになります。この場合、10（マシン数）x 10,000（負荷インデックス）x 10%（構成された容量バッファ）は10,000に等しくなります。したがって、1台のマシンの電源がオンになります。

    - 電源がオンになっているすべてのマシン（M1～M6）の負荷インデックス値は、ベースライン負荷（負荷インデックスは0）です。

- ユーザーがログオンします
    - セッションは、構成されたゾーン設定を通じてマシン M1～M5 でホストされるように指示され、これらのオンプレミス マシン間で負荷分散されます。
    - 電源がオンになっているマシン（M1～M5）の負荷インデックス値が増加します。
    - 電源がオンになっているマシン M6 の負荷インデックス値は、ベースライン負荷です。
- ユーザーが負荷を増やし、すべてのオンプレミス リソースを消費します
    - セッションは、構成されたゾーン設定を通じてマシン M1～M5 でホストされるように指示され、これらのオンプレミス マシン間で負荷分散されます。
    - 起動中のすべてのマシン (M1～M5) のロードインデックス値が10,000に達しました。
    - 起動中のマシンM6のロードインデックス値は、ベースライン負荷のままです。
- もう1人のユーザーがログオンします
    - セッションはゾーン設定を超過し、クラウドマシンM6でホストされるように指示されます。
    - 起動中のすべてのマシン (M1～M5) のロードインデックス値が10,000に達しました。
    - 起動中のマシンM6のロードインデックス値は増加し、ベースライン負荷ではなくなります。ロードインデックスで合計予備容量が10,000を下回るレベルに低下すると、構成された容量バッファのため、Autoscaleは需要を満たすために追加のマシン (M7) の電源をオンにし始めます。マシンM7の電源をオンにするには時間がかかる場合があることに注意してください。そのため、マシンM7が準備できるまでに遅延が発生する可能性があります。
- さらに多くのユーザーがログオンします
    - セッションはマシンM6でホストされるように指示されます。
    - 起動中のすべてのマシン (M1～M5) のロードインデックス値が10,000に達しました。
    - 起動中のマシンM6のロードインデックス値はさらに増加しますが、ロードインデックスで合計予備容量は10,000を上回るレベルにあります。
    - 起動中のマシンM7のロードインデックス値は、ベースライン負荷のままです。
- さらに多くのユーザーがログオンします
    - マシンM7の準備ができた後、セッションはマシンM6とM7でホストされるように指示され、これらのマシン間で負荷分散されます。

    - 起動中のすべてのマシン (M1～M5) のロードインデックス値が10,000に達しました。
    - マシンM7のロードインデックス値は、ベースライン負荷ではなくなります。
    - 稼働中のマシン (M6 および M7) の負荷インデックス値が増加します。
    - 負荷インデックスの観点から、総予備容量は依然として10,000を超えるレベルにあります。

- セッション終了により、ユーザーセッションの負荷が減少します。
    - ユーザーがセッションからログオフするか、アイドルセッションがタイムアウトすると、マシンM1からM7で解放された容量は、他のユーザーが開始したセッションをホストするために再利用されます。
    - 負荷インデックスの観点から総予備容量が10,000を超えるレベルに増加すると、Autoscaleはクラウドマシン (M6からM7) の1つをドレイン状態にします。その結果、新しい変更が発生しない限り、他のユーザーが開始したセッションはそのマシン (たとえばM7) には転送されなくなります。たとえば、ユーザー負荷が再び増加したり、他のクラウドマシンの負荷が最も低くなったりした場合です。
- 1つ以上のクラウドマシンが不要になるまで、ユーザーセッションの負荷はさらに減少します。
    - マシンM7上のすべてのセッションが終了し、指定された電源オフ遅延がタイムアウトすると、Autoscaleはマシン M7の電源をオフにします。
    - 稼働中のすべてのマシン (M1からM5) の負荷インデックス値は、10,000を下回るレベルに低下する可能性があります。
    - 稼働中のマシン (M6) の負荷インデックス値が減少します。
- クラウドマシンが不要になるまで、ユーザーセッションはさらに減少します。
    - マシンM6にユーザーセッションがない場合でも、Autoscaleは予備容量として予約されているため、電源をオフにしません。
    - Autoscaleは、構成された容量バッファのため、残りのクラウドマシンM6の電源をオンのままにします。そのマシンは、着信するユーザーにデスクトップを提供するのを待機しています。
    - オンプレミス環境のマシンに利用可能な容量がある限り、セッションはマシンM6でホストされるようには転送されません。

ユーザーログオフ通知（旧称：ユーザー強制ログオフ）

重要:

この機能は、マルチセッションアプリベースのデリバリーグループ向けのAutoscale™ユーザーインターフェイスでのみ利用可能です。

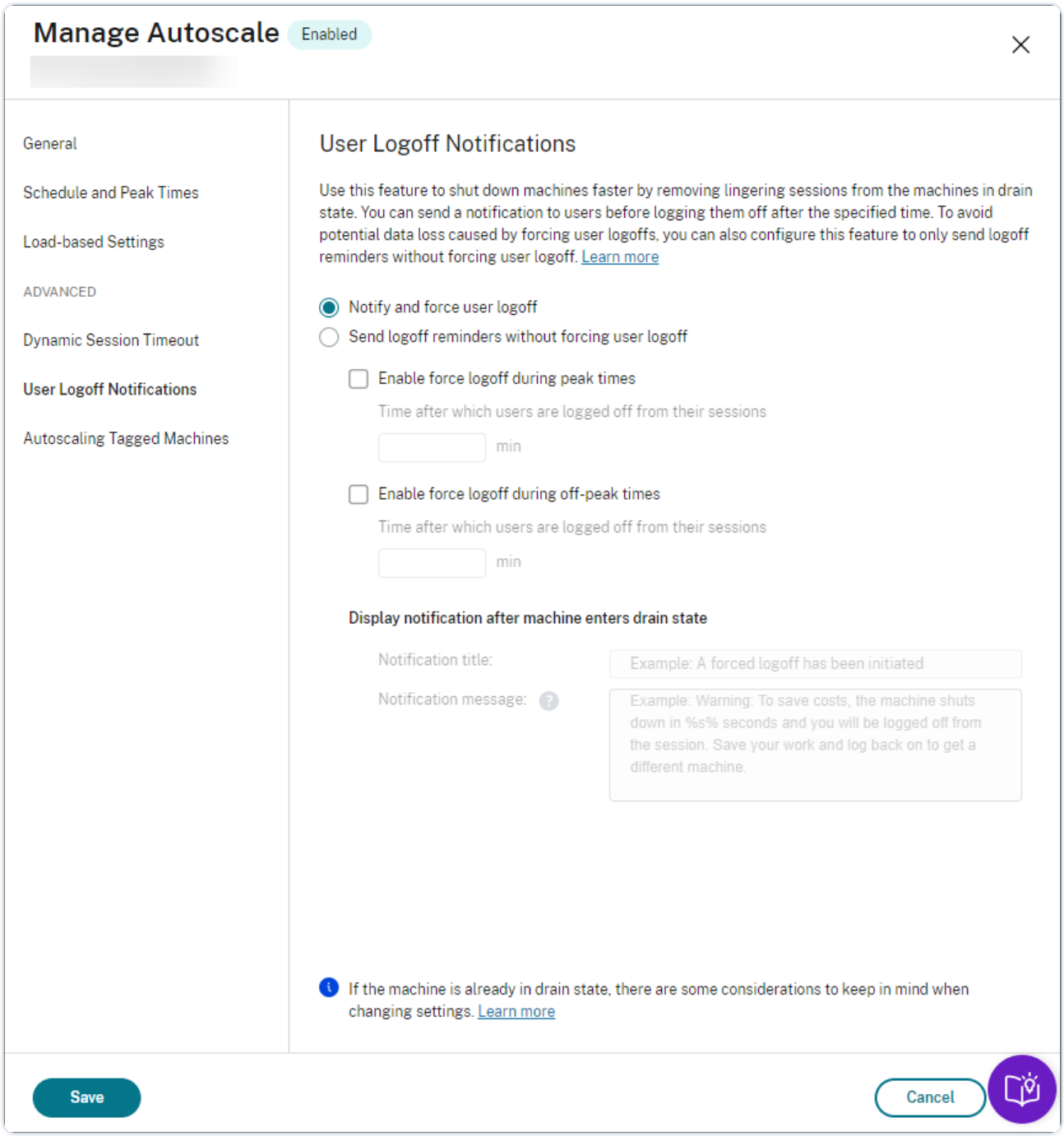
コスト削減をより効果的に実現するため、Autoscaleでは、残存セッションを強制的にログオフできます。これは、ユーザーにカスタム通知を送信し、セッションが強制的にログオフされるまでの猶予期間を指定することで行われます。これは、ドレイン状態のマシンに対してのみ行われ、すべての電源オンのマシンに対して行われるわけではありません。ユーザーの強制ログオフによって発生する可能性のあるデータ損失を回避するために、この機能は、ユーザーのログオフを強制することなく、ログオフのリマインダーのみを送信するように構成することもできます。

以下の2つのオプションがあります。

- **ユーザーに通知してログオフを強制する**
- **ユーザーのログオフを強制せずにログオフのリマインダーを送信する**

ユーザーに通知してログオフを強制する

これを選択すると、Autoscaleは、以下で指定された時間が経過した後、ユーザーをセッションからログオフします。



ピーク時の強制ログオフを有効にする。これを選択すると、Autoscaleは、指定された時間が経過したピーク時に、それらのユーザーをセッションからログオフします。

オフピーク時の強制ログオフを有効にする。これを選択すると、Autoscaleは、指定された時間が経過したオフピーク時に、それらのユーザーをセッションからログオフします。

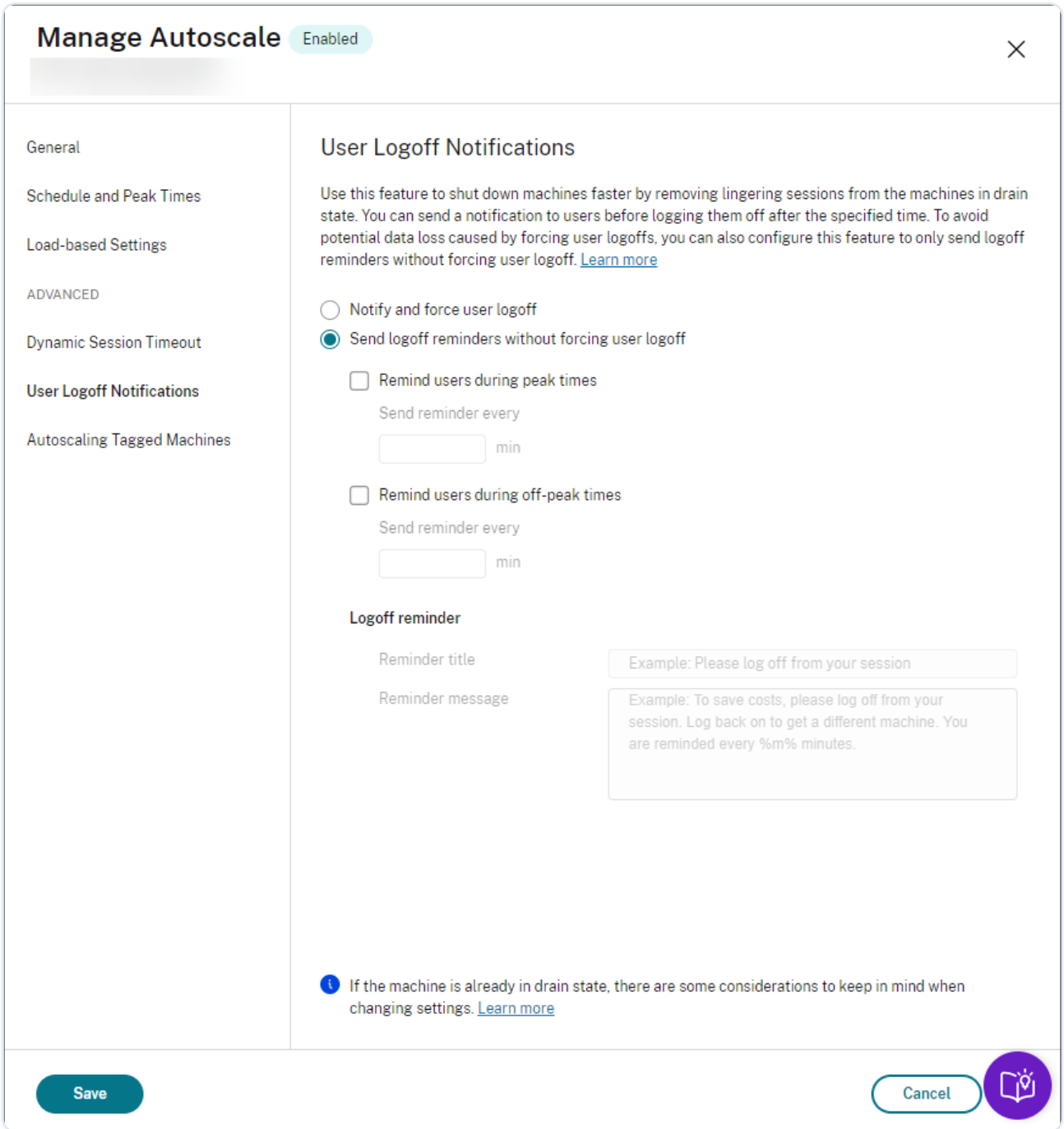
マシンがドレイン状態になった後に通知を表示する。マシンがドレイン状態になった後、ユーザーに通知を送信できます。

- **通知のタイトル。**ユーザーに送信する通知のタイトルを指定できます。例: `A forced logoff has been initiated.`.

- **通知メッセージ**。ユーザーに送信する通知の内容を指定できます。メッセージ内で指定された時間を示す変数として、%s% または %m% を使用できます。時間を秒で表すには %s% を使用します。時間を分で表すには %m% を使用します。例: `Warning: To save costs, the machine shuts down in %s% seconds and you will be logged off from the session. Save your work and log back on to get a different machine.`.

ユーザーのログオフを強制せずにログオフリマインダーを送信する

選択した場合、ユーザーはマシンがドレイン状態になった後、マシンからログオフするようリマインダーを受け取ります。このリマインダーは、以下で指定された間隔で送信されるように構成できます。



ピーク時にユーザーにリマインダーを送信する。選択した場合、ユーザーはピーク時にX分ごとにセッションからログオフするようリマインダーを受け取ります（Xは指定された時間を示します）。

オフピーク時にユーザーにリマインダーを送信する。選択した場合、ユーザーはオフピーク時にX分ごとにセッションからログオフするようリマインダーを受け取ります（Xは指定された時間を示します）。

ログオフリマインダー。マシンがドレイン状態になった後、ユーザーに送信されるリマインダーを構成できます。

- **リマインダーのタイトル**。ユーザーに送信するリマインダーのタイトルを指定できます。例: `Please log off from your session`。
- **リマインダーメッセージ**。ユーザーに送信するメッセージを指定できます。例: `Please log off from your session and log back on to save costs`。

考慮事項

マシンがすでにドレイン状態である場合、設定を変更する際には以下を考慮してください。

- 設定を「**ユーザーのログオフを強制せずにログオフリマインダーを送信する**」から「**ユーザーのログオフを通知して強制する**」に変更した場合、新しい設定はすぐに有効になります。
- 設定を「**ユーザーのログオフを通知して強制する**」から「**ユーザーのログオフを強制せずにログオフリマインダーを送信する**」に変更した場合、新しい設定はマシンが次にドレイン状態になるまで有効になりません。ユーザーは引き続きログオフを強制されます。

Broker PowerShell SDKコマンド

Broker PowerShell SDKを使用して、デリバリーグループのAutoscaleを構成できます。PowerShellコマンドを使用してAutoscaleを構成するには、PowerShell SDKバージョン7.21.0.12以降を使用する必要があります。PowerShell SDKの詳細については、「SDKとAPI」(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/sdk-api.html)を参照してください。

Set-BrokerDesktopGroup

既存のBrokerDesktopGroupを無効または有効にするか、その設定を変更します。このコマンドレットの詳細については、`<https://citrix.github.io/delivery-controller-sdk/Broker/Set-BrokerDesktopGroup/>`を参照してください。

例

PowerShellコマンドレットの使用方法の詳細については、以下の例を参照してください。

Autoscale™を有効にする

- 名前が「MyDesktop」であるデリバリーグループに対してAutoscaleを有効にしたいとします。`Set-BrokerDesktopGroup` PowerShellコマンドを使用します。例:
  - `PS C:\> Set-BrokerDesktopGroup "MyDesktop" -AutoscalingEnabled $true`

ピーク時とオフピーク時で容量バッファを個別に構成する

- 名前が「MyDesktop」であるデリバリーグループに対して、容量バッファをピーク時で20%、オフピーク時で10%に設定したいとします。`Set-BrokerDesktopGroup` PowerShellコマンドを使用します。例:
  - `PS C:\> Set-BrokerDesktopGroup "MyDesktop" -PeakBufferSizePercent 20 -OffPeakBufferSizePercent 10`

切断時のタイムアウト設定を構成する

- 名前が「MyDesktop」であるデリバリーグループに対して、**切断時のタイムアウト**値をピーク時で60分、オフピーク時で30分に設定したいとします。`Set-BrokerDesktopGroup` PowerShellコマンドを使用します。例:
  - `PS C:\> Set-BrokerDesktopGroup "MyDesktop" -PeakDisconnectTimeout 60 -OffPeakDisconnectTimeout 30`

ログオフ時のタイムアウト設定を構成する

- 名前が「MyDesktop」であるデリバリーグループに対して、**ログオフ時のタイムアウト**値をピーク時で60分、オフピーク時で30分に設定したいとします。`Set-BrokerDesktopGroup` PowerShellコマンドを使用します。例:
  - `PS C:\> Set-BrokerDesktopGroup "MyDesktop" -PeakLogOffTimeout 60 -OffPeakLogOffTimeout 30`

電源オフ遅延設定を構成する

- 名前が「MyDesktop」であるデリバリーグループに対して、電源オフ遅延を15分に設定したいとします。`Set-BrokerDesktopGroup` PowerShellコマンドを使用します。例:
  - `PS C:\> Set-BrokerDesktopGroup "MyDesktop" -PowerOffDelay 15`

電源オフ遅延が適用されない期間を構成する

- 「MyDesktop」という名前のデリバリーグループに対して、電源オフ遅延が30分経過するまで適用されるようにしたいとします。`Set-BrokerDesktopGroup` PowerShellコマンドを使用します。例:
  - `C:\PS> Set-BrokerDesktopGroup "MyDesktop" -SettlementPeriodBeforeAutoShutdown 30`。

マシンインスタンスコスト設定を構成する

- 「MyDesktop」という名前のデリバリーグループに対して、1時間あたりのマシンインスタンスコストを0.2ドルに設定したいとします。`Set-BrokerDesktopGroup` PowerShellコマンドを使用します。例:
  - `PS C:\> Set-BrokerDesktopGroup "MyDesktop" -MachineCost 0.2`

New-BrokerPowerTimeScheme

デリバリーグループのBrokerPowerTimeSchemeを作成します。詳細については、`<https://citrix.github.io/delivery-controller-sdk/Broker/New-BrokerPowerTimeScheme/>`を参照してください。

例

UID値が3のデリバリーグループに対して電源時間スキームを作成したいとします。新しいスキームは週末、月曜日、火曜日を対象とします。午前8時から午後6時30分までの時間帯は、スキームに含まれる日のピーク時間として定義されます。ピーク時間の場合、プールサイズ（電源がオンのまま維持されるマシンの数）は20です。オフピーク時間の場合、プールサイズは5です。`Set-BrokerDesktopGroup` PowerShellコマンドを使用できます。例:

- `PS C:\> $ps48=(0..47 | %{ if ($_ -lt 16 -or $_ -gt 37) { 5 } else { 20 } } )`
- `PS C:\> $pt48=(0..47 | %{ if ($_ -lt 16 -or $_ -gt 37) { $false } else { $true } } )`
- `PS C:\> New-BrokerPowerTimeScheme -Name 'First Half Week' -DaysOfWeek Weekend,Monday,Tuesday -DesktopGroupUid 3 -PeakHalfHours $pt48 -PoolSize $ps48`

動的セッションタイムアウトのパラメーター

以下のBroker PowerShell SDKコマンドレットは、複数の新しいパラメーターをサポートすることで、動的セッションタイムアウト用に拡張されました。

- Get-BrokerDesktopGroup

- New-BrokerDesktopGroup
- Set-BrokerDesktopGroup

これらのパラメーターには以下が含まれます。

- **DisconnectPeakIdleSessionAfterSeconds** – ピーク時にアイドル状態のセッションが切断されるまでの時間を秒単位で表します。このプロパティのデフォルト値は0で、ピーク時の関連動作が無効になっていることを示します。0より大きい値は、ピーク時のみデリバリーグループの動作を有効にします。
- **DisconnectOffPeakIdleSessionAfterSeconds** - オフピーク時にアイドル状態のセッションが切断されるまでの時間を秒単位で表します。このプロパティのデフォルト値は0で、オフピーク時の関連動作が無効になっていることを示します。0より大きい値は、オフピーク時のみデリバリーグループの関連動作を有効にします。
- **LogoffPeakDisconnectedSessionAfterSeconds** - ピーク時に切断されたセッションが終了されるまでの時間を秒単位で表します。このプロパティのデフォルト値は0で、ピーク時の関連動作が無効になっていることを示します。0より大きい値は、ピーク時のみデリバリーグループの関連動作を有効にします。
- **LogoffOffPeakDisconnectedSessionAfterSeconds** - オフピーク時に切断されたセッションが終了されるまでの時間を秒単位で表します。このプロパティのデフォルト値は0で、オフピーク時の関連動作が無効になっていることを示します。0より大きい値は、ピーク時のみデリバリーグループの関連動作を有効にします。

例

たとえば、「MyDesktop」という名前のデリバリーグループに対して、ピーク時のアイドルセッションタイムアウトを3,600秒に設定したいとします。`Set-BrokerDesktopGroup` PowerShellコマンドを使用します。例:

- `C:\PS> Set-BrokerDesktopGroup "MyDesktop" -DisconnectOffPeakIdleSessionAfterSeconds 3600`

これにより、「MyDesktop」という名前のデスクトップグループでは、オフピーク時に1時間以上アイドル状態だったセッションが切断されます。

シトリックス インサイトサービス

Citrix Insight Services (CIS) は、計測、テレメトリ、ビジネスインサイト生成のためのCitrixプラットフォームです。その計測およびテレメトリ機能により、技術ユーザー（顧客、パートナー、エンジニア）は、問題を自己診断して修正し、環境を最適化できます。CISとその仕組みに関する詳細

および最新情報については、`<https://cis.citrix.com>` を参照してください（Citrixアカウントの資格情報が必要です）。

Citrixにアップロードされるすべての情報は、製品の品質、信頼性、およびパフォーマンスの向上、ならびにトラブルシューティングと診断の目的で使用されます。ただし、以下の条件に従います。

- `<https://cis.citrix.com/legal>` にあるCitrix Insight Servicesポリシー
- `<https://www.cloud.com/privacy-policy>` にあるCitrixプライバシーポリシー

このCitrix Virtual Apps and Desktops™リリースは、以下のテクノロジーをサポートしています。

- Citrix Virtual Apps and Desktopsのインストールおよびアップグレード分析
- Citrixカスタマーエクスペリエンス向上プログラム (CEIP)
- シトリックス コールホーム
- シトリックス スカウト

CISおよびCitrix Analyticsとは別に、Studioをインストール（またはアップグレード）すると、Google Analyticsが自動的に収集（および後でアップロード）されます。Studioのインストール後、レジストリキー `HKLM\Software\Citrix\DesktopStudio\GAEnabled` を使用してこの設定を変更できます。値が1の場合は収集とアップロードが有効になり、0の場合は収集とアップロードが無効になります。

インストールおよびアップグレード分析

フルプロダクトインストーラーを使用してCitrix Virtual Apps and Desktopsコンポーネントを展開またはアップグレードすると、インストールプロセスに関する匿名情報が、コンポーネントをインストール/アップグレードしているマシンに収集され、保存されます。このデータは、Citrixが顧客のインストールエクスペリエンスを向上させるのに役立てられます。

この情報は、`%ProgramData%\Citrix\CTQs` の下にローカルに保存されます。

このデータの自動アップロードは、フルプロダクトインストーラーのグラフィカルインターフェイスとコマンドラインインターフェイスの両方で、デフォルトで有効になっています。

- レジストリ設定のデフォルト値を変更できます。インストール/アップグレード前にレジストリ設定を変更すると、フルプロダクトインストーラーを使用する際にその値が使用されます。
- コマンドラインインターフェイスでインストール/アップグレードする場合、コマンドでオプションを指定することでデフォルト設定を上書きできます。

自動アップロードの制御:

- インストール/アップグレード分析の自動アップロードを制御するレジストリ設定 (デフォルト = 1):
  - 場所: `HKLM:\Software\Citrix\MetaInstall`
  - 名前: SendExperienceMetrics
  - 値: 0 = 無効、1 = 有効
- PowerShell を使用すると、次のコマンドレットでインストール/アップグレード分析の自動アップロードを無効にできます:

```
New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\MetaInstall -Name
SendExperienceMetrics -PropertyType DWORD -Value 0
```

- XenDesktopServerSetup.exe または XenDesktopVDASetup.exe コマンドで自動アップロードを無効にするには、`/disableexperiencemetrics` オプションを含めます。

  XenDesktopServerSetup.exe または XenDesktopVDASetup.exe コマンドで自動アップロードを有効にするには、`/sendexperiencemetrics` オプションを含めます。

Citrixカスタマーエクスペリエンス向上プログラム

Citrixカスタマーエクスペリエンス向上プログラム (CEIP) に参加すると、匿名の統計情報と使用状況情報がCitrixに送信され、Citrix製品の品質とパフォーマンスの向上に役立てられます。詳細については、https://more.citrix.com/XD-CEIP を参照してください。

サイト作成時またはアップグレード時の登録

サイトを作成すると (最初のDelivery Controller™をインストールした後)、CEIPに自動的に登録されます。最初のデータアップロードは、サイト作成後約7日後に行われます。

サイト作成後、いつでも参加を停止できます。Web Studioの左ペインで**設定**ノードを選択し、**Citrixカスタマーエクスペリエンス向上プログラム**設定をオフにします。

Citrix Virtual Apps and Desktops展開をアップグレードする場合:

- CEIPをサポートしていないバージョンからアップグレードする場合、参加を求められます。
- CEIPをサポートしているバージョンからアップグレードし、参加が有効になっていた場合、アップグレードされたサイトでCEIPが有効になります。
- CEIPをサポートしているバージョンからアップグレードし、参加が無効になっていた場合、アップグレードされたサイトでCEIPが無効になります。

- CEIPをサポートしているバージョンからアップグレードし、参加状況が不明な場合、参加を求められます。

収集された情報は匿名であるため、Citrix Insight Servicesにアップロードされた後は表示できません。

VDAのインストール時の登録

デフォルトでは、Windows VDAをインストールすると、CEIPに自動的に登録されます。このデフォルト設定はレジストリ設定で変更できます。VDAをインストールする前にレジストリ設定を変更した場合、その値が使用されます。

CEIPへの自動登録を制御するレジストリ設定（デフォルト = 1）：

場所: `HKLM:\Software\Citrix\Telemetry\CEIP` 名前: Enabled 値: 0 = 無効、1 = 有効

デフォルトでは、`Enabled` プロパティはレジストリに隠されています。指定されていない場合、自動アップロード機能は有効になります。

PowerShellを使用すると、次のコマンドレットでCEIPへの登録を無効にできます。

```
New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\Telemetry\CEIP -Name Enabled
-PropertyType DWORD -Value 0
```

収集されたランタイムデータポイントは、定期的にファイルとして出力フォルダー（デフォルトは %programdata%/Citrix/VdaCeip）に書き込まれます。

データの初回アップロードは、VDAのインストール後約7日で行われます。

その他の製品およびコンポーネントのインストール時の登録

Citrix Provisioning™、AppDNA、Citrix License Server、Citrix Workspace™ app for Windows、Universal Print Server、Session Recordingなどの関連するCitrix製品、コンポーネント、テクノロジーをインストールする際にもCEIPに参加できます。インストールと参加のデフォルト値の詳細については、それぞれのドキュメントを参照してください。

Citrix コールホーム

Citrix Virtual Apps and Desktopsで特定のコンポーネントと機能をインストールすると、Citrix Call Homeに参加する機会が提供されます。Call Homeは診断データを収集し、そのデータを含むテレメトリパッケージを分析とトラブルシューティングのためにCitrix Insight Servicesに直接（デフォルトポート443のHTTPS経由で）定期的にアップロードします。

Citrix Virtual Apps and Desktopsでは、Call HomeはCitrix Telemetry Serviceという名前のバックグラウンドサービスとして実行されます。詳細については、(https://www.citrix.com/community/cx/call-home.html?utm_campaign=none&utm_content=xa-xd+product+ui+learn+more&utm_source=more.citrix.com/XD-CALLHOME&utm_medium=Vanity+Url)を参照してください。

Call Homeのスケジュール機能はCitrix Scoutでも利用できます。詳細については、(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/manage-deployment/cis/scout.html)を参照してください。

収集される情報

Citrix Diagnostic Facility (CDF) トレースは、トラブルシューティングに役立つ情報をログに記録します。Call Homeは、VDA登録やアプリケーション/デスクトップの起動など、一般的な障害のトラブルシューティングに役立つCDFトレースのサブセットを収集します。このテクノロジーは、常時オンのトレース (AOT) として知られています。AOTログは、C:\Users\CitrixTelemetryService\Appdata\Local\CitrixAOTにディスクに保存されます。

Call Homeは、その他のEvent Tracing for Windows (ETW) 情報を収集しません。また、そのように構成することもできません。

Call Homeは、次のようなその他の情報も収集します。

- `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix`の下にCitrix Virtual Apps and Desktopsによって作成されたレジストリ。
- Citrix名前空間下のWindows Management Instrumentation (WMI) 情報。
- 実行中のプロセスの一覧。
- `%PROGRAMDATA%\Citrix\CDF`に保存されているCitrixプロセスのクラッシュダンプ。
- インストールおよびアップグレード情報。これには、製品の完全なメタインストーラーログ、失敗したMSIログ、MSIログアナライザーからの出力、StoreFront™ログ、ライセンス互換性チェックログ、および予備的なサイトアップグレードテストの結果が含まれます。

トレース情報は収集時に圧縮されます。Citrix Telemetry Serviceは、最大8日間の期間で、最大10 MBの圧縮された最新のトレース情報を保持します。

- データを圧縮することで、Call HomeはVDA上で小さなフットプリントを維持できます。
- トレースは、プロビジョニングされたマシンでのIOPを回避するためにメモリに保持されます。
- トレースバッファは、トレースをメモリに保持するために循環メカニズムを使用します。

Call Homeは、Call Homeの主要データポイントに記載されている主要なデータポイントを収集します。

構成と管理の概要

Call Homeには、製品版インストールウィザードを使用しているとき、または後でPowerShellコマンドレットを使用して登録できます。登録すると、デフォルトでは、診断は毎週日曜日の現地時間午前3時頃に収集され、Citrixにアップロードされます。アップロードは、指定された時刻から2時間のランダムな間隔で行われます。これは、デフォルトのスケジュールを使用したアップロードが午前3時から午前5時の間に行われることを意味します。

スケジュールに基づいて診断情報をアップロードしたくない場合（またはスケジュールを変更したい場合）は、PowerShellコマンドレットを使用して診断を手動で収集してアップロードするか、ローカルに保存することができます。

スケジュールされたCall Homeアップロードに登録する場合、および診断情報を手動でCitrixにアップロードする場合、Citrixアカウントまたは Citrix Cloud™の資格情報を提供します。Citrixは、資格情報を、顧客を識別しデータをアップロードするために使用されるアップロードトークンと交換します。資格情報は保存されません。

アップロードが行われると、Citrixアカウントに関連付けられているアドレスに通知がメールで送信されます。

コンポーネントのインストール時にCall Homeを有効にした場合、後で無効にできます。

前提条件

- マシンはPowerShell 3.0以降を実行している必要があります。
- Citrix Telemetry Serviceがマシン上で実行されている必要があります。
- システム変数 `PSModulePath` は、Telemetryのインストールパス（例: `C:\Program Files\Citrix\Telemetry Service\`）に設定されている必要があります。

コンポーネントのインストール中にCall Homeを有効にする

VDAのインストールまたはアップグレード中: 製品版インストーラーのグラフィカルインターフェイスを使用してVirtual Delivery Agentをインストールまたはアップグレードする際、Call Homeに参加するかどうかを尋ねられます。2つのオプションがあります。

- Call Homeに参加する。
- Call Home に参加しない。

VDA をアップグレードしていて、以前に Call Home に登録していた場合、そのウィザードページは表示されません。

Controller のインストールまたはアップグレード中: グラフィカルインターフェイスを使用して Delivery Controller をインストールまたはアップグレードする際、Call Home に参加するかどうかを尋ねられます。3つのオプションがあります。

Controller をインストールする際、そのサーバーに「サービスとしてログオン」ポリシー設定が適用された Active Directory GPO がある場合、インストールウィザードの Call Home ページで情報を構成することはできません。詳細については、CTX218094 を参照してください。

Controller をアップグレードしていて、以前に Call Home に登録していた場合、参加について尋ねられることはありません。

PowerShell コマンドレット

PowerShell ヘルプには、これらの一般的なユースケースでは使用されないコマンドレットとパラメーターの説明を含む、包括的な構文が記載されています。

アップロードにプロキシサーバーを使用するには、プロキシサーバーの構成 を参照してください。

- **スケジュールされたアップロードを有効にする:** 診断コレクションは自動的に Citrix にアップロードされます。カスタムスケジュール用の追加のコマンドレットを入力しない場合、デフォルトのスケジュールが使用されます。

  ```
  $cred = Get-Credential

  Enable-CitrixCallHome -Credential $cred
  ```

  スケジュールされたアップロードが有効になっていることを確認するには、`Get-CitrixCallHome` を入力します。有効になっている場合、戻り値は `IsEnabled=True` と `IsMasterImage=False` です。

- **マスターイメージから作成されたマシンに対するスケジュールされたアップロードを有効にする:** マスターイメージでスケジュールされたアップロードを有効にすると、マシンカタログで作成される各マシンを構成する必要がなくなります。

  `Enable-CitrixCallHome -Credential $cred -MasterImage`

スケジュールされたアップロードが有効になっていることを確認するには、**Get-CitrixCallHome** を入力します。有効になっている場合、戻り値は `IsEnabled=True` と `IsMasterImage=True` です。

- **カスタムスケジュールを作成する:** 診断コレクションとアップロードの毎日または毎週のスケジュールを作成します。

```
$timespan = New-TimeSpan –Hours hours -Minutes minutes

Set-CitrixCallHomeSchedule –TimeOfDay $timespan –DayOfWeek day
-UploadFrequency {Daily|Weekly}
```

例:

次のコマンドレットは、毎日夜の10時20分にデータをバンドルしてアップロードするスケジュールを作成します。Hours パラメーターは24時間形式を使用します。`UploadFrequency` パラメーターの値が Daily の場合、`DayOfWeek` パラメーターは指定されていても無視されます。

```
$timespan – New-TimeSpan –Hours 22 –Minutes 20

Set-CitrixCallHomeSchedule –TimeOfDay $timespan -UploadFrequency Daily
```

スケジュールを確認するには、`Get-CitrixCallHomeSchedule` を入力します。前の例では、`StartTime=22:20:00, DayOfWeek=Sunday (ignored), Upload Frequency=Daily` が返されます。

次のコマンドレットは、毎週水曜日の夜10時20分にデータをバンドルしてアップロードするスケジュールを作成します。

```
$timespan – New-TimeSpan –Hours 22 –Minutes 20

Set-CitrixCallHomeSchedule –TimeOfDay $timespan –DayOfWeek Wed
-UploadFrequency Weekly
```

スケジュールを確認するには、`Get-CitrixCallHomeSchedule` を入力します。前の例では、`StartTime=22:20:00, DayOfWeek=Wednesday, Upload Frequency=Weekly` が返されます。

Call Homeを無効にする

PowerShellコマンドレットを使用するか、Citrix Scoutを介してCall Homeを無効にできます。

Call Homeのスケジュールされたアップロードが無効になっている場合でも、AOTログは収集され、ディスクに保存されます。(スケジュールされたアップロードが無効になっている場合、AOTログはCitrixに自動的にアップロードされません。)AOTログの収集とローカルストレージを無効にできます。

PowerShellでCall Homeを無効にする

次のコマンドレットを実行した後、診断データはCitrixに自動的にアップロードされません。(Citrix ScoutまたはテレメトリPowerShellコマンドレットを使用して診断データをアップロードすることは引き続き可能です。)

```
Disable-CitrixCallHome
```

Call Homeが無効になっていることを確認するには、`Get-CitrixCallHome` を入力します。無効になっている場合、戻り値は `IsEnabled=False` と `IsMasterImage=False` です。

Citrix Scoutを使用して収集スケジュールを無効にする

Citrix Scoutを使用して診断収集スケジュールを無効にするには、コレクションのスケジュール のガイダンスに従ってください。ステップ3で、**オフ**をクリックして、選択したマシンのスケジュールをキャンセルします。

AOTログの収集を無効にする

次のコマンドレットを実行した後 (`Enabled` フィールドを `false` に設定して)、AOTログは収集されません。

```
Enable-CitrixTrace -Listen'{"trace":{"enabled":false,"persistDirectory":"C:\Users\Public","maxSizeBytes":1000000, "sliceDurationSeconds":300}}'
```

`Listen` パラメーターには、JSON形式の引数が含まれています。

Call Homeのアップロード用にプロキシサーバーを構成する

Call Home が有効になっているマシンで、次のタスクを完了します。以下の手順の図の例には、サーバーアドレスとポート 10.158.139.37:3128 が含まれています。お客様の情報は異なります。

1. ブラウザにプロキシサーバー情報を追加します。Internet Explorer で、 **\> \>** を選択します。" を選択し、プロキシサーバーのアドレスとポート番号を入力します。
2. PowerShell で `netsh winhttp import proxy source=ie` を実行します。

   プロキシサーバーを構成する際の netsh コマンド実行例(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/call-home-proxy-ie.png)

3. テキストエディターを使用して、`C:\Program Files\Citrix\Telemetry Service` にある TelemetryService.exe 構成ファイルを編集します。赤枠で示されている情報を追加します。

   TelemetryService.exe ファイルにプロキシ情報を追加(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/call-home-proxy-config.png)

4. テレメトリサービスを再起動します。

PowerShell で Call Home コマンドレットを実行します。

診断情報を手動で収集してアップロードする

CIS Web サイトを使用して、診断情報バンドルを CIS にアップロードできます。PowerShell コマンドレットを使用して、診断情報を収集し、CIS にアップロードすることもできます。

CIS Web サイトを使用してバンドルをアップロードするには：

1. Citrix アカウントの資格情報を使用して Citrix Insight Services にログオンします。
2. を選択します。
3. を選択し、データの場所に移動します。

CIS は、データアップロードを管理するいくつかの PowerShell コマンドレットをサポートしています。このドキュメントでは、2 つの一般的なケースのコマンドレットについて説明します。

- `Start-CitrixCallHomeUpload` コマンドレットを使用して、診断情報バンドルを手動で収集し、CIS にアップロードします。(バンドルはローカルに保存されません。)
- `Start-CitrixCallHomeUpload` コマンドレットを使用して、データを手動で収集し、診断情報バンドルをローカルに保存します。これにより、データをプレビューできます。後で、`Send-CitrixCallHomeBundle` コマンドレットを使用して、そのバンドルのコピーを手動で CIS にアップロードします。(最初に保存したデータはローカルに残ります。)

PowerShell ヘルプには、これらの一般的なユースケースでは使用されないコマンドレットとパラメーターの説明を含む、包括的な構文が記載されています。

CIS にデータをアップロードするコマンドレットを入力すると、アップロードの確認を求められます。アップロードが完了する前にコマンドレットがタイムアウトした場合は、システムイベントログでアップロードのステータスを確認してください。サービスがすでにアップロードを実行している場合、アップロード要求が拒否されることがあります。

データを収集してバンドルを CIS にアップロードする:

```
Start-CitrixCallHomeUpload [-Credential] PSCredential [-InputPath string]
[-Description string] [-IncidentTime string] [-SRNumber string] [-Name
string] [-UploadHeader string] [-AppendHeaders string] [-Collect string]
[<CommonParameters>]
```

データを収集してローカルに保存する:

```
Start-CitrixCallHomeUpload -OutputPath <String> [-InputPath string] [-
Description string] [-IncidentTime string] [-SRNumber string] [-Name
string] [-UploaderHeader string] [-AppendHeaders string] [-Collect
strings] [<CommonParameters>]
```

次のパラメーターが有効です。

- **Credential:** アップロードを CIS に指示します。
- **InputPath:** バンドルに含める zip ファイルの場所。これは、Citrix サポートが要求する追加ファイルである可能性があります。.zip 拡張子を含めるようにしてください。
- **OutputPath:** 診断情報が保存される場所。このパラメーターは、Call Home データをローカルに保存する場合に必須です。
- **Description and Incident Time:** アップロードに関する自由形式の情報。
- **SRNumber:** Citrix テクニカルサポートのインシデント番号。
- **Name:** バンドルを識別する名前。
- **UploadHeader:** CIS にアップロードされるアップロードヘッダーを指定する JSON 形式の文字列。
- **AppendHeaders:** CIS にアップロードされる追加ヘッダーを指定する JSON 形式の文字列。
- **収集:** 収集または除外するデータを指定するJSON形式の文字列で、{'collector':{'enabled':ブール値}} の形式です。ここでブール値はtrueまたはfalseです。 有効なコレクター値は次のとおりです。
  - 'Windows Management Instrumentation' (ウィンドウズ マネジメント インストゥルメンテーション)
  - 'プロセス'
  - 'レジストリ'
  - 'クラッシュレポート'
  - 'トレース'

- 'ファイル'
- マイクロソフト インストーラー
- 'ローカルデータ'
- 'サイトデータ'
- スカイプ フォー ビジネス

既定では、'sfb' を除くすべてのコレクターが有効になっています。

'sfb' コレクターは、Skype for Business の問題を診断するためにオンデマンドで使用するように設計されています。'enabled' パラメーターに加えて、'sfb' コレクターは、ターゲットユーザーを指定するための 'account' および 'accounts' パラメーターをサポートしています。次のいずれかの形式を使用します。

- "-コレクト "`{'sfb':{'account':'domain\user1'}}`"
- "-コレクト "`{'sfb':{'accounts':['domain\user1', 'domain\user2']}}`"

- **共通パラメーター:** PowerShell のヘルプを参照してください。

以前ローカルに保存されたデータをアップロードする:

`Send-CitrixCallHomeBundle -Credential <PSCredentia\> -Path string [<CommonParameters>]`

`Path` パラメーターは、以前に保存されたバンドルの場所を指定します。

例:

次のコマンドレットは、Call Home データ（WMI コレクターからのデータを除く）を CIS にアップロードするよう要求します。このデータは、Citrix Support ケース 123456 のために午後 2 時 30 分に記録された、Citrix Provisioning VDA の登録失敗に関連しています。Call Home データに加えて、ファイル「`c:\Diagnostics\ExtraData.zip`」がアップロードされたバンドルに組み込まれます。

```
C:\PS\>Start-CitrixCallHomeUpload -InputPath "c:
\Diagnostics\ExtraData.zip" -Description "Registration failures with
Citrix Provisioning VDAs" -IncidentTime "14:30" -SRNumber 123456 -Name
"RegistrationFailure-021812016" -Collect "{'wmi':{'enabled':false}}"
-UploadHeader "{'key1':'value1'}" -AppendHeaders "{'key2':'value2'}"
```

次のコマンドレットは、午前 8 時 15 分に記録された Citrix Support ケース 223344 に関連する Call Home データを保存します。データはネットワーク共有上のファイル mydata.zip に保存されます。Call Home データに加えて、ファイル「`c:\Diagnostics\ExtraData.zip`」が保存されたバンドルに組み込まれます。

```
C:\PS\>Start-CitrixCallHomeUpload -OutputPath \
\mynetwork\myshare\mydata.zip -InputPath "c:\Diagnostics\ExtraData.zip"
-Description "Diagnostics for incident number 223344" -IncidentTime "8:15"
-SRNumber 223344
```

次のコマンドレットは、以前に保存したデータバンドルをアップロードします。

```
$cred=Get-Credential

C:\PS>Send-CitrixCallHomeBundle –Credential $cred -Path \
\mynetwork\myshare\mydata.zip
```

Citrix スカウト

はじめに

Citrix Scout は、診断情報を収集し、ヘルスチェックを実行します。結果を使用して、Citrix Virtual Apps and Desktops™ 展開を維持できます。Citrix は、Citrix Insight Services を通じて、診断コレクションの包括的な自動分析を提供します。また、Scout を使用して、単独で、または Citrix Support のガイダンスを受けて、問題のトラブルシューティングを行うこともできます。

収集ファイルを Citrix にアップロードして、Citrix Support から分析とガイダンスを受けることができます。または、コレクションをローカルに保存して自分で確認し、後でそのコレクションファイルを Citrix にアップロードして分析することもできます。

Scout には、次の手順があります。

- **収集:** サイトで選択したマシンに対して、1 回限りの診断コレクションを実行します。その後、ファイルを Citrix にアップロードするか、ローカルに保存できます。
- **トレースと再現:** 選択したマシンで手動トレースを開始します。次に、それらのマシンで問題を再現します。問題の再現後、トレースは停止します。その後、Scout は他の診断情報を収集し、ファイルを Citrix にアップロードするか、ファイルをローカルに保存します。
- **スケジュール:** 選択したマシンで、指定した時間に毎日または毎週診断コレクションが実行されるようにスケジュールします。ファイルは自動的に Citrix にアップロードされます。

- **ヘルスチェック:** サイトとそのコンポーネントの正常性と可用性を測定するチェックを実行します。Delivery Controller、Virtual Delivery Agent（VDA）、StoreFront™ サーバー、Citrix License Server のヘルスチェックを実行できます。チェック中に問題が検出された場合、Scout は詳細なレポートを提供します。Scout が起動するたびに、更新されたヘルスチェックスクリプトがチェックされます。新しいバージョンが利用可能な場合、Scout はそれらを自動的にダウンロードし、次回のヘルスチェック実行時に使用します。

> **注：**
>
> **トレースと再現、スケジュール、ヘルスチェック**の手順は、現在 Linux VDA では利用できません。

> この記事で説明するグラフィカルインターフェイスは、Scout を使用する主要な方法です。または、PowerShell を使用して、1 回限りの診断コレクションまたはスケジュールされた診断コレクションとアップロードを構成することもできます。「Call Home」を参照してください。

Scout の実行場所:

- オンプレミス展開では、Delivery Controller™ から Scout を実行して、1 つ以上の Virtual Delivery Agent（VDA）、Delivery Controller、StoreFront サーバー、および License Server の診断情報を取得したり、チェックを実行したりします。VDA から Scout を実行して、ローカル診断情報を収集することもできます。
- Citrix DaaS（旧称 Citrix Virtual Apps and Desktops サービス）を使用する Citrix Cloud 環境では、VDA から Scout を実行してローカル診断情報を収集します。

Scout アプリケーションのログは `C:\ProgramData\Citrix\TelemetryService\ScoutUI.log` に保存されます。このファイルはトラブルシューティングに使用できます。

収集されるもの

Scoutが収集する診断情報には、Citrix Diagnostic Facility (CDF) トレースログファイルが含まれます。Always-on Tracing (AOT) と呼ばれるCDFトレースのサブセットも含まれています。AOT情報は、VDA登録やアプリケーション/デスクトップの起動などの一般的な問題のトラブルシューティングに役立ちます。その他のEvent Tracing for Windows (ETW) 情報は収集されません。

収集される情報には以下が含まれます。

- `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix`の下にCitrix Virtual Apps and Desktopsによって作成されたレジストリエントリ。
- **Citrix名前空間**の下にあるWindows Management Instrumentation (WMI) 情報。
- 実行中のプロセス。
- `%PROGRAMDATA%\Citrix\CDF`に保存されているCitrixプロセスのクラッシュダンプ。
- CSV形式のCitrixポリシー情報。
- インストールおよびアップグレード情報。収集される情報には、製品の完全なメタインストーラーログ、失敗したMSIログ、MSIログアナライザーからの出力、StoreFrontログ、ライセンス互換性チェックログ、および予備的なサイトアップグレードテストの結果が含まれる場合があります。

トレース情報について：

- トレース情報は収集時に圧縮されるため、マシン上のフットプリントは小さく保たれます。
- 各マシンで、Citrix Telemetry Serviceは圧縮された最新のトレース情報を最大8日間保持します。
- Citrix Virtual Apps and Desktops 7 1808以降、AOTトレースはデフォルトでローカルディスクに保存されます。（以前のバージョンでは、トレースはメモリに保持されていました。）デフォルトパス = `C:\Users\CitrixTelemetryService\AppData\Local\CitrixAOT`。
- Citrix Virtual Apps and Desktops 7 1811以降、ネットワーク共有に保存されたAOTトレースは、他の診断情報とともに収集されます。
- 最大サイズ（デフォルト = 10 MB）とスライス期間は、`Enable-CitrixTrace`コマンドレットまたは`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Telemetry DefaultListen`レジストリ文字列を使用して変更できます。
- トレースは、ファイルが`MaxSize`の10%に達するまでファイルに追加されます。

Scout が収集するデータポイントのリストについては、Call Home key datapoints を参照してください。

Scout の構成

Scout は Linux VDA で動作するように構成できます。Linux VDA とテレメトリの詳細については、Integrate with the Citrix Telemetry Service を参照してください。

Linux VDA は、`ctxtelemetry` ソケットポートまたはテレメトリサービスのポートを自動的に変更する場合があります。その場合は、ポートを手動で構成する必要があります。

1. C:\Program Files\Citrix\Telemetry Service に移動します

2. ScoutUI.exe.config ファイルを開きます。
3. LinuxVDATelemetryServicePort または LinuxVDATelemetryWakeupPort の値を、Linux VDA で構成された値に変更します。

- `<add key="LinuxVDATelemetryServicePort" value="7502"/>`
- `<add key="LinuxVDATelemetryWakeupPort" value="7503"/>`

1. 変更を保存してファイルを閉じます。
2. Scout を再度開いて、最新の構成が読み込まれていることを確認します。

ヘルスチェックについて

ヘルスチェックデータは、`C:\ProgramData\Citrix\TelemetryService\` の下のフォルダーに保存されます。

サイトヘルスチェック

サイトヘルスチェックは、FlexCast Management Architecture (FMA) サービスの包括的な評価を提供する Environment Test Service に含まれています。これらのチェックは、サービスの可用性を確認するだけでなく、データベース接続などの他のヘルスインジケーターも調べます。

サイトヘルスチェックは Delivery Controller で実行されます。サイトの規模によっては、これらのチェックの完了に最大 1 時間かかる場合があります。

DELIVERY CONTROLLER の構成チェック

サイトの健全性チェックの一環として、Citrix Virtual Apps and Desktopsサイトに関するCitrixの推奨事項に基づき、Delivery Controllerの構成チェックは以下の問題が存在するかどうかを確認します。

- 1つ以上のDelivery Controllerが失敗状態にある。
- サイトにDelivery Controllerが1つしかない。
- Delivery Controllerのバージョンが異なる。

健全性チェックの権限と要件を満たすことに加えて、Delivery Controllerの構成チェックには以下が必要です。

- 少なくとも1つのControllerが電源オンになっていること。
- Controller上でBroker Serviceが実行されていること。
- Controllerからサイトデータベースへの接続が機能していること。

VDAの健全性チェック

VDAの健全性チェックは、一般的なVDA登録、セッション起動、およびタイムゾーンリダイレクトの問題の考えられる原因を特定します。

VDAでの登録について、Scoutは以下をチェックします。

- VDAソフトウェアのインストール
- VDAマシンのドメインメンバーシップ
- VDA通信ポートの可用性
- VDAサービスの状態
- Windows ファイアウォールの構成
- Controller との通信
- Controller との時刻同期
- VDA 登録ステータス

VDA でのセッション起動について、Scout は以下を確認します。

- セッション起動通信ポートの可用性
- セッション起動サービスのステータス
- セッション起動 Windows ファイアウォールの構成
- VDA リモートデスクトップサービス クライアントアクセスライセンス
- VDA アプリケーション起動パス
- セッション起動レジストリ設定

VDA でのタイムゾーンリダイレクトについて、Scout は以下を確認します。

- Windows ホットフィックスのインストール
- Citrix ホットフィックスのインストール
- Microsoft グループポリシー設定
- Citrix グループポリシー設定

VDA 上のプロファイル管理について、Scout は以下をチェックします。

- ハイパーバイザーの検出
- プロビジョニングの検出
- シトリックス バーチャル アプリ アンド デスクトップ

- Personal vDisk の構成
- ユーザー ストア
- プロファイル管理サービスのステータス検出
- Winlogon.exe フック テスト

プロファイル管理のチェックを実行するには、VDA にプロファイル管理をインストールして有効にする必要があります。プロファイル管理の構成チェックの詳細については、Knowledge Center の記事 CTX132805 を参照してください。

StoreFront のヘルスチェック

StoreFront のチェックでは、以下を確認します。

- Citrix Default Domain サービスが実行中であること
- Citrix Credential Wallet サービスが実行中であること
- StoreFront サーバーから Active Directory ポート 88 への接続
- StoreFront サーバーから Active Directory ポート 389 への接続
- ベース URL に有効な FQDN がある
- ベース URL から正しい IP アドレスを取得できる
- IIS アプリケーションプールが .NET 4.0 を使用している
- 証明書がホスト URL の SSL ポートにバインドされているか
- 証明書チェーンが完全であるか
- 証明書の有効期限が切れているか
- 証明書の有効期限が間もなく切れるか（30 日以内）

ライセンスサーバーのチェック

ライセンスサーバーのチェックでは、以下を確認します。

- Delivery Controller からのライセンスサーバー接続
- ライセンスサーバーのファイアウォールリモートアクセスステータス
- Citrix ライセンスサービスのステータス
- ライセンスサーバーの猶予期間の状態
- ライセンスサーバーのポート接続
- Citrix ベンダーデーモン (CITRIX) が実行中であるか
- システムクロックが同期されているかどうか

- Citrix Licensingサービスがローカルサービスアカウントで実行されているかどうか
- `CITRIX.opt`ファイルの存在
- Customer Success Servicesの資格取得日
- Citrix License Server アップデート
- ライセンスサーバー証明書がDelivery Controllerの信頼されたルートストアにあるかどうか

ヘルスチェックの権限と要件を満たすことに加えて、ライセンスサーバーはドメインに参加している必要があります。そうでない場合、ライセンスサーバーは検出されません。

ヘルスチェックの実行

ヘルスチェックの手順は、マシンの選択、チェックの開始、結果レポートの確認で構成されます。

1. Scoutを起動します。マシンの**スタート**メニューから、**Citrix > Citrix Scout**を選択します。開いたページで、**Health Check**をクリックします。
2. マシンを選択します。**Find machine**をクリックしてマシンを検出します。**Select machines**ページには、サイトで検出されたすべてのVDA、Delivery Controller、およびLicense Serverが一覧表示されます。マシン名で表示をフィルタリングできます。診断情報を収集する各マシンの横にあるチェックボックスを選択し、**Continue**をクリックします。

   その他のコンポーネントタイプ（StoreFrontサーバーやVDAマシンなど）を追加するには、マシンを手動で追加およびVDAマシンをインポートを参照してください。Citrix Provisioning™ サーバーまたはLicense Serverを手動で追加することはできません。

   Scoutは、選択された各マシンで検証テストを自動的に起動し、検証テストに記載されている基準を満たしていることを確認します。検証が失敗した場合、**Status**列にメッセージが表示され、そのマシンのチェックボックスがオフになります。次のいずれかを実行できます。

   - 問題を解決し、そのマシンのチェックボックスを再度選択します。これにより、検証テストが再試行されます。
   - そのマシンをスキップします（チェックボックスをオフのままにします）。そのマシンではヘルスチェックは実行されません。

   検証テストが完了したら、**続行**をクリックします。
3. 選択したマシンでヘルスチェックを実行します。概要には、テストが実行されたマシン（検証テストに合格した選択済みのマシン）が一覧表示されます。**チェックの開始**をクリックします。

   チェック中およびチェック後：

- **ステータス**列には、マシンの現在のチェック状態が表示されます。
- 進行中のすべてのチェックを停止するには、ページの右下隅にある**チェックの停止**をクリックします。（単一のマシンのヘルスチェックをキャンセルすることはできません。選択したすべてのマシンのみです。チェックが完了したマシンからの情報は保持されます。）.
- 選択したすべてのマシンのチェックが完了すると、右下隅にある**チェックの停止**ボタンが**完了**に変わります。
- チェックが失敗した場合は、**アクション**列の**再試行**をクリックできます。
- チェックが問題なく完了した場合、**アクション**列は空になります。
- チェックで問題が見つかった場合は、**詳細の表示**をクリックして結果を表示します。
- 選択したすべてのマシンのチェックが完了したら、**戻る**をクリックしないでください。（クリックすると、チェック結果が失われます。）

4. チェックが完了したら、**完了**をクリックしてScoutの開始ページに戻ります。

ヘルスチェックの結果

レポートを生成するCitrixチェックの場合、レポートには以下が含まれます。

- 結果レポートが生成された日時
- チェックされたマシン
- チェックがターゲットマシンで探した条件

権限と要件

権限:

- 診断情報を収集するには:
  - 診断情報を収集する各マシンで、ローカル管理者およびドメインユーザーである必要があります。
  - 各マシンでLocalAppDataディレクトリへの書き込み権限が必要です。
- ヘルスチェックを実行するには:
  - ドメインユーザーグループのメンバーである必要があります。
  - フル管理者であるか、サイトに対する読み取り専用および**環境テストの実行**権限を持つカスタムロールを持っている必要があります。

  - スクリプトの実行を許可するには、スクリプト実行ポリシーを少なくとも`RemoteSigned`に設定します。例: `Set-ExecutionPolicy RemoteSigned`。**注:** 他のスクリプト実行権限でも機能する場合があります。

- Scoutを起動するときは、**管理者として実行**を使用します。

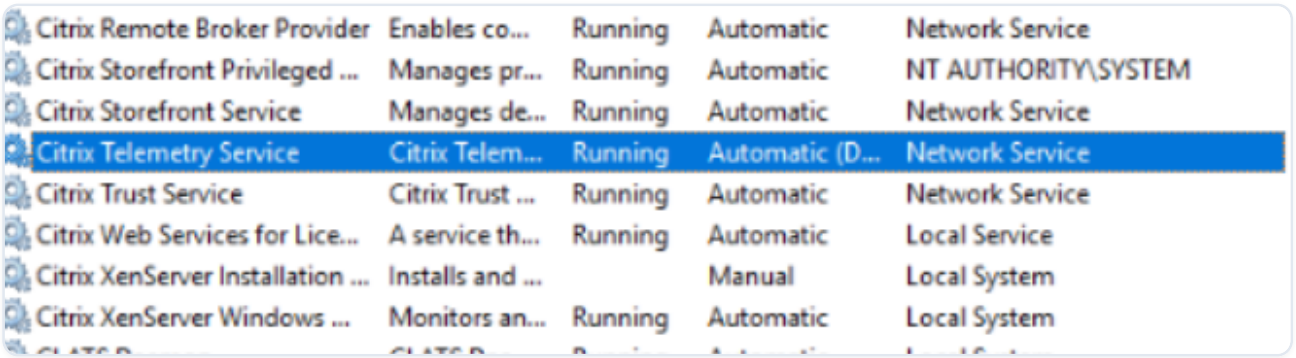
診断情報を収集したり、ヘルスチェックを実行したりする各マシンについて:

- Scoutがマシンと通信できる必要があります。
- ファイルとプリンターの共有が有効になっている必要があります。
- PSRemotingとWinRMが有効になっている必要があります。また、マシンではPowerShell 3.0以降が実行されている必要があります。
- Citrix Telemetry Service はマシン上で実行されている必要があります。
- Windows Management Infrastructure (WMI) アクセスはマシン上で有効になっている必要があります。
- 診断収集のスケジュールを設定するには、マシンで互換性のあるScoutバージョンが実行されている必要があります。

パス名で指定するユーザー名にドル記号 ($) を使用しないでください。診断情報の収集が妨げられます。

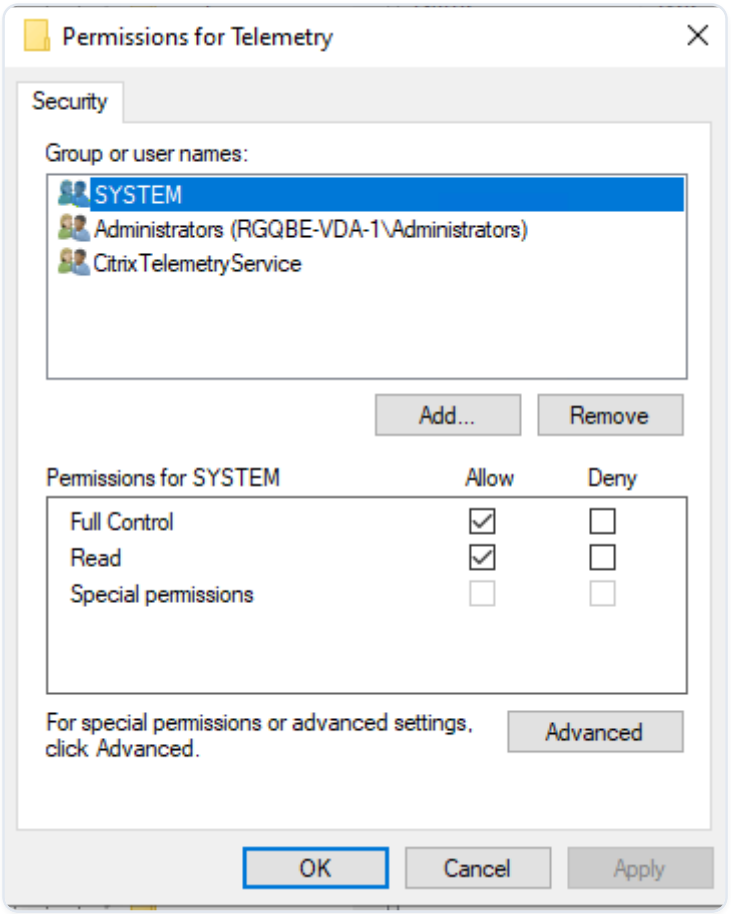
Scout は、選択したマシンで検証テストを実行し、これらの要件が満たされていることを確認します。

Windows 用の Telemetry Service は Network Service で実行されます。

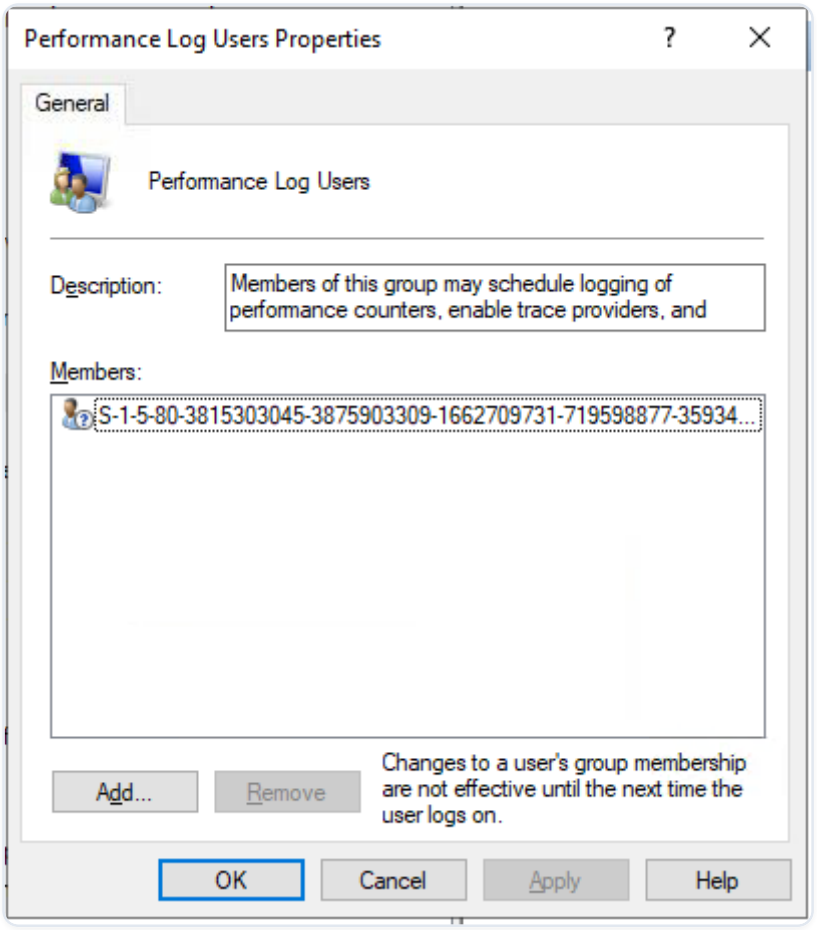


AOT トレースフォルダーは`C:\ProgramData\Citrix\TelemetryService\CitrixAOT`に保存されます。

Administrator グループ、System、および Telemetry Service SID のユーザーのみが`HKEYLOCALMACHINE:SOFTWARE\Citrix\Telemetry`レジストリにアクセスする権限を持っています。



Telemetry Service をアンインストールした後も、Telemetry Service SID は Performance Log Users グループに残りますが、手動で削除できます。



検証テスト

診断収集またはヘルスチェックが開始される前に、選択された各マシンに対して検証テストが自動的に実行されます。これらのテストは、要件が満たされていることを確認します。マシンのテストが失敗した場合、Scout は修正措置の提案とともにメッセージを表示します。

- **Scout がこのマシンに到達できません** - 以下を確認してください。
  - マシンは電源が入っています。
  - ネットワーク接続が正常に機能しています。(これには、ファイアウォールが適切に構成されていることの確認が含まれる場合があります。)
  - ファイルとプリンターの共有がオンになっています。手順については、Microsoft のドキュメントを参照してください。
- **PSRemoting と WinRM を有効にする** - PowerShell リモート処理と WinRM を同時に有効にできます。**管理者として実行**を使用して、`Enable-PSRemoting` コマンドレットを実行します。詳細については、コマンドレットに関する Microsoft のヘルプを参照してください。
- **Scout には PowerShell 3.0 (最小) が必要です** - マシンに PowerShell 3.0 (またはそれ以降) をインストールし、PowerShell リモート処理を有効にします。

- **このマシン上の LocalAppData ディレクトリにアクセスできません** - アカウントに、マシン上の LocalAppData ディレクトリへの書き込み権限があることを確認してください。
- **Citrix Telemetry Service を見つけられません** - Citrix Telemetry Service がマシンにインストールされ、開始されていることを確認してください。
- **スケジュールを取得できません** - マシンを (最小) XenApp および XenDesktop 7.14 にアップグレードしてください。
- **WMI がマシンで実行されていません** - Windows Management Instrumentation (WMI) アクセスが有効になっていることを確認してください。
- **WMI 接続がブロックされています** - Windows ファイアウォールサービスで WMI を有効にしてください。
- **新しいバージョンの Citrix Telemetry Service が必要です** - (バージョンは、収集とトレースおよび再現の場合にのみチェックされます。) マシン上のテレメトリサービスバージョンをアップグレードしてください (インストールとアップグレード を参照)。サービスをアップグレードしない場合、そのマシンは **収集** または **トレースおよび再現** アクションに含まれません。
- **Scout がこのマシン上の systemd ソケットに接続できません** - 以下を確認してください。
  - ポート 7503 が開いています。systemd ctxtelemetry.socket がマシン上のポート 7503 でリッスンしていることを確認してください。ctxtelemetry.socket ポートが変更されている場合、ポートが異なる可能性があります。ポートを調整するには、Scout の構成 を参照してください。
  - ネットワーク接続が正常に機能しています。（これには、ファイアウォールが適切に構成されていることの確認が含まれる場合があります。）
- **このマシンで Linux VDA Telemetry Service が開始されていません** - 以下を確認してください。
  - ポート7502が開いています。マシンにLinux VDAテレメトリーサービスがインストールされ、起動していることを確認してください。テレメトリーサービスのポートが変更されている場合、ポートが異なる可能性があります。ポートを調整するには、Scoutの構成を参照してください。
  - ネットワーク接続が正常に機能しています。（これには、ファイアウォールが適切に構成されていることの確認が含まれる場合があります。）

バージョンの互換性

このバージョンのScout（3.x）は、Citrix Virtual Apps and Desktops（または最低でもXenAppおよびXenDesktop 7.14）のコントローラーおよびVDAで実行することを目的としています。

| 機能 | スカウト 2.23 | スカウト 3.0 | --- | --- | ---| -- | Citrix Virtual Apps and Desktops（XenAppおよびXenDesktop 7.14〜7.18を含む）をサポート | はい | はい XenDesktop 5.x、7.1〜7.13をサポート | はい | いいえ XenApp 6.x、7.5〜7.13をサポート | はい | いいえ 製品に同梱 | 7.1〜7.13 | 7.14以降 CTX記事からダウンロード可能 | はい | いいえ CDFトレースをキャプチャ | はい | はい 常時オンのトレース（AOT）をキャプチャ | いいえ | はい 診断データの収集を許可する | 一度に最大10台のマシン（デフォルト） | 無制限（リソースの可用性による） 診断データをCitrixに送信することを許可する | はい | はい 診断データをローカルに保存することを許可する | はい | はい Citrix Cloud™資格情報をサポート | いいえ | はい Citrix資格情報をサポート | はい | はい アップロード用のプロキシサーバーをサポート | はい | はい スケジュールを調整する | 該当なし | はい スクリプトのサポート | コマンドライン（ローカルControllerのみ） | Call Homeコマンドレットを使用するPowerShell（Telemetry Serviceがインストールされている任意のマシン） ヘルスチェック | いいえ | はい データマスキング | いいえ | 3.17以降

インストールとアップグレード

デフォルトでは、VDAまたはControllerをインストールまたはアップグレードすると、Scoutは Citrix Telemetry Serviceの一部として自動的にインストールまたはアップグレードされます。

VDAのインストール時にCitrix Telemetry Serviceを省略した場合、または後でサービスを削除した場合は、Citrix Virtual Apps and Desktopsインストールメディアの`x64\Virtual Desktop Components`または`x86\Virtual Desktop Components`フォルダーから`TelemetryServiceInstaller_xx.msi`を実行します。

Collectまたは**Trace & Reproduce**アクションを選択すると、マシンが古いバージョンのCitrix Telemetry Serviceを実行している場合に通知されます。Citrixは、最新のサポートされているバージョンを使用することをお勧めします。そのマシンでTelemetry Serviceをアップグレードしない場合、**Collect**または**Trace & Reproduce**アクションには含まれません。Telemetry Serviceをアップグレードするには、インストールと同じ手順を使用します。

アップロードの承認

診断コレクションをCitrixにアップロードする予定がある場合は、CitrixアカウントまたはCitrix Cloudアカウントが必要です。（これらは、Citrixダウンロードにアクセスしたり、Citrix Cloud Control Centerにアクセスしたりするために使用する資格情報です。）アカウントの資格情報が検証されると、トークンが発行されます。

CitrixアカウントまたはCitrix Cloudアカウントで認証する場合は、リンクをクリックして、デフォルトのブラウザーでHTTPSを使用してCitrix Cloudにアクセスします。Citrix Cloudの資格情報を入力すると、トークンが表示されます。トークンをコピーしてScoutに貼り付けます。その後、Scoutウィザードを続行できます。

トークンは、Scoutを実行しているマシンにローカルに保存されます。次回**Collect**または**Trace & Reproduce**を実行するときにそのトークンを使用できるようにするには、**Store token and skip this step in the future**チェックボックスをオンにします。

Scoutの開始ページで**Schedule**を選択するたびに、再承認する必要があります。スケジュールを作成または変更するときに、保存されたトークンを使用することはできません。

アップロードにプロキシを使用する

コレクションをCitrixにアップロードするためにプロキシサーバーを使用したい場合は、Scoutにブラウザーのインターネットプロパティ用に構成されたプロキシ設定を使用するように指示できます。または、プロキシサーバーのIPアドレスとポート番号を指定することもできます。

マシンの検索

Collect、**Trace & Reproduce**、および**Schedule**の手順では、Scoutは自動的に検出したControllerとVDAを一覧表示します。

Delivery ControllerからScout Health Checkを実行するときは、**Find machine**をクリックして、デリバリーコントローラー、VDA、ライセンスサーバー、StoreFrontサーバーなどのマシンを検出します。

Delivery Controllerではないドメイン参加済みマシンからScout Health Checkを実行する場合、Scoutはマシンを自動的に検出できません。add machines manuallyまたはimport VDA machinesする必要があります。

マシンを手動で追加する

Scoutが検出したControllerとVDAをリストした後、StoreFrontサーバー、ライセンスサーバー、Citrix Provisioningサーバーなど、展開内の他のマシンを手動で追加できます。

ヘルスチェックを実行する場合：

- ドメイン内のCitrix License Serverは自動的に検出されます。License Serverを手動で追加することはできません。
- ヘルスチェックは現在、Citrix Provisioningサーバーをサポートしていません。

検出されたマシンを一覧表示するScoutの任意のページで、**+ Add machine**をクリックします。追加するマシンのFQDNを入力し、**Continue**をクリックします。必要に応じて、他のマシンを追加するために繰り返します。（FQDNの代わりにDNSエイリアスを入力しても有効に見えることがありますが、ヘルスチェックが失敗する可能性があります。）

手動で追加されたマシンは、常に検出されたマシンよりも上の、マシンリストの先頭に表示されます。

手動で追加されたマシンを識別する簡単な方法は、行の右端にある赤い削除ボタンです。手動で追加されたマシンのみがそのボタンを持っています。検出されたマシンにはありません。

手動で追加されたマシンを削除するには、行の右端にある赤いボタンをクリックします。削除を確認します。他の手動で追加されたマシンを削除するために繰り返します。

Scoutは、手動で追加されたマシンを削除するまで記憶しています。Scoutを閉じて再度開いても、手動で追加されたマシンはリストの先頭に表示されたままです。

StoreFrontサーバーで**Trace & Reproduce**を使用する場合、CDFトレースは収集されません。ただし、その他のすべてのトレース情報は収集されます。

VDAマシンをインポートする

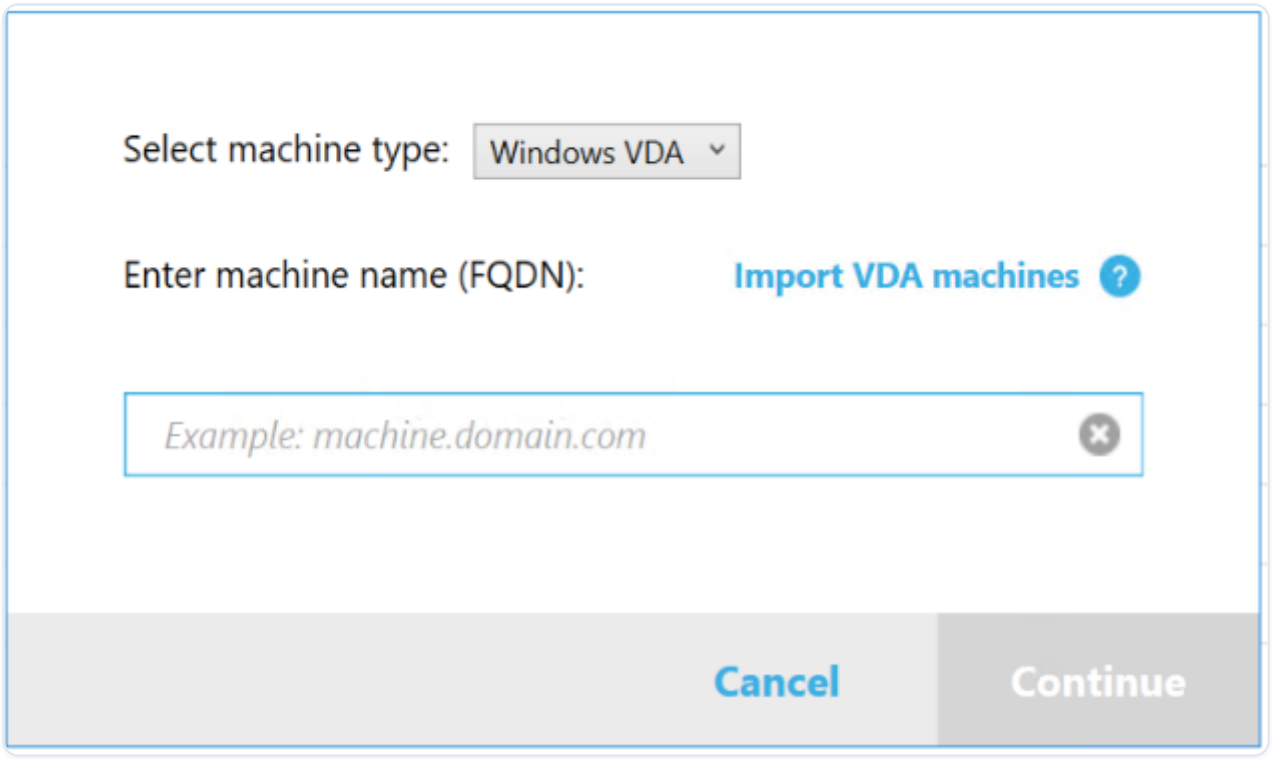
ヘルスチェックを実行する際に、展開内のVDAマシンをインポートできます。

1. Delivery ControllerまたはConnectorで、PowerShellコマンドを使用してマシンリストファイルを生成します。Connectorでは、Citrix資格情報を入力し、ポップアップダイアログで顧客を選択する必要があります。

   ```
   Get-BrokerMachine| foreach { $_.DnsName } | out-file C:\machineList.txt
   ```

2. machineList.txtファイルを、Scout Health Checkを起動したいドメイン参加済みマシンにコピーします。
3. 「Scout Health Check」ページで、 をクリックします。
4. マシンタイプを選択します。
5. をクリックします。
6. machineList.txtファイルを選択します。
7. をクリックします。

インポートされたVDAマシンが「Scout Health Check」ページに一覧表示されます。



診断情報の収集

手順には、マシンの選択、診断情報収集の開始、および収集を含むファイルをCitrixにアップロードするか、ローカルに保存することが含まれます。

1. Scoutを起動します。マシンの メニューから、 > を選択します。開いたページで、 をクリックします。
2. マシンを選択します。

   - コントローラーでは、 ページにサイト内のすべてのVDAとコントローラーが一覧表示されます。マシン名で表示をフィルターできます。その他のマシン（StoreFrontサーバーやCitrix Provisioningサーバーなど）を手動で追加するには、「マシンの手動追加」を参照してください。
   - その他のコンポーネント（VDAサーバーなど）では、 ページにローカルマシンのみが一覧表示されます。マシンの手動追加はサポートされていません。

   診断情報を収集する各マシンの横にあるチェックボックスをオンにし、 をクリックします。

   Scoutは、選択された各マシンで検証テストを自動的に起動し、「検証テスト」に記載されている基準を満たしていることを確認します。検証に失敗した場合、 列にメッセージが表示され、そのマシンのチェックボックスはオフになります。次のいずれかを実行できます。

   - 問題を解決し、マシンのチェックボックスを再度選択します。これにより、検証テストが再試行されます。

- そのマシンをスキップします（チェックボックスは選択しないままにします）。そのマシンからは診断情報が収集されません。

検証テストが完了したら、**続行**をクリックします。

3. 診断情報を収集します。概要には、診断情報が収集されるすべてのマシン（検証テストに合格した選択済みのマシン）が一覧表示されます。**収集開始**をクリックします。

   収集中：

   - **ステータス**列には、マシンの現在の収集状態が表示されます。
   - 単一マシンで進行中の収集を停止するには、そのマシンの**アクション**列にある**キャンセル**をクリックします。
   - すべての進行中の収集を停止するには、ページの右下隅にある**収集の停止**をクリックします。収集が完了したマシンからの診断情報は保持されます。収集を再開するには、各マシンの**アクション**列にある**再試行**をクリックします。
   - 選択したすべてのマシンの収集が完了すると、右下隅にある**収集の停止**ボタンが**続行**に変わります。
   - 診断情報を再度収集するには、そのマシンの**アクション**列にある**再度収集**をクリックします。新しい収集は以前の収集を上書きします。
   - 収集が失敗した場合は、**アクション**列にある**再試行**をクリックできます。成功した収集のみがアップロードまたは保存されます。
   - 選択したすべてのマシンの収集が完了したら、**戻る**をクリックしないでください。（クリックすると、収集は失われます。）

   収集が完了したら、**続行**をクリックします。

4. 収集を保存またはアップロードします。ファイルをCitrixにアップロードするか、ローカルマシンに保存するかを選択します。

   今すぐファイルをアップロードすることを選択した場合は、手順5に進みます。

   ファイルをローカルに保存する場合：

   - Windowsの**保存**ダイアログボックスが表示されます。目的の場所に移動します。
   - ローカル保存が完了すると、ファイルのパス名が表示され、リンクされます。ファイルを表示できます。後でCitrixにファイルをアップロードできます。CTX136396を参照してください。

   完了をクリックして、Scoutの開始ページに戻ります。この手順でこれ以上ステップを完了する必要はありません。

5. アップロードの認証を行い、必要に応じてプロキシを指定します。詳細については、(#upload-authorization)を参照してください。

   - Scoutを介して認証していない場合は、この手順を続行します。
   - Scoutを介して認証済みの場合、保存されている認証トークンがデフォルトで使用されます。これを行う場合は、このオプションを選択して**続行**をクリックします。このコレクションの資格情報は要求されません。手順6に進みます。
   - 以前に認証済みで、再認証して新しいトークンを取得したい場合は、**変更/再認証**をクリックしてこの手順を続行します。

   アップロードの認証にCitrix資格情報を使用するか、Citrix Cloud資格情報を使用するかを選択します。**続行**をクリックします。資格情報ページは、保存されたトークンを使用していない場合にのみ表示されます。

   資格情報ページで：

   - ファイルのアップロードにプロキシサーバーを使用する場合は、**プロキシの構成**をクリックします。Scoutに、ブラウザのインターネットプロパティ用に構成されたプロキシ設定を使用するように指示できます。または、プロキシサーバーのIPアドレスとポート番号を入力することもできます。プロキシダイアログボックスを閉じます。
   - Citrix Cloudアカウントの場合は、**トークンの生成**をクリックします。デフォルトのブラウザがCitrix Cloudページを起動し、トークンが表示されます。トークンをコピーし、Scoutページに貼り付けます。
   - Citrixアカウントの場合は、資格情報を入力します。

   完了したら、**続行**をクリックします。
6. アップロードに関する情報を入力します。

   - 「名前」フィールドには、収集された診断ファイルのデフォルト名が含まれています。ほとんどの収集ではこれで十分ですが、名前を変更することもできます。(デフォルト名を削除して「名前」フィールドを空のままにした場合、デフォルト名が使用されます。)
   - オプションで、8桁のCitrixサポートケース番号を指定します。
   - オプションの**説明**フィールドに、問題の内容と、該当する場合は問題が発生した時期を記述します。

   完了したら、**アップロードの開始**をクリックします。

   アップロード中、ページの左下部分にアップロードの完了パーセンテージの概算が表示されます。進行中のアップロードをキャンセルするには、**アップロードの停止**をクリックします。

アップロードが完了すると、その場所のURLが表示され、リンクされます。リンクをたどってCitrixの場所に移動し、アップロードの分析を表示することも、リンクをコピーすることもできます。

完了をクリックして、Scoutの開始ページに戻ります。

トレースと再現

トレースと再現手順は、マシンの選択、トレースの開始、問題の再現、診断収集の完了、そしてファイルをCitrixへのアップロードまたはローカルへの保存で構成されます。

この手順は、標準の**収集**手順に似ています。ただし、マシンでトレースを開始し、それらのマシンで問題を再現することができます。すべての診断収集にはAOTトレース情報が含まれています。この手順では、トラブルシューティングに役立つCDFトレースが追加されます。

1. Scoutを起動します。マシンの**スタート**メニューから、**Citrix > Citrix Scout**を選択します。開始ページで、**トレースと再現**をクリックします。
2. マシンを選択します。**マシンの選択**ページには、サイト内のすべてのVDAとコントローラーが一覧表示されます。マシン名で表示をフィルタリングできます。トレースと診断を収集する各マシンの横にあるチェックボックスをオンにします。次に、**続行**をクリックします。

   他のマシン（StoreFrontやCitrix Provisioningサーバーなど）を手動で追加するには、「マシンの手動追加」を参照してください。

   Scoutは、選択された各マシンで検証テストを自動的に起動し、「検証テスト」に記載されている基準を満たしていることを確認します。マシンの検証が失敗した場合、**ステータス**列にメッセージが表示され、そのマシンのチェックボックスは選択解除されます。次のいずれかを実行できます。

   - 問題を解決してから、そのマシンのチェックボックスを再度選択します。これにより、検証テストが再試行されます。
   - そのマシンをスキップします（チェックボックスは選択解除のままにします）。診断情報とトレースはそのマシンから収集されません。

   検証テストが完了したら、**続行**をクリックします。
3. トレースを開始します。概要には、トレースが収集されるすべてのマシンが一覧表示されます。**トレースの開始**をクリックします。

   選択した1台以上のマシンで、発生した問題を再現します。その間もトレースの収集は続行されます。問題の再現が完了したら、Scoutで**続行**をクリックします。これによりトレースが停止します。

トレースを停止した後、トレース中に問題が再現されたかどうかを示します。

4. マシンから診断情報を収集します。**収集の開始**をクリックします。収集中：

   - **ステータス**列には、マシンの現在の収集状態が表示されます。
   - 単一マシンで進行中の収集を停止するには、そのマシンの**アクション**列にある**キャンセル**をクリックします。
   - 進行中のすべての収集を停止するには、ページの右下隅にある**収集の停止**をクリックします。収集が完了したマシンからの診断情報は保持されます。収集を再開するには、各マシンの**アクション**列にある**再試行**をクリックします。
   - 選択したすべてのマシンの収集が完了すると、右下隅にある**収集の停止**ボタンが**続行**に変わります。
   - マシンから診断情報を再度収集するには、そのマシンの**アクション**列にある**再収集**をクリックします。新しい収集が以前の収集を上書きします。
   - 収集が失敗した場合は、**アクション**列にある**再試行**をクリックできます。正常に収集されたもののみがアップロードまたは保存されます。
   - 選択したすべてのマシンの収集が完了した後、**戻る**をクリックしないでください。（クリックすると、収集が失われます。）

   収集が完了したら、**続行**をクリックします。

5. 収集を保存またはアップロードします。ファイルをCitrixにアップロードするか、ローカルに保存するかを選択します。

   今すぐファイルをアップロードすることを選択した場合は、手順6に進みます。

   ファイルをローカルに保存することを選択した場合は、次のようになります。

   - Windowsの保存ダイアログボックスが表示されます。目的の場所を選択します。
   - ローカル保存が完了すると、ファイルのパス名が表示され、リンクされます。ファイルを表示できます。注意: 後でCitrixからファイルをアップロードできます。Citrix Insight Servicesについては、CTX136396を参照してください。

   完了をクリックしてScoutの開始ページに戻ります。この手順でこれ以上ステップを完了する必要はありません。

6. アップロードの認証を行い、必要に応じてプロキシを指定します。このプロセスの詳細については、アップロード認証を参照してください。

   - Scoutを通じて認証していない場合は、この手順に進みます。

- Scoutを通じて認証した場合、保存されている認証トークンがデフォルトで使用されます。これを実行したい場合は、このオプションを選択して**続行**をクリックします。このコレクションの資格情報は求められません。手順7に進みます。
- 以前に認証済みで、再認証して新しいトークンを取得したい場合は、**変更/再認証**をクリックしてこの手順に進みます。

アップロードを認証するためにCitrix資格情報を使用するか、Citrix Cloud資格情報を使用するかを選択します。**続行**をクリックします。資格情報ページは、保存されたトークンを使用していない場合にのみ表示されます。

資格情報ページで:

- ファイルアップロードにプロキシサーバーを使用したい場合は、**プロキシの構成**をクリックします。Scoutにブラウザのインターネットプロパティ用に構成されたプロキシ設定を使用するように指示できます。または、プロキシサーバーのIPアドレスとポート番号を入力することもできます。プロキシダイアログボックスを閉じます。
- Citrix Cloudアカウントの場合は、**トークンを生成**をクリックします。デフォルトのブラウザがCitrix Cloudページに起動し、トークンが表示されます。トークンをコピーし、Scoutページに貼り付けます。
- Citrixアカウントの場合は、資格情報を入力します。

完了したら、**続行**をクリックします。

7. アップロードに関する情報を提供します。

アップロードの詳細を入力します。

- 名前フィールドには、収集された診断ファイルのデフォルト名が含まれています。ほとんどのコレクションではこれで十分ですが、名前を変更することもできます。（デフォルト名を削除して名前フィールドを空のままにすると、デフォルト名が使用されます。）
- オプションで、8桁のCitrixサポートケース番号を指定します。
- オプションの「説明」フィールドに、問題の内容と、該当する場合は問題が発生した時期を記述します。

完了したら、 をクリックします。

アップロード中、ページの左下部分にアップロードの完了率が概算で表示されます。進行中のアップロードをキャンセルするには、 をクリックします。

アップロードが完了すると、その場所のURLが表示され、リンクされます。リンクをたどってCitrixの場所にアクセスし、アップロードの分析を表示したり、リンクをコピーしたりできます。

をクリックして、Scoutの開始ページに戻ります。

追加のログ収集を有効にする

機能を使用すると、perfmon、Netsh、DebugView、Wiresharkなどのツールでトレースおよび再現機能を使用できます。

> **注：**
>
> これはローカルマシンにのみ適用されます。

> 追加のログ収集を設定するには：

1. Citrix Scoutを起動します。
2. ギアをクリックします。
3. 「**その他のツールで追加のログ収集を有効にする**」をクリックします。
4. 「**保存**」をクリックします。

追加のログを収集するには：

1. Scoutのホームページで、「**Trace & Reproduce**」をクリックします。
2. 「**Select machines**」ページで、ローカルマシンの右側にある歯車アイコンをクリックします。
3. 「**Select the tools require for logging:**」ページで、「**Download Tools**」をクリックします。
4. 「**Download Tools**」ページで、使用したいツールを選択し、「**Download**」をクリックします。Wiresharkを除き、ツールがダウンロードされます。Wiresharkは手動でのみダウンロードおよびインストールできます。 注：他のツールを手動でダウンロードすることを選択した場合、ダウンロードした.zipファイルの内容を`C:\ProgramData\Citrix\TelemetryService\CDC\Lib\Resources\Tools\<toolname>`に抽出する必要があります。たとえば、DebugView.zipファイルをダウンロードした場合、そのファイルの内容を`C:`

`\ProgramData\Citrix\TelemetryService\CDC\Lib\Resources\Tools\DebugView\`に解凍します。

5. 「**Select the tools require for logging:**」ページで、「**Refresh Status**」をクリックします。選択されたすべてのツールが、ステータス列の下に「**Present**」と表示されます。
6. ログ記録用のツールを選択し、「**Next**」をクリックします。
7. Trace and Reproduceの手順に従います。
8. 完了後、zipファイル内のログを確認します。ログは*CDCLogs*フォルダーに圧縮されています。

> **注：**
>
> Procmonツールがトレース用に選択されている場合、Process Monitorのログはすぐに大きくなる可能性があります。必要なツールのみを選択するようにしてください。ログのサイズは*%temp%\Scout-CDC-Log*で監視することもできます。

コレクションのスケジュール

> **注：**
>
> 現在、コレクションはスケジュールできますが、ヘルスチェックはスケジュールできません。

スケジュール手順は、マシンを選択し、スケジュールを設定またはキャンセルすることから構成されます。スケジュールされたコレクションは自動的にCitrixにアップロードされます。（PowerShellインターフェイスを使用して、スケジュールされたコレクションをローカルに保存できます。Citrix Call Homeを参照してください。）

1. Scoutを起動します。マシンのスタートメニューから「**Citrix > Citrix Scout**」を選択します。開いたページで「**Schedule**」をクリックします。
2. マシンを選択します。サイト内のすべてのVDAとコントローラーが一覧表示されます。マシン名で表示をフィルターできます。

   グラフィカルインターフェイスを使用してVDAとコントローラーをインストールしたときに、Call Homeスケジュールを設定した場合（Citrix Call Homeを参照）、Scoutはデフォルトでそ

れらの設定を表示します。このバージョンのScoutを使用して、スケジュールされた収集を初めて開始したり、以前に構成されたスケジュールを変更したりできます。

コンポーネントのインストール中にマシンごとにCall Homeを有効/無効にした場合でも、Scoutで構成されたスケジュールは、選択したすべてのマシンに影響します。

診断を収集する各マシンの横にあるチェックボックスを選択し、**続行**をクリックします。

他のマシンを手動で追加するには（StoreFrontまたはCitrix Provisioningサーバーなど）、マシンを手動で追加を参照してください。

Scoutは、選択した各マシンで検証テストを自動的に起動し、検証テストの基準を満たしていることを確認します。マシンの検証が失敗した場合、**ステータス**列にメッセージが表示され、そのマシンのチェックボックスは選択解除されます。次のいずれかを実行できます。

- 問題を解決してから、そのマシンのチェックボックスを再度選択します。これにより、検証テストが再試行されます。
- そのマシンをスキップします（チェックボックスをオフのままにします）。そのマシンからは診断（またはトレース）は収集されません。

検証テストが完了したら、**続行**をクリックします。

概要ページには、スケジュールが適用されるマシンが一覧表示されます。**続行**をクリックします。

3. スケジュールを設定します。診断を収集するタイミングを指定します。注意：スケジュールは、選択したすべてのマシンに影響します。

    - 選択したマシンの週次スケジュールを構成するには、**週次**をクリックします。曜日を選択します。収集を開始する時刻（24時間形式）を入力します。
    - 選択したマシンの日次スケジュールを構成するには、**日次**をクリックします。収集を開始する時刻（24時間形式）を入力します。
    - 選択したマシンの既存のスケジュールをキャンセルする（そして別のスケジュールに置き換えない）には、**オフ**をクリックします。これにより、それらのマシンに対して以前に構成されたすべてのスケジュールがキャンセルされます。

    続行をクリックします。

4. アップロードの認証を行い、必要に応じてプロキシを指定します。このプロセスの詳細については、アップロード認証を参照してください。注意：Scoutスケジュールを使用している場合、保存されたトークンを使用して認証することはできません。

アップロードの認証にCitrix資格情報を使用するか、Citrix Cloud資格情報を使用するかを選択します。**続行**をクリックします。

資格情報ページで、:

- ファイルをアップロードするためにプロキシサーバーを使用する場合は、**プロキシの構成**をクリックします。Scoutに、ブラウザのインターネットプロパティで構成されているプロキシ設定を使用するように指示できます。または、プロキシサーバーのIPアドレスとポート番号を入力することもできます。プロキシダイアログボックスを閉じます。
- Citrix Cloudアカウントの場合は、**トークンの生成**をクリックします。デフォルトのブラウザがCitrix Cloudページに起動し、トークンが表示されます。トークンをコピーし、Scoutページに貼り付けます。
- Citrixアカウントの場合は、資格情報を入力します。

完了したら、**続行**をクリックします。

構成されたスケジュールを確認します。**完了**をクリックしてScoutの開始ページに戻ります。

収集中、選択された各マシンのWindowsアプリケーションログには、収集とアップロードに関するエントリが含まれます。

データマスキング

Citrix Scoutを使用して収集された診断情報には、セキュリティ上機密性の高い情報が含まれている場合があります。Citrix Scoutのデータマスキング機能を使用すると、診断ファイルをCitrixにアップロードする前に、機密データをマスクできます。

Scoutのデータマスキングは、IPアドレス、マシン名、ドメイン名、ユーザー名、ハイパーバイザー名、デリバリーグループ名、カタログ名、アプリケーション名、およびSIDをマスクするように構成されています。

> **注：**
>
> CDFトレースは暗号化されており、マスクできません。
>
> Linux VDAログは`.tar.gz2`形式に圧縮されており、マスクできません。

新しい診断情報を収集し、データマスキングを実行する

Citrix Scoutのデータマスキング機能を使用するには、コマンドラインからScoutを起動します。

1. Windowsで、管理者としてコマンドプロンプトを開きます。
2. Scoutがインストールされているディレクトリに移動します: `cd C:\Program Files\Citrix\Telemetry Service`。
3. Scoutを起動します: `ScoutUI.exe datamasking`。
4. 診断情報を収集するには、**Collect** または **Trace & Reproduce** をクリックします。
5. 収集が完了したら、**Enable data masking** を選択します。このオプションはデフォルトで有効になっています。
6. データマスクを構成します。デフォルトのルールを使用することも、ルールをカスタマイズすることもできます。
7. 診断情報の収集をアップロードするか保存するかを選択します。
   - **Upload the diagnostics collection to Citrix** を選択すると、マスクされた診断ファイルがCitrixにアップロードされます。
   - **Save the diagnostics collection on your local machine** を選択すると、元の診断情報とマスクされた診断情報の両方が指定された場所に保存されます。

既存の診断情報に対してデータマスキングを実行する

1. Windowsで、管理者としてコマンドプロンプトを開きます。
2. Scoutがインストールされているディレクトリに移動します: `cd C:\Program Files\Citrix\Telemetry Service`。
3. データマスキングモードでScoutを直接起動します: `ScoutUI.exe datamasking filePath`。
4. 続行するには「Enable data masking」を選択します。このオプションはデフォルトで有効になっています。
5. データマスクを構成します。デフォルトのルールでデータマスキングを実行することも、ルールをカスタマイズすることもできます。
6. 診断コレクションをアップロードするか保存するかを選択します。
   - **診断コレクションをCitrixにアップロード**を選択すると、マスクされた診断ファイルがCitrixにアップロードされます。
   - **診断コレクションをローカルマシンに保存**を選択すると、元の診断とマスクされた診断の両方が指定された場所に保存されます。

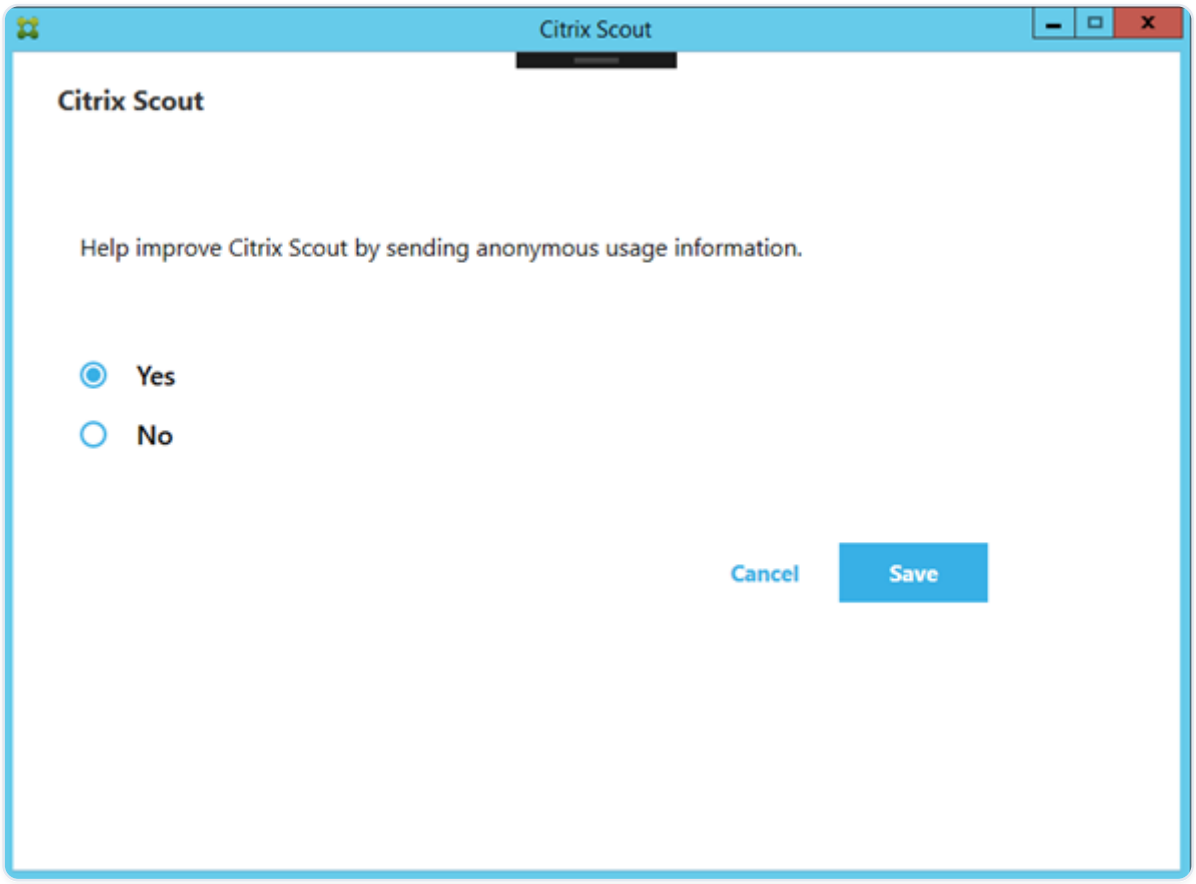
マスクされたデータファイルとマッピングファイルの場所

診断コレクションをアップロードまたは保存した後、リンクをクリックして元の診断とマスクされた診断を開き、マッピング情報ファイルを開きます。

使用状況データの収集

Scoutを使用すると、CitrixはGoogle Analyticsを使用して匿名の使用状況データを収集し、将来の製品機能や改善に役立てます。データ収集はデフォルトで有効になっています。

使用状況データの収集とアップロードを変更するには、Scout UIの**設定**ギアをクリックします。その後、**はい**または**いいえ**を選択し、**保存**をクリックして情報を送信するかどうかを選択できます。



Call Home の主要データポイント

Call Home は、以下の主要データポイントを収集します。

(M) = 手動収集時のみ取得 (PowerShell コマンドレット `Start-CitrixCallHomeUpload`)

ファイル名	カテゴリ	データグループ

		マシン
		エックスディーサイト
		サイト情報
		ブローカーDB情報 (M)
		インストールされているDBバージョン (M)
		ブローカーサービスステータス (M)
		登録済みサービスインスタンス (M)
		ブローカーライセンステスト (M)
		アクティブなHDX™セッション (M)
		ブローカー管理者
		ブローカー管理者権限
		RDS構成 (LicensingSettings、SessionSettings、SpecifiedLicenseServers、およびRegisteredLicenseServersを含む)
		監視サービス (M) (MonitorConfiguration、MonitorDataStore、MonitorDBConnection、MonitorDBSchemaVersion、MonitorService、MonitorServiceAddedCapability、MonitorServiceInstance、MonitorServiceStatus、およ

		びMonitorInstalledDBVersion を含む)
		構成ログ
		接続ログ
		ハイパーバイザー接続 (M)
		ブローカーハイパーバイザー接続
		ハイパーバイザーアラート
		カタログ
		マルチセッションOSエージェント (M)
		シングルセッションOSエージェント (M)
		公開アプリケーション
		デリバリー グループ
		構成済みデリバリーエージェント

		Citrixインストール済みコンポーネント
		Citrix Brokerサービス情報
		ブローカーサービス構成ファイル
		Machine Creation Services™ 構成ファイル
		ホストサービス構成ファイル
		AD IDサービス構成ファイル

		構成サービス構成ファイル
		構成ログサービス構成ファイル
		委任管理サービス構成ファイル
		環境テストサービス構成ファイル
		監視サービス構成ファイル
		Storefront™ サービス構成ファイル
		ワークステーションエージェント構成ファイル
		Citrix VDA情報
		Citrix XD ホットフィックス
		Citrix_VirtualChannel_Graphics_Enum
		Citrix_VirtualChannel_Flash_Enum
		Citrix_VirtualChannel_Printer_Enum

		コンピューター
		BIOS
		メモリ情報
		プロセッサ
		PNP デバイス
		デバイス

		ディスクドライブ
		論理ドライブ
		ページファイル使用状況
		ネットワークアダプター
		ネットワークアダプター構成
		ipConfig
		ビデオコントローラー
		IDE コントローラー
		SCSI コントローラー

		HKLM:\Software\Wow6432Node\Citrix
		HKLM:\System\CurrentControlSet\Control\Citrix
		HKLM:\SOFTWARE\Policies\Citrix
		HKLM:\Software\Microsoft\Cryptography
		HKLM:\Software\Wow6432Node\Microsoft\Cryptography
		HKLM:\Software\Microsoft\Windows NT\CurrentVersion\Windows

		HKLM:\Software\Microsoft\Windows NT\CurrentVersion\Winlogon
		HKLM:\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
		HKLM:\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Policies\Explorer
		HKLM:\SYSTEM\CurrentControlSet\Control\Print\Environments
		HKLM:\System\CurrentControlSet\Control\セッションマネージャー
		HKLM:\System\CurrentControlSet\Control\ターミナルサーバー
		HKCU:\Control Panel\Desktop
		HKLM:\SOFTWARE\Classes\ShockwaveFlash.ShockwaveFlash\CurVer
		HKLM:\SYSTEM\CurrentControlSet\Control\SystemInformation
		HKLM:\SYSTEM\CurrentControlSet\Control\FileSystem

		HKLM: \SYSTEM\CurrentControlSet\ Control\Windows
		HKLM: \SYSTEM\CurrentControlSet\ Control\TimeZoneInformation

		ドライバー
		EnvVariables
		OS
		プロセス
		サービス
		サービスパック
		ジーピーリザルト
		Microsoft ホットフィックス
		ネットスタット
		PNP ドライバー

		システムイベントログ
		AOT (常時オンのトレース)
		クラッシュダンプ

		アップタイム
		メモリ
		コンピューターシステム
		プロセッサ

		ビデオコントローラー
		ディスクドライブ
		ブラウザ情報
		再起動回数
		メモリ使用量
		ディスク使用量
		ICAセッション解像度
		ICAカラー深度
		メタインストーラーCEIPマシンID

		ストア数
		サーバーグループ内のサーバー数
		ストアあたりのDelivery Controller™数
		HTTPS有効
		Citrix Receiver™のクラシックエクスペリエンスが有効
		Citrix レシーバー 用の HTML5 レシーバー設定
		Citrix Receiver向けワークスペースコントロールの有効化
		ストア向けリモートアクセスの有効化
		ゲートウェイ数

		統合されたNetScaler®認証用の明示的なJSONサービス

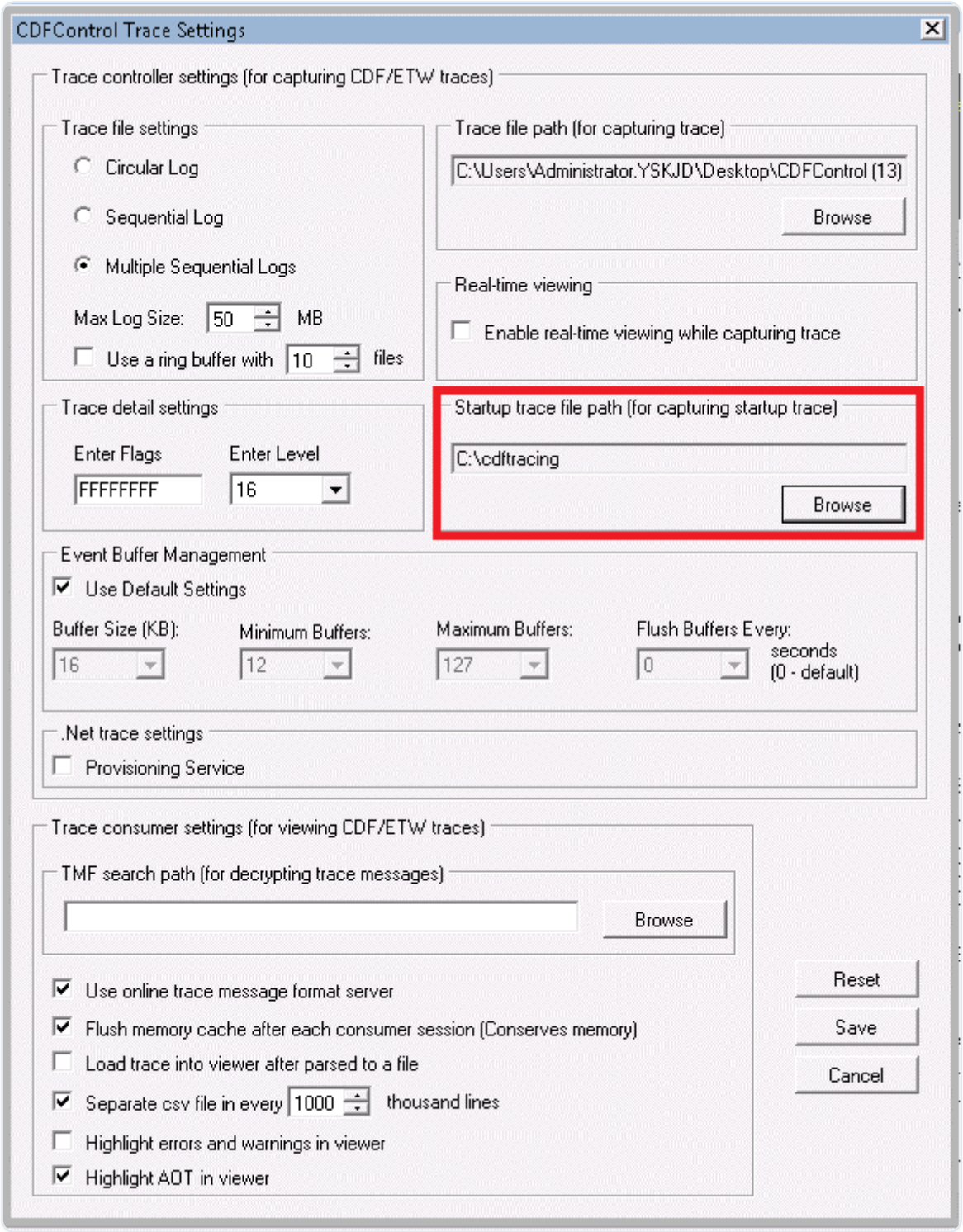
システム起動時にCitrix Diagnostic Facility (CDF) トレースを収集する

CDFControlユーティリティは、さまざまなCitrixトレースプロバイダーから表示されるCitrix Diagnostic Facility (CDF) トレースメッセージをキャプチャするためのイベントトレースコントローラーまたはコンシューマーです。これは、複雑なCitrix関連の問題のトラブルシューティング、フィルターサポートの解析、およびパフォーマンスデータの収集を目的としています。CDFControlユーティリティをダウンロードするには、CTX111961を参照してください。

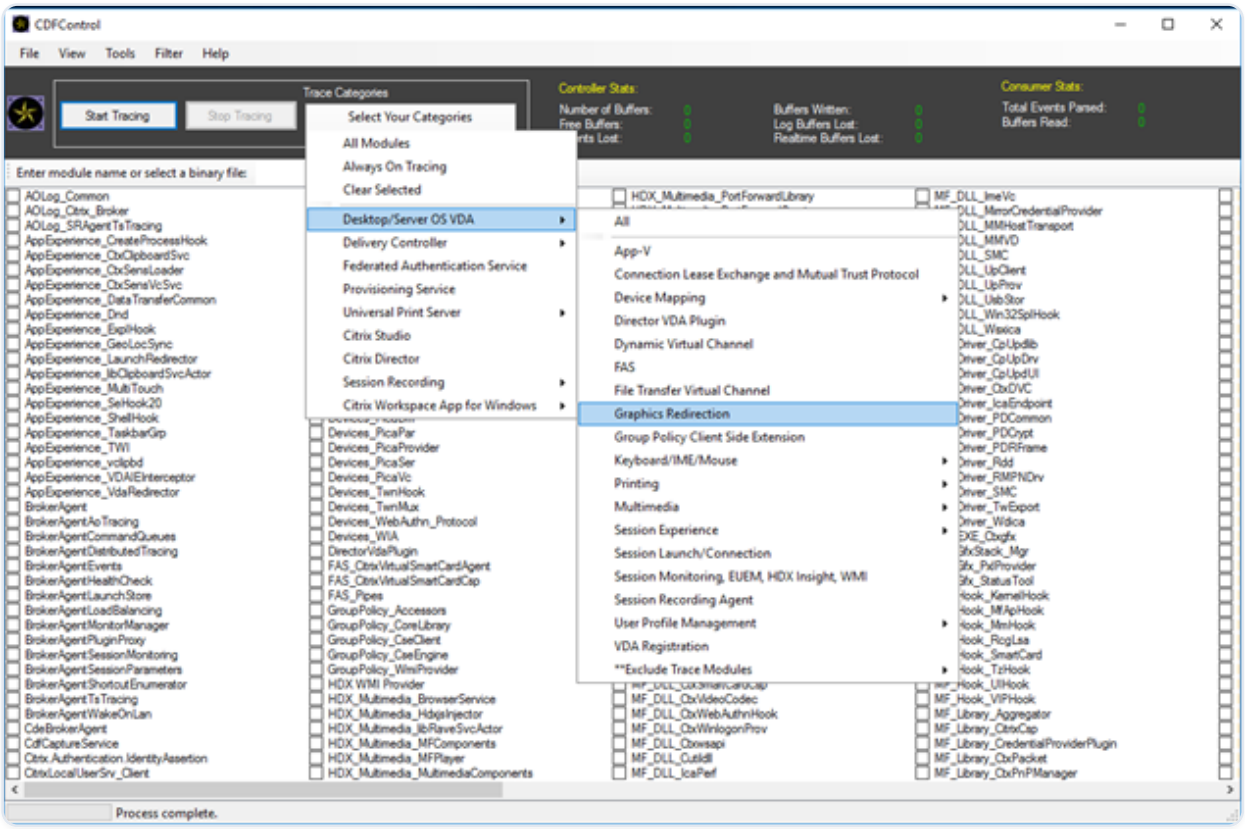
システム起動時にトレースを収集する

システム起動時にCDFトレースを収集するには、次の手順を使用します。管理者権限が必要です。

1. **CDFControl**を起動し、**ツール**メニューから**オプション**を選択します。
2. **起動トレースをキャプチャするための起動トレースファイルパス**セクションでトレースファイルパスを指定します。次に、**保存**をクリックします。



3. Citrixサポートが推奨する**トレースカテゴリ**を選択します。（以下の例では、**グラフィックリダイレクト**が選択されています。この選択は単なる例です。トラブルシューティングしている特定の問題に対してプロバイダーを有効にすることをお勧めします。）



4. **起動トレース**を選択し、**ツール**メニューから**有効にする**を選択します。

   有効にするを選択すると、アニメーションバーがスクロールを開始します。このアクティビティは手順に影響しません。次のステップに進みます。

5. **起動トレース**が有効になったら、**CDFControlユーティリティ**を閉じ、システムを再起動します。

6. **CDFControl**ユーティリティを起動します。システムが再起動し、エラーが表示されたら、**ツール**メニューから**起動トレース**を選択し、**無効にする**をクリックして起動トレースを無効にします。

7. 手順2で指定したトレースファイルパスに移動し、分析のためにトレースログファイル（.etl）を収集します。

委任管理

> **注：**

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

委任管理モデルは、ロールベースおよびオブジェクトベースの制御を使用して、組織が管理アクティビティを委任する方法に合わせる柔軟性を提供します。委任管理は、あらゆる規模の展開に対応し、展開の複雑さが増すにつれて、より詳細な権限の粒度を構成できるようにします。委任管理では、管理者、ロール、スコープという3つの概念を使用します。

- **管理者:** 管理者は、Active Directoryアカウントによって識別される個人またはグループを表します。各管理者は、1つ以上の役割とスコープのペアに関連付けられています。
- **ロール:** ロールは職務を表し、それに関連付けられた定義済みの権限を持ちます。たとえば、Delivery Group Administratorロールには、「Delivery Groupの作成」や「Delivery Groupからのデスクトップの削除」などの権限があります。管理者はサイトに対して複数のロールを持つことができるため、ある人物がDelivery Group AdministratorとMachine Catalog Administratorの両方になることができます。ロールは組み込みまたはカスタムにすることができます。

  組み込みロールは次のとおりです。

ロール	権限
フル管理者	すべてのタスクと操作を実行できます。フル管理者 (Full Administrator) は常に「すべて」のスコープと組み合わされます。
読み取り専用管理者	グローバル情報に加えて、指定されたスコープ内のすべてのオブジェクトを表示できますが、何も変更することはできません。たとえば、Scope=Londonの読み取り専用管理者 (Read Only Administrator) は、すべてのグローバルオブジェクト（構成ログなど）と、ロンドンにスコープが設定されたオブジェクト（ロンドンデリバリーグループなど）を表示できます。ただし、その管理者はニューヨークのスコープ内のオブジェクトを表示できません（ロンドンとニューヨークのスコープが重複しないと仮定した場合）。
ヘルプデスク管理者	デリバリーグループを表示し、それらのグループに関連付けられたセッションとマシンを管理できます。監視対象のデリバリーグループの「マシンカタログ」とホスト情報を表示できます。また、それらのデリバリーグ

ロール	権限
	ループ内のマシンのセッション管理およびマシン電源管理操作を実行できます。
マシンカタログ管理者	マシンカタログを作成および管理し、それらにマシンをプロビジョニングできます。仮想化インフラストラクチャ、Provisioning Services、および物理マシンからマシンカタログを構築できます。このロールはベースイメージを管理し、ソフトウェアをインストールできますが、アプリケーションやデスクトップをユーザーに割り当てることはできません。
デリバリーグループ管理者	アプリケーション、デスクトップ、およびマシンを配信できます。また、関連するセッションを管理できます。ポリシーや電源管理設定などのアプリケーションおよびデスクトップ構成も管理できます。
ホスト管理者	ホスト接続とその関連リソース設定を管理できます。ユーザーにマシン、アプリケーション、またはデスクトップを配信することはできません。

特定の製品エディションでは、組織の要件に合わせてカスタムロールを作成し、より詳細な権限を委任できます。カスタムロールを使用して、コンソールでのアクションまたはタスクの粒度で権限を割り当てることができます。

- **スコープ:** スコープはオブジェクトの集合を表します。スコープは、組織に関連する方法でオブジェクトをグループ化するために使用されます（たとえば、営業チームが使用するデリバリーグループのセットなど）。オブジェクトは複数のスコープに属することができます。オブジェクトが1つ以上のスコープでラベル付けされていると考えることができます。組み込みスコープは1つだけあり、それはすべてのオブジェクトを含む「すべて」です。フル管理者ロールは常に「すべて」スコープとペアになります。

例

XYZ社は、部門（経理、営業、倉庫）とデスクトップオペレーティングシステム（Windows 7またはWindows 8）に基づいてアプリケーションとデスクトップを管理することにしました。管理者

は5つのスコープを作成し、各デリバリーグループに2つのスコープをラベル付けしました。1つは使用される部門用、もう1つは使用されるオペレーティングシステム用です。

次の管理者が作成されました。

管理者	ロール	スコープ
domain/fred	フル管理者	すべて (フル管理者ロールは常に「すべて」スコープを持ちます)
domain/rob	読み取り専用管理者	すべて
domain/heidi	読み取り専用管理者、ヘルプデスク管理者	すべての営業
domain/warehouseadmin	ヘルプデスク管理者	倉庫
domain/peter	デリバリーグループ管理者、マシンカタログ管理者	Win7

- Fredはフル管理者であり、システム内のすべてのオブジェクトを表示、編集、削除できます。
- Robはサイト内のすべてのオブジェクトを表示できますが、それらを編集または削除することはできません。
- Heidiはすべてのオブジェクトを表示でき、Salesスコープ内のデリバリーグループに対してヘルプデスクタスクを実行できます。これにより、彼女はそれらのグループに関連付けられたセッションとマシンを管理できます。ただし、マシンの追加や削除など、デリバリーグループに変更を加えることはできません。
- warehouseadmin Active Directoryセキュリティグループのメンバーである人は誰でも、Warehouseスコープ内のマシンを表示し、ヘルプデスクタスクを実行できます。
- PeterはWindows 7のスペシャリストであり、すべてのWindows 7マシンカタログを管理でき、どの部署スコープに属していても、Windows 7アプリケーション、デスクトップ、およびマシンを提供できます。管理者は、PeterをWin7スコープのフル管理者にすることを検討しました。しかし、フル管理者は「サイト」や「管理者」など、スコープが設定されていないすべてのオブジェクトに対しても完全な権限を持つため、彼女はこれに反対しました。

委任管理の使用方法

一般的に、管理者の数と権限の粒度は、展開の規模と複雑さによって異なります。

- 小規模な展開や概念実証の展開では、1人または数人の管理者がすべての作業を行います。委任はありません。この場合、各管理者を、すべてのスコープを持つ組み込みのフル管理者ロールで作成します。
- マシン、アプリケーション、デスクトップが多い大規模な展開では、より多くの委任が必要です。複数の管理者が、より具体的な機能的責任（ロール）を持つ場合があります。たとえば、2人がフル管理者で、他の管理者がヘルプデスク管理者である場合があります。また、管理者がマシンカタログなど、特定のオブジェクトグループ（スコープ）のみを管理する場合もあります。この場合、新しいスコープを作成し、組み込みロールのいずれかと適切なスコープを持つ管理者を作成します。
- さらに大規模な展開では、より多くの（またはより具体的な）スコープと、型にはまらないロールを持つ異なる管理者が必要になる場合があります。この場合、より多くのスコープを編集または作成し、カスタムロールを作成し、既存および新規のスコープに加えて、組み込みまたはカスタムロールを持つ各管理者を作成します。

柔軟性と構成の容易さのために、管理者を作成するときにスコープを作成できます。マシンカタログまたは接続を作成または編集するときにスコープを指定することもできます。

管理者の作成と管理

ローカル管理者としてサイトを作成すると、ユーザーアカウントは自動的に、すべてのオブジェクトに対する完全な権限を持つフル管理者になります。サイトが作成された後、ローカル管理者には特別な権限はありません。

フル管理者ロールには常にすべてのスコープが割り当てられます。これは変更できません。

既定では、管理者は有効になっています。管理者を今作成しても、その人が後で管理業務を開始しない場合は、管理者を無効にする必要があるかもしれません。既存の有効な管理者については、オブジェクト/スコープを再編成している間に複数人を無効にし、更新された構成で稼働準備が整ったときに再度有効にしたい場合があります。有効なフル管理者がいなくなる場合、フル管理者を無効にすることはできません。管理者の作成、コピー、または編集時に、有効/無効チェックボックスが利用可能です。

管理者をコピー、編集、または削除する際にロール/スコープのペアを削除すると、その管理者に対するロールとスコープ間の関連付けのみが削除されます。ロールまたはスコープ自体は削除されません。また、そのロール/スコープのペアで構成されている他の管理者には影響しません。

管理者を作成および管理するには、次の手順に従います。

1. Web Studioにサインインし、左側のペインで**管理者**をクリックし、次に**管理者**タブをクリックします。

2. 実行するタスクの手順に従います。

   - **管理者を作成する:** アクションバーで**管理者を作成**をクリックします。ユーザーアカウント名を入力または参照し、スコープを選択または作成し、ロールを選択します。新しい管理者は既定で有効になっています。これは変更できます。
   - **管理者をコピーする:** 管理者を選択し、アクションバーで**管理者をコピー**をクリックします。ユーザーアカウント名を入力または参照します。ロール/スコープのペアを選択して編集または削除したり、新しいペアを追加したりできます。新しい管理者は既定で有効になっています。これは変更できます。
   - **管理者を編集する:** 管理者を選択し、アクションバーで**管理者を編集**をクリックします。ロール/スコープのペアを編集または削除したり、新しいペアを追加したりできます。
   - **管理者を削除する:** 管理者を選択し、アクションバーで**管理者を削除**をクリックします。有効なフル管理者がいなくなる場合、フル管理者を削除することはできません。

上部のペインには、作成した管理者が表示されます。管理者を選択すると、下部のペインにその詳細が表示されます。**警告**列は、管理者に関連付けられているロールとスコープのペアに、使用できないロールまたはスコープが含まれているかどうかを示します。関連付けられているロールとスコープのペアに、使用できないロールまたはスコープが含まれている場合、次の警告メッセージが表示されます。

- 関連付けられているロールまたはスコープが使用できません

> **重要:**
>
> 警告メッセージは、関連付けられているロールとスコープのペアに、使用できないロール、スコープ、またはその両方が含まれている場合にのみ表示されます。

> 管理者からロールとスコープのペアを削除するには、次のいずれかの手順を実行します。

- ロールとスコープのペアを削除します。

  a. アクションバーで、**管理者編集**をクリックします。

  b. **管理者名と詳細**ウィンドウで、役割とスコープのペアを選択し、**削除**をクリックします。

  c. 終了するには**保存**をクリックします。

- 管理者を削除します。

  a. アクションバーで、**管理者削除**をクリックします。

b. 確認ウィンドウで、**削除**をクリックします。

役割の作成と管理

管理者が役割を作成または編集する場合、自分自身が持っている権限のみを有効にできます。これにより、管理者が現在持っている権限よりも多くの権限を持つ役割を作成し、それを自分自身に割り当てたり（または既に割り当てられている役割を編集したりする）ことを防ぎます。

役割名には最大64個のUnicode文字を含めることができます。ただし、バックスラッシュ、スラッシュ、セミコロン、コロン、ポンド記号、コンマ、アスタリスク、疑問符、等号、左右の矢印、パイプ、左右の角括弧、左右の丸括弧、引用符、アポストロフィは含めることができません。説明には最大256個のUnicode文字を含めることができます。

組み込みの役割を編集または削除することはできません。カスタム役割が管理者によって使用されている場合、その役割を削除することはできません。

> **注：**
>
> 特定の製品エディションのみがカスタム役割をサポートしています。カスタム役割をサポートするエディションのみが、アクションバーに関連エントリを持っています。

役割を作成および管理するには、次の手順に従います。

1. Web Studioにサインインし、左ペインで**管理者**をクリックし、**役割**タブをクリックします。
2. 完了したいタスクの手順に従います。

   - **役割の詳細を表示:** 役割を選択します。下部のペインに、役割のオブジェクトタイプと関連する権限が一覧表示されます。下部のペインにある**管理者**タブをクリックすると、現在この役割を持つ管理者の一覧が表示されます。
   - **カスタムロールの作成:** アクションペインで**ロールの作成**をクリックします。名前と説明を入力します。オブジェクトの種類と権限を選択します。
   - **ロールのコピー:** ロールを選択し、アクションバーで**ロールのコピー**をクリックします。必要に応じて、名前、説明、オブジェクトの種類、および権限を変更します。
   - **カスタムロールの編集:** ロールを選択し、アクションバーで**ロールの編集**をクリックします。必要に応じて、名前、説明、オブジェクトの種類、および権限を変更します。
   - **カスタムロールの削除:** ロールを選択し、アクションバーで**ロールの削除**をクリックします。プロンプトが表示されたら、削除を確定します。

スコープの作成と管理

サイトを作成するときに利用できるスコープは「すべて」スコープのみであり、これは削除できません。

次の手順でスコープを作成できます。管理者を作成するときにもスコープを作成できます。各管理者は、少なくとも1つのロールとスコープのペアに関連付けられている必要があります。デスクトップ、マシンカタログ、アプリケーション、またはホストを作成または編集するときに、それらを既存のスコープに追加できます。スコープに追加しない場合、それらは「すべて」スコープの一部として残ります。

サイト作成はスコープ化できません。また、委任管理オブジェクト（スコープとロール）もスコープ化できません。ただし、スコープ化できないオブジェクトは「すべて」スコープに含まれます。（フル管理者は常に「すべて」スコープを持ちます。）マシン、電源アクション、デスクトップ、およびセッションは直接スコープ化されません。管理者は、関連するマシンカタログまたはデリバリーグループを通じて、これらのオブジェクトに対する権限を割り当てることができます。

スコープの作成と管理に関するルール:

- スコープ名には、最大64個のUnicode文字を含めることができます。スコープ名には、バックスラッシュ、スラッシュ、セミコロン、コロン、ポンド記号、コンマ、アスタリスク、疑問符、等号、左矢印、右矢印、パイプ、左角かっこまたは右角かっこ、左丸かっこまたは右丸かっこ、引用符、アポストロフィを含めることはできません。
- スコープの説明には、最大256個のUnicode文字を含めることができます。
- スコープをコピーまたは編集する際は、スコープからオブジェクトを削除すると、それらのオブジェクトに管理者がアクセスできなくなる可能性があることに留意してください。編集されたスコープが1つ以上のロールとペアになっている場合、スコープの更新によってどのロール/スコープのペアも使用できなくならないようにしてください。

スコープを作成および管理するには、次の手順に従います。

1. Web Studioにサインインし、左ペインで**管理者**をクリックしてから、**スコープ**タブをクリックします。
2. 完了したいタスクの手順に従います。

    - **スコープの作成:** アクションバーで**新しいスコープの作成**をクリックします。名前と説明を入力します。特定の種類のすべてのオブジェクト（例: デリバリーグループ）を含めるには、オブジェクトの種類を選択します。特定のオブジェクトを含めるには、種類を展開し、個々のオブジェクト（例: 営業チームが使用するデリバリーグループ）を選択します。

- **スコープをコピー:** スコープを選択し、アクションバーで**スコープのコピー**をクリックします。名前と説明を入力します。必要に応じて、オブジェクトの種類とオブジェクトを変更します。
- **スコープを編集:** スコープを選択し、アクションバーで**スコープの編集**をクリックします。必要に応じて、名前、説明、オブジェクトの種類、およびオブジェクトを変更します。
- **スコープを削除:** スコープを選択し、アクションバーで**スコープの削除**をクリックします。プロンプトが表示されたら、削除を確認します。

レポートの作成

委任管理レポートには、次の2種類を作成できます。

- 管理者に関連付けられている役割/スコープのペアと、各種類のオブジェクト（例：デリバリーグループとマシンカタログ）の個々の権限を一覧表示するHTMLレポート。このレポートはWeb Studioから生成します。

  このレポートを作成するには、次の手順に従います。

  a. Web Studioにサインインし、左ペインで「**管理者**」をクリックします。

  b. 管理者を選択し、アクションバーで「**レポートの作成**」をクリックします。

  管理者の作成、コピー、または編集時に、このレポートを要求することもできます。
- すべての組み込み役割とカスタム役割を権限にマッピングするHTMLまたはCSVレポート。このレポートは、OutputPermissionMapping.ps1という名前のPowerShellスクリプトを実行して生成します。

  このスクリプトを実行するには、フル管理者、読み取り専用管理者、または役割を読み取る権限を持つカスタム管理者である必要があります。スクリプトは、Program Files\Citrix\DelegatedAdmin\SnapIn\Citrix.DelegatedAdmin.Admin.V1\Scriptsにあります。

  構文：

  `OutputPermissionMapping.ps1 [-Help] [-Csv] [-Path string] [-AdminAddress string] [-Show] [CommonParameters]`

パラメーター	説明
`-Help`	スクリプトのヘルプを表示します。
`-Csv`	CSV出力を指定します。デフォルト = HTML

パラメーター	説明
`-Path string`	出力の書き込み先。デフォルト = stdout
`-AdminAddress string`	接続先のDelivery Controller™のIPアドレスまたはホスト名。デフォルト = localhost
`-Show`	(`-Path` パラメーターも指定されている場合にのみ有効) 出力をファイルに書き込むと、`-Show` によって出力がWebブラウザーなどの適切なプログラムで開かれます。
共通パラメーター	`Verbose`、`Debug`、`ErrorAction`、`ErrorVariable`、`WarningAction`、`WarningVariable`、`OutBuffer`、および `OutVariable`。詳細については、Microsoftのドキュメントを参照してください。

次の例では、HTMLテーブルをRoles.htmlという名前のファイルに書き込み、そのテーブルをWebブラウザーで開きます。

```
& "$env:ProgramFiles\Citrix\DelegatedAdmin\SnapIn\

Citrix.DelegatedAdmin.Admin.V1\Scripts\OutputPermissionMapping.ps1"

-Path Roles.html –Show
```

次の例では、CSVテーブルをRoles.csvという名前のファイルに書き込みます。テーブルは表示されません。

```
& "$env:ProgramFiles\Citrix\DelegatedAdmin\SnapIn\

Citrix.DelegatedAdmin.Admin.V1\Scripts\OutputPermissionMapping.ps1"

–CSV -Path Roles.csv
```

Windowsのコマンドプロンプトから、上記の例のコマンドは次のとおりです。

```
powershell -command "& '%ProgramFiles%\Citrix\DelegatedAdmin\SnapIn\

Citrix.DelegatedAdmin.Admin.V1\Scripts\OutputPermissionMapping.ps1'

-CSV -Path Roles.csv"
```

デリバリーコントローラー

注：

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

Delivery Controllerは、ユーザーアクセスの管理、接続の仲介と最適化を担当するサーバー側コンポーネントです。コントローラーは、デスクトップおよびサーバーイメージを作成するMachine Creation Services™も提供します。

サイトには少なくとも1つのコントローラーが必要です。最初のコントローラーをインストールした後、サイトの作成時または後でコントローラーを追加できます。サイトに複数のコントローラーを配置することには、主に2つの利点があります。

- **冗長性:** ベストプラクティスとして、本番サイトでは、常に異なる物理サーバー上に少なくとも2つのコントローラーを配置してください。1つのコントローラーが故障した場合でも、他のコントローラーが接続を管理し、サイトを管理できます。
- **スケーラビリティ:** サイトのアクティビティが増加すると、コントローラーのCPU使用率とデータベースのアクティビティも増加します。追加のコントローラーにより、より多くのユーザー、アプリケーション、およびデスクトップ要求を処理できるようになり、全体的な応答性を向上させることができます。

各コントローラーはサイトデータベースと直接通信します。複数のゾーンがあるサイトでは、各ゾーンのコントローラーは、プライマリゾーンのサイトデータベースと通信します。

重要:

> サイトの構成後、コントローラーのコンピューター名またはドメインメンバーシップを変更しないでください。

VDAがコントローラーに登録する方法

VDAを使用する前に、サイト内のDelivery Controllerに登録（通信を確立）する必要があります。VDA登録の詳細については、「VDA registration with Controllers」を参照してください。

コントローラーの追加、削除、または移動

コントローラーを追加、削除、または移動するには、「Databases」の記事に記載されているサーバーロールとデータベースロールの権限が必要です。

SQLクラスタリングまたはSQLミラーリングインストール内のノードにコントローラーをインストールすることはサポートされていません。

サイトにDelivery Controller™を追加するときは、高可用性のために使用するすべてのレプリカSQL Serverに、そのマシンのログオン資格情報を追加してください。

展開でデータベースミラーリングを使用している場合:

- コントローラーを追加、削除、または移動する前に、プリンシパルデータベースとミラーデータベースの両方が実行されていることを確認してください。さらに、SQL Server Management Studioでスクリプトを使用している場合は、スクリプトを実行する前にSQLCMDモードを有効にしてください。
- コントローラーを追加、削除、または移動した後にミラーリングを確認するには、PowerShell `Get-configdbconnection` コマンドレットを実行します。このコマンドレットは、ミラーへの接続文字列にフェールオーバーパートナーが設定されていることを確認します。

Controller を追加、削除、または移動した後:

- 自動更新が有効になっている場合、VDA は 90 分以内に更新された Controller のリストを受け取ります。
- 自動更新が有効になっていない場合は、すべての VDA で Controller ポリシー設定または ListOfDDCs レジストリキーが更新されていることを確認してください。Controller を別のサイトに移動した後、両方のサイトでポリシー設定またはレジストリキーを更新してください。

Controller を追加する

サイトの作成時および後から Controller を追加できます。このソフトウェアの以前のバージョンでインストールされた Controller を、このバージョンで作成されたサイトに追加することはできません。

1. サポートされているオペレーティングシステムを含むサーバーでインストーラーを実行します。Delivery Controller コンポーネントと、必要なその他のコアコンポーネントをインストールします。インストールウィザードを完了します。
2. まだサイトを作成していない場合は、この Controller で Citrix Site Manager を実行してサイトを作成します。この Controller の IP アドレスは、新しいサイトに自動的に追加されます。

   データベースを初期化するスクリプトを生成する予定がある場合は、スクリプトを生成する前に Controller を追加してください。
3. すでにサイトを作成している場合は、次の手順に従います。

   a. この Controller で Citrix Site Manager を実行し、 をクリックして、参加するサイトの Controller のアドレスを入力します。

   b. Web Studio に Controller を追加するには、Studio 構成ツール を実行します。

Controller を削除する

サイトから Controller を削除しても、Citrix ソフトウェアやその他のコンポーネントがアンインストールされるわけではありません。この操作は、Controller をデータベースから削除し、接続の仲介やその他のタスクに使用できなくするものです。Controller を削除しても、後で同じサイトまたは別のサイトに再度追加できます。サイトには少なくとも 1 つの Controller が必要であるため、Web Studio に表示されている最後の Controller を削除することはできません。

サイトから Controller を削除しても、データベースサーバーへの Controller のログオンは削除されません。これにより、同じマシン上の他の製品のサービスで使用されているログオンが誤って削除されるのを防ぎます。ログオンが不要になった場合は、手動で削除する必要があります。ログオンを削除するには、`securityadmin` サーバーロールの権限が必要です。

Controller を削除した後:

- 自動更新を使用しているVDAは、他の利用可能なコントローラーに再登録します。この再登録は、自動更新メカニズムが有効になっており、VDAが他のコントローラー（削除されたコントローラーと同じセカンダリゾーン内、またはオンプレミス展開のプライマリゾーン内）に到達できる場合にのみ発生します。
- Citrix StoreFrontでコントローラー情報を更新します。詳細については、「コントローラーの管理」を参照してください。

- Citrix StoreFrontで、Citrix Gatewayを介したリモートアクセス用のSecure Ticket Authority (STA) URLを更新します。詳細については、「Secure Ticket Authority の管理」を参照してください。
- Citrix Gatewayで、仮想サーバーのSTA URLを更新します。詳細については、「Citrix Gateway」を参照してください。

重要:

サイトからコントローラーを削除するまでは、Active Directoryからコントローラーを削除しないでください。

1. Web Studioが、削除するコントローラーをロードして表示できるように、コントローラーの電源がオンになっていることを確認してください。
2. Web Studioがコントローラーを完全にロードしたら、コントローラー上のすべてのサービスが実行されており、コントローラーの電源がオンのままであることを確認します。
3. Web Studioにサインインし、左ペインで を選択します。
4. タイルを見つけて、 をクリックします。
5. ページで、削除するコントローラーを選択します。
6. を選択します。適切なデータベースロールと権限がない場合は、データベース管理者がコントローラーを削除できるようにするスクリプトを生成するオプションが提示されます。

   Web Studioは、コントローラーを削除する前に事前チェックを実行します。コントローラーの電源がオフで、以下のサービスステータスではない場合、安全に削除できます。

   - 不明
   - 失敗保留中
   - 古いバージョン
   - 新しいバージョン
   - バージョン変更が進行中
   - 必須機能が不足しています

   Controller の電源がオフになっておらず、上記のいずれかのサービスステータスである場合、Web Studio は Controller の電源をオフにするよう求めます。
7. データベースサーバーから Controller のマシンアカウントを削除する必要があります。削除する前に、別サービスがそのアカウントを使用していないことを確認してください。

Web Studio を使用して Controller を削除した後、現在のタスクが適切に完了するように、その Controller へのトラフィックがしばらく残る場合があります。短時間で Controller の削除を強制したい場合は、Citrix は、インストールされていたサーバーをシャットダウンするか、そのサーバーを Active Directory から削除することを推奨します。その後、サイト上の他の Controller を再起動して、削除された Controller とのそれ以上の通信がないことを確認してください。

Controller を別のゾーンに移動する

サイトに複数のゾーンが含まれている場合、Controller を別のゾーンに移動できます。この移動が VDA 登録やその他の操作にどのように影響するかについては、「ゾーン」を参照してください。

1. 左ペインで を選択します。
2. 中央ペインでゾーンを選択し、Controller を選択します。
3. アクションバーで を選択します。
4. 表示される ページで、Controller を移動するゾーンを選択します。
5. 「**保存**」をクリックします。

VDA を別のサイトに移動する

Citrix Provisioning™ を使用してプロビジョニングされた VDA、または既存のイメージである VDA は、アップグレード時や、テストサイトで作成された VDA イメージを本番サイトに移動する際に、別のサイト（サイト 1 からサイト 2 へ）に移動できます。Machine Creation Services (MCS) を使用してプロビジョニングされた VDA は、あるサイトから別のサイトに移動できません。MCS は、VDA が Controller に登録するためにチェックする ListOfDDCs の変更をサポートしていません。MCS を使用してプロビジョニングされた VDA は、常に作成されたサイトに関連付けられた ListOfDDCs をチェックします。

VDA を別のサイトに移動する方法は、インストーラーを使用する方法と Citrix ポリシーを使用する方法の 2 つがあります。

インストーラー

インストーラーを実行し、サイト2のControllerのFQDN（DNSエントリ）を指定してControllerを追加します。

インストーラーでControllerを指定するのは、Controllerポリシー設定が使用されていない場合のみです。

グループポリシーエディター

次の例では、複数のVDAをサイト間で移動します。

1. サイト1で以下の設定を含むポリシーを作成し、そのポリシーをデリバリーグループレベルにフィルターして、サイト間の段階的なVDA移行を開始します。
   - Controller: サイト2の1つ以上のControllerのFQDN（DNSエントリ）を含みます。
   - Controllerの自動更新を有効にする: 無効に設定します。
2. デリバリーグループ内の各VDAは、新しいポリシーが適用されてから90分以内に通知を受け取ります。VDAは受信したControllerのリストを無視し（自動更新が無効になっているため）、ポリシーで指定されたControllerの1つを選択します。このポリシーにはサイト2のControllerがリストされています。
3. VDAがサイト2のControllerに正常に登録されると、サイト2のListOfDDCsとポリシー情報を受け取ります。これらはデフォルトで自動更新が有効になっています。VDAがサイト1で登録されていたControllerは、サイト2のControllerから送信されたリストには含まれていません。そのため、VDAはサイト2のリストにあるControllerの中から選択して再登録します。それ以降、VDAはサイト2からの情報で自動的に更新されます。

グループポリシーエディターの使用方法については、Citrixポリシーのドキュメントを参照してください。

IPv4/IPv6 のサポート

このリリースでは、純粋な IPv4、純粋な IPv6、および重複する IPv4 と IPv6 ネットワークを使用するデュアルスタック展開をサポートしています。

次のコンポーネントは IPv4 のみをサポートします。その他すべてのコンポーネントは IPv4 と IPv6 をサポートします。

- XenServer®
- **IPv6 Controller 登録のみを使用**ポリシー設定によって制御されていないVirtual Delivery Agent (VDA)

IPv6 通信は、VDA 接続に関連する2つの Citrix® ポリシー設定によって制御されます。

- **IPv6 の使用を強制する主要な設定:** IPv6 Controller 登録のみを使用。

  このポリシー設定は、VDA が Delivery Controller に登録するために使用するアドレス形式を制御します。

  有効にすると、VDA は次の優先順位で選択された単一の IPv6 アドレスを使用して Controller と登録および通信します: グローバル IP アドレス、ユニークローカルアドレス (ULA)、リンクローカルアドレス (他の IPv6 アドレスが利用できない場合のみ)。

無効にすると、VDA はマシンの IPv4 アドレスを使用して Controller と登録および通信します。これがデフォルト値です。

チームが頻繁に IPv6 ネットワークを使用する場合は、**IPv6 Controller 登録のみを使用**ポリシー設定が有効になっているイメージまたは組織単位 (OU) に基づいて、それらのユーザー向けにデスクトップとアプリケーションを公開します。

チームが頻繁に IPv4 ネットワークを使用する場合は、**IPv6 Controller 登録のみを使用**ポリシー設定が無効になっているイメージまたは OU に基づいて、それらのユーザー向けにデスクトップとアプリケーションを公開します。

- **IPv6 ネットマスクを定義する依存設定:** Controller 登録 IPv6 ネットマスク。

  マシンは複数の IPv6 アドレスを持つことができます。このポリシー設定により、管理者は、登録されている場合に、VDA をグローバル IP ではなく、優先サブネットのみに制限できます。この設定は、VDA が登録するネットワークを指定します。VDA は、指定されたネットマスクに一致する最初のアドレスにのみ登録します。

  この設定は、**IPv6 Controller 登録のみを使用**ポリシー設定が有効になっている場合にのみ有効です。デフォルト = 空の文字列

展開に関する考慮事項

環境に IPv4 と IPv6 の両方のネットワークが含まれている場合は、IPv4 のみのクライアントと IPv6 ネットワークにアクセスできるクライアント用に個別のデリバリーグループ構成を作成します。ユーザーを区別するために、命名、手動の Active Directory グループ割り当て、または SmartAccess フィルターの使用を検討してください。 接続が IPv6 ネットワークで開始され、その後 IPv4 アクセスのみを持つクライアントから再接続しようとすると、セッションの再接続が失敗する可能性があります。

注記 - DNS解決が有効になっている場合は、これらの考慮事項は適用されません。

Web Studio を使用した Citrix Virtual Apps and Desktops™ のライセンス

> **注:**
>
> - Citrix Virtual Apps and Desktops の展開は、Web Studio (Web ベース) と Citrix Studio (Windows ベース) の 2 つの管理コンソールを使用して管理できます。この記事では Web

Studio のみを取り上げます。Citrix Studio については、Citrix Virtual Apps and Desktops 7 2212 以前の同等の記事を参照してください。

- License Activation Service (LAS) は、従来の Citrix® レガシーライセンスに代わる新しいクラウドベースのライセンスソリューションです。LAS はアクティベーション用の新しいモジュールを導入し、ライセンス管理へのシームレスで最新のアプローチを保証します。詳細については、「License Activation Service」を参照してください。

Web Studio から、ライセンスサーバーが Web Studio と同じドメイン内にあるか、信頼されたドメイン内にある場合、ライセンスを管理および追跡できます。ライセンスタスクの詳細については、「ライセンスドキュメント」および「複数タイプのライセンス」を参照してください。

次の表に、サポートされているエディションとライセンスモデルを示します。

製品	エディション	ライセンスモデル
シトリックス バーチャル アプリ	プレミアム、アドバンスト、スタンダード	同時使用
シトリックス バーチャル デスクトップ	プレミアム、アドバンスト、スタンダード	ユーザー/デバイスおよび同時使用

詳細については、「同時使用ライセンス」および「ユーザー/デバイスライセンス」を参照してください。

サポートされている現在のリリース (CR) および長期サービスリリース (LTSR) のバージョン

次の表に、Citrix Virtual Apps and Desktops、XenApp、およびXenDesktopの**最小互換LSバージョン**を示します。Citrix製品のライフサイクル日付の詳細については、「製品マトリックス」を参照してください。

重要:

次の表の情報は、製品の互換性のみを目的として提供されています。Citrixは、機能またはセキュリティの改善の恩恵を受けるために、常にCitrixライセンスサーバーの最新バージョンを使用することを強くお勧めします。

注:

License Server VPXは非推奨となり、今後のメンテナンスやセキュリティ修正は提供されません。License Server VPXのバージョン11.16.6以前を使用しているお客様は、できるだけ早くWindows用License Serverの最新バージョンに移行することをお勧めします。

現在のリリース	互換性のあるLSの最小バージョン
2305	11.17.2.0 ビルド 35000
2303	11.17.2.0 ビルド 35000
2212	11.17.2.0 ビルド 35000
2209	11.17.2.0 ビルド 35000
2206	11.17.2.0 ビルド 35000
2203	11.17.2.0 ビルド 35000
2112	11.17.2.0 ビルド 35000
2109	11.17.2.0 ビルド 35000
2106	11.17.2.0 ビルド 35000
2103	11.16.3.0 ビルド 28000

長期サービスリリース	互換性のあるLSの最小バージョン
2203 LTSR	11.17.2.0 ビルド 35000
1912 LTSR	11.16.3.0 ビルド 28000
7.15 LTSR	11.15.0.0 ビルド 24100
7.6 LTSR	11.14.0.1 ビルド 21103

レガシー製品および製品バージョンについては、「レガシー製品マトリックス」を参照してください。

以下のタスクを完了するには、完全なライセンス管理者である必要があります。Web Studioでライセンス情報を表示するには、管理者は少なくとも「ライセンスの読み取り」の委任管理権限を持っている必要があります。組み込みの「完全管理者」および「読み取り専用管理者」の役割には、その権限があります。

Web Studioを使用してCitrixからライセンスをダウンロードしてインストールする

1. Web Studioにサインインし、左ペインで**Licensing**を選択します。
2. アクションバーで**Allocate Licenses**を選択します。
3. ライセンスの購入または更新後にCitrixからメールで受け取ったライセンスアクセスコードを入力します。
4. 製品を選択し、**Allocate Licenses**を選択します。その製品で利用可能なライセンスが割り当てられ、ダウンロードされます。特定のライセンスアクセスコードのすべてのライセンスを割り当ててダウンロードした後、そのライセンスアクセスコードを再利用することはできません。同じコードで他のトランザクションを行うには、My Accountにログオンしてください。

ローカルコンピューターまたはネットワークに保存されているライセンスを追加する

1. Web Studioにサインインし、左ペインで**Licensing**を選択します。
2. アクションバーで**Add Licenses**を選択します。
3. ライセンスファイルを参照し、ライセンスサーバーに追加します。

ライセンスサーバーを変更する

1. Web Studioにサインインし、左ペインで**Licensing**を選択します。
2. アクションバーで**Change License Server**を選択します。
3. ライセンスサーバーのアドレスを*name:port*の形式で入力します。ここで、nameはDNS、NetBIOS、またはIPアドレスです。ポート番号を指定しない場合、デフォルトポート（27000）が使用されます。

使用するライセンスの種類を選択する

- サイトを構成する際、ライセンスサーバーを指定した後、使用するライセンスの種類を選択するよう求められます。サーバーにライセンスがない場合、ライセンスなしで製品を30日間試用するオプションが自動的に選択されます。

- サーバーにライセンスがある場合、その詳細が表示され、そのうちの1つを選択できます。または、ライセンスファイルをサーバーに追加してから、そのファイルを選択することもできます。

製品エディションとライセンスモデルを変更する

1. Web Studioにサインインし、左側のペインで**［ライセンス］**を選択します。
2. アクションバーで**［製品エディションの編集］**を選択します。
3. 適切なオプションを更新します。

License Administration Consoleにアクセスするには、アクションバーで**［License Administration Console］**を選択します。コンソールがすぐに表示されるか、ダッシュボードがパスワードで保護されている場合は、License Administration Consoleの資格情報の入力を求められます。コンソールの使用方法の詳細については、ライセンスドキュメントを参照してください。

> **注:**
>
> Web Studioでライセンスを切り替えると、Citrix Directorにその変更が反映されるまでに最大5分かかります。たとえば、AdvancedとPremiumを切り替える場合などです。

ライセンス管理者を追加する

1. Web Studioにサインインし、左側のペインで**［ライセンス］**を選択します。
2. **［ライセンス管理者］**タブを選択します。
3. アクションバーで**［ライセンス管理者の追加］**を選択します。
4. 管理者として追加するユーザーを参照し、アクセス許可を選択します。

ライセンス管理者のアクセス許可を変更またはライセンス管理者を削除する

1. Web Studioにサインインし、左側のペインで**［ライセンス］**を選択します。
2. **［ライセンス管理者］**タブを選択し、管理者を選択します。
3. アクションバーで**ライセンス管理者編集**または**ライセンス管理者削除**のいずれかを選択します。

ライセンス管理者グループを追加する

1. Web Studioにサインインし、左ペインで**ライセンス**を選択します。

2. **ライセンス管理者**タブを選択します。
3. アクションバーで**ライセンス管理者グループの追加**を選択します。
4. ライセンス管理者として機能させたいグループを参照し、権限を選択します。Active Directory グループを追加すると、そのグループ内のユーザーにライセンス管理者権限が付与されます。

ライセンス管理者グループの権限を変更または削除する

1. Web Studioにサインインし、左ペインで**ライセンス**を選択します。
2. **ライセンス管理者**タブを選択し、管理者グループを選択します。
3. アクションバーで**ライセンス管理者グループの編集**または**ライセンス管理者グループの削除**のいずれかを選択します。

ライセンス情報を表示する

Web Studioにサインインし、左ペインで**ライセンス**を選択します。サイトのライセンス使用状況と設定の概要が、指定されたライセンスサーバーに現在インストールされているすべてのライセンスのリストとともに表示されます。

製品タイプ、ライセンスエディション、ライセンスモデルを含むサイトのライセンス設定が、構成済みのライセンスサーバーが使用するライセンスと一致していることを確認してください。一致しない場合は、サイトのライセンス設定に合わせて既存のライセンスをダウンロードまたは割り当てる必要がある場合があります。

ライセンス有効期限アラートを表示する

Web Studioは、Citrix License Serverからライセンスファイルの有効期限を照会します。ライセンスファイルの有効期限が近づいているか、すでに期限切れになっている場合、Web Studioは概要タブで管理者に警告します。

ライセンス テレメトリ データを難読化する

ライセンス テレメトリで送信される情報の機密性を考慮し、Citrix はデータを難読化するオプションを提供します。

次の表に、難読化できるデータを示します。

フィールド	説明	例
ユーザー	セッション起動を開始するユーザーを一意に識別するた	- fullName: `C648FE671A44B3F7`

フィールド	説明	例
	めのユーザー ID を識別します。	
	- samName: `C758LH671A44B3F7`	
	- ユーピーエヌ: `C7948FE671A44B3F7`	
	- userLicenseId: `C265FE671A44B3F7`	
	- userSid: `C097FE671A44B3F7`	
デバイス -> デバイス名	デバイスのフレンドリ名を示します。	`C758LH671A44B3F7`
workerSid	セッションに使用されるVDA の一意の識別子を示します。	`1E5LH671A44B3F7`
AdminLoginList	一意の管理者SamAccountNameのリストを示します	`{AdminLoginList: [UFMJ+JvXOTHO9mQDsOweiw==]}`

スクランブルを有効または無効にするには、Delivery Controllerで次のPowerShellコマンドを実行します。

1. Delivery ControllerホストからPowerShellウィンドウを開きます。
2. コマンド `asnp citrix` を実行して、Citrix固有のPowerShellモジュールをロードします。
3. スクランブルを有効または無効にするには、次のコマンドを実行します。

   デフォルトでは、値は`1`または`true`であり、ライセンステレメトリデータのスクランブルを有効にします。

   無効にするには：

```
Set-BrokerServiceConfigurationData Core.ScrambleLicensingData
-SettingValue $false
```

スクランブルを無効にした後、次のコマンドを使用して有効にできます。

```
Set-BrokerServiceConfigurationData Core.ScrambleLicensingData
-SettingValue $true
```

関連リンク

- 年間および期間ベースの小売ライセンスのCitrixオンプレミスサブスクリプションを参照してください。
- ハイブリッド権限による移行とアップグレード (TTU)を参照してください。

ライセンスアクティベーションサービス

ライセンスアクティベーションサービス (LAS) は、従来のCitrix®レガシーライセンスに代わる、新しいクラウドベースのライセンスソリューションです。LASはアクティベーション用の新しいモジュールを導入し、ライセンス管理へのシームレスで最新のアプローチを保証します。

LASはCitrixライセンスエクスペリエンスを簡素化します。ライセンスサーバーで生成、ダウンロード、またはインストールするライセンスアクセスコードやファイルは不要になりました。ライセンスサーバーをアップグレードし、Citrix Cloudに登録するだけです。互換性のある製品がライセンスサーバーを指すように設定されると、自動的にアクティベートできます。

アクティベーション後、ライセンスサーバーはライセンスアクティベーションサービスと定期的に通信し、アクティベーションを最新の状態に保ちます。LASはクラウドテクノロジーで構築されており、パフォーマンスを向上させ、ダウンタイムがないことを保証します。何らかの理由でライセンスサーバーまたはLASに到達できない場合、システムはライセンスキャッシュモードに入ります。これは、システムがライセンスなしの状態になるのを防ぎ、停止を回避するように設計されています。詳細については、「ライセンスキャッシュモード」を参照してください。

LASの詳細については、ライセンスドキュメントの「ライセンスアクティベーションサービス」を参照してください。

前提条件

- ライセンスサーバーをバージョン11.17.2ビルド53100以降にインストールまたは更新します。
- ライセンスサーバー用の信頼性の高い継続的なインターネット接続。
- デスクトップグループレベルのライセンス設定は無効にする必要があります。

> **注:**

> DGレベルのライセンスが無効になっていることを確認するには、Get-brokerdesktopgroupを使用し、LicenseModelが「None」であることを確認してください。

考慮事項

- Citrix StudioまたはCitrix Web Studioがアクティベーションを促す前に、すべてのDelivery ControllerがLASと互換性がある必要があります。単一のコントローラーサイトは、レガシーライセンスまたはLASのいずれかを使用できます。
- 同じCitrix Cloud ID (CCID) またはOrgIDに複数のライセンスサーバーを登録できます。ただし、サイトは1つのライセンスサーバーのみを指すように構成できます。

制限事項

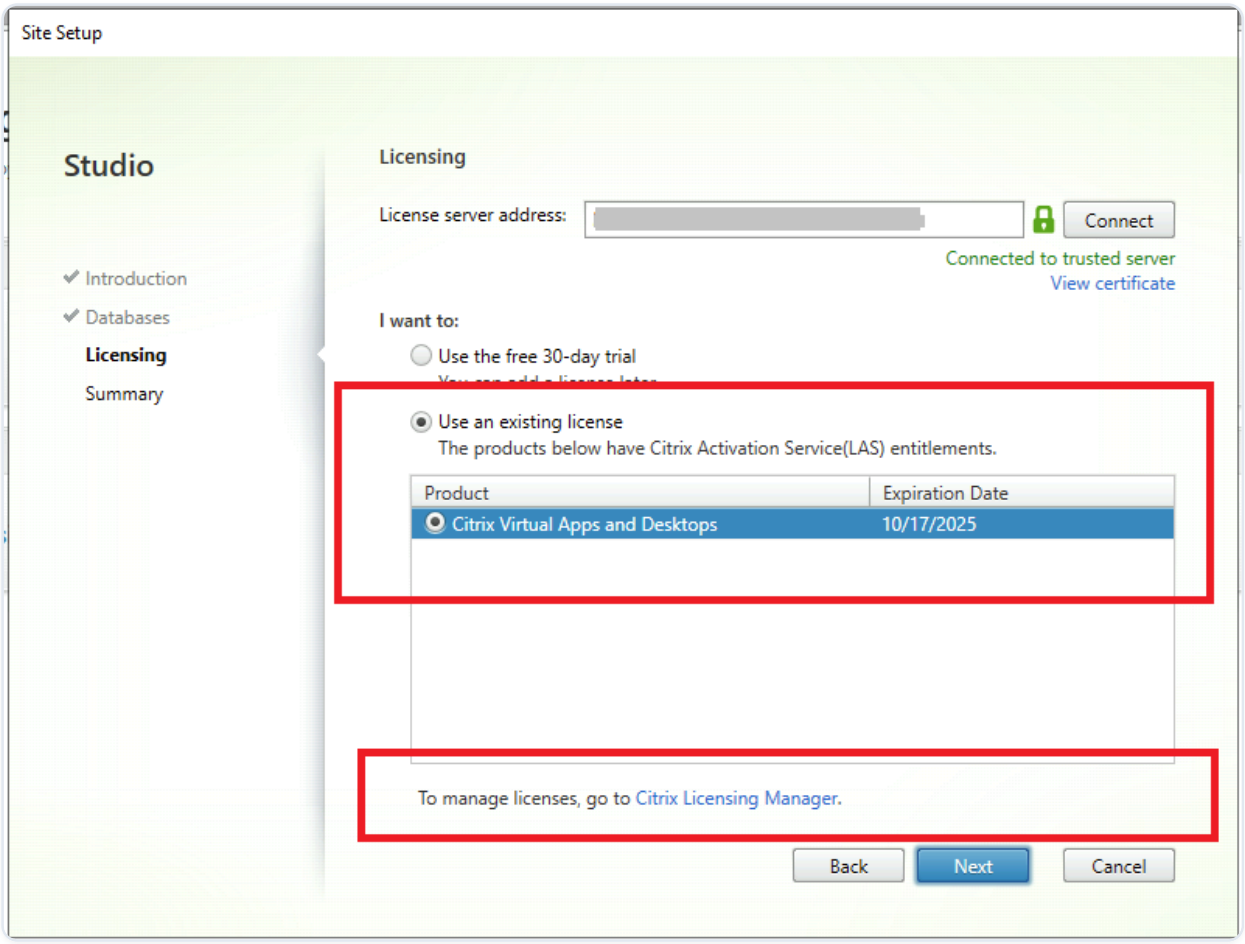
- LASへの移行により、製品エディションは**Premium**に、ライセンスモデルは**Concurrent**に設定されますが、これは将来変更される可能性があります。登録とセッション起動に影響を与える可能性があるため、PowerShellを使用してライセンス構成を変更しないでください。
- 既存のレガシーライセンスからLASへのCitrix Virtual Apps and Desktops™サイトの移行は、Web Studioのみを使用して行うことができます。

主な手順

1. ライセンスサーバーをバージョン11.17.2ビルド53100以降にインストールまたはアップグレードし、「ライセンスアクティベーションサービス用にライセンスサーバーを構成する方法」に記載されている手順に従ってLASを構成します。
2. Citrix Virtual Apps and Desktopsバージョン2402 LTSR CU3以降をインストールします。Citrix Delivery Controller、Citrix Studio、Web Studio、Citrix Directorなどのコアコンポーネントをインストールします。

   > **注:**
   >
   > Citrix Virtual Apps and DesktopsサイトのすべてのDelivery Controllerは、LASと互換性がある必要があります。

3. 必要なコンポーネントをインストールした後、Citrix Site Managerを使用してサイトを作成します。サイトの作成については、「サイトの作成」を参照してください。ライセンスサーバーがLASを使用するように構成されている場合、Metainstallerはエンタイトルメントを表示します。エンタイトルメントは、対応するライセンス有効期限とともに提供されます。



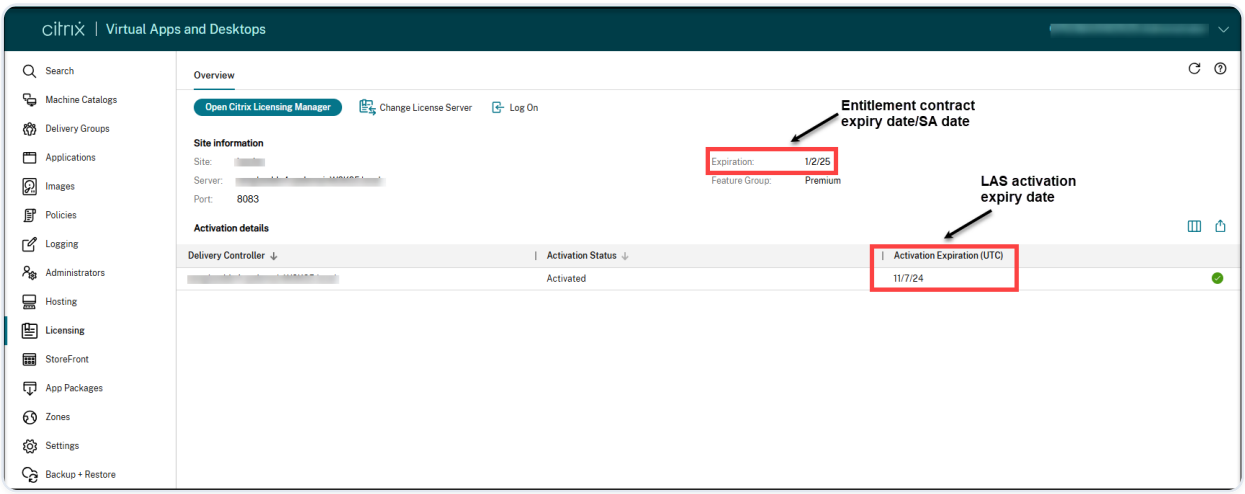
> **注:**
>
> ライセンスサーバーがバージョン53100以降にアップグレードされていない場合、ライセンスエラーが発生します。これらのエラーを無視してCVADサイトのアップグレードを続行すると、サイトが機能しなくなります。

4. ライセンスの詳細を確認する。
5. レガシーライセンスをLASに移行する。

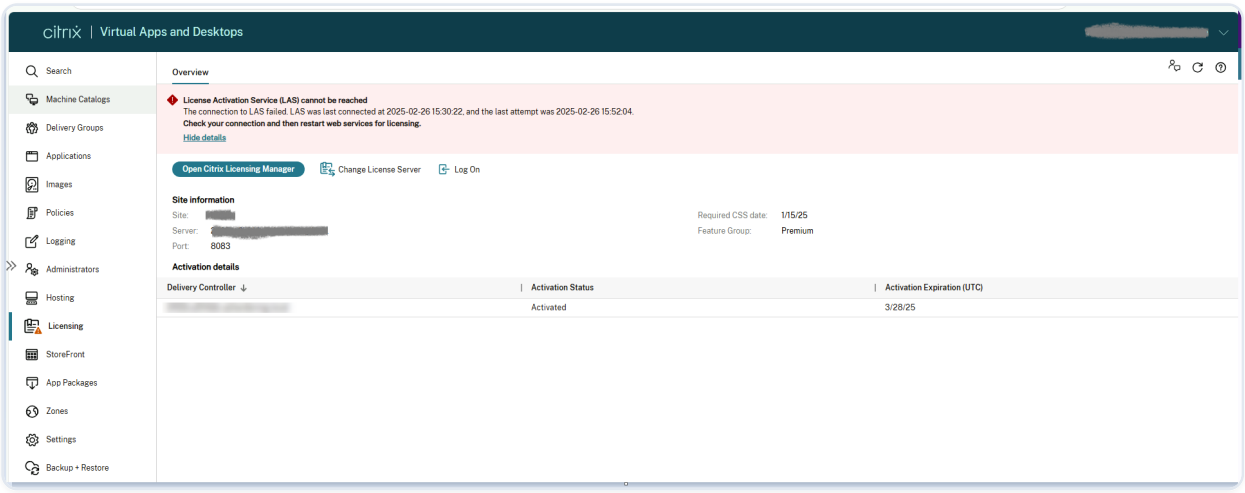
ライセンスの詳細を確認する

サイトを作成したら、Web Studioを使用してライセンスの詳細を確認します。

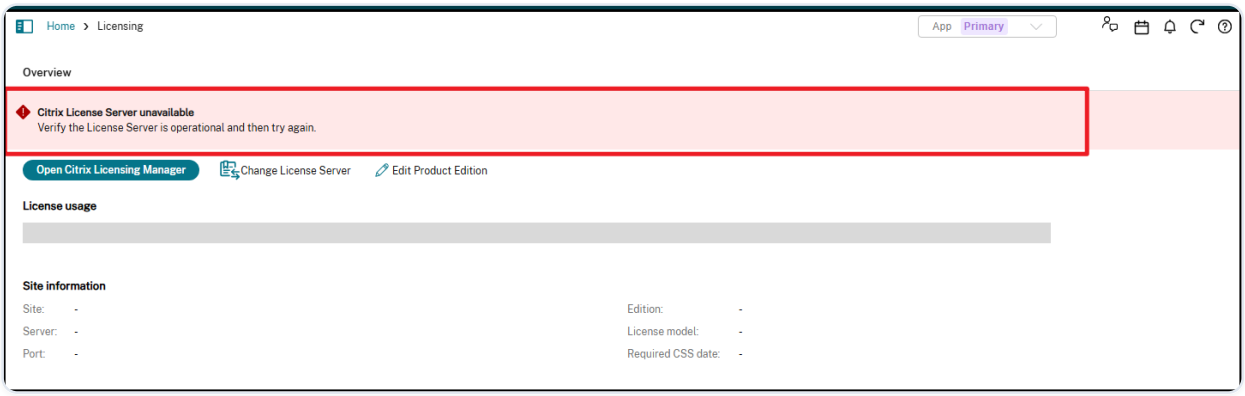
1. Web Studioで、**［ライセンス］**ノードを選択します。
2. **［概要］**タブで、Citrix Virtual Apps and Desktopsサイトに適切なライセンスがあるか、またはLAS機能の使用中にライセンスの有効期限が切れていないかを確認します。



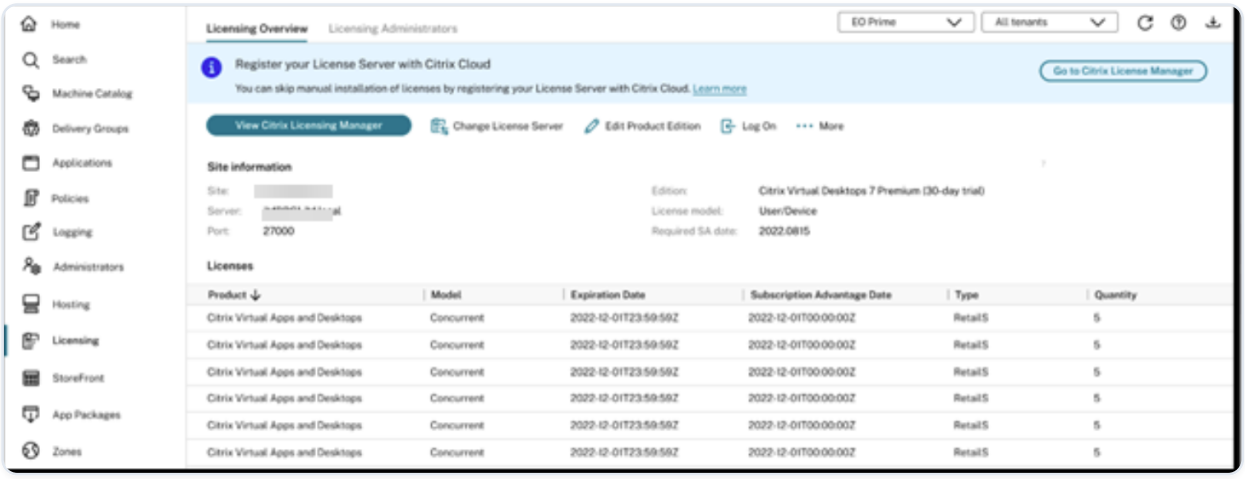
LASに到達できない場合、エラーメッセージが表示されることがあります。



ライセンスサーバーが利用できない場合、エラーメッセージが表示されることがあります。



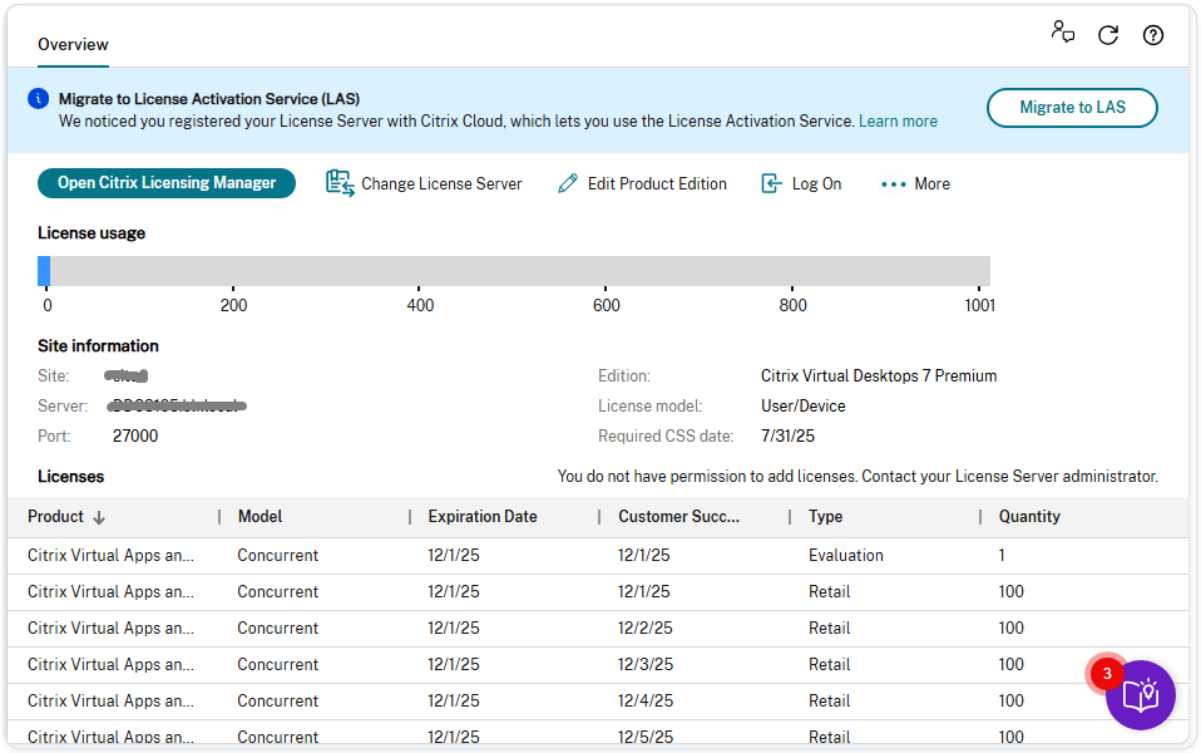
ライセンスサーバーがまだ古いレガシーライセンスを使用しており、Citrix Virtual Apps and DesktopsサイトがLAS対応である場合、Web Studioはライセンスサーバーをクラウドに登録するよう促します。



レガシーライセンスをLASに移行する

ライセンスサーバーをCitrix Cloudに登録済みで、必要なエンタイトルメントがある場合は、ユーザーセッションに影響を与えることなく、既存のCitrix Virtual Apps and Desktopsサイトをレガシーライセンスから LASに移行するために、以下の特定の順序に従う必要があります。

1. **ライセンスサーバーのアップグレード:** ライセンスサーバーをサポートされている最小バージョンにアップグレードします。
2. **Delivery Controllerのアップグレード:** サイト内のすべてのDelivery ControllerをLAS対応バージョンにアップグレードします。
3. **デリバリーグループのライセンス割り当てを削除:**
    - **LASに移行**をクリックする前に、サイトレベルより下で設定されているライセンス割り当て（つまり、デリバリーグループレベルのライセンス割り当て）を手動で削除します。
4. **割り当ての確認:** LASの割り当てが正確であることを確認します。
5. **LASに移行をクリック:**
    - 前の手順が完了したら、**LASに移行**をクリックします。



- LASに移行すると、Citrix Virtual Apps and Desktopsサイトの**ライセンスエディション**は**Citrix Virtual Apps and Desktops Premium**に設定され、**ライセンスモデル**は**同時接続**に構成されます。

LASからレガシーライセンスへのロールバック

LASからレガシーライセンスにロールバックするには、次の手順を実行します。

1. 次のPowerShellコマンドを実行します。

   ```
   Set-ConfigSite -UseLicenseActivationService $false
   ```

2. Web Studioでレガシーライセンスを構成します。

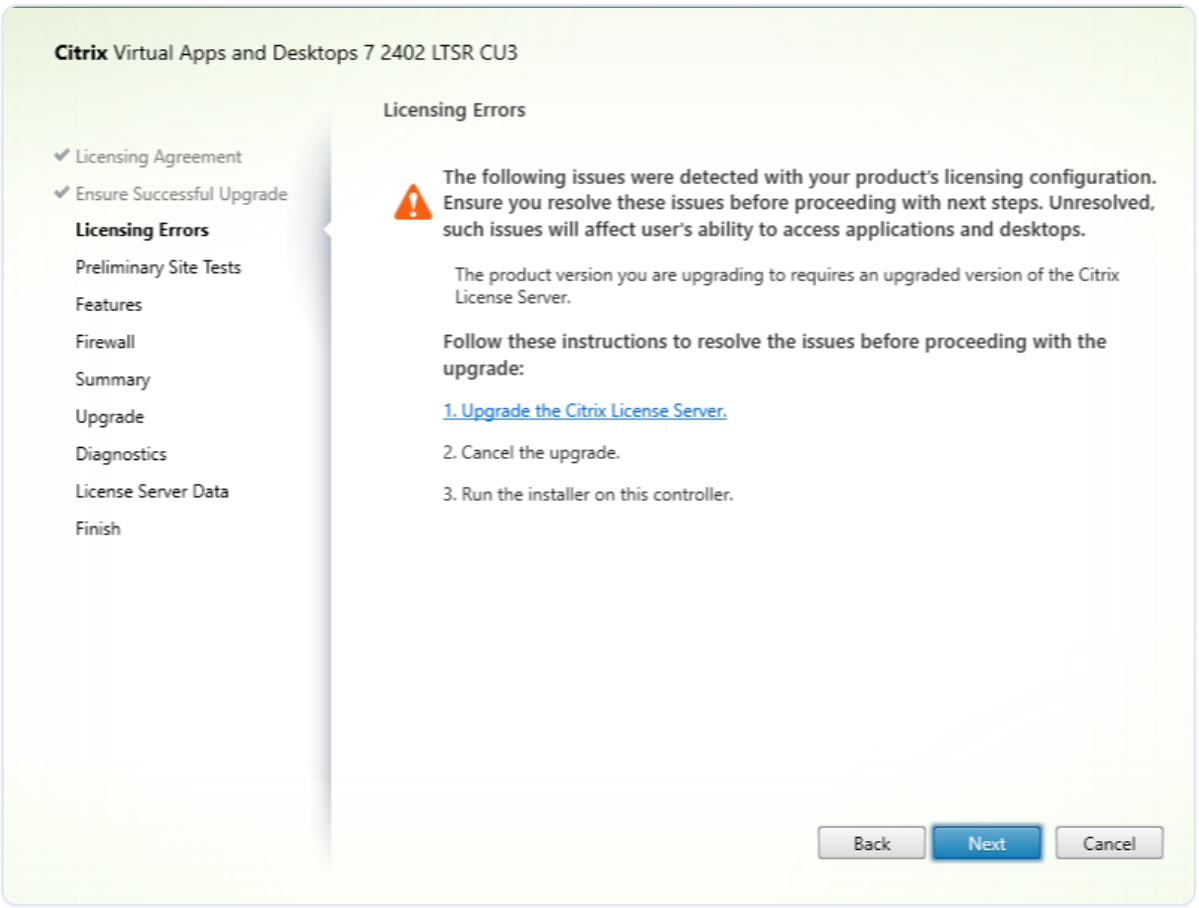
注：

これらの手順は、一時的なトラブルシューティングのみを目的としています。レガシーライセンスファイルは、サポート終了 (EOL) が近づいており、April 15, 2026以降は機能しません。中断のないサービスを確保するため、License Activation Service (LAS) への移行をお勧めします。詳細については、お知らせを参照してください。

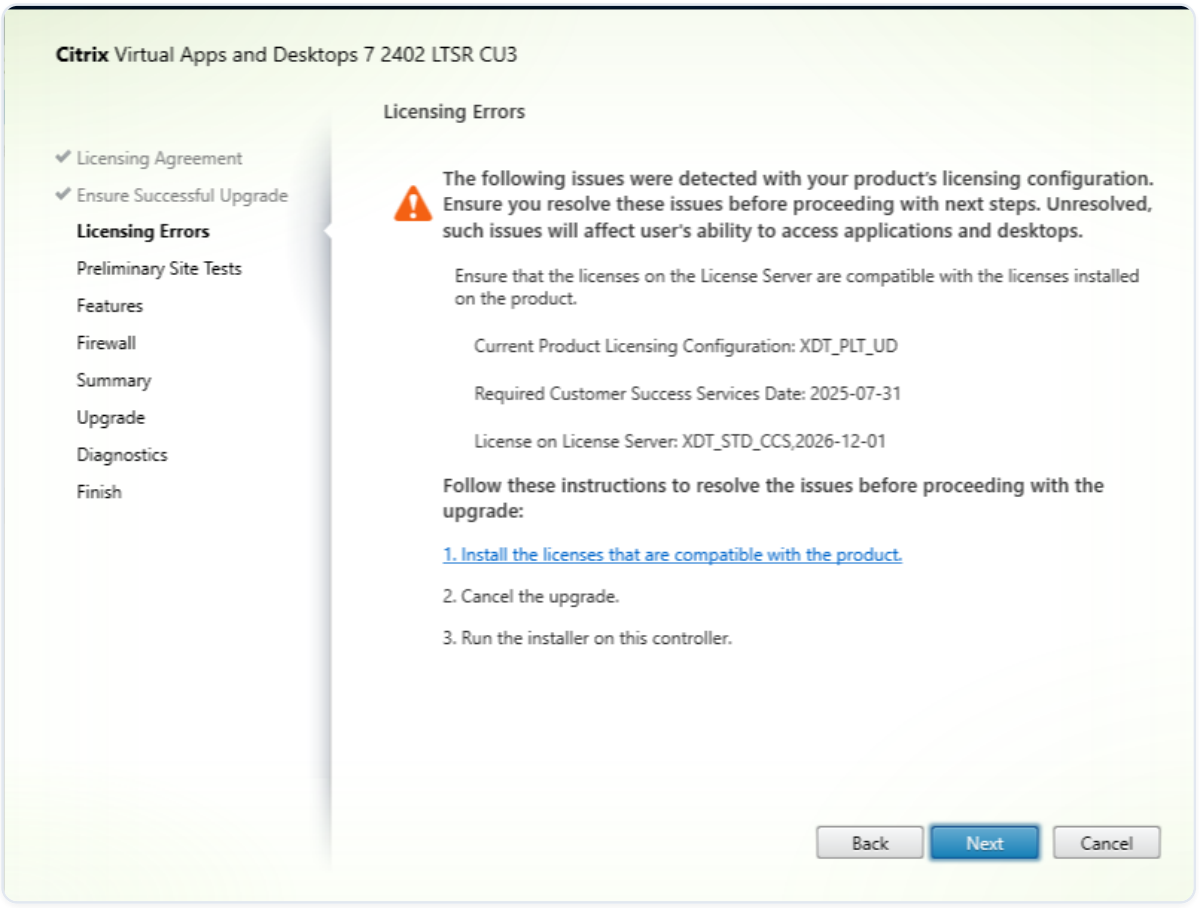
アップグレードに関する重要な考慮事項

以前のCitrix Virtual Apps and Desktopsバージョンから2411以降にアップグレードする場合は、License Serverを最新バージョン（バージョン11.2.17ビルド53100以降）にアップグレードしてください。

- メタインストーラーUIを使用してアップグレード中に、ライセンスエラーページに次のエラーが表示されます。
  - 最新のLicense Serverバージョンにアップグレードしない場合：



  - 古いLicense Serverやライセンスの利用不可など、互換性の問題がある場合：



- コマンドラインを使用してアップグレードする場合は、アップグレードの失敗を避けるために次のコマンドを実行します（マウントされたISOの\x64フォルダー内にいると仮定します）。

1. 次を実行します。

   ```
   \x64\Licensing\CitrixLicensing.exe /quiet
   ```

   ライセンスバイナリをローカルドライブのいずれかにコピーした場合は、次のコマンドを実行します。

   ```
   \x64\Licensing\CitrixLicensing.exe /quiet /l install.log
   ```

2. 次を実行します。

   ```
   \x64\XenDesktop Setup\XenDesktopServerSetup.exe  /components
   "CONTROLLER,DESKTOPSTUDIO,DESKTOPDIRECTOR" /CONFIGURE_FIREWALL
   ```

コアコンポーネントのアンインストール

アップグレード中に、コマンド `\x64\Licensing\CitrixLicensing.exe /quiet` または `\x64\Licensing\CitrixLicensing.exe /quiet /l install.log` を使用して最初にライセンスサーバーをインストールし、その後コアコンポーネントをインストールした場合は、アンインストールも同じ順序で行ってください:

1. コマンドラインを使用してライセンスサーバーをアンインストールします:

   ```
   CitrixLicensing.exe /quiet /uninstall /l uninstall.log
   ```

2. GUIまたはコマンドラインを使用してコンポーネントをアンインストールします。詳細については、コンポーネントの削除 を参照してください。

コマンドライン `XenDesktopServerSetup.exe` または `removeall` を使用してライセンスサーバーとコンポーネントをアンインストールする場合は、レジストリエントリと残りのファイルをクリーンアップしてください。

レジストリエントリをクリーンアップするには:

1. レジストリキー `Citrix Licensing` を検索し、そのエントリを削除します。ほとんどの場合、エントリは次の場所にあります:

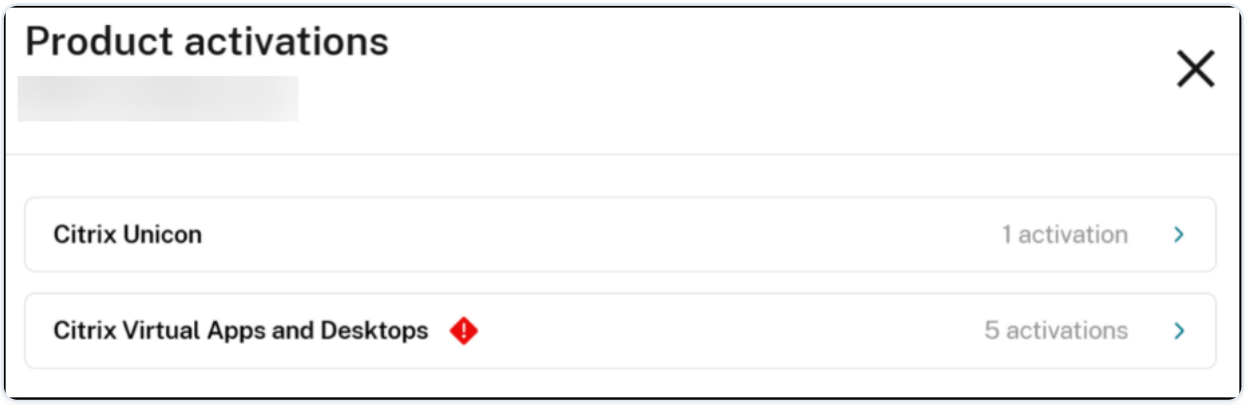
   ```
   "Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\Cur
   rentVersion\Uninstall\
   ```

2. レジストリキー内の **Uninstall String** が指すフォルダーを削除します。

トラブルシューティング

Citrix Cloudでライセンスサーバーのステータスが緑色以外で表示されている場合は、問題が発生している可能性のあるアクティベーションの詳細を把握するために、次の手順を実行します:

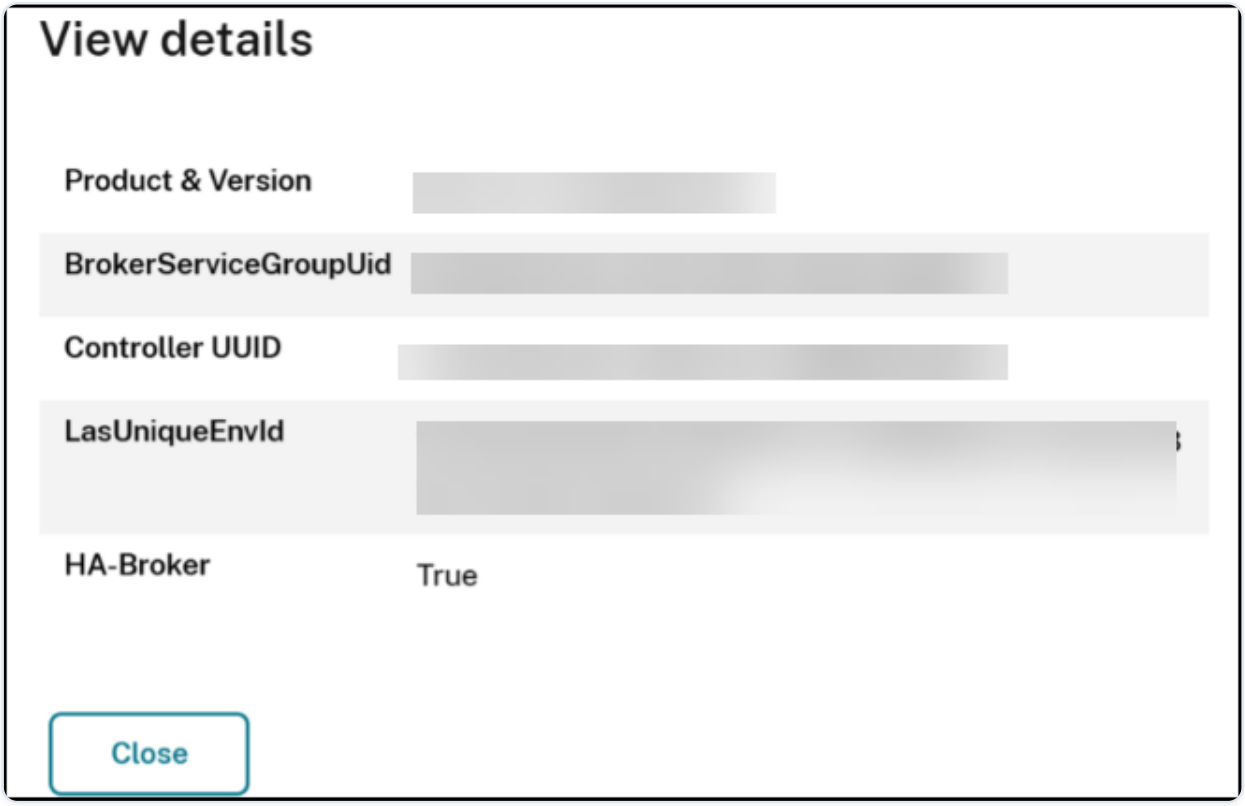
1. Citrix Cloud で、**ライセンス > ライセンス済み展開 > ライセンスサーバー** に移動します。
2. Citrix Virtual Apps and Desktops の横にある展開ボタン **>** をクリックして、アクティベートされたDelivery Controllersのリストを表示します。



3. アクティベーションの横にある **View details** をクリックして、詳細を表示します。

   ID は、アクティベーションを識別するための一意の識別子です。

   次の詳細が提供されます:



- **製品とバージョン**：LASでアクティベートする際に製品が使用するように構成されているProduct_Edition_ModelとBurn In Date。BurnInDateは通常、製品のリリース日です。
- **BrokerServiceGroupUid**：ブローカーサービスグループのUID。
- **Controller UUID**：デリバリーコントローラーのUUID。
- **LasUniqueEnvId**：アクティベーションのためにLASによって提供されるインスタンスの一意のID。
- **HA-Broker**：HAブローカーかメインブローカーかを示すTrueまたはFalse。

アクティベートされたホストの詳細を実際のホストにマッピングするには、ホストで次のコマンドを実行します。

- `Get-BrokerSite`：画面に表示される**BrokerServiceGroupUid**の値を、コマンドの`BrokerServiceGroupId`出力と比較します。
- `Get-BrokerController`：画面に表示される**Controller UUID**の値を、コマンドのUUID出力と比較します。

ライセンスイベントに関連するイベントビューアーログ

イベントID	説明
1112	Citrix Broker Serviceは、ユーザーからリソースへの接続を仲介できませんでした。このサイトの製品およびエディションのライセンス構成では、このタイプのリソースは許可されていません。このサイトに正しいライセンスが選択されていることを確認してください。
1150	Citrix Broker Serviceはライセンスサーバーへの接続に成功しました。
1151	Citrix Broker Serviceはライセンスサーバーに接続できません。ライセンスサーバーが正しく機能していること、およびXenDesktop構成でライセンスサーバーを識別する詳細が正しいことを確認してください。
1152	このXenDesktopサイトには、ライセンスサーバーに必要な製品ライセンスがありません。ライセンス管理コンソールを使用して、関連する製品ライセンスをライセンスサーバーに追加してください。
1153	このXenDesktopサイトのライセンスの有効期限が切れました。Citrix Brokerサービスは、ライセンスサーバーから新しいライセンスを要求します。
1154	このコントローラーは、ライセンスサーバーに接続できなかったため、ライセンスキャッシュモードに入りました。このコントローラーがデスクトップおよびアプリケーション

イベントID	説明
	セッションの提供を停止するまで、残り2時間です。
1155	Citrix Brokerサービスは、デスクトップおよびアプリケーションセッションの提供を停止します。このコントローラーは、ライセンスサーバーとの通信が継続的に失敗したため、ライセンスキャッシュモードではなくなったか、ライセンスキャッシュモードに入れませんでした。ライセンスサーバーが機能していることを確認し、必要に応じて、ライセンス管理コンソールを使用して関連するライセンスをライセンスサーバーに追加してください。
1156	Citrix Brokerサービスはライセンスサーバーと正常に通信しています。このコントローラーはライセンスキャッシュモードではなくなりました。
1157	実行中のライセンスサーバーのバージョンはCitrix Brokerサービスのバージョンよりも古く、互換性がありません。ライセンスサーバーをアップグレードするか、XenDesktop構成で正しいバージョンのライセンスサーバーの場所を指定してください。
1158	Citrix Brokerサービスは、このエディションのこのサイトでライセンスサーバー上の利用可能なライセンス数を超過したことを検出しました。ライセンスサーバーは、オーバードラフトライセンスを付与しました。
1159	Citrix Broker Serviceはデスクトップ接続を拒否しました。このサイトにインストールされているライセンスの最大数を超過しています。このエディションには3つのライセンスがインストールされていますが、このエディションで許可されているライセンスの最大数は2つです。ライセンス制限に準拠するために、関連するライセンスをライセンスサーバーから削除してください。

イベントID	説明
1160	Citrix Brokerサービスは、ライセンスの管理中に内部エラーを検出しました。ライセンスサーバーが正しく機能していること、およびXenDesktop構成でライセンスサーバーを識別する詳細が正しいことを確認してください。Citrix Brokerサービスを再起動すると、問題が解決する場合もあります。この問題が解決しない場合は、Citrix XenDesktop Controllerを再インストールしてください。Citrix Knowledge Baseの記事CTX126990を参照してください。
1161	ライセンスの初期化エラー。ライセンスサーバーの接続を確認してください。
1162	ライセンスの停止エラー。ライセンスサーバーの接続を確認してください。
1163	接続ライセンスがありません。解決するには、不要なセッションを閉じてライセンスを解放するか、ライセンスを追加してください。
1164	接続ライセンスのチェックアウトエラー。ライセンスサーバーの接続を確認してください。
1165	接続ライセンスのチェックインエラー。ライセンスサーバーの接続を確認してください。
1166	ライセンスの可用性確認エラー。ライセンスサーバーの接続を確認してください。
1167	ライセンスの開始に失敗しました。ライセンスサーバーの接続を確認してください。
1168	ライセンスユーザー通知設定の読み取り中にエラーが発生しました。ライセンスサーバーの接続を確認してください。
1169	ライセンスサーバーで適切なライセンスが見つからなかったため、このコントローラーは初期設定のライセンスキャッシュモードに入りました。このコントローラーがデスクトッ

イベントID	説明
	プおよびアプリケーションセッションの提供を停止するまで、残り2時間です。
1170	Citrix Broker Service は、ライセンスサーバー上で適切なライセンスを正常に検出しました。このコントローラーは、初期設定のライセンスキャッシュモードではなくなりました。
1171	ライセンスサーバーが指定されていません。有効なライセンスサーバーが指定されるまで、Citrix Broker Service はユーザーにデスクトップとアプリケーションを提供できません。Citrix Studio または Citrix PowerShell SDK コマンドレット Set-ConfigSite を使用して、ライセンスサーバーを指定できます。
1172	ライセンスサーバーの適合性チェック中にエラーが発生しました。Citrix Broker Service は、マシンがライセンスサーバーとして使用するのに適しているかどうかを確認する際に、予期しない応答を受信しました。コントローラーからマシンに接続できること、およびマシン上のファイアウォールがコントローラーからの接続を許可していることを確認してください。マシンにライセンスサーバーがインストールされている場合は、それが正しく構成され、動作していることを確認してください。
1173	この XenDesktop サイトには、ライセンスサーバーに必要な起動ライセンスがありません。License Administration Console を使用して、関連するライセンスをライセンスサーバーに追加してください。
1174	このXenDesktopサイト用に構成された製品エディションはアプリケーションをサポートしていません。アプリケーションリソースは利用できません。

イベントID	説明
1176	構成された製品エディションはマルチセッションマシンをサポートしていません。登録は拒否されました。
1177	構成された製品エディションはシングルセッションマシンをサポートしていません。登録は拒否されました。
1178	構成された製品エディションはRemotePCをサポートしていません。登録は拒否されました。
1179	構成された製品エディションは、クラウドシステムにプロビジョニングされたマシンをサポートしていません。登録は拒否されました。
1180	このXenDesktopサイト用に構成された製品エディションは、シングルセッション（ワークステーションOS）マシン上のアプリケーションをサポートしていません。アプリケーションリソースの起動は拒否されました。
1181	このXenDesktopサイト用に構成された製品エディションは、マルチセッション（サーバーOS）マシン上のアプリケーションをサポートしていません。アプリケーションリソースの起動は拒否されました。
1182	このXenDesktopサイト用に構成された製品エディションは、シングルセッション（ワークステーションOS）マシン上のデスクトップをサポートしていません。デスクトップリソースの起動は拒否されました。
1183	このXenDesktopサイト用に構成された製品エディションは、マルチセッション（サーバーOS）マシン上のデスクトップをサポートしていません。デスクトップリソースの起動が拒否されました。

イベントID	説明
1196	このコントローラーは、ライセンスサーバー上の使用可能なすべてのライセンスを使い果たしたため、ライセンスバーストモードに入りました。これを解決するには、さらにライセンスを追加してください。このコントローラーがデスクトップおよびアプリケーションセッションの提供を停止するまで、残り2時間です。
1197	Citrix Broker Serviceは、デスクトップおよびアプリケーションセッションの提供を停止します。このコントローラーは、ライセンスサーバー上のライセンスが不足しているため、ライセンスバーストモードではなくなったか、またはライセンスバーストモードに入ることができませんでした。ライセンス管理コンソールを使用して、関連するライセンスをライセンスサーバーに追加してください。
1198	Citrix Broker Serviceは、ライセンスサーバーからライセンスを正常に消費しています。現在の需要を満たすのに十分なライセンスがサーバーにあります。このコントローラーは、ライセンス枯渇によって引き起こされたライセンスバーストモードではなくなりました。
1199	Citrix Broker Serviceは、デスクトップおよびアプリケーションセッションの提供を停止します。このコントローラーは、ライセンスサーバーにライセンスがインストールされていないため、ライセンスキャッシュモードではなくなったか、またはライセンスキャッシュモードに入ることができませんでした。ライセンス管理コンソールを使用して、関連するライセンスをライセンスサーバーに追加してください。
1205	ソフトウェアメンテナンスの有効期限が切れました。Citrix環境は現在サポートされていません。ライセンスサーバーで期限切れのライセンスを確認し、削除してください。ユーザー

イベントID	説明
	が警告メッセージを受け取り始める前に、30日間のライセンスキャッシュモードがあります。
1206	ライセンス証明書のハッシュが無効です。Citrixライセンス証明書のハッシュが無効です。
1300	Citrix Broker Service は、デスクトップおよびアプリケーションセッションの提供を停止します。ライセンスサーバーのシステムクロックに問題があります。
1301	ライセンスサーバーのシステムクロックの問題が修正されました。Citrix Broker Service は通常の操作を再開します。
1302	このコントローラーは、接続ライセンスのチェックインまたはチェックアウトに再度失敗しました。以前に検出された障害はまだ存在します。過剰なイベントログを避けるため、問題が解決されるまで、サービスは関連メッセージ (イベント ID 1163、1164、1165) を抑制しています。ライセンスの試行は継続されます。
1303	このコントローラーは、関連メッセージ (イベント ID 1163、1164、1165) の抑制を停止しました。
1304	Citrix Broker Service は LAS に正常に接続しました。
1305	Citrix Broker Service は LAS に接続できません。LAS が正しく機能していること、および XenDesktop 構成で LAS を識別する詳細が正しいことを確認してください。

詳細情報

サイトの LAS 状態の確認、またはサイトがライセンスキャッシュモードであるかどうかの確認については、以下を参照してください。

- サイトの LAS 状態を確認するにはどうすればよいですか？
- サイトがライセンスキャッシュモードであるかどうかを確認するにはどうすればよいですか？

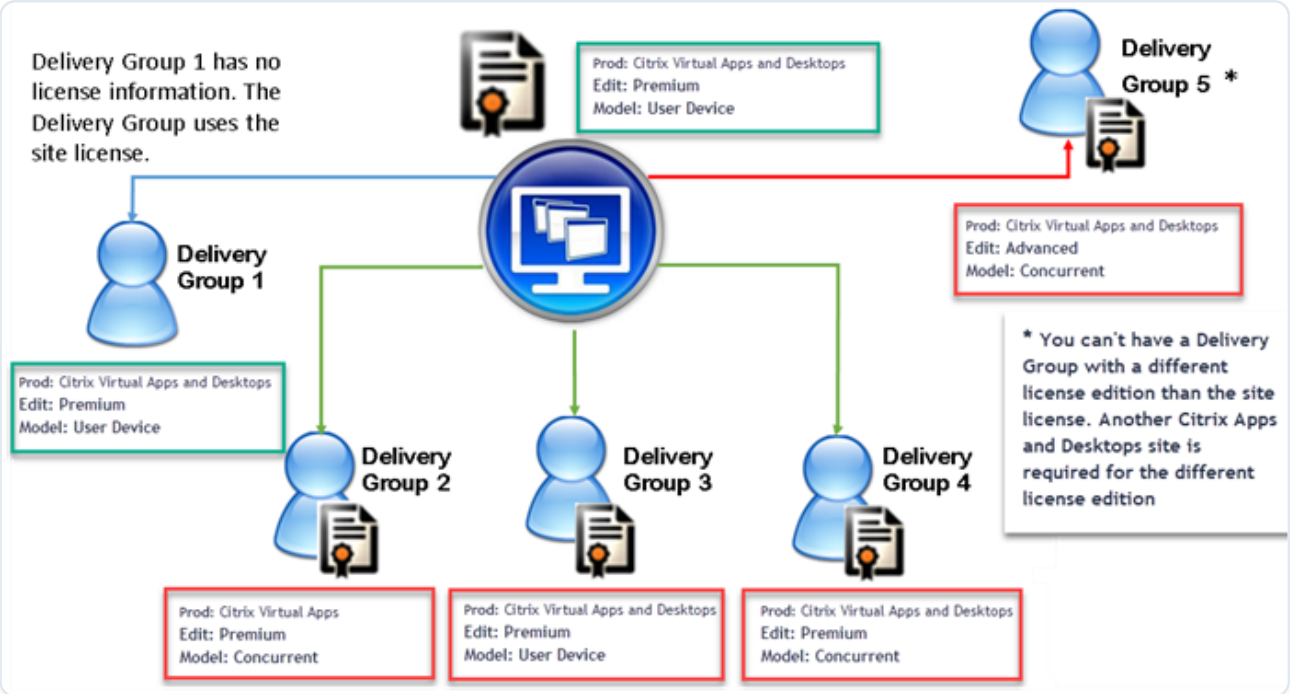
コマンドの詳細については、以下を参照してください。

- Get-BrokerController
- Get-ConfigSite

マルチタイプライセンス

マルチタイプライセンスは、単一の Citrix Virtual Apps and Desktops サイト上のデリバリーグループに対して、異なるライセンスタイプの消費をサポートします。**タイプ**は、製品ID（XDTまたはMPS）とモデル（UserDeviceまたはConcurrent）の単一の組み合わせです。デリバリーグループは、サイトレベルで構成されているものと同じ製品エディション（PLT/PremiumまたはENT/Advanced）を使用する必要があります。Citrix Virtual Apps and Desktops の展開でマルチタイプライセンスを構成する際は、この記事の最後にある特別な考慮事項 に注意してください。

マルチタイプライセンスが構成されていない場合、異なるライセンスタイプは、個別のサイト用に構成されている場合にのみ使用できます。デリバリーグループはサイトライセンスを使用します。マルチタイプライセンスが構成されている場合の重要な通知の制限については、特別な考慮事項 を参照してください。



異なる種類のライセンスを消費するデリバリーグループを特定するには、以下の Broker PowerShell コマンドレットを使用します。

- New-BrokerDesktopGroup

- Set-BrokerDesktopGroup
- Get-BrokerDesktopGroup

ライセンスをインストールするには、以下を使用します。

- シトリックス スタジオ
- シトリックス ライセンシング マネージャー
- citrix.com

Customer Success Services の日付は、各ライセンスファイル、各製品、およびモデルに固有です。異なる設定のデリバリーグループは、互いに異なる Customer Success Services の日付を持つ場合があります。

特別な考慮事項

マルチタイプライセンスは、通常のCitrix Virtual Apps and Desktops™ライセンスとは異なる機能を持ちます。

サイト構成とは異なるタイプを使用するように構成されたデリバリーグループの場合、DirectorまたはStudioからのアラートや通知はありません。

- ライセンスの上限に近づいている場合、またはライセンスバーストモードが有効化された、もしくは期限切れになった場合でも、情報は提供されません。
- 特定のグループに問題がある場合の通知はありません。

マルチタイプライセンス用に構成されたデリバリーグループは、そのライセンスタイプのみを消費し、完全に消費されてもサイト構成にフォールバックしません。

Citrix Virtual Apps StandardとCitrix Virtual Desktops™ Standardのライセンスエディション名はどちらもStandardであることを示していますが、これらは同じエディションではありません。マルチタイプライセンスは、Citrix Virtual Apps StandardおよびCitrix Virtual Desktop Standardライセンスでは利用できません。

ライセンス互換性マトリックス

この表は、古い製品名、新しい製品名、および関連する機能名を詳述しています。4つの互換性列は、どの製品とライセンスモデルの組み合わせがマルチタイプライセンスと互換性があるかを指定します。CCUとCCSは同時接続ライセンスを表し、UDはユーザー/デバイスライセンスを表します。

Old Name	New Name	Feature	Multi-type licensing compatibility			
			STD	ADV	ENT	PLT
Citrix XenApp Standard	Citrix XenApp Standard	MPS_STD_CCU	X			
Citrix XenApp Advanced	Citrix Virtual Apps Standard	MPS_ADV_CCU		X		
Citrix XenApp Enterprise	Citrix Virtual Apps Advanced	MPS_ENT_CCU			X	
Citrix XenApp Platinum	Citrix Virtual Apps Premium	MPS_PLT_CCU				X
Citrix XenDesktop VDI Edition (XDT-U)	Citrix Virtual Desktops Standard- Per User/Device	XDT_STD_UD	X			
Citrix XenDesktop VDI Edition (XDT-C)	Citrix Virtual Desktops Standard - Concurrent	XDT_STD_CCS	X			
Citrix XenDesktop Enterprise Edition (XDT-C)	Citrix Virtual Apps and Desktops Advanced - Concurrent	XDT_ENT_CCS			X	
Citrix XenDesktop Enterprise Edition (XDT-U)	Citrix Virtual Apps and Desktops Advanced - Per User/Device	XDT_ENT_UD			X	
Citrix XenDesktop Platinum Edition (XDT-C)	Citrix Virtual Apps and Desktops Premium - Concurrent	XDT_PLT_CCS				X
Citrix XenDesktop Platinum Edition (XDT-U)	Citrix Virtual Apps and Desktops Premium - Per User/Device	XDT_PLT_UD				X

ブローカー PowerShell SDK

DesktopGroup オブジェクトには、関連するNew-BrokerDesktopGroupおよびSet-BrokerDesktopGroupコマンドレットを使用して操作できる次の2つのプロパティがあります。

名前	値	制限
LicenseModel	グループのライセンスモデルを指定するパラメーター (Concurrent または UserDevice)。指定されていない場合、サイト全体のライセンスモデルが使用されます。	機能トグルが無効になっている場合、プロパティを設定しようとすると失敗します。
ProductCode	XDT (Citrix Virtual Desktops用) またはMPS (Citrix Virtual Apps™用) のテキスト文字列で、グループのライセンス製品IDを指定します。指定されていない場合、サイト全体の製品コードが使用されます。	機能トグルが無効になっている場合、プロパティを設定しようとすると失敗します。

LicenseModelとProductCodeの詳細については、about_Broker_Licensingを参照してください。

New-BrokerDesktopGroup

デスクトップグループのブローカーを管理するためのデスクトップグループを作成します。このコマンドレットの詳細については、`<https://citrix.github.io/delivery-controller-sdk/Broker/New-BrokerDesktopGroup/>`を参照してください。

Set-BrokerDesktopGroup

既存のブローカーデスクトップグループを無効または有効にするか、その設定を変更します。このコマンドレットの詳細については、`<https://citrix.github.io/delivery-controller-sdk/Broker/Set-BrokerDesktopGroup/>`を参照してください。

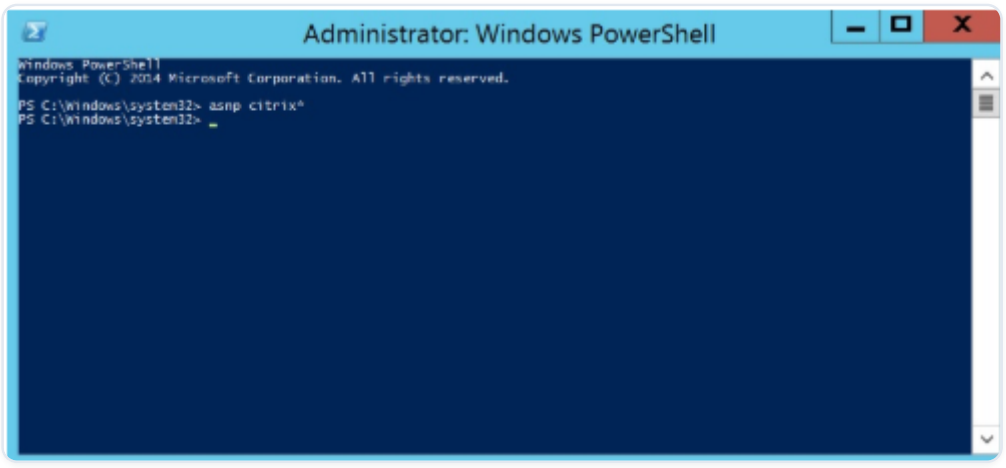
Get-BrokerDesktopGroup

指定された条件に一致するデスクトップグループを取得します。Get-BrokerDesktopGroupコマンドレットの出力には、グループの**ProductCode**および**LicenseModel**プロパティが含まれます。New-BrokerDesktopGroupまたはSet-BrokerDesktopGroupを使用してプロパティが設定されていない場合、null値が返されます。nullの場合、サイト全体のライセンスモデルと製品コードが使用されます。このコマンドレットの詳細については、`<https://citrix.github.io/delivery-controller-sdk/Broker/Get-BrokerDesktopGroup/>`を参照してください。

デリバリーグループごとに異なるライセンス製品とモデルを構成する

> **注：**
>
> 単一のデリバリーグループで、2つ以上の異なる種類の製品、エディション、またはライセンスモデルを構成することはできません。異なる種類の製品、エディション、またはライセンスモデルがある場合は、それらを別々のデリバリーグループで構成してください。

1. 管理者権限でPowerShellを開き、Citrixスナップインを追加します。



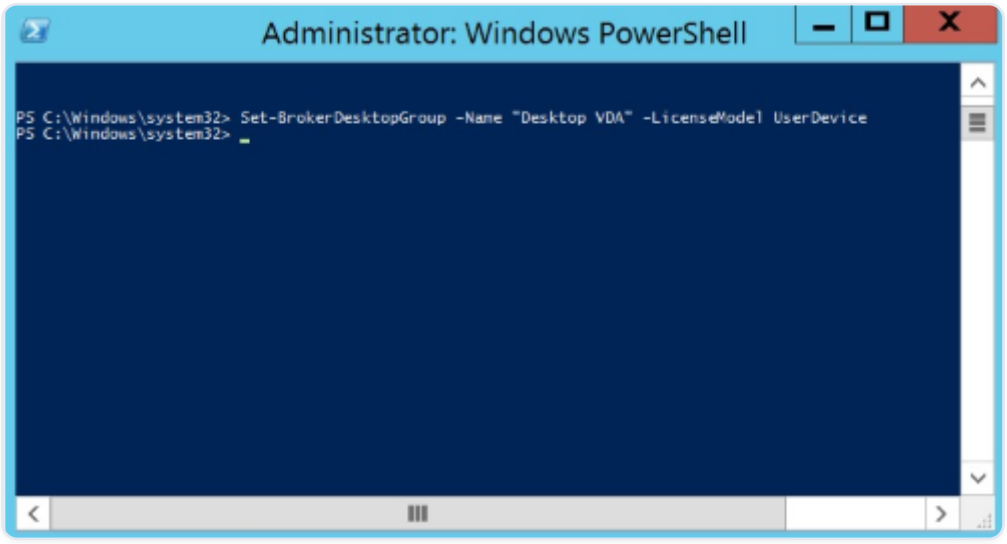
2. コマンド **Get-BrokerDesktopGroup –Name “DeliveryGroupName”** を実行して、現在のライセンス構成を表示します。パラメーター **LicenseModel** と **ProductCode** を見つけます。これらのパラメーターを以前に構成していない場合、空白になっている可能性があります。

> **注：**

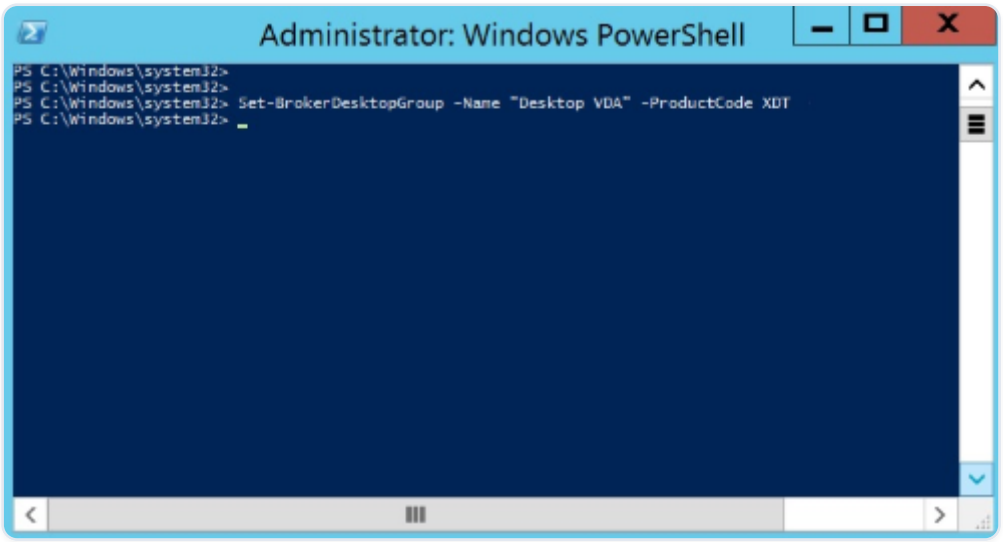
> デリバリーグループにライセンス情報が設定されていない場合、デフォルトで**サイトレベルのサイトライセンス**になります。

> PowerShellコマンド(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/license-configuration-2.png)

3. コマンド **Set-BrokerDesktopGroup –Name “DeliveryGroupName” –LicenseModel LicenseModel** を実行して、ライセンスモデルを変更します。



4. コマンドを実行してライセンス製品を変更します: **Set-BrokerDesktopGroup –Name “DeliveryGroupName” –ProductCode ProductCode**。



5. 変更を検証するには、コマンド **Get-BrokerDesktopGroup –Name “DeliveryGroupName”** を入力します。

> **注：**

> 同じサイト内でエディションを混在させることはできません。たとえば、Premiumライセンスとライセンスなどです。異なるエディションのライセンスがある場合は、複数のサイトが必要です。

> PowerShellコマンド(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/license-configuration-5.png)

6. 前の手順で説明したのと同じ **Set-BrokerDesktopGroup** コマンドを実行し、値を **$null** に設定して、ライセンス構成を削除します。

> **注：**
>
> Studioでは、各デリバリーグループのライセンス構成は表示されません。現在の構成を表示するには、PowerShellを使用します。

> PowerShellコマンド(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/license-configuration-6.png)

例

このPowerShellコマンドレットの例は、既存の2つのデリバリーグループにマルチタイプライセンスを設定し、3つ目のデリバリーグループを作成して設定する方法を示しています。

デリバリーグループに関連付けられているライセンス製品とライセンスモデルを確認するには、**Get-BrokerDesktopGroup** PowerShellコマンドレットを使用します。

1. 最初のデリバリーグループをXenApp®およびConcurrentに設定しました。

   Set-BrokerDesktopGroup -Name "シトリックス バーチャル アプリケーションズ プレミアム コンカレント 用のデリバリーグループ" -ProductCode MPS -LicenseModel Concurrent

2. 2番目のデリバリーグループをXenDesktop®およびConcurrentに設定しました。

   Set-BrokerDesktopGroup -Name "シトリックス バーチャル デスクトップス プレミアム コンカレント 用のデリバリーグループ" -ProductCode XDT -LicenseModel Concurrent

3. 3番目のデリバリーグループをXenDesktopおよびUserDevice用に作成して設定します。

   New-BrokerDesktopGroup -Name "Citrix Virtual Desktops Premium UserDevice 用のデリバリーグループ" -PublishedName "MyDesktop" -DesktopKind Private -ProductCode XDT -LicenseModel UserDevice

Citrix Virtual Apps and Desktops™ テレメトリデータ要素

ブローカー

セッション

ヘッダー

キー	説明	例
バージョン	テレメトリー使用状況イベントのバージョンを示します。	1
id	使用状況イベントの一意の識別子を示します。	d4ce7919-5d80-44de-a8fa-102923fe0ead
タイプ	Citrix Analytic Serviceがクラウド使用状況イベントを識別するために使用するイベントタイプを示します。	SendBrokerTelemetryData
st	Brokerでイベントが生成されたときのタイムスタンプを示します。	2011-08-12T20:17:46.384Z
本番	使用状況イベントの発生元製品と展開を識別します。	XenDesktop.Broker
prodVer	Citrix DaaS/Citrix Virtual Apps and Desktops の製品バージョンを示します。	7.25.0.0
ユーザー	セッション起動を開始するユーザーを一意に識別するためのユーザー ID を識別します。	fullName: C648FE671A44B3F7

キー	説明	例	
		samName:C758LH671A44B3F7 ユーザープリンシパル名:C7948FE671A44B3F7 userLicenseId:C265FE671A44B3F7 userSid:C097FE671A44B3F7	
テナント -> ID	Citrix Cloud™ アカウントの顧客IDを示します。オンプレミス展開の場合、値は常に「CitrixOnPremises」です。	ジョジ1mh0598tj	
dvc から dvcId	セッション起動が開始されたデバイスを一意に識別するためのデバイスIDを示します。	AE18C4D5	
デバイス -> デバイス名	デバイスのフレンドリ名を示します。	C758LH671A44B3F7	

ペイロード

フィールド	説明	例
appProtectionKeyLoggingRequired	セッションがキーロギング保護を有効にして起動されたかどうかを示します。	いいえ

フィールド	説明	例
appProtectionScreenCaptureRequired	セッションが画面キャプチャ保護を有効にして起動されたかどうかを示します。	いいえ
cspTenantCustomerId	CSPテナントのCitrix Cloudアカウントの顧客IDを示します。オンプレミス展開の場合、顧客IDが利用できない場合、このフィールドは空のままになります。	6c2vtxgxyftt
isAnonymousUser	認証されていないセッションが起動されたかどうかを示します。	いいえ
licenseActivityTimeStamp	ペイロードが生成されたときのタイムスタンプを示します。	2011-08-12T20:17:46.384Z
licenseActivityType	ライセンスイベントの種類を示します。このフィールドは、ライセンスイベントの種類が割り当てアクションかリリースアクションかを示します。	接続
licenseModel	展開のライセンスモデルを示します。	UserDevice
productEdition	展開の製品エディションを示します。	Premium または Advanced
productId	展開内の製品の製品IDを示します。	CAVDS
プロトコル	セッションの起動に使用されたプロトコルを示します。	HDX™
sessionKey	セッションの一意の識別子を示します。	uq390c5fc3-86eb-4df3-bd9a-f4a8fed2c9e2

フィールド	説明	例
sessionSupport	セッションサポートの種類を示します。	SingleSession
sessionType	セッションの種類を示します。	アプリケーション
バージョン	ペイロードのバージョンを示します。	1.3
workerSid	セッションに使用されるVDAの一意の識別子を示します。**値はスクランブルされます。**	1E5LH671A44B3F7 **(常にスクランブルされます)**
isWindows365	セッションがWindows 365向けに起動されたかどうかを示します。	はい
entitlementType	お客様のライセンスエンタイトルメントタイプを示します。	本番
siteId	サイトの一意の識別子を示します。	a35647d0-901c-4477-87e0-dcd781d455f4
desktopGroupId	デスクトップまたはデリバリーグループの一意の識別子を示します。	e9d859dc-1bfc-4b3e-bad3-41806bb4e694
clientType	Citrix Workspace™アプリのタイプを示します。	ウィンドウズ
clientVersion	Citrix Workspaceアプリのバージョンを示します。	23.5.1.83
workerCloudType	VDAプロビジョニングに使用されるパブリッククラウドの種類を示します。	アジュール
enabledFeatures	セッションで有効になっている機能を示します。たとえば、`AppProtectionScreenCapt`	66

フィールド	説明	例
	`ureRequired` と `SessionRecording` が有効になっているセッションでは、このフィールドの値は 66 です。	
isEvents	{{page.lic}}における重大な障害を示します。	STデータベースを作成できません。
heartBeatTime	CISまたはCitrix Analytic Serviceへのライセンスサーバーのハートビート時間を示します。	1689058813

ライセンス テレメトリ データを難読化する

ライセンス テレメトリで送信される情報の機密性を考慮し、Citrix はデータを難読化するオプションを提供します。

次の表に、難読化できるデータを示します。

フィールド	説明	例
ユーザー	セッション起動を開始するユーザーを一意に識別するためのユーザー ID を識別します。	• fullName: `C648FE671A44B3F7` • samName: `C758LH671A44B3F7` • ユーピーエヌ: `C7948FE671A44B3F7` • userLicenseId: `C265FE671A44B3F7`

フィールド	説明	例
		• userSid: `C097FE671A44B3F7`
デバイス -> デバイス名	デバイスのフレンドリ名を示します。	`C758LH671A44B3F7`
workerSid	セッションに使用されるVDAの一意の識別子を示します。	`1E5LH671A44B3F7`
AdminLoginList	一意の管理者SamAccountNameのリストを示します	`{AdminLoginList: [UFMJ+JvXOTHO9mQDsOweiw= =]}`

スクランブルを有効または無効にするには、Delivery Controllerで次のPowerShellコマンドを実行します。

1. Delivery ControllerホストからPowerShellウィンドウを開きます。
2. コマンド `asnp citrix` を実行して、Citrix固有のPowerShellモジュールをロードします。
3. スクランブルを有効または無効にするには、次のコマンドを実行します。

   デフォルトでは、値は`0`または`false`であり、ライセンステレメトリデータのスクランブルを無効にします。

   有効にするには:

   ```
   Set-BrokerServiceConfigurationData Core.ScrambleLicensingData
   -SettingValue $true
   ```

   注：

   Citrix Service Provider™ (CSP) のお客様の場合、スクランブルはデフォルトで無効になっています。

   スクランブルを有効にした後、次のコマンドを使用して無効にできます。

```
Set-BrokerServiceConfigurationData Core.ScrambleLicensingData
-SettingValue $false
```

Citrix Virtual Apps and Desktops 2402 LTSR CU1 テレメトリデータ要素

ブローカー

使用方法

ヘッダー

キー	説明	例
バージョン	テレメトリイベントのバージョンを示します。	1
id	使用状況イベントの一意の識別子を示します。	d4ce7919-5d80-44de-a8fa-102923fe0ead
タイプ	Citrix Analytic Service がクラウド使用状況イベントを識別するために使用するイベントタイプを示します。	SendBrokerTelemetryData
st	Broker でイベントが生成されたときのタイムスタンプを示します。	2011-08-12T20:17:46.384Z
本番	使用状況イベントの発生元となる製品と展開を識別します。	XenDesktop.Broker (クラウド) OnPrem.Broker (OnPrem)
prodVer	Citrix DaaS/Citrix Virtual Apps and Desktops の製品バージョンを示します。	7.25.0.0

ペイロード

フィールド	説明	例
TotalPublishedApps	公開されているアプリケーションの総数を示します。	10
TotalPublishedDesktops	公開されているデスクトップの総数を示します。	10
VDAs.Total	VDAの総数を示します。	10
VDAs.OSTypes	Windows、Linux、MacなどのOSタイプ別のVDAの総数を示します。	10
VDAs.OSVersions	Windows 10、11、2022、2019などのOSバージョンごとの合計数を示します。	10
VDAs.HostingLocations.Azure	Azure、AWS、GCP、Nutanix、VMWare、XenServer、HyperVなど、サポートされている各ホスティングロケーションのVDA数を示します。	10
VDAs.HostingLocations.AWS		
VDAs.HostingLocations.Nutanix		
VDAs.HostingLocations.VMWare		
VDAs.HostingLocations.XenServer		
VDAs.HostingLocations.HyperV		
VDAs.ProvisionedMethod.MCS	Machine Creation Service (MCS) によってプロビジョニングされたマシンの数を示します。	10

フィールド	説明	例
VDAs.ProvisionedMethod.ManualOr3P	手動または3Pでプロビジョニングされたマシンの数を示します。	10
VDAs.SessionSupport.StaticSingle	静的に割り当てられたシングルセッションのマシンの数を示します。	10
VDAs.SessionSupport.DynamicSingle	動的に割り当てられたシングルセッションのマシンの数を示します。	10
VDAs.SessionSupport.Multi	マルチセッションマシンの総数を示します。	10
VDAs.RemotePCAccess.Windows	OSタイプ (Win、Mac、Linux) 別のRemote PC Accessマシンの数を示します。	10
VDAs.RemotePCAccess.Linux		
VDAs.RemotePCAccess.MacOS		
VDAs.ActiveSessionRecordingAgents	アクティブなセッション記録エージェントを持つVDAの数を示します。	5
VDAs.Subscriptions	VDAのパブリッククラウドサブスクリプションの数を示します。	2
VDAs.LocationTypes	VDAのロケーションタイプの数を示します。	2
AutoScale.DGWithAutoscaleEnabled	**Autoscale** が有効になっているデリバリーグループの数を示します。	2
AutoScale.TotalMachinesCtrlByAutoscale	Autoscaleによって制御されるマシンの数を示します。	5

フィールド	説明	例
AutoScale.VerticalAutoscaleEnabledByDGandSite	DGとサイトによって**Vertical Autoscale**が有効になっているマシンの数を示します。	2
AutoScale.TaggedBasedAutoscaledDG	タグベースのAutoscaleが適用されたデリバリーグループの数を示します。	2
DeliveryGroup.TotalRebootSchedulesEnabled	**再起動スケジュール**が有効になっているデリバリーグループの数を示します。	2
DeliveryGroup.Total	デリバリーグループの総数を示します。	10
Policy.TotalPolicySets	ポリシーセットの数を示します。	3
Policy.TotalPolicies	グループポリシーの数を示します。	2
Policy.TotalPolicySettings	グループ設定の数を示します。	2
PublishedPackageApps.AppVSingleAdmin	AppVシングルアドミンモードで公開されているパッケージ化されたアプリの総数を示します。	2
PublishedPackageApps.AppVDualAdmin	AppVデュアルアドミンモードで公開されているパッケージ化されたアプリの総数を示します。	2
PublishedPackageApps.Msix	MSIXモードで公開されているパッケージ化されたアプリの総数を示します。	2
PublishedPackageApps.AppAttach	AppAttachモードで公開されているパッケージ化されたアプリの総数を示します。	2

フィールド	説明	例
PublishedPackageApps.FlexApp	FlexAppモードで公開されたパッケージ化されたアプリの総数を示します。	2

セッション

ヘッダー

フィールド	説明	例
バージョン	ライセンス使用状況イベントのバージョンを示します。	1
id	使用状況イベントの一意の識別子を示します。	d4ce7919-5d80-44de-a8fa-102923fe0ead
タイプ	Citrix Analytic Serviceがクラウド使用状況イベントを識別するために使用するイベントタイプを示します。	Cloud.Licensing
st	Brokerでイベントが生成されたときのタイムスタンプを示します。	2011-08-12T20:17:46.384Z
本番	使用状況イベントの発生元製品と展開を識別します。	XenDesktop.Broker (クラウド) OnPrem.Broker (OnPrem)
prodVer	Citrix DaaSまたはCitrix Virtual Apps and Desktopsの製品バージョンを示します。	7.25.0.0

フィールド	説明	例
ユーザー	セッション起動を開始するユーザーを一意に識別するためのユーザーIDを特定します。**値はスクランブルされています。**	fullName: C648FE671A44B3F7 **(常にスクランブルされています)** samName:C758LH671A44B3F7 **(常にスクランブルされています)** upn: C7948FE671A44B3F7 **(常にスクランブルされています)** userLicenseId:C265FE671A44B3F7 **(常にスクランブルされています)** userSid: C097FE671A44B3F7 **(常にスクランブルされています)**
テナント -> ID	Citrix Cloudアカウントの顧客IDを示します。オンプレミス展開の場合、このフィールドは適用されず、値はありません。	ジョジ1mh0598tj
dvc から dvcId	セッション起動が開始されたデバイスを一意に識別するためのデバイスIDを示します。	AE18C4D5

フィールド	説明	例
デバイス -> デバイス名	デバイスのフレンドリ名を示します。**値はスクランブルされています。**	C758LH671A44B3F7 **(常にスクランブルされています)**

ペイロード

フィールド	説明	例
appProtectionKeyLoggingRequired	セッションがキーロギング保護を有効にして起動されたかどうかを示します。	いいえ
appProtectionScreenCaptureRequired	セッションが画面キャプチャ保護を有効にして起動されたかどうかを示します。	いいえ
cspTenantCustomerId	CSPテナントのCitrix Cloudアカウントの顧客IDを示します。オンプレミス展開の場合、このフィールドは適用されず、値はありません。	6c2vtxgxyftt
isAnonymousUser	認証されていないセッションが起動されたかどうかを示します。	いいえ
licenseActivityTimeStamp	ペイロードが生成されたときのタイムスタンプを示します。	2011-08-12T20:17:46.384Z
licenseActivityType	ライセンスイベントの種類を示します。このフィールドは、ライセンスイベント	接続

フィールド	説明	例
	の種類が割り当てアクションかリリースアクションかを示します。	
licenseModel	展開のライセンスモデルを示します。	UserDevice
productEdition	展開の製品エディションを示します。	プレミアム
productId	展開内の製品の製品IDを示します。	CAVDS
プロトコル	セッションの起動に使用されたプロトコルを示します。	HDX
sessionKey	セッションの一意の識別子を示します。	uq390c5fc3-86eb-4df3-bd9a-f4a8fed2c9e2
sessionSupport	セッションサポートの種類を示します。	SingleSession
sessionType	セッションの種類を示します。	アプリケーション
バージョン	ペイロードのバージョンを示します。	1.3
workerSid	セッションに使用されるVDAの一意の識別子を示します。**値はスクランブルされます。**	1E5LH671A44B3F7 **(常にスクランブルされます)**
isWindows365	セッションがWindows 365向けに起動されたかどうかを示します。	はい

フィールド	説明	例
entitlementType	お客様のライセンスエンタイトルメントタイプを示します。	本番
siteId	サイトの一意の識別子を示します。	a35647d0-901c-4477-87e0-dcd781d455f4
desktopGroupId	デスクトップまたはデリバリーグループの一意の識別子を示します。	e9d859dc-1bfc-4b3e-bad3-41806bb4e694
clientType	Citrix Workspaceアプリの種類を示します。	ウィンドウズ
clientVersion	Citrix Workspaceアプリのバージョンを示します。	23.5.1.83
workerCloudType	VDAプロビジョニングに使用されるパブリッククラウドの種類を示します。	アジュール
enabledFeatures	セッションで有効になっている機能を示します。たとえば、`AppProtectionScreenCaptureRequired` と `SessionRecording` が有効になっているセッションでは、このフィールドの値は 66 です。	66
launchRequestSource	起動を要求するために使用された製品を記録します。オンプ	0 (StoreFront or 3P)

フィールド	説明	例
	レミスStoreFront™またはCloud StoreFrontのいずれかです。	1 (ワークスペース)
isEvents	{{page.lic}}における重大な障害を示します。	STデータベースを作成できません。
heartBeatTime	CISまたはCitrix Analytic Serviceへのライセンスサーバーのハートビート時間を示します。	1689058813
vdaTelemetry	App Layering、User Personalization Layer、User Profile management、Workspace Environment Management™、およびHDX機能のためにキャプチャされるペイロードを示します。	vdaTelemetry SessionTelemetry CPM_feature: 32 HDX1: 66 HDX2: 0 MachineTelemetry AL_productVersion: 23.12.0.1001 UPL_isEnabled: 1 CPM_version: 22.3.4000 wem_enableMethod: 1 wem_agentVersion: 2402.1

スタジオ

使用方法

ヘッダー

フィールド	説明	例
バージョン	ライセンス使用状況イベントのバージョンを示します。	1
id	使用状況イベントの一意の識別子を示します。	8c2e20a5-ca3f-4401-ad69-d037933c40a0
タイプ	Citrix Analytic Service がクラウド使用状況イベントを識別するために使用するイベントタイプを示します。	Studio.Usage
st	Studio でイベントが生成されたときのタイムスタンプを示します。	2024-03-22T01:32:23.4056195Z
本番	使用状況イベントの発生元となる製品と展開を識別します。	XenDesktop.Studio
prodVer	Citrix DaaS/Citrix Virtual Apps and Desktops の製品バージョンを示します。	7.42.0.0

ペイロード

フィールド	説明	例
AdminLoginList	一意の管理者 SamAccountName のリストを示します。**値はスクランブルされています。**	{AdminLoginList: [UFMJ+JvXOTHO9mQDsOweiw= =]}**(常にスクランブルされています)**
TotalApiRequests	オーケストレーションサービスの API リクエストを示します。	{TotalApiRequests: 1000}

フィールド	説明	例
BackupCount	Studio 管理者によって操作されたバックアップの数を示します。	{BackupCount: 200}
RestoreCount	Studio管理者によって実行された復元回数を示します。	{RestoreCount: 20}

ディレクター

使用状況レポート

ヘッダー

フィールド	説明	例
バージョン	ライセンス使用状況イベントのバージョンを示します。	1
id	使用状況イベントの一意の識別子を示します。	8c2e20a5-ca3f-4401-ad69-d037933c40a0
タイプ	Citrix Analytic Serviceがクラウド使用状況イベントを識別するために使用するイベントタイプを示します。	テレメトリ
st	Studioでイベントが生成されたときのタイムスタンプを示します。	2024-03-22T01:32:23.4056195Z
本番	使用状況イベントの発生元製品と展開を識別します。	XenApp.Monitor
prodVer	Director製品のバージョンを示します。	7.42.0.0
dvcName	サーバーの名前	C758LH671A44B3F7

ペイロード

フィールド	説明	例
AdminLoginCount	これは、管理者ログインの数を提供するペイロードのセクションです。	type: 管理者ログイン統計 0: 1 1: 7
FeatureUsageCount	ペイロードのこのセクションには、Director で使用されている主要な機能の数が含まれています。	タイプ: FeatureUsage 統計 0: 15 1: 20 5: 10
OdataUsageCount	このペイロードのセクションには、OData APIの使用状況のカウントが含まれています。	タイプ: OData_v3 統計 0: 1 2: 7 5: 9 タイプ: OData_v4 統計
		0: 1
		2: 8
		6: 7
AppUsage	公開されたアプリケーションの週ごとの使用状況メトリックを示します。	タイプ: AppUsage
		ヘッダー: applicationName,pro

フィールド	説明	例
		cessName,totalDurationInMinutes 期間: 01/05/24-07/05/24 値: [Calc_AWTSVDA-1907R,calc.exe,0.13, Notepad_AWTSVDA-1907R,notepad.exe,4]
UniqueAppUsers	公開されたアプリケーションについて、1か月あたりのユニークユーザー数とアプリケーションの合計起動回数を示します。	タイプ: ユニークアプリユーザー ヘッダー: applicationName,totalLaunches,totalUniqueUsers 期間: 04/24 値: [Calc_AWTSVDA-1907R,100,10, Notepad_AWTSVDA-1907R,200,20]
DesktopUsage	公開デスクトップの週次使用状況メトリックを示します。	タイプ: DesktopUsage ヘッダー: desktopGroupName,sessionSupport,totalDurationInMinutes

フィールド	説明	例
		期間: 01/05/24-07/05/24 値: [RdsDesktopAndAppGroup,1,10]
UniqueDesktopUsers	公開デスクトップの月間ユニークユーザー数と合計起動回数を示します。	タイプ: UniqueDesktopUsers ヘッダー: desktopGroupName,totalLaunches,totalUniqueUsers 期間: 04/24 値: [RdsDesktopAndAppGroup,10,5]
AvgLogonDuration	平均ログオン期間を示します。	タイプ: AvgLogonDuration ヘッダー: totalUserLogons, avgLogonDurationInSeconds 期間: 01/05/24-07/05/24 値: [200,4]
CostSaved	顧客が1か月あたりに節約したコストを示します。	タイプ: CostSaved

フィールド	説明	例	
		ヘッダー: ハイパーバイザー,コスト削減,通貨 期間: 04/24 値: [1,221.02,1 2,301.02,2]	

委任管理

使用方法

ヘッダー

キー	説明	例
バージョン	ライセンス使用状況イベントのバージョンを示します。	1
id	使用状況イベントの一意の識別子を示します。	8c2e20a5-ca3f-4401-ad69-d037933c40a0
タイプ	Citrix Analytic Service がクラウド使用状況イベントを識別するために使用するイベントタイプを示します。	DelegatedAdmin.Usage
st	Delegated Admin でイベントが生成されたときのタイムスタンプを示します。	2024-03-22T01:32:23.4056195Z
本番	使用状況イベントの発生元製品と展開を識別します。	XenDesktop.DelegatedAdmin (クラウド)
		OnPrem.DelegatedAdmin (OnPrem)

キー	説明	例
prodVer	Citrix DaaS または Citrix Virtual Apps and Desktops の製品バージョンを示します。	7.42.0.0

ペイロード

キー	説明	例
TotalCustomScopes	カスタムスコープの総数を示します。	2
TotalCustomRoles	カスタムロールの総数を示します。	4

ライセンス テレメトリ データを難読化する

ライセンス テレメトリで送信される情報の機密性を考慮し、Citrix はデータを難読化するオプションを提供します。

次の表に、難読化できるデータを示します。

フィールド	説明	例
ユーザー	セッション起動を開始するユーザーを一意に識別するためのユーザー ID を識別します。	• fullName: `C648FE671A44B3F7` • samName: `C758LH671A44B3F7` • ユーピーエヌ: `C7948FE671A44B3F7` • userLicenseId: `C265FE671A44B3F7`

フィールド	説明	例
		• userSid: `C097FE671A44B3F7`
デバイス -> デバイス名	デバイスのフレンドリ名を示します。	`C758LH671A44B3F7`
workerSid	セッションに使用されるVDAの一意の識別子を示します。	`1E5LH671A44B3F7`
AdminLoginList	一意の管理者SamAccountNameのリストを示します	`{AdminLoginList: [UFMJ+JvXOTHO9mQDsOweiw= =]}`

スクランブルを有効または無効にするには、Delivery Controllerで次のPowerShellコマンドを実行します。

> **注：**
>
> Citrix Service Provider™ (CSP) のお客様の場合、スクランブルは常に無効になっています。CSP のお客様は、PowerShell コマンドを使用してスクランブルを有効にすることはできません。

1. Delivery ControllerホストからPowerShellウィンドウを開きます。
2. コマンド `asnp citrix` を実行して、Citrix固有のPowerShellモジュールをロードします。
3. スクランブルを有効または無効にするには、次のコマンドを実行します。

   デフォルトでは、値は`1`または`true`であり、ライセンステレメトリデータのスクランブルを有効にします。

   無効にするには：

   ```
   Set-BrokerServiceConfigurationData Core.ScrambleLicensingData
   -SettingValue $false
   ```

スクランブルを無効にした後、次のコマンドを使用して有効にできます。

```
Set-BrokerServiceConfigurationData Core.ScrambleLicensingData
-SettingValue $true
```

ライセンスに関するFAQ

注：

- COVID-19パンデミックに関連する事業継続リソースについては、CTX27055を参照してください。
- 事業継続の維持に関する一般情報については、事業継続 - オンデマンドを参照してください。
- 現在のCitrix License Serverの詳細については、ライセンスを参照してください。

Citrix®ライセンス

ライセンスファイルを取得するにはどうすればよいですか?

ライセンスアクセスコードはメールでお送りします。ライセンスアクセスコードを使用してライセンスファイルを生成する方法は3つあります。

- `citrix.com`のMyAccountページから**ライセンスを管理**します。詳細については、citrix.comでライセンスを管理を参照してください。
- Web Studioを使用して購入を割り当てると、ライセンスファイルがCitrix License Serverに自動的にインストールされます。
- Citrix License Server内のCitrix Licensing Managerを使用して購入を割り当て、ライセンスファイルをインストールします。詳細については、ライセンスのインストールを参照してください。

MyAccountでライセンスを割り当てる方法?

ライセンスの割り当てを参照してください。

割り当てられたライセンスをライセンスサーバーに追加する方法?

ライセンスの変更を参照してください。

Citrixライセンスが使用するTCPポートは何ですか?

- License Server のポート番号は 27000 です
- ベンダーデーモンのポート番号は 7279 です
- Web Service for Licensing のポートは 8083 です

Citrix License Server とは何ですか?

Citrix License Server は、ライセンスをネットワーク全体で共有できるシステムです。詳細については、「ライセンス操作の概要」を参照してください。

Citrix License Server を仮想化またはクラスター化できますか?

はい。Citrix License Server を仮想化またはクラスター化できます。詳細については、「クラスター化されたライセンスサーバー」を参照してください。

Citrix License Server を仮想化すると、どのようなメリットがありますか?

Citrix License Server を仮想化すると、冗長なソリューションが提供されます。このソリューションにより、ダウンタイムなしで複数の物理サーバー間を移動できます。

Citrix License Server を仮想化する場合、考慮すべき制限はありますか?

いいえ。

Citrix License Server は、Citrix Virtual Apps and Desktops™ 展開のすべてのライセンスを管理しますか?

Citrix License Server は、Citrix Virtual Apps™ および Desktop 用に受け取るすべてのライセンスを管理しますが、Citrix Gateway で使用される Premium Edition のライセンスは除きます。これらのセキュリティ指向のネットワークデバイスに必要な、ネットワークアプライアンスに組み込まれたライセンスサーバーが、それらのライセンスを管理します。

Citrix Licensing Manager とは何ですか?

Citrix Licensing Manager を使用すると、Citrix Licensing Manager をインストールした License Server からライセンスファイルをダウンロードして割り当てることができます。Citrix Licensing Manager は推奨される License Server 管理方法であり、次のことを可能にします。

- ライセンスサーバーのCitrix Cloud™への短縮コード登録と、登録の簡単な削除。
- ユーザーアカウントとグループアカウントを構成する。
- ダッシュボードを使用して、インストール済み、使用中、期限切れ、利用可能なライセンス、およびCustomer Success Servicesの期日を表示する。
- レポート作成に使用するため、ライセンス使用状況データをエクスポートする。

- 履歴使用状況データの保持期間を構成する。デフォルトのデータ保持期間は180日です。
- ライセンスアクセスコードまたはダウンロードしたファイルを使用して、ライセンスサーバーへのライセンスファイルのインストールを簡素化。
- ライセンスバーストモードを有効化および無効化する。
- 顧客体験向上プログラム (CEIP) とコールホームを設定します。
- Customer Success Servicesの更新ライセンスを自動的または手動で確認し、見つかった場合は通知するか、ライセンスをインストールします。
- ライセンスサーバーの状態（起動ライセンスの不足、時間の問題、アップローダーの障害）を通知する。
- これらのポートを変更する:
  - ライセンスサーバー（デフォルト 27000）
  - ベンダーデーモン（デフォルト 7279）
  - ライセンス用Webサービス（デフォルト 8083）

詳細については、Citrix Licensing Managerを参照してください。

Citrix License Administration Consoleはどこにありますか?

License Administration Consoleはサポートされなくなり、License Serverバージョン11.16.6から削除されました。Citrix Licensing Managerの使用をお勧めします。

License ServerがStudioと同じドメイン内にあるか、信頼されたドメイン内にある場合、Studioを使用してライセンスを管理および追跡できます。

詳細については、Citrix Licensing Managerを参照してください。

ライセンス割り当て期間とは何ですか?

ライセンス割り当て期間とは、Citrix Virtual Apps and Desktopsライセンスがユーザーまたはデバイスに割り当てられる期間のことです。デフォルトのライセンス割り当て期間は90日です。

組織が購入したライセンスの数を確認するにはどうすればよいですか?

購入したすべてのライセンスは、`<https://www.citrix.com>`の**My Account**ページにある安全な**Manage Licenses**ツールボックスから、いつでも（24時間365日）確認およびアクセスできます。

いつでも使用中のライセンス数を確認するにはどうすればよいですか?

Citrix Licensing ManagerとStudioは、リアルタイムのライセンス使用状況に関する詳細を提供します。

License Serverのディザスターリカバリとメンテナンス

License Serverのディザスターリカバリとメンテナンスについては、Citrix Licensingドキュメントのディザスターリカバリとメンテナンスを参照してください。

Citrix Virtual Apps and Desktopsのライセンス

Citrix Virtual Apps and Desktopsはどのようにライセンスされますか?

Citrix Virtual Apps and Desktopsのライセンスは、ユーザー単位とデバイス単位、および同時使用ライセンスモデルを提供します。

ユーザー/デバイス:

柔軟なユーザー/デバイスモデルは、以下と連携します。

- 企業全体のデスクトップ利用。
- 基盤となるMicrosoftデスクトップ仮想化ライセンス。
- 仮想デスクトップとアプリへのアクセスが時々しか必要ないユーザー向けの同時接続ライセンス。

ユーザー/デバイスライセンスにより、ユーザーは無制限のデバイスから仮想デスクトップとアプリにアクセスできます。デバイスライセンスにより、無制限のユーザーが単一のデバイスから仮想デスクトップとアプリにアクセスできます。このアプローチは、最大限の柔軟性を提供し、Microsoftデスクトップ仮想化ライセンスとの整合性を向上させます。

> **重要:**

> ライセンスをユーザーまたはデバイスに手動で割り当てることはできません。ライセンスサーバーまたはクラウドサービスがライセンスを割り当てます。ユーザー/デバイスライセンスでは、一度割り当てられたライセンスは、90日間非アクティブになるまで別のユーザーに割り当てることはできません。

> **同時接続:**

同時接続ライセンスは、任意のユーザーおよび任意のデバイスに対して、無制限の仮想アプリとデスクトップへの1つの接続を許可します。ライセンスはアクティブなセッション中にのみ消費されます。セッションが切断または終了すると、ライセンスはプールに戻されます。

ユーザー/デバイスライセンスの詳細については、ユーザー/デバイスライセンスを、同時接続ライセンスについては、同時接続ライセンスを参照してください。

ライセンスを購入する前にCitrix Virtual Apps and Desktopsを試用することはできますか?

はい。Citrix Virtual Apps and Desktopsソフトウェアをダウンロードし、試用モードで実行できます。試用モードでは、ライセンスなしで、Citrix Virtual Apps and Desktopsをオンプレミスで30日間、10接続まで使用できます。詳細については、評価ライセンスを参照してください。

Citrix Cloud向けのCitrix DaaS™（旧Citrix Virtual Apps and Desktopsサービス）は、承認に基づいて試用サービスとして利用できます。詳細については、Citrix担当者にお問い合わせください。

CitrixはCitrix Virtual Apps and Desktopsの同時接続をどのように定義するか?

Citrix Virtual Apps and Desktopsの同時接続モデルでは、任意のユーザーおよび任意のデバイスに対して、無制限の仮想アプリとデスクトップへの1つの接続を許可します。ライセンスはアクティブなセッション中にのみ消費されます。セッションが切断または終了すると、ライセンスは再発行のためにプールに戻されます。詳細については、同時接続ライセンスを参照してください。

共通のライセンスサーバーに複数のエディションのCitrix Virtual Apps and Desktopsライセンスを展開できるか?

はい。ライセンスサーバーは、Citrix Virtual AppsとCitrix Virtual Desktopsの両方のライセンスを同時に管理します。最新のライセンスサーバーバージョンをインストールすることをお勧めします。お使いのライセンスサーバーのバージョンが最新であるか不明な場合は、Citrixダウンロードサイトの番号と比較して確認してください。

単一のサイトでCitrix Virtual Appsライセンスと Citrix Virtual Apps and Desktopsライセンスの両方を使用できますか?

バージョンによっては、単一のCitrix Virtual AppsまたはCitrix Virtual Apps and Desktopsサイトで、ユーザー/デバイスまたは同時使用のいずれかのライセンスモデルをサポートできます。単一のCitrix Virtual AppsまたはCitrix Virtual Apps and Desktopsサイトでサポートできるエディションは1つだけです。詳しくは、「マルチタイプライセンス」を参照してください。

マルチタイプライセンスをサポートする最小バージョンは、XenAppおよびXenDesktop 7.15 Long Term Service Release (LTSR)とCitrix Virtual Apps and Desktops 7 1808です。

ライセンスサーバーにCitrix Virtual Apps and Desktopsユーザー/デバイスライセンスまたはCitrix Virtual Apps and Desktops同時使用ライセンスがインストールされている場合、製品モデルとしてCitrix Virtual Apps同時使用を選択できますか?

Citrix Virtual AppsをCitrix Virtual Apps and Desktops AdvancedまたはPremium Editionの機能として使用する場合、Citrix Virtual Appsのライセンスモデルは、Citrix Virtual Apps and DesktopsのAdvancedまたはPremium Editionと同じになります。Citrix Virtual Apps and Desktopsを購入した場合、Citrix Virtual Apps機能のみを使用する予定であっても、ライセンスはCitrix Virtual Apps and Desktopsとして構成してください。製品モデルとしてCitrix Virtual Appsを選択するのは、ライセ

ンスサーバーにCitrix Virtual Apps同時使用スタンドアロンライセンスがインストールされている場合のみです。

各Citrix Virtual AppsおよびCitrix Virtual Apps and Desktopsエディションには、どのような製品コンポーネントが含まれていますか?

エディションごとの全機能マトリックスについては、「Citrix Virtual Apps and Desktopsの機能」を参照してください。

Citrix Virtual Apps and Desktops EULAに準拠して、Citrix Virtual Desktops™環境のライセンスを付与するにはどうすればよいですか?

Citrix Virtual Apps and Desktops EULAに準拠して、ユーザー/デバイスまたは同時使用ライセンスモデルでCitrix Virtual Apps and Desktopsを展開するには、ライセンスファイルをライセンスサーバーに適用します。ライセンスサーバーは、ライセンスコンプライアンスを制御および監視します。購入した製品に基づいて製品を構成することをお勧めします。たとえば、Citrix Virtual Apps and Desktops Premiumを購入したが、Citrix Virtual Apps機能のみを使用したい場合は、コンプライアンスを満たすために製品をCitrix Virtual Apps and Desktopsに構成します。詳しくは、「製品ライセンスコンプライアンスセンター」を参照してください。

Citrix Virtual Apps EULAに準拠して、Citrix Virtual Apps環境のライセンスを付与するにはどうすればよいですか?

Citrix Virtual Apps EULAに準拠して、同時使用ライセンスモデルでCitrix Virtual Appsを展開するには、ライセンスファイルをライセンスサーバーに適用します。ライセンスサーバーは、ライセンスコンプライアンスを制御および監視します。

Citrix Virtual Apps and Desktopsのサービスオプション（Long Term Service Release (LTSR)またはCurrent Release (CR)）にライセンス要件はありますか?

Long-Term Service ReleaseなどのCitrix Virtual Apps and Desktopsのサービスオプションは、Customer Success Servicesプログラムの特典です。LTSRの特典を受けるには、アクティブなCustomer Success Servicesが必要です。詳しくは、「[Citrix Virtual Apps、Citrix Virtual Apps and Desktops、およびXenServerのサービスオプション」を参照してください。

Remote Browser Isolation (RBI) サービスのプールされた時間はどのように機能しますか?

サービスを最低25ユーザー購入すると、すべてのユーザーで共有される5000時間のサービス利用権が付与されます。その後のユーザー権限の購入では、プールされた時間の権利は増加しません。サービス時間の権利を増やすには、アドオンパックを購入してください。

CCUライセンスでRemote PC Accessを使用できますか?

はい。

Remote PC Accessの詳細については、Remote PC Accessを参照してください。

Citrix環境のソフトウェアメンテナンスの有効期限が切れるとどうなりますか?

ソフトウェアメンテナンス (SWM) またはサブスクリプションの有効期限が切れると、ソフトウェアアップグレードとテクニカルサポートへのアクセスが一時停止されます。また、ライセンスの種類と製品バージョンによっては、エンドユーザーと管理者に、環境がサポートされていないことを示す特定の警告通知が届きます。

これらの通知は、サーバー上のすべてのライセンスの有効期限が切れた場合にのみトリガーされます。

エンドユーザーエクスペリエンス

ユーザーはセッション起動後に警告メッセージを受け取ります。メッセージには次のように表示されます。

```
Citrix Virtual Apps and Desktops warning: Your corporate Citrix
environment is currently unsupported. Please contact your IT department to
resolve.
```

管理者エクスペリエンス

管理者は、Citrix Studioコンソール内で、間もなく期限切れになる、または現在期限切れになっていることを警告するアラートを確認できます。

ライセンスの種類による有効期限の動作

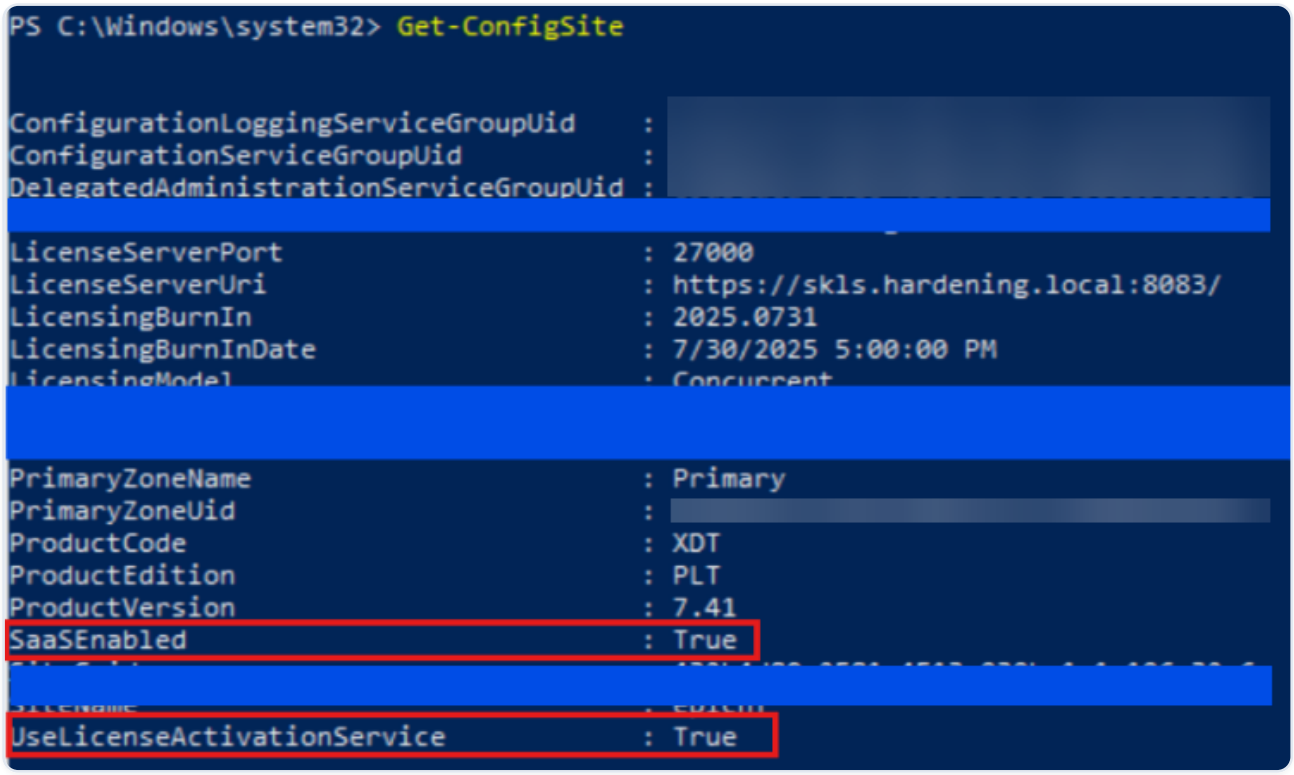
これらのメッセージの表示タイミングは、ライセンスの種類とインストールされているCitrix Virtual Apps and Desktopsのバージョンによって異なります。

オンプレミスサブスクリプションライセンス

- エンドユーザー警告: サブスクリプションの有効期限が切れた後、猶予期間中に表示されます。
- 管理者警告: サブスクリプションの有効期限が切れる30日前にStudioに表示されます。
- サポートされているバージョン:
  - 現在のリリース: Citrix Virtual Apps and Desktops 2411以降。
  - LTSR: 2203 CU6、2402 CU1、およびそれ以降のLTSRリリース

サイトのLAS状態を確認するにはどうすればよいですか?

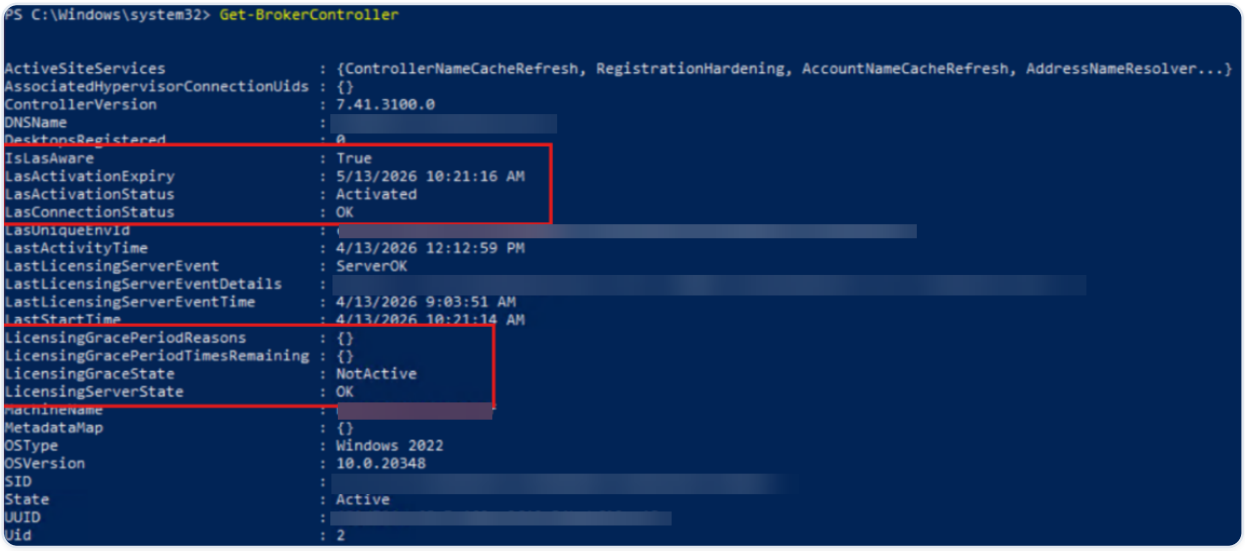
LASアクティベーション状態とSaaSビットステータスを確認するには、`Get-configsite`を実行します。



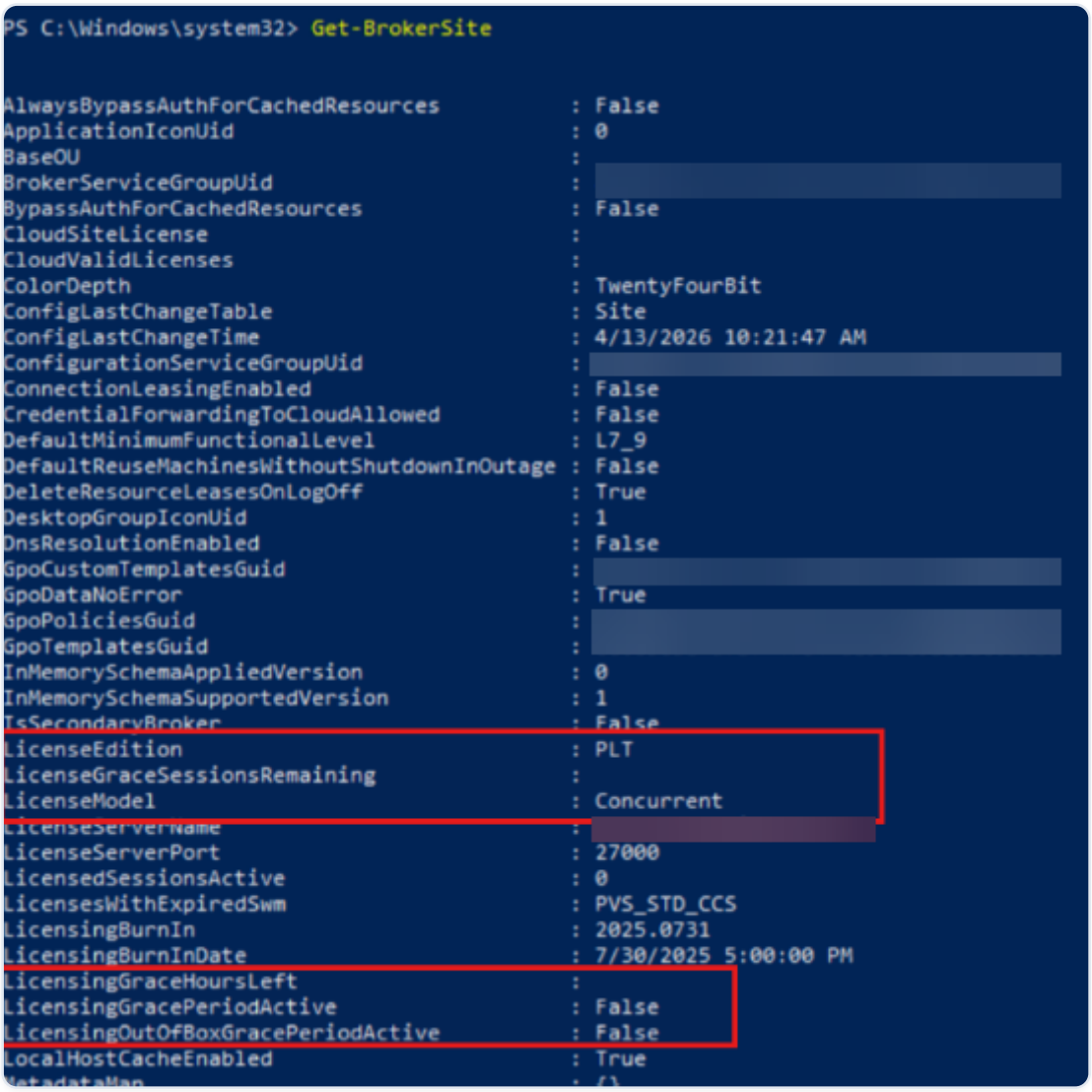
サイトが緊急ライセンスキャッシュモードになっているかを確認するにはどうすればよいですか?

緊急キャッシュモードと残り時間の詳細を取得するには、`Get-Brokercontroller`と`Get-brokersite`を実行します。

- `Get-Brokercontroller`の出力:



- `Get-brokersite`の出力:



コマンドの詳細については、以下を参照してください:

- Get-BrokerController
- Get-ConfigSite

ライセンスに関するDelivery Controllerのイベントビューアーログについては、「ライセンスイベントに関連するイベントビューアーログ」を参照してください。

ユーザー/デバイスライセンス

Citrixは、ユーザー/デバイスライセンスモデルでユーザーにライセンスをどのように割り当てますか?

ユーザー/デバイスライセンスモデルでは、ライセンスサーバーは一意のユーザーIDにライセンスを割り当てます。これにより、その単一ユーザーは無制限のデバイスから無制限の接続を行うことができます。ユーザーがデスクトップまたはデバイスに接続する場合、仮想デスクトップまたはアプリケーションにアクセスするには、そのユーザーに割り当てられた1つのライセンスが必要で

す。ライセンスサーバーまたはクラウドサービスがライセンスを割り当てます。これらのライセンスを手動で割り当てることはできません。ライセンスは共有デバイスではなく、ユーザーに割り当てられます。一度ライセンスが割り当てられると、90日間非アクティブになるまで、別のユーザーに割り当てることはできません。詳細については、「ユーザー/デバイスライセンス」を参照してください。

Citrixは、ユーザー/デバイスライセンスモデルでライセンスデバイスをどのように定義しますか?

ライセンスデバイスには、一意のエンドポイントデバイスIDが必要です。ユーザー/デバイスモデルでは、デバイスとは、Citrix Virtual Apps and Desktopsのインスタンスにアクセスするために、個人が使用することを承認したあらゆる機器を指します。共有デバイスの場合、1つのCitrix Virtual Apps and Desktopsユーザー/デバイスライセンスで、そのデバイスを共有する複数のユーザーをサポートできます。たとえば、共有デバイスは、教室のワークステーションや病院の臨床ワークステーションなどです。

Citrix Virtual Desktops Standard Editionの同時使用ライセンスをユーザー単位とデバイス単位のモデルに変換できますか?

Citrix Virtual Desktops Standard Editionの同時使用ライセンスをCitrix Virtual Desktops Standard Editionのユーザー/デバイスライセンスに変換することはできません。同様に、Citrix Virtual Desktops Standard Editionのユーザー/デバイスライセンスをCitrix Virtual Desktops Standard Editionの同時使用ライセンスに変換することもできません。

Citrix Virtual Desktops Standard Editionの同時使用ライセンスをお持ちで、ユーザー/デバイスライセンスモデルをご希望の場合は、Citrix Virtual Apps and Desktops AdvancedまたはPremium Editionにアップグレードしてください。

元のライセンス	STANDARD同時使用へ	STANDARDユーザー/デバイスへ	ADVANCEDユーザー/デバイスへ	PREMIUMユーザー/デバイスへ
Citrix Virtual Desktops Standard Edition の同時使用ライセンス	該当なし	同時使用からユーザー/デバイスへの変換は許可されていません	ライセンスモデルを変換することはできませんが、Citrix Virtual Apps and Desktops Advanced または Premium Edition にアップグレードすることはできます。	ライセンスモデルを変換することはできませんが、Citrix Virtual Apps and Desktops Advanced または Premium Edition にアップグレードすることはできます。

元のライセンス	STANDARD同時使用へ	STANDARDユーザー/デバイスへ	ADVANCEDユーザー/デバイスへ	PREMIUMユーザー/デバイスへ
シトリックス バーチャル デスクトップ スタンダード エディション ユーザー/デバイス ライセンス	ユーザー/デバイスから同時使用への変換は許可されていません	該当なし	該当なし	該当なし

同時使用ライセンスは、ユーザー/デバイスライセンスとどのように異なりますか?

同時使用ライセンスは、デバイスの同時接続に基づいています。同時使用ライセンスは、デバイスがアクティブな接続を確立している場合にのみ使用されます。接続が終了すると、同時使用ライセンスはライセンスプールに戻り、すぐに使用可能になります。このライセンスモデルは、一時的な使用におすすめです。ユーザー/デバイスライセンスは一定期間リースされ、リース期間が終了するまで他のユーザーは利用できません。

ユーザー/デバイスモデルでは、同じ企業内でユーザーとデバイスの両方にライセンスを割り当てることができます?

はい。両方のタイプを同じ企業内で使用できます。ライセンスサーバーは、使用状況に基づいてユーザーまたはデバイスにライセンスを最適に割り当てます。これらのライセンスを手動で割り当てることはできません。

ライセンスを付与するユーザーまたはデバイスの数をどのように決定すればよいか?

適切なライセンス数を決定するために、ユースケースの要件を評価してください。ユーザー/デバイスライセンスでは、無制限の数のデバイスから、無制限の仮想デスクトップと仮想アプリに無制限にアクセスできます。同時使用ライセンスでは、無制限の数のユーザーが使用できる単一のデバイスから、無制限の仮想デスクトップと仮想アプリに無制限にアクセスできます。次の式を考慮してください。

```
(Number of total users) – (number of users that only access exclusively

 with shared devices) + (number shared devices) = total number

 of licenses to buy.



For example, there are 1000 total users at the hospital. If 700 of them
```

```
access only

Citrix Virtual Desktops from 300 shared devices in the hospital, the
number of

licenses to purchase is 1000 – 700 + 300 = 600 licenses.
```

ユーザー/デバイスモデルでは、ライセンスを持つユーザーが自分の環境に接続するために使用できるデバイスの最大数はいくつですか?

各ライセンスユーザーは、接続されているデバイスまたはオフラインのデバイスを無制限に使用できます。

ユーザー/デバイスモデルでは、ライセンスを持つデバイスにアクセスできるユーザーの最大数はいくつですか?

各ライセンスデバイスは、組織内の無制限の数のユーザーにサービスを提供できます。

ユーザー/デバイスモデルでは、ライセンスユーザーが一度に消費できる仮想デスクトップまたはRBI Webアプリケーションの最大数はいくつですか?

各ライセンスユーザーは、無制限の数の仮想デスクトップまたはWebアプリケーションに接続できます。

既存のCitrix Virtual Apps and Desktops環境で、ライセンスユーザー/デバイスの数を増やすためにCitrix Virtual Apps and Desktopsライセンスを購入できますか?

はい。既存のCitrix Virtual Apps and Desktops環境で、ライセンスユーザー/デバイスの数を増やすためにCitrix Virtual Apps and Desktopsライセンスを購入できます。

承認されたユーザー/デバイスライセンスを解放するにはどうすればよいですか?

承認されたユーザー/デバイスの割り当てを解放するには、EULAの条件に従って`udadmin`ユーティリティを使用します。その後、ライセンスサーバーはライセンスを次の適切なユーザー/デバイスに割り当てます。詳細については、「ユーザーまたはデバイスのライセンスの表示または解放」を参照してください。

購入したユーザー/デバイスライセンス数を超過した場合はどうなりますか?

ユーザー/デバイスライセンスには10%のオーバードラフトが含まれており、これはライセンス生成時に含まれます。オーバードラフトは、インストール済みのライセンス数にも含まれます。使用量の急増がオーバードラフトを含むインストール済み数を超えると、追加ユーザーのアクセスは拒否されます。追加ユーザーのアクセスを有効にするには、新しいライセンスを購入して展開してください。

ライセンスのオーバードラフトを含め、すべてのライセンスが使用中の場合、ライセンスバーストモードにより製品への無制限の接続が可能になります。ライセンスバーストモードは、最大ライセンス数を超過した理由を特定し、ユーザーを中断することなく追加のライセンスを購入する時間を提供します。この期間は、15日が経過するか、追加の小売ライセンスをインストールするかのいずれか早い方まで続きます。詳細については、「ライセンスバーストモード」を参照してください。

Directorはライセンスキャッシュモードの状態を表示します。詳細については、「Directorダッシュボードのパネル」を参照してください。

ライセンスユーザーが一度に消費できる仮想アプリケーションの最大数はいくつですか?

各ライセンスユーザーは、無制限の数の仮想アプリケーションに接続できます。

ライセンスユーザーが組織を離れた場合はどうなりますか?

既存のライセンスユーザーが組織を離れる場合、Citrixに通知することなく、そのユーザーのライセンスを解放できます。ライセンスを解放するには、`udadmin`ユーティリティを使用します。ライセンスを解放しない場合、ライセンスサーバーは90日間の非アクティブ状態の後、自動的にライセンスを解放します。この情報は、EULAに指定された条件に従います。

ライセンスユーザーが長期間不在の場合、どうなりますか?

既存のライセンスユーザーが長期間不在の場合、Citrixに通知することなくライセンスを解放し、再割り当てできるようにすることができます。ライセンスを解放するには、`udadmin`ユーティリティを使用してください。

組織内でライセンスデバイスを交換した場合、どうなりますか?

既存のライセンスデバイスを交換する場合、Citrixに通知することなくライセンスを解放し、再割り当てできるようにすることができます。ライセンスを解放するには、`udadmin`ユーティリティを使用してください。

ライセンスデバイスが長期間サービス停止した場合、どうなりますか?

既存のライセンスデバイスが長期間サービス停止した場合、Citrixに通知することなくライセンスを解放し、再割り当てできるようにすることができます。ライセンスを解放するには、`udadmin`ユーティリティを使用してください。ライセンスを解放しない場合、ライセンスサーバーは90日間アクティビティがないと自動的にライセンスを解放します。この情報は、EULAに規定されている条件に従います。

デバイスまたはユーザーにライセンスを割り当てた後で、ユーザーライセンスをデバイスライセンスに、またはその逆に切り替えることはできますか?

はい、この変更は自動的に行われます。ライセンスサーバーは、使用パターンに基づいてユーザーまたはデバイスのいずれかにライセンスを割り当てます。使用パターンが変更された場合、ライセンスサーバーは新しい使用状況に基づいて割り当てを切り替えることがあります。ライセンスサーバーは常に、お客様にとって最も経済的な方法でライセンスを割り当てます。また、ライセンスサーバーは、90日間の割り当て期間後に**未使用**のライセンスを特定するためにライセンスを監視します。90日間の割り当て期間後に未使用と識別されたライセンスは、他のユーザーまたはデバイスに再割り当てできます。

同時使用ライセンス

同時使用モデルでは、Citrix Virtual Apps and Desktopsのライセンスユーザーが一度に消費できる仮想デスクトップの最大数はいくつですか?

エンドポイントは多数のユーザーにサービスを提供でき、無制限の接続を許可します。

以前のバージョンのCitrix Virtual Apps and Desktopsの同時使用ライセンスと、新しいユーザー/デバイスまたは同時使用ライセンスを単一のライセンスサーバーに展開できますか?

はい。ユーザー/デバイスまたは同時使用ライセンスの展開をサポートするために、同じライセンスサーバーを引き続き使用できます。

同時使用ライセンスとユーザー/デバイスライセンスまたは同時使用ライセンスを単一のライセンスサーバーに展開できます?

はい。同時使用およびユーザー/デバイスまたは同時使用ライセンスの展開をサポートするために、同じライセンスサーバーを引き続き使用できます。

Citrix Virtual Apps and Desktops AdvancedおよびPremiumエディションには、Citrix Virtual Appsの同時使用ライセンスが含まれています?

Citrix Virtual Apps and Desktops AdvancedおよびPremiumのユーザー/デバイスライセンスには、互換性のためのみにCitrix Virtual Appsの同時使用ライセンスが含まれています。これらの同時使用ライセンスは、ユーザー/デバイスライセンスと互換性のない以前の製品バージョンでのみ使用できます。ユーザー/デバイスライセンスに含まれる同時使用互換ライセンスの使用は、XenApp 6.5より前のバージョンおよびXenDesktop 5.0 Service Pack 1より前のバージョンでのみ許可されます。

購入した同時使用ライセンス数を超過した場合、どうなりますか?

すべてのライセンスが使用中の場合、ライセンスバーストモードにより、製品への無制限の接続が可能になります。ライセンスバーストモードは、最大ライセンス数を超過した理由を特定し、ユー

ザーを中断することなく追加のライセンスを購入する時間を与えます。この期間は、15日が経過するか、追加のリテールライセンスをインストールするかのいずれか早い方まで続きます。詳細については、「ライセンスバーストモード」を参照してください。

Directorはライセンスキャッシュモードの状態を表示します。詳細については、「Directorダッシュボードのパネル」を参照してください。

オーバードラフトライセンス

オーバードラフトライセンスを取得するにはどうすればよいですか?

ユーザー/デバイス、ユーザー、またはデバイスライセンスモデルをサポートする製品（Citrix Cloudを除く）には、アクセス拒否を防ぐために限られた数の追加ライセンスを使用できるライセンスオーバードラフト機能が含まれています。オーバードラフト機能は、ライセンスの権利としてではなく、便宜のために提供されます。同時使用ライセンスおよびサーバーライセンスにはオーバードラフトは含まれません。使用されたオーバードラフトライセンスは、初回使用から30日以内に購入する必要がありますが、使用期間は30日に限定されません。Citrixは、新しい製品リリースでオーバードラフト機能を削除する権利を留保します。詳細については、「ライセンスオーバードラフト」を参照してください。

ライセンスオーバードラフトを識別するにはどうすればよいですか?

Citrix Licensing Managerで、オーバードラフト中のライセンス数を含む使用状況情報を表示できます。Studioにもオーバードラフトの使用状況情報が含まれています。

オーバードラフトライセンスが消費されるとどうなりますか?

Citrix Virtual Apps and Desktops環境へのアクセスを可能にするために、インストールされているライセンスからライセンスが割り当てられます。このオーバードラフトライセンスは、他のライセンスと同等のアクセスと機能を提供します。

オーバードラフトライセンスが消費されたときにアラートを受け取ることができます?

現在、オーバードラフトライセンスが消費されたときに提供される特定のアラートはありません。

オーバードラフトライセンスはどのくらいの期間消費できます?

最初の使用から30日以内に使用された超過ライセンスを購入してください。

その他の製品固有のライセンス情報

- シトリックス ADC
- シトリックス クラウド

- シトリックス エンドポイント マネジメント
- シトリックス ゲートウェイ
- XenServer
- シトリックス ライセンシング

マシンの負荷分散

> **注：**
>
> Web Studio (Webベース) と Citrix Studio (Windowsベース) の2つの管理コンソールを使用して、Citrix Virtual Apps and Desktops™ 展開を管理できます。この機能はWeb Studioでのみ利用可能です。

> この機能は、シングルセッションOSまたはマルチセッションOSのすべてのカタログに適用されます。垂直ロードバランシングは、マルチセッションOSマシンにのみ適用されます。

> ロードバランシングは、サイトレベルとデリバリーグループレベルで構成できます。オプションは垂直と水平の2つです。デフォルトでは、水平ロードバランシングが有効になっています。

サイトレベルでのロードバランシング設定

- **垂直ロードバランシング**。受信ユーザーセッションを、まだ最大負荷に達していない最も負荷の高いマシンに割り当てます。これにより、新しいマシンに移行する前に既存のマシンが飽和状態になります。既存のマシンから切断されたユーザーは、それらのマシンの容量を解放します。その後、受信負荷はそれらのマシンに割り当てられます。垂直ロードバランシングはユーザーエクスペリエンスを低下させますが、コストを削減します（セッションは電源オンのマシン容量を最大化します）。

  例：それぞれ10セッション用に構成された2台のマシンがあるとします。最初のマシンが最初の10の同時セッションを処理します。2番目のマシンが11番目のセッションを処理します。

  > **ヒント:**

> マシンがホストできるセッションの最大数を指定するには、最大セッション数 ポリシー設定を使用します。

> または、PowerShellを使用して、サイト全体で垂直負荷分散を有効または無効にできます。`Set-BrokerSite` コマンドレットで `UseVerticalScalingForRdsLaunches` 設定を使用します。`UseVerticalScalingForRdsLaunches` 設定の値を表示するには、`Get-BrokerSite` を使用します。詳細については、コマンドレットのヘルプを参照してください。

- **水平ロードバランシング**。受信ユーザーセッションを、利用可能な最も負荷の低い、電源オンのマシンに割り当てます。水平ロードバランシングはユーザーエクスペリエンスを向上させますが、コストが増加します（より多くのマシンが電源オンのまま維持されるため）。デフォルトでは、水平ロードバランシングが有効になっています。

  例：それぞれ10セッション用に構成された2台のマシンがあるとします。最初のマシンが5つの同時セッションを処理します。2番目のマシンも5つを処理します。

この機能を構成するには、Web Studioから、左ペインで**設定**を選択します。**マルチセッションカタログのロードバランシング**の下にあるオプションを選択します。

デリバリーグループレベルでのロードバランシング設定

デリバリーグループレベルでロードバランシングを構成すると、サイトレベルから継承されたロードバランシング設定を上書きできます。デリバリーグループレベルで垂直ロードバランシングを選択すると、各マシンの最大利用率を達成できます。これにより、パブリッククラウドでのコスト削減に役立ちます。この構成は、新しいデリバリーグループの作成時または既存のデリバリーグループの編集時に行うことができます。

水平ロードバランシング。セッションは電源オンのマシン間で分散されます。たとえば、それぞれ10セッション用に構成された2台のマシンがある場合、最初のマシンが5つの同時セッションを処理し、2番目のマシンも5つを処理します。

垂直ロードバランシング。セッションは電源オンのマシン容量を最大化し、マシンコストを節約します。たとえば、それぞれ10セッション用に構成された2台のマシンがある場合、最初のマシンが最初の10の同時セッションを処理します。2番目のマシンが11番目のセッションを処理します。

ローカルホストキャッシュ

Citrix Virtual Apps and Desktopsサイトデータベースが常に利用可能であることを保証するため、CitrixはMicrosoftの高可用性ベストプラクティスに従って、フォールトトレラントなSQL Server展

開から始めることを推奨します。(サポートされているSQL Serverの高可用性機能については、データベースを参照してください。)しかし、ネットワークの問題や中断により、ユーザーがアプリケーションやデスクトップに接続できなくなる可能性があります。

ローカルホストキャッシュ機能により、障害発生時にサイトでの接続仲介操作を継続できます。障害は、オンプレミスのCitrix®環境でDelivery Controller™とサイトデータベース間の接続が失敗したときに発生します。サイトデータベースに90秒間アクセスできない場合、ローカルホストキャッシュが作動します。

XenAppおよびXenDesktop 7.16以降、接続リース機能（以前のリリースにおける先行の高可用性機能）は製品から削除され、利用できなくなりました。

データコンテンツ

ローカルホストキャッシュには、メインデータベースの情報の一部である以下の情報が含まれます。

- サイトから公開されたリソースへの権限が割り当てられているユーザーおよびグループの ID。
- 現在使用している、または最近使用した、サイトから公開されたリソースのユーザーの ID。
- サイトで構成されている VDA マシン（リモート PC アクセス マシンを含む）の ID。
- 公開されたリソースへの接続に積極的に使用されているクライアントCitrix Receiver™マシンのID（名前とIPアドレス）。

また、メインデータベースが利用できなかった間に確立された、現在アクティブな接続に関する情報も含まれます。

- Citrix Receiverによって実行されたクライアントマシンのエンドポイント分析の結果。
- サイトに関与するインフラストラクチャマシン（NetScaler GatewayやStoreFront™サーバーなど）のID。
- ユーザーによる最近のアクティビティの日時と種類。

動作の仕組み

次の図は、通常の操作中のローカルホストキャッシュのコンポーネントと通信パスを示しています。

ローカルホストキャッシュの通常の操作中の通信パスの図(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/lhc-normal1.png)

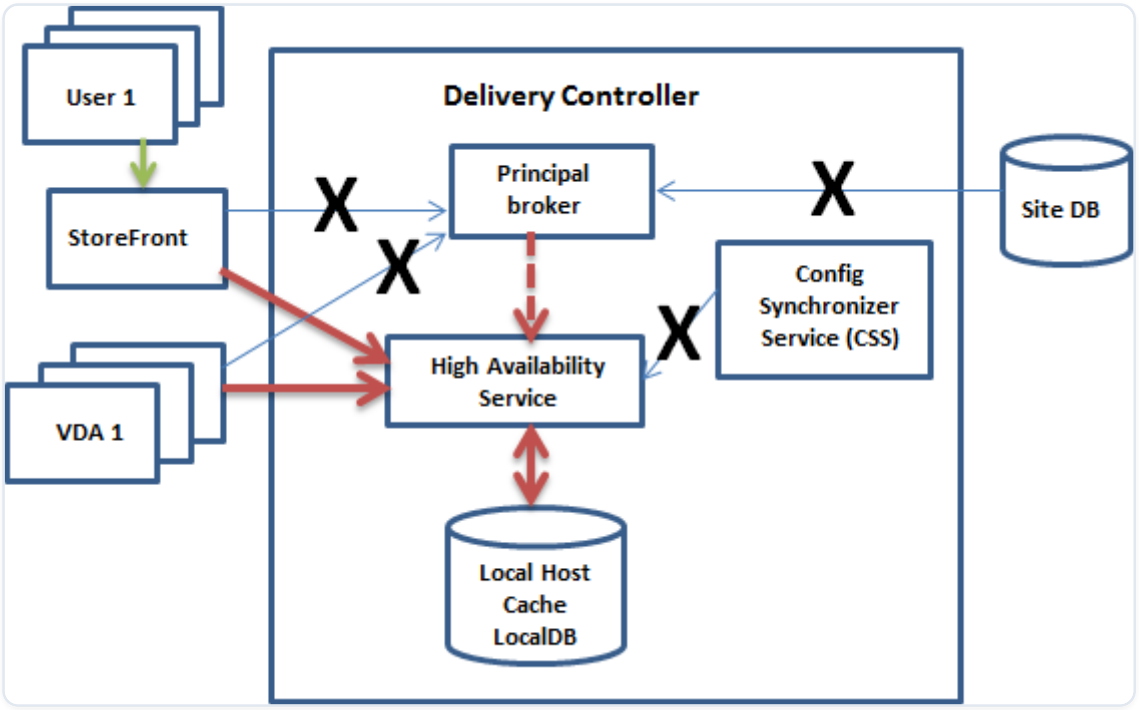
通常の操作中

- Controller上の *プリンシパルブローカー* (Citrix Broker Service) は、StoreFrontからの接続要求を受け入れます。ブローカーはサイトデータベースと通信し、ユーザーをControllerに登録されているVDAに接続します。
- Citrix Config Synchronizer Service (CSS) は、約5分ごとにブローカーに問い合わせて、変更があったかどうかを確認します。これらの変更は、管理者によって開始されたもの（デリバリーグループのプロパティの変更など）またはシステムアクション（マシンの割り当てなど）である可能性があります。
- 前回のチェック以降に構成変更があった場合、CSS は情報を Controller 上のセカンダリブローカーに同期 (コピー) します。(セカンダリブローカーは高可用性サービスとも呼ばれます。)

  前回のチェック以降に変更された項目だけでなく、すべての構成データがコピーされます。CSS は構成データを Controller 上の Microsoft SQL Server Express LocalDB データベースにインポートします。このデータベースはローカルホストキャッシュデータベースと呼ばれます。CSS は、ローカルホストキャッシュデータベースの情報がサイトデータベースの情報と一致することを確認します。ローカルホストキャッシュデータベースは、同期が行われるたびに再作成されます。

  Microsoft SQL Server Express LocalDB (ローカルホストキャッシュデータベースで使用) は、Controller をインストールするときに自動的にインストールされます。(コマンドラインから Controller をインストールする際に、このインストールを禁止できます。) ローカルホストキャッシュデータベースは、複数の Controller 間で共有できません。ローカルホストキャッシュデータベースをバックアップする必要はありません。構成変更が検出されるたびに再作成されます。
- 前回のチェック以降に変更がない場合、データはコピーされません。

次の図は、プリンシパルブローカーがサイトデータベースとの接続を失った場合 (停止が開始された場合) の通信パスの変化を示しています。



停止中

停止が開始されると:

- セカンダリブローカーは接続要求のリッスンと処理を開始します。
- 停止が開始されると、セカンダリブローカーは最新の VDA 登録データを持っていませんが、VDA がセカンダリブローカーと通信すると、登録プロセスがトリガーされます。そのプロセス中に、セカンダリブローカーはその VDA に関する現在のセッション情報も取得します。
- セカンダリブローカーが接続を処理している間、ブローカリングプリンシパルは接続を監視し続けます。接続が復元されると、ブローカリングプリンシパルはセカンダリブローカーに接続情報のリッスンを停止するよう指示し、ブローカリングプリンシパルはブローカリング操作を再開します。次に VDA がブローカリングプリンシパルと通信するときに、登録プロセスがトリガーされます。セカンダリブローカーは、以前の停止からの残りの VDA 登録をすべて削除します。CSS は、展開で構成変更が発生したことを認識すると、情報の同期を再開します。

同期中に停止が開始されるという万が一の事態が発生した場合、現在のインポートは破棄され、最後に認識された構成が使用されます。

イベントログ には、同期と停止に関する情報が提供されます。

停止モードでの運用に時間制限はありません。

通常モードと停止モード間の移行は、既存のセッションには影響しません。新しいセッションの起動のみに影響します。

意図的に停止をトリガーすることもできます。その理由と方法の詳細については、Force an outageを参照してください。

複数のControllerがあるサイト

CSSは、他のタスクの中でも、ゾーン内のすべてのControllerに関する情報をセカンダリブローカーに定期的に提供します。(展開に複数のゾーンが含まれていない場合、このアクションはサイト内のすべてのControllerに影響します。)その情報を持つことで、各セカンダリブローカーは、ゾーン内の他のControllerで実行されているすべてのピアセカンダリブローカーについて認識します。

セカンダリブローカーは、別のチャネルで相互に通信します。これらのブローカーは、停止が発生した場合にゾーン内でブローカー操作を行うセカンダリブローカーを決定（選出）するために、実行されているマシンのFQDN名のアルファベット順リストを使用します。停止中、すべてのVDAは選出されたセカンダリブローカーに登録します。ゾーン内の選出されていないセカンダリブローカーは、受信接続およびVDA登録要求を積極的に拒否します。

停止中に選出されたセカンダリブローカーが失敗した場合、別のセカンダリブローカーが引き継ぐために選出され、VDAは新しく選出されたセカンダリブローカーに登録します。

停止中にControllerが再起動された場合：

- そのControllerが選出されたブローカーでない場合、再起動による影響はありません。
- そのControllerが選出されたブローカーである場合、別のControllerが選出され、VDAが登録されます。再起動されたControllerが起動すると、自動的にブローカー処理を引き継ぎ、VDAが再度登録されます。このシナリオでは、登録中にパフォーマンスが影響を受ける可能性があります。

通常の操作中にControllerの電源をオフにし、停止中に電源をオンにした場合、そのControllerがブローカーとして選出されても、そのControllerではローカルホストキャッシュを使用できません。

イベントログは、選出に関する情報を提供します。

停止中に利用できないもの、およびその他の違い

停止モードでの運用に時間制限はありません。ただし、Citrixは可能な限り迅速に接続を復元することを推奨しています。

停止中：

- Studioを使用できません。
- PowerShell SDKへのアクセスは制限されます。

    - まず、次の操作を行う必要があります。
        - 値が1のレジストリキー `EnableCssTestMode` を追加します: `New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer\LHC -Name EnableCssTestMode -PropertyType DWORD -Value 1`
        - ポート89を使用します: `Get-BrokerMachine -AdminAddress localhost:89 | Select MachineName, ControllerDNSName, DesktopGroupName, RegistrationState`
    - これらのコマンドを実行すると、以下にアクセスできます。
        - すべての `Get-Broker*` コマンドレット。

- ハイパーバイザーの資格情報はホストサービスから取得できません。すべてのマシンは不明な電源状態になり、電源操作は発行できません。ただし、電源がオンになっているホスト上のVMは、接続要求に使用できます。
- 割り当てられたマシンは、通常の操作中に割り当てが行われた場合にのみ使用できます。停止中は新しい割り当てを行うことはできません。
- リモートPCアクセス マシンの自動登録と構成はできません。ただし、通常の操作中に登録および構成されたマシンは使用できます。
- サーバーでホストされているアプリケーションおよびデスクトップのユーザーは、リソースが異なるゾーンにある場合、構成されているセッション制限よりも多くのセッションを使用する可能性があります。
- ユーザーは、現在アクティブ/選出されているセカンダリブローカーを含むゾーン内の登録済みVDAからのみアプリケーションとデスクトップを起動できます。停止中は、ゾーンをまたいだ起動（あるゾーンのセカンダリブローカーから別のゾーンのVDAへの起動）はサポートされません。
- デリバリーグループ内のVDAのスケジュールされた再起動が開始される前にサイトデータベースの停止が発生した場合、再起動は停止が終了したときに開始されます。これにより、予期しない結果が生じる可能性があります。詳しくは、「データベースの停止によりスケジュールされた再起動が遅延する」を参照してください。
- ゾーン優先度 は構成できません。構成されている場合でも、セッション起動時には優先度は考慮されません。
- タグがゾーンの指定に使用されるタグ制限 は、セッション起動ではサポートされません。このようなタグ制限が構成され、StoreFrontストアの高度なヘルスチェック オプションが有効になっている場合、セッションの起動が断続的に失敗する可能性があります。

アプリケーションとデスクトップのサポート

ローカルホストキャッシュは、サーバーでホストされるアプリケーションとデスクトップ、および静的（割り当て済み）デスクトップをサポートします。

ローカルホストキャッシュは、プールされたデリバリーグループ内のデスクトップVDAを次のようにサポートします。

- デフォルトでは、`ShutdownDesktopsAfterUse` プロパティが有効になっているプールされたデリバリーグループ（MCSまたはCitrix Provisioning™によって作成されたもの）の電源管理されたデスクトップVDAは、ローカルホストキャッシュイベント中に新しい接続では利用できません。このデフォルトを変更して、ローカルホストキャッシュ中にこれらのデスクトップを使用できるようにすることができます。

  ただし、障害発生中に電源管理に依存することはできません。（電源管理は、通常の操作が再開された後に再開されます。）また、これらのデスクトップは再起動されていないため、以前のユーザーのデータが含まれている可能性があります。
- デフォルトの動作を上書きするには、サイト全体で、および影響を受ける各デリバリーグループで有効にする必要があります。次のPowerShellコマンドレットを実行します。

  サイト全体：

  ```
  Set-BrokerSite -ReuseMachinesWithoutShutdownInOutageAllowed $true
  ```

  影響を受ける各デリバリーグループに対して、次のPowerShellコマンドを実行します。

  ```
  Set-BrokerDesktopGroup -Name "name" -ReuseMachinesWithoutShutdownInOutage $true
  ```

デリバリーグループ設定をデフォルトで有効にするには、次のPowerShellコマンドを実行します。

```
Set-BrokerSite -DefaultReuseMachinesWithoutShutdownInOutage $true
```

この設定は、この設定を有効にした後に作成されるすべての新しいデリバリーグループに適用されます。

既存のデリバリーグループでこの設定を有効にするには、次のPowerShellコマンドを実行します。

```
Set-BrokerDesktopGroup -Name "name" -ReuseMachinesWithoutShutdownInOutage $true
```

サイトおよびデリバリーグループでこの機能を有効にしても、通常の操作中に構成された `ShutdownDesktopsAfterUse` プロパティがどのように機能するかには影響しません。この機能が有効になっている場合、LHCイベントが完了してもVDAは自動的に再起動しません。プールされたデリバリーグループ内の電源管理されたデスクトップVDAは、VDAが再起動されるまで以前のセッションのデータを保持できます。これは、ユーザーが非LHC操作中にVDAからログオフした場合、または再起動が手動でトリガーされた場合に発生する可能性があります。

> **重要:**
>
> サイトレベルでReuseMachinesWithoutShutdownInOutageAllowedを、デリバリーグループレベルでReuseMachinesWithoutShutdownInOutageを有効にしないと、ローカルホストキャッシュイベント中に、プールされたデリバリーグループ内の電源管理されたデスクトップVDAへのすべてのセッション起動試行が失敗します。

RAM サイズに関する考慮事項

LocalDBサービスは、約1.2 GBのRAM（データベースキャッシュに最大1 GB、SQL Server Express LocalDBの実行に200 MB）を使用できます。障害が長期間続き、多くのログオンが発生する場合（たとえば、10,000ユーザーで12時間）、セカンダリブローカーは最大1 GBのRAMを使用できます。これらのメモリ要件は、コントローラーの通常のRAM要件に追加されるため、合計RAM容量を増やす必要がある場合があります。

サイトデータベースにSQL Server Expressインストールを使用している場合、サーバーには2つのsqlserver.exeプロセスがあります。

CPU コアとソケット構成に関する考慮事項

コントローラーのCPU構成、特にSQL Server Express LocalDBで利用可能なコア数は、メモリ割り当てよりもさらに、ローカルホストキャッシュのパフォーマンスに直接影響します。このCPUオーバーヘッドは、データベースに到達できず、セカンダリブローカーがアクティブな障害期間中にのみ観測されます。

LocalDBは複数のコア（最大4つ）を使用できますが、単一のソケットに制限されています。ソケットを追加してもパフォーマンスは向上しません（たとえば、1コアずつ4つのソケットがある場合）。代わりに、Citrixは複数のコアを持つ複数のソケットを使用することを推奨しています。Citrixのテストでは、2x3（2ソケット、3コア）構成は4x1および6x1構成よりも優れたパフォーマンスを提供しました。

ストレージに関する考慮事項

障害中にユーザーがリソースにアクセスすると、LocalDBは増大します。たとえば、1秒あたり10ログオンで実行されるログオン/ログオフテスト中に、データベースは2〜3分ごとに1 MB増加しました。通常の操作が再開されると、ローカルデータベースが再作成され、スペースが返されます。ただし、障害中のデータベースの増大を許容するために、LocalDBがインストールされているドライブに十分なスペースが利用可能である必要があります。ローカルホストキャッシュは、障害中により多くのI/Oも発生させます。約3 MB/秒の書き込みと、数十万回の読み取りです。

パフォーマンスに関する考慮事項

障害発生時には、1つのセカンダリブローカーがすべての接続を処理するため、通常の操作中に複数のコントローラー間で負荷分散を行うサイト（またはゾーン）では、選出されたセカンダリブローカーが障害発生時に通常よりもはるかに多くの要求を処理する必要がある場合があります。したがって、CPUの要求は高くなります。サイト（ゾーン）内のすべてのセカンダリブローカーは、ローカルホストキャッシュデータベースと影響を受けるすべてのVDAによって課される追加の負荷を処理できる必要があります。これは、障害発生時に選出されるセカンダリブローカーが変更される可能性があるためです。

VDIの制限:

- シングルゾーンVDI展開では、障害発生時に最大10,000台のVDAを効果的に処理できます。
- マルチゾーンVDI展開では、停止中に各ゾーンで最大10,000のVDA、サイト全体で最大40,000のVDAを効果的に処理できます。例えば、以下の各サイトは停止中に効果的に処理できます。
    - 4つのゾーンを持ち、各ゾーンに10,000のVDAを含むサイト。
    - 7つのゾーンを持ち、1つは10,000のVDAを含み、残りの6つはそれぞれ5,000のVDAを含むサイト。

停止中、サイト内の負荷管理が影響を受ける可能性があります。負荷評価器（特にセッション数ルール）が超過する可能性があります。

すべてのVDAがセカンダリブローカーに登録するのにかかる間、そのサービスは現在のセッションに関する完全な情報を持っていない可能性があります。そのため、その期間中のユーザー接続要求は、既存のセッションへの再接続が可能であったとしても、新しいセッションが起動される結果となる可能性があります。この期間（「新しい」セカンダリブローカーが再登録中にすべてのVDAからセッション情報を取得する間）は避けられません。停止が開始されたときに接続されているセッションは移行期間中に影響を受けませんが、新しいセッションやセッションの再接続は影響を受ける可能性があります。

この期間は、VDAが登録する必要がある場合に発生します。

- 停止が開始されたとき: プリンシパルブローカーからセカンダリブローカーに移行するとき。
- 停止中のセカンダリブローカーの障害: 障害が発生したセカンダリブローカーから新しく選出されたセカンダリブローカーに移行するとき。
- 停止からの復旧: 通常の操作が再開され、プリンシパルブローカーが制御を再開するとき。

Citrix Broker Protocolの`HeartbeatPeriodMs`レジストリ値（デフォルト = 600000 ms、つまり10分）を下げることで、間隔を短縮できます。このハートビート値は、VDAがpingに使用する間隔の2倍であるため、デフォルト値では5分ごとにpingが実行されます。

例えば、次のコマンドはハートビートを5分（300000ミリ秒）に変更し、2.5分ごとにpingが実行されるようにします。

```
New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer -Name HeartbeatPeriodMs -PropertyType DWORD –Value 300000
```

ハートビート値を変更する際は注意してください。頻度を上げると、通常モードと停止モードの両方でControllerへの負荷が増大します。

VDAがどれだけ迅速に登録されても、この間隔を完全に排除することはできません。

セカンダリブローカー間の同期にかかる時間は、オブジェクト（VDA、アプリケーション、グループなど）の数が増えるにつれて長くなります。例えば、5000のVDAを同期するには10分以上かかる場合があります。

XenApp 6.xリリースとの違い

このローカルホストキャッシュの実装は、XenApp 6.xおよびそれ以前のXenAppリリースにおけるローカルホストキャッシュ機能と同じ名前を共有していますが、大幅な改善が施されています。この実装は、より堅牢で破損の影響を受けません。定期的な`dsmaint`コマンドの必要性を排除するなど、メンテナンス要件が最小限に抑えられています。このローカルホストキャッシュは、技術的には全く異なる実装です。

ローカルホストキャッシュの管理

ローカルホストキャッシュが正しく機能するには、各ControllerのPowerShell実行ポリシーをRemoteSigned、Unrestricted、またはBypassに設定する必要があります。

SQL Server エクスプレス ローカルDB

ローカルホストキャッシュが使用するMicrosoft SQL Server Express LocalDBソフトウェアは、Controllerをインストールするか、バージョン7.9より前のControllerをアップグレードする際に自動的にインストールされます。このデータベースと通信するのはセカンダリブローカーのみです。

PowerShellコマンドレットを使用して、このデータベースに関する何かを変更することはできません。LocalDBは複数のController間で共有できません。

SQL Server Express LocalDBデータベースソフトウェアは、ローカルホストキャッシュが有効になっているかどうかにかかわらずインストールされます。

そのインストールを防ぐには、`XenDesktopServerSetup.exe`コマンドを使用してControllerをインストールまたはアップグレードし、`/exclude "Local Host Cache Storage (LocalDB)"`オプションを含めます。ただし、ローカルホストキャッシュ機能はデータベースなしでは機能せず、セカンダリブローカーで別のデータベースを使用することはできないことに注意してください。

このLocalDBデータベースのインストールは、サイトデータベースとして使用するためにSQL Server Expressをインストールするかどうかには影響しません。

以前のSQL Server Express LocalDBバージョンを新しいバージョンに置き換える方法については、「Replace SQL Server Express LocalDB」を参照してください。

製品のインストールとアップグレード後のデフォルト設定

Citrix Virtual Apps and Desktopsの新規インストール時（最小バージョン7.16）には、ローカルホストキャッシュが有効になります。

アップグレード後（バージョン7.16以降）は、展開全体で10,000未満のVDAがある場合、ローカルホストキャッシュが有効になります。

ローカルホストキャッシュの有効化と無効化

- ローカルホストキャッシュを有効にするには、次のように入力します。

  ```
  Set-BrokerSite -LocalHostCacheEnabled $true
  ```

  ローカルホストキャッシュが有効になっているかどうかを確認するには、`Get-BrokerSite`と入力します。`LocalHostCacheEnabled`プロパティが`True`であることを確認します。
- ローカルホストキャッシュを無効にするには、次のように入力します。

  ```
  Set-BrokerSite -LocalHostCacheEnabled $false
  ```

注意: XenAppおよびXenDesktop 7.16以降、接続リース（バージョン7.6からローカルホストキャッシュに先行していた機能）は製品から削除され、利用できなくなりました。

ローカルホストキャッシュが機能していることを確認する

ローカルホストキャッシュが正しく設定され、機能していることを確認するには：

- 同期インポートが正常に完了していることを確認します。イベントログを確認してください。
- 各Delivery ControllerにSQL Server Express LocalDBデータベースが作成されていることを確認します。これにより、必要に応じてセカンダリブローカーが引き継ぐことができることが確認されます。
  - Delivery Controllerサーバーで、`C:\Windows\ServiceProfiles\NetworkService`を参照します。
  - `HaDatabaseName.mdf`と`HaDatabaseName_log.ldf`が作成されていることを確認します。
- Delivery Controllerで障害を強制的に発生させます。ローカルホストキャッシュが機能することを確認したら、すべてのControllerを通常モードに戻すことを忘れないでください。これには約15分かかる場合があります。

イベントログ

イベントログは、同期と障害が発生した時期を示します。イベントビューアログでは、障害モードは*HA モード*と呼ばれます*。

構成同期サービス:

通常の操作中、CSSがローカルホストキャッシュブローカーを使用して構成データをローカルホストキャッシュデータベースにインポートする際に、次のイベントが発生する可能性があります。

- 503: Citrix Config Sync Serviceが更新された構成を受信しました。このイベントは、同期プロセスの開始を示します。
- 504: Citrix Config Sync Serviceが更新された構成をインポートしました。構成のインポートが正常に完了しました。
- 505: Citrix Config Sync Serviceがインポートに失敗しました。構成のインポートは正常に完了しませんでした。以前に正常な構成が利用可能な場合、障害発生時にそれが使用されます。ただし、それは現在の構成から古くなっています。以前の構成が利用できない場合、サービスは障害発生時にセッションブローカーに参加できません。この場合、トラブルシューティングセクションを参照し、Citrixサポートに連絡してください。
- 507: システムが障害モードであり、ローカルホストキャッシュブローカーがブローカー処理に使用されているため、Citrix Config Sync Serviceがインポートを中止しました。サービスは新しい構成を受信しましたが、障害が発生したためインポートは中止されました。これは予期される動作です。
- 510: プライマリ構成サービスから構成サービス構成データが受信されませんでした。

- 517: プライマリブローカーとの通信中に問題が発生しました。
- 518: セカンダリブローカー（高可用性サービス）が実行されていないため、構成同期スクリプトが中止されました。

高可用性サービス:

このサービスは、ローカルホストキャッシュブローカーとも呼ばれます。

- 3502: 停止が発生し、ローカルホストキャッシュブローカーがブローカー操作を実行しています。
- 3503: 停止が解決され、通常の操作が再開されました。
- 3504: どのローカルホストキャッシュブローカーが選出されたか、および選出に関与した他のローカルホストキャッシュブローカーを示します。
- 3507: 2分ごとにローカルホストキャッシュのステータス更新を提供し、選出されたブローカーでローカルホストキャッシュモードがアクティブであることを示します。停止期間、VDA登録、セッション情報を含む停止の概要が含まれます。
- 3508: 選出されたブローカーでローカルホストキャッシュがアクティブでなくなり、通常の操作が復元されたことを通知します。停止期間、ローカルホストキャッシュイベント中に登録されたマシンの数、LHCイベント中の正常な起動の数を含む停止の概要が含まれます。
- 3509: 選出されていないブローカーでローカルホストキャッシュがアクティブであることを通知します。2分ごとの停止期間が含まれ、選出されたブローカーを示します。
- 3510: 選出されていないブローカーでローカルホストキャッシュがアクティブでなくなったことを通知します。停止期間が含まれ、選出されたブローカーを示します。

停止を強制する

意図的に停止を強制したい場合があります。

- ネットワークが繰り返しダウンする場合。ネットワークの問題が解決されるまで停止を強制すると、通常モードと停止モード間の継続的な移行（およびその結果として頻繁に発生するVDA登録ストーム）を防ぐことができます。
- ディザスタリカバリ計画をテストするため。
- ローカルホストキャッシュが正しく機能していることを確認するため。
- サイトデータベースサーバーの交換または保守中。

停止を強制するには、Delivery Controller を含む各サーバーのレジストリを編集します。`HKLM\Software\Citrix\DesktopServer\LHC` で、`OutageModeForced` を `REG_DWORD` として `1` に作成して設定します。この設定により、データベースの状態に関係なく、ローカルホスト

キャッシュブローカーは停止モードに入ります。値を`0`に設定すると、ローカルホストキャッシュブローカーは停止モードを終了します。

イベントを確認するには、`C:\ProgramData\Citrix\WorkspaceCloud\Logs\Plugins\HighAvailabilityService`にある`Current_HighAvailabilityService`ログファイルを監視します。

トラブルシューティング

ローカルホストキャッシュデータベースへの同期インポートが失敗し、505イベントが投稿された場合、いくつかのトラブルシューティングツールが利用可能です。

CDFトレース: `ConfigSyncServer`および`BrokerLHC`モジュールのオプションが含まれています。これらのオプションは、他のブローカーモジュールとともに、問題を特定するのに役立つでしょう。

レポート: 同期インポートが失敗した場合、レポートを生成できます。このレポートは、エラーの原因となっているオブジェクトで停止します。このレポート機能は同期速度に影響するため、Citrixは使用しないときは無効にすることを推奨します。

CSSトレースレポートを有効にして生成するには、次のコマンドを入力します。

```
New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer\LHC -Name EnableCssTraceMode -PropertyType DWORD -Value 1
```

HTMLレポートは`C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\CitrixBrokerConfigSyncReport.htm`に投稿されます。

レポートが生成されたら、レポート機能を無効にするには次のコマンドを入力します。

```
Set-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer\LHC -Name EnableCssTraceMode -Value 0
```

ブローカー構成のエクスポート: デバッグ目的で正確な構成を提供します。

```
Export-BrokerConfiguration | Out-File <file-pathname>
```

例: `Export-BrokerConfiguration | Out-File C:\\BrokerConfig.xml`。

ローカルホストキャッシュのPowerShellコマンド

PowerShellコマンドを使用して、Delivery Controllerでローカルホストキャッシュ（LHC）を管理できます。

PowerShellモジュールは、Delivery Controllerの次の場所にあります。

```
C:\Program Files\Citrix\Broker\Service\ControlScripts
```

> **重要:**
>
> このモジュールはDelivery Controllerでのみ実行してください。

PowerShell モジュールのインポート

モジュールをインポートするには、Delivery Controllerで次を実行します。

```
cd C:\Program Files\Citrix\Broker\Service\ControlScripts Import-Module .\HighAvailabilityServiceControl.psm1
```

LHC を管理するための PowerShell コマンド

以下のコマンドは、Delivery Controller で LHC モードをアクティブ化および管理するのに役立ちます。

コマンドレット	機能
`Enable-LhcForcedOutageMode`	ブローカーを LHC モードにします。`Enable-LhcForcedOutageMode` が適切に機能するには、ConfigSync Service によって LHC データベースファイルが正常に作成されている必要があります。この cmdlet は、実行された Delivery Controller 上でのみ LHC を強制します。LHC をアクティブにするには、このコマンドをゾーン内のすべての Delivery Controller で実行する必要があります。
`Disable-LhcForcedOutageMode`	ブローカーを LHC モードから解除します。この cmdlet は、実行された Delivery Controller 上でのみ LHC モードを無効にします。`Disable-LhcForcedOutageMode` は、ゾーン内のすべての Delivery Controller で実行する必要があります。

コマンドレット	機能
`Set-LhcConfigSyncIntervalOverride`	Citrix Config Synchronizer Service (CSS) がサイト内の構成変更をチェックする間隔を設定します。時間間隔は、60 秒 (1 分) から 3600 秒 (1 時間) の範囲で指定できます。この設定は、実行された Delivery Controller にのみ適用されます。Delivery Controller 間で一貫性を持たせるには、各 Delivery Controller でこの cmdlet を実行することを検討してください。例: `Set-LhcConfigSyncIntervalOverride -Seconds 1200`
`Clear-LhcConfigSyncIntervalOverride`	Citrix Config Synchronizer Service (CSS) がサイト内の構成変更をチェックする間隔を、デフォルト値の 300 秒 (5 分) に設定します。この設定は、実行された Delivery Controller にのみ適用されます。Delivery Controller 間で一貫性を持たせるには、各 Delivery Controller でこの cmdlet を実行することを検討してください。
`Enable-LhcHighAvailabilitySDK`	実行された Delivery Controller 内のすべての `Get-Broker*` cmdlet へのアクセスを有効にします。
`Disable-LhcHighAvailabilitySDK`	実行された Delivery Controller 内の Broker cmdlet へのアクセスを無効にします。

注：

- Delivery Controller で `Get-Broker*` cmdlet を実行するときは、ポート 89 を使用します。例:
  - `Get-BrokerMachine -AdminAddress localhost:89`
- LHC モードでない場合、Delivery Controller 上の LHC Broker は構成情報のみを保持します。

- LHC モード中、選出された Delivery Controller 上の LHC Broker は次の情報を保持します。
  - リソースの状態
  - セッションの詳細
  - VDA登録
  - 構成情報

「検索」を使用してマシンとセッションを監視および管理する

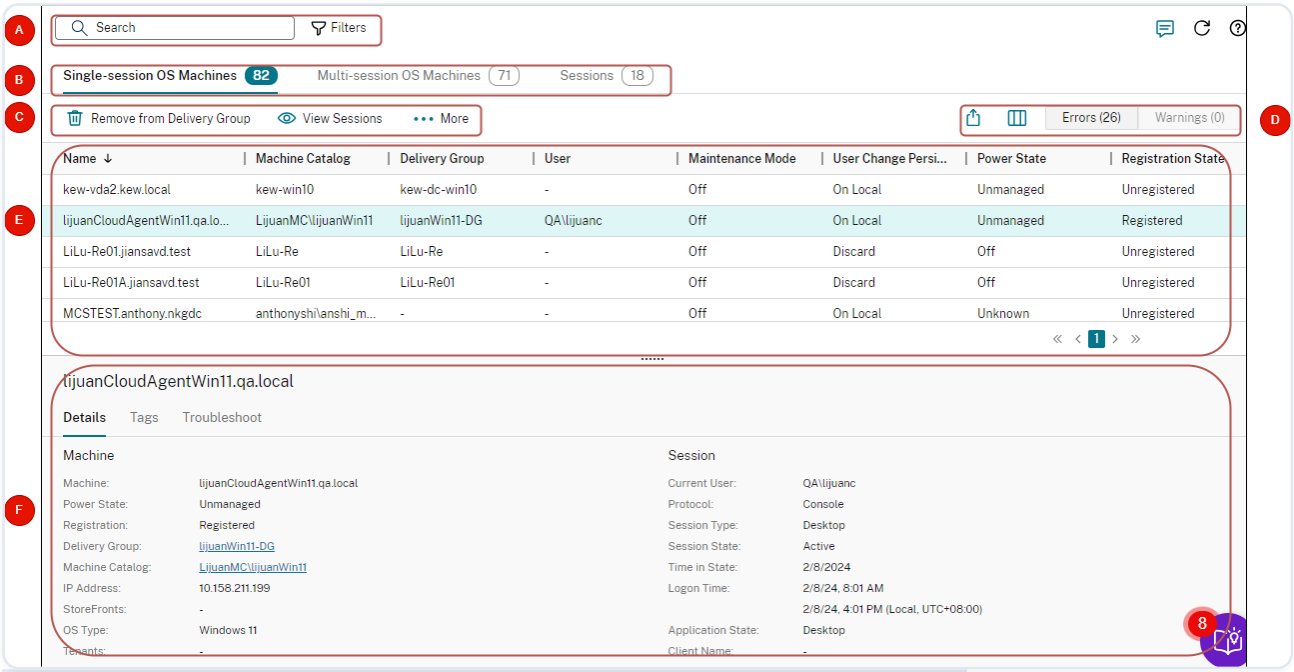
注：

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

この記事では、Web Studioの**検索**ノードを使用してマシンとセッションを監視および管理する方法について説明します。

ノードについて

検索ノードは、マシンとユーザーセッションを監視および管理するための一元的な場所を提供します。



コールアウト	エリア	説明
A	検索バー	複雑な検索条件を定義できるクイック検索とフィルターベースの検索を提供します。詳細については、「インスタンスの検索」を参照してください。
B	タイプタブ	マシンをタイプ別に一覧表示したり、すべてのセッションを一覧表示したりするためのタブを表示します。インスタンス数はタブ名に表示されます。
C	インスタンスレベルのアクション	*選択したインスタンス*（マシンまたはセッション）に対して実行できるアクションを表示します。詳細については、マシンアクションおよびセッション

コールアウト	エリア	説明
		アクションを参照してください。
D	リストレベルのアクション	現在の*リスト*に対して実行できるアクションを表示します。 • **エクスポート**アイコン: メインビューに表示されているインスタンスのリストをCSVファイルにエクスポートします。 • 「**表示する列**」アイコン: リストのメインビューをカスタマイズします。 • **エラー**ラベル: このラベルを有効にすると、メインビューにエラーのある未登録のマシンのみが表示されます。問題の詳細を表示するには、**詳細**ペインの**トラブルシューティング**タブに移動します。

コールアウト	エリア	説明
		• **警告**ラベル: このラベルを有効にすると、メインビューに警告のある未登録のマシンのみが表示されます。問題の詳細を表示するには、**詳細**ペインの**トラブルシューティング**タブに移動します。
E	メインビュー	インスタンスとそのプロパティを表示します。**表示する列**アイコンを選択して、メインビューをカスタマイズできます。利用可能な列の詳細については、マシン列およびセッション列を参照してください。
F	詳細ペイン	次の詳細が表示されます: • 選択したインスタンス（マシンまたはセッション）の詳細 • 選択したマシンに適用されているタグ

コールアウト	エリア	説明	
		• 選択したマシンに関するエラーまたは警告の詳細。問題、考えられる原因、推奨される解決策が含まれます。	

インスタンスの検索

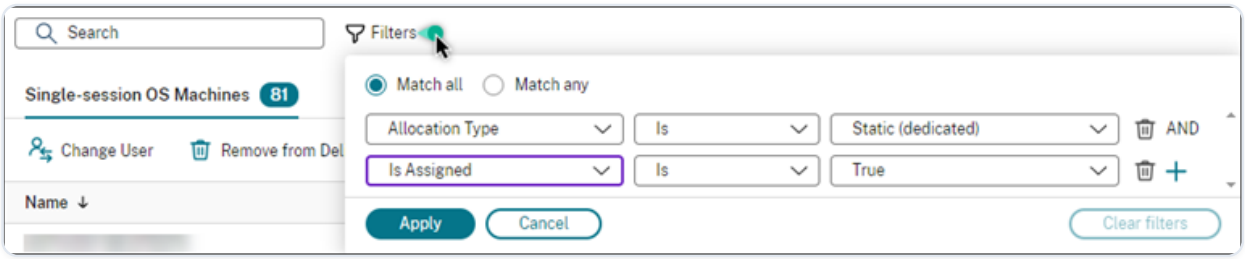
検索機能を使用して、特定のマシンとセッションを見つけます。

- フィルターを使用した検索
- クイック検索のために現在のフィルターセットを保存する
- 検索バーにフィルターフィールドを固定する
- クイック検索ボックスを使用して検索
- 検索を強化するためのヒント

フィルターを使用した検索

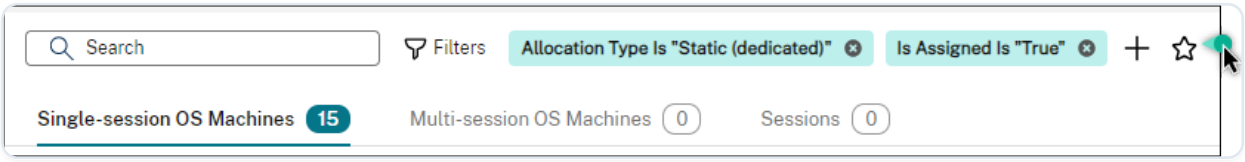
たとえば、*静的でユーザーに割り当てられている*すべてのシングルセッションOSマシンを見つけるには、次の手順に従います。

1. **シングルセッションOSマシン**タブで、**フィルター**アイコンをクリックします。フィルターパネルが表示されます。
2. 必要なフィルター条件を追加します。



3. すべてのフィルター条件に一致する結果を検索で返す場合は、**すべて一致**（AND演算子）を選択します。いずれかのフィルター条件に一致する結果を検索で返す場合は、**いずれか一致**（OR演算子）を選択します。
4. **適用**をクリックします。

フィルターされたリストには、静的でユーザーに割り当てられているすべてのシングルセッションOSマシンが表示されます。



クイック検索のために現在のフィルターセットを保存する

たとえば、静的でユーザーに割り当てられているシングルセッションOSマシンのフィルターセットを将来使用するために保存するには、次の手順に従います。

1. フィルターベースの検索を実行した後、前の図に示すように、検索バーの**星**アイコンをクリックします。
2. 表示されるページで、このフィルターセットの名前を入力します（例：*静的および割り当て済みマシン*）。
3. 「**保存**」をクリックします。

   検索ボックスをクリックすると、保存されたフィルターセットが検索履歴リストに表示されます。

   検索フィルターセット(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/search-filter-set.png)

> **注：**
>
> フィルターセットはユーザーアカウントごとに保存されます。保存されたフィルターセットを管理するには、**管理**を選択します。

検索バーにフィルターフィールドをピン留めする

頻繁に使用するフィルター*フィールド*を検索バーにピン留めすると、簡単にアクセスできます。たとえば、フィルターベースの検索を実行した後、**割り当てタイプ**を検索バーにピン留めしたいとします。次の手順に従います。

1. 検索バーの*フィルター設定*をクリックします。
2. 表示されるパネルで、検索バーにフィルターフィールド（この例では*割り当てタイプ*）をピン留めするには、**ピン**アイコンをクリックします。 検索フィルターのピン(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/search-filter-pin.png)

クイック検索ボックスを使用して検索する

クイック検索ボックスを使用すると、名前関連のプロパティまたは保存されたフィルターセットに基づいてインスタンスを検索する便利な方法が提供されます。詳細な手順は次のとおりです。

1. 検索ボックスをクリックします。最近の検索と保存されたフィルターセットがドロップダウンリストに表示されます。以前の検索またはフィルターセットをクリックして、クイック検索を実行できます。
2. 新しい検索を開始するには、次のオプションから完全または部分的な名前を入力します。

    - マシン名またはDNS名
    - マシンカタログ名
    - デリバリーグループ名
    - セッションユーザー名
    - セッションクライアント名
    - セッションをホストしているVMのフレンドリ名（ハイパーバイザーで使用されるもの）
    - ホストサーバー名

検索を強化するためのヒント

検索機能を使用する際は、以下のヒントを考慮してください。

- **検索**ノードで、任意の列を選択して項目を並べ替えます。
- 検索および並べ替えが可能な表示に含める特性を増やすには、**表示する列**を選択するか、任意の列をクリックして**表示する列**を選択します。**表示する列**ウィンドウで、表示したい項目の横にあるチェックボックスをオンにし、**保存**を選択して終了します。

    > **注：**
    >
    > パフォーマンスを低下させる列には、**パフォーマンスを低下させる**というラベルが付けられています。

- マシンに接続されているユーザーデバイスを見つけるには、**クライアント (IP)** と **Is** を使用し、デバイスのIPアドレスを入力します。
- アクティブなセッションを見つけるには、**セッション状態**、**Is**、および **接続済み** を使用します。

- 配信グループ内のすべてのマシンを一覧表示するには、左ペインで**配信グループ**を選択します。グループを選択し、アクションバーまたはコンテキストメニューから**マシンの表示**を選択します。

並べ替え操作を実行する際は、以下の点を考慮してください。

- 項目の数が5,000を超えない限り、任意の列をクリックして項目を並べ替えることができます。数が5,000を超えると、名前または現在のユーザー（現在表示しているタブによる）でのみ並べ替えることができます。並べ替えを有効にするには、フィルターを使用して項目の数を5,000以下に減らしてください。
- アイテム数が500より多く、5,000以下の場合:
  - ソートパフォーマンスを向上させるため、すべてのデータをローカルにキャッシュします。**シングルセッションOSマシン**タブと**マルチセッションOSマシン**タブでは、ソートのために列（**名前**列を除く任意の列）を初めてクリックしたときにデータをキャッシュします。**セッション**タブでは、ソートのために列（**現在のユーザー**列を除く任意の列）を初めてクリックしたときにデータをキャッシュします。その結果、ソートの完了に時間がかかります。パフォーマンスを向上させるには、名前または現在のユーザーでソートするか、フィルターを使用してアイテム数を減らしてください。
  - テーブルの下に表示される次のメッセージは、データがキャッシュされていることを示します: 最終更新: `<the time when you refreshed the table>`。この場合、ソート操作は以前にロードされたアイテムに基づいています。これらのアイテムは最新ではない可能性があります。最新の状態にするには、更新アイコンをクリックしてください。

表示する列をカスタマイズする

日々の運用に不可欠なプロパティとステータスを表示するパーソナライズされたメインビューを作成します。詳細な手順は次のとおりです。

1. **検索**ノードで、必要に応じて**マルチセッションOSマシン**、**シングルセッションOSマシン**、または**セッション**タブを選択します。
2. アクションバーの**表示する列**アイコンをクリックし、列を選択します。

   利用可能な列とその説明の詳細については、マシン列およびセッション列を参照してください。

列を選択する際、**パフォーマンスを低下させる**というラベルが付いた列が表示されることがあります。これらの列を選択すると、コンソールのパフォーマンスが低下する可能性があります。以下の考慮事項に留意してください:

- カスタマイズが完了すると、選択した列を表示するためにテーブルが更新されます。これらの列が存在すると、テーブルの更新時に遅延が発生する可能性があります。
- ブラウザを更新するか、コンソールからサインアウトして再度サインインすると、それらの列を保持するかどうかを尋ねるメッセージが表示されます。保持することを選択した場合、最適なコンソールパフォーマンスのために、テーブルの更新は1分間に1回までに制限されます。より頻繁に更新するには、パフォーマンスを低下させる列をすべて削除してください。

マシンとセッションの管理

検索ノードのアクションを使用して、マシンとセッションの問題をトラブルシューティングしたり、ユーザー要求を処理したりします。

知っておくとよいこと

マシンはさまざまなレベルで管理できます:

- 個々のマシンレベルで。**検索**ノードを使用して、ターゲットマシンを特定し、アクションを実行します。
- マシンカタログレベルで、カタログのマスターイメージの変更、カタログからのマシンの削除、カタログへのマシンの追加などを行います。詳細については、「マシンカタログの管理」を参照してください。
- デリバリーグループレベルで、グループ内のマシンのメンテナンスモードのオン/オフを切り替えるなどを行います。詳細については、「デリバリーグループの管理」を参照してください。

個々のセッションレベルに加えて、デリバリーグループレベルでセッションを管理することもできます。たとえば、デリバリーグループのセッションの事前起動と残存を構成できます。詳細については、「デリバリーグループの管理」を参照してください。

マシンまたはセッションでアクションを実行する

個々のインスタンスレベルでマシンまたはセッションを管理するには、次の手順に従います。

1. **検索**ノードで、**マルチセッションOSマシン**、**シングルセッションOSマシン**、または**セッション**タブを選択します。
2. 必要に応じて、1つ以上のインスタンスを選択します。
3. アクションバーまたは右クリックメニューから、それらのインスタンスで発生した問題やユーザー要求に基づいてアクションを選択します。

   利用可能なアクションとその説明の詳細については、「マシンアクション」および「セッションアクション」を参照してください。

> **注：**
>
> 2つ以上のインスタンスを選択した場合、それらすべてに適用されるアクションのみが利用可能です。

マシンまたはセッションデータをCSVファイルにエクスポートする

タブに表示されているインスタンス（マシンまたはセッション）のリスト（最大30,000項目）をCSVファイルにエクスポートします。詳細な手順は次のとおりです。

1. **検索**ノードで、必要に応じて**マルチセッションOSマシン**、**シングルセッションOSマシン**、または**セッション**タブを選択します。
2. 右上隅にある「**エクスポート**」アイコンをクリックします。
3. 表示されるダイアログボックスで、「**続行**」をクリックします。

   エクスポートが完了するまでに数分かかる場合があります。ファイルはブラウザのデフォルトのダウンロードフォルダにあります。

> **注：**
>
> **検索**ノードの各タブでは、エクスポートの実行中に別のエクスポートを実行することはできません。

マシンのアクションと列

この記事では、参照用にマシンのアクションと列を説明とともに一覧表示します。

アクション

マシンで実行できるアクションとその説明を表示します。

アクション	説明	適用対象
デリバリーグループから削除	デリバリーグループからマシンを削除します。	シングルセッションおよびマルチセッション
デリバリーグループに追加	マシンをデリバリーグループに追加します。	シングルセッションおよびマルチセッション

アクション	説明	適用対象
セッションの表示	マシンで実行中のセッションを表示します	シングルセッションおよびマルチセッション
タグの管理	マシンにタグを追加して管理します。タグの一般的な使用例について詳しくは、「タグ」を参照してください。	シングルセッションおよびマルチセッション
メンテナンスモードをオンにする	パッチを適用する前、またはトラブルシューティングのために、マシンをメンテナンスモードにします。 このモードでは、そのマシンへの新しい接続が防止されます。ユーザーはそのマシン上の既存のセッションに接続できますが、そのマシン上で新しいセッションを開始することはできません。	シングルセッションおよびマルチセッション
メンテナンスモードをオフにする	マシンのメンテナンスモードをオフにします。	シングルセッションおよびマルチセッション
VDAのアップグレード	マシンのVDAをアップグレードします。	特定の要件を満たすシングルセッションまたはマルチセッションOSマシン: 詳細はこちら。
ログオフ	マシンを強制的にログオフする	シングルセッションおよびマルチセッション
削除	マシンカタログからVMを削除しますが、ハイパーバイザーまたはクラウドサービス上ではそのまま残します。	シングルセッションおよびマルチセッション
ユーザーの変更	特定のユーザーにマシンを割り当てます。	シングルセッションの*静的*マシン。

アクション	説明	適用対象
起動	マシンを起動します。	シングルセッションおよびマルチセッション
シャットダウン	マシンをシャットダウンします。	シングルセッションおよびマルチセッション
再起動	マシンを再起動します	シングルセッションおよびマルチセッション
サスペンド	マシンを休止状態または中断状態にします。マシンを中断すると、Delivery Controllerはマシンのメモリ内容をファイルに保存し、マシンをシャットダウンします。	シングルセッションOSマシン
再開	中断されたマシンを再開します。中断されたマシンを再開すると、Delivery Controllerはマシンを起動し、以前の状態に復元します。	シングルセッションOSマシン
強制再起動	マシンを強制的に再起動します。	シングルセッションOSマシン
強制シャットダウン	マシンを強制的にシャットダウンします。	シングルセッションOSマシン

列

タイプ別にすべてのマシン列とその説明を表示します。

- マシン
- マシンの詳細
- アプリケーション
- ホスティング
- 接続
- 登録
- セッションの詳細

- セッション

マシン

マシンカテゴリの列。

列	説明	適用対象
名前	マシンのDNSホスト名。	シングルセッションおよびマルチセッション
マシンカタログ	マシンが属するカタログの名前。	シングルセッションおよびマルチセッション
デリバリーグループ	マシンが属するデリバリーグループの名前。	シングルセッションおよびマルチセッション
ユーザー表示名	マシンに関連付けられているユーザーのフルネーム（通常は `Firstname Lastname` の形式）。関連付けられているユーザーとは、共有マシンの現在のユーザーと、専用マシンに割り当てられているユーザーのことです。	シングルセッションおよびマルチセッション
ユーザー	マシンに関連付けられているユーザーのユーザー名（「domain\user」の形式）。関連付けられているユーザーとは、共有マシンの現在のユーザーと、専用マシンに割り当てられているユーザーのことです。	シングルセッションおよびマルチセッション

列	説明	適用対象
ユーザープリンシパル名	マシンに関連付けられているユーザーのユーザープリンシパル名（「user@domain」の形式）。関連付けられているユーザーとは、共有マシンの現在のユーザーと、専用マシンに割り当てられているユーザーのことです。	シングルセッションおよびマルチセッション
デスクトップ表示名	セッションの起動に元々使用されたマシンの公開名。Citrix Workspace™ アプリまたはStoreFrontに表示される名前です。 **注：**デスクトップの表示を変更するには、**マシンの更新を実行**権限が必要です。表示名の変更にはマシンプロパティの更新が含まれるためです。	シングルセッションのみ
デスクトップの状態	マシンに対する未解決のデスクトップ状態のリスト。可能な値：Unknown、CPU、ICALatency、およびUPMLogonTime。	シングルセッションおよびマルチセッション
割り当ての種類	マシンの割り当ての種類：ユーザーに永続的に割り当てられ	シングルセッションおよびマルチセッション

列	説明	適用対象
	る場合は**永続**。ランダムに割り当てられる場合は**ランダム**。	
メンテナンスモード	マシンがメンテナンスモードであるかどうかを示します。	シングルセッションおよびマルチセッション
Windows接続設定	Windowsによって報告されるログオンモード。	マルチセッションのみ
	指定可能な値: LogonEnabled、Draining、DrainingUntilRestart、および LogonDisabled。	
割り当て済み	専用デスクトップがユーザーまたはクライアント (名前/アドレス) に割り当てられているかどうかを示します。ユーザーは明示的に割り当てることも、マシンの初回使用時に割り当てることもできます。	シングルセッションおよびマルチセッション
物理マシン	マシンが物理マシンであるかどうかを示します。`True` はマシンが物理マシンであることを示し、Delivery Controller によって電源管理されていないことを意味します。`False`	シングルセッションおよびマルチセッション

列	説明	適用対象	
	はそうでないことを示します。		
プロビジョニングの種類	マシンがどのようにプロビジョニングされたか。指定可能な値 • 手動: PVSまたはMCSを使用してプロビジョニングされていません。 • PVS: PVSを使用してプロビジョニング済み (物理マシン、ブレードマシン、仮想マシン) • MCS: MCSを使用してプロビジョニング済み (VMのみ)	シングルセッションおよびマルチセッション	
スケジュールされた再起動	マシンに対してスケジュールされた再起動操作の状態。指定可能な値 • なし: 再起動はスケジュールされていません。 • 保留中: 再起動を待機中です	シングルセッションおよびマルチセッション	

列	説明	適用対象	
	が、使用可能です。 • ドレイン中: 再起動を待機しており、新しいセッションには利用できません。ただし、既存の接続への再接続は引き続き許可されます。 • 進行中: スケジュールされた再起動がアクティブに進行中です。 • 自然: 自然な再起動が進行中です。マシンは再起動を待機しています。		
ゾーン	マシンが配置されているゾーンの名前。	シングルセッションおよびマルチセッション	
状態	マシンに関連付けられているデスクトップの全体的な状態。これは、セッション状態、登録状態、電源状態など、さまざまな特定の状態から派生しています。	シングルセッションおよびマルチセッション	

列	説明	適用対象
	可能な状態: オフ、未登録、利用可能、切断済み、使用中、準備中。	
タグ	マシンに関連付けられているタグのリスト。	シングルセッションおよびマルチセッション
VDAアップグレード	VDAパッケージのアップグレードアクションのマシン状態。	シングルセッションおよびマルチセッション
	指定可能な値: MissingUpgradeType、UpgradeScheduled、UpgradeAvailable、UpToDate、および Unknown。	
サスペンド可能	マシンが電源操作(サスペンドと再開)をサポートしているかどうかを示します。	シングルセッションおよびマルチセッション
ロードインデックス	現在のロードインデックス。詳細については、詳細はこちらを参照してください。	マルチセッションのみ
ドレイン状態	マシンがドレイン中であり、マシン上のすべてのセッションが終了した後にシャットダウンするかどうかを示しま	マルチセッションのみ

列	説明	適用対象
	す。True は、電源管理されたマルチセッションマシンでのみ表示されます。	
	注: マシンがメンテナンスモードの場合、シャットダウンしません。メンテナンスモードを解除した後にのみシャットダウンします。	

マシンの詳細

マシンの詳細カテゴリの列。

列	説明	適用対象
エージェントバージョン	マシンにインストールされているCitrix Virtual Delivery Agent (VDA) のバージョン。	シングルセッションおよびマルチセッション
IPアドレス	マシンのIPアドレスです。	シングルセッションおよびマルチセッション
割り当て済み	専用デスクトップがユーザーまたはクライアント（名前/アドレス）に割り当てられているかどうかを示します。ユーザーは明示的に割り当てることも、マシンの初回使用時に割り当てることもできます。	シングルセッションおよびマルチセッション
OSの種類	マシンで実行されているオペレーティングシステムの種類です。	シングルセッションのみ

アプリケーション

アプリケーションカテゴリの列。

列	説明	適用対象
使用中のアプリケーション	マシンで使用中のアプリケーションのリスト（ブラウザ名として表示されます）。	シングルセッションおよびマルチセッション
公開アプリケーション	マシンによって公開されたアプリケーションのリスト（ブラウザ名として表示されます）。	シングルセッションおよびマルチセッション

接続

接続カテゴリの列。

列	説明	適用対象
クライアント (IP)	マシンに接続されているクライアントのIPアドレス。	シングルセッションのみ
クライアント	マシンに接続されているクライアントのホスト名。	シングルセッションのみ
プラグインバージョン	接続されているクライアント上のCitrix Workspaceアプリのバージョン。	シングルセッションのみ
接続元	受信接続のホスト名。通常、ゲートウェイ、ルーター、またはクライアントです。	シングルセッションのみ
接続元 (IP)	受信接続のIPアドレス。通常、ゲートウェイ、ルーター、またはクライアントです。	シングルセッションのみ
接続タイプ	セッションに使用されるプロトコル。可能な値：HDX、RDP、およびConsole。注：XenDesktop® 5 VDA上のコンソールセッションの場合、このフィールドは空白になります。	シングルセッションのみ

列	説明	適用対象
最終接続時刻 (UTC)	失敗または成功した、最後に検出された接続試行の時刻。	シングルセッションおよびマルチセッション
最終接続ユーザー	最後にマシンへの接続を試行したユーザーのSAM名（「DOMAIN\user」の形式）。SAM名が利用できない場合は、SIDが使用されます。	シングルセッションおよびマルチセッション
Secure ICA® アクティブ	現在のセッションでSecureICAがアクティブであるかどうかを示します。マルチセッションマシンでは常にnullです。	シングルセッションおよびマルチセッション

ホスティング

ホスティングカテゴリの列。

列	説明	適用対象
VM	セッションを実行しているホストされたマシンの、ハイパーバイザーによって使用されるフレンドリ名。マシンのDNS名またはAD名のいずれとも一致するとは限りません。	シングルセッションおよびマルチセッション
ホスティングサーバー名	管理対象の場合、マシンをホストしているハイパーバイザーのDNS名。	シングルセッションおよびマルチセッション
接続	セッションをホストしているマシンに割り当てられているホスト接続の名前。	シングルセッションおよびマルチセッション

列	説明	適用対象
保留中の更新	ホストされているマシンのVMイメージが古くなっており、次回の再起動時に新しいイメージに更新される必要があるかどうかを示します。	シングルセッションおよびマルチセッション
ユーザー変更の永続性	ユーザーの変更がどのように処理されるかを示し、変更が永続的であるかどうかを示します: • OnLocal: 永続的。ユーザーの変更はローカルに保存されます。 • 破棄: 非永続的。ユーザーの変更は破棄されます。	シングルセッションおよびマルチセッション
保留中の電源操作	マシンに対して保留中の電源操作があるかどうかを示します。	シングルセッションおよびマルチセッション
電源状態	マシンの電源状態。設定可能な値: 管理対象外、不明、利用不可、オフ、オン、サスペンド、起動中、シャットダウン中、サスペンド中、再開中。	シングルセッションおよびマルチセッション

列	説明	適用対象
使用後にシャットダウンされます	電源管理されたシングルセッションマシンにのみ適用されます。マシンが汚染されており、すべてのセッションが終了した後にシャットダウンされるかどうかを示します。	シングルセッションのみ
	注: マシンがメンテナンスモードの場合、シャットダウンされません。メンテナンスモードから解除された後にのみシャットダウンされます。	

登録

登録カテゴリの列。

列	説明	適用対象
最終登録失敗	ブローカーへのマシンの最終登録解除の理由。	シングルセッションおよびマルチセッション
	可能な値は、AgentShutdown、AgentSuspended、AgentRequested、IncompatibleVersion、AgentAddressResolutionFailed、AgentNotContactable、AgentWrongActiveDirectoryOU、	

列	説明	適用対象
	EmptyRegistrationRequest、MissingRegistrationCapabilities、MissingAgentVersion、InconsistentRegistrationCapabilities、NotLicensedForFeature、UnsupportedCredentialSecurityVersion、InvalidRegistrationRequest、SingleMultiSessionMismatch、FunctionalLevelTooLowForCatalog、FunctionalLevelTooLowForDesktopGroup、PowerOff、DesktopRestart、DesktopRemoved、AgentRejectedSettingsUpdate、SendSettingsFailure、SessionAuditFailure、SessionPrepareFailure、ContactLost、SettingsCreationFailure、UnknownError、およびBrokerRegistrationLimitReachedです。	
最終登録失敗時刻 (UTC)	マシンの最終登録解除時刻。	シングルセッションおよびマルチセッション

列	説明	適用対象
登録状態	マシンの登録状態。可能な値：Unregistered、Initializing、Registered、およびAgentError。	シングルセッションおよびマルチセッション
障害状態	マシンの現在の障害状態の概要。可能な値： • なし: 障害なし。マシンは正常です。 • FailedToStart: マシンの最後の電源投入操作が失敗しました。 • StuckOnBoot: 電源投入後、マシンが起動に失敗しました。	シングルセッションおよびマルチセッション
	未登録。マシンが予期された期間内に登録に失敗したか、その登録が拒否されました。	
	最大容量。マシンが最大容量に達していると報告しています。	

セッションの詳細

セッションの詳細カテゴリの列。

列	説明	適用対象
起動元	現在のブローカーセッションの起動に使用されたStoreFrontサーバーのホスト名。マルチセッションマシンでは常にnullです。	シングルセッションおよびマルチセッション
起動元 (IP)	現在のブローカーセッションの起動に使用されたStoreFrontサーバーのIPアドレス。マルチセッションマシンでは常にnullです。	シングルセッションおよびマルチセッション
セッション変更時刻 (UTC)	現在のセッションの最後の状態変更時刻。	シングルセッションのみ
SmartAccessフィルター	現在のセッションのSmart Accessタグ。マルチセッションマシンでは常にヌルです。	シングルセッションおよびマルチセッション

セッション

セッションカテゴリの列。

列	説明	適用対象
セッションの状態	現在のセッションの状態。可能な値: Other、PreparingSession、Connected、Active、Disconnected、Reconnecting、NonBrokeredSession、Unknown。	シングルセッションのみ
現在のユーザー	現在のセッションのユーザー名（「DOMAIN\user」の形式）。	シングルセッションのみ
開始時刻 (UTC)	現在のセッションの開始時刻。	シングルセッションのみ

列	説明	適用対象
セッション数	マシン上のセッション数。	マルチセッションのみ

セッションのアクションと列

この記事では、参照用にマシンのアクションと列を説明とともに一覧表示します。

アクション

セッションで実行できるアクションとその説明を表示します。

アクション	説明	適用対象セッション
ログオフ	セッションからユーザーをログオフします。	シングルセッションOSマシンまたはマルチセッションOSマシン
メッセージを送信	セッションのユーザーにメッセージを送信します。	シングルセッションOSマシンまたはマルチセッションOSマシン
マシンの表示	セッションのホストマシンを表示します。	シングルセッションOSマシンまたはマルチセッションOSマシン
切断	セッションを切断します。セッションが切断されても、セッションはアクティブなままでアプリケーションは実行され続けますが、ユーザーデバイスはDelivery Controllerと通信しなくなります。	シングルセッションOSマシンまたはマルチセッションOSマシン
マシンのシャットダウン	セッションに関連付けられているマシンをシャットダウンします。	シングルセッションOSマシン
マシンの再起動	セッションに関連付けられているマシンを再起動します。	シングルセッションOSマシン

列

セッションの列とその説明を表示します。

列	説明
現在のユーザー	ユーザーの名前。ユーザーのユーザープリンシパル名 (UPN)。
名前	セッションをホストしているマシンのDNSホスト名。
デリバリーグループ	セッションをホストしているマシンを含むデリバリーグループの名前。
マシンカタログ	セッションをホストしているマシンを含むマシンカタログの名前。
エージェントバージョン	セッションをホストしているマシンにインストールされているCitrix Virtual Delivery Agent (VDA) のバージョン。
使用中のアプリケーション	セッションで使用されているアプリケーションのリスト。管理名で識別されます。
自律的に仲介済み	これは、仲介されずに直接接続によって確立されたHDX™セッションであるかどうか。
仲介時間 (UTC)	セッションが仲介された時刻。
仲介ユーザー名	ブローカーユーザーの名前。
クライアント (IP)	セッションに接続されているクライアントのIPアドレス。
クライアント	セッションに接続されているクライアントのホスト名。
プラグインバージョン	セッションに接続されているクライアントで実行されてい

列	説明
	るCitrix Workspace™アプリのバージョン。
接続元	受信接続のホスト名。通常はゲートウェイ、ルーター、またはクライアントです。
接続元 (IP)	受信接続のIPアドレス。通常、ゲートウェイ、ルーター、またはクライアントです。
割り当ての種類	セッションが共有か専用か。
非表示	セッションがユーザーから非表示になっていて、再接続できないかどうか。
VM	セッションをホストしているVMの、ハイパーバイザーで使用されているフレンドリ名。マシンのDNS名またはAD名のいずれとも一致するとは限りません。
ホスティングサーバー名	セッションのホストマシンをホストしているハイパーバイザーのDNS名。
接続	セッションをホストしているマシンに割り当てられているホスト接続の名前。
保留中の更新	ホストされているマシンのVMイメージが古く、次回の再起動時に新しいイメージに更新される予定であるかどうか。

列	説明
メンテナンスモード	セッションをホストしているマシンがメンテナンスモードであるかどうか。
IPアドレス	セッションをホストしているマシンのIPアドレス。
物理マシン	セッションをホストしているマシンが物理マシンであるかどうか。`True` は、マシンが物理マシンであり、Delivery Controllerによって電源管理されていないことを示します。`False` はその逆を示します。
起動元	セッションの起動に使用されたStoreFront™サーバーのホスト名。セッションがWorkspace経由で起動された場合は空白です。
起動元 (IP)	セッションの起動に使用されたStoreFrontサーバーのIPアドレス。セッションがWorkspace経由で起動された場合は空白。
OSの種類	セッションをホストしているオペレーティングシステムの識別文字列。
ユーザー変更の永続性	ユーザーの変更がどのように処理されるかを示し、変更が永続的であるかどうかを示します:

列	説明
	• OnLocal: 永続的。ユーザーの変更はローカルに保存されます。 • 破棄: 非永続的。ユーザーの変更は破棄されます。
接続タイプ	セッションに使用されるプロトコル（HDX、RDP、Consoleなど）。 **注:** XenDesktop® 5 VDA上のコンソールセッションの場合、このフィールドは空白です。
プロビジョニングの種類	セッションをホストしているマシンがどのようにプロビジョニングされたか • 手動: PVSまたはMCSを使用してプロビジョニングされていません。 • PVS: PVSによってプロビジョニングされたもの（物理マシン、ブレードマシン、仮想マシン）。 • MCS: MCSによってプロビジョニングされたもの（VMのみ）。
Secure ICA® アクティブ	セッションでSecureICAがアクティブであるかどうか。
セッションの状態	セッションの状態。可能な値: Connected、Active、Disconnected。L7より前の機

列	説明
	能レベルのマシン上のセッションでは、PreparingSession、Reconnecting、NonBrokeredSession、Other、Unknownなどの他の状態が発生する場合があります。
セッション変更時刻	セッションの最新の状態変更時刻。
アプリケーションの状態	セッション内のアプリケーションの状態。可能な値: PreLogon、PreLaunched、Active、Desktop、Lingering、NoApps。
セッションサポート	セッションをホストしているマシンが複数セッションをサポートするか、単一セッションをサポートするか。
ゾーン	セッションをホストしているマシンが配置されているゾーンの名前。
SmartAccessフィルター	セッションのSmart Accessタグ。
開始時刻 (UTC)	セッションが開始された日時。
状態	マシンの概要状態。可能な値: Unregistered、Disconnected、またはInUse。
状態時間 (UTC)	セッションが現在の状態になってからの時間。

列	説明
デリバリーコントローラー™	セッションのホストマシンが登録されているコントローラーのDNSホスト名。
ユーザー表示名	ユーザーのフルネーム。
デスクトップ表示名	セッションの起動に元々使用されたマシンの公開名。Citrix WorkspaceアプリまたはStoreFrontに表示される名前です。アプリケーションセッションの場合、そのアプリケーションが終了していても、セッションに起動された最初のアプリケーションの名前です。リソースが後で名前変更または削除されても、名前は変更されません。

セキュリティキーの管理

重要:

- この機能は、StoreFront™ 1912 LTSR CU2以降と組み合わせて使用する必要があります。
- Secure XML機能は、Citrix ADCおよびCitrix Gatewayリリース12.1以降でのみサポートされています。

注：

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

> この機能を使用すると、承認されたStoreFrontおよびCitrix Gatewayマシンのみがデリバリーコントローラーと通信できるようになります。この機能を有効にすると、キーを含まないすべての要求はブロックされます。この機能を使用して、内部ネットワークからの攻撃から保護するための追加のセキュリティ層を追加します。

この機能を使用するための一般的なワークフローは次のとおりです。

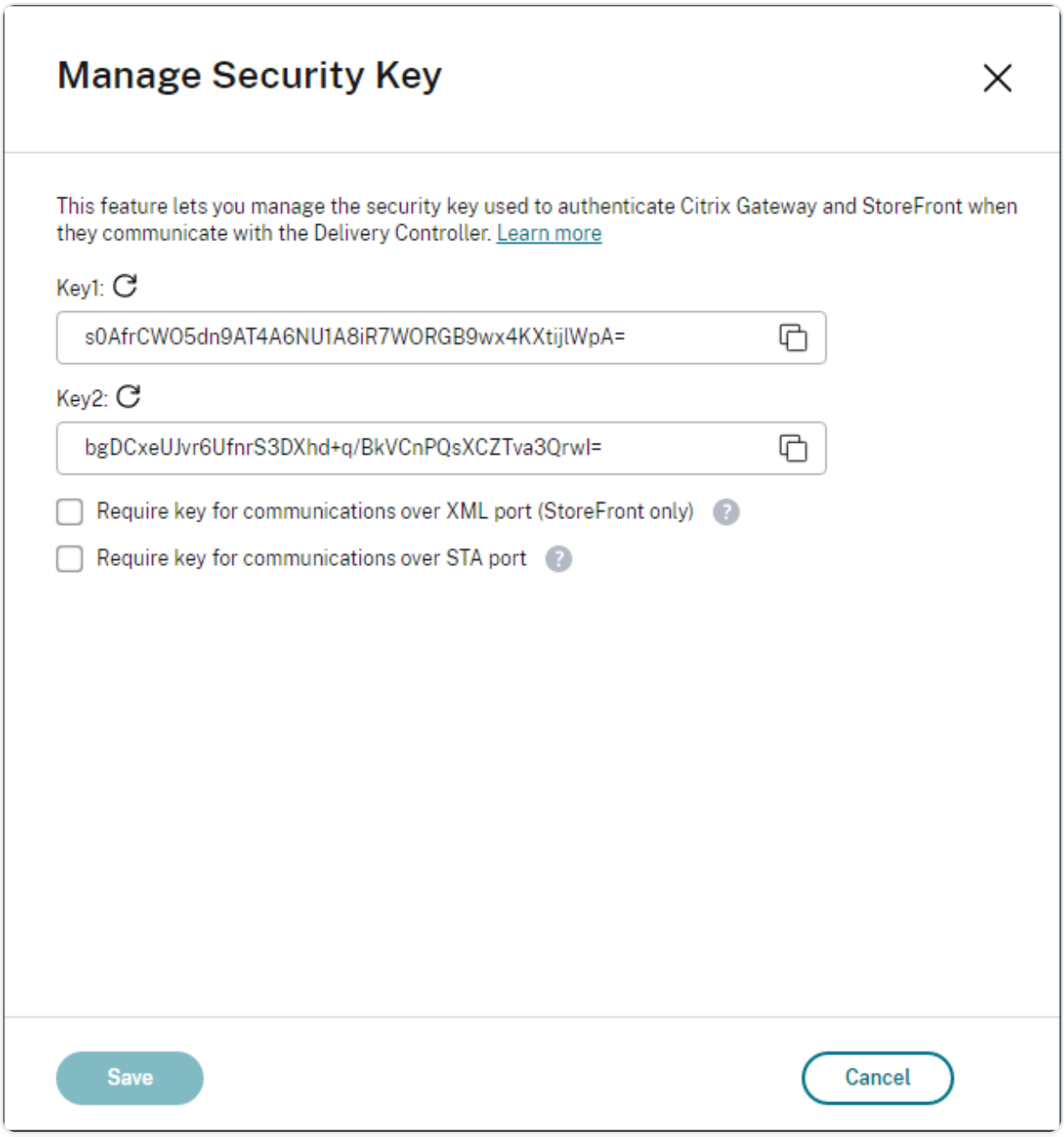
1. Web Studioを有効にして、機能設定を表示します。
2. サイトの設定を構成します。
3. StoreFrontの設定を構成します。
4. Citrix ADCの設定を構成します。

サイトの設定を構成する

Web StudioまたはPowerShellを使用して、サイトのセキュリティキー設定を構成できます。

Web Studioを使用する

1. Web Studioにサインインし、左ペインで を選択します。
2. **「セキュリティキーの管理」**タイルを見つけて**「編集」をクリックします。**「セキュリティキーの管理」**ページが表示されます。



3. 更新アイコンをクリックしてキーを生成します。

重要:

- 使用できるキーは2つあります。XMLポートおよびSTAポートを介した通信には、同じキーまたは異なるキーを使用できます。一度に1つのキーのみを使用することをお勧めします。未使用のキーは、キーローテーションにのみ使用されます。
- 使用中のキーを更新するために更新アイコンをクリックしないでください。クリックすると、サービスが中断されます。

4. 通信にキーが必要な場所を選択します。
   - **XMLポートを介した通信にキーを要求する（StoreFrontのみ）**。選択した場合、XMLポートを介した通信を認証するためにキーが必要になります。StoreFrontはこのポートを介してCitrix Cloudと通信します。XMLポートの変更については、Knowledge Centerの記事CTX127945を参照してください。
   - **STAポートを介した通信にキーを要求する**。選択した場合、STAポートを介した通信を認証するためにキーが必要になります。Citrix GatewayとStoreFrontはこのポートを介してCitrix Cloudと通信します。STAポートの変更については、Knowledge Centerの記事CTX101988を参照してください。
5. **「保存」**をクリックして変更を適用し、ウィンドウを閉じます。

PowerShell を使用する

以下は、Web Studioの操作に相当するPowerShellの手順です。

1. Citrix Virtual Apps and Desktops Remote PowerShell SDK を実行します。
2. コマンドウィンドウで、次のコマンドを実行します。
   - `Add-PSSnapIn Citrix*`
3. キーを生成し、Key1を設定するには、次のコマンドを実行します。
   - `New-BrokerXmlServiceKey`
   - `Set-BrokerSite -XmlServiceKey1 <the key you generated>`
4. 以下のコマンドを実行してキーを生成し、Key2 をセットアップします。
   - `New-BrokerXmlServiceKey`
   - `Set-BrokerSite -XmlServiceKey2 <the key you generated>`
5. 通信の認証でキーの使用を有効にするには、以下のコマンドのいずれか、または両方を実行します。
   - XMLポート経由の通信を認証するには:
     - `Set-BrokerSite -RequireXmlServiceKeyForNFuse $true`
   - STAポート経由の通信を認証するには:
     - `Set-BrokerSite -RequireXmlServiceKeyForSta $true`

ガイダンスと構文については、PowerShellコマンドのヘルプを参照してください。

StoreFrontの設定を構成する

サイトの構成が完了したら、PowerShellを使用してStoreFrontの関連設定を構成する必要があります。

StoreFront サーバーで、以下の PowerShell コマンドを実行します。

XMLポートを介した通信用のキーを構成するには、コマンドを使用します。例:

```
$store = Get-STFStoreService -VirtualPath [Path to store]

$farm = Get-STFStoreFarm -StoreService $store -FarmName [Resource feed
name]

Set-STFStoreFarm -Farm $farm -XMLValidationEnabled $true
-XMLValidationSecret [secret]
```

次のパラメータに適切な値を入力します。

- `Path to store`
- `Resource feed name`
- `secret`

STAポート経由の通信用にキーを構成するには、`New-STFSecureTicketAuthority`および`Set-STFRoamingGateway`コマンドを使用します。例:

```
$gateway = Get-STFRoamingGateway -Name [Gateway name]

$sta1 = New-STFSecureTicketAuthority -StaUrl [STA1 URL]
-StaValidationEnabled $true -StaValidationSecret [secret]

$sta2 = New-STFSecureTicketAuthority -StaUrl [STA2 URL]
-StaValidationEnabled $true -StaValidationSecret [secret]

Set-STFRoamingGateway -Gateway $gateway -SecureTicketAuthorityObjs
$sta1,$sta2
```

次のパラメータに適切な値を入力します。

- `Gateway name`

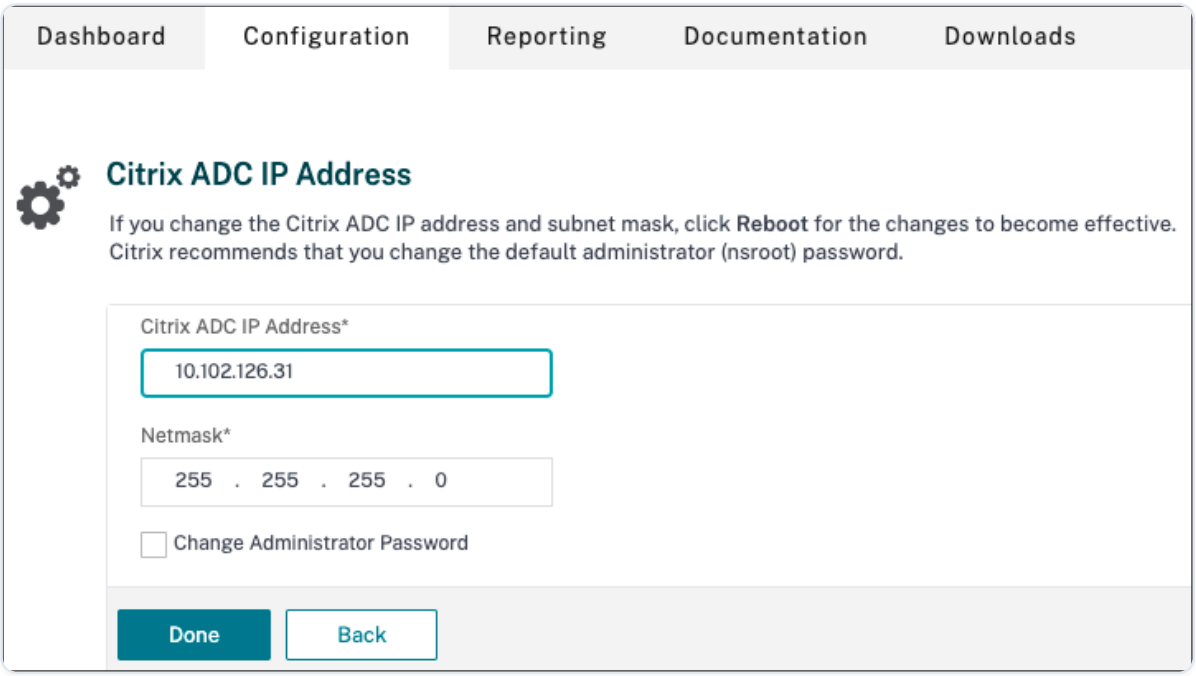
- `STA URL`
- `Secret`

ガイダンスと構文については、PowerShellコマンドのヘルプを参照してください。

Citrix ADCの設定を構成する

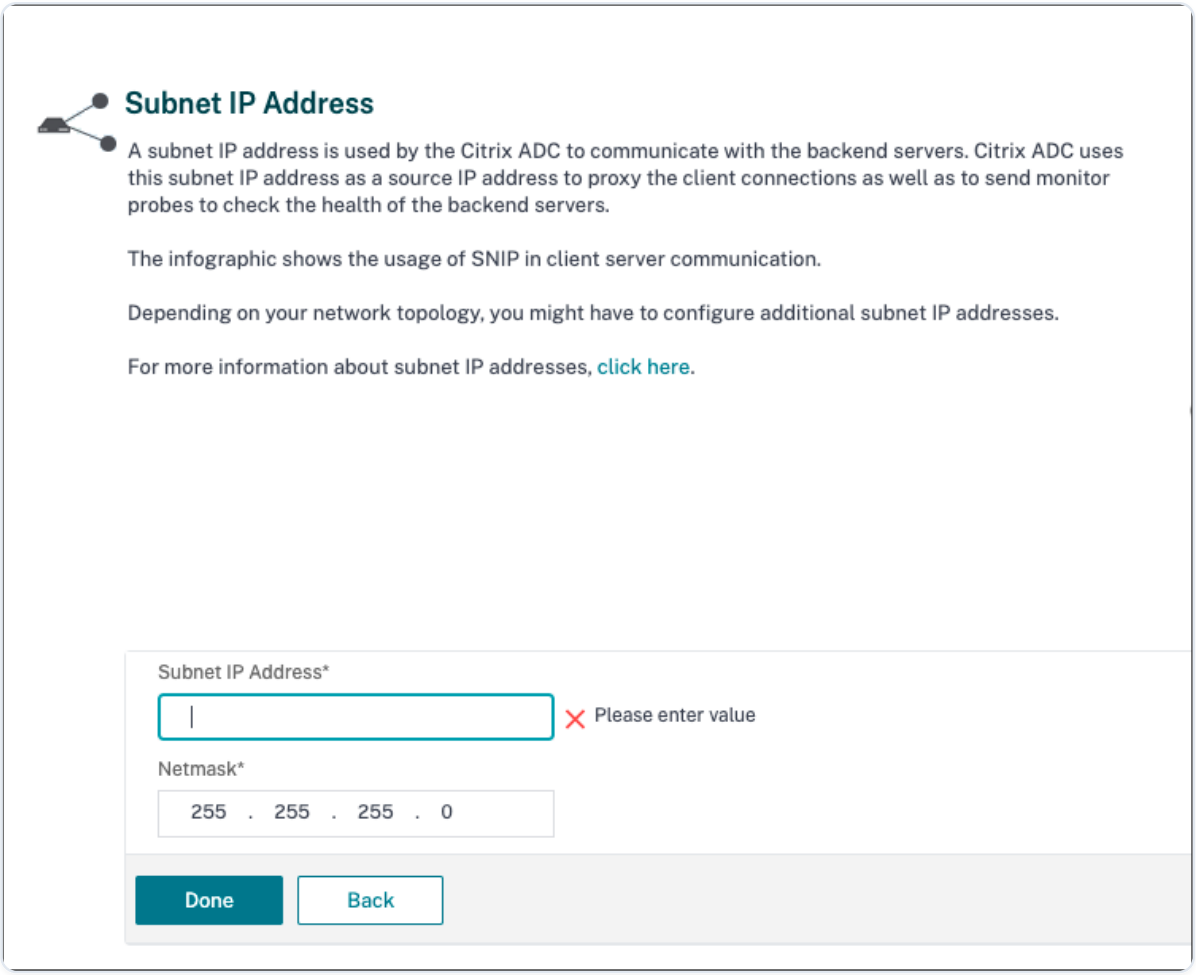
> **注：**
>
> Citrix ADCをゲートウェイとして使用しない限り、Citrix ADCのこの機能の構成は不要です。Citrix ADCを使用する場合は、次の手順に従います。

1. 次の前提条件となる構成がすでに設定されていることを確認してください。
   - 次のCitrix ADC関連のIPアドレスが構成されています。
     - Citrix ADCコンソールにアクセスするための Citrix ADC管理IP (NSIP) アドレス。詳細については、「NSIPアドレスの構成」を参照してください。

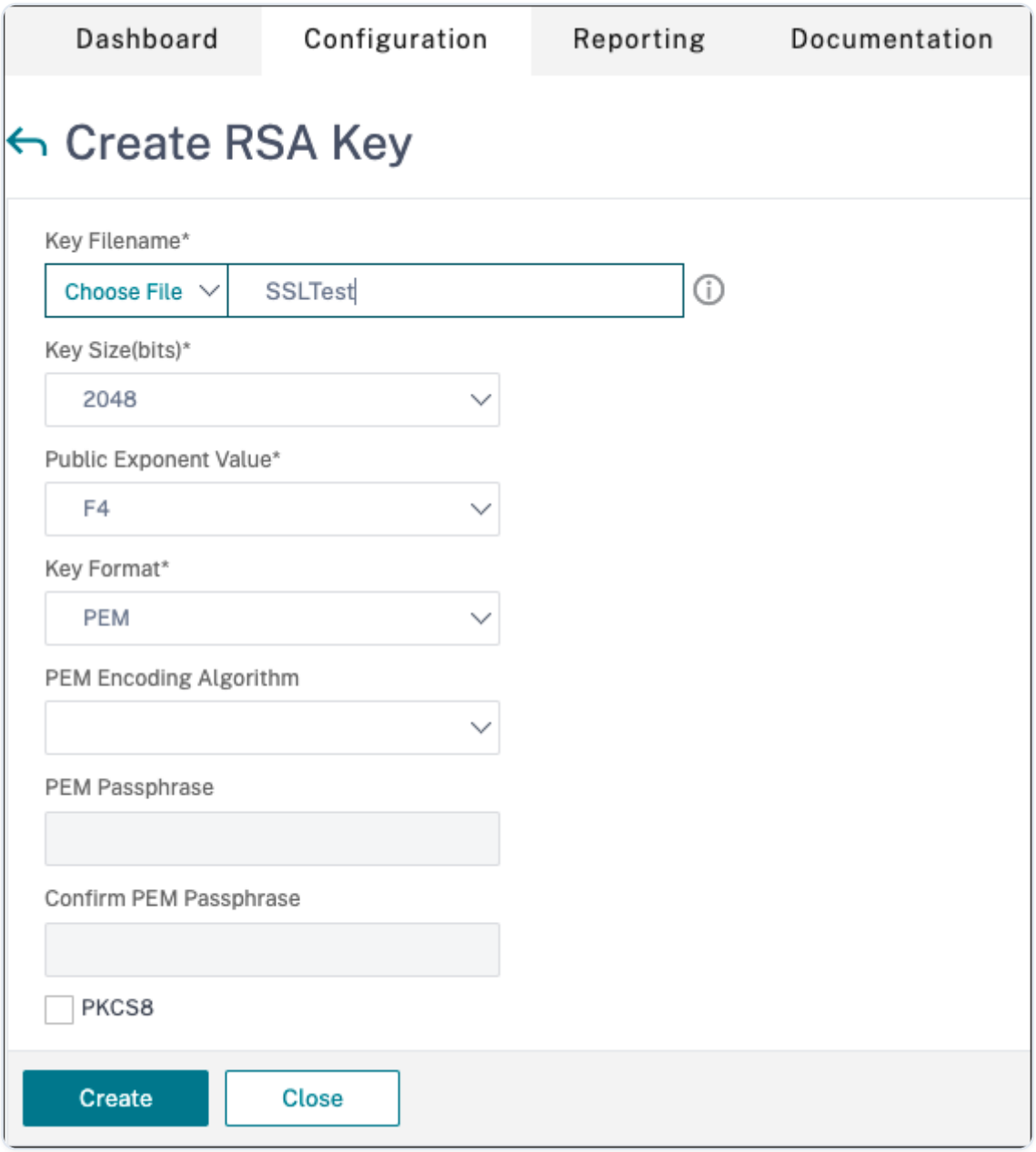


     - Citrix ADCアプライアンスとバックエンドサーバー間の通信を有効にするためのサブネットIP（SNIP）アドレス。詳細については、「サブネットIPアドレスの構成」を参照してください。

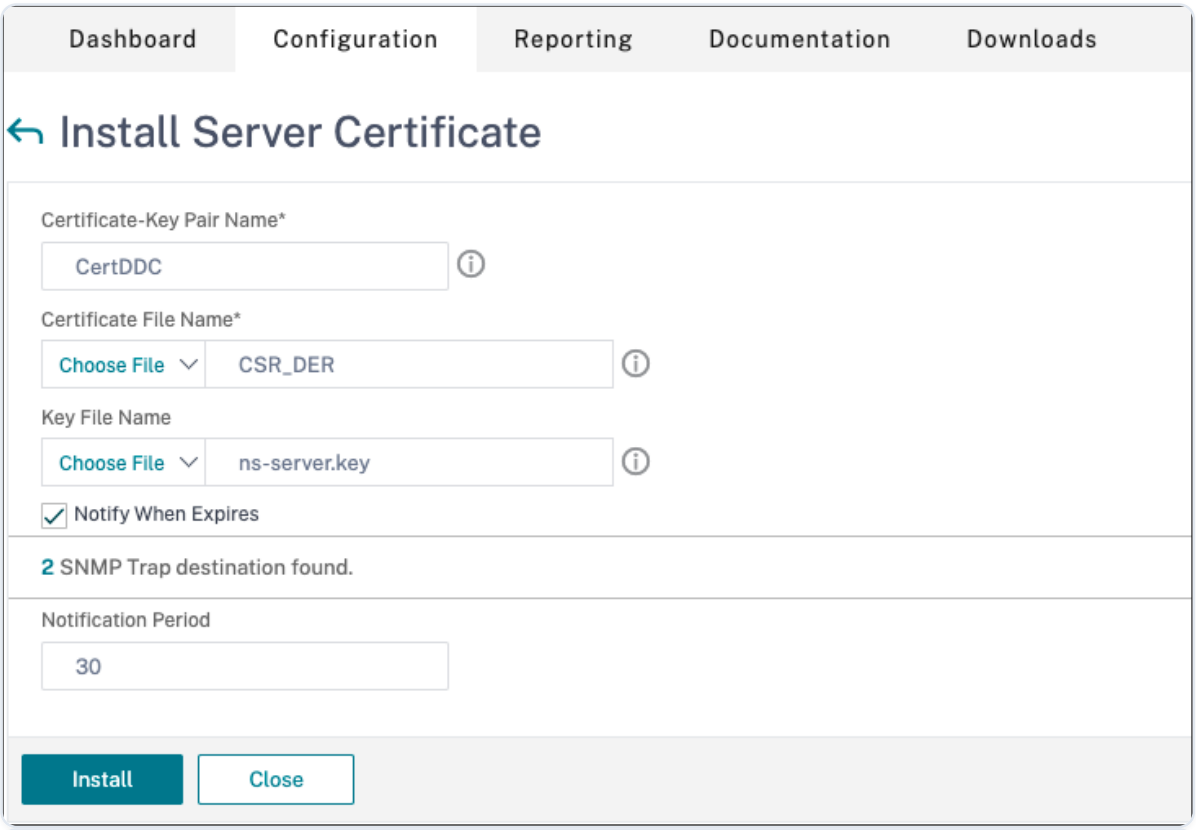
- セッション起動のためにADCアプライアンスにログインするためのCitrix Gateway仮想IPアドレスとロードバランサー仮想IPアドレス。詳細については、「仮想サーバーの作成」を参照してください。

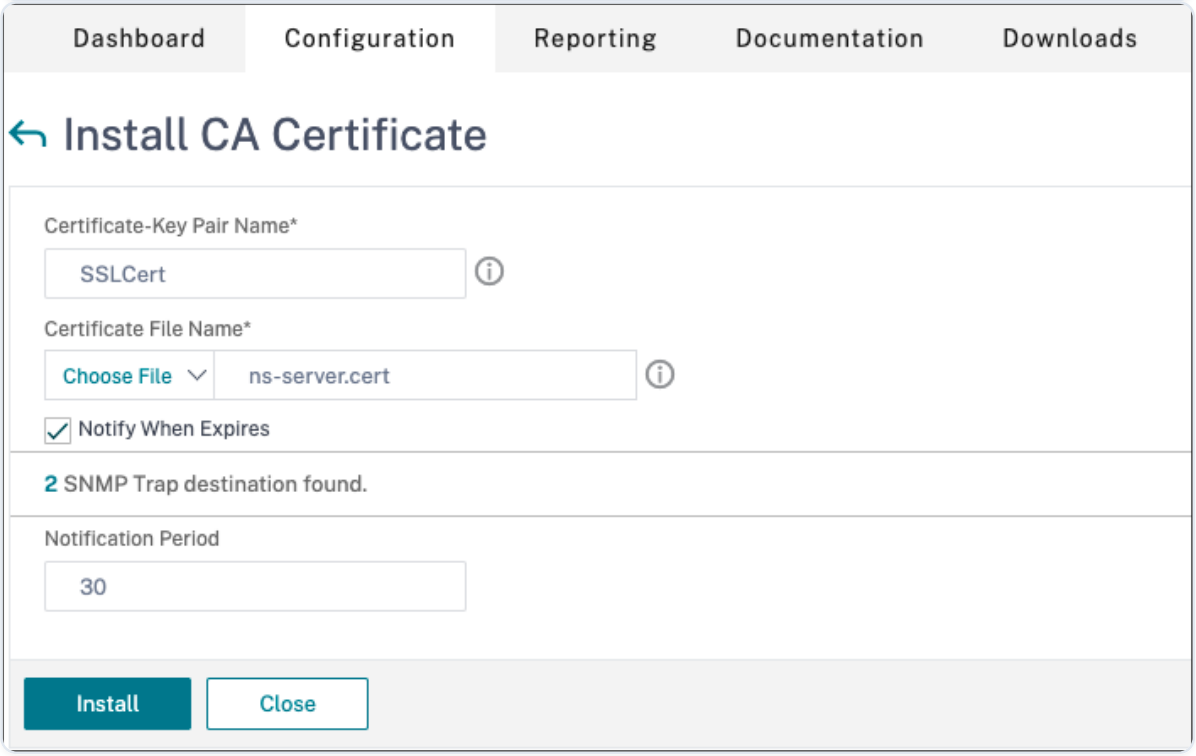


- Citrix ADCアプライアンスで必要なモードと機能が有効になっています。
  - モードを有効にするには、Citrix ADC GUIで **System > Settings > Configure Mode** に移動します。
  - 機能を有効にするには、Citrix ADC GUIで **System > Settings > Configure Basic Features** に移動します。
- 証明書関連の構成が完了しています。
  - 証明書署名要求（CSR）が作成されます。詳細については、「証明書の作成」を参照してください。

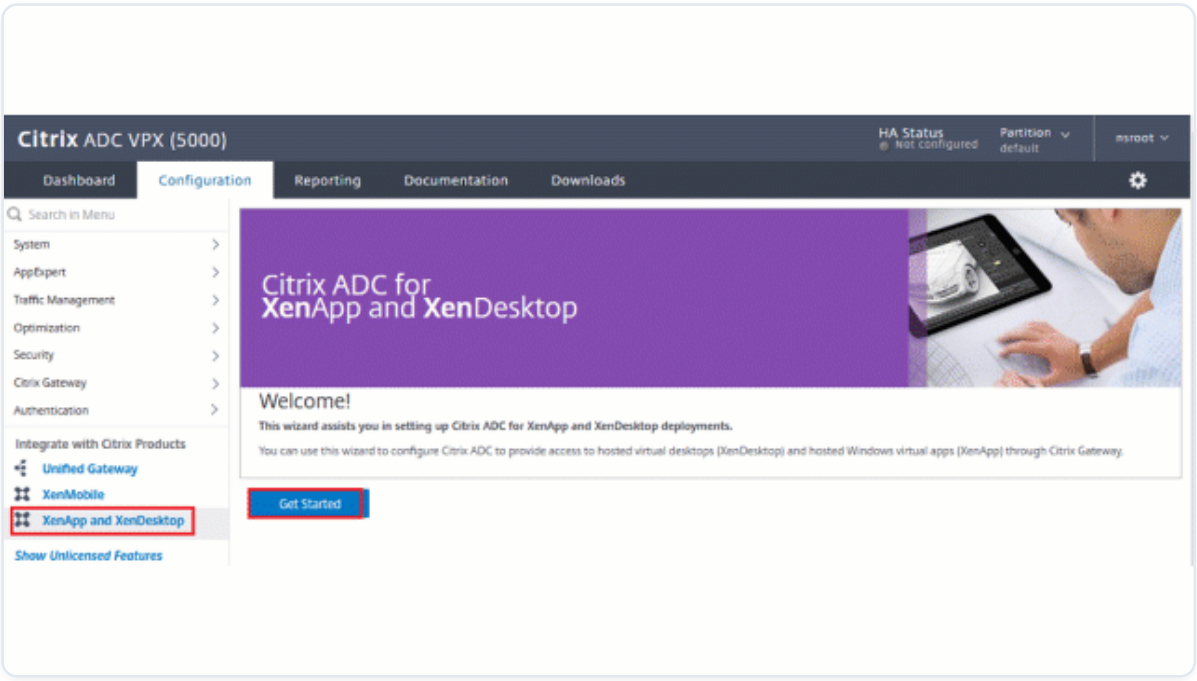


- サーバー証明書、CA証明書、およびルート証明書がインストールされます。詳細については、「インストール、リンク、および更新」を参照してください。





- Citrix Virtual Desktops用にCitrix Gatewayが作成されました。仮想サーバーがオンラインであることを確認するには、**Test STA Connectivity**ボタンをクリックして接続をテストします。詳細については、「Setting up Citrix ADC for Citrix Virtual Apps and Desktops」を参照してください。



2. リライトアクションを追加します。詳細については、「リライトアクションの構成」を参照してください。

   a. 「**AppExpert > Rewrite > Actions**」に移動します。

   b. 新しい書き換えアクションを追加するには、**追加**をクリックします。アクションの名前は「set Type to INSERT_HTTP_HEADER」にすることができます。

   書き換えアクションの追加(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/adc-appexpert-rewrite-action.png)

   a. **タイプ**で、**INSERT_HTTP_HEADER**を選択します。

   b. **ヘッダー名**に「X-Citrix-XmlServiceKey」と入力します。

   c. **式**に、引用符付きで`<XmlServiceKey1 value>`を追加します。XmlServiceKey1 の値は、Desktop Delivery Controller™ の構成からコピーできます。

   XMLサービスキーの値(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/xml-service-key-values.png)

3. 書き換えポリシーを追加します。詳細については、「書き換えポリシーの構成」を参照してください。

   a. 「**AppExpert > Rewrite > Policies**」に移動します。

   b. 新しいポリシーを追加するには、**追加**をクリックします。

   書き換えポリシーの追加(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/adc-appexpert-rewrite-policy.png)

a. **アクション**で、前の手順で作成したアクションを選択します。

b. **式**に「HTTP.REQ.IS_VALID」を追加します。

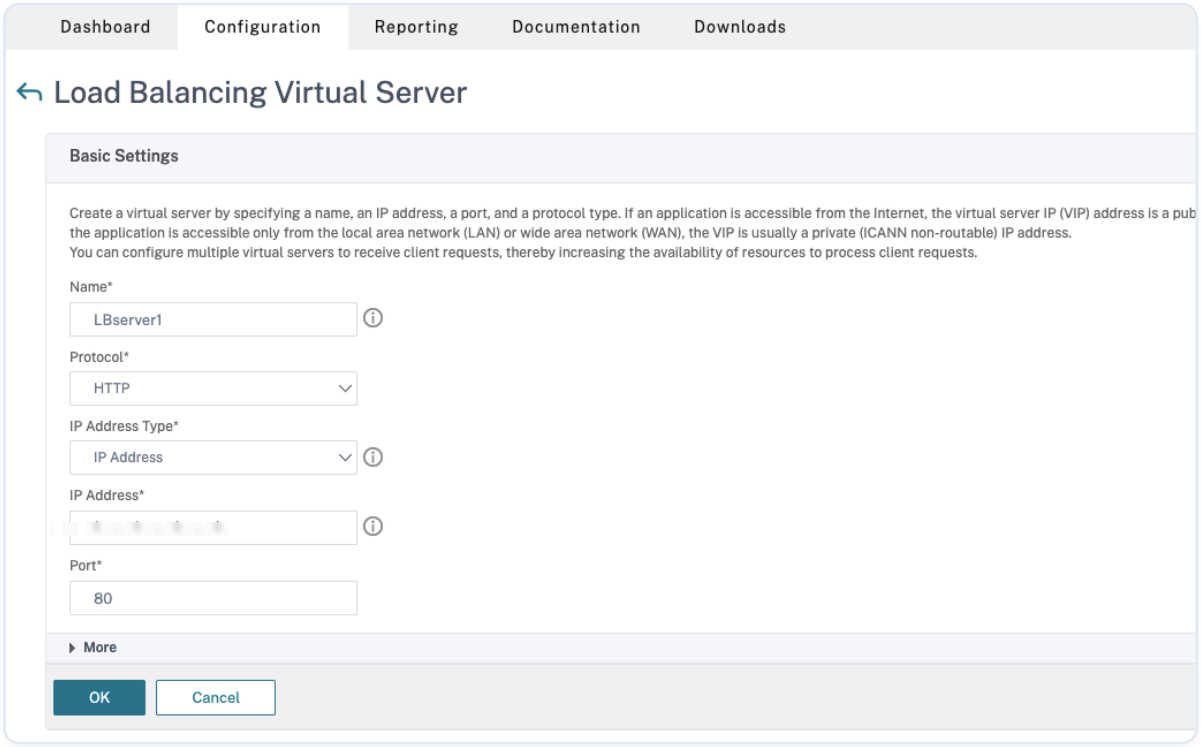
c. **OK**をクリックします。

4. 負荷分散を設定します。STAサーバーごとに1つの負荷分散仮想サーバーを構成する必要があります。構成しない場合、セッションの起動に失敗します。

   詳細については、基本的な負荷分散のセットアップを参照してください。

   a. 負荷分散仮想サーバーを作成します。

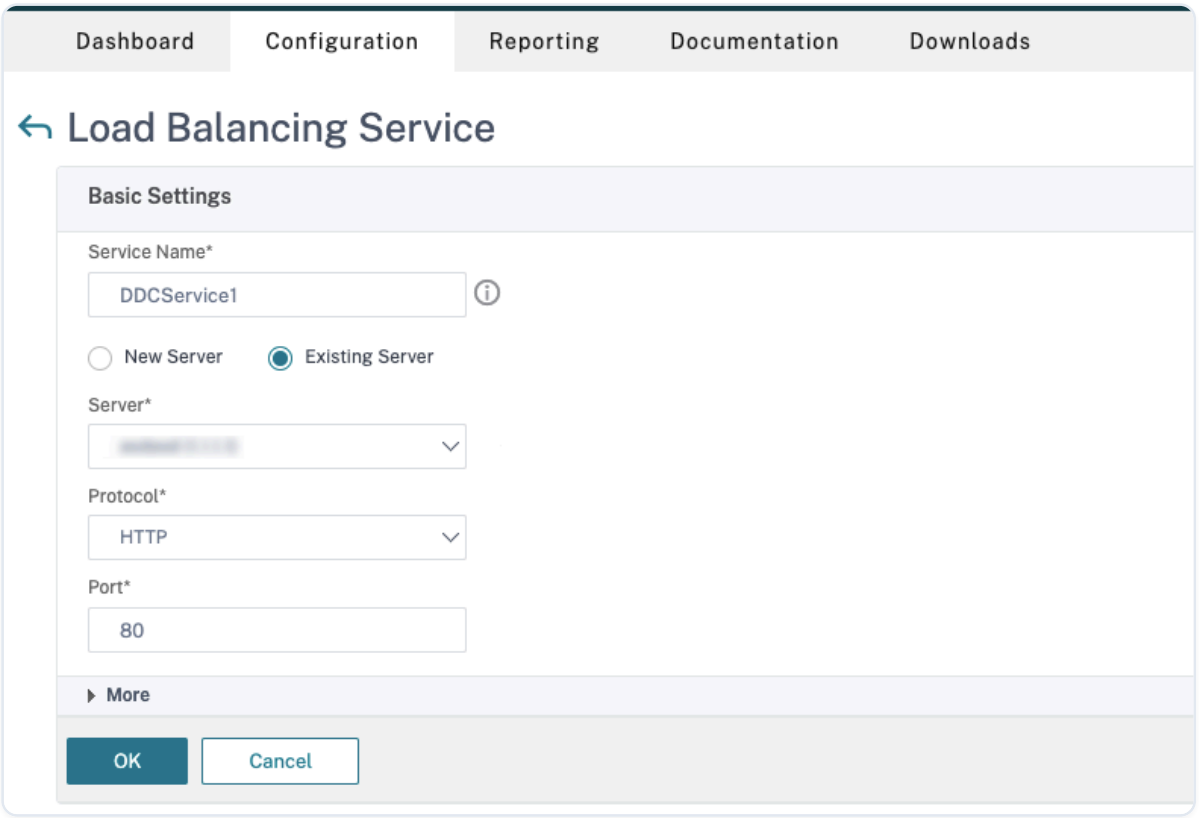
      - **トラフィック管理 > ロードバランシング > サーバー**に移動します。
      - **Virtual Servers**ページで、**Add**をクリックします。



      - **Protocol**で、**HTTP**を選択します。
      - 負荷分散仮想IPアドレスを追加し、**Port**で**80**を選択します。
      - **OK**をクリックします。

   b. 負荷分散サービスを作成します。

      - **トラフィック管理 > ロードバランシング > サービス**に移動します。



- **Existing Server**で、前のステップで作成した仮想サーバーを選択します。
- **Protocol**で**HTTP**を選択し、**Port**で**80**を選択します。
- **OK**をクリックし、その後**Done**をクリックします。

c. サービスを仮想サーバーにバインドします。

- 以前に作成した仮想サーバーを選択し、**編集**をクリックします。
- **サービスとサービスグループ**で、**ロードバランシング仮想サーバーサービスバインディングなし**をクリックします。

仮想サーバーにサービスをバインド(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/adc-bind-service-to-lbvserver.png)

- **Service Binding**で、以前に作成したサービスを選択します。
- **バインド**をクリックします。

d. 以前に作成した書き換えポリシーを仮想サーバーにバインドします。

- 以前に作成した仮想サーバーを選択し、**編集**をクリックします。
- **詳細設定**で、**ポリシー**をクリックし、次に**ポリシー**セクションで**+**をクリックします。

書き換えポリシーをバインド(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/adc-bind-rewrite-policy.png)

- **ポリシーの選択**で**書き換え**を選択し、**タイプの選択**で**要求**を選択します。
- **続行**をクリックします。
- **ポリシーの選択**で、以前に作成した書き換えポリシーを選択します。
- **バインド**をクリックします。
- **完了**をクリックします。

e. 必要に応じて、仮想サーバーの永続性を設定します。

- 以前に作成した仮想サーバーを選択し、**編集**をクリックします。
- **詳細設定**で、**永続性**をクリックします。

永続性の設定(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/adc-lb-vserver-persistence.png)

- 永続性の種類として**その他**を選択します。
- 仮想サーバーによって選択されたサービスのIPアドレス（宛先IPアドレス）に基づいて永続性セッションを作成するには、**DESTIP**を選択します。
- **IPv4ネットマスク**で、DDCと同じネットワークマスクを追加します。
- **OK**をクリックします。

f. 他の仮想サーバーについても、これらの手順を繰り返します。

Citrix ADCアプライアンスがCitrix Virtual Desktops™で既に構成されている場合の構成の変更点

Citrix ADCアプライアンスをCitrix Virtual Desktopsで既に構成している場合、Secure XML機能を使用するには、以下の構成変更を行う必要があります。

- セッション起動前に、ゲートウェイの**セキュリティチケット機関URL**を、負荷分散仮想サーバーのFQDNを使用するように変更します。
- `TrustRequestsSentToTheXmlServicePort` パラメーターがFalseに設定されていることを確認してください。デフォルトでは、`TrustRequestsSentToTheXmlServicePort` パラメーターはFalseに設定されています。ただし、顧客がCitrix Virtual Desktops用にCitrix ADCを既に構成している場合、`TrustRequestsSentToTheXmlServicePort` はTrueに設定されます。

1. Citrix ADC GUIで、**構成 > Citrix製品との統合**に移動し、**XenApp and XenDesktop®**をクリックします。
2. ゲートウェイインスタンスを選択し、編集アイコンをクリックします。

   既存のゲートウェイ構成を編集(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/edit-gateway-instance.png)
3. StoreFrontペインで、編集アイコンをクリックします。

   StoreFrontの詳細を編集(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/edit-storefront-details.png)
4. **Secure Ticket Authority URL**を追加します。

   - Secure XML機能が有効になっている場合、STA URLはロードバランシングサービスのURLである必要があります。
   - Secure XML機能が無効になっている場合、STA URLはSTAのURL（DDCのアドレス）である必要があり、DDC上のTrustRequestsSentToTheXmlServicePortパラメーターはTrueに設定する必要があります。

   STA URLを追加(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/add-sta-urls.png)

セッションの回復性設定

セッションアクティビティを維持することは、最高のユーザーエクスペリエンスを提供するために不可欠です。信頼性の低いネットワーク、変動の大きいネットワーク遅延、ワイヤレスデバイスの範囲制限による接続の喪失は、ユーザーの不満につながる可能性があります。デバイス間を素早く移動し、ログオンするたびに同じアプリケーションにアクセスすることは、医療従事者などの多くのモバイルワーカーにとって優先事項です。

この記事で説明する機能は、セッションの信頼性を最適化し、不便さ、ダウンタイム、生産性の損失を軽減します。これらの機能を使用することで、モバイルユーザーはデバイス間を迅速かつ簡単にローミングできます。

セッションの信頼性

セッションの信頼性により、ネットワーク接続が中断されてもセッションはアクティブな状態を保ち、ユーザーの画面に表示されます。ユーザーは、ネットワーク接続が再開されるまで、使用しているアプリケーションを引き続き見ることができます。

この機能は、ワイヤレス接続を使用するモバイルユーザーにとって特に便利です。たとえば、ワイヤレス接続を使用しているユーザーが鉄道トンネルに入り、一時的に接続が失われたとします。通常、セッションは切断されてユーザーの画面から消え、ユーザーは切断されたセッションに再接続する必要があります。セッションの信頼性を使用すると、セッションはマシン上でアクティブなままになります。接続が失われたことを示すために、ユーザーのディスプレイはフリーズし、カーソルはトンネルの反対側で接続が再開されるまで回転する砂時計に変わります。ユーザーは中断中もディスプレイにアクセスし続け、ネットワーク接続が復元されるとアプリケーションとの対話を再開できます。セッションの信頼性により、再認証のプロンプトなしでユーザーが再接続されます。

Citrix Workspace™アプリのユーザーは、Controllerの設定を上書きできません。

セッションの信頼性は、トランスポート層セキュリティ (TLS) とともに使用できます。TLSは、ユーザーデバイスとCitrix Gatewayの間で送信されるデータのみを暗号化します。

次のポリシー設定でセッションの信頼性を有効にして構成します。

- セッションの信頼性接続ポリシー設定は、セッションの信頼性を許可または禁止します。
- セッションの信頼性タイムアウトポリシー設定のデフォルトは180秒、つまり3分です。セッションの信頼性がセッションを開いたままにする時間を延長することはできますが、この機能はユーザーの利便性のために設計されています。そのため、ユーザーに再認証を促すことはありません。セッションを開いたままにする時間を延長すると、ユーザーが注意散漫になり、ユーザーデバイスから離れてしまう可能性が高まります。これらの行動は、セッションを不正なユーザーがアクセスできる状態にする可能性があります。
- 受信セッションの信頼性接続は、セッションの信頼性ポート番号ポリシー設定でポート番号を変更しない限り、ポート2598を使用します。
- ユーザーが再認証なしで中断されたセッションに再接続するのを防ぐには、自動クライアント再接続機能を使用します。自動クライアント再接続認証ポリシー設定を構成して、中断されたセッションに再接続する際にユーザーに再認証を促すことができます。

セッションの信頼性と自動クライアント再接続の両方を使用する場合、これら2つの機能は順次動作します。セッションの信頼性は、セッションの信頼性タイムアウトポリシー設定で指定した時間の経過後、ユーザーセッションを閉じるか、切断します。その後、自動クライアント再接続ポリシー設定が有効になり、切断されたセッションにユーザーを再接続しようとします。

クライアントの自動再接続

自動クライアント再接続機能を使用すると、Citrix WorkspaceアプリはICA®セッションの意図しない切断を検出し、影響を受けるセッションにユーザーを自動的に再接続できます。この機能が

サーバーで有効になっている場合、ユーザーは作業を続行するために手動で再接続する必要はありません。

アプリケーションセッションの場合、Citrix Workspaceアプリは、再接続が成功するか、ユーザーが再接続の試行をキャンセルするまで、セッションへの再接続を試みます。

デスクトップセッションの場合、Citrix Workspaceアプリは、再接続が成功するか、ユーザーが再接続の試行をキャンセルしない限り、指定された期間、セッションへの再接続を試行します。デフォルトでは、この期間は5分です。この期間を変更するには、ユーザーデバイスで以下のレジストリ設定を編集します（`seconds` は、セッションの再接続がそれ以上試行されなくなるまでの秒数です）。

`HKLM\Software\Citrix\ICA Client\TransportReconnectRetryMaxTimeSeconds; DWORD;<seconds>`

以下のポリシー設定でAuto Client Reconnectを有効にして構成します。

- **Auto Client Reconnect:** 接続が中断された後にCitrix Workspaceアプリによる自動再接続を有効または無効にします。
- **Auto Client Reconnect authentication:** 自動再接続後のユーザー認証の要件を有効または無効にします。
- **Auto Client Reconnect logging:** イベントログへの再接続イベントのログ記録を有効または無効にします。ログ記録はデフォルトで無効になっています。有効にすると、サーバーのシステムログに、成功および失敗した自動再接続イベントに関する情報が記録されます。各サーバーは、再接続イベントに関する情報を独自のシステムログに保存します。サイトは、すべてのサーバーの再接続イベントの統合ログを提供しません。

> **注：**

> 再認証なしのAuto Client Reconnectは、パスワード認証でのみサポートされています。フェデレーション認証サービスまたはスマートカード認証を使用している場合、再認証なしのAuto Client Reconnectはサポートされません。そのような場合、ユーザーはログイン画面にリダイレクトされます。

> Auto Client Reconnectは、暗号化されたユーザー資格情報に基づく認証メカニズムを組み込んでいます。ユーザーが最初にログオンすると、サーバーはユーザー資格情報を暗号化してメモリに保存します。サーバーはまた、暗号化キーを含むCookieを作成し、Citrix Workspaceアプリに送信します。Citrix Workspaceアプリは、再接続のためにキーをサー

> バーに送信します。サーバーは資格情報を復号化し、認証のためにWindowsログオンに送信します。Cookieの有効期限が切れると、ユーザーはセッションに再接続するために再認証する必要があります。

Auto Client Reconnect認証設定を有効にすると、Cookieは使用されません。代わりに、Citrix Workspaceアプリが自動的に再接続を試みるときに、資格情報を要求するダイアログボックスがユーザーに表示されます。

ユーザー資格情報とセッションを最大限に保護するために、クライアントとサイト間のすべての通信に暗号化を使用してください。

icaclient.admファイルを使用して、Windows版Citrix WorkspaceアプリでAuto Client Reconnectを無効にします。詳細については、お使いのWindows版Citrix Workspaceアプリのバージョンのドキュメントを参照してください。

接続の設定もAuto Client Reconnectに影響します。

- デフォルトでは、前述のとおり、Auto Client Reconnectはサイトレベルのポリシー設定によって有効になっています。ユーザーの再認証は不要です。ただし、サーバーのICA TCP接続が、通信リンクが切断されたセッションをリセットするように構成されている場合、自動再接続は行われません。Auto Client Reconnectは、接続が切断されたかタイムアウトした場合にサーバーがセッションを切断する場合にのみ機能します。このコンテキストでは、ICA TCP接続とは、TCP/IPネットワーク上のセッションに使用されるサーバーの仮想ポート（実際のネットワーク接続ではなく）を指します。
- デフォルトでは、サーバー上のICA TCP接続は、切断された接続またはタイムアウトした接続を持つセッションを切断するように設定されています。切断されたセッションはシステムメモリにそのまま残り、Citrix Workspaceアプリによる再接続が可能です。
- 接続は、切断された接続またはタイムアウトした接続を持つセッションをリセットまたはログオフするように構成できます。セッションがリセットされると、再接続を試みると新しいセッションが開始されます。使用中のアプリケーションでユーザーを同じ場所に戻すのではなく、アプリケーションが再起動されます。
- サーバーがセッションをリセットするように構成されている場合、Auto Client Reconnectは新しいセッションを作成します。このプロセスでは、ユーザーがサーバーにログオンするために資格情報を入力する必要があります。
- Citrix Workspaceアプリまたはプラグインが誤った認証情報を送信した場合、自動再接続が失敗することがあります。これは、攻撃中に発生したり、サーバーが切断された接続を検出してから時間が経ちすぎたと判断した場合に起こりえます。

ICA キープアライブ

ICA Keep-Alive機能を有効にすると、途切れた接続が切断されるのを防ぎます。有効にすると、サーバーがアクティビティを検出しない場合、この機能によりリモートデスクトップサービスがそのセッションを切断するのを防ぎます。アクティビティがない例としては、クロックの変更、マウスの移動、画面の更新がないことなどが挙げられます。サーバーは数秒ごとにキープアライブパケットを送信して、セッションがアクティブであるかどうかを検出します。セッションがアクティブでなくなった場合、サーバーはそのセッションを切断済みとしてマークします。

> **重要:**

> ICA Keep-Aliveは、セッションの信頼性を使用していない場合にのみ機能します。セッションの信頼性には、途切れた接続が切断されるのを防ぐ独自のメカニズムがあります。ICA Keep-Aliveは、セッションの信頼性を使用しない接続に対してのみ構成してください。

> ICA Keep-Alive設定は、Windowsグループポリシーで構成されているキープアライブ設定を上書きします。

次のポリシー設定を使用して、ICA Keep-Aliveを有効にして構成します。

- **ICAキープアライブタイムアウト:** ICAキープアライブメッセージの送信に使用される間隔（1～3600秒）を指定します。途切れた接続が非常にまれで、ユーザーがセッションに再接続できることが問題にならない環境で、ネットワーク監視ソフトウェアに非アクティブな接続を閉じさせたい場合は、このオプションを構成しないでください。

  デフォルトの間隔は60秒です。ICA Keep-Aliveパケットは60秒ごとにユーザーデバイスに送信されます。ユーザーデバイスが60秒以内に応答しない場合、ICAセッションのステータスは切断済みに変わります。

- **ICAキープアライブ:** ICAキープアライブメッセージの送信を許可または禁止します。

ワークスペースコントロール

ワークスペースコントロールにより、デスクトップとアプリケーションはユーザーに追従し、デバイス間を移動できます。このローミング機能により、ユーザーはログオンするだけで、各デバイスでデスクトップやアプリケーションを再起動することなく、どこからでもすべてのデスクトップや開いているアプリケーションにアクセスできます。たとえば、ワークスペースコントロールは、病院で異なるワークステーション間を素早く移動し、ログオンするたびに同じアプリケーションセットにアクセスする必要がある医療従事者を支援できます。ワークスペースコントロールオプションを許可するように構成すると、これらの医療従事者は1つのクライアントデバイスで複数の

アプリケーションから切断し、別のクライアントデバイスで同じアプリケーションを開くために再接続できます。

ワークスペースコントロールは、次のアクティビティに影響します。

- **ログオン:** デフォルトでは、ワークスペースコントロールにより、ユーザーはログオン時に実行中のすべてのデスクトップとアプリケーションに自動的に再接続でき、手動で再開する必要がなくなります。ワークスペースコントロールを通じて、ユーザーは切断されたデスクトップまたはアプリケーション、および別のクライアントデバイスでアクティブなものを開くことができます。デスクトップまたはアプリケーションから切断しても、それはサーバー上で実行されたままになります。一部のデスクトップまたはアプリケーションを1つのクライアントデバイスで実行したままにし、別のクライアントデバイスでデスクトップまたはアプリケーションのサブセットに再接続する必要があるローミングユーザーがいる場合、ユーザーが以前に切断したデスクトップまたはアプリケーションのみを開くようにログオン再接続動作を構成できます。
- **再接続:** サーバーにログオンした後、ユーザーは「再接続」をクリックすることで、いつでもすべてのデスクトップまたはアプリケーションに再接続できます。デフォルトでは、「再接続」は切断されたデスクトップまたはアプリケーション、および現在別のクライアントデバイスで実行中のものを開きます。ユーザーが以前に切断したデスクトップまたはアプリケーションのみを開くように「再接続」を構成できます。
- **ログオフ:** StoreFront™を介してデスクトップまたはアプリケーションを開くユーザーの場合、**ログオフ**コマンドを構成して、ユーザーをStoreFrontとすべてのアクティブなセッションからログオフさせるか、StoreFrontからのみログオフさせることができます。
- **切断:** ユーザーは、個別に切断する必要なく、実行中のすべてのデスクトップとアプリケーションから一度に切断できます。

ワークスペースコントロールは、Citrix StoreFront接続を介してデスクトップおよびアプリケーションにアクセスするCitrix Workspaceアプリユーザーのみが利用できます。デフォルトでは、ワークスペースコントロールは仮想デスクトップセッションでは無効になっていますが、ホスト型アプリケーションでは有効になっています。公開されたデスクトップと、それらのデスクトップ内で実行されている公開されたアプリケーションとの間で、セッション共有はデフォルトでは行われません。

ユーザーが新しいクライアントデバイスに移動すると、ユーザーポリシー、クライアントドライブマッピング、およびプリンター構成が適切に変更されます。ポリシーとマッピングは、ユーザーがセッションにログオンしているクライアントデバイスに応じて適用されます。たとえば、医療従事者が救急治療室のデバイスからログオフし、X線検査室のワークステーションにログオンする場

合、X線検査室でのセッションに適したポリシー、プリンターマッピング、およびクライアントドライブマッピングがセッション開始時に有効になります。

ユーザーが場所を変更したときに表示されるプリンターをカスタマイズできます。また、ユーザーがローカルプリンターに印刷できるかどうか、ユーザーがリモートで接続したときに消費される帯域幅の量、およびその他の印刷エクスペリエンスの側面を制御することもできます。

ユーザー向けにワークスペースコントロールを有効化および構成する方法については、StoreFrontのドキュメントを参照してください。

セッションローミング

> **注：**
>
> 以下の情報は、PowerShellを使用してセッションローミングを構成する方法を説明しています。代わりにWeb Studioを使用することもできます。詳細については、「デリバリーグループの管理」を参照してください。

> デフォルトでは、セッションはユーザーとともにクライアントデバイス間をローミングします。ユーザーがセッションを起動し、別のデバイスに移動すると、同じセッションが使用され、両方のデバイスでアプリケーションが利用可能になります。アプリケーションは、デバイスや現在のセッションの有無にかかわらず追従します。多くの場合、アプリケーションに割り当てられたプリンターやその他のリソースも追従します。

このデフォルトの動作には多くの利点がありますが、すべての場合に理想的とは限りません。PowerShell SDKを使用してセッションローミングを防止できます。

例1：医療従事者が2つのデバイスを使用しており、デスクトップPCで保険フォームを完成させ、タブレットで患者情報を閲覧しています。

- セッションローミングが有効になっている場合、両方のアプリケーションが両方のデバイスに表示されます（1つのデバイスで起動されたアプリケーションは、使用中のすべてのデバイスで表示されます）。これはセキュリティ要件を満たさない可能性があります。
- セッションローミングが無効になっている場合、患者記録はデスクトップPCに表示されず、保険フォームはタブレットに表示されません。

例2：生産管理者が自分のオフィスにあるPCでアプリケーションを起動します。デバイス名と場所によって、そのセッションで利用可能なプリンターやその他のリソースが決まります。その日の後半、彼は会議のために隣の建物のオフィスに行き、プリンターを使用する必要があります。

- セッションローミングが有効になっている場合、生産管理者は会議室近くのプリンターにアクセスできない可能性があります。なぜなら、彼がオフィスで以前に起動したアプリケーションによって、その場所近くのプリンターやその他のリソースが割り当てられたためです。
- セッションローミングが無効になっている場合、彼が別のマシンに（同じ資格情報を使用して）ログオンすると、新しいセッションが開始され、近くのプリンターやリソースが利用可能になります。

セッションローミングの構成

セッションローミングを構成するには、「SessionReconnection」プロパティを持つ以下のエンタイトルメントポリシー規則コマンドレットを使用します。オプションで、「LeasingBehavior」プロパティも指定できます。

デスクトップセッションの場合：

```
Set-BrokerEntitlementPolicyRule <Delivery-Group-name> -SessionReconnection <value> -LeasingBehavior Allowed|Disallowed
```

アプリケーションセッションの場合：

```
Set-BrokerAppEntitlementPolicyRule <Delivery-Group-name> -SessionReconnection <value> -LeasingBehavior Allowed|Disallowed
```

`value` には、次のいずれかを指定できます。

- **Always:** セッションは、クライアントデバイスやセッションが接続されているか切断されているかに関係なく、常にローミングします。これがデフォルト値です。
- **DisconnectedOnly:** 既に切断されているセッションにのみ再接続します。それ以外の場合は、新しいセッションを起動します。（セッションは、最初に切断するか、Workspace Control を使用して明示的にローミングすることで、クライアントデバイス間をローミングできます。）別のクライアントデバイスからのアクティブな接続済みセッションは使用されません。代わりに、新しいセッションが起動されます。
- **SameEndpointOnly:** ユーザーは、使用するクライアントデバイスごとに一意のセッションを取得します。これにより、ローミングが完全に無効になります。ユーザーは、以前セッションで使用したのと同じデバイスにのみ再接続できます。

「LeasingBehavior」プロパティについては、以下で説明します。

その他の設定による影響：

セッションローミングを無効にすると、デリバリーグループのアプリケーションのプロパティにあるアプリケーション制限 **ユーザーごとにアプリケーションのインスタンスを1つのみ許可する** の影響を受けます。

- セッションローミングを無効にする場合は、「アプリケーションのインスタンスを1つのみ許可する...」アプリケーション制限も無効にします。
- 「アプリケーションのインスタンスを1つのみ許可する...」アプリケーション制限を有効にする場合は、新しいデバイスで新しいセッションを許可する2つの値のいずれも構成しないでください。

ログオン間隔

デスクトップVDAを含む仮想マシンがログオンプロセス完了前に閉じられた場合、そのプロセスにより多くの時間を割り当てることができます。バージョン7.6以降のデフォルトは180秒です（バージョン7.0〜7.5のデフォルトは90秒です）。

マシン（またはマシンカタログで使用されるマスターイメージ）で、次のレジストリキーを設定します。

キー: `HKLM\SOFTWARE\Citrix\PortICA`

- 値: `AutoLogonTimeout`
- 種類: `DWORD`
- 0〜3600の範囲で、10進数の時間を秒単位で指定します。

マスターイメージを変更した場合は、カタログを更新します。

この設定は、デスクトップVDAを持つVMにのみ適用されます。Microsoftは、サーバーVDAを持つマシンでのログオンタイムアウトを制御します。

設定

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

> Web Studioを使用して、以下の設定を管理できます。

- 認証の管理
- Citrixカスタマーエクスペリエンス向上プログラム
- デリバリーコントローラーの削除
- ログデータベースの変更
- 日付と時刻の設定
- サイト管理の一元化
- リモートPCアクセスでの複数ユーザーの自動割り当てを有効にする
- DNS解決の有効化
- XML信頼の有効化
- セキュリティキーの管理
- Studioコンソールの非アクティブタイムアウトの設定

認証の管理

デフォルトでは、ユーザーはドメインのユーザー名とパスワードを使用してWeb Studioにログオンします。スマートカード認証や統合Windows認証など、ユーザーに対して別の認証方法を選択することもできます。

Studio を使用して管理

ユーザーの認証方法を選択するには、次の手順に従います。

1. Web Studio にサインインし、左ペインで を選択します。
2. タイルを見つけて をクリックし、オプションを選択します。

    - **ドメイン資格情報**
    - **ドメイン資格情報または統合 Windows 認証**

      統合 Windows 認証が有効になっている場合、ユーザーは Windows 資格情報 (Kerberos/NTLM) またはクライアント証明書を使用して Web Studio にアクセスできます。

      Web Studio と Delivery Controller™ が異なるマシンにインストールされている場合、統合 Windows 認証を機能させるには、クロスオリジンアクセスを許可し、Web Studio サーバーの URL を許可リストに追加します。

      > **重要**

> Web Studio が Delivery Controller のプロキシとして構成されている場合、統合 Windows 認証は機能しません。

- **スマートカード認証**
- **ドメイン資格情報またはスマートカード認証**

  スマートカード認証を有効にするには、追加の構成が必要です。詳細については、「Web Studio のスマートカード認証を設定する」を参照してください。

PowerShell スクリプトを使用して管理

認証方法は Delivery Controller データベースで構成されます。次の PowerShell スクリプトを使用して認証方法を設定できます。

1. Delivery Controller で次のコマンドを実行して、現在のサイト ID を取得します。

   `Get-ConfigSite | Select SiteGuid`

2. 以下のスクリプトを実行して認証方法を設定します。

```
# Generate a new bearer token

$bearerData = New-TrustBearerToken

# Define the Delivery Controller DNS name and Site ID

$ddc = "ddc.dc.com" # replace this with the Delivery Controller's DNS
name

$siteid = "c68a8f89-42af-4bea-a6e9-c8c936353f49" # replace this with
the site ID you get from step #1

# Define the URL and headers

$url = "https://$ddc/citrix/orchestration/api/CitrixOnPremises/Sites/
$siteid/Settings"

$headers = @{

"Content-Type" = "application/json"

"Authorization" = "Bearer $($bearerData.Token)"
```

```
}

# Define the JSON body

$body = @{

SupportedAuthenticators = "BasicAndSmartCard" # replace this with a
required authentication method: "Basic" for "Domain credentials";
"BasicAndIntegratedWindowsAuthentication" for "Domain credentials or
integrated Windows authentication"; "BasicAndSmartCard" for "Domain
credentials or smart card authentication"; "SmartCard" for "Smart card
authentication"

} | ConvertTo-Json -Depth 10

# Send the PATCH request

Invoke-RestMethod -Uri $url -Method Patch -Headers $headers -Body $body
```

統合Windows認証用にブラウザーを構成する

ドメイン資格情報または統合Windows認証を使用して*統合Windows認証*を有効にすると、次回ユーザーがサインインするときに自動的にサインインされます。ユーザーとして自動的にサインインできない場合は、以下の手順に従ってWebブラウザーを構成し、統合Windows認証を許可してください。

Google Chromeの場合：

1. コントロールパネルから、**インターネットオプション**を選択します。
2. **詳細設定**タブを選択します。
3. **統合Windows認証を有効にする**を選択します。
4. **セキュリティ**タブを選択します。
5. **ローカルイントラネット > サイト > 詳細設定**を選択します。
6. **このWebサイトをゾーンに追加する**ボックスで：
   - Web StudioとDelivery Controllerが同じサーバー上にある場合は、Web Studioを実行しているホストのURLを入力します。
   - そうでない場合は、ワイルドカードドメインを入力します。例：Delivery Controllerが `ddc.domain.com` にある場合、`*.domain.com` と入力します。

7. **追加 > 閉じる**をクリックします。

Mozilla Firefoxの場合：

1. ブラウザーから、URLボックスに`about:config`と入力します。
2. 「**検索**」ボックスに「`network negotiate`」と入力します。
3. **network.negotiate-auth.trusted-uris** を右クリックし、「**変更**」を選択します。
4. 「**文字列値を入力**」ボックスで、次のようにします。
   - Web Studio と Delivery Controller が同じサーバー上にある場合は、Web Studio をホストしているサーバー名を参照する URL および/またはエイリアスのコンマ区切りリストを追加します。
   - そうでない場合は、次のように URL を追加します。例: Delivery Controller が`ddc.domain.com`にある場合、「`*.domain.com`」と入力します。

ブラウザーを設定したら、サインインページで「**Windows 統合サインイン**」をクリックして再試行できます。

Web Studio と Delivery Controller が異なるマシンにインストールされている場合、統合 Windows 認証を機能させるには、「**クロスオリジンアクセスを許可**」を有効にする必要があります。

「**クロスオリジンアクセスを許可**」を有効にするには、次の手順に従います。

1. 「**クロスオリジンアクセスを許可**」チェックボックスをオンにします。
2. Web Studio サーバーの URL を許可リストに追加します。
3. 「**URL を入力**」フィールドに URL を入力します。必要に応じて、「**追加**」をクリックしてさらに追加します。

> **注**
>
> - URL は正しい形式`<scheme>://<hostname>`に従う必要があります。パスや末尾のスラッシュを含まないようにしてください。
> - IP アドレスと FQDN がサポートされています。URL を追加するときは、Web Studio へのアクセス方法と一致していることを確認してください。たとえば、IP アドレスを使用して Web Studio にアクセスする場合は、IP アドレスベースの URL をリストに追加します。

- デフォルト以外のポートを使用する場合は、ポート番号を含めるようにしてください。

4. 必要に応じて、「**追加**」をクリックしてさらに追加します。
5. 完了したら、「**完了**」をクリックして保存し、終了します。

タイムゾーンを設定する

日付と時刻の形式を好みに合わせてカスタマイズするには、次の手順に従います。

1. Web Studio にサインインし、左ペインで「**設定**」を選択します。
2. 「**日付と時刻**」タイルを見つけて「**編集**」をクリックし、次のオプションを設定します。
   - **時刻形式:**
     - 12時間形式（例: 午後09:00）または24時間形式（例: 21:00）で時刻を表示するように選択します。
   - **日付形式:**
     - yyyy/MM/dd のように、好みに合わせて日付形式を設定します。
   - **タイムゾーン:**
     - **UTC:** ユーザーインターフェイス全体で日付と時刻をUTCで表示します。日付と時刻にマウスを合わせると、その情報がローカルタイムゾーンで表示されます。
     - **ローカルタイムゾーン:** ユーザーインターフェイス全体で日付と時刻をローカルタイムゾーンで表示します。日付と時刻にマウスを合わせると、その情報がUTCで表示されます。

注：

これらの設定は、各ユーザーアカウントに固有のものです。

DNS解決を有効にする

ICA®ファイルでIPアドレスの代わりにDNS名を表示するには、次の手順に従います。

1. Web Studioにサインインし、左側のペインで**設定**を選択します。

2. **DNS解決を有効にする**設定をオンにします。

Studioコンソールの非アクティビティタイムアウトを設定する

管理者がStudioコンソールから自動的にサインアウトされるまでの非アクティビティ期間を設定できます。

1. Web Studioにサインインし、左側のペインで**設定**を選択します。
2. 10分から24時間の範囲で期間を入力します。
3. この設定を適用するには、ページを更新するか、サインアウトしてから再度サインインします。

サイト管理の一元化

この機能を使用すると、1つのWeb Studioコンソールで複数のCitrix Virtual Apps and Desktopsサイトを管理できます。詳細については、「複数のサイト管理を有効にする」を参照してください。

タグ

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

はじめに

タグは、マシン、アプリケーション、デスクトップ、デリバリーグループ、アプリケーショングループ、ポリシーなどの項目を識別する文字列です。タグを作成して項目に追加すると、特定のタグを持つ項目にのみ適用されるように特定の操作を調整できます。

- Web Studioでの検索表示を調整します。

  たとえば、テスター向けに最適化されたアプリケーションのみを表示するには、「test」という名前のタグを作成し、それらのアプリケーションに追加（適用）します。これで、Web Studioの検索を「test」タグでフィルタリングできます。

- アプリケーショングループからアプリケーションを公開したり、デリバリーグループから特定のデスクトップを公開したりする際に、選択したデリバリーグループ内のマシンの一部のみを考慮します。これは*タグ制限*と呼ばれます。

  タグ制限を使用すると、既存のマシンを複数の公開タスクに使用できるため、より多くのマシンを展開および管理するコストを節約できます。タグ制限は、デリバリーグループ内のマシンを細分化（またはパーティション分割）するものと考えることができます。その機能は、XenApp 7.xより前のリリースにおけるワーカーグループと似ていますが、同一ではありません。

  タグ制限付きのアプリケーショングループまたはデスクトップを使用すると、デリバリーグループ内のマシンの一部を分離してトラブルシューティングする際に役立ちます。

- デリバリーグループ内のマシンの一部に対して定期的な再起動をスケジュールします。

  マシンにタグ制限を使用すると、新しいPowerShellコマンドレットを使用して、デリバリーグループ内のマシンの一部に対して複数の再起動スケジュールを構成できます。例と詳細については、「デリバリーグループの管理」を参照してください。

- 指定されたタグを持つ（または持たない）デリバリーグループ、デリバリーグループの種類、またはOU内のマシンの一部にCitrixポリシーの適用（割り当て）を調整します。

  たとえば、より強力なワークステーションにのみCitrixポリシーを適用したい場合は、それらのマシンに「high power」という名前のタグを追加します。次に、ポリシー作成ウィザードの**ポリシーの割り当て**ページで、そのタグと**有効にする**チェックボックスを選択します。デリバリーグループにタグを追加し、そのグループにCitrixポリシーを適用することもできます。詳細については、「ポリシーの作成」を参照してください。

タグは以下に適用できます。

- マシン
- アプリケーション
- マシンカタログ（PowerShellのみ。詳細については、「マシンカタログのタグ」を参照してください）
- デリバリーグループ
- アプリケーショングループ

Web Studioで以下を作成または編集する際に、タグ制限を構成できます。

- 共有デリバリーグループ内のデスクトップ
- アプリケーショングループ

重要:

タグは、明示的にマシンに適用することも、マシンカタログまたはデリバリーグループレベルで明示的に適用することもできます。タグがマシンカタログまたはデリバリーグループレベルで適用されると、そのカタログまたはデリバリーグループ内のすべてのマシンが暗黙的にそのタグを継承します。これらの継承されたタグは、マシンレベルで削除することはできません。タグの効果を削除するには、マシンカタログまたはデリバリーグループレベルからタグを削除する必要があります。

デスクトップまたはアプリケーショングループのタグ制限

タグ制限にはいくつかの手順があります。

- タグを作成し、マシンに追加（適用）します。
- タグ制限付きのグループを作成または編集します（つまり、「タグxを持つマシンへの起動を制限する」）。

タグ制限は、ブローカーのマシン選択プロセスを拡張します。ブローカーは、アクセスポリシー、構成されたユーザーリスト、ゾーン設定、起動準備、およびタグ制限（存在する場合）に従って、関連付けられたデリバリーグループからマシンを選択します。アプリケーションの場合、ブローカーは優先順位に従って他のデリバリーグループにフォールバックし、検討対象の各デリバリーグループに同じマシン選択ルールを適用します。

例1：シンプルなレイアウト

この例では、タグ制限を使用して、特定のデスクトップおよびアプリケーションの起動に考慮されるマシンを制限するシンプルなレイアウトを紹介します。このサイトには、1つの共有デリバリーグループ、1つの公開デスクトップ、および2つのアプリケーションで構成された1つのアプリケーショングループがあります。

シンプルなレイアウトでタグ制限を使用する例。(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/tags-example.png)

- 3台のマシン（VDA 101～103）のそれぞれにタグが追加されています。
- 共有デリバリーグループ内のデスクトップは、「Red」という名前のタグ制限付きで作成されました。デスクトップは、そのデリバリーグループ内で「Red」タグを持つマシン（VDA 101および102）でのみ起動できます。

- アプリケーショングループは「Orange」タグ制限付きで作成されたため、そのアプリケーション（CalculatorとNotepad）はそれぞれ、「Orange」タグを持つデリバリーグループ内のマシン（VDA 102および103）でのみ起動できます。

マシンVDA 102は両方のタグ（RedとOrange）を持っているため、アプリケーションとデスクトップの起動に考慮されます。

例2：より複雑なレイアウト

この例には、タグ制限付きで作成された複数のアプリケーショングループが含まれています。これにより、デリバリーグループのみを使用した場合に必要となるよりも少ないマシンで、より多くのアプリケーションを配信できるようになります。

例2の構成方法は、この例でタグを作成および適用し、タグ制限を構成するために使用される手順を示しています。

複雑なレイアウトでタグ制限を使用する例。(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/tags-example2.png)

この例では、10台のマシン（VDA 101～110）、1つのデリバリーグループ（D01）、および3つのアプリケーショングループ（A100、A200、A300）を使用します。各マシンにタグを適用し、各アプリケーショングループの作成時にタグ制限を指定することで、次のことが可能になります。

- グループ内の経理ユーザーは、5台のマシン（VDA 101～105）で必要なアプリにアクセスできます
- グループ内のCAD設計者は、5台のマシン（VDA 106-110）で必要なアプリにアクセスできます
- グループ内でOfficeアプリケーションを必要とするユーザーは、10台のマシン（VDA 101～110）でOfficeアプリにアクセスできます

使用されるマシンは10台のみで、デリバリーグループは1つだけです。デリバリーグループのみを使用する場合（アプリケーショングループなし）は、マシンが1つのデリバリーグループにしか属せないため、2倍の数のマシンが必要になります。

タグとタグ制限の管理

タグは、Web Studioの**［タグの管理］**アクションを通じて、選択したアイテムに対して作成、追加（適用）、編集、削除されます。

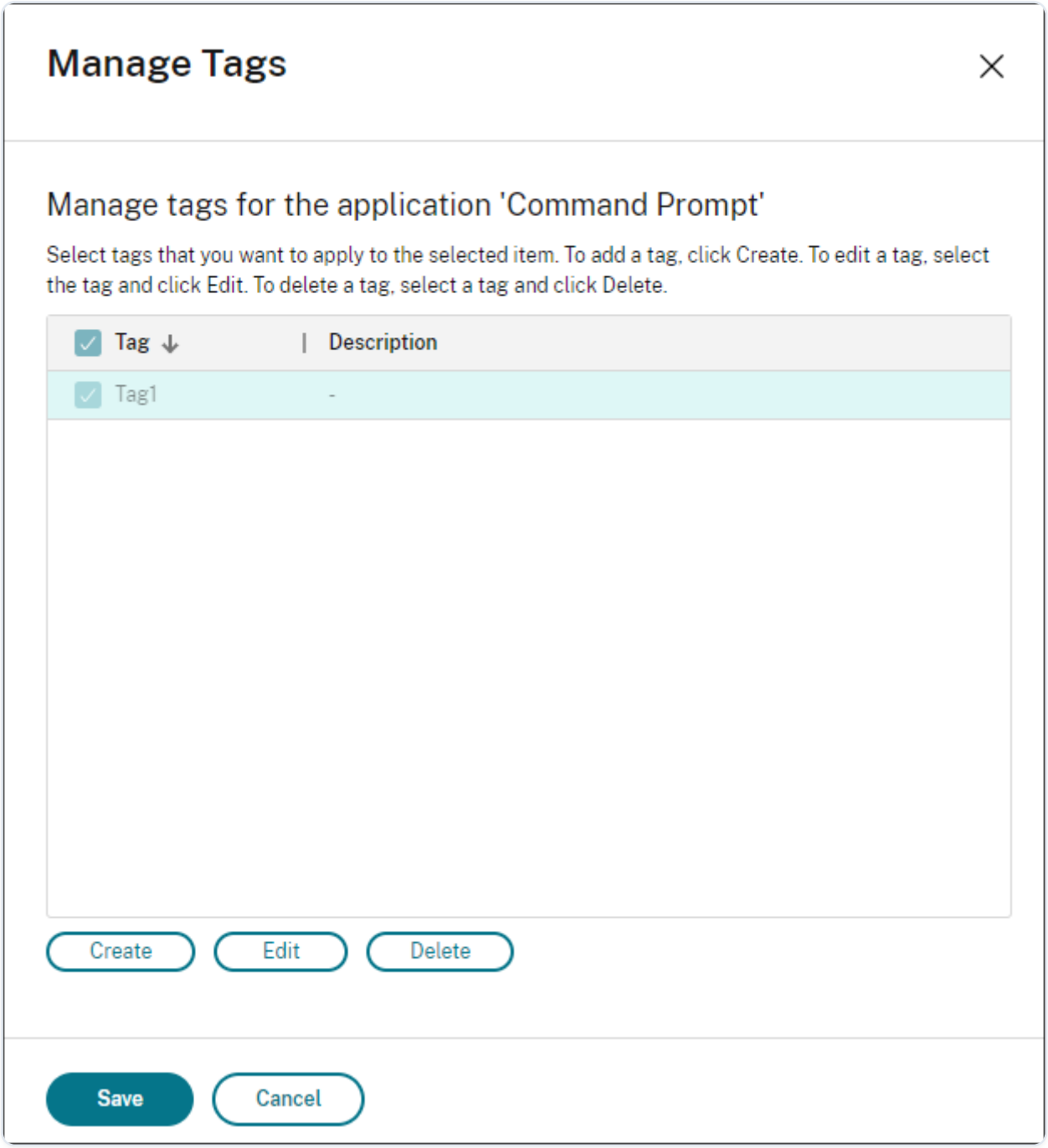
（例外：ポリシー割り当てに使用されるタグは、Web Studioの**［タグの管理］**アクションを通じて作成、編集、削除されます。ただし、タグはポリシーの作成時に適用（割り当て）されます。詳細については、「ポリシーの作成」を参照してください。）

タグ制限は、デリバリーグループでデスクトップを作成または編集するとき、およびアプリケーショングループを作成および編集するときに構成されます。

Web Studioで［タグの管理］ダイアログを使用する

Web Studioで、タグを適用するアイテム（1つまたは複数のマシン、アプリケーション、デスクトップ、デリバリーグループ、またはアプリケーショングループ）を選択し、アクションバーで**［タグの管理］**を選択します。ダイアログボックスには、選択したアイテムだけでなく、サイトで作成されたすべてのタグが一覧表示されます。

- チェックマークが付いたチェックボックスは、そのタグが選択したアイテムに既に追加されていることを示します。（以下のスクリーンショットでは、選択したマシンに「Tag1」という名前のタグが適用されています。）
- 複数のアイテムを選択した場合、ハイフンが付いたチェックボックスは、選択したアイテムの一部にのみそのタグが追加されていることを示します。



次のアクションは、**［タグの管理］**ダイアログボックスから利用できます。タグの操作に関する注意点を必ず確認してください。

- **タグを作成するには:**

  作成をクリックします。名前と説明を入力します。タグ名は一意である必要があり、大文字と小文字は区別されません。次に、**OK**をクリックします。（タグを作成しても、選択した項目に自動的に適用されるわけではありません。チェックボックスを使用してタグを適用します。）

- **1つ以上のタグを追加（適用）するには:**

タグ名の横にあるチェックボックスをオンにします。複数の項目を選択していて、タグの横にあるチェックボックスにハイフンが含まれている場合（選択した項目の一部にのみタグが適用されていることを示す）、それをチェックマークに変更すると、選択したすべてのマシンに影響します。

1つ以上のマシンにタグを追加しようとして、そのタグがアプリケーショングループで制限として使用されている場合、その操作によってそれらのマシンが起動可能になる可能性があるという警告が表示されます。それが意図したとおりであれば、続行してください。

- **1つ以上のタグを削除するには:**

  タグ名の横にあるチェックボックスをオフにします。複数の項目を選択していて、タグの横にあるチェックボックスにハイフンが含まれている場合（選択した項目の一部にのみタグが適用されていることを示す）、チェックボックスをオフにすると、選択したすべてのマシンからタグが削除されます。

  タグを制限として使用しているマシンからタグを削除しようとすると、その操作が起動対象となるマシンに影響を与える可能性があるという警告が表示されます。それが意図したとおりであれば、続行してください。

- **タグを編集するには:**

  タグを選択し、**編集**をクリックします。新しい名前、説明、またはその両方を入力します。一度に編集できるタグは1つだけです。

- **1つ以上のタグを削除するには:**

  タグを選択し、**削除**をクリックします。「タグの削除」ダイアログボックスには、現在選択されているタグを使用している項目の数が表示されます（例：「2台のマシン」）。項目をクリックすると、詳細情報が表示されます。たとえば、「2台のマシン」項目をクリックすると、そのタグが適用されている2台のマシンの名前が表示されます。タグを削除するかどうかを確認します。

  Web Studioを使用して、制限として使用されているタグを削除することはできません。まず、アプリケーショングループを編集してタグ制限を削除するか、別のタグを選択してください。

タグの管理ダイアログボックスでの作業が完了したら、**保存**をクリックします。

マシンにタグが適用されているかどうかを確認するには、左ペインで**デリバリーグループ**を選択します。中央ペインでデリバリーグループを選択し、アクションバーで**マシンの表示**を選択します。中央ペインでマシンを選択し、**詳細**ペインで**タグ**タブを選択します。

タグ制限を管理する

タグ制限の構成は複数の手順からなるプロセスです。まずタグを作成し、それをマシンに追加/適用します。次に、アプリケーショングループまたはデスクトップに制限を追加します。

- **タグを作成して適用する：**

  タグを作成し、前述の**タグの管理**アクションを使用して、タグ制限の影響を受けるマシンにそのタグを追加（適用）します。

- **アプリケーショングループにタグ制限を追加するには：**

  アプリケーショングループを作成または編集します。**デリバリーグループ**ページで、**タグを持つマシンへの起動を制限する**を選択し、リストからタグを選択します。

- **アプリケーショングループのタグ制限を変更または削除するには：**

  グループを編集します。**デリバリーグループ**ページで、リストから別のタグを選択するか、**タグを持つマシンへの起動を制限する**のチェックを外してタグ制限を完全に削除します。

- **デスクトップにタグ制限を追加するには：**

  デリバリーグループを作成または編集します。**デスクトップ**ページで、**追加**または**編集**をクリックします。「デスクトップの追加」ダイアログボックスで、**タグを持つマシンへの起動を制限する**を選択し、メニューからタグを選択します。

- **デリバリーグループのタグ制限を変更または削除するには：**

  グループを編集します。デスクトップページで、**編集**をクリックします。ダイアログボックスで、リストから別のタグを選択するか、**タグを持つマシンへの起動を制限する**のチェックを外してタグ制限を完全に削除します。

タグを使用する際の注意点

アイテムに適用されたタグはさまざまな目的に使用できるため、タグの追加、削除、および削除が意図しない影響を与える可能性があることに留意してください。Web Studioの検索フィールドでマシンの表示を並べ替えるためにタグを使用できます。アプリケーショングループまたはデスクトップを構成する際に、同じタグを制限として使用できます。タグは、そのタグを持つ指定されたデリバリーグループ内のマシンのみに起動の考慮を制限します。

デスクトップまたはアプリケーショングループのタグ制限として構成されたタグをマシンに追加しようとすると、警告が表示されます。そのタグを追加すると、マシンが追加のアプリケーションまたはデスクトップの起動に利用可能になる可能性があります。それが意図したものであれば、続行してください。そうでない場合は、操作をキャンセルできます。

例えば、「Red」タグ制限付きのアプリケーショングループを作成したとします。その後、そのアプリケーショングループで使用されているのと同じデリバリーグループに、さらにいくつかのマシンを追加します。そのマシンに「Red」タグを追加しようとすると、Web Studioは次のようなメッセージを表示します。「タグ「Red」は、以下のアプリケーショングループの制限として使用されています。このタグを追加すると、選択したマシンがこのアプリケーショングループでアプリケーションを起動できるようになる可能性があります。」その後、それらの追加マシンにそのタグを追加するかどうかを確認またはキャンセルできます。

同様に、アプリケーショングループが起動を制限するためにタグを使用している場合、Web Studioは、そのタグを制限として削除するためにグループを編集するまで、タグを削除できないことを警告します。（アプリケーショングループで制限として使用されているタグを削除することが許可された場合、そのアプリケーショングループに関連付けられているデリバリーグループ内のすべてのマシンでアプリケーションの起動が許可される可能性があります。）デスクトップの起動の制限としてタグが使用されている場合も、タグの削除に対する同じ禁止が適用されます。そのタグ制限を削除するために、アプリケーショングループまたはデリバリーグループ内のデスクトップを編集した後、タグを削除できます。

すべてのマシンが同じアプリケーションセットを持っているとは限りません。ユーザーは複数のアプリケーショングループに属することができ、それぞれ異なるタグ制限と、デリバリーグループからの異なるまたは重複するマシンセットを持っています。以下の表は、マシンの考慮事項がどのように決定されるかを示しています。

アプリケーションが追加された場合	選択されたデリバリーグループ内のこれらのマシンが起動対象と見なされます
タグ制限のない1つのアプリケーショングループ	任意のマシン。
タグ制限Aのある1つのアプリケーショングループ	タグAが適用されているマシン。
2つのアプリケーショングループ（1つはタグ制限A、もう1つはタグ制限B）	タグAとタグBを持つマシン。利用可能なマシンがない場合は、タグAまたはタグBを持つマシン。
2つのアプリケーショングループ（1つはタグ制限A、もう1つはタグ制限なし）	タグAを持つマシン。利用可能なマシンがない場合は、任意のマシン。

マシン再起動スケジュールでタグ制限を使用した場合、タグの適用または制限に影響を与える変更は、次のマシン再起動サイクルに影響します。変更が行われている間に進行中の再起動サイクルには影響しません。

例2の構成方法

以下の手順では、タグを作成して適用し、2番目の例で示されているアプリケーショングループのタグ制限を構成する手順を示します。

VDAとアプリケーションはすでにマシンにインストールされており、デリバリーグループも作成されています。

マシンにタグを作成して適用します。

1. Web Studioで、デリバリーグループD01を選択し、アクションバーで**マシンを表示**を選択します。
2. マシンVDA 101～105を選択し、アクションバーで**タグの管理**を選択します。
3. タグの管理ダイアログボックスで、**作成**をクリックし、`CADApps`という名前のタグを作成します。**OK**をクリックします。
4. もう一度**作成**をクリックし、OfficeAppsという名前のタグを作成します。**OK**をクリックします。
5. **タグの管理**ダイアログボックスにいる間に、新しく作成したタグを、各タグの名前（`CADApps`と`OfficeApps`）の横にあるチェックボックスを有効にすることで、選択したマシンに追加（適用）します。完了したら、ダイアログボックスを閉じます。
6. デリバリーグループD01を選択し、アクションバーで**マシンを表示**を選択します。
7. マシンVDA 106～110を選択し、アクションバーで**タグの管理**を選択します。
8. **タグの管理**ダイアログボックスで、**作成**をクリックします。`AcctgApps`という名前のタグを作成します。**OK**をクリックします。
9. 新しく作成した`AcctgApps`タグと`OfficeApps`タグを、各タグ名の横にあるチェックボックスをクリックして、選択したマシンに適用し、ダイアログボックスを閉じます。

タグ制限付きのアプリケーショングループを作成します。

1. Web Studioで、左ペインの**アプリケーション**を選択し、**アプリケーショングループ**タブを選択し、アクションバーで**アプリケーショングループの作成**を選択します。アプリケーショングループ作成ウィザードが起動します。
2. ウィザードの**デリバリーグループ**ページで、デリバリーグループD01を選択します。**タグを持つマシンへの起動を制限する**を選択し、リストから`AcctgApps`タグを選択します。
3. ウィザードを完了し、会計ユーザーと会計アプリケーションを指定します。(アプリケーションを追加する際は、`AcctgApps`タグを持つマシン上のアプリケーションを検索する****ソースを選択します。) ****ページで、グループに`A100`という名前を付けます。

4. 前述の手順を繰り返して、`CADApps`タグを持つマシンと、適切なユーザーおよびアプリケーションを指定し、アプリケーショングループ`A200`を作成します。
5. 手順を繰り返して、`OfficeApps`タグを持つマシンと、適切なユーザーおよびアプリケーションを指定し、アプリケーショングループ`A300`を作成します。

マシンカタログのタグ

マシンカタログでタグを使用できます。タグを作成してカタログに適用する全体的な手順は、前述のとおりです。ただし、カタログへのタグの適用はPowerShellインターフェイスを介してのみサポートされています。Web Studioを使用してカタログにタグを適用したり、カタログからタグを削除したりすることはできません。Web Studioのカタログ表示では、タグが適用されているかどうかは示されません。

概要: Web StudioまたはPowerShellを使用して、カタログで使用するタグを作成または削除できます。PowerShellを使用して、タグをカタログに適用します。

カタログでタグを使用する例をいくつか示します。

- デリバリーグループには複数のカタログのマシンが含まれていますが、特定のカタログ内のマシンのみに操作（再起動スケジュールなど）を適用したい場合があります。そのカタログにタグを適用することで、これが実現します。
- アプリケーショングループでは、アプリケーションセッションを特定のカタログ内のマシンに制限したい場合があります。そのカタログにタグを適用することで、これが実現します。

影響を受けるPowerShellコマンドレット:

- `Add-BrokerTag`や`Remove-BrokerTag`などのコマンドレットにカタログオブジェクトを渡すことができます。
- `Get-BrokerTagUsage`は、タグを含むカタログの数を示します。
- `Get-BrokerCatalog`には、`Tags`という名前のプロパティがあります。

たとえば、次のコマンドレットは、`acctg`という名前のカタログに`fy2018`という名前のタグを追加します。`Get-BrokerCatalog -Name acctg | Add-BrokerTag fy2018`。(このタグは、以前にWeb StudioまたはPowerShellを使用して作成されています。)

詳細なガイダンスと構文については、PowerShellコマンドレットのヘルプを参照してください。

自動タグ (プレビュー)

自動タグ付けにより、管理者はカスタムルールに基づいて、さまざまなCitrix Virtual Apps and Desktopsオブジェクトにタグを自動的に設定および削除できます。この機能強化により、環境最適化のために定期的に実行されるさまざまなスクリプトを維持する必要がなくなります。

ユースケース

自動タグ付けを使用すると、コスト削減、インフラストラクチャの最適化、消費の促進など、ビジネスドライバーに関連するルールを実装できます。以下にいくつかのユースケースを示します。

- **未使用のVDIを再利用** - 事前設定された日数以上使用されていない専用ワークロードを、利用可能なプールに解放するため。
- **アプリの煩雑さを解消** - 事前設定された日数以上使用されていないアプリケーションを特定することで、アプリケーションの煩雑さを軽減するため。
- **X未満の機能レベルを持つDG** - 特定の機能レベル未満のデリバリーグループを見つけるため。
- **非アクティブユーザー** - 事前設定された日数以上ログオンしていないユーザーのリソースを再利用するため。

PowerShellコマンド

PowerShellコマンドを使用して自動タグを作成できます。自動タグルールが作成されると、600秒の頻度で評価されます。詳細については、New-BrokerAutoTagRuleを参照してください。

例

`New-BrokerAutoTagRule`は、`Get-BrokerMachine`コマンドレットと同じオブジェクトタイプとフィルターパラメーターを使用します。詳細については、GetBrokerMachineを参照してください。

1. 30日以上使用されていない専用VDIにID 123でタグ付けします。
    a. 未使用のVDIにタグ付けするためのタグを定義します。例えば、**unused-VDI**です。
        - タグ名 : unused-VDI
        - タグID : 123
    b. 未使用のマシンにタグ付けするための自動タグ付けルールを作成します。ルールパラメーターを定義します。
        - 名前 : ルールの一般的な名前。
        - オブジェクトタイプ : マシン。

- ルールテキスト : 静的で、最終接続時間が30日を超えるか、値がない割り当て済みマシン。
- タグUID : 関連付けたいタグID、123。

```
New-BrokerAutoTagRule -Name ‘UnusedVdi’ -ObjectType ‘Machine’ -RuleText “-AllocationType Static -IsAssigned $true -Filter { SummaryState -ne `”InUse`” -and ( LastConnectionTime -lt ‘-30’ -or LastConnectionTime -eq `$null ) }” -TagUid 123
```

c. **unused-VDI**タグが付けられたマシンを確認し、それらを解放します。

2. X未満の機能レベルを持つデリバリーグループにタグを付けるには (**L7_20** をしきい値機能レベルとして使用):

```
New-BrokerAutoTagRule -Name 'LowFL' -ObjectType 'DesktopGroup' -RuleText "-Filter { MinimumFunctionalLevel -lt 'L7_20' } " -TagUid 123
```

1. フォルダーなしで公開された、ユーザーに表示されるアプリにタグを付けるには:

```
New-BrokerAutoTagRule -Name 'NoFolder' -ObjectType 'Application' -RuleText "-Enabled $true -Filter { ClientFolder -eq $null )} " -TagUid 123
```

詳細情報

ブログ投稿: 特定のサーバーにデスクトップを割り当てる方法。

ユーザープロファイル

デフォルトでは、Virtual Delivery Agentをインストールすると、Citrix Profile Managementはマスターイメージにサイレントインストールされますが、プロファイルソリューションとしてProfile Managementを使用する必要はありません。

ユーザーのさまざまなニーズに合わせて、Citrix Virtual Apps and Desktops™ポリシーを使用して、各デリバリーグループのマシンに異なるプロファイル動作を適用できます。たとえば、あるデリバリーグループでは、テンプレートが1つのネットワークロケーションに保存されているCitrix強制プロファイルが必要な場合があります。一方、別のデリバリーグループでは、複数のリダイレクトされたフォルダーを持つ別のロケーションに保存されているCitrixローミングプロファイルが必要な場合があります。

- 組織内の他の管理者がCitrix Virtual Apps and Desktopsのポリシーを担当している場合は、Delivery Group全体でプロファイル関連のポリシーが設定されていることを確認するために、彼らと協力してください。

- Profile Managementポリシーは、グループポリシー、Profile Management .iniファイル、および個々の仮想マシン上でローカルに設定することもできます。プロファイル動作を定義するこれらの複数の方法は、次の順序で読み取られます。

  a. グループポリシー（.admまたは.admxファイル）

  b. ポリシーノード内のCitrix Virtual Apps and Desktopsポリシー

  c. ユーザーが接続する仮想マシン上のローカルポリシー

  d. Profile Management .iniファイル

  たとえば、グループポリシーとポリシーノードの両方で同じポリシーを構成した場合、システムはグループポリシーのポリシー設定を読み取り、Citrix Virtual Apps and Desktopsポリシー設定を無視します。

どのプロファイルソリューションを選択しても、Director管理者は診断情報にアクセスし、ユーザープロファイルのトラブルシューティングを行うことができます。詳細については、Directorのドキュメントを参照してください。

自動構成

デスクトップの種類は、Virtual Delivery Agentのインストールに基づいて自動的に検出され、Studioで行う構成の選択に加えて、それに応じてProfile Managementのデフォルトを設定します。

Profile Managementが調整するポリシーを次の表に示します。デフォルト以外のポリシー設定はすべて保持され、この機能によって上書きされることはありません。各ポリシーの詳細については、Profile Managementのドキュメントを参照してください。プロファイルを作成するマシンの種類は、調整されるポリシーに影響します。主な要因は、マシンが永続的かプロビジョニング済みか、および複数のユーザーで共有されるか、1人のユーザー専用であるかです。

永続システムには何らかのローカルストレージがあり、その内容はシステムがオフになっても永続することが期待されます。永続システムは、SANなどのストレージテクノロジーを使用して、ローカルディスクのエミュレーションを提供する場合があります。対照的に、プロビジョニングシステムは、ベースディスクと何らかのIDディスクから「オンザフライ」で作成されます。ローカルストレージは通常、RAMディスクまたはネットワークディスクによってエミュレートされ、後者は高速リンクを備えたSANによって提供されることがよくあります。プロビジョニングテクノロジーは通常、Citrix ProvisioningまたはMachine Creation Services™（あるいはサードパーティの同等品）です。プロビジョニングシステムが永続的なローカルストレージを持つこともあります。これらは永続的として分類されます。

これら2つの要素を合わせると、以下のマシンタイプが定義されます。

- **永続的かつ専用**。例としては、Machine Creation Servicesで作成された静的割り当てと永続的なローカルストレージを持つシングルセッションOSマシン、物理ワークステーション、ラップトップなどがあります。
- **永続的かつ共有**。例としては、Machine Creation Servicesで作成されたマルチセッションOSマシン、およびCitrix Virtual Appsサーバーなどがあります。
- **プロビジョニング済みかつ専用**。例としては、静的割り当てを持つが永続ストレージを持たないシングルセッションOSマシンで、Citrix Provisioning Service (Citrix Virtual Desktops™内) で作成されたものなどがあります。
- **プロビジョニング済みかつ共有**。例としては、ランダム割り当てを持つシングルセッションOSマシンで、Citrix Provisioning™ Service (Citrix Virtual Desktops内) で作成されたもの、およびCitrix Virtual Appsサーバーなどがあります。

以下のProfile Managementポリシー設定は、異なるマシンタイプに対する推奨ガイドラインです。ほとんどの場合にうまく機能しますが、展開の要件に応じてこれらから逸脱することもできます。

> **重要:**
>
> **ログオフ時にローカルにキャッシュされたプロファイルを削除**、**プロファイルストリーミング**、および**常にキャッシュ**は、自動構成機能によって適用されます。その他のポリシーは手動で調整してください。

永続マシン

ポリシー	永続的かつ専用	永続的かつ共有
ログオフ時にローカルにキャッシュされたプロファイルを削除する	無効	有効
プロファイルストリーミング	無効	有効
常にキャッシュ	有効 (注1)	無効 (注2)
アクティブライトバック	無効	無効 (注3)
ローカル管理者によるログオンの処理	有効	無効 (注4)

プロビジョニング済みマシン

ポリシー	プロビジョニング済みと専用の両方	プロビジョニング済みと共有の両方
ログオフ時にローカルにキャッシュされたプロファイルを削除する	無効 (注5)	有効
プロファイルストリーミング	有効	有効
常にキャッシュ	無効 (注6)	無効
アクティブライトバック	有効	有効
ローカル管理者によるログオンの処理	有効	有効 (注7)

1. このマシンタイプでは**Profile streaming**が無効になっているため、**Always cache**設定は常に無視されます。
2. **Always cache**を無効にします。ただし、このポリシーを有効にし、ファイルサイズ制限 (MB単位) を定義することで、ログオン後できるだけ早く大きなファイルがプロファイルにロードされるようにすることができます。このサイズ以上のファイルは、できるだけ早くローカルにキャッシュされます。
3. Citrix Virtual Appsサーバー間をローミングするユーザーのプロファイルに変更を保存する場合を除き、**Active write back**を無効にします。この場合は、このポリシーを有効にします。
4. ホスト型共有デスクトップの場合を除き、**Process logons of local administrators**を無効にします。この場合は、このポリシーを有効にします。
5. **Delete locally cached profiles on logoff**を無効にします。この設定は、ローカルにキャッシュされたプロファイルを保持します。マシンはログオフ時にリセットされますが、個々のユーザーに割り当てられているため、プロファイルがキャッシュされているとログオンが高速になります。
6. **Always cache**を無効にします。ただし、このポリシーを有効にし、ファイルサイズ制限 (MB単位) を定義することで、ログオン後できるだけ早く大きなファイルがプロファイルにロードされるようにすることができます。このサイズ以上のファイルは、できるだけ早くローカルにキャッシュされます。

7. Citrix Virtual Apps and Desktopsサーバー間をローミングするユーザーのプロファイルの場合を除き、**Process logons of local administrators**を有効にします。この場合は、このポリシーを無効にします。

フォルダーリダイレクト

フォルダーリダイレクトを使用すると、プロファイルが保存されている場所とは異なるネットワーク共有にユーザーデータを保存できます。フォルダーリダイレクトはプロファイルのサイズとロード時間を削減しますが、ネットワーク帯域幅に影響を与える可能性があります。フォルダーリダイレクトは、Citrixユーザープロファイルが使用されていることを必要としません。独自のユーザープロファイルを管理し、フォルダーをリダイレクトすることもできます。

StudioのCitrixポリシーを使用してフォルダーリダイレクトを構成します。

- リダイレクトされたフォルダーのコンテンツを保存するために使用されるネットワークの場所が利用可能であり、適切な権限を持っていることを確認してください。場所のプロパティは検証されます。
- リダイレクトされたフォルダーはネットワーク上に設定され、その内容はログオン時にユーザーの仮想デスクトップから取り込まれます。

フォルダーリダイレクトは、CitrixポリシーまたはActive Directoryグループポリシーオブジェクトのいずれか一方のみを使用して構成し、両方は使用しないでください。両方のポリシーエンジンを使用してフォルダーリダイレクトを構成すると、予期しない動作が発生する可能性があります。

高度なフォルダーリダイレクト

複数のオペレーティングシステム（OS）を使用する展開では、ユーザープロファイルの一部を各OSで共有したい場合があります。プロファイルの残りの部分は共有されず、1つのOSでのみ使用されます。OS間で一貫したユーザーエクスペリエンスを確保するには、各OSで異なる構成、つまり高度なフォルダーリダイレクトが必要です。たとえば、2つのOSで実行されているアプリケーションの異なるバージョンが共有ファイルを読み取ったり編集したりする必要がある場合、両方のバージョンがアクセスできる単一のネットワーク場所にリダイレクトすることを選択できます。あるいは、**スタートメニュー**フォルダーの内容が2つのOSで異なる構造になっているため、両方ではなく1つのフォルダーのみをリダイレクトすることを選択できます。このアプローチにより、各OSで**スタートメニュー**フォルダーとその内容が分離され、ユーザーに一貫したエクスペリエンスが保証されます。

展開で高度なフォルダーリダイレクトが必要な場合は、ユーザーのプロファイルデータの構造を理解し、そのどの部分をOS間で共有できるかを判断する必要があります。フォルダーリダイレクトが正しく使用されないと、予期しない動作が発生する可能性があります。

高度な展開でフォルダーをリダイレクトするには：

- 各OSに個別のデリバリーグループを使用します。
- 仮想デスクトップ上の仮想アプリケーションを含む、仮想アプリケーションがユーザーデータと設定をどこに保存するか、およびデータがどのように構造化されているかを理解します。
- 安全にローミングできる共有プロファイルデータ（各OSで同じ構造であるため）については、各デリバリーグループ内のコンテナフォルダーをリダイレクトします。
- ローミングできない非共有プロファイルデータについては、デスクトップグループのいずれか1つ（通常は最も使用されているOSまたはデータが最も関連性の高いOS）のコンテナフォルダーをリダイレクトします。あるいは、OS間でローミングできない非共有データについては、両方のシステムのコンテナフォルダーを別々のネットワーク場所にリダイレクトします。

高度な展開の例

この展開には、Windows 10デスクトップで実行されるMicrosoft OutlookおよびInternet Explorerのバージョンを含むアプリケーションと、Windows Server 2019によって配信されるOutlookおよびInternet Explorerの他のバージョンを含むアプリケーションがあります。2つのOS用に2つのデリバリーグループを既に設定しています。ユーザーは、両方のアプリケーションのバージョンで同じ**連絡先**と**お気に入り**のセットにアクセスしたいと考えています。

重要： 以下の決定とアドバイスは、説明されているOSと展開に有効です。組織では、リダイレクトするフォルダーとそれらを共有するかどうかの決定は、特定の展開に固有のさまざまな要因によって異なります。

- デリバリーグループに適用されるポリシーを使用して、次のフォルダーをリダイレクトするように選択します。

フォルダ	WINDOWS 10でリダイレクトされますか？	WINDOWS SERVER 2019でリダイレクトされますか？
マイドキュメント	はい	はい
アプリケーションデータ	いいえ	いいえ
連絡先	はい	はい
デスクトップ	はい	いいえ
ダウンロード	いいえ	いいえ
お気に入り	はい	はい

フォルダ	WINDOWS 10でリダイレクトされますか？	WINDOWS SERVER 2019でリダイレクトされますか？
リンク	はい	いいえ
マイミュージック	はい	はい
マイピクチャ	はい	はい
マイビデオ	はい	はい
検索	はい	いいえ
保存されたゲーム	いいえ	いいえ
スタートメニュー	はい	いいえ

- 共有され、リダイレクトされるフォルダーの場合：
  - OutlookとInternet Explorerの異なるバージョンによって保存されたデータの構造を分析した結果、**連絡先**フォルダーと**お気に入り**フォルダーを共有しても安全であると判断しました。
  - **マイドキュメント**、**マイミュージック**、**マイピクチャ**、**マイビデオ**フォルダーの構造はOS間で標準的であることがわかっています。そのため、これらのフォルダーを各デリバリーグループで同じネットワークロケーションに保存しても安全です。
- 共有されない、リダイレクトされるフォルダーの場合：
  - Windows Serverデリバリーグループでは、デスクトップ、リンク、検索、または**スタートメニュー**フォルダーをリダイレクトしません。これらのフォルダー内のデータは2つのOSで異なる方法で整理されているためです。したがって、共有することはできません。
  - この共有されないデータの予測可能な動作を保証するために、Windows 10デリバリーグループでのみリダイレクトします。Windows 10は、ユーザーが日常業務でより頻繁に使用します。ユーザーはWindows Serverによって提供されるアプリケーションにたまにしかアクセスしません。また、この場合、共有されないデータはアプリケーション環境よりもデスクトップ環境により関連性が高くなります。たとえば、デスクトップショートカットは**デスクトップ**フォルダーに保存され、Windows 10マシンから作成されたものであれば役立つ可能性がありますが、Windows Serverマシンから作成されたものではありません。
- リダイレクトされないフォルダーの場合:

- ユーザーがダウンロードしたファイルでサーバーを煩雑にしたくないため、ダウンロードフォルダーをリダイレクトしないことを選択します
- 個々のアプリケーションからのデータは互換性やパフォーマンスの問題を引き起こす可能性があるため、アプリケーションデータフォルダーをリダイレクトしないことを決定します

フォルダーリダイレクトの詳細については、「フォルダーリダイレクト、オフラインファイル、および移動ユーザープロファイルの概要」を参照してください。

フォルダーリダイレクトと除外

Citrix Profile Management（Studioではない）では、パフォーマンス強化により、除外を使用してフォルダーが処理されないようにすることができます。この機能を使用する場合、リダイレクトされたフォルダーを除外しないでください。フォルダーリダイレクト機能と除外機能は連携して動作します。リダイレクトされたフォルダーが除外されないようにすることで、後でリダイレクトしないと決定した場合でも、Profile Managementはそれらをプロファイルフォルダー構造に戻し、データの整合性を維持できます。除外の詳細については、「項目の含める/除外」を参照してください。

VDA登録

はじめに

> **注：**
>
> オンプレミス環境では、VDAはDelivery Controllerに登録します。Citrix Cloudサービス環境では、VDAはCloud Connectorに登録します。ハイブリッド環境では、一部のVDAはDelivery Controllerに登録し、他のVDAはCloud Connectorに登録します。

> VDAを使用する前に、サイト上の1つ以上のControllerまたはCloud Connectorに登録（通信を確立）する必要があります。VDAは、`ListofDDCs`と呼ばれるリストを確認して、ControllerまたはConnectorを見つけます。VDA上の`ListOfDDCs`には、そのVDAをサイト上のControllerまたはCloud Connectorにポイントするエントリが含まれています。負荷分散のために、VDAはリスト内のすべてのControllerまたはCloud Connectorに接続を自動的に分散します。

VDA登録がそれほど重要であるのはなぜですか？

- セキュリティの観点から見ると、登録は機密性の高い操作です。ControllerまたはCloud ConnectorとVDAの間に接続を確立しています。このような機密性の高い操作では、すべてが完璧な状態でない場合、接続を拒否するのが期待される動作です。事実上、VDAからControllerまたはCloud Connectorへ、そしてControllerまたはCloud ConnectorからVDAへの2つの別々の通信チャネルを確立しています。接続にはKerberosが使用されるため、時刻同期やドメインメンバーシップの問題は許容されません。Kerberosはサービスプリンシパル名 (SPN) を使用するため、負荷分散されたIP\ホスト名は使用できません。
- Controller（またはCloud Connector）を追加および削除する際に、VDAが正確で最新のControllerまたはCloud Connector情報を持っていない場合、VDAは、リストにないControllerまたはCloud Connectorによって仲介されるセッション起動を拒否する可能性があります。無効なエントリは、仮想デスクトップシステムソフトウェアの起動を遅らせる可能性があります。VDAは、不明で信頼できないControllerまたはCloud Connectorからの接続を受け入れません。

`ListofDDCs`に加えて、`ListOfSIDs`（セキュリティID）は、`ListofDDCs`内のどのマシンが信頼されているかを示します。`ListofSIDs`は、Active Directoryの負荷を軽減したり、侵害されたDNSサーバーからの潜在的なセキュリティ脅威を回避したりするために使用できます。詳細については、ListOfSIDsを参照してください。

`ListofDDCs`が複数のControllerまたはCloud Connectorを指定している場合、VDAはランダムな順序でそれらに接続しようとします。オンプレミス展開では、`ListofDDCs`にはControllerグループも含まれる場合があります。VDAは、`ListofDDCs`内の他のエントリに移動する前に、グループ内の各Controllerに接続しようとします。

Citrix Virtual Apps and Desktops™は、VDAのインストール中に構成されたControllerまたはCloud Connectorへの接続を自動的にテストします。ControllerまたはCloud Connectorに到達できない場合、エラーが表示されます。ControllerまたはCloud Connectorに接続できないという警告を無視した場合（またはVDAのインストール中にControllerまたはCloud Connectorのアドレスを指定しなかった場合）、メッセージが表示されて通知されます。

ControllerまたはCloud Connectorアドレスを構成する方法

管理者は、VDAが初めて登録するとき（初回登録）に使用する構成方法を選択します。初回登録中に、VDA上に永続的なキャッシュが作成されます。その後の登録では、構成の変更が検出されない限り、VDAはこのローカルキャッシュからControllerまたはCloud Connectorのリストを取得します。

その後の登録でそのリストを取得する最も簡単な方法は、自動更新機能を使用することです。自動更新はデフォルトで有効になっています。詳細については、「自動更新」を参照してください。

VDA上でControllerまたはCloud Connectorアドレスを構成する方法はいくつかあります。

- ポリシーベース（LGPOまたはGPO）
- レジストリベース（手動、グループポリシー設定（GPP）、VDAインストール時に指定）
- Active Directory OUベース（レガシーOU検出）
- MCSベース (personality.ini)

VDAをインストールする際に、初期登録方法を指定します。(自動更新を無効にした場合、VDAインストール時に選択した方法がその後の登録に使用されます。)

次の図は、VDAインストールウィザードの**Delivery Controller**ページを示しています。

VDAインストールウィザードのDelivery Controllerページ(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/vda-install-controllers-all.png)

ポリシーベース (LGPO\\GPO)

Citrix®は、初期VDA登録にGPOを使用することを推奨します。これは最も高い優先順位を持ちます。(自動更新が最も高い優先順位としてリストされていますが、自動更新は初期登録後にのみ使用されます。) ポリシーベースの登録は、構成にグループポリシーを使用することによる一元化の利点を提供します。

この方法を指定するには、以下の両方の手順を完了します。

- VDAインストールウィザードの**Delivery Controller**ページで、**後で実行 (詳細設定)** を選択します。VDAインストール中にControllerアドレスを指定しない場合でも、ウィザードはControllerアドレスを指定するよう何度か通知します。(VDA登録はそれほど重要です。)
- `Virtual Delivery Agent Settings > Controllers`設定を使用して、Citrixポリシーを介してポリシーベースのVDA登録を有効または無効にします。(セキュリティが最優先事項である場合は、`Virtual Delivery Agent Settings > Controller SIDs`設定を使用します。)

この設定は`HKLM\Software\Policies\Citrix\VirtualDesktopAgent (ListOfDDCs)`に保存されます。

レジストリベース

この方法を指定するには、以下のいずれかの手順を完了します。

- VDAインストールウィザードの**Delivery Controller**ページで、**手動で実行** を選択します。次に、インストールされているControllerのFQDNを入力し、**追加** をクリックします。複数のControllerをインストールしている場合は、それらのアドレスを追加します。
- コマンドラインVDAインストールの場合、/controllersオプションを使用し、インストールされているControllerまたはCloud ConnectorのFQDNを指定します。

この情報は、レジストリキー`HKLM\Software\Citrix\VirtualDesktopAgent`または`HKLM\Software\Wow6432Node\Citrix\VirtualDesktopAgent`の下のレジストリ値`ListOfDDCs`に保存されます。

このレジストリキーを手動で構成することも、グループポリシー設定 (GPP) を使用することもできます。この方法は、ポリシーベースの方法よりも好ましい場合があります (たとえば、異なるControllerまたはCloud Connectorの条件付き処理が必要な場合。例: XDW-001-で始まるコンピューター名にはXDC-001を使用する)。

`ListOfDDCs` レジストリキーを更新します。このキーには、サイト内のすべてのControllerまたはCloud ConnectorのFQDNが一覧表示されます。(このキーはActive DirectoryサイトOUに相当します。)

`HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent\ListOfDDCs (REG_SZ)`

もし`HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent`レジストリの場所に`ListOfDDCs`と`FarmGUID`の両方のキーが含まれている場合、ControllerまたはCloud Connectorの検出には`ListOfDDCs`が使用されます。VDAのインストール時にサイトOUが指定された場合、`FarmGUID`が存在します。(これはレガシー展開で使用される場合があります。)

オプションで、`ListOfSIDs` レジストリキーを更新します (詳細については、「ListOfSIDs」を参照してください)。

`HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent\ListOfSIDs (REG_SZ)`

注意: Citrixポリシーを介してポリシーベースのVDA登録も有効にすると、VDAインストール時に指定した設定が上書きされます。これは、ポリシーベースの登録の方が優先度の高い方法であるためです。

Active Directory OUベース (レガシー)

この方法は主に下位互換性のためにサポートされており、推奨されません。まだこの方法を使用している場合は、別の方法に変更することをお勧めします。

この方法を指定するには、以下の両方の手順を完了します。

- VDAインストールウィザードの **Delivery Controller** ページで、**Active Directoryから場所を選択** を選択します。
- `Set-ADControllerDiscovery.ps1` スクリプト (すべてのControllerで利用可能) を使用します。また、各VDAで `FarmGuid` レジストリエントリを構成して、適切なOUを指すようにします。この設定はグループポリシーを使用して構成できます。

MCSベース

MCSを使用してVMをプロビジョニングする場合、MCSはControllerまたはCloud Connectorのリストを設定します。この機能は自動更新と連携します。カタログの作成時、MCSは初期プロビジョニング中にControllerまたはCloud Connectorのリストを `Personality.ini` ファイルに挿入します。自動更新により、リストは最新の状態に保たれます。

この方法を指定するには、VDAインストールウィザードの **Delivery Controller** ページで、**Machine Creation Services™に任せる** を選択します。

レビューと推奨事項

ベストプラクティスとして:

- 初期登録にはグループポリシー登録方法を使用します。
- 自動更新（デフォルトで有効）を使用して、Controller のリストを最新の状態に保ちます。
- マルチゾーン展開では、初期構成にはグループポリシーを使用します（Controller または Cloud Connector が少なくとも2つある場合）。VDA を、そのゾーン内のローカルな Controller または Cloud Connector に向けます。自動更新を使用して、それらを最新の状態に保ちます。自動更新は、サテライトゾーンの VDA の `ListofDDCs` を自動的に最適化します。
- Controllerが利用できない場合の登録の問題を防ぐため、`ListOfDDCs` レジストリキーに複数のControllerをスペースまたはコンマで区切ってリストします。例:

```
DDC7x.xd.local DDC7xHA.xd.local



32-bit: HKEY_LOCAL_MACHINE
\Software\Citrix\VirtualDesktopAgent\ListOfDDCs



HKEY_LOCAL_MACHINE \Software\Citrix\VirtualDesktopAgent\ListOfDDCs
(REG_SZ)
```

- `ListofDDCs` の下にリストされているすべての値が有効な完全修飾ドメイン名にマッピングされていることを確認し、起動時の登録遅延を防ぎます。

自動更新

自動更新（XenApp および XenDesktop 7.6 で導入）は、デフォルトで有効になっています。これは、VDA 登録を最新の状態に保つための最も効率的な方法です。初期登録には使用されませんが、初期登録時に自動更新ソフトウェアが `ListofDDCs` をダウンロードし、VDA 上の永続キャッシュに保存します。このプロセスは、各 VDA に対して実行されます。キャッシュにはマシンポリシー情報も保持され、ポリシー設定が再起動後も維持されるようにします。

自動更新は、MCS または Citrix Provisioning™ を使用してマシンをプロビジョニングする場合にサポートされます。ただし、Citrix Provisioning のサーバー側キャッシュは除きます。サーバー側キャッシュは、自動更新キャッシュ用の永続ストレージがないため、一般的なシナリオではありません。

この方法を指定するには:

- 設定 `Virtual Delivery Agent Settings > Enable auto update of Controllers` を含む Citrix ポリシーを通じて、自動更新を有効または無効にします。この設定はデフォルトで有効になっています。

仕組み:

- VDA が再登録されるたびに（たとえば、マシンの再起動後）、キャッシュが更新されます。各 Controller または Cloud Connector も、90分ごとにサイトデータベースをチェックします。前回のチェック以降に Controller または Cloud Connector が追加または削除された場合、あるいは VDA 登録に影響するポリシー変更が発生した場合、Controller または Cloud Connector は登録済みの VDA に更新されたリストを送信し、キャッシュが更新されます。VDA は、最新のキャッシュされたリストにあるすべての Controller または Cloud Connector からの接続を受け入れます。
- VDA が、登録されている Controller または Cloud Connector を含まないリストを受け取った場合（つまり、その Controller または Cloud Connector がサイトから削除された場合）、VDA は、`ListofDDCs` 内の Controller または Cloud Connector の中から選択して再登録します。

例:

- 展開には、A、B、C の3つの Controller があります。VDA は Controller B に登録されます（これは VDA のインストール中に指定されました）。
- その後、2つの Controller（D と E）がサイトに追加されます。90分以内に、VDA は更新されたリストを受け取り、Controller A、B、C、D、E からの接続を受け入れます。（VDA が再起動されるまで、負荷はすべての Controller に均等に分散されません。）

- さらにその後、Controller B が別のサイトに移動されます。90分以内に、元のサイトの VDA は、前回のチェック以降に Controller の変更があったため、更新されたリストを受け取ります。元々 Controller B に登録されていた VDA（リストにはもうありません）は、現在のリスト（A、C、D、E）にある Controller の中から選択して再登録します。

マルチゾーン展開では、サテライトゾーンの自動更新は、まずすべてのローカル Controller を自動的にキャッシュします。プライマリゾーンのすべての Controller は、バックアップグループにキャッシュされます。サテライトゾーンにローカル Controller が利用できない場合、プライマリゾーンの Controller で登録が試行されます。

次の例に示すように、キャッシュファイルにはホスト名とセキュリティID (`ListofSIDs`) のリストが含まれています。VDAはSIDを照会しないため、Active Directoryの負荷が軽減されます。

VDAの登録キャッシュファイルの例(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/vda-registration-cache-file.png)

キャッシュファイルはWMI呼び出しで取得できます。ただし、SYSTEMアカウントのみが読み取り可能な場所に保存されています。

> **重要:**
>
> この情報は情報提供のみを目的としています。このファイルを変更しないでください。このファイルまたはフォルダーへの変更は、サポートされていない構成になります。

```
Get-WmiObject -Namespace "Root\Citrix\DesktopInformation" -Class "Citrix_VirtualDesktopInfo" -Property "PersistentDataLocation"
```

セキュリティ上の理由から (Active Directoryの負荷軽減とは別に) `ListofSIDs` を手動で構成する必要がある場合、自動更新機能は使用できません。詳細については、ListOfSIDs を参照してください。

自動更新の優先順位の例外

自動更新は通常、すべてのVDA登録方法の中で最も高い優先順位を持ち、他の方法の設定を上書きしますが、例外があります。キャッシュ内の `NonAutoListOfDDCs` 要素は、初期VDA構成方法を指定します。自動更新はこの情報を監視します。初期登録方法が変更された場合、登録プロセスは自動更新をスキップし、次に高い優先順位で構成された方法を使用します。このプロセスは、VDAを別のサイトに移動する場合 (たとえば、ディザスターリカバリー中) に役立ちます。

構成に関する考慮事項

一般的なVDA登録構成を表示します。

<iframe src="https://www.youtube.com/embed/MgGMZp4SnZgEq9ieibQc9j" width="720px" height="480px" frameborder="0" title="YouTube video player" allowfullscreen=""> </iframe>
VDA登録手順を表示します。

<iframe src="https://www.youtube.com/embed/iwsbajSVY5QvoUTh6m7AjG" width="720px" height="480px" frameborder="0" title="YouTube video player" allowfullscreen=""> </iframe>
VDA登録に影響を与える可能性のある項目を構成する際は、次の点を考慮してください。

ControllerまたはCloud Connectorのアドレス

ControllerまたはCloud Connectorを指定するためにどの方法を使用するかにかかわらず、CitrixはFQDNアドレスを使用することを推奨します。IPアドレスはDNSレコードよりも侵害されやすいため、信頼できる構成とは見なされません。`ListofSIDs` を手動で入力する場合、`ListofDDCs` でIPを使用できます。ただし、FQDNが引き続き推奨されます。

負荷分散

前述のとおり、VDAは `ListofDDCs` 内のすべてのControllerまたはCloud Connectorに接続を自動的に分散します。フェールオーバーと負荷分散機能は、Citrix Brokering Protocol (CBP) に組み込まれています。構成で複数のControllerまたはCloud Connectorを指定した場合、必要に応じて登録はそれらの間で自動的にフェールオーバーします。自動更新により、すべてのVDAで自動フェールオーバーが自動的に発生します。

セキュリティ上の理由から、Citrix ADCなどのネットワークロードバランサーを使用することはできません。VDA登録はKerberos相互認証を使用します。この認証では、クライアント (VDA) がサービス (Controller) に対して自身のIDを証明する必要があります。ただし、ControllerまたはCloud ConnectorもVDAに対して自身のIDを証明する必要があります。これは、VDAとControllerまたはCloud Connectorが同時にサーバーとクライアントとして機能することを意味します。この記事の冒頭で述べたように、VDAからController/Cloud Connectorへ、およびController/Cloud ConnectorからVDAへの2つの通信チャネルがあります。

このプロセスにおけるコンポーネントは、サービスプリンシパル名 (SPN) と呼ばれ、Active Directoryコンピューターオブジェクトのプロパティとして保存されます。VDAがControllerまたはCloud Connectorに接続するときは、通信相手を指定する必要があります。このアドレスがSPNです。負荷分散されたIPを使用する場合、相互Kerberos認証は、そのIPが予期されたControllerまたはCloud Connectorに属していないことを正しく認識します。

詳細については、以下を参照してください。

- Kerberosの概要
- Kerberosを使用した相互認証

自動更新によるCNAMEの置き換え

自動更新機能は、XenAppおよびXenDesktop 7.xより前のバージョンにおけるCNAME (DNSエイリアス) 機能を置き換えます。CNAME機能は、XenAppおよびXenDesktop 7以降では無効になっています。CNAMEの代わりに自動更新を使用してください。(CNAMEを使用する必要がある場合は、CTX137960を参照してください。DNSエイリアスを常に機能させるには、自動更新とCNAMEを同時に使用しないでください。)

Controller/Cloud Connectorグループ

特定のシナリオでは、ControllerまたはCloud Connectorをグループで処理し、一方のグループを優先し、すべてのController/Cloud Connectorが失敗した場合に他方のグループをフェールオーバーに使用したい場合があります。ControllerまたはCloud Connectorはリストからランダムに選択されるため、グループ化することで優先的な使用を強制するのに役立ちます。

これらのグループは、単一のサイト内での使用を目的としています（複数のサイトではありません）。

Controller/Cloud Connectorのグループを指定するには、かっこを使用します。たとえば、4つのController（プライマリ2つとバックアップ2つ）がある場合、グループ化は次のようになります。

```
(XDC-001.cdz.lan XDC-002.cdz.lan) (XDC-003.cdz.lan XDC-004.cdz.lan)
```

この例では、最初のグループのController（001と002）が最初に処理されます。両方が失敗した場合、2番目のグループのController（003と004）が処理されます。

XenDesktop 7.0以降の場合、**登録グループ**機能を使用するには、追加の手順を実行する必要があります。Studioから**Controllerの自動更新を有効にする**ポリシーを**禁止**する必要があります。

ListOfSIDs

VDAが登録のために連絡できるControllerのリストは`ListofDDCs`です。VDAはどのControllerを信頼すべきかも知っている必要があります。VDAは`ListofDDCs`内のControllerを自動的に信頼しません。`ListofSIDs` (セキュリティID) は、信頼されたControllerを識別します。VDAは信頼されたControllerとのみ登録を試みます。

ほとんどの環境では、`ListofSIDs`は`ListofDDCs`から自動的に生成されます。CDFトレースを使用して`ListofSIDs`を読み取ることができます。

一般的に、`ListofSIDs`を手動で変更する必要はありません。いくつかの例外があります。最初の2つの例外は、新しいテクノロジーが利用可能になったため、もはや有効ではありません。

- **Controller の役割の分離:** XenApp および XenDesktop 7.7 でゾーンが導入される前は、Controller の一部のみが登録に使用される場合、`ListofSIDs` は手動で構成されていました。たとえば、XDC-001 と XDC-002 を XML ブローカーとして使用し、XDC-003 と XDC-004 を VDA 登録に使用する場合、すべての Controller を `ListofSIDs` に、XDC-003 と XDC-004 を `ListofDDCs` に指定していました。これは一般的または推奨される構成ではありません。新しい環境では使用しないでください。代わりにゾーンを使用してください。
- **Active Directory の負荷軽減:** XenApp および XenDesktop 7.6 で自動更新機能が導入される前は、ドメインコントローラーの負荷を軽減するために `ListofSIDs` が使用されていました。`ListofSIDs` を事前に入力することで、DNS 名から SID への解決をスキップできます。ただし、この永続キャッシュには SID が含まれているため、自動更新機能によりこの作業は不要になります。Citrix は自動更新機能を有効にしておくことを推奨します。
- **セキュリティ:** 一部の高度に保護された環境では、侵害されたDNSサーバーからの潜在的なセキュリティ脅威を回避するために、信頼されたControllerのSIDが手動で構成されていました。ただし、これを行う場合は、自動更新機能も無効にする必要があります。そうしないと、永続キャッシュからの構成が使用されます。

したがって、特別な理由がない限り、`ListofSIDs` を変更しないでください。

`ListofSIDs` を変更する必要がある場合は、`HKLM\Software\Citrix\VirtualDesktopAgent` の下に `ListOfSIDs (REG_SZ)` という名前のレジストリキーを作成します。値は信頼された SID のリストで、複数ある場合はスペースで区切ります。

次の例では、1 つの Controller が VDA 登録 (`ListofDDCs`) に使用されていますが、2 つの Controller がブローカー処理 (List OfSIDs) に使用されています。

登録とブローカー処理に使用される異なる Controller の例(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/vda-registration-listofsids.png)

VDA 登録中の Controller 検索

VDA が登録を試行すると、Broker Agent はまずローカルドメインで DNS ルックアップを実行し、指定された Controller に到達できることを確認します。

最初のルックアップで Controller が見つからない場合、Broker Agent は AD でフォールバックのトップダウンクエリを開始できます。このクエリはすべてのドメインを検索し、頻繁に繰り返されます。Controller アドレスが無効な場合 (たとえば、管理者が VDA のインストール時に誤った

FQDN を入力した場合)、そのクエリのアクティビティがドメインコントローラーで分散型サービス拒否 (DDoS) 状態を引き起こす可能性があります。

次のレジストリキーは、Broker Agent が最初の検索中に Controller を見つけられない場合に、フォールバックのトップダウンクエリを使用するかどうかを制御します。

`HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent`

- 名前: `DisableDdcWildcardNameLookup`
- 種類: `DWORD`
- 値: `0` (デフォルト) または任意のゼロ以外の値

`0` に設定すると、フォールバック検索が有効になります。Controller の最初の検索が失敗した場合、フォールバックのトップダウン検索が開始されます。これはデフォルトの動作です。ただし、ゼロ以外の値に設定すると、フォールバック検索は無効になります。Controller の最初の検索が失敗した場合、Broker Agent は検索を停止します。

読み取り専用ドメインコントローラーを使用した VDA 登録中の LDAP バインディングシーケンス

VDA が読み取り専用ドメインコントローラー (RODC) に登録する場合、Broker Agent は無視する Light Directory Access Protocol (LDAP) バインディングを選択する必要があります。この選択を行うには、Broker Agent に適切なレジストリキーが必要です。

レジストリキーが指定されていない場合、またはレジストリキーフィールドが空の場合、RODCへのVDA登録は、元のLDAPバインディングシーケンスを経由する必要があるため、時間がかかります。

LDAPバインディングシーケンスを変更するために、レジストリキー`ListofIgnoredBindings`が`HKEY_LOCAL_MACHINE\Software\Policies\Citrix\VirtualDesktopAgent`に追加されました。`ListofIgnoredBindings`を使用すると、必要に応じてLDAPバインディングシーケンスを変更でき、RODCへのVDA登録を高速化できます。

- 名前: `ListofIgnoredBindings`
- 種類: `REG_SZ`
- 値: `DefaultPath`、`DomainPath`、`PDCPath`

値は、コンマで区切られたバインディングパスオプションのリストです。レジストリキーは、有効と認識しない値をすべて無視します。

VDA登録の問題のトラブルシューティング

前述のとおり、仲介されたセッションを起動する際に考慮されるには、VDAがDelivery ControllerまたはCloud Connectorに登録されている必要があります。未登録のVDAは、利用可能なリソースの利用率低下につながる可能性があります。VDAが登録されない理由はさまざまあり、その多くは管理者がトラブルシューティングできます。Studioは、カタログ作成ウィザードと、デリバリーグループ作成後にトラブルシューティング情報を提供します。

- **マシンカタログ作成中の問題の特定:** カタログ作成ウィザードで、既存のマシンを追加した後、コンピューターアカウント名のリストは、各マシンがカタログに追加するのに適しているかどうかを示します。各マシンの横にあるアイコンにカーソルを合わせると、そのマシンに関する情報メッセージが表示されます。

  メッセージで問題のあるマシンが特定された場合、そのマシンを削除する（**削除**ボタンを使用）か、マシンを追加することができます。たとえば、マシンに関する情報が取得されなかった（おそらく一度も登録されなかったため）ことを示すメッセージが表示された場合でも、そのマシンを追加することを選択できます。

  カタログの機能レベルは、カタログ内のマシンで利用できる製品機能を制御します。新しい製品バージョンで導入された機能を使用するには、新しいVDAが必要になる場合があります。機能レベルを設定すると、そのバージョンで導入されたすべての機能（および機能レベルが変更されない場合はそれ以降のバージョン）がカタログ内のマシンで利用可能になります。ただし、以前のVDAバージョンを持つカタログ内のマシンは登録できません。
- **デリバリーグループ作成後の問題の特定:** デリバリーグループを作成すると、Studioはそのグループに関連付けられているマシンに関する詳細を表示します。

  デリバリーグループの詳細ペインには、登録されるべきだが登録されていないマシンの数が表示されます。言い換えれば、電源が入っていてメンテナンスモードではないが、現在Controllerに登録されていないマシンが1台以上存在する可能性があります。「登録されていないが、登録されるべき」マシンを表示する際は、詳細ペインの**トラブルシューティング**タブで、考えられる原因と推奨される是正措置を確認してください。

VDA登録のトラブルシューティングに関する詳細情報

- 機能レベルの詳細については、「VDAのバージョンと機能レベル」を参照してください。
- VDA登録のトラブルシューティングについて詳しくは、「CTX136668」を参照してください。
- VDA登録とセッション起動のトラブルシューティングには、Citrix Scoutのヘルスチェックも使用できます。詳細については、「ヘルスチェックについて」を参照してください。

仮想IPおよび仮想ループバック

重要:

- Windows 10 Enterprise multi-session は Remote Desktop IP Virtualization (Virtual IP) をサポートしていません。また、Windows 10 Enterprise multi-session では Remote Desktop IP Virtualization または仮想ループバックをサポートしていません。
- Remote Desktop IP Virtualization (Virtual IP) は、クラウドホスト型マシンではサポートされていません。 詳細については、Microsoft のドキュメントを参照してください。

Remote Desktop IP Virtualization および仮想ループバック機能は、Windows Server 2016、Windows Server 2019、および Windows Server 2022 マシンでサポートされています。これらの機能は、Windows デスクトップ OS マシンには適用されません。

Microsoft Remote Desktop IP Virtualization アドレス機能は、公開アプリケーションにセッションごとに一意の動的に割り当てられた IP アドレスを提供します。Citrix 仮想ループバック機能を使用すると、localhost (デフォルトでは 127.0.0.1) との通信に依存するアプリケーションを、localhost 範囲 (127.*) 内の一意の仮想ループバックアドレスを使用するように構成できます。

CRM や Computer Telephony Integration (CTI) などの特定のアプリケーションは、アドレス指定、ライセンス、識別、または一意の IP アドレスやループバックアドレスを必要とするその他の目的で IP アドレスを使用します。他のアプリケーションは静的ポートにバインドする可能性があり、その場合、マルチユーザー環境でアプリケーションの追加インスタンスを起動しようとすると、ポートが使用中であるため失敗します。このようなアプリケーションが Citrix Virtual Apps™ 環境で正しく機能するには、デバイスごとに一意の IP アドレスが必要です。

Remote Desktop IP Virtualization と仮想ループバックは、互いに独立した機能です。どちらか一方、または両方を使用できます。

管理者アクションの概要:

- Microsoft Remote Desktop IP Virtualization を使用するには、Windows サーバーでこれを有効にして構成します。(Citrix® ポリシー設定は不要です。)
- Citrix仮想ループバックを使用するには、Citrixポリシーで2つの設定を構成します。

リモートデスクトップIP仮想化 (仮想IP)

Windows サーバーで Remote Desktop IP Virtualization が有効になり構成されると、セッションで実行されている構成済みの各アプリケーションは、一意のアドレスを持っているように見えます。ユーザーは、Citrix Virtual Apps サーバー上のこれらのアプリケーションに、他の公開アプリケーションと同じ方法でアクセスします。プロセスが Remote Desktop IP Virtualization を必要とするのは、次のいずれかのケースです。

- プロセスがハードコードされたTCPポート番号を使用している
- プロセスがWindowsソケットを使用しており、一意のIPアドレスまたは指定されたTCPポート番号を必要としている

アプリケーションが Remote Desktop IP Virtualization アドレスを使用する必要があるかどうかを判断するには：

1. Microsoft から **TCPView** ツールを入手します。このツールは、特定の IP アドレスとポートをバインドするすべてのアプリケーションを一覧表示します。TCPView の詳細については、Microsoft ドキュメント を参照してください。
2. **IP アドレスの解決**機能を無効にして、ホスト名ではなくアドレスが表示されるようにします。
3. アプリケーションを起動し、**TCPView** を使用して、アプリケーションが開いている IP アドレスとポート、およびこれらのポートを開いているプロセス名を確認します。
4. サーバーのIPアドレス、0.0.0.0、または127.0.0.1を開くプロセスを構成します。
5. アプリケーションが異なるポートで同じ IP アドレスを開かないようにするには、アプリケーションの別のインスタンスを起動します。

Microsoft Remote Desktop (RD) IP仮想化の仕組み

- Microsoftサーバーで仮想IPアドレス指定を有効にする必要があります。

  たとえば、Windows Server 2016 環境では、サーバーマネージャーから **Remote Desktop Services > RD Session Host Connections** を展開して、RD IP Virtualization 機能を有効にし、セッションごとまたはプログラムごとに動的ホスト構成プロトコル (DHCP) サーバーを使用して IP アドレスを動的に割り当てる設定を構成します。Remote Desktop IP Virtualization の構成の詳細については、Microsoft ドキュメント を参照してください。
- 機能を有効にすると、セッションの起動時に、サーバーはDHCPサーバーから動的に割り当てられたIPアドレスを要求します。
- The **RD IP Virtualization**機能は、リモートデスクトップ接続にセッションごとまたはプログラムごとにIPアドレスを割り当てます。複数のプログラムにIPアドレスを割り当てる場合、それらはセッションごとのIPアドレスを共有します。

- セッションにアドレスが割り当てられると、以下の呼び出しが行われるたびに、システムプライマリIPアドレスではなく仮想アドレスがセッションで使用されます:
  `bind`、`closesocket`、`connect`、`WSAConnect`、`WSAAccept`、`getpeername`、`getsockname`、`sendto`、`WSASendTo`、`WSASocketW`、`gethostbyaddr`、`getnameinfo`、`getaddrinfo`。

リモートデスクトップセッションホスティング構成内でMicrosoft IP仮想化機能を使用する場合、アプリケーションとWinsock関数呼び出しの間に「フィルター」コンポーネントを挿入することで、アプリケーションは特定のIPアドレスにバインドされます。これにより、アプリケーションは使用すべき正しいIPアドレスのみを認識します。アプリケーションがTCPまたはUDP通信をリッスンしようとすると、自動的に割り当てられた仮想IPアドレス（またはループバックアドレス）にバインドされます。アプリケーションによって開かれた発信接続はすべて、アプリケーションにバインドされたIPアドレスから発信されます。

アドレスを返す関数（Windowsポリシーが制御する`GetAddrInfo()`など）でローカルホストIPアドレスが要求された場合、リモートデスクトップIP仮想化は返されたIPアドレスを調べ、それをセッションのリモートデスクトップIP仮想化アドレスに変更します。このような名前関数を介してローカルサーバーのIPアドレスを取得しようとするアプリケーションは、そのセッションに割り当てられた一意のリモートデスクトップIP仮想化アドレスのみを認識します。このIPアドレスは、bindやconnectなどの後続のソケット呼び出しでよく使用されます。Windowsポリシーの詳細については、「RDS IP Virtualization in Windows Server」を参照してください。

多くの場合、アプリケーションはアドレス0.0.0.0でリッスンするためにポートへのバインドを要求します。アプリケーションがこれを行い、静的ポートを使用する場合、アプリケーションの複数のインスタンスを起動することはできません。リモートデスクトップIP仮想化アドレス機能は、これらの呼び出しタイプでも0.0.0.0を探します。特定の仮想IPアドレスでリッスンするように呼び出しを変更するため、複数のアプリケーションが同じコンピューター上の同じポートでリッスンできるようになります。これは、すべて異なるアドレスでリッスンしているためです。この呼び出しは、ICAセッション内であり、リモートデスクトップIP仮想化アドレス機能が有効になっている場合にのみ変更されます。たとえば、異なるセッションで実行されているアプリケーションの2つのインスタンスが、両方ともすべてのインターフェイス（0.0.0.0）と特定のポート（9000など）にバインドしようとした場合、それらはVIPAddress1:9000とVIPAddress2:9000にバインドされ、競合は発生しません。

仮想ループバック

Citrix Remote Desktop IP Virtualization loopback policy設定を有効にすると、各セッションが通信用に独自のループバックアドレスを持つことができます。アプリケーションがWinsock呼び出しでlocalhostアドレス（デフォルト = 127.0.0.1）を使用すると、仮想ループバック機能は127.0.0.1を127.X.X.Xに置き換えます。ここで、X.X.Xはセッション ID + 1を表します。たとえば、

セッションIDが7の場合、127.0.0.8になります。セッションIDが第4オクテット（255を超える）を超過する可能性は低いですが、その場合はアドレスは次のオクテット（127.0.1.0）にロールオーバーし、最大127.255.255.255までとなります。

プロセスが仮想ループバックを必要とするのは、次のいずれかのケースです。

- プロセスがWindowsソケットループバック（localhost）アドレス（127.0.0.1）を使用している場合
- プロセスがハードコードされたTCPポート番号を使用している場合

プロセス間通信にループバックアドレスを使用するアプリケーションには、仮想ループバックポリシー設定を使用します。追加の構成は不要です。仮想ループバックは仮想IPに依存しないため、Microsoftサーバーを構成する必要はありません。

- 仮想IPループバックサポート。有効にすると、このポリシー設定により、各セッションが独自の仮想ループバックアドレスを持つことができます。この設定はデフォルトで無効になっています。この機能は、仮想IP仮想ループバックプログラムリストポリシー設定で指定されたアプリケーションにのみ適用されます。
- 仮想IP仮想ループバックプログラムリスト。このポリシー設定は、仮想IPループバック機能を使用するアプリケーションを指定します。この設定は、仮想IPループバックサポートポリシー設定が有効になっている場合にのみ適用されます。

関連機能

仮想IPよりも仮想ループバックが優先されるように、以下のレジストリ設定を使用できます。この機能は優先ループバックと呼ばれます。ただし、注意して進めてください。

- 優先ループバックは、仮想IPと仮想ループバックの両方が有効になっている場合にのみ使用してください。そうしないと、意図しない結果が生じる可能性があります。
- レジストリを誤って編集すると、オペレーティングシステムの再インストールが必要になるような深刻な問題が発生する可能性があります。Citrixは、レジストリエディターの誤った使用によって生じる問題が解決できることを保証できません。レジストリエディターは自己責任で使用してください。編集する前に必ずレジストリをバックアップしてください。

アプリケーションが常駐するサーバーでregeditを実行します。

- `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\VIP`
- 名前: PreferLoopback, 種類: REG_DWORD, データ: 1
- 名前: PreferLoopbackProcesses, 種類: REG_MULTI_SZ, データ: \<プロセスのリスト\>

ゾーン

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

WANで接続された広範囲に分散した場所にまたがる展開では、ネットワークの遅延と信頼性により課題が生じる可能性があります。これらの課題を軽減する2つのオプションがあります。

- 複数のサイトを展開し、それぞれに独自のSQL Serverサイトデータベースを持たせる。

  このオプションは、大規模なエンタープライズ展開に推奨されます。複数のサイトは個別に管理され、それぞれに独自のSQL Serverサイトデータベースが必要です。各サイトは独立したCitrix Virtual Apps™展開です。

- 単一サイト内に複数のゾーンを構成する。

  ゾーンを構成することで、リモート地域のユーザーがWANの大部分を通過することなくリソースに接続できるようになります。ゾーンを使用すると、単一のWeb Studioコンソール、Citrix Director、およびサイトデータベースから効果的なサイト管理が可能になります。これにより、リモートロケーションに個別のデータベースを含むより多くのサイトを展開、人員配置、ライセンス供与、および運用するコストを節約できます。

  ゾーンは、あらゆる規模の展開で役立ちます。ゾーンを使用して、アプリケーションとデスクトップをエンドユーザーの近くに配置することで、パフォーマンスを向上させることができます。ゾーンには、冗長性と回復性のために1つ以上のControllerをローカルにインストールできますが、必須ではありません。

  サイトに構成されているControllerの数は、サイト自体に新しいControllerを追加するなどの一部の操作のパフォーマンスに影響を与える可能性があります。これを避けるため、Citrix Virtual AppsまたはCitrix Virtual Desktops™サイトのゾーン数を50以下に制限することをお勧めします。

  ゾーンのネットワーク遅延が250ミリ秒RTTを超える場合は、ゾーンではなく複数のサイトを展開することをお勧めします。

この記事全体を通して、「ローカル」という用語は、議論されているゾーンを指します。たとえば、「VDAがローカルControllerに登録する」とは、VDAがVDAが配置されているゾーン内のControllerに登録することを意味します。

このリリースでのゾーンは、XenAppバージョン6.5以前のゾーンと似ていますが、同一ではありません。たとえば、このゾーンの実装では、データコレクターはありません。サイト内のすべてのControllerは、プライマリゾーンの1つのサイトデータベースと通信します。また、このリリースではフェールオーバーゾーンと優先ゾーンの動作が異なります。

ゾーンの種類

サイトには常に1つのプライマリゾーンがあります。オプションで1つ以上のサテライトゾーンを持つこともできます。サテライトゾーンは、災害復旧、地理的に離れたデータセンター、支店、クラウド、またはクラウド内のアベイラビリティゾーンに使用できます。

プライマリゾーン:

プライマリゾーンのデフォルト名は「Primary」です。このゾーンには、SQL Serverサイトデータベース（および使用されている場合は高可用性SQLサーバー）、Web Studio、Director、Citrix StoreFront™、Citrix License Server、およびCitrix Gatewayが含まれます。サイトデータベースは常にプライマリゾーンに保持してください。

プライマリゾーンには、冗長性のために少なくとも2つのControllerが必要です。プライマリゾーンには、データベースおよびインフラストラクチャと密接に連携するアプリケーションを持つVDAを配置できます。

サテライトゾーン:

サテライトゾーンには、1つ以上のVDA、Controller、StoreFrontサーバー、およびCitrix Gatewayサーバーが含まれます。通常の運用では、サテライトゾーンのControllerはプライマリゾーンのデータベースと直接通信します。

サテライトゾーン、特に大規模なゾーンには、そのゾーンのマシンをプロビジョニングおよび保存するために使用されるハイパーバイザーが含まれる場合もあります。サテライトゾーンを構成する際、ハイパーバイザーまたはその他のサービス接続を関連付けることができます。（その接続を使用するカタログがすべて同じゾーンにあることを確認してください。）

サイトには、独自のニーズと環境に基づいて、さまざまな構成のサテライトゾーンを含めることができます。次の図は、プライマリゾーンとサテライトゾーンの例を示しています。

プライマリゾーンとサテライトゾーンの図(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/zones1.png)

図では、次のようになります。

- **プライマリゾーン:** 2つのController、Web Studio、Director、StoreFront、License Server、およびサイトデータベース（高可用性SQL Server展開を含む）が含まれます。プライマリゾーンには、複数のVDAとCitrix Gatewayも含まれます。
- **サテライトゾーン1: Controllerを持つVDA:** サテライトゾーン1には、Controller、VDA、およびStoreFrontサーバーが含まれます。このサテライトゾーンのVDAは、ローカルのControllerに登録されます。ローカルのControllerは、プライマリゾーンのサイトデータベースおよびライセンスサーバーと通信します。

  WANが失敗した場合、ローカルホストキャッシュ機能により、サテライトゾーンのControllerは、そのゾーンのVDAへの接続の仲介を続行できます。このような展開は、従業員がローカルのStoreFrontサイトとローカルのControllerを使用してローカルリソースにアクセスするオフィスで効果的です。
- **サテライトゾーン2: 冗長Controllerを持つVDA:** サテライトゾーン2には、2つのController、VDA、およびStoreFrontサーバーが含まれます。これは最も回復力のあるゾーンタイプであり、WANとローカルControllerの1つが同時に障害を起こした場合でも保護を提供します。

VDAの登録先とControllerのフェールオーバー先

プライマリゾーンとサテライトゾーンを含むサイトで、VDAの最小バージョンが7.7の場合:

- プライマリゾーンのVDAは、プライマリゾーンのControllerに登録されます。プライマリゾーンのVDAは、サテライトゾーンのControllerに登録しようとすることはありません。
- サテライトゾーンのVDAは、可能であればローカルのControllerに登録されます。（これは優先Controllerと見なされます。）ローカルのControllerが利用できない場合（たとえば、VDAの登録をこれ以上受け入れられない、または障害が発生した場合など）、VDAはプライマリゾーンのControllerに登録しようとします。この場合、サテライトゾーンのControllerが再び利用可能になったとしても、VDAはプライマリゾーンに登録されたままになります。サテライトゾーンのVDAは、別のサテライトゾーンのControllerに登録しようとすることはありません。
- VDAのController検出で自動更新が有効になっており、VDAのインストール中にControllerアドレスのリストを指定した場合、初期登録のためにそのリストからControllerがランダムに選択されます（Controllerがどのゾーンにあるかに関わらず）。そのVDAを持つマシンが再起動されると、VDAはローカルゾーンのControllerへの登録を優先し始めます。
- サテライトゾーンのControllerが故障した場合、可能であれば別のローカルControllerにフェールオーバーします。ローカルControllerが利用できない場合は、プライマリゾーンのControllerにフェールオーバーします。

- Controllerをゾーンの内外に移動し、自動更新が有効になっている場合、両方のゾーンのVDAは、どのControllerがローカルで、どのControllerがプライマリゾーンにあるかを示す更新されたリストを受け取り、どのControllerに登録し、どのControllerから接続を受け入れることができるかを知ることができます。
- カタログを別のゾーンに移動すると、そのカタログ内のVDAは、カタログを移動したゾーンのControllerに再登録します。（カタログを別のゾーンに移動する際は、このゾーンと関連するホスト接続があるゾーンが適切に接続されていることを確認してください。帯域幅が制限されているか、待ち時間が長い場合は、ホスト接続を関連するマシンカタログを含む同じゾーンに移動してください。）

プライマリゾーンのすべてのControllerが故障した場合：

- Web Studioはサイトに接続できません。
- プライマリゾーンのVDAへの接続はできません。
- プライマリゾーンのControllerが利用可能になるまで、サイトのパフォーマンスが低下します。

VDAバージョン7.7より前のバージョンを含むサイトの場合：

- サテライトゾーンのVDAは、ローカルゾーンおよびプライマリゾーンのControllerからの要求を受け入れます。（最小バージョン7.7のVDAは、他のサテライトゾーンのController要求を受け入れることができます。）
- サテライトゾーンのVDAは、プライマリゾーンまたはローカルゾーンのControllerにランダムに登録します。（最小バージョン7.7のVDAはローカルゾーンを優先します。）

ゾーンの優先順位

ゾーン優先機能を使用するには、最小限StoreFront 3.7およびCitrix Gateway 11.0-65.xを使用している必要があります。

マルチゾーンサイトでは、ゾーン優先機能により、管理者はアプリケーションまたはデスクトップの起動に使用されるVDAをより柔軟に制御できます。

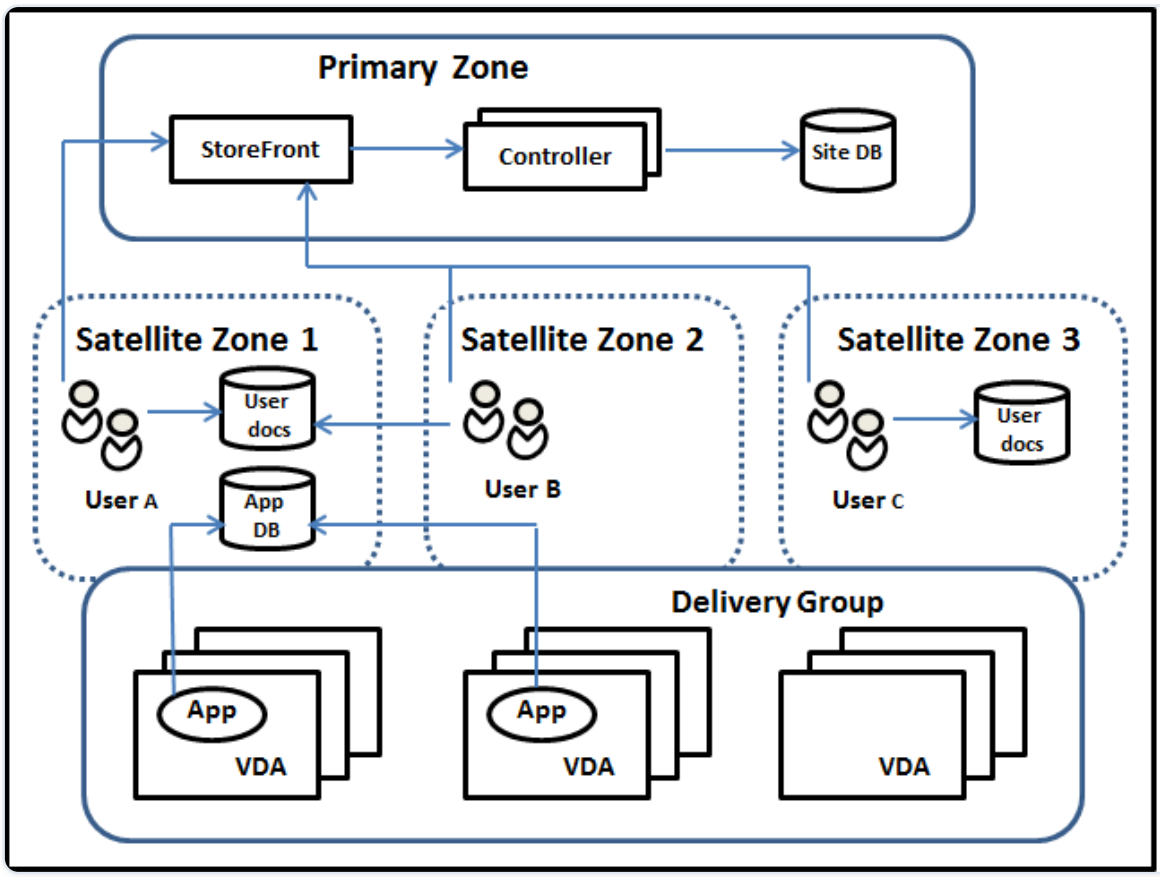
ゾーンの優先順位の仕組み

ゾーンの優先順位には3つの形式があります。特定のゾーンのVDAを使用することを優先する場合があります。その理由は次のとおりです。

- アプリケーションのデータが保存されている場所。これはアプリケーションホームと呼ばれます。

- ユーザーのホームデータ（プロファイルやホーム共有など）の場所。これはユーザーホームと呼ばれます。
- ユーザーの現在の場所（Citrix Workspace™アプリが実行されている場所）。これはユーザーの場所と呼ばれます。

次の図は、マルチゾーン構成の例を示しています。



この例では、VDAは3つのサテライトゾーンに分散していますが、すべて同じデリバリーグループに属しています。そのため、ブローカーはユーザーの起動リクエストに対してどのVDAを使用するかを選択する可能性があります。この例は、ユーザーがCitrix Workspaceアプリのエンドポイントを実行できる場所がいくつかあることを示しています。

- ユーザーAは、サテライトゾーン1でCitrix Workspaceアプリがインストールされたデバイスを使用しています。
- ユーザーBは、サテライトゾーン2でデバイスを使用しています。
- ユーザーのドキュメントはさまざまな場所に保存できます。
  - ユーザーAとBは、サテライトゾーン1にある共有を使用します。
  - ユーザーCは、サテライトゾーンCの共有を使用します。
  - 公開されているアプリケーションの1つは、サテライトゾーン1にあるデータベースを使用します。

ユーザーまたはアプリケーションのホームゾーンを構成することで、ユーザーまたはアプリケーションをゾーンに関連付けます。Delivery Controller™のブローカーは、リソースが利用可能な場合、これらの関連付けを使用してセッションが起動されるゾーンの選択を支援します。次のことができます。

- ユーザーをゾーンに追加して、ユーザーのホームゾーンを構成します。
- アプリケーションのプロパティを編集して、アプリケーションのホームゾーンを構成します。

ユーザーまたはアプリケーションは、一度に1つのホームゾーンしか持つことができません。（ユーザーグループのメンバーシップにより複数のゾーンメンバーシップが発生する場合、ユーザーには例外が発生する可能性があります。「その他の考慮事項」セクションを参照してください。ただし、この場合でも、ブローカーは1つのホームゾーンのみを使用します。）

ユーザーとアプリケーションのゾーン設定を構成できますが、ブローカーは起動に対して1つの優先ゾーンのみを選択します。優先ゾーンを選択するためのデフォルトの優先順位は、アプリケーションホーム \> ユーザーホーム \> ユーザーロケーションです。この順序を制限できます。詳細については、ゾーン設定の調整を参照してください。ユーザーがアプリケーションを起動すると：

- そのアプリケーションにゾーン関連付け（アプリケーションホーム）が構成されている場合、優先ゾーンはそのアプリケーションのホームゾーンになります。
- アプリケーションにゾーン関連付けが構成されていないが、ユーザーにゾーン関連付け（ユーザーホーム）が構成されている場合、優先ゾーンはそのユーザーのホームゾーンになります。
- アプリケーションにもユーザーにもゾーン関連付けが構成されていない場合、優先ゾーンはユーザーがCitrix Workspaceアプリインスタンスを実行しているゾーン（ユーザーロケーション）になります。そのゾーンが定義されていない場合、ランダムなVDAとゾーンの選択が使用されます。優先ゾーン内のすべてのVDAに負荷分散が適用されます。優先ゾーンがない場合、デリバリーグループ内のすべてのVDAに負荷分散が適用されます。

ゾーンの優先順位の調整

ユーザーまたはアプリケーションのホームゾーンを構成（または削除）する際、ゾーン設定の使用方法をさらに制限することもできます。

- **必須のユーザーホームゾーンの使用：** デリバリーグループでは、セッションがユーザーのホームゾーン（構成されている場合）で起動し、ホームゾーンに利用可能なリソースがない場合に他のゾーンへのフェイルオーバーを行わないように指定できます。この制限は、ゾーン間で大きなプロファイルやデータファイルをコピーするリスクを回避する必要がある場合に役立ちます。言い換えれば、別のゾーンでセッションを起動するよりも、セッションの起動を拒否する方が望ましいということです。

- **アプリケーションのホームゾーンの強制使用:** 同様に、アプリケーションのホームゾーンを構成する場合、そのアプリケーションは、アプリケーションのホームゾーンでリソースが利用できない場合に別のゾーンにフェールオーバーすることなく、そのゾーンでのみ起動されるように指定できます。
- **アプリケーションのホームゾーンなし、および構成されたユーザーホームゾーンを無視:** アプリケーションのホームゾーンを指定しない場合、そのアプリケーションを起動するときに、構成されたユーザーゾーンを考慮しないように指定することもできます。たとえば、一部のユーザーが異なるホームゾーンを持っている場合でも、ユーザーロケーションゾーンの優先設定を使用して、ユーザーがデバイスの近くのVDAでアプリケーションを実行することを好む場合があります。

優先ゾーンがセッションの使用に与える影響

ユーザーがアプリケーションまたはデスクトップを起動すると、ブローカーは既存のセッションを使用するよりも優先ゾーンを使用することを優先します。

アプリケーションまたはデスクトップを起動するユーザーが、起動されるリソースに適したセッション（たとえば、アプリケーションのセッション共有を使用できるセッション、または起動されるリソースがすでに実行されているセッション）をすでに持っているが、そのセッションがユーザー/アプリケーションの優先ゾーン以外のゾーンのVDAで実行されている場合、システムは新しいセッションを作成する可能性があります。これにより、そのユーザーのセッション要件にとって優先度の低いゾーンのセッションに再接続するよりも前に、正しいゾーンでの起動（利用可能な容量がある場合）が満たされます。

到達不能になる可能性のある孤立したセッションを防ぐため、既存の切断されたセッションへの再接続は、それらが非優先ゾーンにある場合でも許可されます。

起動を満たすためのセッションの望ましさの順序は次のとおりです。

1. 優先ゾーン内の既存のセッションに再接続する。
2. 優先ゾーン以外のゾーンで、既存の切断されたセッションに再接続する。
3. 優先ゾーンで新しいセッションを開始します。
4. 優先ゾーン以外のゾーンで、接続されている既存のセッションに再接続する。
5. 優先ゾーン以外のゾーンで、新しいセッションを開始する。

その他のゾーン優先度に関する考慮事項

- ユーザーグループ（セキュリティグループなど）にホームゾーンを構成すると、そのグループのユーザー（直接的または間接的なメンバーシップを通じて）は指定されたゾーンに関連付けられます。ただし、ユーザーは複数のセキュリティグループのメンバーになることができ、そ

のため、他のグループメンバーシップを通じて異なるホームゾーンが構成されている場合があります。このような場合、そのユーザーのホームゾーンの決定は曖昧になる可能性があります。

ユーザーがグループメンバーシップを通じて取得したものではない構成済みのホームゾーンを持っている場合、そのゾーンがゾーン優先度に使用されます。グループメンバーシップを通じて取得されたゾーン関連付けはすべて無視されます。

ユーザーがグループメンバーシップのみを通じて取得した複数の異なるゾーン関連付けを持っている場合、ブローカーはゾーンの中からランダムに選択します。ブローカーがこの選択を行うと、そのゾーンは、ユーザーのグループメンバーシップが変更されるまで、その後のセッション起動に使用されます。

- ユーザーロケーションゾーンの優先設定では、デバイスが接続するCitrix Gatewayによって、エンドポイントデバイス上のCitrix Workspaceアプリが検出される必要があります。Citrix Gatewayは、IPアドレスの範囲を特定のゾーンに関連付けるように構成する必要があり、検出されたゾーンIDはStoreFrontを介してControllerに渡される必要があります。

ゾーンの優先設定の詳細については、「ゾーンの優先設定の内部」を参照してください。

考慮事項、要件、およびベストプラクティス

- ゾーンには、Controller、マシンカタログ、ホスト接続、ユーザー、およびアプリケーションを配置できます。カタログがホスト接続を使用する場合、カタログと接続が同じゾーンにあることを確認してください。（ただし、低遅延で高帯域幅の接続が利用可能な場合は、異なるゾーンに配置することもできます。）」
- サテライトゾーンにアイテムを配置すると、サイトがそれらやそれらに関連する他のオブジェクトとどのようにやり取りするかに影響します。
    - Controllerがサテライトゾーンに配置されると、それらのマシンは同じゾーン内のハイパーバイザーおよびVDAに対して良好な（ローカル）接続性を持っていると見なされます。そのサテライトゾーンのControllerは、それらのハイパーバイザーおよびVDAマシンを処理するために、プライマリゾーンのControllerよりも優先して使用されます。
    - ハイパーバイザー接続がサテライトゾーンに配置されると、そのハイパーバイザー接続を介して管理されるすべてのハイパーバイザーもそのサテライトゾーンに存在すると見なされます。そのサテライトゾーンのControllerは、そのハイパーバイザー接続と通信する際に、プライマリゾーンのControllerよりも優先して使用されます。
    - マシンカタログがサテライトゾーンに配置されると、そのカタログ内のすべてのVDAマシンがサテライトゾーンにあると見なされます。各VDAの最初の登録後にControllerリストの

自動更新メカニズムがアクティブになった後、サイトへの登録を試みる際には、プライマリゾーンのControllerよりもローカルのControllerが優先して使用されます。

- Citrix Gatewayインスタンスもゾーンに関連付けることができます。これは、ここで説明されている他の要素の場合のようにサイト構成の一部としてではなく、StoreFront Optimal HDX™ルーティング構成の一部として行われます。Citrix Gatewayがゾーンに関連付けられている場合、そのゾーン内のVDAマシンへのHDX接続が使用されるときに、そのCitrix Gatewayが優先的に使用されます。

- 実稼働サイトを作成し、最初のカタログとデリバリーグループを作成すると、すべての項目はプライマリゾーンに配置されます。この初期設定が完了するまで、サテライトゾーンを作成することはできません。（空のサイトを作成した場合、プライマリゾーンには最初はコントローラーのみが含まれます。カタログとデリバリーグループを作成する前または後にサテライトゾーンを作成できます。）
- 1つ以上の項目を含む最初のサテライトゾーンを作成すると、サイト内の他のすべての項目はプライマリゾーンに残ります。
- プライマリゾーンはデフォルトで「Primary」という名前ですが、この名前は変更できます。Web Studioはどのゾーンがプライマリゾーンであるかを示しますが、プライマリゾーンには識別しやすい名前を使用するのがベストプラクティスです。プライマリゾーンを再割り当て（つまり、別のゾーンをプライマリゾーンにする）できますが、常にサイトデータベースと高可用性サーバーが含まれている必要があります。
- サイトデータベースは常にプライマリゾーンに保持してください。
- ゾーンを作成した後、後で項目をあるゾーンから別のゾーンに移動できます。この柔軟性により、近接して最適に機能する項目を分離できる可能性があります。たとえば、カタログ内のマシンを作成する接続（ホスト）とは異なるゾーンにカタログを移動すると、パフォーマンスに影響を与える可能性があります。項目をゾーン間で移動する前に、潜在的な意図しない影響を考慮してください。カタログとそれが使用するホスト接続は同じゾーンに、または適切に接続されたゾーン（たとえば、低遅延で高帯域幅のネットワーク経由）に保持してください。
- 最適なパフォーマンスを得るには、Web StudioとDirectorはプライマリゾーンにのみインストールしてください。Web StudioとDirectorはWebアプリケーションであるため、サテライトゾーン（たとえば、プライマリゾーンがアクセス不能になった場合のフェイルオーバーとして使用するコントローラーを含むサテライトゾーン）からアクセスできます。
- 理想的には、サテライトゾーンのCitrix Gatewayは、他のゾーンまたは外部の場所からそのゾーンに入ってくるユーザー接続に使用されますが、ゾーン内の接続にも使用できます。
- 注意: ゾーン優先機能を使用するには、StoreFront 3.7およびCitrix Gateway 11.0-65.x以降を使用している必要があります。

接続品質の制限

サテライトゾーンのコントローラーは、サイトデータベースと直接SQL対話を行います。これにより、サテライトゾーンとサイトデータベースを含むプライマリゾーン間のリンクの品質にいくつかの制限が課せられます。具体的な制限は、サテライトゾーンに展開されているVDAの数と、それらのVDA上のユーザーセッションの数に比例します。したがって、VDAとセッションが少ないサテライトゾーンは、VDAとセッションが多いサテライトゾーンよりも、データベースへの接続品質が低い場合でも機能できます。

詳細については、「Latency and SQL Blocking Query Improvements」を参照してください。

遅延がブローカリングパフォーマンスに与える影響

ゾーンによってユーザーは高遅延リンク上にいることができますが、ローカルブローカーが存在する場合でも、追加の遅延は必然的にエンドユーザーエクスペリエンスに影響を与えます。ユーザーが行うほとんどの作業において、サテライトゾーンのコントローラーとサイトデータベース間のラウンドトリップによって引き起こされる遅延を経験します。

アプリケーションを起動する場合、セッションブローカリングプロセスがセッション起動要求を送信するのに適したVDAを特定する際に、追加の遅延が発生します。

ゾーンの作成と管理

フル管理者であれば、すべてのゾーン作成および管理タスクを実行できます。ただし、ゾーンの作成、編集、削除を許可するカスタムロールを作成することもできます。ゾーン間でアイテムを移動する場合、ゾーン関連の権限（ゾーン読み取り権限を除く）は必要ありませんが、移動するアイテムに対する編集権限が必要です。たとえば、カタログをあるゾーンから別のゾーンに移動するには、そのカタログに対する編集権限が必要です。詳しくは、「委任管理」を参照してください。

Citrix Provisioning™を使用している場合： Citrix Provisioningコンソールはゾーンを認識しないため、サテライトゾーンのカタログを作成するにはWeb Studioを使用することをお勧めします。Web Studioでカタログを作成し、正しいサテライトゾーンを指定します。その後、Citrix Provisioningコンソールを使用して、そのカタログ内のマシンをプロビジョニングします。（Citrix Provisioningウィザードを使用してカタログを作成した場合、カタログはプライマリゾーンに配置されます。後でWeb Studioを使用してサテライトゾーンに移動する必要があります。）

ゾーンの作成

1. Web Studioにサインインします。
2. 左側のペインで を選択します。
3. アクションバーで を選択します。

4. ゾーンの名前と説明（オプション）を入力します。名前はサイト内で一意である必要があります。
5. 新しいゾーンに配置するアイテムを選択します。選択可能なアイテムのリストをフィルター処理したり、検索したりできます。空のゾーンを作成することもできます。その場合は、どのアイテムも選択しないでください。
6. 「**保存**」をクリックします。

この方法の代わりに、Web Studioで1つ以上のアイテムを選択し、アクションバーで を選択することもできます。

ゾーン名または説明の変更

1. Web Studioにサインインします。
2. 左側のペインで を選択します。
3. 中央のペインでゾーンを選択し、アクションバーで**ゾーンの編集**を選択します。
4. ゾーン名、説明、またはその両方を変更します。プライマリゾーンの名前を変更する場合は、そのゾーンがプライマリゾーンとして容易に識別できることを確認してください。
5. または をクリックします。

ゾーン間でアイテムを移動する

1. Web Studioにサインインします。
2. 左側のペインで を選択します。
3. 中央ペインでゾーンを選択し、1つ以上の項目を選択します。
4. アイテムを移動先のゾーンにドラッグするか、アクションバーで を選択し、移動先のゾーンを指定します。

確認メッセージには、選択したアイテムが一覧表示され、それらすべてを移動してもよろしいかどうかが尋ねられます。

注意: カタログがハイパーバイザーまたはその他のサービスへのホスト接続を使用する場合、カタログと接続の両方を同じゾーンに配置してください。そうしないと、パフォーマンスに影響が出る可能性があります。一方を移動する場合は、もう一方も移動してください。

ゾーンを削除する

ゾーンは、削除する前に空である必要があります。プライマリゾーンは削除できません。

1. Web Studioにサインインします。

2. 左側のペインで を選択します。
3. 中央のペインでゾーンを選択します。
4. アクションバーから を選択します。ゾーンが空でない場合（アイテムが含まれている場合）、それらのアイテムを移動するゾーンを選択するよう求められます。
5. 削除を確認します。

ユーザーのホームゾーンを追加する

ユーザーのホームゾーンを構成することは、*ユーザーをゾーンに追加する*とも呼ばれます。

1. Web Studioにサインインします。
2. 左側のペインで を選択し、中央のペインでゾーンを選択します。
3. アクションバーで**Add Users to Zone**を選択します。
4. **Add Users to Zone**ダイアログボックスで、**Add**をクリックし、ゾーンに追加するユーザーとユーザーグループを選択します。すでにホームゾーンを持つユーザーを指定した場合、メッセージに2つの選択肢が表示されます。**Yes** = ホームゾーンを持たない指定したユーザーのみを追加します。**No** = ユーザー選択ダイアログに戻ります。
5. **OK**をクリックします。

ホームゾーンが構成されているユーザーの場合、セッションをそのホームゾーンからのみ起動するように要求できます。

1. デリバリーグループを作成または編集します。
2. **ユーザー**ページで、**セッションをユーザーのホームゾーンで起動することを要求する（構成されている場合）**チェックボックスをオンにします。

そのデリバリーグループのユーザーが起動するすべてのセッションは、そのユーザーのホームゾーン内のマシンから起動する必要があります。デリバリーグループ内のユーザーにホームゾーンが構成されていない場合、この設定は無効です。

ユーザーのホームゾーンを削除する

この手順は、ゾーンからユーザーを削除することとも呼ばれます。

1. Web Studioにサインインします。
2. 左ペインで**Zones**を選択し、中央ペインでゾーンを選択します。
3. アクションバーで**Remove Users from Zone**を選択します。

4. **Add Users to Zone**ダイアログボックスで、**Remove**をクリックし、ゾーンから削除するユーザーとグループを選択します。この操作では、ユーザーはゾーンからのみ削除されます。それらのユーザーは、所属するデリバリーグループおよびアプリケーショングループに残ります。
5. プロンプトが表示されたら削除を確定します。

アプリケーションのホームゾーンを管理する

アプリケーションのホームゾーンを構成することは、アプリケーションをゾーンに追加することとも呼ばれます。デフォルトでは、マルチゾーン環境では、アプリケーションにホームゾーンはありません。

アプリケーションのホームゾーンは、アプリケーションのプロパティで指定されます。アプリケーションをグループに追加するとき、または後でアプリケーションのプロパティを構成できます。

- デリバリーグループを作成するとき、アプリケーショングループを作成するとき、または既存のグループにアプリケーションを追加するときに、ウィザードの**Applications**ページで**Properties**を選択します。
- アプリケーションの追加後にアプリケーションのプロパティを変更するには、左ペインで**Applications**を選択します。アプリケーションを選択し、アクションバーで**Edit Application Properties**を選択します。

アプリケーションのプロパティ/設定の ページで、次の操作を行います。

- アプリケーションにホームゾーンを設定する場合：
  - **Use the selected zone to decide**ラジオボタンを選択し、ゾーンを選択します。
  - アプリケーションを、選択したゾーンからのみ（他のゾーンからは起動しないように）起動する場合は、ゾーン選択の下にあるチェックボックスをオンにします。
- アプリケーションにホームゾーンを設定しない場合：
  - ラジオボタンを選択します。
  - このアプリケーションを起動する際に、ブローカーが構成済みのユーザーゾーンを考慮しないようにする場合は、ラジオボタンの下にあるチェックボックスを選択します。この場合、アプリケーションまたはユーザーのホームゾーンのいずれも、このアプリケーションを起動する場所を決定するために使用されません。

ゾーンの指定を含むその他のアクション

少なくとも1つのサテライトゾーンを作成した後、ホスト接続を追加するか、カタログを作成する際にゾーンを指定できます。

通常、プライマリゾーンがデフォルトです。Machine Creation Services™を使用してカタログを作成する場合、ホスト接続用に構成されたゾーンが自動的に選択されます。

サイトにサテライトゾーンが含まれていない場合、プライマリゾーンが想定され、ゾーン選択ボックスは表示されません。

モニター

管理者とヘルプデスク担当者は、さまざまな機能とツールを使用してCitrix Virtual Apps and Desktops™サイトを監視できます。これらのツールを使用すると、以下を監視できます。

- ユーザーセッションとセッションの使用状況
- ログオンパフォーマンス
- 接続とマシン（障害を含む）
- 負荷評価
- 履歴トレンド
- インフラストラクチャ

Citrix Director (シトリックス ディレクター)

Directorは、監視とトラブルシューティング、およびエンドユーザーのサポートタスクの実行に使用できるリアルタイムのWebツールです。

詳細については、Director の記事を参照してください。

構成ログ

構成ログを使用すると、管理者はサイトへの管理変更を追跡できます。構成ログは、構成変更が行われた後の問題の診断とトラブルシューティング、変更管理と構成の追跡を支援し、管理アクティビティを報告するのに役立ちます。

Studioから、ログに記録された情報のレポートを表示および生成できます。また、Directorでトレンドビューを使用して、ログに記録された項目を表示し、構成変更の通知を受け取ることもできます。この機能は、Studioにアクセスできない管理者にとって役立ちます。

トレンドビューは、一定期間にわたる構成変更の履歴データを提供するため、管理者は、サイトに対してどのような変更がいつ誰によって行われたかを評価し、問題の原因を特定できます。このビューは、構成情報を次の3つのカテゴリに分類します。

- 接続障害
- 失敗したシングルセッションマシン

- 失敗したマルチセッションマシン

構成ログを有効にして構成する方法の詳細については、構成ログを参照してください。Directorの記事では、そのツールからログに記録された情報を表示する方法について説明しています。

イベントログ

Citrix Virtual Apps and Desktops内のサービスは、発生したイベントをログに記録します。イベントログは、操作の監視とトラブルシューティングに使用されます。

詳細については、イベントログを参照してください。個々の機能の記事にもイベント情報が含まれている場合があります。

構成ログ

構成ログは、サイト構成の変更と管理アクティビティをデータベースにキャプチャする機能です。この機能はデフォルトで有効になっています。ログに記録されたコンテンツは、次の目的で使用できます。

- 構成変更後、問題の診断とトラブルシューティングを行います。ログは追跡記録を提供します。
- 変更管理の支援と構成の追跡。
- 管理アクティビティを報告します。

Citrix Studioから、構成ログ設定の指定、構成ログの表示、HTMLおよびCSVレポートの生成を行うことができます。構成ログの表示は、日付範囲や全文検索結果でフィルタリングできます。強制ログが有効になっている場合、ログに記録できない構成変更は行えません。適切な権限があれば、構成ログからエントリを削除できます。構成ログ機能を使用してログコンテンツを編集することはできません。

構成ログは、PowerShell SDKと構成ログサービスを使用します。構成ログサービスは、サイト内のすべてのControllerで実行されます。いずれかのControllerが失敗した場合、別のControllerのサービスが自動的にログ要求を処理します。

デフォルトでは、構成ログ機能は有効になっており、サイト作成時に作成されるデータベース（サイト構成データベース）を使用します。データベースの別の場所を指定できます。構成ログデータベースは、サイト構成データベースと同じ高可用性機能をサポートしています。

構成ログへのアクセスは、委任管理を通じて、「ログ設定の編集」および「構成ログの表示」の権限で制御されます。

構成ログは作成時にローカライズされます。たとえば、英語で作成されたログは、リーダーのロケールに関係なく、英語で読み取られます。

ログに記録される内容

Studio、Director、およびPowerShellスクリプトから開始された構成変更と管理アクティビティがログに記録されます。ログに記録される構成変更の例には、以下に関する作業（作成、編集、削除、割り当て）が含まれます。

- マシンカタログ
- デリバリーグループ（電源管理設定の変更を含む）
- 管理者ロールとスコープ
- ホストリソースと接続
- Studioを介したCitrixポリシー

ログに記録される管理変更の例には、以下が含まれます。

- 仮想マシンまたはユーザーデスクトップの電源管理
- StudioまたはDirectorがユーザーにメッセージを送信する

次の操作はログに記録されません。

- プール管理による仮想マシンの電源投入などの自律的な操作。
- グループポリシー管理コンソール (GPMC) を介して実装されたポリシーアクション。これらのアクションのログを表示するには、Microsoftツールを使用してください。
- レジストリ、データベースへの直接アクセス、またはStudio、Director、PowerShell以外のソースを通じて行われた変更。
- 展開が初期化されると、最初の構成ログサービスインスタンスが構成サービスに登録されたときに、構成ログが利用可能になります。したがって、構成の初期段階（たとえば、データベーススキーマが取得および適用されるとき、ハイパーバイザーが初期化されるとき）はログに記録されません。

構成ログの管理

デフォルトでは、構成ログはサイトの作成時に作成されるデータベース（サイト構成データベースとも呼ばれます）を使用します。Citrixは、次の理由により、構成ログデータベース（および監視データベース）に別の場所を使用することを推奨します。

- 構成ログデータベースのバックアップ戦略は、サイト構成データベースのバックアップ戦略とは異なる可能性があります。
- 構成ログ（および監視サービス）のために収集されるデータ量によって、サイト構成データベースで利用可能な領域に悪影響が及ぶ可能性があります。
- これにより、3つのデータベースの単一障害点が分割されます。

構成ログをサポートしない製品エディションには、Studioにログノードがありません。

構成ログと強制ログの有効化と無効化

デフォルトでは、構成ログは有効になっており、強制ログは無効になっています。

1. Web Studio にサインインし、左側のペインで **Logging** を選択します。
2. アクションバーで **Preferences** を選択します。構成ログのダイアログボックスには、データベース情報が含まれており、構成ログと強制ログが有効か無効かを示します。
3. 希望するアクションを選択します。

   構成ログを有効にするには、**Enable** を選択します。これはデフォルト設定です。データベースに書き込みができない場合、ログ情報は破棄されますが、操作は続行されます。

   構成ログを無効にするには、**Disable** を選択します。以前にログが有効になっていた場合、既存のログはPowerShell SDKで読み取り可能です。

   強制ログを有効にするには、**Prevent changes to the site configuration when the database is not available** を選択します。通常ログに記録される構成変更や管理アクティビティは、構成ログデータベースに書き込みが可能な場合にのみ許可されます。強制ログは、構成ログが有効になっている場合（**Enable** が選択されている場合）にのみ有効にできます。構成ログサービスが失敗し、高可用性が使用されていない場合、強制ログが有効であると見なされます。そのような場合、通常ログに記録される操作は実行されません。

   強制ログを無効にするには、**Allow changes when to the site configuration when the database is not available** を選択します。構成ログデータベースにアクセスできない場合でも、構成変更と管理アクティビティが許可されます。これはデフォルト設定です。

構成ログデータベースの場所を変更する

強制ログが有効になっている場合、データベースの場所を変更することはできません。場所の変更には、ログに記録できない短い切断期間が含まれるためです。

1. サポートされているSQL Serverバージョンを使用して、データベースサーバーを作成します。
2. Web Studio にサインインし、左側のペインで **Logging** を選択します。

3. アクションバーで **Preferences** を選択します。
4. ログ設定ダイアログボックスで、**Change logging database** を選択します。
5. ログデータベースの変更ダイアログボックスで、新しいデータベースサーバーを含むサーバーの場所を指定します。有効な形式については、データベースアドレス形式を参照してください。
6. Studio がデータベースを作成できるようにするには、**OK** をクリックします。プロンプトが表示されたら **OK** をクリックすると、データベースが自動的に作成されます。Studio は、現在のStudioユーザーの資格情報を使用してデータベースにアクセスしようとします。それが失敗した場合、データベースユーザーの資格情報の入力を求められます。その後、Studio はデータベーススキーマをデータベースにアップロードします。（資格情報はデータベース作成中のみ保持されます。）
7. データベースを手動で作成するには、**データベーススクリプトの生成**をクリックします。生成されたスクリプトには、データベースを手動で作成するための手順が含まれています。スキーマをアップロードする前に、データベースが空であり、少なくとも1人のユーザーがデータベースにアクセスして変更する権限を持っていることを確認してください。

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

構成ログの内容を表示する

構成の変更や管理アクティビティを開始すると、StudioとDirectorによって作成された上位レベルの操作が、Studioの上部中央ペインに一覧表示されます。上位レベルの操作は、1つ以上のサービスおよびSDK呼び出し（下位レベルの操作）をもたらします。上部ペインで上位レベルの操作を選択すると、下部ペインに下位レベルの操作が表示されます。

操作が完了する前に失敗した場合、ログ操作がデータベースで完了しないことがあります。たとえば、開始レコードに対応する停止レコードがない場合があります。このような場合、ログには情報が不足していることが示されます。時間範囲に基づいてログを表示すると、ログ内のデータが条件に一致する場合、不完全なログが表示されます。たとえば、過去5日間のすべてのログが要求され、過去5日間に開始時刻があるが終了時刻がないログが存在する場合、それは含まれます。

PowerShellコマンドレットを呼び出すスクリプトを使用する場合、親の上位レベルの操作を指定せずに下位レベルの操作を作成すると、構成ログは代替の上位レベルの操作を作成します。

構成ログの内容を表示するには、Studioナビゲーションペインで ［**ログ**］ を選択します。デフォルトでは、中央ペインにログの内容が日付ごとに区切られ、時系列順（最新のエントリが最初）に一覧表示されます。次のことができます。

- 列ヘッダーで表示を並べ替える。
- 日数を指定するか、 ［**検索**］ ボックスにテキストを入力して表示をフィルター処理します。検索を使用した後に標準表示に戻るには、 ［**検索**］ ボックスのテキストをクリアします。

レポートを生成する

構成ログデータを含むCSVおよびHTMLレポートを生成できます。

- CSVレポートには、指定された時間間隔のすべてのログデータが含まれます。データベース内の階層データは、単一のCSVテーブルにフラット化されます。データのどの側面もファイル内で優先されません。書式設定は使用されず、人間が読み取れることは想定されていません。ファイル（MyReportという名前）には、普遍的に利用可能な形式でデータが含まれています。CSVファイルは、データのアーカイブや、Microsoft Excelなどのレポート作成ツールまたはデータ操作ツールのデータソースとしてよく使用されます。
- HTMLレポートは、指定された時間間隔のログデータを人間が読み取れる形式で提供します。変更を確認するための構造化されたナビゲート可能なビューを提供します。HTMLレポートは、SummaryとDetailsという名前の2つのファイルで構成されます。Summaryには、各操作がいつ、誰によって、どのような結果になったかなど、高レベルの操作が一覧表示されます。各操作の横にある**Details**リンクをクリックすると、Detailsファイル内の低レベルの操作に移動し、追加情報が表示されます。

構成ログレポートを生成するには、Studioナビゲーションペインで**Logging**を選択し、アクションバーで**Create custom report**を選択します。

- レポートの日付範囲を選択します。
- レポート形式（CSV、HTML、またはその両方）を選択します。
- レポートを保存する場所を参照します。

構成ログコンテンツを削除する

構成ログを削除するには、特定の委任管理権限とSQL Serverデータベース権限が必要です。

- **委任管理:** 展開構成の読み取りを許可する委任管理ロールが必要です。完全管理者ロールにはこの権限があります。カスタムロールには、カテゴリでまたはが選択されている必要があります。

構成ログデータを削除する前にバックアップを作成するには、カスタムロールのカテゴリでまたはが選択されている必要もあります。

- **SQL Serverデータベース:** データベースからレコードを削除する権限を持つSQL Serverログインが必要です。これには2つの方法があります。
  - データベースサーバー上のあらゆるアクティビティを実行できるsysadminサーバーロールを持つSQL Serverデータベースログインを使用します。または、`serveradmin`または`setupadmin`サーバーロールを使用すると、削除操作を実行できます。
  - 展開でより高いセキュリティが必要な場合は、データベースからレコードを削除する権限を持つデータベースユーザーにマッピングされた非sysadminデータベースログインを使用します。
    a. SQL Server Management Studioで、「sysadmin」以外のサーバーロールを持つSQL Serverログインを作成します。
    b. ログインをデータベース内のユーザーにマッピングします。SQL Serverは、ログインと同じ名前のユーザーをデータベース内に自動的に作成します。
    c. データベースロールメンバーシップで、データベースユーザーのロールメンバーのうち少なくとも1つを指定します: `ConfigurationLoggingSchema_ROLE` または `dbowner`。

    詳細については、SQL Server Management Studioのドキュメントを参照してください。

構成ログを削除するには:

1. Web Studioにサインインし、左ペインで**ログ**を選択します。
2. アクションバーで**ログの削除**を選択します。
3. ログを削除する前にバックアップを作成するかどうかを尋ねられます。バックアップを作成することを選択した場合、バックアップアーカイブが保存される場所を参照します。バックアップはCSVファイルとして作成されます。

構成ログがクリアされた後、ログの削除は空のログに投稿される最初のアクティビティです。そのエントリには、誰がいつログを削除したかに関する詳細が記載されています。

APIおよびPowerShellログの表示

現在のセッション中に作成されたAPIリクエストを監視するには、**API**タブをクリックします。APIログは、Web Studioからサインアウトするとクリアされます。

その日に行ったUIアクションに対応するPowerShellコマンドを表示するには、**PowerShell**タブをクリックします。

構成ログにメタデータを関連付ける

ログレコードに`MetadataMap`と呼ばれる`name-value`ペアを関連付けることで、構成ログにメタデータを添付できます。

> **注：**
>
> - メタデータは、高レベルの操作オブジェクトにのみ添付できます。
> - メタデータは、実行時に既存のレコードに関連付けられます。

メタデータを設定する

ログレコードを`MetadataMap`に関連付けるには、PowerShellコマンド`Set-LogHighLevelOperationMetadata`を実行します。 `Set-LogHighLevelOperationMetadata`は次のパラメーターを受け取ります。

- **Id**: 上位レベルの操作のID。
- **InputObject**: メタデータを追加する上位レベルの操作。これは、上位レベルの操作オブジェクトまたはオブジェクトのリストがPowerShellコマンドに渡される`Id`パラメーターの代替です。
- **Name**: 追加するメタデータのプロパティ名。このプロパティは、指定された上位レベルの操作に対して一意である必要があります。このプロパティには、次の文字を含めることはできません: ()\/;:#.*?=<>|'"。
- **Value**: プロパティの値。
- **Map**: プロパティの(名前、値)ペアの辞書。これは、`-Name`および`-Value`パラメーターを使用してメタデータを設定する代替手段です。

たとえば、Id 40を持つすべての高レベルログレコードにメタデータを添付するには、次のPowerShellコマンドを実行します。

```
Get-LogHighLevelOperation – Id 40 | Set-LogHighLevelOperationMetadata -Name A -Value B
```

ユーザー`abc@example.com`を持つ上位レベルのレコードにメタデータを添付するには、次のPowerShellコマンドを実行します。

```
Get-LogHighLevelOperation – User `abc@example.com` | Set-LogHighLevelOperationMetadata -Name C -Value D
```

メタデータを使用して取得する

関連付けられたメタデータを使用してログレコードを取得するには、次のPowerShellコマンドを実行します。

- キーと値で検索:

  ```
  Get-LogHighLevelOperation -Metadata "Key:Value"
  ```

- 値で任意のキーを検索:

  ```
  Get-LogHighLevelOperation -Metadata "*:Value"
  ```

- キーと任意の値で検索:

  ```
  Get-LogHighLevelOperation -Metadata "Key:*"
  ```

メタデータを削除する

関連付けられたメタデータを削除するには、PowerShell コマンド `Remove-LogHighLevelOperationMetadata` を実行します。 `Remove-LogHighLevelOperationMetadata` は次のパラメーターを受け入れます。

- **Id**: 高レベル操作のID。
- **InputObject**: メタデータを追加する高レベル操作。これは、高レベル操作オブジェクトまたはオブジェクトのリストがPowerShellコマンドに渡される `Id`` パラメーターの代替です。
- **Name**: 削除するメタデータのプロパティ名。指定されたオブジェクトのすべてのメタデータを削除するには、$null に設定します。
- **Map**: プロパティの (名前、値) ペアの辞書。これはハッシュテーブル (@{"name1" = "val1"; "name2" = "val2"} で作成) または文字列辞書 (new-object "System.Collections.Generic.Dictionary" で作成) のいずれかです。マップ内のキーと名前が一致するプロパティは削除されます。

イベントログ

以下の記事では、Citrix Virtual Apps and Desktops 内のサービスによってログに記録される可能性のあるイベントを一覧表示し、説明します。

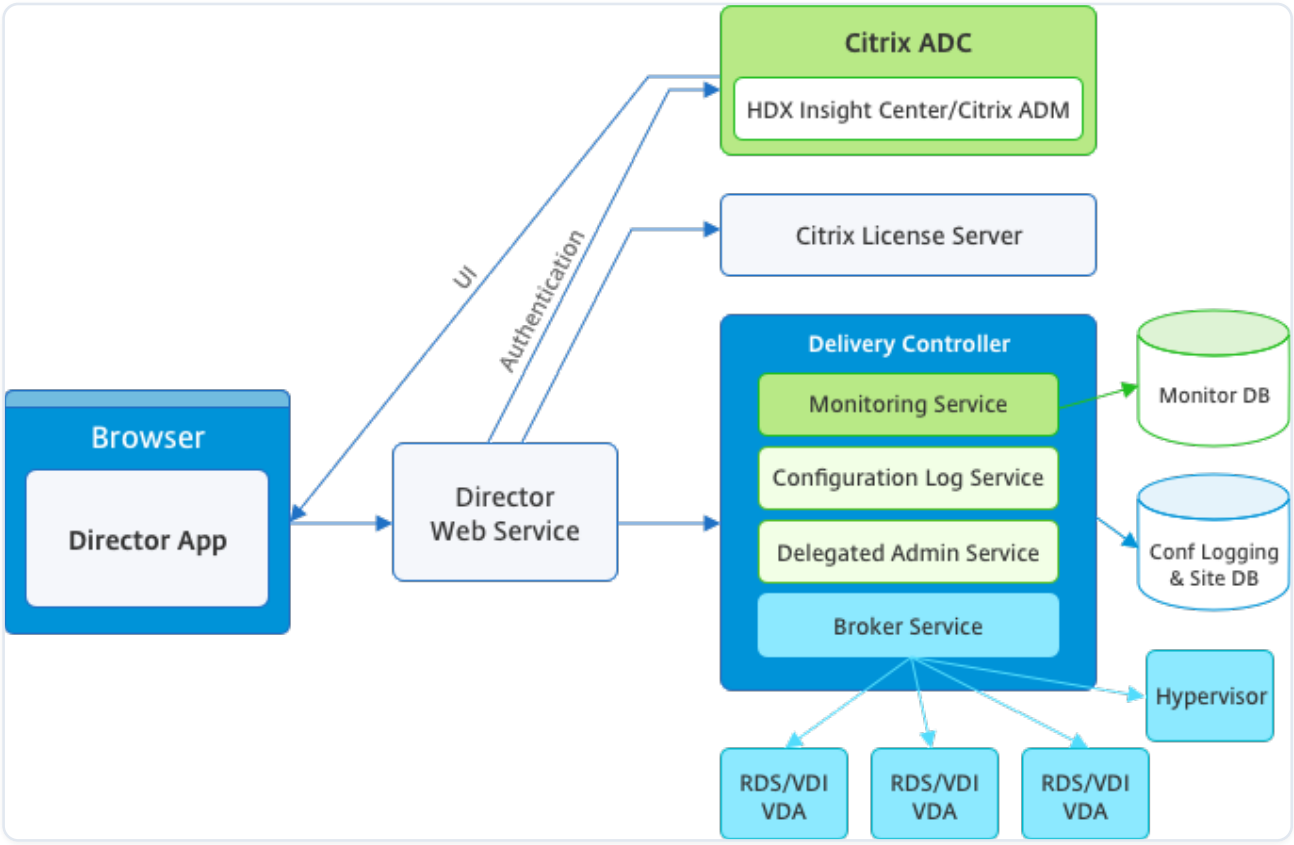
この情報は網羅的ではありません。読者は、追加のイベント情報について、個々の機能記事を確認してください。

- Citrix Broker Service イベント
- Citrix FMA Service SDK イベント

- シトリックス コンフィギュレーションサービス イベント
- シトリックス デリゲート管理サービス イベント

ディレクター

ディレクターは、Citrix Virtual Apps and Desktops 用の監視およびトラブルシューティングコンソールです。



ディレクターは以下にアクセスできます:

- Analytics、Performance Manager、および Network Inspector と統合された統合コンソールを使用して、Broker Agent からリアルタイムデータにアクセスします。以下の分析はCitrix ADMによって提供され、Citrix Virtual Apps™ または Desktops 環境におけるネットワークに起因するボトルネックを特定します:
  - 健全性と容量の保証のためのパフォーマンス管理
  - 履歴トレンドとネットワーク分析
- Configuration Loggingデータベースにアクセスするためにモニターデータベースに保存されている履歴データ。
- Citrix ADM を使用してCitrix Gateway からのICA®データ。

- Citrix Virtual Apps または Desktops の仮想アプリケーション、デスクトップ、およびユーザーのエンドユーザーエクスペリエンスの可視性を得る。
- 効果的なトラブルシューティングのために、ネットワークデータをアプリケーションデータおよびリアルタイムメトリックと関連付ける。
- Citrix Virtual Desktop 7 Director監視ツールと統合する。

ディレクターは、Citrix Virtual Apps または Desktops Site のリアルタイムおよび履歴の健全性監視を提供するトラブルシューティングダッシュボードを使用します。この機能により、リアルタイムで障害を確認でき、エンドユーザーが何を経験しているかをよりよく把握できます。

Director機能とDelivery Controller (DC)、VDA、およびその他の依存コンポーネントとの互換性に関する詳細については、「機能互換性マトリックス」を参照してください。

> **注：**
>
> MeltdownおよびSpectreの投機的実行サイドチャネル脆弱性の開示に伴い、Citrixは、関連する緩和パッチをインストールすることを推奨します。これらのパッチはSQL Serverのパフォーマンスに影響を与える可能性があります。詳細については、Microsoftサポート記事「SpectreおよびMeltdownサイドチャネル脆弱性からのSQL Serverの保護」を参照してください。Citrixは、本番環境にパッチを展開する前に、規模をテストし、ワークロードを計画することを推奨します。

> Director は、デフォルトで Delivery Controller 上の Web サイトとしてインストールされます。前提条件およびその他の詳細については、このリリースの システム要件 ドキュメントを参照してください。Director のインストールと構成に関する具体的な情報については、Director のインストールと構成 を参照してください。

Director へのログオン

Director の Web サイトは、https または `http://<Server FQDN>/Director` にあります。

マルチサイト展開でいずれかのサイトがダウンしている場合、ダウンしているサイトへの接続を試行するため、ログオンに少し時間がかかります。

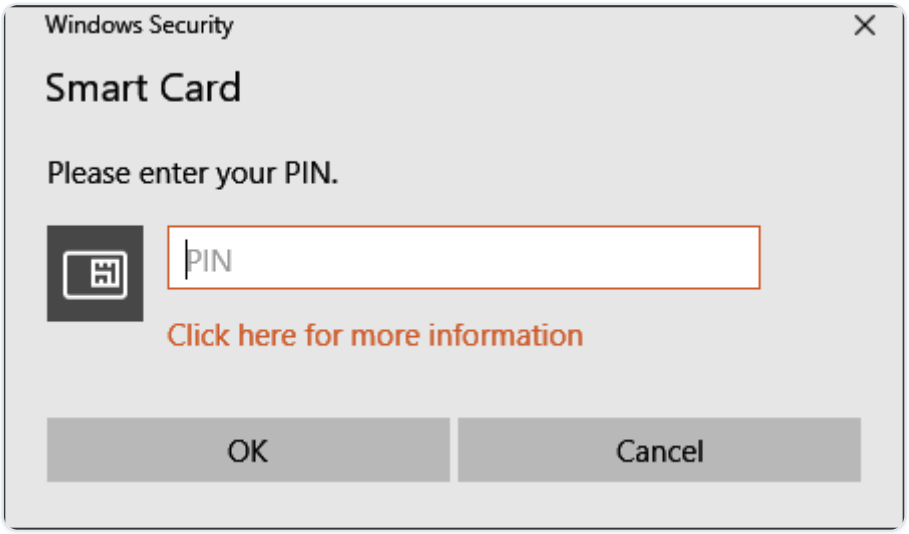
PIV スマートカード認証での Director の使用

Director は、Personal Identity Verification (PIV) ベースのスマートカード認証によるログオンをサポートするようになりました。この機能は、アクセス制御にスマートカードベースの認証を使用する組織や政府機関にとって有用です。 スマートカード認証には、Director サーバーおよび Active Directory での特定の構成が必要です。構成手順については、PIV スマートカード認証の構成 で詳しく説明されています。

> **注：**
>
> スマートカード認証は、同じ Active Directory ドメインのユーザーのみがサポートされます。

必要な構成を実行した後、スマートカードを使用して Director にログオンできます。

1. スマートカードをスマートカードリーダーに挿入します。
2. ブラウザーを開き、Director の URL `https://<directorfqdn>/Director` にアクセスします。
3. 表示されたリストから有効なユーザー証明書を選択します。
4. スマートカードトークンを入力します。



5. 認証されると、Director ログオンページで追加の資格情報を入力することなく Director にアクセスできます。

統合 Windows 認証での Director の使用

統合Windows認証（IWA）を使用すると、ドメイン参加ユーザーはDirectorログオンページで資格情報を再入力することなく、Directorに直接アクセスできます。統合Windows認証とDirectorを使用するための前提条件は次のとおりです。

- DirectorをホストするIIS Webサイトで統合Windows認証を有効にします。Directorをインストールすると、匿名認証とフォーム認証が有効になります。統合Windows認証とDirectorをサポートするには、匿名認証を無効にし、Windows認証を有効にします。ドメイン外のユーザーの認証のために、フォーム認証は有効のままにしておく必要があります。

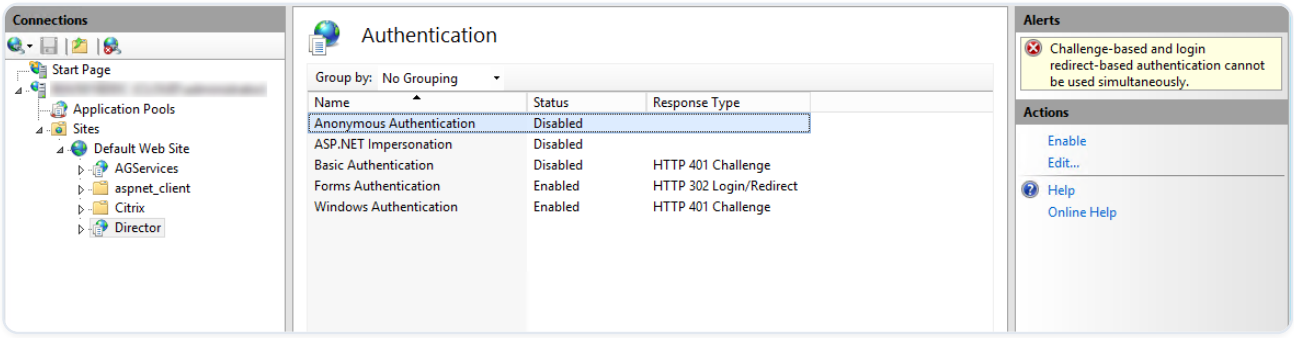
  a. IISマネージャーを起動します。

  b. **サイト** \> **既定のWebサイト** \> **Director**に移動します。

  c. **認証**を選択します。

  d. **匿名認証**を右クリックし、**無効**を選択します。

  e. **Windows認証**を右クリックし、**有効**を選択します。



- Directorマシンに対してActive Directoryの委任権限を構成します。構成が必要となるのは、DirectorとDelivery Controller™が別々のマシンにインストールされている場合のみです。

  a. Active Directoryマシンで、Active Directory管理コンソールを開きます。

  b. Active Directory管理コンソールで、**ドメイン名** \> **コンピューター**に移動します。Directorマシンを選択します。

  c. 右クリックして**プロパティ**を選択します。

  d. プロパティで、**委任**タブを選択します。

  e. **このコンピューターを、任意のサービスへの委任のために信頼する（Kerberosのみ）**オプションを選択します。

- Directorへのアクセスに使用するブラウザーは、統合Windows認証をサポートしている必要があります。FirefoxおよびChromeでは、追加の構成手順が必要になる場合があります。詳細については、ブラウザーのドキュメントを参照してください。

- 監視サービスは、Microsoft .NET Framework 4.5.1 以降の、Director のシステム要件に記載されているサポート対象バージョンを実行している必要があります。詳しくは、「」(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/system-requirements.html#citrix-director)を参照してください。

ユーザーがDirectorからログオフするか、セッションがタイムアウトすると、ログオンページが表示されます。ログオンページから、ユーザーは認証の種類を**自動ログオン**または**ユーザー資格情報**に設定できます。

インターフェイスビュー

Directorは、特定の管理者向けに調整されたさまざまなインターフェイスビューを提供します。製品の権限によって、表示される内容と利用可能なコマンドが決まります。

たとえば、ヘルプデスク管理者は、ヘルプデスクタスクに合わせて調整されたインターフェイスを表示します。Directorを使用すると、ヘルプデスク管理者は問題を報告しているユーザーを検索し、そのユーザーに関連付けられたアクティビティを表示できます。たとえば、ユーザーのアプリケーションとプロセスのステータスなどです。応答しないアプリケーションやプロセスを終了する、ユーザーのマシンでシャドウ操作を実行する、マシンを再起動する、ユーザープロファイルをリセットするなどのアクションを実行することで、問題を迅速に解決できます。

対照的に、完全な管理者はサイト全体を表示および管理し、複数のユーザーおよびマシンに対してコマンドを実行できます。ダッシュボードは、セッションのステータス、ユーザーログオン、サイトインフラストラクチャなど、展開の主要な側面を概観できます。情報は毎分更新されます。問題が発生した場合、発生した障害の数と種類に関する詳細が自動的に表示されます。

Directorにおけるさまざまな役割とその権限について詳しくは、「」(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/director/install-and-configure/permissions.html)を参照してください。

Google Analyticsによる使用状況データの収集

Directorのインストール後、DirectorサービスはGoogle Analyticsを使用して使用状況データの収集を開始します。トレンドページの使用状況に関する統計とOData API呼び出し分析が収集されます。分析データの収集は、Citrixプライバシーポリシーに準拠しています。Directorをインストールすると、データ収集はデフォルトで有効になります。

Google Analyticsのデータ収集をオプトアウトするには、Directorがインストールされているマシンでレジストリキーを編集します。レジストリキーが存在しない場合は、作成して目的の値に設定します。レジストリキーの値を変更した後、Directorインスタンスを更新してください。

注意：レジストリエディターを誤って使用すると、オペレーティングシステムの再インストールが必要になる深刻な問題が発生する可能性があります。Citrixは、レジストリエディターの誤用によって発生した問題が解決されることを保証できません。レジストリエディターは、ご自身の責任において使用してください。Citrixは、Windowsレジストリを変更する前にバックアップすることをお勧めします。

場所：HKEY_LOCAL_MACHINE\Software\Citrix\Director

名前：DisableGoogleAnalytics

値：0 = 有効（デフォルト）、1 = 無効

Google Analyticsによるデータ収集を無効にするには、次のPowerShellコマンドレットを使用できます。

```
New-Item HKLM:\SOFTWARE\Citrix -Name Director



New-ItemProperty HKLM:\SOFTWARE\Citrix\Director -Name
DisableGoogleAnalytics -PropertyType DWORD -Value 1
```

新機能ガイド

Directorには、Pendoを使用して、現在のバージョンのDirectorでリリースされた新機能に関する洞察を提供する製品内ガイドがあります。適切な製品内メッセージと組み合わせた簡単な概要は、製品の新機能を理解するのに役立ちます。

この機能をオプトアウトするには、Directorがインストールされているマシンで、以下に説明するようにレジストリキーを編集します。レジストリキーが存在しない場合は、作成して目的の値に設定します。レジストリキーの値を変更した後、Directorインスタンスを更新してください。

注意:

レジストリエディターを誤って使用すると、オペレーティングシステムの再インストールが必要になるような深刻な問題が発生する可能性があります。Citrixは、レジストリエディターの誤った使用に起因する問題が解決できることを保証できません。レジストリエディターは自己責任で使用してください。Citrixは、変更を加える前にWindowsレジストリをバックアップすることをお勧めします。

> 場所: HKEY_LOCAL_MACHINE\Software\Citrix\Director

名前: DisableGuidedHelp

値: 0 = 有効（デフォルト）、1 = 無効

製品内ガイドを無効にするには、次のPowerShellコマンドレットを使用できます。

```
New-Item HKLM:\SOFTWARE\Citrix -Name Director



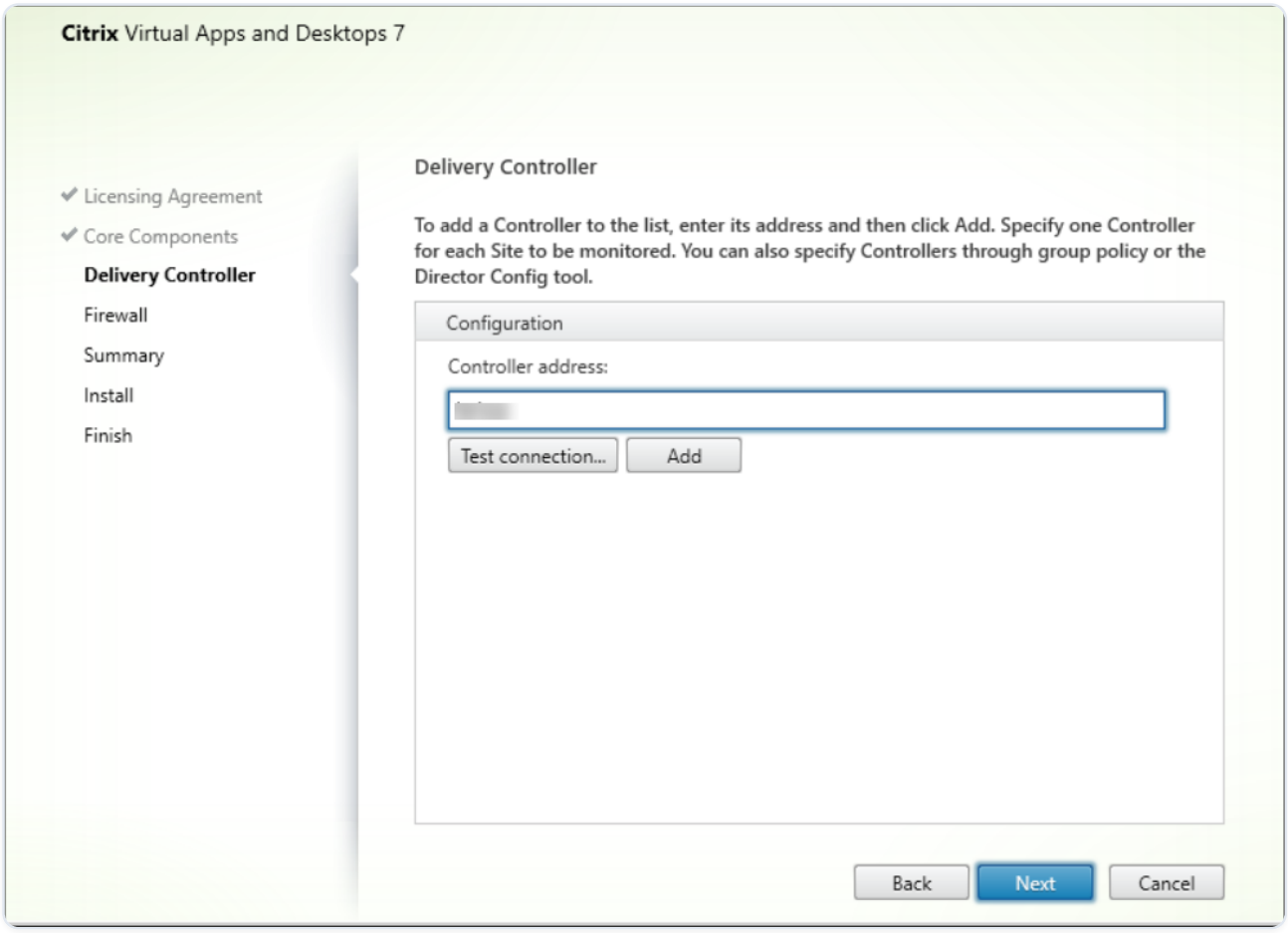
New-ItemProperty HKLM:\SOFTWARE\Citrix\Director -Name DisableGuidedHelp
-PropertyType DWORD -Value 1
```

インストールと構成

Directorのインストール

Citrix Virtual Apps and Desktopsのフル製品ISOインストーラーを使用してDirectorをインストールします。これにより、前提条件の確認、不足しているコンポーネントのインストール、Director Webサイトのセットアップ、および基本的な構成が実行されます。前提条件およびその他の詳細については、このリリースのシステム要件ドキュメントを参照してください。このリリースのDirectorは、Virtual Apps 6.5より前の展開、またはVirtual Desktops 7より前の展開とは互換性がありません。 ISOインストーラーによって提供されるデフォルト構成は、一般的な展開に対応します。インストール時にDirectorが含まれていなかった場合は、ISOインストーラーを使用してDirectorを追加します。追加のコンポーネントを追加するには、ISOインストーラーを再実行し、インストールするコンポーネントを選択します。ISOインストーラーの使用方法については、インストールドキュメントのコアコンポーネントのインストールを参照してください。Citrixでは、.MSIファイルではなく、フル製品ISOインストーラーのみを使用してインストールすることをお勧めします。

DirectorがControllerにインストールされている場合、サーバーアドレスとしてlocalhostが自動的に構成され、Directorはデフォルトでローカルのcontrollerと通信します。Controllerから離れた専用サーバーにDirectorをインストールする場合は、ControllerのFQDNまたはIPアドレスを入力するよう求められます。



注：

追加をクリックして、監視するControllerを追加します。

Directorはデフォルトで、指定されたControllerと通信します。監視するサイトごとにControllerアドレスを1つだけ指定してください。Directorは、同じサイト内の他のすべてのControllerを自動的に検出し、指定したControllerが失敗した場合は、それらの他のControllerにフォールバックします。

注：

DirectorはController間で負荷分散を行いません。

ブラウザーとWebサーバー間の通信を保護するために、Citrix®は、DirectorをホストするIIS WebサイトでTLSを実装することをお勧めします。手順については、Microsoft IISのドキュメントを参照してください。TLSを有効にするためにDirectorの構成は必要ありません。

Directorの展開と構成

Directorが複数のサイトを含む環境で使用される場合、Controller、Director、およびその他のコアコンポーネントがインストールされているすべてのサーバーでシステムクロックを同期してください。そうしないと、Directorでサイトが正しく表示されない可能性があります。

> **重要:**
>
> ネットワーク経由でプレーンテキストで送信されるユーザー名とパスワードのセキュリティを保護するため、Director接続にはHTTPではなくHTTPSのみを使用してください。特定のツールは、HTTP（暗号化されていない）ネットワークパケット内のプレーンテキストのユーザー名とパスワードを読み取ることができ、ユーザーにとって潜在的なセキュリティリスクを生み出す可能性があります。

権限の構成

Directorにログオンするには、Directorの権限を持つ管理者はActive Directoryドメインユーザーであり、以下の権限を持っている必要があります。

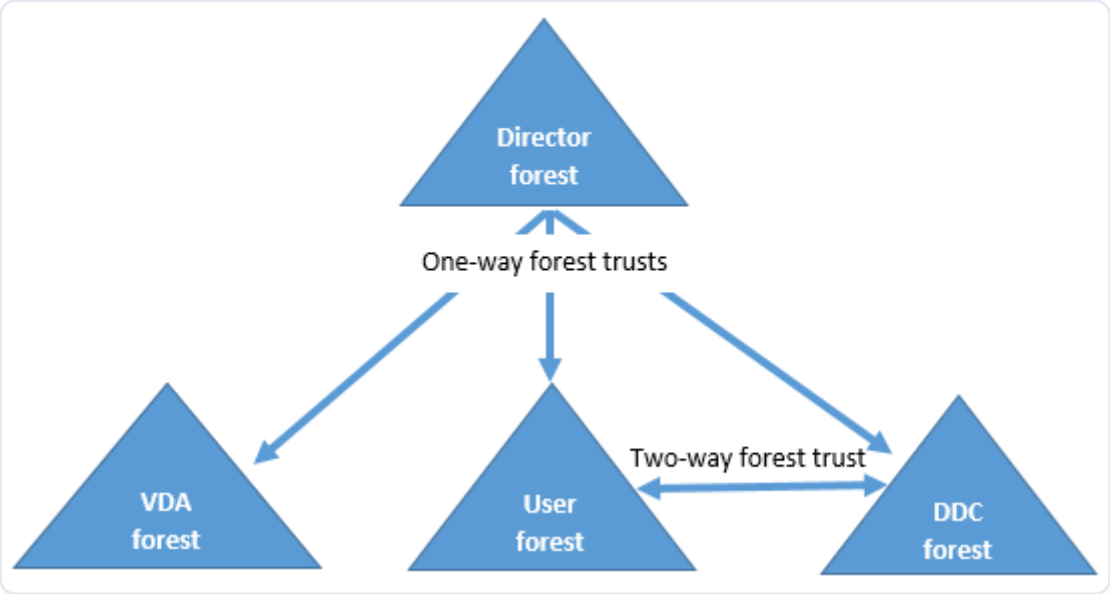
- 検索対象となるすべてのActive Directoryフォレストにおける読み取り権限（高度な構成を参照）。
- 構成された委任管理者ロール ((/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/director/install-and-configure/permissions.html)の「委任管理とDirector」を参照)。
- ユーザーをシャドウするには、管理者はWindowsリモートアシスタンス用のMicrosoftグループポリシーを使用して構成する必要があります。さらに：
  - VDAをインストールする際、すべてのユーザーデバイスでWindowsリモートアシスタンス機能が有効になっていることを確認してください（デフォルトで選択されています）。
  - Directorをサーバーにインストールする場合、Windowsリモートアシスタンスがインストールされていることを確認してください（デフォルトで選択されています）。ただし、サーバーではデフォルトで無効になっています。Directorがエンドユーザーにアシスタンスを提供するために、この機能を有効にする必要はありません。Citrixは、サーバーのセキュリティを向上させるために、この機能を無効のままにしておくことを推奨します。
  - 管理者がWindowsリモートアシスタンスを開始できるようにするには、リモートアシスタンス用の適切なMicrosoftグループポリシー設定を使用して、必要な権限を付与します。詳しくは、CTX127388: How to Enable Remote Assistance for Desktop Directorを参照してください。

高度な構成

Directorは、ユーザー、Delivery Controller (DC)、VDA、およびDirectorが異なるフォレストに配置されているフォレスト構成にまたがるマルチフォレスト環境をサポートできます。これには、フォレスト間の信頼関係と構成設定の適切なセットアップが必要です。

マルチフォレスト環境での推奨構成

推奨される構成では、フォレスト間で送信および受信フォレスト信頼関係を作成し、ドメイン全体の認証を行う必要があります。



Directorからの信頼関係により、異なるフォレストに配置されているユーザーセッション、VDA、およびDelivery Controllerの問題をトラブルシューティングできます。

Directorが複数のフォレストをサポートするために必要な高度な構成は、Internet Information Services (IIS) マネージャーで定義された設定によって制御されます。

> **重要:**
>
> IISで設定を変更すると、Directorサービスが自動的に再起動し、ユーザーがログオフされます。

> IISを使用して高度な設定を構成するには：

1. Internet Information Services (IIS) マネージャーコンソールを開きます。
2. デフォルトのWebサイトの下にあるDirector Webサイトに移動します。
3. **アプリケーション設定**をダブルクリックします。

4. 設定をダブルクリックして編集します。
5. **追加**をクリックして新しい設定を追加します。

DirectorはActive Directoryを使用してユーザーを検索し、より多くのユーザーおよびマシン情報を参照します。デフォルトでは、Directorは次のドメインまたはフォレストを検索します。

- 管理者アカウントがメンバーです。
- Director Webサーバーがメンバーです（異なる場合）。

Directorは、Active Directoryグローバルカタログを使用してフォレストレベルで検索を実行しようとします。フォレストレベルで検索する権限がない場合、ドメインのみが検索されます。

別のActive Directoryドメインまたはフォレストからデータを検索または参照するには、検索するドメインまたはフォレストを明示的に設定する必要があります。IISマネージャーでDirector Webサイトに次のアプリケーション設定を構成します。

```
Connector.ActiveDirectory.Domains = (user),(server)
```

値属性のuserとserverは、それぞれDirectorユーザー（管理者）とDirectorサーバーのドメインを表します。

追加のドメインまたはフォレストからの検索を有効にするには、この例に示すように、ドメイン名をリストに追加します。

```
Connector.ActiveDirectory.Domains = (user),(server),\&lt;domain1\>,
\&lt;domain2\>
```

リスト内の各ドメインについて、Directorはフォレストレベルで検索を実行しようとします。フォレストレベルで検索する権限がない場合、ドメインのみが検索されます。

ドメインローカルグループの構成

ほとんどのCitrixサービスプロバイダー（CSP）は、インフラストラクチャフォレストにVDA、DC、およびDirectorで構成される同様の環境設定を持っています。ユーザーまたはユーザーグループのレコードは顧客フォレストに属します。インフラストラクチャフォレストから顧客フォレストへの一方向の送信信頼が存在します。

CSP管理者は通常、インフラストラクチャフォレストにドメインローカルグループを作成し、顧客フォレストのユーザーまたはユーザーグループをこのドメインローカルグループに追加します。

推奨されるマルチフォレストサイト構成(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/domainlocalgroup-config.png)

Directorはこのようなマルチフォレスト設定をサポートし、ドメインローカルグループを使用して構成されたユーザーのセッションを監視できます。

1. IISマネージャーでDirector Webサイトに次のアプリケーション設定を追加します。

   ```
   Connector.ActiveDirectory.DomainLocalGroupSearch= true



   DomainLocalGroupSearchDomains= \&lt;domain1\>,\&lt;domain2\>
   ```

   \<domain1\>\<domain2\> は、ドメインローカルグループが存在するフォレストの名前です。
2. Web Studioでドメインローカルグループをデリバリーグループに割り当てます。
3. 変更を有効にするには、IISを再起動し、Directorに再度ログオンします。これで、Directorはこれらのユーザーのセッションを監視し、表示できるようになります。

Directorにサイトを追加する

Directorがすでにインストールされている場合は、複数のサイトで動作するように構成します。構成するには、各DirectorサーバーでIISマネージャーコンソールを使用して、アプリケーション設定のサーバーアドレスリストを更新します。

次の設定に、各サイトのControllerのアドレスを追加します。

```
Service.AutoDiscoveryAddresses = SiteAController,SiteBController
```

SiteAControllerとSiteBControllerは、異なる2つのサイトのDelivery Controllerのアドレスです。

アクティビティマネージャーで実行中のアプリケーションの可視性を無効にする

デフォルトでは、DirectorのActivity Managerは、ユーザーセッションのすべての実行中アプリケーションのリストを表示します。この情報は、DirectorのActivity Manager機能にアクセスできるすべての管理者が閲覧できます。委任された管理者ロールの場合、これには完全管理者、デリバリーグループ管理者、およびヘルプデスク管理者が含まれます。

ユーザーのプライバシーと実行中のアプリケーションを保護するために、**アプリケーション**タブを無効にして、実行中のアプリケーションを一覧表示しないようにすることができます。

警告:

レジストリを誤って編集すると、オペレーティングシステムを再インストールする必要があるような深刻な問題が発生する可能性があります。Citrix® は、レジストリエディターの誤った使用によって生じる問題が解決されることを保証しません。レジストリエディターは自己責任で使用してください。編集する前に必ずレジストリをバックアップしてください。

1. VDAで、`HKEY_LOCAL_MACHINE\Software\Citrix\Director\TaskManagerDataDisplayed` のレジストリキーを変更します。デフォルトでは、キーは1に設定されています。値を0に変更します。これは、VDAから情報が収集されず、Activity Managerに表示されないことを意味します。
2. Directorがインストールされているサーバーで、実行中のアプリケーションの可視性を制御する設定を変更します。デフォルトでは、値は「true」であり、アプリケーションタブで実行中のアプリケーションの可視性を許可します。値を「false」に変更すると、可視性が無効になります。このオプションは、VDAではなく、DirectorのActivity Managerのみに影響します。 次の設定の値を変更します。 UI.TaskManager.EnableApplications = false

重要:

実行中のアプリケーションの表示を無効にするには、Activity Managerにデータが表示されないように、両方の変更を行ってください。

PIVスマートカード認証の構成

この記事では、スマートカード認証機能を有効にするためにDirectorサーバーとActive Directoryで必要な構成を一覧表示します。

注：

スマートカード認証は、同じActive Directoryドメインのユーザーのみサポートされます。

Directorサーバーの構成

Directorサーバーで次の構成手順を実行します。

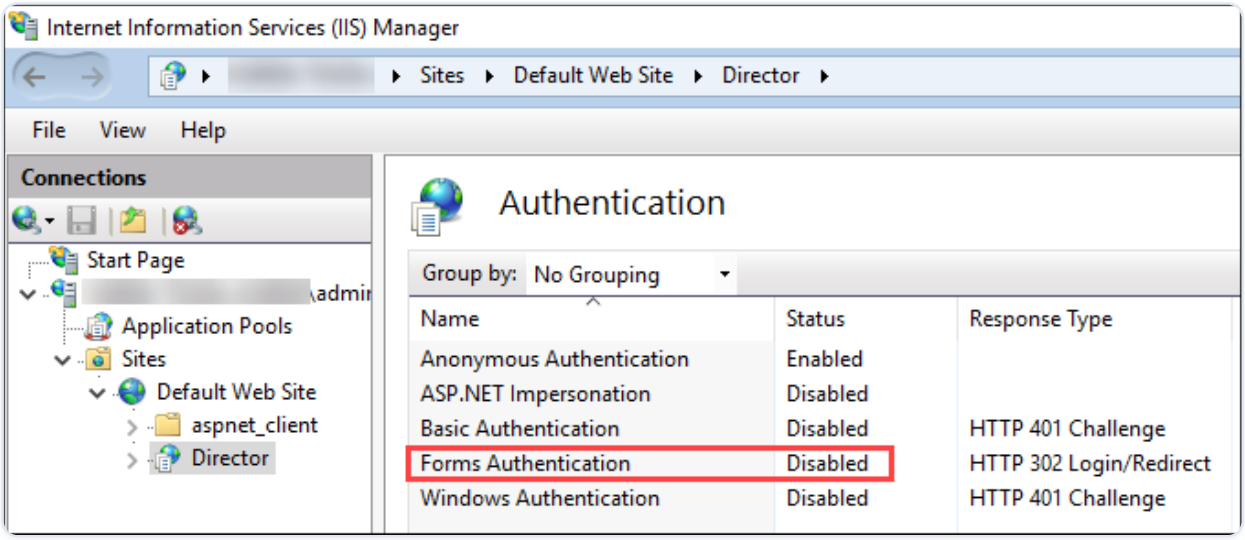
1. クライアント証明書マッピング認証をインストールして有効にします。Microsoftドキュメントのクライアント証明書マッピング認証に記載されている**Active Directory を使用したクライアント証明書マッピング認証**の手順に従います。
2. Directorサイトでフォーム認証を無効にします。

   IISマネージャーを起動します。

   サイト \> **Default Web Site** \> **Director**に移動します。

   認証を選択します。

   フォーム認証を右クリックし、**無効**を選択します。



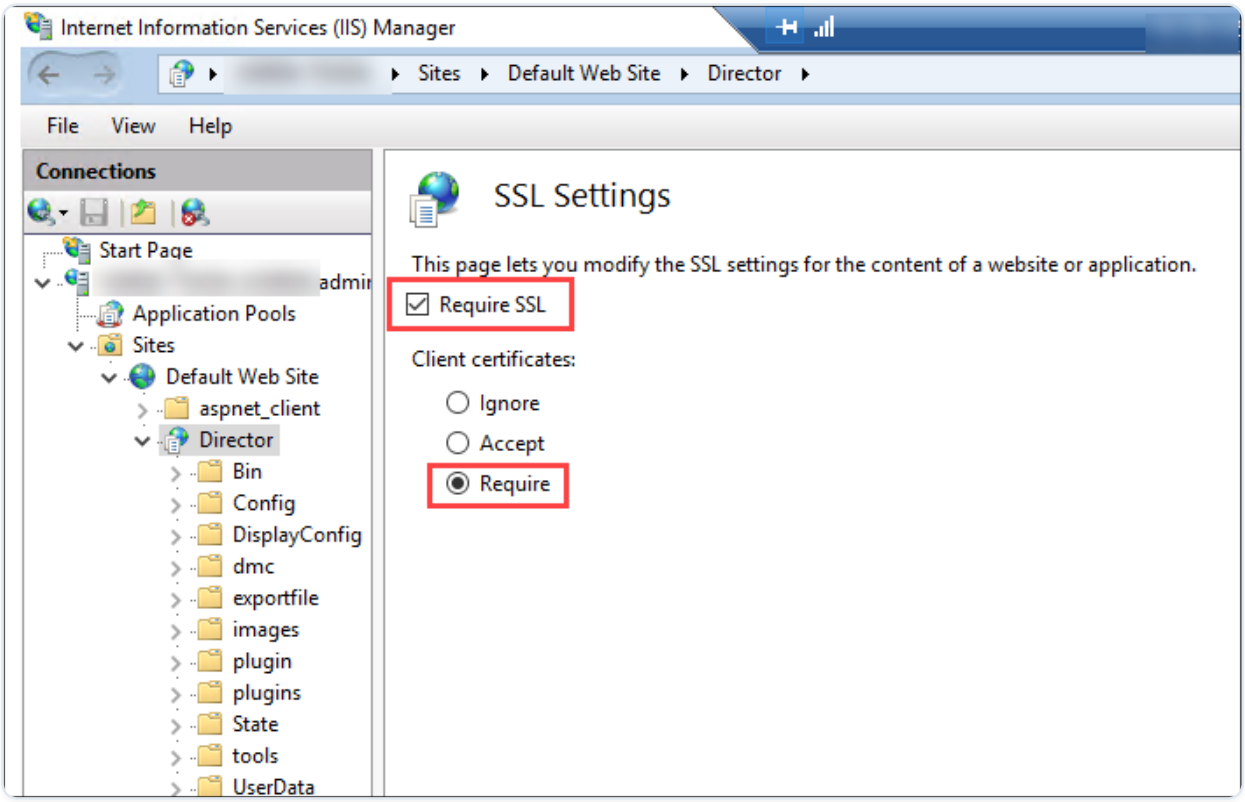
3. クライアント証明書認証のために、Director URLをより安全なhttpsプロトコル (HTTPではなく) 用に構成します。

   a. IISマネージャーを起動します。

   b. **サイト** \> **Default Web Site** \> **Director**に移動します。

   c. **SSL設定**を選択します。

   d. **SSLを必須にする**と**クライアント証明書** \> **必須**を選択します。



4. web.configを更新します。テキストエディターを使用して、web.configファイル（`c:\inetpub\wwwroot\Director`にあります）を開きます。

`<system.webServer>`親要素の下に、次のスニペットを最初の子要素として追加します。

```
&lt;defaultDocument>

   &lt;files>

       &lt;add value="LogOn.aspx"/>

   &lt;/files>

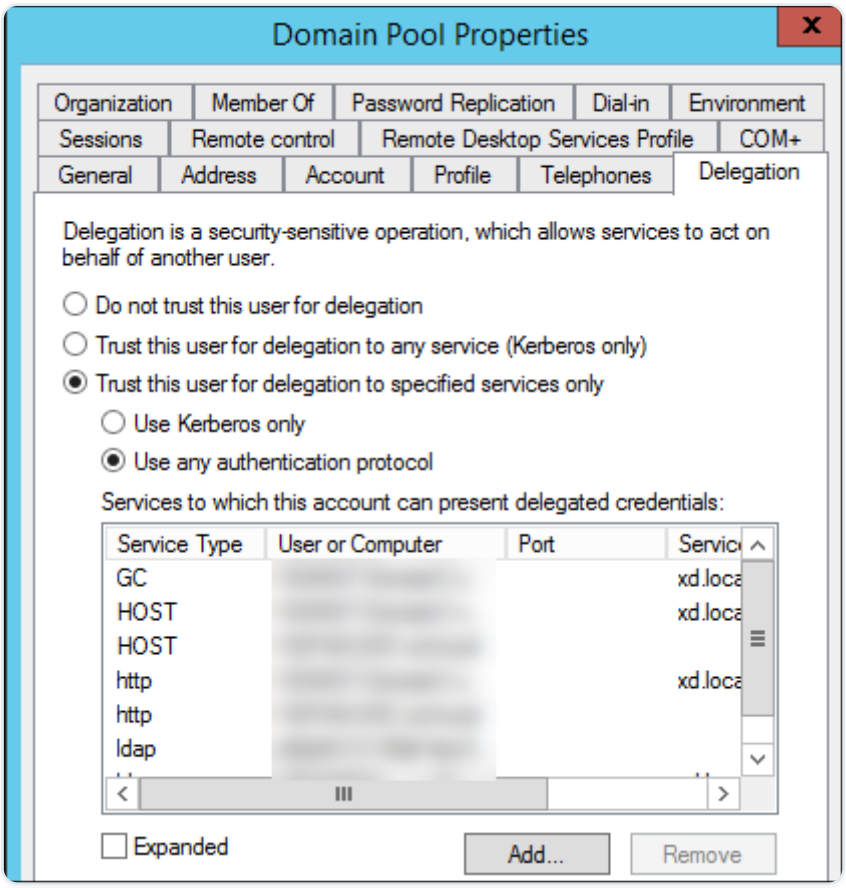
&lt;/defaultDocument>
```

Active Directoryの構成

デフォルトでは、Directorアプリケーションは**アプリケーションプール**のIDプロパティで実行されます。スマートカード認証には委任が必要であり、そのためにはDirectorアプリケーションのIDがサービスホスト上でTrusted Computing Base（TCB）権限を持っている必要があります。

Citrixでは、アプリケーションプールID用に個別のサービスアカウントを作成することをお勧めします。Microsoft MSDNの記事「Protocol Transition with Constrained Delegation Technical Supplement」の手順に従って、サービスアカウントを作成し、TCB権限を割り当ててください。

新しく作成したサービスアカウントをDirectorアプリケーションプールに割り当てます。次の図は、サンプルサービスアカウント「Domain Pool」のプロパティダイアログを示しています。

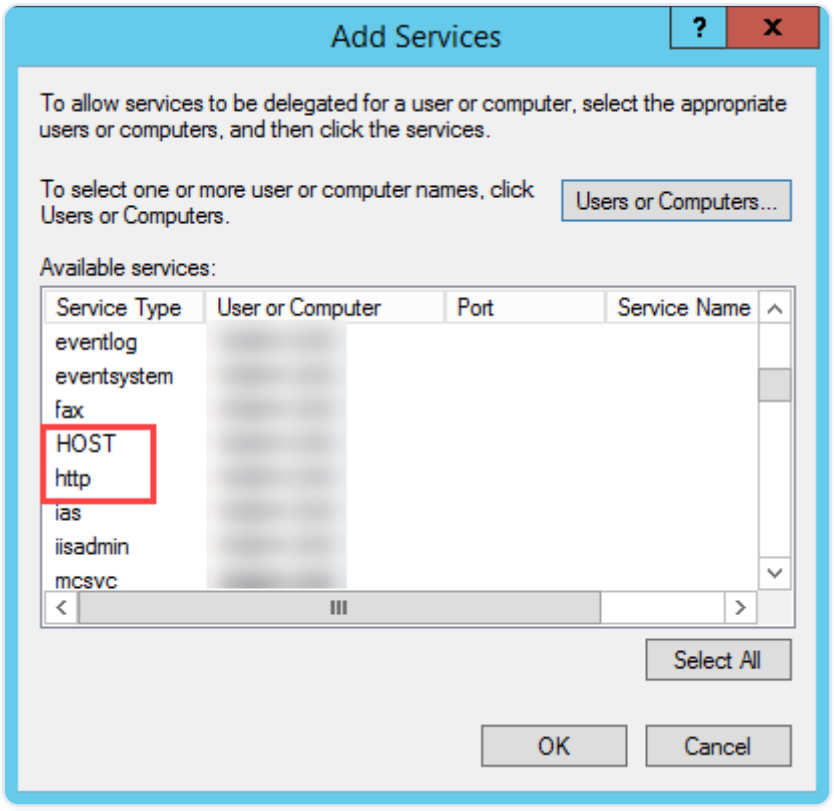


このアカウントに対して、次のサービスを構成します。

- デリバリーコントローラー™: ホスト、HTTP
- Director: ホスト、HTTP
- アクティブディレクトリ：GC、LDAP

構成するには、,

1. ユーザーアカウントのプロパティダイアログで、 をクリックします。
2. ダイアログで、 または をクリックします。
3. Delivery Controllerのホスト名を選択します。
4. の一覧から、 と の を選択します。



同様に、**Director** および **Active Directory** ホストのサービスの種類を追加します。

サービスプリンシパル名レコードを作成する

各Directorサーバーと、Directorサーバーのプールへのアクセスに使用される負荷分散された仮想IP（VIP）ごとにサービスアカウントを作成する必要があります。新しく作成されたサービスアカウントへの委任を構成するには、サービスプリンシパル名（SPN）レコードを作成する必要があります。

- DirectorサーバーのSPNレコードを作成するには、次のコマンドを使用します。

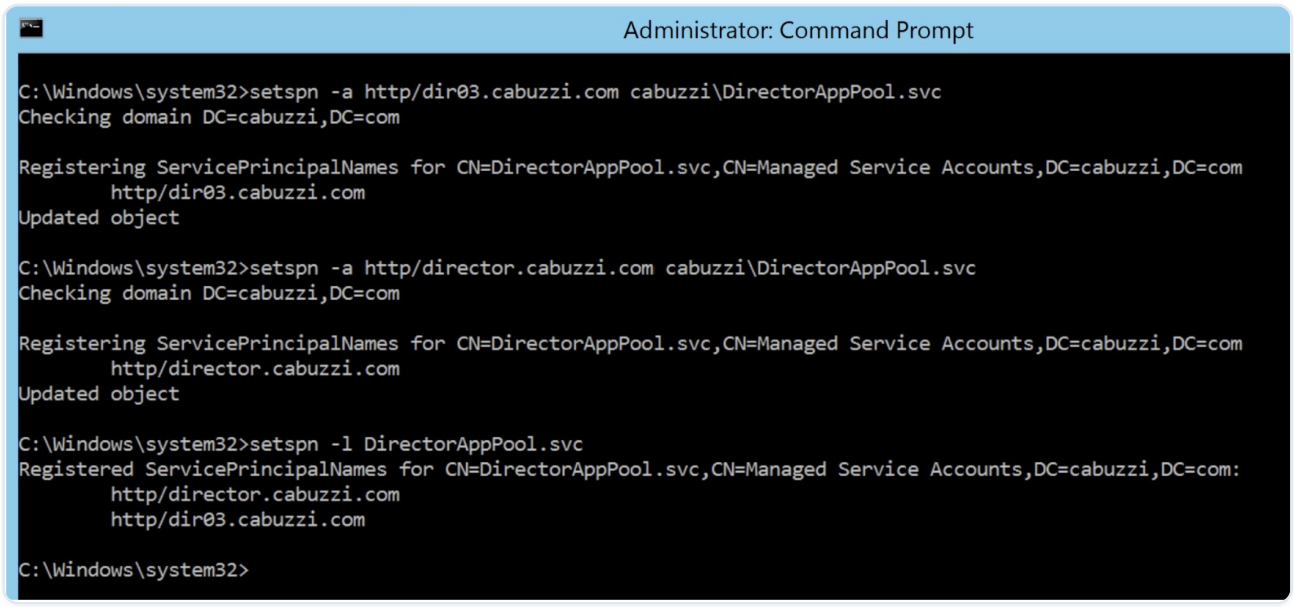
```
  setspn -a http/<directorServer>.<domain_fqdn>
<domain>\<DirectorAppPoolServiceAcct>
```

- 負荷分散されたVIPのSPNレコードを作成するには、次のコマンドを使用します。

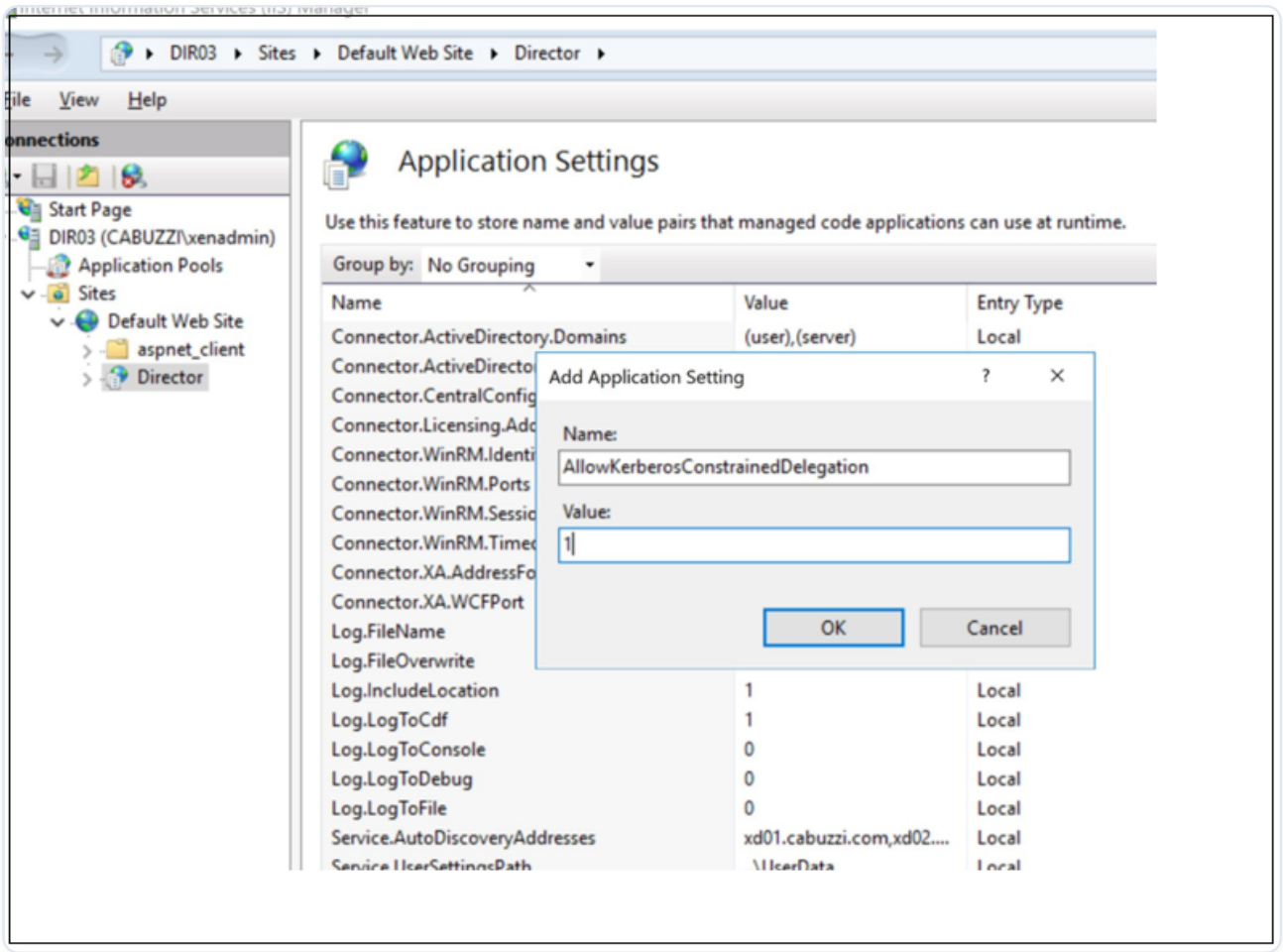
```
  setspn -S http/<DirectorFQDN> <domain>\<DirectorAppPoolServiceAcct>
```

- 作成されたSPNを表示またはテストするには、次のコマンドを使用します。

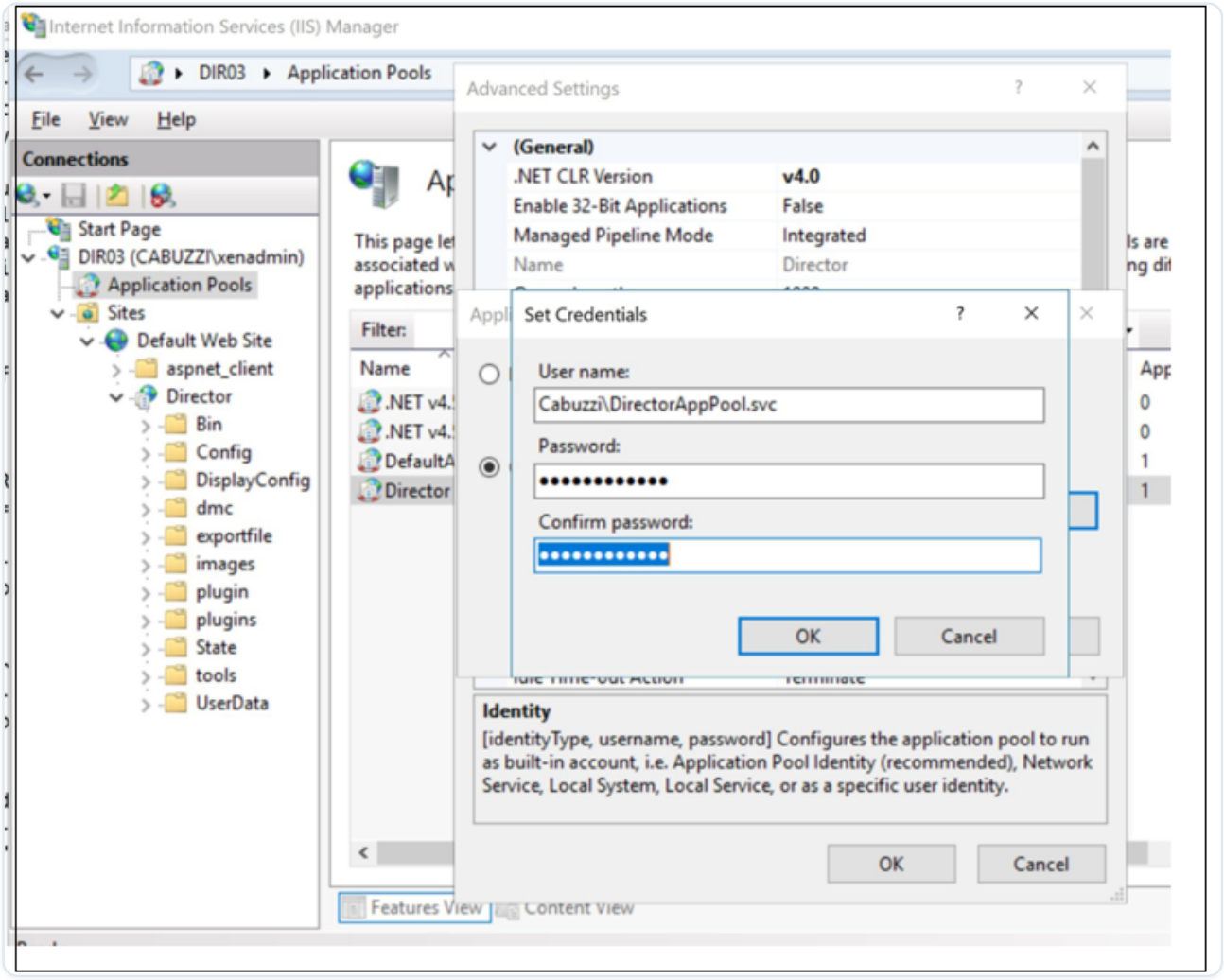
```
setspn –l <DirectorAppPoolServiceAcct>
```



- 左ペインでDirector仮想ディレクトリを選択し、 をダブルクリックします。 ウィンドウで をクリックし、**AllowKerberosConstrainedDelegation** が1に設定されていることを確認します。



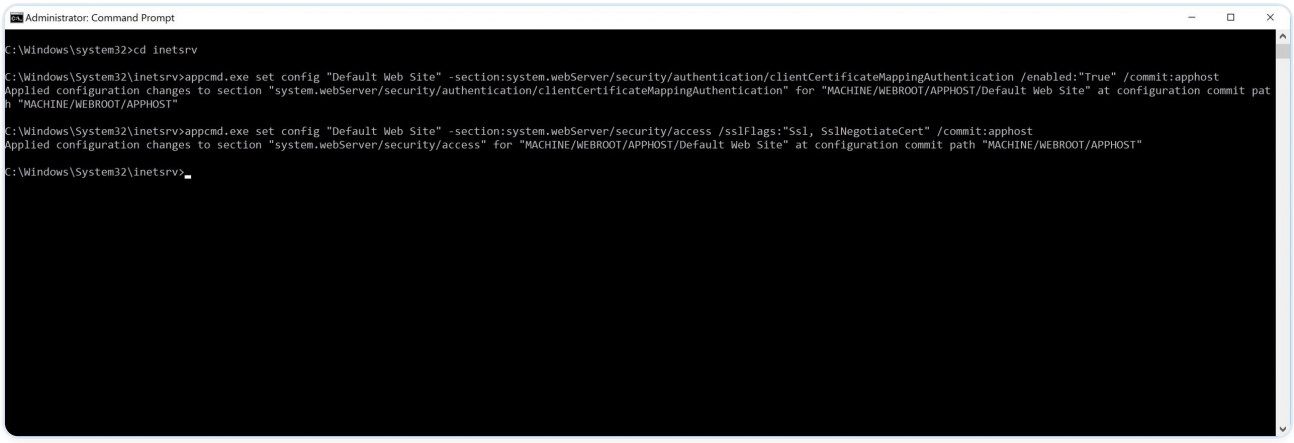
- 左側のペインで を選択し、Directorアプリケーションプールを右クリックして を選択します。
- 「**Identity**」を選択し、省略記号（「…」）をクリックしてサービスアカウントのドメイン\ログオンとパスワードの資格情報を入力します。IISコンソールを閉じます。



- 管理者として実行したコマンドプロンプトから、ディレクトリを C:\Windows\System32\inetsrv に変更し、次のコマンドを入力します。

```
   appcmd.exe set config “Default Web Site” -section:system.webServer/
security/authentication/clientCertificateMappingAuthentication /
enabled:”True” /commit:apphost
```

```
    appcmd.exe set config “Default Web Site” -section:system.webServer/
security/access /sslFlags:”Ssl, SslNegotiateCert” /commit:apphost
```



Firefoxブラウザーの構成

Firefoxブラウザーを使用するには、OpenSC 0.17.0 で入手できるPIVドライバーをインストールします。インストールと構成の手順については、「Installing OpenSC PKCS#11 Module in Firefox, Step by Step」を参照してください。 Directorでのスマートカード認証機能の使用方法については、Directorの記事の「Use Director with PIV based smart card authentication」セクションを参照してください。

ネットワーク分析の構成

> **注：** この機能の利用可否は、組織のライセンスと管理者権限によって異なります。

DirectorはCitrix ADMと統合され、ネットワーク分析とパフォーマンス管理を提供します。

- ネットワーク分析は、Citrix ADMのHDX™ Insightレポートを使用して、ネットワークのアプリケーションおよびデスクトップのコンテキストビューを提供します。この機能により、Directorは展開環境におけるICAトラフィックの高度な分析を提供します。
- パフォーマンス管理は、履歴データの保持と傾向レポートを提供します。リアルタイム評価と比較して履歴データを保持することで、容量や健全性の傾向を含む傾向レポートを作成できます。

Directorでこの機能を有効にすると、HDX InsightレポートはDirectorに追加情報を提供します。

- ページの タブには、展開環境全体におけるアプリケーション、デスクトップ、およびユーザーの待機時間と帯域幅の影響が表示されます。
- ページには、特定のユーザーセッションに固有の待機時間と帯域幅の情報が表示されます。

制限事項:

- ビューでは、バージョン7より前のVDAのHDX接続ログオンデータは収集されません。それ以前のVDAの場合、グラフデータは0として表示されます。

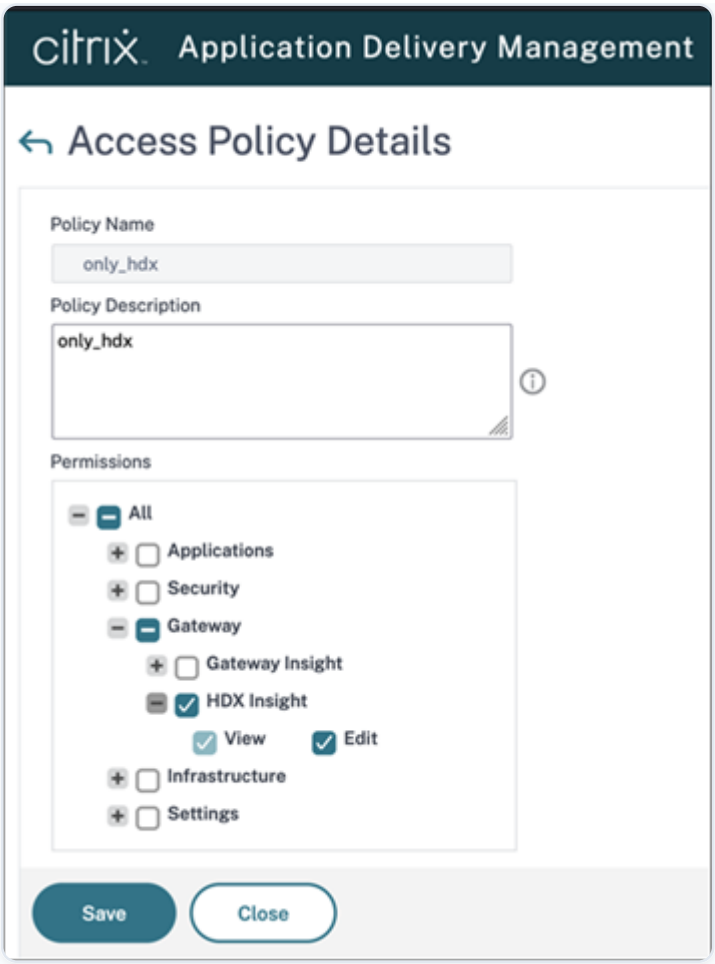
ネットワーク分析を有効にするには、DirectorにCitrix ADMをインストールして構成する必要があります。Directorには、Citrix ADMバージョン11.1ビルド49.16以降が必要です。MASはXenServer上で動作する仮想アプライアンスです。ネットワーク分析を使用すると、Directorは展開環境に関連する情報を通信および収集します。

詳しくは、Citrix ADM ドキュメントを参照してください。

> **注：**
>
> Citrix NetScaler Insight Centerは、15 May 2018をもってメンテナンス終了日を迎えました。Citrix製品マトリックス を参照してください。ネットワーク分析のためにDirectorをCitrix ADMと統合してください。NetScaler Insight CenterをCitrix ADMに移行するには、「NetScaler Insight CenterからCitrix ADMへの移行」を参照してください。

1. Directorがインストールされているサーバーで、`C:\inetpub\wwwroot\Director\tools` にあるDirectorConfigコマンドラインツールを見つけ、コマンドプロンプトからパラメーター /confignetscaler を指定して実行します。
2. プロンプトが表示されたら、Citrix ADMマシン名（FQDNまたはIPアドレス）、ユーザー名、パスワード、HTTPS接続タイプ（HTTPよりも推奨）、およびCitrix ADM統合を選択します。
3. 変更を確認するには、ログオフしてから再度ログオンします。

> **注:**
>
> セキュリティ上の理由から、HDX Insightへのアクセスに十分な権限を持つ、DirectorとのADM統合用のカスタムロールを作成することをお勧めします。



詳細については、アクセスポリシーの構成を参照してください。

委任管理とDirector

委任管理では、管理者、役割、スコープという3つの概念を使用します。権限は、管理者の役割と、その役割のスコープに基づいています。たとえば、管理者は、スコープが1つのサイトのエンドユーザーに対する責任を含むヘルプデスク管理者ロールを割り当てられる場合があります。

委任管理者の作成については、メインの委任管理の記事を参照してください。

管理権限によって、管理者に表示されるDirectorインターフェイスと、実行できるタスクが決まります。権限によって以下が決定されます。

- 管理者がアクセスできるビュー（総称してビューと呼ばれます）。
- 管理者が表示および操作できるデスクトップ、マシン、セッション。
- 管理者が実行できるコマンド（ユーザーセッションのシャドウイングやメンテナンスモードの有効化など）。

組み込みの役割と権限は、管理者がDirectorをどのように使用するかを決定します。

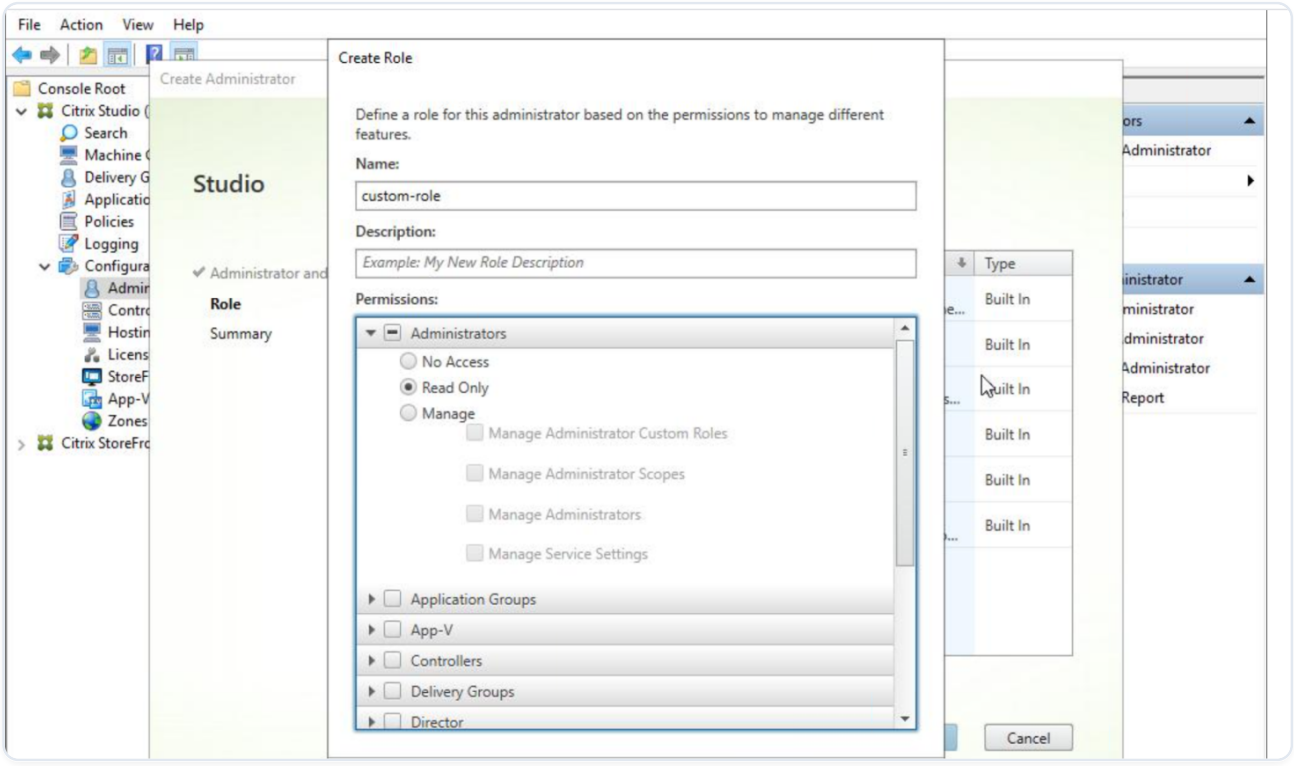
管理者ロール	DIRECTORでの権限
フル管理者	すべてのビューへのフルアクセス、およびすべてのコマンド（ユーザーセッションのシャドウイング、メンテナンスモードの有効化、トレンドデータのエクスポートなど）を実行できます。
デリバリーグループ管理者	すべてのビューへのフルアクセスが可能で、ユーザーセッションのシャドウイング、電源管理とセッション管理、メンテナンスモードの有効化、トレンドデータのエクスポートを含むすべてのコマンドを実行できます。
読み取り専用管理者	指定されたスコープ内のすべてのビューにアクセスし、すべてのオブジェクトとグローバル情報を表示できます。HDX™チャネルからレポートをダウンロードでき、トレンドビューの「エクスポート」オプションを使用してトレンドデータをエクスポートできます。その他のコマンドを実行したり、ビュー内の何かを変更したりすることはできません。
ヘルプデスク管理者	ヘルプデスクビューとユーザー詳細ビューのみにアクセスでき、管理者が管理を委任されているオブジェクトのみを表示できます。ユーザーセッションのシャドウイングを行い、そのユーザーのコマンドを実行できます。メンテナンスモード操作を実行できます。シングルセッションOSマシンに対して電源制御オプションを使用できます。ダッシュボード、トレンド、アラート、またはフィルタービューにはアクセスできません。マルチセッションOSマシンに対して電源制御オプションを使用することはできません。
マシンカタログ管理者	マシン詳細ページ（マシンベース検索）のみにアクセスできます。
ホスト管理者	アクセスなし。この管理者はDirectorではサポートされておらず、データを表示できません。

Director管理者用のカスタム役割を構成する

Studioでは、組織の要件により厳密に一致させ、権限をより柔軟に委任するために、Director固有のカスタム役割を構成することもできます。たとえば、組み込みのヘルプデスク管理者役割を制限して、この管理者がセッションをログオフできないようにすることができます。

Director権限を持つカスタム役割を作成する場合、その役割に他の一般的な権限も付与する必要があります。

- Delivery Controller™ にログオンするための権限 - 管理者ノードで少なくとも読み取り専用アクセス
- Directorでそれらのデリバリーグループに関連するデータを表示するためのデリバリーグループへの権限 - 少なくとも読み取り専用アクセス



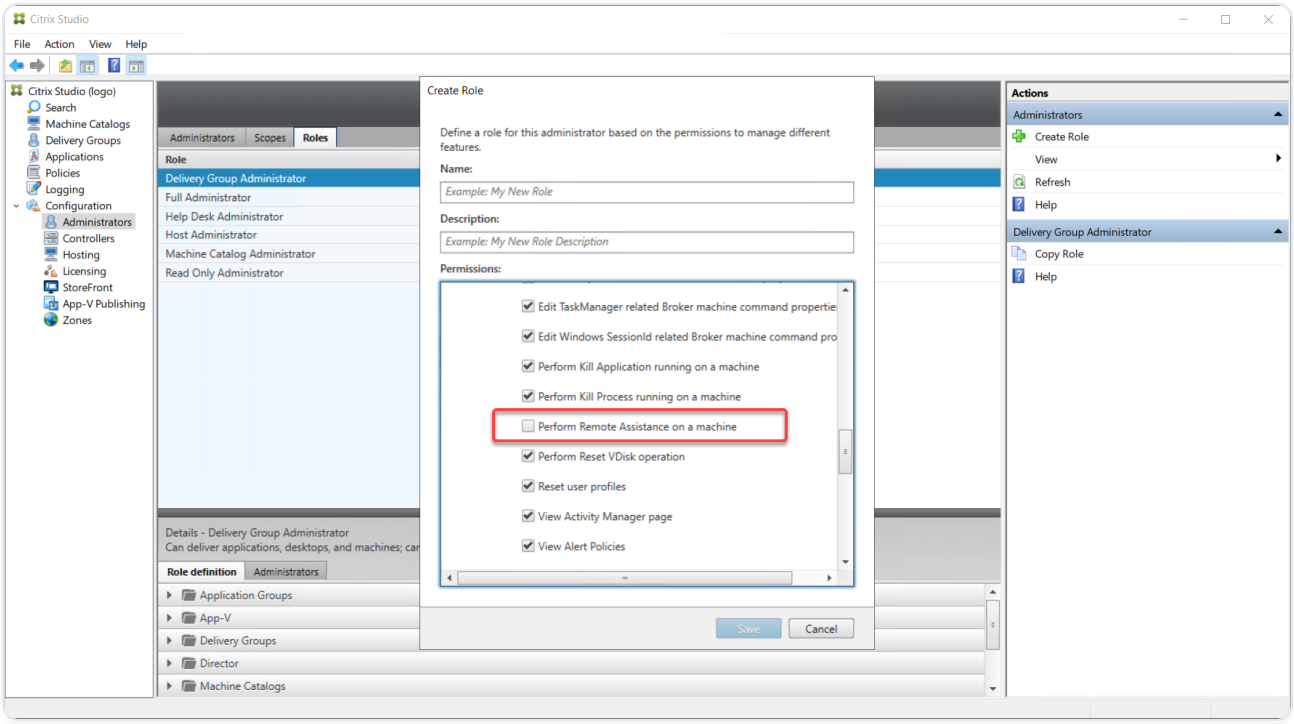
または、既存のロールをコピーして、さまざまなビューの追加の権限を含めることで、カスタムロールを作成できます。たとえば、ヘルプデスクロールをコピーして、ダッシュボードまたはフィルターページを表示する権限を含めることができます。

カスタムロールのDirector権限を選択します。これには以下が含まれます。

- マシン上で実行中のアプリケーションの強制終了を実行する
- マシン上で実行中のプロセスの強制終了を実行する
- マシン上でリモートアシスタンスを実行する
- ユーザープロファイルをリセットする

- クライアント詳細ページを表示
- ダッシュボードページの表示
- フィルターページを表示する
- マシン詳細ページを表示
- トレンドページの表示
- ユーザー詳細ページを表示

この例では、シャドウイング（マシン上でリモートアシスタンスを実行する）が無効になっています。



権限は、UIで適用可能になるために他の権限に依存する場合があります。たとえば、**マシン上で実行中のアプリケーションの強制終了を実行する**権限を選択すると、ロールに権限があるパネルでのみ**アプリケーションの終了**機能が有効になります。次のパネル権限を選択できます。

- フィルターページを表示する
- ユーザー詳細ページを表示
- マシン詳細ページを表示
- クライアント詳細ページを表示

さらに、他のコンポーネントの権限リストから、デリバリーグループの以下の権限を検討してください。

- デリバリーグループのメンバーシップを使用して、マシンのメンテナンスモードを有効/無効にする。

- デリバリーグループのメンバーシップを使用して、Windowsデスクトップマシンで電源操作を実行する。
- デリバリーグループのメンバーシップを使用して、マシンでセッション管理を実行する。

Directorの展開を保護する

この記事では、Directorの展開および構成時にシステムセキュリティに影響を与える可能性のある領域について説明します。

Microsoft インターネット インフォメーション サービス (IIS) の構成

制限されたIIS構成でDirectorを構成できます。

アプリケーションプールのリサイクル制限

以下のアプリケーションプールリサイクル制限を設定できます。

- 仮想メモリ制限: 4,294,967,295
- プライベートメモリ制限: StoreFront™サーバーの物理メモリのサイズ
- 要求制限: 4,000,000,000

ファイル名拡張子

リストにないファイル名拡張子を許可しないように設定できます。

Directorでは、要求フィルタリングで以下のファイル名拡張子が必要です。

- .aspx ファイル
- ．css
- .html ファイル
- .js
- ．png
- ．svc
- ．gif
- ドットジェイソン
- ドットウォフ
- ドットウォフ2
- ドットティーティーエフ

Directorでは、要求フィルタリングで以下のHTTP動詞が必要です。リストにない動詞を許可しないように設定できます。

- GET
- POST
- HEAD

Directorは以下を必要としません。

- ISAPIフィルター
- ISAPI拡張機能
- CGIプログラム
- FastCGIプログラム

重要:

- Directorには完全な信頼が必要です。グローバルな.NET信頼レベルを「高」またはそれ以下に設定しないでください。
- Directorは個別のアプリケーションプールを維持します。Directorの設定を変更するには、Directorサイトを選択して変更します。

ユーザー権限の構成

Directorがインストールされると、そのアプリケーションプールには以下が付与されます。

- **サービスとしてログオン**のログオン権限
- **プロセスに対するメモリクォータの調整**、**セキュリティ監査の生成**、および**プロセスレベルトークンの置き換え**の特権

言及されている権限と特権は、アプリケーションプールが作成される際の通常のインストール動作です。

これらのユーザー権限を変更する必要はありません。これらの特権は Director では使用されず、自動的に無効になります。

Directorの通信

実稼働環境では、Directorとサーバー間でやり取りされるデータを保護するために、インターネットプロトコルセキュリティ (IPsec) またはHTTPSプロトコルを使用してください。

IPsecは、インターネットプロトコルの標準拡張機能のセットであり、データの整合性とリプレイ保護を備えた認証済みおよび暗号化された通信を提供します。IPsecはネットワーク層プロトコルセットであるため、上位レベルのプロトコルは変更なしで使用できます。HTTPSは、トランスポート層セキュリティ (TLS) プロトコルを使用して強力なデータ暗号化を提供します。

注：

- Citrix®は、イントラネットネットワーク内でのDirectorコンソールへのアクセスを制限することを強くお勧めします。
- Citrixは、実稼働環境でDirectorへの保護されていない接続を有効にしないことを強くお勧めします。
- Directorからの安全な通信には、接続ごとに個別の構成が必要です。
- SSLプロトコルは推奨されません。代わりに、より安全なTLSプロトコルを使用してください。
- Citrix ADCとの通信は、IPsecではなくTLSを使用して保護してください。

DirectorとCitrix Virtual Apps and Desktopsサーバー間の通信 (監視およびレポート用) を保護するには、「データアクセスセキュリティ」を参照してください。

DirectorとCitrix ADC間の通信 (Citrix Insight用) を保護するには、「ネットワーク分析の構成」を参照してください。

Directorとライセンスサーバー間の通信を保護するには、ライセンス管理コンソールを保護するを参照してください。

Director のセキュリティ分離

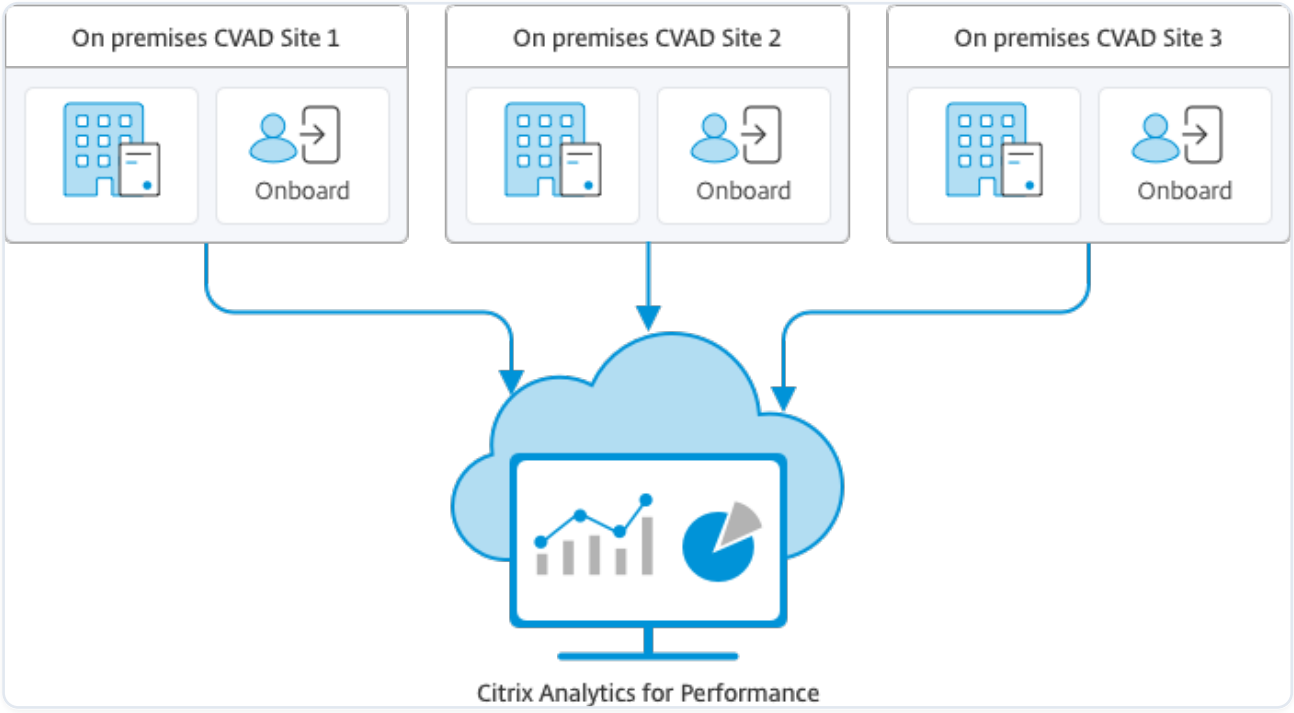
Director と同じ Web ドメイン（ドメイン名とポート）に任意の Web アプリケーションを展開できます。ただし、それらの Web アプリケーションのセキュリティリスクは、Director 展開のセキュリティを低下させる可能性があります。より高度なセキュリティ分離が必要な場合は、Citrix では Director を別の Web ドメインに展開することをお勧めします。

Citrix Analytics for Performance™ を使用したオンプレミスサイトの構成

Citrix Analytics for Performance (Performance Analytics) は、Citrix Analytics Cloud Serviceが提供する包括的なパフォーマンス監視ソリューションです。Performance Analyticsは、パフォーマンスメトリックに基づいて構築された高度なインサイトと分析を提供します。Performance Analyticsは、組織内の1つ以上のCitrix Virtual Apps and Desktops™サイトの使用状況とパフォーマンスメトリックを監視および表示するのに役立ちます。

Performance Analyticsの詳細については、Performance Analyticsの記事を参照してください。

サイトからCitrix Cloud™上のCitrix Analytics for Performanceにパフォーマンスデータを送信して、その高度なパフォーマンス分析機能を活用できます。Performance Analyticsを表示および使用するには、まず**Director**の**Analytics**タブからCitrix Analytics for Performanceを使用してオンプレミスサイトを構成する必要があります。



Performance Analyticsは安全な方法でデータにアクセスし、Citrix Cloudからオンプレミス環境にデータが転送されることはありません。

前提条件

DirectorからCitrix Analytics for Performanceを構成するために、新しいコンポーネントをインストールする必要はありません。次の要件が満たされていることを確認してください。

- Delivery ControllerとDirectorがバージョン1912 CU2以降であること。詳細については、機能互換性マトリックスを参照してください。

> **注：**

- Delivery ControllerがMicrosoft .NET Frameworkバージョン4.8より前のバージョンを実行している場合、DirectorからCitrix Analytics for Performanceを使用してオンプレミスサイトを構成すると、失敗する可能性があります。回避策として、Delivery Controllerの.NET Frameworkをバージョン4.8にアップグレードしてください。LCM-9255。
- DirectorからCitrix Analytics for Performanceを使用してCitrix Virtual Apps and Desktopsバージョン2012を実行しているオンプレミスサイトを構成すると、構成が数時間後、またはDelivery ControllerでCitrix Monitor Serviceを再起動した後に失敗する可能性があります。この場合、Analyticsタブには「未接続」ステータスが表示されます。回避策として、Delivery Controllerのレジストリにencryptionフォルダーを作成します。場所: HKEY_LOCAL_MACHINE\Software\Citrix\XDservices\Monitor、フォルダー名: Encryption。CitrixMonitorアカウントがEncryptionフォルダーに対してフルコントロールアクセス権を持っていることを確認してください。Citrix Monitor Serviceを再起動します。DIR-14324。

- この構成を実行するための**Analytics**タブへのアクセスは、フル管理者のみが利用できます。
- Performance Analyticsがパフォーマンスメトリックにアクセスできるようにするには、すべてのDelivery ControllerとDirectorがインストールされているマシンで、アウトバウンドインターネットアクセスが利用可能である必要があります。具体的には、次のURLへのアクセス可能性を確認してください。
  - Citrixキー登録: `https://*.citrixnetworkapi.net/`
  - シトリックス クラウド: `https://*.citrixworkspacesapi.net/`
  - シトリックス アナリティクス: `https://*.cloud.com/`
  - Microsoft Azure: `https://*.windows.net/` Delivery ControllerとDirectorマシンがイントラネット内にあり、アウトバウンドインターネットアクセスがプロキシサーバー経由である場合、以下を確認してください。
- プロキシサーバーは、上記のURLリストを許可する必要があります。
- Director web.config および citrix.monitor.exe.config ファイルに次の構成を追加します。この構成は **configuration** タグ内に追加してください。

```
&lt;system.net>

    &lt;defaultProxy>
```

```
        &lt;proxy  usesystemdefault = "false"  proxyaddress = "http://
&lt;your_proxyserver_address>:80" bypassonlocal = "true"  />

    &lt;/defaultProxy>

&lt;/system.net>
```

- Director web.config は、Director がインストールされているマシンの `C:\inetpub\wwwroot\Director\web.config` にあります。
- citrix.monitor.exe.config は、Delivery Controller がインストールされているマシンの `C:\Program Files\Citrix\Monitor\Service\Citrix.Monitor.exe.Config` にあります。

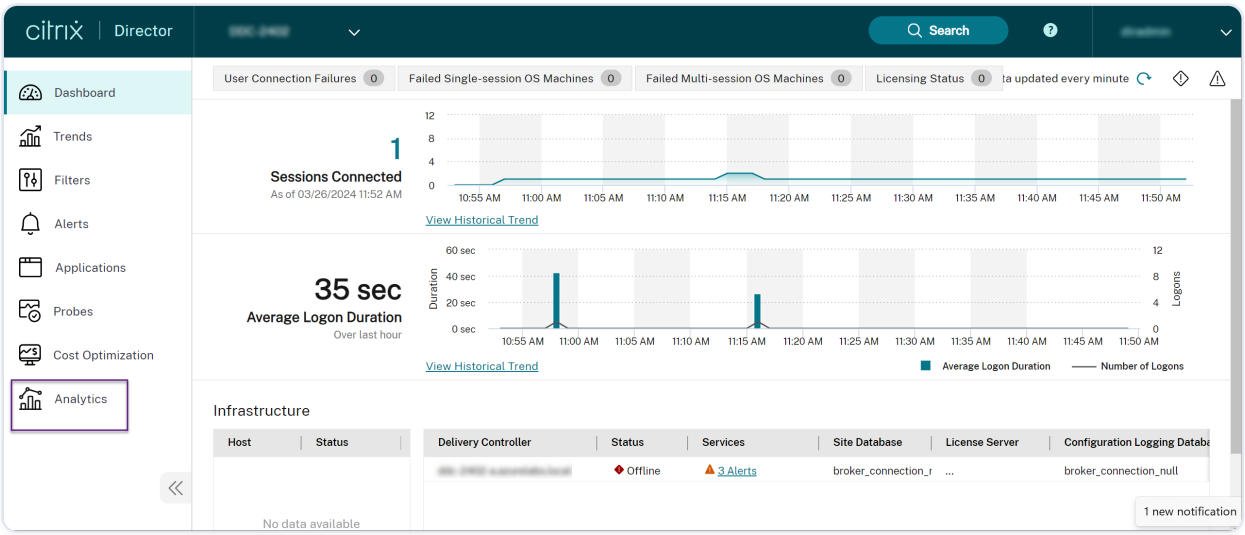
この設定は、IIS 上で Microsoft によって提供されます。詳細については、`https://docs.microsoft.com/ja-jp/dotnet/framework/network-programming/proxy-configuration` を参照してください。 構成ファイルの **defaultproxy** フィールドは、Director および Monitor Service のアウトバウンドアクセスを制御します。Performance Analytics との構成および通信には、**defaultproxy** フィールドを **true** に設定する必要があります。有効なポリシーによってこのフィールドが false に設定されている可能性があります。この場合、フィールドを手動で true に設定する必要があります。変更を行う前に構成ファイルのバックアップを取ってください。変更を有効にするには、Delivery Controller™ 上の監視サービスを再起動してください。

- Citrix Analytics for Performance の有効な Citrix Cloud エンタイトルメントをお持ちであること。
- Citrix Cloudアカウントは、製品登録エクスペリエンスに対する権限を持つ管理者アカウントである必要があります。管理者権限の詳細については、「管理者権限の変更」を参照してください。

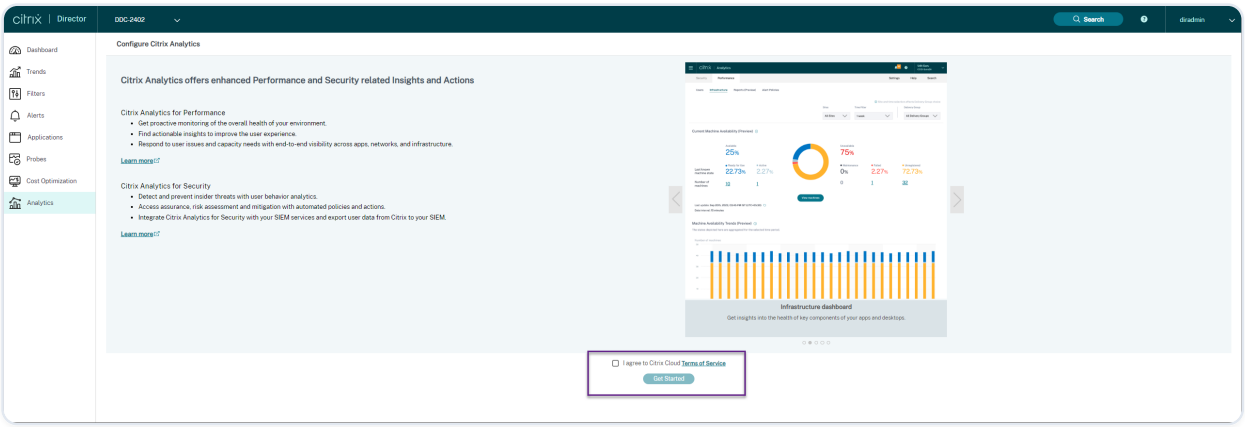
構成手順

前提条件を確認したら、次の手順を実行します。

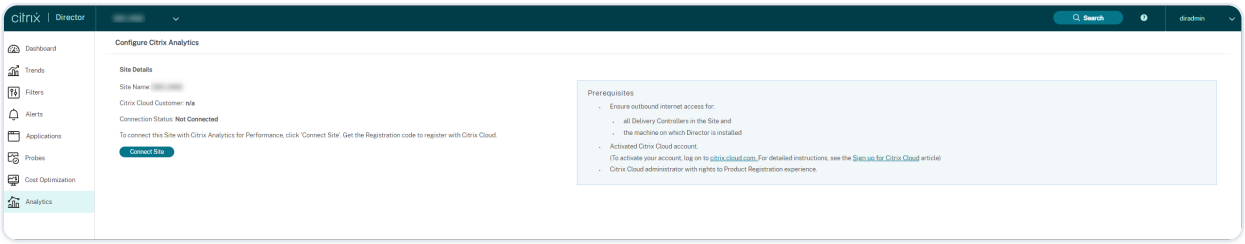
1. Director にフル管理者としてサインインし、Performance Analytics で構成するサイトを選択します。Director ダッシュボードページが表示されます。



2. **Analytics** タブをクリックします。**Citrix Analytics の構成**ページが表示されます。

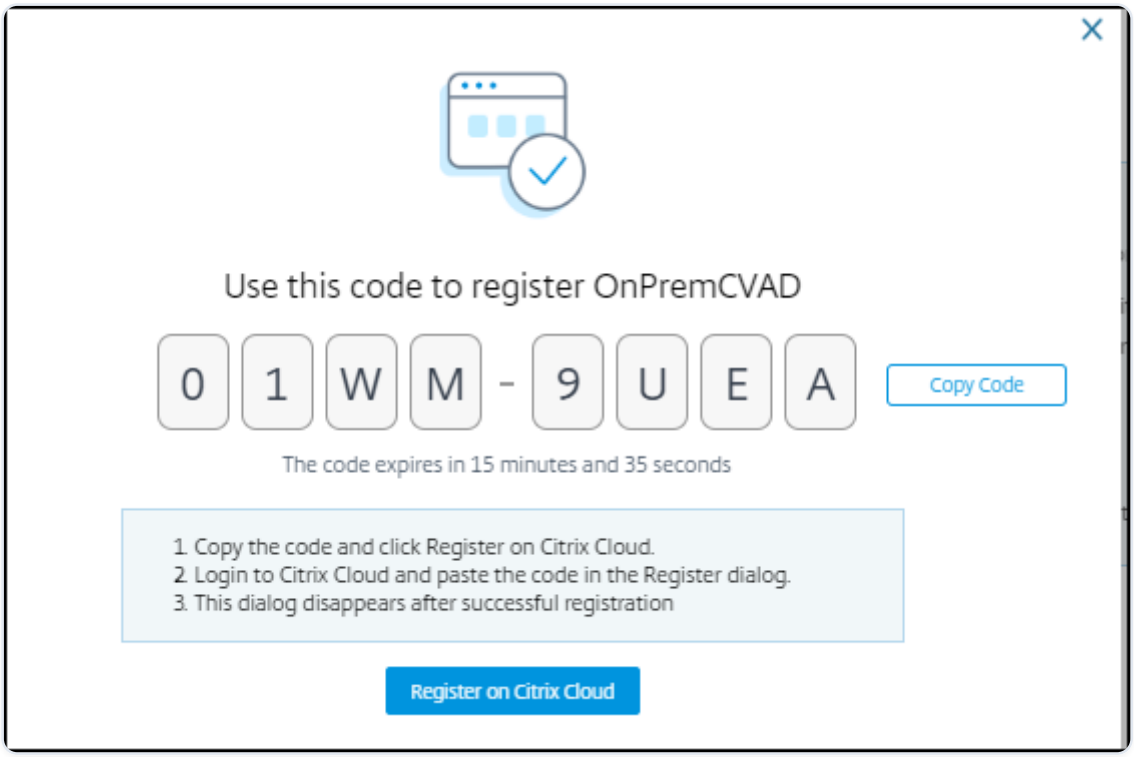


3. 手順を確認し、サービス利用規約を選択してから、**開始**をクリックします。**サイトの詳細**ページが表示されます。



4. 前提条件を確認し、満たされていることを確認します。サイトの詳細を確認します。
5. 構成プロセスを開始するには、**サイトの接続**をクリックします。

   このサイトを Citrix Cloud に登録するために使用する、一意の8桁の登録コードが生成されます。



6. **Copy Code** をクリックしてコードをコピーし、**Register on Citrix Cloud** をクリックします。Citrix Cloudの登録URLにリダイレクトされます。
7. Citrix Cloudの資格情報でサインインし、顧客を選択します。
8. Citrix Cloudの「製品登録」ページに、コピーした登録コードを貼り付けます。登録するには、**［続行］**をクリックします。登録の詳細を確認し、［登録］**をクリックします。

   Citrix Cloudでの登録(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/dir-onboarding6.png)

   オンプレミスサイトがCitrix Cloudに登録されます。
9. **Director**から、**［Analytics］**タブの**［Analyticsに移動］**をクリックします。

   Analyticsに移動(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/dir-onboarding7.png)

   Performance Analyticsがブラウザーの新しいタブで開きます。 Performance Analyticsダッシュボード(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/dir-onboarding-pa-dashboard.png)

   Citrix Cloudセッションの有効期限が切れている場合、Citrix.comまたはMy Citrixアカウントのログオンページにリダイレクトされることがあります。
10. 複数のサイトをPerformance Analyticsに登録するには、Directorから各サイトについて前述の構成手順を繰り返します。構成されているすべてのサイトのメトリックがPerformance Analyticsダッシュボードに表示されます。

サイトごとに複数のDirectorインスタンスが実行されている場合は、いずれか1つのDirectorインスタンスから構成します。サイトに接続されている他のすべてのDirectorインスタンスは、構成プロセス後の次回の更新時に更新されます。

11. サイトをCitrix Cloudから切断するには、**［サイトの切断］**をクリックします。このオプションは、既存の構成を削除します。

> **注:**
>
> サイトを初めて構成するとき、サイトからのイベントの処理には時間がかかる場合があり（約1時間）、Performance Analyticsダッシュボードにメトリックが表示されるまでに遅延が生じます。その後、イベントは定期的に更新されます。
>
> 切断後、新しいアカウントからのイベントが送信されるまで、古いアカウントからのデータ送信はしばらく継続されます。データ送信が停止してから約1時間、古いアカウントに関連する分析はPerformance Analyticsダッシュボードに表示されたままになります。
>
> Citrix Analyticsサービスへのエンタイトルメントの有効期限が切れると、サイトメトリックがPerformance Analyticsに送信されなくなるまでに最大1日かかります。

LTSR展開用Directorの独立リリース

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

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

- シトリックス バーチャル アップス アンド デスクトップス 2407 リリース
- シトリックス バーチャル アップス アンド デスクトップス 2411 リリース

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

利点

- **新機能へのアクセス**: 2402 LTSR発表後にリリースされたDirector機能（Citrix Virtual Apps and Desktops™ 2407および2411累積リリース（CR）の機能を含む）にアクセスできます。
- **ターゲットを絞ったアップグレード:** LTSRインフラストラクチャの残りの部分に影響を与えることなく、Directorおよび監視サービスコンポーネントのみをアップグレードします。
- **LTSR互換性**: 最新のDirector機能強化の恩恵を受けながら、LTSR環境を維持します。
- **ロールバックオプション:** 必要に応じて、以前のDirectorバージョンにロールバックする柔軟性があります。

重要な考慮事項

アップグレードされたDirectorコンポーネントはLTSR互換ですが、LTSRコアコンポーネントのサポート対象ではありません。ただし、LTSRインフラストラクチャの残りの部分は、既存のサポートを維持します。

前提条件

- Citrix Virtual Apps and Desktops 2402 LTSR CU1サイトを使用していることを確認してください。
- Microsoft SQL Serverバージョン2019以降を使用していることを確認してください。

概要

Citrix Virtual Apps and Desktops 2402 LTSR CU1サイトをCurrent Releaseの最新機能でアップグレードするには、次の手順に従います。

1. **データベースをバックアップする**: アップグレードする前に、監視データベースをバックアップしてください。アップグレードプロセスではデータベースも更新されるため、この手順は非常に重要です。
2. **サイトをアップグレードする**: 現在のリリースで新しい機能を取り込むために、サイトのアップグレードを進めます。
3. **ロールバックオプション**: アップグレードされたサイトの使用を継続しないと決定した場合、ロールバック手順を使用して以前のサイトに戻すことができます。

アップグレード手順

1. Monitorサービスデータベースのバックアップを作成します。
2. Citrix Virtual Apps and Desktopsインストーラーで**アップグレード**をクリックします。
3. ライセンス契約に同意します。

4. **コアコンポーネント**画面で、次のいずれかのオプションを選択します。
   - **Delivery Controller™** - このオプションのみが選択されている場合、Current Release Monitor Serviceのみがインストールされます。
   - **Director** - このオプションのみが選択されている場合、Current Release Director Serviceのみがインストールされます。
   - **Delivery Controller**と**Director** - これら両方のオプションが選択されている場合、DirectorとMonitor Serviceの両方のCurrent Releaseがインストールされます。
5. **機能**画面で、**Install Director Current Release `<version>`**チェックボックスを選択します。

   > **注：**
   >
   > **Install Director Current Release `<version>`**チェックボックスは、4番目の手順のいずれかのオプションが選択されている場合にのみ選択できます。

6. 画面の指示に従ってアップグレードを完了します。
7. 「**概要**」ページで、インストールされるコンポーネントを確認できます。「**コアコンポーネント**」ページと「**機能**」ページでの選択に基づいて、コンポーネントのインストールは次のようになります。

コアコンポーネントページの選択	「DIRECTORの現在のリリースをインストール `<VERSION>` 」チェックボックスの選択	コンポーネントのインストール
デリバリーコントローラー	選択済み	Monitoring Serviceの現在のリリースがインストールされます。
デリバリーコントローラー	未選択	Monitoring Serviceの累積アップグレードがインストールされます。
ディレクター	選択済み	Director Serviceの現在のリリースがインストールされます。

コアコンポーネントページの選択	「DIRECTORの現在のリリースをインストール `<VERSION>`」チェックボックスの選択	コンポーネントのインストール
ディレクター	未選択	Director Serviceの累積アップグレードがインストールされます。
デリバリーコントローラーとディレクター	選択済み	Monitoring Service と Director Service の現在のリリースがインストールされています。
デリバリーコントローラーとディレクター	未選択	Monitoring Service と Director Service の累積アップグレードがインストールされています。

8. インストールが完了したら、**Citrix Site Manager を開く**チェックボックスをオンにします。
9. 自動サイトアップグレードを開始します。
10. Director で新機能が利用可能であることを確認します。

コマンドラインインストール

サイトを新規インストールまたはアップグレードするには、次のサンプルコマンドを使用します。

```
\x64\XenDesktop Setup\XenDesktopServerSetup.exe /components
controller,desktopstudio,licenseserver,director /configure_firewall /
quiet /enable_new_monitoring_features
```

ロールバック手順

1. Monitoring データベースのバックアップを必ず取得してください。
2. データベースロールバックスクリプト dbollback.zip をダウンロードして実行します。

> **注：**

> `dbrollback.zip` ファイルに含まれる PowerShell スクリプト (`dbrollback.ps1`) は、sqlcmd が DDC にインストールされている場合に rollback.sql スクリプトを実行する方法を示しています。

3. すでに取得済みのバックアップから監視データベースを復元します。詳細については、ナレッジ共有記事 CTX135207 を参照してください。
4. コントロールパネルから以下をアンインストールします。
   - **Citrix Monitor Service PowerShell Snap-in- x64** を選択し、**アンインストール**をクリックします。
   - **Citrix Monitor Service - x64** を選択し、**アンインストール**をクリックします。
   - **Citrix Director** を選択し、**アンインストール**をクリックします。
5. Citrix Virtual Apps and Desktops インストーラーを使用して、Delivery Controller と Director を再インストールします。詳細については、「コアコンポーネントのインストール」を参照してください。

   または、,

   次のコマンドを使用してコンポーネントを再インストールすることもできます。

   ```
   XenDesktopServerSetup.exe /components controller,director /
   configure_firewall /quiet
   ```

6. **Install Director Current Release** `<version>` チェックボックスが選択されていないことを確認します。
7. インストールが完了したら、**Open Citrix Site Manager** チェックボックスを選択します。
8. Citrix Site Manager で推奨されている場合は、サイトのアップグレードを実行します。

サポートとコンプライアンス

サポート

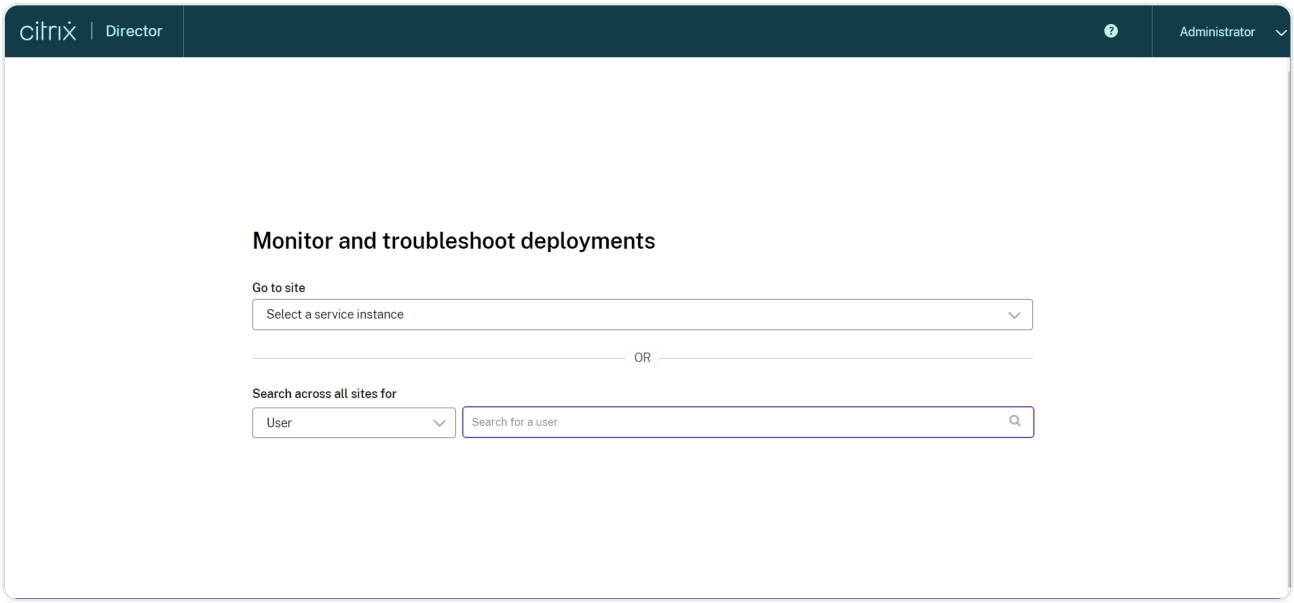
- Director の累積リリース (CR) バージョンは LTSR と互換性がありますが、LTSR に準拠していません。
- アップグレード後、必要なすべてのサポートチケットとバグ修正は、Director の次の累積リリース (CR) に追加されます。
- 変更または修正を含む CR は、次の累積更新プログラム (CU) で利用可能になります。

508/WCAG 2.1

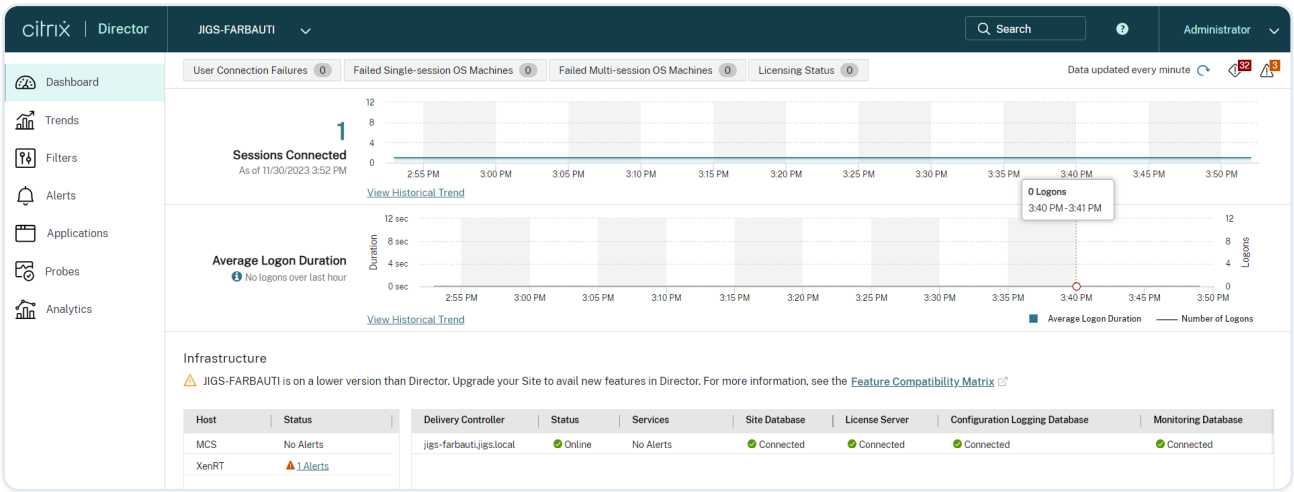
- 508/WCAG 2.1 準拠の義務があるお客様には、すべてのコアコンポーネントの LTSR バージョンを継続して使用することをお勧めします。

サイト分析

Director を使用して、展開の健全性を監視できます。オンボードされたすべてのサイトでユーザー、エンドポイント、またはマシンを検索することで、パフォーマンスの問題をトラブルシューティングできます。



完全な管理者権限があれば、Directorを開くと、ダッシュボードは、サイトの健全性と使用状況を監視するための一元的な場所を提供します。



現在障害がなく、過去60分間に障害が発生していない場合、パネルは折りたたまれたままになります。障害が発生すると、特定の障害パネルが自動的に表示されます。

> **注：**

> 組織のライセンスと管理者権限によっては、一部のオプションまたは機能が利用できない場合があります。

Director ダッシュボードのパネル

ユーザー接続障害

過去60分間の接続障害。合計数の横にあるカテゴリをクリックすると、その種類の障害のメトリックが表示されます。隣接するテーブルでは、その数がデリバリーグループ別に分類されています。接続障害には、アプリケーション制限に達したことによる障害が含まれます。アプリケーション制限の詳細については、「アプリケーション」を参照してください。

失敗したシングルセッションOSマシンまたは失敗したマルチセッションOSマシン

過去60分間の合計障害数（デリバリーグループ別）。障害は、起動失敗、起動中に停止、未登録などの種類別に分類されます。マルチセッションOSマシンでは、障害には最大負荷に達したマシンも含まれます。

ライセンスステータス

ライセンスサーバーアラートには、ライセンスサーバーから送信されたアラートと、アラートを解決するために必要なアクションが表示されます。ライセンスサーバーバージョン11.12.1以降が必要です。デリバリーコントローラーアラートには、コントローラーから見たライセンス状態の詳細が表示され、コントローラーによって送信されます。XenApp 7.6またはXenDesktop 7.6以降のコントローラーが必要です。Studioでアラートのしきい値を設定できます。**Delivery Controllers** > **Details** > **Product Editions** > **PLT** に表示されるライセンスステータスは、**Premium** を示し、**Platinum** ではありません。

猶予状態

Directorには、次のいずれかの猶予状態が表示されます。この情報はデリバリーコントローラーから取得されます。

1. **非アクティブ:** いかなる種類のライセンスキャッシュモードでもありません。通常のライセンス制限が適用されます。
2. **緊急猶予:** ライセンスサーバーに到達できない場合、または接続を仲介している間にライセンス情報を取得できない場合に有効になります。ユーザーには影響ありません。Directorに表示されるエラーは、ライセンスサーバーに到達可能になるまで閉じることができません。
3. **猶予期間の期限切れ:** 緊急ライセンスキャッシュモードの有効期限が切れました。

詳細については、ライセンスの超過 および ライセンスバーストモード を参照してください。

接続されたセッション

過去60分間のすべてのデリバリーグループにわたる接続セッション。

平均ログオン時間

過去60分間のログオンデータ。左側の大きな数字は、1時間あたりの平均ログオン時間です。XenDesktop 7.0より前のVDAのログオンデータは、この平均には含まれません。詳細については、ユーザーログオンの問題の診断 を参照してください。

インフラストラクチャ

サイトのインフラストラクチャ（ホストとコントローラー）を一覧表示します。XenServerまたはVMwareのインフラストラクチャの場合、パフォーマンスアラートを表示できます。たとえば、管理対象サーバーまたは仮想マシンでCPU、ネットワークI/O、またはディスクI/Oの使用率が指定されたしきい値を超えたときに、XenCenterがパフォーマンスアラートを生成するように構成できます。デフォルトでは、アラートの繰り返し間隔は60分ですが、これも構成できます。詳細については、XenServer製品ドキュメント のXenCenterパフォーマンスアラートのセクションを参照してください。

> **注：**
>
> 特定のメトリックにアイコンが表示されない場合、そのメトリックは使用しているホストの種類でサポートされていないことを示します。たとえば、System Center Virtual Machine Manager（SCVMM）ホスト、AWS、CloudStackでは、正常性情報は利用できません。

> 以下のオプションを使用して問題のトラブルシューティングを続行します（以下のセクションで説明されています）。

- ユーザーマシンの電源を制御する
- マシンへの接続を防止する

セッションの監視

セッションが切断されても、セッションはアクティブなままでアプリケーションは実行され続けますが、ユーザーデバイスはサーバーと通信しなくなります。

アクション	説明
ユーザーの現在接続されているマシンまたはセッションを表示する	アクティビティマネージャーとユーザー詳細ビューから、ユーザーが現在接続しているマシンまたはセッション、およびこのユーザーがアクセスできるすべてのマシンとセッションのリストを表示します。このリストにアクセスするには、ユーザータイトルバーのセッションスイッチャーアイコンをクリックします。詳細については、セッションの復元 を参照してください。
すべてのデリバリーグループにおける接続済みセッションの総数を表示する	ダッシュボードの**接続済みセッション**ペインで、過去60分間のすべてのデリバリーグループにおける接続済みセッションの合計数を表示します。次に、大きな合計数をクリックすると、フィルタービューが開き、選択したデリバリーグループと範囲、およびデリバリーグループ全体の使用状況に基づいてグラフィカルなセッションデータを表示できます。
アイドルセッションを終了する	セッションフィルタービューには、すべてのアクティブなセッションに関連するデータが表示されます。関連ユーザー、デリバリーグループ、セッション状態、およびしきい値期間を超えるアイドル時間に基づいてセッションをフィルター処理します。フィルター処理されたリストから、ログオフまたは切断するセッションを選択します。詳細については、アプリケーションのトラブルシューティング を参照してください。
より長い期間のデータを表示する	トレンドビューで、**セッション**タブを選択すると、より長い期間（つまり、過去60分より前のセッション合計）の接続済みセッションと切断済みセッションに関するより具体的な使用状況データをドリルダウンして表示できます。この情報を表示するには、**履歴トレンドの表示**をクリックします。

注：

ユーザーデバイスがレガシーVirtual Delivery Agent（VDA）（バージョン7より前のVDAやLinux VDAなど）を実行している場合、Directorはセッションに関する完全な情報を表示できません。代わりに、情報が利用できないことを示すメッセージが表示されます。

デスクトップ割り当て規則の制限: Web Studioでは、異なるユーザーまたはユーザーグループに対して複数のデスクトップ割り当て規則（DAR）をデリバリーグループ内の単一のVDAに割り当てることができます。StoreFront™は、ログインユーザーのDARに従って、対応する**表示名**で割り当てられたデスクトップを表示します。ただし、DirectorはDARをサポートしておらず、ログインユーザーに関係なく、デリバリーグループ名を使用して割り当てられたデスクトップを表示します。その結果、Directorで特定のデスクトップをマシンにマッピングすることはできません。 StoreFrontに表示される割り当てられたデスクトップを、Directorに表示されるデリバリーグループ名にマッピングするには、次のPowerShellコマンドを使用します。

```
Get-BrokerDesktopGroup | Where-Object { $\_.Uid -eq (Get-
BrokerAssignmentPolicyRule | Where-Object { $\_.PublishedName -eq
"\&lt;Name on StoreFront\>" }).DesktopGroupUid } | Select-Object -Property
Name, Uid
```

セッション転送プロトコル

セッションの詳細パネルで、現在のセッションのHDX接続タイプで使用されている転送プロトコルを表示します。この情報は、VDAバージョン7.13以降で起動されたセッションで利用できます。

転送プロトコル (/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/sessions-transport-protocol.png)

- **HDX™** 接続タイプの場合、,
  - HDX接続にEDTが使用されている場合、プロトコルは **UDP** と表示されます。
  - HDX接続にTCPが使用されている場合、プロトコルは **TCP** と表示されます。
- **RDP**接続タイプの場合、プロトコルは**n/a**と表示されます。

アダプティブトランスポートが構成されている場合、セッション転送プロトコルは、ネットワークの状態に基づいてEDT（UDP経由）とTCPの間で動的に切り替わります。EDTを使用してHDXセッションを確立できない場合、TCPプロトコルにフォールバックします。

アダプティブトランスポートの構成の詳細については、「アダプティブトランスポート」を参照してください。

レポートのエクスポート

定期的な使用状況および容量管理レポートを生成するために、トレンドデータをエクスポートできます。エクスポートは、PDF、Excel、CSVのレポート形式をサポートしています。PDFおよびExcel形式のレポートには、グラフと表で表されたトレンドが含まれます。CSV形式のレポートには、ビューを生成するために処理できる、またはアーカイブできる表形式のデータが含まれます。

レポートをエクスポートするには：

1. **トレンド**タブに移動します。
2. フィルター条件と期間を設定し、**適用**をクリックします。傾向グラフと表にデータが入力されます。
3. **エクスポート**をクリックし、レポートの名前と形式を入力します。

Directorは、選択したフィルター条件に基づいてレポートを生成します。フィルター条件を変更した場合は、**エクスポート**をクリックする前に**適用**をクリックしてください。

> **注：**
>
> 大量のデータをエクスポートすると、Directorサーバー、Delivery Controller、およびSQLサーバーのメモリとCPUの使用量が大幅に増加します。最適なエクスポートパフォーマンスを実現するために、サポートされる同時エクスポート操作の数とエクスポートできるデータ量は、デフォルトの制限に設定されています。

サポートされるエクスポート制限

エクスポートされたPDFおよびExcelレポートには、選択されたフィルター条件に対する完全なグラフが含まれます。ただし、すべてのレポート形式の表形式データは、テーブル内の行数またはレコード数のデフォルト制限を超えると切り捨てられます。サポートされるデフォルトのレコード数は、レポート形式に基づいて定義されます。

Internet Information Services (IIS) のDirectorアプリケーション設定を構成することで、デフォルトの制限を変更できます。

レポート形式	サポートされるレコードのデフォルト数	DIRECTORアプリケーション設定のフィールド	サポートされるレコードの最大数
PDF	500	UI.ExportPdfDrilldownLimit	5000

レポート形式	サポートされるレコードのデフォルト数	DIRECTORアプリケーション設定のフィールド	サポートされるレコードの最大数
エクセル	100,000	UI.ExportExcelDrilldownLimit	100,000
CSV	100,000 (「**セッション**」タブでは10,000,000)	UI.ExportCsvDrilldownLimit	100,000

エクスポートできるレコード数の制限を変更するには：

1. IISマネージャーコンソールを開きます。
2. デフォルトのWebサイトの下にあるDirector Webサイトに移動します。
3. 「**アプリケーション設定**」をダブルクリックします。
4. 必要に応じて、UI.ExportPdfDrilldownLimit、UI.ExportExcelDrilldownLimit、またはUI.ExportCsvDrilldownLimitフィールドの設定を編集または追加します。

アプリケーション設定でこれらのフィールド値を追加すると、デフォルト値が上書きされます。

> **警告:**
>
> サポートされている最大レコード数を超えるフィールド値を設定すると、エクスポートのパフォーマンスに影響を与える可能性があり、サポートされていません。

エラー処理

このセクションでは、エクスポート操作中に発生する可能性のあるエラーの対処方法について説明します。

- **Directorがタイムアウトしました**

このエラーは、ネットワークの問題、DirectorサーバーまたはMonitor Serviceでの高いリソース使用率が原因で発生する可能性があります。

デフォルトのタイムアウト期間は100秒です。Director Serviceのタイムアウト期間を長くするには、Internet Information Services (IIS) のDirectorアプリケーション設定で、**Connector.DataServiceContext.Timeoutフィールド**の値を設定します。

1. IISマネージャーコンソールを開きます。
2. デフォルトのWebサイトの下にあるDirector Webサイトに移動します。
3. **アプリケーション設定**をダブルクリックします。
4. **Connector.DataServiceContext.Timeout**の値を編集します。

- **Monitorがタイムアウトしました**

このエラーは、ネットワークの問題、Monitor ServiceまたはSQLサーバーでの高いリソース使用率が原因で発生する可能性があります。

Monitor Serviceのタイムアウト期間を長くするには、Delivery Controllerで次のPowerShellコマンドを実行します。

```
asnp Citrix.*

Get-MonitorConfiguration

Set-MonitorConfiguration -MonitorQueryTimeoutSeconds &lt;timeout value>
```

- **同時実行中のエクスポートまたはプレビュー操作の最大数**

Directorは、エクスポートまたはプレビューのインスタンスを1つサポートしています。「**同時実行中のエクスポートまたはプレビュー操作の最大数**」エラーが発生した場合は、次のエクスポート操作を後でもう一度試してください。

同時実行できるエクスポートまたはプレビュー操作の数を増やすことは可能ですが、Directorのパフォーマンスに影響を与える可能性があり、サポートされていません。

1. IISマネージャーコンソールを開きます。
2. デフォルトのWebサイトの下にあるDirector Webサイトに移動します。
3. **アプリケーション設定**をダブルクリックします。
4. 値**UI.ConcurrentExportLimit**を編集します。

- **Directorのディスク容量不足**

各エクスポート操作には、Windows Tempフォルダーに最大2 GBのハードディスク容量が必要です。空き容量を確保するか、Directorサーバーにハードディスク容量を追加してから、エクスポートを再試行してください。

Monitorのホットフィックス

特定のVDAマシン（物理またはVM）にインストールされているホットフィックスを表示するには、「**マシンの詳細**」ビューを選択します。

ユーザーマシンの電源状態を制御する

Directorで選択したマシンの状態を制御するには、電源制御オプションを使用します。これらのオプションは、シングルセッションOSマシンで利用できますが、マルチセッションOSマシンでは利用できない場合があります。

注：

この機能は、物理マシンまたはリモートPCアクセスを使用するマシンでは利用できません。

コマンド	機能
再起動	VMの順序だった（ソフト）シャットダウンを実行し、VMを再起動する前に実行中のすべてのプロセスを個別に停止します。たとえば、Directorで「起動に失敗しました」と表示されるマシンを選択し、このコマンドを使用して再起動します。
強制再起動	シャットダウン手順を最初に実行せずにVMを再起動します。このコマンドは、物理サーバーのプラグを抜き、再度差し込んで電源を入れ直すのと同じように機能します。
シャットダウン	VMの正常な（ソフト）シャットダウンを実行します。すべての実行中のプロセスは個別に停止されます。
強制シャットダウン	シャットダウン手順を最初に実行せずにVMをシャットダウンします。このコマンドは、物理サーバーのプラグを抜くのと同じように機能します。常にすべての実行中のプロセスをシャットダウンするとは限ら

コマンド	機能
	ず、この方法でVMをシャットダウンするとデータが失われるリスクがあります。
一時停止	実行中のVMを現在の状態で一時停止し、その状態をデフォルトのストレージリポジトリ上のファイルに保存します。このオプションを使用すると、VMのホストサーバーをシャットダウンし、後で再起動した後、VMを再開して元の実行状態に戻すことができます。
再開	一時停止されたVMを再開し、元の実行状態に戻します。
開始	VMがオフのときに起動します（コールドスタートとも呼ばれます）。

電源制御アクションが失敗した場合、アラートにマウスを重ねると、失敗の詳細を示すポップアップメッセージが表示されます。

マシンへの接続を防止する

適切な管理者がイメージのメンテナンス作業を実行している間、メンテナンスモードを使用して新しい接続を一時的に防止します。

マシンでメンテナンスモードを有効にすると、無効にするまで新しい接続は許可されません。ユーザーが現在ログオンしている場合、すべてのユーザーがログオフするとすぐにメンテナンスモードが有効になります。ログオフしないユーザーには、マシンが特定の時間にシャットダウンされることを通知するメッセージを送信し、電源制御を使用してマシンを強制的にシャットダウンします。

1. ユーザー詳細ビューから、またはフィルタービューでマシンのグループから、マシンを選択します。
2. **メンテナンスモード**を選択し、オプションをオンにします。

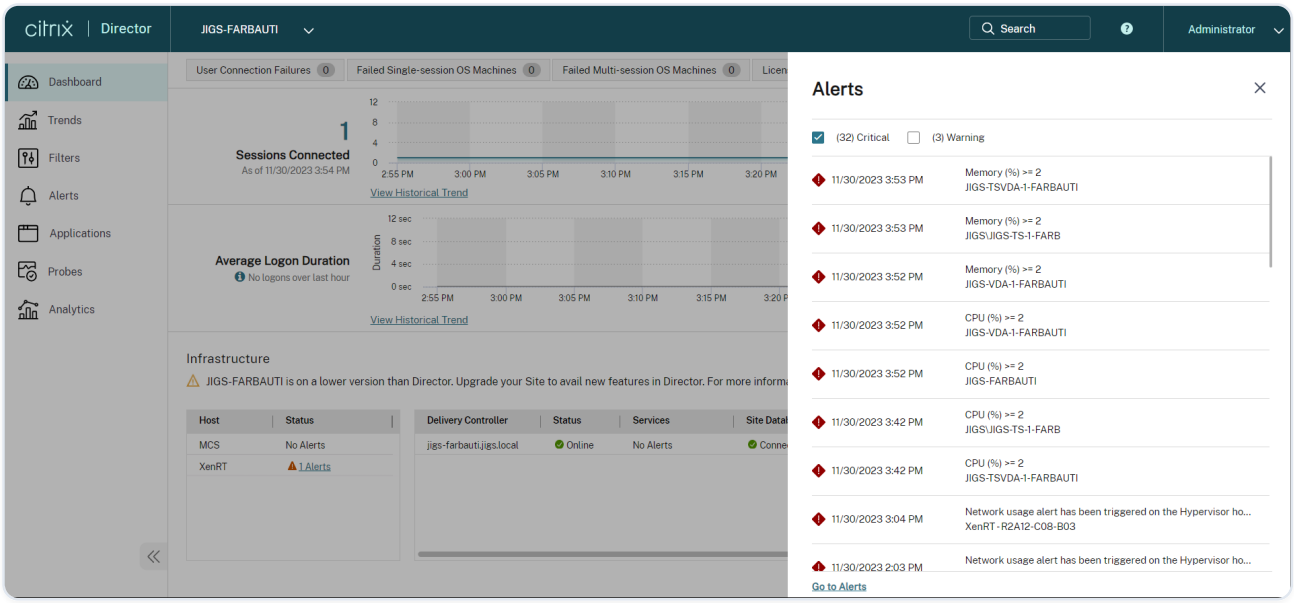
ユーザーが割り当てられたデスクトップにメンテナンスモード中に接続しようとすると、デスクトップが利用できないことを示すメッセージが表示されます。メンテナンスモードを無効にするまで、新しい接続はできません。

アプリケーション分析

アプリケーションタブには、アプリケーションベースの分析が単一の統合ビューで表示され、アプリケーションのパフォーマンスを効率的に分析および管理するのに役立ちます。サイトで公開されているすべてのアプリケーションの健全性と使用状況に関する貴重な洞察を得ることができます。プローブ結果、アプリケーションごとのインスタンス数、公開されているアプリケーションに関連する障害やエラーなどのメトリックが表示されます。詳細については、**アプリケーションのトラブルシューティング**のアプリケーション分析セクションを参照してください。

アラートと通知

アラートは、Directorのダッシュボードやその他の上位レベルのビューに、警告および重大なアラートシンボルとともに表示されます。アラートは**Premium**ライセンスサイトで利用できます。アラートは1分ごとに自動的に更新されます。オンデマンドでアラートを更新することもできます。



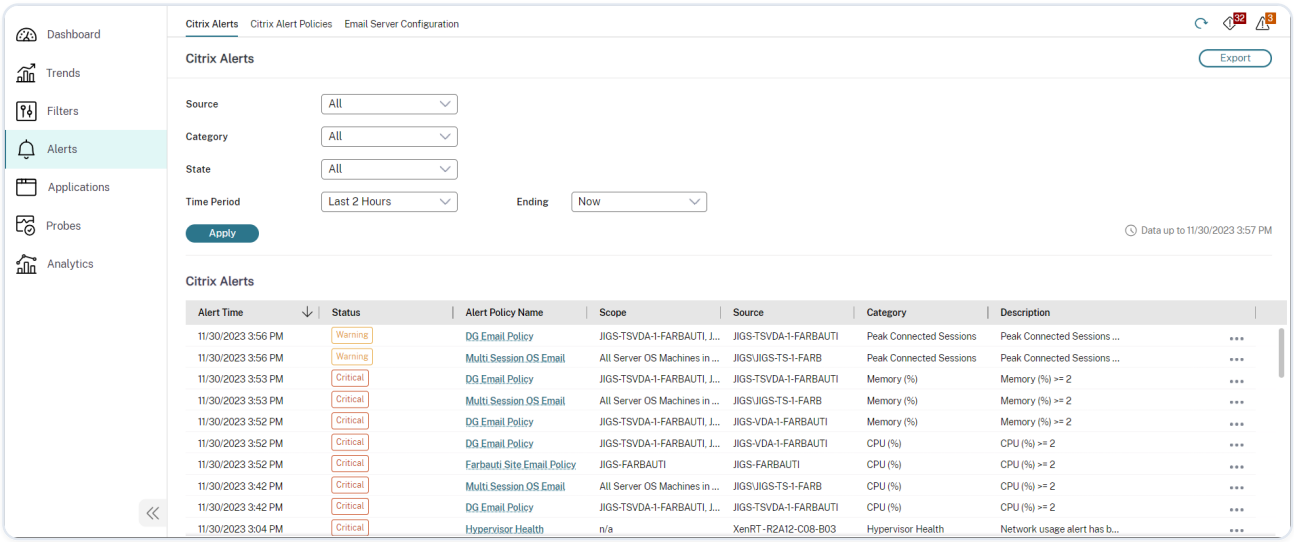
警告アラート（琥珀色の三角形）は、条件の警告しきい値に達したか、それを超えたことを示します。

重大なアラート（赤い円）は、条件の重大なしきい値に達したか、それを超えたことを示します。

アラートに関する詳細情報は、サイドバーからアラートを選択するか、サイドバーの下部にある**Go to Alerts**リンクをクリックするか、Directorページの上部から**Alerts**を選択することで表示できます。

アラートビューでは、アラートをフィルタリングしてエクスポートできます。たとえば、過去1か月間の特定のデリバリーグループの失敗したマルチセッションOSマシン、または特定のユーザー

のすべてのアラートなどです。詳細については、「レポートのエクスポート」を参照してください。



Citrix®アラート

Citrixアラートは、Citrixコンポーネントから発生し、Directorで監視されるアラートです。Citrixアラートは、Directorの**Alerts** \> **Citrix Alerts Policy**で構成できます。構成の一部として、アラートが設定したしきい値を超えた場合に、個人やグループにメールで通知を送信するように設定できます。Citrixアラートの設定の詳細については、「アラートポリシーの作成」を参照してください。

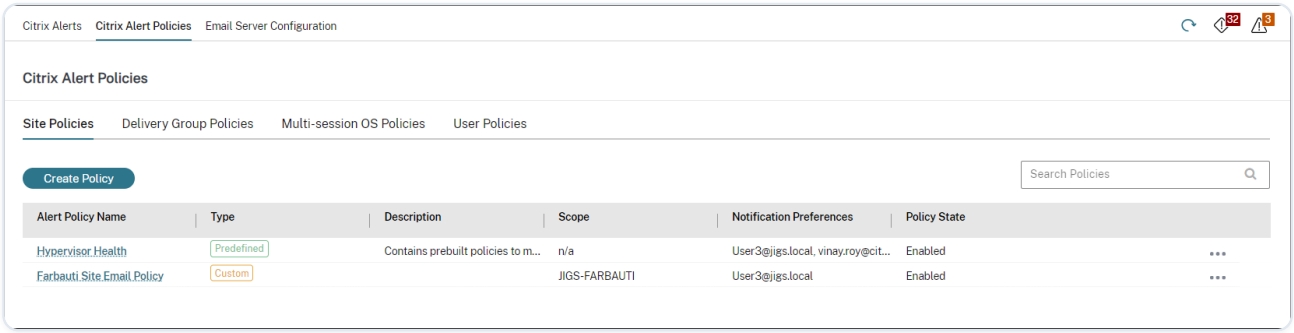
> **注：**
>
> ファイアウォール、プロキシ、またはMicrosoft Exchange Serverがメールアラートをブロックしないようにしてください。

スマートアラートポリシー

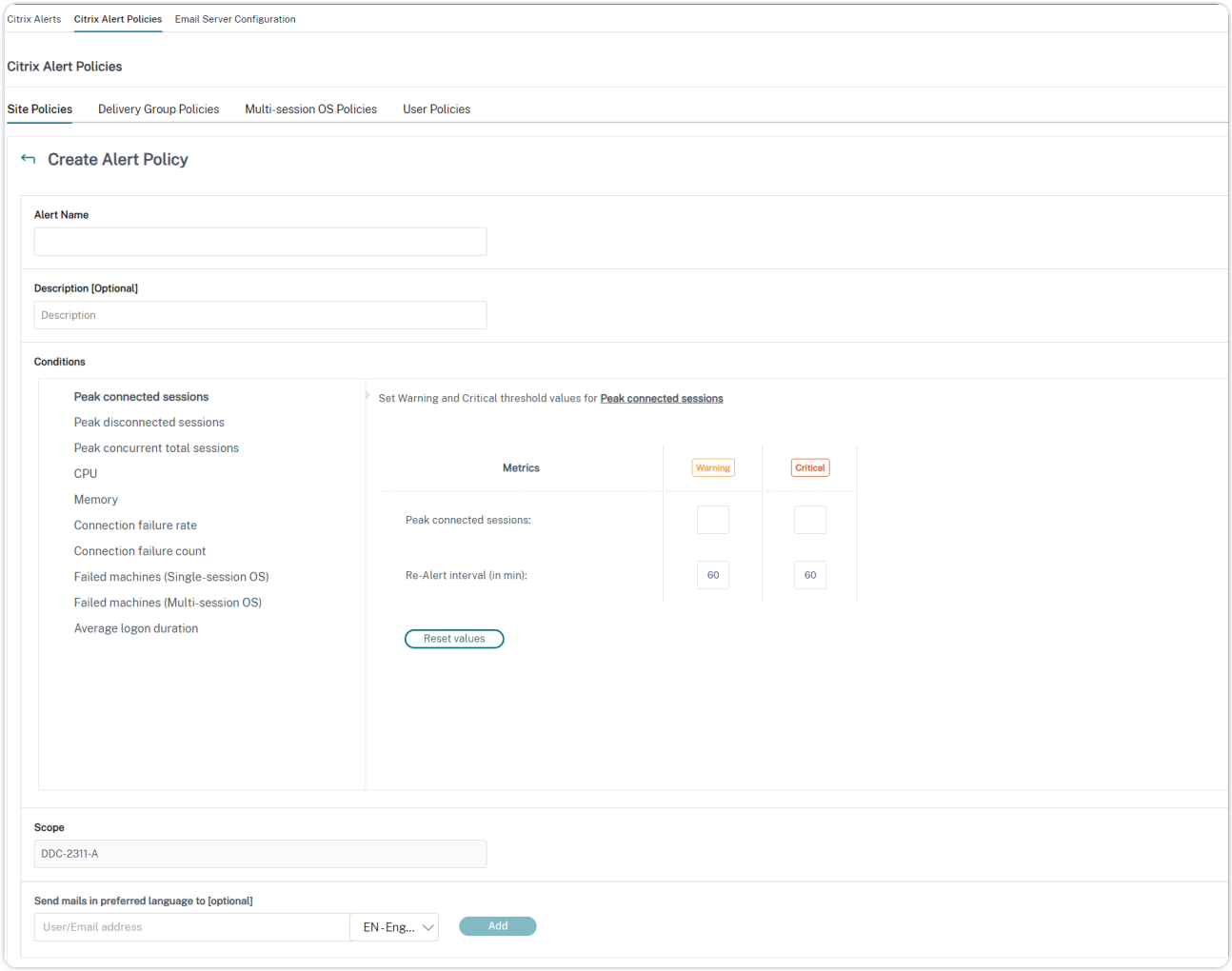
事前定義されたしきい値を持つ一連の組み込みアラートポリシーは、デリバリーグループおよびマルチセッションOS VDAスコープで利用できます。この機能には、Delivery Controllerバージョン7.18以降が必要です。組み込みアラートポリシーのしきい値パラメーターは、**Alerts** \> **Citrix Alerts Policy**で変更できます。 これらのポリシーは、サイトに少なくとも1つのアラートターゲット（デリバリーグループまたはマルチセッションOS VDA）が定義されている場合に作成されます。さらに、これらの組み込みアラートは、新しいデリバリーグループまたはマルチセッションOS VDAに自動的に追加されます。

Directorとサイトをアップグレードする場合、以前のDirectorインスタンスのアラートポリシーは引き継がれます。組み込みアラートポリシーは、Monitorデータベースに対応するアラートルールが存在しない場合にのみ作成されます。

組み込みアラートポリシーのしきい値については、「アラートポリシーの条件」セクションを参照してください。



アラートポリシーを作成する



新しいアラートポリシーを作成するには、たとえば、特定のセッション数条件が満たされたときにアラートを生成するには、次の手順を実行します。

1. **Alerts** > **Citrix Alerts Policy**に移動し、たとえば、マルチセッションOSポリシーを選択します。
2. **Create** をクリックします。
3. ポリシーに名前を付けて説明し、アラートがトリガーされるために満たす必要がある条件を設定します。たとえば、ピーク接続セッション、ピーク切断セッション、およびピーク同時合計セッションの警告値と危険値を指定します。警告値は危険値より大きくしてはいけません。詳細については、アラートポリシーの条件を参照してください。
4. 再アラート間隔を設定します。アラートの条件が引き続き満たされている場合、この時間間隔でアラートが再度トリガーされ、アラートポリシーで設定されている場合は、メール通知が生成されます。却下されたアラートは、再アラート間隔でメール通知を生成しません。
5. スコープを設定します。たとえば、特定のデリバリーグループに設定します。
6. 通知設定で、アラートがトリガーされたときにメールで通知されるべきユーザーを指定します。アラートポリシーでメール通知設定を行うには、**Email Server Configuration**タブでメールサーバーを指定する必要があります。
7. 「**保存**」をクリックします。

スコープに20以上のデリバリーグループが定義されたポリシーを作成する場合、構成の完了に約30秒かかることがあります。この間、スピナーが表示されます。

最大20のユニークなデリバリーグループ（合計1000のデリバリーグループターゲット）に対して50を超えるポリシーを作成すると、応答時間が増加する可能性があります（5秒以上）。

アクティブなセッションを含むマシンをあるデリバリーグループから別のデリバリーグループに移動すると、マシンパラメーターを使用して定義された誤ったデリバリーグループアラートがトリガーされる可能性があります。

> **注：** アラートポリシーを削除した後、そのポリシーによって生成されたアラート通知が停止するまでに最大30分かかる場合があります。

アラートポリシーの条件

以下に、アラートカテゴリ、アラートを軽減するための推奨アクション、および定義されている場合は組み込みポリシー条件を示します。組み込みのアラートポリシーは、アラートおよび再アラートの間隔が60分に設定されています。

ピーク接続セッション

- Directorのセッショントレンドビューで、接続済みセッションのピークを確認します。

- セッション負荷に対応する十分な容量があることを確認してください。
- 必要に応じて新しいマシンを追加する

ピーク切断セッション

- Directorのセッショントレンドビューで、切断済みセッションのピークを確認します。
- セッション負荷に対応できる十分な容量があることを確認します。
- 必要に応じて、新しいマシンを追加します。
- 必要に応じて、切断されたセッションをログオフします。

ピーク時の同時合計セッション数

- Directorのセッショントレンドビューで、同時実行セッションのピークを確認します。
- セッション負荷に対応できる十分な容量があることを確認します。
- 必要に応じて、新しいマシンを追加します。
- 必要に応じて、切断されたセッションをログオフします。

CPU

CPU 使用率の割合は、プロセスを含む VDA 上の全体的な CPU 消費量を示します。個々のプロセスによる CPU 使用率の詳細については、対応する VDA の ページで確認できます。

- **マシン詳細 > 履歴使用率の表示 > 上位10プロセス**に移動し、CPUを消費しているプロセスを特定します。プロセスレベルのリソース使用状況統計の収集を開始するには、プロセス監視ポリシーが有効になっていることを確認してください。
- 必要に応じてプロセスを終了します。
- プロセスを終了すると、保存されていないデータが失われます。
- すべてが期待どおりに機能している場合は、将来的に追加のCPUリソースを追加します。

> **注：**
>
> ポリシー設定**リソース監視を有効にする**は、VDAがインストールされているマシンでのCPUおよびメモリのパフォーマンスカウンターの監視に対して、デフォルトで許可されています。このポリシー設定が無効になっている場合、CPUおよびメモリの状態に関するアラートはトリガーされません。詳細については、「監視ポリシー設定」を参照してください。

> **スマートポリシー条件:**

- **スコープ：** デリバリーグループ、マルチセッションOSスコープ
- **しきい値:** 警告 - 80%、危険 - 90%

メモリ

メモリ使用率は、VDA上の全体的なメモリ消費量（プロセスによるものを含む）を示します。個々のプロセスによるメモリ使用量に関する詳細な情報は、対応するVDAの**マシン詳細**ページから取得できます。

- **マシン詳細 > 履歴使用率の表示 > 上位10プロセス**に移動し、メモリを消費しているプロセスを特定します。プロセスレベルのリソース使用状況統計の収集を開始するには、プロセス監視ポリシーが有効になっていることを確認してください。
- 必要に応じてプロセスを終了します。
- プロセスを終了すると、保存されていないデータが失われます。
- すべてが期待どおりに機能している場合は、将来的に追加のメモリを追加します。

> **注：**
>
> ポリシー設定**リソース監視を有効にする**は、VDAがインストールされているマシンでのCPUおよびメモリのパフォーマンスカウンターの監視に対して、デフォルトで許可されています。このポリシー設定が無効になっている場合、CPUおよびメモリの状態に関するアラートはトリガーされません。詳細については、「監視ポリシー設定」を参照してください。

> **スマートポリシー条件:**

- **スコープ：** デリバリーグループ、マルチセッションOSスコープ
- **閾値:** 警告 - 80%、危機的 - 90%

接続失敗率

過去1時間の接続失敗の割合。

- 試行された総接続数に対する総失敗数に基づいて計算されます。
- Directorの接続失敗トレンドビューで、構成ログから記録されたイベントを確認します。
- アプリケーションまたはデスクトップが到達可能であるかどうかを判断します。

接続失敗数

過去1時間の接続失敗数。

- Directorの接続失敗トレンドビューで、構成ログから記録されたイベントを確認します。
- アプリケーションまたはデスクトップが到達可能であるかどうかを判断します。

ICA® RTT (平均)

平均ICAラウンドトリップ時間。

- 根本原因を特定するために、ICA RTTの内訳についてCitrix ADMを確認してください。詳細については、Citrix ADMドキュメントを参照してください。
- Citrix ADMが利用できない場合は、DirectorのユーザーDetailビューでICA RTTと遅延を確認し、ネットワークの問題か、アプリケーションまたはデスクトップの問題かを判断してください。

ICA RTT (セッション数)

閾値のICAラウンドトリップ時間を超えるセッションの数。

- ICA RTTが高いセッション数についてCitrix ADMを確認してください。詳細については、Citrix ADMドキュメントを参照してください。
- Citrix ADMが利用できない場合は、ネットワークチームと協力して根本原因を特定してください。

  スマートポリシーの条件:

  - **スコープ:** デリバリーグループ、マルチセッションOSスコープ
  - **しきい値:** 警告 - 5セッション以上で300ミリ秒、重大 - 10セッション以上で400ミリ秒

ICA RTT (セッションの割合)

平均ICAラウンドトリップ時間を超えるセッションの割合。

- ICA RTTが高いセッション数についてCitrix ADMを確認してください。詳細については、Citrix ADMドキュメントを参照してください。
- Citrix ADMが利用できない場合は、ネットワークチームと協力して根本原因を特定してください。

ICA RTT (ユーザー)

指定されたユーザーによって起動されたセッションに適用されるICAラウンドトリップ時間。ICA RTTが少なくとも1つのセッションでしきい値を超えた場合、アラートがトリガーされます。

失敗したマシン（シングルセッションOS）

失敗したシングルセッションOSマシンの数。失敗は、Directorのダッシュボードビューとフィルタービューに示されているように、さまざまな理由で発生する可能性があります。

- Citrix Scout診断を実行して、根本原因を特定します。

  スマートポリシー条件:

  - **スコープ:** デリバリーグループ、マルチセッションOSスコープ
  - **しきい値:** 警告 - 1、重大 - 2

失敗したマシン (マルチセッションOS)

失敗したマルチセッションOSマシンの数。失敗は、Directorのダッシュボードビューとフィルタービューに示されているように、さまざまな理由で発生する可能性があります。

- Citrix Scout診断を実行して、根本原因を特定します。

  スマートポリシー条件:

  - **スコープ:** デリバリーグループ、マルチセッションOSスコープ
  - **しきい値:** 警告 - 1、重大 - 2

失敗したマシン (割合)

デリバリーグループ内の失敗したシングルセッションおよびマルチセッションOSマシンの割合。失敗したマシンの数に基づいて計算されます。このアラート条件を使用すると、デリバリーグループ内の失敗したマシンの割合としてアラートしきい値を構成でき、30秒ごとに計算されます。 失敗は、Directorのダッシュボードビューとフィルタービューに示されているように、さまざまな理由で発生する可能性があります。根本原因を特定するには、Citrix Scout診断を実行してください。詳細については、ユーザーの問題のトラブルシューティングを参照してください。

平均ログオン時間

過去1時間に発生したログオンの平均ログオン時間。

- ログオン期間に関する最新のメトリックを取得するには、Directorダッシュボードを確認してください。短期間に多数のユーザーがログオンすると、ログオン期間が長くなる可能性があります。
- ベースラインとログオンの内訳を確認して、原因を絞り込みます。詳細については、「ユーザーログオンの問題の診断」を参照してください。

  スマートポリシー条件:

- **スコープ:** デリバリーグループ、マルチセッションOSスコープ
- **しきい値:** 警告 - 45秒、重大 - 60秒

ログオン時間（ユーザー）

過去1時間に発生した、指定されたユーザーのログオンのログオン時間。

負荷評価インデックス

過去5分間の負荷評価インデックスの値。

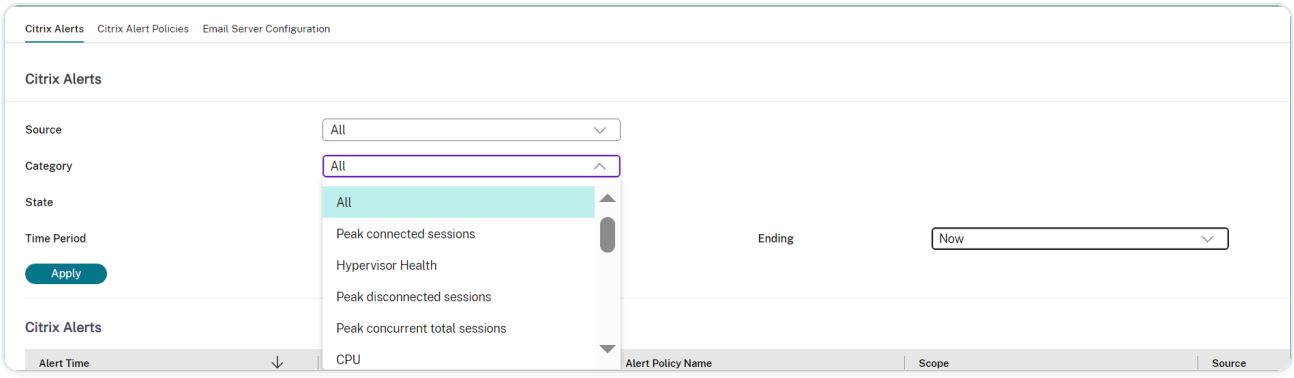
- Directorで、ピーク負荷（最大負荷）が発生している可能性のあるマルチセッションOSマシンを確認します。ダッシュボード（障害）とトレンドの負荷評価インデックスレポートの両方を確認します。

  スマートポリシーの条件:

  - **スコープ:** デリバリーグループ、マルチセッションOSスコープ
  - **しきい値:** 警告 - 80%、重大 - 90%

ハイパーバイザーアラートの監視

Directorは、ハイパーバイザーの健全性を監視するためのアラートを表示します。XenServer®およびVMware vSphereからのアラートは、ハイパーバイザーのパラメーターと状態の監視に役立ちます。ハイパーバイザーへの接続ステータスも監視され、ホストのクラスターまたはプールが再起動されたり、利用できなくなったりした場合にアラートが提供されます。

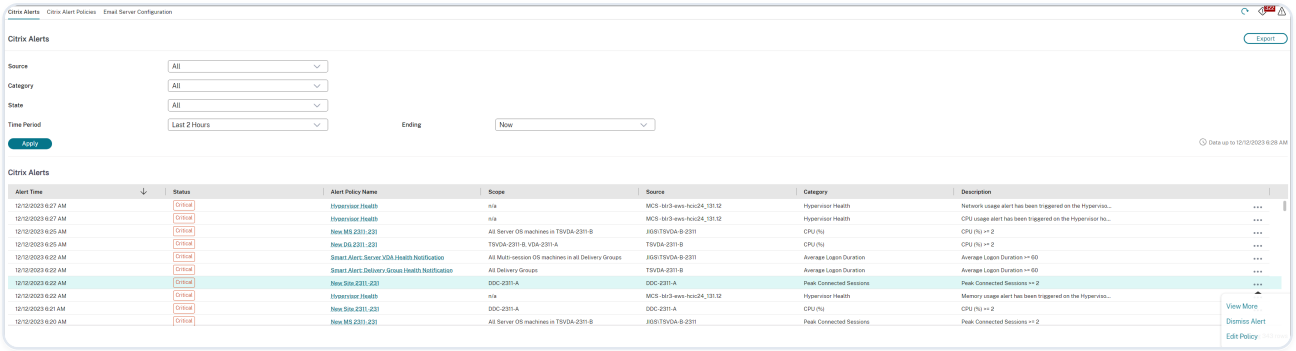


ハイパーバイザーアラートを受信するには、Web Studioでホスティング接続が作成されていることを確認してください。詳細については、「接続とリソース」を参照してください。ハイパーバイザーアラートの監視対象となるのは、これらの接続のみです。

これらのアラートは、しきい値に達するか、それを超えると表示されます。ハイパーバイザーアラートには次のものがあります。

- 重大 — ハイパーバイザーアラームポリシーの重大なしきい値に達したか、超えた場合

- 警告 — ハイパーバイザーアラームポリシーの警告しきい値に達したか、超えた場合
- 却下済み — アクティブなアラートとして表示されなくなったアラート



この機能には、Delivery Controller™バージョン7 1811以降が必要です。Directorの古いバージョンをサイト7 1811以降で使用している場合、ハイパーバイザーアラートの数のみが表示されます。アラートを表示するには、Directorをアップグレードする必要があります。

次の表は、ハイパーバイザーアラートのさまざまなパラメーターと状態について説明しています。

アラート	サポートされているハイパーバイザー	トリガー元	条件	構成
CPU使用率	ゼノサーバー、ヴイエムウェアブイスフィア	ハイパーバイザー	CPU使用率アラートのしきい値に達したか、超えた場合	アラートのしきい値はハイパーバイザーで構成する必要があります。
メモリ使用量	ゼノサーバー、ヴイエムウェアブイスフィア	ハイパーバイザー	メモリ使用量アラートしきい値に達したか、超過しました	アラートのしきい値はハイパーバイザーで構成する必要があります。
ネットワーク使用量	ゼノサーバー、ヴイエムウェアブイスフィア	ハイパーバイザー	ネットワーク使用量アラートしきい値に達したか、超過しました	アラートのしきい値はハイパーバイザーで構成する必要があります。
ディスク使用量	ヴイエムウェアブイスフィア	ハイパーバイザー	ディスク使用量アラートしきい値に達したか、超過しました	アラートのしきい値はハイパーバイザーで構成

アラート	サポートされているハイパーバイザー	トリガー元	条件	構成
				する必要があります。
ホスト接続または電源状態	ヴイエムウェア ブイスフィア	ハイパーバイザー	ハイパーバイザーホストが再起動されたか、利用できません	アラートはVMware vSphereにプリビルドされています。追加の構成は不要です。
ハイパーバイザー接続が利用できません	ゼノサーバー、ヴイエムウェア ブイスフィア	デリバリーコントローラー	ハイパーバイザー（プールまたはクラスター）への接続が失われたか、電源がオフになったか、再起動されました。このアラートは、接続が利用できない間、1時間ごとに生成されます。	アラートはDelivery Controllerにプリビルドされています。追加の構成は不要です。

注：

アラートの構成の詳細については、Citrix XenCenter Alerts を参照するか、VMware vCenter Alertsのドキュメントを確認してください。

メール通知設定は、**Citrix Alerts Policy > Site Policy > Hypervisor Health**で構成できます。ハイパーバイザーアラートポリシーのしきい値条件は、Directorからではなく、ハイパーバイザーからのみ構成、編集、無効化、または削除できます。ただし、メール設定の変更やアラートの解除はDirectorで行うことができます。インフラストラクチャの監視が役割に含まれていない場合は、アラートを無効にできます。

重要:

- ハイパーバイザーによってトリガーされたアラートは、Directorで取得および表示されます。ただし、ハイパーバイザーアラートのライフサイクル/状態の変更はDirectorには反映されません。
- ハイパーバイザーコンソールで正常、却下、または無効化されたアラートは、Directorに表示され続け、明示的に却下する必要があります。
- Directorで却下されたアラートは、ハイパーバイザーコンソールでは自動的に却下されません。

障害のトラブルシューティングのためにデータをフィルタリングする

ダッシュボードの数値をクリックするか、フィルターメニューから事前定義されたフィルターを選択すると、選択したマシンまたは障害タイプに基づいてデータを表示するフィルタービューが開きます。

事前定義されたフィルターは編集できませんが、事前定義されたフィルターをカスタムフィルターとして保存し、後で変更できます。また、すべてのデリバリーグループにわたるマシン、接続、セッション、およびアプリケーションインスタンスのカスタムフィルタービューを作成できます。

1. ビューを選択します。

   - **マシン**。シングルセッションOSマシンまたはマルチセッションOSマシンを選択します。これらのビューには、構成されたマシンの数が表示されます。マルチセッションOSマシンのタブには、ロード評価インデックスも含まれており、これはパフォーマンスカウンターの分布と、リンクにカーソルを合わせると表示されるセッション数のツールヒントを示します。
   - **セッション**。セッションビューからセッション数を確認することもできます。アイドル時間測定を使用して、しきい値期間を超えてアイドル状態になっているセッションを特定します。**関連ユーザー**をクリックすると、そのユーザーのアクティビティマネージャーが開きます。**エンドポイント**名をクリックすると、そのエンドポイントのアクティビティマネージャーが開きます。**詳細表示**をクリックすると、それぞれ**ユーザーの詳細**ページまたは**エンドポイントの詳細**ページが開きます。詳細については、「ユーザーの詳細」を参照してください。
   - **接続**。接続を、過去60分、過去24時間、過去7日間など、異なる期間でフィルタリングします。

- **アプリケーションインスタンス**。このビューには、サーバーおよびシングルセッションOSのVDA上のすべてのアプリケーションインスタンスのプロパティが表示されます。マルチセッションOSのVDA上のアプリケーションインスタンスでは、セッションアイドル時間の測定値が利用可能です。

> **注：**
>
> Windows 10 1809コンピューターにインストールされたVDAでデスクトップセッションを起動した場合、Directorのアクティビティマネージャーでは、Microsoft EdgeとOfficeがアクティブに実行されているアプリケーションとして表示されることがありますが、実際にはバックグラウンドでのみ実行されています。

2. **フィルター条件**で、基準を選択します。
3. 必要に応じて、各ビューの追加タブを使用してフィルターを完了します。
4. 必要に応じて、追加の列を選択してさらにトラブルシューティングを行います。
5. フィルターを保存して名前を付けます。
6. 複数のDirectorサーバーからフィルターにアクセスするには、それらのサーバーからアクセス可能な共有フォルダーにフィルターを保存します。
   - 共有フォルダーには、Directorサーバー上のアカウントに対する変更権限が必要です。
   - Directorサーバーは、共有フォルダーにアクセスするように構成する必要があります。構成するには、**IIS マネージャー**を実行します。**サイト \> 既定のWebサイト \> Director\ > アプリケーション設定**で、**Service.UserSettingsPath**設定を共有フォルダーのUNCパスを反映するように変更します。
7. 後でフィルターを開くには、**フィルター**メニューからフィルタータイプ（マシン、セッション、接続、またはアプリケーションインスタンス）を選択し、保存されたフィルターを選択します。
8. **エクスポート**をクリックして、データをCSV形式ファイルにエクスポートします。最大100,000レコードのデータをエクスポートできます。この機能は、Delivery Controller™バージョン1808以降で利用可能です。
9. 必要に応じて、**マシン**または**接続**ビューでは、フィルターされたリストで選択したすべてのマシンに対して電源コントロールを使用します。セッションビューでは、セッションコントロールまたはメッセージ送信オプションを使用します。

10. 「**マシン**」ビューと「**接続**」ビューで、失敗したマシンまたは接続の「**障害理由**」をクリックすると、障害の詳細な説明と、障害のトラブルシューティングに推奨されるアクションが表示されます。マシンおよび接続の障害理由と推奨されるアクションについては、Citrix Director の障害理由とトラブルシューティングを参照してください。
11. **マシン**ビューで、マシン名リンクをクリックすると、対応する**マシン詳細**ページに移動します。このページには、マシンの詳細が表示され、電源コントロールが提供され、CPU、メモリ、ディスク監視、および GPU 監視グラフが表示されます。また、**履歴使用率の表示**をクリックすると、マシンのリソース使用率の傾向を確認できます。詳細については、マシンのトラブルシューティングを参照してください。
12. **アプリケーションインスタンス**ビューで、しきい値期間よりも長い**アイドル時間**に基づいて並べ替えまたはフィルター処理を行います。終了するアイドル状態のアプリケーションインスタンスを選択します。アプリケーションインスタンスのログオフまたは切断により、同じセッション内のすべてのアクティブなアプリケーションインスタンスが終了します。詳細については、「アプリケーションのトラブルシューティング」を参照してください。Director、Delivery Controller、およびVDAがバージョン7.13以降の場合、アプリケーションインスタンスフィルターページとセッションフィルターページでのアイドル時間の測定値が利用可能です。

> **注：** Web Studioでは、配信グループ内の単一のVDAに、異なるユーザーまたはユーザーグループに対して複数のデスクトップ割り当てルール（DAR）を割り当てることができます。StoreFront™は、ログインユーザーのDARに従って、対応する表示名で割り当てられたデスクトップを表示します。ただし、DirectorはDARをサポートしておらず、ログインユーザーに関係なく、配信グループ名を使用して割り当てられたデスクトップを表示します。その結果、Directorで特定のデスクトップをマシンにマッピングすることはできません。StoreFrontに表示される割り当てられたデスクトップをDirectorに表示される配信グループ名にマッピングするには、次のPowerShellコマンドを使用します。

```
Get-BrokerDesktopGroup | Where-Object { $\_.Uid -eq (Get-
BrokerAssignmentPolicyRule | Where-Object { $\_.PublishedName -eq "\<Name
on StoreFront\>" }).DesktopGroupUid } | Select-Object -Property Name, Uid
```

サイト全体の履歴トレンドを監視する

トレンドビューは、以下のパラメータについて、各サイトの履歴トレンド情報にアクセスします。

- セッション
- 接続障害

- マシン障害
- ログオンパフォーマンス
- 負荷評価
- キャパシティ管理
- マシン使用状況
- リソース使用率
- 各サイトのネットワーク分析。

この情報を見つけるには、**トレンド**メニューをクリックします。

ズームイン ドリルダウン機能を使用すると、期間をズームイン（グラフのデータポイントをクリック）し、トレンドに関連する詳細を表示するためにドリルダウンすることで、トレンドグラフをナビゲートできます。この機能により、誰が、または何が影響を受けているかの詳細をよりよく理解できます。

各グラフのデフォルトのスコープを変更するには、データに別のフィルターを適用します。

履歴トレンド情報が必要な期間を選択してください。期間の利用可能性は、Directorの展開によって次のように異なります。

- Premiumライセンスサイトでは、最大1年間 (365日) のトレンドレポートを利用できます。
- Advancedライセンスサイトでは、最大1か月間 (31日) のトレンドレポートを利用できます。
- PremiumおよびAdvanced以外のライセンスサイトでは、最大7日間のトレンドレポートを利用できます。

> **注：**
>
> - すべてのDirector展開において、期間が「先月」（**現在まで**）以下に設定されている場合、セッション、障害、ログオンパフォーマンスのトレンド情報はグラフとテーブルとして利用できます。期間がカスタム終了日を指定した「先月」または「昨年」として選択されている場合、トレンド情報はグラフとして利用でき、テーブルとしては利用できません。
> - Monitor Serviceのグルーミング保持値によって、トレンドデータの可用性が制御されます。デフォルト値は、データ粒度と保持で確認できます。Premiumライセンスサイトのお客様は、グルーミング保持を希望する保持日数に変更できます。

- IIS Managerの以下のパラメータは、選択可能なカスタム終了日の範囲を制御します。ただし、選択された日付のデータ可用性は、測定される特定のメトリックのグルーミング保持設定によって異なります。

パラメーター	デフォルト値
UI.TrendsLast2HoursRange	3
UI.TrendsLast24HoursRange	32
UI.TrendsLast7DaysRange	32
UI.TrendsLastMonthRange	365

利用可能なトレンド

セッションの傾向を表示: 「**セッション**」タブから、デリバリーグループと期間を選択して、同時セッション数に関する詳細情報を表示します。

「**セッションの自動再接続**」列には、セッション内の自動再接続の数が表示されます。自動再接続は、セッションの信頼性ポリシーまたはクライアント自動再接続ポリシーが有効な場合に有効になります。エンドポイントでネットワークの中断が発生した場合、次のポリシーが有効になります。

- セッションの信頼性が有効になり（デフォルトで3分間）、Citrix Receiver™またはCitrix Workspace™アプリがVDAへの接続を試行します。
- クライアント自動再接続が3分から5分の間に有効になり、クライアントがVDAへの接続を試行します。

両方の再接続がキャプチャされ、ユーザーに表示されます。この情報は、再接続が発生してからDirector UIに表示されるまでに最大5分かかる場合があります。

自動再接続情報は、中断のあるネットワーク接続の表示とトラブルシューティングに役立ちます。また、シームレスなエクスペリエンスを持つネットワークも分析します。フィルターで選択した特定のデリバリーグループまたは期間の再接続数を表示できます。ドリルダウンでは、セッションの信頼性やクライアント自動再接続、タイムスタンプ、エンドポイントIP、Workspaceアプリがインストールされているマシンのエンドポイント名などの追加情報が提供されます。

デフォルトでは、ログはイベントのタイムスタンプの降順でソートされます。この機能は、Windows用Citrix Workspaceアプリ、Mac用Citrix Workspaceアプリ、Windows用Citrix Receiver、およびMac用Citrix Receiverで利用できます。この機能には、Delivery Controller™バージョン7 1906以降、およびVDA 1906以降が必要です。

セッションの再接続の詳細については、「セッション」を参照してください。

ポリシーの詳細については、「クライアント自動再接続ポリシー設定」および「セッションの信頼性ポリシー設定」を参照してください。

自動再接続データがDirectorに表示されない場合があります。その理由は次のとおりです。

- WorkspaceアプリがVDAに自動再接続データを送信していません。
- VDAがモニターサービスにデータを送信していません。
- Delivery Controllerは、対応するセッションがない可能性があるため、VDAペイロードを破棄します。

> **注：**
>
> 特定のCitrix Gatewayポリシーが設定されている場合、クライアントIPアドレスが正しく取得されないことがあります。

> **接続障害の傾向を表示:** 「障害」タブから、接続、マシンタイプ、障害タイプ、デリバリーグループ、および期間を選択して、サイト全体のユーザー接続障害に関する詳細情報を含むグラフを表示します。

マシン障害の傾向を表示: Single-session OS Machine FailuresタブまたはMulti-session OS Machinesタブから、障害タイプ、デリバリーグループ、および期間を選択すると、サイト全体のマシン障害に関する詳細情報を含むグラフが表示されます。

ログオンパフォーマンスの傾向を表示: ログオンパフォーマンスタブから、デリバリーグループと期間を選択すると、サイト全体のユーザーログオン時間の詳細情報と、ログオン数がパフォーマンスに影響するかどうかを示すグラフが表示されます。このビューには、ブローカー処理時間やVM起動時間など、ログオンフェーズの平均時間も表示されます。 このデータはユーザーログオン専用であり、切断されたセッションから再接続しようとするユーザーは含まれません。 グラフの下の表には、ユーザーセッションごとのログオン時間が表示されます。表示する列を選択し、任意の列でレポートを並べ替えることができます。 詳細については、「ユーザーログオンの問題の診断」を参照してください。

負荷評価の傾向を表示: Load Evaluator Indexタブから、Multi-session OSマシン間で分散される負荷に関する詳細情報を含むグラフを表示します。このグラフのフィルターオプションには、デリバリーグループまたはデリバリーグループ内のMulti-session OSマシン、Multi-session OSマシン（デリバリーグループ内のMulti-session OSマシンが選択されている場合にのみ利用可能）、および範囲が含まれます。

ホストされたアプリケーションの使用状況を表示: この機能の利用可能性は、組織のライセンスによって異なります。 **Capacity Management**タブから、**Hosted Applications Usage**タブを選択します。デリバリーグループと期間を選択すると、ピーク時の同時使用状況を示すグラフと、アプリケーションベースの使用状況を示す表が表示されます。Application Based Usage表から、特定のアプリケーションを選択して詳細と、そのアプリケーションを使用している、または使用したユーザーのリストを確認できます。

Single-sessionおよびMulti-session OSの使用状況を表示: トレンドビューには、サイト別およびデリバリーグループ別のSingle-session OSの使用状況が表示されます。**サイト**を選択すると、デリバリーグループごとの使用状況が表示されます。デリバリーグループを選択すると、ユーザーごとの使用状況が表示されます。 トレンドビューには、サイト別、デリバリーグループ別、およびマシン別のMulti-session OSの使用状況も表示されます。**サイト**を選択すると、デリバリーグループごとの使用状況が表示されます。デリバリーグループを選択すると、マシンごとおよびユーザーごとの使用状況が表示されます。マシンが選択されている場合は、ユーザーごとの使用状況が表示されます。

仮想マシンの使用状況を表示: マシン使用状況タブから、**シングルセッションOSマシンまたはマルチセッションOSマシン**を選択すると、VMの使用状況をリアルタイムで確認でき、サイトのキャパシティニーズを迅速に評価できます。 シングルセッションOSの可用性 - サイト全体または特定のデリバリーグループにおけるシングルセッションOSマシン（VDI）の可用性による現在の状態を表示します。 マルチセッションOSの可用性 - サイト全体または特定のデリバリーグループにおけるマルチセッションOSマシンの可用性による現在の状態を表示します。

> **注:** 利用可能なカウンターに表示されるマシンの数には、メンテナンスモードのマシンが含まれます。

> **リソース使用率の表示: リソース使用率**タブから、**シングルセッションOSマシンまたはマルチセッションOSマシン**を選択すると、CPUおよびメモリ使用量、IOPS、各VDIマシンのディスク待機時間に関する履歴トレンドデータを確認でき、より適切なキャパシティプランニングに役立ちます。 この機能には、Delivery ControllerおよびVDAの**バージョン7.11**以降が必要です。 グラフには、平均CPU、平均メモリ、平均IOPS、ディスク待機時間、ピーク時

の同時セッションのデータが表示されます。マシンにドリルダウンして、CPUを消費している上位10個のプロセスのデータとグラフを表示できます。

デリバリーグループと期間でフィルターします。CPU、メモリ使用量、およびピーク時の同時セッションのグラフは、過去2時間、24時間、7日間、1か月、1年間で利用できます。平均IOPSとディスク遅延のグラフは、過去24時間、1か月、1年間で利用できます。

注：

- 履歴マシン使用率ページの「上位10プロセス」テーブルでデータを収集して表示するには、監視ポリシー設定の**プロセス監視を有効にする**を**許可**に設定する必要があります。このポリシーは、デフォルトで**禁止**に設定されています。すべてのリソース使用率データはデフォルトで収集されます。これは、**リソース監視を有効にする**ポリシー設定を使用して無効にできます。グラフの下のテーブルには、マシンごとのリソース使用率データが表示されます。詳細については、「監視ポリシー設定」を参照してください。
- 平均IOPSは日次平均を示します。ピークIOPSは、選択した期間のIOPS平均の最高値として計算されます。（IOPS平均とは、VDAで1時間中に収集されたIOPSの時間平均です）。
- マシンのドリルダウンでは、平均CPUまたは平均メモリ使用量が1%を超えるプロセスが一覧表示されます。これは、場合によっては10個未満のプロセスしか表示されない可能性があることを意味します。

ネットワーク分析データの表示: この機能の可用性は、組織のライセンスと管理者権限によって異なります。この機能には、Delivery Controllerの**バージョン7.11**以降が必要です。

ネットワークタブから、ネットワーク分析を監視します。これにより、ネットワークのユーザー、アプリケーション、デスクトップのコンテキストビューが提供されます。この機能により、DirectorはCitrix ADMからのHDX Insightレポートを通じて、展開におけるICAトラフィックの高度な分析を提供します。詳細については、「ネットワーク分析の構成」を参照してください。

アプリケーション障害の表示: アプリケーション障害タブには、VDA上の公開アプリケーションに関連する障害が表示されます。

この機能には、Delivery ControllerおよびVDAの**バージョン7.15**以降が必要です。Windows Vista以降を実行するシングルセッションOS VDA、およびWindows Server 2008以降を実行するマルチ

セッションOS VDAがサポートされています。 詳細については、「履歴アプリケーション障害監視」を参照してください。

デフォルトでは、マルチセッションOS VDAからのアプリケーション障害のみが表示されます。監視ポリシーを使用して、アプリケーション障害の監視を設定できます。詳細については、「監視ポリシー設定」を参照してください。

プローブ結果の表示: プローブ結果タブには、構成ページでプローブ用に構成されたアプリケーションおよびデスクトップのプローブ結果が表示されます。ここでは、障害が発生した起動の段階が記録されます。

詳しくは、「アプリケーションおよびデスクトップのプローブ」を参照してください。

カスタマイズされたレポートの作成: カスタムレポートタブは、監視データベースからリアルタイムおよび履歴データを表形式で含むカスタムレポートを生成するためのユーザーインターフェイスを提供します。

この機能には、Delivery Controllers **バージョン7.12**以降が必要です。

以前に保存したカスタムレポートクエリのリストから、**実行してダウンロード**をクリックしてレポートをCSV形式でエクスポートしたり、**ODataをコピー**をクリックして対応するODataクエリをコピーして共有したり、**編集**をクリックしてクエリを編集したりできます。 マシン、接続、セッション、またはアプリケーションインスタンスに基づいてカスタムレポートクエリを作成できます。マシン、デリバリーグループ、期間などのフィールドに基づいてフィルター条件を指定します。カスタムレポートに必要な追加の列を指定します。プレビューには、レポートデータのサンプルが表示されます。カスタムレポートクエリを保存すると、保存されたクエリのリストに追加されます。

コピーしたODataクエリに基づいてカスタムレポートクエリを作成できます。これを行うには、ODataクエリオプションを選択し、コピーしたODataクエリを貼り付けます。結果のクエリは後で実行するために保存できます。

> **注:** ODataクエリを使用して生成されたプレビューおよびエクスポートレポートの列名はローカライズされておらず、英語で表示されます。

> グラフ上のフラグアイコンは、特定の期間における重要なイベントまたはアクションを示します。フラグにマウスを合わせ、クリックしてイベントまたはアクションを一覧表示します。

注：

- HDX™接続ログオンデータは、7より前のVDAでは収集されません。それより前のVDAの場合、グラフデータは0と表示されます。
- Citrix Studioで削除されたデリバリーグループは、関連データが整理されるまで、Director Trendsフィルターで選択可能です。削除されたデリバリーグループを選択すると、保持期間までの利用可能なデータのグラフが表示されます。ただし、テーブルにはデータは表示されません。
- アクティブなセッションを含むマシンをあるデリバリーグループから別のデリバリーグループに移動すると、新しいデリバリーグループの**リソース使用率と負荷評価インデックス**テーブルに、古いデリバリーグループと新しいデリバリーグループから統合されたメトリックが表示されます。

Autoscaleで管理されているマシンの監視

Autoscaleは、デリバリーグループ内の登録済みすべてのマルチセッションおよびシングルセッションOSマシンに対するプロアクティブな電源管理を可能にする電源管理機能です。Web Studioで、選択したデリバリーグループに対してAutoscaleを構成できます。詳しくは、「Autoscale」(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/manage-deployment/autoscale.html)を参照してください。 Directorを使用して、Autoscaleが有効なマシンの主要なメトリックを監視できます。

マシン使用状況

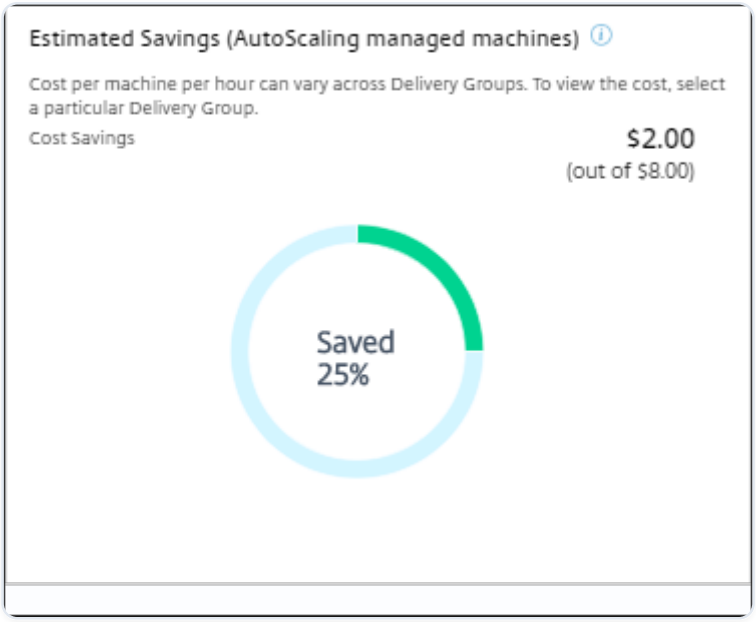
マシン使用状況ページには、選択したデリバリーグループと期間について、電源がオンになっているAutoscaleが有効なマルチセッションおよびシングルセッションOSマシンの合計数が表示されます。このメトリックは、デリバリーグループ内のマシンの実際の使用状況を示します。 **シングルセッションOSマシン**タブまたは**マルチセッションOSマシン**タブから、デリバリーグループと期間を選択します。

このグラフには、次のメトリックが表示されます:

- **電源オンのマシン** - 電源がオンになっているAutoscaleが有効なマシンの数
- **登録済みマシン** - 登録済みのマルチセッションまたはシングルセッションOSマシンの数
- **メンテナンス中のマシン** - メンテナンスモードがオンになっているマルチセッションまたはシングルセッションOSマシンの数

推定節約額

マシン使用状況ページには、選択したデリバリーグループでAutoscaleを有効にすることによって達成された推定コスト削減額も表示されます。



推定節約額は、**デリバリーグループの編集** > **Autoscale**で構成されている、1時間あたりのマシンごとの節約額（米ドル）の割合として計算されます。マシンごとの節約額の構成について詳しくは、「Autoscale」(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/manage-deployment/autoscale.html)を参照してください。

すべてのデリバリーグループを選択すると、すべてのデリバリーグループにおける推定節約額の平均値が表示されます。

推定節約額は、管理者が既存のインフラストラクチャを統合し、最大限の節約と利用率を達成するためのキャパシティを計画するのに役立ちます。

マシンとセッションのアラート通知

Directorダッシュボードには、アラート通知が表示されます。これらの通知はさらにドリルダウンできます。アラートの詳細は、**アラート**ページに表示されます。

- デリバリーグループでアラートポリシーを作成するには、**アラート** > **Citrixアラートポリシー** > **デリバリーグループポリシー**に移動します。
- ここでは、次の警告および重大なしきい値を設定できます。
  - 失敗したマシン（シングルセッションOS）および失敗したマシン（マルチセッションOS）、,
  - デリバリーグループ内のピーク接続セッション、ピーク切断セッション、およびピーク同時合計セッション。

- デリバリーグループ内の対応するメトリックがしきい値に達すると、アラートが生成されます。

アラートポリシーの条件と新しいアラートポリシーの作成に関する詳細については、「アラートと通知」を参照してください。

マシンのステータス

- **フィルター** > **マシン**には、すべてのマシンの電源状態が表形式で表示されます。特定のデリバリーグループでフィルターできます。
- **フィルター** > **セッション**には、マシン名でフィルターして、関連するセッションとそのリアルタイムステータスが表示されます。
- **トレンド** > **セッション**で、デリバリーグループと期間を選択すると、セッションとその関連メトリックのトレンドが表示されます。

詳細については、「障害のトラブルシューティングのためのデータのフィルター」(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/director/site-analytics/filters-data.html)を参照してください。

負荷評価のトレンド

トレンド > **負荷評価インデックス**ページには、マルチセッションOSマシン間で分散される負荷に関する詳細情報を含むグラフが表示されます。このグラフのフィルターオプションには、デリバリーグループまたはデリバリーグループ内のマルチセッションOSマシン、マルチセッションOSマシン（デリバリーグループ内のマルチセッションOSマシンが選択されている場合にのみ利用可能）、および範囲が含まれます。負荷評価インデックスは、CPU合計、メモリ、ディスク、またはセッションの割合として表示され、最後の間隔での接続ユーザー数と比較して示されます。

展開のトラブルシューティング

ヘルプデスク管理者として、問題を報告しているユーザーを検索し、そのユーザーに関連付けられているセッションまたはアプリケーションの詳細を表示できます。同様に、問題が報告されているマシンまたはエンドポイントを検索します。関連するメトリックを監視し、適切なアクションを実行することで、問題を迅速に解決します。

利用可能なアクションは次のとおりです。

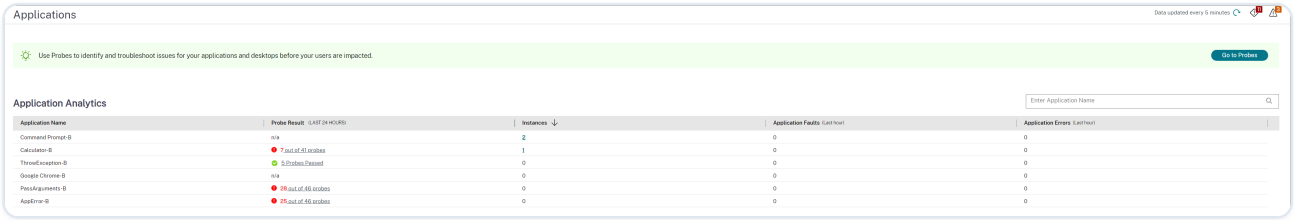
- 応答しないアプリケーションまたはプロセスを終了する
- ユーザーのマシンでのシャドウ操作
- 応答しないセッションからログオフする
- マシンを再起動する

- マシンをメンテナンスモードにする
- ユーザープロファイルをリセットする

アプリケーションのトラブルシューティング

アプリケーション分析

「**アプリケーション**」ビューには、アプリケーションベースの分析が統合された単一のビューで表示され、アプリケーションのパフォーマンスを効率的に分析および管理するのに役立ちます。サイトで公開されているすべてのアプリケーションの正常性と使用状況に関する貴重な洞察を得ることができます。デフォルトビューは、実行中の上位アプリケーションを特定するのに役立ちます。 この機能には、Delivery Controllersバージョン7.16以降およびVDAバージョン7.15以降が必要です。



「**プローブ結果**」列には、過去24時間で実行されたアプリケーションプローブの結果が表示されます。プローブ結果リンクをクリックすると、「**トレンド**」\>「**アプリケーションプローブ結果**」ページで詳細を確認できます。アプリケーションプローブの構成方法の詳細については、「アプリケーションおよびデスクトップのプローブ」を参照してください。

「**インスタンス**」列には、アプリケーションの使用状況が表示されます。これは、現在実行中のアプリケーションインスタンスの数（接続済みおよび切断済みの両方のインスタンス）を示します。さらにトラブルシューティングを行うには、「**インスタンス**」フィールドをクリックして、対応する「**アプリケーションインスタンス**」フィルターページを表示します。ここで、ログオフまたは切断するアプリケーションインスタンスを選択できます。

> **注：**
>
> カスタムスコープ管理者向けに、Directorはアプリケーショングループで作成されたアプリケーションインスタンスを表示しません。すべてのアプリケーションインスタンスを表示するには、フル管理者である必要があります。詳細については、Knowledge Centerの記事「CTX256001」を参照してください。

「**アプリケーション障害**」列と「**アプリケーションエラー**」列で、サイトで公開されているアプリケーションの正常性を監視します。これらの列には、過去1時間に該当するアプリケーションの起動中に発生した障害とエラーの集計数が表示されます。「**アプリケーション障害**」または「**アプリケーションエラー**」フィールドをクリックすると、選択したアプリケーションに対応する「**トレンド**」\>「**アプリケーション障害**」ページで障害の詳細を確認できます。

アプリケーション障害ポリシー設定は、障害とエラーの可用性と表示を管理します。ポリシーとそれらを変更する方法の詳細については、「**監視ポリシー**」設定の「アプリケーション障害監視のポリシー」を参照してください。

リアルタイムアプリケーション監視

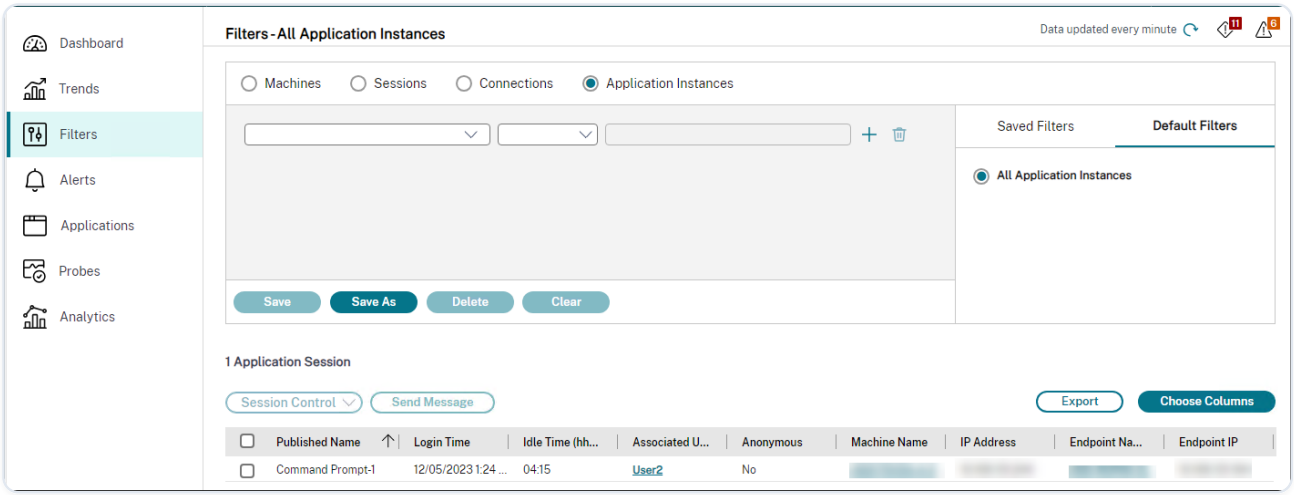
アイドル時間メトリックを使用して、特定の時間制限を超えてアイドル状態になっているインスタンスを特定することで、アプリケーションとセッションのトラブルシューティングを行うことができます。

アプリケーションベースのトラブルシューティングの典型的なユースケースは、従業員がアプリケーションライセンスを共有する医療分野にあります。そこでは、Citrix Virtual Apps and Desktops™環境をパージしたり、パフォーマンスの低いサーバーを再構成したり、アプリケーションを保守およびアップグレードしたりするために、アイドル状態のセッションとアプリケーションインスタンスを終了する必要があります。

アプリケーションインスタンスフィルターページには、サーバーおよびシングルセッションOSのVDA上のすべてのアプリケーションインスタンスが一覧表示されます。関連するアイドル時間測定値は、少なくとも10分間アイドル状態であったマルチセッションOSのVDA上のアプリケーションインスタンスに対して表示されます。

注： アプリケーションインスタンスのメトリックは、すべてのライセンスエディションのサイトで利用できます。

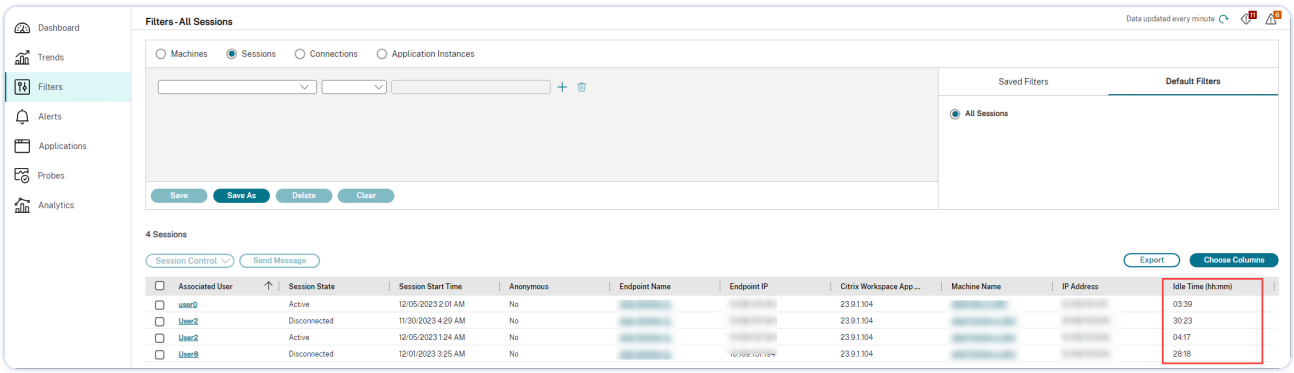
この情報を使用して、特定の期間を超えてアイドル状態になっているアプリケーションインスタンスを特定し、必要に応じてログオフまたは切断します。これを行うには、**フィルター** \> **アプリケーションインスタンス**を選択し、事前に保存されたフィルターを選択するか、**すべてのアプリケーションインスタンス**を選択して独自のフィルターを作成します。



フィルターの例は次のとおりです。**フィルター条件**として、**公開名**（アプリケーションの）と**アイドル時間**を選択します。次に、**アイドル時間**を特定の時間制限**以上**に設定し、再利用のためにフィルターを保存します。フィルターされたリストから、アプリケーションインスタンスを選択します。メッセージを送信するオプションを選択するか、**セッション制御**ドロップダウンから**ログオフ**または**切断**を選択してインスタンスを終了します。

> **注：** アプリケーションインスタンスをログオフまたは切断すると、現在のセッションがログオフまたは切断され、同じセッションに属するすべてのアプリケーションインスタンスが終了します。

セッションフィルターページから、セッションの状態とセッションアイドル時間メトリックを使用して、アイドル状態のセッションを特定できます。**アイドル時間**列で並べ替えるか、特定の時間制限を超えてアイドル状態になっているセッションを特定するためのフィルターを定義します。アイドル時間は、少なくとも10分間アイドル状態であったマルチセッションOSのVDA上のセッションに対して表示されます。



セッションまたはアプリケーションインスタンスが次の条件の場合、**アイドル時間**は**N/A**と表示されます。

- 10分以上アイドル状態になっていない場合、,
- シングルセッションOSのVDAで起動されている場合、または

- Version 7.12以前のVDAで起動されます。

アプリケーション障害の履歴監視

トレンド -\> **アプリケーション障害**タブには、VDA上の公開アプリケーションに関連する障害が表示されます。

アプリケーション障害の傾向は、PremiumおよびAdvancedライセンスサイトでは過去2時間、24時間、7日間、および1か月間利用できます。その他のライセンスタイプでは、過去2時間、24時間、および7日間利用できます。「Application Errors」をソースとしてイベントビューアにログ記録されたアプリケーション障害が監視されます。**エクスポート**をクリックすると、CSV、Excel、またはPDF形式でレポートを生成できます。

アプリケーション障害監視のグルーミング保持設定であるGroomApplicationErrorsRetentionDaysとGroomApplicationFaultsRetentionDaysは、Premiumおよび非Premiumライセンスサイトの両方で、デフォルトで1日に設定されています。この設定は、PowerShellコマンドを使用して変更できます。

```
Set-MonitorConfiguration -\<setting name\> \<value\>
```

アプリケーション障害の傾向(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/dir_application_faults.png)

障害は、その重大度に基づいて**アプリケーションフォールト**または**アプリケーションエラー**として表示されます。アプリケーションフォールトタブには、機能またはデータの損失に関連する障害が表示されます。アプリケーションエラーは、すぐには関連しない問題を示し、将来問題を引き起こす可能性のある状態を示します。

公開アプリケーション名、**プロセス名**、**デリバリーグループ**、および**期間**に基づいて障害をフィルタリングできます。テーブルには、フォールトまたはエラーコードと障害の簡単な説明が表示されます。詳細な障害の説明はツールチップとして表示されます。

> **注：** 対応するアプリケーション名を導出できない場合、公開されたアプリケーション名は「不明」と表示されます。これは通常、起動されたアプリケーションがデスクトップセッションで失敗した場合、または依存する実行可能ファイルによって処理されない例外が原因で失敗した場合に発生します。

> デフォルトでは、マルチセッションOS VDAでホストされているアプリケーションの障害のみが監視されます。監視グループポリシー（アプリケーション障害の監視を有効にする、シ

> ングルセッションOS VDAでのアプリケーション障害の監視を有効にする、障害監視から除外されるアプリケーションのリスト）を通じて監視設定を変更できます。詳細については、監視ポリシー設定のアプリケーション障害監視のポリシーを参照してください。

トレンド \> アプリケーションプローブ結果ページには、過去24時間および7日間にサイトで実行されたアプリケーションプローブの結果が表示されます。アプリケーションプローブの構成方法の詳細については、アプリケーションプローブを参照してください。

マシンのトラブルシューティング

> **注：**
>
> **Citrix Health Assistant** は、未登録のVDAにおける構成の問題をトラブルシューティングするためのツールです。このツールは、VDA登録の失敗、セッション起動の問題、タイムゾーンリダイレクト構成の問題の根本原因を特定するために、いくつかのヘルスチェックを自動化します。Knowledge Centerの記事「Citrix Health Assistant - Troubleshoot VDA Registration and Session Launch」には、**Citrix Health Assistant** ツールのダウンロードと使用方法が記載されています。

> Directorコンソールの **フィルター > マシン** ビューには、サイトで構成されているマシンが表示されます。「マルチセッションOSマシン」タブには、パフォーマンスカウンターの分布を示すロード評価インデックスと、リンクにカーソルを合わせるとセッション数のツールヒントが表示されます。

失敗したマシンの **失敗理由** 列をクリックすると、失敗の詳細な説明と、その失敗をトラブルシューティングするために推奨されるアクションが表示されます。マシンおよび接続の失敗の理由と推奨されるアクションは、「Citrix Director の失敗理由とトラブルシューティング」で確認できます。

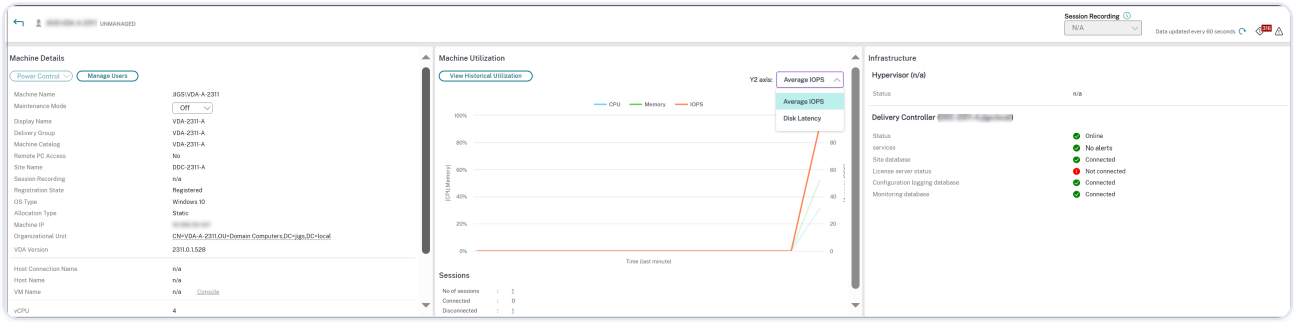
マシン名のリンクをクリックすると、**マシン詳細** ページに移動します。

マシン詳細ページには、マシンの詳細、インフラストラクチャの詳細、およびマシンに適用されたホットフィックスの詳細が一覧表示されます。

マシンベースのリアルタイムリソース使用率

マシン使用率パネルには、CPUとメモリのリアルタイム使用率を示すグラフが表示されます。さらに、Delivery ControllerとVDAのバージョンが**7.14**以降のサイトでは、ディスクおよびGPU監視グラフも利用できます。

ディスク監視グラフ、平均IOPS、およびディスク遅延は、VDAディスクに関連する問題を監視およびトラブルシューティングするのに役立つ重要なパフォーマンス測定値です。平均IOPSグラフは、ディスクへの読み取りおよび書き込みの平均数を表示します。**ディスク遅延**を選択すると、データ要求からディスクからの応答までの遅延（ミリ秒単位で測定）を示すグラフが表示されます。



GPU使用率

マルチセッションおよびシングルセッションOS VDAでのGPU関連の問題をトラブルシューティングするには、**GPU使用率**を選択して、GPU、GPUメモリ、エンコーダー、およびデコーダーの利用率（パーセンテージ）を確認します。

サポートされているGPUバージョン:

- ディスプレイドライバーバージョン369.17以降を実行しているNVIDIA Tesla M60 GPU。詳細については、「NVIDIA vGPU Software」を参照してください。
- AMD Radeon Instinct MI25 GPUおよびAMD EPYC 7V12(Rome) CPU。詳細については、「AMD Drivers and Support」を参照してください。

ドライバー:

適切なドライバーまたは拡張機能をVDAにインストールする必要があります。

- NVIDIA GPUの場合、GRIDドライバーを手動または拡張機能経由でインストールします。詳細については、NVIDIA vGPU Softwareを参照してください。
  - NVIDIAの場合、GRIDドライバーのみがサポートされています。CUDAドライバーはNVadsA10 v5シリーズでは動作せず、サポートされていません。
  - Azureベースのマシンに拡張機能経由でNvidia Grid GPUドライバーをインストールする手順の例については、NVIDIA GRID drivers. NVIDIA GPU Driver Extension - Azure Windows VMs - Azure Virtual Machinesを参照してください。
  - Nvidia Grid GPUドライバーを手動でインストールする手順の例については、Azure N-series NVIDIA GPU driver setup for Windows - Azure Virtual Machinesを参照してください。

- AMD GPUの場合、AMDグラフィックドライバーを手動または拡張機能経由でインストールします。詳細については、AMD Drivers and Supportを参照してください。
    - Azureベースのマシンに拡張機能経由でAMD GPUドライバーをインストールする手順の例については、AMD GPU Driver Extension - Azure Windows VMs - Azure Virtual Machinesを参照してください。
    - AzureマシンにAMD GPUドライバーを手動でインストールする手順の例については、Install AMD GPU drivers on N-series VMs running Windowsを参照してください。

使用上の注意:

- GPU使用率グラフは、64ビットWindowsを実行しているVDAでのみ利用可能です。
- GPUアクセラレーションを提供するには、VDAでHDX 3D Proが有効になっている必要があります。詳細については、GPU acceleration for Windows Single-session OSおよびGPU acceleration for Windows Multi-session OSを参照してください。
- VDAが複数のGPUにアクセスする場合、使用率グラフには個々のGPUから収集されたGPUメトリックの平均が表示されます。GPUメトリックはVDA全体に対して収集され、個々のプロセスに対しては収集されません。
- AMDの場合、エンコーダーとデコーダーの使用状況は個別にサポートされていません。GPUを使用するエンコード/デコードのワークロードは、GPU使用率における一般的な3D負荷として報告されます。
- インストール中にNVIDIA WMIをインストールしてください。このウィンドウは手動インストール時にのみ利用可能です。
- ドライバーがインストールされているのにDirectorがGPUを検出しない場合
    - タスクマネージャーを確認してください。ドライバーが適切にインストールされていれば、GPUはタスクマネージャーに表示されるはずです。
    - マシンが登録されているか確認してください。マシンがオンラインとして検出されるまでに時間がかかる場合があります。
- DirectorでGPU使用率にアクティビティが表示されない場合は、実行しているワークロードがGPUを使用していることを確認してください。グラフィックワークロードの場合、これは > > > > から有効にできます。「高パフォーマンス」をオンにしてください。場合によっては、他の設定に基づいて、これがシステムデフォルトまたは省電力に設定されていると、Windowsはグラフィックワークロードに CPUを使用するようデフォルトで設定されます。
- データは1分ごとに更新され、**GPU使用率**を選択してから1分以内にデータの視覚化が開始されます。

マシンベースの履歴リソース使用率

マシン使用率パネルで、**履歴使用率の表示**をクリックして、選択したマシンのリソースの履歴使用率を表示します。 使用率グラフには、CPU、メモリ、ピーク時の同時セッション、平均IOPS、ディスク遅延の重要なパフォーマンスカウンターが含まれます。

> **注：**
>
> 監視ポリシー設定の**プロセス監視を有効にする**は、履歴マシン使用率ページの「上位10プロセス」テーブルでデータを収集および表示するために、「許可」に設定する必要があります。収集はデフォルトで禁止されています。

> CPUとメモリの使用率、平均IOPS、ディスク遅延データはデフォルトで収集されます。「**Enable Resource Monitoring**」ポリシー設定を使用して、この収集を無効にできます。



1. **マシン詳細**ビューの**マシン使用率**パネルから、**履歴使用率の表示**を選択します。
2. **履歴マシン使用率**ページで、**期間**を「過去2時間」、「過去24時間」、「過去7日間」、「月」、「年」に設定して使用状況を表示します。

> **注：**
>
> 平均IOPSとディスク遅延の使用状況データは、現在までの過去24時間、月、年についてのみ利用可能です。カスタム終了時刻はサポートされていません。

3. **適用**をクリックし、必要なグラフを選択します。
4. グラフの異なるセクションにカーソルを合わせると、選択した期間の詳細情報が表示されます。



例えば、「**Last 2 hours**」を選択した場合、ベースライン期間は選択した時間範囲の前の2時間です。過去2時間とベースライン時間のCPU、メモリ、セッションの傾向を表示します。「**Last month**」を選択した場合、ベースライン期間は前月です。過去1か月とベースライン時間の平均IOPSとディスク遅延を表示するように選択します。

1. 選択した期間のリソース使用率データをエクスポートするには、「**Export**」をクリックします。詳細については、Monitor DeploymentsのExport reportsセクションを参照してください。
2. グラフの下の表には、CPUまたはメモリ使用率に基づいて上位10個のプロセスが一覧表示されます。選択した時間範囲におけるアプリケーション名、ユーザー名、セッションID、平均CPU、ピークCPU、平均メモリ、ピークメモリを表示する任意の列で並べ替えることができます。IOPSとディスク遅延の列は並べ替えることができません。

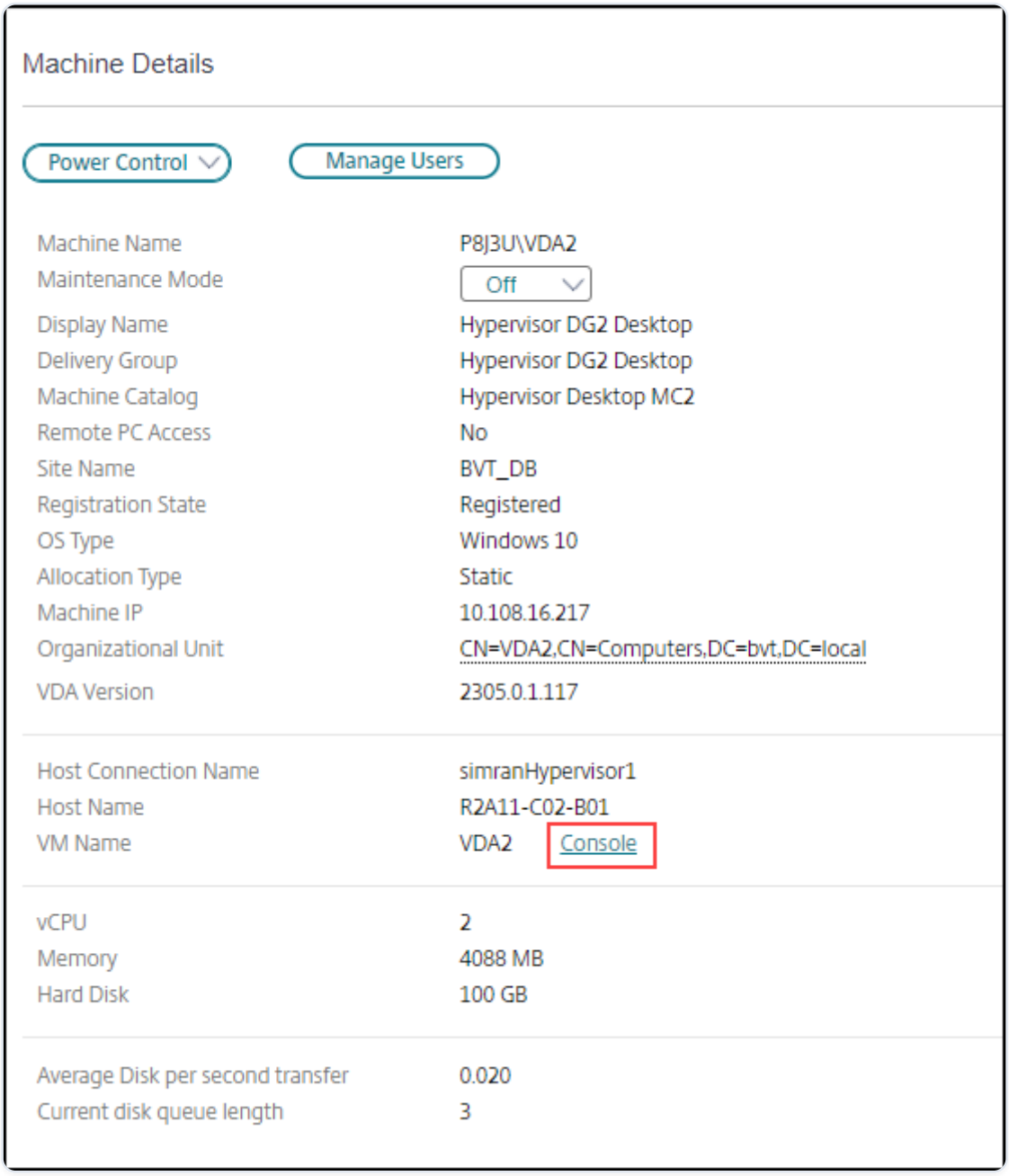
> **注：**
>
> システムプロセスのセッションIDは「0000」と表示されます。

3. 特定のプロセスのリソース消費の履歴傾向を表示するには、上位10個のプロセスのいずれかをドリルダウンします。

マシンコンソールへのアクセス

XenServerバージョン7.3以降でホストされているシングルセッションおよびマルチセッションOSマシンのコンソールには、Directorから直接アクセスできます。これにより、XenServerでホストされているVDAの問題をトラブルシューティングするためにXenCenterは必要ありません。この機能を利用するには：

- バージョン7.16以降のDelivery Controllerが必要です。
- マシンをホストしているXenServerはバージョン7.3以降である必要があり、Director UIからアクセスできる必要があります。



マシンのトラブルシューティングを行うには、対応するマシン詳細パネルの**コンソール**リンクをクリックします。提供されたホスト資格情報が認証されると、WebベースのVNCクライアントで

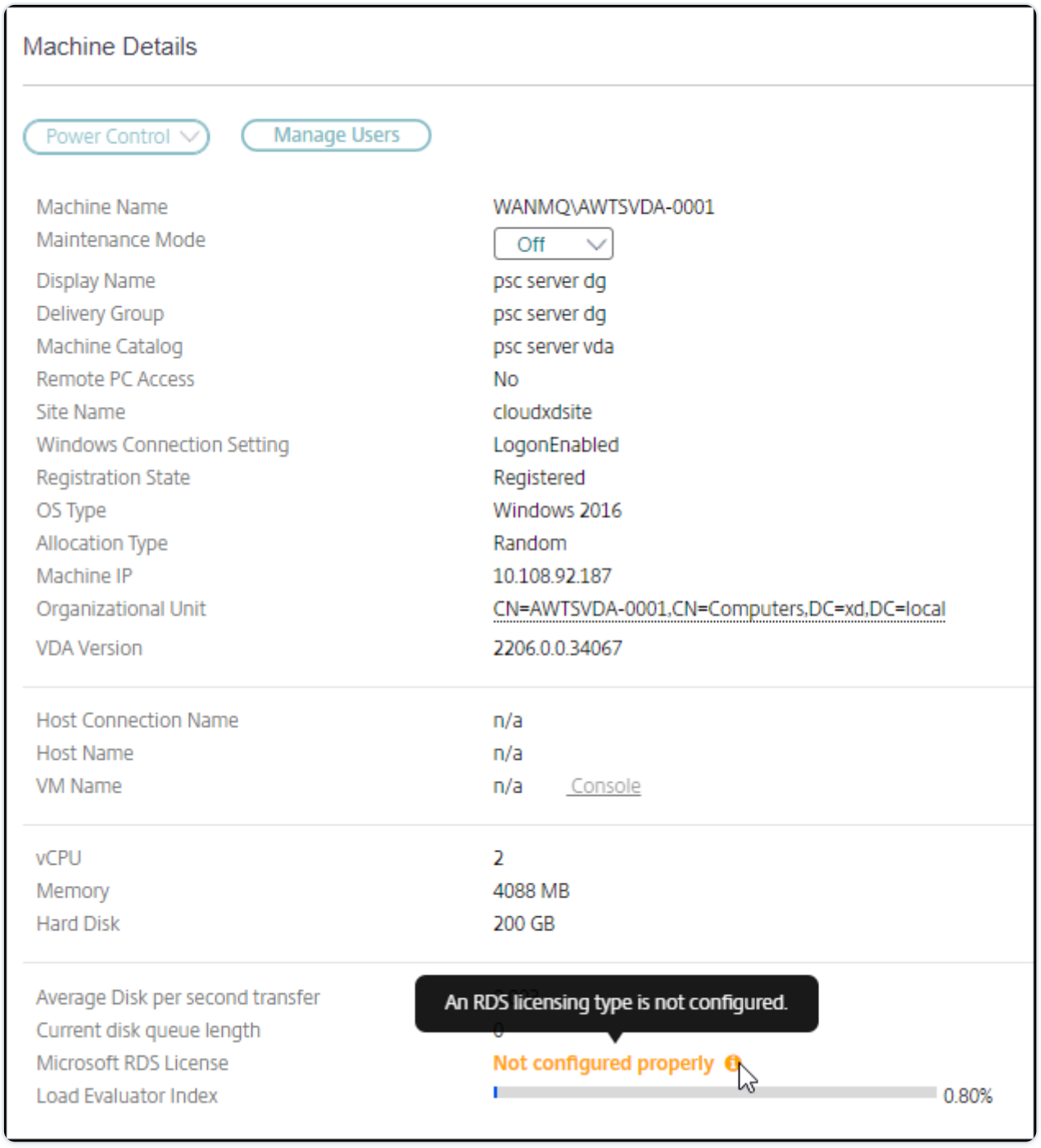
あるnoVNCを使用して、マシンコンソールが別のタブで開きます。これで、コンソールにキーボードとマウスでアクセスできるようになります。

注：

- この機能はInternet Explorer 11ではサポートされていません。
- マシンコンソールのマウスカーソルがずれている場合は、問題を解決する手順についてCTX230727を参照してください。
- Directorは新しいタブでコンソールアクセスを起動します。ブラウザの設定でポップアップが許可されていることを確認してください。
- セキュリティ上の理由から、Citrix®はブラウザにSSL証明書をインストールすることを推奨しています。

Microsoft RDSライセンスの健全性

マルチセッションOSマシンの「**Machine Details**」および「**User Details**」ページの「Machine Details」パネルで、Microsoft RDSライセンスのステータスを表示できます。



次のいずれかのメッセージが表示されます。

- ライセンス利用可能
- 適切に構成されていません（警告）
- ライセンスエラー（エラー）
- 互換性のないVDAバージョン（エラー）

> **注：**

有効なライセンスを持つ猶予期間中のマシンのMicrosoft RDSライセンスの健全性ステータスは、緑色で「**License available**」メッセージを表示します。ライセンスの有効期限が切れる前に更新してください。

警告メッセージとエラーメッセージについては、情報アイコンにカーソルを合わせると、次の表に示す追加情報が表示されます。

メッセージの種類	DIRECTOR内のメッセージ
エラー	VDAバージョン7.16以降で利用可能です。
エラー	新しいRDS接続は許可されていません。
エラー	Microsoft RDSライセンスの猶予期間が過ぎました。
エラー	必要なOSレベルに対して、デバイスごとのクライアントアクセスライセンスの種類でライセンスサーバーが構成されていません。
エラー	構成されているライセンスサーバーは、デバイスごとのクライアントアクセスライセンスの種類でRDSホストOSレベルと互換性がありません。
警告	Personal Terminal Serverは、Citrix Virtual Apps and Desktops™展開において有効なRDSライセンスの種類ではありません。
警告	管理用リモートデスクトップは、Citrix Virtual Apps and Desktops展開において有効なライセンスの種類ではありません。
警告	RDSライセンスの種類が構成されていません。
警告	ユーザーごとのクライアントアクセスRDSライセンスの種類では、ドメインコントローラーまたはライセンスサーバーに到達できません。

メッセージの種類	DIRECTOR内のメッセージ
警告	デバイスごとのクライアントアクセスライセンスの種類では、必要なOSレベルのライセンスサーバーに到達できないため、クライアントデバイスライセンスを判別できません。

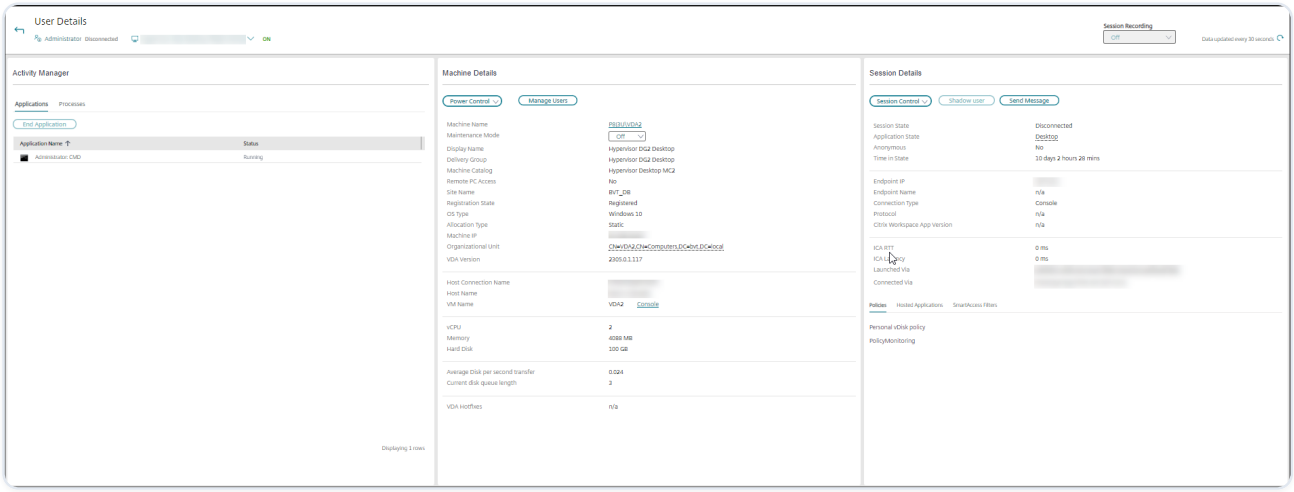
> **注：**
>
> この機能は、Microsoft RDS CAL (クライアントアクセスライセンス) にのみ適用されます。

ユーザーの問題のトラブルシューティング

Directorの**ヘルプデスク**ビュー（**アクティビティマネージャー**ページ）を使用して、ユーザーまたはセッションに関する情報を表示します。

ユーザーの詳細(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/dir-user-details-summary.png)

アクティビティマネージャーからユーザーに対して**詳細の表示**をクリックすると、**ユーザーの詳細**ページが開きます。 アクティビティマネージャーからエンドポイントに対して**詳細の表示**をクリックすると、**エンドポイントの詳細**ページが開きます。



セッションセレクター

ユーザーが複数のセッションを開始している場合、セッションセレクターはセッションの選択に役立ちます。

セッションセレクター(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/dir-session-selector.png)

詳細を表示するセッションを選択します。

- セッション、ユーザーのサインインエクスペリエンス、セッションの起動、接続、およびアプリケーションに関する詳細を確認します。
- ユーザーのマシンをシャドウできます。
- ICA®セッションを記録します。

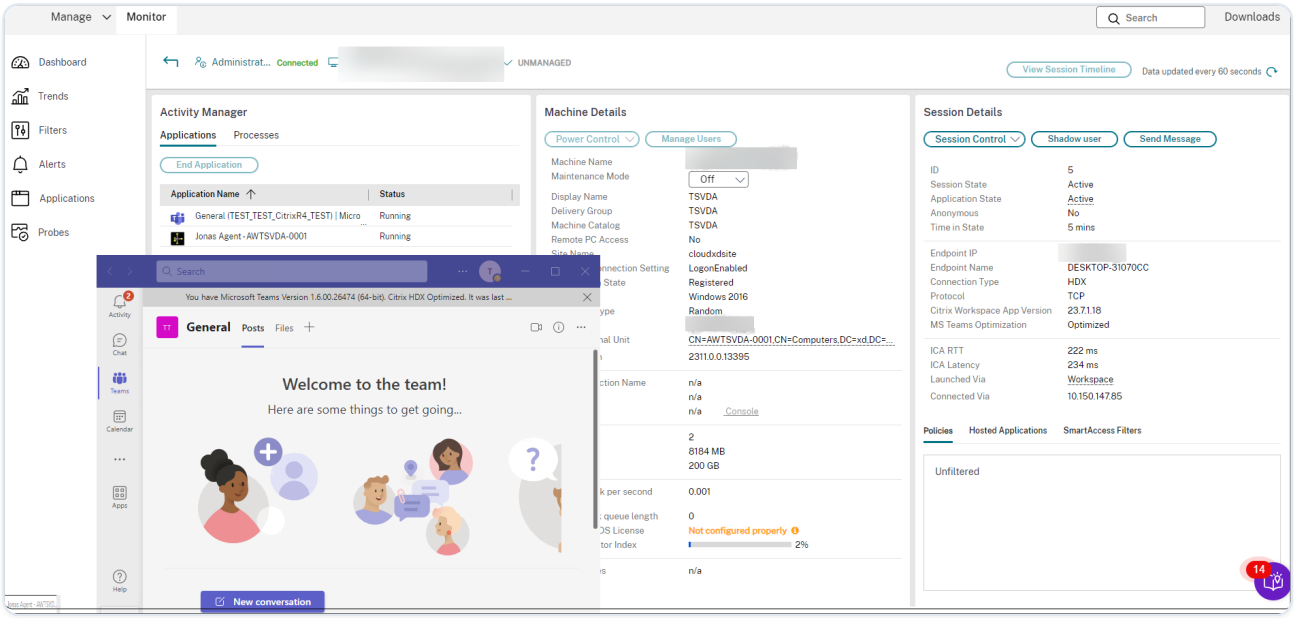
Microsoft Teamsの最適化ステータス

Directorは、HDX™セッションのMicrosoft Teamsの最適化ステータスを、**ユーザーの詳細**ページ > **セッションの詳細**パネル > **MS Teamsの最適化**フィールドに表示します。Microsoft Teamsが最適化されていることは、クリアなオーディオやビデオなど、より良いユーザーエクスペリエンスにとって重要です。Microsoft Teamsの最適化ステータスの可視性は、チケット解決にかかる時間を短縮し、トラブルシューティング中に管理者が重要なメトリックを特定するのに役立ちます。

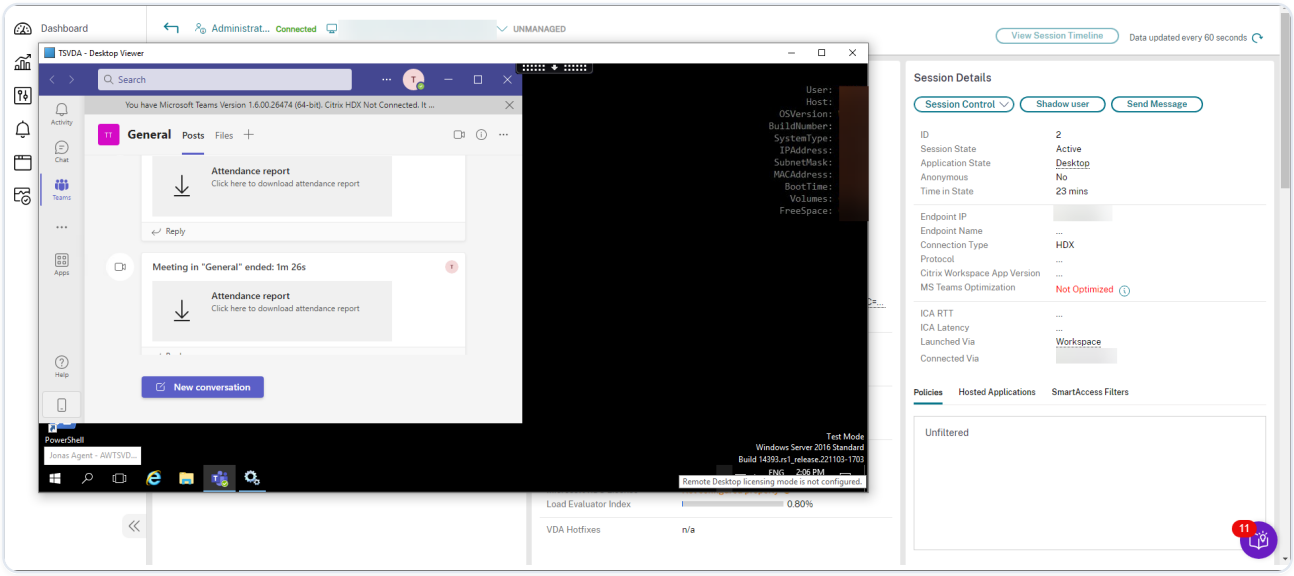
> **注：**
>
> Citrix Directorは、Microsoft Teamsバージョン2.1以前をサポートしています。

> 前提条件:

- VDAはバージョン2311以降を実行しています。
- Citrix Workspace app でサポートされているバージョンは、Microsoft Teams の最適化に記載されています。
- Microsoft Teams は、公開アプリケーションとして、または公開デスクトップ内で実行されます。
- Citrix HDX HTML5 Video Redirection Service などの重要なサービスが実行されています。



Microsoft Teams が最適化されていない場合、ツールヒントには、Microsoft Teams を最適化するためのヒントを含む、HDX からの外部トラブルシューティングライブ記事へのリンクが表示されます。HDX 最適化のトラブルシューティング。



トラブルシューティングのヒント

以下の表に記載されている推奨されるアクションで問題をトラブルシューティングし、必要に応じて適切な管理者に問題をエスカレートしてください。

ユーザーの問題	提案
ログオンに時間がかかる、または断続的または繰り返し失敗する	ユーザーログオンの問題を診断する

ユーザーの問題	提案
セッションの起動に時間がかかる、または断続的または繰り返し失敗する	セッション起動の問題を診断する
セッションの応答が遅い、または応答しない	セッションパフォーマンスの問題を診断する
アプリケーションが遅い、または応答しない	アプリケーション障害の解決
接続に失敗しました	デスクトップ接続の復元
セッションが遅い、または応答しない	セッションの復元
セッションを記録する	セッションの記録
ビデオが遅い、または品質が悪い	HDXチャネルシステムレポートの実行

注: マシンがメンテナンスモードになっていないことを確認するには、ユーザー詳細ビューからマシン詳細パネルを確認してください。

セッションログオン

ユーザー詳細ビュー > **セッションログオン**タブには、セッションログオンプロセスの包括的なビューが表示されます。このタブには、さまざまなログオンフェーズがプロットされたログオン期間フェーズチャートが含まれています。このデータを使用して、ユーザーログオンの問題をトラブルシューティングします。詳細については、ユーザーログオンの問題の診断を参照してください。

セッションパフォーマンス

セッションパフォーマンスタブには、ユーザーセッション内の問題を特定するためにリアルタイムメトリックを関連付ける機能から始まる、強化されたトラブルシューティングワークフローがあります。**セッショントポロジ**パネルは、接続されたHDXセッションのセッション内パスを視覚的に表現します。**パフォーマンスメトリック**パネルは、ICARTT、ICA遅延、1秒あたりのフレーム数、利用可能な出力帯域幅、消費された出力帯域幅などのセッションメトリックの傾向を提供し、これらのメトリックが時間の経過とともにどのようにパフォーマンスを発揮したかを示します。詳細については、セッションパフォーマンスの問題の診断を参照してください。

検索のヒント

検索フィールドにユーザー名を入力すると、Director は Director をサポートするように構成されているすべてのサイトのユーザーについて、Active Directory でユーザーを検索します。

検索フィールドにマルチユーザーマシンの名前を入力すると、Director は指定されたマシンのマシン詳細を表示します。

検索フィールドにエンドポイント名を入力すると、Director は特定のEndpointに接続されている認証されていない（匿名）セッションと認証済みセッションを使用します。この検索により、認証されていないセッションのトラブルシューティングが可能になります。認証されていないセッションのトラブルシューティングを可能にするには、エンドポイント名が一意であることを確認してください。

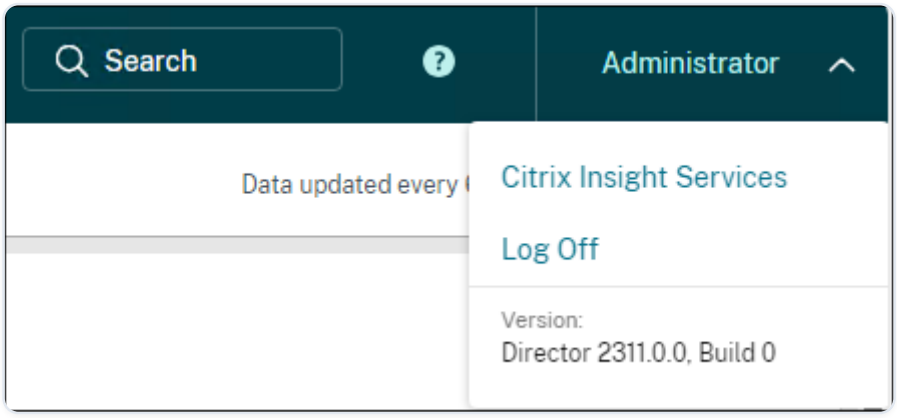
検索結果には、現在マシンを使用していない、またはマシンに割り当てられていないユーザーも含まれます。

- 検索では大文字と小文字は区別されません。
- 部分的な入力では、一致する可能性のあるリストが生成されます。
- スペースで区切られた2つの部分からなる名前の数文字を入力すると、両方の文字列に一致する結果が表示されます。2つの部分からなる名前の例としては、ユーザー名、姓と名、または表示名があります。たとえば、「jo rob」と入力すると、「John Robertson」や「Robert Jones」などの文字列が結果に含まれる場合があります。

ランディングページに戻るには、**Director ロゴ**をクリックします。

Citrix Insight Servicesへのアクセス

Director の ドロップダウンリストから Citrix Insight Services (CIS) にアクセスして、追加の診断情報を取得できます。CIS で利用できるデータは、Call Home や Citrix Scout などのソースから取得されます。



トラブルシューティング情報をCitrixテクニカルサポートにアップロードする

単一のDelivery Controller™またはVDAからCitrix Scoutを実行して、主要なデータポイントとCitrix Diagnostics Facility (CDF) トレースをキャプチャし、選択したコンピューターのトラブルシューティングを行います。Scoutは、データをCISプラットフォームに安全にアップロードして、Citrix

テクニカルサポートのトラブルシューティングを支援する機能を提供します。Citrixテクニカルサポートは CISプラットフォームを使用して、顧客から報告された問題の解決時間を短縮します。

ScoutはCitrix Virtual Apps and Desktops™コンポーネントとともにインストールされます。Windowsのバージョンに応じて、Citrix Virtual Apps and Desktopsをインストールまたはアップグレードすると、Scoutは**Windowsのスタート**メニューまたはスタート画面に表示されます。

Scoutを起動するには、スタートメニューまたはスタート画面から **\>** を選択します。

Scoutの使用方法と構成、およびFAQについては、CTX130147を参照してください。

セッション起動の問題を診断する

ユーザーログオンの問題の診断セクションで述べられているログオンプロセスフェーズに加えて、Directorはセッション起動時間を表示します。これは、**ユーザーの詳細**ページと**マシンの詳細**ページで、Workspace Appセッション起動時間とVDAセッション起動時間に分けられます。これらの2つの期間は、さらに個々のフェーズを含み、その起動時間も表示されます。このデータは、セッション起動時間の長さの原因を理解し、トラブルシューティングするのに役立ちます。さらに、セッション起動に関わる各フェーズの期間は、個々のフェーズに関連する問題のトラブルシューティングに役立ちます。たとえば、ドライブマッピングの時間が長い場合、GPOまたはスクリプトですべての有効なドライブが正しくマッピングされているか確認できます。この機能は、Delivery Controllerバージョン7 1906以降およびVDA 1903以降で利用可能です。

前提条件

セッション起動時間のデータが表示されるには、以下の前提条件が満たされていることを確認してください。

- デリバリーコントローラー™ 7 1906 以降。
- VDA 1903以降。
- Citrix End User Experience Monitoring (EUEM)サービスがVDAで実行されている必要があります。

制限事項

Directorがセッション起動時間のデータを表示する際には、以下の制限が適用されます。

- セッション起動時間は、HDX™セッションでのみ利用可能です。
- iOSおよびAndroid OSからのセッション起動の場合、VDA起動時間のみが利用可能です。
- ICA®ファイルダウンロード時間 (IFDCD) は、ブラウザから起動する際にWorkspace Appが検出された場合にのみ利用可能です。

- Mac OSからのセッション起動の場合、IFDCDはWorkspace App 1902以降でのみ利用可能です。
- Windows OSからのセッション起動の場合、IFDCDはWorkspace app 1902以降で利用可能です。それ以前のバージョンでは、IFDCDはブラウザからWorkspace appが検出されたアプリ起動の場合にのみ表示されます。

注:

- 前提条件が満たされた後もセッション起動時間の表示に問題がある場合は、CTX130320に記載されているDirectorサーバーおよびVDAログを確認してください。 共有セッション（同じセッションで複数のアプリケーションが起動された場合）の場合、Workspace Appの起動メトリックは、最新の接続または最新のアプリケーション起動に対して表示されます。
- VDAセッション起動の一部のメトリックは、再接続時には適用されません。そのような場合、メッセージが表示されます。

セッション起動(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/session_startup.png)

Workspace App セッション起動フェーズ

セッション起動クライアント期間 (SSCD)

このメトリックが高い場合、起動時間が長くなるクライアント側の問題を示しています。問題の根本原因を特定するために、後続のメトリックを確認してください。SSCD は、要求 (マウスクリック) の時刻にできるだけ近い時点から開始されます。クライアントデバイスと VDA 間の ICA 接続が確立されたときに終了します。共有セッションの場合、サーバーへの新しい接続の作成に関連するセットアップコストの多くが発生しないため、この期間ははるかに短くなります。次のレベルでは、いくつかの詳細なメトリックが利用可能です。

ICA ファイルダウンロード期間

これは、クライアントがサーバーから ICA ファイルをダウンロードするのにかかる時間です。全体的なプロセスは次のとおりです。

1. ユーザーは Workspace Application でリソース (アプリケーションまたはデスクトップ) をクリックします。
2. ユーザーからの要求は、Citrix Gateway (構成されている場合) を介して StoreFront™ に送信され、StoreFront™ はその要求を Delivery Controller に送信します。

3. Delivery Controller は要求に利用可能なマシンを見つけ、マシン情報とその他の詳細を StoreFront に送信します。また、StoreFront は Secure Ticket Authority からワンタイムチケットを要求し、受け取ります。
4. StoreFront は ICA ファイルを生成し、Citrix Gateway (構成されている場合) を介してユーザーに送信します。

IFDCD は、完全なプロセス (ステップ 1〜4) にかかる時間を表します。IFDCD 期間は、クライアントが ICA ファイルを受信したときにカウントを停止します。

LPWD は、プロセスの StoreFront コンポーネントです。

IFDCD が高い (ただし LPWD が正常である) 場合、起動のサーバー側処理は成功しましたが、クライアントデバイスと StoreFront の間に通信の問題がありました。これは、2つのマシン間のネットワークの問題に起因します。したがって、まず潜在的なネットワークの問題をトラブルシューティングできます。

起動ページ WEB サーバー期間 (LPWD)

これは、StoreFront で起動ページ (launch.aspx) を処理するのにかかる時間です。LPWD が高い場合、StoreFront にボトルネックがある可能性があります。

考えられる原因は次のとおりです。

- StoreFrontの負荷が高い。Internet Information Services (IIS) のログや監視ツール、タスクマネージャー、パフォーマンスモニターなどを確認して、遅延の原因を特定してください。
- StoreFrontがDelivery Controllerなどの他のコンポーネントとの通信に問題がある。StoreFrontとDelivery Controller間のネットワーク接続が遅いか、一部のDelivery Controllerがダウンしているか、過負荷になっていないかを確認してください。

名前解決WEBサーバー期間 (NRWD)

これは、Delivery Controllerが公開アプリケーション/デスクトップの名前をVDAマシンのIPアドレスに解決するのにかかる時間です。

このメトリックが高い場合、Delivery Controllerが公開アプリケーションの名前をIPアドレスに解決するのに時間がかかっていることを示します。

可能性のある原因としては、クライアント側の問題、Delivery Controllerの過負荷などのDelivery Controllerの問題、またはそれらの間のネットワークリンクの問題が挙げられます。

チケット応答WEBサーバー期間 (TRWD)

この期間は、Secure Ticket Authority (STA) サーバーまたはDelivery Controllerからチケットを取得するのにかかる時間を示します（必要な場合）。この期間が長い場合、STAサーバーまたはDelivery Controllerが過負荷になっていることを示します。

セッション検索クライアント期間 (SLCD)

この期間は、要求された公開アプリケーションをホストするためにすべてのセッションを照会するのにかかる時間を表します。既存のセッションがアプリケーション起動要求を処理できるかどうかを判断するために、クライアントでチェックが実行されます。使用される方法は、セッションが新規か共有かによって異なります。

セッション作成クライアント期間 (SCCD)

この期間は、wfica32.exe（または同様の同等ファイル）が起動されてから接続が確立されるまでの、セッション作成にかかる時間を表します。

VDAセッション起動フェーズ

セッション起動VDA期間 (SSVD)

この期間は、VDAが起動操作全体を実行するのにかかる時間を含む、高レベルのサーバー側接続起動メトリックです。このメトリックが高い場合、セッション起動時間を増加させるVDAの問題があることを示します。これには、VDAで起動操作全体を実行するのに費やされた時間が含まれます。

資格情報取得VDA期間 (COVD)

VDAがユーザー資格情報を取得するのにかかる時間。

ユーザーが時間内に資格情報を提供できない場合、この期間は人為的に増加する可能性があります。そのため、VDA起動期間には含まれません。この時間は、手動ログインが使用され、サーバー側の資格情報ダイアログが表示される場合（またはログイン開始前に法的通知が表示される場合）にのみ重要となる可能性があります。

資格情報認証VDA期間 (CAVD)

これは、VDAが認証プロバイダーに対してユーザーの資格情報を認証するのにかかる時間です。認証プロバイダーは、Kerberos、Active Directory、またはセキュリティサポートプロバイダーインターフェイス (SSPI) のいずれかです。

グループポリシーVDA期間 (GPVD)

この期間は、ログオン中にグループポリシーオブジェクトを適用するのにかかる時間です。

ログオンスクリプト実行VDA期間 (LSVD)

これは、VDAがユーザーのログオンスクリプトを実行するのにかかる時間です。

ユーザーまたはグループのログオンスクリプトを非同期にすることを検討してください。アプリケーション互換性スクリプトを最適化するか、代わりに環境変数を使用することを検討してください。

プロファイルロードVDA期間 (PLVD)

これは、VDAがユーザープロファイルをロードするのにかかる時間です。

この期間が長い場合は、ユーザープロファイル構成を検討してください。ローミングプロファイルのサイズと場所は、セッションの起動が遅くなる原因となります。ユーザーがターミナルサービスローミングプロファイルとホームフォルダーが有効になっているセッションにログオンすると、ローミングプロファイルの内容と当該フォルダーへのアクセスがログオン中にマッピングされます。これには追加のリソースが必要です。場合によっては、CPU使用率を大幅に消費することがあります。この問題を軽減するために、リダイレクトされた個人フォルダーとともに**ターミナルサービスホーム**フォルダーを使用することを検討してください。一般に、Citrix環境でユーザープロファイルを管理するには、Citrix Profile Managementの使用を検討してください。Citrix Profile Managementを使用しており、ログオン時間が遅い場合は、アンチウイルスソフトウェアがCitrix Profile Managementツールをブロックしていないか確認してください。

プリンター作成VDA期間 (PCVD)

これは、VDAがユーザーのクライアントプリンターを同期的にマッピングするのにかかる時間です。プリンター作成が非同期で実行されるように構成されている場合、セッション起動の完了に影響しないため、PCVDの値は記録されません。

プリンターのマッピングに過剰な時間が費やされるのは、多くの場合、プリンターの自動作成ポリシー設定が原因です。ユーザーのクライアントデバイスにローカルで追加されたプリンターの数と、印刷構成がセッションの開始時間に直接影響を与える可能性があります。セッションが開始されると、Citrix Virtual Apps and Desktops™ は、クライアントデバイス上のローカルにマップされたすべてのプリンターを作成する必要があります。特にユーザーが多数のローカルプリンターを持っている場合は、作成されるプリンターの数を減らすために、印刷ポリシーを再構成することを検討してください。これを行うには、Delivery Controller および Citrix Virtual Apps and Desktops でプリンターの自動作成ポリシーを編集します。

ドライブマッピングVDA期間 (DMVD)

これは、VDAがユーザーのクライアントドライブ、デバイス、ポートをマッピングするのにかかる時間です。

ICAプロトコルを最適化し、セッション全体のパフォーマンスを向上させるために、ベースポリシーに未使用の仮想チャネル（オーディオやCOMポートのマッピングなど）を無効にする設定が含まれていることを確認してください。

アプリケーション/デスクトップ起動VDA期間 (ALVD/DLVD)

このフェーズは、UserinitとShellの期間の組み合わせです。ユーザーがWindowsマシンにログオンすると、winlogonがuserinit.exeを実行します。Userinit.exeはログオンスクリプトを実行し、ネットワーク接続を再確立してからExplorer.exeを開始します。Userinitは、userinit.exeの開始から仮想デスクトップまたはアプリケーションのユーザーインターフェイスの開始までの期間を表します。Shell期間は、ユーザーインターフェイスの初期化からユーザーがキーボードとマウスの制御を受け取るまでの時間です。

セッション作成VDA期間 (SCVD)

この時間には、VDAでのセッション作成時間におけるその他の遅延が含まれます。

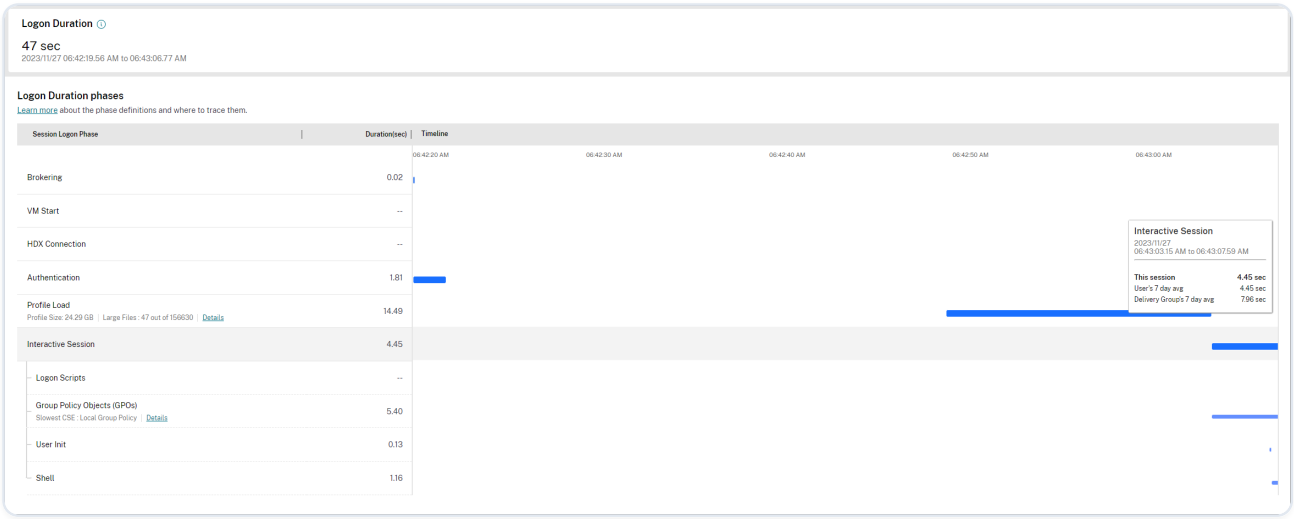
ユーザーログオンの問題を診断する

「**ユーザー詳細**」ビュー > 「**セッションログオン**」タブには、セッションログオンプロセスの包括的なビューが表示されます。このデータを使用して、ユーザーログオンの問題をトラブルシューティングします。

ログオン期間は、HDX を使用したデスクトップまたはアプリへの初回接続の場合にのみ測定されます。このデータには、リモートデスクトッププロトコルで接続しようとしているユーザーや、切断されたセッションから再接続しているユーザーは含まれません。具体的には、ユーザーが最初に非 HDX プロトコルを使用して接続し、HDX を使用して再接続する場合、ログオン期間は測定されません。

ユーザーがCitrix Virtual Apps and Desktops™にログオンすると、Monitor Serviceはログオンプロセスのフェーズを追跡します。フェーズは、ユーザーがCitrix Workspace™アプリから接続した時点から、アプリまたはデスクトップが使用可能になるまでの時間で始まります。

「**セッションログオン**」タブには、さまざまなログオンフェーズがプロットされたログオン時間フェーズチャートが含まれています。ログオン時間は、接続を確立し、Delivery Controller™からアプリまたはデスクトップを取得するのに費やされた時間と、仮想アプリまたはデスクトップに認証してログオンするのに費やされた時間を表します。時間の情報は秒（または秒の端数）で表示されます。



ログオン期間フェーズチャートは、さまざまなログオンフェーズとその開始時刻および終了時刻を明確に表示します。このチャートは、個々のログオンフェーズの重複を示します。合計ログオン時間は、個々のログオンフェーズの期間の合計ではない場合があります。これは、個々のフェーズが重複する可能性があり、すべてのログオンフェーズがこの表現の一部ではないためです。また、特定のフェーズは、ユーザーが仮想アプリまたはデスクトップとの対話を開始した後も延長される可能性があり、この期間は全体のログオン期間の一部として測定されません。

このビューを使用して、セッション起動の遅延を引き起こしている特定のログオンフェーズを特定します。各ログオンフェーズの定義と、情報を追跡できるイベントソースは、さらなるトラブルシューティングに役立ちます。チャートにカーソルを合わせると、現在のセッションのフェーズ期間、ユーザーの7日間平均、およびデリバリーグループの7日間平均を含むツールチップが表示されます。この情報は、現在のセッションログオン期間を7日間平均値と比較するのに役立ちます。GPOおよびプロファイルの詳細の場合、サブフェーズ測定にさらにドリルダウンできます。この視覚化は、ログオン期間関連の問題を簡単に理解し、トラブルシューティングするのに役立ちます。

前提条件

ログオン期間データとドリルダウンが表示されるように、次の前提条件が満たされていることを確認してください。

1. VDA に **Citrix User Profile Manager** と **Citrix User Profile Manager WMI Plugin** をインストールします。
2. Citrix Profile Management Service が実行されていることを確認します。
3. XenApp および XenDesktop サイト 7.15 以前の場合、GPO 設定 **レガシー実行リストを処理しない** を無効にします。
4. 対話型セッションのドリルダウンには、監査プロセス追跡を有効にする必要があります。
5. GPO ドリルダウンの場合、グループポリシーの運用ログのサイズを増やします。

注:

- ログオン時間は、デフォルトのWindowsシェル (explorer.exe) でのみサポートされ、カスタムシェルではサポートされません。
- Remote PC Accessのログオン時間は、Remote PC Accessのインストール中に**Citrix User Profile Manager**と**Citrix User Profile Manager WMI Plugin**が追加コンポーネントとしてインストールされている場合にのみ利用可能です。詳細については、「Remote PC Accessの構成とシーケンスに関する考慮事項」のステップ4を参照してください。

ユーザーログオンの問題をトラブルシューティングする手順

1. 「**ユーザー詳細**」ビュー > 「**セッションログオン**」タブから、ログオン時間チャートを使用してログオン状態をトラブルシューティングします。
   - ユーザーがログオン中の場合、ビューにはログオンのプロセスが反映されます。
   - ユーザーがログオンしている場合、ログオン時間パネルには、ユーザーが現在のセッションにログオンするまでにかかった時間が表示されます。
2. ログオンプロセスのフェーズを検査します。

ログオンプロセスのフェーズ

ブローカリング

ユーザーに割り当てるデスクトップを決定するまでにかかった時間。

VM起動

セッションがマシンの起動を必要とする場合、VM起動は仮想マシンの起動にかかる時間です。

HDX接続

クライアントから仮想マシンへのHDX接続の設定に必要な手順を完了するのにかかった時間。

認証

リモートセッションへの認証を完了するのにかかった時間。

GPO

仮想マシンでグループポリシー設定が有効になっている場合、これはログオン中にグループポリシーオブジェクトを適用するのにかかる時間です。CSE（クライアント側拡張）ごとの各ポリシーの適用にかかる時間のドリルダウンは、GPOバーにカーソルを合わせるとツールチップとして表示されます。



詳細をクリックすると、ポリシーの状態と対応するGPO名を含むテーブルが表示されます。ドリルダウンの時間期間はCSE処理時間のみを表し、合計GPO時間には加算されません。ドリルダウンテーブルをコピーして、さらなるトラブルシューティングやレポートでの使用に役立てることができます。ポリシーのGPO時間は、イベントビューアログから取得されます。ログは、運用ログに割り当てられたメモリ（デフォルトサイズは4 MB））に応じて上書きされる可能性があります。運用ログのログサイズを増やす方法の詳細については、Microsoft TechNetの記事「イベントログの構成」を参照してください。

ログオンスクリプト

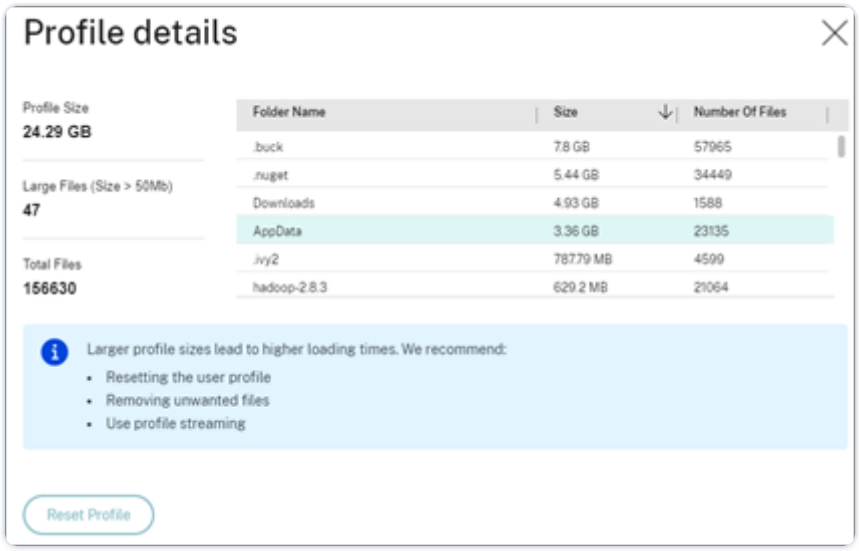
セッションにログオンスクリプトが構成されている場合、これはログオンスクリプトの実行にかかる時間です。

プロファイル読み込み

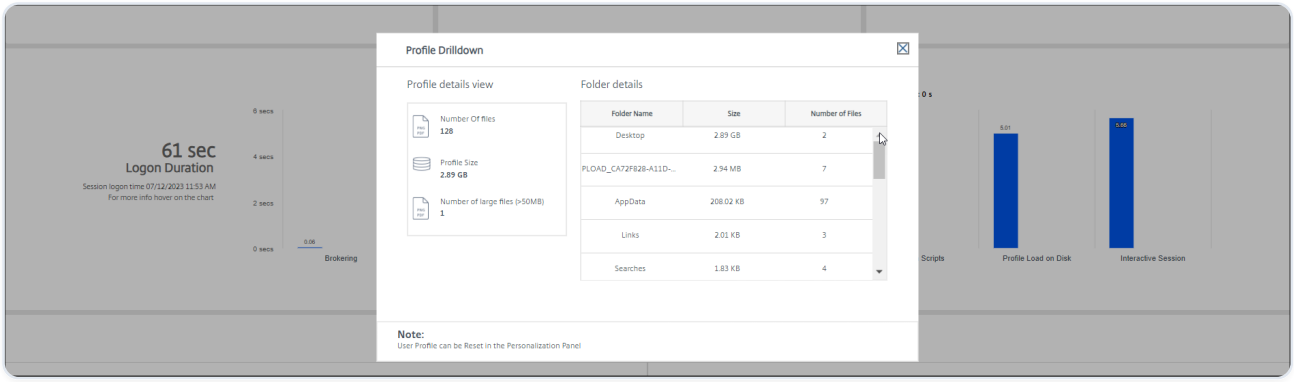
ユーザーまたは仮想マシンにプロファイル設定が構成されている場合、これはプロファイルの読み込みにかかる時間です。

Citrix Profile Managementが構成されている場合、プロファイルロードバーには、Citrix Profile Managementがユーザープロファイルを処理するのにかかった時間が含まれます。この情報は、管理者がプロファイル処理時間の長さの問題をトラブルシューティングするのに役立ちます。Profile Managementが構成されている場合、プロファイルロードバーには増加した期間が表示されます。この増加は、この機能強化によって引き起こされるものであり、パフォーマンスの低下を反映するものではありません。この機能強化は、VDA 1903以降で利用可能です。

プロファイルロードバーにカーソルを合わせると、現在のセッションのユーザープロファイルの詳細を示すツールチップが表示されます。



「**詳細**」をクリックして、プロファイルルートフォルダー（例：C:/Users/username）内の個々のフォルダー、そのサイズ、およびファイル数（ネストされたフォルダー内のファイルを含む）をさらにドリルダウンします。



プロファイルのドリルダウンは、Delivery Controllerバージョン7 1811以降およびVDA 1811以降で利用できます。プロファイルのドリルダウン情報を使用して、高いプロファイルロード時間に関連する問題を解決できます。次のことができます。

- ユーザープロファイルをリセットする
- 不要な大きなファイルを削除してプロファイルを最適化する
- ネットワーク負荷を軽減するためにファイル数を減らす
- プロファイルストリーミングを使用する

デフォルトでは、プロファイルルート内のすべてのフォルダーがドリルダウンに表示されます。フォルダーの表示を非表示にするには、VDAマシンで次のレジストリ値を編集します。

> **警告:**

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

1. VDAで、HKEY_LOCAL_MACHINE\Software\Citrix\Director\ に新しいレジストリ値 **ProfileFoldersNameHidden** を追加します。
2. 値を1に設定します。この値はDWORD（32ビット）値である必要があります。これでフォルダー名の表示が無効になります。
3. フォルダー名を再度表示するには、値を0に設定します。

> **注：** 複数のマシンにレジストリ値の変更を適用するには、GPOまたはPowerShellコマンドを使用できます。GPOを使用してレジストリ変更を展開する方法の詳細については、ブログを参照してください。

追加情報

- プロファイルのドリルダウンでは、リダイレクトされたフォルダーは考慮されません。
- ルートフォルダー内のNTUser.datファイルは、エンドユーザーには表示されない場合があります。ただし、これらはプロファイルのドリルダウンに含まれ、**ルートフォルダー**のファイルリストに表示されます。
- AppDataフォルダー内の一部の隠しファイルは、プロファイルのドリルダウンに含まれません。
- ファイル数とプロファイルサイズデータは、特定のWindowsの制限により、パーソナライゼーションパネルのデータと一致しない場合があります。

対話型セッション

インタラクティブセッションとは、ユーザープロファイルがロードされた後、キーボードとマウスの制御をユーザーに「引き渡す」のにかかる時間です。これは通常、ログオンプロセスのすべてのフェーズの中で最も長い期間であり、**インタラクティブセッション期間 = デスクトップ準備完了イベントタイムスタンプ (VDA上のEventId 1000) - ユーザープロファイルロード済みイベントタイムスタンプ (VDA上のEventId 2)** として計算されます。インタラクティブセッションには、Pre-userinit、Userinit、Shellの3つのサブフェーズがあります。インタラクティブセッションにカーソルを合わせると、次のツールチップが表示されます。

- サブフェーズ

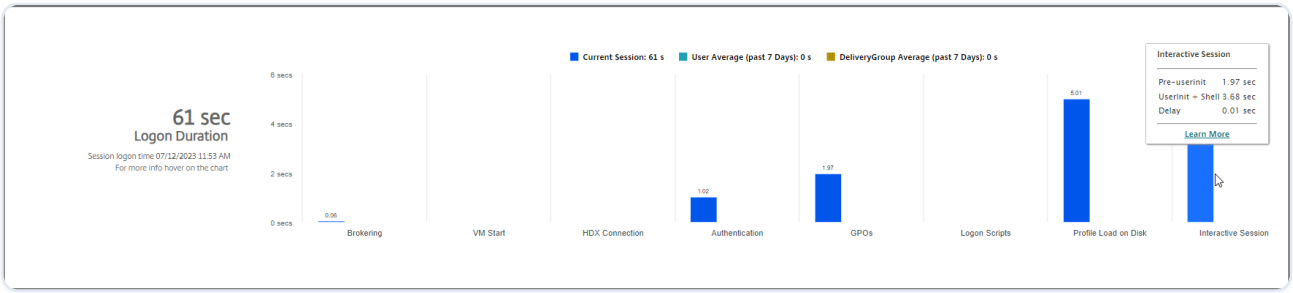
- 各サブフェーズにかかる時間
- これらのサブフェーズ間の累積合計時間遅延

> **注：**
>
> この機能はVDA 1811以降で利用できます。7.18より前のサイトでセッションを起動し、その後7.18以降にアップグレードした場合、「サーバーエラーのためドリルダウンが利用できません」というメッセージが表示されます。ただし、アップグレード後にセッションを起動した場合は、エラーメッセージは表示されません。

各サブフェーズの期間を表示するには、VM (VDA) で監査プロセス追跡を有効にします。監査プロセス追跡が無効になっている場合 (デフォルト)、Pre-userinitの期間と、UserinitおよびShellの合計期間が表示されます。グループポリシーオブジェクト (GPO) を使用して監査プロセス追跡を有効にするには、次の手順を実行します。

1. GPOを作成し、GPOエディターを使用して編集します。
2. **コンピューターの構成 > Windows の設定 > セキュリティの設定 > ローカル ポリシー > 監査ポリシー**に移動します。
3. 右側のペインで、**監査プロセス追跡**をダブルクリックします。
4. **成功**を選択し、OKをクリックします。
5. このGPOを必要なVDAまたはグループに適用します。

監査プロセス追跡とその有効化または無効化の詳細については、Microsoftドキュメントの監査プロセス追跡を参照してください。



ユーザー詳細ビューのログオン期間パネル。

- **インタラクティブセッション – Pre-userinit:** グループポリシーオブジェクトとスクリプトと重複するインタラクティブセッションのセグメント。このサブフェーズは、GPOとスクリプトを最適化することで短縮できます。

- **インタラクティブセッション – Userinit:** ユーザーがWindowsマシンにログオンすると、Winlogonはuserinit.exeを実行します。Userinit.exeはログオンスクリプトを実行し、ネットワーク接続を再確立してから、Windowsユーザーインターフェイスであるexplorer.exeを起動します。インタラクティブセッションのこのサブフェーズは、Userinit.exeの開始から仮想デスクトップまたはアプリケーションのユーザーインターフェイスの開始までの期間を表します。
- **インタラクティブセッション – Shell:** 前のフェーズで、UserinitはWindowsユーザーインターフェイスの初期化を開始します。Shellサブフェーズは、ユーザーインターフェイスの初期化からユーザーがキーボードとマウスの制御を受け取るまでの期間を捕捉します。
- **遅延:** これは、**Pre-userinitとUserinit**サブフェーズ間、および**Userinitとシェル**サブフェーズ間の累積時間遅延です。

合計ログオン時間は、これらのフェーズの正確な合計ではありません。たとえば、一部のフェーズは並行して発生し、一部のフェーズでは、合計よりも長いログオン期間につながるより多くの処理が発生します。 合計ログオン時間には、ICAファイルのダウンロードとアプリケーションのICAファイル起動の間の時間であるICA®アイドル時間は含まれません。 アプリケーション起動時にICAファイルを自動的に開くには、ICAファイルのダウンロード時にブラウザがICAファイルを自動的に起動するように設定します。詳細については、CTX804493を参照してください。

> **注：** ログオン期間グラフは、ログオンフェーズを秒単位で表示します。1秒未満の期間値は、サブ秒値として表示されます。1秒を超える値は、最も近い0.5秒に丸められます。グラフは、Y軸の最大値が200秒として表示されるように設計されています。200秒を超える値は、バーの上に実際の値が表示されます。

トラブルシューティングのヒント

グラフ内の異常な値や予期しない値を特定するには、現在のセッションの各フェーズにかかった時間と、このユーザーの過去7日間の平均所要時間、およびこのデリバリーグループ内のすべてのユーザーの過去7日間の平均所要時間を比較します。

必要に応じてエスカレートします。たとえば、VMの起動が遅い場合、問題はハイパーバイザーにある可能性があるため、ハイパーバイザー管理者にエスカレートできます。または、ブローカリング時間が遅い場合は、サイト管理者に問題をエスカレートして、Delivery Controllerの負荷分散を確認できます。

以下を含む異常な相違点を調べます。

- 欠落している（現在の）ログオンバー
- 現在の所要時間とこのユーザーの平均所要時間の間の大きな不一致。原因は次のとおりです。

    - 新しいアプリケーションがインストールされた。
    - オペレーティングシステムのアップデートが行われた。
    - 構成変更が行われた。
    - ユーザーのプロファイルサイズが大きい。この場合、プロファイルロードが高い。
- ユーザーのログオン数値（現在の期間と平均期間）とデリバリーグループの平均期間との間に大きな不一致がある場合。

必要に応じて、**再起動**をクリックしてユーザーのログオンプロセスを監視し、VM起動やブローカリングなどの問題をトラブルシューティングします。

セッションパフォーマンスの問題を診断する

「ユーザー詳細ページ」の「**セッションパフォーマンス**」タブには、HDX™ユーザーセッション内の問題を特定するのに役立つ、強化されたトラブルシューティングワークフローが用意されています。「セッショントポロジ」および「パフォーマンスメトリック」パネルは、セッションのコンポーネントビューと複数のパフォーマンスメトリックを単一のビューで関連付け、セッションエクスペリエンスの問題解決にかかる平均時間を短縮します。

セッションパフォーマンスビュー(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/dir-session-performance.png)

エンドツーエンドのネットワークホップビュー

エンドツーエンドのネットワークホップビューは、トラブルシューティングワークフローを強化するための次のステップです。「**ユーザー詳細**」>「**セッションパフォーマンス**」>「**セッショントポロジ**」セクションでは、接続されたHDXセッションのエンドツーエンドのネットワークホップビューを視覚的に表現します。

接続されたセッションのセッショントポロジには、セッションパスに関与するコンポーネントとそのメタデータ、コンポーネント間のリンク、およびVDAで公開されているアプリケーションが表示されます。 さらに、セッションには以下のセッションパフォーマンスメトリックが表示されます。

- ICA® Latency - 遅延は基本的にネットワーク遅延です。このパラメーターは、ネットワークが遅いかどうかを示します。
- ICA RTT - ICARTTは、ユーザーのアクションから画面に表示されるグラフィック応答までの時間間隔です。この測定には、ICA Latency、Endpoint Delay、およびHost Delayが含まれます。

このビューを使用して、セッションデータが流れるコンポーネントを理解し、パフォーマンスの問題を引き起こしている可能性のある特定のホップを特定できます。

セッショントポロジビューのパフォーマンスメトリックは、接続状態のHDXセッションでのみ利用可能です。

セッショントポロジのシナリオ

サイトの展開シナリオに応じて、セッションに関与するコンポーネントは次のすべてまたは一部です。

- エンドポイント上のCitrix Workspace™アプリ
- Gatewayサービス/オンプレミスGateway
- Cloud Connector – ハイブリッド接続の場合、GatewayはCloud Connectorを介してDaaSに接続されます。
- VDA

したがって、可能なネットワークトポロジは次のとおりです。

- エンドポイント上のCitrix Workspaceアプリは、Citrix WorkspaceおよびGateway Serviceを介してオンプレミスのVDAに接続します。VDAへの接続にCloud Connectorは使用されません。

セッショントポロジビュー(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/dir-session-topology1.png)

- エンドポイント上のCitrix Workspaceアプリは、Citrix WorkspaceおよびGateway Serviceを介して、Cloud Connector経由でオンプレミスのVDAに接続します。

セッショントポロジビュー(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/dir-session-topology2.png)

- エンドポイント上のCitrix Workspaceアプリは、StoreFront™およびオンプレミスGatewayを介してオンプレミスVDAに接続します。

セッショントポロジビュー(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/dir-session-topology3.png)

- エンドポイント上のCitrix Workspaceアプリは、StoreFrontを介してオンプレミスVDAに接続します。

セッショントポロジビュー(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/dir-session-topology4.png)

パフォーマンスメトリック

「**パフォーマンスメトリック**」パネルは、ユーザーセッション内の問題を特定する際にリアルタイムメトリックを関連付ける機能を提供します。セッションメトリックの傾向は、これらのメトリックが時間の経過とともにどのように推移したかを示すのに役立ちます。「**セッションパフォーマンス**」タブをクリックすると、リアルタイムデータとともに、ページロード時間を待つことなく過去15分間のデータを表示できます。プロットは、複数のコンポーネントパフォーマンスメトリックを単一のビューで関連付けるのに役立ちます。

セッションパフォーマンスメトリック(/en-us/citrix-virtual-apps-desktops/2402-ltsr/media/dir-session-performance-trends.png)

> **注：**
>
> 過去15分間のメトリックサポートにより、グラフはセッションが接続および切断された期間にわたってプロットされます。切断されたセッションのメトリックは、値ゼロで表示されます。
>
> ICARTTとICA Latencyの他に、以下のメトリックが利用可能です。

- Frames Per Second - フレーム/秒は、セッションの応答性を示す重要なメトリックです。
  Output Bandwidth Available - 利用可能な出力帯域幅は、VDAからエンドポイントにデータを送信するために利用可能な総帯域幅の測定値です。
- 出力帯域幅の消費量 - 出力帯域幅の消費量は、ユーザーにセッションを表示するためにVDAからエンドポイントへ送信された実際のデータ量を示します。

出力帯域幅の利用可能量と出力帯域幅の消費量を分析することで、セッションを提供するために十分な帯域幅が利用可能であるかを確認し、セッションが帯域幅不足の影響を受けているかどうかを検出するのに役立ちます。

シャドウユーザー

Directorから、シャドウユーザー機能を使用して、ユーザーの仮想マシンまたはセッションを直接表示したり操作したりできます。Windows VDAとLinux VDAの両方をシャドウできます。シャドウするマシンにユーザーが接続している必要があります。これは、ユーザーのタイトルバーに表示されているマシン名を確認することで検証できます。

Directorは新しいタブでシャドウを開始します。DirectorのURLからのポップアップを許可するようにブラウザ設定を更新してください。

シャドウ機能は、**ユーザーの詳細**ビューからアクセスします。ユーザーセッションを選択し、アクティビティマネージャービューまたはセッション詳細パネルで**シャドウ**をクリックします。

Linux VDAのシャドウ

シャドウは、RHEL7.3またはUbuntuバージョン16.04のLinuxディストリビューションを実行している、バージョン7.16以降のLinux VDAで利用できます。

注：

- シャドウが機能するには、VDAがDirector UIからアクセス可能である必要があります。したがって、シャドウはDirectorクライアントと同じイントラネット内のLinux VDAでのみ可能です。
- DirectorはFQDNを使用してターゲットLinux VDAに接続します。Directorクライアントが Linux VDAのFQDNを解決できることを確認してください。
- VDAには、python websockifyおよびx11vncパッケージがインストールされている必要があります。
- VDAへのnoVNC接続はWebSocketプロトコルを使用します。デフォルトでは、**ws://** WebSocketプロトコルが使用されます。セキュリティ上の理由から、Citrixは安全な **wss://** プロトコルを使用することを推奨します。各DirectorクライアントとLinux VDAにSSL証明書をインストールしてください。

セッションシャドウ の手順に従って、シャドウ用にVDAを構成してください。

1. **シャドウ**をクリックすると、シャドウ接続が初期化され、ユーザーデバイスに確認プロンプトが表示されます。
2. ユーザーに**はい**をクリックするよう指示して、マシンまたはセッションの共有を開始します。
3. 管理者はシャドウされたセッションを表示することのみ可能です。

Windows VDA のシャドウイング

Windows VDA セッションは、Windows リモートアシスタンスを使用してシャドウイングされます。VDA のインストール中に、**ユーザー Windows リモートアシスタンス**機能を有効にします。詳細については、「機能の有効化または無効化」を参照してください。

1. **シャドウ**をクリックすると、シャドウイング接続が初期化され、.msrc インシデントファイルを開くか保存するかを求めるダイアログボックスが表示されます。

2. デフォルトで選択されていない場合は、リモートアシスタンスビューアーでインシデントファイルを開きます。ユーザーデバイスに確認プロンプトが表示されます。
3. ユーザーに**はい**をクリックするよう指示して、マシンまたはセッションの共有を開始します。
4. より詳細な制御を行うには、ユーザーにキーボードとマウスの制御を共有するよう依頼します。

シャドウイング用に MICROSOFT INTERNET EXPLORER ブラウザーを合理化する

ダウンロードした Microsoft Remote Assistance (.msra) ファイルをリモートアシスタンスクライアントで自動的に開くように、Microsoft Internet Explorer ブラウザーを構成します。

これを行うには、グループポリシーエディターで 設定を有効にする必要があります。

コンピューターの構成 \> 管理用テンプレート \> Windows コンポーネント \> Internet Explorer \> インターネットコントロールパネル \> セキュリティページ \> インターネットゾーン \> ファイルのダウンロード時に自動的に確認する。

デフォルトでは、このオプションはローカルイントラネットゾーンのサイトで有効になっています。Director サイトがローカルイントラネットゾーンにない場合は、このゾーンにサイトを手動で追加することを検討してください。

ユーザーにメッセージを送信する

Directorから、1台以上のマシンに接続しているユーザーにメッセージを送信します。この機能を使用して、デスクトップのメンテナンス、マシンのログオフと再起動、プロファイルのリセットなど、差し迫った管理操作に関する即時通知を送信します。

1. アクティビティマネージャービューで、ユーザーを選択し、 をクリックします。
2. ユーザー詳細ビューで、セッション詳細パネルを見つけ、 をクリックします。
3. および フィールドにメッセージ情報を入力し、 をクリックします。

メッセージが正常に送信されると、Directorに確認メッセージが表示されます。メッセージはユーザーのマシンに表示されます。

メッセージが正常に送信されなかった場合、Directorにエラーメッセージが表示されます。エラーメッセージに従って問題をトラブルシューティングします。完了したら、件名とメッセージテキストを再度入力し、もう一度 をクリックします。

アプリケーションの障害を解決する

「**アクティビティマネージャー**」ビューで、タブをクリックします。このユーザーがアクセスできるすべてのマシン上のすべてのアプリケーション（現在接続されているマシンのローカルアプリケーションとホスト型アプリケーションを含む）と、それぞれのステータスを表示できます。

> **注：**
>
> タブがグレー表示されている場合は、タブを有効にする権限を持つ管理者に連絡してください。

> このリストには、セッション内で起動されたアプリケーションのみが含まれます。

マルチセッションOSマシンおよびシングルセッションOSマシンでは、切断されたセッションごとにアプリケーションが一覧表示されます。ユーザーが接続されていない場合、アプリケーションは表示されません。

アクション	説明
応答しないアプリケーションを終了する	応答しないアプリケーションを選択し、[アプリケーションの終了]をクリックします。アプリケーションが終了したら、ユーザーに再度起動するよう依頼します。
応答しないプロセスを終了する	必要な権限がある場合は、[プロセス]タブをクリックします。アプリケーションに関連する、または大量のCPUリソースやメモリを使用しているプロセスを選択し、[プロセスの終了]をクリックします。ただし、プロセスを終了するのに必要な権限がない場合、プロセスを終了しようとしても失敗します。
ユーザーのマシンを再起動する	シングルセッションOSマシンのみの場合、選択したセッションで[再起動]をクリックします。または、[マシン詳細]ビューから、電源コントロールを使用してマシンを再起動またはシャットダウンします。アプリケーションを再確認できるように、ユーザーに再度ログオンするよう指示します。マルチセッションOSマシンでは、再起動オプションは利用できませ

アクション	説明
	ん。代わりに、ユーザーからログオフし、ユーザーに再度ログオンさせます。
マシンをメンテナンスモードにする	マシンのイメージにパッチやその他の更新などのメンテナンスが必要な場合は、マシンをメンテナンスモードにします。[マシン詳細]ビューから[詳細]をクリックし、メンテナンスモードオプションをオンにします。適切な管理者にエスカレートしてください。

デスクトップ接続を復元する

Directorから、ユーザーのタイトルバーで現在のマシンに対するユーザーの接続ステータスを確認します。

デスクトップ接続が失敗した場合、失敗の原因となったエラーが表示され、トラブルシューティングの方法を決定するのに役立ちます。

アクション	説明
マシンがメンテナンスモードではないことを確認します	ユーザー詳細ページで、メンテナンスモードがオフになっていることを確認します。
ユーザーのマシンを再起動する	マシンを選択し、**再起動**をクリックします。ユーザーのマシンが応答しない、または接続できない場合にこのオプションを使用します。たとえば、マシンが異常に高いCPUリソースを使用しており、CPUが使用不能になっている場合などです。

セッションを復元する

セッションが切断されても、セッションはアクティブなままでアプリケーションは実行され続けますが、ユーザーデバイスはサーバーと通信しなくなります。

ユーザー詳細ビューで、**セッションの詳細**パネルのセッション障害をトラブルシューティングします。セッションIDで示される現在のセッションの詳細を表示できます。

アクション	説明
応答しないアプリケーションまたはプロセスを終了する	**アプリケーション**タブをクリックします。応答しないアプリケーションを選択し、**アプリケーションの終了**をクリックします。同様に、応答しない対応するプロセスを選択し、**プロセスの終了**をクリックします。また、異常に大量のメモリまたはCPUリソースを消費しているプロセスを終了します。これにより、CPUが使用不能になる可能性があります。
Windowsセッションを切断する	**セッション制御**をクリックし、**切断**を選択します。このオプションは、ブローカーされたマルチセッションOSマシンでのみ利用可能です。ブローカーされていないセッションの場合、このオプションは無効になります。
ユーザーのセッションからログオフする	**セッション制御**をクリックし、**ログオフ**を選択します。

セッションをテストするには、ユーザーはセッションに再度ログオンを試みることができます。また、ユーザーをシャドウして、このセッションをより詳細に監視することもできます。

HDX™ チャネルシステムレポートを実行する

ユーザーの詳細ビューで、**HDX**パネルにあるユーザーのマシン上のHDXチャネルのステータスを確認します。このパネルは、ユーザーのマシンがHDXを使用して接続されている場合にのみ利用可能です。

情報が現在利用できないことを示すメッセージが表示された場合は、ページが更新されるまで1分間待つか、**更新**ボタンを選択します。HDXデータの更新には、他のデータよりも少し時間がかかります。

詳細については、エラーまたは警告アイコンをクリックしてください。

> ヒント:
>
> タイトルバーの左隅にある左右の矢印をクリックすると、同じダイアログボックスで他のチャネルに関する情報を表示できます。

HDXチャネルシステムレポートは、主にCitrixサポートがさらなるトラブルシューティングのために使用します。

1. HDXパネルで、をクリックします。
2. .xmlレポートファイルを表示または保存できます。
    - .xmlファイルを表示するには、をクリックします。.xmlファイルは、Directorアプリケーションと同じウィンドウに表示されます。
    - .xmlファイルを保存するには、をクリックします。ウィンドウが表示され、Directorマシン上のファイルのダウンロード先を尋ねられます。

ユーザープロファイルをリセットする

注意:

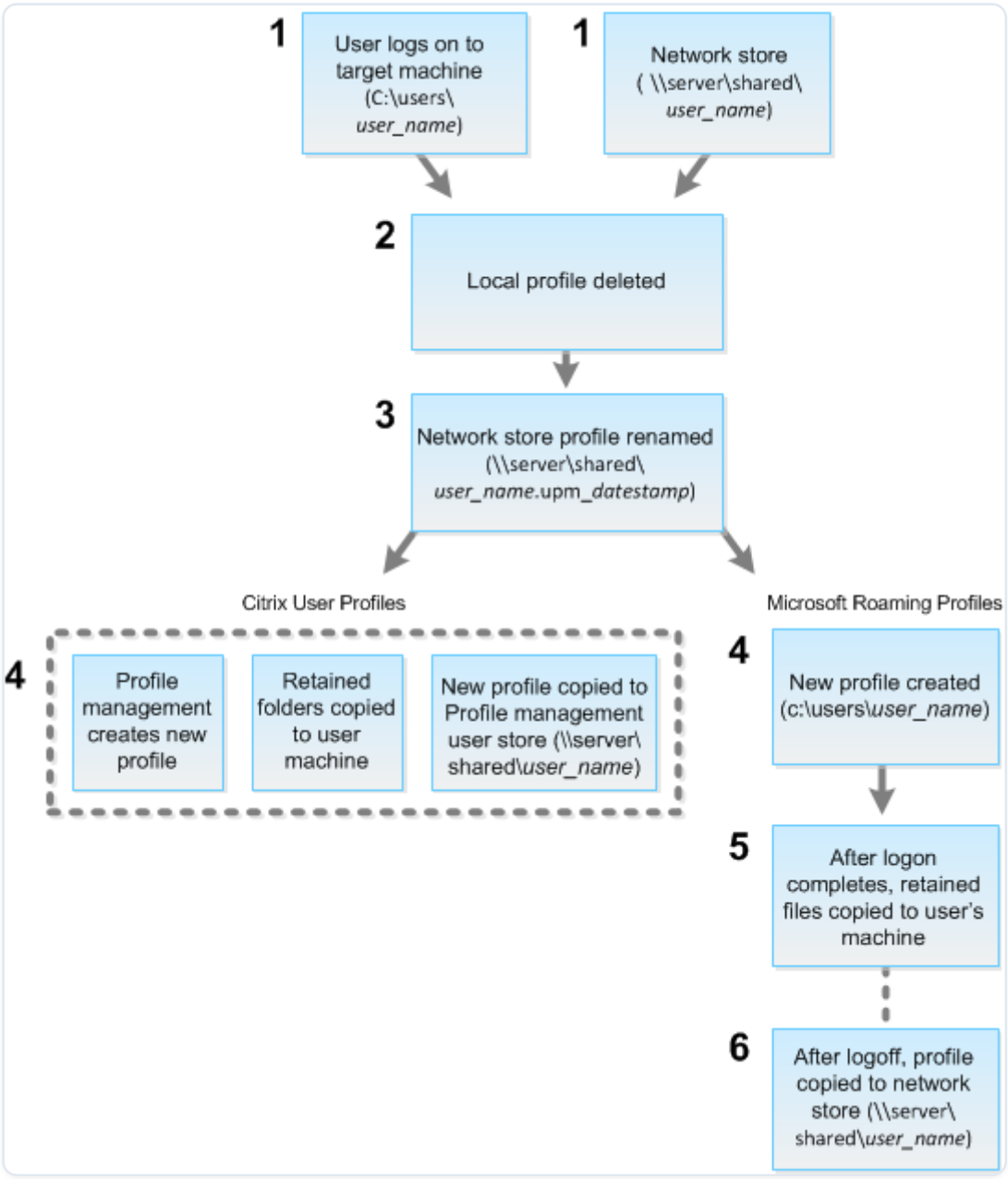
プロファイルがリセットされると、ユーザーのフォルダーとファイルは保存され、新しいプロファイルにコピーされます。ただし、ほとんどのユーザープロファイルデータは失われます（たとえば、レジストリがリセットされ、アプリケーション設定が削除される可能性があります）。

リセット機能は、ファイルベースとコンテナベースの両方のプロファイルソリューションに適用されます。

リセットされたプロファイルの処理方法

Citrix®ユーザープロファイルまたはMicrosoftローミングプロファイルのいずれもリセットできます。ユーザーがログオフし、リセットコマンド（DirectorまたはPowerShell SDKを使用して）を選択すると、Directorはまず使用中のユーザープロファイルを識別し、適切なリセットコマンドを発行します。Directorは、プロファイルサイズ、種類、ログオン時間などの情報をProfile Managementを通じて受け取ります。

この図は、ユーザープロファイルがリセットされた場合の、ユーザーログオン後のプロセスを示しています。



Directorによって発行されるリセットコマンドは、プロファイルの種類を指定します。その後、Profile Managementサービスはその種類のプロファイルをリセットしようとし、適切なネットワーク共有（ユーザーストア）を探します。ユーザーがProfile Managementによって処理されているにもかかわらず、ローミングプロファイルコマンドを受け取った場合、それは拒否されます（またはその逆も同様です）。

1. ローカルプロファイルが存在する場合、それは削除されます。
2. ネットワークプロファイルの名前が変更されます。
3. 次のアクションは、リセットされるプロファイルがCitrixユーザープロファイルかMicrosoftローミングプロファイルかによって異なります。

Citrixユーザープロファイルの場合、新しいプロファイルはProfile Managementのインポートルールを使用して作成されます。フォルダーはネットワークプロファイルにコピーされ、ユーザーは通常どおりログオンできます。リセットにローミングプロファイルが使用される場合、ローミングプロファイル内のレジストリ設定はリセットされたプロファイルに保持されます。必要に応じて、テンプレートプロファイルがローミングプロファイルを上書きするようにProfile Managementを構成できます。

Microsoftローミングプロファイルの場合、Windowsはプロファイルを作成し、ユーザーがログオンすると、フォルダーはユーザーデバイスにコピーされます。ユーザーが再度ログオフすると、新しいプロファイルはネットワークストアにコピーされます。

Directorでユーザープロファイルをリセットするには

Citrix Virtual Desktops™ (Desktop VDA) を使用している場合は、次の操作を行います。

1. **Director** で、プロファイルをリセットするユーザーを検索し、そのユーザーのセッションを選択します。
2. をクリックします。
3. ユーザーにすべてのセッションからログオフするよう指示します。
4. ユーザーに再度ログオンするよう指示します。 ユーザーのプロファイルから保存されたフォルダーとファイルは、新しいプロファイルにコピーされます。

Citrix Virtual Desktops (Server VDA) を使用している場合、プロファイルのリセットを実行するにはログオンしている必要があります。その後、ユーザーはログオフし、再度ログオンしてプロファイルのリセットを完了する必要があります。

重要:

ユーザーが複数のプラットフォーム (Windows 8 や Windows 7 など) でプロファイルを持っている場合、ユーザーが問題として報告したのと同じデスクトップまたはアプリに最初に再度ログオンするよう指示します。このログオン操作により、正しいプロファイルがリセットされます。プロファイルがCitrixユーザープロファイルの場合、ユーザーのデスクトップが表示されるまでにプロファイルはすでにリセットされています。プロファイルがMicrosoftローミングプロファイルの場合、フォルダーの復元が短時間進行中の可能性があります。ユーザーは復元が完了するまでログオンしたままにする必要があります。

> プロファイルが正常にリセットされない場合 (たとえば、ユーザーがマシンに正常にログオンできない、または一部のファイルが欠落している場合) は、元のプロファイルを手動で復元する必要があります。

次の点に注意してください。

- ユーザープロファイルソリューションとしてユーザーストアが有効になっている場合、新しいプロファイルには元のユーザープロファイルから次の個人用フォルダーが含まれます。
  - デスクトップ
  - クッキー
  - お気に入り
  - ドキュメント
  - ピクチャ
  - ミュージック
  - ビデオ
- Citrix Managementプロファイルコンテナがユーザープロファイルソリューション全体として有効になっている場合、新しいプロファイルには、以前の個人用フォルダーは含まれません。
- Windows 8以降では、プロファイルがリセットされると、Cookieは新しいプロファイルにコピーされません。

リセットに失敗したプロファイルを手動で復元するには

1. ユーザーにすべてのセッションからログオフするよう指示します。
2. ローカルプロファイルが存在する場合は削除します。
3. ネットワーク共有上で、フォルダー名に日付と時刻が付加されたアーカイブフォルダー（.upm_datestamp拡張子を持つフォルダー）を見つけます。
4. 現在のプロファイル名、つまりupm_datestamp拡張子がない方を削除します。
5. アーカイブされたフォルダーを元のプロファイル名にリネームします。つまり、日付と時刻の拡張子を削除します。これにより、プロファイルはリセット前の元の状態に戻ります。

PowerShell SDKを使用してプロファイルをリセットするには

Broker PowerShell SDKを使用してプロファイルをリセットできます。

NEW-BROKERMACHINECOMMAND

特定のユーザー、セッション、またはマシンへの配信のためにキューに入れられたコマンドを作成します。このコマンドレットの詳細については、`<https://citrix.github.io/delivery-controller-sdk/Broker/New-BrokerMachineCommand/>`を参照してください。

例

プロファイルをリセットするためのPowerShellコマンドレットの使用方法の詳細については、以下の例を参照してください。

Profile Managementプロファイルをリセットする

- user1のプロファイルをリセットしたいとします。New-BrokerMachineCommand PowerShellコマンドを使用します。例：
  - `New-BrokerMachineCommand -Category UserProfileManager -CommandName "ResetUpmProfile" -DesktopGroups 1 -CommandData $byteArray -SendTrigger logon -user domain1\user1`

> **重要:**
>
> `CommandData $byteArray`は次の形式である必要があります: `<SID>[,<backup path>]`。バックアップパスを指定しない場合、Profile Managementは現在の日時で名前が付けられたバックアップフォルダーを生成します。

Windowsローミングプロファイルをリセットする

- user1 のローミングプロファイルをリセットしたいとします。New-BrokerMachineCommand PowerShell コマンドを使用します。例:
  - `New-BrokerMachineCommand -Category UserProfileManager -CommandName "ResetRoamingProfile" -DesktopGroups 1 -CommandData $byteArray -SendTrigger logon -user domain1\user1`

セッションを記録する

Directorの**ユーザー詳細**画面と**マシン詳細**画面にあるセッション記録コントロールを使用して、ICA®セッションを記録できます。この機能は、**Premium**サイトのお客様にご利用いただけます。

動的セッション記録

ユーザー詳細画面のセッション記録コントロールを使用して、現在アクティブなセッションを記録できます。動的セッション記録について詳しくは、(/ja-jp/session-recording/service.html)の記事を参照してください。

ポリシーベースのセッション記録

DirectorConfigツールを使用してDirectorでポリシーベースのセッション記録を構成するには、(/ja-jp/session-recording/current-release/configure/policies/session-recording-policies.html#configure-the-director-to-use-the-session-recording-serverording-server)の「**セッション記録サーバーを使用するようにDirectorを構成する**」セクションを参照してください。 セッション記録コントロールは、ログオンしているユーザーがセッション記録ポリシーを変更する権限を持っている場合にのみDirectorで利用できます。この権限は、(/ja-jp/session-recording/current-release/configure/settings-on-session-recording-server/grant-access-rights.html)で説明されているように、セッション記録承認コンソールで設定できます。

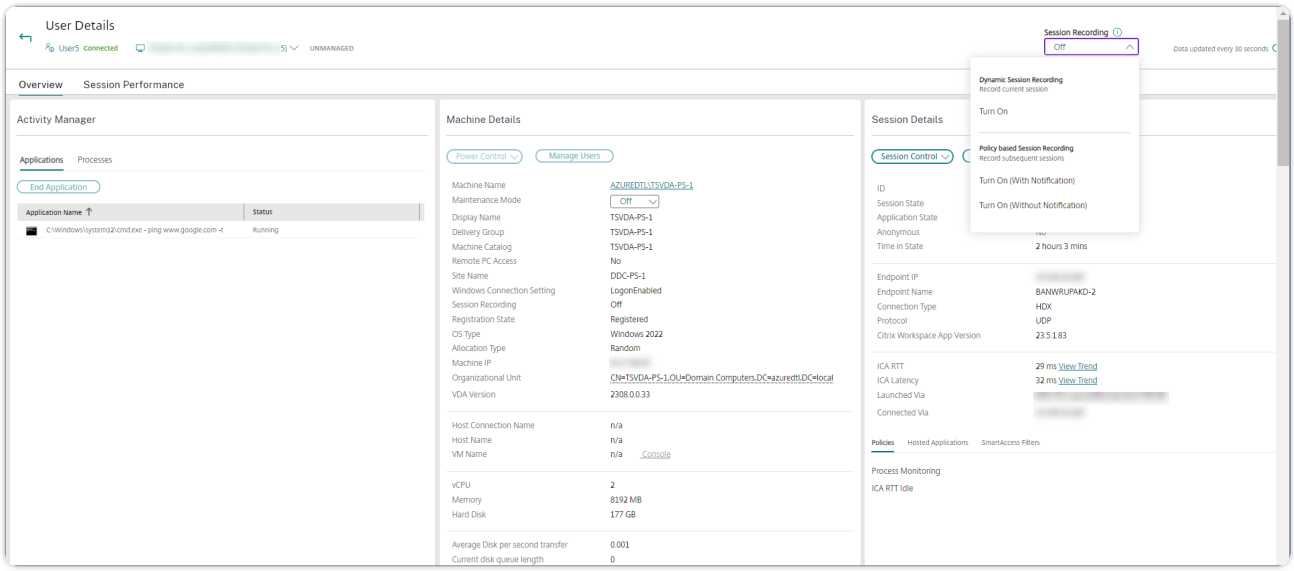
> **注：** DirectorまたはセッションS録画ポリシーコンソールを介して行われたセッション録画設定への変更は、次回のICAセッションから有効になります。

Directorのセッション記録コントロール

ユーザー詳細 > **セッション記録**アクションを使用して、現在または以降のセッションを記録できます。

- 動的セッション記録をオンにする - 現在のセッションが記録されます。
- オンにする（通知あり） - 以降のセッションが記録され、ICAセッションにログオンする際に、セッションが記録されていることがユーザーに通知されます。
- オンにする（通知なし） - 以降のセッションが記録され、ユーザーに通知することなく、セッションはサイレントに記録されます。
- オフにする - ユーザーのセッション記録を無効にする。

ポリシーパネルには、アクティブなセッション記録ポリシーの名前が表示されます。



マシン詳細パネルには、マシンのセッション記録ポリシーのステータスが表示されます。

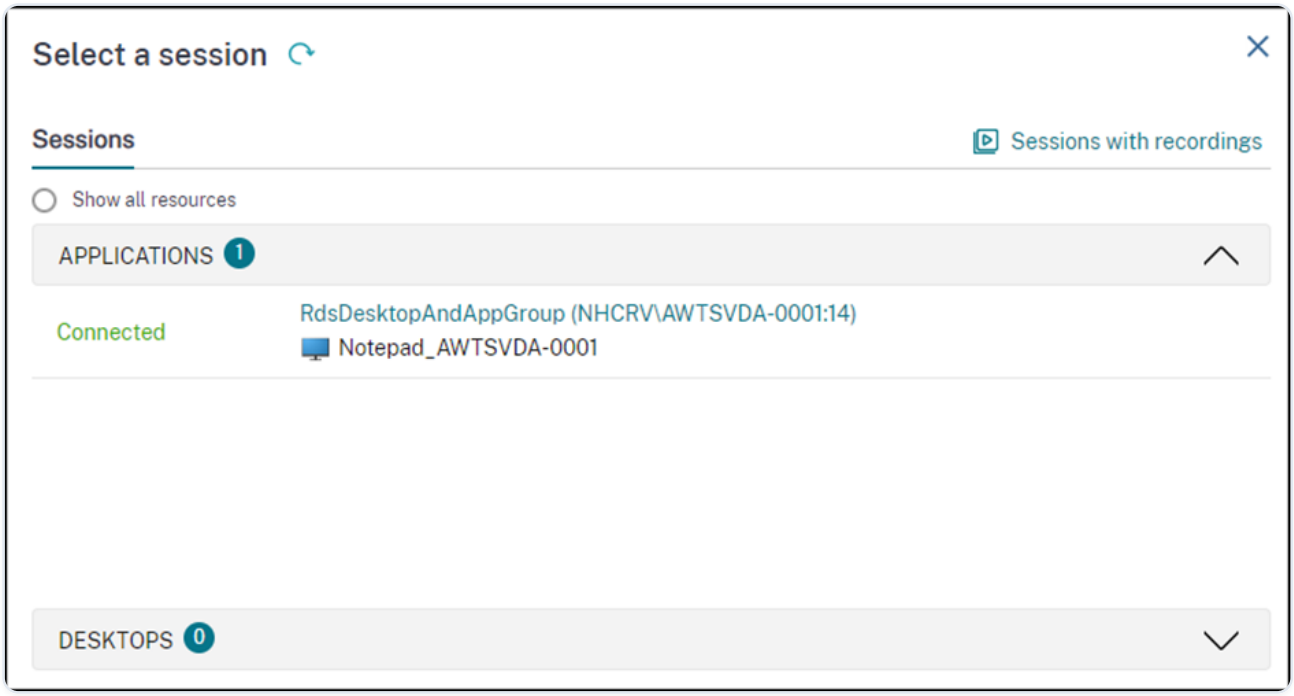
ライブセッションと録画セッションを再生する

ユーザーが遭遇した問題を理解するために、録画されたユーザーセッションとライブユーザーセッションを再生できます。Directorコンソール内で録画とセッション関連のメトリックにすぐにアクセスできるため、複数のセッション録画サーバーで録画を検索したり、録画を表示するためのサードパーティ製アプリを探したりする必要がなくなります。これにより、録画で発見された問題とパフォーマンスメトリックを関連付けるのに役立ちます。

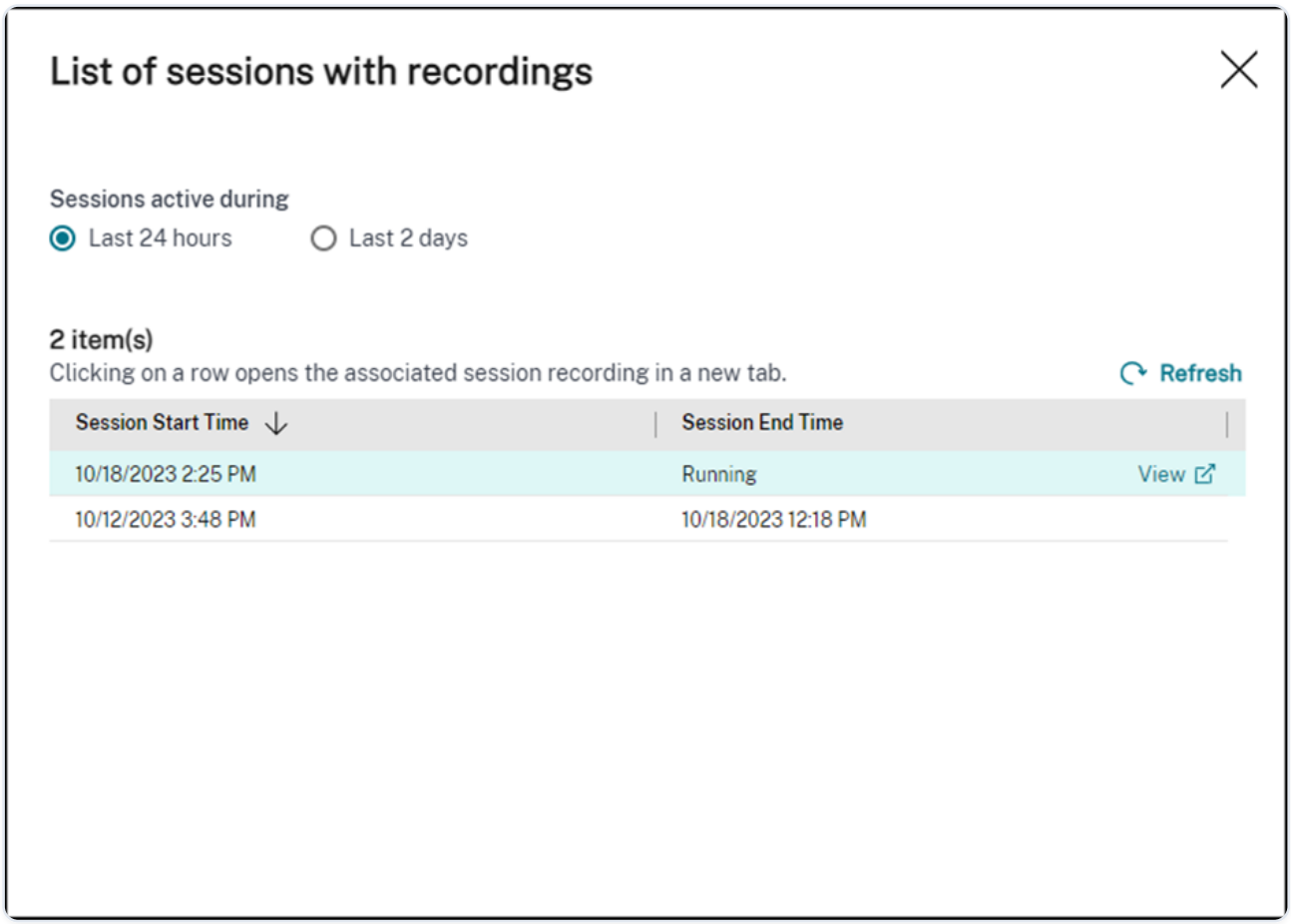
この機能には、以下が必要です。

- VDAとセッション録画サーバーはバージョン2308以降であること。
- Delivery Controller™とDirectorはバージョン2311以降であること。

Directorはセッション録画を一元的なリポジトリに保存します。「**Session Selector**」モーダル > 「**Sessions with recordings**」リンクをクリックすると、ユーザーに属する録画のリストが表示されます。



過去24時間または過去2日間にアクティブだったセッションの録画を表示することを選択できます。現在アクティブなセッションのライブ録画は、「**Session End Time**」が「**Running**」と表示されます。



「**View**」リンクをクリックすると、Citrix Session Recording再生サーバーを使用して新しいタブで録画を再生できます。

アプリケーションおよびデスクトップのプロービング

アプリケーションとデスクトップのプロービングは、StoreFront を使用してサイトに公開されているアプリとデスクトップをテスト起動することで、それらの正常性をチェックするプロセスを自動化します。プロービングの結果は Director で確認できます。

要件

- アプリケーションプロービングには Delivery Controller バージョン 7.18 以降、デスクトッププロービングにはバージョン 1906 以降が必要です。
- プローブエージェントを実行するエンドポイントマシンは、アプリケーションプロービングにはCitrix Workspace™ app for Windowsバージョン1808以降、デスクトッププロービングにはバージョン1906以降を搭載したWindowsマシンです。Unified Windows Platform (UWP) 用のWorkspaceアプリはサポートされていません。
- Citrix Probe Agent は、Active Directory 資格情報を使用した StoreFront および Citrix Workspace 経由の認証をサポートしています。エンドポイントデバイスが Citrix Gateway 経由で StoreFront / Workspace に接続されている場合、Citrix Gateway ドメイン資格情報または多要素認証 (MFA) を使用して認証できます。Citrix Probe Agent は、シングルサインオン (SSO) などの他の認証方法をサポートしていません。
- プローブエージェントをインストールするエンドポイントマシンに、Microsoft .NET Frameworkバージョン4.7.2以降がインストールされていることを確認してください。

プロービングの実行に必要なユーザーアカウント/権限：

- 各エンドポイントマシンでプローブする一意の StoreFront ユーザー。StoreFront ユーザーは管理者である必要はありません。プローブは非管理者コンテキストで実行できます。
- エンドポイントマシンにCitrix Probe Agentをインストールおよび構成するためのWindows管理者権限を持つユーザーアカウント。
- ユーザーは、アプリケーションまたはデスクトップの起動に使用されるVDAと同じドメインのメンバーである必要があります。Probe Agentは現在、複数のドメインをサポートしていません。
- 既存のユーザーアカウントをプロービングに再利用すると、ユーザーのアクティブなセッションからログオフする可能性があります。フル管理者ユーザーアカウント、または以下の権限を持つカスタムロールが必要です。
    - デリバリーグループの権限:
        - 読み取り専用

- Directorの権限:
  - アラートメールサーバー構成の作成\\編集\\削除 - (メールサーバーがまだ構成されていない場合)
  - プローブ構成の作成\\編集\\削除
  - 構成ページの表示
  - トレンドページの表示

構成

複数の地域で、ピーク時間外にプローブを実行するようにスケジュールできます。包括的なプローブ結果は、ユーザーが問題に遭遇する前に、アプリケーション、ホストマシン、または接続に関連する問題をトラブルシューティングするのに役立ちます。

Citrix Probe Agent バージョン 2103 以降は、サイト集約をサポートしています。Citrix Probe Agent を構成するときは、集約されたサイトからのアプリケーションとデスクトップの列挙を有効にするために、Workspace (StoreFront) Site Aggregation Enabled オプションを選択します。以下のサイトの組み合わせがサポートされています。

- 1つの StoreFront URL を持つ複数のオンプレミスサイト。
- StoreFront または Workspace URL のいずれかを持つオンプレミスサイトとクラウドサイト。
- 1つの Workspace URL を持つ複数のクラウドサイト。
- Citrix Gateway 経由で StoreFront または Workspace に接続されているオンプレミスサイト。

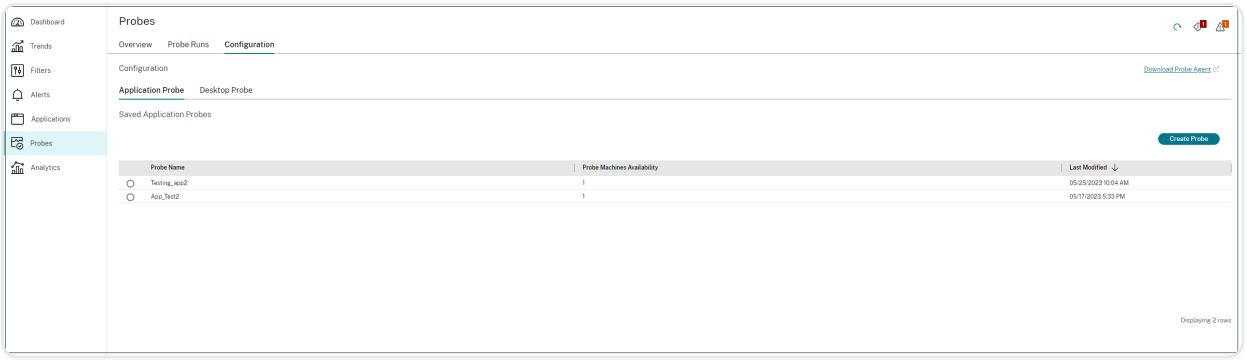
> **注:**
>
> 1つのサイトにのみアクセスできるプローブを構成するには、個別の管理者またはユーザーを作成する必要があります。

ステップ1：Citrix Probe Agentをインストールして構成する

Citrix Probe Agent は、ユーザーが StoreFront を介して実際のアプリケーションまたはデスクトップを起動するのをシミュレートする Windows 実行可能ファイルです。Director で構成された起動をテストし、その結果を Director に報告します。

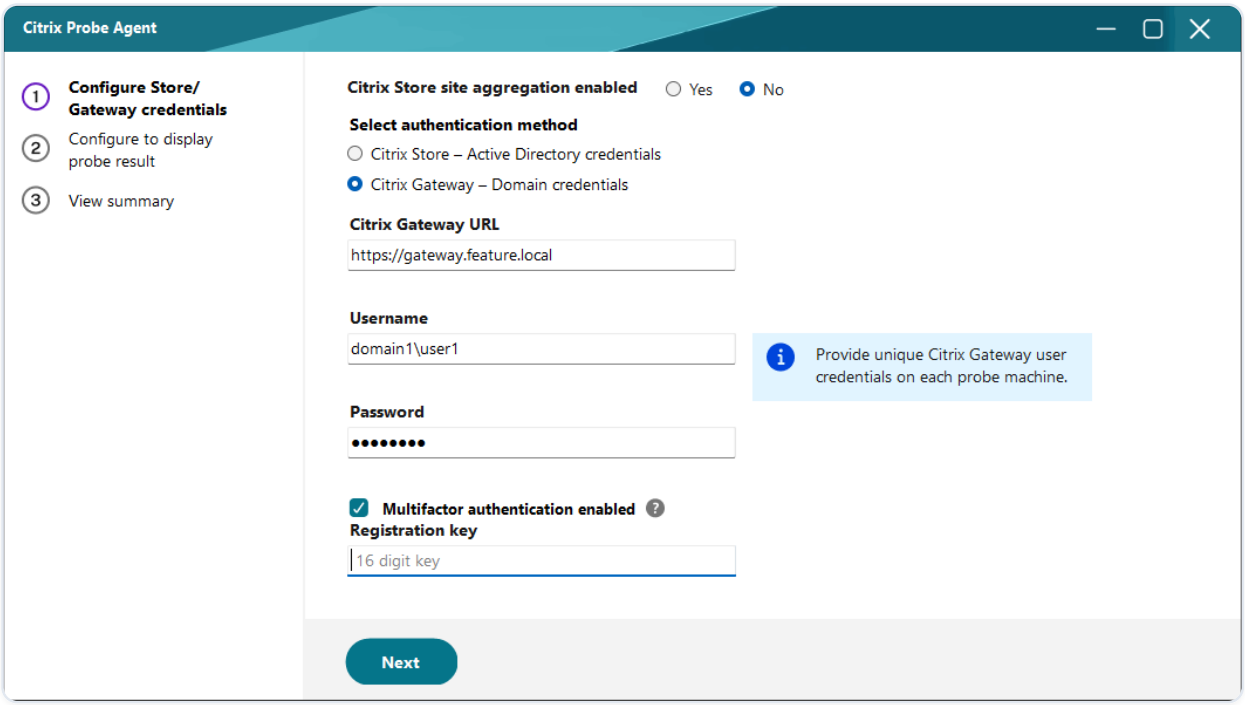
1. プロービングを実行するエンドポイントマシンを特定します。

2. 管理者権限を持つユーザーは、エンドポイントマシンに Citrix Probe Agent をインストールして構成できます。`<https://www.citrix.com/downloads/citrix-virtual-apps-and-desktops/components/app-probe-agent.html>`で入手可能な Citrix Probe Agent 実行可能ファイルをダウンロードしてください。ダウンロードリンクは、Director の タブでも利用できます。

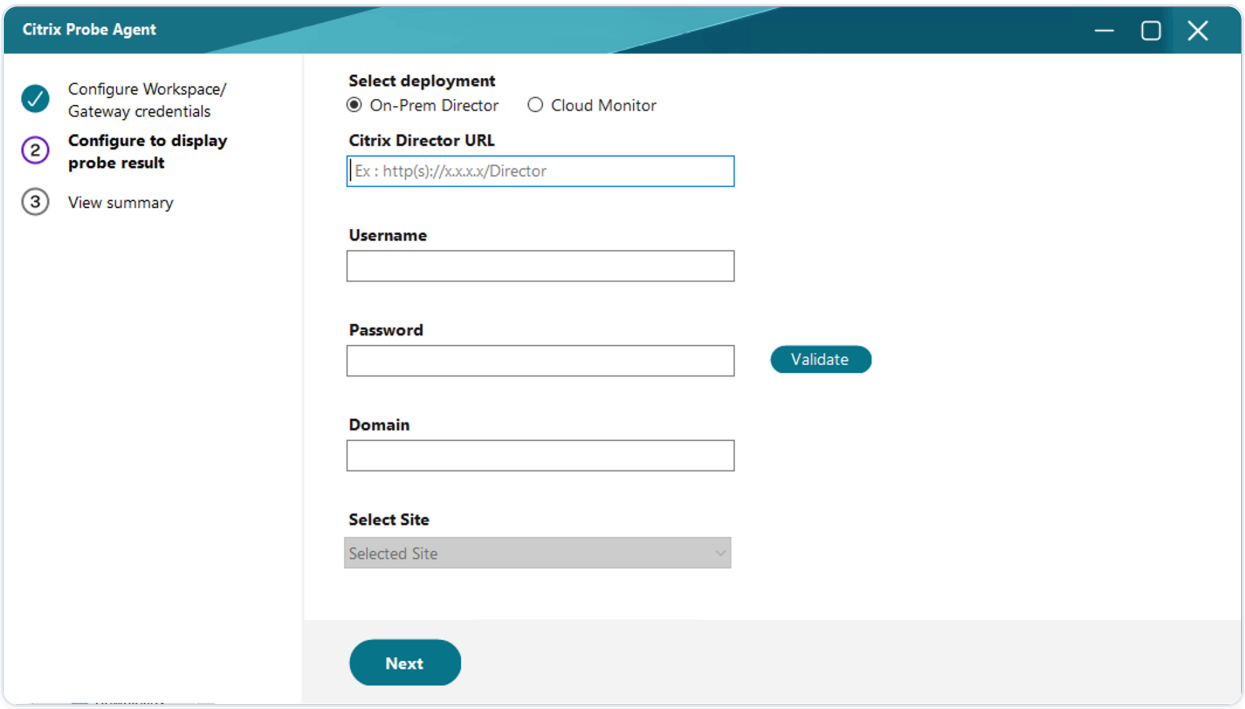


。

3. 集約されたサイトがある場合は、集約されたサイトからのアプリケーションとデスクトップの列挙を有効にするために、Workspace (StoreFront) Site Aggregation Enabled オプションを選択します。
4. 認証方法を選択し、関連する資格情報を入力します。資格情報は暗号化され、安全に保存されます。
5. StoreFront の Active Directory 資格情報で構成します。各エンドポイントマシンで一意の Workspace (StoreFront) ユーザーを構成します。
6. エンドポイントがCitrix Gatewayを介してStoreFrontに接続されている場合は、Citrix Gatewayオプションを選択し、Citrix Gatewayドメインの資格情報で構成します。



7. Gatewayがサポートしている場合は、多要素認証オプションを選択し、16桁の認証キーを入力します。これは、LDAPとシングルログインスキーマを使用したネイティブOTPで構成されたCitrix Gatewayでのみ利用可能です。
8. タブで、Director の資格情報を入力し、 をクリックします。



9. サイトを選択し、**次へ**をクリックします。
10. 「**概要の表示**」タブで、構成された詳細が正確であることを確認します。変更が必要な場合は、該当するタブに移動して更新します。

注:

Automating Citrix Probe Agent Installation and Configuration に含まれるPowerShellスクリプトを使用して、Citrix Probe Agentのインストールと構成を自動化できます。

ステップ2：Directorでプロービングを構成する

制限事項:

対話型ログオンメッセージバナーが有効になっているWindows VDAからアプリケーションまたはデスクトップがテスト起動されると、プロービングは失敗します。これは、対話型ログオンメッセージの承認を待機しているためにタイムアウトが発生するためです。 サーバーVDAでログオンメッセージを無効にするには、 > > > > に移動します。

以下のフィールドのテキストを削除し、Microsoftポリシーを更新します。

- 対話型ログオン: ログオンしようとしているユーザーへのメッセージテキスト
- 対話型ログオン: ログオンしようとしているユーザーへのメッセージタイトル

プローブがアプリケーションまたはデスクトップの起動状態を通過できるように、対話型ログオンメッセージバナーを無効にして、この特定のサーバーVDAにプローブユーザーを割り当てます。

詳細については、`<https://learn.microsoft.com/ja-jp/windows/security/threat-protection/security-policy-settings/interactive-logon-message-text-for-users-attempting-to-log-on>`を参照してください。

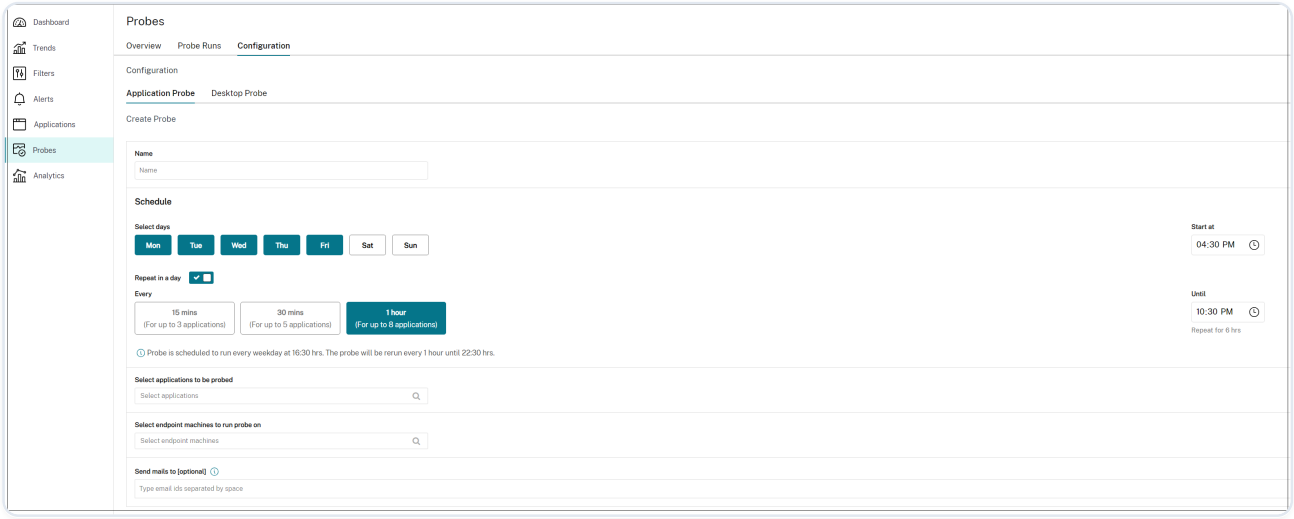
1. **プローブ** \> **アプリケーションプローブ**または**デスクトッププローブ**に移動し、**プローブの作成**をクリックします。
2. 「**プローブの作成**」ページで、プローブの名前を入力します。
3. スケジュールを選択します。

    a. プローブを実行する曜日を選択します。

b. プローブを実行する開始時刻を入力します。

c. さらに、「**1日あたりの繰り返し**」オプションを選択できます。プローブを1日の中で繰り返す終了時刻と間隔を入力します。たとえば、以下の構成では、毎週月曜日、水曜日、木曜日、日曜日に、12:08から16:34まで30分ごとにアプリケーションプローブが実行されます。

4. 間隔に応じて、プローブするアプリケーションまたはデスクトップの推奨数を選択します。
5. プローブを実行する必要があるエンドポイントマシンを選択します。
6. 失敗したプローブの結果を送信する管理者のメールアドレスを入力します。メールサーバーは、**アラート** > **メールサーバーの構成**で構成します。



この構成では、毎週月曜日、水曜日、木曜日、日曜日に、アプリケーションセッションが12:08、12:38、13:08といった具合に16:08まで起動します。

注:

- 構成後、エージェントは次の時間から構成されたプローブを実行します。
- 「**1日あたりの繰り返し**」オプションが導入される前に設定されたプローブは、スケジュールされた時刻に引き続き実行されます。これらのプローブでは、「**1日あたりの繰り返し**」オプションはデフォルトで無効になっています。
- 重複を防ぐため、各実行に5分の期間があるようにプローブを構成することをお勧めします。

ステップ3：プローブの実行

エージェントは、Directorから定期的に取得するプローブ構成に従ってプロービングを実行します。

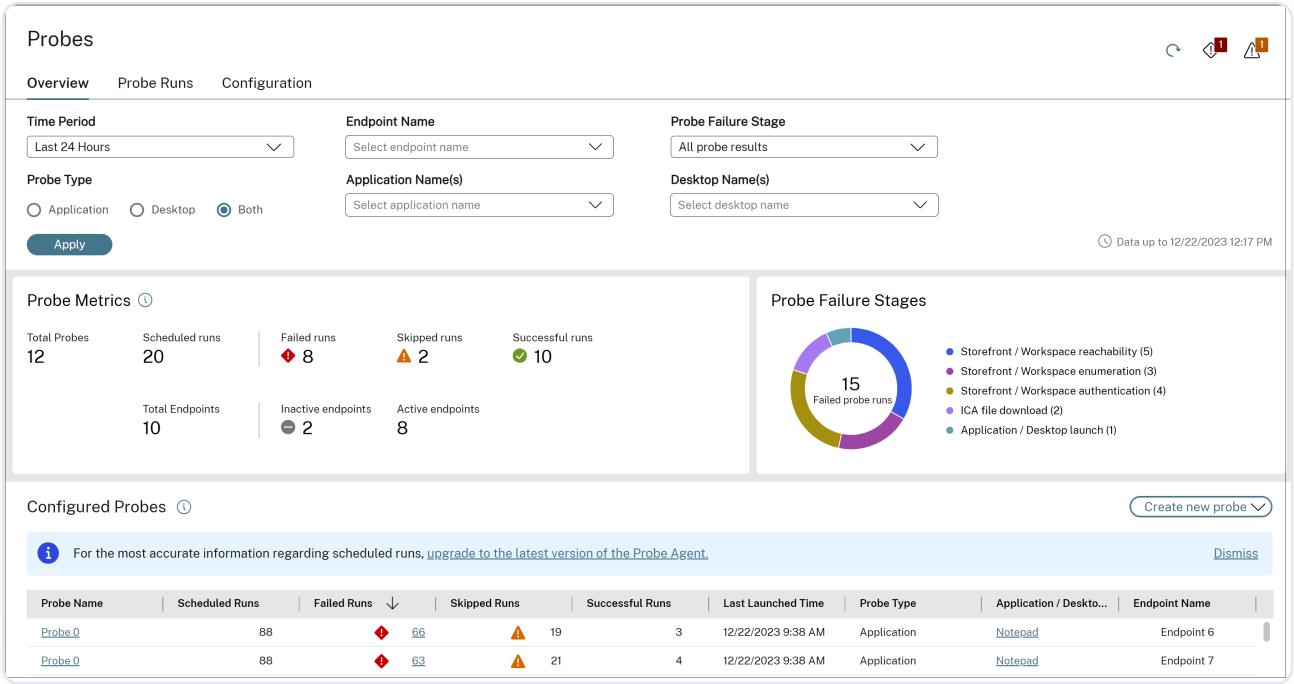
StoreFrontを使用して、選択されたアプリケーションを順次起動します。エージェントは、Monitorデータベースを介して結果をDirectorに報告します。障害は5つの特定の段階で報告されます。

- **StoreFront到達可能性** - 構成されたStoreFront URLに到達できません。
- **StoreFront認証** - 構成されたStoreFront資格情報が無効です。
- **StoreFront列挙** - StoreFrontのアプリケーション列挙リストに、プローブ対象のアプリケーションまたはデスクトップが含まれていません。
- **ICA®ダウンロード** - ICAファイルが利用できません。
- **アプリケーション/デスクトップの起動** – アプリケーションまたはデスクトップを起動できませんでした。

ステップ4：プローブ結果の表示

プローブでプローブ結果を確認できます。プローブビューでは、プローブ結果の包括的な概要が示されます。これらの結果は、問題をプロアクティブに分析およびトラブルシューティングし、ユーザーのセッション起動エクスペリエンスをよりスムーズにするのに役立ちます。

概要タブには、構成されているすべてのプローブの概要が1つのビューに表示されます。



プローブは、期間、プローブタイプ、エンドポイント名、アプリケーション名、デスクトップ名、およびプローブ結果タイプに基づいてフィルターできます。フィルター条件に一致するプローブ

は、プローブ、アプリケーション/デスクトップ、およびエンドポイントごとに次の詳細とともに表示されます。

プローブメトリックには、スケジュール済み、計画済み、スキップ済み、成功、失敗した実行の数が表示されます。

- 完了した実行 – 完了まで実行されたプローブ実行の数。
- 失敗した実行 – 失敗したプローブ実行の数。
- スキップされた実行 – エンドポイントが非アクティブであるか、サービスが利用できないために完了しなかった実行の数。
- 成功した実行 – アプリ/デスクトップの起動中に、どの段階でも失敗することなく正常に完了したプローブの数。

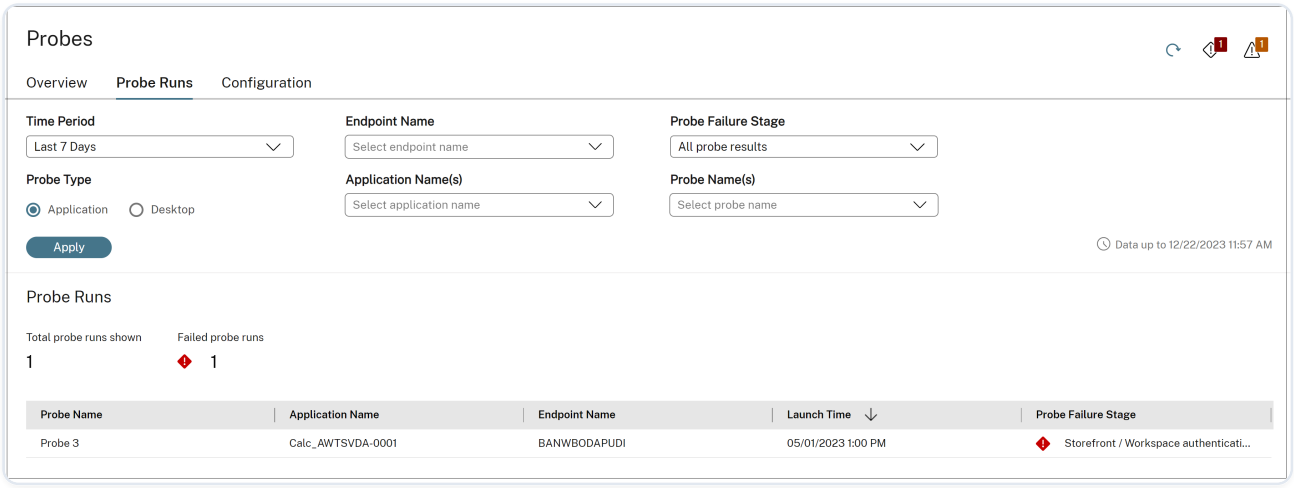
エンドポイントマシンの総数も、アクティブなマシンと非アクティブなマシンの数とともに表示されます。

プローブ失敗ステージは、各失敗グループの失敗分布を視覚的に内訳表示します。ほとんどの失敗が発生したステージを分析することで、プローブ結果の解釈と問題のトラブルシューティングが容易になります。グラフィカル表示では、アプリケーション/デスクトップの起動、ICAファイルのダウンロード、Storefront/Workspaceの列挙、Storefront/Workspaceの到達可能性、Storefront/Workspaceの認証における失敗したプローブ実行の数が示されます。

ほとんどの失敗が発生したステージを分析するのに役立ちます。この情報は、プローブ結果を迅速に理解し、トラブルシューティングを行うのに役立ちます。

エンドポイントが非アクティブであるか、サービスが利用できないために、一部のプローブ実行が完了しない場合があります。

プローブ実行タブには、完了したプローブ実行の結果が詳細に表示されます。選択したプローブの個々の実行の詳細を確認するためにドリルダウンできます。重要なピボットポイントに基づいて、さらにフィルタリングおよび分析できます。



プローブ実行は、期間、プローブタイプ、エンドポイント名、アプリケーション名、デスクトップ名、プローブ失敗ステージに基づいてフィルタリングできます。プローブ失敗ステージは、プローブが失敗したステージを表示します。プローブ名、スケジュールされた実行、失敗した実行、アプリケーション/デスクトップ名のリンクをクリックすると、フィルタ条件に一致するプローブ実行のリストが表示されたプローブ実行ページに移動します。

機能互換性マトリックス

Citrix Director 7 2402 は以下と互換性があります:

- Citrix Virtual AppsおよびDesktops™ 7 2112 以降
- Citrix Virtual AppsおよびDesktops 7 1912 長期サービスリリース

各サイト内で、Director を以前のバージョンの Delivery Controller™ とともに使用することはできますが、Director の最新バージョンのすべての機能が利用できるとは限りません。Citrix は、Director、Delivery Controller、および VDA を同じバージョンにすることを推奨しています。

> **注：**
>
> Delivery Controller をアップグレードした後、Studio を開くとサイトのアップグレードを促されます。詳細については、展開のアップグレード の「**アップグレードシーケンス**」セクションを参照してください。

> Director のアップグレード後に初めてログインすると、構成済みのサイトでバージョンチェックが実行されます。いずれかのサイトが Director より古いバージョンの Controller を実行している場合、Director コンソールにサイトのアップグレードを推奨するメッセージが

表示されます。さらに、サイトのバージョンが Director より古い間は、この不一致を示すメモが Director ダッシュボードに表示され続けます。

注：

以前のバージョンの Citrix Director では、最近の VDA バージョンで実行されているユーザーセッションに適用されたポリシーは表示されません。Citrix Director 1912 およびそれ以前のバージョンでは、VDA バージョン 2003 以降で実行されているユーザーセッションに適用されたポリシーは表示されません。これらのポリシーを表示するには、Citrix Director バージョン 2003 以降を使用してください。

Delivery Controller (DC)、VDA、およびその他の必要な依存コンポーネントの最小バージョンとライセンスエディションを含む特定の Director 機能は、次の表に記載されています。

DIRECTOR バージョン	機能	依存関係 - 必要な最小バージョン	エディション
2311	ライブおよび録画セッションの再生	VDA 2308 および DDC 2311	すべて
2311	セッショントポロジ	なし	すべて
2311	最適な画面解像度	なし	すべて
2311	MS Teams の最適化	VDA 2311 および DDC 最新版	すべて
2311	プローブの概要の機能強化	なし	すべて
2311	刷新されたセッションログオン期間ビュー	なし	すべて
2308	「プローブの概要とドリルダウン」(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/director/	なし	すべて

DIRECTOR バージョン	機能	依存関係 - 必要な最小バージョン	エディション
	probes.html#step-4-view-probe-results)		
2308	「Citrix Gateway 多要素認証の Citrix Probe Agent サポート」(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/director/probes.html#step-1-install-and-configure-the-citrix-probe-agent)	シトリックス ゲートウェイ	すべて
2308	「ハイパーバイザーアラートの無効化」(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/director/site-analytics/alerts-notifications.html#hypervisor-alerts-monitoring)	なし	すべて
2308	「セッションエクスペリエンスメトリックの傾向」(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/director/troubleshoot-deployments/user-issues.html#trends-for-session-performance-metrics)	なし	すべて
2305	「Citrix Gateway を介した認証のサポート」(/ja-jp/citrix-virtual-apps-	なし	すべて

DIRECTOR バージョン	機能	依存関係 - 必要な最小バージョン	エディション
	desktops/2402-ltsr/director/probes.html)		
2305	「Director での Autoscale 管理」(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/director/site-analytics/autoscale-managed-machines.html)	なし	すべて
2303	失敗したマシンアラート(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/director/site-analytics/alerts-notifications.html#failed-machines-in-)	DC 7 2303	プレミアム
2203	TLS 1.3 のサポート	-	すべて
2212	AMD GPUでリアルタイムGPU使用率が利用可能	64ビットWindowsおよびHDX 3D Proが有効なDC 7.14およびVDA 7.14	すべて
2212	高度なプローブスケジューリング(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/director/probes.html)	DC 7 1906 と シトリックス プローブ エージェント 2209	プレミアム
1909	Citrix Analytics for Performance を使用してオンプレミスサイトを構成する(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/director/install-and-	DC 7 1906およびVDA 1906	すべて

DIRECTOR バージョン	機能	依存関係 - 必要な最小バージョン	エディション
	configure/onboarding.html)		
1906	セッションの自動再接続	DC 7 1906およびVDA 1906	すべて
1906	セッション起動時間	DC 7 1906およびVDA 1903	すべて
1906	デスクトッププロービング	DC 7 1906 と シトリックス プローブ エージェント 1903	プレミアム
7.9以降	プロファイルロードにおけるCitrix Profile Managementの期間	VDA 1903	すべて
1811	プロファイルドリルダウン	DC 7 1811およびVDA 1811	すべて
1811	ハイパーバイザーアラート監視	DC 7 1811	プレミアム
1811	アプリケーションプロービング	DC 7 1811 および Citrix アプリケーション プローブ エージェント 1811	プレミアム
1811	Microsoft RDS ライセンスの健全性	DC 7 1811 および VDA 7.16	すべて
1811	主要なRTOPデータ表示	DC 7 1811 および VDA 1808	プレミアム
1808	フィルターデータの書き出し	DC 7 1808	すべて
1808	インタラクティブセッションのドリルダウン	DC 7 1808およびVDA 1808	すべて

DIRECTOR バージョン	機能	依存関係 - 必要な最小バージョン	エディション
1808	GPOのドリルダウン	DC 7 1808およびVDA 1808	すべて
1808	OData APIを使用したマシンの履歴データ利用可能	DC 7 1808	すべて
7.18	アプリケーションプロービング	DC 7.18	プレミアム (旧 Platinum)
7.18	スマートアラートポリシー	DC 7.18	プレミアム (旧 Platinum)
7.18	Health Assistant リンク	なし	すべて
7.18	インタラクティブセッションのドリルダウン	なし	すべて
7.17	PIV スマートカード認証	なし	すべて
7.16	アプリケーション分析	DC 7.16およびVDA 7.15	すべて
7.16	OData API バージョン4	DC 7.16	すべて
7.16	Shadow Linux VDA ユーザー	VDA 7.16	すべて
7.16	ドメインローカルグループのサポート	なし	すべて
7.16	マシンコンソールアクセス	DC 7.16	すべて
7.15	アプリケーション障害監視	DC 7.15およびVDA 7.15	すべて

DIRECTOR バージョン	機能	依存関係 - 必要な最小バージョン	エディション
7.14	アプリケーション中心のトラブルシューティング	DC 7.13およびVDA 7.13	すべて
7.14	ディスク監視	DC 7.14およびVDA 7.14	すべて
7.14	GPU監視	DC 7.14およびVDA 7.14	すべて
7.13	セッション詳細パネルのトランスポートプロトコル	DC 7.x および VDA 7.13	すべて
7.12	ユーザーフレンドリーな接続およびマシン障害の説明	DC 7.12 および VDA 7.x	すべて
7.12	Enterpriseエディションでの履歴データ可用性の向上	DC 7.12 および VDA 7.x	エンタープライズ
7.12	カスタムレポート	DC 7.12 および VDA 7.x	プレミアム (旧 Platinum)
7.11	リソース使用率レポート	DC 7.11およびVDA 7.11	すべて
7.11	CPU、メモリ、ICA RTT条件に対するアラート機能の拡張	DC 7.11およびVDA 7.11	プレミアム (旧 Platinum)
7.11	レポートのエクスポート機能の改善	DC 7.11およびVDA 7.x	すべて
7.11	Citrix ADMとの統合	DC 7.11、VDA 7.x、およびMASバージョン11.1ビルド49.16	プレミアム (旧 Platinum)

DIRECTOR バージョン	機能	依存関係 - 必要な最小バージョン	エディション
7.9	ログオン期間の内訳	DC 7.9 および VDA 7.x	すべて
7.7	プロアクティブな監視とアラート	DC 7.7 および VDA 7.x	プレミアム (旧 Platinum)
7.7	Windows認証統合	DC 7.x および VDA 7.x	すべて
7.7	シングルセッションおよびマルチセッションOSの使用状況	DC 7.7 および VDA 7.x	プレミアム (旧 Platinum)
7.6.300	Framehawk仮想チャネルのサポート(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/director/troubleshoot-deployments/user-issues/hdx-channel-reports.html)	DC 7.6 および VDA 7.6	すべて
7.6.200	セッション記録の統合(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/director/troubleshoot-deployments/user-issues/record-sessions.html)	DC 7.6 および VDA 7.x	プレミアム (旧 Platinum)
7	HDX Insightの統合(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/director/install-and-configure/hdx-insight.html)	DC 7.6、VDA 7.x、およびCitrix ADM	プレミアム (旧 Platinum)

データ粒度と保持

データ値の集計

Monitor Serviceは、ユーザーセッションの使用状況、ユーザーログオンパフォーマンスの詳細、セッション負荷分散の詳細、接続およびマシン障害情報など、さまざまなデータを収集します。データはカテゴリに応じて異なる方法で集計されます。OData Method APIを使用して提示されるデータ値の集計を理解することは、データを解釈するために不可欠です。例:

- 接続されたセッションとマシン障害は一定期間に発生します。したがって、それらは期間中の最大値として公開されます。
- ログオン期間は時間の長さを測定するものであるため、期間中の平均値として公開されます。
- ログオン数と接続障害は一定期間に発生した回数であるため、期間中の合計値として公開されます。

同時データ評価

セッションは、同時と見なされるためには重複している必要があります。ただし、時間間隔が1分の場合、その1分間のすべてのセッション（重複しているかどうかにかかわらず）は同時と見なされます。間隔のサイズが非常に小さいため、精度を計算するのに伴うパフォーマンスオーバーヘッドは、追加される価値に見合いません。セッションが同じ時間内に発生しても、同じ分内に発生しない場合、それらは重複しているとは見なされません。

サマリーテーブルと生データの相関

データモデルは、メトリックを2つの異なる方法で表します。

- サマリーテーブルは、分、時間、日ごとの時間粒度でメトリックの集計ビューを表します。
- 生データは、セッション、接続、アプリケーション、およびその他のオブジェクトで追跡される個々のイベントまたは現在の状態を表します。

API呼び出し間またはデータモデル自体内でデータを相関させようとするときは、以下の概念と制限を理解することが重要です。

- **部分的な間隔のサマリーデータはありません。** メトリックのサマリーは、長期間にわたる履歴トレンドのニーズを満たすように設計されています。これらのメトリックは、完全な間隔でサマリーテーブルに集計されます。データ収集の開始時（利用可能な最も古いデータ）または終了時の部分的な間隔には、サマリーデータはありません。1日の集計（Interval=1440）を表示する場合、これは最初と最新の不完全な日にはデータがないことを意味します。これらの部分的な間隔には生データが存在する可能性がありますが、それは決して要約されません。特定

のデータ粒度について、特定のサマリーテーブルから最小および最大のSummaryDateを抽出することで、最も早い集計間隔と最も遅い集計間隔を決定できます。SummaryDate列は間隔の開始を表します。Granularity列は、集計データの期間の長さを表します。

- **時間による相関。** メトリックは、前述のセクションで説明されているように、完全な間隔でサマリーテーブルに集計されます。これらは履歴トレンドに使用できますが、生イベントはトレンド分析のために要約されたものよりも現在の状態をより正確に反映している可能性があります。サマリーと生データの時間ベースの比較では、発生する可能性のある部分的な間隔、または期間の開始と終了にはサマリーデータがないことを考慮する必要があります。
- **見逃されたイベントと潜在的なイベント。** 集計テーブルに集計されるメトリックは、イベントが見逃されたり、集計期間に対して潜在的であったりする場合、わずかに不正確になる可能性があります。モニターサービスは正確な現在の状態を維持しようとしますが、見逃されたイベントや潜在的なイベントのために、集計テーブルの集計を再計算するために過去に遡ることはありません。
- **接続の高可用性。** 接続の高可用性中、現在の接続のサマリーデータカウントにギャップが生じますが、セッションインスタンスは引き続き生データで実行されます。
- **データ保持期間。** サマリーテーブルのデータは、生イベントデータのスケジュールとは異なるグルーミングスケジュールで保持されます。サマリーテーブルまたは生テーブルからグルーミングによってデータが削除されたため、データが欠落している可能性があります。保持期間は、サマリーデータの異なる粒度によっても異なる場合があります。粒度の低いデータ（分単位）は、粒度の高いデータ（日単位）よりも早くグルーミングされます。グルーミングによってある粒度からデータが欠落している場合でも、より高い粒度で見つかる可能性があります。API呼び出しは要求された特定の粒度のみを返すため、ある粒度でデータが受信されないからといって、同じ期間のより高い粒度でデータが存在しないという意味ではありません。
- **タイムゾーン。** メトリックはUTCタイムスタンプで保存されます。サマリーテーブルは、時間単位のタイムゾーン境界で集計されます。時間単位の境界に該当しないタイムゾーンの場合、データが集計される場所に関して多少の不一致が生じる可能性があります。

粒度と保持

Directorによって取得される集計データの粒度は、要求された時間 (T) スパンの関数です。ルールは次のとおりです。

- 0 \< T \<= 1時間 - 分単位の粒度を使用
- 0 \< T \<= 30日 - 時間単位の粒度を使用
- T \> 31日 - 日単位の粒度を使用

集計データから取得されない要求データは、生のセッションおよび接続情報から取得されます。このデータは急速に増加する傾向があるため、独自のグルーミング設定があります。グルーミングは、関連データのみが長期的に保持されることを保証します。グルーミングは、レポートに必要な粒度を維持しながら、より良いパフォーマンスを保証します。Premiumライセンスサイトのお客様は、グルーミング保持を希望する保持日数に変更できます。変更しない場合はデフォルトが使用されます。サイトデータベースとの接続が失われた場合、モニターサービスは以下の表で指定されているPremiumエンタイトルメントのデフォルトの保持日数を使用します。

設定にアクセスするには、Delivery Controller™ で次のPowerShellコマンドを実行します。

```
asnp Citrix.*

 Get-MonitorConfiguration

 Set-MonitorConfiguration -<setting name> <value>
```

#	設定名	影響を受けるスキーマテーブル	モニターページで影響を受けるテーブルとグラフ	PREMIUMの保持日数	ADVANCEDの保持日数
1	GroomSessionsRetentionDays	MonitorData.Session および Monitordata.Connection テーブル	この設定は、トレンドページのセッションの詳細、ユーザーセッションごとのログオン期間、アプリケーションベースの使用状況テーブルに影響します。	90	31
2	GroomFailuresRetentionDays	MonitorData.MachineFailureLog および MonitorData	トレンドページ：この設定は、障害タブのグラフと	90	31

#	設定名	影響を受けるスキーマテーブル	モニターページで影響を受けるテーブルとグラフ	PREMIUMの保持日数	ADVANCEDの保持日数
		.ConnectionFailureLog	テーブルに影響します。		
3	GroomLoadIndexesRetentionDays	MonitorData.LoadIndex	この設定は、トレンドページの「ロードエバリュエーターインデックス」タブに表示されるデータに影響します。	3	3
4	GroomDeletedRetentionDays	LifecycleStateが「Deleted」であるMonitorData.Machine、MonitorData.Catalog、MonitorData.DesktopGroup、およびMonitorData.Hypervisorエンティティ。この設定は、関連するSession、SessionDetail、Summary、Failure、または	LifecycleStateが「Deleted」であるMachine、Catalog、DesktopGroup、およびHypervisorエンティティ。この設定は、関連するSession、SessionDetail、Summary、Failure、またはLoadIndexレコードも	90	31

#	設定名	影響を受けるスキーマテーブル	モニターページで影響を受けるテーブルとグラフ	PREMIUMの保持日数	ADVANCEDの保持日数
		LoadIndex レコードも削除します。	削除します。		
5	GroomSummariesRetentionDays	MonitorData.DesktopGroupSummary、MonitorData.FailureLogSummary、および MonitorData.LoadIndexSummary	この設定は、トレンドページ上のすべてのグラフデータに影響します。	365	31
6	GroomMachineHotfixLogRetentionDays	MonitorData.Hotfix	この設定は、マシン詳細ページに表示されるVDAホットフィックスデータに影響します。	90	31
7	GroomMinuteRetentionDays	すべてのサマリーテーブル	この設定は、トレンドページに表示される「過去2時間」の時間期間のグラフに影響します。	3	3

#	設定名	影響を受けるスキーマテーブル	モニターページで影響を受けるテーブルとグラフ	PREMIUMの保持日数	ADVANCEDの保持日数
8	GroomHourlyRetentionDays	すべてのサマリーテーブル	これは、トレンドページに表示される週次グラフに影響します。	32	31
9	GroomApplicationInstanceRetentionDays	MonitorData.ApplicationInstance	この設定は、キャパシティ管理タブのグラフとテーブル、およびトレンドページのアプリケーション使用状況テーブルに影響します。	90	該当なし
10	GroomNotificationLogRetentionDays	MonitorData.NotificationLog	この設定は、Monitorに表示されるアラートに影響します。	90	該当なし
11	GroomResourceUsageRawDataRetentionDays	MonitorData.Resourceutilization	この設定は、「履歴マシン使用率」のマシン詳細ページに表示されるCPUおよびメモリのグラフに	3	3

#	設定名	影響を受けるスキーマテーブル	モニターページで影響を受けるテーブルとグラフ	PREMIUMの保持日数	ADVANCEDの保持日数
			影響します。		
12	GroomResourceUsageMinuteDataRetentionDays	MonitorData.ResourceUtilizationSummary	この設定は、「履歴マシン使用率」のマシン詳細ページに表示される「過去2時間」の時間範囲のCPUおよびメモリのグラフに影響します。	7	7
13	GroomResourceUsageHourDataRetentionDays	MonitorData.Resourceutilizationsummary	この設定は、「履歴マシン使用率」のマシン詳細ページに表示されるCPUおよびメモリのグラフに影響します。	30	30
14	GroomResourceUsageDayDataRetentionDays	MonitorData.Resourceutilizationsummary	この設定は、トレンドページの「リソース使用率」のマシンに表示されるCPUとメモリのグラフ、および	365	31

#	設定名	影響を受けるスキーマテーブル	モニターページで影響を受けるテーブルとグラフ	PREMIUMの保持日数	ADVANCEDの保持日数
			特定の「マシン使用率」ページに影響します。		
15	GroomProcessUsageRawDataRetentionDays	MonitorData.ProcessUtilization	この設定は、マシンの履歴使用状況ページに表示されるプロセスごとのリソース傾向情報に影響します。	1	1
16	GroomProcessUsageMinuteDataRetentionDays	MonitorData.ProcessUtilizationMinuteSummary	この設定は、履歴マシン使用率ページに表示される「過去2時間」のプロセスごとのCPUとメモリ使用量グラフに影響します。	3	3
17	GroomProcessUsageHourDataRetentionDays	MonitorData.ProcessUtilizationHourSummary	この設定は、マシンの履歴使用状況ページに表示されるプロセスごとのCPUおよびメモリ使用量の	7	7

#	設定名	影響を受けるスキーマテーブル	モニターページで影響を受けるテーブルとグラフ	PREMIUMの保持日数	ADVANCEDの保持日数
			傾向に影響します。		
18	GroomProcessUsageDayDataRetentionDays	MonitorData.ProcessUtilizationDaySummary	この設定は、マシンの履歴使用状況ページに表示されるプロセスごとのCPUおよびメモリ使用量の傾向に影響します。	30	30
19	GroomSessionMetricsDataRetentionDays	MonitorData.Sessionmetrics	この設定は、ユーザー詳細ページの「セッションパフォーマンス」タブに表示されるすべてのグラフに影響します。	1	1
20	GroomMachineMetricDataRetentionDays	MonitorData.Machinemetrics	この設定は、トレンドページの「リソース使用率」タブにあるグラフと表に影響します。	3	3

#	設定名	影響を受けるスキーマテーブル	モニターページで影響を受けるテーブルとグラフ	PREMIUMの保持日数	ADVANCEDの保持日数
21	GroomMachineMetricDaySummaryDataRetentionDays	MonitorData.MachineMetricDaySummary	この設定は、トレンドページの「リソース使用率」タブにあるグラフと表に影響します。	365	31
22	GroomApplicationErrorsRetentionDays	MonitorData.ApplicationError	この設定は、アプリケーションページの「アプリケーションエラー」列に表示されるエラー詳細に影響します。	1	1
23	GroomApplicationFaultsRetentionDays	MonitorData.Applicationfailure	この設定は、アプリケーションページの「アプリケーション障害」列に影響します。	1	1

注意:

> Monitor Serviceデータベースの値を変更した場合、新しい値を有効にするにはサービスを再起動する必要があります。Monitor Serviceデータベースへの変更は、Citrixサポートの指示の下でのみ行うことをお勧めします。

> 設定GroomProcessUsageRawDataRetentionDays、GroomResourceUsageRawDataRetentionDays、およびGroomSessionMetricsDataRetentionDaysはデフォルト値の1に制限されており、GroomProcessUsageMinuteDataRetentionDaysはデフォルト値の3に制限されています。プロセス使用状況データは急速に増加する傾向があるため、これらの値を設定するPowerShellコマンドは無効になっています。 また、ライセンスベースの保持設定は次のとおりです。

- **Premiumライセンスサイト -** すべての設定のグルーミング保持期間は1000日（Citrixは365日を推奨）に制限されています。
- **Advancedライセンスサイト -** すべての設定のグルーミング保持期間は31日に制限されています。
- **その他のすべてのサイト -** すべての設定のグルーミング保持期間は7日に制限されています。

例外:

- GroomApplicationInstanceRetentionDays は、Premiumライセンスサイトでのみ設定できます。
- GroomApplicationErrorsRetentionDays および GroomApplicationFaultsRetentionDays は、Premiumライセンスサイトでは31日間に制限されます。

長期間データを保持すると、テーブルサイズに以下の影響があります:

- **時間単位のデータ。** 時間単位のデータが最大2年間データベースに残ることを許可すると、1000のデリバリーグループを持つサイトでは、データベースが次のように増加する可能性があります:

  1000のデリバリーグループ x 24時間/日 x 365日/年 x 2年 = 17,520,000行のデータ。集計テーブル内のこれほど大量のデータがパフォーマンスに与える影響は甚大です。ダッシュボードデータはこのテーブルから取得されるため、データベースサーバーへの要件は大きくなる可能性があります。過度に大量のデータは、パフォーマンスに劇的な影響を与える可能性があります。

- **セッションおよびイベントデータ。** セッションが開始され、接続/再接続が行われるたびに収集されるデータです。大規模なサイト（10万ユーザー）の場合、このデータは急速に増加しま

す。たとえば、これらのテーブルの2年分のデータは1TBを超えるデータとなり、ハイエンドのエンタープライズレベルのデータベースが必要になります。

Citrix Director の障害理由とトラブルシューティング

以下の表は、さまざまな障害カテゴリ、その理由、および問題を解決するために必要なアクションについて説明しています。詳細については、「列挙型、エラーコード、および説明」を参照してください。

接続障害エラー

カテゴリ	理由	問題	アクション
該当なし	[0] 不明。このエラーコードはマッピングされていません。	監視サービスは、ブローカリングサービスから共有された情報から、報告された起動または接続障害の理由を判断できません。	コントローラーでCDFログを収集し、Citrixサポートに連絡してください。
[0] なし	[1] なし	なし	該当なし
[2] MachineFailure	[2] SessionPreparation	デリバリーコントローラーからVDAへのセッション準備要求が失敗しました。考えられる原因：コントローラーとVDA間の通信の問題、Broker Serviceが準備要求を作成する際に発生した問題、またはVDAが要求を受け入れない原因となるネットワークの問題。	コントローラーとVDA間の通信問題を引き起こす一般的な問題については、ナレッジセンターの記事「Citrix Virtual Apps and Desktops におけるデリバリーコントローラーへの Virtual Delivery Agent登録のトラブルシューティング」に記載されているトラブルシューティング手順を参照してください。
[2] MachineFailure	[3] RegistrationTimeout	VDAは電源がオンになっていましたが、	Citrix Broker Service がデリバリーコント

カテゴリ	理由	問題	アクション
		デリバリーコントローラーへの登録中にタイムアウトが発生しました。	ローラーで実行されていること、およびDesktopサービスがVDAで実行されていることを確認します。停止している場合は、それぞれを開始します。
[1] クライアント接続の失敗	[4] ConnectionTimeout	セッション起動のためにVDAが準備された後、クライアントがVDAに接続しませんでした。セッションは正常に仲介されましたが、クライアントがVDAに接続するのを待っている間にタイムアウトが発生しました。考えられる原因：ファイアウォール設定、ネットワーク中断、またはリモート接続を妨げる設定。	Directorコンソールで、クライアントが現在アクティブな接続を持っているかどうかを確認します。アクティブな接続がある場合、ユーザーは影響を受けていません。セッションが存在しない場合は、クライアントとVDAのイベントログでエラーを確認します。クライアントとVDA間のネットワーク接続に関する問題を解決します。
[4] 利用可能なライセンスなし	[5] ライセンス	ライセンス要求が失敗しました。考えられる原因：ライセンス数が不足しているか、ライセンスサーバーが30日以上ダウンしている。	ライセンスサーバーがオンラインで到達可能であることを確認します。ライセンスサーバーへのネットワーク接続の問題を解決するか、ライセンスサーバーが誤動作しているように見える場合は再起動します。環境内に十分なライセンスがあることを確認し、必

カテゴリ	理由	問題	アクション
			要に応じて追加で割り当てます。
[1] クライアント接続の失敗	[6] チケット	チケット発行中に障害が発生しました。これは、VDAへのクライアント接続が仲介された要求と一致しないことを示しています。起動要求チケットはBrokerによって準備され、ICA®ファイルで配信されます。ユーザーがセッションを起動しようとすると、VDAはICAファイル内の起動チケットをBrokerで検証します。考えられる原因：ICAファイルが破損しているか、ユーザーが不正な接続を試みている。	デリバリーグループで定義されたユーザーグループに基づいて、ユーザーがアプリケーションまたはデスクトップにアクセスできることを確認します。ユーザーにアプリケーションまたはデスクトップを再起動するよう指示し、これが一時的な問題であるかどうかを判断します。問題が再度発生する場合は、クライアントデバイスのイベントログでエラーを確認します。ユーザーが接続しようとしているVDAが登録されていることを確認します。登録されていない場合は、VDAのイベントログを確認し、登録に関する問題を解決します。
[1] クライアント接続の失敗	[7] その他	クライアントがVDAに最初に接続した後、接続シーケンスを完了する前に、セッションがVDAから終了したと報告されました。	起動前にユーザーによってセッションが終了されなかったことを確認します。セッションを再起動してみてください。問題が解決しない場合は、CDFログを収集してCitrixサポート

カテゴリ	理由	問題	アクション
			に連絡してください。
[1] クライアント接続の失敗	[8] 一般的な失敗	セッションの起動に失敗しました。考えられる原因：ブローカーが起動中または初期化中にブローカーによる起動が要求されたか、起動のブローカー処理フェーズ中に内部エラーが発生しました。	Citrix Broker Serviceが実行されていることを確認し、セッションの起動を再試行してください。
[5] 構成	[9] メンテナンスモード	VDA、またはVDAが属するデリバリーグループがメンテナンスモードに設定されています。	メンテナンスモードが必要かどうかを判断します。不要な場合は、該当するデリバリーグループまたはマシンでメンテナンスモードを無効にし、ユーザーに再接続を試みるよう指示してください。
[5] 構成	[10] アプリケーション無効	アプリケーションは管理者によって無効にされているため、エンドユーザーはアクセスできません。	アプリケーションが本番環境で使用されることを意図している場合は、アプリケーションを有効にし、ユーザーに再接続するよう指示してください。
[4] 利用可能なライセンスなし	[11] ライセンス機能が拒否されました	使用されている機能は、既存のライセンスではカバーされていません。	既存のCitrix Virtual Apps and Desktops™ライセンスのエディションとタイプでカバーされている機能を確認す

カテゴリ	理由	問題	アクション
			るには、Citrixの営業担当者にお問い合わせください。
[3] NoCapacityAvailable	[13] セッション制限に達しました	すべてのVDAが使用中で、これ以上セッションをホストする容量がありません。考えられる原因: すべてのVDAが使用中である（シングルセッションOS VDAの場合）、またはすべてのVDAが構成された最大同時セッション数に達している（マルチセッションOS VDAの場合）。	メンテナンスモードのVDAがないか確認してください。より多くの容量を解放するために不要な場合は、メンテナンスモードを無効にしてください。サーバーVDAあたりのセッション数を増やすには、Citrixポリシー設定の**最大セッション数**の値を増やすことを検討してください。マルチセッションOS VDAを追加することを検討してください。シングルセッションOS VDAを追加することを検討してください。
[5] 構成	[14] 許可されていないプロトコル	ICAおよびRDPプロトコルは許可されていません。	デリバリーコントローラーで**Get-BrokerAccessPolicyRule** PowerShellコマンドを実行し、**AllowedProtocols**の値に目的のプロトコルがすべてリストされていることを確認してください。この問題は、構成ミスがある場合にのみ発生します。

カテゴリ	理由	問題	アクション
[5] 構成	[15] リソースが利用できません	ユーザーが接続しようとしているアプリケーションまたはデスクトップが利用できません。このアプリケーションまたはデスクトップが存在しないか、実行できるVDAがありません。考えられる原因: アプリケーションまたはデスクトップが非公開になっている、アプリケーションまたはデスクトップをホストしているVDAが最大負荷に達している、またはアプリケーションまたはデスクトップがメンテナンスモードに設定されている。	アプリケーションまたはデスクトップがまだ公開されており、VDAがメンテナンスモードではないことを確認してください。マルチセッションOS VDAがフルロード状態であるかどうかを判断してください。もしそうであれば、より多くのマルチセッションOS VDAをプロビジョニングしてください。接続に利用可能なシングルセッションOS VDAがあることを確認してください。必要に応じて、より多くのシングルセッションOS VDAをプロビジョニングしてください。
[5] 構成	[16] ActiveSessionReconnectDisabled	ICAセッションはアクティブで、別のエンドポイントに接続されています。ただし、**アクティブセッションの再接続**が無効になっているため、クライアントはアクティブなセッションに接続できません。	デリバリーコントローラーで、**アクティブセッションの再接続**が有効になっていることを確認します。レジストリの **HKEY_LOCAL_MACHINE\Software\Citrix\Desktop\Server** にある **DisableActiveSessionReconnect**の値が0に設定されていることを確認します。

カテゴリ	理由	問題	アクション
[2] MachineFailure	[17] NoSessionToReconnect	クライアントは特定のセッションへの再接続を試みましたが、セッションは終了しました。	ワークスペースコントロールの再接続を再試行してください。
[2] MachineFailure	[18] SpinUpFailed	セッション起動のためにVDAの電源をオンにできません。これはハイパーバイザーによって報告された問題です。	マシンがまだ電源オフの状態である場合は、Citrix Studioからマシンの起動を試行します。これが失敗する場合は、ハイパーバイザーの接続と権限を確認します。VDAがPVSプロビジョニングされたマシンの場合は、PVSコンソールでマシンが実行されていることを確認します。実行されていない場合は、マシンにパーソナルvDiskが割り当てられていることを確認し、ハイパーバイザーにログインしてVMをリセットします。
[2] MachineFailure	[19] 拒否	デリバリーコントローラーは、エンドユーザーからの接続に備えるようVDAに要求を送信しますが、VDAはこの要求を積極的に拒否します。	pingで、デリバリーコントローラーとVDAが正常に通信できることを確認します。できない場合は、ファイアウォールまたはネットワークルーティングの問題を解決してください。

カテゴリ	理由	問題	アクション
[2] MachineFailure	[20] 構成セットの失敗	セッション起動中に、デリバリーコントローラーがポリシー設定やセッション情報などの必要な構成データをVDAに送信しませんでした。考えられる原因としては、コントローラーとVDA間の通信の問題、構成セット要求の作成中にBroker Serviceで発生した問題、またはVDAが要求を受け入れない原因となるネットワークの問題が挙げられます。	-
[3] NoCapacityAvailable	[21] 最大インスタンス数を超過	アプリケーションの最大インスタンス数に達しました。VDA上でアプリケーションの追加インスタンスを開くことはできません。この問題は、アプリケーション制限機能に関連しています。	ライセンスが許す場合、アプリケーション設定の「**同時に実行するインスタンス数を制限する**」をより高い値に増やすことを検討してください。
[3] NoCapacityAvailable	[22] ユーザーごとの最大インスタンス数を超過	ユーザーがアプリケーションの複数のインスタンスを開こうとしていますが、アプリケーションはユーザーごとに1つのインスタンスのみを許可するように構成されています。この問題は、アプリ	デフォルトでは、ユーザーごとにアプリケーションのインスタンスは1つのみ許可されています。ユーザーごとに複数のインスタンスが必要な場合は、アプリケーション設定で「**ユーザーごとに1つのインスタンスに**

カテゴリ	理由	問題	アクション
		ケーション制限機能に関連しています。	**制限する**」設定をクリアすることを検討してください。
[1] クライアント接続の失敗	[23] 通信エラー	デリバリーコントローラーは、接続の準備を要求するなどの情報をVDAに送信しようとしましたが、通信中にエラーが発生しました。これはネットワークの中断が原因である可能性があります。	すでに開始されている場合は、VDA上のデスクトップサービスを再起動して登録プロセスを再開し、VDAが正常に登録されていることを確認します。アプリケーションイベントログの詳細を通じて、VDA用に構成されているデリバリーコントローラーが正確であることを確認します。
[3] NoCapacityAvailable	[100] NoMachineAvailable 監視サービスは、[12] NoDesktopAvailable をこのエラーコードに変換します。	セッションを起動するために割り当てられたVDAが無効な状態であるか、利用できません。考えられる原因：VDAの電源状態が不明または利用できない、前回のユーザーセッション以降VDAが再起動されていない、現在のセッションでセッション共有が必要なのに無効になっている、またはVDAがデリバリーグループまたはサイトから削除された。	VDAがデリバリーグループ内にあることを確認します。ない場合は、適切なデリバリーグループに追加します。公開された共有デスクトップまたはユーザーが要求したアプリケーションを起動できるように、十分なVDAが登録され、準備状態にあることを確認します。VDAをホストしているハイパーバイザーがメンテナンスモードではないことを確認します。
[2] MachineFailure	[101] MachineNotFunction	VDAが動作していません。考えられる原	VDAがデリバリーグループ内にあること

カテゴリ	理由	問題	アクション
	al。監視サービスは、[12] NoDesktopAvailableをこのエラーコードに変換します。	因：VDAがデリバリーグループから削除された、VDAが未登録である、VDAの電源状態が利用できない、またはVDAが内部的な問題を抱えている。	を確認します。ない場合は、適切なデリバリーグループに追加します。VDAがCitrix Studioで電源オンとして表示されていることを確認します。複数のマシンの電源状態が不明な場合は、ハイパーバイザーへの接続に関する問題またはホストの障害を解決します。VDAをホストしているハイパーバイザーがメンテナンスモードではないことを確認します。これらの問題が解決されたら、VDAを再起動します。

マシン障害の種類

エラーコード	エラーコードID	問題	アクション
不明	-	-	-
未登録	3	-	-
最大容量（Directorでは最大負荷として表示）	4	マシンが最大容量、つまり最大負荷インデックスを報告しています	すべてのハイパーバイザーの電源がオンになっていることを確認します。ハイパーバイザーの容量を増やすか、ハイパーバイザーを追加することで、影響を受けるデリバリーグ

エラーコード	エラーコードID	問題	アクション
			ループにマシンを追加します。
StuckOnBoot	2	VMが起動シーケンスを完了せず、ハイパーバイザーと通信していません。	VMがハイパーバイザー上で正常に起動したことを確認します。OSの問題など、VM上の他のメッセージを確認します。ハイパーバイザーツールがVMにインストールされていることを確認します。VDAがVMにインストールされていることを確認します。
FailedToStart	1	VMがハイパーバイザー上で起動しようとしたときに問題が発生しました。	ハイパーバイザーのログを確認します。
なし	0	-	-

マシンの登録解除理由 (障害の種類が「未登録」または「不明」の場合に適用)

エラーコード	エラーコードID	問題	アクション
AgentShutdown	0	VDAは正常にシャットダウンされました。	既存の電源管理ポリシーに基づいてVDAがオフになっていると想定されない場合は、VDAの電源をオンにします。イベントログのエラーを確認します。

エラーコード	エラーコードID	問題	アクション
AgentSuspended	1	VDAは休止状態またはスリープモードです。	VDAを休止状態から復帰させます。電源設定を介してCitrix Virtual Apps and Desktops VDAの休止状態を無効にすることを検討してください。
IncompatibleVersion	100	Citrixプロトコルバージョンの不一致により、VDAはデリバリーコントローラーと通信できません。	VDAとデリバリーコントローラーのバージョンを合わせてください。
AgentAddressResolutionFailed	101	デリバリーコントローラーはVDAのIPアドレスを解決できませんでした。	VDAマシンアカウントがADに存在することを確認します。存在しない場合は、作成します。DNS内のVDAの名前とIPアドレスが正確であることを確認します。正確でない場合は、修正します。広範囲にわたる場合は、デリバリーコントローラーのDNS設定を検証します。コントローラーから `nslookup` コマンドを実行してDNS解決を確認します。
[Cloud]:AgentAddressResolutionFailed	101	デリバリーコントローラーはVDAのIPアドレスを解決できませんでした。	VDAマシンアカウントがADに存在することを確認します。存在しない場合は、作成します。DNS内のVDAの名前とIPアドレスが正確であるこ

エラーコード	エラーコードID	問題	アクション
			とを確認します。正確でない場合は、修正します。
AgentNotContactable	102	デリバリーコントローラーとVDA間で通信の問題が発生しました。	pingを使用して、デリバリーコントローラーとVDAが正常に通信できることを確認します。通信できない場合は、ファイアウォールまたはネットワークの問題を解決してください。コントローラーとVDA間の通信問題を引き起こす一般的な問題については、Knowledge Centerの記事「Troubleshooting Virtual Delivery Agent Registration with delivery controllers in Citrix Virtual Apps and Desktops (CTX136668)」に記載されているトラブルシューティング手順を参照してください。
[Cloud]: AgentNotContactable	102	デリバリーコントローラーとVDA間で通信の問題が発生しました。	コントローラーとVDA間の通信問題を引き起こす一般的な問題については、Knowledge Centerの記事「Troubleshooting Virtual Delivery Agent Registration

エラーコード	エラーコードID	問題	アクション
			with delivery controllers in Citrix Virtual Apps and Desktops (CTX136668)」に記載されているトラブルシューティング手順を参照してください。Citrixサポートに連絡してください。
AgentWrongActiveDirectoryOU	103	Active Directoryの検出設定が誤っています。VDAレジストリで構成されているサイト固有のOU（サイトコントローラー情報がADに保存されている場所）が、別のサイト用です。	Active Directoryの設定が正しいことを確認するか、レジストリ設定を確認してください。
EmptyRegistrationRequest	104	VDAからデリバリーコントローラーに送信された登録要求が空でした。これは、VDAソフトウェアのインストールが破損していることが原因である可能性があります。	VDA上のDesktopサービスを再起動して、登録プロセスを再開し、アプリケーションイベントログを介してVDAが正しく登録されていることを確認してください。
MissingRegistrationCapabilities	105	VDAのバージョンがデリバリーコントローラーと互換性がありません。	VDAをアップグレードするか、VDAを削除してから再インストールしてください。
MissingAgentVersion	106	VDAのバージョンがデリバリーコントローラーと互換性がありません。	問題がすべてのマシンに影響している場合は、VDAソフトウェアを再インス

エラーコード	エラーコードID	問題	アクション
			トールしてください。
InconsistentRegistrationCapabilities	107	VDAはBrokerにその機能を通知できません。これは、VDAとデリバリーコントローラーのバージョン間の非互換性が原因である可能性があります。バージョンごとに変更される登録機能は、登録要求と一致しない形式で表現されています。	VDAとデリバリーコントローラーのバージョンを合わせてください。
NotLicensedForFeature	108	使用しようとしている機能はライセンスされていません。	Citrixライセンスエディションを確認するか、VDAを削除してから再インストールしてください。
[Cloud]: NotLicensedForFeature	108	使用しようとしている機能はライセンスされていません。	Citrixサポートにお問い合わせください。
サポートされていないCredentialSecurityバージョン	109	VDAとデリバリーコントローラーが同じ暗号化メカニズムを使用していません。	VDAとデリバリーコントローラーのバージョンを合わせてください。
無効な登録リクエスト	110	VDAがブローカーに登録リクエストを行いましたが、リクエストの内容が破損しているか無効です。	コントローラーとVDA間の通信問題を引き起こす一般的な問題については、Knowledge Centerの記事「Troubleshooting Virtual Delivery Agent Registration with delivery controllers in Citrix

エラーコード	エラーコードID	問題	アクション
			Virtual Apps and Desktops (CTX136668)」に記載されているトラブルシューティング手順を参照してください。
シングル/マルチセッションの不一致	111	VDAのオペレーティングシステムタイプは、マシンカタログまたはデリバリーグループと互換性がありません。	VDAを、適切なマシンカタログタイプまたは同じオペレーティングシステムを持つマシンを含むデリバリーグループに追加してください。
FunctionalLevelTooLowForCatalog	112	マシンカタログは、インストールされているVDAバージョンよりも高いVDA機能レベルに設定されています。	VDAのマシンカタログ機能レベルがVDAの機能レベルと一致していることを確認してください。マシンカタログをVDAの機能レベルに合わせてアップグレードまたはダウングレードしてください。
FunctionalLevelTooLowForDesktopGroup	113	デリバリーグループは、インストールされているVDAバージョンよりも高いVDA機能レベルに設定されています。	VDAのデリバリーグループ機能レベルがVDAの機能レベルと一致していることを確認してください。マシンカタログをVDAの機能レベルに合わせてアップグレードまたはダウングレードしてください。

エラーコード	エラーコードID	問題	アクション
PowerOff	200	VDAが正常にシャットダウンされませんでした。	VDAが電源オン状態であるべき場合は、Citrix StudioからVDAの起動を試み、VDAが正常に起動して登録されることを確認してください。起動または登録に関する問題があればトラブルシューティングを行ってください。VDAが再び稼働したら、イベントログを確認してシャットダウンの根本原因を特定するのに役立ててください。
AgentRejectedSettingsUpdate	203	Citrixポリシーなどの設定が変更または更新されましたが、VDAへの更新の送信中にエラーが発生しました。これは、更新がインストールされているVDAバージョンと互換性がない場合に発生する可能性があります。	必要に応じてVDAをアップグレードしてください。適用された更新がVDAバージョンでサポートされているかどうかを確認してください。
SessionPrepareFailure	206	ブローカーは、VDAで実行されているセッションの監査を完了しませんでした。	広範囲にわたる場合は、デリバリーコントローラーでCitrix Broker Serviceを再起動してください。
[Cloud]: SessionPrepareFailure	206	ブローカーは、VDAで実行されているセッションの監査を	Citrixサポートにお問い合わせください。

エラーコード	エラーコードID	問題	アクション
		完了しませんでした。	
ContactLost	207	デリバリーコントローラーがVDAとの接続を失いました。これはネットワーク障害が原因である可能性があります。	デリバリーコントローラーでCitrix Broker Serviceが実行されており、VDAでDesktop Serviceが実行されていることを確認します。停止している場合は、それぞれを開始します。すでに開始されている場合は、VDAでDesktop Serviceを再起動して登録プロセスを再開し、VDAが正常に登録されることを確認します。アプリケーションイベントログの詳細を通じて、VDA用に構成されているデリバリーコントローラーが正確であることを確認します。pingを使用して、デリバリーコントローラーとVDAが正常に通信できることを確認します。通信できない場合は、ファイアウォールまたはネットワークの問題を解決します。
[Cloud]: ContactLost	207	デリバリーコントローラーがVDAとの接続を失いました。これはネットワーク	VDAでDesktop Serviceが実行されていることを確認します。停止している場合は開始します。

エラーコード	エラーコードID	問題	アクション
		障害が原因である可能性があります。	
BrokerRegistrationLimitReached	301	デリバリーコントローラーが、同時に登録できるVDAの構成済み最大数に達しました。デフォルトでは、デリバリーコントローラーは10,000の同時VDA登録を許可します。	サイトにデリバリーコントローラーを追加するか、サイトを作成することを検討してください。また、**HKEY_LOCAL_MACHINE\Software\Citrix\DesktopServer\MaxWorkers** レジストリキーを使用して、デリバリーコントローラーに同時に登録できるVDAの数を増やすこともできます。詳細については、Knowledge Centerの記事「Citrix Virtual Apps and Desktops で使用されるレジストリキーエントリ (CTX117446)」を参照してください。この数を増やすと、コントローラーにより多くのCPUおよびメモリリソースが必要になる場合があります。
SettingsCreationFailure	208	ブローカーがVDAに送信する設定と構成のセットを構築しませんでした。ブローカーがデータを収集できない場合、登録は失敗し、VDAは登録解除されます。	デリバリーコントローラーのイベントログでエラーを確認してください。ログに特定の問題が明らかでない場合は、ブローカーサービスを再起動してくださ

エラーコード	エラーコードID	問題	アクション
			い。ブローカーサービスが再起動されたら、影響を受けるVDAでデスクトップサービスを再起動し、それらが正常に登録されることを確認してください。
[Cloud]: SettingsCreationFailure	208	ブローカーがVDAに送信する設定と構成のセットを構築しませんでした。ブローカーがデータを収集できない場合、登録は失敗し、VDAは登録解除されます。	影響を受けるVDAでデスクトップサービスを再起動し、それらが正常に登録されることを確認してください。Citrixサポートに連絡してください。
SendSettingsFailure	204	ブローカーが設定および構成データをVDAに送信しませんでした。ブローカーがデータを収集できるが送信できない場合、登録は失敗します。	単一のVDAに限定される場合は、VDA上のデスクトップサービスを再起動して再登録を強制し、アプリケーションイベントログを介してVDAが正常に登録されることを検証してください。発生したエラーをトラブルシューティングしてください。コントローラーとVDA間の通信問題を引き起こす一般的な問題については、Knowledge Centerの記事「Citrix Virtual Apps and Desktops でのデリバリーコントローラーとのVirtual Delivery Agent登録のトラブ

エラーコード	エラーコードID	問題	アクション
			ルシューティング (CTX136668)」に記載されているトラブルシューティング手順を参照してください。
エージェント要求	2	不明なエラーが発生しました。	Citrixサポートにお問い合わせください。
デスクトップの再起動	201	不明なエラーが発生しました。	Citrixサポートにお問い合わせください。
デスクトップが削除されました	202	不明なエラーが発生しました。	Citrixサポートにお問い合わせください。
セッション監査の失敗	205	不明なエラーが発生しました。	Citrixサポートにお問い合わせください。
UnknownError	300	不明なエラーが発生しました。	Citrixサポートにお問い合わせください。
RegistrationStateMismatch	302	不明なエラーが発生しました。	Citrixサポートにお問い合わせください。
不明	-	不明なエラーが発生しました。	Citrixサポートにお問い合わせください。

Secure Private Access と Director の統合 (プレビュー)

Secure Private Access と Director の統合により、ヘルプデスク管理者または完全な管理者は、Director 内のすべての Secure Private Access セッションを監視およびトラブルシューティングできます。この機能をサポートするには、Director、Secure Private Access、Citrix Workspace™ app、および VDA のバージョン 2402 以降を使用する必要があります。

利用可能なアクションには、以下の詳細の表示が含まれます。

- **セッションの選択**ポップアップ > **セッション**タブ > **WebアプリとSaaSアプリ**の下にあるユーザーの Secure Private Access アクティブセッション

- **セッションの選択**ポップアップ > **アクセス拒否**タブの下にある Secure Private Access の失敗またはブロックされた列挙、および失敗したアプリ起動
- アクティブなアプリ起動と失敗したアプリ起動のセッションとアプリケーションの詳細ビュー
- 失敗およびブロックされた列挙のセッションとアプリケーションの詳細ビュー

> **注：**
>
> Secure Private Access と Director の統合は、Director のフォームベース認証のみをサポートしており、統合 Windows 認証またはスマートカードベース認証はサポートしていません。

前提条件

1. この機能をサポートするには、以下を使用する必要があります。
   - Director 2402 以降のバージョン
   - Secure Private Access 2402 以降のバージョン
   - Citrix Workspace app 2402 以降のバージョン
2. 少なくとも1つの Citrix Virtual Apps and Desktops™ サイトが Director に構成されていることを確認してください。
3. Secure Private Access をセットアップする。
4. Director サーバーが Secure Private Access サーバーへのネットワーク接続を持っていることを確認してください。

   > **注：**
   >
   > Citrix Director への接続を正常に確立するには、Secure Private Access サーバーに信頼された証明書がインストールされている必要があります。

5. Director 管理者ユーザーが次の権限を持っていることを確認します。
   a. Secure Private Access 管理コンソールで、Secure Private Access のフル管理者または読み取り専用管理者。
   b. Citrix Studio コンソールで、Citrix Virtual Apps™ または Desktops のヘルプデスク、フル管理者、または読み取り専用管理者。

Director を Secure Private Access で構成する

1. Director がインストールされているマシンで、管理者としてコマンドプロンプトを開きます。
2. 次のコマンドを実行して、`DirectorConfig` ツールのパスに移動します。

```
cd c:\inetpub\wwwroot\Director\tools
```

3. Secure Private Access を構成するには、次のコマンドを実行します。

```
DirectorConfig.exe /configspa
```

4. Secure Private Access がインストールされているマシンの FQDN とポート番号を入力します。
5. Secure Private Access (サーバーまたはロードバランサー) への接続が安全であり、信頼された証明書が適用されていることを確認してください。

```
PS C:\inetpub\wwwroot\Director\tools> .\DirectorConfig.exe /configspa

 Make sure the SPA server or load balancer is reachable from this Director machine
 Enter SPA server or load balancer FQDN including port [https://spa-server.mydomain.com:4443] : https://spa1.gwonprem.corp:4443

 Checking connectivity to https://spa1.gwonprem.corp:4443

 Spa Server or load balancer: https://spa1.gwonprem.corp:4443 is reachable.

 Checking Spa Server or load balancer is valid

 Retry with correct Spa Server FQDN which is reachable

 Director configuration encountered an error


=====================================================
Spa Server or load balancer FQDN https://spa1.gwonprem.corp:4443 is either invalid or Spa server/load balancer is down
=====================================================
```

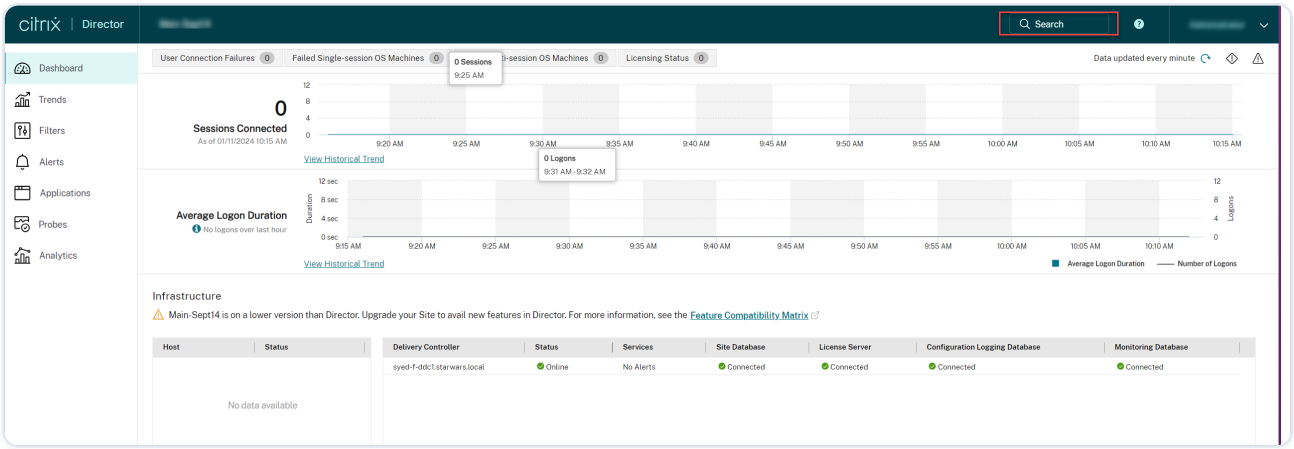
注：

Director で Secure Private Access セッションの詳細を表示するには、管理者を Secure Private Access コンソールに追加する必要があります。詳細については、「管理者の管理」を参照してください。

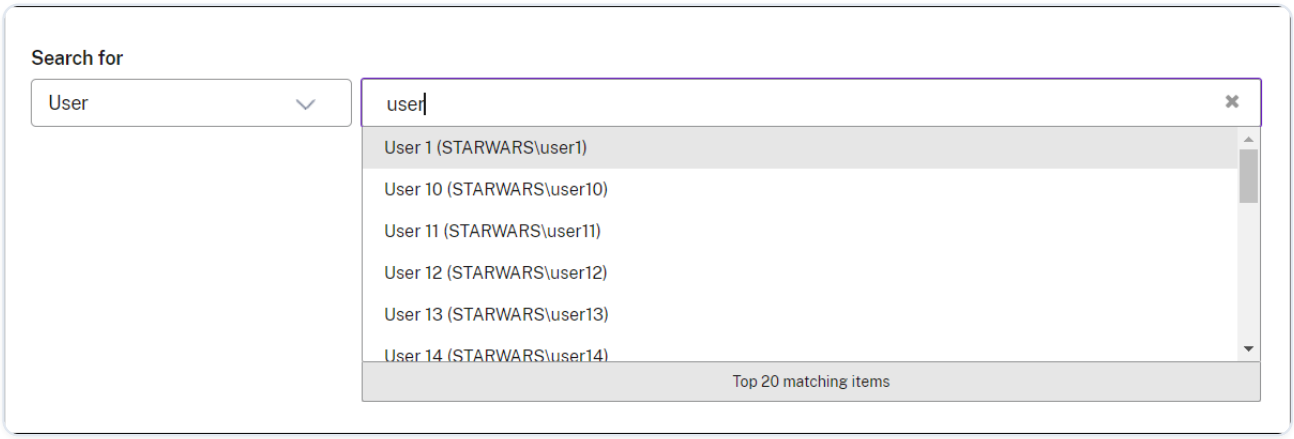
ユーザー別にSecure Private Accessセッションを表示する

Director ダッシュボードで、**「検索」をクリックし、ユーザー名を入力します。**「セッションの選択」**画面が表示されます。

フル管理者:

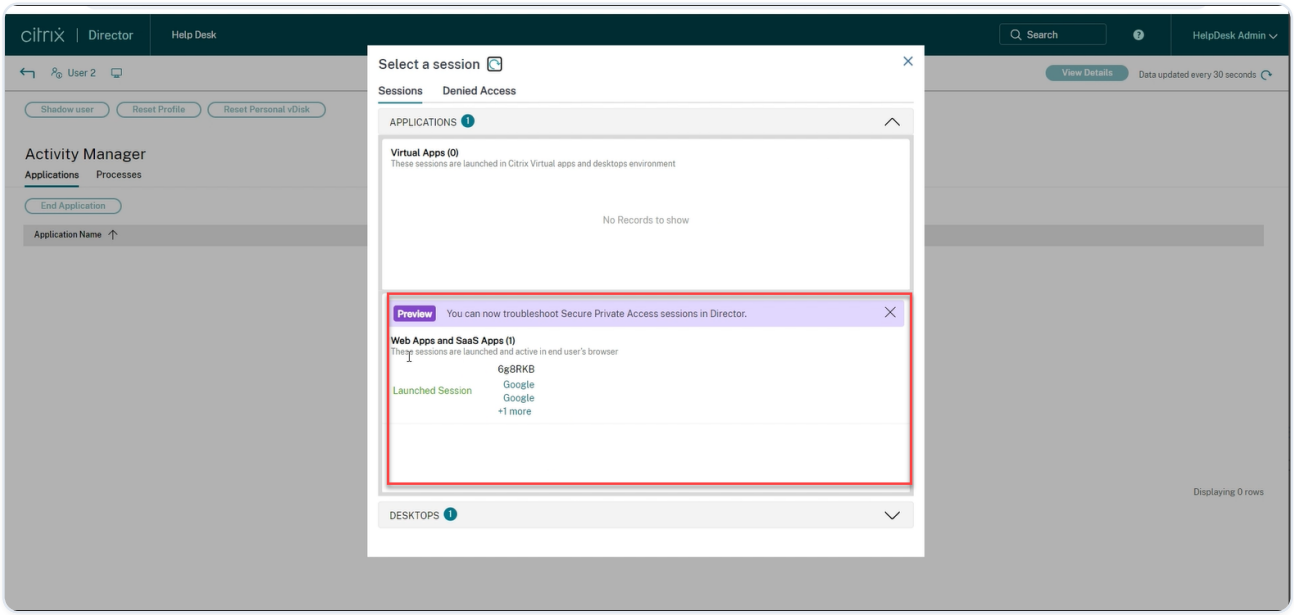


ヘルプデスク管理者:

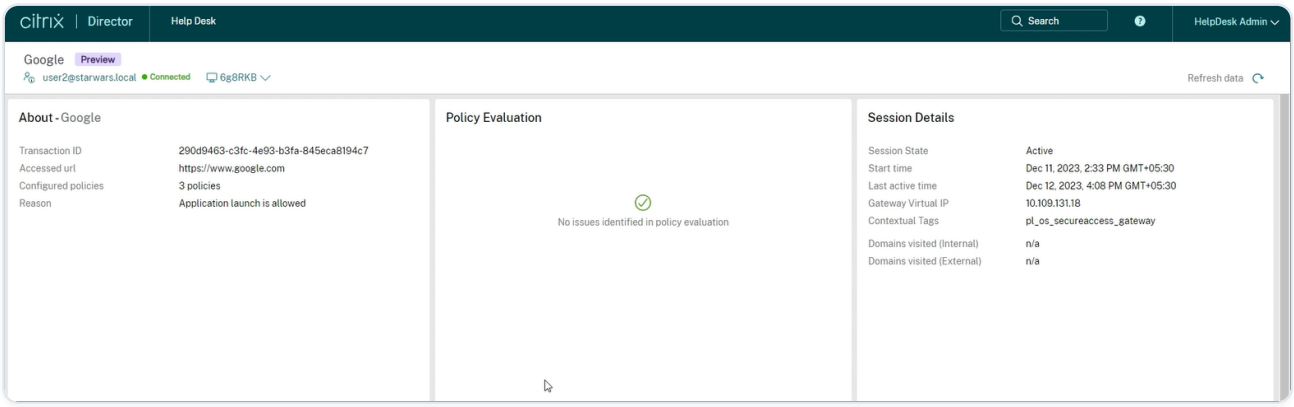


正常に起動されたWebアプリとSaaSアプリを表示する

正常に起動されたアプリは、**WebアプリとSaaSアプリ**セクションに表示されます。



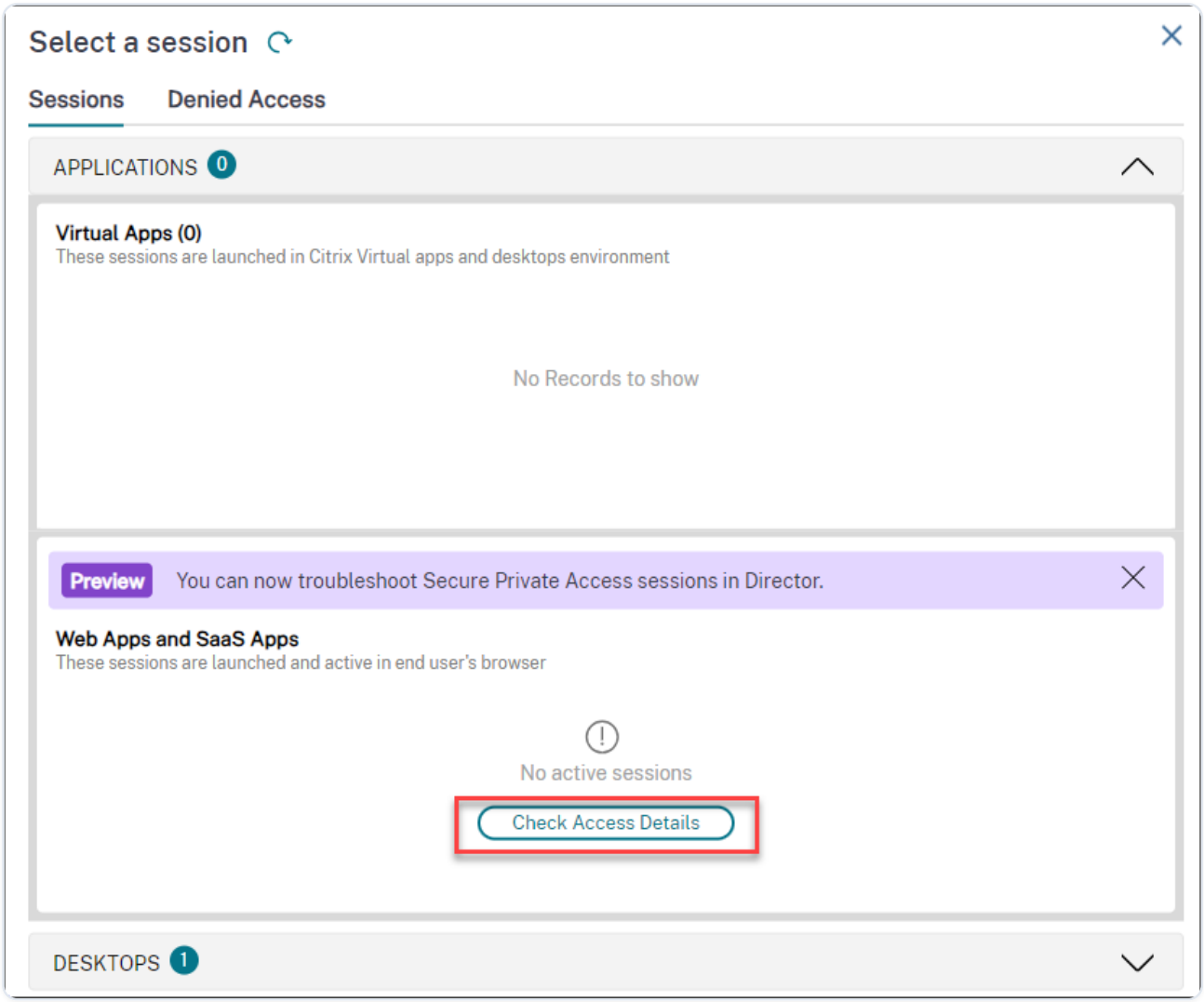
詳細を表示するには、**WebアプリとSaaSアプリ**セクションからアプリをクリックします。



成功コードの詳細については、「Citrix Director関連コード」を参照してください。

アクセスが拒否されたアプリの詳細を表示する

セッションの選択画面で、**アクセス詳細の確認**をクリックします。



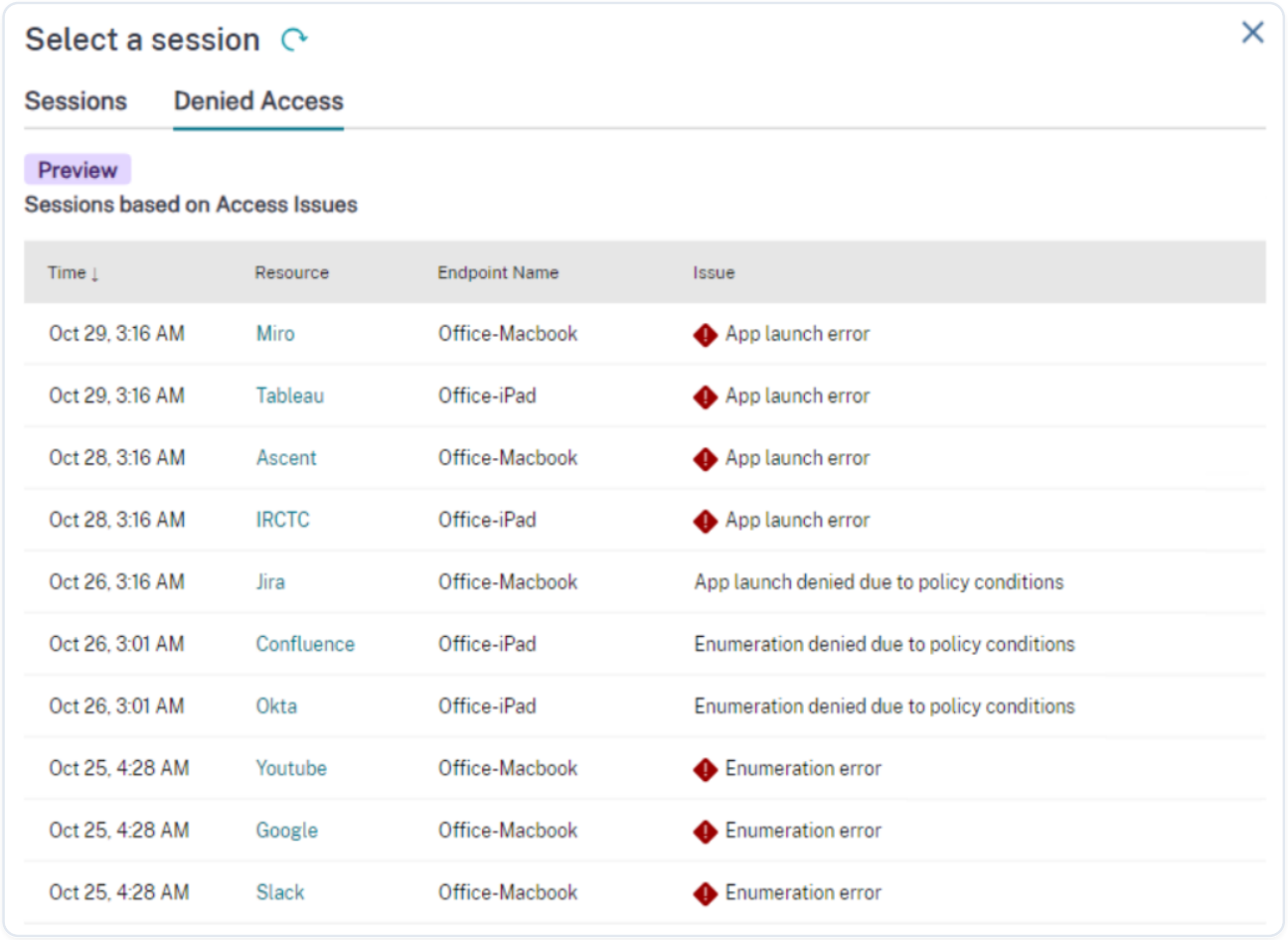
> **注：**

> **アクセス詳細の確認**ボタンは、アクティブなセッションがない場合に表示されます。

> または、,

アクセスが拒否されたアプリを表示するには、**アクセス拒否**タブをクリックします。

アクセス拒否タブが開きます。

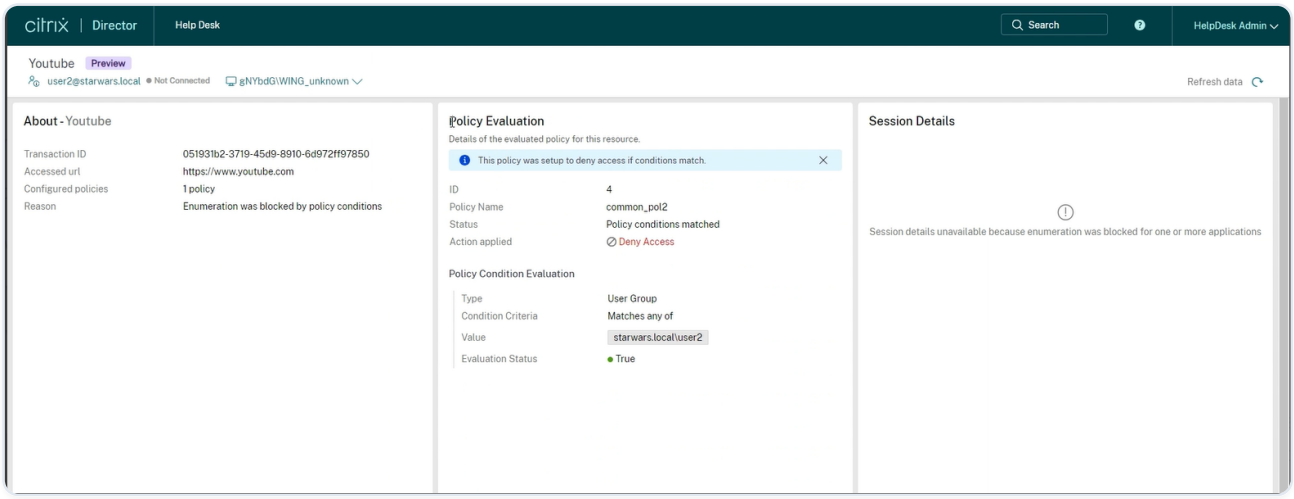


時間、リソース、エンドポイント名、失敗の理由などのセッション詳細が表示されます。エラーコードの詳細については、「Citrix Director関連コード」を参照してください。

現在、以下の問題が確認されています。

- ポリシー条件により列挙が拒否されました
- アプリの起動エラー
- 列挙エラー
- ポリシー条件によりアプリの起動が拒否されました

詳細を表示するには、**Denied Access** タブ > **Resource** 列からアプリを選択します。



成功または失敗したセッションについて、以下の詳細が表示されます。

- アプリについて
- ポリシー評価
- セッションの詳細

アプリについて

成功、失敗、または拒否されたアプリの名前が表示されます。それに加えて、成功または失敗したアプリの以下の詳細が表示されます。

フィールド	説明
トランザクションID	セッションまたは列挙中のCitrixトランザクションID。
アクセスされたURL	セッションまたは列挙中にアクセスされたURL。
構成済みポリシー	セッションまたは列挙内で使用されるポリシーの数。
理由	セッションまたは列挙アクティビティの分析。

ポリシー評価

成功したセッションの評価中に問題が検出されなかったことを表示します。失敗したセッションまたは列挙の場合、評価されたポリシーの次の詳細が表示されます。

フィールド	説明
ID	Citrix トランザクション ID。
ポリシー名	ポリシーの名前。
ステータス	ポリシーのステータス。
適用されたアクション	ポリシーに適用されたアクション。例: アクセス拒否。
ポリシー条件の評価	
タイプ	ポリシー条件の種類。
条件基準	失敗したセッションまたは列挙で適用されたポリシーの条件基準。
値	ポリシーの値。
評価ステータス	ポリシーの評価ステータス。

セッションの詳細

失敗したセッションの場合、セッション失敗の理由が表示されます。成功したセッションの場合、次の詳細が表示されます。

フィールド	説明
セッションの状態	セッションがアクティブか非アクティブか、その状態を表示します。
開始時刻	セッションの開始時刻を表示します。
最終アクティブ時刻	成功したセッションの最終アクティブ時刻を表示します。
ゲートウェイ仮想IP	正常に接続されたセッションが接続されているゲートウェイの仮想IPアドレスを表示します。
コンテキストタグ	コンテキストタグを表示します。Secure Private Accessプラグインのコンテキストタグは、認証済みユーザーのセッションに適用さ

フィールド	説明
	れるNetScaler® Gatewayポリシー（セッション、事前認証、EPA）の名前です。
アクセス済みドメイン (内部)	成功したセッションを使用してアクセスされた内部ドメインを表示します。
アクセス済みドメイン (外部)	成功したセッションを使用してアクセスされた外部ドメインを表示します。

サードパーティ通知

Citrix Virtual Apps and Desktops™ のこのリリースには、以下のドキュメントに定義されている条件に基づいてライセンスされたサードパーティ製ソフトウェアが含まれている場合があります。

- Citrix Virtual Apps and Desktops サードパーティ通知(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/downloads/third-party-notices-apps-and-desktops.pdf) (PDFダウンロード)
- FlexNet Publisher 2017 (11.15.0.0) の非商用ソフトウェア開示(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/downloads/fnp-licensing-11-15-0-ncsd-summary.pdf) (PDFダウンロード)
- FlexNet Publisher 11.15.0 で使用されている FlexNet Publisher ドキュメント補足 サードパーティおよびオープンソースソフトウェア(/ja-jp/citrix-virtual-apps-desktops/2402-ltsr/downloads/fnp-licensing-11-15-0-opensource.pdf) (PDFダウンロード)

SDKおよびAPI

このリリースでは、いくつかのSDKとAPIが利用可能です。SDKとAPIにアクセスするには、Build anything with Citrixにアクセスしてください。そこから、**Citrix Workspace**を選択して、Citrix Virtual Apps and Desktopsおよび関連コンポーネントのプログラミング情報にアクセスします。

> **注：**
>
> Citrix Virtual Apps and Desktops™ SDKとCitrix Group Policy SDKは、モジュールまたはスナップインとしてインストールできます。いくつかのコンポーネントSDK（Citrix Licensing、Citrix Provisioning、StoreFrontなど）は、スナップインのみを使用してインストールされます。

> この製品はPowerShellバージョン3から5をサポートしています。

シトリックス バーチャル アプリおよびデスクトップ SDK

このSDKは、Delivery Controller™またはStudioをインストールすると、PowerShellモジュールとして自動的にインストールされます。これにより、スナップインを追加することなく、このSDKのコマンドレットを使用できます。（このSDKをスナップインとしてインストールすることを選択した場合の指示は以下に記載されています。）

権限

Citrix管理権限を持つIDを使用してシェルまたはスクリプトを実行する必要があります。Controller上のローカル管理者グループのメンバーは、Citrix Virtual AppsまたはCitrix Virtual Desktops™をインストールするための完全な管理権限を自動的に持っていますが、Citrixは、通常の操作では、ローカル管理者アカウントを使用するのではなく、適切な権限を持つCitrix管理者を作成することを推奨します。

コマンドレットにアクセスして実行する

1. PowerShellでシェルを起動します。Studioを開き、**PowerShell**タブを選択し、**Launch PowerShell**をクリックします。

2. スクリプト内でSDKコマンドレットを使用するには、PowerShellで実行ポリシーを設定します。PowerShellの実行ポリシーについては、Microsoftのドキュメントを参照してください。
3. (モジュールではなく) スナップインを使用する場合は、`Add-PSSnapin` (または`asnp`) コマンドレットを使用してスナップインを追加します。

   V1とV2はスナップインのバージョンを示します。XenDesktop 5のスナップインはバージョン1です。Citrix Virtual Apps and Desktops、およびそれ以前のXenDesktop 7バージョンのスナップインはバージョン2です。例えば、Citrix Virtual Apps and Desktopsスナップインをインストールするには、`Add-PSSnapin Citrix.ADIdentity.Admin.V2`と入力します。すべてのコマンドレットをインポートするには、次のように入力します: `Add-PSSnapin Citrix.*.Admin.V*`

これで、コマンドレットとヘルプファイルを使用できます。

- このSDKのヘルプファイルにアクセスするには、Categoriesリストで製品またはコンポーネントを選択し、次に**Citrix Virtual Apps and Desktops SDK**を選択します。
- PowerShellのガイダンスについては、Windows PowerShell Integrated Scripting Environment (ISE)を参照してください。

グループポリシーSDK

Citrix Group Policy SDKを使用すると、グループポリシーの設定とフィルターを表示および構成できます。このSDKは、PowerShellプロバイダーを使用して、マシンおよびユーザーの設定とフィルターに対応する仮想ドライブを作成します。このプロバイダーは、`New-PSDrive`の拡張機能として表示されます。

Group Policy SDKを使用するには、StudioまたはCitrix Virtual Apps and Desktops SDKのいずれかがインストールされている必要があります。

Citrix Group Policy PowerShell プロバイダーは、モジュールまたはスナップインとして利用できます。

- モジュールを使用する場合、追加の作業は不要です。
- スナップインを追加するには、`Add-PSSnapin citrix.common.grouppolicy` と入力します。

ヘルプにアクセスするには、`help New-PSDrive -path localgpo:/` と入力します。

仮想ドライブを作成し、設定をロードするには、`New-PSDrive <Standard Parameters> [-PSProvider] CitrixGroupPolicy -Controller <string>` と入力します。ここで、Controller 文字列は、接続して設定をロードしたいサイト内の Controller の完全修飾ドメイン名です。

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

Citrix Virtual Apps and Desktops REST API を使用すると、Citrix Virtual Apps and Desktops 展開内のリソースの管理を自動化できます。

Citrix Virtual Apps and Desktops REST API は `<https://developer.cloud.com/citrixworkspace/citrix-daas-rest-apis/docs/citrix-virtual-apps-and-desktops-apis>` で利用できます。Citrix Virtual Apps and Desktops に適用されない API は、そのようにマークされています。そこにあるガイダンスに従って、API サービスへのアクセスを設定し、API を使用してリソースを管理および最適化してください。

モニターサービス OData

Monitor API を使用すると、OData API のバージョン 3 または 4 を使用して Monitor Service データにアクセスできます。Monitor Service データからクエリされたデータに基づいて、カスタマイズされた監視およびレポートダッシュボードを作成できます。OData V.4 は ASP.NET Web API に基づいており、集計クエリをサポートしています。

詳細については、Monitor Service OData API を参照してください。

__index__

サイト全体の履歴トレンドを監視する

トレンドビューは、以下のパラメータについて、各サイトの履歴トレンド情報にアクセスします。

- セッション
- 接続障害
- マシン障害
- ログオンパフォーマンス
- 負荷評価
- キャパシティ管理
- マシン使用状況
- リソース使用率
- 各サイトのネットワーク分析。

この情報を見つけるには、**トレンド**メニューをクリックします。

ズームイン ドリルダウン機能を使用すると、期間をズームイン（グラフのデータポイントをクリック）し、トレンドに関連する詳細を表示するためにドリルダウンすることで、トレンドグラフをナビゲートできます。この機能により、誰が、または何が影響を受けているかの詳細をよりよく理解できます。

各グラフのデフォルトのスコープを変更するには、データに別のフィルターを適用します。

履歴トレンド情報が必要な期間を選択してください。期間の利用可能性は、Directorの展開によって次のように異なります。

- Premiumライセンスサイトでは、最大1年間 (365日) のトレンドレポートを利用できます。
- Advancedライセンスサイトでは、最大1か月間 (31日) のトレンドレポートを利用できます。
- PremiumおよびAdvanced以外のライセンスサイトでは、最大7日間のトレンドレポートを利用できます。

> **注：**

- すべてのDirector展開において、期間が「先月」（**現在まで**）以下に設定されている場合、セッション、障害、ログオンパフォーマンスのトレンド情報はグラフとテーブルとして利用できます。期間がカスタム終了日を指定した「先月」または「昨年」として選択されている場合、トレンド情報はグラフとして利用でき、テーブルとしては利用できません。
- Monitor Serviceのグルーミング保持値によって、トレンドデータの可用性が制御されます。デフォルト値は、データ粒度と保持で確認できます。Premiumライセンスサイトのお客様は、グルーミング保持を希望する保持日数に変更できます。
- IIS Managerの以下のパラメータは、選択可能なカスタム終了日の範囲を制御します。ただし、選択された日付のデータ可用性は、測定される特定のメトリックのグルーミング保持設定によって異なります。

パラメーター	デフォルト値
UI.TrendsLast2HoursRange	3
UI.TrendsLast24HoursRange	32
UI.TrendsLast7DaysRange	32
UI.TrendsLastMonthRange	365

利用可能なトレンド

セッションの傾向を表示: 「**セッション**」タブから、デリバリーグループと期間を選択して、同時セッション数に関する詳細情報を表示します。

「**セッションの自動再接続**」列には、セッション内の自動再接続の数が表示されます。自動再接続は、セッションの信頼性ポリシーまたはクライアント自動再接続ポリシーが有効な場合に有効になります。エンドポイントでネットワークの中断が発生した場合、次のポリシーが有効になります。

- セッションの信頼性が有効になり（デフォルトで3分間）、Citrix Receiver™またはCitrix Workspace™アプリがVDAへの接続を試行します。
- クライアント自動再接続が3分から5分の間に有効になり、クライアントがVDAへの接続を試行します。

両方の再接続がキャプチャされ、ユーザーに表示されます。この情報は、再接続が発生してからDirector UIに表示されるまでに最大5分かかる場合があります。

自動再接続情報は、中断のあるネットワーク接続の表示とトラブルシューティングに役立ちます。また、シームレスなエクスペリエンスを持つネットワークも分析します。フィルターで選択した特定のデリバリーグループまたは期間の再接続数を表示できます。ドリルダウンでは、セッションの信頼性やクライアント自動再接続、タイムスタンプ、エンドポイントIP、Workspaceアプリがインストールされているマシンのエンドポイント名などの追加情報が提供されます。

デフォルトでは、ログはイベントのタイムスタンプの降順でソートされます。この機能は、Windows用Citrix Workspaceアプリ、Mac用Citrix Workspaceアプリ、Windows用Citrix Receiver、およびMac用Citrix Receiverで利用できます。この機能には、Delivery Controller™バージョン7 1906以降、およびVDA 1906以降が必要です。

セッションの再接続の詳細については、「セッション」を参照してください。

ポリシーの詳細については、「クライアント自動再接続ポリシー設定」および「セッションの信頼性ポリシー設定」を参照してください。

自動再接続データがDirectorに表示されない場合があります。その理由は次のとおりです。

- WorkspaceアプリがVDAに自動再接続データを送信していません。
- VDAがモニターサービスにデータを送信していません。
- Delivery Controllerは、対応するセッションがない可能性があるため、VDAペイロードを破棄します。

> **注：**
>
> 特定のCitrix Gatewayポリシーが設定されている場合、クライアントIPアドレスが正しく取得されないことがあります。

> **接続障害の傾向を表示:** 「障害」タブから、接続、マシンタイプ、障害タイプ、デリバリーグループ、および期間を選択して、サイト全体のユーザー接続障害に関する詳細情報を含むグラフを表示します。

マシン障害の傾向を表示: Single-session OS Machine FailuresタブまたはMulti-session OS Machinesタブから、障害タイプ、デリバリーグループ、および期間を選択すると、サイト全体のマシン障害に関する詳細情報を含むグラフが表示されます。

ログオンパフォーマンスの傾向を表示: ログオンパフォーマンスタブから、デリバリーグループと期間を選択すると、サイト全体のユーザーログオン時間の詳細情報と、ログオン数がパフォーマンスに影響するかどうかを示すグラフが表示されます。このビューには、ブローカー処理時間やVM起動時間など、ログオンフェーズの平均時間も表示されます。 このデータはユーザーログオン専用であり、切断されたセッションから再接続しようとするユーザーは含まれません。 グラフの下の表には、ユーザーセッションごとのログオン時間が表示されます。表示する列を選択し、任意の列でレポートを並べ替えることができます。 詳細については、「ユーザーログオンの問題の診断」を参照してください。

負荷評価の傾向を表示: Load Evaluator Indexタブから、Multi-session OSマシン間で分散される負荷に関する詳細情報を含むグラフを表示します。このグラフのフィルターオプションには、デリバリーグループまたはデリバリーグループ内のMulti-session OSマシン、Multi-session OSマシン（デリバリーグループ内のMulti-session OSマシンが選択されている場合にのみ利用可能）、および範囲が含まれます。

ホストされたアプリケーションの使用状況を表示: この機能の利用可能性は、組織のライセンスによって異なります。 **Capacity Management**タブから、**Hosted Applications Usage**タブを選択します。デリバリーグループと期間を選択すると、ピーク時の同時使用状況を示すグラフと、アプリケーションベースの使用状況を示す表が表示されます。Application Based Usage表から、特定のアプリケーションを選択して詳細と、そのアプリケーションを使用している、または使用したユーザーのリストを確認できます。

Single-sessionおよびMulti-session OSの使用状況を表示: トレンドビューには、サイト別およびデリバリーグループ別のSingle-session OSの使用状況が表示されます。**サイト**を選択すると、デリバリーグループごとの使用状況が表示されます。デリバリーグループを選択すると、ユーザーごとの使用状況が表示されます。 トレンドビューには、サイト別、デリバリーグループ別、およびマシン別のMulti-session OSの使用状況も表示されます。**サイト**を選択すると、デリバリーグループごとの使用状況が表示されます。デリバリーグループを選択すると、マシンごとおよびユーザーごとの使用状況が表示されます。マシンが選択されている場合は、ユーザーごとの使用状況が表示されます。

仮想マシンの使用状況を表示: マシン使用状況タブから、**シングルセッションOSマシンまたはマルチセッションOSマシン**を選択すると、VMの使用状況をリアルタイムで確認でき、サイトのキャパシティニーズを迅速に評価できます。 シングルセッションOSの可用性 - サイト全体または特定のデリバリーグループにおけるシングルセッションOSマシン（VDI）の可用性による現在の状態を表示します。 マルチセッションOSの可用性 - サイト全体または特定のデリバリーグループにおけるマルチセッションOSマシンの可用性による現在の状態を表示します。

注: 利用可能なカウンターに表示されるマシンの数には、メンテナンスモードのマシンが含まれます。

リソース使用率の表示: リソース使用率タブから、**シングルセッションOSマシンまたはマルチセッションOSマシン**を選択すると、CPUおよびメモリ使用量、IOPS、各VDIマシンのディスク待機時間に関する履歴トレンドデータを確認でき、より適切なキャパシティプランニングに役立ちます。 この機能には、Delivery ControllerおよびVDAの**バージョン7.11**以降が必要です。 グラフには、平均CPU、平均メモリ、平均IOPS、ディスク待機時間、ピーク時の同時セッションのデータが表示されます。マシンにドリルダウンして、CPUを消費している上位10個のプロセスのデータとグラフを表示できます。

デリバリーグループと期間でフィルターします。CPU、メモリ使用量、およびピーク時の同時セッションのグラフは、過去2時間、24時間、7日間、1か月、1年間で利用できます。平均IOPSとディスク遅延のグラフは、過去24時間、1か月、1年間で利用できます。

注：

- 履歴マシン使用率ページの「上位10プロセス」テーブルでデータを収集して表示するには、監視ポリシー設定の**プロセス監視を有効にする**を**許可**に設定する必要があります。このポリシーは、デフォルトで**禁止**に設定されています。すべてのリソース使用率データはデフォルトで収集されます。これは、**リソース監視を有効にする**ポリシー設定を使用して無効にできます。グラフの下のテーブルには、マシンごとのリソース使用率データが表示されます。詳細については、「監視ポリシー設定」を参照してください。
- 平均IOPSは日次平均を示します。ピークIOPSは、選択した期間のIOPS平均の最高値として計算されます。（IOPS平均とは、VDAで1時間中に収集されたIOPSの時間平均です）。
- マシンのドリルダウンでは、平均CPUまたは平均メモリ使用量が1%を超えるプロセスが一覧表示されます。これは、場合によっては10個未満のプロセスしか表示されない可能性があることを意味します。

ネットワーク分析データの表示: この機能の可用性は、組織のライセンスと管理者権限によって異なります。この機能には、Delivery Controllerの**バージョン7.11**以降が必要です。

ネットワークタブから、ネットワーク分析を監視します。これにより、ネットワークのユーザー、アプリケーション、デスクトップのコンテキストビューが提供されます。この機能により、

DirectorはCitrix ADMからのHDX Insightレポートを通じて、展開におけるICAトラフィックの高度な分析を提供します。詳細については、「ネットワーク分析の構成」を参照してください。

アプリケーション障害の表示: アプリケーション障害タブには、VDA上の公開アプリケーションに関連する障害が表示されます。

この機能には、Delivery ControllerおよびVDAの**バージョン7.15**以降が必要です。Windows Vista以降を実行するシングルセッションOS VDA、およびWindows Server 2008以降を実行するマルチセッションOS VDAがサポートされています。 詳細については、「履歴アプリケーション障害監視」を参照してください。

デフォルトでは、マルチセッションOS VDAからのアプリケーション障害のみが表示されます。監視ポリシーを使用して、アプリケーション障害の監視を設定できます。詳細については、「監視ポリシー設定」を参照してください。

プローブ結果の表示: プローブ結果タブには、構成ページでプローブ用に構成されたアプリケーションおよびデスクトップのプローブ結果が表示されます。ここでは、障害が発生した起動の段階が記録されます。

詳しくは、「アプリケーションおよびデスクトップのプローブ」を参照してください。

カスタマイズされたレポートの作成: カスタムレポートタブは、監視データベースからリアルタイムおよび履歴データを表形式で含むカスタムレポートを生成するためのユーザーインターフェイスを提供します。

この機能には、Delivery Controllers **バージョン7.12**以降が必要です。

以前に保存したカスタムレポートクエリのリストから、**実行してダウンロード**をクリックしてレポートをCSV形式でエクスポートしたり、**ODataをコピー**をクリックして対応するODataクエリをコピーして共有したり、**編集**をクリックしてクエリを編集したりできます。 マシン、接続、セッション、またはアプリケーションインスタンスに基づいてカスタムレポートクエリを作成できます。マシン、デリバリーグループ、期間などのフィールドに基づいてフィルター条件を指定します。カスタムレポートに必要な追加の列を指定します。プレビューには、レポートデータのサンプルが表示されます。カスタムレポートクエリを保存すると、保存されたクエリのリストに追加されます。

コピーしたODataクエリに基づいてカスタムレポートクエリを作成できます。これを行うには、ODataクエリオプションを選択し、コピーしたODataクエリを貼り付けます。結果のクエリは後で実行するために保存できます。

注: ODataクエリを使用して生成されたプレビューおよびエクスポートレポートの列名はローカライズされておらず、英語で表示されます。

グラフ上のフラグアイコンは、特定の期間における重要なイベントまたはアクションを示します。フラグにマウスを合わせ、クリックしてイベントまたはアクションを一覧表示します。

注：

- HDX™接続ログオンデータは、7より前のVDAでは収集されません。それより前のVDAの場合、グラフデータは0と表示されます。
- Citrix Studioで削除されたデリバリーグループは、関連データが整理されるまで、Director Trendsフィルターで選択可能です。削除されたデリバリーグループを選択すると、保持期間までの利用可能なデータのグラフが表示されます。ただし、テーブルにはデータは表示されません。
- アクティブなセッションを含むマシンをあるデリバリーグループから別のデリバリーグループに移動すると、新しいデリバリーグループの**リソース使用率と負荷評価インデックス**テーブルに、古いデリバリーグループと新しいデリバリーグループから統合されたメトリックが表示されます。