シトリックス Virtual Apps and Desktops 7 2503

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

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

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

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

以前のリリース

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

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

シトリックス Cloud™ での シトリックス Virtual Apps and Desktops

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

役立つリンク

- Citrix サポート機能パック
- LTSR FAQ
- Citrix Virtual Apps and Desktops サービスオプション
- 製品ライフサイクル日付
- Citrix Workspaceアプリ向けLTSRプログラム

シトリックス Virtual Apps and Desktops™ 7 2503

リリースについて

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

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

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

インストールとアップグレードの手順：

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

サポートされているバージョンとレガシーバージョンのドキュメント

サポートされているバージョンのドキュメントは、「Citrix Virtual Apps and Desktops」にあります。

ライフサイクル終了 (EOL) バージョンのドキュメントPDFは、「レガシー ドキュメント」にアーカイブされています。

シトリックス Virtual Apps and Desktops 7 2503

仮想デリバリーエージェント (VDA)

VDAアップグレードサービス (プレビュー)

Citrix VDA Upgrade Service (VUS) は、Citrix DaaS™ 内での VDA アップグレードを効率化し、パフォーマンスとセキュリティを向上させます。管理者は VUS を使用して、更新の確認、アップグレードのスケジュール設定、進行状況の監視を行うことができ、即時またはスケジュールされた更新のオプションがあります。アップグレードトラックは2つあります。安定性重視の Long-Term Service Release (LTSR) と、最新機能重視の Current Release (CR) です。

SSO を使用した Citrix Workspace™ からのシームレスなログオン

この機能により、シングルサインオン (SSO) を使用して、Citrix Workspace から VDA 上にある Citrix Secure Access (CSA) クライアントにシームレスにログオンできます。この機能は、シングルセッション VDA とマルチセッション VDA の両方に適用されます。詳細については、「VDA 上の Citrix Secure Access クライアントからのシームレスなログオン」を参照してください。

Cloud Connector スタンドアロン Citrix Secure Ticketing Authority (STA) サービス

Citrix Workspace でオンプレミスのサイト集約を使用している場合、または StoreFront で Citrix Gateway Service を使用している場合、Cloud Connector は Citrix Virtual Apps and Desktops サイトの Secure Ticket Authority (STA) トラフィックを処理します。スタンドアロン STA サービスを使用すると、環境内の STA チケットの配信をより詳細に制御できます。詳細については、「Cloud Connector スタンドアロン Citrix Secure Ticketing Authority (STA) サービス」を参照してください。

LHC モードでの WebSocket VDA のサポート

この機能により、LHC モードでも VDA とデリバリーコントローラー間の WebSocket 接続が成功します。詳細については、「VDA とデリバリーコントローラー間の WebSocket 通信」を参照してください。

HDX

デバイス

TWAIN リダイレクトの 64 ビットアプリのサポート。HDX セッションで 64 ビットアプリケーションを使用してドキュメントをスキャンできるようになりました。

ダブルホップシナリオでの FIDO2 リダイレクトのサポート。ユーザーは、ダブルホップシナリオで FIDO2 リダイレクトを使用するアプリケーションに対して認証できるようになりました。中間ホップ VDA ホストには、Citrix Virtual Apps and Desktops 2503 がインストールされている必要があります。

FIDO2 リダイレクトを使用するカスタムアプリケーションのワイルドカード Studio ポリシーのサポート。管理者は、Studio で FIDO2 リダイレクトを使用する必要があるカスタムのセッション内アプリケーションのファイルパスを構成できるようになり、ファイルパス変数でワイルドカード文字も使用できるようになりました。

WIA リダイレクトの機能強化。管理者は、WIA リダイレクトを使用するために **Allowlist** アプリケーションにフック変更を加える必要がなくなりました。**Allowlist** レジストリにファイルパスを追加するだけで済みます。

Unicode 入力モードのサポートの強化。この機能強化により、Unicode 入力モードを使用する際の品質が大幅に向上し、より広範なキーボードレイアウトがサポートされます。

PDF 印刷エクスペリエンスの強化 。この機能強化により、PDF 印刷に関連するオプションと設定のサポートが拡張され、他の印刷形式と同等になります。

Linuxエンドポイントからのスキャンを最適化 。この機能強化により、Linuxエンドポイントからリモートセッションホストに接続する際のスキャンエクスペリエンスが向上します。

グラフィック

インテリジェントなBuild to Lossless機能。インテリジェントなBuild to Losslessは、既存のBuild to Lossless機能の強化版であり、よりスマートで効率的なエクスペリエンスを提供するように設計されています。インテリジェントなBuild to Losslessを使用すると、管理者はBuild to Losslessを手動で構成する必要がなくなり、必要なモニターのセッションに動的に自動的に適用されます。必要がなくなると、Thinwireはシームレスにこれを無効にし、最適なパフォーマンスのために通常のエンコーディングに戻ります。

HDX 接続

EDT MTU再検出。EDT MTU検出は、アクティブなセッション中にMTUの変更を検出し、必要に応じてセッションのMTU値を調整できるようになりました。詳細については、「Enlightened Data Transport」を参照してください。

EDTタイムアウト構成。Workspaceアプリの構成メカニズムが強化され、VDAからのタイムアウト設定を使用するようになりました。これにより、クライアントデバイスでタイムアウトを構成する必要がなくなります。さらに、デフォルトのEDTタイムアウトが25秒から10秒に変更され、ネットワークの中断をより迅速に検出できるようになりました。詳細については、「Configure EDT timeout」を参照してください。

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

認証済みプロキシのRendezvous V2サポート。Rendezvousは、制御トラフィックの認証済みプロキシをサポートするようになりました。詳細については、「Rendezvous V2」を参照してください。

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

マルチメディア

オーディオパフォーマンスを向上させるAudio Quality Enhancerを有効にする 。バージョン2503以降、Adaptive AudioにAudio Quality Enhancer (v1) が追加されました。

Audio Quality Enhancerは、以前のサンプルからオーディオをインテリジェントに再構築することで、短期間のパケット損失や中断を効果的に管理し、品質の著しい低下を防ぎます。Audio Quality Enhancerは、良好なネットワーク条件と不良なネットワーク条件の両方で、オーディオ再生と録音の品質を最適化します。

Browser Content Redirectionにおけるブラウザプロファイル共有 。Browser Content Redirection (BCR) は、新しいプロファイル共有機能により、VDA側の認証とCookie共有を可能にし、合理化されたユーザーエクスペリエンスを提供します。この機能強化により、冗長なログインが不要になり、BCRウィンドウが閉じられた後でもBCRセッション全体で認証とCookieの永続性を維持することで生産性が向上します。このシームレスなエクスペリエンスは、認証がクライアントではなくVDAから行われることを保証することで、セキュリティをさらに強化します。

例:

- **以前のエクスペリエンス:** 以前は、BCR内で認証済みページを開くたびに、ユーザーは資格情報を再入力する必要があり、SSOの永続性が失われていました。SSOはBCRウィンドウが開いている間のみ維持されていました。ウィンドウを閉じて再度開くと、ユーザーはログインプロセスを繰り返す必要がありました。
- **新機能:** プロファイル共有により、ユーザーは資格情報の入力を求められなくなりました。SSOはVDAブラウザからシームレスに維持され、中断のない改善されたエクスペリエンスを提供します。

プレビューの要件

- シトリックス バーチャル アプリ アンド デスクトップ 2503
- シトリックス ワークスペース アプリ 2503
- ブラウザリダイレクト拡張機能 25.3.4 以降
  - Microsoft Edge 拡張機能
  - Google Chrome 拡張機能

この機能を有効にする方法については、ブラウザコンテンツリダイレクト のドキュメントを参照してください。

フィードバックフォーム

ウェブ スタジオ

シトリックス パーソナライゼーション フォー App-V - VDA は、シトリックス バーチャル デリバリー エージェント の アプリケーション パッケージ デリバリー コンポーネント に名称変更されました

VDAインストール時の追加コンポーネントセクションにある**Citrix Personalization for App-V - VDA**チェックボックスが、**App Packages Delivery Component**に名称変更されました。このコンポーネントにより、Citrix環境内でMicrosoftアプリケーションパッケージ（App-V、MSIX、VHD、VHDX、CMFS、Liquidware Flexapp oneアプリケーションパッケージとしてのApp Attach）の管理と配信が可能になります。これにより、ユーザーはVDAから配信される仮想化アプリケーションにアクセスできます。

Web Studio のホームページ

Web Studio にホームページが追加されました。このページでは、Citrix Virtual Apps and Desktops の展開とワークロードの概要、およびサブスクリプションを最大限に活用するための情報が提供されます。このページは以下の部分で構成されています。

- **最近使用した項目。** 最近アクセスしたオブジェクトの履歴を表示します。
- **サイトの詳細。** Citrix Virtual Apps and Desktops展開の概要を提供します。主要な情報には、ライセンスの種類、Studioのバージョン、およびDelivery Controllerのバージョンとステータスが含まれます。
- **リソース。** 展開されたリソースの数と、カテゴリごとのカウントを表示します。
- **セッション。** 過去7日間に毎日起動されたデスクトップおよびアプリセッションの数を表示します。
- **開始。** Citrix Virtual Apps and Desktops展開のセットアップに役立つ一連の質問に案内します。
- **エラーと警告。** Citrix Virtual Apps and Desktops展開からのエラーと警告を一元的に表示します。

Web Studioのホームページ(/en-us/citrix-virtual-apps-desktops/2503/media/studio-home.png)

詳細については、ホームページを参照してください。

履歴使用状況を使用してAutoscale™設定を調整する

新しいAutoscale設定タブ「**Autoscale Insights**」では、Autoscale設定と前週のマシン使用状況データを視覚的に比較できる包括的なグラフが提供されます。このグラフを使用すると、Autoscale設定の有効性に関する洞察を得ることができます。

- **費用対効果が低い。** 容量の過剰なプロビジョニングにより、財政的な無駄が生じています。
- **ユーザーエクスペリエンスが低い。** 容量のプロビジョニング不足により、ユーザーエクスペリエンスに悪影響が及んでいます。
- **ユーザーエクスペリエンスとコストの良好なバランス。** プロビジョニングされた容量は、履歴使用状況と一致しています。

詳細については、Autoscale設定の有効性を分析するを参照してください。

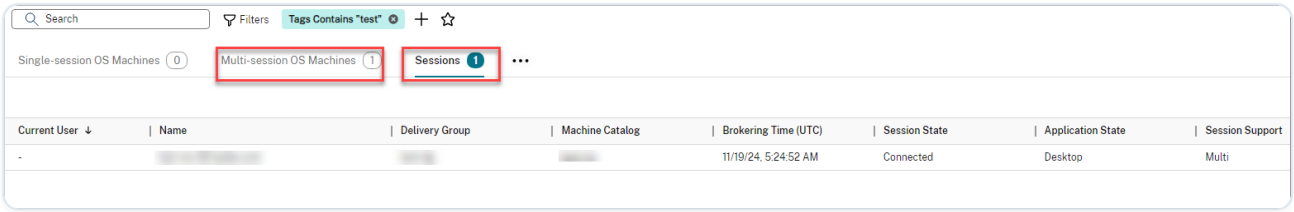
サイトのデフォルトタイムゾーンを設定する

Web Studioでは、サイトのデフォルトタイムゾーンを選択できるようになりました。これを行うには、**設定 > 日付と時刻**に移動します。Web Studioは、スケジュールされた再起動や自動スケーリングなど、すべての時刻表示とスケジューリングにこのタイムゾーンを使用します。この設定により、時刻の管理が容易になり、サイト全体の時刻の一貫性が確保されます。

個々のリソースのタイムゾーンを変更できます。たとえば、異なるリージョンのマシンにサービスを提供するデリバリーグループに異なるタイムゾーンを設定できます。詳細については、デリバリーグループのユーザー設定を変更するを参照してください。

タグベースの検索におけるセッションの可視性の向上

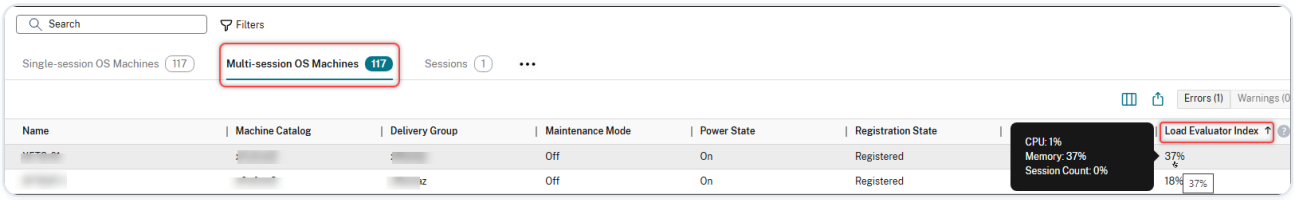
検索ノードでタグによってマシンを検索すると、一致するマシン上のアクティブなユーザーセッションが**セッション**タブに表示されるようになりました。この機能強化により、アクティブなセッションを持つマシンの意図しないシャットダウンが、それらのセッションを明確に可視化することで防止され、管理効率が向上します。



マルチセッションVDAのリソース監視の強化

Web Studioは、マルチセッションVDAの詳細なリソース使用率と機能に関するインサイトを提供するようになりました。**検索**ノードでマルチセッションVDAの**負荷評価インデックス**列にカーソルを合わせると、CPU、メモリ、ディスク使用量、許可されるセッションの最大数などの詳細なメトリックが表示されます。表示される特定のメトリックは、有効なポリシー設定によって異なります。

この機能強化により、PowerShellコマンドレットを実行したり、複数の手順を経てMonitorに切り替えてこのデータを収集したりする必要がなくなり、Web Studio内で直接同じ機能が提供されます。詳細については、マシンアクションと列を参照してください。



ポリシー割り当てのクライアントプラットフォームフィルター

新しいフィルター**クライアントプラットフォーム**を使用して、ポリシー割り当てをより正確に制御できるようになりました。このフィルターを使用すると、Windows、macOS、Linux、iOS、Android、HTML5など、ユーザーデバイスのオペレーティングシステムに基づいてポリシーを割り当て（許可）または除外（拒否）できます。この機能強化により、ポリシー割り当ての柔軟性と精度が向上し、管理対象デバイスと非管理対象デバイス全体でカスタマイズされた統一されたエクスペリエンスが保証されます。

構成ログのラベル付け

ログ > イベントタブで構成ログにラベルを付けられるようになり、ログの識別とエクスポートが容易になりました。さらに、ログノードでは、CSVファイルへのログのエクスポート、高度な検索、**イベント**タブの表形式表示などの機能が強化されました。詳細については、ポリシー割り当てを参照してください。

ドメイン選択の強化

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

- 検索の高速化: 大規模なディレクトリの参照をスキップし、結果を直接かつ即座に取得できます。
- 時間の節約: ディレクトリ全体の読み込みをなくし、ワークフローを高速化します。
- エクスペリエンスの向上: 特に大規模なディレクトリを持つ環境で、管理者管理の効率が向上します。

マシンカタログ作成におけるユーザー名検索の改善

マシンカタログ作成時のユーザー名による管理者検索の機能を強化しました。**マシンカタログのセットアップ > 資格情報の入力**ページへの主な機能強化は次のとおりです。

- **ドメインの指定:** このページに新しいオプション**ドメイン**が追加され、ドメイン名またはSIDを入力して検索を絞り込むことができるようになりました。
- **SamName検索の最適化:** SamNameを使用した検索は、指定されたドメインに限定されるようになりました。

これらの機能強化により、ユーザー検索がより高速かつ効率的になります。

マシンのテンプレートプロパティを使用したAWS VMの作成はサポートされなくなりました

マシンテンプレートプロパティをキャプチャしてAWS VMを作成するサポートは、マシンプロファイルを使用してVMを作成する移行の一環として削除されました。**Apply machine template properties to virtual machines** オプションは **Machine Template** ページから削除されました。代わりに、マシンプロファイルを使用してAWS VMを作成することで、同様のより合理化されたエクスペリエンスを実現できます。詳しくは、「Studioを使用してマシンプロファイルベースのマシンカタログを作成する」を参照してください。

Red Hat OpenShiftマシンの配信と電源管理のサポート（プレビュー）

Web Studio を使用すると、Red Hat OpenShiftサーバークラスターへの接続を作成し、マシンカタログの作成時にこれらの接続を指定できるようになりました。この機能により、既存のOpenShiftマシンをカタログに配置して追加できるため、Red Hat OpenShift環境でマシンの配信と電源管理を行うことができます。

詳しくは、「Red Hat OpenShiftへの接続を作成する」および「OpenShiftマシンカタログを作成する」を参照してください。

Autoscaleを無効にしても電源ポリシーが有効なままであることを管理者に警告する

この機能強化は、Autoscaleを無効にしてもデリバリーグループの電源ポリシー設定には影響しないことを管理者に通知するためのものです。この機能により、管理者はAutoscale無効化の範囲を認識し、Autoscaleがオフになっても電源ポリシーが有効であることを明確にできます。

使用中のActive Directory（AD）アカウントをリセットするオプション

Studioを使用すると、マシンのステータスが**使用中**の場合でも、マシンのActive Directory (AD) アカウントをリセットできるようになりました。これは、システムがマシンが「汚染された」状態にあることを正しく検出できない場合があるため、必要です。

ホスティングユニットのリージョンに基づいてマスターイメージをフィルタリングする

Azureプラットフォームのマシンカタログ作成時に、Web Studioはホスティングユニットのリージョンとは異なるリージョンに属するマスターイメージをフィルタリングして除外できるようになりました。この機能により、ホスティングユニットと同じリージョンのイメージのみが選択可能になります。

最小負荷方式でストレージの負荷分散を最適化する

以前は、Machine Creation Services™ (MCS) は、ストレージリポジトリ全体にVMを分散するためにラウンドロビン方式を使用していましたが、これによりストレージの使用率が不均一になることがよくありました。

Studioでは、**最小負荷方式でストレージの負荷分散を最適化する**オプションが導入されました。カタログ作成時に2つ以上のOSデータストレージの場所を選択すると、このオプションが利用可能になり、ディスクを最も負荷の低いストレージリポジトリに割り当てることができます。

この機能は、負荷分散を強化し、システムの安定性を向上させます。XenServer、VMware、SCVMMの仮想化環境でサポートされています。詳細については、「ストレージの選択」を参照してください。

AWSでのMCSIO対応MCSマシンカタログ作成のサポート

AWSでMCSIO対応MCSマシンカタログを作成できるようになりました。これにより、書き込み操作をライトバックキャッシュに誘導することで書き込みIOPSを向上させ、OSディスクの永続化が有効になっている場合の起動時間を短縮できます。詳細については、「Machine Creation Services (MCS) ストレージの最適化」を参照してください。

AWSからのVMインポートにおけるUIパフォーマンスの向上

AWSからCitrix Virtual Apps and DesktopsにVMをインポートするプロセスを最適化することで、Web StudioのUIパフォーマンスを向上させました。多数のAMIの取得によって発生するタイムアウトを防ぐため、Web Studioはこのプロセス中にAMIを取得しなくなりました。

AWSの起動テンプレートをマシンプロファイルとして選択するサポート

MCSを使用してAWS VMをプロビジョニングする際、起動テンプレートをマシンプロファイルとして選択できるようになりました。起動テンプレートはバージョン管理を容易にします。詳細については、「イメージとマシンプロファイル」を参照してください。

Web Studioを使用して、サスペンド可能なVM専用のデリバリーグループを作成する

Web Studio > デリバリーグループの作成に新しいオプション「**このデリバリーグループにはサスペンド機能が必要**」が導入されました。このオプションを使用すると、サスペンド可能なVMのみを含むデリバリーグループを作成でき、デリバリーグループレベルでのマシンの電源管理が容易になります。この機能は、シングルセッションOS VMにのみ適用されます。詳細については、「デリバリーグループの作成」を参照してください。

Azure GPU休止状態のサポート

GPUをサポートするAzureマシンSKUの休止状態をサポートするオプションが利用可能になりました。サポートされているVMサイズに関する詳細については、Microsoftのドキュメントを参照してください。

カタログ作成後のライトバックキャッシュ設定の更新

MCSIOが有効なMCSカタログの作成後、ライトバックキャッシュのメモリおよびディスクキャッシュサイズを更新できるようになりました。この機能強化により、カタログを再作成することなくキャッシュ設定を調整する柔軟性が向上します。

Azure、AWS、および VMware 環境でレガシー MCS マシンカタログをマシンプロファイルベースのカタログに変換

Web Studio を使用すると、マシンプロファイルベースではないマシンカタログをマシンプロファイルベースのマシンカタログに変換できるようになりました。この機能は、Azure、AWS、および VMware 環境のカタログで利用できます。この機能により、カタログを作成することなく、レガシー MCS マシンカタログを推奨されるマシンプロファイルベースの形式にアップグレードできます。

詳細については、「レガシー MCS カタログをマシンプロファイルベースのカタログに変換する」を参照してください。

AzureでMCSによって作成されたカタログのセカンダリVMのスケールアップまたはスケールダウンリストを構成するサポート

Web Studioでは、AzureでMCSによって作成されたカタログをスケールアップおよびスケールダウンするためのセカンダリVMを定義できるようになりました。CPUおよびメモリリソースの使用状況に基づいて、CPUまたはメモリの使用量が特定のしきい値を超えた場合、システムは自動的にセカンダリVMを使用して負荷を処理します。あるいは、使用量が特定のレベルを下回った場合、システムはリソースを節約するために一部のVMを自動的にシャットダウンします。

オンプレミスActive DirectoryマシンID管理用のサービスアカウント

MCSは、サービスアカウントを使用してオンプレミスActive DirectoryマシンIDを管理するための新しいメカニズムを開発しました。サービスアカウントは、毎回ドメイン資格情報を入力することなく、オンプレミスActive Directoryのコンピューターアカウントを管理するのに役立ちます。詳細については、「マシンID管理用のサービスアカウント」を参照してください。

孤立したリソース検出のための新しい権限

以前は、**Full Administrator** または **Cloud Administrator** ロールのみが孤立したリソース検出を実行できました。**Hosts** カテゴリに **Use Host Connection to Detect Orphaned Resources in Hypervisor** 権限が導入されたことにより、この権限が割り当てられたすべてのロールが孤立したリソースを検出できるようになりました。

詳細については、「孤立した Azure リソースを検出する」および「孤立したリソースのリストを取得する」を参照してください。

フルコピー複製を使用したWindows Server OSでの永続VMのプロビジョニングのサポート

Web Studioは、フルコピー複製アプローチを使用してWindows Server OS上に永続的なVMをプロビジョニングすることをサポートするようになりました。このアプローチにより、データ復旧と移行機能が向上し、マシンの作成後のIOPS削減に役立ちます。

詳細については、「デスクトップエクスペリエンスの選択」および「仮想マシンコピーモード」を参照してください。

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

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

GCPにおけるマスターイメージとしてのディスクのスナップショットまたはOSイメージのサポート

Studioを使用すると、GCP環境でMCSマシンカタログを作成するためのマスターイメージとして、ディスクのスナップショットまたはディスクのイメージを選択できるようになりました。ディスクのスナップショットまたはディスクのイメージは、リージョンのみであるVMインスタンスと比較して、リージョンおよびマルチリージョンにすることができます。この機能により、イメージ管理ワークフローが大幅に簡素化され、GCPでのイメージ管理に必要な時間と労力が削減されます。

シトリックス スタジオ

MMCベースのStudioの今後の廃止

Web Studioへの移行の一環として、MMCベースのStudioはCR 2511インストーラーから削除されます。この変更により、Web Studioが単一の管理コンソールとして確立され、管理者に一貫したエクスペリエンス、最新のインターフェイス、合理化されたワークフロー、および強化された機能が提供されます。

MMCベースのStudioの廃止は、2411リリースで最初に発表されました。更新された機能と直感的なデザインを活用するために、Web Studioへの移行をお勧めします。

Citrix Director (シトリックス ディレクター)

Azureワークロードのコストモデリング

新しいコストモデリング機能はAzureワークロードをサポートし、使用パターンに基づいて推奨事項を提供します。顧客は、Azure ReservationsとSavings Planのどちらが最大のコスト削減を提供するために適しているかについて推奨事項を受け取ります。Azure Reservationsの顧客は、割引された定額料金で特定の数のマシンを事前に予約しますが、Savings Planでは、割引料金のためにドル額をコミットできます。この機能は、過去28日間のデータを分析して推定推奨事項を提供します。この機能は、リソース割り当てに関する情報に基づいた意思決定を行うことで、顧客がコストを節約するのに役立ちます。

> **注:**
>
> 最適な推定値を得るには、過去28日間の安定した環境からのデータを使用することをお勧めします。休暇や急激な使用量の増加など、異常な活動期間のデータは使用しないでください。これらの推奨事項を適用する前に、使用量がベースラインレベルに戻るまで待ってください。

> **利点:**

- カスタマイズされたコスト削減の推奨事項を提供します。
- 予約プランとセービングプランの両方をサポートします。
- 正確なインサイトを得るために、最近の使用状況データを分析します。
- リソース割り当ての最適化と経費削減に役立ちます。
- デリバリーグループ、タグ、VMシリーズ、およびリージョンの選択において柔軟性を提供します。

詳細については、コストモデリングページを参照してください。

コスト削減ページの機能強化

コストを管理する際に、より優れた柔軟性とインサイトを提供するために、コスト削減ページに以下の機能強化が行われました。

- **サービスプロバイダーフィルターのサポートオプション**: サービスプロバイダーでフィルターできるようになりました。サイトにクラウドとオンプレミスの両方のワークロードがある場合、すべてのクラウドプロバイダー、すべてのオンプレミスプロバイダー、または個々のプロバイダーでフィルターできます。

  > **注:**
  >
  > フィルターは、適用ボタンなしで選択するとすぐに適用されます。

- **複数のデリバリーグループの選択**: 以前は、単一のデリバリーグループ (DG) またはすべてのDGしか選択できませんでした。現在は、一度に最大15個のDGを選択できます。サイトに15個未満のDGしかない場合は、利用可能なすべてのDGを選択できます。また、特定のDGを選択から除外して、残りのDGのデータを表示することもできます。
- **失敗したマシンのインサイト**: **コスト削減**ページで、失敗した状態または未登録状態のマシンに関する可視性が提供されるようになりました。以下の2つの新しいフィールドが含まれています。
  - **セッションなしの失敗状態**: このフィールドには、失敗状態であり、アクティブなセッションがないマシンの数が表示されます。
  - **セッションありで未登録**：このフィールドには、未登録状態だがアクティブなセッションを持つマシンの数が表示されます。

上記の各状態にあるマシンの数を確認し、障害の原因、時間、デリバリーグループに基づいて対応できます。これらの数はクリック可能なリンクとなっており、さらなるアクションのために**フィルター**ページに移動します。この数には、シングルセッションマシンとマルチセッションマシンの両方が含まれます。

> **注:**
>
> フィルターはページナビゲーション全体で保持されます。

> 詳細については、コスト削減ページを参照してください。

DirectorとuberAgent®の統合

Citrix uberAgentは、Citrix Virtual Apps and Desktopsのインストールにデフォルトで含まれるようになり、強化された監視機能とCitrix Directorとのシームレスな統合を提供します。管理者は、

Virtual Delivery Agentのセットアップ中に**オプションソフトウェア**画面で選択を解除することで、インストールから除外できます。

主な機能と利点

- **ローカルアプリケーション使用状況の監視**：Citrix uberAgentを使用すると、ローカルアプリケーションの使用状況を監視でき、Directorとの統合により、データはDirectorダッシュボードで直接利用できます（Platinumライセンスで利用可能）。

構成するポリシー

Citrix uberAgentをインストールした後、DirectorとuberAgentを完全に統合して使用するために、Citrix Web Studio™で以下のポリシーを構成します。

- **uberAgentデータ収集ポリシーを有効にする**：有効にすると、uberAgentはアプリケーションの使用状況とパフォーマンス、システムヘルス、ネットワークメトリック、セキュリティ分析に関する洞察を提供します。このポリシーはデフォルトで無効になっています。
- **uberAgentデータポリシーでDirectorを強化する**：このポリシーはDirector統合を有効にします。これにより、DirectorはuberAgentが提供するデータを処理して、ローカルアプリケーションの使用状況の監視を含む監視機能を強化できます。このポリシーはデフォルトで有効になっています。

詳細については、DirectorとのCitrix uberAgent統合を参照してください。

ローカルアプリケーション使用状況レポート

このリリースでは、Citrix uberAgent が Citrix Virtual Apps and Desktops と統合されました。Citrix uberAgent を有効にすると、Citrix Director は仮想デスクトップセッション内で起動されたアプリケーション（ローカルアプリケーションとも呼ばれます）の使用状況を監視するのに役立ちます。

アプリケーション使用状況レポートは、最も使用されているアプリケーション、ほとんど使用されていないアプリケーション、および使用されていないアプリケーションの可視性を提供します。最も使用されているアプリケーションはダッシュボードに表示され、IT 管理者またはアプリケーション管理者がどのローカルアプリケーションが頻繁に使用されているか、およびその使用状況の程度を把握するのに役立つ厳選されたグラフが含まれています。また、ほとんど使用されていないローカルアプリケーションや未使用のローカルアプリケーションのレポートも見つけることができます。このレポートは、デスクトップイメージをスリムに保つためにバージョンレベルの使用状況統計に焦点を当てることで、どのアプリケーションが廃止の候補であるかを管理者が理解できるように、四半期ごとに計算されるのがデフォルトです。

アプリケーションの使用状況を使用して、Power BI 統合または ODATA クエリを使用してデータをエクスポートすることもできます。

前提条件:

- この機能は、プラチナライセンスサイトでのみ利用可能です。
- uberAgent は Director と統合されている必要があります。

> **注:**

> 環境が同じアプリケーションを公開アプリとデスクトップ内にインストールされたアプリ（ローカルアプリ）の両方として提供している場合、そのアプリが公開アプリレポートとローカルアプリレポートの両方に表示されることがあります。

> 詳細については、「アプリケーション使用状況の監視」を参照してください。

Director ダッシュボードの新しいメトリック

Citrix Director ダッシュボードには、管理者にとって貴重な洞察を提供する次の 2 つのメトリックが追加されました。

- **合計接続ユーザー数**: 過去 24 時間および過去 7 日間に少なくとも 1 つの接続があったユーザーの数を示します。管理者が役員に導入傾向を示すのに役立ちます。
- **環境内で検出された Citrix Workspace アプリのバージョン**: 組織全体で使用されている Citrix Workspace アプリのバージョンの概要を提供します。異なるバージョンを使用しているデバイスの数を示すことで、バージョンを統一するのに役立ちます。**プラットフォーム**ドロップダウンリストから**すべて**または特定の OS を選択できます。

この機能は、管理者が環境を効果的に監視および管理するために不可欠なデータポイントを提供します。

VDA ログオン期間の詳細の監視

Citrix Director に、VDA ログオン時間の詳細情報が含まれるようになりました。これにより、VDA へのログオンにかかる時間が可視化されます。VDA ログオン時間の詳細を表示するために、以下の項目が追加されました。

- **トレンドグラフの VDA ログオン時間グラフ**: 新しい VDA ログオン時間グラフが、**トレンド** > **ログオンパフォーマンス** タブに追加されました。また、以下のメトリックが内訳メトリックとしてツールチップに追加されました。
  - **AppXファイル関連付け**: 新しいVDAセッション中にAppXファイルを関連付けるのにかかった時間。
  - **AppXパッケージの読み込み**: 新しいVDAセッション中にAppXパッケージを読み込むのにかかった時間。

  これらのメトリックは PDF および CSV 形式でエクスポートされ、グラフもエクスポートされたファイルに含まれます。
- **フィルター** タブの **合計ログオン時間（秒）** および **VDA 時間（秒）**: これらのメトリックは **フィルター** ビューに追加され、セッション検索とカスタムレポートをフィルターできるようになりました。
- **セッションログオン** タブの **クライアントとコントローラーの期間** および **VDA ログオン時間**: **セッションログオン** タブのグラフが再編成され、以下の詳細な期間をサポートするようになりました。
  - **クライアントとコントローラーの期間**: ユーザーがアプリまたはデスクトップアイコンをクリックしてから、キーボードとマウスの制御がエンドユーザーに渡され、セッションを操作できるようになるまでの時間。
  - **VDA ログオン時間**: セッションを作成するために VDA でかかった時間。
- **セッションログオン** タブの **シェル** ステップの内訳: AppX ファイルの関連付けと AppX パッケージの読み込みが、**セッションログオン** グラフタブのグラフ上のインタラクティブセッションステップの内訳として追加されました。

利点:

- 正確なトラブルシューティング: 管理者がログオンの遅延の原因（多くの場合、展開タイプ、GPO、プロファイル、ユーザー操作に起因する可能性があります）を正確に特定するのに役立ちます。
- 是正措置: 管理者が適切な領域で是正措置を講じ、全体的なユーザーエクスペリエンスを向上させることを可能にします。

この機能は、セッションログオンの内訳を改善し、ログオンパフォーマンスとDirectorヘルプデスクのセッションログオントリアージをより正確に表現するように設計されています。

詳細については、「ログオンプロセスフェーズ」を参照してください。

Provisioning Service の追加メトリック収集

Provisioning Serviceサーバーについて、次の詳細が監視されるようになりました。

- **合計再接続数**: セッションが再接続された回数を表示します。
- **PXE サービス**: Preboot Execution Environment サービスのステータスを表示します。このメトリックは、Windows サービスのステータスを示します。可能な値は、Not running、Running、Not Installed、および n/a (ヘルプアイコン付き) です。
- **TFTP サービス**: Trivial FTP サービスのステータスを表示します。このメトリックは、Windows サービスのステータスを示します。可能な値は、Not running、Running、Not Installed、および n/a (ヘルプアイコン付き) です。

管理者は、PXE および TFTP サービスの健全性ステータスに基づいてアラートを設定できます。これらの Citrix コンポーネントの監視とアラートにより、配信への影響を軽減し、ユーザーエクスペリエンスを向上させることができます。コンポーネントの健全性に関する重要なデータセットを提供することで、問題のトラブルシューティングが改善されます。

詳細については、「Provisioning Service の健全性メトリック」を参照してください。

Microsoft Teams以外のHDX最適化の監視を拡張するオプション

Citrix Director に、Microsoft Teams 以外の HDX 最適化の監視を拡張するオプションが追加されました。以前は、HDX 最適化の監視には Microsoft Teams のみが利用可能で、**セッショントポロジ**画面で最適化されているかどうかを表示していました。この新機能では、**Microsoft Teams** の代わりに、**リアルタイム通信**という新しいパラメーターが**セッショントポロジ**画面に追加されます。現在、HDX 最適化ステータスについては Microsoft Teams のみが監視されています。ただし、この機能により、将来的には Microsoft Teams だけでなく、より多くのソフトウェアを監視に追加できる可能性が提供されます。この機能により、管理者は HDX 最適化の有無にかかわらずアプリケーションを監視およびトラブルシューティングでき、より良いユーザーエクスペリエンスを提供できます。

アプリケーションの横にある **詳細を表示** をクリックすると、サードパーティ最適化と HDX 最適化の分類など、追加情報を表示できます。Microsoft Teams Slims コアの場合、サードパーティ最適化の一部です。サードパーティ最適化の一部でない場合は、HDX 最適化されています。

主な機能と利点:

- **包括的な監視**: HDX最適化されたアプリケーションと最適化されていないアプリケーションの両方を監視およびトラブルシューティングします。
- **詳細なインサイト**: アプリケーションの最適化ステータスに関する詳細情報を表示します。

注:

- この新機能を使用するには、Citrix Workspace アプリ for Windows バージョン 2503 および VDA バージョン 2503 を使用していることを確認してください。
- Microsoft Teams Slims coreを使用するには、エンドポイントにプラグインマネージャーをインストールし、仮想チャネルの許可リストを構成し、仮想チャネルが開いていることを確認する必要があります。この機能はHDXセッション専用です。

詳細については、「HDX最適化の詳細」を参照してください。

フィルタータブとカスタムレポートで利用可能なエンドポイントメトリック

以前は、エンドポイントメトリックは、**ユーザー詳細** > **セッションパフォーマンス** > **セッショントポロジ** セクションのエンドポイントビューでのみ利用可能でした。

この機能強化により、Directorの接続またはセッションフィルターとカスタムレポートで、以下のより多くのエンドポイントメトリックを表示できるようになりました。

- パブリックIPアドレス
- ISP
- 場所 (国または都市)
- ワークスペースの種類 - Citrix Workspaceアプリ (アプリまたはブラウザ)
- アクセスタイプ（WorkspaceまたはStoreFront™経由）

この機能強化により、以下のことが可能になります。

- **フィルター**タブで列選択の一部としてエンドポイントメトリックを選択できます。
- **カスタムクエリ**オプションを使用して、出力列としてエンドポイントメトリックを選択することで、カスタムレポートを作成できます。

Citrix Director向けの統合されたプラットフォームエクスペリエンス

Citrix Directorは、Citrix Cloud™内の他のすべてのコンポーネントと連携し、統一されたプラットフォームエクスペリエンスを提供します。ユーザーインターフェイスは、最新のルックアンドフィールに刷新され、より簡単なナビゲーションとより良いデータ表現を提供します。強化された

インターフェイスは直感的で、ユーザーがCitrixセッションの監視とトラブルシューティングに必要なデータを簡単に理解できるように設計されています。

フィルタービューとセッションパフォーマンスタブでのセッション自動再接続の詳細

これで、**フィルター** > **セッション**タブと**セッションパフォーマンス**タブの両方で、セッションの自動再接続の詳細を表示できるようになりました。この機能強化により、セッション内の自動再接続の数にすばやくアクセスして分析できます。

フィルタービュー:

- 新しい**セッションの自動再接続**列を表示するには、**列の選択**に移動し、**フィルター** > **セッション**タブで**セッションの自動再接続**を選択します。
- ドリルダウンでは、セッションの信頼性またはクライアントの自動再接続、タイムスタンプ、エンドポイントIP、Citrix Workspaceアプリがインストールされているマシンのエンドポイント名などの追加情報が提供されます。この情報は以前は**トレンド**タブで利用可能でした。詳細については、履歴トレンドページを参照してください。

セッションパフォーマンスタブ:

- セッションの自動再接続の詳細は、**セッションパフォーマンス**タブの**過去48時間**タブで表示できるようになりました。
- グラフには、合計セッション再接続数、クライアントの自動再接続数、およびセッションの信頼性再接続数が表示されます。

自動再接続情報は、中断を伴うネットワーク接続の表示とトラブルシューティング、およびシームレスなエクスペリエンスのためのネットワーク分析に役立ちます。

Directorアクションの機能強化

Citrix Directorは、ユーザーエクスペリエンスを向上させ、アクションをより詳細に制御するための新機能を導入します。この更新には、アクションの進行状況バーの追加と、ユーザーロールに基づいてアクションの範囲を制限するサポートが含まれます。

アクションの進行状況バー

この機能強化により、電源制御機能（再起動など）のようなアクションが進行中の場合、アクションのステータスと、アクションが完了したときにダイアログボックスが表示されます。この機能は、**フィルター**タブのすべてのアクションに適用されます。ただし、単一のアクションではステータスバーは利用できません。

進行状況バーは、実行された一括アクションの結果を示します。現在、お客様は自分たちのアクションが成功したか失敗したか、また何セッションで成功または失敗したかを知ることができません。この機能強化により、実行されたアクションが明確になります。

ユーザーアクションの一括アクションオプションを制限するカスタムロール

この機能強化により、管理者が表示および制御できる内容を制限するためにカスタムロールを追加できます。新しいカスタムロールは、ログオフ、切断、メッセージなどの一括アクションを選択する機能を制限します。この制御は、ユーザーに対する意図しない、または悪意のある一括アクションを防ぐために必要です。

これらの機能強化により、Citrix Director内でアクションを効果的に管理および制御し、より安全で効率的な環境を確保できます。

詳細については、「ユーザーアクションの一括操作オプションを制限するカスタムロール」を参照してください。

Provisioning ServiceおよびDelivery Controller™のサイトレベルアラートを設定する規定

以前は、単一サイトに複数のサーバーがある場合、サーバーごとに1つのアラートが複数届いていました。この機能強化により、管理者は次のオプションを利用できるようになりました。

- Provisioning Serviceサイトまたは個々のProvisioning Serviceサーバーに基づいてProvisioning Serviceアラートを構成します。
- Delivery Controllerサイトまたは個々のDelivery Controllerサーバーに基づいてDelivery Controllerアラートを構成します。

この機能強化により、個々のサーバーレベルではなく、サイトレベルでアラートを送信できます。

単一サイトに単一のアラートを設定するには、**高度なアラートポリシー**に移動し、必要に応じてスコープを選択します。たとえば、Provisioning Serviceの場合、**すべてのProvisioning Service**を選択すると、サイトに2つのサーバーがある場合でも、単一のアラートのみを受信します。このアラートはサイトレベルのアラートです。

この機能強化により、アラートが設定されると、**Citrix Alerts**ページにサイト名とともにアラートのあるサーバーの数が表示されます。この数をクリックすると、**インフラストラクチャ監視**タブに移動し、アラートがあったサーバーのみが表示されます。アラートの原因となっているコンポーネントの詳細なリストを含むこのターゲットを絞った通知は、アラートの過負荷を軽減するのに役立ちます。

詳細については、「インフラストラクチャ監視のアラート」を参照してください。

Webhookとの統合

Citrix DirectorはWebhookと統合されました。この機能を使用すると、「**Integrations and data exports**」ページの「**Alerting and ITSM**」セクションから必要なツールを選択し、「**Get Started**」をクリックできます。このページには、ツールの特定のチャネルとWebhook URLを作成するための参照リンクが表示されます。これが最初のステップです。最初のステップが完了すると、Webhookプロファイルを作成できます。

Citrix Director の**［Integrations and data exports］**> **［Developer tools］**ページで Webhook プロファイルを作成することもできます。Citrix Director と次のアラートおよび ITSM ツールを統合するための手順とリソースを見つけることができます。

- スラック
- マイクロソフト Teams
- ServiceNow

この機能は、受信Webhook URLが構成されている上記のサードパーティアプリケーションにアラート通知を送信するのに役立ちます。

主な機能:

- Slack、Microsoft Teams、ServiceNow、およびその他のサポートされているプラットフォーム用の新しい統合タイル。
- 各統合の初回ユーザーページへのナビゲーション。
- Webhook URL、ヘッダー、本文を提供し、Webhook構成をテストして保存するためのUIワークフローを備えたWebhook構成ページの作成または編集。
- 作成されたWebhookプロファイルを一覧表示し、Webhookプロファイルを編集、削除する機能を提供します。
- 作成されたWebhookプロファイルを高度なアラートポリシーにマッピングします。

詳細については、「アラートおよびITSMツールとの統合」を参照してください。

セッションパフォーマンスタブの更新

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

- WAN遅延 - NetScaler®からエンドユーザーまでの、ネットワークのクライアント側によって引き起こされる遅延。

- DC遅延 - NetScalerからバックエンドサーバーまでの、ネットワークのサーバー側によって引き起こされる遅延
- L7クライアント遅延 - ICA®クライアントとNetScalerインスタンス間で観測される平均L7遅延。このメトリックは、配信パスにCitrix以外のデバイスが存在する場合に役立ちます。
- L7サーバーの待機時間 - NetScalerデバイスとCitrix Virtual Appの間で観測された平均L7待機時間。このメトリックは、配信パスにCitrix以外のデバイスが存在する場合に役立ちます。
- クライアントの再送信 - NetScalerとエンドユーザー間の接続で再送信されたパケットの数。このメトリックの値が高い場合、再送信による高い帯域幅使用率を示しますが、必ずしもユーザーエクスペリエンスが悪いことを意味するわけではありません。
- サーバー側の再送信 - NetScalerとバックエンドサーバー間の接続で再送信されたパケットの数。
- クライアント側のゼロウィンドウ数 - クライアントがゼロTCPウィンドウをアドバタイズした回数。
- サーバー側のゼロウィンドウ数 - サーバーがゼロTCPウィンドウをアドバタイズした回数。
- 「Last 15 min」タブと「48 hours」タブにあるWAN待機時間、DC待機時間、L7クライアント待機時間、L7サーバー待機時間、クライアント再送信、サーバー再送信のグラフ。

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

詳細については、「セッションパフォーマンスの問題の診断」ページを参照してください。

Citrix Infrastructure Monitor の自動接続

自動接続機能は、Citrix Infrastructure Monitorを自動的にダウンロードおよびインストールし、接続を検証することで、オンボーディングプロセスを効率化します。この新機能では、管理者は自動接続でコンポーネントの詳細を提供するだけでよく、情報を提供する前にすべての前提条件が満たされていることを確認する必要があります。

自動接続機能の目的は、Citrix管理者のオンボーディングプロセスを簡素化することです。この新機能により、UIには自動接続と手動接続の2つのオプションが用意されました。

詳細については、「Citrix Infrastructure Monitorの自動接続」を参照してください。

Citrix Infrastructure Monitorのアップグレード

Citrix Infrastructure Monitorの古いバージョンを使用している場合、バージョンアップグレードが利用可能かどうか、およびその実行方法についてプロンプトが表示されるようになりました。これはProvisioning ServiceとStorefrontにのみ適用されます。

自動または手動でアップグレードを選択できます。自動アップグレードでは進行状況が表示され、管理者資格情報が必要です。アップグレードプロンプトは、新しいバージョンが利用可能な場合にのみ表示されます。アップグレードに登録は不要です。アップグレード後、最新バージョンが反映されるまでに約5分かかります。

詳細については、インフラストラクチャ監視の概要を参照してください。

スカウト

ScoutはProvisioning Serviceサイトからのデータ収集をサポートします

以前は、ScoutはローカルのProvisioning Serviceマシンのみをサポートしていました。このリリースにより、ScoutはProvisioning Serviceサイト内の複数のProvisioning Serviceサーバーをサポートするようになりました。この機能強化により、Provisioning Service環境全体でより包括的なデータ収集と監視が可能になります。

主な機能と利点:

- サポートの拡大: Scoutはサイト内の複数のProvisioning Serviceサーバーをサポートするようになり、環境の全体像をより包括的に把握できるようになりました。
- パフォーマンスと安定性の向上: このリリースでは、全体的なパフォーマンスと安定性を向上させるためにいくつかの問題が解決されています。
- ユーザーインターフェイスの強化: ScoutのUIが改善され、ユーザーエクスペリエンスが向上しました。

これらの更新により、管理者はProvisioning Service環境をより効果的に監視およびトラブルシューティングできるようになり、パフォーマンスと信頼性の向上につながります。

FASとのScout統合

以前は、ScoutはFederated Authentication Service (FAS) と統合されておらず、そこからの情報収集ができませんでした。このリリースにより、ScoutはFASと統合されました。この機能はデフォルトで利用可能であり、ScoutはFASをVDAやStoreFrontなどと同様のCitrixマシンタイプとして検出および認識できるようになります。

主な機能と利点:

- 統合されたデータ収集: Scoutは、**Collect**オプションを使用してFAS AOTログを収集できるようになりました。

- トラブルシューティングの強化: **Trace & Reproduce**オプションを使用して、CDFログと追加のFAS構成情報を有効にして取得します。
- 監視の改善: FASサーバーマシン向けに統合されたデータ収集エクスペリエンスを保証します。

> **注記:**
>
> 現在、FASサーバー上のScoutは、FAS構成の問題を診断するための「Health Check」をサポートしていません。

uberAgent

ウーバーエージェントとCitrix Virtual Apps and Desktopsとの統合

Citrix uberAgentは、Citrix Virtual Apps and Desktopsのインストールにデフォルトで含まれるようになり、強化された監視機能とCitrix Directorとのシームレスな統合を提供します。管理者は、Virtual Delivery Agentのセットアップ中に**オプションソフトウェア**画面で選択を解除することで、インストールから除外できます。

主な機能と利点

- **強化された監視機能**: uberAgentは、アプリケーションの使用状況とパフォーマンス、システムの状態、ネットワークメトリック、およびセキュリティ分析に関する詳細な洞察を提供します。
- **柔軟な構成オプション**: uberAgentは、Splunk、Elastic Search、Azure Monitor、Microsoft ADX、またはApache Kafkaなどの顧客のバックエンドにデータを送信するための柔軟な構成オプションを提供します。

構成するポリシー

Citrix uberAgentをインストールした後、Citrix Web Studioで以下のポリシーを構成して、uberAgentをCitrix Virtual Apps and Desktopsと完全に統合して使用します。

- **uberAgentデータ収集ポリシーを有効にする**: 有効にすると、uberAgentはアプリケーションの使用状況とパフォーマンス、システムの状態、ネットワークメトリック、およびセキュリティ分析に関する洞察を提供します。このポリシーはデフォルトで無効になっています。
- **uberAgentデータポリシーでDirectorを強化する**: このポリシーはDirectorの統合を有効にします。これにより、DirectorはuberAgentによって提供されるデータを処理し、ローカルアプリ

ケーションの使用状況の監視を含む監視機能を強化できます。このポリシーはデフォルトで有効になっています。

- **uberAgent構成アーカイブパス**: このポリシーは、uberAgent構成アーカイブを含むディレクトリへのパスを指定します。デフォルトでは、パスは空です。
- **uberAgentライセンスパス**: このポリシーは、少なくとも1つのuberAgentライセンスを含むディレクトリへのパスを指定します。デフォルトでは、パスは空です。

この統合により、管理者はCitrix環境を効果的に監視および管理でき、より良いユーザーエクスペリエンスとシステムパフォーマンスの向上を提供します。

マシン作成サービス (MCS)

Citrix管理のOpenShiftプラグインのサポート（プレビュー）

この機能により、CitrixはCitrix管理のOpenShiftプラグインを介してRed Hat OpenShiftワークロードを管理します。このプラグインを使用すると、OpenShiftクラスターへのホスティング接続とホスティングユニットの作成、カタログの作成、およびPowerShellコマンドを使用したカタログ内のマシンの電源管理を行うことができます。詳細については、以下を参照してください。

- Red Hat OpenShift仮想化環境
- Red Hat OpenShiftへの接続
- Red Hat OpenShiftカタログの作成
- Red Hat OpenShift VMの電源管理

既存のMCSプロビジョニング済みカタログを準備済みイメージマシンカタログに移行する

この機能により、既存のマスターイメージからプロビジョニングされたMCSカタログを、準備されたイメージを使用するカタログに変換できます。準備されたイメージの詳細については、「イメージ管理」を参照してください。

ただし、移行後にレガシーカタログに戻すことはできません。現在、この機能はAzureおよびVMware仮想化環境に適用されます。移行手順の詳細については、「既存のMCSプロビジョニング済みカタログを準備済みイメージマシンカタログに移行する」を参照してください。

VMwareにおける非永続VMの移行

以前は、VMware環境では、永続VMディスクのみをあるストレージから別のストレージに移行できました。この機能により、Move-ProvVMDisk PowerShellコマンドを使用して、非永続VMディ

スクをあるストレージから別のストレージに移行できます。移行できるのは、OSディスク、IDディスク、およびライトバックキャッシュ（WBC）ディスクです。

詳細については、「VMのストレージ移行」を参照してください。

既存の永続および非永続カタログのTrusted Launchを有効にする

この機能により、既存のTrusted Launchではない永続および非永続マシンカタログを、Trusted Launchが有効なカタログに更新できます。

信頼できる起動でマシンカタログを正常に作成または更新するには、マシンプロファイルを使用する必要があります。ただし、信頼できる起動が有効なマスターイメージと、信頼できる起動が有効でないマシンプロファイルを使用すると、マスターイメージとマシンプロファイルの間で信頼できる起動の構成が一致しないため、警告メッセージが表示されます。

詳細については、「Trusted Launch を使用したマシンカタログ」を参照してください。

AWSでのクロスアカウントプロビジョニング

Delivery Controller をプライマリ AWS アカウント（**共有サービスアカウント**または**サイトコンポーネントアカウント**）に配置し、クロスアカウントアクセス（クロスアカウント IAM ロール）を持つ IAM ロールを使用し、MCS でプロビジョニングされたマシンカタログを別のセカンダリ AWS アカウント（**ワークロードアカウント**）に配置するユースケースがあります。この場合、別の追加の Delivery Controller は必要ありません。このようなシナリオをサポートするため、この機能は VPC ピアリングと IAM ロールを使用したクロスアカウントアクセスを利用して、複数の AWS アカウントを管理する企業が異なる AWS アカウント間でプロビジョニングできるようにします。

VPC ピアリングを使用すると、Delivery Controller と、異なるリージョンまたはアカウントにプロビジョニングされた VM が相互に通信できるようになります。

IAM ロールを使用したクロスアカウントアクセスを使用すると、プライマリアカウント（Delivery Controller アカウント）が IAM ロールを引き受けて、セカンダリアカウント（マシンカタログ VM）の AWS リソースにアクセスできるようになります。

詳細については、「クロスアカウントプロビジョニング」を参照してください。

AWSにおけるVMのバックアップSKUリストのサポート

パブリッククラウドでは、特定のEC2インスタンスタイプ（**プライマリSKU**）の容量が不足することがあります。プライマリVM構成が利用できない場合、VMを起動できず、時間の損失やビジネスの中断につながります。

この機能を使用すると、AWS 仮想化環境で、容量関連の問題が発生した場合に MCS がフォールバックできるバックアップ EC2 インスタンスタイプ（**オンデマンド**インスタンスになり得る**バックアップ SKU**）のリストを PowerShell を使用して提供できます。MCS は、リストで指定された順序でバックアップ EC2 インスタンスタイプへのフォールバックを試行します。MCS が提供されたすべてのバックアップ EC2 インスタンスタイプへのフォールバックに失敗した場合、エラーメッセージが表示されます。この機能は、永続および非永続 MCS マシンカタログの両方に適用されます。

詳細については、「VM のバックアップ SKU リスト」を参照してください。

Azureシークレット環境でのホスト接続の検証

この機能を使用すると、PowerShell コマンド `Test-HypHypervisorConnection` を使用して、ホスト接続が Azure シークレット環境で必要な権限を持っているかどうかを検証できます。検証結果を正常に取得するには、既存のホスト接続を作成または更新して、カスタムプロパティ `AuthenticationObjectId` を持つようにする必要があります。このプロパティには、ホスティング接続に関連付けられたサービスプリンシパルのオブジェクト ID が格納されます。

詳細については、「Azure シークレット環境でのホスト接続の検証」を参照してください。

Citrix管理のHPE Moonshotプラグインがデフォルトでインストールされる

Citrix管理のHPE Moonshotプラグインは、Citrix Virtual Apps and Desktopsバージョン2503のアップグレードまたはインストール時に自動的にインストールされます。HPE Moonshot仮想化環境を参照してください。

AzureにおけるNVMe専用SKUのサポート

以前は、MCSはSCSIストレージコントローラータイプのみをサポートしていました。この機能により、MCSはNVMeストレージコントローラータイプもサポートし、Azure上の新しいVM SKUをサポートします。NVMeの詳細については、MicrosoftドキュメントのNVMeに関する一般的なFAQを参照してください。以下のサービス提供を使用してMCSマシンカタログを作成する方法については、次を参照してください。

- SCSIとNVMeの両方をサポートしている場合は、SCSIとNVMeの両方をサポートするサービス提供を使用してカタログを作成するを参照してください。
- NVMeのみをサポートしている場合は、NVMeのみをサポートするサービス提供を使用してカタログを作成するを参照してください。

VMの柔軟なストレージ場所オプション

以前は、VMの割り当てはSR1などの固定ストレージサービス（SR）から開始され、SR2、SR3と順次進行していました。また、場合によっては、ストレージの負荷がストレージ全体に均等に分散されないことがありました。

この機能により、以下の方法を使用して、異なるストレージサービス間でVMの割り当てをバランスさせることができます。

- 強化された現在のラウンドロビン割り当て方法：常に同じ固定SRから開始するのではなく、MCSは最後に使用されたSRの直後のSRから割り当てを開始するようになりました。
- 最小負荷ベースの割り当て方法：同じマシンカタログ内の各SR上のVMの総数を比較して決定される、現在の負荷が最も低い場所にVMを配置します。たとえば、マシンカタログに100個のVMが次のように分散されている場合：SR1に20個のVM、SR2に30個のVM、SR3に50個のVMがある場合、新しいVMは最初にSR1に割り当てられます。この方法により、SR1、SR2、SR3間の負荷がバランスされます。この方法は、ホスト接続の作成または更新時にカスタムプロパティ **Name="StorageBalanceType`" Value="VMCountBasedLeastLoad** を追加することで使用できます。

この機能は次のとおりです。

- OSディスクストレージのみに適用されます。
- すべてのオンプレミスハイパーバイザー（VMware、XenServer®、Hyper-V）に適用されます。
- 既存のVMには適用されません。

負荷ベースの割り当てオプションを使用して既存のホスト接続を作成または更新する方法については、VMの柔軟なストレージロケーションオプションを参照してください。

Azureでのブート整合性監視のサポート

この機能により、Azure仮想化環境では、`GuestAttenstation`拡張機能がインストールされているマシンプロファイル（VMまたはテンプレート仕様）を使用して、MCSマシンカタログVM（永続VMおよび非永続VM）に対して**ブート整合性監視**を有効にできます。ブート整合性監視は、セキュアブートと仮想トラステッドプラットフォームモジュール（vTPM）を使用するTrusted Launchおよび機密VMでのみサポートされています。

VMでセキュアブートとvTPMが有効になっており、`GuestAttestation`拡張機能がインストールされている場合、Microsoft Defender for Cloudは、VMが正しく起動するかどうかをリモートで検

証できます。この監視は**ブート整合性監視**と呼ばれます。ブート整合性監視の詳細については、「ブート整合性監視の概要」を参照してください。

ブート整合性監視が有効なカタログの作成については、「ブート整合性監視」を参照してください。

AWSでのMCSIO対応MCSマシンカタログ作成のサポート

AWS環境では、PowerShellコマンドを使用して、MCSストレージ最適化（MCSIO）が有効な非永続カタログを作成できるようになりました。このようなカタログを作成するには、VDAのインストールまたはアップグレード中にMCSIOドライバーをインストールする必要があります。デフォルトでは、このドライバーはインストールされていません。カタログの作成の詳細については、「MCSIO対応カタログ」を参照してください。

MCSで作成されたCitrix ProvisioningカタログのUEFIブートプログラムとCitrix Provisioningバージョンの照合

Citrix Provisioningサーバーは、UEFIブートプログラムを含むBDMディスクを使用します。この機能により、MCSを使用してCitrix Provisioningカタログを作成する際に、`PVSBOOT.INI`ファイルとともに`BOOTX64.EFI`ファイルが生成されます。その結果、ターゲットデバイスは最新のブート設定ファイルから起動でき、ターゲットデバイスがCitrix Provisioningのバージョンと一致するようになります。

オートスケール

Autoscaleを使用してVMを休止状態にする

Autoscaleの構成可能な設定を通じてVMの休止状態をサポートするように、電源管理が強化されました。PowerShellコマンド`Get-BrokerDesktopGroups`、`New-BrokerDesktopGroups`、または`Set-BrokerDesktopGroups`を使用して、パラメーター`AutoscaleScaleDownActionDuringPeak`（ピーク時）または`AutoscaleScaleDownActionDuringOffPeak`（オフピーク時）に次の正の値を設定し、電源アクションを定義します。

- 0: スケールダウン時にVMをシャットダウンする
- 1: スケールダウン時に一時停止（VMを休止状態にする）

休止状態にできないVMはシャットダウンされます。

Autoscaleが休止状態のVMの電源をオンにする

この機能により、Azureでは、Autoscaleは、ピーク時にセッションがない休止状態のマルチセッションRemote Desktop Services (RDS) および共有シングルセッションVMの電源をオンにできます。VMはMCSおよび非MCSマシンカタログのいずれでもかまいません。

アプリケーション

Workspace およびデスクトップでのアプリケーションの可視性を制限する

デフォルトでは、パッケージ化されたアプリケーションはどこでも表示されます。この機能を使用すると、PowerShell を使用して、パッケージ化されたアプリケーションを Workspace に表示するか、ユーザーの VDI デスクトップセッションに展開するかを制御できるようになります。詳細については、「Workspace およびデスクトップでのアプリケーションの可視性を制限する」を参照してください。

プロファイル管理

新機能については、別のドキュメントの「新機能」の記事を参照してください。

シトリックス プロビジョニング

新機能については、別のドキュメントの「新機能」の記事を参照してください。

macOS 用 Citrix バーチャル デリバリー エージェント

新機能については、別のドキュメントの「新機能」の記事を参照してください。

リナックス ブイディーエー

新機能については、別のドキュメントの「新機能」の記事を参照してください。

セッション録画

新機能については、別のドキュメントの「新機能」の記事を参照してください。

ワークスペース環境管理™

新機能については、(/ja-jp/workspace-environment-management/current-release/whats-new.html)の「新機能」の記事を参照してください。

フェデレーション認証サービス

新機能については、(/ja-jp/federated-authentication-service/current-release/whats-new.html)の「新機能」の記事を参照してください。

修正された問題

Citrix Virtual Apps and Desktops™ 7 2503 には、以下の修正された問題が含まれています。

全般

- Azure Arc Onboarding は、Citrix Virtual Apps and Desktops のバージョンではサポートされていません。
- Windows Server 2025 を実行しているマシンに Citrix Virtual Apps and Desktops コンポーネントをインストールするためにメタインストーラーを使用すると、`MsiInstall` イベントがイベントログに書き込まれません。
- Windows 10 から Windows 11 へのインプレース OS アップグレードを実行した後、Citrix Desktop Service が起動に失敗する場合があります。この問題を解決するには、マシンを再起動してください。
- 管理者権限でアプリケーションを実行している場合、FIDO2 に関連付けられた Windows セキュリティダイアログボックスは ICA® セッションウィンドウの前面に表示されません。昇格されたプロセスとして実行されている場合、Windows セキュリティダイアログボックスが ICA セッションウィンドウの背後に隠れるのは、オペレーティングシステムの設計によるものです。
- Windows オペレーティングシステムのアップグレード後に **スタート** メニューにアクセスできなくなる問題が修正されました。
- HDX セッション内で Zoom や Microsoft Teams などのビデオ会議アプリケーションを起動すると、RemotePC ユーザーがクラッシュする可能性がある問題が修正されました。

オーディオ

- シングルセッションVDAで実行されている一部のサードパーティ製アプリケーション（例：ZoomアプリやTeamsアプリ）では、ICAセッションの切断、再接続、またはハードリセット後

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

HDX 接続

- HDX Insight L7 遅延計算が HDX Adaptive Scaling と競合し、L7 遅延測定の不正確さやセッションスループットの低下につながります。回避策として、HDX Insight L7 遅延計算または HDX Adaptive Scaling を無効にすることができます。

Web Studio を使用した Secure Private Access

- ユーザーが タブ > 「ライセンスサーバー URL の追加」リンクから > ページにリダイレクトされると、ナビゲーションバーが部分的にしか表示されません。ナビゲーションバーを表示するには、ページを更新してください。
- 不正確なゲートウェイURLが入力されると、空白の警告ポップアップが表示されます。警告メッセージを表示するには、警告アイコンにカーソルを合わせます。
- コンソールのすべてのタブで、垂直スクロールバーが部分的に表示されます。この問題に対する回避策は不要であり、機能やユーザーエクスペリエンスに影響はありません。
- **設定 > 統合**タブで、ブラウザウィンドウが小さい場合、ページの最下部に水平スクロールバーが表示されません。ブラウザウィンドウが最大化されている場合、水平スクロールバーは不要です。
- **トラブルシューティング**ログで、ログ詳細ダイアログボックスが開いているときに、ページの最下部に垂直スクロールバーが表示されません。この問題に対する回避策は不要であり、機能やユーザーエクスペリエンスに影響はありません。
- Secure Private Accessコンソールにログインするとき、またはWSに戻ってSecure Private Accessコンソールに戻るときに、**概要**タブが強調表示されません。この問題に対する回避策は不要であり、機能やユーザーエクスペリエンスに影響はありません。

Citrix ディレクター

- Director OData API を介して `MonthlyCostSummaries` の OData V4 または V3 リクエストを開始すると、500 内部エラーが発生する可能性があります。

既知の問題

Citrix Virtual Apps and Desktops™ 7 2503 には、以下の既知の問題が含まれています。

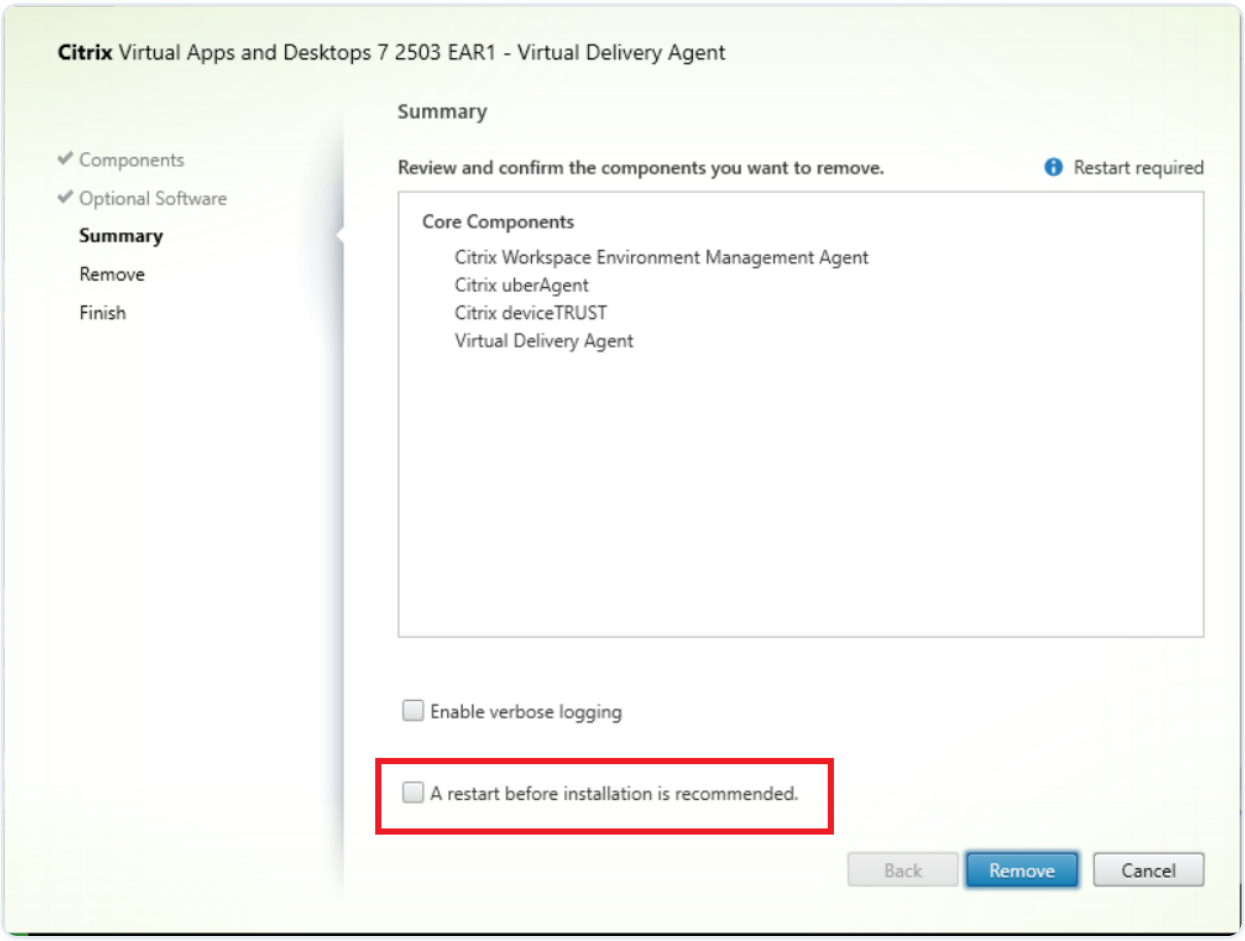
注記

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

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

全般

- Delivery Controller が Citrix Virtual Apps and Desktops 2402 CU1 から 2503 へのアップグレードに失敗します。
- 最初のサイト設定中、Citrix Config Synchronizer Service (CSS) からの構成同期の遅延により、Broker Service は一時的に License Activation Service の設定が `false` に設定された状態で起動します。これにより、同期が完了すると自動的に解決される一度限りのエラーが発生します。
- VDAエージェントのアンインストール時に、メタインストーラーに新しいオプション「**インストール前に再起動することをお勧めします**」が追加されました。ただし、2503 EARリリースではこのチェックボックスが正しく機能しないため、使用しないことをお勧めします。



- アプリバーを起動し、Citrix Workspace™ app for Windows で接続センターメニューを開くと、アプリバーはそれをホストするサーバーの下に表示されません。
- マルチセッションVDAの**セッション制限**設定は、Windows Server 2022、Windows 10 Enterpriseマルチセッション、およびWindows 11 Enterpriseマルチセッションを実行しているセッションホストでは拒否されます。
- Microsoftは、Modern Print Dialogを使用している場合に印刷ジョブ間で印刷設定が保持されない問題があることを確認しており、現在その問題に対処しています。現在の予測では、2025年前半に解決される見込みです。Modern Print Dialogは、Windows 11やWindows Server 2025などの新しいOSバージョンでデフォルトで有効になっています。OSをレガシー印刷ダイアログを使用するように構成するには、次のアクションを実行します。

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

- 管理者権限でアプリケーションを実行している場合、FIDO2 に関連付けられた Windows セキュリティダイアログボックスは ICA® セッションウィンドウの前面に表示されません。昇格されたプロセスとして実行されている場合、Windows セキュリティダイアログボックスが ICA セッションウィンドウの背後に隠れるのは、オペレーティングシステムの設計によるものです。
- Windows 10またはWindows 11マルチセッションOSはWindowsシステム復元をサポートしていません。そのため、UIで復元ポイントを作成するオプションは利用できません。コマンドラインオプションの/EnableRestoreまたは/EnableRestoreCleanupは無視され、「Windows 10/11マルチセッションOSでは現在システム復元はサポートされていません」というメッセージがログに記録されます。
- Citrix Virtual Apps and Desktops 2411 では、Desktop Viewer ツールバーの Connection Strength Indicator (CSI) が正しいプロトコル情報を表示しません。代わりに、CSI の詳細ではプロトコルが N/A と表示されます。
- ポリシー設定の更新とサイトサービスでのBLOBの生成との間に5分間の遅延があります。その結果、ポリシーがセッションに反映されるまでに時間がかかる場合があります。
- ブラウザコンテンツリダイレクトでリダイレクトされたウィンドウで使用した場合、**戻る**ボタンのアクションが機能しないことがあります。
- シングルサインオン (SSO) に拡張ドメインパススルーを使用する場合、ユーザーが最初に接続したときはセッション内のアプリケーションへのSSOは期待どおりに機能します。しかし、ユーザーが切断し、後で同じセッションに再接続すると、セッション内のSSOが機能しなくなることがあります。これは、2025年3月および4月にリリースされたWindowsアップデートで導入されたリグレッションが原因です。この問題が発生しているお客様は、Microsoftにサポートケースをオープンし、追跡ID 2410230030007977を参照することをお勧めします。

Web Studio を使用した Secure Private Access

- 「**設定 > 統合**」タブで、エラーメッセージがダイアログボックスの手前ではなく、その背後に表示されます。この問題に対する回避策はなく、機能やユーザーエクスペリエンスには影響しません。

注：

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

ディレクター

- Director OData APIを介して`MonthlyCostSummaries`のOData V4またはV3リクエストを開始すると、500内部エラーが発生する場合があります。回避策として、Director UIの「**トレンド**

」>「**カスタムレポート**」>「**ODataクエリ**」セクションからODataクエリを使用してください。

マシン作成サービス™

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

プロファイル管理

- Profile Management 2503ドキュメントには、このリリースでの更新に関する具体的な情報が記載されています。

リナックス ブイディーエー

- Linux VDA 2503ドキュメントには、このリリースでの更新に関する具体的な情報が記載されています。

セッション記録

- Session Recording 2503 ドキュメント は、このリリースでの更新に関する詳細情報を提供します。

ワークスペース環境管理™

- Workspace Environment Management 2503 ドキュメント は、このリリースでの更新に関する詳細情報を提供します。

シトリックス プロビジョニング™

- Citrix Provisioning 2503 ドキュメント は、このリリースでの更新に関する詳細情報を提供します。

フェデレーション認証サービス

- Federated Authentication Service 2503 ドキュメント は、このリリースでの更新に関する詳細情報を提供します。

廃止予定

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

廃止予定と削除

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

非推奨

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

項目	非推奨が発表されたバージョン	代替案
`Repair-AcctADAccount` PowerShellコマンドのサポート	2503	次のコマンドを使用してください • `Repair-AcctIdentity`: IDアカウントの現在の状態を変更せずに修復するため。これは、既存のプロビジョニング済みVMの既存の使用中のIDアカウントを修復できます。例えば、Hybrid Azure ADに参加しているIDアカウントの `repair userCertificate` 属性。ADに参加しているIDアカウントの `Repair identity info`（マシンパスワード/信頼キーペアを含む）。 • `Reset-AcctIdentity`: IDアカウントを初期状態にリセットするため

項目	非推奨が発表されたバージョン	代替案
		(例: 汚染済みから利用可能へ)。これにより、汚染されたIDアカウントを利用可能なIDアカウントとしてプールに戻すことができます。
3D HDXグラフィックポリシーの最適化	2411	圧縮に「画面全体」に設定されたビデオコーデックを使用します。`<https://docs.citrix.com/ja-jp/citrix-virtual-apps-desktops/2503/policies/reference/ica-policy-settings/graphics-policy-settings.html#use-video-codec-for-compression>`を参照してください。
NVIDIA GPUハードウェアエンコーディング (NVENC) (以下の場合): vGPU 15以前、およびドライバーバージョン529.19以前。	2411	現在サポートされているNVIDIAドライバーを使用してください: vGPU 16以降、およびドライバーバージョン536.22以降。詳細については、NVIDIAがサポートするvGPUおよびドライバーバージョンに関する

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

項目	非推奨が発表されたバージョン	代替案
MMCベースのStudio	2411	Web Studioを使用してください。
複数モニターフック	2407	-
ドメインパススルー認証	2407	シングルサインオン用の拡張ドメインパススルーを使用してください。
ランデブー V1	2402	Rendezvous V2を使用してください。
セキュア ICA®	2402	Secure HDXを使用してください。
Windows Server 2016でのVDAサポート	2402	最新のWindows Serverバージョンにアップグレードしてください。
Windows Server 2016でのDelivery Controller™、Web Studio、Citrix Director、Citrix License Server、Citrix StoreFront、シングルセッションOS用Server VDI、マルチセッションOS用VDA、Active Directoryフォレストとドメイン、およびUniversal Print Serverのサポート	2402	最新バージョンのWindows Serverにアップグレードしてください。
サイト構成、構成ログ、および監視データベース用の	2402	最新バージョンのMicrosoft SQL Serverにアップグ

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

項目	非推奨が発表されたバージョン	代替案
HDX Graphics におけるプログレッシブモードのサポート	2311	Thinwire を使用します。「プログレッシブモード」を参照してください。(/ja-jp/citrix-virtual-apps-desktops/2503/policies/reference/hdx-registry-settings#progressive-mode).
Internet Explorer 11 でのブラウザコンテンツリダイレクトのサポート	2311	Google Chromeベースのブラウザコンテンツリダイレクトを使用してください。
BrokerでのSQL Server 2016のサポート	2308	最新バージョンを使用してください。詳細については、システム要件を参照してください。
DirectorでのXenApp 5.xのサポート	2308	---
DirectorでのXenApp 6.xのサポート	2308	---
Directorでのアラート用SCOMパック	2308	---
Directorでのプラグインのサポート	2308	---
WebRTC SDP形式（Plan B）のサポート	2308	Citrix Workspace™ アプリをサポートされているバージョンにアップグレードしてください。

項目	非推奨が発表されたバージョン	代替案
Microsoft Teams最適化におけるシングルウィンドウモードのサポート	2308	Citrix Workspaceアプリをマルチウィンドウモードをサポートするバージョンにアップグレードしてください。詳細については、「機能マトリックスとバージョンサポート」を参照してください。
AWS環境で使用される `AwsCaptureInstanceProperties` のサポート	2308	マシンプロファイルを使用します。「マシンプロファイルを使用してカタログを作成する」を参照してください。
`Schedule-ProvVMUpdate` PowerShellコマンド	2305	`Set-ProvVMUpdateTimeWindow` を使用します。
`Request-ProvVMUpdate` PowerShell コマンド	2305	`-StartsNow` と `-DurationInMinutes -1` パラメーターを指定して `Set-ProvVMUpdateTimeWindow` を使用します。
`Cancel-ProvVMUpdate` PowerShell コマンド	2305	`Clear-ProvVMUpdateTimeWindow` を使用します。
`New-ProvScheme` コマンドで使用される	2303	`TenancyType` パラメーターを使用します。

項目	非推奨が発表されたバージョン	代替案
`DedicatedTenancy` パラメーター		
ライセンス サーバー VPX	2206	---
Azure 環境で VM をプロビジョニングするためのアンマネージドディスク。	2206	マネージドディスクを使用する。
ホストからクライアントへの (URL) リダイレクト(/ja-jp/citrix-virtual-apps-desktops/2503/general-content-redirection/bidirectional-content-redirection-configuration/host-to-client-redirection.html)	2203	双方向コンテンツリダイレクト(/ja-jp/citrix-virtual-apps-desktops/2503/general-content-redirection/bidirectional-content-redirection-configuration/bidirectional-content-redirection.html)。
クラウドおよびオンプレミス環境で使用される4つのAWS固有コマンドのサポート: `Revoke-HypSecurityGroupIngress`、`Revoke-HypSecurityGroupEgress`、`Grant-HypSecuritygroupegress`、および `Grant-HypSecurityGroupIngress`。	2203	---

項目	非推奨が発表されたバージョン	代替案
VDAメタインストーラーからのCitrix Files for WindowsおよびCitrix Files for Outlook。	2203	スタンドアロンインストーラーを使用してください。
VDAメタインストーラーからのWEMエージェントコンポーネント。	2203	---
Remote PC Access用のSCCM統合Wake on LANオプション。	2012	スタンドアロンのWake on LAN機能を使用してください。
XenAppおよびXenDesktop、Provisioning Services、StoreFront用Citrix SCOM Management Pack。監視可能な製品バージョンについては、Citrix SCOM Management Packs documentationを参照してください。	1912	展開の監視と管理にはDirectorを使用してください。SCOM EOLと代替策の詳細については、https://support.citrix.com/article/CTX266943を参照してください。
モビリティSDK / モバイルSDK (旧シトリックスラボ製)	7.16	モバイルエクスペリエンスポリシー設定、およびホスト型デスクトップ/アプリのネイティブエクスペリエンスに置き換えられました。

削除

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

項目	廃止が発表されたバージョン	削除されたバージョン	代替策
AWSボリュームワーカーのサポートを削除しました	2311	2503	直接ディスクのアップロードとダウンロードを使用します。直接ディスクのアップロードとダウンロードを参照してください。
SQL Server 2016および2017のサポート	2402および2308	2411	SQL Server 2019および2022を使用します
ディスクキャッシュのみを含み、メモリキャッシュを含まないようにMCS I/Oライトバックキャッシュを構成するサポート	2402	2411	ライトバックキャッシュが有効なマシンを作成する際、**メモリキャッシュサイズ (MB)** オプションを選択し、ゼロ以外のサイズを指定します。
Citrix StudioでのPVSインポートウィザードのサポート	1912 LTSR	2311	以下のいずれかの方法でCitrix Provisioning™マシンをプロビジョニングする

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

項目	廃止が発表されたバージョン	削除されたバージョン	代替策
			Create Citrix Provisioning catalogs in Citrix Studioを参照してください。
Citrix Workspaceアプリ Windows用 1912	---	2402	最新バージョンを使用してください。
HDX Graphics FullScreen + テキスト最適化	2311	2311	
HDX 3D ProでのNVIDIA Frame Buffer Capture (NVFBC) のサポート	2308	2311	Desktop Duplication API (DDAPI) を使用します。
ポリシー設定「インボックスプリンタードライバーの自動インストール」に対するVDAサポート。	7.16	2311	なし。このポリシー設定は、以前のOS（Windows 7、Windows Server 2012 R2以前）上のVDAでのみサポートされています。
NVIDIA GPU ハードウェアエンコーディング (NVENC)	2305	2305	現在サポートされているNVIDIAドライバーを使用して

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

項目	廃止が発表されたバージョン	削除されたバージョン	代替策
するNVIDIA GPU (NVENC)によるハードウェアエンコード。			2003以降のVDAでGRID 10ディスプレイドライバーを使用するか、Citrix Virtual Apps and Desktops 7 1912 LTSR VDAを使用してください。
セルフサービスパスワードリセット (SSPR)機能。	2003	2006	---
VDAおよびコアサーバーコンポーネントに対するバージョン4.8より前のMicrosoft .NET Frameworkバージョンのサポート。Delivery Controller、Studio、Directorが含まれます。	1912	2003	.NET Frameworkバージョン4.8にアップグレードしてください。
Windows Server 2012 R2上のバーチャルデリバリーエージェント。	1912	2003	サポートされているオペレーティングシステムにVDAをインストールしてください。
Citrix Virtual Apps and Desktops Premiumエディ	1909	2003	---

項目	廃止が発表されたバージョン	削除されたバージョン	代替策
ションのAppDNA®アプリケーション移行コンポーネント。			
32ビット (x86) マシンへのStudioのインストール。	1909	2003	サポートされているx64オペレーティングシステムにインストールします。
シームレスアプリケーションにおけるExcelフックのサポート。これは、Microsoft Excel 2010の各ワークブックに対して個別のタスクバーアイコンを作成するために使用されていました。	1909	1909	---
Windows Server 2012 R2（サービスパックを含む）上のコアサーバーコンポーネント。以下が含まれます: Delivery Controller、Studio、Director。	1906	2003	より新しいサポートされているオペレーティングシステムにインストールします。
Microsoft SQL Server 2008 R2、2012、	1906	2003	サポートされているMicrosoft SQL Server

項目	廃止が発表されたバージョン	削除されたバージョン	代替策
2014の各バージョン（すべてのサービスパックとエディションを含む）におけるサイト構成、構成ログ、および監視データベースのサポート。			バージョンにデータベースをインストールします。
x86プラットフォーム上のWindows 10におけるVDAのサポート。	1906	1909*	サポートされているx64オペレーティングシステムにVDAをインストールします。*この機能は、Citrix Virtual Apps and Desktops 7 1912 LTSRで引き続きサポートされています。
Citrix Virtual Apps and Desktopsインストールメディアからの Citrix Smart Tools Agentの削除。	1903	1906	---
Red Hat Enterprise Linux/CentOS 7.5でのLinux VDAのサポート。	1903	1903	Red Hat Enterprise Linuxの以降のバージョンにLinux VDAをインストールします。

項目	廃止が発表されたバージョン	削除されたバージョン	代替策
Citrix Virtual Apps and Desktops（旧XenAppおよびXenDesktop）とCitrix Receiver、およびWorkspace Hub間のTLS 1.0およびTLS 1.1プロトコルに対するStoreFrontのサポート。	7.17	2203	TLS 1.2プロトコルをサポートするCitrix WorkspaceアプリにCitrix Receiverをアップグレードします。Citrix Workspaceアプリの詳細については、https://docs.citrix.com/ja-jp/citrix-workspace-app を参照してください。
ポリシー設定「インボックスプリンタードライバーの自動インストール」に対するVDAのサポート。	7.16	2311	なし。ポリシー設定は、以前のOS (Windows 7、Windows Server 2012 R2およびそれ以前) のVDAでのみサポートされています。
Framehawkディスプレイリモートテクノロジーのサポート	1811	1903	Thinwireをアダプティブトランスポートを有効にして使用します。
すべてのCitrix Virtual Apps and Desktops (およびXenApp and XenDesktop) バージョンにお	1808	1906	電力管理機能の改善のために、Citrix Cloud上のVirtual Apps and Desktops Serviceの使用

項目	廃止が発表されたバージョン	削除されたバージョン	代替策
けるCitrix Smart Scaleのサポート。この機能は、31 May 2019にサポート終了となります。			を検討してください。
Citrix StoreFront、Citrix VDA、Citrix Studio、Citrix Director、およびCitrix Delivery Controllerによる Microsoft .NET Frameworkバージョン4.5.1、4.5.2、4.6、4.6.1、4.6.2、および4.7のサポート。	7.18	1808	.NET Frameworkバージョン4.7.1以降にアップグレードしてください。(インストーラーは、.NET Framework 4.7.1がまだインストールされていない場合、自動的にインストールします。)
Red Hat Enterprise Linux 7.3での Linux VDAのサポート。	7.18	1808	Red Hat Enterprise Linuxの以降のバージョンに Linux VDAをインストールします。
SUSE Linux Enterprise Server 11 Service Pack 4 上での Linux VDA のサポート。	7.16	7.16	サポートされているSUSEバージョンにLinux VDAをインストールします。

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

項目	廃止が発表されたバージョン	削除されたバージョン	代替策
デスクトップコンポジションリダイレクト (以前はDirectX Command Remotingとして知られていました) (DCR)	7.15 LTSR	7.16	Thinwireを使用します。
Windows Server 2012およびWindows Server 2008 R2 (Service Packを含む) 上のコアコンポーネント。含まれるもの: Delivery Controller、Studio、Director、StoreFront、License Server、Universal Print Server。	7.15 LTSR	7.18	サポートされているオペレーティングシステムにコンポーネントをインストールします。
Windows Server 2012およびWindows Server 2008 R2 (Service Packを含む) 上のセルフサービスパスワードリセット (SSPR) 機能	7.15 LTSR	7.18	より新しいサポート対象のオペレーティングシステムにインストールしてください。
Windows 7、Windows 8、およびWindows	7.15 LTSR	7.18	サポート対象のオペレーティングシステムに

項目	廃止が発表されたバージョン	削除されたバージョン	代替策
8.1（Service Packを含む）上のStudio			Studioをインストールしてください。
Flashリダイレクト	7.15 LTSR	1912	ビデオコンテンツはHTML5ビデオとして作成してください。管理対象コンテンツにはHTML5ビデオリダイレクトを、公開Webサイトにはブラウザーコンテンツリダイレクトを使用してください。詳しくは、Flashリダイレクトのサポート終了の注記を参照してください。
StoreFrontとのCitrix Online統合（Goto製品）	7.14（およびStoreFront 3.11）	StoreFront 3.12	---
VDAのインストール中に作成され、VDAマシンのローカル管理者グループに追加されていたユーザーアカウントCtxAppVCOMAdminは、作成されなくなりま	7.14	7.14	WindowsサービスCtxAppVServiceは同じ機能を実行します。これは自動的にインストールおよび構成され、ユーザーによる操作は不要です。

項目	廃止が発表されたバージョン	削除されたバージョン	代替策
した。基盤となる「COM」メカニズムも削除されました。			
Windows Server 2008 32 ビット版での Universal Print Server UpsServer コンポーネントのサポート	7.14	7.14	より新しいサポート対象のオペレーティングシステムにインストールしてください。
Internet Explorer 8 でのストアフロントおよびレシーバー・フォー・ウェブ	7.13	7.13	---
Citrix App-Vコンポーネントのインストールを防止するためのVDAコマンドラインインストールオプション / no_appv	7.13	7.13	コマンドラインインストールオプション / exclude "Citrix Personalization for App-V – VDA" を使用します。
フルプロダクトインストーラーは、新規インストール時にCitrix.Common.Commandsスナップインをインストールしなくなり、既存のインストールをアップグレード	7.13	7.13	Citrix.Common.Commandsスナップインによって提供されていた一部のPowerShellコマンドは、XenApp 6.5 SDKで引き続き利用できます。

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

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

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

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

システム要件

はじめに

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

インストールを開始する前に、インストール準備 を確認してください。

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

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

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

ハードウェア要件

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

次の表に、コアコンポーネントの最小要件を示します。

コンポーネント	最小
すべてのコアコンポーネントとStoreFront™を1台のサーバーにインストールする場合（評価目的のみで、実稼働環境への展開ではない）	5 GB RAM

コンポーネント	最小
すべてのコアコンポーネントとStoreFrontを1台のサーバーにインストールする場合（テスト展開または小規模な実稼働環境向け）	12 GB RAM
Delivery Controller (ローカルホストキャッシュにはより多くのディスク容量が必要です)	5 GB RAM、800 MB ハードディスク、データベース: サイジングガイダンスを参照
スタジオ	1 GB RAM、100 MB ハードディスク
ディレクター	2 GB RAM、200 MB ハードディスク
StoreFront	2 GB RAM、ディスクの推奨事項についてはStoreFrontのドキュメントを参照
ライセンスサーバー	8 GB RAM。ディスクの推奨事項についてはライセンスドキュメントを参照

デスクトップとアプリケーションを提供するVMのサイジング

ハードウェアの提供は複雑で動的な性質を持つため、具体的な推奨事項を提供することはできません。また、すべての展開には固有のニーズがあります。一般的に、Citrix Virtual Apps™ VMのサイジングは、ユーザーのワークロードではなくハードウェアに基づいています。例外はRAMです。より多くのRAMを消費するアプリケーションには、より多くのRAMが必要です。

詳細については、以下を参照してください。

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

マイクロソフト Visual C++

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

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

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

デリバリーコントローラー

サポートされているオペレーティングシステム:

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

要件:

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

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

データベース

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

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

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

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

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

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

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

- コントローラーをインストールする際、ローカルホストキャッシュ機能で使用するために、累積更新プログラム15適用済みのMicrosoft SQL Server Express LocalDB 2022がインストールされます。(このインストールは、サイトデータベース用のデフォルトのSQL Server Expressインストールとは別です。)
- コントローラーをアップグレードする際、既存のMicrosoft SQL Server Express LocalDBのバージョンは自動的にアップグレードされません。交換要件と手順については、「SQL Server Express LocalDBの交換」を参照してください。

その他のデータベース情報:

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

ウェブスタジオ

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

> サポートされているオペレーティングシステム:

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

Citrix ディレクター

サポートされているオペレーティングシステム:

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

要件:

- Microsoft .NET Framework 4.8（またはそれ以降のバージョン）がまだインストールされていない場合、自動的にインストールされます。

- Microsoft Internet Information Services (IIS) 7.0およびASP.NET 2.0。IISサーバーの役割に静的コンテンツの役割サービスがインストールされていることを確認してください。このソフトウェアがまだインストールされていない場合、Windows Serverのインストールメディアを要求するプロンプトが表示され、その後、そのソフトウェアがインストールされます。
- Citrix Directorがインストールされているマシンでイベントログを表示するには、Microsoft .NET Framework 2.0をインストールする必要があります。

シトリックス プロファイル管理：

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

システムセンター オペレーションズマネージャー (SCOM) 統合の要件：

- システムセンター 2012 R2 オペレーションズマネージャー

Directorの表示に対応しているブラウザ:

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

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

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

サポートされているオペレーティングシステム:

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

要件:

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

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

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

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

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

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

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

サポートされているオペレーティングシステム:

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

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

- Microsoft .NET Framework 4.8は、まだインストールされていない場合（またはそれ以降のバージョンがインストールされていない場合）に自動的にインストールされます。

- Microsoft Visual C++ 2015–2022 再頒布可能パッケージ。

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

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

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

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

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

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

ホスト / 仮想化リソース

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

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

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

サポートされているハイパーバイザー:

- **ゼノサーバー (旧 シトリックス ハイパーバイザー™)**

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

詳しくは、「XenServer仮想化環境」を参照してください。

- **マイクロソフト System Center Virtual Machine Manager**

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

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

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

- **Nutanix アクロポリス**

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

  詳細については、「Nutanix仮想化環境」を参照してください。

- **ブイエムウェア vスフィア (vセンター + ESXi)**

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

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

  詳細については、「VMware仮想化環境」を参照してください。

サポートされているパブリッククラウドホスト:

- **アマゾン ウェブ サービス (AWS)**

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

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

- **マイクロソフト アジュール リソース マネージャー**

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

- **Nutanix クラウドおよびパートナーソリューション**

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

- **VMware クラウドおよびパートナーソリューション**

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

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

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

Active Directoryの機能レベル

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

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

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

HDX

オーディオ

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

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

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

HDX ウィンドウズ メディア 配信

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

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

HDX 3D プロ

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

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

- GPUパススルーは以下で利用可能です。
  - XenServer®
  - ニュータニックス AHV
  - VMware vSphereおよびVMware ESX (ここでは仮想Direct Graphics Acceleration (vDGA) と呼ばれます)
- vGPU は以下で利用可能です:

- XenServer
- ニュータニックス AHV
- ヴイエムウェア ヴイスフィア

`<https://docs.citrix.com/ja-jp/citrix-virtual-apps-desktops/2503/graphics/hdx-3d-pro>`を参照してください。

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

グラフィック処理ユニット (GPU):

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

ユーザーデバイス:

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

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

ユニバーサル プリント サーバー

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

UpsServerコンポーネントは以下でサポートされています。

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

要件:

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

詳細については、プリンターのプロビジョニングを参照してください。

その他

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

バージョン互換性の詳細については、製品マトリックスを参照してください。

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

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

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

複数のNICがサポートされています。

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

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

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

この製品はPowerShellバージョン3から5をサポートしています。

技術概要

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

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

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

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

主要コンポーネント

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

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

一般的な展開における主要コンポーネント (/en-us/citrix-virtual-apps-desktops/2503/media/components-new-op.png)

デリバリーコントローラー™

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

- アプリケーションとデスクトップを配信する

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

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

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

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

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

データベース

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

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

仮想デリバリーエージェント (VDA)

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

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

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

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

シトリックス ストアフロント™

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

シトリックス ワークスペース™ アプリ

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

スタジオ

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

Web スタジオ

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

詳細については、「Web Studioのインストール」(/ja-jp/citrix-virtual-apps-desktops/2503/install-configure/install-core/install-web-studio.html)を参照してください。

シトリックス スタジオ

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

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

セキュア プライベート アクセス

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

シトリックス ディレクター

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

Directorには以下が表示されます。

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

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

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

Citrixライセンスサーバー

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

ハイパーバイザーまたはその他のサービス

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

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

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

追加コンポーネント

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

シトリックス プロビジョニング™

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

シトリックス ゲートウェイ

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

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

シトリックス SD-WAN™

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

一般的な展開の仕組み

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

展開におけるコンポーネント間の通信(/en-us/citrix-virtual-apps-desktops/2503/media/deployment-overview.png)

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

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

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

ユーザー接続の処理方法

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

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

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

ユーザー接続フロー(/en-us/citrix-virtual-apps-desktops/2503/media/user-connections.png)

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

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

Controllerはユーザーの資格情報とともにVDAにメッセージを送信し、その後、ユーザーと接続に関するすべてのデータをVDAに送信します。VDAは接続を受け入れ、同じ経路を通じてCitrix Workspaceアプリに情報を送り返します。StoreFrontで必要なパラメータのセットが収集されます。これらのパラメータは、Citrix WorkspaceアプリとStoreFront間のプロトコル会話の一部として、または独立コンピューティングアーキテクチャ (ICA) ファイルに変換されてダウンロードされる形で、Citrix Workspaceアプリに送信されます。サイトが適切に設定されていれば、このプロセス全体を通じて資格情報は暗号化されたままです。

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

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

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

データアクセスが機能する方法

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

展開におけるデータアクセス(/en-us/citrix-virtual-apps-desktops/2503/media/data-access.png)

Controller内では、ブローカーサービスがリアルタイムデータを提供するマシンのすべてのセッションのセッションデータを報告します。モニターサービスもリアルタイムデータを追跡し、監視データベースに履歴データとして保存します。

Studioはブローカーサービスとのみ通信します。リアルタイムデータのみにアクセスします。Directorは、ブローカーエージェントのプラグインを介してブローカーサービスと通信し、サイトデータベースにアクセスします。

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

デスクトップとアプリケーションの配信

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

マシンカタログ

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

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

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

有効なマシンタイプは次のとおりです。

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

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

デリバリーグループ

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

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

デリバリーグループのユーザーがアクセスできるリソースを定義します。たとえば、異なるアプリケーションを異なるユーザーに配信するには、1つのカタログのマスターイメージにすべてのアプリケーションをインストールし、そのカタログに十分な数のマシンを作成して、複数のデリバ

リーグループに分散させることができます。その後、各デリバリーグループを構成して、マシンにインストールされているアプリケーションの異なるサブセットを配信できます。

詳細については、デリバリーグループの作成 を参照してください。

アプリケーショングループ

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

詳細については、「」(/ja-jp/citrix-virtual-apps-desktops/2503/install-configure/application-groups-create.html)を参照してください。

詳細情報

- Citrix Virtual Apps and Desktopsに関する図
- ネットワークポート
- データベース
- サポートされるハイパーバイザーおよびその他のサービス

データベース

> **注:**

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

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

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

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

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

Citrixは、データベースに関して以下を推奨します。

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

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

高可用性

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

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

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

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

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

サイト内のすべてのControllerが失敗した場合、VDAを高可用性モードで動作するように構成でき、これによりユーザーはデスクトップとアプリケーションへのアクセスを継続できます。高可用性モードでは、VDAはControllerによって仲介される接続ではなく、ユーザーからの直接ICA接続を受け入れます。この機能は、すべてのControllerとの通信が失敗するまれな場合にのみ使用してください。この機能は、他の高可用性ソリューションの代替ではありません。詳しくは、「CTX127564」を参照してください。

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

データベースソフトウェアのインストール

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

> デフォルトでは、そのサーバーで別のSQL Serverインスタンスが検出されない場合、最初のDelivery Controller™をインストールするときにSQL Server Expressエディションがインストールされます。このデフォルトのアクションは、概念実証またはパイロット展開には通常

> 十分です。ただし、SQL Server ExpressはMicrosoftの高可用性機能をサポートしていません。

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

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

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

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

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

サイト作成ウィザードからデータベースをセットアップする

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

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

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

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

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

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

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

自動セットアップ

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

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

スクリプトによるセットアップ

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

1. サイト作成ウィザードの**データベース**ページで、**手動でセットアップするためのスクリプトを生成**を選択します。この操作により、以下の主要データベースとレプリカデータベース（サイト、監視、ログデータベース）それぞれについて、次の3種類のスクリプトが生成されます。

    - *名前に「SysAdmin」を含むスクリプト*。データベースとDelivery Controllerのログインを作成するスクリプトです。これらのタスクにはsecurityadmin権限が必要です。
    - *名前に「DbOwner」を含むスクリプト*。データベースにユーザーロールを作成し、ログインを追加し、データベーススキーマを作成するスクリプトです。これらのタスクには `db_owner` 権限が必要です。

- *名前に「Mixed」を含むスクリプト*。必要な権限に関係なく、すべてのタスクを1つのスクリプトにまとめたものです。

スクリプトの保存場所を指定できます。

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

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

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

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

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

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

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

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

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

データベースのセットアップに必要な権限

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

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

操作	目的	サーバーロール	データベースロール
スキーマを更新する	スキーマの更新またはホットフィックスを適用する		`db_owner`

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

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

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

優先データベース権限スクリプト

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

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

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

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

詳細については、コマンドレットのヘルプを参照してください。

データベースアドレスの形式

データベースアドレスは、次のいずれかの形式で指定できます。

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

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

データベースの場所を変更する

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

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

データベースの場所を変更するには：

1. Microsoft SQL Server を使用している場合は、データベースを配置するサーバーにサポートされているバージョンがインストールされていることを確認してください。必要に応じて、高可用性機能をセットアップします。
2. Web Studio にサインインし、左ペインで **設定** を選択します。
3. **データベース** タイルを見つけて、**編集** を選択します。
4. 「**データベースの管理**」ページで、新しい場所を指定するデータベースを選択し、アクションバーで「**データベースの変更**」を選択します。
5. 新しい場所とデータベース名を指定します。データベースがAzure SQLでホストされている場合、データベースを管理する権限を持つサービスプリンシパルの資格情報を入力します。

6. Web Studioにデータベースを作成させたい場合で、適切な権限がある場合は、「**完了**」をクリックします。プロンプトが表示されたら「**完了**」をクリックすると、Web Studioが自動的にデータベースを作成します。Web Studioは、ユーザーの資格情報を使用してデータベースへのアクセスを試行します。失敗した場合は、データベースユーザーの資格情報の入力を求められます。その後、Web Studioはデータベーススキーマをデータベースにアップロードします。資格情報は、データベース作成期間中のみ保持されます。
7. Web Studioにデータベースを作成させたくない場合、または十分な権限がない場合は、「**データベーススクリプトの生成**」をクリックします。生成されたスクリプトには、必要に応じてデータベースとミラーデータベースを手動で作成するための手順が含まれています。スキーマをアップロードする前に、データベースが空であり、少なくとも1人のユーザーがデータベースにアクセスして変更する権限を持っていることを確認してください。

詳細情報

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

配信方法

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

はじめに

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

- **インストール済みアプリ:** アプリケーションはベースデスクトップイメージの一部です。インストールプロセスには、レジストリの変更に加えて、dll、exe、およびその他のファイルをイメージドライブにコピーする作業が含まれます。詳しくは、「マシンカタログの作成」を参照してください。
- **ストリーミングアプリ (Microsoft App-V):** アプリケーションはプロファイルされ、オンデマンドでネットワーク経由でデスクトップに配信されます。アプリケーションファイルとレジストリ設定は、仮想デスクトップ上のコンテナに配置され、ベースオペレーティングシステムおよび相互から分離されます。この分離により、互換性の問題に対処できます。詳しくは、「App-Vアプリケーションの展開と配信」を参照してください。

- **レイヤー化されたアプリ (Citrix App Layering):** 各レイヤーには、単一のアプリケーション、エージェント、またはオペレーティングシステムが含まれています。1つのOSレイヤー、1つのプラットフォームレイヤー（VDA、Citrix Provisioningエージェント）、および多数のアプリケーションレイヤーを統合することで、管理者は新しい展開可能なイメージを簡単に作成できます。レイヤー化により、OS、エージェント、およびアプリケーションが単一のレイヤーに存在するため、継続的なメンテナンスが簡素化されます。レイヤーを更新すると、そのレイヤーを含むすべての展開済みイメージが更新されます。詳しくは、「Citrix App Layering」を参照してください。
- **ホスト型Windowsアプリ:** マルチユーザーのCitrix Virtual Appsホストにインストールされ、デスクトップではなくアプリケーションとして展開されるアプリケーションです。ユーザーは、VDIデスクトップまたはエンドポイントデバイスからホスト型Windowsアプリにシームレスにアクセスでき、アプリがリモートで実行されているという事実を意識することはありません。詳しくは、「デリバリーグループの作成」を参照してください。
- **ローカルアプリ:** エンドポイントデバイスに展開されるアプリケーションです。アプリケーションインターフェイスは、エンドポイントで実行されているにもかかわらず、ユーザーのホスト型VDIセッション内に表示されます。詳しくは、「ローカルアプリアクセスとURLリダイレクト」を参照してください。

デスクトップの場合は、公開デスクトップまたはVDIデスクトップを検討してください。

Citrix Virtual Apps™の公開アプリとデスクトップ

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

ユースケース:

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

利点と考慮事項:

- データセンター内で管理可能でスケーラブルなソリューション。
- 最も費用対効果の高いアプリケーション配信ソリューション。

- ホストされたアプリケーションは一元的に管理され、ユーザーはアプリケーションを変更できません。これにより、一貫性があり、安全で、信頼性の高いユーザーエクスペリエンスが提供されます。
- ユーザーはアプリケーションにアクセスするためにオンラインである必要があります。

ユーザーエクスペリエンス:

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

アプリケーションの処理、ホスト、および配信:

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

セッション管理と割り当て:

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

  例えば、ユーザーがログオンしてアプリケーションを要求すると、そのマシン上の1つのセッションは他のユーザーには利用できなくなります。2人目のユーザーがログオンし、そのマシンがホストするアプリケーションを要求すると、同じマシン上の2つ目のセッションも利用できなくなります。両方のユーザーがさらにアプリケーションを要求しても、ユーザーは同じセッションを使用して複数のアプリケーションを実行できるため、追加のセッションは必要ありません。さらに2人のユーザーがログオンしてデスクトップを要求し、同じマシン上で2つのセッションが利用可能であれば、その単一のマシンは4つの異なるユーザーをホストするために4つのセッションを使用していることになります。

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

VMホスト型アプリ

シングルセッションOSマシンを使用して、VMホスト型アプリケーションを提供します。

ユースケース:

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

利点と考慮事項:

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

ユーザーエクスペリエンス：

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

アプリケーションの処理、ホスト、および配信：

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

セッション管理と割り当て：

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

VDIデスクトップ

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

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

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

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

- **ランダム非永続デスクトップ（プールされたVDIデスクトップとも呼ばれる）：** ユーザーがこれらのデスクトップのいずれかにログオンするたびに、そのユーザーはデスクトップのプールから選択されたデスクトップに接続します。このプールは単一のマスターイメージに基づいています。デスクトップへのすべての変更は、マシンが再起動すると失われます。
- **静的非永続デスクトップ：** 最初のログオン時に、ユーザーはデスクトップのプールからデスクトップを割り当てられます。（プール内の各マシンは単一のマスターイメージに基づいてい

ます。）最初の使用後、ユーザーがデスクトップを使用するためにログオンするたびに、そのユーザーは最初の使用時に割り当てられたのと同じデスクトップに接続します。デスクトップへのすべての変更は、マシンが再起動すると失われます。

- **静的永続デスクトップ:** 他の種類のVDIデスクトップとは異なり、ユーザーはこれらのデスクトップを完全にパーソナライズできます。最初のログオン時に、ユーザーはデスクトッププールからデスクトップを割り当てられます。そのユーザーによるその後のログオンは、初回使用時に割り当てられた同じデスクトップに接続します。デスクトップへの変更は、マシンの再起動後も保持されます。

リモートPCアクセス

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

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

詳細については、Remote PC Accessを参照してください。

HDX™

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

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

仮想チャネル(/en-us/citrix-virtual-apps-desktops/2503/media/hdx-vir-channels.png)

HDX は、次の3つの技術原則に基づいて設計されています。

- インテリジェントなリダイレクト
- アダプティブ圧縮
- データ重複排除

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

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

  適応型圧縮(/en-us/citrix-virtual-apps-desktops/2503/media/hdx-adaptive-compression.png)
- **データ重複排除** - ネットワークトラフィックの重複排除は、クライアントとサーバー間で送信される集約データを削減します。これは、ビットマップグラフィック、ドキュメント、印刷ジョブ、ストリーミングメディアなど、一般的にアクセスされるデータ内の繰り返されるパターンを利用することで実現されます。これらのパターンをキャッシュすることで、変更のみがネットワーク経由で送信され、重複するトラフィックが排除されます。HDX は、マルチメディアストリームのマルチキャストもサポートしています。これは、ソースからの単一の送信が、各ユーザーへの1対1の接続ではなく、1つの場所で複数のサブスクライバーによって表示されるものです。

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

デバイス上での動作

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

ネットワーク上

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

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

データセンター内

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

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

HDX インサイト

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

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

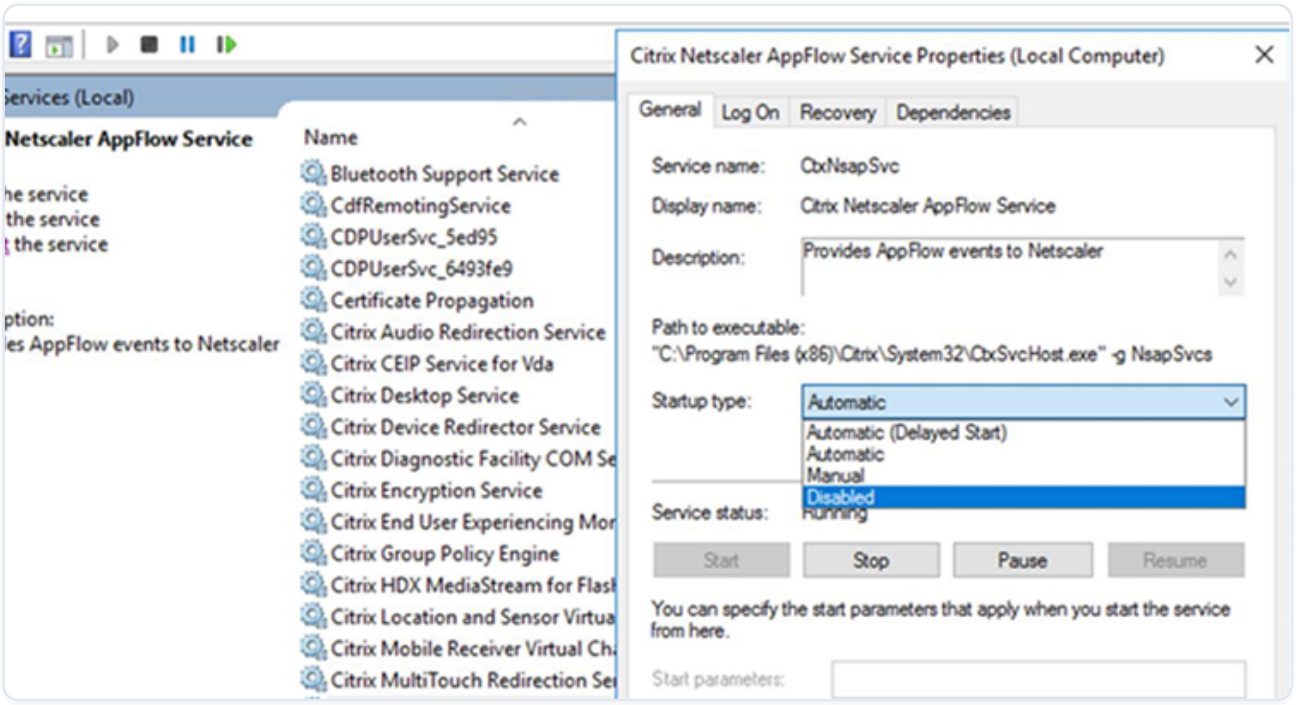
最小要件:

- NetScaler バージョン 12.0 ビルド 57.x

- Windows版 Citrix Workspace™ アプリ 1808
- Windows版 Citrix レシーバー 4.10
- シトリックス ワークスペースアプリ for Mac 1808
- シトリックス レシーバー for Mac 12.8

HDX Insight仮想チャネルを有効または無効にする

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



仮想デスクトップでHDX機能を体験する

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

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

  b. ブラウザコンテンツリダイレクトが仮想デスクトップへのマルチメディアコンテンツの配信をどのように高速化するかを体験するには、YouTubeなどのHTML5ビデオを含むWebサイトからデスクトップでビデオを視聴します。ユーザーはブラウザコンテンツリダイレクトが実行されていることを知りません。ブラウザコンテンツリダイレクトが使用されているかどうかを確認するには、ブラウザウィンドウを素早くドラッグします。ビューポート

とユーザーインターフェイスの間に遅延またはフレーム外の表示が見られます。また、Webページを右クリックしてメニューで**About HDX Browser Redirection**を探すこともできます。

- HDXが高品位オーディオをどのように配信するかを確認するには：

  a. 最大のオーディオ品質が得られるようにCitrixクライアントを構成します。詳細については、Citrix Workspaceアプリのドキュメントを参照してください。

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

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

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

知っておくと良いこと：

- HDX機能のサポートと要件については、「システム要件」の記事を参照してください。特に記載がない限り、HDX機能はサポートされているWindowsマルチセッションOSおよびWindowsシングルセッションOSマシン、およびリモートPCアクセスデスクトップで利用できます。
- このコンテンツでは、ユーザーエクスペリエンスの最適化、サーバーのスケーラビリティの向上、または帯域幅要件の削減方法について説明します。Citrixポリシーとポリシー設定の使用方法については、このリリースの「Citrixポリシー」ドキュメントを参照してください。
- レジストリの編集を含む手順については、注意して使用してください。レジストリを誤って編集すると、オペレーティングシステムの再インストールが必要になるような深刻な問題が発生

する可能性があります。Citrixは、レジストリエディターの誤った使用によって生じる問題が解決できることを保証できません。レジストリエディターは自己責任で使用してください。編集する前に必ずレジストリをバックアップしてください。

自動クライアント再接続とセッションの信頼性

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

自動クライアント再接続：

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

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

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

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

デフォルトの自動クライアント再接続設定：

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

詳細については、(/ja-jp/citrix-virtual-apps-desktops/2503/policies/reference/ica-policy-settings/auto-client-reconnect-policy-settings.html)のを参照してください。

セッションの信頼性:

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

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

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

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

デフォルトのセッションの信頼性設定

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

詳細については、(/ja-jp/citrix-virtual-apps-desktops/2503/policies/reference/ica-policy-settings/session-reliability-policy-settings.html)のを参照してください。

NetScalerと自動クライアント再接続およびセッションの信頼性:

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

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

HDX アダプティブスループット

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

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

> **重要:**

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

> この機能には、以下の要件があります。

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

ユーザーデバイスに送信される画質の向上

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

- 視覚品質。ユーザーデバイスに表示される画像の視覚品質を制御します：中、高、常にロスレス、ビルドトゥロスレス（デフォルト = 中）。デフォルト設定の「中」を使用した場合の実際のビデオ品質は、利用可能な帯域幅によって異なります。
- ターゲットフレームレート。仮想デスクトップからユーザーデバイスに送信される1秒あたりの最大フレーム数を指定します（デフォルト = 30）。CPUが遅いデバイスの場合、低い値を指定するとユーザーエクスペリエンスが向上する可能性があります。1秒あたりの最大サポートフレームレートは60です。

- 表示メモリ制限。セッションの最大ビデオバッファサイズをキロバイト単位で指定します（デフォルト = 65536 KB）。より深い色深度と高い解像度を必要とする接続の場合、制限を増やします。必要な最大メモリを計算できます。

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

ビデオ会議のパフォーマンスを向上させる

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

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

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

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

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

ネットワークトラフィックの優先順位

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

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

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

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

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

警告:

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

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

- マルチポートポリシー - この設定は、複数の接続にわたるICAトラフィックのポートを指定し、ネットワークの優先順位を確立します。
    - CGPデフォルトポート優先順位リストから優先順位を選択します。デフォルトでは、プライマリポート（2598）は高優先順位です。

    - 必要に応じて、CGP port1、CGP port2、CGP port3にさらにCGPポートを入力し、それぞれの優先順位を識別します。各ポートには一意の優先順位が必要です。

  追加のTCPトラフィックを許可するように、VDA上のファイアウォールを明示的に構成します。

- マルチストリームコンピューター設定 - この設定はデフォルトで無効になっています。環境でマルチストリームをサポートするCitrix NetScaler SD-WANを使用している場合、この設定を構成する必要はありません。目的のQuality of Serviceを実現するために、サードパーティ製ルーターまたはレガシーNetScaler SD-WANを使用する場合は、このポリシー設定を構成してください。
- マルチストリームユーザー設定 - この設定はデフォルトで無効になっています。

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

リモート言語バーを表示または非表示にする

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

VDAから言語バー機能のクライアント制御を無効にするには：

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

Unicodeキーボードマッピング

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

Unicode キーボードレイアウトマッピングを有効または無効にする

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

KEY_LOCAL_MACHINE/SOFTWARE/Citrix/CtxKlMap

名前: EnableKlMap

種類: DWORD

値: 1

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

Unicodeキーボードレイアウトマッピング互換モードを有効にする

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

HKEY_LOCAL_MACHINE/SOFTWARE/Citrix/CtxKlMap

名前: DisableWindowHook

種類: DWORD

値: 1

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

Citrix ICA® 仮想チャネル

> **警告:**

> レジストリを誤って編集すると、オペレーティングシステムの再インストールが必要になるような深刻な問題が発生する可能性があります。Citrixは、レジストリエディターの誤った使用によって生じる問題が解決できることを保証できません。レジストリエディターは、ご自

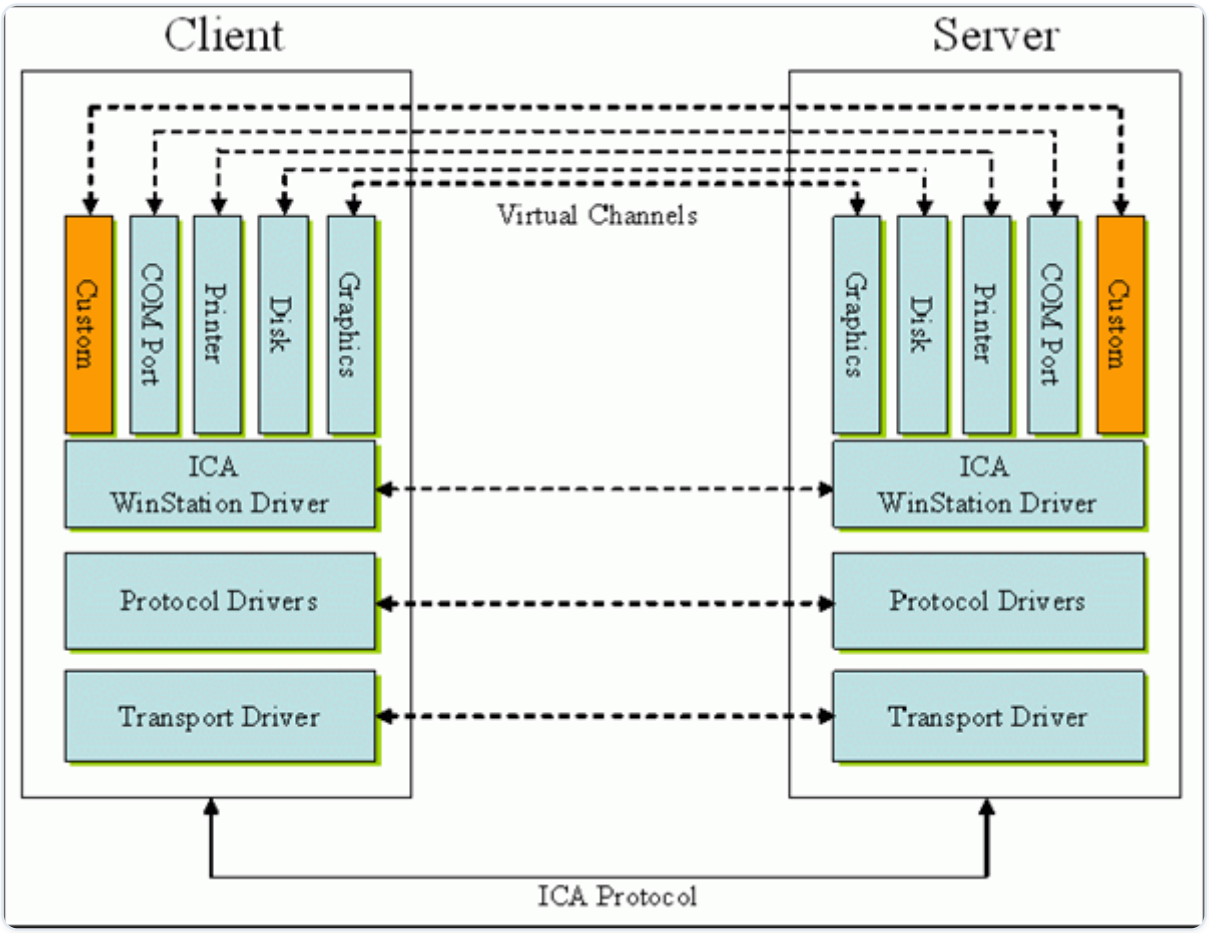
> 身の責任において使用してください。編集する前に、必ずレジストリをバックアップしてください。

ICA仮想チャネルとは何ですか?

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

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

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



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

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

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

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

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

または

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

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

> **注:**

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

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

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

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

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

64ビット互換性

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

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

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

汎用USB仮想チャネル

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

- ctxusbm.sys
- ctxusbr.sys

ICA仮想チャネルの仕組み

仮想チャネルは複数の方法でロードされます。シェル（サーバーの場合はWfShell、ワークステーションの場合はPicaShell）は一部の仮想チャネルをロードします。一部の仮想チャネルはWindowsサービスとしてホストされます。

シェルによってロードされる仮想チャネルモジュール（例）：

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

いくつかカーネルモードとしてロードされるものがあります。例:

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

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

サーバー側のグラフィック仮想チャネル

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

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

Windowsサービスでの特殊チャネルのホスティング

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

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

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

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

仮想チャネル接続(/en-us/citrix-virtual-apps-desktops/2503/media/virtual-channel-connection.png)

この概要では、仮想チャネルを使用したクライアント-サーバー間のデータ交換について説明します。

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

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

> **注:**

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

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

注:

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

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

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

重要:

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

仮想チャネルのパススルー機能

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

次の機能は、シングルホップまたはマルチホップで同じように動作します。

- クライアント COM ポートマッピング
- クライアントドライブマッピング
- クライアントプリンターマッピング
- クライアント UPD
- エンドユーザーエクスペリエンスモニタリング
- 汎用 USB
- ケルベロス

- マルチメディア サポート
- スマートカード サポート
- 透過キーパススルー
- ツイン

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

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

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

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

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

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

以下の従来の仮想チャネルとその機能をサポートしています。

- クライアント
- クライアントCOMポートマッピング
- クライアントドライブマッピング

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

セキュリティとICA仮想チャネル

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

ベストプラクティス

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

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

仮想チャネルの命名:

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

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

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

ダブルホップサポート:

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

参照

- ICA仮想チャネルSDK

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

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

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

ダブルホップ(/en-us/citrix-virtual-apps-desktops/2503/media/double-hop.png)

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

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

システム要件

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

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

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

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

限られた範囲で技術サポートを提供できます。トラブルシューティングの一環として、最初のホップにCitrix Virtual Desktopが必要になる場合があります。

ダブルホップにおけるHDX™の展開に関する考慮事項

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

グラフィック

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

遅延

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

マルチメディア

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

USBデバイスのリダイレクト

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

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

注:

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

サポートの例外

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

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

インストールと構成

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

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

準備

インストール準備 を確認し、必要なタスクをすべて完了します。

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

コアコンポーネントのインストール

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

サイトの作成

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

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

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

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

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

オプションコンポーネントのインストール

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

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

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

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

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

マシンカタログを作成する

Studioでサイトを作成した後、マシンカタログの作成に誘導されます。

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

デリバリーグループを作成する

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

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

アプリケーショングループを作成する (オプション)

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

既知の制限事項

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

マシンID

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

マシンIDの種類

次のマシンIDの種類がサポートされています。

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

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

サポートされる構成

以下は、各シナリオでサポートされる構成の詳細です。

サポートされるインフラストラクチャ

マシンID	シトリックス VIRTUAL APPS AND DESKTOPS ™	シトリックス WORKSPACE™	シトリックス ストアフロント	シトリックス ゲートウェイ サービス	CITRIX GATEWAY (シトリックス ゲートウェイ)
AD参加済み	はい	はい	はい	はい	はい
Azure Active Directory参加済み	いいえ	はい	いいえ	はい	いいえ
ハイブリッド Azure AD 参加済み	はい	はい	はい	はい	はい
ドメイン非参加	はい	はい	いいえ	はい	いいえ

サポートされているワークスペース認証IDプロバイダー

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

Active Directoryに参加済み

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

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

この製品は以下をサポートします。

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

類の展開では、Controllerおよび仮想デスクトップのコンピューターアカウントを含むドメインが、ユーザーアカウントを含むドメインを信頼する必要があります。フォレストの信頼または外部の信頼を使用できます。この種類の展開では、すべてのドメイン機能レベルとフォレスト機能レベルがサポートされます。

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

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

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

複数のActive Directoryフォレスト環境に展開する

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

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

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

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

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

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

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

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

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

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

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

- 名前: `SupportMultipleForestDdcLookup`
- 種類: `REG_DWORD`

- データ: `0x00000001 (1)`

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

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

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

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

外部信頼が設定されている場合は、VDAで次の変更を行います。

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

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

次の表に、サポートされている信頼の種類を示します。

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

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

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

次のステップ

オンプレミスのActive Directory (AD) に参加しているマシンIDのIDプールを作成する方法については、オンプレミスのActive Directoryに参加しているマシンIDのIDプールを参照してください。

ハイブリッド Azure Active Directory 参加済み

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

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

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

> **注:**

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

ハイブリッド Azure Active Directory 参加済みの要件

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

ハイブリッド Azure Active Directory 参加済みの制限事項

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

Hybrid Azure Active Directory参加済みに関する考慮事項

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

  a. `gpedit.msc` を実行します。

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

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

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

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

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

$MaxCount = 60



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

{

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

  {

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

    if ($provider -eq 'Citrix')

    {

        break;

    }
```

```
    if ($provider -eq 1)

    {

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

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

        Start-Sleep 5

        dsregcmd /join

        break

    }

  }



  Start-Sleep 1

}
```

- デフォルトでは、Azure AD Connectは30分ごとに同期します。プロビジョニングされたマシンがHybrid Azure AD参加済みになるまで、初回起動時に最大30分かかる場合があります。

Microsoft Intuneに登録されているHybrid Azure AD参加済みカタログ

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

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

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

この機能を有効にする前に、以下を確認してください:

- お使いのAzure環境がMicrosoft Intuneを使用するためのライセンス要件を満たしていること。詳細については、Microsoftドキュメントを参照してください。

- 共同管理が有効になっている有効なConfiguration Manager展開があること。詳細については、Microsoftドキュメントを参照してください。

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

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

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

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

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

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

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

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

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

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

でください。SCCMServerは、お使いの環境のSCCMサーバー名です。詳細については、Microsoftドキュメントを参照してください。

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

  キー:

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

  値の名前: `MdmSccmSiteCode`

  値の型: **String**

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

次のステップ

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

ドメインに参加していない

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

要件

- コントロールプレーン: サポートされる構成を参照
- VDAタイプ: シングルセッション（デスクトップのみ）またはマルチセッション（アプリおよびデスクトップ）
- VDAバージョン: 2311以降
- プロビジョニングタイプ: Machine Creation Services™ (MCS)、永続的および非永続的
- 割り当てタイプ: 専用およびプール
- ホスティングプラットフォーム: MCSでサポートされるすべてのプラットフォーム

- Rendezvous V2を有効にする必要があります

制限事項

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

VDAのインストールと構成

VDAをインストールする手順に従ってください。

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

    Azure AD構成1(/en-us/citrix-virtual-apps-desktops/2503/media/azure-ad-config-1.png)

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

    Azure AD構成2(/en-us/citrix-virtual-apps-desktops/2503/media/azure-ad-config-2.png)

次のステップ

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

インストール準備

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

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

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

> **注:**

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

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

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

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

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

インストール前に確認する情報

- 技術概要：製品とそのコンポーネントに慣れるため。
- セキュリティ：展開環境を計画する際。
- 既知の問題：このバージョンで発生する可能性のある問題。

- データベース：システムデータベースとその構成方法について学習します。Controllerのインストール中に、サイトデータベースとして使用するSQL Server Expressをインストールできます。ほとんどのデータベース情報は、コアコンポーネントのインストール後にサイトを作成する際に構成します。
- Remote PC Access：ユーザーがオフィスにある物理マシンにリモートでアクセスできる環境を展開する場合。
- 接続とリソース：アプリケーションおよびデスクトップ用のVMをホストまたはプロビジョニングするためにハイパーバイザーまたはその他のサービスを使用している場合。最初の接続は、サイトを作成する際（コアコンポーネントのインストール後）に構成できます。それまでに仮想化環境をセットアップしてください。
- Microsoft System Center Configuration Manager：ConfigMgrを使用してアプリケーションとデスクトップへのアクセスを管理している場合、またはRemote PC AccessでWake on LAN機能を使用している場合。
- **パブリッククラウドホスト接続：** ハイブリッド権限ライセンスをお持ちの場合、パブリッククラウドへのホスト接続を作成できます。ハイブリッド権限ライセンスに関する情報については、「ハイブリッド権限の更新」を参照してください。パブリッククラウドの資格とこの変更の理由に関する情報については、「CTX270373」を参照してください。

コンポーネントのインストール場所

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

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

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

  他のサーバーに他のコンポーネントをインストールする前に、Citrix License Serverとライセンスをインストールしてください。

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

1台のサーバーにDelivery Controller™とマルチセッションOS用VDAの両方をインストールできます。インストーラーを起動し、Delivery Controller（およびそのマシンにインストールしたいその他のコアコンポーネント）を選択します。その後、インストーラーを再度起動し、マルチセッションOS用の**Virtual Delivery Agent**を選択します。

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

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

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

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

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

> **ヒント:**
>
> デフォルト値は`HostTime="UTC"`です。この値をUTC以外のもの（例: `Local`）に変更します。この変更により、ホストとの時刻同期が実質的に無効になります。

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

コンポーネントをインストールしてはいけない場所:

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

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

権限とActive Directoryの要件

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

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

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

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

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

詳細については、以下を参照してください。

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

インストールのガイダンス、考慮事項、およびベストプラクティス

いずれかのコンポーネントのインストール中

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

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

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

- 通常、コンポーネントに前提条件がある場合、インストーラーはそれらが存在しない場合に展開します。一部の前提条件では、マシンの再起動が必要になる場合があります。
- インストール前、インストール中、インストール後にオブジェクトを作成するときは、各オブジェクトに一意の名前を指定してください。たとえば、ネットワーク、グループ、カタログ、リソースには一意の名前を付けてください。
- コンポーネントが正常にインストールされなかった場合、インストールはエラーメッセージとともに停止します。正常にインストールされたコンポーネントは保持されます。それらを再インストールする必要はありません。
- コンポーネントをインストール（またはアップグレード）すると、Citrix Analytics が自動的に収集されます。デフォルトでは、インストールが完了するとそのデータは自動的にCitrixにアップロードされます。また、コンポーネントをインストールすると、匿名データをアップロードするCitrixカスタマーエクスペリエンス向上プログラム（CEIP）に自動的に登録されます。

  インストール中に、メンテナンスとトラブルシューティングのための診断情報を収集する他のCitrixテクノロジーに参加することも選択できます。これらのプログラムの詳細については、「Citrix Insight Services」を参照してください。
- Studioをインストール（またはアップグレード）すると、Google Analyticsが自動的に収集され（その後アップロードされます）、インストール後にレジストリキー `HKLM\Software\Citrix\DesktopStudio\GAEnabled` でこの設定を変更できます。値が**1**の場合、収集とアップロードが有効になり、**0**の場合、収集とアップロードが無効になります。
- VDAのインストールが失敗した場合、MSIアナライザーは失敗したMSIログを解析し、正確なエラーコードを表示します。既知の問題である場合、アナライザーはCTX記事を提案します。アナライザーは、失敗エラーコードに関する匿名化されたデータも収集します。このデータは、CEIPによって収集された他のデータに含まれます。CEIPへの登録を終了すると、収集されたMSIアナライザーデータはCitrixに送信されなくなります。

VDAのインストール中

- Windows用Citrix Workspace™アプリは利用可能ですが、VDAをインストールする際にはデフォルトではインストールされません。ユーザーまたは管理者は、Citrix Webサイトから Windows用Citrix Workspaceアプリおよびその他のCitrix Workspaceアプリをダウンロード、イ

ンストール（およびアップグレード）できます。または、StoreFrontサーバーからこれらのCitrix Workspaceアプリを利用可能にすることもできます。StoreFrontのドキュメントを参照してください。

- Microsoft Print Spoolerサービスは有効にする必要があります。このサービスが無効になっている場合、VDAを正常にインストールすることはできません。
- ほとんどのサポートされているWindowsエディションには、Microsoft Media Foundationがすでにインストールされています。マシンにMedia Foundationがない場合（Nエディションなど）、いくつかのマルチメディア機能はインストールされず、動作しません。
  - Windows Mediaリダイレクト
  - HTML5ビデオのリダイレクト
  - HDX™ RealTimeウェブカメラのリダイレクト

  制限を認識するか、VDAのインストールを終了して、Media Foundationのインストール後に再開することができます。グラフィカルインターフェイスでは、この選択肢はメッセージで表示されます。コマンドラインでは、`/no_mediafoundation_ack` オプションを使用して制限を認識できます。
- VDAをインストールすると、**Direct Access Users**という新しいローカルユーザーグループが自動的に作成されます。シングルセッションOS用VDAでは、このグループはRDP接続にのみ適用されます。マルチセッションOS用VDAでは、このグループはICA®およびRDP接続に適用されます。
- VDAは、通信するための有効なControllerアドレスを持っている必要があります。そうでない場合、セッションを確立できません。Controllerアドレスは、VDAのインストール時または後で指定できます。必ず実行してください。詳細については、「VDA登録」を参照してください。

VDAインストール後およびインストール中の再起動

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

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

VDAインストール中に必要な再起動の回数を最小限に抑えるには、次の手順を実行します。

- VDAのインストールを開始する前に、サポートされている.NET Frameworkバージョンがインストールされていることを確認してください。

- WindowsマルチセッションOSマシンでは、VDAをインストールする前にRDSロールサービスをインストールして有効にしてください。

VDAをインストールする前にこれらの前提条件をインストールしない場合：

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

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

インストールまたはアップグレードの失敗時の復元

> **注：**

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

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

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

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

この機能を有効にしてマルチセッションVDAのインストールまたはアップグレードを開始すると、インストーラーは実際のインストールまたはアップグレードを開始する前にサーバーバックアップを作成します。VDAのインストールまたはアップグレードが失敗した場合、マシンはバックアップ状態に戻されます。`%temp%/Citrix`フォルダーには、展開ログと復元に関するその他の情報が含まれています。サーバーバックアップの作成にかかる時間は、必要なバックアップのサ

イズとサーバーで利用可能なリソースの量に基づきます。バックアップは *C:\WindowsImageBackup\servername* に保存されます。

デフォルトでは、この機能は無効になっています。

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

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

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

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

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

インストーラー

フルプロダクトインストーラー

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

- コアコンポーネント（Delivery Controller、Studio、Director、License Server）をインストール、アップグレード、または削除します。

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

> **注:**
>
> Workspace Environment Management™ Agentインストーラーはローカライズされていません。英語のみで提供されます。

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

スタンドアロン VDA インストーラー

スタンドアロンVDAインストーラーは、Citrixダウンロードページで入手できます。（製品インストールメディアからは入手できません。）スタンドアロンVDAインストーラーは、フルプロダクトISOよりもはるかに小さく、次のような展開に容易に対応できます。

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

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

ダウンロードできるスタンドアロンVDAインストーラーは3種類あります。

VDAServerSetup.exe:

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

VDAWorkstationSetup.exe:

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

VDAWorkstationCoreSetup.exe:

Remote PC Access展開またはコアVDIインストール用に最適化されたシングルセッションOS用VDAをインストールします。Remote PC Accessは物理マシンを使用します。コアVDIインストールは、イメージとして使用されていないVMです。このような展開のVDA接続に必要なコアサービスのみをインストールします。そのため、フルプロダクトインストーラーまたは `VDAWorkstationSetup.exe` インストーラーで有効なオプションのサブセットのみをサポートします。

このインストーラーは、次の目的で使用されるコンポーネントをインストールまたは含みません。

- App-V (アプリケーション仮想化)。
- プロファイル管理。Citrix Profile Management をインストールから除外すると、Citrix Director の表示に影響します。詳しくは、「VDA のインストール」を参照してください。
- マシン ID サービス。
- Citrix サポートツール。
- ウィンドウズ版Citrix Files。
- アウトルック版Citrix Files。

`VDAWorkstationCoreSetup.exe` インストーラーは、Citrix Workspace アプリ for Windows をインストールまたは含んでいません。

`VDAWorkstationCoreSetup.exe` を使用することは、フルプロダクトまたは `VDAWorkstationSetup` インストーラーを使用してシングルセッション OS VDA をインストールすることと同等であり、次のいずれかになります。

- グラフィカルインターフェイスの場合：**［環境］**ページで［Remote PC Access］オプションを選択します。
- コマンドラインインターフェイスの場合：`/remotepc` オプションを指定します。

- コマンドラインインターフェイスの場合：`/components vda` と、有効な追加コンポーネント名をすべてリストする `/exclude` オプションを指定します。

省略されたコンポーネント/機能は、後でフルプロダクトインストーラーを実行してインストールできます。この操作により、不足しているすべてのコンポーネントをインストールできます。

`VDAWorkstationCoreSetup.exe` インストーラーは、Browser Content Redirection MSI を自動的にインストールします。この自動インストールは、VDA リリース 2003 以降のサポート対象リリースに適用されます。

Citrix インストールリターンコード

インストールログには、コンポーネントのインストールの結果が Microsoft の値ではなく Citrix のリターンコードとして含まれます。

- 0 = 成功
- 1 = 失敗
- 2 = 部分的な成功
- 3 = 部分的な成功と再起動が必要
- 4 = 失敗と再起動が必要
- 5 = ユーザーによってキャンセルされました
- 6 = 不正なコマンドライン引数
- 7 = 新しいバージョンが見つかりました
- 8 = 成功と再起動が必要
- 9 = ファイルロック再起動
- 10 = 中止
- 11 = メディア失敗
- 12 = ライセンス失敗
- 13 = 事前チェック失敗
- 14 = 再起動保留チェック中止
- 15 = 事前チェック合格 - これは、新しい /precheckonly コマンドラインオプションを使用した後に事前チェックが合格した場合に返されます。
- 16 = 事前チェック失敗 - これは、新しい /precheckonly コマンドラインオプションを使用した後に事前チェックが失敗した場合に返されます。

- 17 = オプションソフトウェアの失敗 - これは、新しいオプションソフトウェアコンポーネントのいずれかのインストールが失敗し、「他の選択されたコンポーネントのインストールが失敗した場合でも、VDAのインストールまたはアップグレードを続行する」が選択されている場合に返されます。

たとえば、Microsoft System Center Configuration Managerなどのツールを使用する場合、インストールログにリターンコード3が含まれていると、スクリプトによるVDAインストールが失敗したように見えることがあります。これは、VDAインストーラーが、ユーザーが開始する必要のある再起動を待機している場合に発生する可能性があります（たとえば、サーバーへのRDSロールの前提条件のインストール後など）。VDAのインストールは、すべての前提条件と選択されたコンポーネントがインストールされ、インストール後にマシンが再起動された場合にのみ成功と見なされます。

あるいは、インストールをCMDスクリプト (Microsoftの終了コードを返します) でラップするか、Configuration Managerパッケージの成功コードを変更できます。

Windows Serverワークロード向けにMicrosoft RDSライセンスサーバーを構成する

この製品は、Windows 2016などのWindows Serverワークロードを提供するときに、Windows Serverのリモートセッション機能にアクセスします。これには通常、リモートデスクトップサービス クライアントアクセスライセンス (RDS CAL) が必要です。VDAは、RDS CALを要求するためにRDSライセンスサーバーに接続できる必要があります。ライセンスサーバーをインストールしてアクティブ化します。詳細については、Microsoftドキュメント「リモートデスクトップサービスライセンスサーバーをアクティブ化する」を参照してください。概念実証環境では、Microsoftが提供する猶予期間を使用できます。

この方法では、このサービスにライセンスサーバー設定を適用させることができます。イメージ上のRDSコンソールで、ライセンスサーバーとユーザーごとのモードを構成できます。Microsoftグループポリシー設定を使用してライセンスサーバーを構成することもできます。詳細については、Microsoftドキュメント「クライアントアクセスライセンス (CAL) を使用してRDS展開をライセンスする」を参照してください。

グループポリシー設定を使用してRDSライセンスサーバーを構成するには:

1. 利用可能なマシンにリモートデスクトップサービスライセンスサーバーをインストールします。マシンは常に利用可能である必要があります。Citrix製品のワークロードは、このライセンスサーバーに到達できる必要があります。

2. Microsoftグループポリシーを使用して、ライセンスサーバーアドレスとユーザーごとのライセンスモードを指定します。詳細については、Microsoftドキュメント「RDセッションホストサーバーのリモートデスクトップライセンスモードを指定する」を参照してください。

Windows 10ワークロードには、適切なWindows 10ライセンスのアクティベーションが必要です。Windows 10ワークロードをアクティベートするには、Microsoftのドキュメントに従うことをお勧めします。

詳細情報

特定のホストタイプのリソースの場所を設定するには：

- AWSクラウド環境
- XenServer仮想化環境(/ja-jp/citrix-virtual-apps-desktops/2503/install-configure/install-prepare/xenserver.html)
- Google Cloud環境(/ja-jp/citrix-virtual-apps-desktops/2503/install-configure/install-prepare/gcp.html)
- Microsoft Azure Resource Managerクラウド環境(/ja-jp/citrix-virtual-apps-desktops/2503/install-configure/install-prepare/azure.html)
- マイクロソフト システムセンター コンフィギュレーションマネージャー 環境
- Microsoft System Center Virtual Machine Manager を使用する仮想化環境
- Nutanix仮想化環境(/ja-jp/citrix-virtual-apps-desktops/2503/install-configure/install-prepare/nutanix.html)
- Nutanixクラウドおよびパートナーソリューション(/ja-jp/citrix-virtual-apps-desktops/2503/install-configure/install-prepare/nutanix-cloud-patrner-solutions.html)
- VMware仮想化環境(/ja-jp/citrix-virtual-apps-desktops/2503/install-configure/install-prepare/vmware.html)
- VMwareクラウドおよびパートナーソリューション(/ja-jp/citrix-virtual-apps-desktops/2503/install-configure/install-prepare/vmware-cloud-partner-solutions.html)

AWSクラウド環境

この記事では、AWSアカウントをCitrix Virtual Apps and Desktopsで使用できるリソースの場所として設定する手順を説明します。このリソースの場所には、概念実証や、複数のアベイラビリティゾーンにリソースを分散させる必要がないその他の展開に最適な、基本的なコンポーネントセットが含まれています。これらのタスクを完了すると、VDAのインストール、マシンのプロビジョニング、マシンカタログの作成、デリバリーグループの作成が可能になります。

この記事のタスクを完了すると、リソースの場所には次のコンポーネントが含まれます。

- 単一のアベイラビリティゾーン内にパブリックサブネットとプライベートサブネットを持つ仮想プライベートクラウド（VPC）。
- VPCのプライベートサブネット内に配置され、Active Directoryドメインコントローラーと DNSサーバーの両方として実行されるインスタンス。
- VPCのパブリックサブネットで踏み台ホストとして機能するインスタンス。このインスタンスは、管理目的でプライベートサブネット内のインスタンスへのRDP接続を開始するために使用されます。リソースの場所の設定が完了したら、このインスタンスをシャットダウンして、簡単にアクセスできないようにすることができます。VDAインスタンスなど、プライベートサブネット内の他のインスタンスを管理する必要がある場合は、踏み台ホストインスタンスを再起動できます。

タスクの概要

パブリックサブネットとプライベートサブネットを持つ仮想プライベートクラウド（VPC）を設定します。 このタスクを完了すると、AWSはパブリックサブネットにElastic IPアドレスを持つNATゲートウェイを展開します。このアクションにより、プライベートサブネット内のインスタンスがインターネットにアクセスできるようになります。パブリックサブネット内のインスタンスはインバウンドのパブリックトラフィックにアクセスできますが、プライベートサブネット内のインスタンスはアクセスできません。

セキュリティグループを構成します。 セキュリティグループは、VPC内のインスタンスのトラフィックを制御する仮想ファイアウォールとして機能します。パブリックサブネット内のインスタンスがプライベートサブネット内のインスタンスと通信できるようにするルールをセキュリティグループに追加します。また、これらのセキュリティグループをVPC内の各インスタンスに関連付けます。

DHCPオプションセットを作成します。 Amazon VPCでは、DHCPおよびDNSサービスがデフォルトで提供されており、Active DirectoryドメインコントローラーでDNSを構成する方法に影響します。AmazonのDHCPは無効にできず、AmazonのDNSはパブリックDNS解決にのみ使用でき、Active Directoryの名前解決には使用できません。DHCPを介してインスタンスに渡されるドメインとネームサーバーを指定するには、DHCPオプションセットを作成します。このセットは、Active Directoryドメインサフィックスを割り当て、VPC内のすべてのインスタンスのDNSサーバーを指定します。インスタンスがドメインに参加したときにホスト（A）および逆引き参照（PTR）レコードが自動的に登録されるようにするには、プライベートサブネットに追加する各インスタンスのネットワークアダプタープロパティを構成します。

踏み台ホストとドメインコントローラーをVPCに追加します。 踏み台ホストを介して、プライベートサブネット内のインスタンスにログオンし、ドメインを設定してインスタンスをドメインに参加させることができます。

タスク1：VPCを設定する

1. AWS管理コンソールから、**VPC**を選択します。
2. VPCダッシュボードから、**VPCを作成**を選択します。
3. **VPCなど**を選択します。
4. NATゲートウェイ ($) で、「**1 AZ内**」または「**AZごとに1つ**」を選択します。
5. DNSオプションで、「**DNSホスト名を有効にする**」が選択されたままにします。
6. 「**VPCを作成**」を選択します。AWSは、パブリックサブネットとプライベートサブネット、インターネットゲートウェイ、ルートテーブル、およびデフォルトのセキュリティグループを作成します。

タスク2：セキュリティグループの構成

このタスクでは、VPC 用に次のセキュリティグループを作成および構成します:

- パブリックサブネット内のインスタンスに関連付けるためのパブリックセキュリティグループ。
- プライベートサブネット内のインスタンスに関連付けるためのプライベートセキュリティグループ。

セキュリティグループを作成するには：

1. VPC ダッシュボードで、「**Security Groups**」を選択します。
2. パブリックセキュリティグループ用のセキュリティグループを作成します。「**Create Security Group**」を選択し、グループの名前タグと説明を入力します。VPC で、以前に作成した VPC を選択します。「**Yes, Create**」を選択します。

パブリックセキュリティグループの構成

1. セキュリティグループのリストから、パブリックセキュリティグループを選択します。
2. 「**インバウンドルール**」タブを選択し、「**編集**」を選択して、次のルールを作成します。

タイプ	送信元
すべてのトラフィック	プライベートセキュリティグループを選択します。

タイプ	送信元
すべてのトラフィック	パブリックセキュリティグループを選択します。
ICMP	0.0.0.0/0
22 (SSH)	0.0.0.0/0
80 (HTTP)	0.0.0.0/0
443 (HTTPS)	0.0.0.0/0
1494 (ICA/HDX)	0.0.0.0/0
2598 (セッションの信頼性)	0.0.0.0/0
3389 (RDP)	0.0.0.0/0

3. 完了したら、**保存**を選択します。
4. **［Outbound Rules］**タブを選択し、［Edit］**を選択して、次のルールを作成します。

タイプ	宛先
すべてのトラフィック	プライベートセキュリティグループを選択します。
すべてのトラフィック	0.0.0.0/0
ICMP	0.0.0.0/0

5. 完了したら、**保存**を選択します。

プライベートセキュリティグループを構成する

1. セキュリティグループリストから、プライベートセキュリティグループを選択します。
2. パブリックセキュリティグループからのトラフィックを設定していない場合は、TCPポートを設定する必要があります。**［Inbound Rules］**タブを選択し、［Edit］**を選択して、次のルールを作成します。

タイプ	送信元
すべてのトラフィック	プライベートセキュリティグループを選択します。
すべてのトラフィック	パブリックセキュリティグループを選択します。
ICMP	パブリックセキュリティグループを選択します。
TCP 53 (DNS)	パブリックセキュリティグループを選択します。
UDP 53 (DNS)	パブリックセキュリティグループを選択します。
80 (HTTP)	パブリックセキュリティグループを選択します。
TCP 135	パブリックセキュリティグループを選択します。
TCP 389	パブリックセキュリティグループを選択します。
UDP 389	パブリックセキュリティグループを選択します。
443 (HTTPS)	パブリックセキュリティグループを選択します。
TCP 1494 (ICA/HDX)	パブリックセキュリティグループを選択します。
TCP 2598 (セッション信頼性)	パブリックセキュリティグループを選択します。
3389 (RDP)	パブリックセキュリティグループを選択します。
TCP 49152–65535	パブリックセキュリティグループを選択します。

3. 完了したら、**保存**を選択します。
4. **アウトバウンドルール**タブを選択し、**編集**を選択して、次のルールを作成します。

タイプ	宛先
すべてのトラフィック	プライベートセキュリティグループを選択します。
すべてのトラフィック	0.0.0.0/0
ICMP	0.0.0.0/0
UDP 53 (DNS)	0.0.0.0/0

5. 完了したら、**保存**を選択します。

タスク 3: インスタンスを起動する

次の手順を実行して、2つのEC2インスタンスを作成し、Amazonが生成するデフォルトの管理者パスワードを復号します。

1. AWS管理コンソールから、**EC2**を選択します。
2. EC2ダッシュボードから、**Launch Instance**を選択します。
3. Windows Serverマシンイメージとインスタンスタイプを選択します。
4. **Configure Instance Details**ページで、インスタンスの名前を入力し、以前に設定したVPCを選択します。
5. **Subnet**で、各インスタンスについて次の選択を行います。
   - Bastionホスト：パブリックサブネットを選択します
   - ドメインコントローラー：プライベートサブネットを選択します
6. **Auto-assign Public IP address**で、各インスタンスについて次の選択を行います。
   - 踏み台ホスト: **Enable**を選択します。
   - ドメインコントローラー: **Use default setting**または**Disable**を選択します。
7. **Network Interfaces**で、ドメインコントローラーのプライベートサブネットのIP範囲内のプライマリIPアドレスを入力します。
8. 必要に応じて、**Add Storage**ページでディスクサイズを変更します。
9. **Tag Instance**ページで、各インスタンスにわかりやすい名前を入力します。

10. 「**セキュリティグループの設定**」ページで、「**既存のセキュリティグループを選択**」を選択し、各インスタンスについて以下の選択を行います。
    - Bastionホスト: パブリックセキュリティグループを選択します。
    - ドメインコントローラー: プライベートセキュリティグループを選択します。
11. 選択内容を確認し、「**起動**」を選択します。
12. 新しいキーペアを作成するか、既存のキーペアを選択します。新しいキーペアを作成する場合は、秘密キー (.pem) ファイルをダウンロードして安全な場所に保管してください。インスタンスのデフォルトの管理者パスワードを取得する際には、秘密キーを提供する必要があります。
13. 「**インスタンスの起動**」を選択します。「**インスタンスの表示**」を選択して、インスタンスのリストを表示します。新しく起動したインスタンスがすべてのステータスチェックに合格するまで待ってからアクセスしてください。
14. 各インスタンスのデフォルトの管理者パスワードを取得します。
    a. インスタンスリストからインスタンスを選択し、「**接続**」を選択します。
    b. 「**RDPクライアント**」タブに移動し、「**パスワードの取得**」を選択し、プロンプトが表示されたら秘密キー (`.pem`) ファイルをアップロードします。
    c. 「**パスワードの復号**」を選択して、人間が読めるパスワードを取得します。AWSがデフォルトのパスワードを表示します。
15. 2つのインスタンスを作成するまで、手順2から繰り返します。
    - パブリックサブネット内のBastionホストインスタンス1つ
    - ドメインコントローラーとして使用するプライベートサブネット内のインスタンス1つ.

タスク4：DHCPオプションセットを作成する

1. VPCダッシュボードから、「**DHCPオプションセット**」を選択します。
2. 次の情報を入力します。
    - 名前タグ：セットのわかりやすい名前を入力します。
    - ドメイン名：ドメインコントローラーインスタンスを設定するときに使用する完全修飾ドメイン名を入力します。
    - ドメインネームサーバー：ドメインコントローラーインスタンスに割り当てたプライベートIPアドレスと、カンマで区切られた文字列「**AmazonProvidedDNS**」を入力します。
    - NTPサーバー：このフィールドは空白のままにします。

- NetBIOSネームサーバー：ドメインコントローラーインスタンスのプライベートIPアドレスを入力します。
- NetBIOSノードタイプ：「**2**」と入力します。

3. **はい、作成**を選択します。
4. 新しいセットをVPCに関連付けます。

   a. VPCダッシュボードから、**Your VPCs**を選択し、以前に設定したVPCを選択します。

   b. **アクション > DHCPオプションセットの編集**を選択します。

   c. プロンプトが表示されたら、作成した新しいセットを選択し、「**保存**」を選択します。

タスク5: インスタンスを構成する

1. RDPクライアントを使用して、踏み台ホストインスタンスのパブリックIPアドレスに接続します。プロンプトが表示されたら、管理者アカウントの資格情報を入力します。
2. 踏み台ホストインスタンスから、リモートデスクトップ接続を起動し、構成するインスタンスのプライベートIPアドレスに接続します。プロンプトが表示されたら、インスタンスの管理者資格情報を入力します。
3. プライベートサブネット内のすべてのインスタンスについて、DNS設定を構成します。

   a. **> > > >** を選択します。表示されているネットワーク接続をダブルクリックします。

   b. **> >** を選択します。

   c. **>** を選択します。次の設定が有効になっていることを確認し、 を選択します。

      - この接続のアドレスをDNSに登録する
      - この接続のDNSサフィックスをDNS登録で使用する

4. ドメインコントローラーを構成するには:

   a. Server Manager を使用して、Active Directory ドメインサービス の役割をすべてのデフォルト機能とともに追加します。

   b. インスタンスをドメインコントローラーに昇格させます。昇格中にDNSを有効にし、DHCPオプションセットを作成したときに指定したドメイン名を使用します。プロンプトが表示されたらインスタンスを再起動します。

次のステップ

- コアコンポーネントをインストールする
- VDAのインストール

- サイトを作成する
- AWS での接続の作成と管理については、AWS への接続を参照してください。

詳細情報

- 接続とリソースの作成および管理
- マシンカタログの作成

XenServer® 仮想化環境

XenServer は運用管理を簡素化し、負荷の高いワークロードでも高精細なユーザーエクスペリエンスを保証します。

XenServer のセットアップについては、「インストール準備」を参照してください。

次に行うこと

- コアコンポーネントのインストール
- VDAのインストール
- サイトの作成
- XenServer での接続の作成と管理については、「XenServer への接続」を参照してください。

詳細情報

- 接続とリソースの作成および管理
- マシンカタログの作成

Google Cloud環境

Citrix Virtual Apps and Desktops™ を使用すると、Google Cloud 上でマシンをプロビジョニングおよび管理できます。

要件

- Citrix Cloud™ アカウント。この記事で説明されている機能は、Citrix Cloud でのみ利用できます。
- Google Cloud プロジェクト。このプロジェクトには、マシンカタログに関連付けられているすべてのコンピューティングリソースが保存されます。既存のプロジェクトでも新規のプロジェクトでもかまいません。
- Google Cloud プロジェクトで4つのAPIを有効にします。詳細については、「Google Cloud APIを有効にする」を参照してください。

- Google Cloud サービスアカウント。サービスアカウントはGoogle Cloudに対して認証を行い、プロジェクトへのアクセスを有効にします。詳細については、「サービスアカウントの構成と更新」を参照してください。
- Google プライベートアクセスを有効にします。詳細については、「Google プライベートアクセスを有効にする」を参照してください。

Google Cloud APIを有効にする

Web Studio を介して Google Cloud 機能を使用するには、Google Cloud プロジェクトで次の API を有効にします。

- コンピュート エンジン API
- クラウド リソース マネージャー API
- ID およびアクセス管理 (IAM) API
- クラウド ビルド API
- クラウド キー マネジメント サービス (KMS)

Google Cloudコンソールから、次の手順を実行します。

1. 左上のメニューで、**APIs and Services > Dashboard** を選択します。

   APIs and Services Dashboard の選択画像(/en-us/citrix-virtual-apps-desktops/2503/media/gcp-api-service-select-dashboard.png)

2. **ダッシュボード**画面で、Compute Engine API が有効になっていることを確認します。 有効になっていない場合は、次の手順に従います。

   a. **APIs and Services > Library** に移動します。

      API とサービスライブラリの画像(/en-us/citrix-virtual-apps-desktops/2503/media/gcp-api-library.png)

   b. 検索ボックスに「*Compute Engine*」と入力します。

   c. 検索結果から、**Compute Engine API** を選択します。

   d. **Compute Engine API** ページで、**Enable** を選択します。

3. Cloud Resource Manager APIを有効にします。

   a. **APIs and Services > Library** に移動します。

   b. 検索ボックスに「*Cloud Resource Manager*」と入力します。

   c. 検索結果から、**Cloud Resource Manager API** を選択します。

d. **Cloud Resource Manager API** ページで、**Enable** を選択します。API のステータスが表示されます。

4. 同様に、**Identity and Access Management (IAM) API** と **Cloud Build API** を有効にします。

Google Cloud Shellを使用してAPIを有効にすることもできます。これを行うには：

1. Google Console を開き、Cloud Shell をロードします。
2. Cloud Shell で次の4つのコマンドを実行します。
   - compute.googleapis.com サービスを有効にする
   - cloudresourcemanager.googleapis.com サービスを有効にする
   - gcloud services enable iam.googleapis.com コマンド
   - gcloud services enable cloudbuild.googleapis.com コマンド
3. Cloud Shellがプロンプトを表示した場合、「**承認**」をクリックします。

サービスアカウントの構成と更新

> **注:**
>
> GCP は、Cloud Build Service のデフォルトの動作とサービスアカウントの使用に関して、April 29, 2024 以降に変更を導入します。詳細については、Cloud Build Service Account Change を参照してください。April 29, 2024 より前に Cloud Build API が有効になっている既存の Google プロジェクトは、この変更の影響を受けません。ただし、April 29 以降も既存の Cloud Build Service の動作を維持したい場合は、Cloud Build API を有効にする前に、組織ポリシーを作成または適用して制約の適用を無効にすることができます。その結果、以下のコンテンツは Before April 29, 2024 と After April 29, 2024 の2つに分かれています。新しい組織ポリシーを設定する場合は、Before April 29, 2024 のセクションに従ってください。

April 29, 2024 以前

Citrix Cloudは、Google Cloudプロジェクト内で3つの個別のサービスアカウントを使用します。

- *Citrix Cloud Service Account*: このサービスアカウントにより、Citrix Cloud は Google プロジェクトにアクセスし、マシンをプロビジョニングおよび管理できます。このサービスアカウントは、Google Cloud によって生成された キー を使用して Google Cloud に対して認証を行います。

このサービスアカウントは、ここに概説されているように手動で作成する必要があります。詳細については、Citrix Cloud Service Account の作成 を参照してください。

このサービスアカウントはメールアドレスで識別できます。例: `<my-service-account>@<project-id>.iam.gserviceaccount.com`。

- *Cloud Build サービスアカウント*: このサービスアカウントは、Google Cloud API を有効にする で言及されているすべての API を有効にすると自動的にプロビジョニングされます。自動的に作成されたすべてのサービスアカウントを表示するには、**Google Cloud** コンソールで **IAM と管理 > IAM** に移動し、**Google 提供のロール付与を含める**チェックボックスを選択します。

  このサービスアカウントは、**プロジェクト ID** と「**cloudbuild**」という単語で始まるメールアドレスで識別できます。例: `<project-id>@cloudbuild.gserviceaccount.com`

  サービスアカウントに以下のロールが付与されていることを確認します。ロールを追加する必要がある場合は、Cloud Build サービスアカウントにロールを追加するに記載されている手順に従ってください。

  - Cloud Build サービスアカウント
  - Compute インスタンス管理者
  - サービスアカウントユーザー

- *Cloud Compute サービスアカウント*: このサービスアカウントは、Compute API がアクティブ化されると、Google Cloud によって Google Cloud で作成されたインスタンスに追加されます。このアカウントには、操作を実行するための IAM 基本編集者ロールがあります。ただし、より詳細な制御を行うためにデフォルトの権限を削除した場合、次の権限を必要とする**ストレージ管理者**ロールを追加する必要があります。

  - resourcemanager.projects.get
  - storage.objects.create
  - storage.objects.get
  - storage.objects.list

このサービスアカウントは、**プロジェクト ID** と「**compute**」という単語で始まるメールアドレスで識別できます。例: `<project-id>-compute@developer.gserviceaccount.com`。

CITRIX CLOUD サービスアカウントを作成する

Citrix Cloud サービスアカウントを作成するには、次の手順に従います。

1. Google Cloud コンソールで、**IAM と管理 > サービスアカウント**に移動します。

2. **サービスアカウント**ページで、**サービスアカウントを作成**を選択します。
3. **サービスアカウントの作成**ページで、必要な情報を入力し、**作成して続行**を選択します。
4. **このサービスアカウントにプロジェクトへのアクセス権を付与**ページで、**ロールを選択**ドロップダウンメニューをクリックし、必要なロールを選択します。さらにロールを追加する場合は、**+別のロールを追加**をクリックします。

   各アカウント（個人またはサービス）には、プロジェクトの管理を定義するさまざまなロールがあります。このサービスアカウントに次のロールを付与します。

   - Compute 管理者
   - Storage 管理者
   - Cloud Build 編集者
   - サービスアカウントユーザー
   - クラウド データストア ユーザー
   - Cloud KMS 暗号オペレーター

   Cloud KMS Crypto Operatorには次の権限が必要です。

   - cloudkms.cryptoKeys.get
   - cloudkms.cryptoKeys.list
   - cloudkms.keyRings.get
   - cloudkms.keyRings.list
   - cloudkms.cryptoKeyVersions.useToDecrypt
   - cloudkms.cryptoKeyVersions.useToEncrypt

   > **注:**
   >
   > 新しいサービスアカウントを作成する際に利用可能なロールの完全なリストを取得するには、すべてのAPIを有効にしてください。

5. **続行**をクリックします
6. **このサービスアカウントへのユーザーアクセスを許可**ページで、このサービスアカウントでアクションを実行するためのアクセス権を付与するユーザーまたはグループを追加します。
7. **完了**をクリックします。

8. IAMメインコンソールに移動します。
9. 作成されたサービスアカウントを特定します。
10. ロールが正常に割り当てられていることを確認します。

考慮事項:

サービスアカウントを作成する際は、以下を考慮してください。

- **このサービスアカウントにプロジェクトへのアクセスを許可**および**このサービスアカウントへのユーザーアクセスを許可**のステップはオプションです。これらのオプションの構成ステップをスキップすることを選択した場合、新しく作成されたサービスアカウントは**IAMと管理 > IAM**ページに表示されません。
- サービスアカウントに関連付けられたロールを表示するには、オプションの手順をスキップせずにロールを追加します。このプロセスにより、構成されたサービスアカウントにロールが表示されるようになります。

CITRIX CLOUDサービスアカウントキー

Citrix DaaS で接続を作成するには、Citrix Cloud サービスアカウントキーが必要です。キーは資格情報ファイル (.json) に含まれています。キーを作成すると、ファイルは自動的にダウンロードされ、**ダウンロード**フォルダーに保存されます。キーを作成するときは、キータイプを JSON に設定してください。そうしないと、Web Studio はそれを解析できません。

サービスアカウントキーを作成するには、**IAM と管理 > サービスアカウント**に移動し、Citrix Cloud サービスアカウントのメールアドレスをクリックします。**キー**タブに切り替え、**キーを追加 > 新しいキーを作成**を選択します。キータイプとして**JSON**を必ず選択してください。

> **ヒント:**
>
> Google Cloud コンソールの**サービスアカウント**ページを使用してキーを作成します。セキュリティ上の理由から、キーを定期的に変更することをお勧めします。既存の Google Cloud 接続を編集することで、新しいキーを Citrix Virtual Apps and Desktops アプリケーションに提供できます。

CITRIX CLOUD サービスアカウントにロールを追加する

Citrix Cloud サービスアカウントにロールを追加するには：

1. Google Cloud コンソールで、**IAM と管理 > IAM** に移動します。

2. **IAM > 権限**ページで、作成したサービスアカウントを電子メールアドレスで特定し、見つけます。

   例: `<my-service-account>@<project-id>.iam.gserviceaccount.com`

3. 鉛筆アイコンを選択して、サービスアカウントのプリンシパルへのアクセスを編集します。
4. 選択したプリンシパルオプションの**「project-id」へのアクセスを編集**ページで、**別のロールを追加**を選択して、必要なロールをサービスアカウントに1つずつ追加し、**保存**を選択します。

CLOUD BUILD サービスアカウントにロールを追加する

Cloud Build サービスアカウントにロールを追加するには：

1. Google Cloud コンソールで、**IAM と管理 > IAM**に移動します。
2. **IAM**ページで、**Project ID**と**cloudbuild**という単語で始まるメールアドレスで識別できるCloud Buildサービスアカウントを見つけます。

   例: `<project-id>@cloudbuild.gserviceaccount.com`

3. 鉛筆アイコンを選択して、Cloud Buildアカウントの役割を編集します。
4. 選択したプリンシパルオプションの「**Edit access to "project-id" page**」で、**ADD ANOTHER ROLE**を選択して必要な役割をCloud Buildサービスアカウントに1つずつ追加し、**SAVE**を選択します。

> **注:**
>
> 役割の完全なリストを取得するには、すべてのAPIを有効にします。

April 29, 2024 以降

Citrix Cloudは、Google Cloudプロジェクト内で2つの異なるサービスアカウントを使用します。

- *Citrix Cloud Service Account*: このサービスアカウントにより、Citrix CloudはGoogleプロジェクトにアクセスし、マシンをプロビジョニングおよび管理できます。このサービスアカウントは、Google Cloudによって生成されたキーを使用してGoogle Cloudに対して認証を行います。

  このサービスアカウントは手動で作成する必要があります。

  このサービスアカウントは、メールアドレスで識別できます。例: `<my-service-account>@<project-id>.iam.gserviceaccount.com`。

- *Cloud Compute Service Account*: このサービスアカウントは、Enable Google Cloud APIsに記載されているすべてのAPIを有効にすると自動的にプロビジョニングされます。自動的に作成されたすべてのサービスアカウントを表示するには、**Google Cloud**コンソールで**IAM & Admin > IAM**に移動し、**Include Google-provided role grants**チェックボックスをオンにします。このアカウントには、操作を実行するためのIAM基本編集者ロールがあります。ただし、より詳細な制御を行うためにデフォルトの権限を削除する場合は、次の権限を必要とする**Storage Admin**ロールを追加する必要があります。

  - resourcemanager.projects.get
  - storage.objects.create
  - storage.objects.get
  - storage.objects.list

  このサービスアカウントは、**プロジェクトID**と**compute**という単語で始まるメールアドレスで識別できます。例：`<project-id>-compute@developer.gserviceaccount.com.`.

  サービスアカウントに次のロールが付与されていることを確認します。

  - Cloud Build サービスアカウント
  - Compute Instance 管理者
  - サービスアカウントユーザー

CITRIX CLOUD サービスアカウントを作成する

Citrix Cloud サービスアカウントを作成するには、次の手順に従います。

1. Google Cloud コンソールで、**IAM と管理 > サービスアカウント**に移動します。
2. **サービスアカウント**ページで、**サービスアカウントを作成**を選択します。
3. **サービスアカウントの作成**ページで、必要な情報を入力し、**作成して続行**を選択します。
4. 「**このサービスアカウントにプロジェクトへのアクセスを許可する**」ページで、「**ロールを選択**」ドロップダウンメニューをクリックし、必要なロールを選択します。さらにロールを追加する場合は、「**+別のロールを追加**」をクリックします。

   各アカウント（個人またはサービス）には、プロジェクトの管理を定義するさまざまなロールがあります。このサービスアカウントには、以下のロールを付与してください。

   - Compute 管理者
   - Storage 管理者
   - Cloud Build エディター

- サービスアカウントユーザー
- クラウド データストア ユーザー
- クラウド KMS クリプト オペレーター

Cloud KMS Crypto Operator には、次の権限が必要です。

- cloudkms.cryptoKeys.get
- cloudkms.cryptoKeys.list
- cloudkms.keyRings.get
- cloudkms.keyRings.list

> **注:**
>
> 新しいサービスアカウントを作成する際に利用可能なロールの完全なリストを取得するには、すべてのAPIを有効にしてください。

5. **続行**をクリックします
6. **このサービスアカウントへのユーザーアクセスを許可**ページで、ユーザーまたはグループを追加して、このサービスアカウントでのアクションを実行するアクセス権を付与します。
7. **完了**をクリックします。
8. IAMメインコンソールに移動します。
9. 作成されたサービスアカウントを特定します。
10. 役割が正常に割り当てられていることを確認します。

考慮事項：

サービスアカウントを作成する際は、次の点を考慮してください。

- **このサービスアカウントにプロジェクトへのアクセス権を付与する**および**このサービスアカウントにユーザーアクセス権を付与する**の手順はオプションです。これらのオプションの構成手順をスキップすることを選択した場合、新しく作成されたサービスアカウントは**IAMと管理 > IAM**ページに表示されません。
- サービスアカウントに関連付けられた役割を表示するには、オプションの手順をスキップせずに役割を追加します。このプロセスにより、構成されたサービスアカウントに役割が表示されるようになります。

CITRIX CLOUDサービスアカウントキー

Citrix DaaSで接続を作成するには、Citrix Cloudサービスアカウントキーが必要です。キーは資格情報ファイル（.json）に含まれています。キーを作成すると、ファイルは自動的にダウンロードされ、**ダウンロード**フォルダーに保存されます。キーを作成する際は、キーの種類をJSONに設定してください。そうしないと、Web Studioはそれを解析できません。

サービスアカウントキーを作成するには、**IAMと管理 > サービスアカウント**に移動し、Citrix Cloudサービスアカウントのメールアドレスをクリックします。**キー**タブに切り替えて、**キーを追加 > 新しいキーを作成**を選択します。キーの種類として**JSON**が選択されていることを確認してください。

> **ヒント：**
>
> Google Cloudコンソールの**サービスアカウント**ページを使用してキーを作成します。セキュリティ上の理由から、定期的にキーを変更することをお勧めします。既存のGoogle Cloud接続を編集することで、新しいキーをCitrix Virtual Apps and Desktopsアプリケーションに提供できます。

CITRIX CLOUDサービスアカウントに役割を追加する

Citrix Cloudサービスアカウントに役割を追加するには：

1. Google Cloud コンソールで、**IAM と管理 > IAM** に移動します。
2. **IAM > 権限**ページで、作成したサービスアカウントを電子メールアドレスで特定し、見つけます。

   例: `<my-service-account>@<project-id>.iam.gserviceaccount.com`
3. 鉛筆アイコンを選択して、サービスアカウントのプリンシパルへのアクセスを編集します。
4. 選択したプリンシパルオプションの **「project-id」へのアクセスを編集** ページで、**別の役割を追加** を選択して、必要な役割をサービスアカウントに1つずつ追加し、**保存** を選択します。

CLOUD COMPUTEサービスアカウントに役割を追加する

Cloud Computeサービスアカウントに役割を追加するには:

1. Google Cloudコンソールで、**IAMと管理 > IAM** に移動します。
2. **IAM** ページで、**プロジェクトID** と **compute** という単語で始まるメールアドレスで識別できるCloud Computeサービスアカウントを見つけます。

   例: `<project-id>-compute@developer.gserviceaccount.com`

3. 鉛筆アイコンを選択して、Cloud Buildアカウントの役割を編集します。
4. 選択したプリンシパルオプションの **「project-id」へのアクセスを編集** ページで、**別の役割を追加** を選択して、必要な役割をCloud Buildサービスアカウントに1つずつ追加し、**保存** を選択します。

> **注:**
>
> 役割の完全なリストを取得するには、すべてのAPIを有効にします。

ストレージの権限とバケット管理

Citrix Virtual Apps and Desktopsは、Google Cloudサービスのクラウドビルド障害を報告するプロセスを改善します。このサービスは、Google Cloudでビルドを実行します。Citrix Virtual Apps and Desktopsは、Google Cloudサービスがビルドログ情報をキャプチャする `citrix-mcs-cloud-build-logs-{region}-{5 random characters}` という名前のストレージバケットを作成します。このバケットには、30日後にコンテンツを削除するオプションが設定されています。このプロセスでは、接続に使用されるサービスアカウントに、Google Cloudの権限が `storage.buckets.update` に設定されている必要があります。サービスアカウントにこの権限がない場合、Citrix Virtual Apps and Desktopsはエラーを無視し、カタログ作成プロセスを続行します。この権限がないと、ビルドログのサイズが増加し、手動でのクリーンアップが必要になります。

プライベート Google アクセスを有効にする

VMにネットワークインターフェースに割り当てられた外部IPアドレスがない場合、パケットは他の内部IPアドレスの宛先にのみ送信されます。プライベートアクセスを有効にすると、VMはGoogle APIおよび関連サービスで使用される外部IPアドレスのセットに接続します。

> **注:**
>
> プライベートGoogleアクセスが有効になっているかどうかにかかわらず、パブリックIPアドレスを持つVMと持たないVMのすべてがGoogle Public APIにアクセスできる必要があります。特に、サードパーティのネットワークアプライアンスが環境にインストールされている場合はその限りではありません。

> MCSプロビジョニングのために、サブネット内のVMがパブリックIPアドレスなしでGoogle APIにアクセスできるようにするには、次の手順を実行します。

1. Google Cloudで、**VPC network configuration**にアクセスします。
2. サブネットの詳細画面で、「**Private Googleアクセス**」をオンにします。

プライベートGoogleアクセス(/en-us/citrix-virtual-apps-desktops/2503/media/gcp-private-access.png)

詳細については、「Configuring Private Google Access」を参照してください。

> **重要:**

> ネットワークがVMのインターネットアクセスを防止するように構成されている場合、VMが接続されているサブネットに対してPrivate Googleアクセスを有効にすることに関連するリスクを組織が負うことを確認してください。

次のステップ

- コアコンポーネントのインストール
- VDAのインストール
- サイトの作成
- Google Cloud 環境での接続の作成と管理については、「Google Cloud 環境への接続」を参照してください。

詳細情報

- 接続とリソースの作成および管理(/ja-jp/citrix-virtual-apps-desktops/2503/install-configure/connections.html)
- マシンカタログの作成(/ja-jp/citrix-virtual-apps-desktops/2503/install-configure/machine-catalogs-create.html)

HPE Moonshot 仮想化環境

Citrix Virtual Apps and Desktops™ は、Citrix 管理の HPE Moonshot プラグインを介して HPE Moonshot ワークロードを管理します。Citrix 管理の HPE Moonshot プラグインは、Citrix Virtual Apps and Desktops バージョン 2503 のアップグレードまたはインストール時に自動的にインストールされます。このプラグインを使用すると、HPE Moonshot シャーシへの接続を作成し、カタログを作成し、カタログ内のマシンの電源管理を行うことができます。

主な手順

1. HPE 環境をセットアップします。
2. HPE Moonshot シャーシへの接続を作成します。
3. マシンカタログを作成します。

> **注:**
>
> カタログを作成する前に、1 つ以上の HPE Moonshot カートリッジノードがあることを確認し、それらのノードに VDA をインストールしてください。HPE Moonshot シャーシをハイパーバイザー、カートリッジノードを VM と考えることができます。

4. デリバリーグループを作成します。
5. 管理されていない残りの HPE Moonshot ノードを、管理対象のカタログまたはデリバリーグループに移行します。

> **注:**
>
> MMC ベースの Studio の代わりに Web Studio を使用してください。

トラブルシューティング

Citrix管理とHPE管理の両方のHPE Moonshotプラグインがインストールされている場合、

- **HPE管理のMoonshotプラグイン**を使用したい場合は、Citrix管理のHPE Moonshotプラグインをアンインストールし、`RegisterPlugin` キャッシュを更新する必要があります。これを行うには：

  a. PowerShellを管理者として開き、Citrix管理のHPE Moonshotプラグインをアンインストールするために次のコマンドを実行します。

  ```
  $CtxMnsht = Get-WmiObject -Class Win32_Product | Where-
  Object{$_.Name -Contains "Citrix HPE Moonshot Plugin"}

  $CtxMnsht.Uninstall()
  ```

  b. HPE管理のMoonshotプラグインを登録するために、次のコマンドを実行します。

```
cd "C:\Program Files\Common Files\Citrix\HCLPlugins\"

.\RegisterPlugins.exe -PluginsRoot "C:\Program Files\Common
Files\Citrix\HCLPlugins\CitrixMachineCreation\v1.0.0.0\"
```

c. プラグインの登録が成功したら、**タスクマネージャー**から次のサービスを再起動します。

   a. CitrixBrokerService

   b. CitrixHostService

   c. CitrixMachineCreationService

d. `Get-HypHypervisorPlugins` を実行して、プラグインが Delivery Controller にインストールされているかを確認します。出力の `DisplayName` フィールドには、HPE Moonshot Machine Manager と表示されている必要があります。

- Citrix管理のHPE Moonshotプラグインを再度インストールしたい場合は、次の手順を実行します。

   a. `E:\x64\Citrix Desktop Delivery Controller\MoonshotPlugin.msi`をインストールします。`E:\`はISOです。

   b. PowerShellを管理者として開き、Citrix管理のHPE Moonshotプラグインを登録するために次のコマンドを実行します。

```
C:\Program Files\Common Files\Citrix\HCLPlugins> .
\RegisterPlugins.exe -pluginsroot .\CitrixMachineCreation\v1.0.0.0\
```

   c. プラグインの登録が成功したら、タスクマネージャーから次のサービスを再起動します。

      a. CitrixBrokerService

      b. CitrixHostService

      c. CitrixMachineCreationService

1. `Get-HypHypervisorPlugins`を実行して、プラグインがDelivery Controllerにインストールされているかを確認します。出力のDisplayNameフィールドにはHPE Moonshotと表示されている必要があります。

次に行うこと

- コアコンポーネントのインストール

- VDAのインストール
- サイトの作成
- HPE Moonshotでの接続の作成と管理については、HPE Moonshotへの接続を参照してください。

詳細情報

- 接続とリソースの作成および管理
- マシンカタログの作成

Microsoft Azure Resource Manager クラウド環境

Citrix Virtual Apps and Desktops™展開でMicrosoft Azure Resource Managerを使用して仮想マシンをプロビジョニングする場合、以下について理解しておいてください。

- アジュール Active Directory: `<https://docs.microsoft.com/en-in/azure/active-directory/fundamentals/active-directory-whatis/>`
- 同意フレームワーク: `<https://docs.microsoft.com/ja-jp/azure/active-directory/manage-apps/plan-an-application-integration>`
- サービスプリンシパル: `<https://docs.microsoft.com/ja-jp/azure/active-directory/develop/app-objects-and-service-principals/>`

Microsoft Azure Resource Manager をセットアップするには、インストール準備 を参照してください。

次のステップ

- コアコンポーネントのインストール
- VDAのインストール
- サイトの作成
- Azure環境での接続の作成と管理については、「Microsoft Azureへの接続」を参照してください。

詳細情報

- 接続とリソースの作成および管理
- マシンカタログの作成
- CTX219211: Microsoft Azure Active Directoryアカウントのセットアップ
- CTX219243: XenAppおよびXenDesktopにAzureサブスクリプションへのアクセスを許可する

- CTX219271: サイト間VPNを使用してハイブリッドクラウドを展開する

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

Microsoft System Center Virtual Machine Manager (VMM) と Hyper-V を使用して仮想マシンを提供する場合は、このガイダンスに従ってください。

このリリースでは、システム要件に記載されている VMM バージョンがサポートされています。

> **注:**
>
> 混在 Hyper-V クラスター（異なる Hyper-V バージョンを実行しているサーバーを含む）はサポートされていません。

> Citrix Provisioning（旧Provisioning Services）および Machine Creation Services™ を使用して、以下をプロビジョニングできます。

- 第1世代のサポート対象デスクトップまたはサーバーOS VM。
- セキュアブートのサポートを含む、第2世代のサポート対象デスクトップまたはサーバーOS VM。

ハイパーバイザーのインストールと構成

> **重要:**
>
> すべての Delivery Controller は、VMM サーバーと同じフォレスト内にある必要があります。

1. Microsoft Hyper-V サーバーと VMM をサーバーにインストールします。
2. すべての Controller に System Center Virtual Machine Manager コンソールをインストールします。コンソールのバージョンは、管理サーバーのバージョンと一致している必要があります。以前のコンソールでも管理サーバーに接続できますが、バージョンが異なる場合、VDA のプロビジョニングは失敗します。
3. 次のアカウント情報を確認します。

Studio でホストを指定するために使用するアカウントは、関連する Hyper-V マシンに対する VMM 管理者または VMM 委任管理者である必要があります。このアカウントが VMM で委任管理者ロールのみを持っている場合、ホスト作成プロセス中に Studio にストレージデータが表示されません。

Studio統合に使用されるユーザーアカウントは、各Hyper-Vサーバーのadministratorsローカルセキュリティグループのメンバーである必要もあります。この構成は、VMの作成、更新、削除などのVMライフサイクル管理をサポートします。

Hyper-Vを実行しているサーバーにControllerをインストールすることはサポートされていません。

単一のSCVMMが異なるデータセンター内の複数のクラスターを管理する大規模な展開では、委任管理者のホストグループのスコープを制限できます。

ホストグループのスコープを制限するには、Microsoft System Center Virtual Machine Manager (VMM) コンソールで委任された管理者ロールを使用します。

1. **ユーザーロールの作成ウィザード**で、ユーザーロールとしてFabric Administrator (Delegated Administrator) を選択します。
2. **メンバー**で、委任された管理者として使用するActive Directoryのユーザーアカウントを追加します。
3. **スコープ**で、委任された管理者にアクセスを許可するホストグループを選択します。
4. 委任された管理者ユーザーの資格情報を使用して、新しい**実行アカウント**を作成します。これらの資格情報を使用して、後でハイパーバイザー接続を作成します。メインの管理者ロールアカウントは使用しないでください。

次のステップ

- コアコンポーネントのインストール
- VDAのインストール
- サイトの作成
- SCVMM での接続の作成と管理については、Microsoft System Center Virtual Machine Manager への接続を参照してください。

詳細情報

- 接続とリソースの作成および管理
- マシンカタログの作成

Nutanix クラウドおよびパートナーソリューション

Citrix Virtual Apps and Desktops™ は、以下の Nutanix クラウドおよびパートナーソリューションをサポートしています。

- AWS 上のニュータニックス クラウドクラスター

AWS 上のニュータニックス クラウドクラスター

Citrix Virtual Apps and Desktops は、AWS 上の Nutanix Cloud Clusters をサポートしています。Nutanix クラスターは、プライベートクラウドまたは複数のパブリッククラウドでアプリケーションを実行する方法を簡素化します。AWS 上の Nutanix Cloud Clusters の詳細については、「Nutanix Cloud Clusters on AWS Deployment and User Guide」を参照してください。

> **ヒント:**
>
> このサポートは、Nutanix オンプレミス クラスターと同じ機能を提供します。サポートされるクラスターは、*Prism Element* の 1 つのみです。詳細については、こちら を参照してください。

要件

AWS で Nutanix クラスターを使用するには、以下が必要です。

- Nutanix アカウント。
- 次の権限を持つ AWS アカウント:
  - IAMFullAccess
  - AWSConfigRole
  - AWSCloudFormationFullAccess

Nutanix クラスターの作成

Nutanix Clusterを作成するには：

1. Nutanix アカウントにログインします。
2. 「**Nutanix cluster**」オプションを見つけて、「**Launch**」をクリックします。「**Nutanix Console**」が開きます。詳細については、Get Started with Nutanix Cluster on AWS を参照してください。
3. **new VPC** を作成することを選択します。

クラスター作成プロセスは、以下のエラーで失敗する可能性があります。

- クラスターは指定された時間内に作成できませんでした。クラスターを削除しています。
- ホスト Nutanix Cluster - ノード `XXXXXXXXXX: Instance i-xxxxxxxxxxxxx: disable network interface source/dest check error.`.
- ホスト Nutanix Cluster - ノード `XXXXXXXXXX: Unable to obtain instance i-xxxxxxxxxxxxx network interface info.`.

クラスターの作成に失敗した場合：

- 別のリージョンで再作成してみてください。
- 再試行する前に、Nutanix CloudFormation Stack (CFS) を削除してください。

他のリソースに加えて、Nutanix CFSは以下を作成します。

- *Nutanix Cluster xxxxxxxxxxxx* 10.0.0.0/16 という名前の1つのVPC
- 2つのサブネット 10.0.128.0/24 および 10.0.129.0/24
- 1つのインターネットゲートウェイ
- NATゲートウェイ1つ

クラスターが作成されたら、**Nutanix Prism**のアドレスを取得します。

1. **Nutanix Console**に移動します。
2. コンソールの右上にある**Launch Prism Element**リンクにマウスオーバーし、URLをコピーします。

次のステップ

- コアコンポーネントをインストールする(/ja-jp/citrix-virtual-apps-desktops/2503/install-configure/install-core-components.html)
- VDAをインストールする(/ja-jp/citrix-virtual-apps-desktops/2503/install-configure/install-vdas.html)
- サイトを作成する(/ja-jp/citrix-virtual-apps-desktops/2503/install-configure/site-create.html)
- Nutanixクラウドおよびパートナーソリューションの接続を作成および管理するには、「Nutanixクラウドおよびパートナーソリューションへの接続」を参照してください。(/ja-jp/citrix-virtual-apps-desktops/2503/install-configure/connections/connection-nutanix-cloud-and-partner-solutions.html)

詳細情報

- 接続とリソースを作成および管理する(/ja-jp/citrix-virtual-apps-desktops/2503/install-configure/connections.html)
- マシンカタログを作成する(/ja-jp/citrix-virtual-apps-desktops/2503/install-configure/machine-catalogs-create.html)

Red Hat OpenShift 仮想化環境

Citrix® は、Citrix が管理する OpenShift プラグインを介して Red Hat OpenShift ワークロードを管理します。このプラグインを使用すると、OpenShift クラスターへのホスティング接続とホスティングユニットの作成、カタログの作成、およびカタログ内のマシンの電源管理を行うことができます。

> **注：**
>
> OpenShiftプラグインは、Red Hat OpenShiftクラスターバージョン4.17および4.18でテストされています。

主な手順

- Red Hat OpenShift 環境をセットアップします。
- OpenShift クラスターへの接続とリソースを作成します。
- マシンカタログを作成します。
- デリバリーグループを作成します。

Red Hat OpenShift 環境をセットアップする

1. *OpenShift クラスターを作成し、クラスター API アドレスを取得する*: OpenShift コンソールで、クラスターをセットアップした後、［**ホーム**］>［**概要**］>［**詳細**］ に移動し、クラスター API アドレスを取得します。
2. *OpenShift コマンドラインインターフェイス (CLI) (oc コマンド) を使用してサービスアカウントを作成し、サービスアカウントトークンを取得する*: サービスアカウントトークンは、サービスアカウントに関連付けられた認証資格情報です。サービスアカウントは、OpenShift プラグインを OpenShift で認証するために使用されます。各サービスアカウントは、1 つの namespace に関連付けられています。

3. *サービスアカウントのアクセス許可を構成する*: サービスアカウントは複数のロールを持つことができ、各ロールは OpenShift プラグインがどのリソースに対してどのようなアクションを実行できるかを定義するアクセス許可で構成されます。ロールは **ロールバインディング** を介してバインドされ、**ロールバインディング** には次の 2 種類があります。

   a. **クラスター全体のロールバインディング**: OpenShiftからイベントを受信するために使用されます。 名前空間にバインドされたロールバインディング: 特定の名前空間でVMを管理するために使用されます。

   b. **名前空間にバインドされたロールバインディング**: 特定の名前空間でVMを管理するために使用されます。

4. *名前空間 (プロジェクト) の作成*: OpenShift の名前空間は、VM やネットワークなどのリソースをグループ化する分離された環境であり、より良い組織化とアクセス制御を可能にします。**名前空間**は Kubernetes の用語であり、**プロジェクト**は OpenShift の用語です。OpenShift プラグインの観点からは、これらは同じです。VM を展開するには名前空間が必要です。OpenShift コンソールまたは OpenShift Container Platform CLI を使用して名前空間を作成します。

5. *ターゲット名前空間の下にネットワークアタッチメント定義を1つ作成する*: ネットワークアタッチメント定義は、OpenShift で実行されている VM のネットワーク構成を指定します。**Networking > NetworkAttachmentDefinitions** の下で、各名前空間のネットワークアタッチメント定義を確認できます。

6. *ストレージクラスの構成*: ストレージクラスは、VM ストレージがどのように割り当てられるかを定義します。**Storage > StorageClass** の下で、ストレージプロバイダーのリストを構成および確認できます。

サービスアカウントを作成する

1. oc コマンドラインツールをダウンロードして解凍します。
2. ログインIDを使用してOpenShiftコンソールにアクセスします。
3. ユーザープロファイルをクリックし、**ログインコマンドをコピー**をクリックします。
4. **トークンを表示**をクリックし、トークンをコピーします。
5. ocコマンドラインを使用してログインコマンドを実行します。例:

```
.\oc.exe login --token=<token> --server=<server address>
```

6. サービスアカウントを作成します。

   - デフォルトの名前空間の下にサービスアカウントを作成する場合は、次を実行します。

```
.\oc.exe create sa <service account name>
```

- 独自のの名前空間の下にサービスアカウントを作成する場合は、次を実行します。

```
.\oc.exe create sa <service account name> -n mynamespace
```

7. シークレット用の `YAML` ファイルを作成します。例:

- デフォルトのネームスペースでサービスアカウントを作成する場合:

```
apiVersion: v1

kind: Secret

metadata:

name: service account name

annotations:

kubernetes.io/service-account.name: service account name

type: kubernetes.io/service-account-token
```

- 独自のネームスペースでサービスアカウントを作成する場合:

```
apiVersion: v1

kind: Secret

metadata:

name: service account name

namespace: mynamespace

annotations:

kubernetes.io/service-account.name: service account name
```

```
type: kubernetes.io/service-account-token
```

8. YAMLを適用します。

```
.\oc.exe apply -f <yamlFile.yaml>
```

> **注:**
>
> `oc` はトークンを取得するためのシークレットを記述しています。そのトークンはパスワードとして使用されます。

サービスアカウントのロールとロールバインディングを作成する

クラスター全体のロールバインディングにより、サービスアカウントはクラスター全体のすべてのVMイベントを読み取る権限を持ち、OpenShiftプラグインがすべてのVM関連イベントに対して単一のイベントウォッチャーを維持できるようになります。

名前空間のロールバインディングにより、サービスアカウントはターゲットの名前空間でVMを管理する権限を持ちます。

スクリプトを使用してロールを作成し、サービスアカウントにバインドすることも、OpenShiftコンソールまたはCLIを使用してロールとロールバインディングを作成することもできます。

次のステップ

- コアコンポーネントをインストールする
- VDAをインストールする
- サイトを作成する
- 接続の作成と管理については、Red Hat OpenShiftへの接続を参照してください。

詳細情報

- 接続とリソースを作成および管理する
- マシンカタログを作成する

VMware 仮想化環境

仮想マシンを提供するのにVMwareを使用する場合は、このガイダンスに従ってください。

vCenter Serverと適切な管理ツールをインストールします。(vSphere vCenter Linked Mode操作はサポートされていません。)

MCSを使用する予定がある場合は、vCenter ServerのDatastore Browser機能 (https://kb.vmware.com/s/article/2101567で説明) を無効にしないでください。この機能を無効にすると、MCSは正しく動作しません。

次のステップ

- コアコンポーネントのインストール
- VDAのインストール
- サイトの作成
- VMware環境での接続の作成と管理については、「Connection to VMware」を参照してください。

詳細情報

- 接続とリソースの作成および管理
- マシンカタログの作成

VMware クラウドおよびパートナーソリューション

Citrix Virtual Apps and Desktops™ は、以下の VMware クラウドおよびパートナーソリューションをサポートしています。

- アジュール VMware ソリューション (AVS)
- グーグルクラウド VMware エンジン
- アマゾン ウェブ サービス (AWS) 上の VMware Cloud

アジュール VMware ソリューション (AVS) の統合

Citrix Virtual Apps and Desktop サービスはAVSをサポートしています。AVSは、Azureインフラストラクチャによって作成されたvSphereクラスターを含むクラウドインフラストラクチャを提供します。オンプレミス環境でvSphereを使用するのと同じ方法で、Citrix Virtual Apps and Desktop Serviceを活用してAVSをVDAワークロードのプロビジョニングに使用できます。

AVSクラスターのセットアップ

Citrix Virtual Apps™ and Desktop ServiceでAVSを使用できるようにするには、Azureで次の手順を実行します。

- ホストクォータを要求する

- Microsoft.AVS リソース プロバイダーを登録する
- ネットワークチェックリスト
- Azure VMware Solution プライベートクラウドを作成する
- Azure VMware Solution プライベートクラウドにアクセスする
- AzureでVMwareプライベートクラウドのネットワークを構成する
- Azure VMware Solution の DHCP を構成する
- Azure VMware Solution にネットワークセグメントを追加する
- Azure VMware Solution 環境を確認する

AZURE ENTERPRISE AGREEMENTのお客様のホストクォータを要求する

Azureポータルの**ヘルプとサポート**ページで、**新しいサポートリクエスト**を選択し、次の情報を含めます。

- 問題の種類: 技術
- サブスクリプション: サブスクリプションを選択してください
- サービス: すべてのサービス > Azure VMware Solution
- リソース: 一般的な質問
- 概要: 容量が必要
- 問題の種類: 容量管理の問題
- 問題のサブタイプ: 追加ホストクォータ/容量に関するお客様からのリクエスト

サポートチケットの に、 タブで次の情報を含めます。

- POC または本番環境
- リージョン名
- ホスト数
- その他の詳細

> **注:**
>
> AVS には最低 3 つのホストが必要であり、N+1 ホストの冗長性を使用することをお勧めします。

> サポートチケットの詳細を指定した後、**Review + Create** を選択してAzureにリクエストを送信します。

MICROSOFT.AVS リソース プロバイダーを登録する

ホスト クォータを要求した後、リソース プロバイダーを登録します。

1. Azureポータルにサインインします。
2. Azureポータルメニューで、**すべてのサービス** を選択します。
3. **すべてのサービス** メニューで、サブスクリプションを入力し、**サブスクリプション** を選択します。
4. サブスクリプションリストからサブスクリプションを選択します。
5. **リソースプロバイダー** を選択し、検索バーに **Microsoft.AVS** と入力します。
6. リソースプロバイダーが登録されていない場合は、**登録** を選択します。

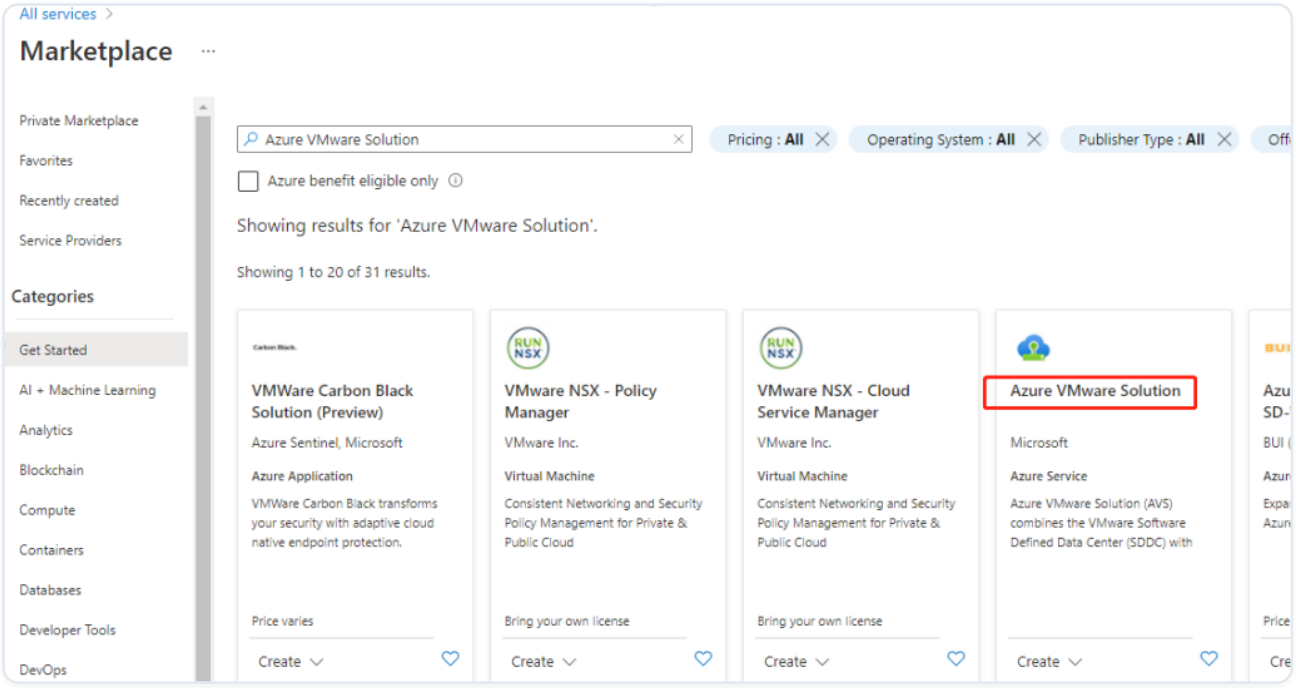
ネットワークに関する考慮事項

AVSは、特定のネットワークアドレス範囲とファイアウォールポートを必要とするネットワークサービスを提供します。詳細については、Azure VMware Solution のネットワーク計画チェックリスト を参照してください。

AZURE VMWARE SOLUTION プライベートクラウドを作成する

環境のネットワーク要件を考慮した後、AVS プライベートクラウドを作成します。

1. Azureポータルにサインインします。
2. **新しいリソースの作成**を選択します。
3. **Marketplace の検索**テキストボックスに「*Azure VMware Solution*」と入力し、リストから**Azure VMware Solution**を選択します。



image

Azure VMware Solutionウィンドウで、:

1. **作成**を選択します。
2. タブをクリックします。
3. 以下の表の情報を使用して、フィールドに値を入力します。

フィールド	値
サブスクリプション	デプロイに使用する予定のサブスクリプションを選択します。Azure サブスクリプション内のすべてのリソースはまとめて請求されます。
リソースグループ	プライベートクラウドのリソースグループを選択します。Azureリソースグループは、Azureリソースがデプロイおよび管理される論理コンテナです。または、プライベートクラウド用に新しいリソースグループを作成することもできます。
場所	east us のような場所を選択します。これは、計画フェーズで定義したリージョンです。
リソース名	Azure VMware Solution プライベートクラウドの名前を指定します。

フィールド	値
SKU	AV36 を選択します。
ホスト	プライベートクラウドクラスターに割り当てられたホストの数を表示します。デフォルト値は3で、デプロイ後に増減できます。
アドレスブロック	プライベートクラウドのIPアドレスブロックを指定します。CIDRはプライベートクラウド管理ネットワークを表し、vCenter ServerやNSX-T Managerなどのクラスター管理サービスに使用されます。例えば、10.175.0.0/22 のように /22 アドレス空間を使用します。このアドレスは一意であり、他のAzure仮想ネットワークやオンプレミスネットワークと重複しないようにしてください。
仮想ネットワーク	Azure VMware Solution ExpressRoute 回線はデプロイ後の手順として確立されるため、ここは空白のままにします。

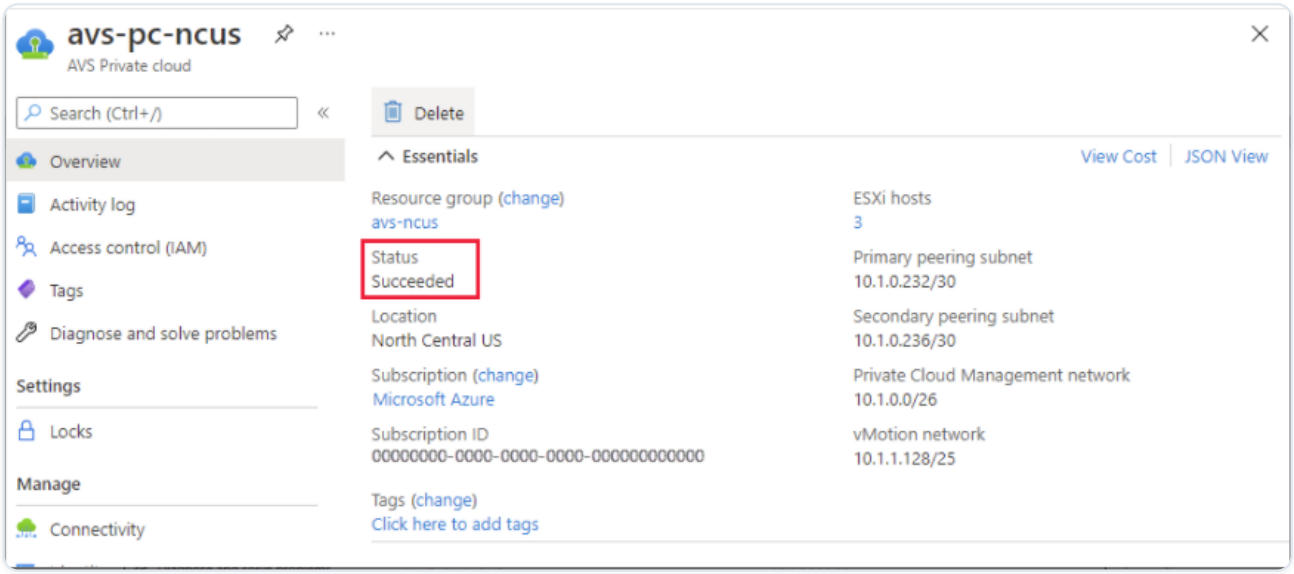
「**プライベートクラウドの作成**」画面で、:

1. 「**場所**」フィールドで、AVS が存在するリージョンを選択します。リソースグループのリージョンは AVS リージョンと同じです。
2. 「**SKU**」フィールドで「**AV36 Node**」を選択します。
3. 「**Address Block**」フィールドにIPアドレスを指定します。例: 10.15.0.0/22。
4. 「**Review + Create**」を選択します。
5. 情報を確認したら、「**Create**」をクリックします。

Azure ASV プライベートクラウドの作成(/en-us/citrix-virtual-apps-desktops/2503/media/azure-avs-create-private-cloud.png)

> **ヒント:**
>
> プライベートクラウドの作成には3〜4時間かかる場合があります。クラスターに単一ホストを追加するには30〜45分かかる場合があります。

> 展開が成功したことを確認します。作成したリソースグループに移動し、プライベートクラウドを選択します。**ステータス**が**成功**になったら、展開は完了です。



AZURE VMWARE SOLUTION プライベートクラウドへのアクセス

プライベートクラウドを作成したら、Windows VMを作成し、プライベートクラウドのローカルvCenterに接続します。
新しいWindows仮想マシンの作成

1. リソースグループで「**+ Add**」を選択し、「**Microsoft Windows 10/2016/2019**」を検索して選択します。
2. 「**Create**」をクリックします。
3. 必要な情報を入力し、「**Review + Create**」を選択します。
4. 検証に合格したら、**作成**を選択して仮想マシンの作成プロセスを開始します。

プライベートクラウドのローカルvCenterに接続する

1. クラウド管理者として **vSphere Client with VMware vCenter SSO** にサインインします。

   Azure ASV vSphere ログイン(/en-us/citrix-virtual-apps-desktops/2503/media/azure-avs-vsphere-login.png)

2. Azure portal でプライベートクラウドを選択し、 **>** を選択します。

プライベートクラウドのvCenterおよびNSX-T ManagerのURLとユーザー資格情報が表示されます。

Azure ASV セットアップ vCenter(/en-us/citrix-virtual-apps-desktops/2503/media/azure-avs-setup-vcenter.png)

URLとユーザー資格情報を確認した後:

1. 前の手順で作成したVMに移動し、仮想マシンに接続します。
2. Windows VMでブラウザを開き、vCenterおよびNSX-T ManagerのURLを2つのブラウザタブで開きます。vCenterタブで、前の手順の*cloudadmin@vmcp.local*ユーザー資格情報を入力します。

AZUREでVMWAREプライベートクラウドのネットワークを構成する

ASVプライベートクラウドにアクセスした後、仮想ネットワークとゲートウェイを作成してネットワークを構成します。
仮想ネットワークを作成する

1. Azure portal にサインインします。
2. 以前に作成したリソースグループに移動します。
3. 「**+ 追加**」を選択して、新しいリソースを定義します。
4. 「**Marketplace を検索**」テキストボックスに「*仮想ネットワーク*」と入力します。仮想ネットワークリソースを見つけて選択します。
5. 「**仮想ネットワーク**」ページで、「**作成**」を選択してプライベートクラウドの仮想ネットワークを設定します。
6. 「**仮想ネットワークの作成**」ページで、仮想ネットワークの詳細を入力します。
7. 「**基本**」タブで、仮想ネットワークの名前を入力し、適切なリージョンを選択して、「**次へ : IP アドレス**」をクリックします。
8. 「**IP アドレス**」タブの IPv4 アドレス空間の下に、以前に作成したアドレスを入力します。

> **重要:**
>
> プライベートクラウドを作成したときに使用したアドレス空間と重複しないアドレスを使用してください。

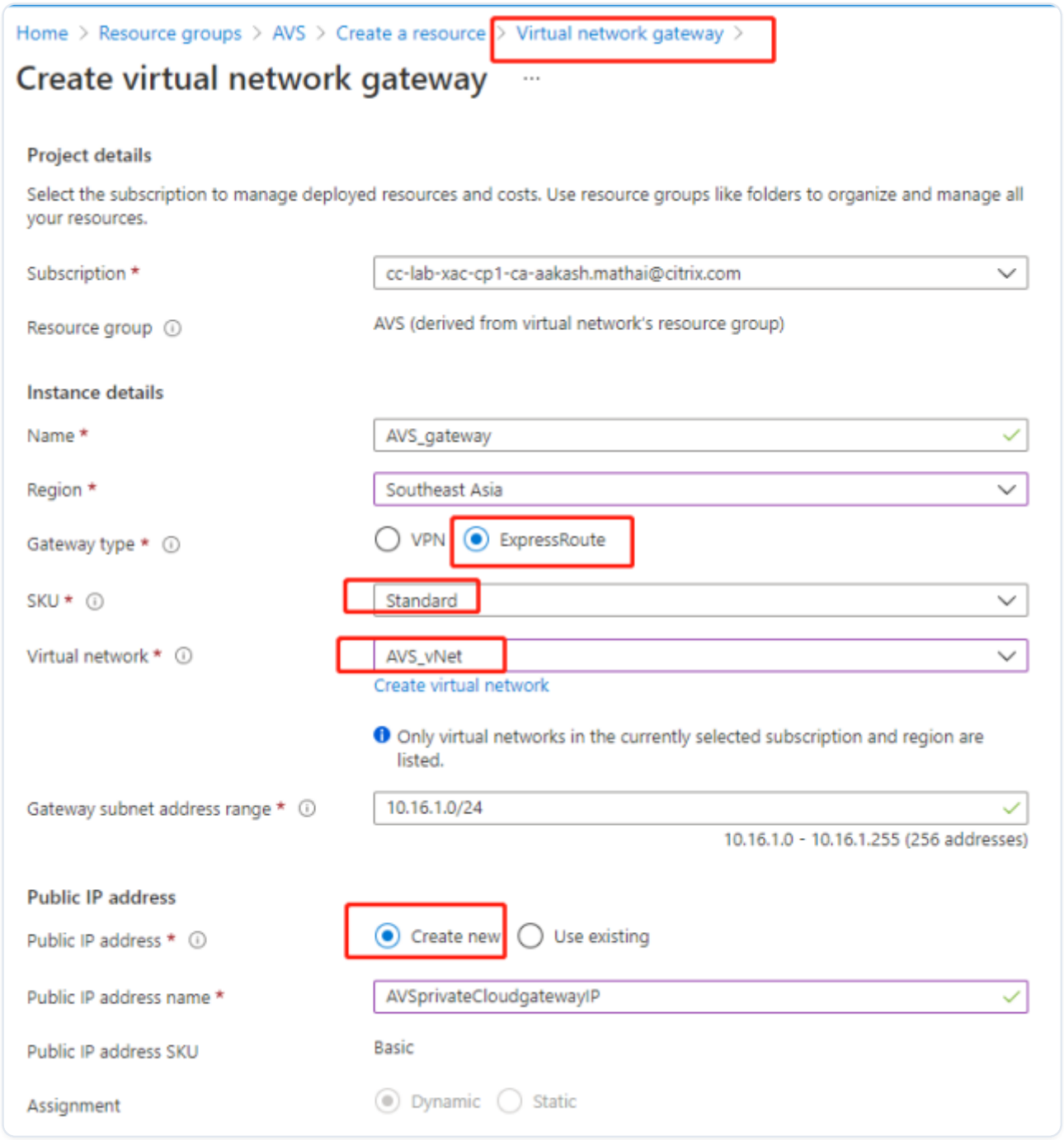
アドレス空間を入力した後:

1. 「**+ サブネットの追加**」を選択します。
2. 「**サブネットの追加**」ページで、サブネットに名前と適切なアドレス範囲を割り当てます。
3. 「**追加**」をクリックします。
4. 「**確認 + 作成**」を選択します。

5. 情報を確認し、「**作成**」をクリックします。デプロイが完了すると、仮想ネットワークがリソースグループに表示されます。

仮想ネットワークゲートウェイを作成する
仮想ネットワークを作成した後、仮想ネットワークゲートウェイを作成します。

1. リソースグループで、新しいリソースを追加するために**+ 追加**を選択します。
2. **Marketplace を検索**テキストボックスに「*仮想ネットワークゲートウェイ*」と入力します。仮想ネットワークリソースを見つけて選択します。
3. **仮想ネットワークゲートウェイ**ページで、**作成**をクリックします。
4. **仮想ネットワークゲートウェイの作成**ページの**基本**タブで、フィールドの値を入力します。
5. **確認 + 作成**をクリックします。



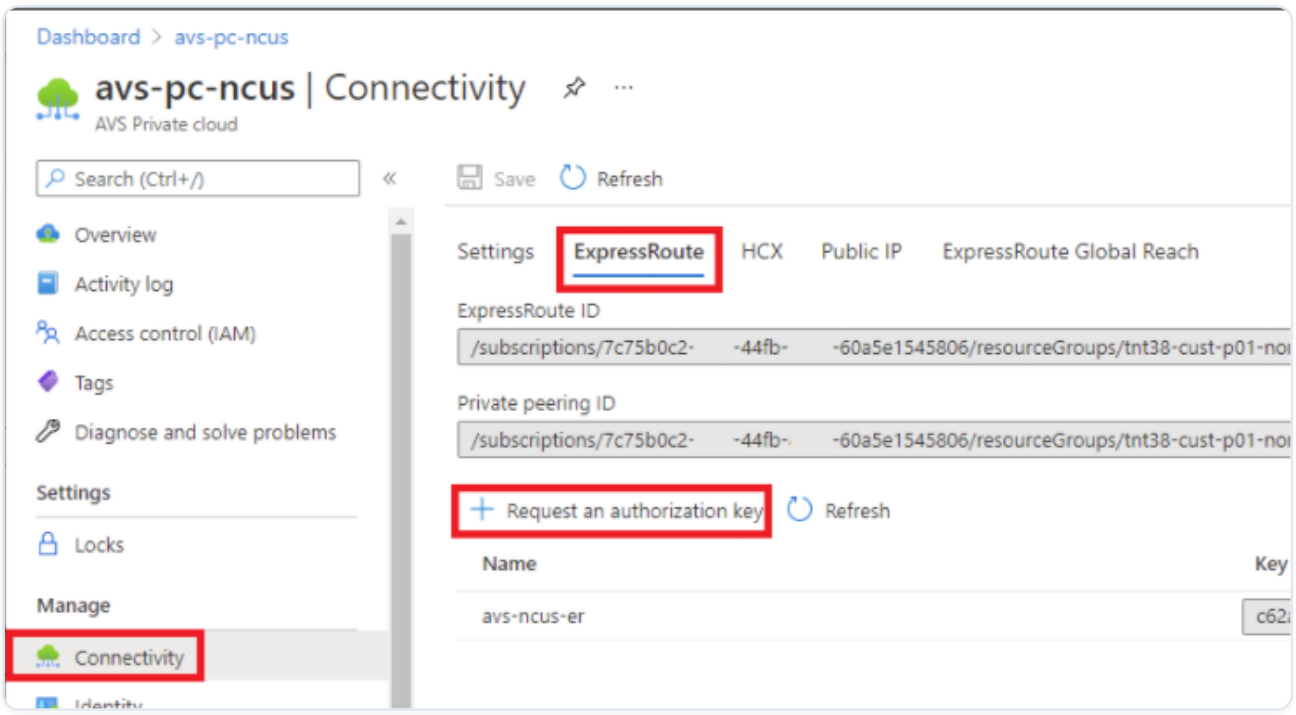
仮想ネットワークゲートウェイの構成を確認したら、**作成**をクリックして仮想ネットワークゲートウェイを展開します。 展開が完了したら、**ExpressRoute**接続をAzure AVSプライベートクラウドを含む仮想ネットワークゲートウェイに接続します。

EXPRESSROUTEを仮想ネットワークゲートウェイに接続する

仮想ネットワークゲートウェイを展開した後、それとAzure AVSプライベートクラウドの間に接続を追加します。

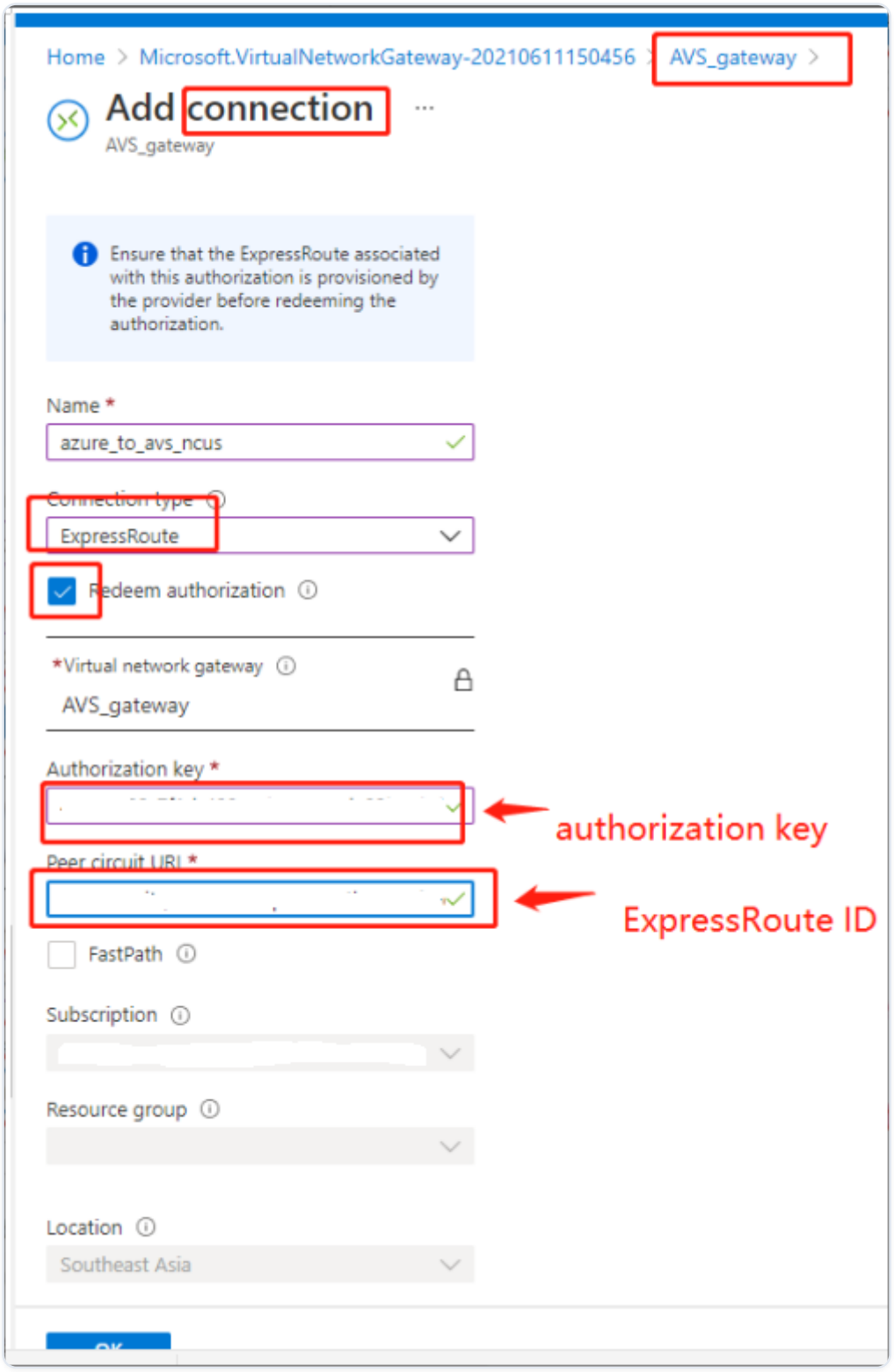
1. ExpressRoute承認キーを要求します。

2. Azureポータルで、**Azure VMware Solution private cloud**に移動します。「**Manage> Connectivity > ExpressRoute**」を選択し、次に「**+ Request an authorization key**」を選択します。

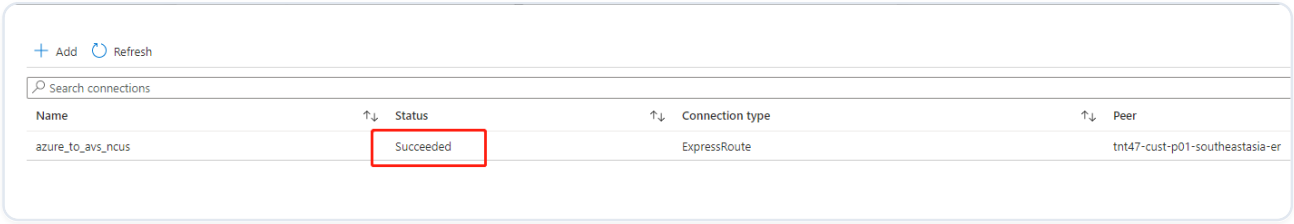


承認キーを要求した後：

1. キーの名前を入力し、**作成**をクリックします。キーの作成には約30秒かかる場合があります。作成されると、新しいキーはプライベートクラウドの承認キーのリストに表示されます。
2. **承認キー**と**ExpressRoute ID**をコピーします。これらはピアリングプロセスを完了するために必要です。承認キーはしばらくすると消えるため、表示されたらすぐにコピーしてください。
3. 使用する**仮想ネットワークゲートウェイ**に移動し、**接続 > + 追加**を選択します。
4. **接続の追加**ページで、フィールドに値を入力し、**OK**を選択します。



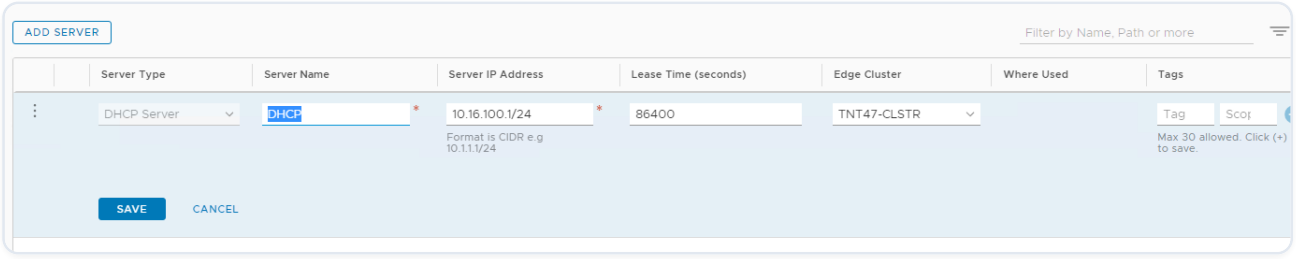
ExpressRoute回線と仮想ネットワーク間の接続が確立されます。



AZURE VMWARE SOLUTION の DHCP を構成する

ExpressRouteを仮想ゲートウェイに接続した後、DHCPを構成します。
NSX-T を使用して DHCP サーバーをホストする
NSX-T Manager において:

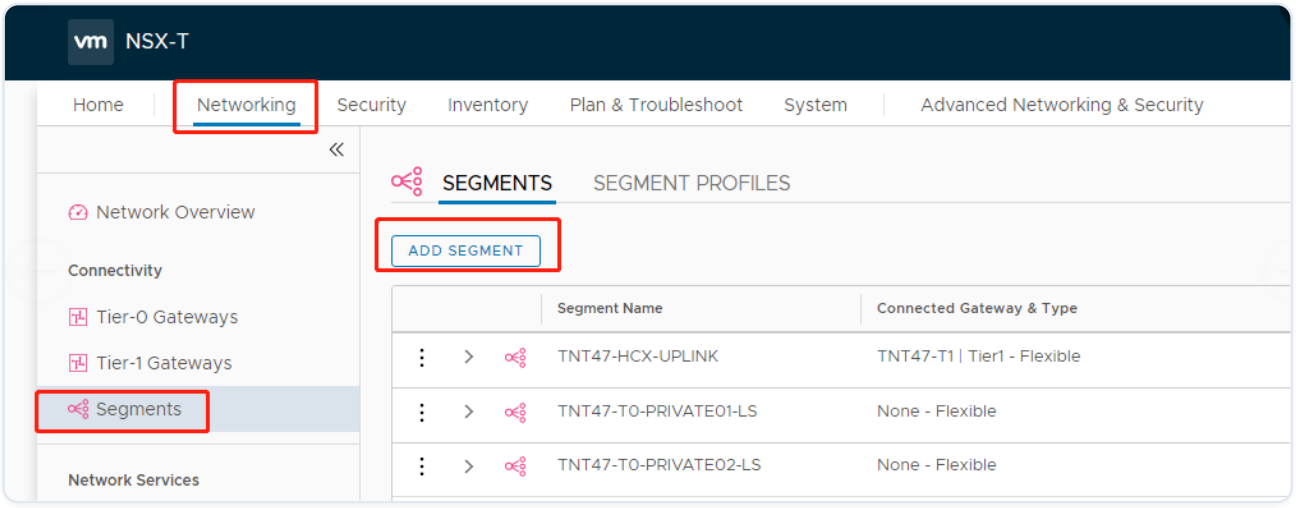
1. **ネットワーク > DHCP** を選択し、**サーバーの追加**を選択します。
2. **サーバーの種類**として**DHCP**を選択し、サーバー名と IP アドレスを入力します。
3. **保存**をクリックします。
4. **Tier 1 ゲートウェイ**を選択し、Tier-1 ゲートウェイの縦の省略記号を選択してから、**編集**を選択します。
5. サブネットを追加するには、**IP 割り当てなし**を選択します。
6. 「**タイプ**」には「**DHCP Local Server**」を選択します。
7. 「**DHCP Server**」には「**Default DHCP**」を選択し、「**Save**」をクリックします。
8. 再度「**Save**」をクリックし、「**Close Editing**」を選択します。



AZURE VMWARE SOLUTIONでネットワークセグメントを追加する

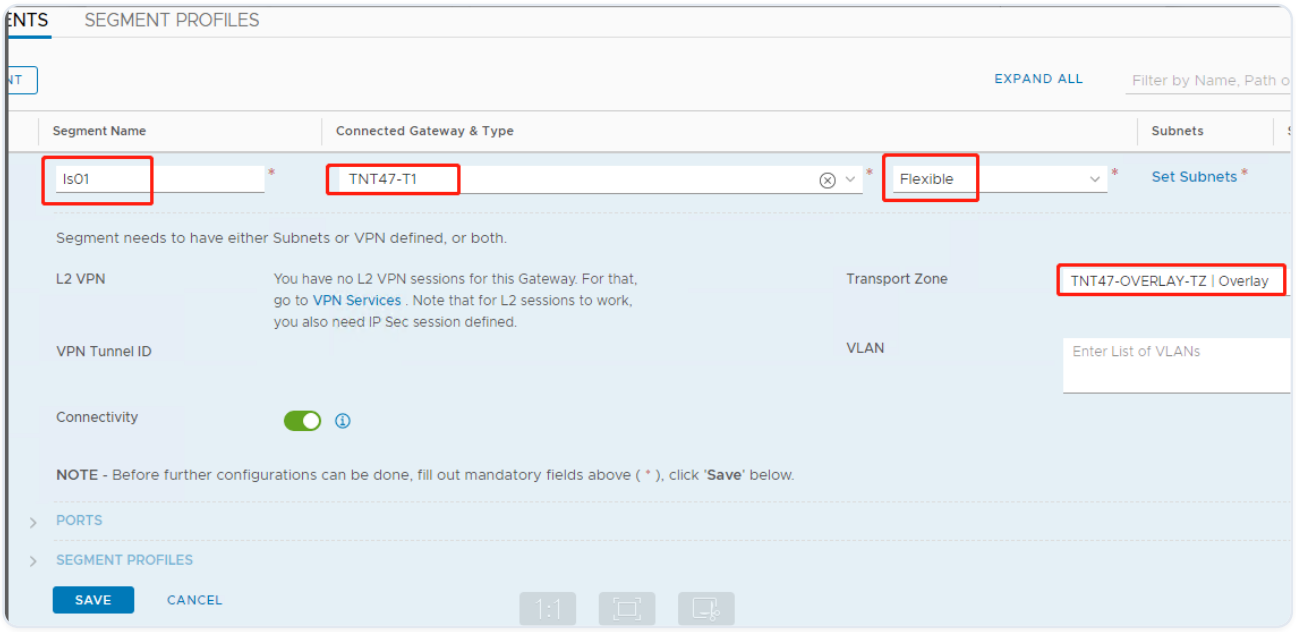
DHCPを設定した後、ネットワークセグメントを追加します。

ネットワークセグメントを追加するには、NSX-T Managerで「**Networking> Segments**」を選択し、「**Add Segment**」をクリックします。



「**Segments profile**」画面で:

1. セグメントの**名前**を入力します。
2. 「**Connected Gateway**」として「**Tier-1 Gateway (TNTxx-T1)**」を選択し、「**タイプ**」は「**Flexible**」のままにします。
3. 事前構成済みのオーバーレイ「**Transport Zone(TNTxx-OVERLAY-TZ)**」を選択します。
4. 「**Set Subnets**」をクリックします。



「**Subnets**」セクションで:

1. ゲートウェイIPアドレスを入力します。
2. **Add**を選択します。

> **重要:**
>
> このセグメントIPアドレスは、Azureゲートウェイ IPアドレス10.15.0.0/22に属している必要があります。
>
> DHCP範囲はセグメントIPアドレスに属している必要があります。

Azure ASVでNSX-Tセグメントの DHCP範囲を追加(/en-us/citrix-virtual-apps-desktops/2503/media/azure-avs-nsx-t-dhcp-range.png)

セグメントの構成を続行するオプションを拒否するには、 を選択します:

Azure ASVでNSX-Tのセットアップを完了(/en-us/citrix-virtual-apps-desktops/2503/media/azure-avs-nsx-t-finish-setup.png)

vCenterで、 > を選択します:

Azure ASVでNSX-T vCenterを追加(/en-us/citrix-virtual-apps-desktops/2503/media/azure-avs-nsx-t-vcenter.png)

AZURE AVS環境を確認する

Azureリソースグループで直接接続とコネクタを設定します。

Azure ASVでASV接続を確認(/en-us/citrix-virtual-apps-desktops/2503/media/azure-avs-verify-connection-create-dc-v2.png)

vCenterの資格情報で接続を確認します。

Azure ASVでNSX-T vCenterを追加(/en-us/citrix-virtual-apps-desktops/2503/media/azure-avs-final-setup.png)

Google Cloud VMware エンジン

Citrix Virtual Apps and Desktopsを使用すると、VMwareベースのオンプレミスCitrixワークロードをGoogle Cloud VMware Engineに移行できます。

Google Cloud VMware エンジンの構成

次の手順では、Google Cloud VMware Engineでクラスターを取得してセットアップする方法について説明します。

VMWARE ENGINEポータルにアクセスする

1. **Google Cloud コンソール**で、ナビゲーションメニューをクリックします。
2. **Compute**セクションで、**VMware Engine**をクリックして、新しいブラウザータブでVMware Engineを開きます。

最初のプライベートクラウドを作成するための要件

Google Cloud VMware Engineへのアクセス権、利用可能なVMware Engineノードクォータ、および適切なIAMロールが必要です。プライベートクラウドの作成を続行する前に、以下の要件を準備してください。

1. APIアクセスとノードクォータをリクエストします。詳細については、「APIアクセスとクォータのリクエスト」を参照してください。
2. VMware管理アプライアンスおよびHCX展開ネットワークに使用するアドレス範囲をメモします。詳細については、「ネットワーク要件」を参照してください。
3. VMware Engine Service Admin IAMロールを取得します。

最初のプライベートクラウドを作成する

1. VMware Engineポータルにアクセスします。
2. VMware Engineのホームページで、**Create a private cloud**をクリックします。ホスティングの場所とハードウェアノードのタイプが一覧表示されます。
3. プライベートクラウドのノード数を選択します。少なくとも3つのノードが必要です。
4. VMware管理ネットワークのクラスレスドメイン間ルーティング（CIDR）範囲を入力します。
5. HCX展開ネットワークのCIDR範囲を入力します。

> **重要:**
>
> CIDR範囲は、オンプレミスまたはクラウドのサブネットと重複してはなりません。CIDR範囲は/27以上である必要があります。

6. を選択します。
7. 設定を確認します。設定を変更するには、 をクリックします。
8. プライベートクラウドの作成を開始するには、 をクリックします。

VMware Engineが新しいプライベートクラウドを作成すると、いくつかのVMwareコンポーネントが展開され、プライベートクラウド内のクラスターの初期Autoscale™ポリシーが設定されます。プライベートクラウドの作成には30分から2時間かかる場合があります。プロビジョニングが完了すると、メールが届きます。

GOOGLE CLOUD VMWARE ENGINE VPNゲートウェイをセットアップする

Google Cloud VMware Engineへの初期接続を確立するには、VPNゲートウェイを使用できます。これはOpenVPNベースのクライアントVPNであり、これを使用してVMware Software Defined Data Center (SDDC) vCenterに接続し、必要な初期構成を行うことができます。

VPNゲートウェイを展開する前に、SDDCが展開されているリージョンの**Edge Services**範囲を構成します。これを行うには：

1. **Google Cloud VMware Engine**ポータルにログオンし、 **>** に移動します。 をクリックします。
2. SDDCが展開されているリージョンを選択し、 と を有効にします。
3. 計画中にメモしたEdge Servicesの範囲を入力し、 をクリックします。これらのサービスを有効にするには10〜15分かかります。

完了すると、地域設定ページでエッジサービスが**有効**と表示されます。これらの設定を有効にすると、SDDCにパブリックIPを割り当てることができます。これはVPNゲートウェイを展開するための要件です。

VPNゲートウェイを展開するには：

1. **Google Cloud VMware Engine**ポータルで、**ネットワーク > VPNゲートウェイ**に移動します。**新しいVPNゲートウェイの作成**をクリックします。
2. VPNゲートウェイの名前と、計画中に予約したクライアントサブネットを入力します。**次へ**をクリックします。
3. VPNアクセスを許可するユーザーを選択します。**次へ**をクリックします。
4. VPN経由でアクセス可能にする必要があるネットワークを指定します。**次へ**をクリックします。
5. 概要画面が表示されます。選択内容を確認し、**送信**をクリックしてVPNゲートウェイを作成します。新しいVPNゲートウェイのステータスが**作成中**としてVPNゲートウェイページに表示されます。
6. ステータスが**稼働中**に変わったら、新しいVPNゲートウェイをクリックします。
7. **VPN構成をダウンロード**をクリックして、VPNゲートウェイ用の事前構成済みOpenVPNプロファイルを含むZIPファイルをダウンロードします。UDP/1194およびTCP/443経由で接続するためのプロファイルが利用可能です。好みを選択してOpenVPNにインポートし、接続します。
8. **リソース**に移動し、SDDCを選択します。

VPNを接続する

1. VPNゲートウェイの設定を通じて、オンプレミスネットワークとプライベートクラウド間のポイントツーサイト接続を確立します。「Google Cloud VMware Engine VPNゲートウェイのセットアップ」(#set-up-google-cloud-vmware-engine-vpn-gateway)を参照してください。
2. 「Google Cloud VMware Engine VPNゲートウェイのセットアップ」(#set-up-google-cloud-vmware-engine-vpn-gateway)でダウンロードしたVPN構成をアップロードします。
3. VPNクライアント（たとえば、OpenVPN Connect）にインポートします。

詳細については、VPNを使用した接続を参照してください。

最初のサブネットを作成する

VMware EngineポータルからNSX-T Managerにアクセスする
サブネットの作成プロセスはNSX-Tで行われ、VMware Engineを介してアクセスします。NSX-T Managerにアクセスするには、次の手順を実行します。

1. **Google Cloud VMware Engine**ポータルにログオンします。
2. メインナビゲーションから、**リソース**に移動します。
3. サブネットを作成するプライベートクラウドに対応する**プライベートクラウド名**をクリックします。
4. プライベートクラウドの詳細ページで、**vSphere Management Network**タブをクリックします。
5. NSX-T Managerに対応する**FQDN**をクリックします。
6. プロンプトが表示されたら、サインイン資格情報を入力します。vIDMを設定し、Active DirectoryなどのIDソースに接続している場合は、代わりにIDソースの資格情報を使用します。

> **注意:**
>
> 生成された資格情報は、プライベートクラウドの詳細ページから取得できます。

サブネットのDHCPサービスを設定する
サブネットを作成する前に、DHCPサービスを設定します。

NSX-T マネージャーで:

1. **ネットワーキング > DHCP**に移動します。ネットワーキングダッシュボードには、DHCPサービスが1つのTier-0と1つのTier-1ゲートウェイを作成することが示されます。
2. DHCPサーバーのプロビジョニングを開始するには、**サーバーの追加**をクリックします。
3. **サーバータイプ**で**DHCP**を選択し、サーバー名とIPアドレスを入力します。
4. DHCPサービスを作成するには、**保存**をクリックします。

このDHCPサービスを関連するTier-1ゲートウェイにアタッチするには、次の手順を実行します。デフォルトのTier-1ゲートウェイは、DHCPサービスによってすでにプロビジョニングされています。

1. **Tier 1ゲートウェイ**を選択し、Tier-1ゲートウェイの縦の省略記号を選択してから、**編集**を選択します。
2. **IPアドレス管理**フィールドで、**IP割り当てなし**を選択します。
3. **タイプ**で**DHCPローカルサーバー**を選択します。
4. **DHCPサーバー**で、作成したDHCPサーバーを選択します。
5. **保存**をクリックします。

6. **編集を閉じる**をクリックします。

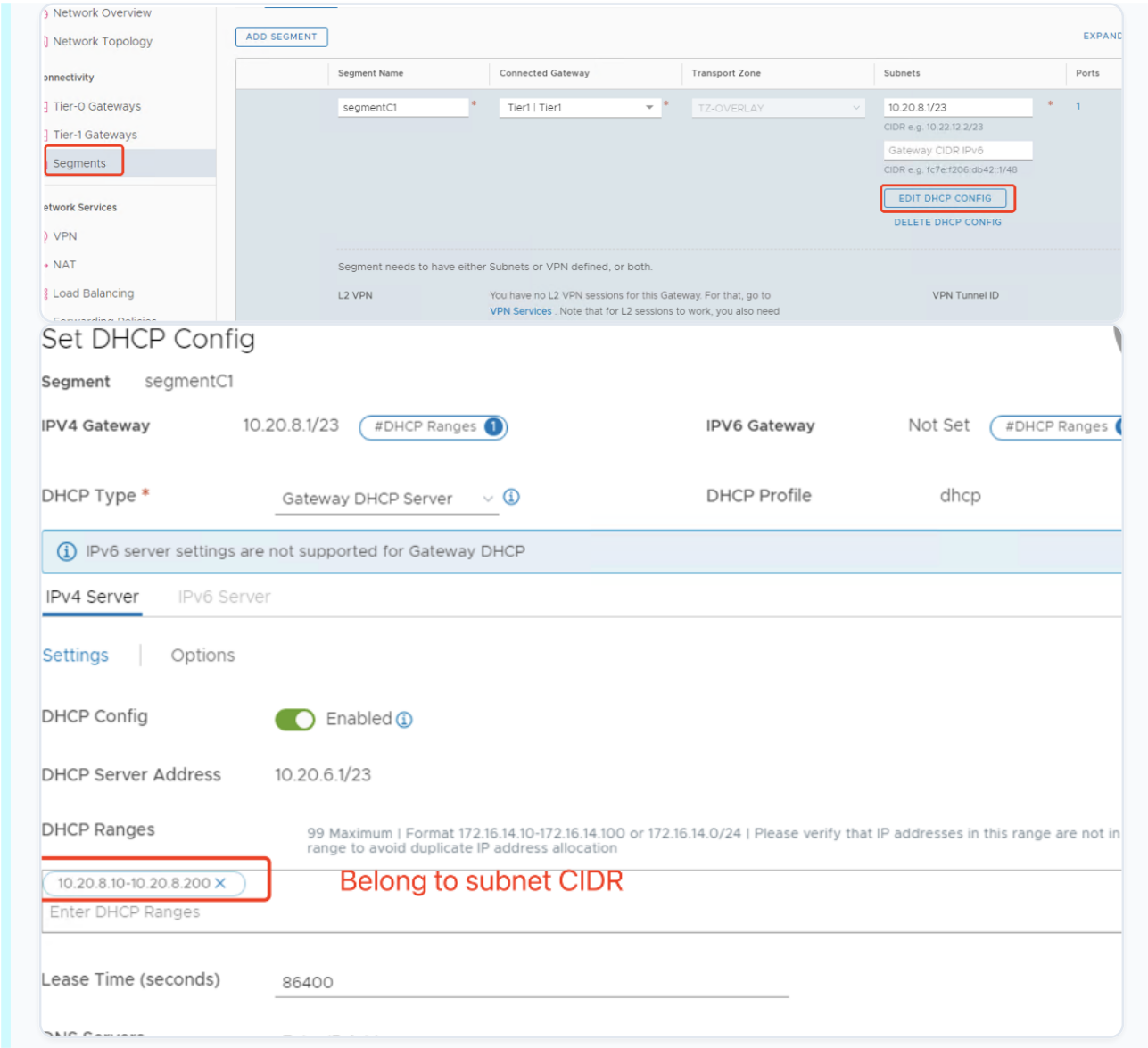
これで、NSX-T でネットワークセグメントを作成できます。NSX-T の DHCP の詳細については、DHCP に関する VMware ドキュメントを参照してください。
NSX-T でネットワークセグメントを作成する
ワークロード VM の場合、プライベートクラウドの NSX-T ネットワークセグメントとしてサブネットを作成します。

1. NSX-T Manager で、「**Networking > Segments**」に移動します。
2. 「**Add Segment**」をクリックします。
3. セグメントの名前を入力します。
4. 「**Connected Gateway**」として「**Tier-1**」を選択し、「Type」は「**Flexible**」のままにします。
5. 「**Set Subnets**」をクリックします。
6. 「**Add Subnets**」をクリックします。
7. 「**Gateway IP/Prefix Length**」にサブネット範囲を入力します。最後のオクテットが「**.1**」となるようにサブネット範囲を指定します。例: **10.12.2.1/24**。
8. DHCP範囲を指定し、**ADD**をクリックします。
9. **Transport Zone**で、ドロップダウンリストから**TZ-OVERLAY**を選択します。
10. **Save**をクリックします。これで、VMを作成する際にvCenterでこのネットワークセグメントを選択できます。

特定のリージョンでは、VMware EngineからVPC networkへのプライベートサービスアクセスを使用して、最大100個の一意のルートを設定できます。これには、たとえば、プライベートクラウド管理IPアドレス範囲、NSX-Tワークロードネットワークセグメント、HCXネットワークIPアドレス範囲が含まれます。この制限には、リージョン内のすべてのプライベートクラウドが含まれます。

> **注:**

> Google Cloudの構成上の問題により、DHCP範囲設定を複数回構成する必要があります。したがって、Google Cloudの構成後にDHCP範囲設定を必ず構成してください。DHCP範囲を構成するには、**EDIT DHCP CONFIG**をクリックします。



CITRIX STUDIOでGOOGLE CLOUD VMWARE接続を作成する

1. vCenterでマシンを作成します。
2. Citrix Studioを起動します。
3. ホスティングノードを選択し、「**接続とリソースの追加**」をクリックします。
4. 「**接続**」画面で、「**新しい接続の作成**」を選択し、次の詳細を入力します。

   接続とリソースの追加(/en-us/citrix-virtual-apps-desktops/2503/media/gcp-vmware-add-connection.png)

   a. 「**Connection type**」として「**VMware vSphere**」を選択します。
   b. 「**接続アドレス**」にvCenterのプライベートIPアドレスを入力します。
   c. vCenterの資格情報を入力します。
   d. 接続名を入力します。

e. 仮想マシンを作成するツールを選択します。

5. **ネットワーク**画面で、NSX-Tサーバーで作成されたサブネットを選択します。
6. ウィザードを完了します。

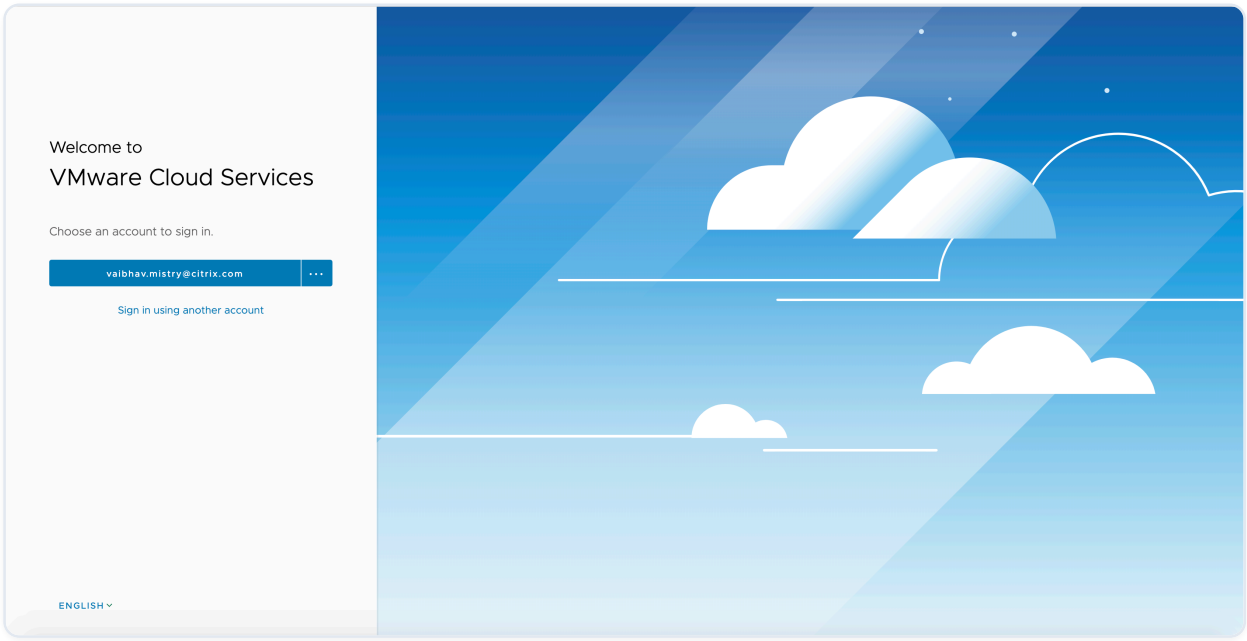
アマゾン ウェブ サービス (AWS) 上の ヴイエムウェア クラウド

Amazon Web Services (AWS) 上のVMware Cloudを使用すると、VMwareベースのオンプレミスCitrixワークロードをAWS Cloudに移行できます。

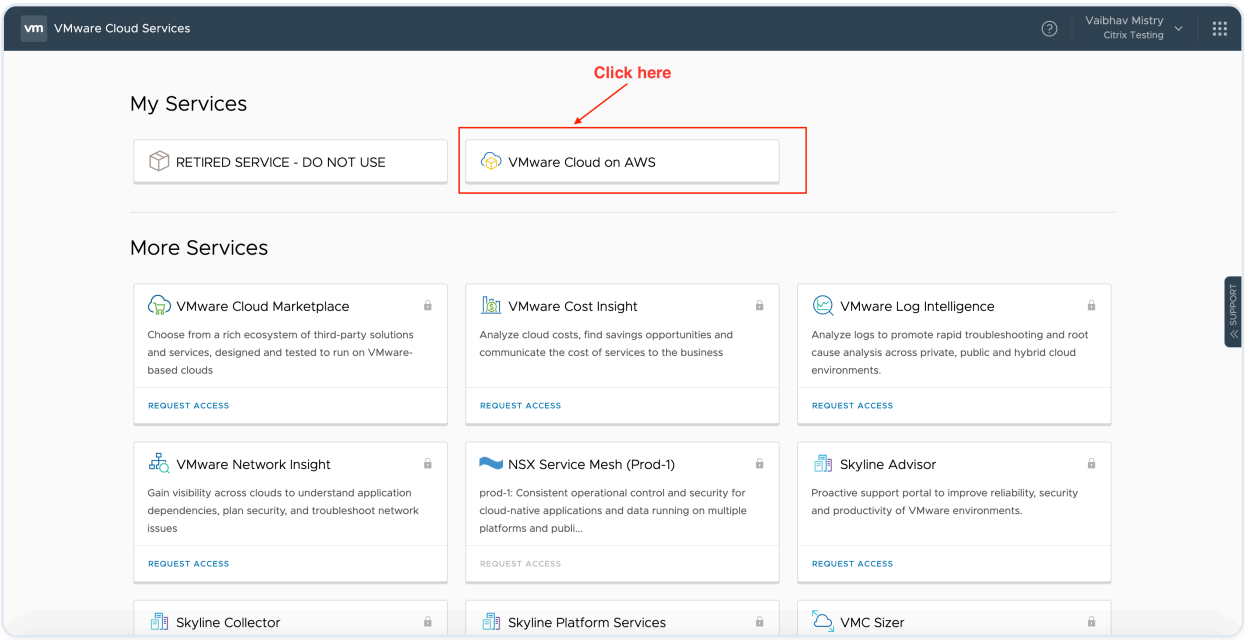
この記事では、AWS上にVMware Cloudをセットアップする手順について説明します。

VMware Cloud環境にアクセスする

1. URL `<https://console.cloud.vmware.com/>` を使用してVMware Cloudサービスにログインします。



2. **VMware Cloud on AWS** をクリックします。Software-Defined Data Centers (SDDC) ページが表示されます。

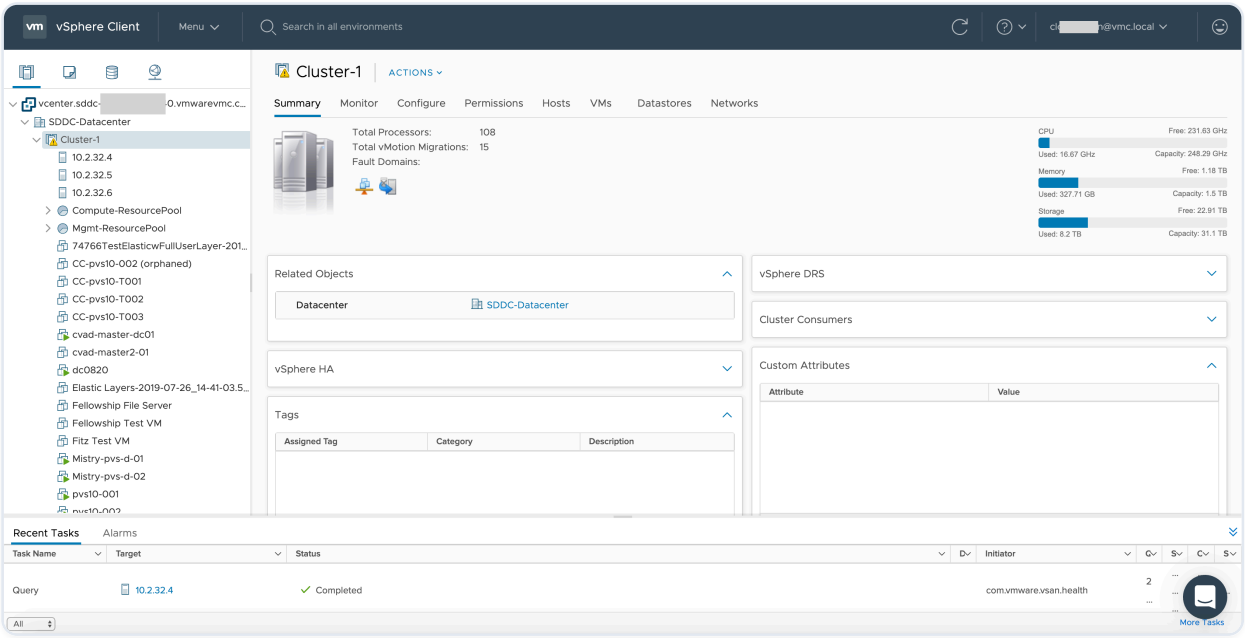


3. **OPEN VCENTER** をクリックし、次に **SHOW CREDENTIALS** をクリックします。後で使用するために資格情報を控えておきます。

   「vCenterを開く」(/en-us/citrix-virtual-apps-desktops/2503/media/vmc-sddc.png)

   「資格情報を表示」(/en-us/citrix-virtual-apps-desktops/2503/media/show-credentials-vmc.png)

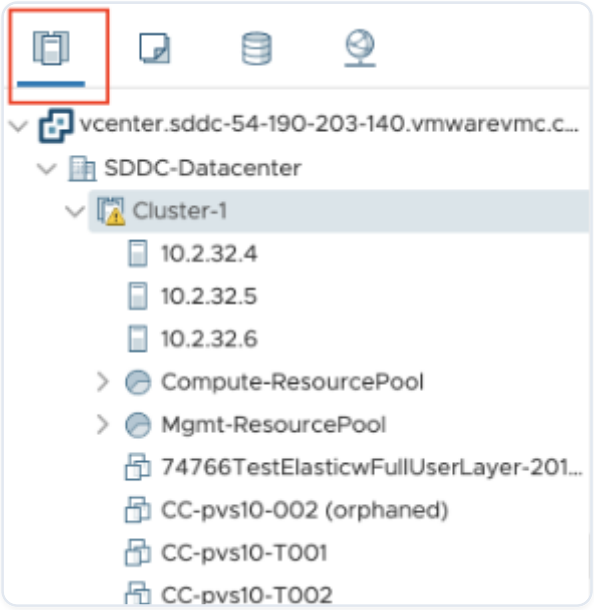
4. Webブラウザを開き、vSphere Web Client のURLを入力します。
5. 控えておいた資格情報を入力し、**Login** をクリックします。vSphereクライアントのWebページは、オンプレミス環境のものと似ています。



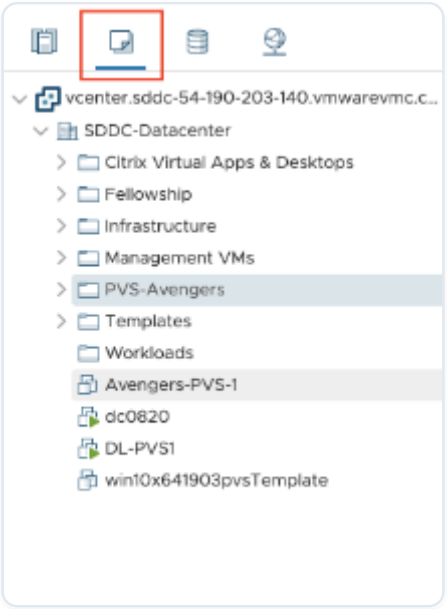
VMwareクラウド環境について

vSphereクライアントのWebページには4つのビューがあります。

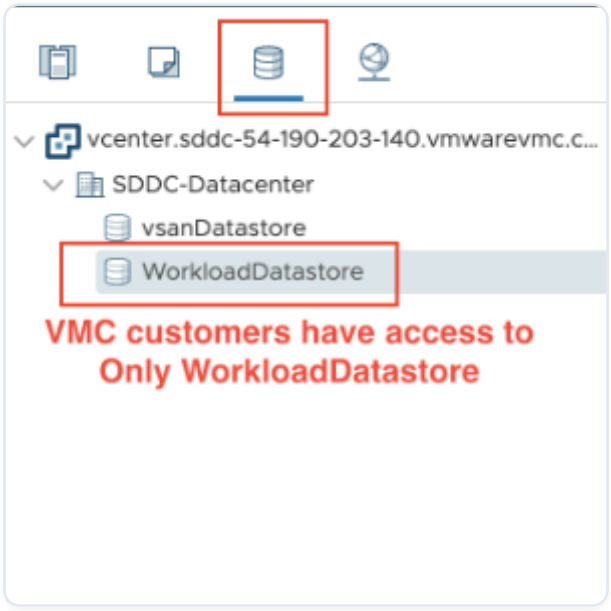
- ホストとクラスタのビュー: 新しいクラスタを作成することはできませんが、クラウド管理者は複数のリソースプールを作成できます。



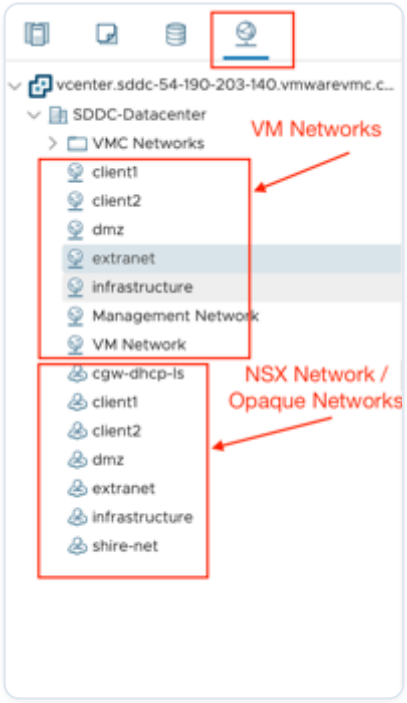
- VMとテンプレートのビュー: クラウド管理者は多くのフォルダを作成できます。



- ストレージビュー: Citrix Studioでホスティングユニットを追加する際、Workload Datastoreにのみアクセスできるため、**WorkloadDatastore**ストレージを選択します。



- ネットワークビュー: VMwareクラウドネットワークと不透明なネットワークでは、アイコンが異なります。



クラスターをセットアップした後、接続とリソースを追加するには、VMware仮想化環境を参照してください。

次のステップ

- コアコンポーネントのインストール
- VDAのインストール
- サイトの作成

- 接続の作成と管理については、「VMware Cloudおよびパートナーソリューションへの接続」を参照してください。

詳細情報

- 接続とリソースの作成と管理
- マシンカタログの作成

コアコンポーネントをインストールする

> **重要:**
>
> Citrix は、ライセンスコンプライアンスを含む正当な利益のために、必要に応じて基本的なライセンスデータを収集します。詳細については、「Citrix ライセンスデータ」を参照してください。

> コアコンポーネントは、Citrix Delivery Controller™、Citrix Studio、Web Studio、Citrix Director、および Citrix License Server です。

> **注:**
>
> Citrix Studio は、オンプレミスの Citrix Virtual Apps and Desktops 展開を構成および管理できる Windows ベースの管理コンソールです。Web Studio は Citrix Studio の次世代版であり、Citrix Studio と完全に同等の機能を提供する Web ベースの管理コンソールです。Web Studio の詳細については、「Web Studio のインストール」を参照してください。

> (2003 より前のバージョンでは、コアコンポーネントに Citrix StoreFront が含まれていました。**Citrix StoreFront** タイルをクリックするか、インストールメディアで利用可能なコマンドを実行することで、StoreFront をインストールできます。)

インストールを開始する前に、この記事と「インストールの準備」を確認してください。

この記事では、コアコンポーネントのインストール時のインストールウィザードのシーケンスについて説明します。コマンドラインの同等機能も提供されています。詳細については、「コマンドラインを使用したインストール」を参照してください。

ステップ 1. 製品ソフトウェアをダウンロードしてウィザードを起動する

Citrix アカウントの資格情報を使用して、Citrix Virtual Apps and Desktops™ のダウンロードページにアクセスします。製品の ISO ファイルをダウンロードします。

ファイルを解凍します。必要に応じて、ISO ファイルを DVD に書き込みます。

コアコンポーネントをインストールするマシンに、ローカル管理者アカウントを使用してログオンします。

DVD をドライブに挿入するか、ISO ファイルをマウントします。インストーラーが自動的に起動しない場合は、**AutoSelect** アプリケーションまたはマウントされたドライブをダブルクリックします。

ステップ 2. インストールする製品を選択する

コンポーネントインストーラーの製品選択ページ(/en-us/citrix-virtual-apps-desktops/2503/media/product-selector2-75.png)

インストールする製品（Virtual Apps または Virtual Apps and Desktops）の横にある「**開始**」をクリックします。

(マシンにCitrix Virtual Apps and Desktopsコンポーネントがすでにインストールされている場合、このページは表示されません。)

コマンドラインオプション: `/xenapp` を使用してCitrix Virtual Appsをインストールします。オプションを省略すると、Citrix Virtual Apps and Desktopsがインストールされます。

ステップ3. インストールするものを選択する

コンポーネントインストーラーのコンポーネント選択ページ(/en-us/citrix-virtual-apps-desktops/2503/media/what-to-install-2.png)

初めて使用する場合は、「**Delivery Controller**」を選択します。(後のページで、このマシンにインストールする特定のコンポーネントを選択します。)

Controllerをすでにインストールしている場合（このマシンまたは別のマシンに）で、別のコンポーネントをインストールしたい場合は、「**展開の拡張**」セクションからコンポーネントを選択します。

コマンドラインオプション: `/components`

ステップ4. ライセンス契約を読んで同意する

コンポーネントインストーラーのライセンス契約ページ(/en-us/citrix-virtual-apps-desktops/2503/media/core-license-75.png)

「**ライセンス契約**」ページで、ライセンス契約を読んだ後、読んだことと同意したことを示します。その後、「**次へ**」をクリックします。

ステップ5. インストールするコンポーネントとインストール場所を選択する

コンポーネントインストーラーのコアコンポーネントページ(/en-us/citrix-virtual-apps-desktops/2503/media/core-components-75.png)

「**コアコンポーネント**」ページで:

- **場所:** デフォルトでは、コンポーネントは `C:\Program Files\Citrix` にインストールされます。ほとんどの展開では、デフォルトで問題ありません。別の場所を指定する場合は、ネットワークサービスに対する実行権限が必要です。
- **コンポーネント:** デフォルトでは、すべてのコアコンポーネントのチェックボックスが選択されています。すべてのコアコンポーネントを1台のサーバーにインストールすることは、概念実証、テスト、または小規模な本番環境の展開には問題ありません。大規模な本番環境では、Citrix は Director、StoreFront、Secure Private Access、およびライセンスサーバーを別々のサーバーにインストールすることを推奨します。

> **注:**
>
> 複数のサーバーにコンポーネントをインストールする場合は、他のサーバーに他のコンポーネントをインストールする前に、Citrix License Server とライセンスを最初にインストールしてください。ガイダンスについては、Citrix Virtual Apps and Desktops のライセンスガイド の「自動インストール」セクションを参照してください。

> このマシンに必須のコアコンポーネントをインストールしないことを選択した場合、アイコンで警告が表示されます。その警告は、そのコンポーネントをインストールする必要があることを示していますが、必ずしもこのマシンにインストールする必要があるわけではありません。

Nextをクリックします。

コマンドラインオプション: `/installdir`、`/components`、`/exclude`

ハードウェアチェック

Delivery Controller をインストールまたはアップグレードすると、ハードウェアがチェックされます。マシンに推奨される RAM 容量 (5 GB) より少ない場合、インストーラーは警告を表示します。これはサイトの安定性に影響を与える可能性があります。詳細については、「ハードウェア要件」を参照してください。

グラフィカルインターフェイス: ダイアログボックスが表示されます。

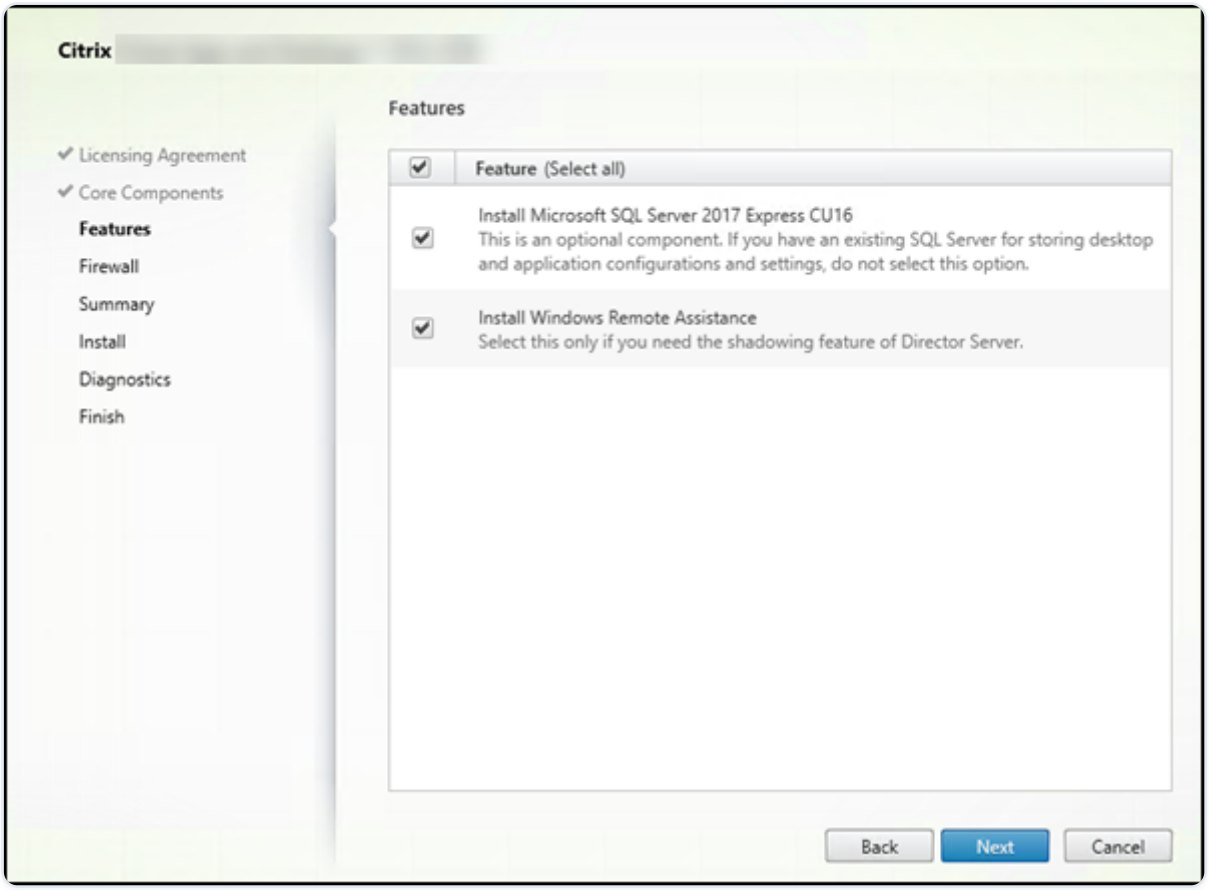
- 推奨: **キャンセル** をクリックしてインストールを停止します。マシンに RAM を追加してから、再度インストールを開始します。
- または、**次へ** をクリックしてインストールを続行します。サイトで安定性の問題が発生する可能性があります。

コマンドラインインターフェイス: インストール/アップグレードが終了します。インストールログには、検出された内容と利用可能なオプションを説明するメッセージが含まれています。

- 推奨: マシンに RAM を追加してから、再度コマンドを実行します。
- または、`/ignore_hw_check_failure` オプションを指定してコマンドを再度実行し、警告を上書きします。サイトで安定性の問題が発生する可能性があります。

アップグレード時には、OS または SQL Server のバージョンがサポートされなくなった場合にも通知されます。詳細については、「展開のアップグレード」を参照してください。

手順 6. 機能の有効化または無効化



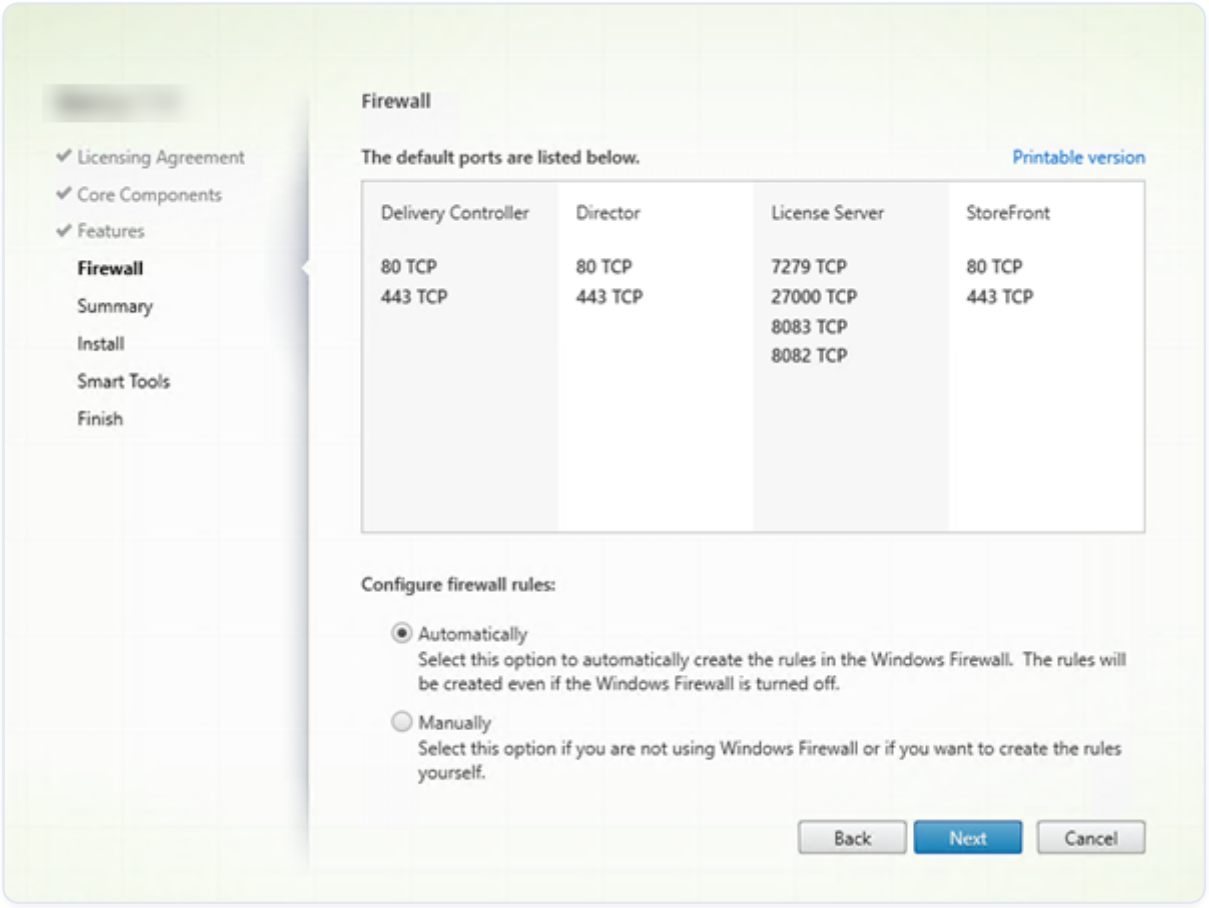
機能ページで、:

- サイトデータベースとして使用するためにMicrosoft SQL Server Expressをインストールするかどうかを選択します。デフォルトでは、この選択は有効になっています。Citrix Virtual Apps and Desktopsデータベースに慣れていない場合は、データベースを確認してください。
- Directorをインストールすると、Windowsリモートアシスタンスが自動的にインストールされます。Directorのユーザーシャドウイングで使用するために、Windowsリモートアシスタンスでシャドウイングを有効にするかどうかを選択します。シャドウイングを有効にすると、TCPポート3389が開きます。デフォルトでは、この機能は有効になっています。ほとんどの展開では、デフォルト設定で問題ありません。この機能は、Directorをインストールしている場合にのみ表示されます。

Nextをクリックします。

コマンドラインオプション: `/nosql` (インストールを防止するため)、`/no_remote_assistance` (有効化を防止するため)

手順7. Windowsファイアウォールポートを開く



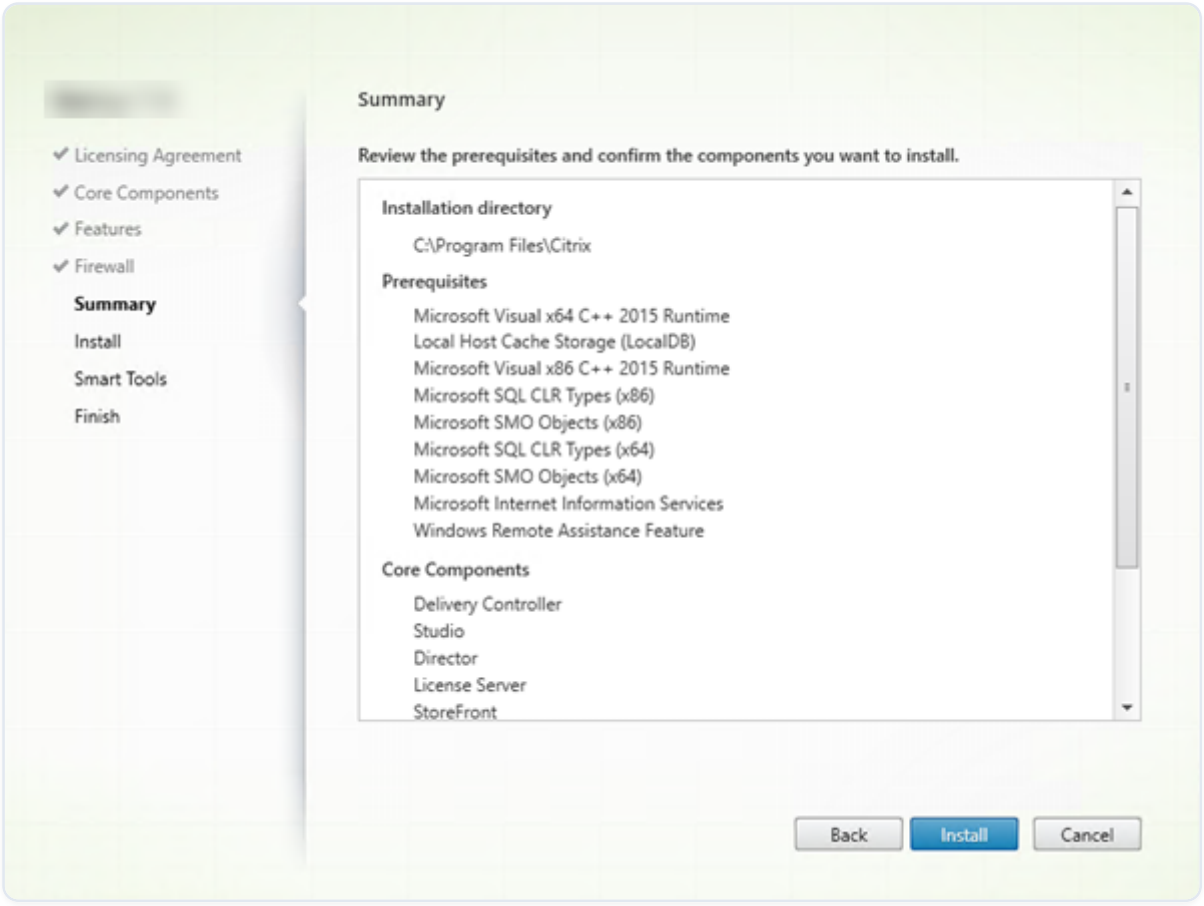
デフォルトでは、Windowsファイアウォールサービスが実行されている場合、ファイアウォールが有効になっていなくても、**ファイアウォール**ページ上のポートは自動的に開かれます。ほとんどの展開では、デフォルト設定で問題ありません。ポート情報については、ネットワークポートを参照してください。

Nextをクリックします。

（このグラフィックは、このマシンにすべてのコアコンポーネントをインストールしたときのポートリストを示しています。この種のインストールは通常、テスト展開のみを対象としています。）」

コマンドラインオプション: `/configure_firewall`

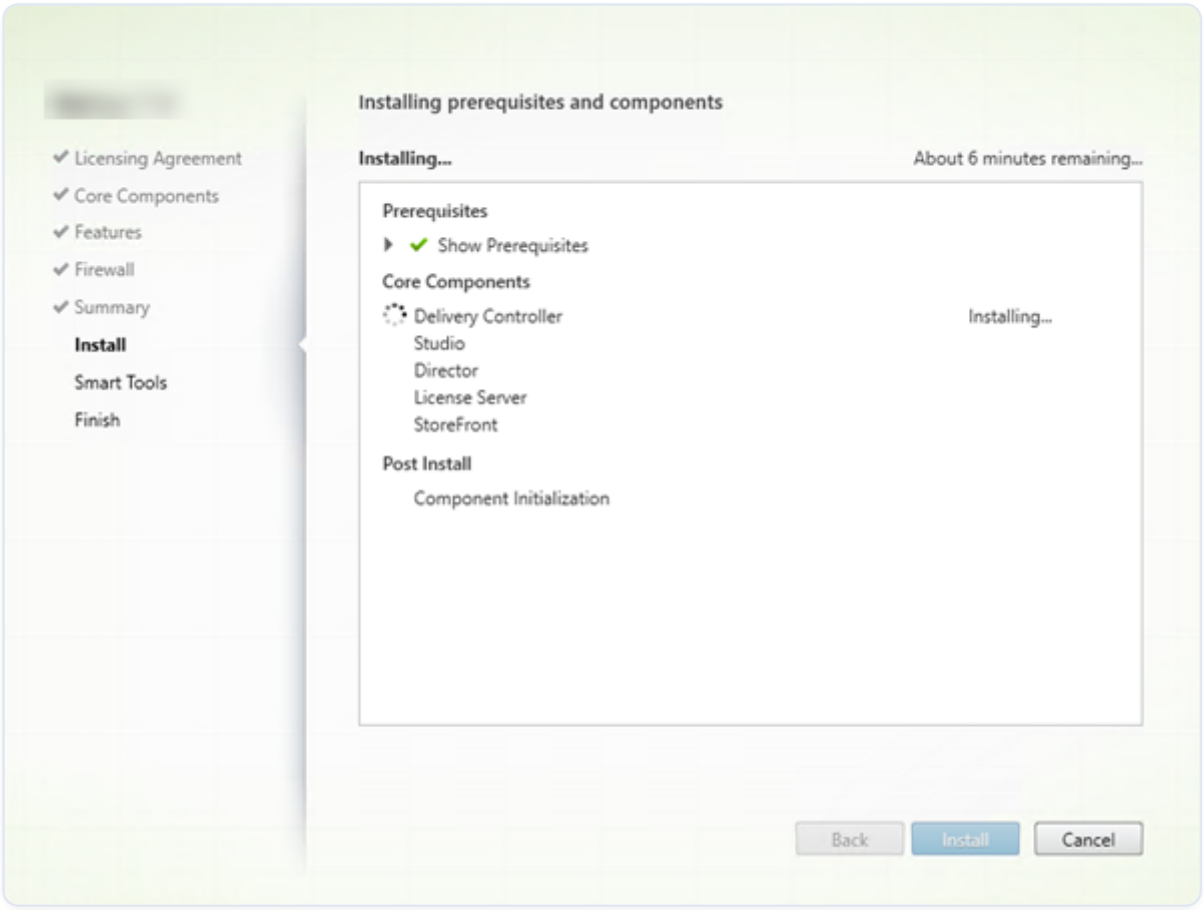
手順8. 前提条件を確認し、インストールを確定する



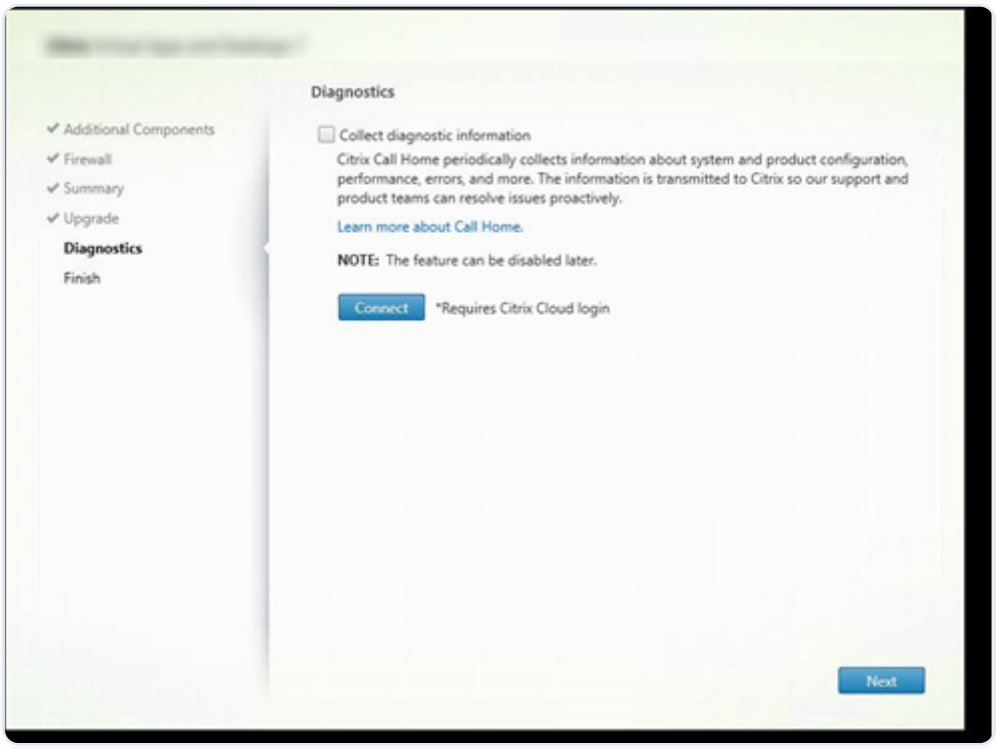
概要ページには、インストールされるものが一覧表示されます。必要に応じて、**戻る**ボタンを使用して以前のウィザードページに戻り、選択を変更します。

準備ができたら、**インストール**をクリックします。

画面にはインストールの進行状況が表示されます。



ステップ9. 診断情報をCloud Software Groupと共有する



診断ページで、Citrix Call Homeに参加するかどうかを選択します。

このページは、グラフィカルインターフェイスを使用してDelivery Controllerをインストールするときに表示されます。StoreFrontをインストールする場合（ただし、Controllerではない場合）、ウィザードはこのページを表示します。その他のコアコンポーネントをインストールする場合（ただし、ControllerまたはStoreFrontではない場合）、ウィザードはこのページを表示しません。

アップグレード中に、Call Homeがすでに有効になっている場合、またはインストーラーがCitrix Telemetry Serviceに関連するエラーを検出した場合は、このページは表示されません。

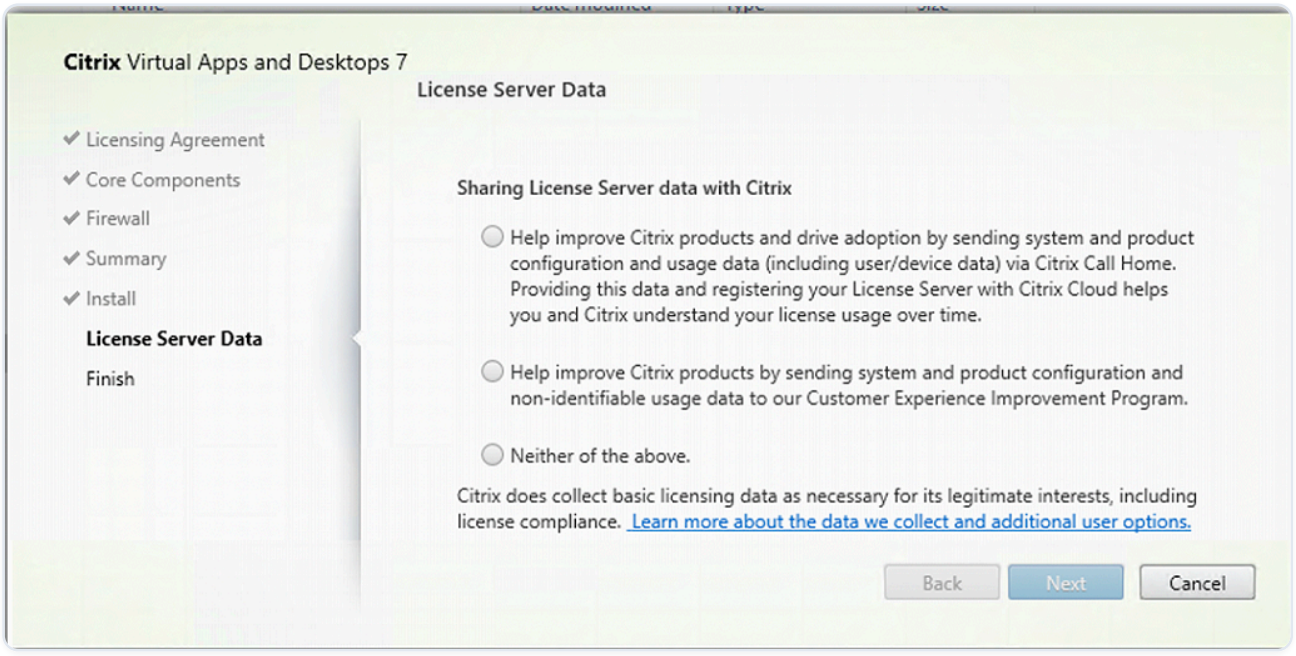
参加することを選択した場合（デフォルト）、**接続**をクリックします。プロンプトが表示されたら、Citrixアカウントの資格情報を入力します。登録の選択は、インストール後に変更できます。

資格情報が検証された後（または参加しないことを選択した場合）、**次へ**をクリックします。

診断ページで、最初に**診断情報の収集**を選択せずに**接続**をクリックすると、**Citrix Insight Servicesへの接続**ダイアログを閉じた後、**次へ**ボタンが無効になります。次のページに進むことはできません。**次へ**ボタンを再度有効にするには、**診断情報の収集**を選択し、すぐに選択を解除します。

詳細については、「Call Home」を参照してください。

ステップ10. ライセンスサーバーデータをCloud Software Groupと共有する



「**ライセンスサーバーデータ**」ページでは、お客様の支援のため、Call Homeデータまたはカスタマーエクスペリエンス向上プログラム（CEIP）データのいずれかを共有していただくようお願い

しています。さらに、Cloud Software Groupは、正当な利益のために、ライセンスコンプライアンスを含む基本的なライセンスデータの収集も必要としています。

「**ライセンスサーバーデータ**」ページは、ライセンスサーバーをインストールしたときに表示されます。

- スタンドアロンとして。
- Delivery Controllerのインストール中に、コアコンポーネントとして。

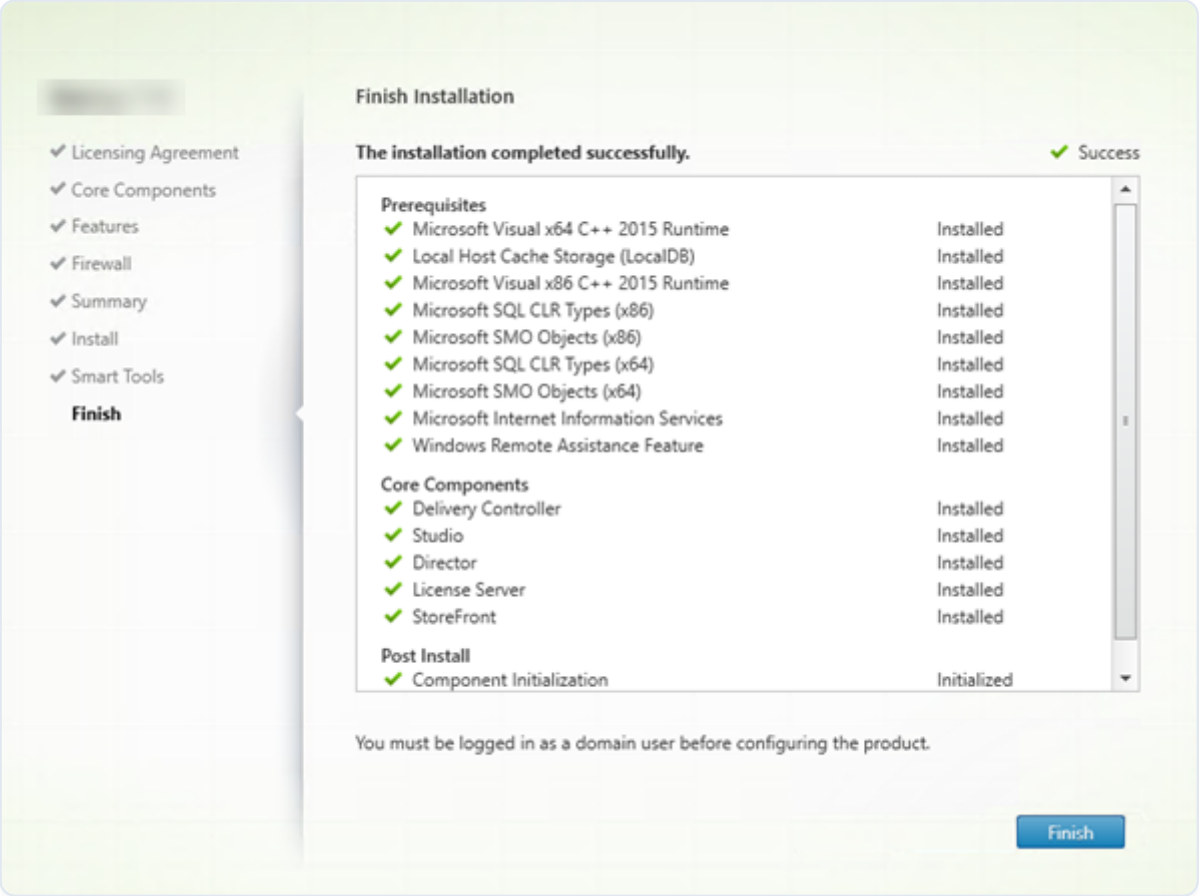
アップグレード中に、構成が`/CITRIX.opt:`ファイルにすでに設定されている場合、このページは表示されません。

ライセンスサーバーは、ライセンスデータ、Call Homeデータ、CEIPデータなど、いくつかの種類のユーザーデータを監視します。Call HomeデータとCEIPデータの収集を有効にするには、参加（オプトイン）を選択する必要があります。

コマンドラインを使用してインストールする際のCall HomeおよびCEIPデータ収集の有効化方法について詳しくは、「コアコンポーネントをインストールするためのコマンドラインオプション」を参照してください。

Cloud Software Groupのライセンスデータ収集について詳しくは、「Citrixライセンスデータ収集プログラム」を参照してください。

手順11. このインストールを完了する



「**完了**」ページには、正常にインストールおよび初期化されたすべての前提条件とコンポーネントに緑色のチェックマークが表示されます。

「**完了**」をクリックします。

手順12. 残りのコアコンポーネントを他のマシンにインストールする

すべてのコアコンポーネントを1台のマシンにインストールした場合は、「次の手順」に進みます。そうでない場合は、他のマシンでインストーラーを実行して他のコンポーネントをインストールします。他のサーバーにControllerを追加でインストールすることもできます。

次の手順

すべての必須コンポーネントをインストールした後、Studio を使用してサイトを作成します(/ja-jp/citrix-virtual-apps-desktops/2503/install-configure/site-create.html)。

サイトを作成した後、VDA をインストールします(/ja-jp/citrix-virtual-apps-desktops/2503/install-configure/install-vdas.html)。

いつでも、フルプロダクトインストーラーを使用して、以下のコンポーネントで展開を拡張できます。

- **Universal Print Server サーバーコンポーネント:** プリンターサーバーでインストーラーを起動します。

  a. **展開の拡張**セクションで**Universal Print Server**を選択します。

  b. ライセンス契約に同意します。

  c. **ファイアウォール**ページでは、Windows ファイアウォールサービスが実行されている場合、ファイアウォールが有効になっていなくても、デフォルトでTCPポート7229と8080がファイアウォールで開かれます。ポートを手動で開きたい場合は、このデフォルトのアクションを無効にできます。

  このコンポーネントをコマンドラインからインストールするには、「Universal Print Server のインストールに関するコマンドラインオプション」を参照してください(/ja-jp/citrix-virtual-apps-desktops/2503/install-configure/install-command.html#command-line-options-for-installing-a-universal-print-server)。
- フェデレーション認証サービス(/ja-jp/federated-authentication-service.html).
- セッションレコーディング(/ja-jp/session-recording.html).
- ワークスペース環境管理(/ja-jp/workspace-environment-management/current-release.html)。

コマンドラインを使用したインストール

> **重要:**
>
> - アップグレード中で、現在のバージョンでPersonal vDiskまたはAppDisksソフトウェアが使用されているかインストールされている場合は、「PvD、AppDisks、およびサポートされていないホストの削除」を参照してください。
> - Citrixは、ライセンスコンプライアンスを含む正当な利益のために、基本的なライセンスデータを収集します。詳細については、「Citrixライセンスデータ」を参照してください。

はじめに

この記事は、Windowsオペレーティングシステムを搭載したマシンへのコンポーネントのインストールに適用されます。Linuxオペレーティングシステム用VDAについては、「Linux Virtual Delivery Agent」を参照してください。

この記事では、製品インストールコマンドの発行方法について説明します。インストールを開始する前に、「インストールの準備」を確認してください。この記事には、利用可能なインストーラーの説明が含まれています。

コマンド実行の進行状況と戻り値を確認するには、元の管理者であるか、**管理者として実行**を使用する必要があります。詳細については、Microsoftのコマンドドキュメントを参照してください。

インストールコマンドを直接使用することに加えて、Active Directory内のマシンにVDAをインストール、アップグレード、または削除するサンプルスクリプトが製品ISOに用意されています。詳細については、「スクリプトを使用したVDAのインストール」を参照してください。

このCitrix Virtual Apps and Desktopsのバージョンでサポートされていないバージョンにインストールまたはアップグレードしようとすると、オプションに関する情報を示すメッセージが表示されます。「以前のオペレーティングシステム」を参照してください。

Citrixがコンポーネントインストールの結果を報告する方法については、「Citrixインストールのリターンコード」を参照してください。

フル製品インストーラーを使用する

フル製品インストーラーのコマンドラインインターフェイスにアクセスするには：

1. Citrixから製品パッケージをダウンロードします。ダウンロードサイトにアクセスするには、Citrixアカウントの資格情報が必要です。
2. ファイルを解凍します。必要に応じて、ISOファイルをDVDに書き込みます。
3. コンポーネントをインストールするサーバーに、ローカル管理者アカウントを使用してログオンします。
4. DVDをドライブに挿入するか、ISOファイルをマウントします。
5. メディア上の `\x64\XenDesktop Setup` ディレクトリから、適切なコマンドを実行します。

   コアコンポーネントをインストールするには： Command-line options for installing core componentsに記載されているオプションを使用して、`XenDesktopServerSetup.exe` を実行します。

   VDAをインストールするには： Command-line options for installing a VDAに記載されているオプションを使用して、`XenDesktopVDASetup.exe` を実行します。

   StoreFrontをインストールするには: インストールメディアの `x64 > StoreFront` フォルダーで `CitrixStoreFront-x64.exe` を実行します。

Universal Print Serverをインストールするには： Command-line options for installing a Universal Print Serverのガイダンスに従ってください。

Federated Authentication Serviceをインストールするには： Citrixでは、グラフィカルインターフェイスの使用を推奨しています。

Session Recordingをインストールするには: Session Recording のガイダンスに従ってください。

Workspace Environment Managementをインストールするには： Workspace Environment Managementのガイダンスに従ってください。

Secure Private Accessをインストールするには： インストールメディアの`x64 > XenDesktop` Setupフォルダーで`XenDesktopSPASetup.exe`を実行します。Command-line options for installing a Secure Private Accessのガイダンスに従ってください。

コアコンポーネントのインストール用コマンドラインオプション

`XenDesktopServerSetup.exe`コマンドでコアコンポーネントをインストールする場合、以下のパラメーターオプションが有効です。オプションの詳細については、Install core componentsを参照してください。

> **注:**
>
> - コアコンポーネントをインストールするためのコマンドラインオプションを使用している間は、`/exclude`を使用しないでください。
> - `/components` を使用して1つのコンポーネントをアップグレードすると、他のコンポーネントもアップグレードされる場合があります。これは、異なるコンポーネント間の潜在的な互換性の問題を回避するためです。
> - 1つのコンポーネントのみをアップグレードする場合は、そのコンポーネントの個別のインストーラーを使用してください。展開のアップグレード を参照してください。

- **/ceipoptin** *CEIPオプトイン ...*

  Call Homeデータおよびカスタマーエクスペリエンス向上プログラム（CEIP）データの収集を有効にします。有効な値は次のとおりです。

  - `DIAGNOSTIC`: Citrix LicensingがCall Homeデータを収集できるようにするには、この値を選択します。

- `ANONYMOUS`: Citrix Licensingが未識別のCEIPデータ（ユーザーを特定しないデータ）を収集できるようにするには、この値を選択します。
- `NONE`: Citrix LicensingによるCEIPデータの収集を無効にするには、この値を選択します。

Call Homeデータ収集の詳細については、Citrix Licensing Call Home を参照してください。

CEIPデータ収集の詳細については、Citrix Licensing Customer Experience Improvement Program を参照してください。

CEIPデータの詳細については、Citrix Licensing CEIP data elements を参照してください。

License Serverのライセンスデータの詳細については、Citrix Licensing Data を参照してください。

- **/components** *コンポーネント* ...

  インストールまたは削除するコンポーネントのコンマ区切りリスト。有効な値は次のとおりです。

  - `CONTROLLER`: コントローラー
  - `DESKTOPSTUDIO`: スタジオ
  - `WEBSTUDIO`: Web Studio (ウェブスタジオ)
  - `DESKTOPDIRECTOR`: Director (ディレクター)
  - `LICENSESERVER`: Citrix License Server (Citrixライセンスサーバー)
  - `SECUREPRIVATEACCESS`: Secure Private Access (セキュアプライベートアクセス)
  - `VDA`: Virtual Delivery Agent (仮想デリバリーエージェント)
  - `CSA`: Citrix Secure Access™ クライアント
  - `DT`: Citix Device Trust (Citixデバイス トラスト)
  - `PLUGINS`: Windows用 Citrix Workspace™ アプリ
  - `UBERAGENT`: Citrix ウーバーエージェント
  - `UPL`: Citrix ユーザーパーソナライゼーションレイヤー
  - `WEM`：Citrix Workspace Environment マネジメント™ エージェント

  VDAとWindows用Citrix Workspaceアプリをインストールするには、/components vda,plugins を指定するか、またはコンポーネントをまったく指定しないでください。コンポーネントが指定されていない場合、VDA、Citix Device Trust、Citrix uberAgent、およびCitrix Workspace

Environment Management Agentがデフォルトでインストールされます。(環境内の既存のuberAgentがスタンドアロンであり、Citrixによって展開されていない場合、Citrix uberAgentはインストール、アップグレード、またはアンインストールされません。)

VDAのみをインストールし、他のCitrixコンポーネントのインストールを除外するには、/components vda を指定します。

このオプションは、VDAWorkstationCoreSetup_xxxx.exe インストーラーを使用する場合は無効です。そのインストーラーは、Citrix Workspaceアプリやその他のCitrixコンポーネントをインストールできません。

このオプションを省略すると、すべてのコンポーネントがインストールされます（`/remove` オプションも指定されている場合は削除されます）。

(2003年より前のリリースでは、有効な値には`STOREFRONT`が含まれていました。バージョン2003以降では、フル製品インストーラーの使用に記載されている専用のStoreFrontインストールコマンドを使用してください)。

- **前提条件のみ**

  選択したコンポーネントの前提条件のみがインストールされます。Citrix製品コンポーネントはインストールされません。

- **/configure_firewall**

  Windowsファイアウォールサービスが実行されている場合、ファイアウォールが有効になっていなくても、インストールされるコンポーネントで使用されるすべてのポートをWindowsファイアウォールで開きます。サードパーティのファイアウォールを使用している場合、またはファイアウォールを使用していない場合は、手動でポートを開く必要があります。

- **エクスペリエンスメトリックを無効にする**

  インストール、アップグレード、または削除中に収集された分析データがCitrixに自動的にアップロードされるのを防ぎます。

- **/プレチェックオンリー**

  インストールまたはアップグレードを開始することなく、すべての事前チェックを実行し、事前チェック結果を生成します。

- **/help** または **/h**

  コマンドのヘルプを表示します。

- **/ignore_hw_check_failure**

ハードウェアチェックが失敗した場合（たとえば、RAM不足のため）、Delivery Controllerのインストールまたはアップグレードを続行できるようにします。詳細については、ハードウェアチェックを参照してください。

- **/ignore_site_test_failure**

  Controllerのアップグレード中にのみ有効です。通常、サイトテストの失敗は無視され、アップグレードが続行されます。省略された場合（またはfalseに設定された場合）、サイトテストの失敗はインストーラーの失敗を引き起こし、アップグレードは実行されません。デフォルト = false

  アップグレード中に、サポートされていないSQL Serverバージョンが検出された場合、このオプションは無視されます。詳細については、SQL Server version check を参照してください。

- **/インストールディレクトリ *ディレクトリ***

  コンポーネントがインストールされる既存の空のディレクトリ。デフォルト = `c:\Program Files\Citrix`。

- **/ログパス *パス***

  ログファイルの場所。指定されたフォルダーは存在している必要があります。インストーラーは作成しません。デフォルト = `TEMP%\Citrix\XenDesktop Installer`

- **/no_remote_assistance**

  Director のインストール時にのみ有効です。Windows リモートアシスタンスを使用するユーザーシャドウイング機能を無効にします。

- **/再起動なし**

  インストール後の再起動を防止します。（ほとんどのコアコンポーネントでは、再起動はデフォルトで有効になっていません。）

- **/再開なし**

  デフォルトでは、インストール中にマシンの再起動が必要な場合、再起動が完了するとインストーラーは自動的に再開します。デフォルトを上書きするには、`/noresume`を指定します。これは、メディアを再マウントする必要がある場合や、自動インストール中に情報を取得したい場合に役立ちます。

- **/SQLなし**

  Controller をインストールするサーバーへの Microsoft SQL Server Express のインストールを防止します。このオプションを省略すると、サイトデータベースとして使用するために SQL Server Express がインストールされます。

このオプションは、ローカルホストキャッシュに使用される SQL Server Express LocalDB のインストールには影響しません。

- **サイレント** または **パッシブ**

  インストール中にユーザーインターフェイスは表示されません。インストールプロセスの唯一の証拠は、Windowsタスクマネージャーにあります。このオプションを省略すると、グラフィカルインターフェイスが起動します。

- **削除**

  `/components`オプションで指定されたコアコンポーネントを削除します。

- **すべて削除**

  インストールされているすべてのコアコンポーネントを削除します。

- **/SKIPHDXDRIVERCHECK**

  VDA Meta-installer への HDX™ ドライバーのチェックをスキップします。

- **エクスペリエンスメトリクスを送信**

  インストール、アップグレード、または削除中に収集された分析データをCitrixに自動的に送信します。このオプションを省略した場合（または`/disableexperiencemetrics`が指定されている場合）、分析データはローカルで収集されますが、自動的には送信されません。

- **一時ディレクトリ** *ディレクトリ*

  インストール中に一時ファイルを保持するディレクトリ。デフォルト = `c:\Windows\Temp`。

- **XenApp**

  Citrix Virtual Appsをインストールします。このオプションを省略すると、Citrix Virtual Apps and Desktops™がインストールされます。

- **事前チェックのみ**

  インストールまたはアップグレードを開始することなく、すべての事前チェックを実行し、事前チェック結果を生成します。

コアコンポーネントのインストール例

次のコマンドは、サーバーにDelivery Controller™、Studio、Citrix Licensing、およびSQL Server Expressをインストールします。コンポーネント通信に必要なファイアウォールポートは自動的に開かれます。

`\x64\XenDesktop Setup\XenDesktopServerSetup.exe /components controller,desktopstudio,licenseserver /configure_firewall`

次のコマンドは、サーバーにCitrix Virtual Apps™ Controller、Studio、およびSQL Server Expressをインストールします。コンポーネント通信に必要なファイアウォールポートは自動的に開かれます。

`\x64\XenDesktop Setup\\XenDesktopServerSetup.exe /xenapp /components controller,desktopstudio /configure_firewall`

次のコマンドは、サーバーにDelivery Controller、Secure Private Access、およびSQL Server Expressをインストールします。コンポーネント通信に必要なファイアウォールポートは自動的に開かれます。

`\x64\XenDesktop Setup XenDesktopServerSetup.exe /xenapp /components controller,secureprivateaccess /configure_firewall`

Citrix Virtual Apps and Desktopsバージョン2407から2411以降にアップグレードする場合、またはバージョン2411以降の新規インストールを実行する場合は、最初のステップとしてLicense Serverを最新バージョン（バージョン11.2.17ビルド51000）に更新してください。その後、Delivery Controllerをアップグレードします。これを怠ると、コマンドラインによるインストールとアップグレードが失敗します。License Serverと、Delivery Controller、Web Studio、Citrix Directorなどのコンポーネントをアップグレードするには、次のコマンドを実行します（マウントされたISOの\x64フォルダー内にいることを前提とします）。

1. 次を実行します。

   ```
   \x64\Licensing\CitrixLicensing.exe /quiet
   ```

   ライセンスバイナリをローカルドライブのいずれかにコピーした場合は、次のコマンドを実行します。

   ```
   \x64\Licensing\CitrixLicensing.exe /quiet /l install.log
   ```

2. 次を実行します。

   ```
   \x64\XenDesktop Setup\XenDesktopServerSetup.exe  /components
   "CONTROLLER,DESKTOPSTUDIO,DESKTOPDIRECTOR" /CONFIGURE_FIREWALL
   ```

スタンドアロンVDAインストーラーを使用する

ダウンロードサイトにアクセスするには、Citrixアカウントの資格情報が必要です。インストールを開始する前に、管理者特権を昇格させるか、**管理者として実行**を使用する必要があります。

1. Citrixから適切なパッケージをダウンロードします。
   - マルチセッションOS Virtual Delivery Agent: `VDAServerSetup_xxxx.exe`
   - シングルセッションOS Virtual Delivery Agent: `VDAWorkstationSetup_xxxx.exe`
   - シングルセッションOS コアサービス Virtual Delivery Agent: `VDAWorkstationCoreSetup_xxxx.exe`
2. まずパッケージから既存のディレクトリにファイルを抽出し、その後インストールコマンドを実行するか、または単にパッケージを実行します。

   ファイルをインストールする前に抽出するには、絶対パスを指定して`/extract`を使用します（例: `C:\YourExtractFolder\VDAWorkstationCoreSetup.exe /extract %temp%\CitrixVDAInstallMedia`）。ディレクトリは存在している必要があります。そうでない場合、抽出は失敗します。その後、別のコマンドで、この記事に記載されている有効なオプションを使用して、適切なコマンドを実行します。

   - `VDAServerSetup_XXXX.exe` の場合は、`<extract folder>\Extract\Image-Full\x64\XenDesktop Setup\XenDesktopVDASetup.exe` を実行します
   - `VDAWorkstationCoreSetup_XXXX.exe` の場合は、`<extract folder>\Extract\Image-Full\x64\XenDesktop Setup\XenDesktopRemotePCSetup.exe` を実行します
   - `VDAWorkstationSetup_XXXX.exe` の場合は、`<extract folder>\Extract\Image-Full\x64\XenDesktop Setup\XenDesktopVDASetup.exe` を実行します

   ダウンロードしたパッケージを実行するには、その名前（`VDAServerSetup.exe`、`VDAWorkstationSetup.exe`、または`VDAWorkstationCoreSetup.exe`）を実行します。この記事に記載されている有効なオプションを使用してください。

フル製品インストーラーに慣れている場合：

- スタンドアロンの`VDAServerSetup.exe`または`VDAWorkstationSetup.exe`インストーラーを、その名前を除いて、`XenDesktopVdaSetup.exe`コマンドであるかのように実行します。
- `VDAWorkstationCoreSetup.exe`インストーラーは異なります。これは、他のインストーラーで利用可能なオプションのサブセットをサポートしているためです。

VDAのインストール用コマンドラインオプション

次のオプションは、以下の1つ以上のコマンド（インストーラー）で有効です: `VDAServerSetup_xxxx.exe`、`VDAWorkstationSetup_xxxx.exe`、および `VDAWorkstationCoreSetup_xxxx.exe`。

オプションの詳細については、VDAのインストールを参照してください。

- **/components** *コンポーネント*\[,*コンポーネント*\]

  インストールまたは削除するコンポーネントのコンマ区切りリスト。有効な値は次のとおりです。

  - `VDA`: 仮想デリバリーエージェント
  - `PLUGINS`: Windows向けCitrix Workspaceアプリ

  VDA と Citrix Workspace app for Windows をインストールするには、`/components vda,plugins` を指定するか、コンポーネントをまったく指定しないでください。コンポーネントが指定されていない場合、デフォルトでは VDA のみがインストールされます。

  VDA のみをインストールし、Citrix Workspace app のインストールを除外するには、`/components vda` を指定します。

  このオプションは、`VDAWorkstationCoreSetup_xxxx.exe` インストーラーを使用している場合は無効です。そのインストーラーでは Citrix Workspace app をインストールできません。

- **前提条件のみ**

  選択したコンポーネントの前提条件のみがインストールされます。Citrix 製品コンポーネントはインストールされません。

- **/controllers** "*コントローラー*\[*コントローラー*\]"

  VDA が通信できるコントローラーのスペース区切りの FQDN を、引用符で囲んで指定します。`/site_guid` オプションと `/controllers` オプションの両方を指定しないでください。

- **エクスペリエンスメトリクスを無効にする**

  インストール、アップグレード、または削除中に収集された分析データが Citrix に自動的にアップロードされるのを防ぎます。

- **/enable_hdx_ports**

Windows ファイアウォールサービスが検出された場合、ファイアウォールが有効になっていなくても、VDA および有効な機能 (Windows リモートアシスタンスを除く) で必要となる Windows ファイアウォールのポートを開きます。別のファイアウォールを使用している場合、またはファイアウォールを使用していない場合は、ファイアウォールを手動で構成する必要があります。ポート情報については、「ネットワークポート」を参照してください。

HDX アダプティブトランスポートが使用する UDP ポートを開くには、この `/enable_hdx_ports` オプションに加えて、`/enable_hdx_udp_ports` オプションを指定します。

- **/enable_hdx_udp_ports**

  Windows ファイアウォールサービスが検出された場合、ファイアウォールが有効になっていなくても、HDX アダプティブトランスポートが使用する Windows ファイアウォールの UDP ポートを開きます。別のファイアウォールを使用している場合、またはファイアウォールを使用していない場合は、ファイアウォールを手動で構成する必要があります。ポート情報については、「ネットワークポート」を参照してください。

  VDAが使用する追加ポートを開くには、この`/enable_hdx_udp_ports`オプションに加えて、`/enable_hdx_ports`オプションを指定します。

- **/enable_hdx_tls_dtls**

  HDX Direct V1用にTCPおよびUDPポート443を開きます。

- **/enable_real_time_transport**

  オーディオパケットに UDP を使用するかどうかを有効または無効にします（オーディオのリアルタイムオーディオトランスポート）。この機能を有効にすると、オーディオパフォーマンスが向上する可能性があります。Windows ファイアウォールサービスが検出されたときに UDP ポートを自動的に開く場合は、`/enable_hdx_ports` オプションを含めます。

- **/enable_remote_assistance**

  Director で使用するために、Windows リモートアシスタンスのシャドウ機能が有効になります。このオプションを指定すると、Windows リモートアシスタンスはファイアウォールで動的ポートを開きます。

- **/enablerestore** または **/enablerestorecleanup**

  （シングルセッションVDAにのみ有効）VDAのインストールまたはアップグレードが失敗した場合に、復元ポイントへの自動復帰を有効にします。

  インストール/アップグレードが正常に完了した場合：

  - `/enablerestorecleanup`は、インストーラーに復元ポイントを削除するよう指示します。
  - `/enablerestore`は、使用されなかった場合でも、インストーラーに復元ポイントを保持するように指示します。

詳細については、インストールまたはアップグレードの失敗時の復元を参照してください。

- **/ENABLE_SECURE_DEFAULTS**

  より安全な初期設定のために、さまざまな機能のデフォルト設定を有効から無効に変更します。関連する機能は次のとおりです: クライアントドライブリダイレクト、特殊フォルダーリダイレクト、ドラッグアンドドロップ、クライアントTWAINデバイスリダイレクト、クライアントUSBプラグアンドプレイデバイスリダイレクト、クライアントプリンターリダイレクト、クライアントクリップボードリダイレクト、クライアントマイクデバイスリダイレクト。

- **/enable_ss_ports**

  Windows ファイアウォールサービスが検出された場合、ファイアウォールが有効になっていなくても、画面共有に必要なポートをWindows ファイアウォールで開きます。別のファイアウォールを使用している場合、またはファイアウォールを使用していない場合は、ファイアウォールを手動で構成する必要があります。

- **/除外** "*コンポーネント*"\[,"*コンポーネント*"\]

  コンマで区切られた1つ以上のオプションコンポーネントのインストールを防止します。各コンポーネントは二重引用符で囲む必要があります。たとえば、MCSで管理されていないイメージにVDAをインストールまたはアップグレードする場合、Machine Identity Serviceコンポーネントは不要です。有効な値は次のとおりです。

マルチセッションOS	シングルセッションOS	シングルセッションOSコアサービス
`Citrix Authentication Identity Assertion VDA Plug-in`	`Citrix Authentication Identity Assertion VDA Plug-in`	`Citrix Authentication Identity Assertion VDA Plug-in`
`Citrix Backup and Restore`	`Citrix Backup and Restore`	`Citrix Browser Content Redirection`
`Citrix deviceTRUST`	`Citrix deviceTRUST`	`Citrix deviceTRUST`
`uberAgent`	`uberAgent`	`uberAgent`

マルチセッションOS	シングルセッションOS	シングルセッションOSコアサービス
Citrix Secure Access Client	Citrix Secure Access Client	Citrix Secure Access Client
Citrix Workspace Environment Management Agent	Citrix Workspace Environment Management Agent	Citrix Workspace Environment Management Agent
Citrix Browser Content Redirection	Citrix Browser Content Redirection	Citrix Personalization for App-V - VDA
Citrix MCS IODriver	Citrix MCS IODriver	Citrix Telemetry Service
Citrix Personalization for App-V - VDA	Citrix Personalization for App-V - VDA	Citrix Universal Print Client
Citrix Profile Management	Citrix Profile Management	Citrix Vda Log Capture Service
Citrix Profile Management WMI Plug-in	Citrix Profile Management WMI Plug-in	CSE Component
Citrix Rendezvous V2	Citrix Rendezvous V2	Director VDA Plug-in
Citrix Telemetry Service	Citrix Telemetry Service	Machine Management Provider
Citrix Universal Print Client	Citrix Universal Print Client	VDA Monitor Plug-in
Citrix Vda Log Capture Service	Citrix Vda Log Capture Service	VDA WMI Proxy Plug-in
Citrix VDA Upgrade Agent	Citrix VDA Upgrade Agent	
CSE Component	CSE Component	
Director VDA Plug-in	Director VDA Plug-in	

マルチセッションOS	シングルセッションOS	シングルセッションOSコアサービス
`Machine Identity Service`	`Machine Identity Service`	
`Machine Management Provider`	`Machine Management Provider`	
`VDA Monitor Plug-in`	`User Personalization Layer`	
`VDA WMI Proxy Plug-in`	`VDA Monitor Plug-in`	
	`VDA WMI Proxy Plug-in`	
`Citrix App Protection Component`	`Citrix App Protection Component`	`Citrix App Protection Component`
`Citrix HyperV Filter Driver`	`Citrix HyperV Filter Driver`	
`Citrix Personalization for App-V - VDA`	`Citrix Personalization for App-V - VDA`	`Citrix Personalization for App-V - VDA`

Citrix Profile Managementをインストールから除外すると（`/exclude "Citrix Profile Management"`）、Citrix DirectorによるVDAの監視とトラブルシューティングに影響します。**ユーザー詳細**ページと**エンドポイント**ページでは、パーソナライゼーションパネルとログオン期間パネルが機能しません。**ダッシュボード**ページと**トレンド**ページでは、平均ログオン期間パネルは、Profile Managementがインストールされているマシンのみのデータを表示します。

サードパーティのユーザープロファイル管理ソリューションを使用している場合でも、Citrix Profile Management Serviceをインストールして実行することをお勧めします。Citrix Profile Management Serviceを有効にする必要はありません。

同じコンポーネント名で`/exclude`と`/includeadditional`の両方を指定した場合、そのコンポーネントはインストールされません。

このオプションは、`VDAWorkstationCoreSetup.exe`インストーラーを使用している場合は無効です。このインストーラーは、これらの項目の多くを自動的に除外します。

- **/h** または **/help**

コマンドのヘルプを表示します。

- **/includeadditional** "*コンポーネント*"\[,"*コンポーネント*"\]

  1つまたは複数のコンマ区切りのオプションコンポーネント（それぞれを引用符で囲む）のインストールを含めます。このオプションは、Remote PC Access展開を作成していて、デフォルトで含まれていない他のコンポーネントをインストールしたい場合に役立ちます。有効な値は次のとおりです。

マルチセッションOS	シングルセッションOS
`Citrix Backup and Restore`	`Citrix Backup and Restore`
`Citrix MCS IODriver`	`Citrix MCS IODriver`
`Citrix Personalization for App-V - VDA`	`Citrix Personalization for App-V - VDA`
`Citrix Profile Management`	`Citrix Profile Management`
`Citrix Profile Management WMI Plug-in`	`Citrix Profile Management WMI Plug-in`
`Citrix Rendezvous V2`	`Citrix Rendezvous V2`
`Citrix VDA Upgrade Agent`	`Citrix VDA Upgrade Agent`
`Citrix Web Socket Vda Registration Tool`	`Citrix Web Socket Vda Registration Tool`
`Machine Identity Service`	`Machine Identity Service`
	`User Personalization Layer`

  `/exclude` と `/includeadditional` の両方を同じコンポーネント名で指定した場合、そのコンポーネントはインストールされません。

- **/installdir** *ディレクトリ*

  コンポーネントがインストールされる既存の空のディレクトリ。デフォルト = `c:\Program Files\Citrix`。

- **/install_mcsio_driver**

使用しないでください。代わりに `/includeadditional "Citrix MCS IODriver"` または `/exclude "Citrix MCS IODriver"` を使用してください。

- **/logpath** *パス*

  ログファイルの場所。指定されたフォルダーは存在している必要があります。インストーラーは作成しません。デフォルト = 「`%TEMP%\Citrix\XenDesktop Installer`」

  このオプションはグラフィカルインターフェイスでは利用できません。

- **/マスターイメージ**

  VM に VDA をインストールする場合にのみ有効です。VDA を他のマシンを作成するために使用するイメージとして設定します。このオプションは `/mastermcsimage` と同等です。

  このオプションは `VDAWorkstationCoreSetup_xxxx.exe` インストーラーを使用する場合は無効です。

- **/マスターMCSイメージ**

  このマシンが Machine Creation Services でイメージとして使用されることを指定します。このオプションは `/masterimage` と同等です。

- **/マスターPVSイメージ**

  このマシンが、Citrix Provisioning™ またはサードパーティのプロビジョニングツール (Microsoft System Center Configuration Manager など) を使用してVMをプロビジョニングするためのイメージとして使用されることを指定します。

- **/websockettoken** *WebSocket トークン*

  Web Socket VDAを作成します。WebSocketTokenは、必要なトークン用です。

- **/websockettokenfile** *WebSock トークンを含むファイル*

  Web Socket VDAを作成します。*FileContainingWebSockToken* は、必要なトークンを含むファイル用です。

- **ウェブソケットトークン標準入力** *<ウェブソケットトークン>*

  Web Socket VDAを作成します。*<WebSocketToken* は、STDINによって渡される必要なトークン用です。

- **/no_mediafoundation_ack**

  Microsoft Media Foundationがインストールされていないことを確認し、いくつかのHDXマルチメディア機能がインストールされず、動作しないことを承認します。このオプションが省略

され、Media Foundationがインストールされていない場合、前提条件が満たされていないため、VDAのインストールは終了します。ほとんどのサポートされているWindowsエディションには、Nエディションを除いて、Media Foundationがすでにインストールされています。Windows機能 > メディア機能 を *手動* で 有効にした場合、Citrix Meta Installerが探すレジストリキーに値が設定されていない可能性があります。インストールプロセスを開始する前に、`SOFTWARE\Microsoft\Windows\CurrentVersion\Setup\Windows-Features\WindowsMediaVersion` レジストリキーを確認して、値が存在し、空でないことを確認してください。

- **デスクトップエクスペリエンスなし**

  拡張デスクトップエクスペリエンス機能は利用できなくなりました。このオプション（およびポリシー設定）は、指定されても無視されます。

  マルチセッションOS用VDAをインストールする場合にのみ有効です。拡張デスクトップエクスペリエンス機能の有効化を防止します。この機能は、拡張デスクトップエクスペリエンスCitrixポリシー設定でも制御されます。

- **再起動しない**

  インストール後の再起動を防止します。VDAは再起動するまで使用できません。

- **再開しない**

  デフォルトでは、インストール中にマシンの再起動が必要な場合、再起動が完了するとインストーラーは自動的に再開します。デフォルトを上書きするには、`/noresume` を指定します。これは、メディアを再マウントする必要がある場合や、自動インストール中に情報を取得したい場合に役立ちます。

- **物理マシン**

  RemotePCインストールでは、`/remotepc` とともにこの引数を使用してください。そうしないと、特定のユーザーシナリオでVDAが期待どおりに動作しない可能性があります。

- ***/*ポート番号** *ポート*

  `/reconfig` オプションが指定されている場合にのみ有効です。VDAとController間の通信を有効にするポート番号。以前に構成されたポートは、ポート80でない限り無効になります。

- ***/*プロキシ構成** “*アドレスまたはPACファイルパス*”

  環境内でGateway Serviceなどのサービスとともに Rendezvous V2プロトコルを使用する予定があり、アウトバウンド接続用にネットワークに非透過プロキシがある場合は、ここでプロキシを指定します。HTTPプロキシのみがサポートされています。Rendezvousプロトコルで使用するプロキシのアドレスまたはPACファイルパス。このコマンドラインは、/includeadditional

"Citrix Rendezvous V2" が使用されたかのように、Citrix Rendezvous V2を自動的にインストールします。機能の詳細については、「Rendezvous プロトコル」を参照してください。

  - プロキシアドレス形式: `http://<url-or-ip>:<port>`
  - PACファイル形式: `http://<url-or-ip>:<port>/<path>/<filename>.pac`

- **サイレント** または **パッシブ**

  インストール中にユーザーインターフェイスは表示されません。インストールおよび構成プロセスの唯一の証拠は、Windowsタスクマネージャーにあります。このオプションを省略すると、グラフィカルインターフェイスが起動します。

- **/再構成**

  `/portnumber`、`/controllers`、または `/enable_hdx_ports` オプションと組み合わせて使用すると、以前に構成されたVDA設定をカスタマイズします。`/quiet` オプションを指定せずにこのオプションを指定すると、VDAをカスタマイズするためのグラフィカルインターフェイスが起動します。

- **/リモートPC**

  Remote PC Access展開（シングルセッションOS）またはブローカー接続（マルチセッションOS）の場合にのみ有効です。追加コンポーネントのインストールは除外されます（`/exclude` および `/includeadditional` オプションのコンポーネントリストを参照）。

  このオプションは、`VDAWorkstationCoreSetup.exe` インストーラーを使用する場合は無効です。そのインストーラーは、これらのコンポーネントのインストールを自動的に除外します。

  `/remotepc` は `/servervdi` オプションと互換性がありません。

- **/削除**

  `/components` オプションで指定されたコンポーネントを削除します。

- **/remove_appdisk_ack**

  インストールされている場合、AppDisks™ VDA プラグインをアンインストールすることを VDA インストーラーに許可します。

- **/remove_pvd_ack**

  インストールされている場合、Personal vDisk をアンインストールすることを VDA インストーラーに許可します。

- **/すべて削除**

VDAを削除します。Citrix Workspaceアプリ（インストールされている場合）は削除しません。

- **/REMOVEALLWITHCWA**

  VDA とともに CWA を削除します。

- **/エクスペリエンスメトリックを送信**

  インストール、アップグレード、または削除中に収集された分析データをCitrixに自動的に送信します。このオプションが省略された場合（または`/disableexperiencemetrics`オプションが指定された場合）、分析データはローカルで収集されますが、自動的には送信されません。

- **サーバーVDI**

  サポートされているWindowsマルチセッションマシンにシングルセッションOS用VDAをインストールします。Windowsマルチセッションマシンにマルチセッション OS用VDAをインストールする場合は、このオプションを省略してください。

  このオプションを使用する前に、サーバーVDIを参照してください。

  このオプションは、フルプロダクトVDAインストーラーでのみ使用してください。

- **/site_guid** *GUID*

  サイトのActive Directory組織単位（OU）のグローバル一意識別子。これは、検出にActive Directoryを使用している場合に、仮想デスクトップをサイトに関連付けます（自動更新が推奨されるデフォルトの検出方法です）。サイトGUIDは、Studioに表示されるサイトプロパティです。`/site_guid`と`/controllers`の両方のオプションを指定しないでください。

- **/tempdir** *ディレクトリ*

  インストール中に一時ファイルを保持するディレクトリ。デフォルト = c:\\Windows\\Temp。

  このオプションは、グラフィカルインターフェイスでは使用できません。

- **/仮想マシン**

  VMにVDAをインストールする場合にのみ有効です。インストーラーによる物理マシンの検出を上書きします。VMに渡されるBIOS情報により、VMが物理マシンとして表示される場合があります。

  このオプションは、グラフィカルインターフェイスでは使用できません。

- **/XenDesktopクラウド**

VDAがCitrix DaaS (Citrix Cloud™) 展開にインストールされていることを示します。

VDAのインストール例

フルプロダクトインストーラーを使用したVDAのインストール：

以下のコマンドは、シングルセッションOS用VDAとCitrix Workspaceアプリを VMのデフォルトの場所にインストールします。このVDAはイメージとして使用され、MCSを使用してVMをプロビジョニングします。VDAは、`mydomain` ドメイン内の `Contr-Main` という名前のサーバー上のControllerに最初に登録されます。VDAはユーザーパーソナライゼーションレイヤーとWindowsリモートアシスタンスを使用します。

```
\x64\XenDesktop Setup\XenDesktopVdaSetup.exe /quiet /components vda,plugins /
controllers "Contr-Main.mydomain.local" /enable_hdx_ports /includeadditional
"user personalization layer" /mastermcsimage /enable_remote_assistance
```

VDAWorkstationCoreSetupスタンドアロンインストーラーを使用してシングルセッションOS VDAをインストールする:

以下のコマンドは、リモートPCアクセスまたはVDI展開で使用するために、シングルセッションOSにコアサービスVDAをインストールします。Citrix Workspaceアプリおよびその他の非コアサービスはインストールされません。Controllerのアドレスが指定され、Windowsファイアウォールサービス内のポートは自動的に開かれます。管理者が再起動を処理します。

```
VDAWorkstationCoreSetup .exe /quiet /controllers "Contr-East.domain.com" /
enable_hdx_ports /noreboot
```

VDAをカスタマイズする

VDAをインストールした後、いくつかの設定をカスタマイズできます。製品メディアの `\x64\XenDesktop Setup` ディレクトリから、VDAのインストール用コマンドラインオプションで説明されている以下のオプションを1つ以上使用して、`XenDesktopVdaSetup.exe` を実行します。

- `/reconfigure` (VDAのカスタマイズ時に必須)
- `/h` または `/help`
- `/quiet`
- `/noreboot`
- `/controllers`
- `/portnumber port`

- `/enable_hdx_ports`

VDAのトラブルシューティング

- デリバリーグループのStudio表示で、**詳細**ペインの**インストール済みVDAバージョン**エントリが、マシンにインストールされているバージョンと異なる場合があります。マシンのWindowsのプログラムと機能の表示には、実際のVDAバージョンが表示されます。
- VDAがインストールされた後、Delivery Controllerに登録されるまで、ユーザーにアプリやデスクトップを配信することはできません。

  VDA登録方法と登録の問題のトラブルシューティングについて学ぶには、VDA登録を参照してください。

Universal Print Serverをインストールするためのコマンドラインオプション

次のオプションは、`XenDesktopPrintServerSetup.exe`コマンドで有効です。

- **/enable_upsserver_port**

このオプションが指定されていない場合、インストーラーはグラフィカルインターフェイスから**ファイアウォール**ページを表示します。インストーラーにWindowsファイアウォールルールを自動的に追加させるには**自動**を選択し、管理者がファイアウォールを手動で構成できるようにするには**手動**を選択します。

印刷サーバーにソフトウェアをインストールした後、(/ja-jp/citrix-virtual-apps-desktops/2503/printing/printing-provision-printers.html)のガイダンスを使用してUniversal Print Serverを構成します。

Secure Private Accessをインストールするためのコマンドラインオプション

以下のオプションは、両方で有効です。

1. CVADインストーラー: `XenDesktopSPASetup.exe`
2. SPAオンプレミスインストーラー: `SecurePrivateAccessSetup_XXXX.exe`

- **/enable_spa_ports**

  Windowsファイアウォールサービスが検出された場合、ファイアウォールが有効になっていなくても、Secure Private Accessに必要なWindowsファイアウォールのポートを開きます。別のファイアウォールを使用している場合、またはファイアウォールを使用していない場合は、ファイアウォールを手動で構成する必要があります。ポート情報については、「ネットワークポート」を参照してください。

- **SQLを使用しない**

  Secure Private Accessをインストールするサーバーへの Microsoft SQL Server Expressのインストールを防止します。このオプションを省略すると、サイトデータベースとして使用するためにSQL Server Expressがインストールされます。

- **/help または /h または /?**

  コマンドヘルプを表示します。

- **再起動なし**

  インストール後の再起動を防止します。Secure Private Accessは再起動するまで使用できません。

- **/quiet または /passive**

  インストール中にユーザーインターフェイスは表示されません。インストールと構成プロセスの唯一の証拠は、Windowsタスクマネージャーにあります。このオプションを省略すると、グラフィカルインターフェイスが起動します。

- **削除**

  Secure Private Accessを削除します。

オプションの詳細については、Secure Private Accessインストーラーを参照してください。

詳細情報

コンポーネントインストールの結果をCitrixがどのように報告するかについては、「Citrixインストールリターンコード」を参照してください。

Web Studioのインストール

はじめに

Citrix Studioは、Citrix Virtual Apps and Desktopsの展開を構成および管理できるWindowsベースの管理コンソールです。Web Studioは、Citrix Studioの次世代版であり、Citrix Studioと完全に同等の機能を備えたWebベースの管理コンソールです。(/ja-jp/citrix-daas/overview#studio)と同じルックアンドフィールで、Web Studioはネイティブの Webエクスペリエンスを提供することで、管理エクスペリエンスを最新化します。

Web Studioは、Internet Information Service (IIS) がインストールされている任意のWindowsサーバーに展開できます。展開オプションは2つあります。

- 専用サーバーにインストールする:

パフォーマンスとスケーラビリティが重要となる大規模な環境では、Web Studioを専用サーバーにインストールすることをお勧めします。このサーバーは、オプションでDirectorもホストできます。

- Delivery Controller™と統合する:

  迅速な展開やシンプルな環境では、Web StudioをDelivery Controllerに直接インストールします。このアプローチは、管理オーバーヘッドを最小限に抑えることが優先される小規模な展開に最適です。

次の図は、Web Studioのアーキテクチャを示しています。

Web Studioのアーキテクチャ(/en-us/citrix-virtual-apps-desktops/2503/media/web-studio-architecture.png)

Web Studioを稼働させるための一般的なワークフローは次のとおりです。

1. Web Studioをインストールする(#install-web-studio-1)。
2. TLSの証明書を構成する(#configure-a-certificate-for-tls)。
3. サイトをセットアップする(#set-up-a-site)。
4. 管理のためにDelivery ControllerをWeb Studioに追加する(#add-delivery-controllers-to-web-studio-for-management)。
5. (オプション) Web StudioをDelivery Controllerのプロキシとして構成する
6. (オプション) Pendoを無効にする。
7. Web Studioにサインインする。

負荷分散されたWeb Studio展開をセットアップするには、この記事を参照してください。

Web Studioで利用可能な新機能

新機能の記事を参照してください。

システム要件

サポートされているオペレーティングシステム:

- Windows Server 2025、StandardおよびDatacenter Edition、Server Coreオプション付き
- Windows Server 2022、StandardおよびDatacenter Edition、Server Coreオプション付き
- Windows Server 2019、StandardおよびDatacenter Edition、Server Coreオプション付き
- Windows Server 2016、StandardおよびDatacenter Edition、Server Coreオプション付き

サポートされているブラウザ:

- マイクロソフト エッジ 92
- Firefox ESR (延長サポート版) 90
- グーグル クローム 92
- サファリ 14

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

前提条件

このWeb Studioリリースは、Citrix Virtual Apps and Desktops™ 2212以降の展開と互換性があります。

2212より前の展開の場合、まず2212にアップグレードしてからWeb Studioをインストールします。

既知の制限事項

Web StudioとCitrix Studioを相互に利用する場合、次の制限事項を考慮してください。Web Studioで作成されたテンプレートはCitrix Studioには表示されず、その逆も同様です。これは、Web Studioがテンプレートの保存にCitrix Studioとは異なるデータベースを使用するためです。回避策として、Web Studioでテンプレートからポリシーを作成し、次にCitrix Studioでこのポリシーからテンプレートを作成します。その逆も同様です。

- Web Studioのインストールを成功させるには、Internet Information Services (IIS) マネージャーでデフォルトのサイト名 (**Default Web Site**) を変更しないでください。デフォルトのサイト名を変更すると、インストールが失敗します。

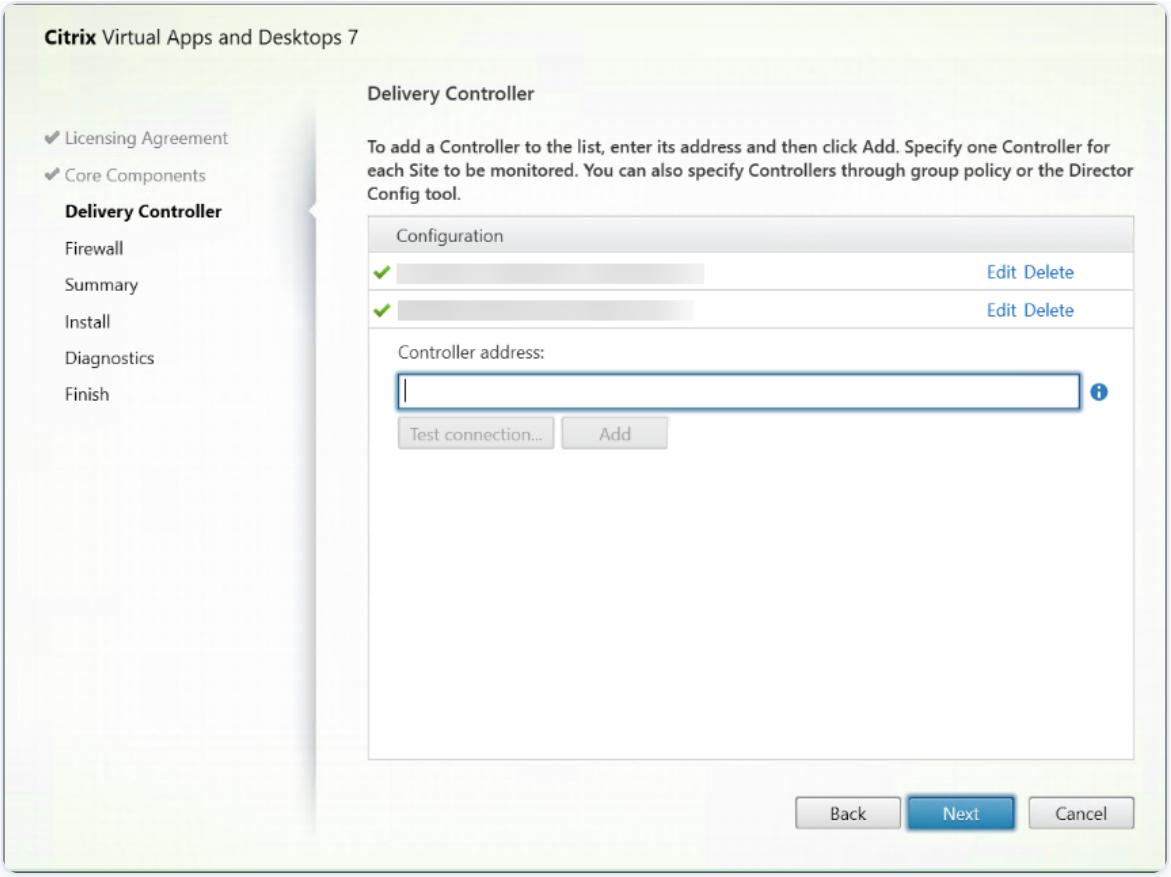
Web Studioのインストール

以下の情報は、コアコンポーネントのインストールのガイダンスを補足するものです。Web Studioをインストールするには：

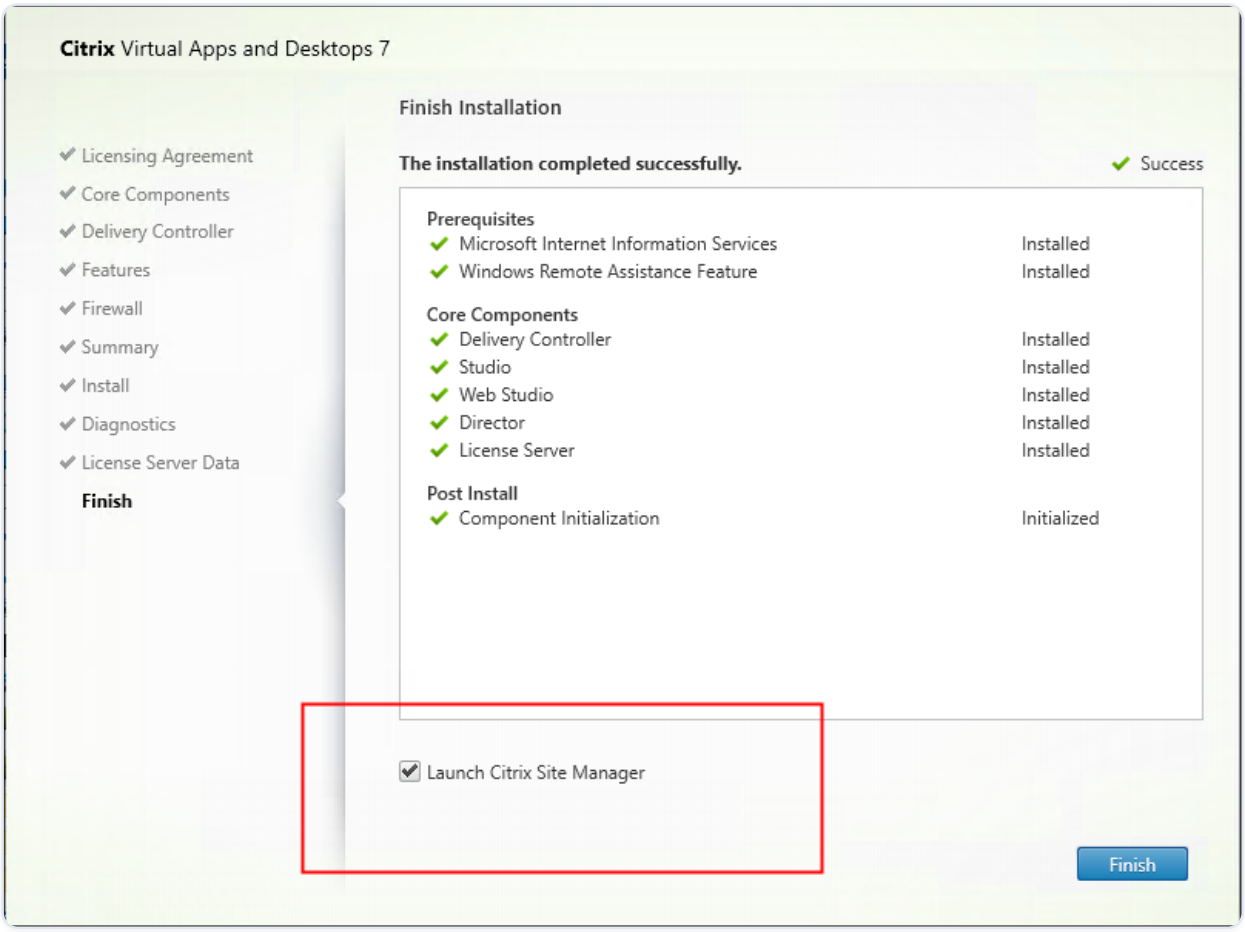
- Citrix Virtual Apps and Desktopsのフル製品ISOインストーラーを使用してWeb Studioをインストールします。ISOインストーラーは前提条件をチェックし、不足しているコンポーネントをインストールし、Web Studioウェブサイトをセットアップし（Delivery Controllerのインストールに含まれている場合はDelivery Controller上に）、基本的な構成を実行します。
- インストール時にWeb Studioが含まれていなかった場合は、インストーラーを使用してWeb Studioを追加します。
- Web Studioのインストール時に、Delivery ControllerのFQDNを入力するよう求められます。

注:

- 複数のDelivery Controllerを追加できます。Web Studioはランダムな順序でそれらに接続を試みます。Web Studioが接続しようとしているDelivery Controllerに到達できない場合、Web Studioは自動的に他のDelivery Controllerにフォールバックします。
- **Core Components**でDirectorが選択され、インストールされている場合、ここに追加するDelivery ControllerはWeb StudioとDirectorの両方に使用されます。
- デリバリーコントローラーがTLS用に構成されている（推奨）場合、入力されたFQDNは、デリバリーコントローラーにインストールされている証明書のコモンネームまたはサブジェクトの別名と一致する必要があります。



- **Finish**ページでは、**Launch Site Manager**チェックボックスがデフォルトで選択されているため、Citrix Site Managerが自動的に開きます。後で起動するには、デスクトップのスタートメニューを開き、**Citrix > Citrix Site Manager**を選択します。Web Studioを起動する前に、Citrix Site Managerを使用してサイトを作成するか、既存のサイトに参加する必要があります。詳しくは、「サイトのセットアップ」を参照してください。



注:

コマンドラインを使用してWeb Studioをインストールすることもできます。例：`.\XenDesktopServerSetup.exe /components webstudio /controllers "ddc1.studio.local" /configure_firewall /quiet`。詳しくは、「コマンドラインを使用したインストール」を参照してください。

TLS 用の証明書を構成する

デフォルトでは、IISがHTTPS用にまだ構成されていない場合、インストーラーはサーバーのFQDNを証明書のコモンネームとして使用して自己署名証明書を作成し、それをポート443にバインドします。この動作により、ユーザーはローカルマシンからWeb Studioにアクセスできますが、他のマシンから接続するユーザーには、証明書が信頼されていないためセキュリティ警告が表示されます。この証明書を、エンタープライズまたはパブリック認証局（CA）によって署名された証明書に置き換えることをお勧めします。詳しくは、「Web StudioおよびDirectorでTLSを有効にする」を参照してください。IISでTLS証明書がすでに構成されている場合、インストーラーは何も変更しません。

> **注:**
>
> Web Studio展開のセキュリティ保護について詳しくは、「Web Studio展開のセキュリティ保護」を参照してください。

サイトをセットアップする

Citrix Virtual Apps and Desktops 展開（サイトとも呼ばれます）をセットアップするには、Citrix Site Manager ツールを使用します。このツールは、Delivery Controller とともに自動的にインストールされます。

サイトをセットアップするには、次の手順に従います。

1. デリバリーコントローラーで、デスクトップのスタートメニューを開き、**Citrix > Citrix Site Manager**を選択します。
2. Citrix Site Managerで、**サイトの作成**を選択します。サイトセットアップウィザードが表示されます。
3. サイトを作成し、その設定を次のように構成します。
   - **はじめに**ページで、サイトの名前を入力します。
   - **データベース**ページには、サイト、監視、および構成ログデータベースを設定するための選択肢が含まれています。詳細については、手順3. データベースを参照してください。
   - **ライセンス**ページで、ライセンスサーバーのアドレスを指定し、次に使用する（インストールする）ライセンスを示します。詳細については、手順4. ライセンスを参照してください。
4. **概要**ページで、すべての設定を確認し、**送信**をクリックします。

   このコントローラーのIPアドレスは、自動的にサイトに追加されます。

   > **注:**
   >
   > サイトを作成したユーザーは、そのサイトのフル管理者になります。詳細については、委任管理を参照してください。

サイトの作成後に新しいコントローラーをインストールする場合、そのコントローラーをサイトに追加する必要があります。詳細な手順は次のとおりです。

1. この新しいコントローラーでCitrix Site Managerを実行します。
2. **既存のサイトに参加**を選択します。
3. 既にサイトに追加されているコントローラーのアドレスを入力します。
4. **送信**をクリックします。

管理のためにDelivery ControllerをWeb Studioに追加する

Studio構成ツールを使用して、管理のためにDelivery ControllerをWeb Studioに追加します。このツールはWeb Studioのインストールフォルダーにあります。

デフォルトでは、このツールは次のデフォルトフォルダーにインストールされます。

- `C:\Program Files\Citrix\Web Studio\Tool\StudioConfig.exe`

Web Studioで管理したいサイトに対して、次の2つのDelivery Controller (`ddc1.studio.local` と `ddc2.studio.local`) を構成するとします。次のPowerShellコマンドを実行します。

- `.\StudioConfig.exe --server "ddc1.studio.local,ddc2.studio.local"`

注:

- このツールには、コンピューターの管理者権限が必要です。
- IISサーバーのキャッシュ設定により、Delivery Controllerの構成変更がすぐに反映されない場合があります。すぐに反映させるには、Web Studioサーバーに移動し、インターネットインフォメーションサービス (IIS) マネージャーを開き、*Server_name* **> Sites > Default Web Site**に移動して、Webサイトの管理ペインで**Restart**を選択します。
- 新しいFQDNでDelivery Controllerを再展開する場合は、`StudioConfig.exe`を使用してWeb Studioで、および`C:\Program Files\Citrix\Web Studio\Site\assets\json\manifest.json`ファイルでFQDNを更新します。`manifest.json`ファイルを更新しないと、古いFQDNがWeb Studioのサインインウィンドウに表示されたままになります。その結果、サインイン時に新しいFQDNを代替として入力する必要があります。
- サポートされているすべてのパラメーターを表示するには、`StudioConfig.exe --help`を実行します。

(オプション) Web StudioをDelivery Controllerのプロキシとして構成する

デフォルトでは、Web Studioコンソールを使用して展開を管理する場合、Webブラウザーを介してWeb StudioサーバーとDelivery Controllerの両方に接続します。Web StudioサーバーをDelivery Controllerのプロキシとして構成するオプションを提供しています。その結果、展開を管理する際にはWeb Studioサーバーにのみ接続します。

このセクションでは、Web StudioサーバーをDelivery Controllerのプロキシとして構成する方法を説明します。Web StudioとDelivery Controllerは異なるサーバーにインストールされていることを前提としています。

開始する前に、展開に必要なすべてのコアコンポーネントがインストールされていることを確認してください。詳細については、「コアコンポーネントのインストール」を参照してください。

Web Studio のプロキシモードを有効にするには、次の手順に従います。

1. Web Studio サーバーで、Windows PowerShell を管理者として実行します。
2. `fqdn_of_webstudio_machine` を Web Studio サーバーの FQDN に置き換えて、次のコマンドを実行します。

   ```
   & "c:\Program Files\Citrix\Web Studio\Tool\StudioConfig.exe" --enableproxy --proxyserver "fqdn_of_webstudio_machine"
   ```

   > **注:**
   >
   > ロードバランスされた Web Studio 展開がある場合は、`fqdn_of_webstudio_machine` をロードバランサーサーバー (仮想サーバーとも呼ばれます) の FQDN に置き換えます。詳細については、「ロードバランスされた Web Studio 展開のセットアップ」を参照してください。

Web Studio のプロキシモードを無効にするには、この PowerShell コマンドを実行します。

```
& "c:\Program Files\Citrix\Web Studio\Tool\StudioConfig.exe" --disableproxy
```

(オプション) Pendo を有効または無効にする

バージョン 2411 以降、Web Studio は Pendo を統合しており、これはデフォルトで有効になっています。Pendo は、Citrix プライバシーポリシー に従って使用状況データを収集します。また、Web Studio の右下隅にアイコンを追加し、コンテキストに応じた機能情報とフィードバックオプ

ションを提供します。使用状況データを共有したくない場合は、Studio 構成ツールを使用して Pendo を無効にできます。

このツールは Web Studio のインストールフォルダーにあります。デフォルトでは、ツールは次のフォルダーにインストールされます: `C:\Program Files\Citrix\Web Studio\Tool\StudioConfig.exe`。

Pendo を無効にするには、次の手順に従います。

1. Web Studio にサインインします。右下隅にアイコンが表示されている場合、Pendo は有効になっています。
2. Web Studio サーバーで、Windows PowerShell を管理者として実行します。 この PowerShell コマンドを実行します。

```
& "c:\Program Files\Citrix\Web Studio\Tool\StudioConfig.exe" --
disablependo
```

Pendo を有効にするには、このコマンドを実行します。

```
& "c:\Program Files\Citrix\Web Studio\Tool\StudioConfig.exe" --enablependo
```

Web Studio にサインインする

1. デフォルトのポート番号443が使用されている場合、`https://<address of the server hosting Web Studio>/Citrix/Studio`でWeb Studioにアクセスします。別のポートが構成されている場合は(/ja-jp/citrix-virtual-apps-desktops/2503/secure/tls-studio#optional-change-the-default-port-number)、`https://<address of the server hosting Web Studio>:<port number>/Citrix/Studio`を使用します。

   Web StudioにDelivery Controllerを追加しており(#add-delivery-controllers-to-web-studio-for-management)、それらに到達可能な場合、サインインページが表示されます。

   > **注:**
   >
   > 以下の場合は、**サインインできません**ページが表示されます。

- サイトにDelivery Controllerが指定されていません。接続するには、Delivery Controllerを追加するよう求められます。
- 指定されたDelivery Controllerに到達できません。接続を確認するには、**［テスト］をクリックします。または、別のDelivery Controllerを入力して**［接続］**をクリックします。

2. **ユーザー名、パスワード、ドメイン**を入力します。
3. **［サインイン］**をクリックします。

次の手順

1. VDAのインストール
2. Web Studioを使用して、次の方法で仮想アプリとデスクトップをユーザーに配信します。
   a. マシンカタログを作成する(/ja-jp/citrix-virtual-apps-desktops/2503/install-configure/machine-catalogs-create.html)
   b. デリバリーグループを作成する(/ja-jp/citrix-virtual-apps-desktops/2503/install-configure/delivery-groups-create.html)
   c. アプリケーショングループを作成する（オプション）(/ja-jp/citrix-virtual-apps-desktops/2503/install-configure/application-groups-create.html)

VDAのインストール

重要:

- アップグレード中で、現在のバージョンにPersonal vDiskまたはAppDisksソフトウェアがインストールされている場合は、PvD、AppDisks、およびサポートされていないホストの削除を参照してください。
- Citrix®によって配布されるバイナリは署名されています。署名されたバイナリは、Citrixが生成した証明書または信頼できるサードパーティの証明書によって検証されていることを示します。

> Windowsマシン用のVDAには、マルチセッションOS用VDAとシングルセッションOS用VDAの2種類があります。(Linuxマシン用VDAについては、Linux Virtual Delivery Agentのドキュメントを参照してください。)

インストールを開始する前に、インストールの準備を確認し、すべての準備タスクを完了してください。

VDAをインストールする前に、コアコンポーネントをインストールします。VDAをインストールする前にサイトを作成することもできます。

この記事では、VDAをインストールする際のインストールウィザードのシーケンスについて説明します。コマンドラインの同等機能が提供されています。詳細については、コマンドラインを使用したインストールを参照してください。

ステップ1. 製品ソフトウェアをダウンロードしてウィザードを起動する

フル製品インストーラーを使用している場合:

1. 製品ISOをまだダウンロードしていない場合:
   - Citrixアカウントの資格情報を使用して、Citrix Virtual Apps and Desktops™のダウンロードページにアクセスします。製品ISOファイルをダウンロードします。
   - ファイルを解凍します。必要に応じて、ISOファイルをDVDに書き込みます。
2. VDAをインストールするイメージまたはマシンで、ローカル管理者アカウントを使用します。DVDをドライブに挿入するか、ISOファイルをマウントします。インストーラーが自動的に起動しない場合は、マウントされたドライブ上の**AutoSelect**アプリケーションをダブルクリックします。

   インストールウィザードが起動します。

スタンドアロンパッケージを使用している場合:

1. Citrixアカウントの資格情報を使用して、Citrix Virtual Apps and Desktopsのダウンロードページにアクセスします。適切なパッケージをダウンロードします。
   - `VDAServerSetup_2308.exe`: マルチセッションOS VDA *バージョン*
   - `VDAWorkstationSetup_2308.exe`: シングルセッションOS VDA *バージョン*
   - `VDAWorkstationCoreSetup_2308.exe`: シングルセッションOSコアサービスVDA *バージョン*
2. パッケージを右クリックし、**管理者として実行**を選択します。

インストールウィザードが起動します。

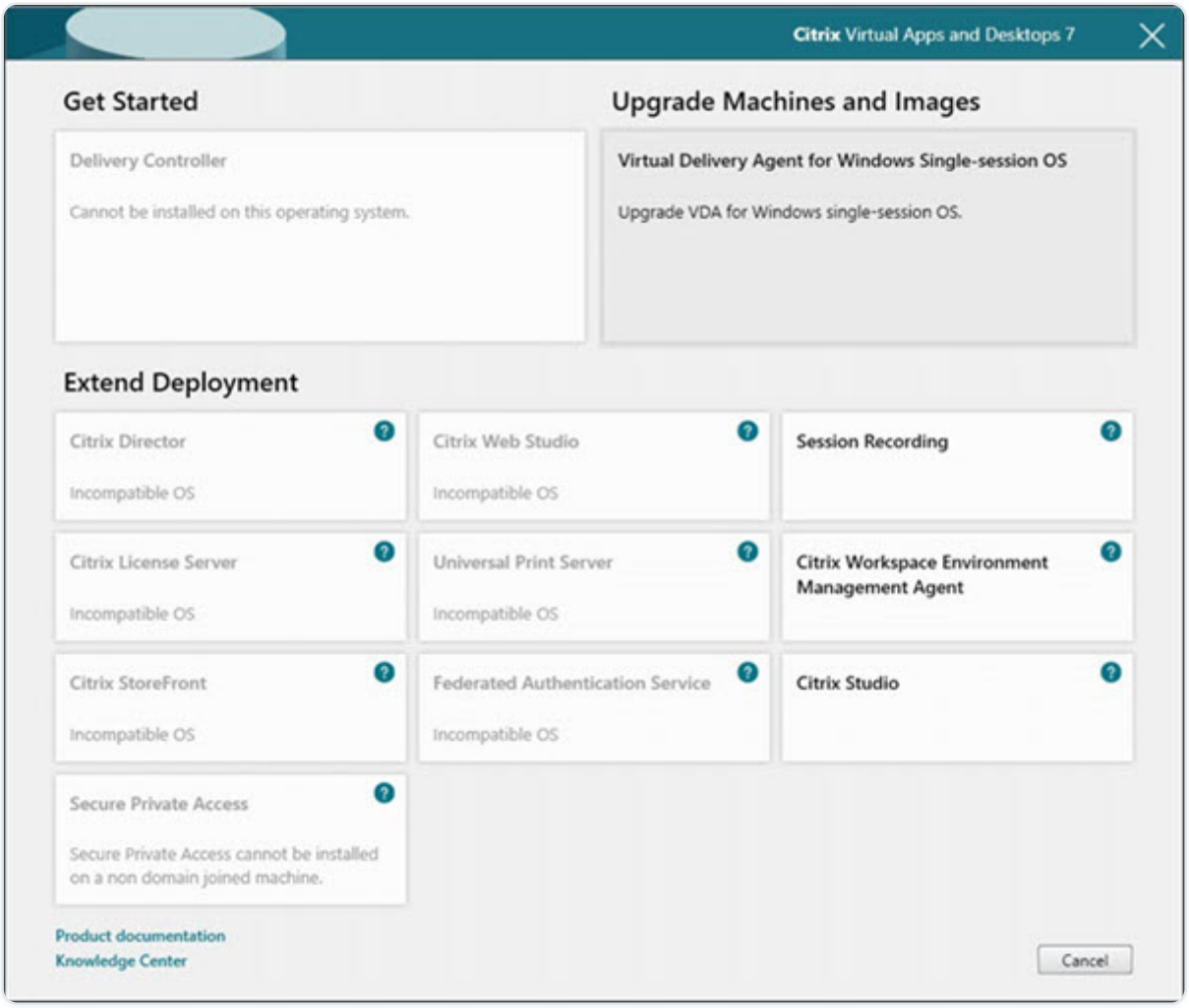
ステップ2. インストールする製品を選択する



インストールする製品（Citrix Virtual AppsまたはCitrix Virtual Desktops）の横にある**開始**をクリックします。（マシンにCitrix Virtual AppsまたはCitrix Virtual Desktopsコンポーネントがすでにインストールされている場合、このページは表示されません。）

コマンドラインオプション: Citrix Virtual Appsをインストールするための`/xenapp`。このオプションが省略された場合、Citrix Virtual Desktopsがインストールされます。

ステップ3. VDAを選択する



Virtual Delivery Agentエントリを選択します。インストーラーは、シングルセッションOSまたはマルチセッションOSのどちらで実行されているかを認識するため、適切なVDAタイプのみを提供します。

例えば、Windows Server 2019マシンでインストーラーを実行すると、マルチセッションOS用VDAオプションが利用可能です。シングルセッションOS用VDAオプションは提供されません。

このCitrix Virtual Apps and Desktopsバージョンでサポートされていないオスに Windows VDAをインストール（またはアップグレード）しようとすると、オプションに関する情報を示すメッセージが表示されます。

ステップ4. VDAの使用方法を指定する

VDAインストーラーの環境ページ(/en-us/citrix-virtual-apps-desktops/2503/media/vda-ss-environment.png)

ページで、VDAの使用方法を指定します。このマシンをイメージとして使用して、さらに多くのマシンをプロビジョニングするかどうかを示します。

選択したオプションは、どのCitrix Provisioning™ツールが自動的にインストールされるか（もしあれば）、およびVDAインストーラーのページのデフォルト値に影響します。

VDAをインストールすると、複数のMSI（プロビジョニング用およびその他）が自動的にインストールされます。これらのインストールを防止する唯一の方法は、コマンドラインインストールで`/exclude`オプションを使用することです。

次のいずれかを選択してください。

- **マスターMCSイメージを作成する:** Machine Creation Services™を使用してVMをプロビジョニングする予定がある場合は、このオプションを選択してVMイメージにVDAをインストールします。このオプションは、Machine Identity Serviceをインストールします。これがデフォルトのオプションです。

  コマンドラインオプション: `/mastermcsimage` または `/masterimage`

> **重要:**
>
> インストールメディアまたはISOイメージはローカルにマウントする必要があります。ソフトウェアのインストール目的でネットワークドライブからISOイメージをマウントすることはサポートされていません。

- **Citrix Provisioningまたはサードパーティのプロビジョニングツールを使用してマスターイメージを作成する:** Citrix Provisioningまたはサードパーティのプロビジョニングツール（Microsoft System Center Configuration Managerなど）を使用してVMをプロビジョニングする予定がある場合は、このオプションを選択してVMイメージにVDAをインストールします。

  コマンドラインオプション: `/masterpvsimage`

- （マルチセッションOSマシンでのみ表示）**サーバーへの仲介接続を有効にする:** 他のマシンをプロビジョニングするためのイメージとして使用されない物理マシンまたは仮想マシンにVDAをインストールするには、このオプションを選択します。

  コマンドラインオプション: `/remotepc`

- (シングルセッションOSマシンにのみ表示されます) **Remote PC Accessを有効にする:** 物理マシンにVDAをインストールしてRemote PC Accessで使用するには、このオプションを選択します。

  コマンドラインオプション: `/remotepc`

Nextをクリックします。

このページは表示されません:

- VDAをアップグレードする場合
- `VDAWorkstationCoreSetup_2308.exe`、`VDAServerSetup_2308.exe`、または`VDAWorkstationSetup_2308.exe`インストーラーを使用している場合

ステップ5. VDAをインストールする場所を選択します

VDAインストーラーのコンポーネントページ(/en-us/citrix-virtual-apps-desktops/2503/media/vda-ss-components.png)

> **注:**
>
> 「オプションソフトウェア」ページが新設されました。CWAとCSAは、コンポーネントページから新しい「オプションソフトウェア」ページに移動しました。

コンポーネントページで:

- **場所:** デフォルトでは、VDAは`C:\Program Files\Citrix`にインストールされます。このデフォルトはほとんどの展開で問題ありません。別の場所を指定する場合、その場所にはネットワークサービスに対して`execute`権限が必要です。

Nextをクリックします。

ステップ6. 追加コンポーネントをインストールします

VDAインストーラーの追加コンポーネントページ(/en-us/citrix-virtual-apps-desktops/2503/media/vda-ss-addtnl-components.png)

> **注:**
>
> “Citrix Personalization for App-V - VDA” は “App Packages Delivery Component” に名称変更されました。

追加コンポーネントページには、VDA とともに他の機能やテクノロジーのインストールを有効または無効にするためのチェックボックスが含まれています。コマンドラインインストー

> ルでは、`/exclude` または `/includeadditional` オプションを使用して、利用可能なコンポーネントを明示的に除外または含めることができます。

- **/includeadditional** "*コンポーネント*"\[,"*コンポーネント*"\] ...
- **/exclude** "*コンポーネント*"\[,"*コンポーネント*"\] ...

次の表は、このページの項目のデフォルト設定を示しています。デフォルト設定は、**環境**ページで選択したオプションによって異なります。

追加コンポーネントページ	環境ページ: 「MCS を使用したマスターイメージ」または「CITRIX PROVISIONING を使用したマスターイメージ」が選択されている場合	環境ページ: 「サーバーへのブローカー接続を有効にする」（マルチセッション OS の場合）または「リモート PC アクセス」（シングルセッション OS の場合）が選択されている場合
アプリパッケージ配信コンポーネント	選択されていません	選択されていません
ユーザーパーソナライゼーションレイヤー	選択されていません	このユースケースでは無効なため、表示されません。
シトリックス プロファイル管理	選択済み	未選択
Citrix Profile Management WMI プラグイン	選択済み	未選択
シトリックス VDA アップグレード エージェント	未選択	未選択
シトリックス バックアップおよびリストア	未選択	未選択
シトリックス MCS IODriver	未選択	未選択
Citrix ランデブー V2	選択されていません	選択されていません

このページは、次の場合には表示されません。

- `VDAWorkstationCoreSetup.exe` インストーラーを使用している場合。また、追加コンポーネントのコマンドラインオプションは、そのインストーラーでは無効です。

- VDA をアップグレードしていて、すべての追加コンポーネントがすでにインストールされている場合。一部の追加コンポーネントがすでにインストールされている場合、そのページにはインストールされていないコンポーネントのみが表示されます。

次のチェックボックスをオンまたはオフにします。(コンポーネントはインストーラーで異なる順序で表示される場合があります。)

- **App Packages Delivery Component:** Microsoft App-Vパッケージのアプリケーションを使用する場合は、このコンポーネントをインストールします。詳しくは、「App-Vアプリケーションの展開と配信」を参照してください。

  コマンドラインオプション: コンポーネントのインストールを有効にするには `/includeadditional "Citrix Personalization for App-V – VDA"`、コンポーネントのインストールを防止するには `/exclude "Citrix Personalization for App-V – VDA"`。

- **Citrixユーザーパーソナライゼーションレイヤー:** ユーザーパーソナライゼーションレイヤー用のMSIをインストールします。詳細については、「ユーザーパーソナライゼーションレイヤー」を参照してください。

  このコンポーネントは、シングルセッションのWindows 10マシンにVDAをインストールする場合にのみ表示されます。

  コマンドラインオプション: コンポーネントのインストールを有効にするには `/includeadditional "User Personalization Layer"`、コンポーネントのインストールを防止するには `/exclude "User Personalization Layer"`。

- **Citrix Profile Management:** このコンポーネントは、ユーザープロファイル内のユーザーパーソナライゼーション設定を管理します。詳細については、「Profile Management」を参照してください。

  Citrix Profile Managementをインストールから除外すると、Citrix DirectorによるVDAの監視とトラブルシューティングに影響します。**ユーザーの詳細**ページと**エンドポイント**ページでは、**パーソナライゼーション**パネルと**ログオン期間**パネルが機能しません。**ダッシュボード**ページと**傾向**ページでは、**平均ログオン期間**パネルはProfile Managementがインストールされているマシンのみのデータを表示します。

  サードパーティのユーザープロファイル管理ソリューションを使用している場合でも、Citrixは Citrix Profile Management Serviceをインストールして実行することをお勧めします。Citrix Profile Management Serviceを有効にする必要はありません。

コマンドラインオプション: コンポーネントのインストールを有効にするには `/includeadditional "Citrix Profile Management"`、コンポーネントのインストールを防止するには `/exclude "Citrix Profile Management"`。

- **Citrix Profile Management WMIプラグイン:** このプラグインは、WMI（Windows Management Instrumentation）オブジェクト（プロファイルプロバイダー、プロファイルタイプ、サイズ、ディスク使用量など）でProfile Managementのランタイム情報を提供します。WMIオブジェクトは、Directorにセッション情報を提供します。

  コマンドラインオプション: コンポーネントのインストールを有効にするには `/includeadditional "Citrix Profile Management WMI Plug-in"`、コンポーネントのインストールを防止するには `/exclude "Citrix Profile Management WMI Plug-in"`。

- **VDAアップグレードエージェント:** Citrix DaaS（旧Citrix Virtual Apps and Desktopsサービス）展開にのみ適用されます。VDAがVDAアップグレード機能に参加できるようにします。この機能を使用して、管理コンソールから、即時またはスケジュールされた時間にカタログのVDAをアップグレードできます。このエージェントがインストールされていない場合、マシン上でVDAインストーラーを実行してVDAをアップグレードできます。

  コマンドラインオプション: コンポーネントのインストールを有効にするには `/includeadditional "Citrix VDA Upgrade Agent"`、コンポーネントのインストールを防止するには `/exclude "Citrix VDA Upgrade Agent"`。

- **ストレージ最適化のためのMCSIOライトキャッシュ:** Citrix MCS I/Oドライバーをインストールします。詳細については、ハイパーバイザーで共有されるストレージおよび一時データ用のキャッシュの構成を参照してください。

  コマンドラインオプション: コンポーネントのインストールを有効にするには `/includeadditional "Citrix MCS IODriver"`、コンポーネントのインストールを防止するには `/exclude "Citrix MCS IODriver"`。

- **プロキシ構成:** 環境でGateway Service、VDA Upgrade ServiceなどでRendezvousプロトコルを使用する予定があり、アウトバウンド接続のためにネットワークに非透過型プロキシがある場合は、ここでプロキシを指定します。HTTPプロキシのみがサポートされています。

  このコンポーネントをインストールする場合は、**Rendezvousプロキシ構成**ページでプロキシのアドレスまたはPACファイルのパスを指定します。機能の詳細については、「Rendezvousプロトコル」を参照してください。

  コマンドラインオプション: コンポーネントのインストールを有効にするには `/includeadditional "Citrix Rendezvous V2"`、コンポーネントのインストールを防止するには `/exclude "Citrix Rendezvous V2"`。

- **Citrix Backup and Restore:** VDAのインストールまたはアップグレードが失敗した場合、このコンポーネントはマシンをインストールまたはアップグレード前のバックアップ状態に戻すことができます。

  インストール準備に記載されているMicrosoftの前提条件が満たされていることを確認してください。

  コマンドラインオプション: コンポーネントのインストールを有効にするには `/includeadditional "Citrix Backup and Restore"`、コンポーネントのインストールを防止するには `/exclude "Citrix Backup and Restore"`。

  > **注:**
  >
  > MCSストレージ最適化が有効になっている場合、Windowsサーバーまたはデスクトップオペレーティングシステムのバックアップまたは復元が失敗する可能性があります。これを解決するには、メタインストーラーでMCSストレージ最適化オプションを無効にしてください。

手順 7. オプションソフトウェアのインストール

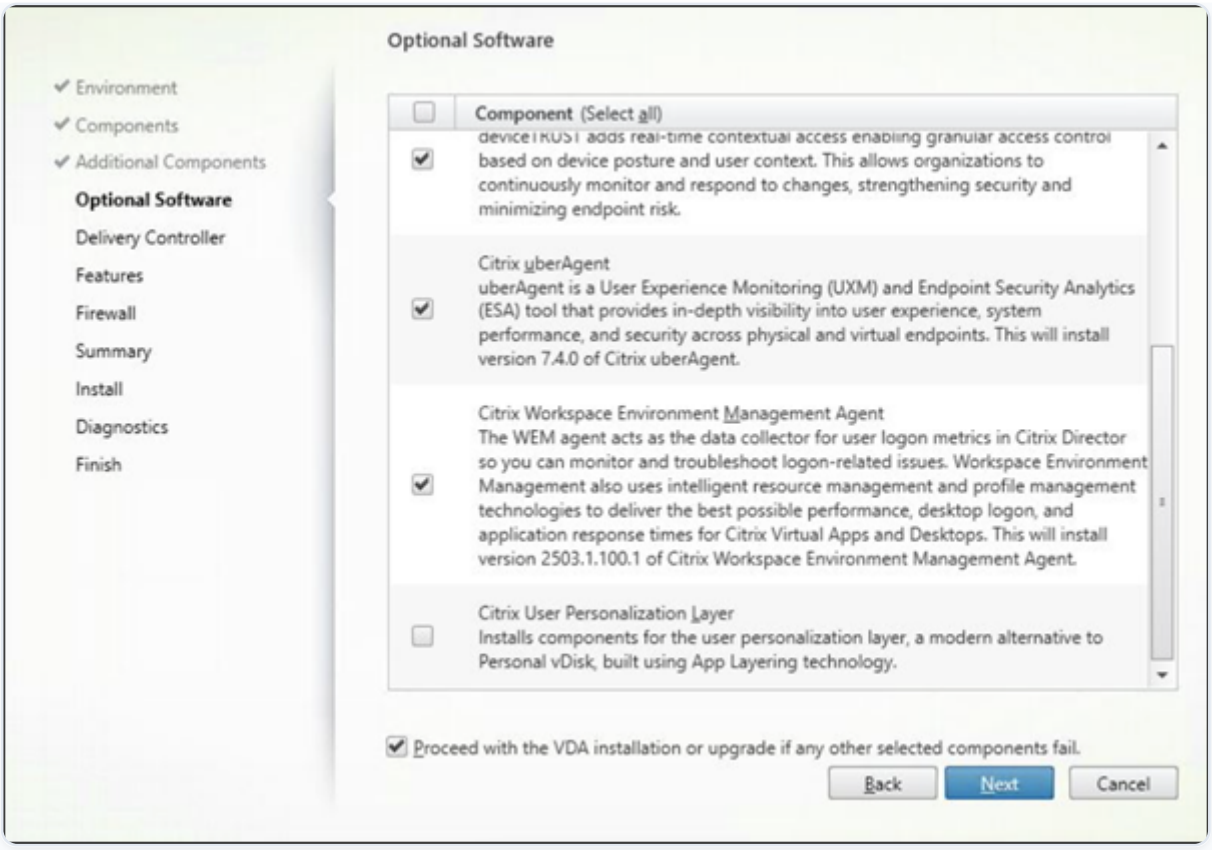
> **注:**
>
> 「オプションソフトウェア」ページは、このバージョンで新たに追加されたもので、VDAに追加のCitrixソフトウェアをインストールする際の柔軟性を顧客に提供します。

Citrix Workspace™アプリとCitrix Secure Access™クライアントは、コンポーネントページからオプションソフトウェアページに移動されました。

Citrix Device Trust、Uber Agent Component、およびCitrix Workspace Environment Management™ Agentがオプションソフトウェアページに追加され、デフォルトでインストールが選択されるようになりました。

ユーザーパーソナライゼーションレイヤーも、追加コンポーネントページからオプションソフトウェアページに移動されました。その選択ロジックは、追加コンポーネントページに

あったときと同じです。つまり、ユーザーパーソナライゼーションレイヤーがすでにインストールされている場合、「必須」として選択され、コンポーネントはアップグレードされます。



オプションソフトウェアページで、次の操作を行います。

- **コンポーネント**: デフォルトでは、Windows用Citrix WorkspaceアプリはVDAと一緒にインストールされません。`VDAWorkstationCoreSetup.exe`インストーラーを使用している場合、Windows用Citrix Workspaceアプリはインストールされないため、このチェックボックスは表示されません。

Nextをクリックします。

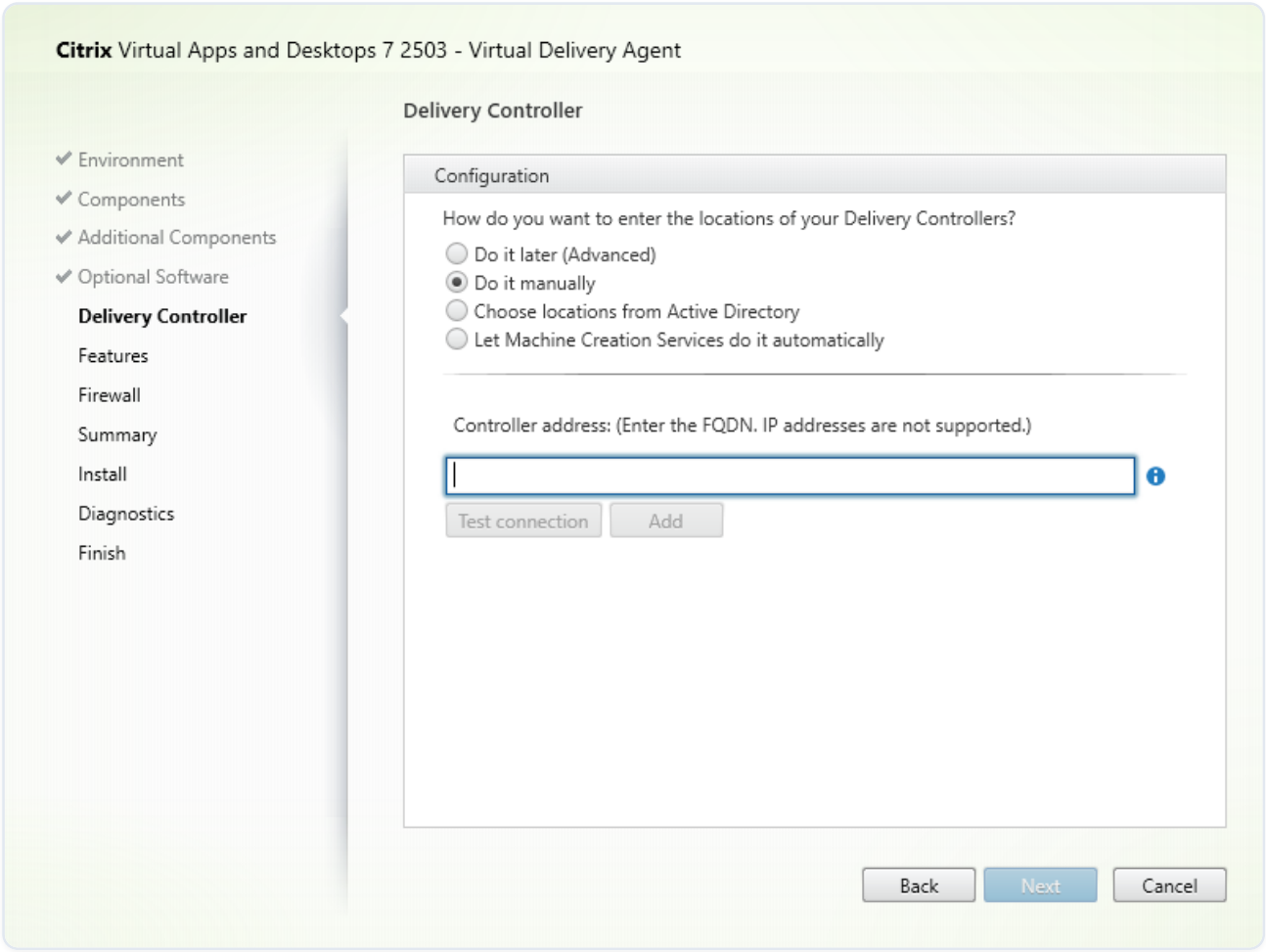
コマンドラインオプション: `'/installdir "C:\Program Files\VDA" /components "VDA","CSA","DT","UBERAGENT","PLUGINS"`。指定されたディレクトリにVirtual Delivery Agent、Citrix Secure Access Client、Citrix deviceTRUST、Citrix uberAgent、およびCitrix Workspace Appをインストールします。

注:

VDAのインストール、アップグレード、またはアンインストール中に、以下のシナリオでCitrix Workspaceアプリおよびその他のコンポーネントをインストール、アップグレード、またはアンインストールすることを選択できます。

- VDAのインストール中に、ここでコンポーネントとCWAプラグインをインストールすることを選択できます。デフォルトでは、Citrix Workspaceアプリ、Citrix Secure Access Client、およびCitrix User Personalization LayerはVDAのインストール中にインストールされません。Citrix deviceTrust®、Citrix uberAgent、Citrix Workspace Environment Managementエージェントなどの残りのすべてのコンポーネントは、デフォルトでインストールが選択されています。
- VDAのアップグレード中に、Citrix Workspaceアプリ、Citrix Secure Access Client、Citrix User Personalization LayerがVDAにまだインストールされていない場合、それらをインストールすることを選択できます。
- VDAのアップグレード中に、Citrix Workspaceアプリおよびその他のインストール済みプラグインのバージョンをアップグレードできる場合、それらをアップグレードするオプションが表示されます。
- インストールまたはアップグレード中に、Citrix Workspaceアプリ（CWA）プラグインまたはコンポーネントのインストールまたはアップグレードが失敗した場合、**「選択したコンポーネントのインストールが失敗してもVDAのアップグレードまたはインストールを続行する」**チェックボックスをオンにすることで、その失敗を上書きしてコアVDAのインストールを続行できます。
- VDAのアンインストール中に、Citrix Workspaceアプリおよびその他のインストール済みコンポーネントをアンインストールしないことを選択できます。デフォルトでは、VDAのアンインストール中にCitrix Workspaceアプリおよびその他のインストール済みコンポーネントはアンインストールされます。

手順8. Delivery Controller™のアドレス



Delivery Controllerページで、インストールされているControllerのアドレスを入力する方法を選択します。Citrixでは、VDAのインストール中にアドレスを指定することをお勧めします（**手動で実行**）。VDAはこの情報がないとControllerに登録できません。VDAが登録できない場合、ユーザーはそのVDA上のアプリケーションやデスクトップにアクセスできません。

- **手動で実行:**（デフォルト）インストールされているControllerのFQDNを入力し、**「追加」**をクリックします。複数のControllerをインストールしている場合は、それらのアドレスを追加します。
- **後で実行（詳細設定）:** このオプションを選択すると、ウィザードは続行する前にその操作でよいか確認を求めます。後でアドレスを指定するには、インストーラーを再実行するか、Citrixグループポリシーを使用します。ウィザードは**概要**ページでも通知します。
- **Active Directoryから場所を選択:** マシンがドメインに参加しており、ユーザーがドメインユーザーである場合にのみ有効です。
- **WebSocketトークンを使用:** WebSocket VDAを作成します。WebSocketTokenは、必要なトークン用です。
- **Machine Creation Servicesに自動的に実行させる:** MCSを使用してマシンをプロビジョニングする場合にのみ有効です。

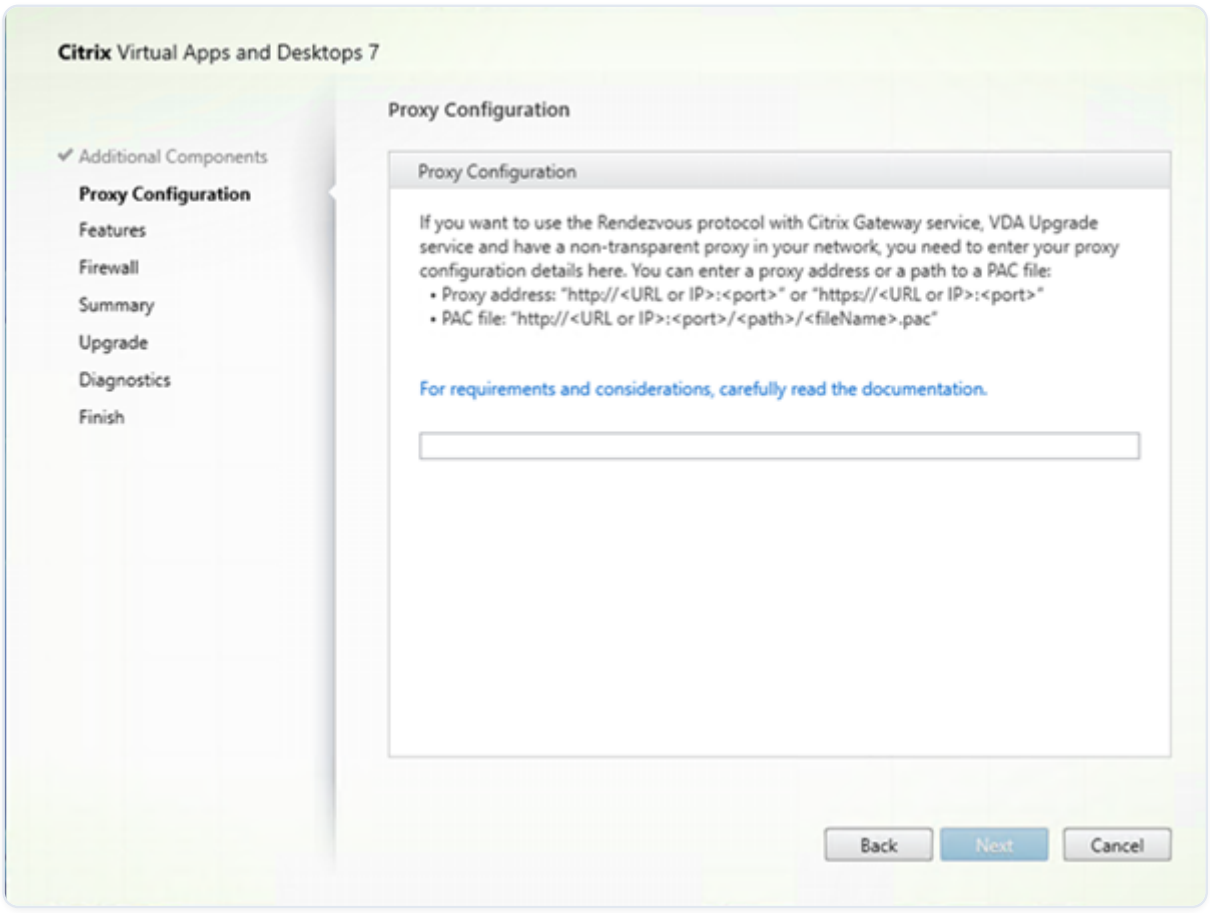
「次へ」をクリックします。「後で実行（詳細設定）」**を選択した場合、Controllerアドレスを後で指定することを確認するプロンプトが表示されます。

その他の考慮事項：

- アドレスに英数字以外の文字を含めることはできません。
- VDAインストール時とグループポリシーでアドレスを指定した場合、ポリシー設定がインストール時に指定された設定を上書きします。
- VDAの登録を成功させるには、Controllerとの通信に使用されるファイアウォールポートが開いている必要があります。このアクションは、ウィザードの**ファイアウォール**ページでデフォルトで有効になっています。
- Controllerの場所を指定した後（VDAインストール中またはインストール後）、Controllerが追加または削除されたときにVDAを更新するために自動更新機能を使用できます。VDAがControllerを検出して登録する方法の詳細については、「VDA登録」を参照してください。

コマンドラインオプション：`/controllers`

ステップ9. プロキシ構成



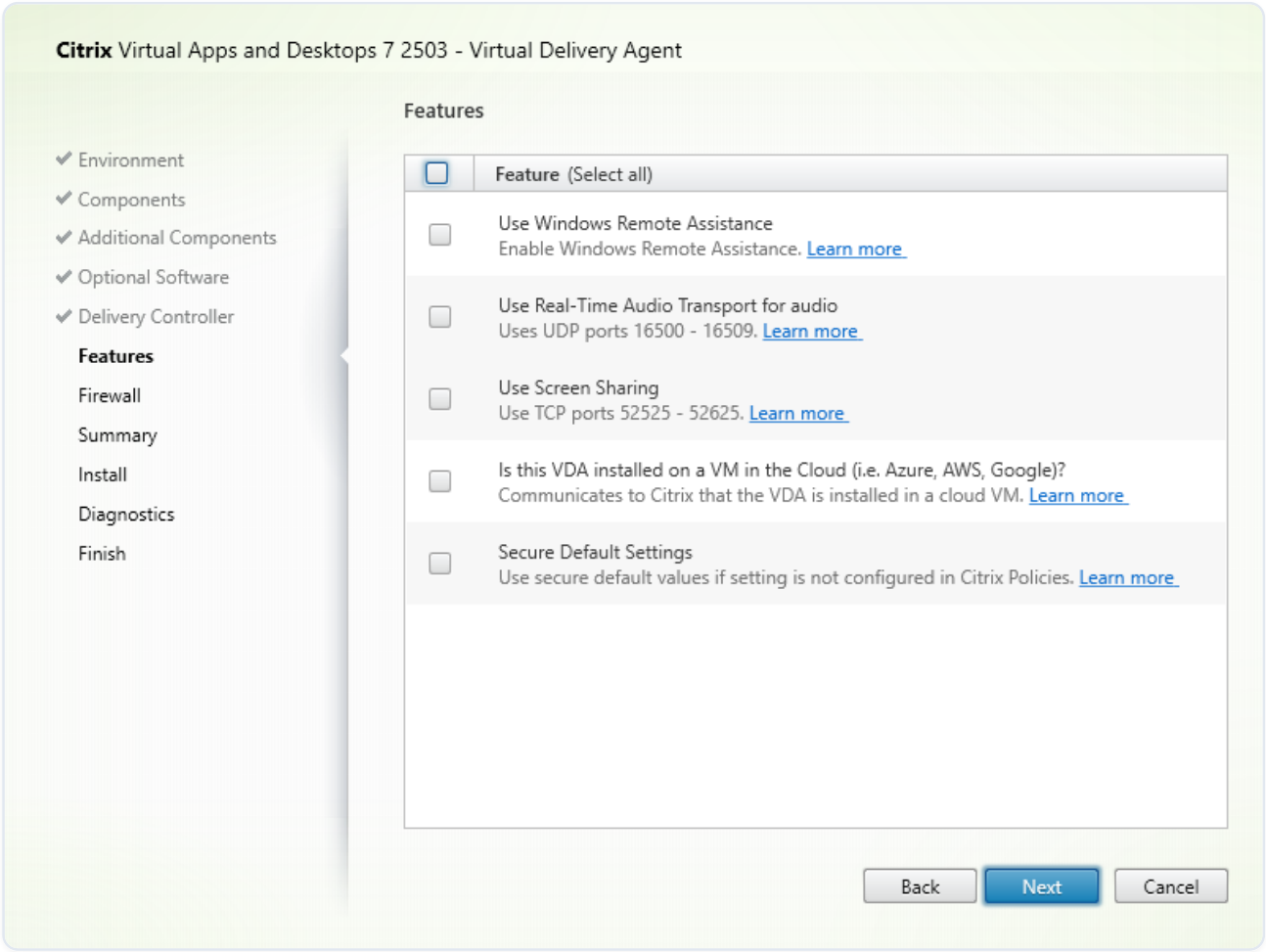
プロキシ構成ページは、**追加コンポーネント**ページで**プロキシ構成**チェックボックスを有効にした場合にのみ表示されます。

1. プロキシソースをプロキシアドレスで指定するか、PACファイルパスで指定するかを選択します。
2. プロキシアドレスまたはPACファイルパスを指定します。
   - プロキシアドレスの形式: `http://<url-or-ip>:<port>`
   - PACファイルの形式: `http://<url-or-ip>:<port>/<path>/<filename>.pac`

接続テストを成功させるには、プロキシポートのファイアウォールが開いている必要があります。プロキシに接続できない場合でも、VDAのインストールを続行するかどうかを選択できます。

コマンドラインオプション：`/proxyconfig`

ステップ10. 機能の有効化または無効化



機能ページで、チェックボックスを使用して、使用する機能を有効または無効にします。

- **Windows リモートアシスタンスを使用する:** この機能を有効にすると、Director のユーザーシャドウ機能で Windows リモートアシスタンスが使用されます。Windows リモートアシスタンスは、ファイアウォールで動的ポートを開きます。(デフォルト = 無効)

  コマンドラインオプション: `/enable_remote_assistance`

- **オーディオにリアルタイムオーディオトランスポートを使用する:** ネットワークで Voice-over-IP が広く使用されている場合は、この機能を有効にします。この機能は、遅延を減らし、損失の多いネットワークでのオーディオの回復力を向上させます。RTP over UDP トランスポートを使用してオーディオデータを送信できます。(デフォルト = 無効)

  コマンドラインオプション: `/enable_real_time_transport`

- **画面共有を使用する:** 有効にすると、画面共有で使用されるポートが Windows ファイアウォールで開かれます。(デフォルト = 無効)

  コマンドラインオプション: `/enable_ss_ports`

- **この VDA はクラウド内の VM にインストールされていますか:** この設定は、Citrix がテレメトリ目的でオンプレミスおよびサービス (Citrix Cloud™) VDA 展開のリソースの場所を正しく識別するのに役立ちます。この機能は、顧客側の利用には影響しません。展開で Citrix DaaS を使用している場合は、この設定を有効にします。(デフォルト = 無効).

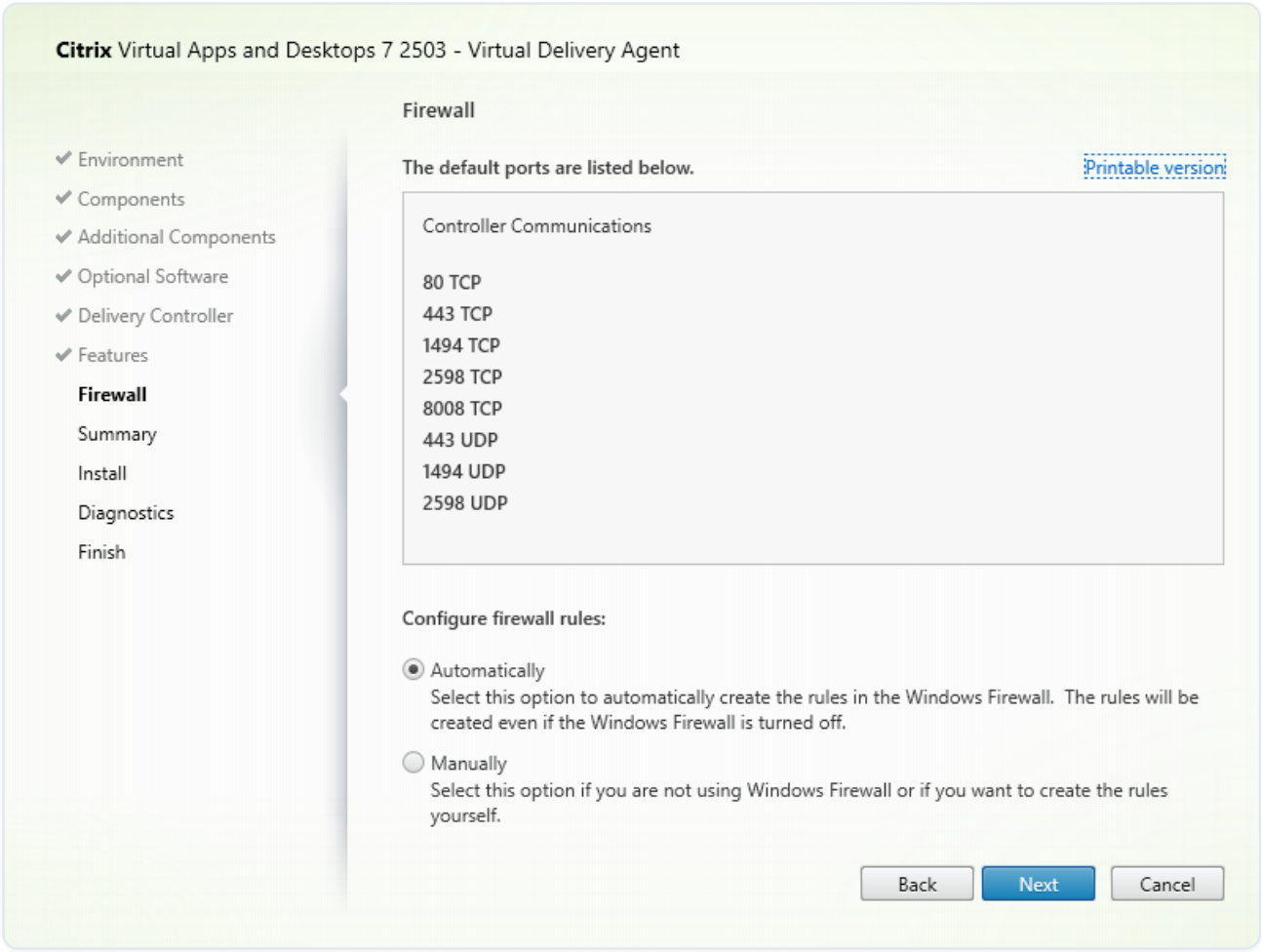
  コマンドラインオプション: `/xendesktopcloud`

- **セキュアなデフォルト設定:** このオプションは、より安全な初期設定のために、さまざまな機能のデフォルト設定を有効から無効に変更します。関連する機能は次のとおりです: クライアントドライブリダイレクト、特殊フォルダーリダイレクト、ドラッグアンドドロップ、クライアント TWAIN デバイスリダイレクト、クライアント USB プラグアンドプレイデバイスリダイレクト、クライアントプリンターリダイレクト、クライアントクリップボードリダイレクト、クライアントマイクのリダイレクト。

コマンドラインオプション: `/ENABLE_SECURE_DEFAULTS`

Nextをクリックします。

ステップ 11. ファイアウォールポート

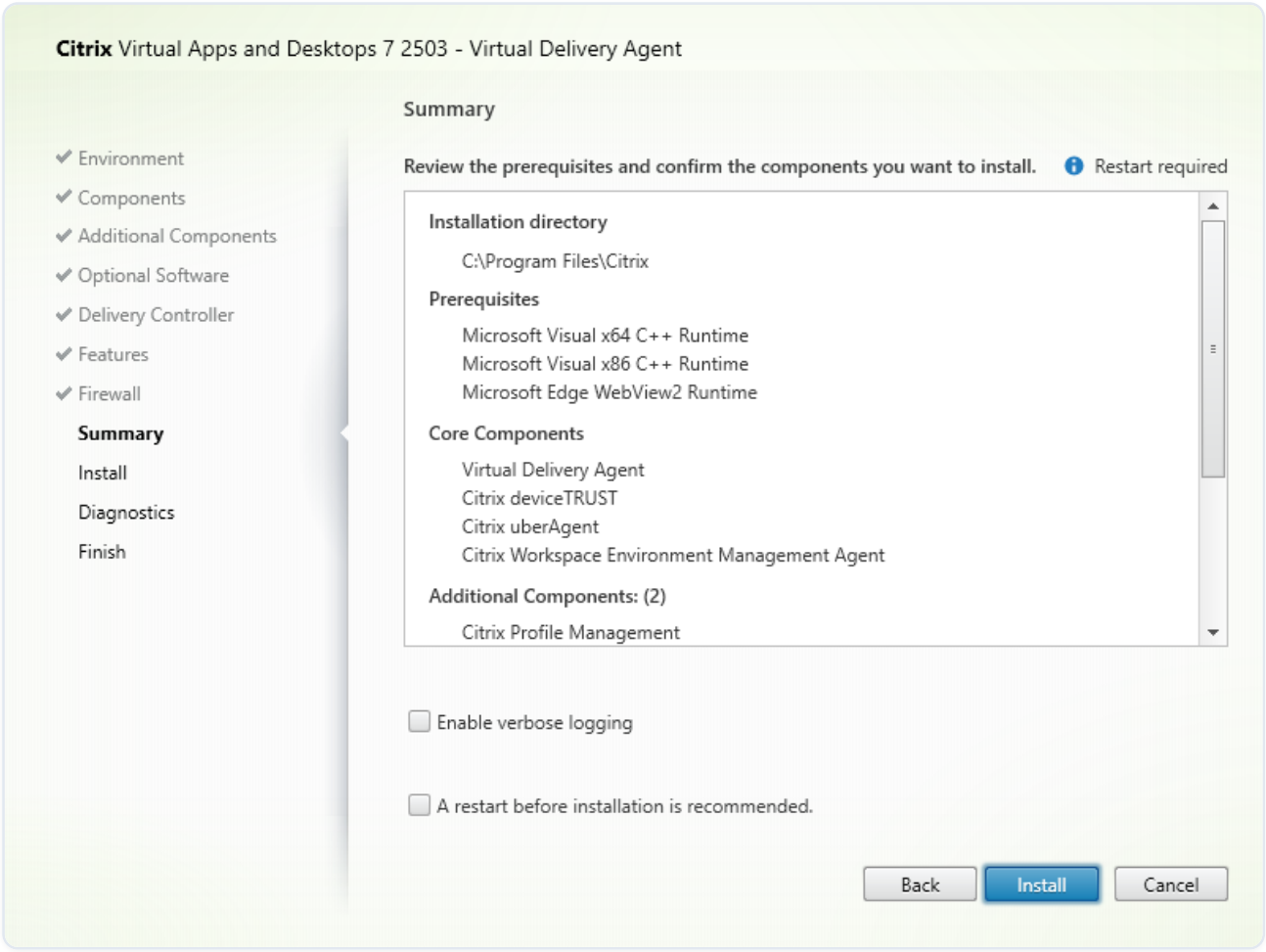


「**ファイアウォール**」ページでは、デフォルトで、Windows ファイアウォールサービスが実行されている場合、ファイアウォールが有効になっていなくてもポートは自動的に開かれます。このデフォルト設定は、ほとんどの展開で問題ありません。ポート情報については、「ネットワークポート」を参照してください。

Nextをクリックします。

コマンドラインオプション: `/enable_hdx_ports`

手順 12. 前提条件を確認し、インストールを確定する



概要ページには、インストールされるものが一覧表示されます。**戻る**ボタンを使用して、以前のウィザードページに戻り、選択を変更します。

準備ができたら、**インストール**をクリックします。

前提条件がまだインストールまたは有効化されていない場合、マシンが1回以上再起動する可能性があります。インストールの準備を参照してください。

手順 13. 診断

VDAインストーラーの診断ページ(/en-us/citrix-virtual-apps-desktops/2503/media/vda-ss-diagnostics.png)

診断ページで、Citrix Call Homeに参加するかどうかを選択します。参加することを選択した場合（デフォルト）は、「**接続**」をクリックします。プロンプトが表示されたら、Citrixアカウントの資格情報を入力します。

資格情報が検証された後（または参加しないことを選択した場合）、**次へ**をクリックします。

フル製品インストーラーを使用している場合、**診断**ページで、最初に**診断情報の収集**を選択せずに**接続**をクリックすると、**Citrix Insight Servicesへの接続**ダイアログを閉じると、**次へ**ボタンが無効になります。次のページに進むことができません。**次へ**ボタンを再度有効にするには、**診断情報の収集**を選択し、すぐに選択を解除します。

詳しくは、Call Homeを参照してください。

手順 14. このインストールを完了する

VDAインストーラーのインストール完了ページ(/en-us/citrix-virtual-apps-desktops/2503/media/vda-ss-finish.png)

完了ページには、正常にインストールおよび初期化されたすべての前提条件とコンポーネントの緑色のチェックマークが表示されます。

完了をクリックします。デフォルトでは、マシンは自動的に再起動します。この自動再起動を無効にすることはできますが、マシンが再起動するまでVDAは使用できません。

次のステップ

必要に応じて、上記のプロシージャを繰り返して、他のマシンまたはイメージにVDAをインストールします。

すべてのVDAをインストールしたら、Studioを起動します。まだサイトを作成していない場合は、Studioが自動的にそのタスクに誘導します。それが完了すると、Studioはマシンカタログを作成し、次にデリバリーグループを作成するように誘導します。参照：

- サイトの作成
- マシンカタログの作成
- 「デリバリーグループの作成」(/ja-jp/citrix-virtual-apps-desktops/2503/install-configure/delivery-groups-create.html)

シトリックス オプティマイザー

Citrix Optimizerは、Citrix管理者がさまざまなコンポーネントを削除および最適化することでVDAを最適化するのに役立つWindows OS用のツールです。

VDAをインストールし、最終的な再起動を完了した後、Citrix Optimizerをダウンロードしてインストールします。「CTX224676」を参照してください。CTXの記事には、ダウンロードパッケージと、Citrix Optimizerのインストールおよび使用方法に関する手順が含まれています。

VDAをカスタマイズする

インストール済みのVDAをカスタマイズするには：

1. プログラムの削除または変更のためのWindows機能から、**Citrix Virtual Delivery Agent**または**Citrix Remote PC Access/VDI Core Services VDA**を選択します。次に右クリックして**変更**を選択します。
2. **Virtual Delivery Agent設定のカスタマイズ**を選択します。インストーラーが起動したら、以下を変更できます。

   - Controllerアドレス
   - Controllerに登録するTCP/IPポート（デフォルト = 80）
   - Windowsファイアウォールポートを自動的に開くかどうか

トラブルシューティング

- Citrixがコンポーネントインストールの結果を報告する方法については、「Citrixインストールのリターンコード」を参照してください。
- デリバリーグループのStudio表示で、**詳細**ペインの**インストール済みVDAバージョン**エントリが、マシンにインストールされているバージョンと異なる場合があります。マシンのWindowsのプログラムと機能の表示には、実際のVDAバージョンが表示されます。
- VDAがインストールされても、Delivery Controllerに登録されるまでは、ユーザーにアプリやデスクトップを配信できません。

  VDAの登録方法と登録の問題のトラブルシューティングについては、「VDA登録」を参照してください。

既知の制限事項

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

VDAインストールに関連するWindows Defenderアクセス制御の構成

顧客は、未署名のバイナリのロードを禁止するために、Windows Defenderアクセス制御 (WDAC) 設定を構成します。VDAインストーラーを通じて配布される未署名のバイナリは、VDAのインストールを制限するため、禁止されます。

Citrix®は現在、すべてのCitrix生成バイナリにCitrixコード署名証明書で署名しています。さらに、Citrixは、当社の製品とともに配布されるサードパーティ製バイナリについても、それらのサードパーティ製バイナリを信頼されたバイナリとして認証する証明書で署名しています。

重要:

未署名のサードパーティ製バイナリを含む古いVDAから、署名済みバイナリを含む新しいVDAバージョンにアップグレードしても、アップグレードされたマシンに署名済みバイナリが常に配置されるとは限りません。 これは、システムのアップグレードが同じバージョンのバイナリを置き換えないというOS内のメカニズムによるものです。 サードパーティ製バイナリは署名されていますが、サードパーティによって管理されているそのバージョンはCitrixによって更新できないため、これらのバイナリは更新されません。この制限を回避するには:

1. バイナリを許可リストに含めます。これにより、バイナリに署名する必要がなくなります。
2. 古いVDAをアンインストールし、新しいVDAをインストールします。これはVDAの新規インストールに似ており、署名されたバージョンがインストールされます。

ウィザードを使用して新しいベースポリシーを作成する

WDACを使用すると、信頼されたバイナリをシステムで実行できるように追加できます。WDACのインストール後、**Windows Defenderアプリケーション制御ポリシーウィザード**が自動的に開きます。

バイナリを追加するには、新しいベースWDACポリシーを作成する必要があります。ベースポリシーを作成するためのCitrix推奨ガイドラインは、このセクションで提供されます。

- ベーステンプレートとして**署名済みおよび評判モード**を選択します。これは、Windowsオペレーティングコンポーネント、Microsoft Storeからインストールされたアプリ、すべてのMicrosoft署名済みソフトウェア、およびサードパーティのWindowsハードウェア互換ドライバーを承認するためです。
- **監査モードを有効にする**。これは、新しいWindows Defenderアプリケーション制御ポリシーを適用する前にテストできるためです。
- アプリケーションが識別され信頼されるレベルを指定し、参照ファイルを提供するために、**ファイルルール**に**カスタムルール**を追加します。ルールタイプとして「発行元」を選択することで、Citrix証明書のいずれかで署名された参照ファイルを選択できます。

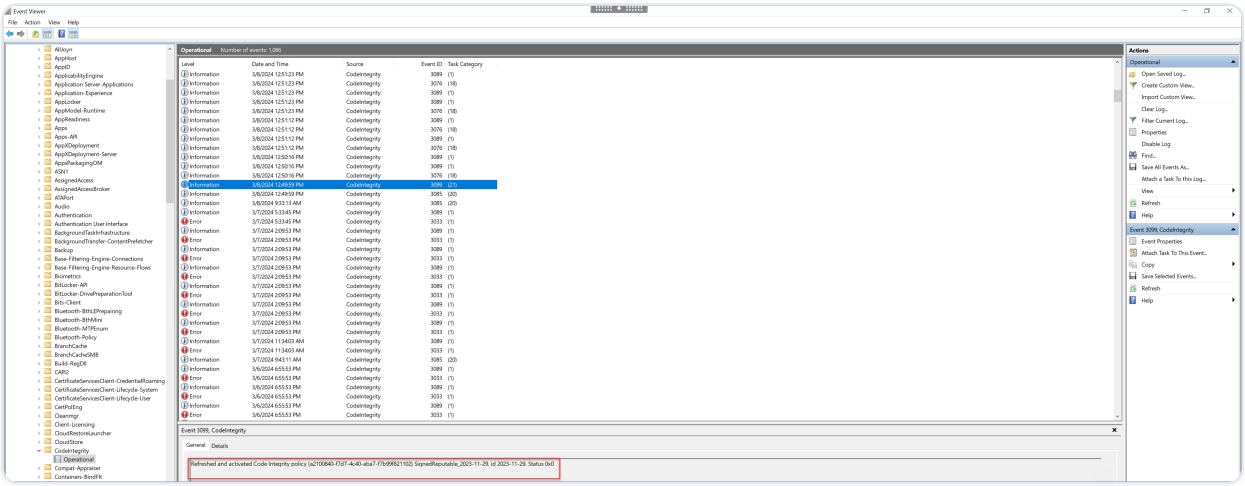
- ルールが追加されたら、`.XML`と`.CIP`ファイルが保存されているフォルダーに移動します。`.XML`ファイルには、ポリシーで定義されているすべてのルールが含まれています。これは、任意のルールを変更、追加、または削除するように構成できます。
- WDACポリシーを展開する前に、`.XML`ファイルをバイナリ形式に変換する必要があります。WDACファイルは`.XML`ファイルを`.CIP`ファイルに変換します。
- `.CIP`ファイルをC:\WINDOWS\System32\CodeIntegrity\CiPolicies\Activeにコピーして貼り付け、マシンを再起動します。生成されたポリシーは監査モードで適用されます。
- ベースポリシーを作成するためのステップバイステップのプロセスについては、「ウィザードを使用して新しいベースポリシーを作成する」を参照してください。

このポリシーが適用されると、WDACは、指定された発行元/CA機関によって署名されているCitrixファイルについて警告を発しません。

同様に、サードパーティによって署名されたファイルに対して、発行元レベルのルールを作成できます。

適用されたポリシーを確認する

1. マシンが再起動された後、**イベントビューアー**を開き、**アプリケーションとサービスログ > Microsoft > Windows > CodeIntegrity > Operational**に移動します。
2. 適用されたポリシーがアクティブになっていることを確認します。



3. ポリシーに違反したログを探し、そのファイルのプロパティを確認します。まず、署名されていることを確認します。署名されていない場合で、このマシンがVDAアップグレードを経ている場合、これは上記の制限で説明されているケースである可能性が高いです。署名されている場合、このファイルは、前述のとおり、代替証明書で署名されている可能性があります。

Citrix証明書で署名されたCitrix生成ファイルの例は`C:\Windows\System32\drivers\picadm.sys`です。 Citrixサードパーティ証明書で署名されたサー

ドパーティバイナリの例は`C:\Program Files\Citrix\IcaConfigTool\Microsoft.Practices.Unity.dll`です。

VDAのインストールとアップグレードの事前チェック

VDAのインストールとアップグレードのための分離された事前フライトチェックを導入し、お客様が続行する前に潜在的な問題を事前に特定できるようにします。このチェックは、すべての依存関係と前提条件を検証し、各条件について明確な合否ステータスを提供します。失敗が発生した場合は、具体的な推奨事項を含む詳細な修復ガイダンスが提供されます。実際のインストールまたはアップグレードプロセスは別個のものであり、事前チェックが完了した後に手動で開始する必要があります。

この記事では、VDAのインストールとアップグレードの事前チェックを実行する手順について説明します。

ステップ1. コマンドラインを実行する

> **注:**
>
> - 事前チェックはコマンドラインモードでのみサポートされています。
> - このコマンドを実行しても、インストールまたはアップグレードは開始されません。

> 事前チェックを実行するには、インストールまたはアップグレードによく使用するコマンドに`/precheckonly`オプションを追加します。VDAのインストールまたはアップグレードに関するすべての事前チェック条件が確認されます。

デフォルトのインストールとアップグレードの事前チェックを実行する

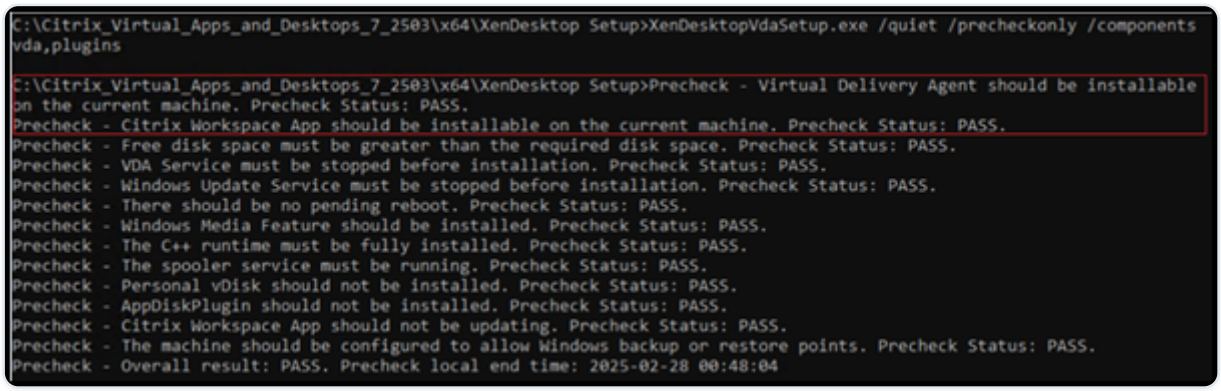
次のコマンドを実行して事前チェックを行い、マシンの状態が許容可能な状態であることを確認します。`\x64\XenDesktop Setup\XenDesktopVdaSetup.exe /quiet /precheckonly`

```
C:\Citrix_Virtual_Apps_and_Desktops_7_2503\x64\XenDesktop Setup>XenDesktopVdaSetup.exe /quiet /precheckonly

C:\Citrix_Virtual_Apps_and_Desktops_7_2503\x64\XenDesktop Setup>Precheck - Virtual Delivery Agent should be installable on the
current machine. Precheck Status: PASS.
Precheck - Citrix uberAgent should be installable on the current machine. Precheck Status: PASS.
Precheck - Citrix Workspace Environment Management Agent should be installable on the current machine. Precheck Status: PASS.
Precheck - Citrix deviceTRUST should be installable on the current machine. Precheck Status: PASS.
Precheck - Free disk space must be greater than the required disk space. Precheck Status: PASS.
Precheck - VDA Service must be stopped before installation. Precheck Status: PASS.
Precheck - Windows Update Service must be stopped before installation. Precheck Status: PASS.
Precheck - There should be no pending reboot. Precheck Status: PASS.
Precheck - Windows Media Feature should be installed. Precheck Status: PASS.
Precheck - The C++ runtime must be fully installed. Precheck Status: PASS.
Precheck - The spooler service must be running. Precheck Status: PASS.
Precheck - Personal vDisk should not be installed. Precheck Status: PASS.
Precheck - AppDiskPlugin should not be installed. Precheck Status: PASS.
Precheck - Citrix Workspace App should not be updating. Precheck Status: PASS.
Precheck - The machine should be configured to allow Windows backup or restore points. Precheck Status: PASS.
Precheck - Overall result: PASS. Precheck local end time: 2025-02-27 23:26:07
```

指定されたコンポーネントのインストールとアップグレードの事前チェックを実行する

インストールまたはアップグレードの前に特定のコンポーネントの前提条件を確認するには、コマンドに`/precheckonly`を追加します。 `\x64\XenDesktop Setup\XenDesktopVdaSetup.exe /quiet /precheckonly /components vda,plugins`



追加コンポーネント（Citrix Backup and Restore）のインストールとアップグレードの事前チェックを実行する

コマンド`\x64\XenDesktop Setup\XenDesktopVdaSetup.exe /quiet /precheckonly`は、オプションのチェックとして Citrix Backup and Restore コンポーネントの前提条件を確認します。オプションのチェックを除いてすべての事前チェックが合格した場合、全体の結果は PASS となります。

追加コンポーネントの事前チェック(/en-us/citrix-virtual-apps-desktops/2503/media/precheck-for-additional-components.png)

次のコマンドは、必須チェックの一部として Citrix Backup and Restore コンポーネントの前提条件を確認します。

- `\x64\XenDesktop Setup\XenDesktopVdaSetup.exe /quiet /precheckonly /includeadditional "Citrix Backup and Restore"`
- `\x64\XenDesktop Setup\XenDesktopVdaSetup.exe /quiet /precheckonly /enablerestore`
- `\x64\XenDesktop Setup\XenDesktopVdaSetup.exe /quiet /precheckonly /enablerestorecleanup`

Citrix Backup and Restore の事前チェック(/en-us/citrix-virtual-apps-desktops/2503/media/precheck-for-citrix-backup-and-restore.png)

ステップ 2. 事前チェック結果の表示

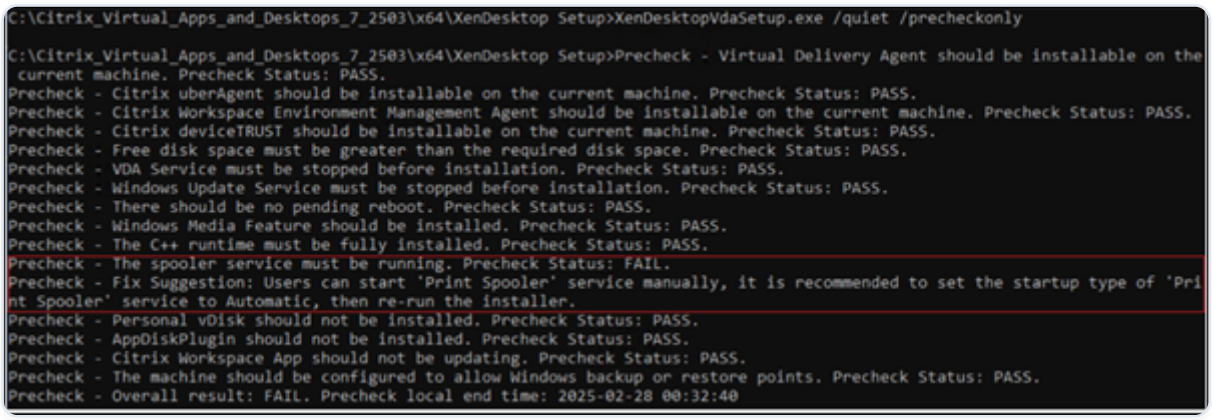
事前チェックの結果はコマンドラインに表示され、`%temp%/Citrix/XenDesktop Installer/XenDesktop Installation.log` にログ記録され、`%temp%/Citrix/XenDesktop Installer/PrecheckResult_{yyyyMMddHHmmss}.json` に保存されます。事前チェックが失敗した場合、全体の結果は `FAIL` となり、各問題に対する推奨される修正が表示されます。

コマンドライン出力

コマンドラインの事前チェック結果には、以下が含まれます。

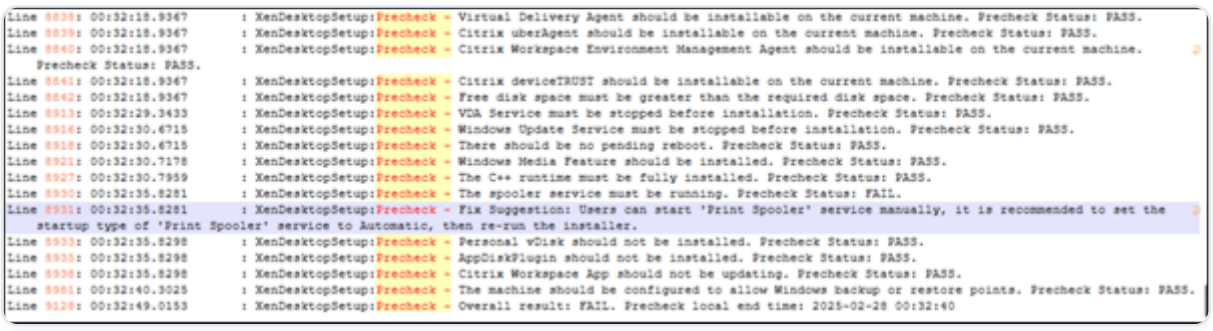
- 事前チェック基準
- 事前チェックステータス
- 失敗に対する修正案
- 全体結果
- 終了時刻。

結果が `FAIL` の場合、修正の提案は、**Precheck - Fix Suggestion:** で始まる行にあります。



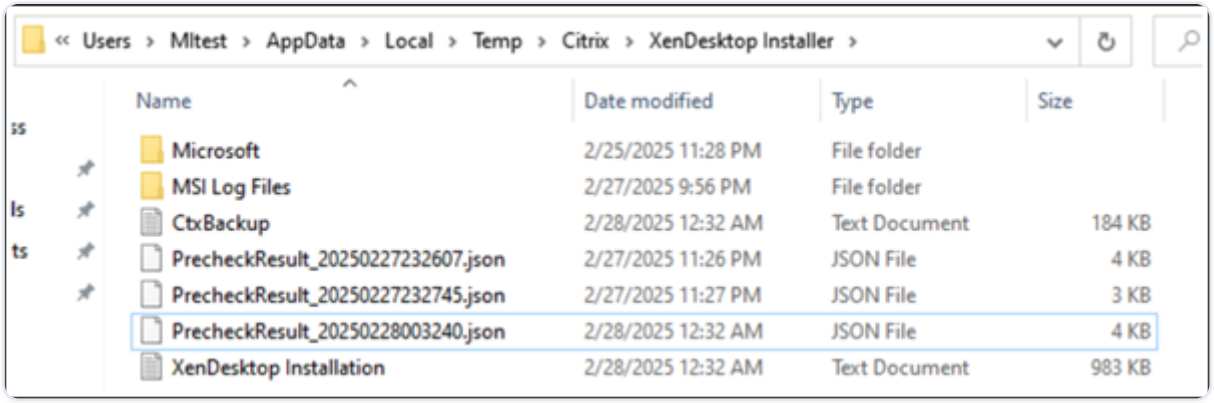
ログ出力

`XenDesktop Installation.log` の事前チェック結果は、コマンドラインに表示されるものと同じです。それらを見つけるには、ログファイルで `Precheck -` を検索してください。 全体的な結果が `FAIL` の場合、修正の提案は `Precheck - Fix Suggestion:` を含む行にあります。



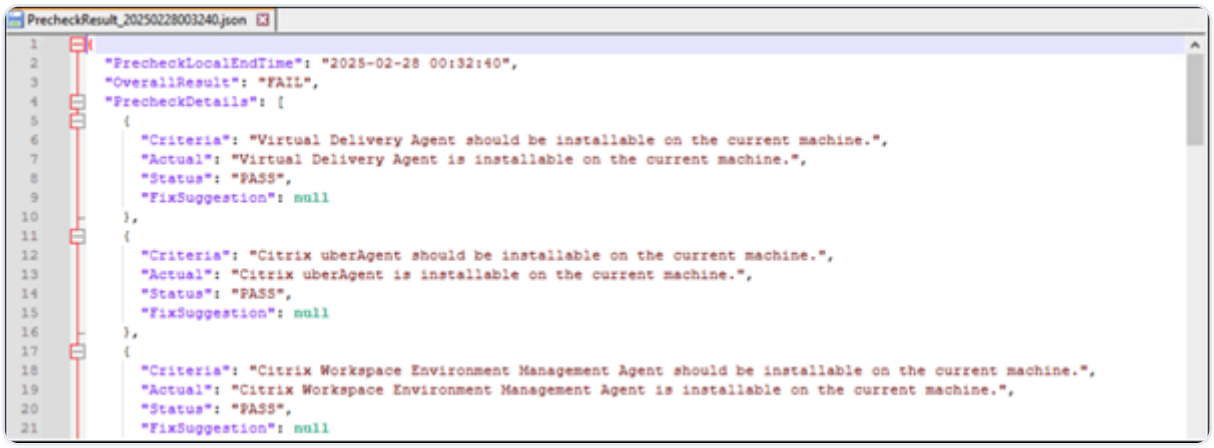
JSON 出力

`/quiet /precheckonly` を含むコマンドが実行されるたびに、`.json` ファイルが生成されます。ファイル名は `PrecheckResult_{yyyyMMddHHmmss}.json` で、タイムスタンプのサフィックスが付いています。

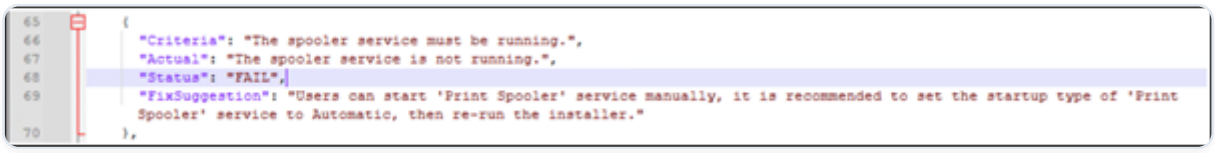


`.json` ファイルには以下が含まれます:

- 事前チェックのローカル終了時刻
- 全体的な結果
- 事前チェックの詳細
  - 基準
  - 実際の値
  - ステータス
  - 修正提案



`FAIL` のステータスを持つ各事前チェック項目に対する修正の提案は、`.json` ファイルの事前チェックの詳細セクションにあります。



スクリプトを使用してVDAをインストールする

注:

Citrixは、顧客の運用環境に合わせて調整されたスクリプトによって引き起こされる問題について責任を負いません。インストール関連のCitrixの問題については、Citrixサポートポータルを使用して、関連するインストールログとともにテクニカルサポートケースをオープンしてください。

この記事は、Windowsオペレーティングシステムを搭載したマシンにVDAをインストールする場合に適用されます。Linuxオペレーティングシステム用VDAの詳細については、Linux Virtual Delivery Agentのドキュメントを参照してください。

インストールメディアには、Active Directory内のマシンにVirtual Delivery Agent（VDA）をインストール、アップグレード、または削除するサンプルスクリプトが含まれています。これらのスクリプトは、Machine Creation Services™およびCitrix Provisioning（旧Provisioning Services）で使用されるマスターイメージの保守にも使用できます。

必要なアクセス権:

- スクリプトは、VDAインストールコマンドが配置されているネットワーク共有への「Everyone読み取り」アクセス権を必要とします。インストールコマンドは、完全な製品ISOでは`XenDesktopVdaSetup.exe`、スタンドアロンインストーラーでは`VDAWorkstationSetup.exe`または`VDAServerSetup.exe`です。
- ログの詳細は各ローカルマシンに保存されます。レビューと分析のために結果を一元的にログに記録するには、スクリプトは適切なネットワーク共有への「Everyone読み取り/書き込み」アクセス権を必要とします。

スクリプトの実行結果を確認するには、中央ログ共有を調べます。キャプチャされたログには、スクリプトログ、インストーラーログ、およびMSIインストールログが含まれます。各インストールまたは削除の試行は、タイムスタンプ付きのフォルダーに記録されます。フォルダーのタイトルは、PASSまたはFAILのプレフィックスで操作結果を示します。標準のディレクトリ検索ツールを使用して、中央ログ共有で失敗したインストールまたは削除を見つけることができます。これらのツールは、ターゲットマシンでローカルに検索する代替手段を提供します。

インストールを開始する前に、インストールの準備のタスクを読み、完了してください。

スクリプトを使用してVDAをインストールまたはアップグレードする

1. インストールメディアの\\Support\\AdDeploy\\からサンプルスクリプト**InstallVDA.bat**を入手します。Citrixは、スクリプトをカスタマイズする前に元のスクリプトのバックアップを作成することをお勧めします。
2. スクリプトを編集します。
   - インストールするVDAのバージョンを指定します: `SET DESIREDVERSION`。完全な値は、インストールメディアのProductVersion.txtファイルにあります。ただし、完全な一致は必要ありません。
   - インストーラーが呼び出されるネットワーク共有を指定します。レイアウトのルート（ツリーの最上位）を指します。スクリプトの実行時に、インストーラーの適切なバージョン（32ビットまたは64ビット）が自動的に呼び出されます。例: `SET DEPLOYSHARE=\\fileserver1\share1`。
   - オプションで、集中ログを保存するためのネットワーク共有場所を指定します。例: `SET LOGSHARE=\\fileserver1\log1)`。
   - コマンドラインを使用したインストールで説明されているように、VDA構成オプションを指定します。`/quiet`と`/noreboot`オプションは、スクリプトにデフォルトで含まれており、必須です: `SET COMMANDLINEOPTIONS=/QUIET /NOREBOOT /NORESUME`。
3. グループポリシーのスタートアップスクリプトを使用して、スクリプトをマシンを含むOUに割り当てます。このOUには、VDAをインストールしたいマシンのみを含める必要があります。そのOU内のマシンが再起動されると、スクリプトはすべてのマシンで実行されます。サポートされているオペレーティングシステムを持つ各マシンにVDAがインストールされます。

スクリプトを使用してVDAを削除する

1. インストールメディアの\\Support\\AdDeploy\\からサンプルスクリプトUninstallVDA.batを入手します。Citrixは、スクリプトをカスタマイズする前に元のスクリプトのバックアップを作成することを推奨します。
2. スクリプトを編集します。
   - 削除するVDAのバージョンを指定します: `SET CHECK\_VDA\_VERSION`。完全な値は、インストールメディアのProductVersion.txtファイル（例: 7.0.0.3018）に記載されています。ただし、完全一致は必須ではありません。
   - オプションで、集中ログを保存するためのネットワーク共有場所を指定します。
3. グループポリシーのスタートアップスクリプトを使用して、スクリプトをマシンを含むOUに割り当てます。このOUには、VDAを削除したいマシンのみを含める必要があります。OU内の

マシンが再起動されると、スクリプトはすべてのマシンで実行されます。各マシンからVDAが削除されます。

トラブルシューティング

- スクリプトは、スクリプトの実行状況を記述する内部ログファイルを生成します。スクリプトは、展開開始から数秒以内に`Kickoff_VDA_Startup_Script`ログを中央ログ共有にコピーします。これにより、全体的なプロセスが機能していることを確認できます。このログが期待どおりに中央ログ共有にコピーされない場合は、ローカルマシンを検査してさらにトラブルシューティングを行ってください。スクリプトは、各マシンの`%temp%`フォルダーに2つのデバッグログファイルを配置します。

  - `Kickoff_VDA_Startup_Script_<DateTimeStamp>.log`
  - `VDA_Install_ProcessLog_<DateTimeStamp>.log`

  スクリプトが次のことを確認するために、これらのログを確認します。

  - 期待どおりに実行されていること。
  - ターゲットオペレーティングシステムを適切に検出する。
  - `DEPLOYSHARE`共有の`ROOT`を指すように正しく構成されている (`AutoSelect.exe`という名前のファイルが含まれています)。
  - `DEPLOYSHARE`と`LOG`の両方の共有に対して認証できる。

- Citrixがコンポーネントインストールの結果を報告する方法については、Citrixインストールリターンコードを参照してください。
- 配信グループのStudio表示では、**詳細**ペインの**インストール済みVDAバージョン**エントリは、マシンにインストールされているバージョンではない場合があります。マシンのプログラムと機能の表示には、実際のVDAバージョンが表示されます。
- VDAがインストールされた後、Delivery Controllerに登録されるまで、ユーザーにアプリやデスクトップを配信できません。

  VDA登録方法と登録問題のトラブルシューティング方法については、VDA登録を参照してください。

サードパーティ製VDAの展開方法

Microsoft System Center Configuration Manager (SCCM) や、Ansible、Microsoft Intunes などの同様のソフトウェア配布ツールを使用して Virtual Delivery Agent (VDA) を正常に展開するには、Citrix® はVDAインストーラーを段階的に使用することを推奨します。

> **注:**
>
> 以下の記事では、Citrix が環境をテストした方法に基づいた推奨事項のみを説明しています。これらの手順は、必要に応じてカスタマイズできます。Citrix は、お客様のニーズに合わせてこれに必要な更新や調整について責任を負いません。

- SCCM を使用した VDA のインストール
- Ansible を使用した VDA のインストール
- Microsoft Intune を使用した VDA のインストール

SCCM を使用した VDA のインストール

概要

Microsoft Endpoint Configuration Manager (旧称 System Center Configuration Manager (SCCM)) は、企業全体でデバイスとアプリケーションの管理、展開、セキュリティを可能にする Windows 製品です。

> **注:**
>
> 以下の記事では、Citrix® が環境をテストした方法に基づいた推奨事項のみを説明しています。これらの手順は、お客様のニーズに合わせてカスタマイズできます。Citrix は、お客様のニーズに合わせてこれに必要な更新や調整について責任を負いません。

推奨事項

- SCCM または同様のソフトウェア配布ツールを使用して Virtual Delivery Agent (VDA) を正常に展開するには、Citrix は一連の手順での VDA インストーラーの使用を推奨します。
- Citrix は、VDA のインストールまたはアップグレードの一部として VDA Cleanup Utility を使用することを推奨しません。VDA インストーラーが以前に失敗した場合にのみ、VDA Cleanup Utility を使用してください。

始める前に

VDA のインストール中に必要な再起動の回数は、環境によって異なります。例:

- 保留中の更新や以前のソフトウェアインストールからの再起動のために、再起動が必要になる場合があります。

- 他のプロセスによって以前にロックされたファイルは更新が必要になる場合があり、追加の再起動を強制します。
- VDA インストーラーの一部のオプションコンポーネント (Citrix Profile Management や Citrix Files など) は、再起動が必要になる場合があります。
- VDA をアップグレードする場合、それがインストールされているマシンは、セッションなしでメンテナンスモードである必要があります。
- マシンで VDA インストールが初めて実行されると、使用されている VDA インストーラーがそのマシンにコピーされます。 VDA のインストールに関する詳細については、インストーラーを参照してください。

SCCM タスクシーケンサーは、必要なすべての再起動を管理します。

SCCM を使用して VDA を展開するための主要な手順

以下の手順では、仮想マシンに SCCM を使用して VDA を展開する方法について説明します。

1. VDA をインストールする。
2. 組織単位 (OU) を作成する。
3. マシンを検証する。
4. VDA を使用してコンテンツを配布する。

ステップ 1: VDA をインストールする

前提条件をすべて特定した後、**SCCM Task Sequencer** を使用して、以下のタスクを完了します。

1. インストールメディアのアクセス可能なコピーから、またはVDAスタンドアロンインストーラーのいずれかからVDAをインストールします。

   - `VDAWorkstationSetup_XXXX.exe`
   - `VDAServerSetup_XXXX.exe`
   - `VDAWorkstationCoreSetup_XXXX.exe`

   VDA インストーラーの詳細については、インストーラーを参照してください。

> **注:**
>
> VDAをアップグレードする場合、VDAがインストールされているマシンは、セッションがないメンテナンスモードである必要があります。

2. マシンでVDAのインストールが初めて実行されると、使用されているVDAインストーラーがそのマシンにコピーされます。

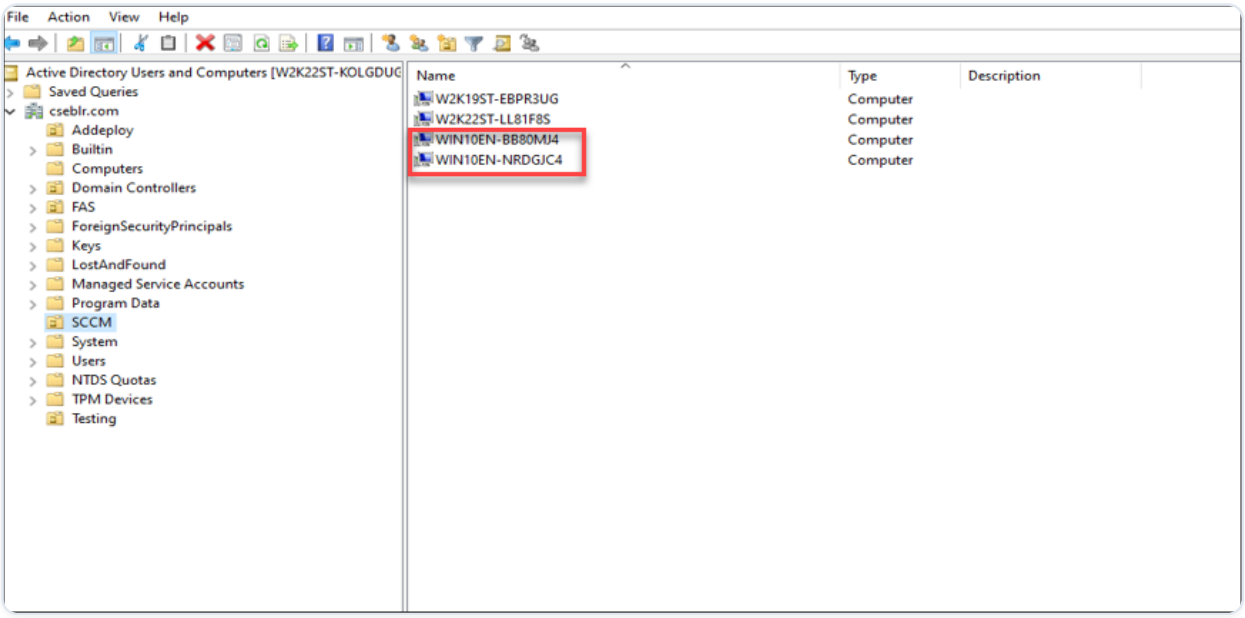
   - `VDAWorkstationCoreSetup_XXXX.exe`以外のVDAインストーラーを使用すると、VDAインストーラーは`%ProgramData%\Citrix\XenDesktopSetup\XenDesktopVdaSetup.exe`にコピーされます。
   - `VDAWorkstationCoreSetup_XXXX.exe`を使用すると、VDAインストーラーは`%ProgramData%\Citrix\XenDesktopSetup\XenDesktopRemotePCSetup.exe.`にコピーされます。

3. VDAインストーラーのディレクトリの場所は、レジストリ`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\MetaInstall”“MetaInstallerInstallLocation”`にも保存されます。
4. コマンドラインオプションに`/NOREBOOT`、`/NORESUME`、および`/QUIET`を追加します。

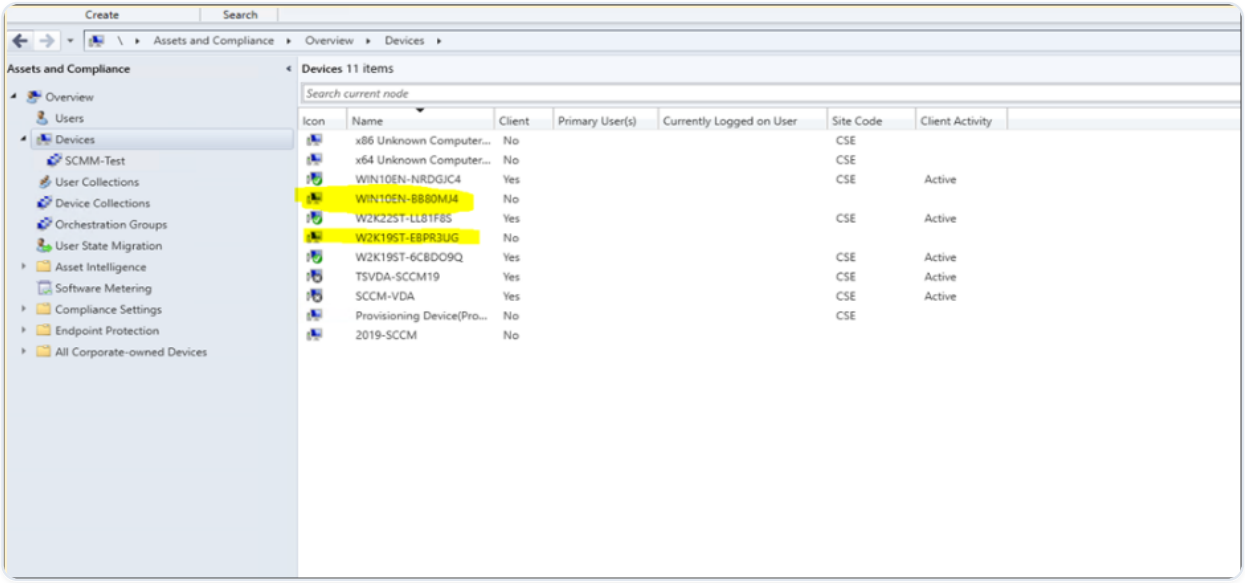
   - `/QUIET`: インストール中にユーザーインターフェイスを表示しないようにします。これにより、SCCMがインストールプロセスを制御できます。
   - `/NOREBOOT`: VDAインストーラーが自動的に再起動するのを抑制します。SCCMは必要に応じて再起動をトリガーします。
   - `/NORESUME`: 通常、インストール中に再起動が必要な場合、VDAインストーラーはrunonceレジストリキー(`\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce`)を設定します。Windowsは、マシンが再起動したときにVDAインストーラーを開くためにこのキーを使用します。これはSCCMにとって問題となります。なぜなら、SCCMはインストールを監視し、終了コードをキャプチャできないためです。

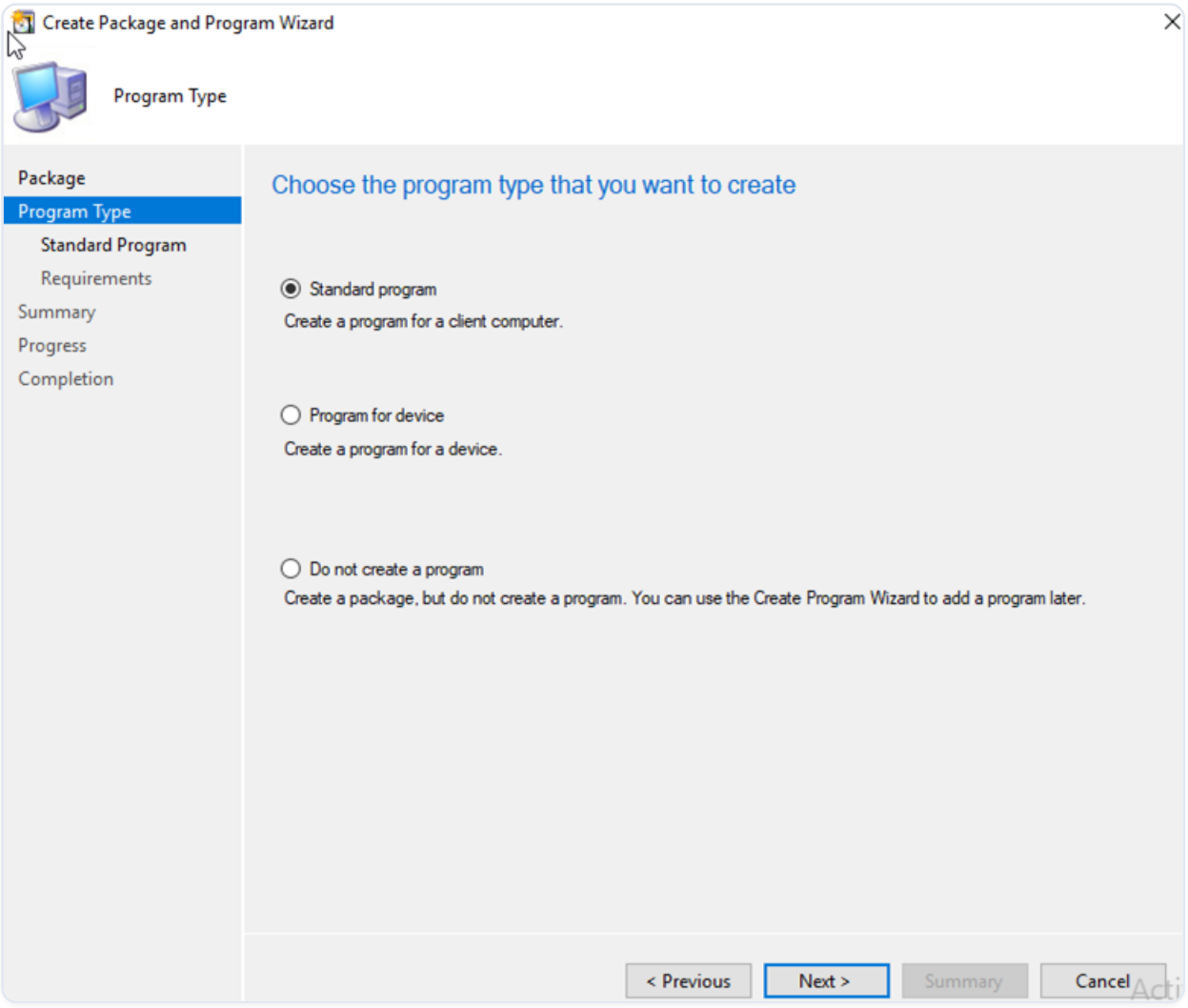
ステップ2: 組織単位 (OU) を作成する

1. OUに追加するドメイン参加済み仮想マシンを2台作成します。仮想マシンが最初に作成されたとき、それらは**Computers**フォルダーにあります。仮想マシンを**SCCM**フォルダーに移動します。 例: WIN10EN-BB80MJ4.cseblr.com W2K19ST-EBPR3UG.cseblr.com

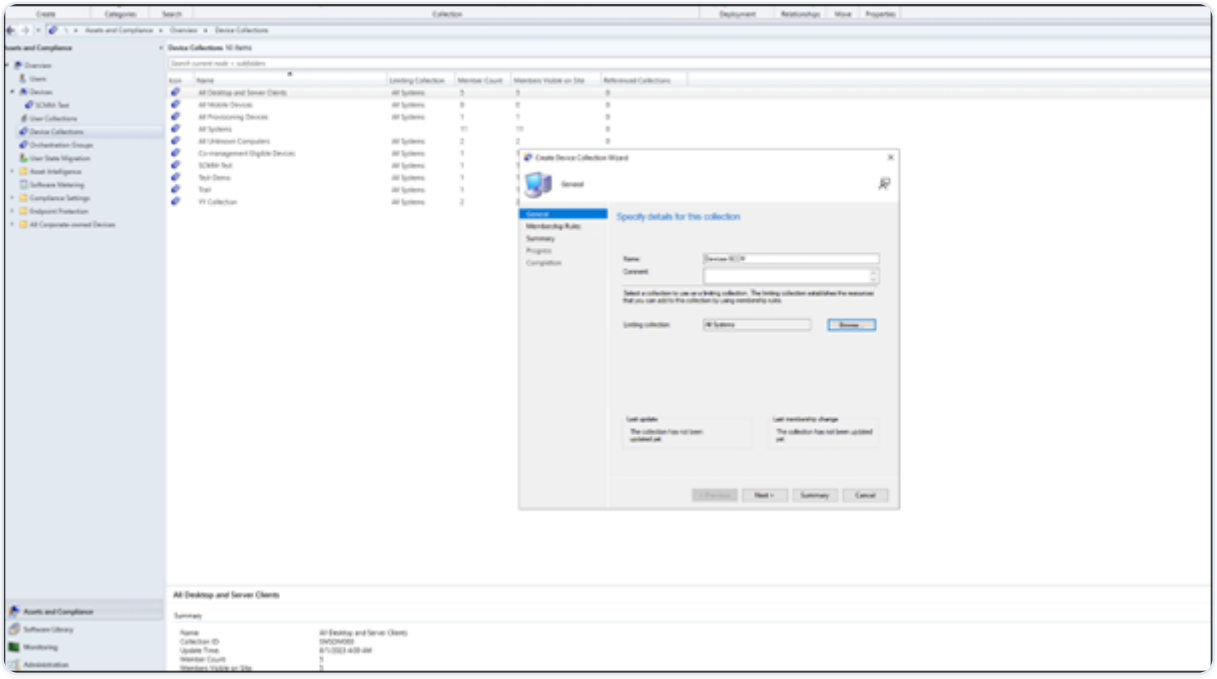


2. Microsoft Configuration Manager で、`\Administration\Overview\Hierarchy Configuration\Discovery Methods\` に移動します。
3. **Active Directory システム検出**をクリックし、**Active Directory システム検出を有効にする**チェックボックスを選択して、新しく作成された仮想マシンの自動検出を有効にします。
4.  アイコンをクリックして、新しいコンテナーを選択します。
5. **場所**セクションで、SCCM 仮想マシンが配置されている**パス**を追加します。
6. `\Administration\Overview\Site Configuration\Sites` に移動し、SCCM VDA を右クリックします。
7. **>** を選択します。「**クライアントプッシュインストールのプロパティ**」ウィンドウが開きます。
8. VM が `Enabled` に設定されると、以下の図に示すように VM のリストが表示されます。





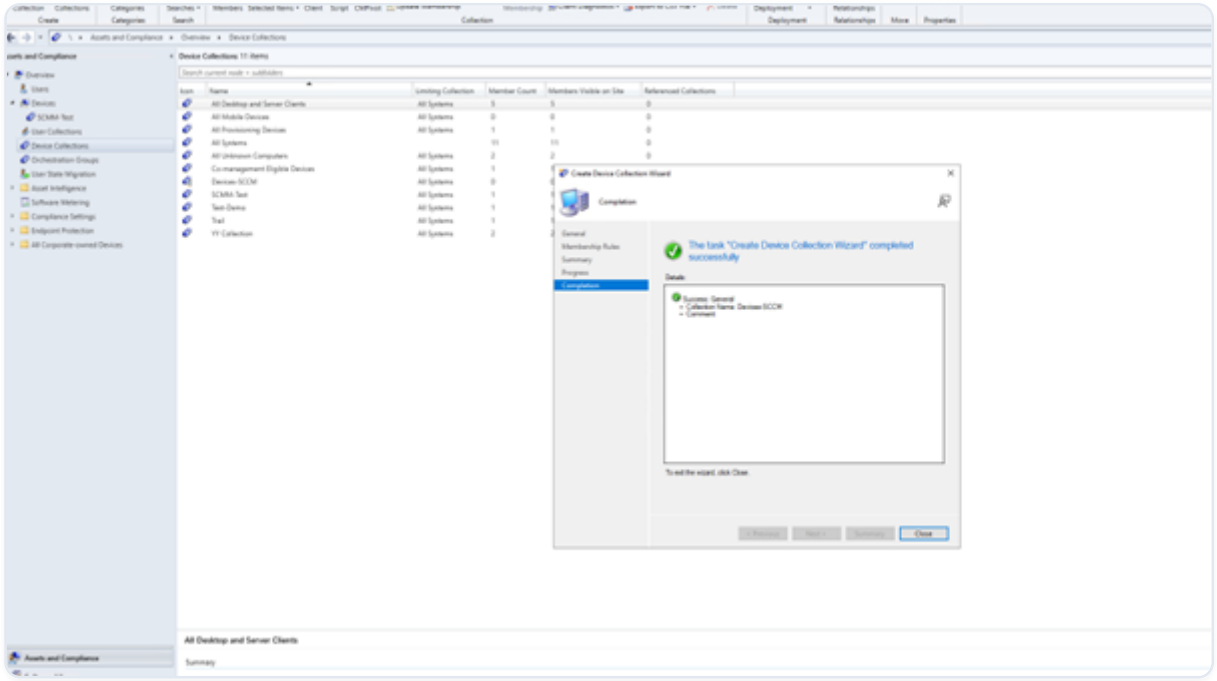
9. OU を作成するには、**デバイスコレクション**を作成します。コレクション名の**名前**を入力します。



10. ウィザードの指示に従います。

メンバーシップルール(/en-us/citrix-virtual-apps-desktops/2503/media/sccm-membership-rules.png)

OU が作成されました。



11. 作成したVMを、新しく作成したデバイスコレクションに追加します。

    a. VM を右クリックします。 **>** を選択します。

    項目の追加(/en-us/citrix-virtual-apps-desktops/2503/media/sccm-add-item-to-device-collection.png)

    b. 「**コレクションの選択**」ウィンドウで、必要なデバイス名を選択します。この例では、`Devices-SCCM` です。

    デバイスリスト(/en-us/citrix-virtual-apps-desktops/2503/media/sccm-list.png)

`Devices-SCCM` は、「**資産とコンプライアンス > 概要 > デバイスコレクション**」に表示されます。

デバイスがリスト表示されました(/en-us/citrix-virtual-apps-desktops/2503/media/devices-sccm.png)

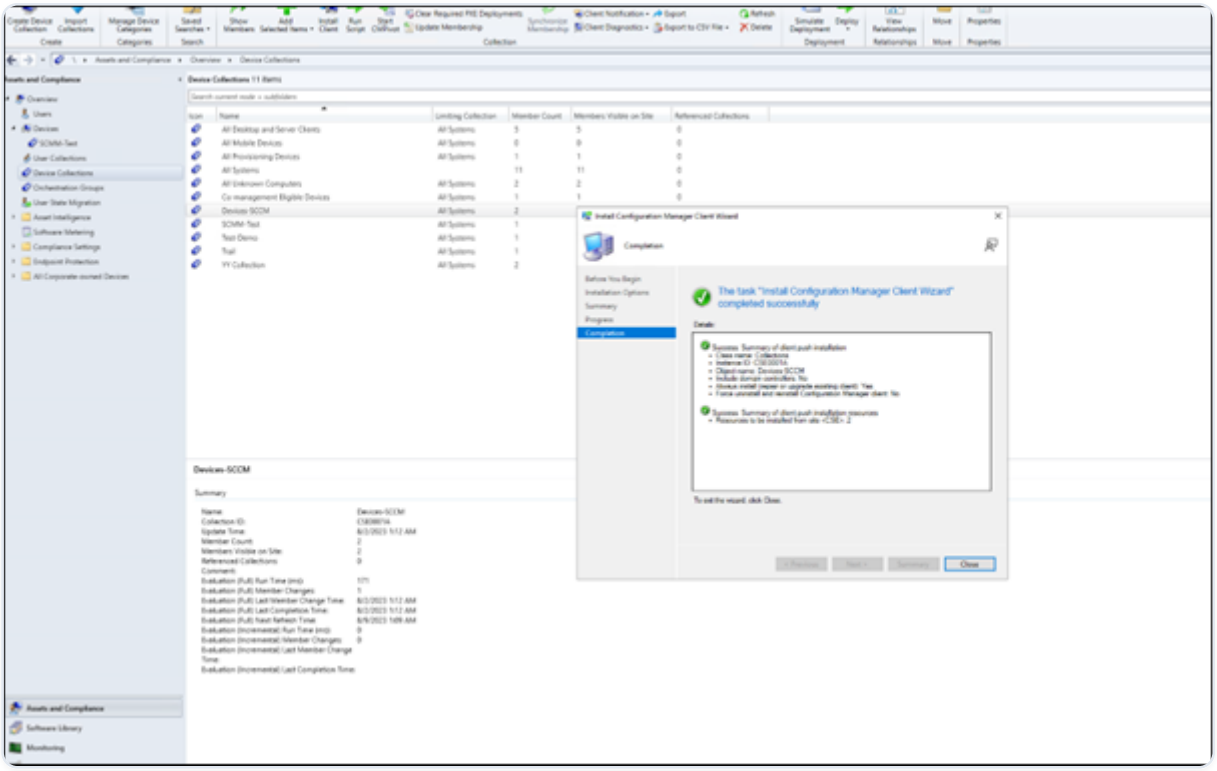
12. デバイスコレクターで「**クライアントのインストール**」を選択します。

    クライアントのインストール(/en-us/citrix-virtual-apps-desktops/2503/media/sccm-install-client.png)

13. 必要なインストール「**サイト**」を選択します。

サイトのインストール(/en-us/citrix-virtual-apps-desktops/2503/media/sccm-install-client-1.png)

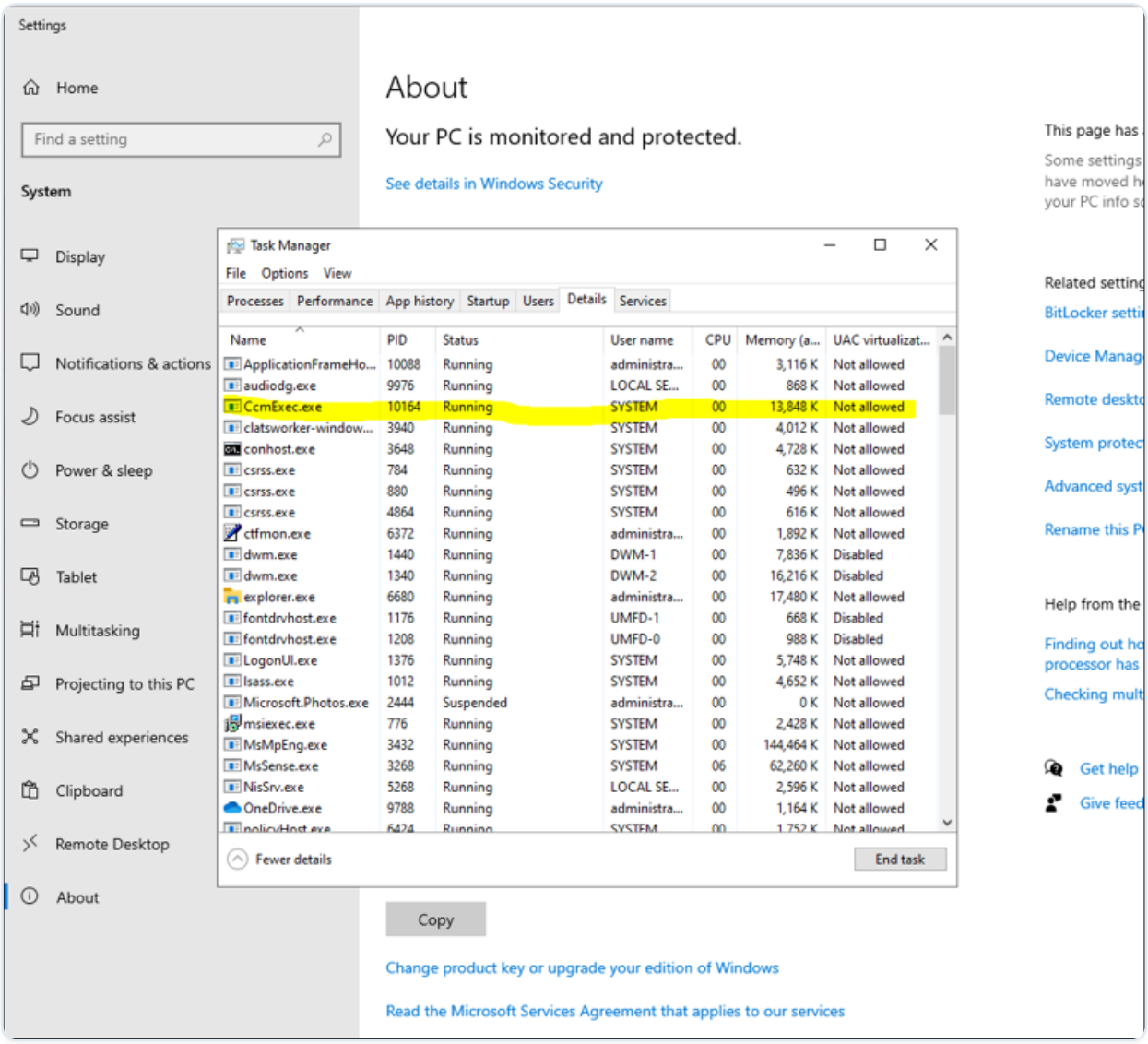
14. ウィザードの指示に従います。**Configuration Manager クライアントのインストールウィザードが正常に完了しました。**



詳細については、Microsoft ドキュメントの コレクションの管理 を参照してください。

ステップ 3: マシンの検証

1. クライアントマシンで、`CCMExec` プロセスが実行されていることを確認して、クライアントがインストールされていることを確認します。



2. SCCM 上の VM でクライアントが実行されていることを確認します。

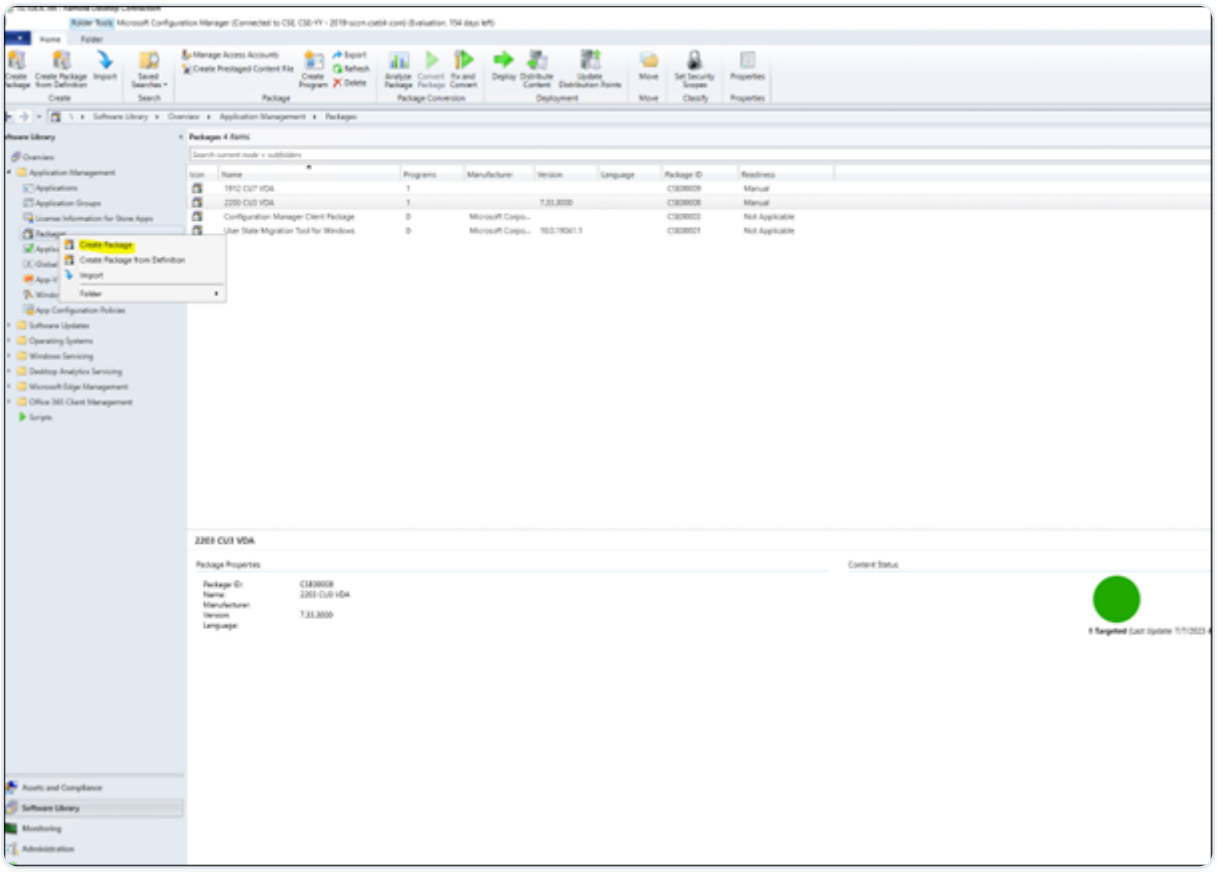
ステップ 4: VDA を使用してコンテンツを配布する

次の手順では、展開された VDA を使用して、関連付けられた仮想マシンにコンテンツを配布する方法について説明します。

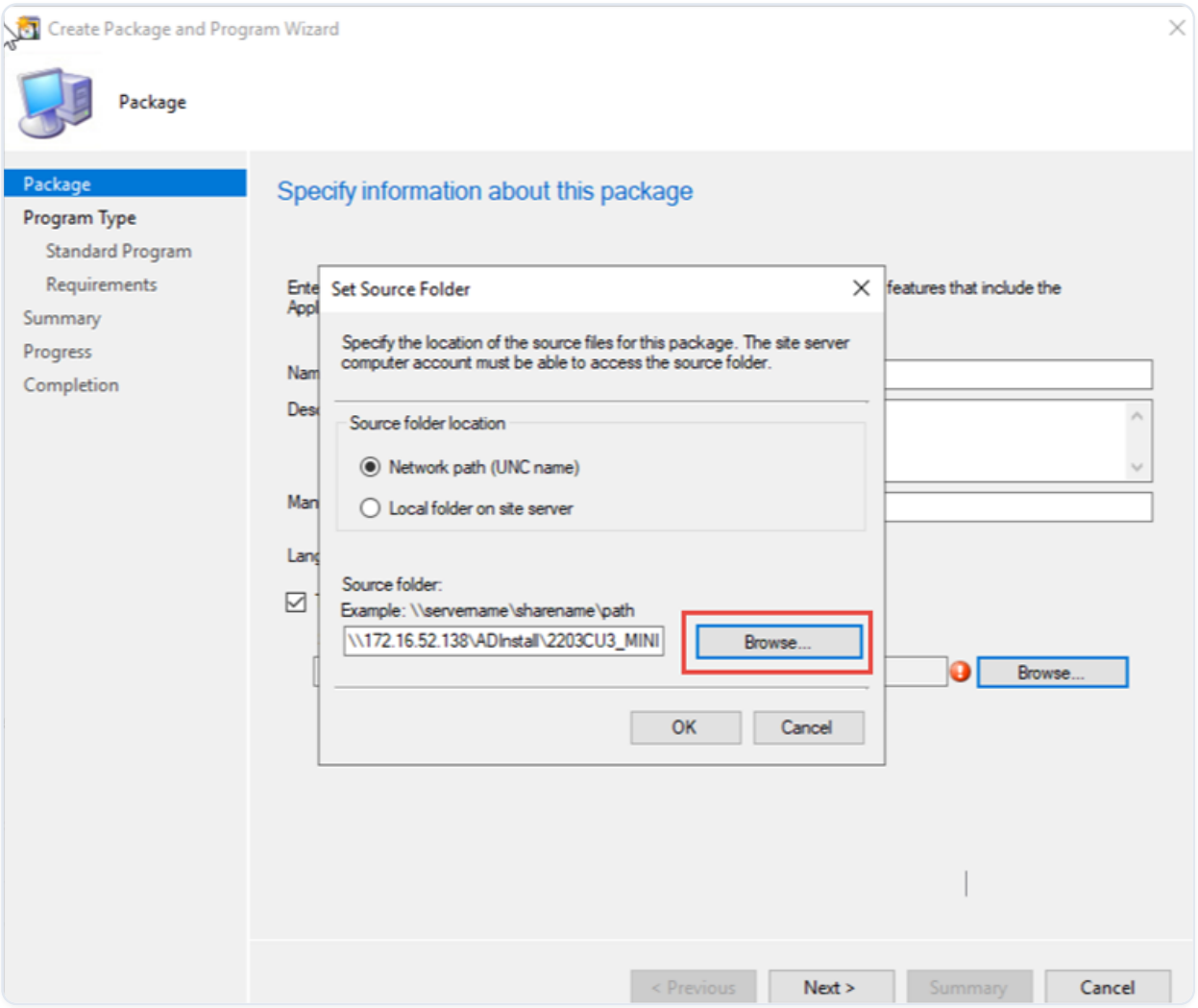
1. パッケージの作成
2. コンテンツの配布

パッケージの作成

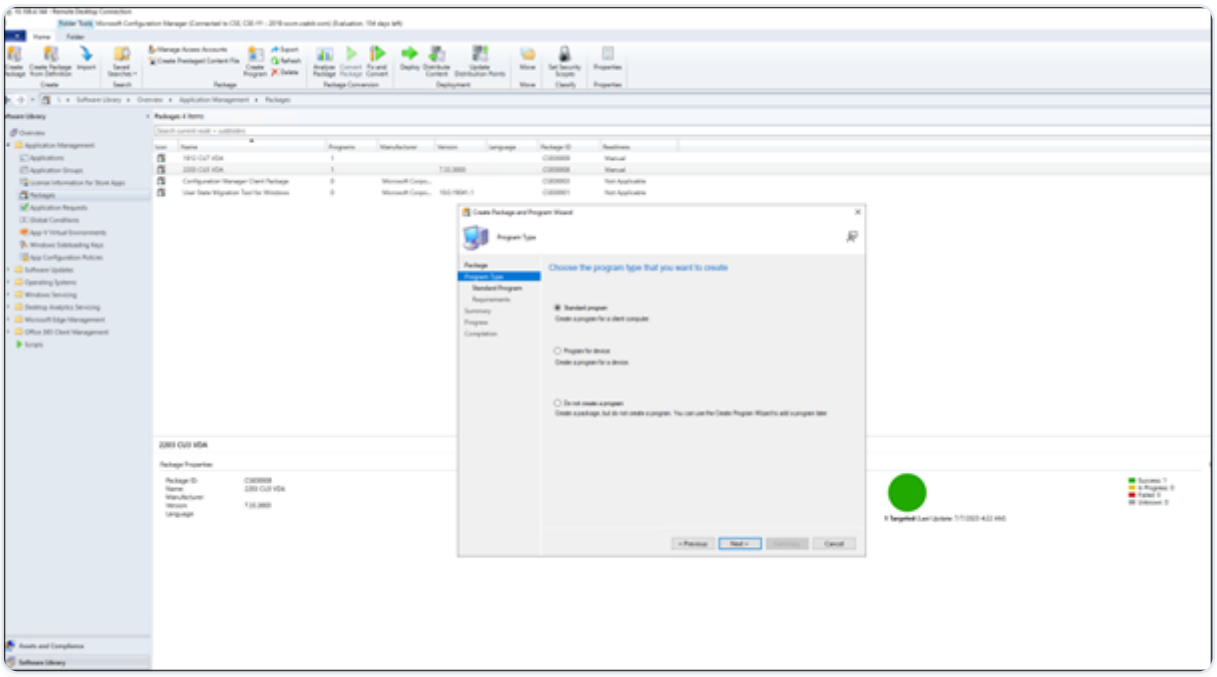
1. パッケージを作成するには、目的の VDA を右クリックし、 をクリックします。



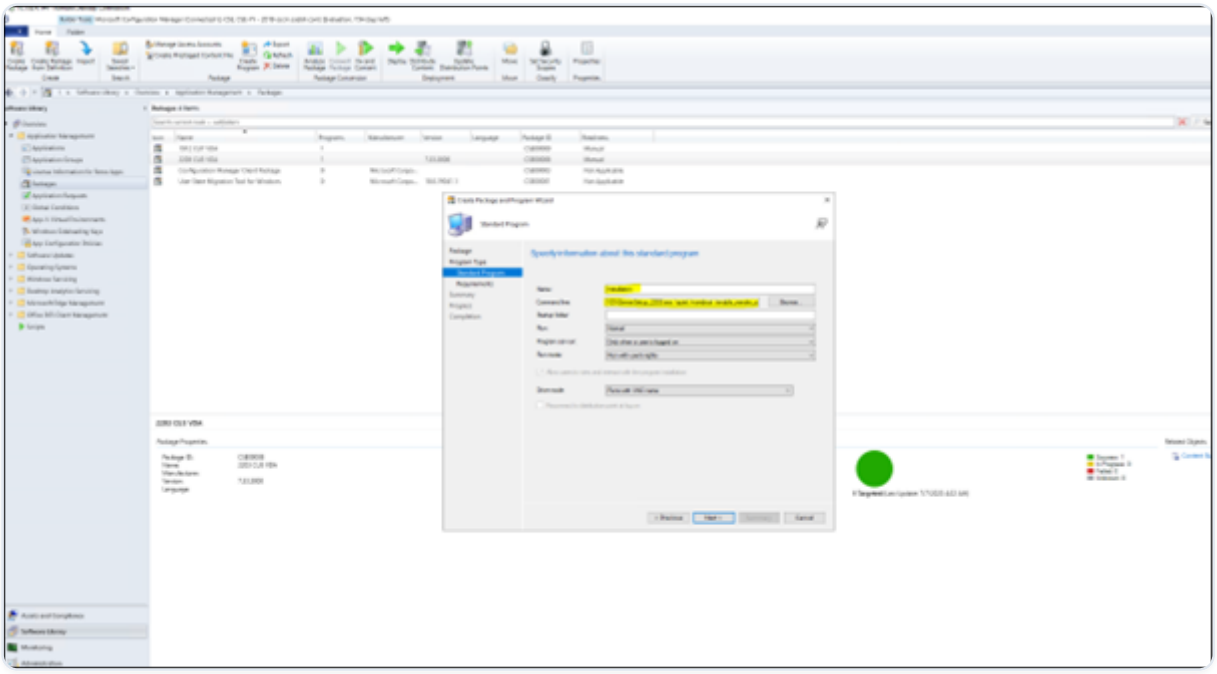
2. をクリックして、このパッケージのソースファイルの場所を指定します。



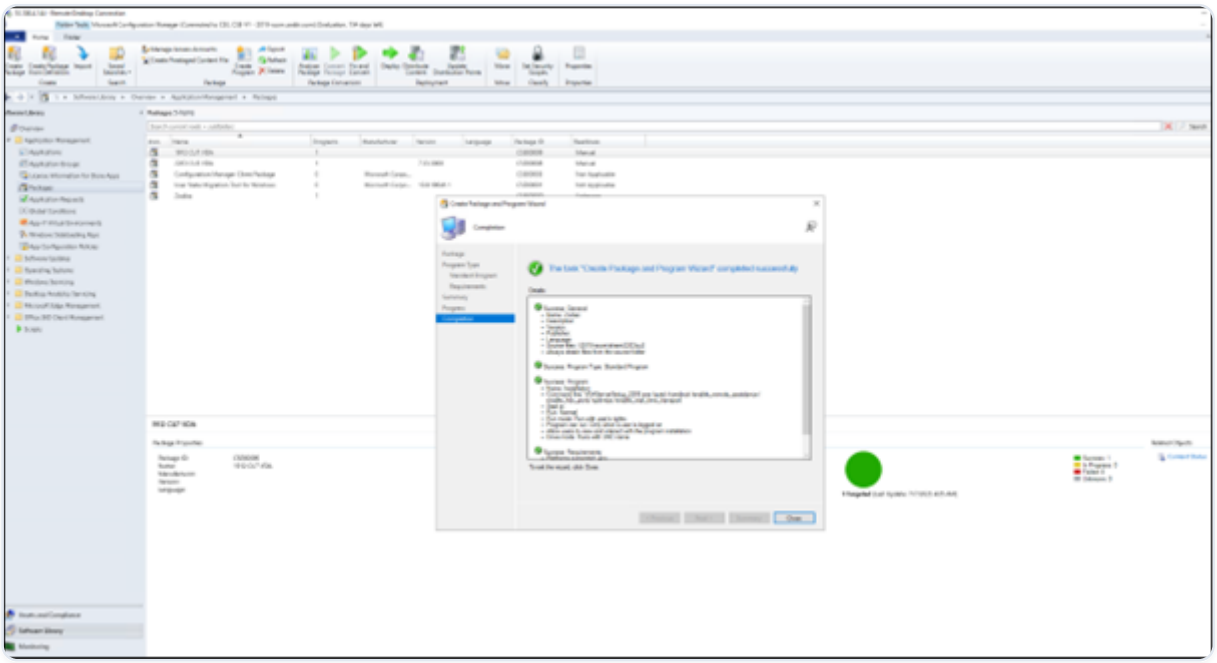
3. 必要なパッケージの種類を選択します。



4. パッケージの**名前**と**コマンドライン**を入力します。



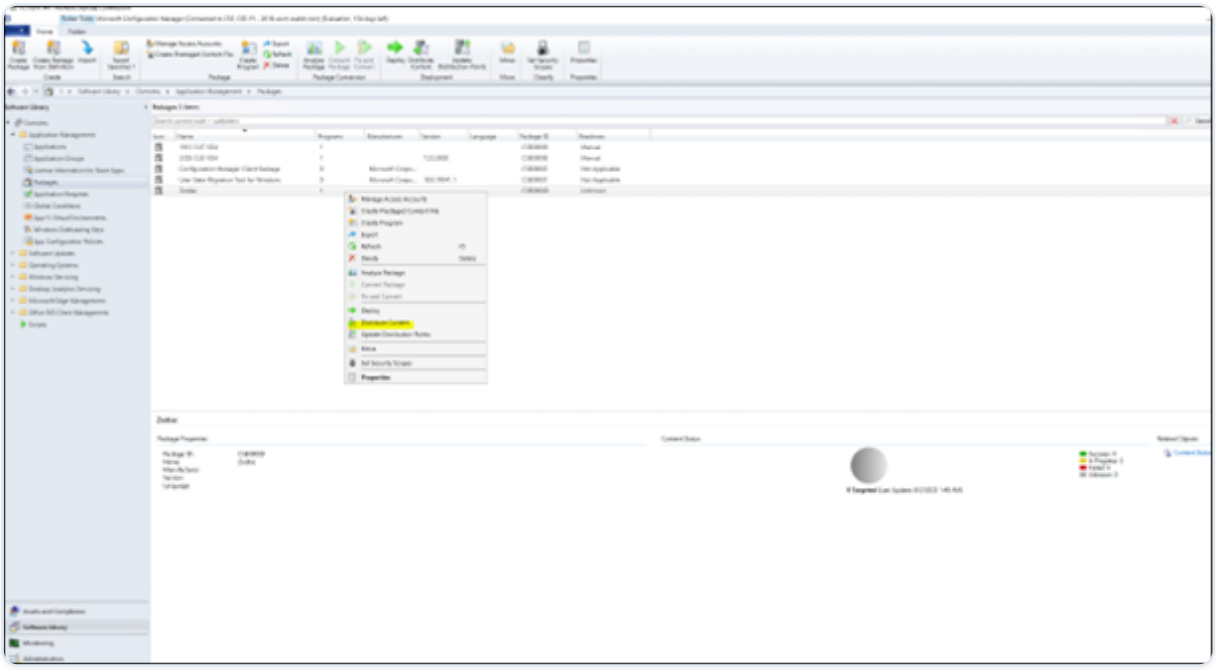
5. **Next**をクリックします。



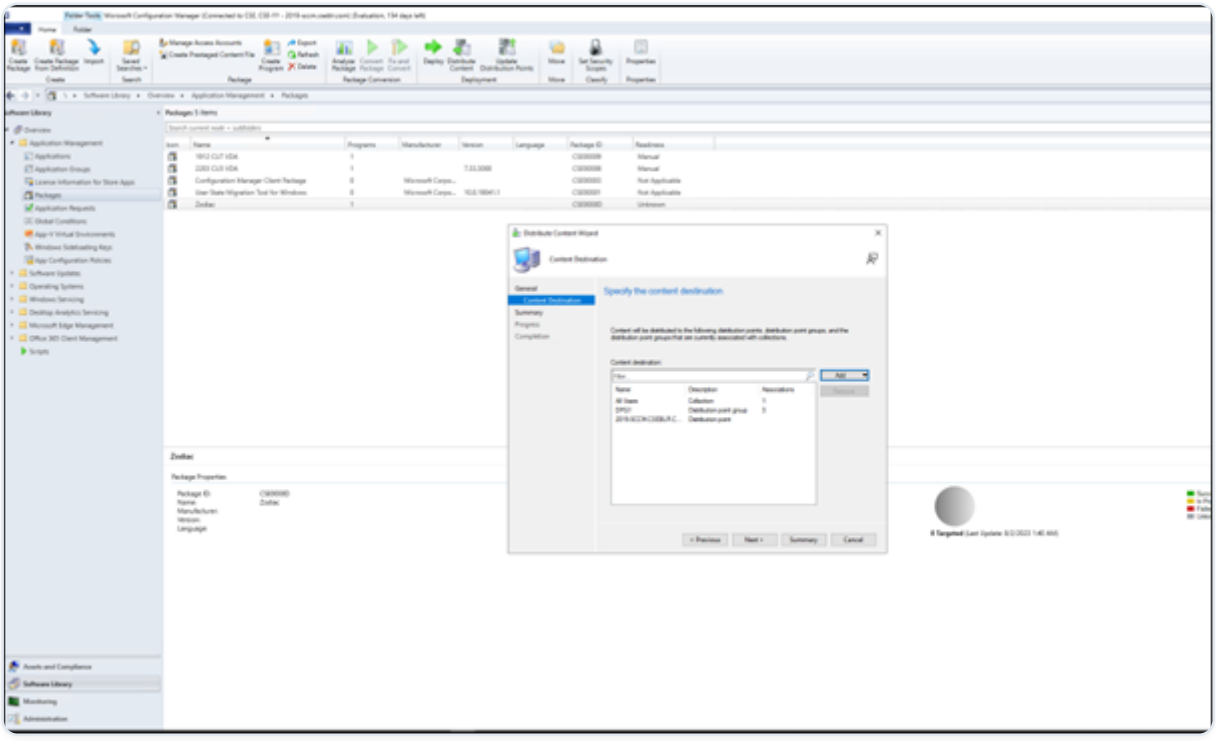
詳細については、Microsoft ドキュメントの「Configuration Manager のパッケージとプログラム」を参照してください。

コンテンツの配布

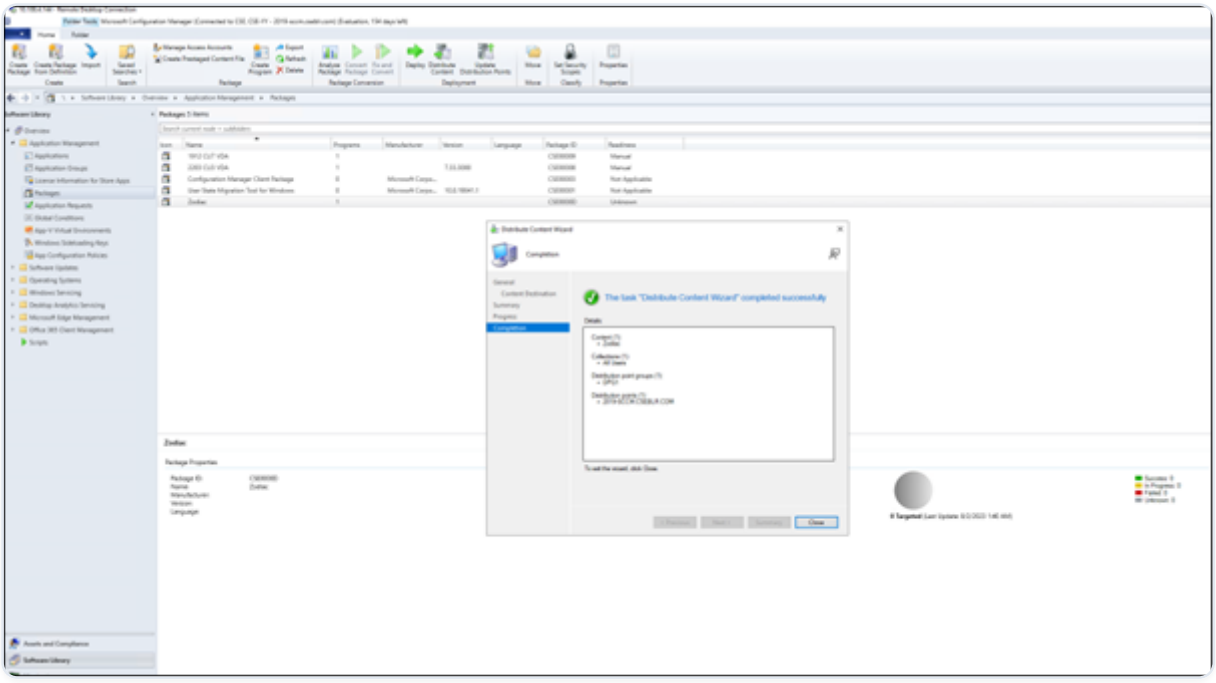
1. 作成したパッケージ名を右クリックします。
2. **コンテンツの配布**を選択します。



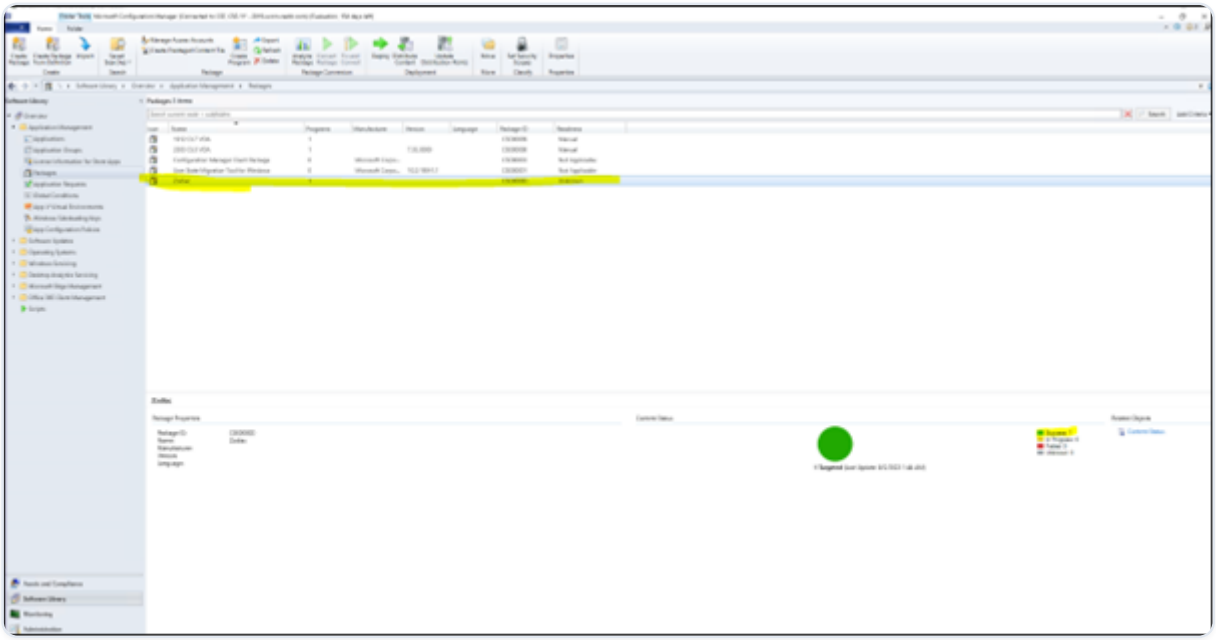
3. **コンテンツの配布ウィザード**ウィンドウで、作成したパッケージのソースファイルの場所を選択します。この例では、`2019-SCCM`です。**次へ**をクリックします。



4. パッケージ（この例では`Zodiac`）が展開可能であることを確認します。



次の図は、パッケージが展開可能であることを示しています。

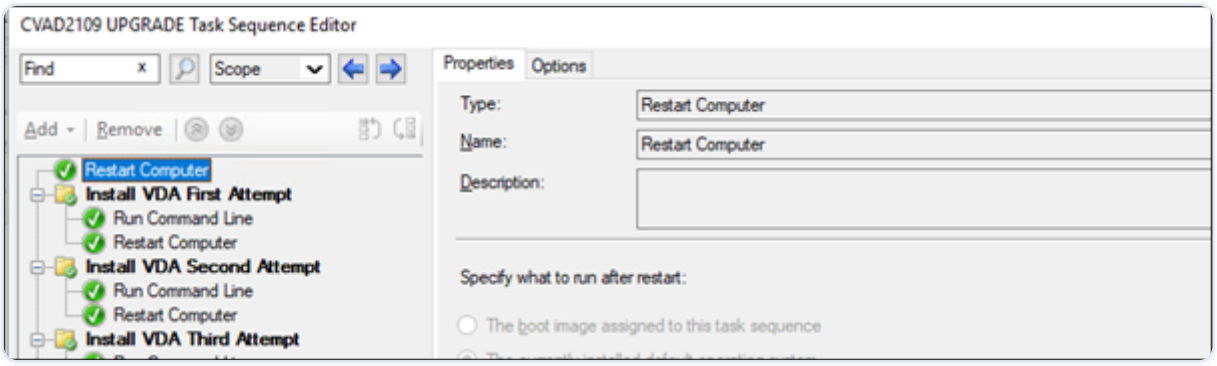


詳細については、Microsoft ドキュメントの「Configuration Manager のコンテンツの展開と管理」を参照してください。

SCCM を使用したインストールシーケンスの例

次の例は、インストールシーケンスを示しています。

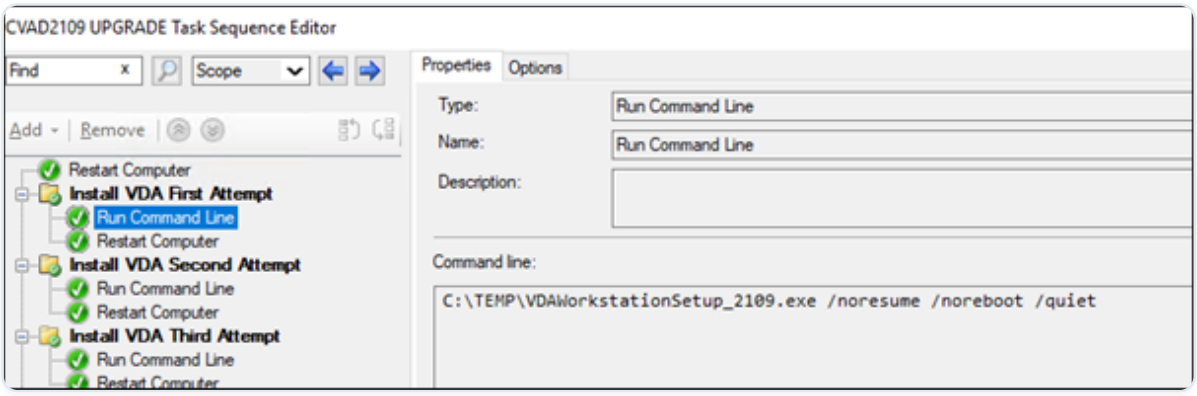
1. **コンピューターの再起動:** マシンを再起動して準備します。



2. **VDA のインストール (初回試行):** VDA のインストールを開始します。

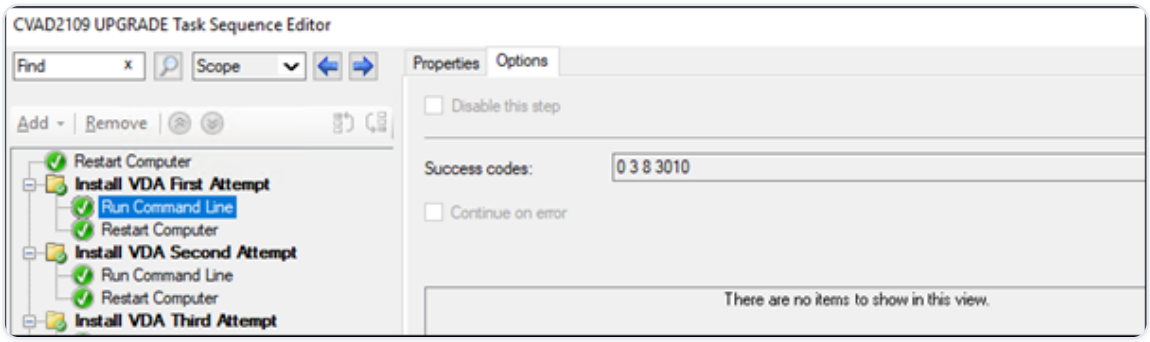
   a. コマンドラインオプションに `/quiet`、`/noreboot`、および `/noresume` オプションを追加します。

   b. 選択した VDA インストーラー (ローカルイメージまたは最小インストーラーのいずれか) を実行します。

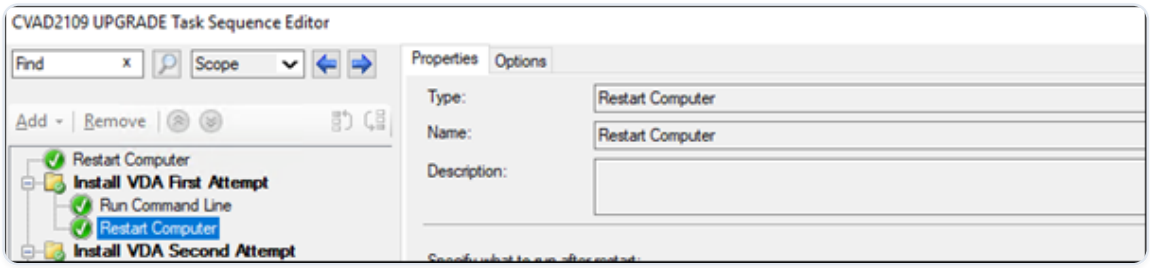


   c. SCCM はリターンコードをキャプチャする必要があります。

   - リターンコードが 0 または 8 の場合、インストールは完了しており、再起動が必要です。



   - リターンコードが 3 の場合は、マシンを再起動してから、**VDA のインストール (2 回目の試行)** に制御を渡します。



3. **VDAの2回目のインストール:** VDAのインストールを続行します。

   a. **VDAのインストール（初回試行）**の後、ファイル `%programdata%\Citrix\XenDesktopSetup\CitrixVirtualDesktopAgent.xml` が存在する場合、インストールは完了しておらず、再起動の完了後に続行する必要があります。



   b. **VDAのインストール（2回目試行）**は、ファイル `%programdata%\Citrix\XenDesktopSetup\CitrixVirtualDesktopAgent.xml` が存在しなくなるか、0または8以外のリターンコードが返されるまで繰り返されます。その他のリターンコードはエラーとして扱い、VDAのインストール（2回目試行）はエラーを報告して停止する必要があります。

   c. コマンドラインパラメーターなしで、ファイル `%programdata%\Citrix\XenDesktopSetup\` ディレクトリから適切なVDAインストーラー（ほとんどの場合 `XenDesktopVdaSetup.exe`、`VDAWorkstationCoreSetup_XXXX.exe` が使用された場合は `XenDesktopRemotePCSetup.exe`）を実行して、VDAのインストールを再開します。（VDAインストーラーは、インストーラーの初回実行時に保存したパラメーターを使用します。）

「アップグレードタスクシーケンスエディター」(/en-us/citrix-virtual-apps-desktops/2503/media/upgrade-task-sequence-editor.png)

   d. VDAインストーラーからのリターンコードに注意してください。

      - 0または8: 成功、インストール完了、再起動が必要。

「成功、インストール完了」(/en-us/citrix-virtual-apps-desktops/2503/media/success-installation-complete.png)

- 3: インストールが完了していません。マシンを再起動し、ファイル `%programdata%\Citrix\XenDesktopSetup\CitrixVirtualDesktopAgent.xml` が存在しなくなるか、0または8が返されるまで INSTALL VDA SECOND ATTEMPT を繰り返します。その他のリターンコードはエラーとして扱い、INSTALL VDA SECOND ATTEMPT はエラーを報告して終了する必要があります。

リターンコードの詳細については、Citrix インストールリターンコード を参照してください。

VDAインストールのコマンド例

利用可能なインストールオプションは、使用するインストーラーによって異なります。コマンドラインオプションの詳細については、以下の記事を参照してください。

- VDAのインストール
- コマンドラインを使用したインストール

REMOTE PC ACCESS 用のインストールコマンド

- 次のコマンドは、シングルセッションコア VDA インストーラー (`VDAWorkstationCoreSetup.exe`) を使用します。

  ```
  VDAWorkstationCoreSetup.exe /quiet /controllers “control.domain.com” /enable_hdx_ports /noresume /noreboot
  ```

- 次のコマンドは、シングルセッションフル VDA インストーラー (`VDAWorkstationSetup.exe`) を使用します。

  ```
  VDAWorkstationSetup.exe /quiet /remotepc /physicalmachine /controllers “control.domain.com” /enable_hdx_ports /noresume /noreboot
  ```

専用 VDI のインストールコマンド

- 次のコマンドは、シングルセッションの完全なVDAインストーラー (`VDAWorkstationSetup.exe`) を使用します:

  ```
  VDAWorkstationSetup.exe /quiet /components vda /controllers “control.domain.com” /enable_hdx_ports /enable_remote_assistance /noresume /noreboot
  ```

Microsoft Intune を使用して VDA をインストールする

概要

この記事では、Microsoft Intune を使用して VDA を展開する方法について説明します。詳細については、Microsoft のドキュメントを参照してください。

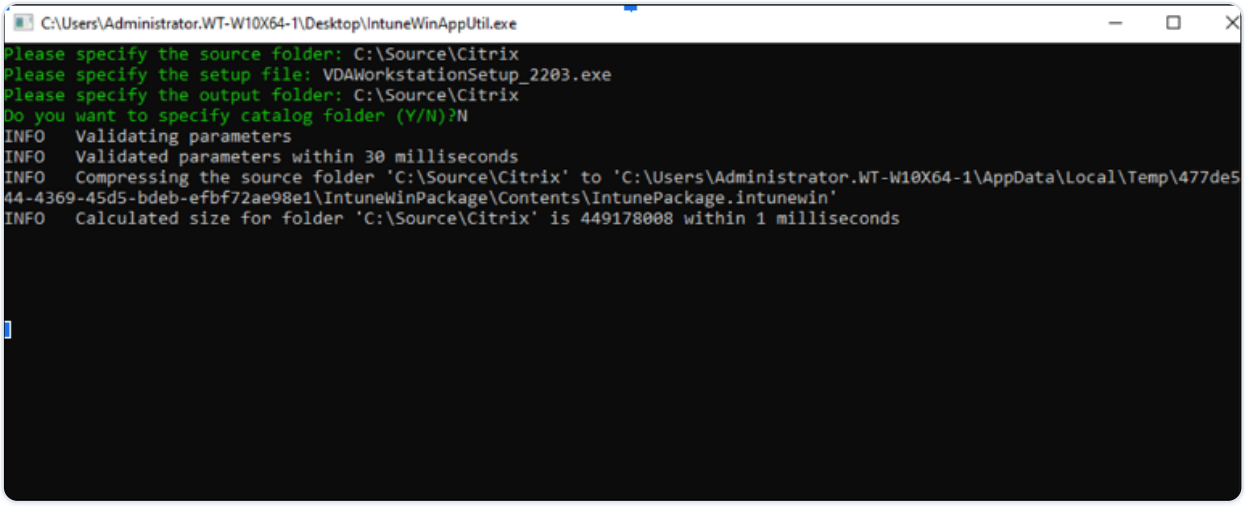
> **注:**
>
> 以下の記事は、Citrix® が環境をテストした方法に基づいた推奨事項のみを説明しています。これらの手順は、お客様のニーズに合わせてカスタマイズできます。Citrix は、お客様のニーズに合わせてこれに必要な更新や調整について責任を負いません。

Microsoft Intune を使用して VDA を展開するための主要な手順

1. Citrix VDA のインストールを準備する。
2. Microsoft 365 開発者プログラムのサブスクライバーを設定する。
3. アプリを追加して割り当てる。
4. 登録済みデバイスにアプリをインストールする。

ステップ 1: CITRIX VDA のインストールを準備する

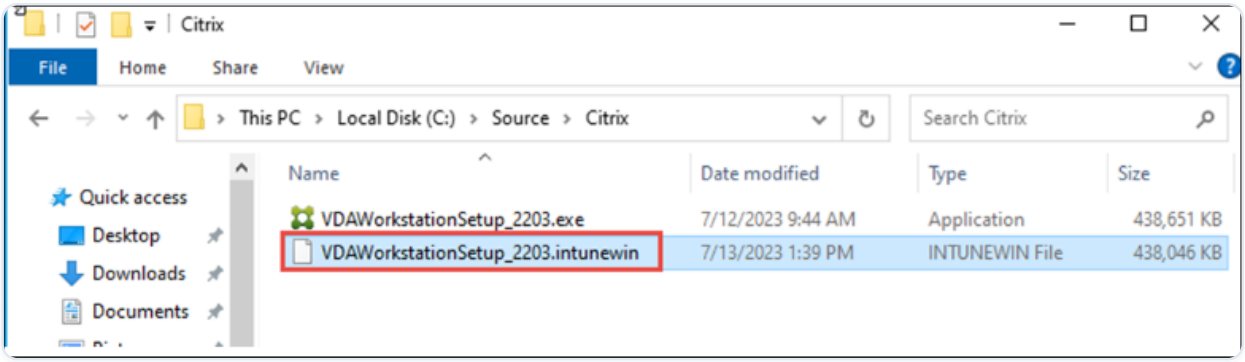
1. 更新された IntuneWinAppUtil.exe を GitHub からダウンロードします。
2. **管理者として実行**を使用して、`IntuneWinAppUtil.exe` ファイルを実行します。
3. 次のデータを入力します。



   a. **ソースフォルダーを指定してください**: アプリケーションのセットアップファイルが含まれているフォルダーを入力します。例: C:\source\Citrix。
   b. **セットアップファイルを指定してください**: セットアップファイル名 (setup.exe や setup.msi など) を入力します。例: VDAWorkstationSetup_2203.exe。
   c. **出力フォルダーを指定してください**: .intunewin ファイルを生成する出力フォルダーのパスを入力します。例: C:\source\Citrix。
   d. **カタログフォルダーを指定しますか (Y/N)**: N と入力します。

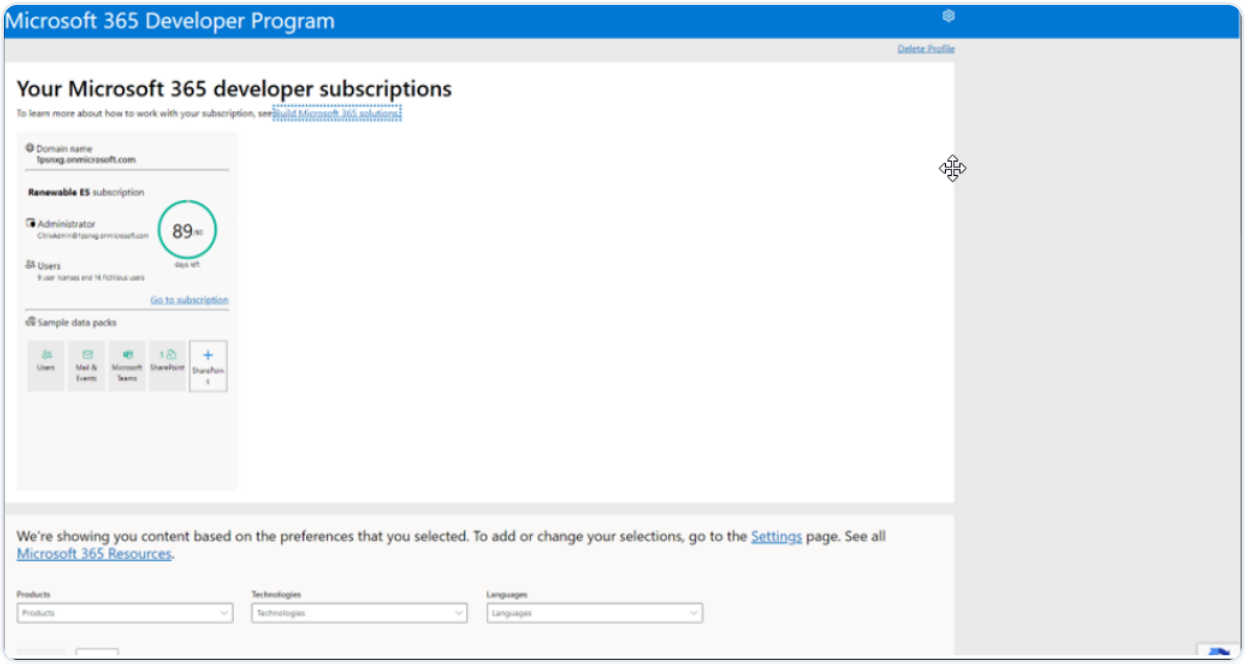
> **注:**
>
> **Win32 Content Prep Tool** の実行中に数分間お待ちください。`.intunewin` ファイルが生成されると、コマンドプロンプトの下部にステータスが 100% と表示されます。

4. プロセスが完了したら、出力フォルダー (この例では `C:\source\Citrix`) に移動して、Microsoft Intune 展開ファイルを取得します。
5. Microsoft Intune の無料試用版にサインアップします。

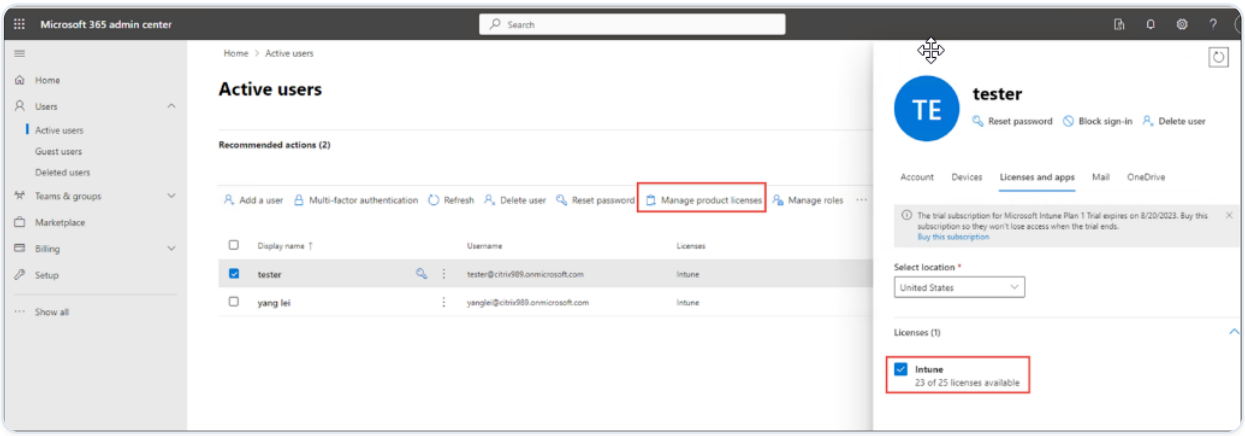


ステップ 2: MICROSOFT 365 DEVELOPER PROGRAM サブスクライバーをセットアップする

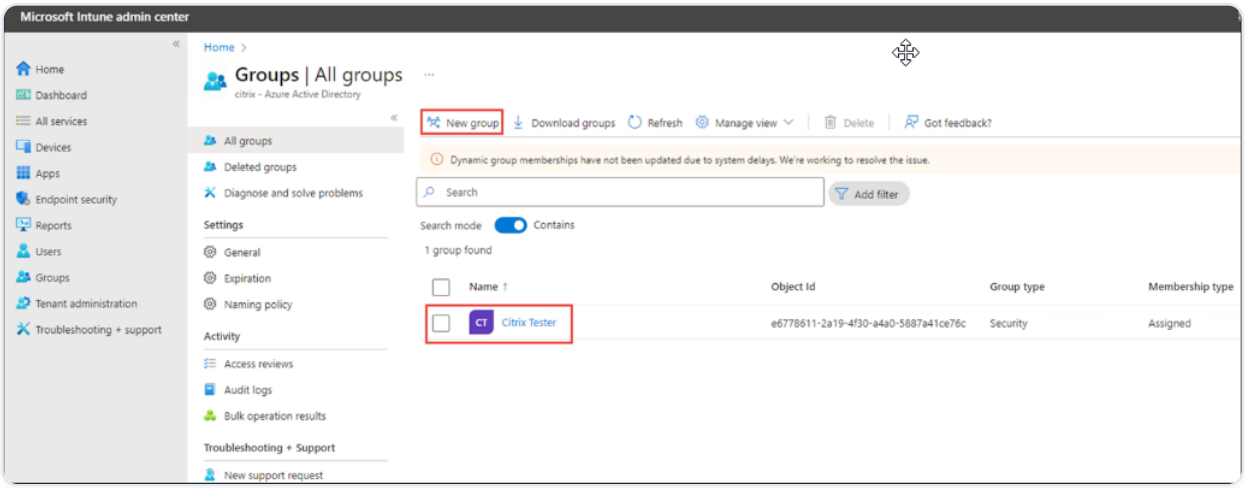
1. サブスクリプションをアクティブ化するために、インスタントサンドボックスを作成します。開発者サンドボックスを取得するには、Microsoft 365 Developer Program ダッシュボード にアクセスし、**Add a new subscription** を選択します。



2. Microsoft 365 管理センターでユーザーを作成し、そのユーザーにライセンスを割り当てます。



3. グループを作成します。



4. グループが作成されたら、そのグループにMDM機関を提供する必要があります。自動登録を設定します。アクティブ化には1分ほどかかる場合があります。 または、以下の手順を完了することで、MDM機関をグループに手動で追加することもできます。

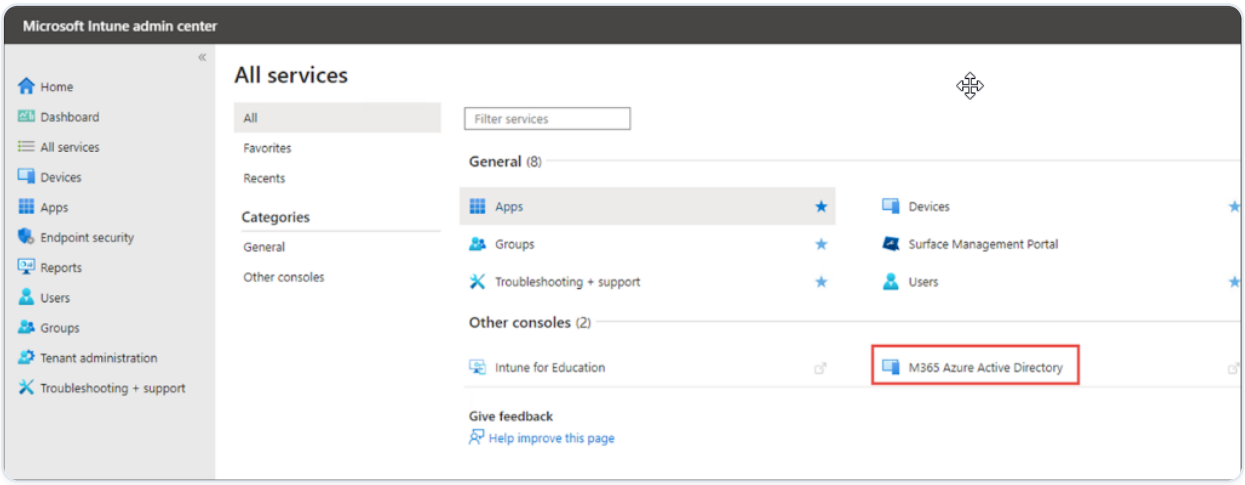
   a. **すべてのサービス > Microsoft Entra** に移動します。

   b. 「**設定 > モビリティ**」に移動し、「**Microsoft Intune**」を選択します。

   c. 作成したばかりのグループを選択します。これにより、MDMユーザー範囲のページが開きます。

   d. 「**保存**」をクリックします。

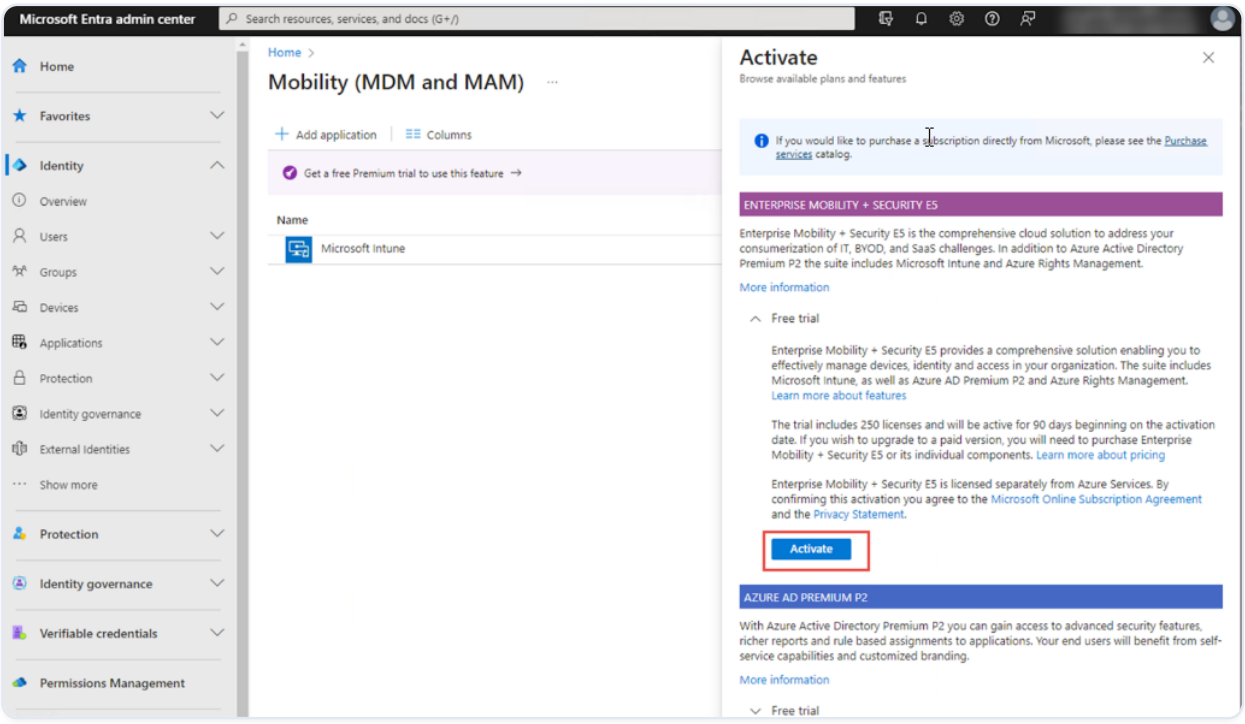
5. 「**すべてのサービス**」タブで、「**M365 Azure Active Directory**」をクリックします。



6. 「**この機能を使用するための無料Premium試用版を入手**」をクリックします。



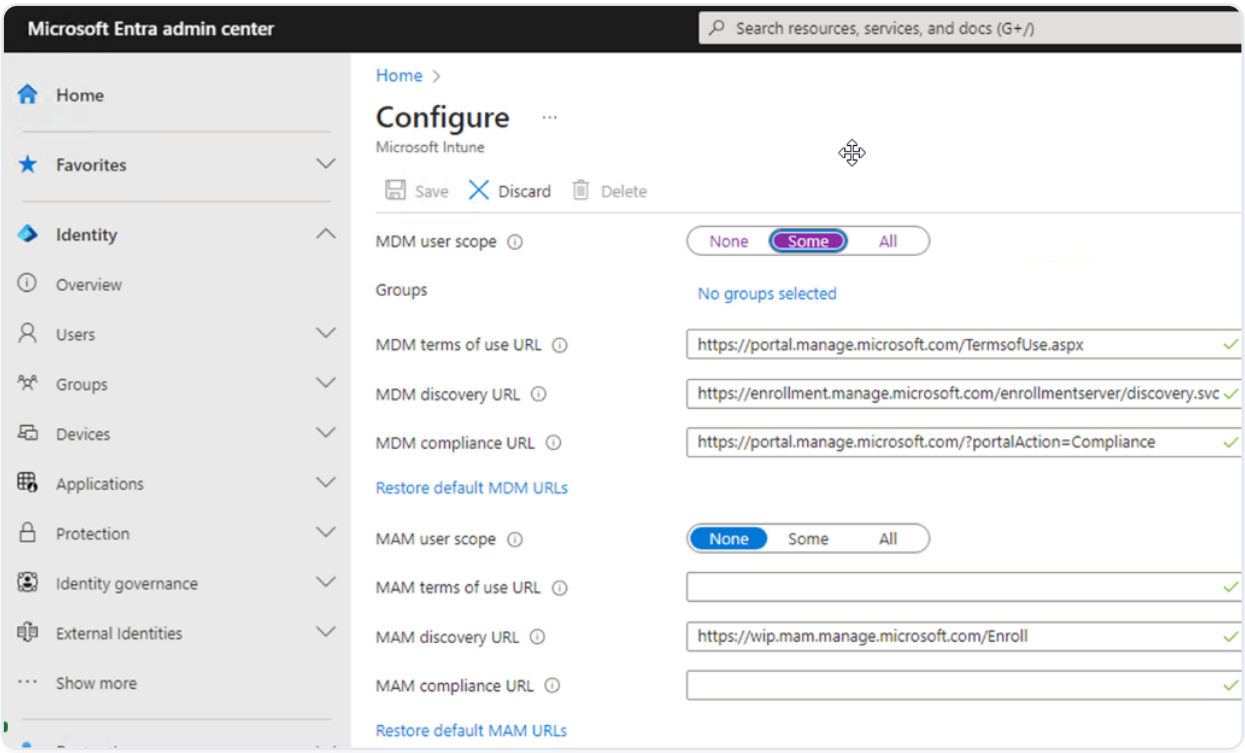
7. 「**アクティブ化**」をクリックします。



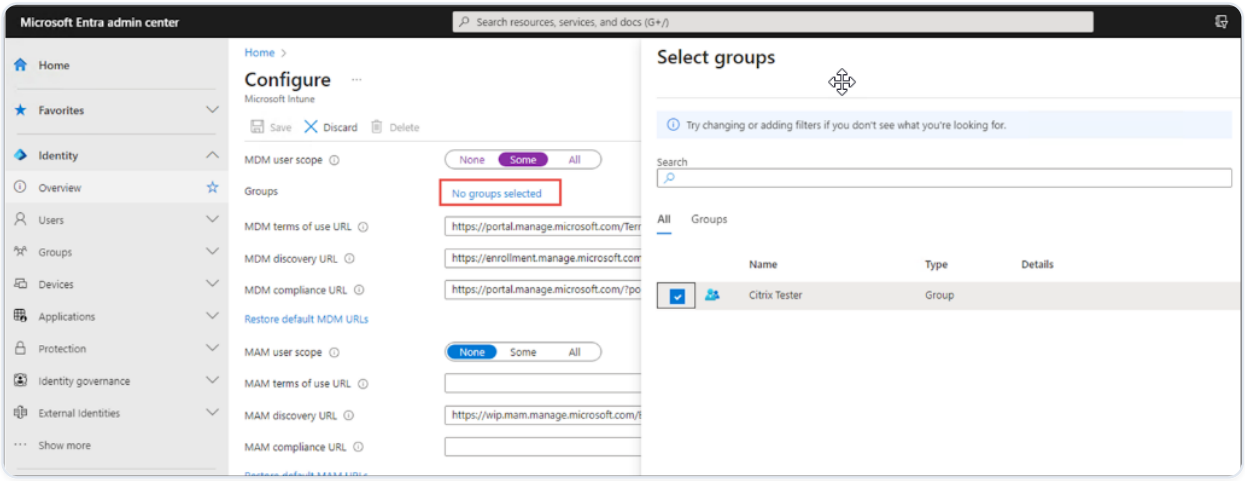
8. 次に、「**Microsoft Intune**」をクリックします。

「MS Intune の選択」(/en-us/citrix-virtual-apps-desktops/2503/media/select-ms-intune.png)

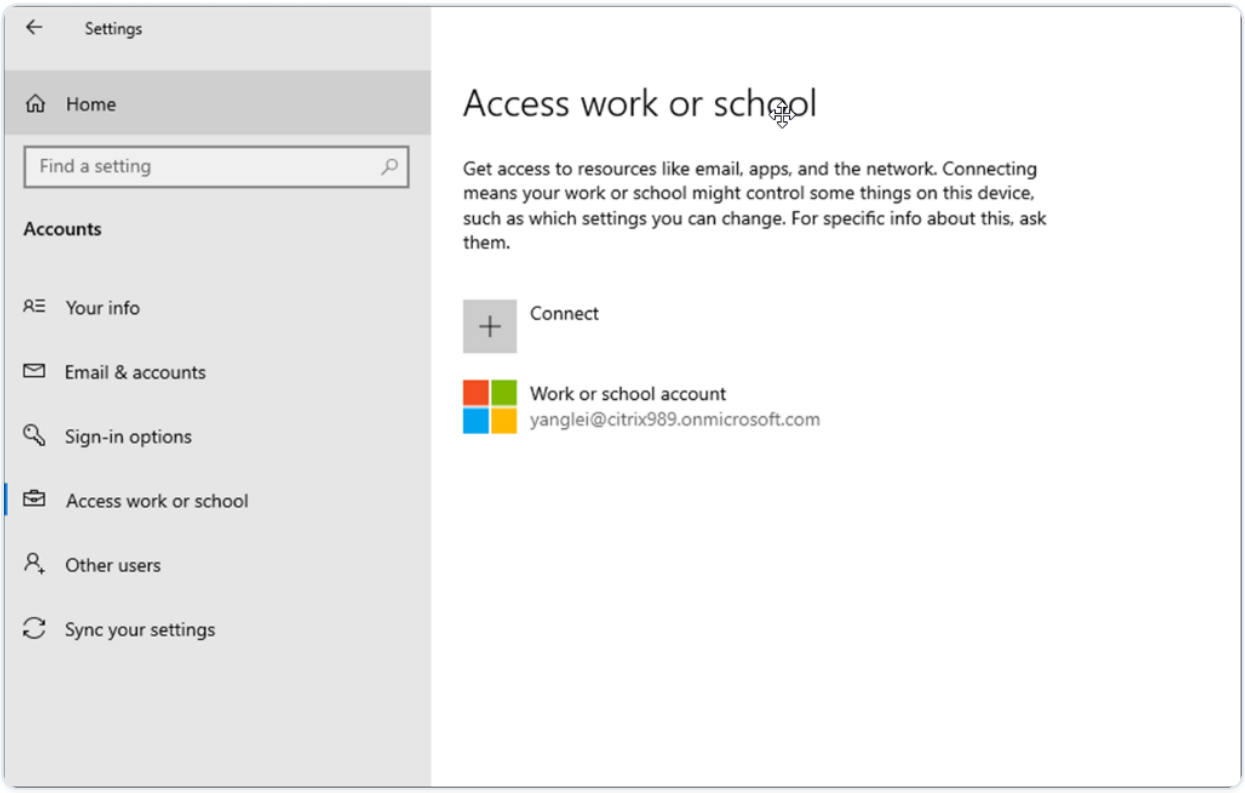
9. 「**構成**」タブで、必要な構成を入力します。



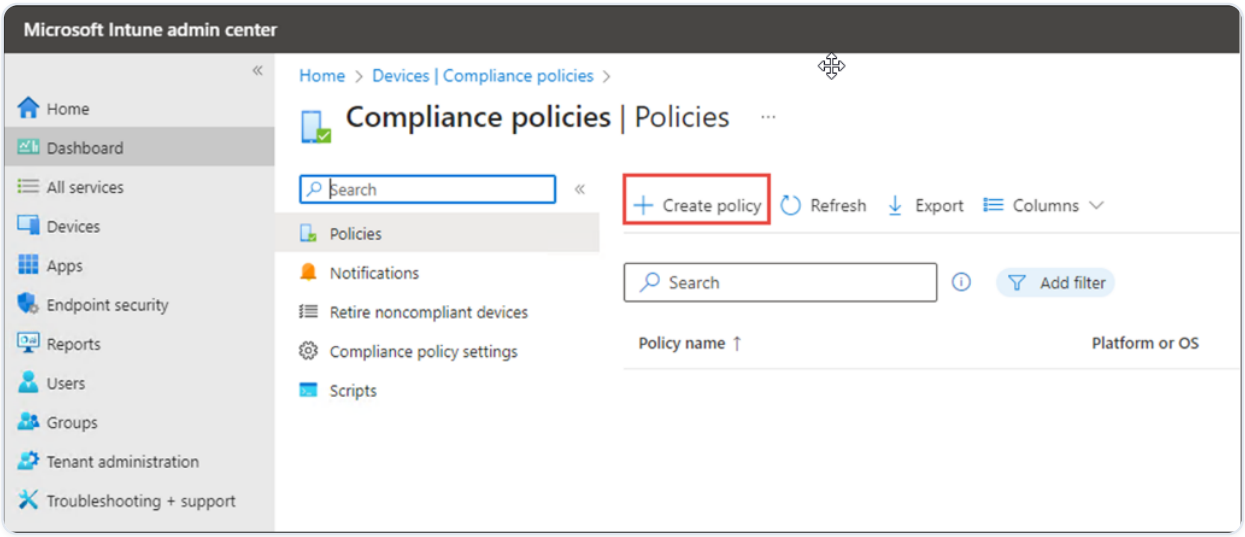
10. グループを追加するには、「**グループが選択されていません**」をクリックします。



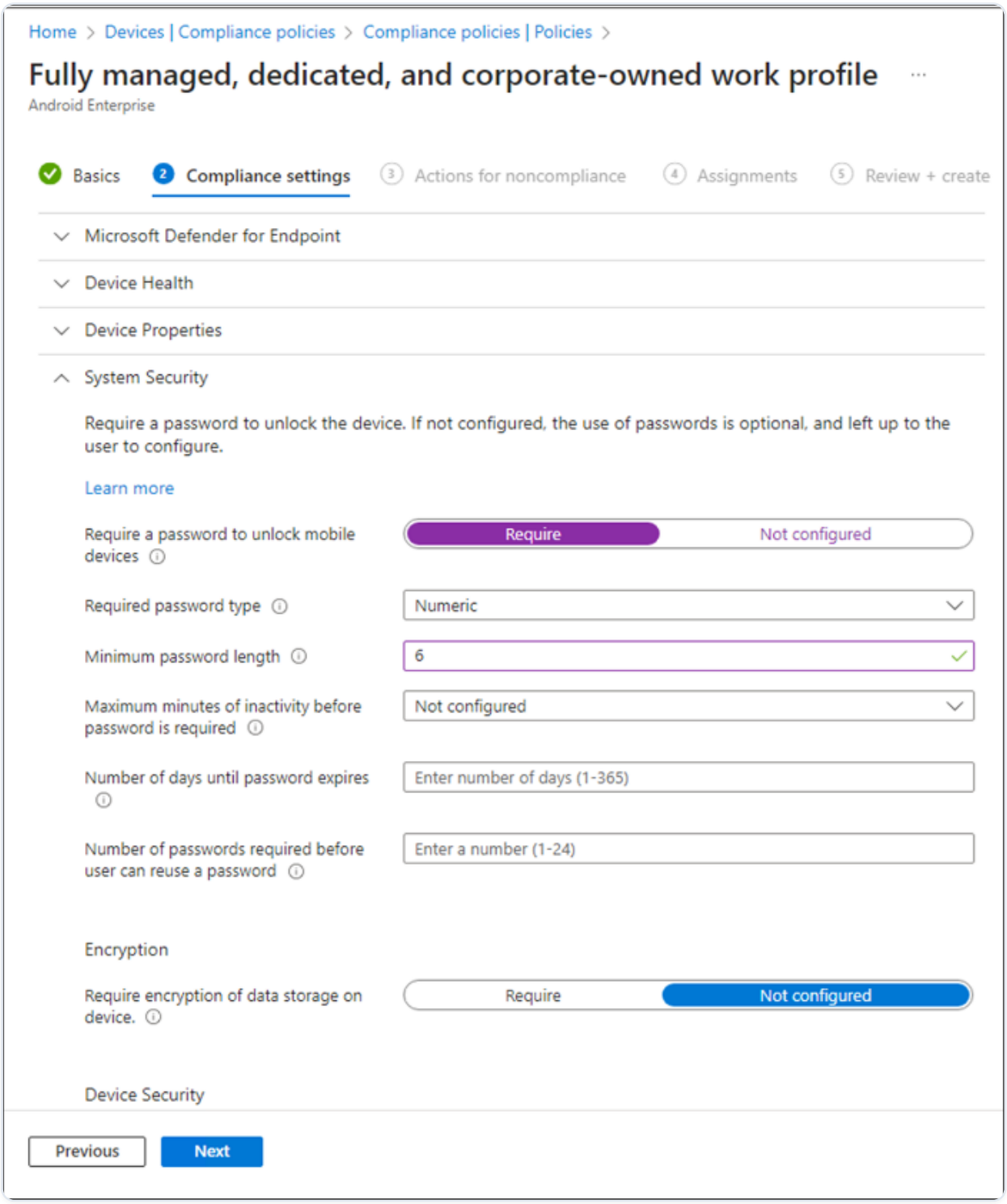
11. デバイスを登録します。



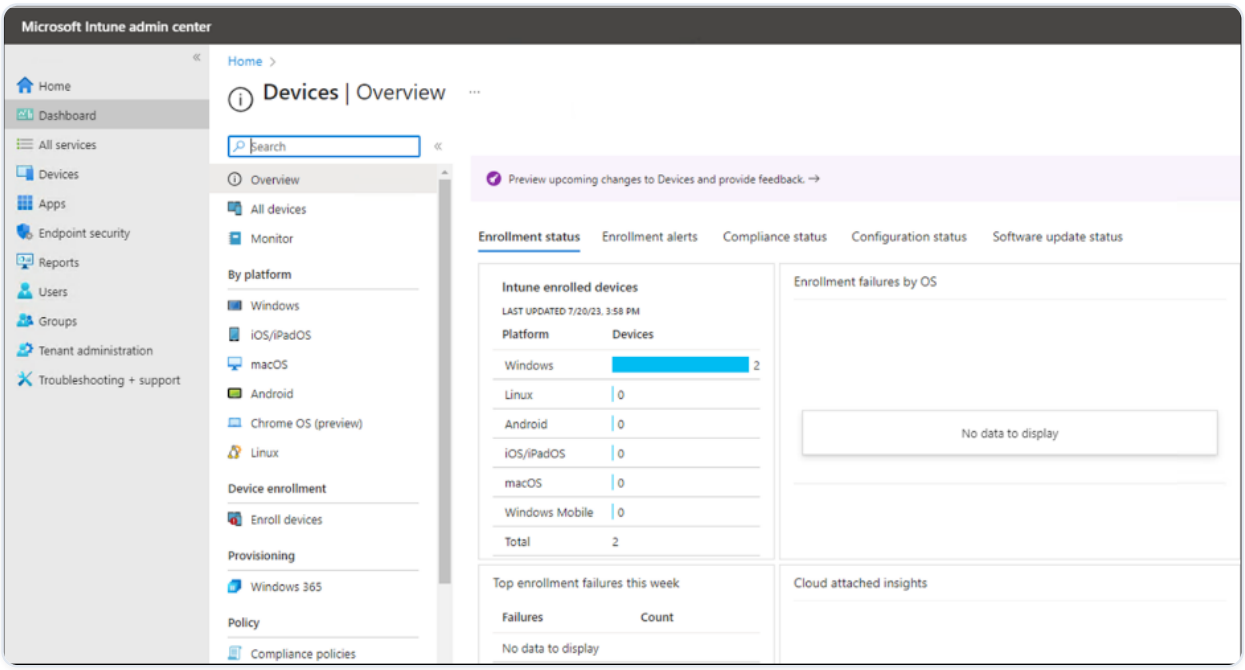
12. 新しく作成したデバイスのコンプライアンスを`Compliant`に変更するためのデバイスコンプライアンスポリシーを作成します。



13. 新しく作成したグループを追加するには、 タブに移動します。



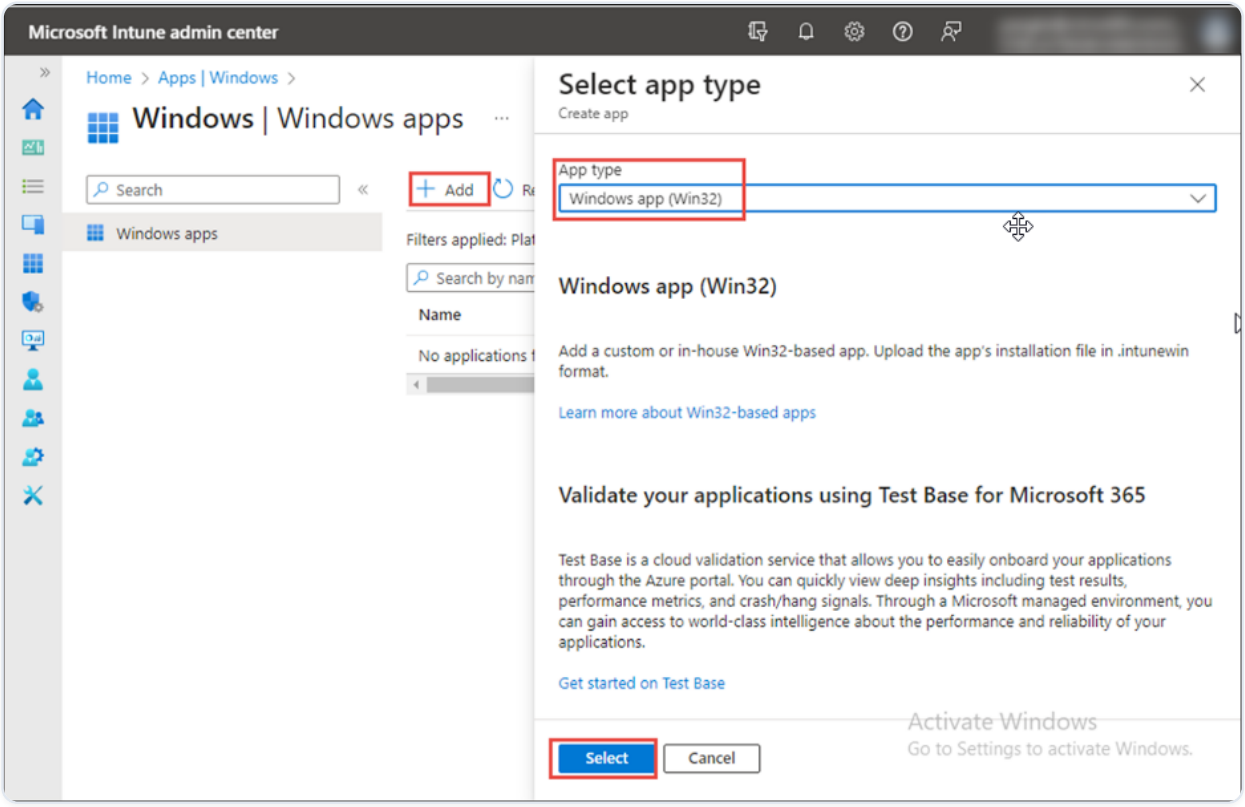
14. デバイスの登録を確認します。



詳細については、Microsoft 365 developer programを参照してください。

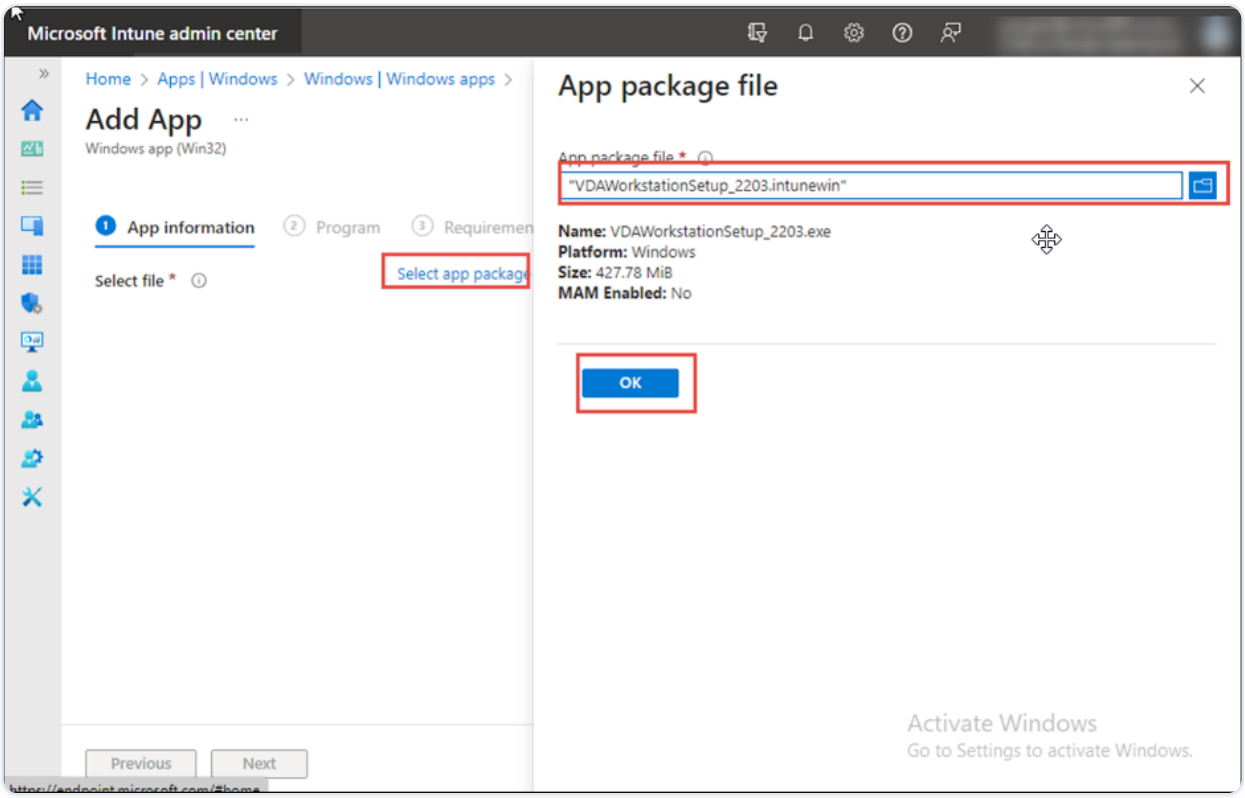
ステップ3：アプリの追加と割り当て

1. Microsoft Intune admin centerにサインインします。
2. **> >** を選択するか、 **> >** に移動します。



3. 「**アプリの種類の選択**」ペインで、「**その他のアプリの種類 > Windows アプリ (Win32)**」を選択し、「**選択**」をクリックします。

4. ペインで、 をクリックします。 をクリックします。
5. 拡張子 `.intunewin` の準備済みファイルを選択します。準備済みファイルは、Citrix VDA のインストールの準備 の手順で作成されます。アプリに関する詳細情報を含むページが表示されます。

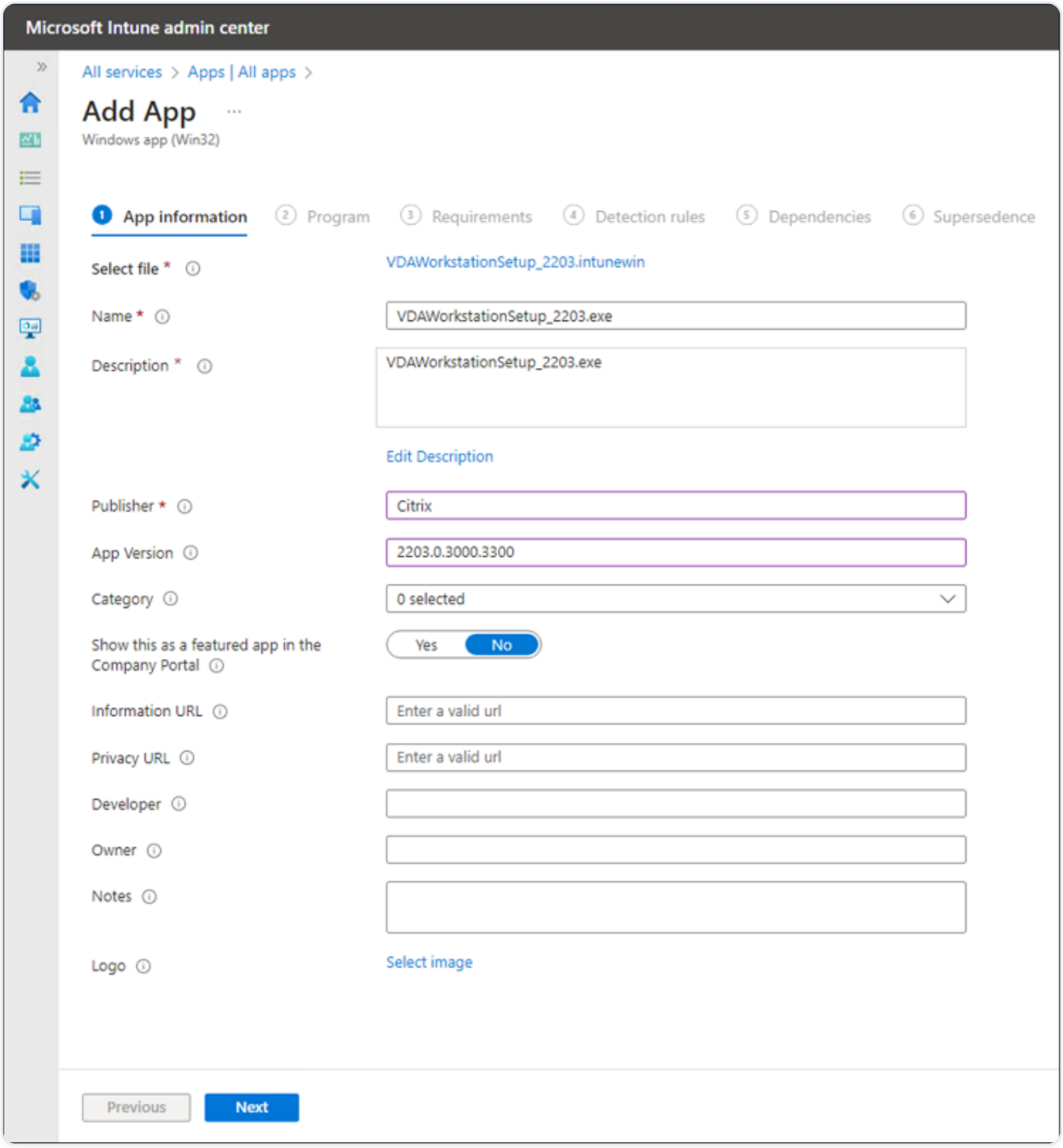


注：

- サーバーコアマシンを使用している場合は、VDAワークステーションコアを使用する必要があります。
- Windows 10デスクトップOSを使用している場合は、VDAワークステーションを使用する必要があります。
- サーバーOS（例：Windows 2022）を使用している場合は、VDAサーバーセットアップを使用する必要があります。
- この例ではバージョン2203を使用していますが、これはすべてのバージョンに適用されます。

6. **App package file**ペインで**OK**をクリックします。

7. 次の画面で、「**アプリ情報**」タブの下にあるアプリの「**名前**」とWindowsアプリの「**説明**」を入力します。「**発行元**」の名前を `Citrix` と入力し、ここで追加のアプリ情報を指定できます。「**次へ**」をクリックします。



8. 次の画面で、次の値を入力します。

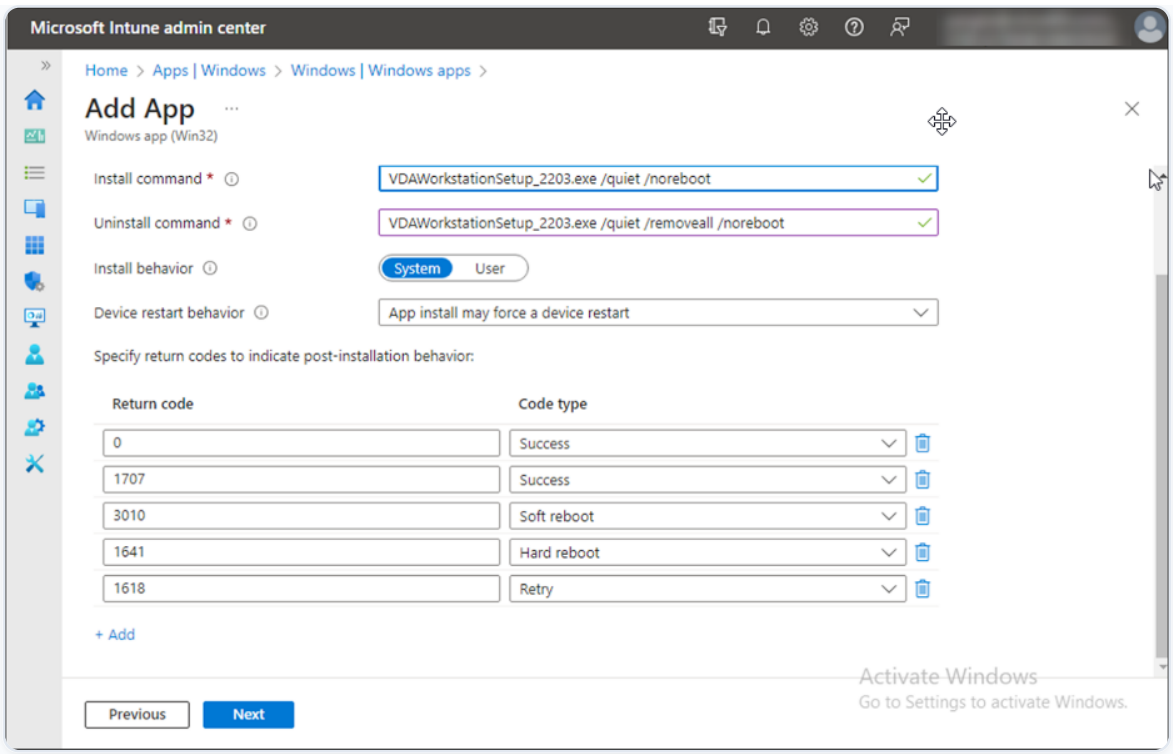
   - **インストールコマンド**: `VDAWorkstationSetup_2203.exe /quiet /noreboot`
   - **アンインストールコマンド**: `VDAWorkstationSetup_2203.exe /quiet /removeall /noreboot`
   - **インストール動作**:

- **システム**: このオプションを選択すると、グループ内のすべてのデバイスにアプリがインストールされます。
- **ユーザー**: このオプションを選択すると、グループ内の特定のユーザーデバイスにのみアプリがインストールされます。

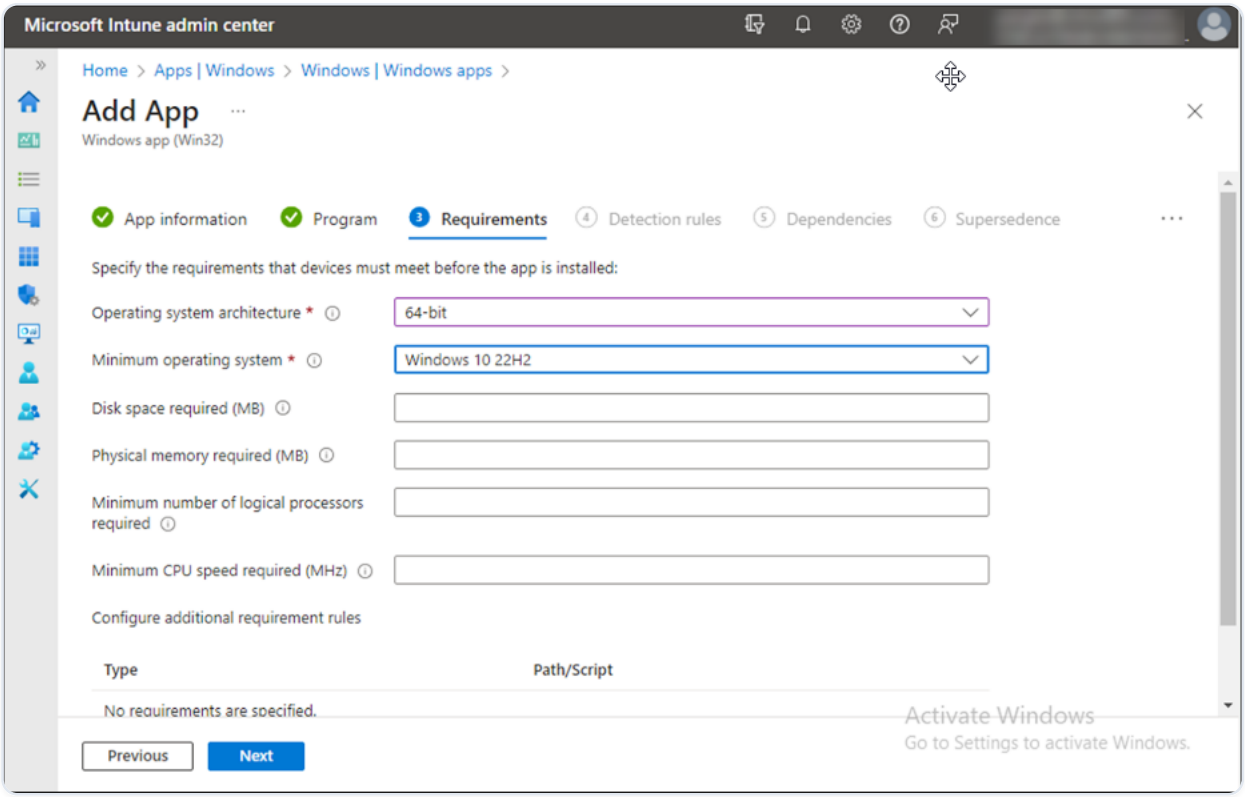
9. **Next**をクリックします。

注:

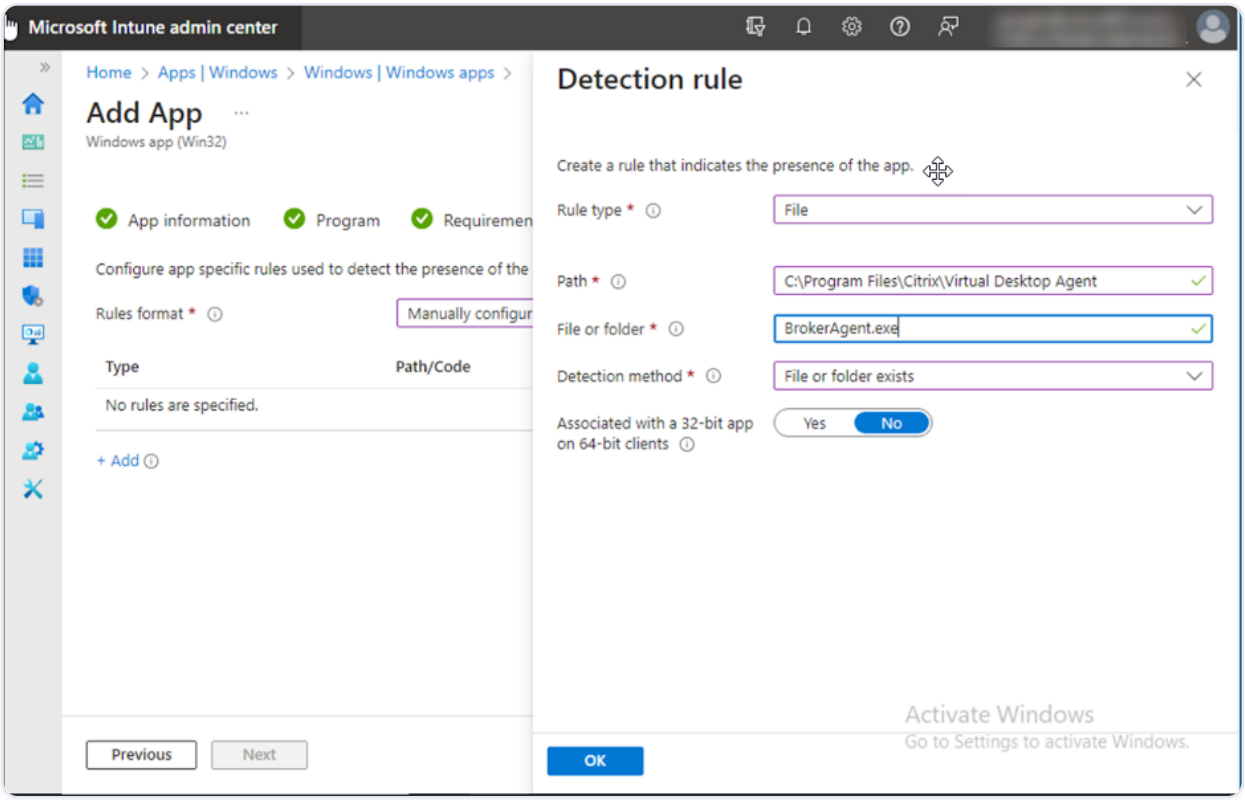
- この例ではバージョン2203を使用していますが、どのバージョンでも使用できます。
- コマンドに`/noreboot`を追加しても、インストールまたは展開中に再起動が発生しないという意味ではなく、強制的な再起動が適用されるだけです。 スクリプトの詳細については、「VDAのインストール用コマンドラインオプション」を参照してください。
- **デバイスの再起動動作**には、**Intuneが強制的にデバイスを再起動します**を選択します。
- **リターンコード**テキストボックスに、インストール後の成功を示す`0`、`3`、および`8`を入力します。 その他のリターンコードについては、「Citrixインストールリターンコード」を参照してください。



10. 次の画面で、「**要件**」タブの下に、必要な値を入力します。「**次へ**」をクリックします。

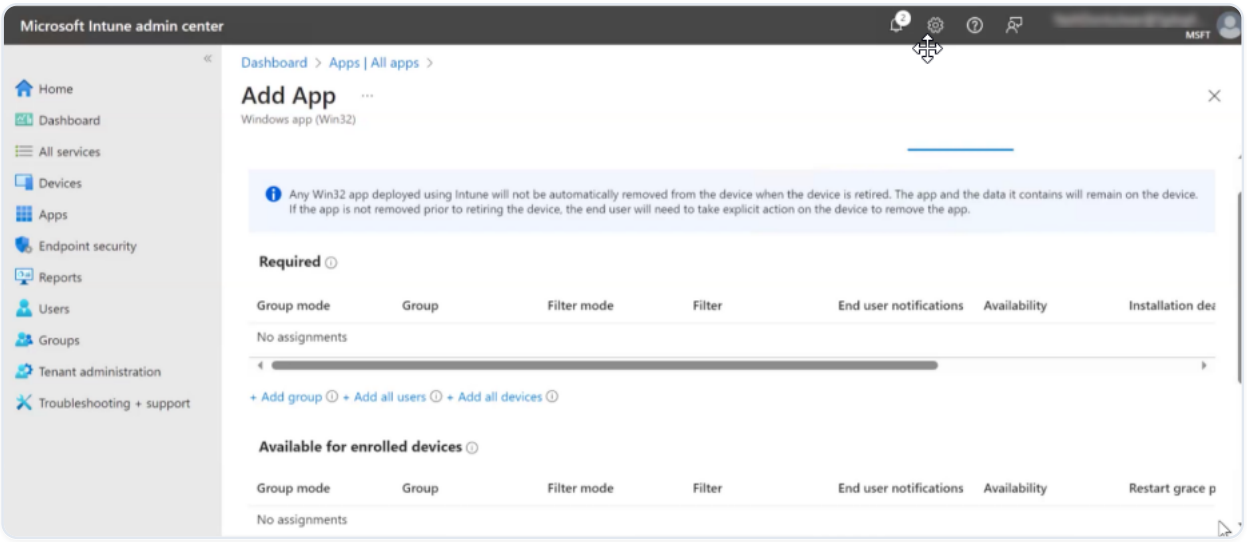


11. 次の画面で、**検出ルール**タブの下にある**検出ルール**を追加して、Brokerエージェントを追加します。**OK**をクリックします。

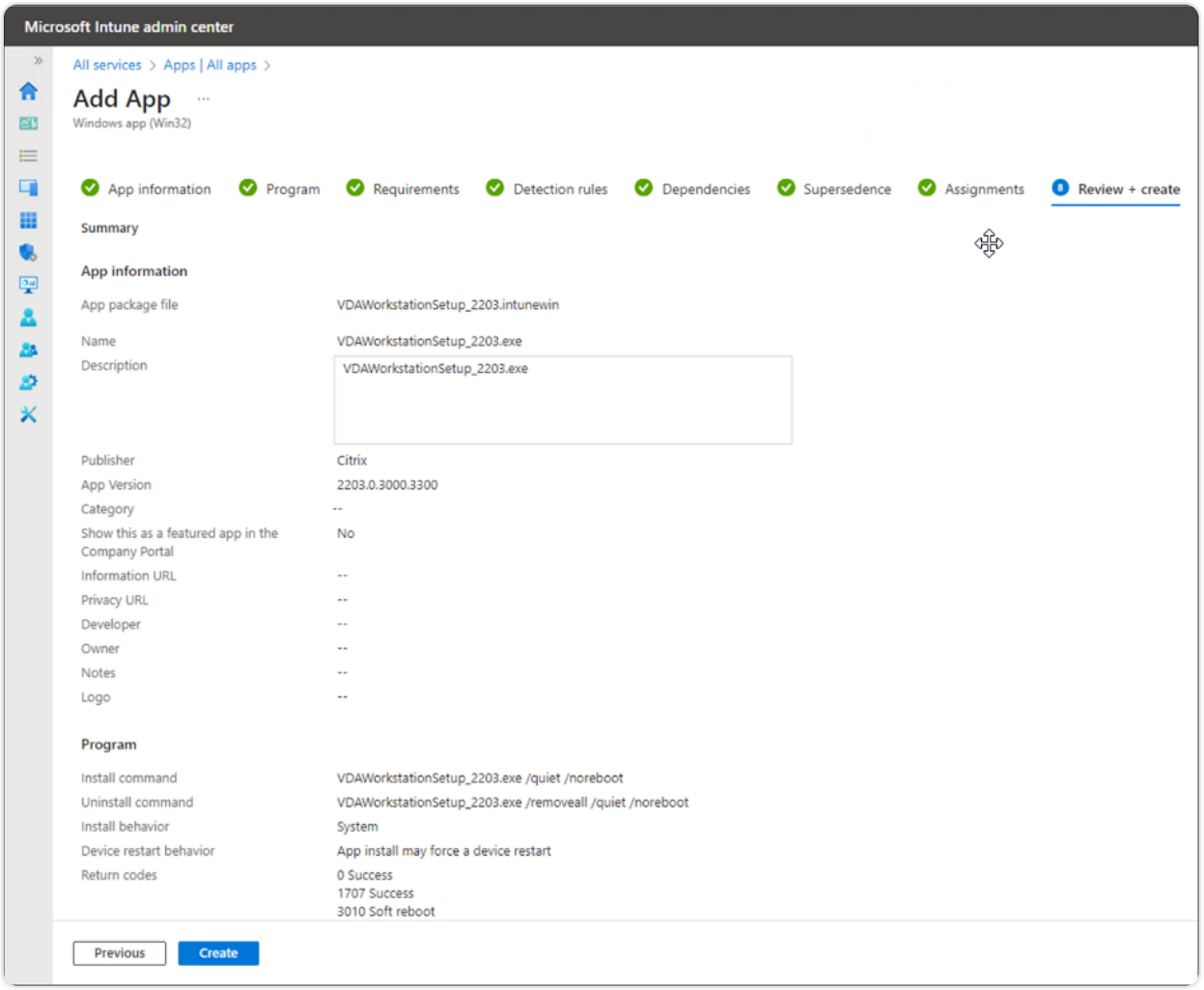


12. **割り当て**タブで、デバイスを次のように追加できます。

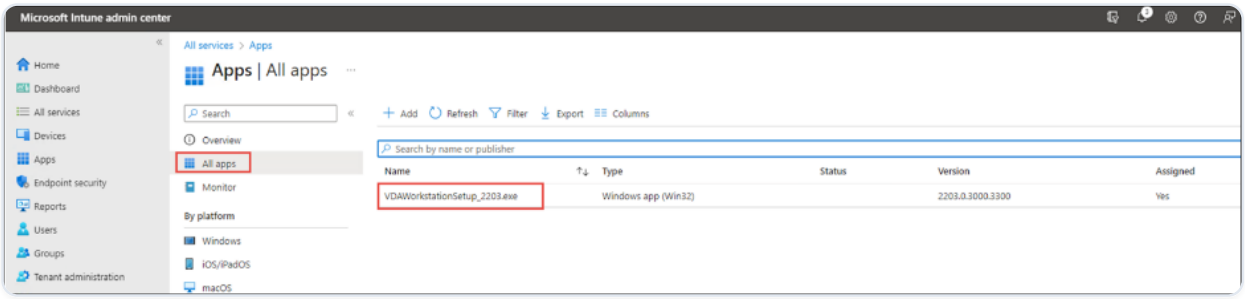
- **必須**: 更新が自動的に行われるデバイス。
- **登録済みデバイスで利用可能**: 更新が手動で行われるデバイス。



13. 詳細を確認し、「**作成**」をクリックします。



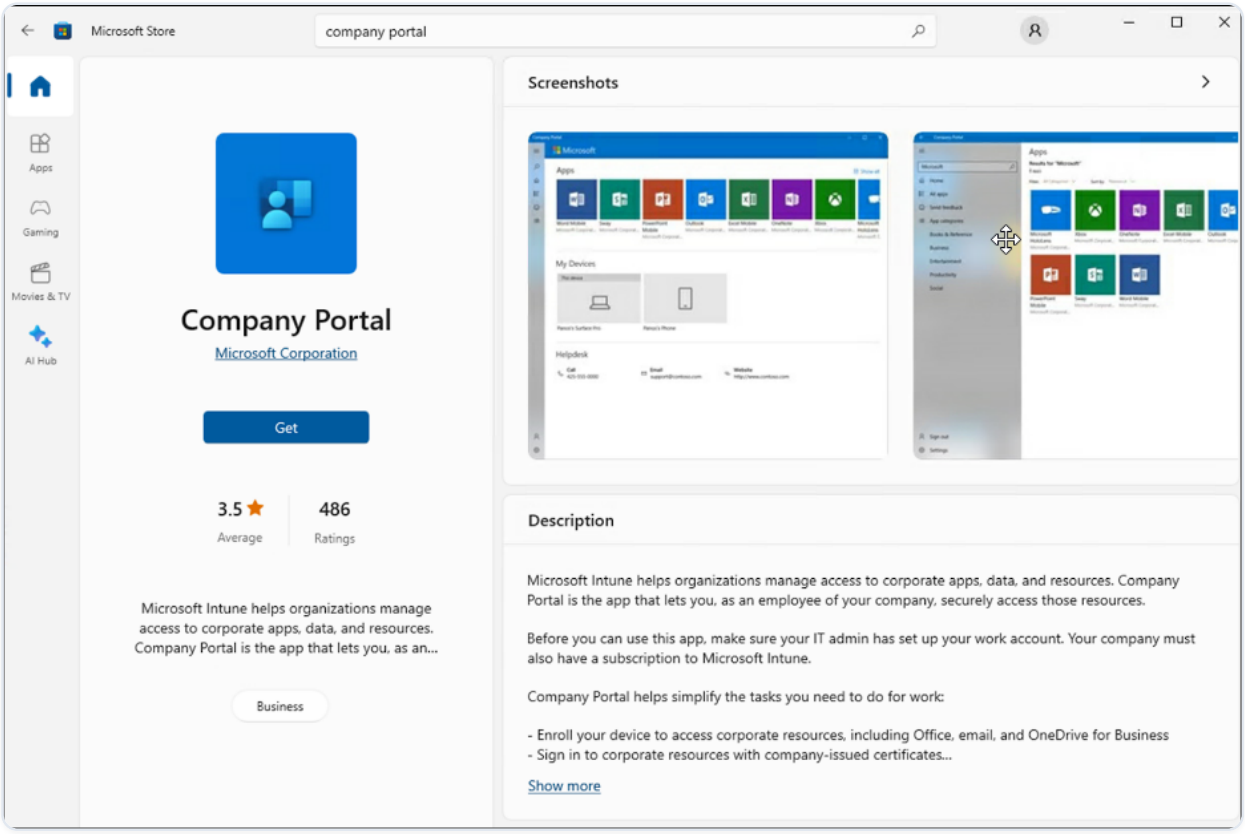
アプリが正常に割り当てられました。



詳細については、「アプリの追加と割り当て」を参照してください。

ステップ 4: 登録済みデバイスにアプリをインストールする

1. 登録済みのWindows 10デスクトップデバイスにサインインします。 デバイスはMicrosoft Intuneに登録されている必要があります。また、アプリに割り当てたグループに含まれるアカウントを使用してデバイスにサインインする必要があります。詳細については、Microsoftのドキュメントを参照してください。
2. 「**スタート**」メニューから「**Microsoft Store**」を開きます。
3. 「**Company Portal**」アプリを検索してインストールします。



4. 「**Company Portal**」アプリを実行します。
5. Microsoft Intuneを使用して追加したアプリをクリックします。 Intuneユーザーにアプリを正常に割り当てなかった場合、次のメッセージが表示されます。 `Your IT administrator did not make any apps available to you.`

6. **Install**をクリックします。

サイトを作成する

> **注：**
>
> - サイト作成中、ハイブリッド権限ライセンスを有効にするライセンスを追加した後、サイト作成が完了するまで、パブリッククラウドホスト（Microsoft Azure、Google Cloud Platform、Amazon Web Servicesなど）は接続の種類リストに表示されません。
> - ライセンスアクティベーションサービスを有効にしている間、または有効にした後に、製品エディションやライセンスモデルを手動で変更しないでください。

> サイトとは、Citrix Virtual Apps and Desktops™展開に付ける名前です。これには、Delivery Controllerおよびその他のコアコンポーネント、Virtual Delivery Agent（VDA）、ホストへの接続、マシンカタログ、デリバリーグループが含まれます。コアコンポーネントをインストールした後、最初のマシンカタログとデリバリーグループを作成する前にサイトを作成します。

ControllerがServer Coreにインストールされている場合は、Citrix Virtual Apps and Desktops SDKのPowerShellコマンドレットを使用してサイトを作成します。

サイトを作成すると、Citrixカスタマーエクスペリエンス向上プログラム（CEIP）に自動的に登録されます。CEIPは匿名の統計情報と使用状況情報を収集し、Citrixに送信します。最初のデータパッケージは、サイト作成後約7日後にCitrixに送信されます。サイト作成後いつでも登録を変更できます。Web Studioの左ペインで**設定**を選択し、**Citrixカスタマーエクスペリエンス向上プログラム**の設定を見つけます。詳細については、`<http://more.citrix.com/XD-CEIP>`を参照してください。

サイトを作成したユーザーは、フル管理者になります。詳しくは、委任管理を参照してください。

サイトを作成する前にこの記事を確認して、何が期待できるかを知っておいてください。

ステップ1. サイト作成ウィザードを開く - Citrix Site Manager

Citrix Virtual Apps and Desktops展開（サイトとも呼ばれます）を設定するには、Citrix Site Managerツールを使用します。このツールは、Delivery Controllerをインストールすると自動的にインストールされます。

このツールを実行するには、Delivery Controllerでデスクトップのスタートメニューを開き、**Citrix > Citrix Site Manager**を選択します。Web Studioのインストールを参照してください。

ステップ2. サイト名

はじめにページで、サイトの名前を入力します。

ステップ3. データベース

> **注:**
>
> バージョン2411以降、データベースにAzure SQL Managed Instanceを使用できます。
>
> **データベース**ページには、サイト、監視、および構成ログデータベースの設定に関する選択肢が含まれています。データベースのセットアップの選択肢と要件の詳細については、データベースを参照してください。

> **注:**
>
> SQL Server Always On ListenerがTLS暗号化用に構成されている場合、データベース作成権限を持つ資格情報の入力を求められることがあります。有効な管理者資格情報を入力しても、データベースの作成は失敗します。SQL Server証明書に、Subject Alternative Names (SAN) にリスナーのDNS名が含まれていることを確認してください。詳細については、`<https://docs.microsoft.com/ja-jp/sql/database-engine/availability-groups/windows/listeners-client-connectivity-application-failover#SSLcertificates>`を参照してください。
>
> サイトデータベースとしてSQL Server Expressをインストールすることを選択した場合（デフォルト）、そのソフトウェアのインストール後に再起動が発生します。サイトデータベースとしてSQL Server Expressソフトウェアをインストールしないことを選択した場合、その再起動は発生しません。

デフォルトのSQL Server Expressを使用しない場合、サイトを作成する前に、SQL Serverソフトウェアがマシンにインストールされていることを確認してください。システム要件でサポートされているバージョンが一覧表示されています。

サイトにDelivery Controllerを追加したい場合、そして、すでに他のサーバーにControllerソフトウェアをインストールしている場合、このページからそれらのControllerを追加できます。データベースをセットアップするスクリプトを生成する予定がある場合、スクリプトを生成する前にControllerを追加してください。

ステップ4. ライセンス

ライセンスページで、ライセンスサーバーのアドレスを指定し、使用する（インストールする）ライセンスを指定します。

> **注:**
>
> - License Activation Service (LAS) は、従来のCitrixレガシーライセンスに代わるものを提供するクラウドベースのライセンスソリューションです。詳細については、以下を参照してください:
>   - Citrix Virtual Apps and Desktops ドキュメント: ライセンスアクティベーションサービス
>   - ライセンスドキュメント: License Activation Service
> - License Activation Serviceを有効にしている間、または有効にした後に、製品エディションやライセンスモデルを手動で変更しないでください。

- ライセンスサーバーのアドレスを`name:[port]`の形式で指定します。*名前*はFQDN、NetBIOS、またはIPアドレスである必要があります。FQDNを推奨します。ポート番号を省略した場合、デフォルトは27000です。**接続**をクリックします。ライセンスサーバーへの接続が成功するまで、次のページに進むことはできません。
- 接続が確立されると、デフォルトで**既存のライセンスを使用**が選択されます。表示には、現在インストールされているライセンスに基づいて、この製品が構成できる互換性のある製品が一覧表示されます。
  - ライセンスサーバーがLicense Activation Service (LAS)を使用するように構成されている場合、Metainstallerはエンタイトルメントを表示します。エンタイトルメントは、対応するライセンスの有効期限とともに提供されます。この製品を、リストされている製品のいずれかとして、それらのライセンスのいずれかを使用して構成したい場合は、そのエントリを選択します。

- この製品で使用するためにライセンスを割り当ててダウンロード済み（Citrix Manage Licenses Toolを使用）だが、まだライセンスをインストールしていない場合：
  - **ライセンスファイルを参照**をクリックします。
  - ファイルエクスプローラーで、ダウンロードしたライセンスを見つけて選択します。関連する製品がサイト作成ウィザードの**ライセンス**ページに表示されます。使用したいエントリを選択します。
- 目的の製品が表示されない場合、または割り当て済みでダウンロード済みのライセンスがない場合は、ライセンスを割り当て、ダウンロードしてインストールできます。これを行うには、ライセンスサーバーがインターネットにアクセスできる必要があります。目的の製品のライセンスアクセスコードが必要です。Citrixからそのコードがメールで送信されます。
  - **割り当ててダウンロード**をクリックします。
  - **ライセンスの割り当て**ダイアログで、Citrixから送信されたライセンスアクセスコードを入力します。**ライセンスを割り当てる**をクリックします。
  - 新しいライセンスに関連付けられた製品が、サイト作成ウィザードの**ライセンス**ページに表示されます。使用したいエントリを選択します。

- または、**30日間の無料試用版を使用**を選択し、後でライセンスをインストールします。詳細については、ライセンスドキュメントを参照してください。

ステップ5. 概要

概要ページには、指定した情報が一覧表示されます。変更する場合は、**戻る**ボタンを使用します。完了したら、**完了**をクリックします。

詳細情報

ホスト接続、ネットワーク、およびストレージ

ハイパーバイザーまたはその他のサービス上のVMを使用してアプリケーションとデスクトップを配信する場合、オプションでそのホストへの最初の接続を作成できます。その接続のストレージとネットワークリソースも指定できます。サイト作成後、この接続とリソースを変更したり、さらに接続を作成したりできます。詳細については、「接続とリソース」を参照してください。

- 「**接続**」ページで指定する情報については、「接続とリソース」を参照してください。

  - ハイパーバイザーまたはその他のサービス上のVMを使用しない場合（またはWeb Studioを使用して専用ブレードPC上のデスクトップを管理する場合）は、接続の種類として**なし**を選択します。
  - Remote PC Accessサイトを構成していて、Wake on LAN機能を使用する予定がある場合は、接続の種類として**Microsoft System Center Virtual Machine Manager**または**Remote PC Wake on LAN**を選択します。詳細については、「Wake on LAN」を参照してください。

  接続の種類に加えて、Citrixツール（Machine Creation Services™など）またはその他のツールを使用してVMを作成するかどうかを指定します。

- 「**ストレージ**」および「**ネットワーク**」ページで指定する情報については、「ホストストレージ」、「ストレージ管理」、および「ストレージの選択」を参照してください。
- ハイブリッド権限ライセンスを所有しており、パブリッククラウドホスト接続（AWSなど）を追加している場合、それらの接続がここに一覧表示されます。これらのパブリッククラウドホスト接続を表示するには、追加後数分経ってからWeb Studioを更新してください。

リモートPCアクセス

Remote PC Accessの展開については、Remote PC Accessを参照してください。

Wake on LAN機能を使用する場合は、サイトを作成する前にMicrosoft System Center Configuration Managerで構成手順を完了してください。詳細については、「Configuration ManagerとRemote PC Access Wake on LAN」を参照してください。

接続とリソースを作成および管理する

> **重要:**

> Citrix Virtual Apps and Desktops™ 7 2006以降、現在の展開で以下のいずれかのテクノロジーを使用している場合、それらのテクノロジーを使用するサポート終了 (EOL) アイテムを削除した後にのみ、現在のリリースにアップグレードできます。

> - パーソナルvDisk (PvD)
> - AppDisks™
> - パブリッククラウドホストの種類：Citrix CloudPlatform、Microsoft Azure Classic

詳細については、「PVD、AppDisks、およびサポートされていないホストの削除」を参照してください。

注:

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

展開にパブリッククラウドホスト接続を使用する場合は、新規インストールまたは現在のリリースへのアップグレードを完了するためにHybrid Rights Licenseが必要です。

インストーラーがサポートされていないテクノロジーまたはHybrid Rights Licenseのないホスト接続を1つ以上検出すると、アップグレードが一時停止または停止し、説明メッセージが表示されます。インストーラーログには詳細が含まれています。詳細については、「展開のアップグレード」を参照してください。

Hybrid Rights Licenseがホスト接続に与える影響

Hybrid Rights Licenseの資格に基づいて、パブリッククラウドホストへのホスト接続が影響を受ける3つのシナリオがあります。

- パブリッククラウドホストへの新しいホスト接続を作成するには、Hybrid Rights Licenseが必要です。
- Hybrid Rights Licenseを所有しているがライセンスの有効期限が切れている場合、パブリッククラウドホストへの既存の接続は資格なしとマークされ、メンテナンスモードに入ります。既存のホスト接続がメンテナンスモードの場合、次の操作はできません。
  - ホスト接続を追加または変更する
  - カタログを作成し、イメージを更新する
  - 電源操作を実行する
- 権限のないホスト接続が権限ありに変更されると、既存のホスティング接続が再度有効になります。

はじめに

サイトを作成するときに、ホスティングリソースへの最初の接続をオプションで作成できます。後で、その接続を変更したり、他の接続を作成したりできます。接続の構成には、サポートされているハイパーバイザーの中から接続タイプを選択すること、およびその接続のリソースから選択するストレージとネットワークが含まれます。

読み取り専用管理者は、接続とリソースの詳細を表示できます。接続とリソースの管理タスクを実行するには、フル管理者である必要があります。詳細については、「委任管理」を参照してください。

接続タイプに関する情報の検索場所

サポートされている仮想化プラットフォームを使用して、Citrix Virtual AppsまたはCitrix Virtual Desktops環境でマシンをホストおよび管理できます。「システム要件」の記事に、サポートされている種類が記載されています。

詳細については、以下の情報源を参照してください。

- **ゼノサーバー (旧称 シトリックス ハイパーバイザー™):**
  - XenServer仮想化環境。
  - XenServer®ドキュメント。
- **ニュータニックス・アクロポリス:**
  - Nutanix仮想化環境。
  - Nutanix のドキュメント。
- **ヴイエムウェア:**
  - VMware仮想化環境。
  - VMware製品ドキュメント。
- **マイクロソフト Hyper-V:**
  - Microsoft System Center Virtual Machine Manager 仮想化環境の記事。
  - Microsoft ドキュメント。
- **パブリッククラウドホスト接続（AWS、Google Cloud、Microsoft Azure、Nutanix Cloudおよびパートナーソリューション、VMware Cloudおよびパートナーソリューション）：** パブ

リッククラウドホストに関する情報については、「リソースタイプのセットアップ」を参照してください。

> **注:**
>
> 情報源は Citrix DaaS™ のドキュメントを参照しています。Citrix DaaS 製品のパブリッククラウドホストに精通している場合でも、オンプレミスバージョンにはいくつかの違いがあります。オンプレミスの Virtual Apps and Desktops では、管理インターフェイスは Web Studio と呼ばれます。更新はサービスに約4週間ごとに展開されます。そのため、サービスで利用できる特定の機能がオンプレミスバージョンでは利用できない場合があります。

ホストストレージ

サポートされているハイパーバイザーによって管理されている場合、ストレージ製品はサポートされます。Citrix Supportは、これらのストレージ製品ベンダーが問題のトラブルシューティングと解決を支援し、必要に応じてナレッジセンターにそれらの問題を文書化します。

マシンをプロビジョニングする際、データはタイプ別に分類されます。

- マスターイメージを含むオペレーティングシステム（OS）データ。
- 一時データ。このデータには、MCSプロビジョニングマシンに書き込まれるすべての非永続データ、Windowsページファイル、ユーザープロファイルデータ、およびShareFileと同期されるすべてのデータが含まれます。このデータは、マシンが再起動するたびに破棄されます。

各データタイプに個別のストレージを提供することで、各ストレージデバイスの負荷を軽減し、パフォーマンスを向上させ、ホストの利用可能なリソースを最大限に活用できます。また、異なるデータタイプに適切なストレージを使用できるようになります。一部のデータでは、永続性と回復性が他のデータよりも重要です。

ストレージは共有（中央に配置され、どのホストからも独立しており、すべてのホストで使用される）することも、ハイパーバイザーにローカルに配置することもできます。たとえば、中央共有ストレージは、1つ以上のWindows Server 2012クラスター化ストレージボリューム（接続されたストレージの有無にかかわらず）であるか、ストレージベンダーのアプライアンスである場合があります。中央ストレージは、ハイパーバイザーのストレージ制御パスやパートナープラグインを介した直接アクセスなど、独自の最適化を提供する可能性もあります。

一時データをローカルに保存することで、共有ストレージにアクセスするためにネットワークを介する必要がなくなります。また、共有ストレージデバイスの負荷も軽減されます。共有ストレージはより高価になる可能性があるため、データをローカルに保存することで費用を削減できます。これらの利点は、ハイパーバイザーサーバー上の十分なストレージの可用性と比較検討する必要があります。

接続を作成するときは、ハイパーバイザーによって共有されるストレージ、またはハイパーバイザーにローカルなストレージの2つのストレージ管理方法のいずれかを選択します。

1つ以上のXenServerホストで一時データストレージにローカルストレージを使用する場合、プール内の各ストレージの場所に一意の名前があることを確認してください。（XenCenter®で名前を変更するには、ストレージを右クリックして名前プロパティを編集します。）

ハイパーバイザーで共有されるストレージ

ハイパーバイザーによって共有されるストレージ方式は、より長期的な永続性が必要なデータを中央に保存し、一元化されたバックアップと管理を提供します。このストレージにはOSディスクが格納されます。

この方法を選択すると、一時的なマシンデータにローカルストレージ（同じハイパーバイザープール内のサーバー上）を使用するかどうかを選択できます。この方法は、共有ストレージ内のデータ（*一時データキャッシュ*と呼ばれる）ほど永続性や回復性を必要としません。ローカルディスクは、メインOSストレージへのトラフィックを削減するのに役立ちます。このディスクは、マシンの再起動ごとにクリアされます。ディスクはライトスルーメモリキャッシュを介してアクセスされます。一時データにローカルストレージを使用する場合、プロビジョニングされたVDAは特定のハイパーバイザーホストに紐付けられます。そのホストが故障すると、VMは起動できません。

例外: Microsoft System Center Virtual Machine Managerは、クラスター共有ボリューム（CSV）を使用する場合、ローカルストレージ上の一時データキャッシュディスクを許可しません。

一時データをローカルに保存するための接続を作成し、各VMのキャッシュディスクサイズとメモリサイズの非デフォルト値を有効にして構成します。デフォルト値は接続タイプに合わせて調整されており、ほとんどの場合に十分です。詳細については、マシンカタログの作成を参照してください。

ハイパーバイザーは、ディスクイメージのローカルでの読み取りキャッシュを通じて最適化テクノロジーを提供することもできます。たとえば、XenServerはIntelliCache™を提供しており、これにより中央ストレージへのネットワークトラフィックが削減されます。

ハイパーバイザーのローカルストレージ

ハイパーバイザーにローカルなストレージ方式は、データをハイパーバイザー上にローカルに保存します。この方法では、マスターイメージやその他のOSデータがサイト内のハイパーバイザーに転送されます。このプロセスは、初期のマシン作成時および将来のイメージ更新時に発生します。このプロセスにより、管理ネットワーク上でかなりのトラフィックが発生します。イメージ転送には時間もかかり、各ホストでイメージが利用可能になるタイミングも異なります。

接続とリソースの作成

サイトの作成時に、最初の接続をオプションで作成できます。サイト作成ウィザードには、以下のセクションで説明する接続関連のページが含まれています。

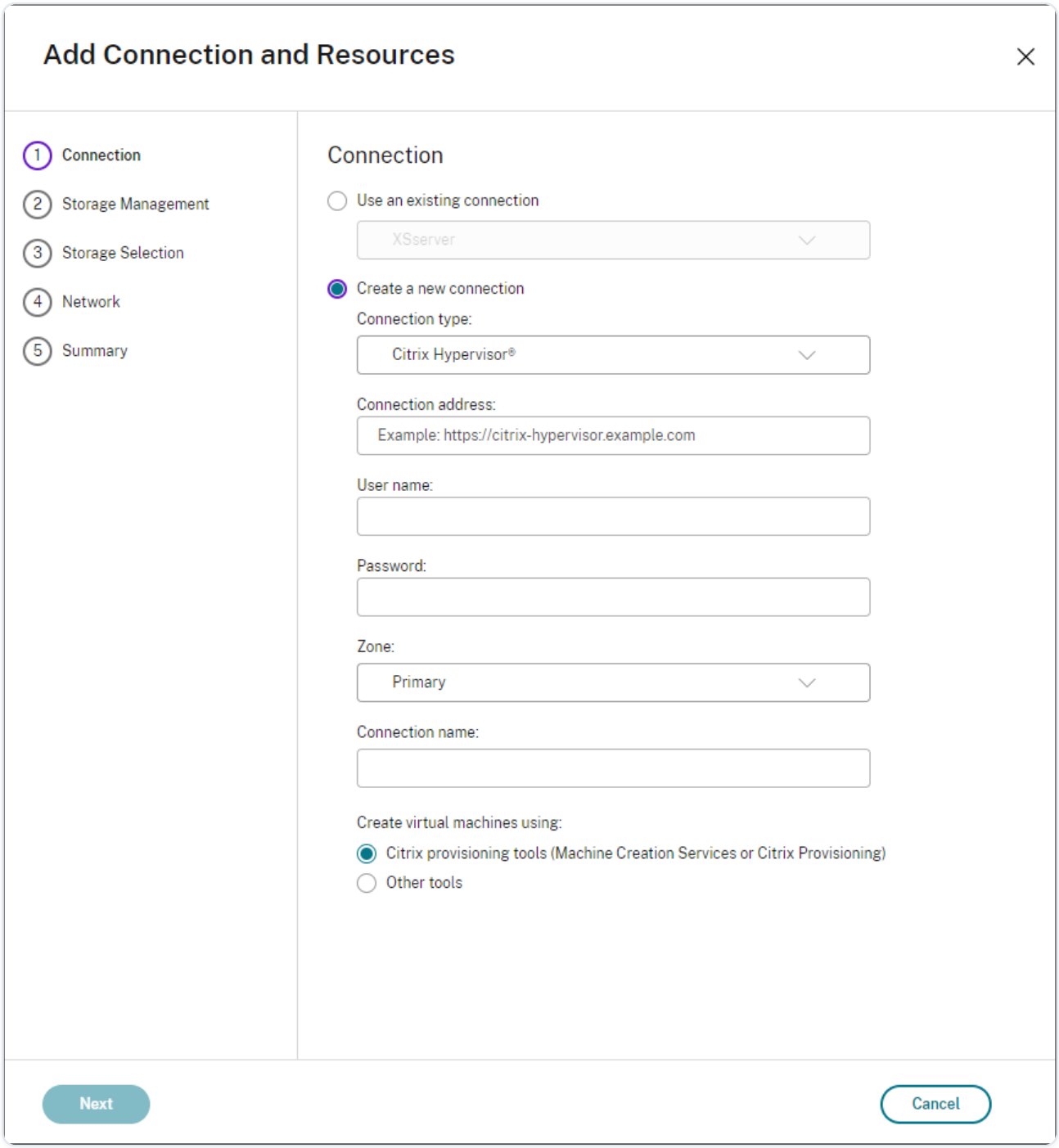
サイトの作成後に接続を作成する場合は、手順1から開始します。

> **重要:**

> 接続を作成する前に、ホストリソース（ストレージとネットワーク）が利用可能である必要があります。

1. Web Studioにサインインします。
2. 左ペインで**ホスティング**を選択します。
3. アクションバーで**接続とリソースの追加**を選択します。
4. ウィザードは以下のページを案内します（特定のページ内容は選択した接続タイプによって異なります）。各ページを完了したら、**次へ**をクリックして**概要**ページに進みます。

接続



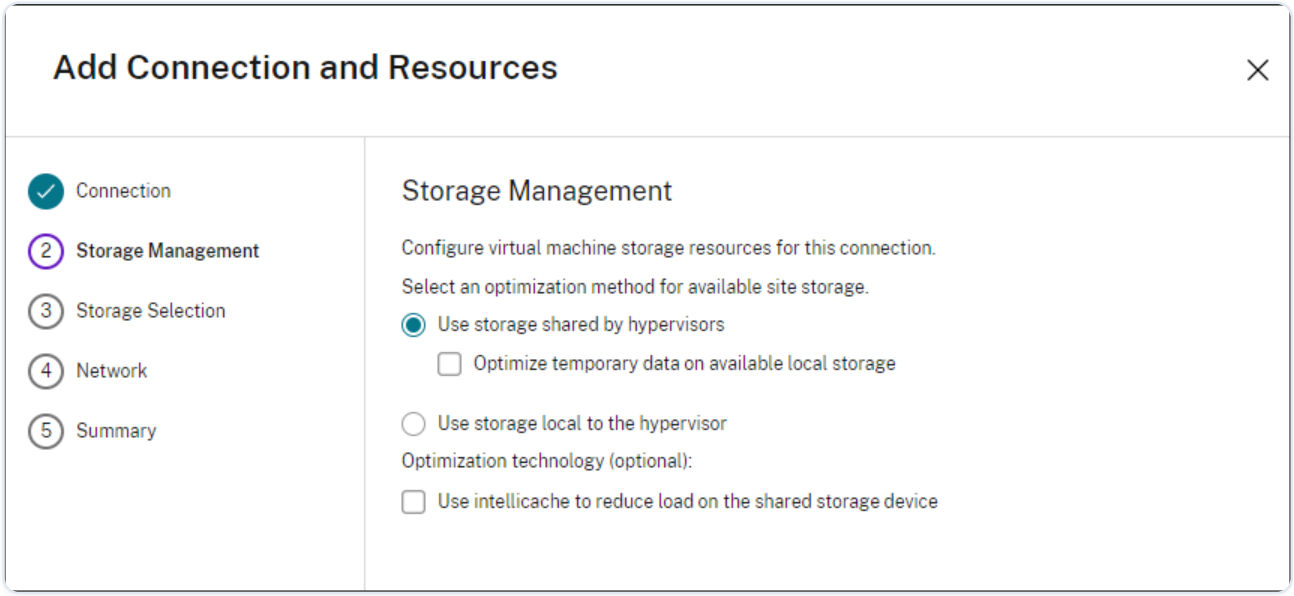
「**接続**」ページで：

- 接続を作成するには、**新しい接続の作成**を選択します。既存の接続と同じホスト構成に基づいて接続を作成するには、**既存の接続を使用**を選択し、関連する接続を選択します。
- **接続タイプ**フィールドで、使用しているハイパーバイザーを選択します。パブリッククラウドホスト接続は、ハイブリッドライツライセンスを使用している場合にのみドロップダウンリストに表示されます。または、PowerShellコマンド `Get-HypHypervisorPlugin [-ZoneUid] $rluid [-IncludeUnavailable]` false/true を使用して、以下を取得できます。

  - サードパーティ製プラグインを含む、Citrixがサポートするすべてのハイパーバイザープラグインのリスト。
  - ハイパーバイザープラグインの可用性。可用性ステータスが**false**の場合、ハイパーバイザープラグインが正しくインストールされていないか、ハイブリッドライツライセンスが付与されていない可能性があります。

- 接続アドレスと資格情報フィールドは、選択した接続タイプによって異なります。要求された情報を入力してください。
- 接続名を入力します。この名前はWeb Studioに表示されます。
- 仮想マシンの作成に使用するツールを選択します。Web Studioツール（Machine Creation Services™やCitrix Provisioningなど）またはその他のツール。

ストレージ管理



ストレージ管理の種類と方法については、「ホストストレージ」を参照してください。

Hyper-VまたはVMwareホストへの接続を構成する場合は、クラスター名を参照して選択します。その他の接続タイプでは、クラスター名は要求されません。

ストレージ管理方法を選択します。ハイパーバイザーで共有されるストレージ、またはハイパーバイザーにローカルなストレージ。

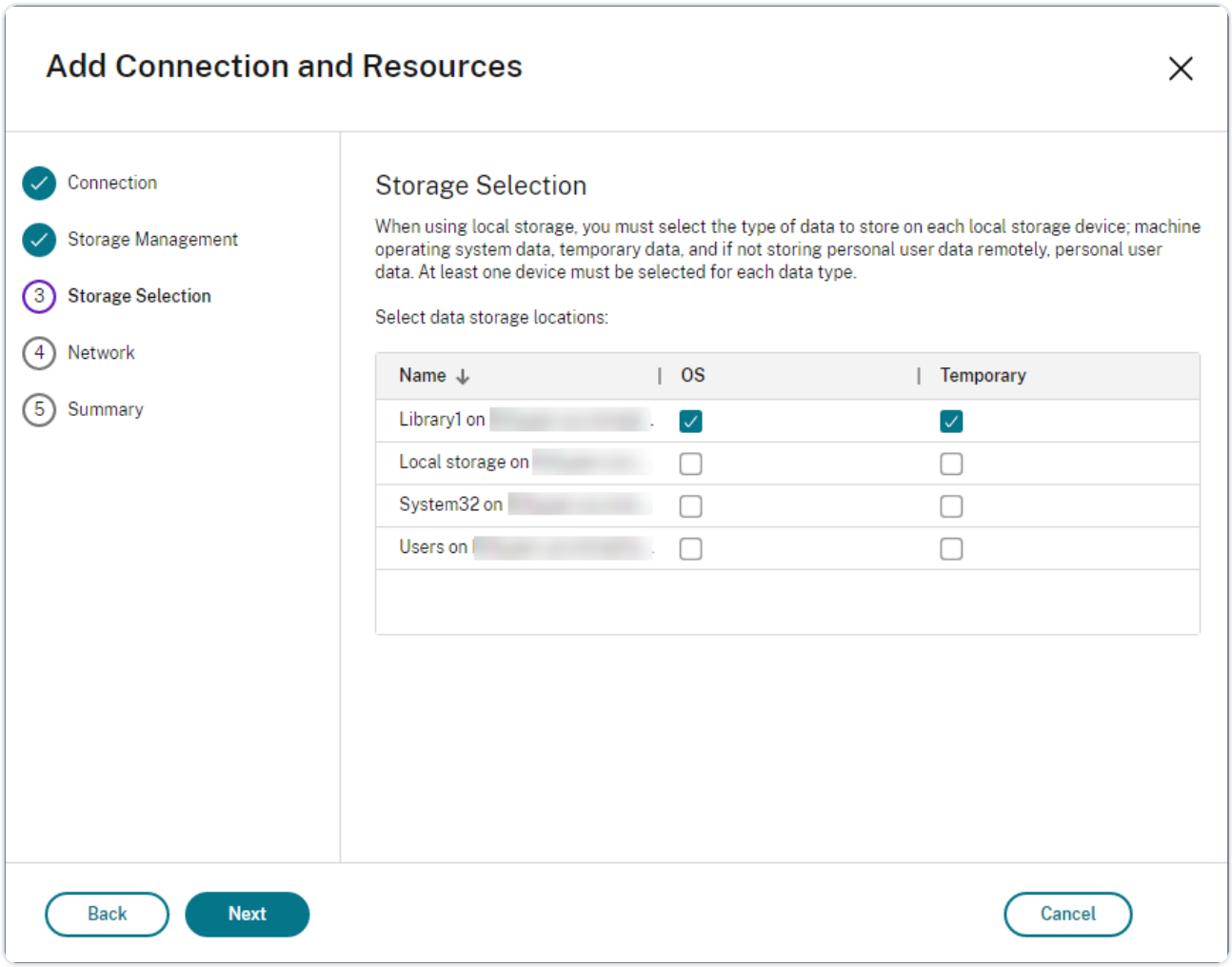
- ハイパーバイザーで共有されるストレージを選択した場合、利用可能なローカルストレージに一時データを保持するかどうかを指定します。（この接続を使用するマシンカタログで、デフォルト以外のテンポラリストレージサイズを指定できます。）**例外：** クラスター共有ボリューム（CSV）を使用する場合、Microsoft System Center Virtual Machine Managerはローカルストレージ上の一時データキャッシュディスクを許可しません。Web Studioでそのストレージ管理設定を構成すると失敗します。

XenServerプールで共有ストレージを使用している場合、共有ストレージデバイスの負荷を軽減するためにIntelliCacheを使用するかどうかを指定します。「XenServer接続にIntelliCacheを使用する」を参照してください。

注:

XenServer、VMware、およびSCVMM仮想化環境では、OSディスクと同じストレージ場所にライトバックキャッシュ（WBC）ディスクを配置できます。この場合、**利用可能なローカルストレージで一時データを最適化する**を選択しないでください。

ストレージの選択



ストレージの選択の詳細については、「ホストストレージ」を参照してください。

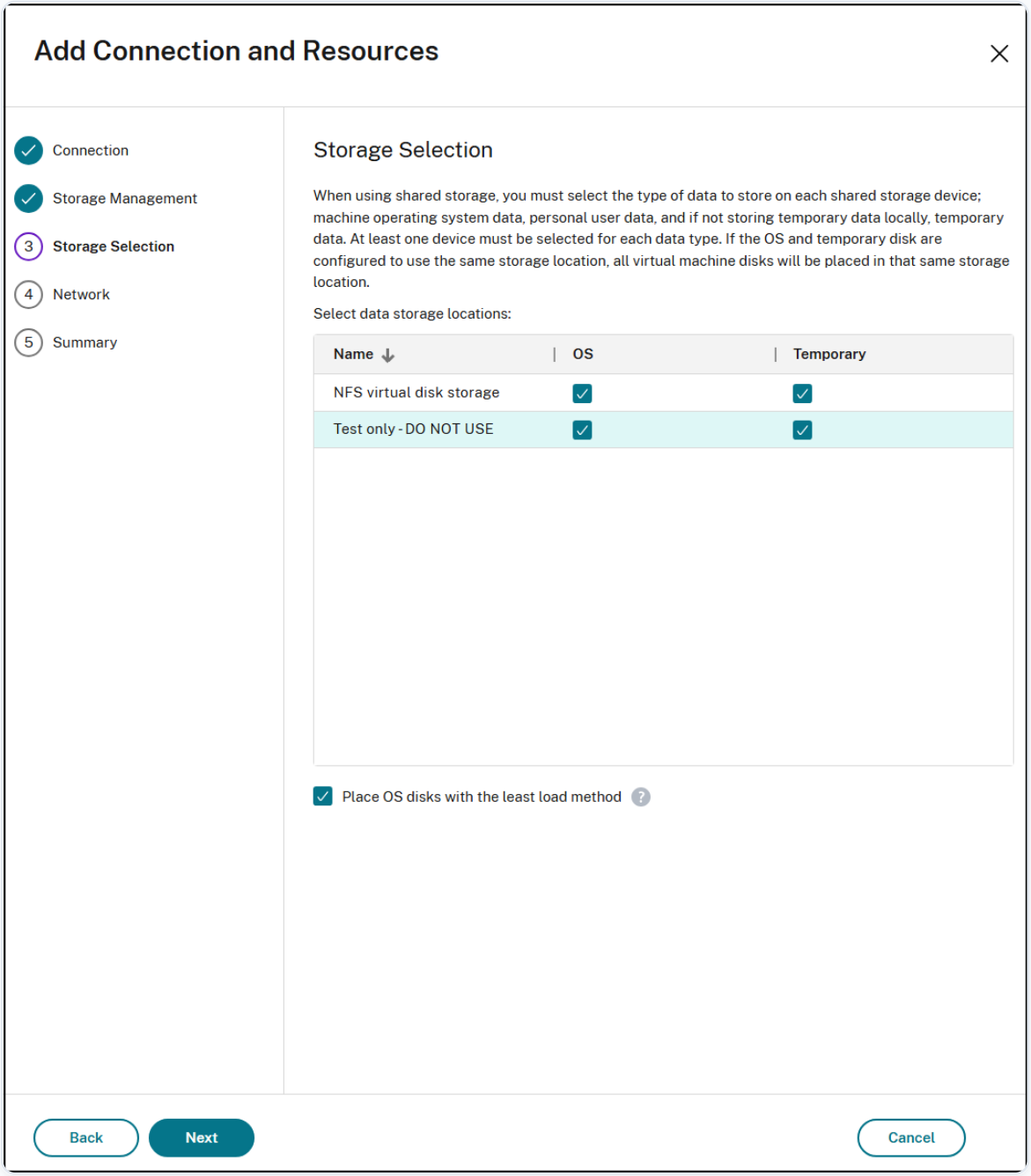
利用可能なデータタイプごとに、少なくとも1つのホストストレージデバイスを選択します。前のページで選択したストレージ管理方法によって、このページで選択できるデータタイプが決まりま

す。ウィザードの次のページに進む前に、サポートされているデータタイプごとに少なくとも1つのストレージデバイスを選択してください。

注:

- XenServer、VMware、SCVMM仮想化環境では、利用可能なOSストレージリストと利用可能な一時ストレージリストを同じように構成した場合、MCSはライトバックキャッシュ（WBC）ディスクをOSディスクと同じストレージの場所に配置します。
- 2つ以上のOSデータストレージの場所を選択すると、「**最小負荷方式によるストレージ負荷分散の最適化**」オプションが表示されます。このオプションを使用すると、ディス

ク割り当てのために最も負荷の低いストレージリポジトリを選択できます。



- 「**概要**」ページには、選択内容に応じてオプションが「**有効**」か「**無効**」かが表示されます。「**詳細**」パネルには、ストレージ割り当て方法の変更が表示されます。「**OSストレージ**」ページの「**ストレージの編集**」オプションを使用して調整できます。または、PowerShellを使用して同じ目標を達成できます。「VMの柔軟なストレージ場所オプション」を参照してください。

「**ストレージ管理**」ページで「**ハイパーバイザーで共有されるストレージを使用**」を選択し、「**利用可能なローカルストレージ上の一時データを最適化**」を選択すると、「**ストレー**

> **ジの選択**」ページでより多くの構成オプションを利用できます。たとえば、一時データに使用するローカルストレージデバイス（同じハイパーバイザープール内）を選択できます。

現在選択されているストレージデバイスの数が表示されます (上記のグラフィックでは「1 storage device selected」)。そのエントリにカーソルを合わせると、選択されているデバイス名が表示されます。

1. 使用するストレージデバイスを変更するには、「**選択**」をクリックします。
2. 「**ストレージの選択**」ダイアログボックスで、ストレージデバイスのチェックボックスをオンまたはオフにし、「**OK**」をクリックします。

ネットワーク

「**ネットワーク**」ページで、リソースの名前を入力します。この名前は、Web Studioに表示され、接続に関連付けられたストレージとネットワークの組み合わせを識別します。

VMが使用するネットワークを1つ以上選択します。

概要

「**概要**」ページで、選択内容を確認します。完了したら、「**完了**」をクリックします。

注意: 一時データをローカルに保存すると、この接続を使用するマシンを含むマシンカタログを作成するときに、一時データストレージの非デフォルト値を構成できます。「マシンカタログの作成」を参照してください。

接続設定の編集

接続の名前変更や接続の作成には、この手順を使用しないでください。これらの接続は異なる操作です。現在ホストされているマシンのアドレスが変更された場合にのみ、アドレスを変更してください。別のアドレスを別のマシンに入力すると、接続のMachine Catalogsが破損します。

このリソースにアクセスするマシンカタログは、適切なGPU固有のマスターイメージを使用する必要があるため、接続の**GPU**設定を変更することはできません。接続を作成してください。

1. Web Studioにサインインします。
2. 左ペインで**ホスティング**を選択します。
3. 接続を選択し、アクションバーで**接続の編集**を選択します。
4. 接続を編集する際に利用できる設定のガイダンスに従ってください。
5. 完了したら、**Apply**をクリックして変更を適用し、ウィンドウを開いたままにするか、**Save**をクリックして変更を適用してウィンドウを閉じます。

接続プロパティページ:

- 接続アドレスと資格情報を変更するには、**Edit settings...**を選択し、新しい情報を入力します。
- XenServer接続の高可用性サーバーを指定するには、**Edit servers...**を選択し、サーバーを選択します。Citrixは、プールマスターが失敗した場合にXenServerとの通信を可能にするために、プール内のすべてのサーバーを選択することを推奨します。

> **注:**
>
> HTTPSを使用しており、高可用性サーバーを構成したい場合は、プール内のすべてのサーバーにワイルドカード証明書をインストールしないでください。各サーバーには個別の証明書が必要です。

Advancedページ:

- Remote PC Accessで使用されるMicrosoft System Center Configuration Manager (ConfMgr) Wake on LAN接続タイプの場合、**ConfMgr Wake Proxy**、マジックパケット、およびパケット送信情報を入力します。
- スロットリングしきい値設定を使用すると、接続で許可される最大電源アクション数を指定できます。これらの設定は、電源管理設定が同時に起動するマシンの数が多すぎたり少なすぎたりする場合に役立ちます。各接続タイプには、ほとんどのケースに適した特定のデフォルト値があり、変更してはなりません。
- 「**同時実行アクション (すべての種類)**」設定では、この接続で同時に発生できる最大絶対数と、この接続を使用するすべてのマシンの最大割合の2つの値を指定します。絶対値とパーセンテージ値の両方を指定する必要があります。適用される実際の制限は、これらの値の小さい方です。

  たとえば、34台のマシンがある展開で、「**同時実行アクション (すべての種類)**」が絶対値10、パーセンテージ値10に設定されている場合、適用される実際の制限は3です (つまり、34の10パーセントを最も近い整数に丸めたもので、絶対値10台のマシンよりも小さい)。
- 「**1分あたりの最大新規アクション数**」は絶対数です。パーセンテージ値はありません。
- **接続オプション**フィールドには、Citrixサポート担当者の指示または明示的なドキュメントの指示がある場合にのみ情報を入力してください。

共有テナントページ:

この接続のサブスクリプションとAzure Compute Galleryを共有するテナントとサブスクリプションを追加します。これにより、カタログの作成または更新時に、それらのテナントとサブスクリプションから共有イメージを選択できます。

- この接続に関連付けられているアプリケーションの**アプリケーションID**と**アプリケーションシークレット**を入力します。この情報を使用して、Azureに認証できます。セキュリティを確保するために、定期的にキーを変更することをお勧めします。
- 共有テナントとサブスクリプションを指定します。最大8つの共有テナントを追加できます。各テナントには、最大8つのサブスクリプションを追加できます。
- 完了したら、**保存**と**適用**をクリックします。

接続オプションフィールドには、Citrixサポート担当者の指示がある場合にのみ情報を入力してください。

ネットワークの編集

接続のネットワークを変更できます。次の手順を実行します。

1. **ホスティング**に移動します。
2. 接続下のターゲットリソースを選択し、アクションバーで**ネットワークの編集**を選択します。
3. 仮想マシンが使用するネットワークを1つ以上選択します。
4. 変更を保存して終了するには、**保存**をクリックします。

接続のメンテナンスモードをオンまたはオフにする

接続のメンテナンスモードをオンにすると、新しい電源操作がその接続に保存されているマシンに影響を与えるのを防ぎます。ユーザーはメンテナンスモードのマシンに接続できません。ユーザーがすでに接続している場合、メンテナンスモードはログオフ時に有効になります。

1. Web Studioにサインインします。
2. 左ペインで**ホスティング**を選択します。
3. 接続を選択します。メンテナンスモードをオンにするには、アクションバーで**Turn On Maintenance Mode**を選択します。メンテナンスモードをオフにするには、**Turn Off Maintenance Mode**を選択します。

個々のマシンのメンテナンスモードをオンまたはオフにすることもできます。また、マシンカタログまたはデリバリーグループ内のマシンのメンテナンスモードをオンまたはオフにすることもできます。

接続を削除する

接続を削除すると、多数のマシンが削除され、データが失われる可能性があります。影響を受けるマシン上のユーザーデータがバックアップされているか、不要であることを確認してください。

接続を削除する前に、以下を確認してください。

- すべてのユーザーが接続に保存されているマシンからログオフしていること。
- 切断されたユーザーセッションが実行されていないこと。
- プールされたマシンと専用マシンのメンテナンスモードがオンになっていること。
- 接続で使用されているマシンカタログ内のすべてのマシンが電源オフになっていること。

カタログによって参照されている接続を削除すると、マシンカタログは使用できなくなります。この接続がカタログによって参照されている場合、カタログを削除するオプションがあります。カタログを削除する前に、他の接続で使用されていないことを確認してください。

1. Web Studio にサインインします。
2. 左ペインで を選択します。
3. 接続を選択し、アクションバーで を選択します。
4. この接続にマシンが保存されている場合、マシンを削除するかどうかを尋ねられます。削除する場合は、関連付けられているActive Directoryコンピューターアカウントをどうするかを指定します。

接続の名前を変更またはテストする

1. Web Studio にサインインします。
2. 左ペインで を選択します。
3. 接続を選択し、アクションバーで または を選択します。

接続上のマシンの詳細を表示する

1. Web Studio にサインインします。
2. 左ペインで を選択します。
3. 接続を選択し、アクションバーで を選択します。

上部のペインには、接続を介してアクセスされるマシンが一覧表示されます。マシンを選択すると、下部のペインにその詳細が表示されます。開いているセッションのセッション詳細も提供されます。

検索機能を使用して、マシンをすばやく見つけます。ウィンドウ上部のリストから保存された検索を選択するか、新しい検索を作成します。マシン名のすべてまたは一部を入力して検索するか、高度な検索に使用する式を作成できます。式を作成するには、 をクリックし、プロパティと演算子のリストから選択します。

接続上のマシンを管理する

1. Web Studio にサインインします。
2. 左側のペインで を選択します。
3. 接続を選択し、 ペインで を選択します。
4. アクションバーで次のいずれかを選択します。一部のアクションは、マシンの状態と接続ホストの種類によっては使用できません。

アクション	説明
起動	マシンが電源オフまたは中断状態の場合に起動します。
中断	マシンをシャットダウンせずに一時停止し、マシンの一覧を更新します。
シャットダウン	オペレーティングシステムにシャットダウンを要求します。
強制シャットダウン	マシンの電源を強制的にオフにし、マシンの一覧を更新します。
再起動	オペレーティングシステムにシャットダウンを要求し、その後マシンを再起動します。オペレーティングシステムがこれに応じられない場合、デスクトップは現在の状態のままになります。
メンテナンスモードを有効にする	マシンへの接続を一時的に停止します。この状態では、ユーザーはマシンに接続できません。ユーザーが接続している場合、メンテナンスモードはログオフ時に有効になります。（上記で説明したように、接続を介してアクセスされるすべてのマシンに対してメンテナンスモードをオンまたはオフにすることもできます。）

アクション	説明
デリバリーグループから削除	マシンをデリバリーグループから削除しても、そのデリバリーグループが使用するマシンカタログから削除されるわけではありません。マシンは、ユーザーが接続していない場合にのみ削除できます。マシンを削除している間、ユーザーが一時的に接続できないようにするには、メンテナンスモードをオンにします。
削除	マシンを削除すると、ユーザーはそのマシンにアクセスできなくなり、マシンはマシンカタログから削除されます。マシンを削除する前に、すべてのユーザーデータがバックアップされているか、不要になっていることを確認してください。マシンは、ユーザーが接続していない場合にのみ削除できます。マシンを削除している間、ユーザーが一時的に接続できないようにするには、メンテナンスモードをオンにします。

マシンのシャットダウンを伴う操作の場合、マシンが10分以内にシャットダウンしないと、電源がオフになります。シャットダウン中にWindowsが更新プログラムのインストールを試みる場合、更新プログラムが完了する前にマシンの電源がオフになるリスクがあります。

ストレージの編集

接続を使用するVMのオペレーティングシステムデータと一時データを保存するために使用されるサーバーのステータスを表示できます。また、各データタイプのストレージにどのサーバーを使用するかを指定することもできます。

1. Web Studioにサインインします。
2. 左ペインで を選択します。
3. 接続を選択し、アクションバーで を選択します。
4. 左ペインで、データタイプ（オペレーティングシステムまたは一時）を選択します。
5. 選択したデータタイプに対して、1つ以上のストレージデバイスのチェックボックスをオンまたはオフにします。
6. 「**OK**」をクリックします。

リスト内の各ストレージデバイスには、その名前とストレージステータスが含まれています。有効なストレージステータスの値は次のとおりです。

- **使用中:** ストレージはマシンの作成に使用されています。
- **廃止済み:** ストレージは既存のマシンにのみ使用されています。このストレージには新しいマシンは追加されません。
- **未使用:** ストレージはマシンの作成に使用されていません。

現在**使用中**のデバイスのチェックボックスをオフにすると、そのステータスは**廃止済み**に変わります。既存のマシンはそのストレージデバイスを引き続き使用し（データを書き込むこともできます）、そのため、マシンの作成に使用されなくなった後でも、その場所がいっぱいになる可能性があります。

リソースの削除、名前の変更、またはテスト

1. Web Studioにサインインします。
2. 左ペインで**ホスティング**を選択します。
3. リソースを選択し、アクションバーで適切なエントリ（**リソースの削除**、**リソースの名前変更**、または**リソースのテスト**）を選択します。

VMの柔軟なストレージ場所オプション

マシンカタログ内のVMには、さまざまなストレージサービス（SR）が割り当てられます。異なるストレージでのVM割り当てのバランスを取るには、2つのオプションがあります。

- **拡張された現在のラウンドロビン割り当て方法**: 常に同じ固定SRから開始するのではなく、MCSは最後に使用されたSRの直後のSRから割り当てを開始します。
- **最小負荷ベースの割り当て方法**: 同じマシンカタログ内の各SR上のVMの総数を比較することによって決定される、現在の最小負荷にVMを配置します。たとえば、マシンカタログに100個のVMがSR1に20個、SR2に30個、SR3に50個というように分散されている場合、新しいVMは最初にSR1に割り当てられます。この方法により、SR1、SR2、SR3間の負荷がバランスされます。

この機能は次のとおりです。

- すべてのオンプレミスハイパーバイザー（VMware、XenServer、およびHyper-V）に適用されます。
- OSディスクストレージのみに適用されます。
- 既存のVMには適用されません。

負荷ベースの割り当てオプションを実装するには、ホスト接続の作成または更新時にカスタムプロパティ `Name="StorageBalanceType"` `Value="VMCountBasedLeastLoad` を追加します。このカスタムプロパティと値を使用しない場合、デフォルトで拡張ラウンドロビン方式が適用されます。

例：

- ホスト接続の作成時：

```
New-Item -CustomProperties "<CustomProperties xmlns=`"http://
schemas.citrix.com/2014/xd/machinecreation`" xmlns:xsi=`"http://
www.w3.org/2001/XMLSchema-instance`"><Property
xsi:type=`"StringProperty`" Name=`"StorageBalanceType`"
Value=`"VMCountBasedLeastLoad`" /></CustomProperties>"
-HypervisorConnectionName "Xen-Connection" -NetworkPath @("XDHyp:
\Connections\Xen-Connection\Network 0.network") -Path @("XDHyp:
\HostingUnits\XS-Network") -PersonalvDiskStoragePath @() -RootPath
"XDHyp:\Connections\Xen-Connection\" -StoragePath @("XDHyp:
\Connections\Xen-Connection\NFS virtual disk storage.storage")
```

- ホスト接続の更新時：

```
Set-Item  -CustomProperties "<CustomProperties xmlns=`"http://
schemas.citrix.com/2014/xd/machinecreation`" xmlns:xsi=`"http://
www.w3.org/2001/XMLSchema-instance`"><Property
xsi:type=`"StringProperty`" Name=`"StorageBalanceType`"
Value=`"VMCountBasedLeastLoad`" /></CustomProperties>" -Path @("XDHyp:
\HostingUnits\XS-Network")
```

孤立したAzureリソースの検出

孤立したリソースは、システム内に存在する使用されていないリソースであり、不要な費用につながる可能性があります。

クラウド管理者以外に、**ホスト**の下にある「**ハイパーバイザー内の孤立したリソースを検出するためにホスト接続を使用する**」権限を持つ新しく作成されたロールは、孤立したリソースを検出できます。

この機能を使用すると、Citrix Virtual Apps and Desktopsサイトのホストにある孤立したAzureリソースを検出できます。

Web Studioで次の手順を実行します。

1. **管理**から、左ペインで**ホスティング**を選択します。
2. 接続を選択し、アクションバーで**孤立したリソースの検出**を選択します。**孤立したリソースの検出**ダイアログボックスに、孤立したリソースレポートが表示されます。
3. 孤立したリソースレポートを表示するには、**レポートの表示**を選択します。

PowerShell を使用して、孤立した Azure リソースを検出することもできます。詳細については、「孤立したリソースのリストを取得する」を参照してください。

孤立したリソースの原因を理解し、その後の対処方法については、「Citrix を使用して孤立した Azure リソースを効率的に管理する」を参照してください。

接続タイマー

ポリシー設定を使用して、次の3つの接続タイマーを構成できます。

- **最大接続タイマー：** ユーザーデバイスと仮想デスクトップ間の途切れない接続の最大継続時間を決定します。**セッション接続タイマー**および**セッション接続タイマー間隔**のポリシー設定を使用します。
- **接続アイドルタイマー：** ユーザーからの入力がない場合に、仮想デスクトップへの途切れないユーザーデバイス接続が維持される期間を決定します。**セッションアイドルタイマー**および**セッションアイドルタイマー間隔**のポリシー設定を使用します。
- **切断タイマー：** 切断されロックされた仮想デスクトップが、セッションがログオフされる前にロックされたままになる期間を決定します。**切断セッションタイマー**および**切断セッションタイマー間隔**のポリシー設定を使用します。

これらの設定のいずれかを更新する場合は、展開全体で一貫性があることを確認してください。

詳細については、ポリシー設定のドキュメントを参照してください。

孤立したリソースのリストを取得する

MCSによって作成されたものの、MCSによって追跡されなくなった孤立したリソースのリストを取得できます。これは現在、Azure環境に適用されます。リストを取得するには、PowerShellコマンドを使用できます。接続を使用してフィルター処理できます。

デフォルトでは、**フル管理者**および**クラウド管理者**の役割にこの権限が割り当てられています。他の役割がこのアクションを実行できるようにするには、**ホスト**の下にある**ハイパーバイザーで孤立したリソースを検出するためにホスト接続を使用する**権限を割り当てます。詳細については、「役割の作成と管理」を参照してください。

注：

- プロビジョニングまたはイメージの更新が進行中の場合、PowerShellコマンドは拒否されます。
- すべてのCitrixタグが付けられた顧客管理リソースは、孤立したリソースとして検出されます。ただし、そのリソースに値がtrueのCitrixDetectIgnoreという別のタグを追加すると、孤立したリソースの検出時にそのリソースは無視されます。

制限事項

- 組み込みのフル管理者またはクラウド管理者ロールの管理者ユーザーのみが、PowerShellコマンドを実行して孤立したリソースのリストを取得できます。
- 孤立したリソースの誤認識を避けるため、孤立したリソースをフィルタリングしている間はVMの電源を入れないでください。
- 負荷が高い可能性がある場合、約2,000件のレコードが孤立していると表示されます。

孤立リソースのリストを表示するには：

1. **PowerShell**ウィンドウを開きます。
2. 次のコマンドを実行します：
   a. 接続UIDを取得します。接続UIDは、HypervisorConnectionUid属性の値です。

   ```
   Get-ChildItem xdhyp:\connections | where { $_.PluginId -like
   'Azure*' }"
   ```

   b. 孤立したリソースのリストを取得します。

   ```
   get-provorphanedresource -HypervisorConnectionUid <connection uid>
   ```

サブスクリプションIDから孤立リソースのリストを表示するには：

1. **PowerShell**ウィンドウを開きます。
2. 次のコマンドを実行します：
   a. サブスクリプションIDを使用して接続UIDを見つけます。接続UIDはHypervisorConnectionUid属性の値です。

```
Get-ChildItem xdhyp:\connections | where { $_.CustomProperties
-match '<subscriptionId>' }
```

b. 孤立したリソースのリストを取得します：

```
get-provorphanedresource -HypervisorConnectionUid <connection uid>
```

注:

削除する前にリソースを慎重に確認してください。

次のステップ

特定のホストタイプへの接続については、以下を参照してください。

- AWSへの接続
- XenServerへの接続
- Google Cloud環境への接続
- Microsoft Azureへの接続
- マイクロソフト システム センター バーチャル マシン マネージャー への接続
- Nutanixへの接続
- Nutanixクラウドおよびパートナーソリューションへの接続
- VMwareへの接続
- VMwareクラウドおよびパートナーソリューションへの接続

初期展開プロセス中の場合は、マシンカタログを作成します。

AWSへの接続

(/ja-jp/citrix-virtual-apps-desktops/2503/install-configure/connections.html)では、接続を作成するウィザードについて説明します。以下の情報では、AWSクラウド環境に固有の詳細について説明します。

注:

> AWSへの接続を作成する前に、まずAWSアカウントをリソースの場所として設定を完了する必要があります。(/ja-jp/citrix-virtual-apps-desktops/2503/install-configure/install-prepare/aws.html)を参照してください。

接続を作成する

Web Studioから接続を作成する場合：

- APIキーとシークレットキーの値を指定する必要があります。これらの値を含むキーファイルをAWSからエクスポートし、インポートできます。また、リージョン、アベイラビリティゾーン、VPC名、サブネットアドレス、ドメイン名、セキュリティグループ名、および資格情報も指定する必要があります。
- ルートAWSアカウントの資格情報ファイル（AWSコンソールから取得）は、標準のAWSユーザー向けにダウンロードされた資格情報ファイルと同じ形式ではありません。そのため、Citrix Virtual Apps and Desktops™管理では、このファイルを使用してAPIキーとシークレットキーのフィールドに値を入力することはできません。AWS Identity Access Management (IAM) 資格情報ファイルを使用していることを確認してください。

> **注:**
>
> 接続を作成した後、APIキーとシークレットキーの更新が失敗する場合があります。この問題を解決するには、プロキシサーバーまたはファイアウォールの制限を確認し、次のアドレスにアクセスできることを確認してください: `https://*.amazonaws.com`。

ホスト接続のデフォルト値

AWSクラウド環境でホスト接続を作成すると、次のデフォルト値が表示されます。

オプション	絶対値	パーセンテージ
同時実行アクション（すべての種類）	125	100
1分あたりの新規アクションの最大数	125	

MCS は、デフォルトで最大 100 の同時プロビジョニング操作をサポートしています。

クロスアカウントプロビジョニング

Delivery Controllerを、クロスアカウントアクセス（クロスアカウントIAMロール）を持つIAMロールとともにプライマリAWSアカウント（**共有サービスアカウント**または**サイトコンポーネントアカウント**）に配置し、MCSでプロビジョニングされたマシンカタログを別のセカンダリAWSアカウント（**ワークロードアカウント**）に配置するユースケースがあります。この場合、別のAWSアカウントに追加のDelivery Controllerは必要ありません。このようなシナリオをサポートするために、この機能はVPCピアリングとIAMロールを使用したクロスアカウントアクセスを利用して、複数のAWSアカウントを管理する企業向けに異なるAWSアカウント間でのプロビジョニングを可能にします。

VPCピアリングを使用すると、Delivery ControllerとプロビジョニングされたVMを異なるリージョンやアカウントに配置しても、相互に通信できるようになります。

IAMロールを使用したクロスアカウントアクセスを使用すると、プライマリアカウント（Delivery Controllerアカウント）がIAMロールを引き受けて、セカンダリアカウント（マシンカタログVM）内のAWSリソースにアクセスできるようになります。

Delivery Controllerがセカンダリアカウントのリソースにアクセスできるようにするには、セカンダリアカウントからIAMロールを引き受けた後にホスト接続を作成します。

前提条件

クロスアカウントプロビジョニング用のホスト接続を作成する前に、以下を設定してください。

- VPCピアリングを設定し、両方のリージョンまたはアカウントでセキュリティグループを構成します。「VPCピアリングの設定」を参照してください。
- IAMロールを使用してクロスアカウントアクセスを委任します。「（以下のトピックへのリンク）」を参照してください。

VPCピアリングを設定する

VPC Aがプライマリアカウント（アカウントA）にあり、Delivery ControllerとActive Directoryを持っていると仮定します。VPC Bは、VMをプロビジョニングしたいセカンダリアカウント（アカウントB）にあります。

アカウントAとアカウントBの間でVPCピアリング接続を設定するには、次の手順を実行します。

1. VPCピアリング接続を作成します。参照：
    - 異なるアカウント、同じリージョン
    - 異なるアカウント、異なるリージョン

2. VPC Aに移動し、パブリックサブネットに関連付けられているルートテーブルに移動します。
3. **>** をクリックします。 列にVPC BのCIDRブロックを追加し、 列に作成したVPCピアリングを追加します。
4. ステップ2と3を繰り返しますが、VPC AとVPC Bのプライベートサブネットを使用します（VPC AのCIDRブロックを追加します）。VPCピアリング接続のルートテーブルを更新するを参照してください。
5. VPC Aに関連付けられているプライベートセキュリティグループに移動します。
6. を選択し、 を選択します。
7. を選択します。タイプには を選択し、 列に以下を追加します。
   - 異なるリージョンの場合は、VPC BのCIDRブロック。
   - 異なるアカウントだが同じリージョンの場合は、VPC BのアカウントIDとプライベートセキュリティグループIDをスラッシュで区切って追加します（例: 123456789012/sg-1a2b3c4d）。
8. ステップ5から7を繰り返しますが、VPC Bのプライベートセキュリティグループを使用します（ただし、VPC AのCIDRブロック、または同じリージョンだが異なるアカウントのVPC Aのアカウント IDとプライベートセキュリティグループIDを追加します）。ピアセキュリティグループを参照するようにセキュリティグループを更新するを参照してください。

> 「**注：**」:

> VPCピアリング接続の作成に料金はかかりません。ただし、アベイラビリティーゾーン内のVPCピアリングは無料ですが、VPCピアリング接続を介したデータ転送が複数のアベイラビリティーゾーンやリージョンをまたがる場合は料金が発生します。詳細については、VPCピアリング接続の料金を参照してください。

IAMロールを使用したクロスアカウントアクセスの委任

アカウント間で VPC ピアリングを設定した後、IAM ロールを使用してクロスアカウントアクセスを委任します。

IAMロールを使用したクロスアカウントアクセスにより、プライマリアカウント（Delivery Controller™アカウント）はIAMロールを引き受けて、セカンダリアカウント（マシンカタログVM）内のAWSリソースにアクセスできます。

クロスアカウントリソースにアクセスするには、次の手順を実行します。

「注意：」：

VPC Aはプライマリアカウント（アカウントA）にあり、Delivery ControllerとActive Directoryがあります。VPC Bはセカンダリアカウント（アカウントB）にあり、VMをプロビジョニングする場所です。

1. 上記の手順で、アカウント間でVPCピアリングを設定します。
2. アカウントBで、最小限のCitrix IAM権限を持つIAMロールとポリシーを作成します。IAMチュートリアル：IAMロールを使用してAWSアカウント間でアクセスを委任するを参照してください。このロールのARNは「arn:aws:iam::5678:role/citrix-role」とします。
3. ロール「arn:aws:iam::5678:role/citrix-role」に信頼ポリシーを追加し、アカウントAのロール「arn:aws:iam::1234:role/primary-account-citrix-role」からアクセスできるようにします。詳細については、IAMでのクロスアカウントリソースアクセスを参照してください。
4. アカウントAで、上記で述べた「primary-account-citrix role」という名前のIAMロールとポリシーを作成します。これは、アカウントBのIAMロール（arn:aws:iam::5678:role/citrix-role）を引き受け、そのIAMロールを渡す機能を持っています。
5. アカウントAのすべてのDelivery Controllerに、ロール「arn:aws:iam::1234:role/primary-account-citrix-role」を割り当てます。

Delivery Controller は、アカウント B のロール（「arn:aws:iam::5678:role/citrix-role」）を引き受けることができるようになりました。

クロスアカウントプロビジョニング用のホスト接続を作成する

VMをプロビジョニングするセカンダリアカウント（アカウントB）でホスト接続を作成します。これにより、アカウントAのDelivery Controllerは、アカウントBからロールを引き受けた後、アカウントBのリソースにアクセスできるようになります。

PowerShell コマンドを使用してホスト接続を作成し、次の2つのカスタムプロパティを追加します。

- `CrossAccountRoleArn`: `CrossAccountRoleArn` プロパティを指定しない場合、通常のホスト接続が作成されます。この場合、`MaximumAssumeRoleDurationInSeconds` が指定されていても無視されます。
- `MaximumAssumeRoleDurationInSeconds`: `DurationInSeconds` は900秒から3600秒の間である必要があります。デフォルトは900秒です。3600を超える値を指定した場合、`DurationInSeconds` は3600に設定されます。

例:

```
$connectionName = "cross-account-conn"

$cloudRegion = "us-east-1"

$apiKey = "role_based_auth"

$secretKey = "role_based_auth"

$zoneUid = "xxxxxx"

$secureKey = (ConvertTo-SecureString -String $secretKey -AsPlainText
-Force)

$connectionPath = "XDHyp:\Connections\" + $connectionName

$customProperties = '<CustomProperties xmlns="http://schemas.citrix.com/
2014/xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="CrossAccountRoleArn"
Value="arn:aws:iam::5678:role/citrix-role" /><Property
xsi:type="StringProperty" Name="MaximumAssumeRoleDurationInSeconds"
Value="3600" />

"</CustomProperties>'



$connection = New-Item -Path $connectionPath -ConnectionType "AWS"
-HypervisorAddress "https://ec2.$($cloudRegion).amazonaws.com" -Persist
-Scope @() -UserName $apiKey -SecurePassword $secureKey -ZoneUid $zoneUid
-CustomProperties $customProperties



New-BrokerHypervisorConnection -HypHypervisorConnectionUid
$connection.HypervisorConnectionUid
```

ホスト接続が作成されたら、Studio または PowerShell を使用してホスティングユニットを作成します。ただし、VPC とネットワークを選択してください。

サービスエンドポイントURL

標準ゾーンサービスエンドポイントURL

MCSを使用すると、APIキーとAPIシークレットを持つ新しいAWS接続が追加されます。この情報と認証済みアカウントを使用して、MCSはAWS DescribeRegions EC2 API呼び出しを使用して、サポートされているゾーンについてAWSにクエリを実行します。クエリは汎用EC2サービスエンドポイントURL `https://ec2.amazonaws.com/` を使用して行われます。MCSを使用して、サポートされているゾーンのリストから接続するゾーンを選択します。優先されるAWSサービスエンドポイントURLは、そのゾーンに対して自動的に選択されます。ただし、サービスエンドポイントURLを作成した後、そのURLを設定または変更することはできません。

IAM権限を定義する

このセクションの情報を使用して、AWS 上の Citrix Virtual Apps and Desktops の IAM 権限を定義します。Amazon の IAM サービスは、複数のユーザーを持つアカウントを許可しており、それらのユーザーはさらにグループに編成できます。これらのユーザーは、アカウントに関連する操作を実行する能力を制御するために、異なる権限を持つことができます。IAM 権限の詳細については、IAM JSON ポリシーリファレンス を参照してください。

新しいユーザーグループにIAM権限ポリシーを適用するには：

1. AWSマネジメントコンソールにログインし、ドロップダウンリストから**IAMサービス**を選択します。
2. **新しいユーザーグループの作成**を選択します。
3. 新しいユーザーグループの名前を入力し、**続行**を選択します。
4. 「**Permissions**」ページで、「**Custom Policy**」を選択します。「**Select**」を選択します。
5. 「**Permissions policy**」の名前を入力します。
6. 「**Policy Document**」セクションで、関連する権限を入力します。

ポリシー情報を入力した後、「**Continue**」を選択してユーザーグループを完了します。グループ内のユーザーには、Citrix Virtual Apps and Desktopsに必要なアクションのみを実行する権限が付与されます。

> 「**重要:**」：

> 前述の例で提供されているポリシーテキストを使用して、Citrix Virtual Apps and DesktopsがAWSアカウント内でアクションを実行するために使用するアクションを、特定のリソースに

> 制限することなくリストします。Citrixは、テスト目的でこの例を使用することを推奨します。実稼働環境では、リソースにさらなる制限を追加することを選択できます。

IAM権限を設定する

AWSマネジメントコンソールの**IAM**セクションで権限を設定します。

1. **概要**パネルで、**アクセス許可**タブを選択します。
2. **アクセス許可の追加**を選択します。

アイデンティティおよびアクセス管理 (IAM)(/en-us/citrix-virtual-apps-desktops/2503/media/aws-iam-users.png)

アクセス許可の追加先画面で、アクセス許可を付与します。

IAMポリシーの権限を付与する(/en-us/citrix-virtual-apps-desktops/2503/media/aws-iam-grant-permissions.png)

「**JSON**」タブで、以下を例として使用します。

JSONの例(/en-us/citrix-virtual-apps-desktops/2503/media/aws-iam-json-example.png)

> **ヒント:**
>
> 記載されているJSONの例には、お使いの環境に必要なすべての権限が含まれていない場合があります。詳細については、「How to Define Identity Access Management Permissions Running Citrix Virtual Apps and Desktops on AWS」を参照してください。

必要なAWS権限

このセクションには、AWS権限の完全なリストが含まれています。

> **注：**
>
> *iam:PassRole*権限は、**role_based_auth**の場合にのみ必要です。

ホスト接続の作成

AWSからの情報を使用して、新しいホスト接続が追加されます。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:DescribeRegions"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

VM の電源管理

VMの電源がオンまたはオフになります。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
```

```
                "ec2:DescribeInstances",
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:RebootInstances",
                "ec2:DescribeInstanceStatus"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

仮想マシンの作成、更新、または削除

AWSインスタンスとしてプロビジョニングされたVMを使用して、マシンカタログが作成、更新、または削除されます。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:AttachVolume",
                "ec2:AssociateIamInstanceProfile",
                "ec2:AuthorizeSecurityGroupEgress",
```

```
                "ec2:RevokeSecurityGroupEgress",

                "ec2:AuthorizeSecurityGroupIngress",

                "ec2:CreateImage",

                "ec2:CreateLaunchTemplate",

                "ec2:CreateSecurityGroup",

                "ec2:CreateTags",

                "ec2:CreateVolume",

                "ec2:DeleteVolume",

                "ec2:DescribeAccountAttributes",

                "ec2:DescribeAvailabilityZones",

                "ec2:DescribeIamInstanceProfileAssociations",

                "ec2:DescribeImages",

                "ec2:DescribeInstances",

                "ec2:DescribeInstanceTypes",

                "ec2:DescribeInstanceStatus",

                "ec2:DescribeLaunchTemplates",

                "ec2:DescribeLaunchTemplateVersions",

                "ec2:DescribeNetworkInterfaces",

                "ec2:DescribeRegions",

                "ec2:DescribeSecurityGroups",

                "ec2:DescribeSnapshots",

                "ec2:DescribeSubnets",
```

```
                "ec2:DescribeTags",

                "ec2:DescribeSpotInstanceRequests",

                "ec2:DescribeInstanceCreditSpecifications",

                "ec2:DescribeInstanceAttribute",



                "ec2:GetLaunchTemplateData",

                "ec2:DescribeVolumes",

                "ec2:DescribeVpcs",

                "ec2:DetachVolume",

                "ec2:DisassociateIamInstanceProfile",

                "ec2:RunInstances",

                "ec2:StartInstances",

                "ec2:StopInstances",

                "ec2:TerminateInstances"

            ],

            "Effect": "Allow",

            "Resource": "*"

        },

        {

            "Action": [

                "ec2:CreateSecurityGroup",

                "ec2:DeleteSecurityGroup"
```

```
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "ebs:StartSnapshot",
                "ebs:GetSnapshotBlock",
                "ebs:PutSnapshotBlock",
                "ebs:CompleteSnapshot",
                "ebs:ListSnapshotBlocks",
                "ebs:ListChangedBlocks",
                "ec2:CreateSnapshot"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

注：

セキュリティグループに関連するEC2セクションは、カタログ作成時に準備VM用に分離セキュリティグループを作成する必要がある場合にのみ必要です。これが完了すると、これらの権限は不要になります。

直接ディスクのアップロードとダウンロード

直接ディスクアップロードは、マシンカタログのプロビジョニングにおけるボリュームワーカーの要件を排除し、代わりにAWSが提供するパブリックAPIを使用します。この機能により、追加のストレージアカウントに関連するコストが削減され、ボリュームワーカー操作の維持に関する複雑さが軽減されます。

注:

ボリュームワーカーのサポートは削除されました。マシンカタログプロビジョニングには、直接ディスクのアップロードおよびダウンロードの権限が必要です。

以下の権限をポリシーに追加する必要があります。

- `ebs:StartSnapshot`
- `ebs:GetSnapshotBlock`
- `ebs:PutSnapshotBlock`
- `ebs:CompleteSnapshot`
- `ebs:ListSnapshotBlocks`
- `ebs:ListChangedBlocks`
- `ec2:CreateSnapshot`
- `ec2:DeleteSnapshot`
- `ec2:DescribeLaunchTemplates`

重要:

- ボリュームワーカーAMIやボリュームワーカーVMなどのボリュームワーカー操作なしで、既存のマシンカタログにVMを追加できます。

- 以前にボリュームワーカーを使用していた既存のカタログを削除すると、ボリュームワーカー関連を含むすべてのアーティファクトが削除されます。

作成されたボリュームのEBS暗号化

AMIが暗号化されている場合、またはEBSがすべての新しいボリュームを暗号化するように構成されている場合、EBSは新しく作成されたボリュームを自動的に暗号化できます。ただし、この機能を実装するには、IAMポリシーに以下の権限を含める必要があります。

```
{

     "Version": "2012-10-17",

     "Statement": [

        {

            "Effect": "Allow",

            "Action": [

                 "kms:CreateGrant",

                 "kms:Decrypt",

                 "kms:DescribeKey",

                 "kms:GenerateDataKeyWithoutPlainText",

                 "kms:GenerateDataKey",

                 "kms:ReEncryptTo",

                 "kms:ReEncryptFrom"

            ],

            "Resource": "*"

        }

    ]
```

```
}
```

注:

権限は、ユーザーの裁量でリソースと条件ブロックを含めることにより、特定のキーに制限できます。例：**条件付きKMS権限**：

```
{

     "Version": "2012-10-17",

     "Statement": [

        {

            "Effect": "Allow",

            "Action": [

                 "kms:CreateGrant",

                 "kms:Decrypt",

                 "kms:DescribeKey",

                 "kms:GenerateDataKeyWithoutPlainText",

                 "kms:GenerateDataKey",

                 "kms:ReEncryptTo",

                 "kms:ReEncryptFrom"

            ],

            "Resource": [

                "arn:aws:kms:us-east-2:123456789012:key/abcd1234-
a123-456d-a12b-a123b4cd56ef"
```

```
            ],
            "Condition": {
                "Bool": {
                    "kms:GrantIsForAWSResource": true
                }
            }
        }
    ]
}
```

以下のキーポリシーステートメントは、アカウントがIAMポリシーを使用してKMSキーに対するすべてのアクション (kms:*) の権限を委任できるようにするために必要な、KMSキーのデフォルトキーポリシー全体です。

```
{
"Sid": "Enable IAM policies",
"Effect": "Allow",
"Principal": {
"AWS": "arn:aws:iam::111122223333:root"
},
"Action": "kms:",
"Resource": ""
}
```

詳細については、「AWS Key Management Service 公式ドキュメント」を参照してください。

IAMロールベース認証

ロールベース認証をサポートするために、以下の権限が追加されます。

```
{

     "Version": "2012-10-17",

     "Statement": [

        {

            "Effect": "Allow",

            "Action": "iam:PassRole",

            "Resource": "arn:aws:iam::*:role/*"

        }

    ]

}
```

最小限のIAM権限ポリシー

以下のJSONは、現在サポートされているすべての機能に使用できます。このポリシーを使用して、ホスト接続の作成、VMの作成、更新、削除、および電源管理を行うことができます。 このポリシーは、IAM権限の定義セクションで説明されているようにユーザーに適用することも、**role_based_auth**セキュリティキーとシークレットキーを使用してロールベース認証を使用することもできます。

> **重要:**
>
> **role_based_auth** を使用するには、まずサイト内のすべてのDelivery Controllerで目的のIAMロールを構成します。Web Studioを使用してホスティング接続を追加し、認証キーとシークレットに role_based_auth を指定します。これらの設定を持つホスティング接続は、ロールベース認証を使用します。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:AttachVolume",
                "ec2:AssociateIamInstanceProfile",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateImage",
                "ec2:CreateLaunchTemplate",
                "ec2:CreateNetworkInterface",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:DeleteLaunchTemplate",
                "ec2:DeleteNetworkInterface",
                "ec2:DeleteSecurityGroup",
                "ec2:DeleteSnapshot",
                "ec2:DeleteTags",
                "ec2:DeleteVolume",
                "ec2:DeregisterImage",
```

```
                "ec2:DescribeAccountAttributes",

                "ec2:DescribeAvailabilityZones",

                "ec2:DescribeIamInstanceProfileAssociations",

                "ec2:DescribeImages",

                "ec2:DescribeInstances",

                "ec2:DescribeInstanceTypes",

                "ec2:DescribeInstanceStatus",

                "ec2:DescribeLaunchTemplates",

                "ec2:DescribeLaunchTemplateVersions",

                "ec2:DescribeNetworkInterfaces",

                "ec2:DescribeRegions",

                "ec2:DescribeSecurityGroups",

                "ec2:DescribeSnapshots",

                "ec2:DescribeSubnets",

                "ec2:DescribeTags",

                "ec2:DescribeSpotInstanceRequests",

                "ec2:DescribeInstanceCreditSpecifications",

                "ec2:DescribeInstanceAttribute",

                "ec2:GetLaunchTemplateData",

                "ec2:DescribeVolumes",

                "ec2:DescribeVpcs",

                "ec2:DetachVolume",
```

```
                "ec2:DisassociateIamInstanceProfile",
                "ec2:RebootInstances",
                "ec2:RunInstances",
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "ec2:CreateSecurityGroup",
                "ec2:DeleteSecurityGroup"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "ebs:StartSnapshot",
                "ebs:GetSnapshotBlock",
```

```
                "ebs:PutSnapshotBlock",
                "ebs:CompleteSnapshot",
                "ebs:ListSnapshotBlocks",
                "ebs:ListChangedBlocks",
                "ec2:CreateSnapshot"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                 "kms:CreateGrant",
                 "kms:Decrypt",
                 "kms:DescribeKey",
                 "kms:GenerateDataKeyWithoutPlainText",
                 "kms:GenerateDataKey",
                 "kms:ReEncryptTo",
                 "kms:ReEncryptFrom"
            ],
            "Resource": "*"
        },
```

```
        {
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "arn:aws:iam::*:role/*"
        }
    ]
}
```

注:

- SecurityGroupsに関連するEC2セクションは、カタログ作成中に準備VM用に分離セキュリティグループを作成する必要がある場合にのみ必要です。これが完了すると、これらの権限は不要になります。
- KMSセクションは、EBSボリューム暗号化を使用する場合にのみ必要です。
- iam:PassRole 権限セクションは、**role_based_auth** の場合にのみ必要です。
- 要件と環境に基づいて、フルアクセスではなく特定のリソースレベルの権限を追加できます。詳細については、AWSドキュメントのDemystifying EC2 Resource-Level Permissions および Access management for AWS resources を参照してください。

ホスト接続の権限を検証する

ホスト接続の権限を検証して、MCSマシンカタログの作成と管理に関連するタスクを実行できます。この実装により、VMの作成、削除、更新、VMの電源管理、EBS暗号化など、さまざまなシナリオで必要な不足している権限を事前に特定できるため、重要な時期にブロックされるのを回避できます。

PowerShellコマンド`Test-HypHypervisorConnection`を使用して、ホスト接続の権限を検証できます。コマンドの結果はリストとしてキャプチャされ、リスト内の各項目は3つのセクションに分かれています。

- カテゴリ: ユーザーがMCSマシンカタログを作成および管理するために実行できるアクションまたはタスク。
- 修正措置: 管理者がユーザーの不足している権限の不一致を解決するために実行する必要がある手順。
- 不足している権限: カテゴリの不足している権限のリスト。

権限を検証するには、次の手順を実行します。

1. AWSへのホスト接続を作成します。
2. Delivery ControllerホストからPowerShellウィンドウを開きます。
3. Citrix固有のPowerShellモジュールをロードするために`asnp citrix*`を実行します。
4. 以下のコマンドを実行して、権限を検索するために必要な権限があるかどうかを確認します。

   ```
   Test-HypHypervisorConnection -LiteralPath "XDHyp:\Connections\AWSCon"
   ```

5. 権限を検索するために必要な不足している権限を追加した後、以下のコマンドを実行して、次のカテゴリに権限があるかどうかを確認します。

   - 作成、更新、削除
   - 電源管理
   - EBS暗号化

   ```
   Test-HypHypervisorConnection -LiteralPath "XDHyp:
   \Connections\AWSCon" [-SecurePassword -Password] "password" -UserName
   "" -CustomProperties ""
   ```

権限の追加の詳細については、「IAM権限の設定」を参照してください。

次のステップ

- 初期展開プロセス中の場合は、「マシンカタログの作成」を参照してください。
- AWS固有の情報については、AWSカタログの作成を参照してください。

詳細情報

- 接続とリソース
- マシンカタログの作成

XenServer®への接続

接続とリソースの作成および管理では、接続を作成するウィザードについて説明します。以下の情報は、XenServer仮想化環境に固有の詳細を扱っています。

> **注:**
>
> XenServerへの接続を作成する前に、まずXenServerアカウントをリソースの場所として設定を完了する必要があります。XenServer仮想化環境を参照してください。

XenServerへの接続を作成する

XenServer（旧Citrix Hypervisor™）への接続を作成する際は、VM Power Admin以上のユーザーの資格情報を指定する必要があります。

Citrixでは、XenServerとの通信を保護するためにHTTPSを使用することをお勧めします。HTTPSを使用するには、XenServerにインストールされているデフォルトの SSL証明書を置き換える必要があります。

XenServerサーバーで高可用性が有効になっている場合、高可用性を構成できます。Citrix Virtual Apps and Desktopsのバージョン2507 LTSRより前のバージョンでは、プール内のすべてのサーバーにワイルドカード証明書をインストールすることはできません。各サーバーに個別の証明書が必要です。

XenServerがvGPUをサポートしている場合、GPUの種類とグループを選択するか、パススルーすることができます。表示には、選択したものが専用のGPUリソースを持っているかどうかが示されます。

1つ以上のXenServerホストで一時データストレージにローカルストレージを使用する場合は、プール内の各ストレージの場所に一意の名前があることを確認してください。（XenCenter®で名前を変更するには、ストレージを右クリックして名前プロパティを編集します。）

Citrix Provisioning（旧Provisioning Services）およびMachine Creation Services™（MCS）を使用して、以下をプロビジョニングできます。

- サポートされているデスクトップまたはサーバーOS VMのレガシーBIOS。
- Secure Bootを含む、サポートされているデスクトップまたはサーバーOS VMのUEFI。

> **注:**

> MCSを構成する際には、プールオペレーター以上の権限が必要です。

XenServer接続でIntelliCache™を使用する

IntelliCacheを使用すると、共有ストレージとローカルストレージの組み合わせを使用できるため、ホスト型VDI展開はより費用対効果が高くなります。これにより、パフォーマンスが向上し、ネットワークトラフィックが削減されます。ローカルストレージは共有ストレージからマスターイメージをキャッシュし、共有ストレージへの読み取り回数を減らします。共有デスクトップの場合、差分ディスクへの書き込みは、共有ストレージではなくホスト上のローカルストレージに書き込まれます。

- IntelliCacheを使用する場合、共有ストレージはNFSである必要があります。
- Citrixは、可能な限り最速のデータ転送を確保するために、高性能なローカルストレージデバイスを使用することを推奨します。

IntelliCacheを使用するには、この製品とXenServerの両方で有効にする必要があります。

- XenServerをインストールする際、「**シンプロビジョニングを有効にする (仮想デスクトップ向けに最適化されたストレージ)**」を選択します。Citrixは、IntelliCacheが有効なサーバーと無効なサーバーが混在するプールをサポートしていません。詳細については、XenServerのドキュメントを参照してください。
- Citrix Virtual Apps and Desktops™では、IntelliCacheはデフォルトで無効になっています。この設定はXenServer接続を作成するときにのみ変更でき、後でIntelliCacheを無効にすることはできません。XenServer接続を追加する際：
  - ストレージの種類として「**共有**」を選択します。
  - 「**IntelliCacheを使用**」チェックボックスをオンにします。

必要なXenServer権限

XenServerの権限はロールベース (RBAC) です。XenServerのロールベースアクセス制御 (RBAC) 機能を使用すると、ユーザー、ロール、および権限を割り当てて、XenServerへのアクセス権を持つユーザーと実行できるアクションを制御できます。XenServer RBACシステムは、ユーザー (またはユーザーグループ) を定義されたロール (名前付きの権限セット) にマッピングします。ロールには、特定の操作を実行するための関連するXenServer権限があります。

詳細については、「Role-based access control」を参照してください。

権限が増加する順序でのロール階層は次のとおりです：読み取り専用 → VMオペレーター → VM管理者 → VM電源管理者 → プールオペレーター → プール管理者。

次のセクションでは、各プロビジョニングタスクに必要な最小ロールをまとめます。

ホスト接続の作成

タスク	必要な最小ロール
XenServerから取得した情報を使用してホスト接続を追加する	読み取り専用
ユーザーとその割り当てられた役割を表示する	読み取り専用

VMの電源管理

タスク	必要な最小限の役割
VMの電源をオンまたはオフにする	VMオペレーター

VMの作成、更新、または削除

タスク	必要な最小限の役割
既存のスナップショットスケジュールにVMを追加または削除する	VM電源管理者
スナップショットスケジュールの追加、変更、削除	プールオペレーター
マスターイメージの公開	プールオペレーター（スイッチポートロックが必要）
マシンカタログの作成	プールオペレーター: スイッチポートロックが必要
VM の追加または削除 (GPU が有効でない VM)	VM 管理者
VM の追加または削除 (GPU が有効な VM)	プールオペレーター
仮想ディスクまたはCDデバイスの追加、削除、または構成	VM 管理者
タグの管理	VM オペレーター

RBACの役割と権限の詳細については、RBAC roles and permissionsを参照してください。

スイッチポートロックの詳細については、Use switch port lockingを参照してください。

次のステップ

- 初期展開プロセス中の場合、Create machine catalogsを参照してください
- XenServer固有の情報については、Create a XenServer catalogを参照してください

詳細情報

- 接続とリソース
- マシンカタログの作成

Google Cloud環境への接続

「接続とリソースの作成および管理」(/ja-jp/citrix-virtual-apps-desktops/2503/install-configure/connections.html)では、接続を作成するウィザードについて説明しています。以下の情報は、Google Cloud環境に固有の詳細を扱っています。

> **注:**
>
> Google Cloud環境への接続を作成する前に、まずGoogle Cloudアカウントをリソースの場所として設定を完了する必要があります。「Google Cloud環境」(/ja-jp/citrix-virtual-apps-desktops/2503/install-configure/install-prepare/gcp.html)を参照してください。

接続を追加する

「接続とリソースの作成」(/ja-jp/citrix-virtual-apps-desktops/2503/manage-deployment/connections.html)のガイダンスに従ってください。以下の説明は、ホスティング接続の設定方法を案内します。

1. **管理 > 構成**から、左側のペインで**ホスティング**を選択します。
2. アクションバーで**「接続とリソースの追加」**を選択します。
3. **「接続」ページで、「新しい接続の作成」と「Citrix provisioning™ tools」を選択し、「次へ」**を選択します。
    - **接続の種類**。メニューから**Google Cloud**を選択します。
    - **接続名**。接続の名前を入力します。

4. **リージョン**ページで、メニューからプロジェクト名を選択し、使用するリソースを含むリージョンを選択してから、**次へ**を選択します。
5. **ネットワーク**ページで、リソースの名前を入力し、メニューから仮想ネットワークを選択し、サブセットを選択してから、**次へ**を選択します。リソース名は、リージョンとネットワークの組み合わせを識別するのに役立ちます。名前に*(Shared)*サフィックスが付いている仮想ネットワークは、共有VPCを表します。共有VPCのサブネットレベルのIAMロールを構成した場合、共有VPCの特定のサブネットのみがサブネットリストに表示されます。

   > **注:**
   >
   > - リソース名には1～64文字を含めることができ、空白のみ、または文字`\ / ; : # . * ? = < > | [ ] { } " ' ( ) ' )`を含めることはできません。

6. **概要**ページで情報を確認し、**完了**を選択して**接続とリソースの追加**ウィンドウを終了します。

接続とリソースを作成すると、作成した接続とリソースが一覧表示されます。接続を構成するには、接続を選択し、アクションバーで該当するオプションを選択します。

同様に、接続の下に作成されたリソースを削除、名前変更、またはテストできます。これを行うには、接続の下にあるリソースを選択し、アクションバーで該当するオプションを選択します。

サービスエンドポイントURL

次のURLにアクセスできる必要があります。

- `https://oauth2.googleapis.com`
- `https://cloudresourcemanager.googleapis.com`
- `https://compute.googleapis.com`
- `https://storage.googleapis.com`
- `https://cloudbuild.googleapis.com`

Google Cloudプロジェクト

Google Cloudプロジェクトには基本的に2つのタイプがあります。

- プロビジョニングプロジェクト：この場合、現在の管理者アカウントがプロジェクト内のプロビジョニングされたマシンを所有します。このプロジェクトはローカルプロジェクトとも呼ばれます。

- 共有VPCプロジェクト：プロビジョニングプロジェクトで作成されたマシンが共有VPCプロジェクトのVPCを使用するプロジェクト。プロビジョニングプロジェクトに使用される管理者アカウントは、このプロジェクトで限られた権限、具体的にはVPCを使用する権限のみを持ちます。

GCP管理トラフィックのセキュアな環境を作成する

Google Cloudプロジェクトへのプライベートアクセスを許可できます。この実装により、機密データを処理するためのセキュリティが強化されます。これを実現するには、次のいずれかを実行できます。

- Cloud BuildサービスアカウントのVPCサービスコントロールの以下のイングレスルールを含めます。この手順を実行する場合は、GCPマネージドトラフィックのセキュアな環境を作成するための以下の手順に従わないでください。

```
Ingress Rule 1

From:

Identities:

<ProjectID>@cloudbuild.gserviceaccount.com

Source > All sources allowed

To:

Projects =

All projects

Services =

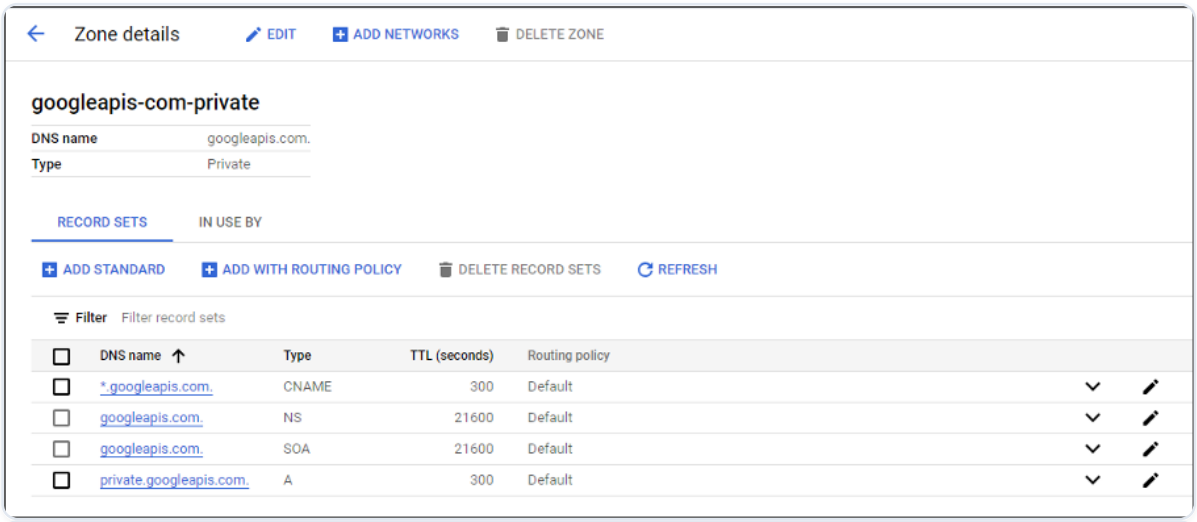
Service name: All services
```

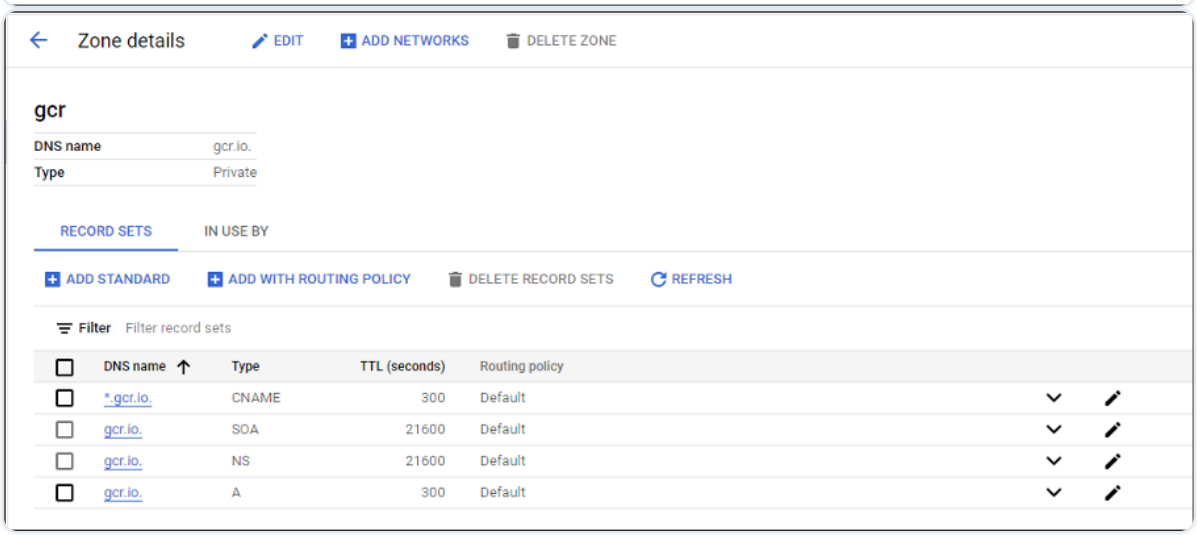
- プライベートワーカープールを使用している場合は、`CustomProperties`に`UsePrivateWorkerPool`を追加します。プライベートワーカープールの詳細については、プライベートプール概要を参照してください。

GCPマネージドトラフィックのセキュアな環境を作成するための要件

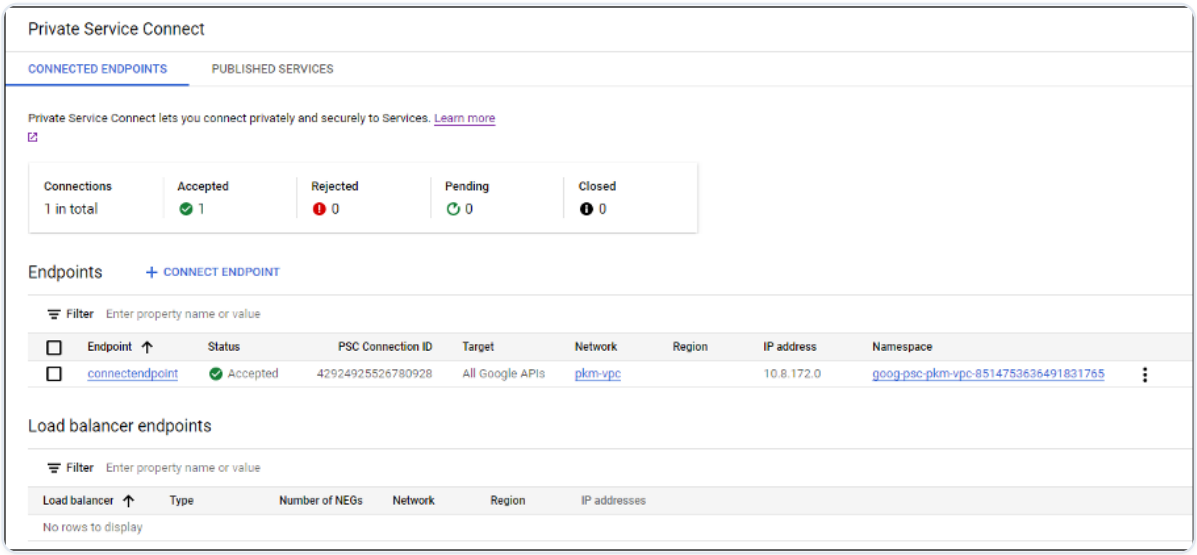
GCPマネージドトラフィックのセキュアな環境を作成するための要件は次のとおりです。

- カスタムプロパティを更新する際は、ホスティング接続がメンテナンスモードであることを確認してください。
- プライベートワーカープールを使用するには、次の変更が必要です。
  - Citrix Cloud™サービスアカウントには、次のIAMロールを追加します。
    - Cloud Build サービスアカウント
    - Compute Instance 管理者
    - サービスアカウントユーザー
    - サービスアカウントトークン作成者
    - Cloud Build WorkerPool 所有者
  - ホスティング接続の作成に使用するのと同じプロジェクトに、Citrix Cloudサービスアカウントを作成します。
  - DNS構成で説明されているように、`private.googleapis.com`と`gcr.io`のDNSゾーンを設定します。

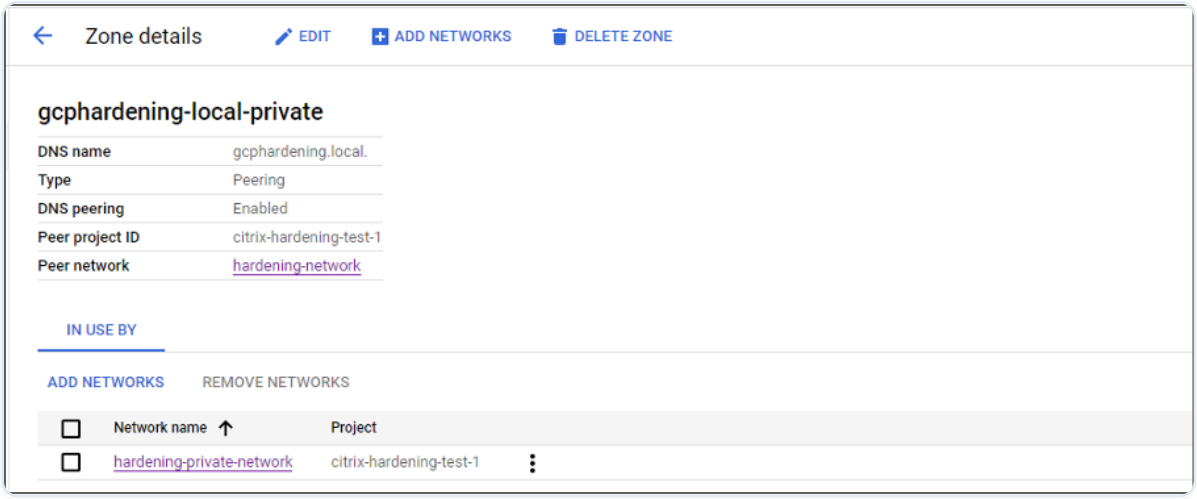




- プライベートネットワークアドレス変換 (NAT) を設定するか、プライベートサービス接続を使用します。詳細については、「エンドポイントを介した Google API へのアクセス」を参照してください。



- ピアリングされた VPC を使用している場合は、ピアリングされた VPC への Cloud DNS ゾーンピアリングを作成します。詳細については、「ピアリングゾーンの作成」を参照してください。



- VPC サービスコントロールで、API と VM がインターネットと通信できるようにエグレスルールを設定します。イングレスルールはオプションです。例:

```
Egress Rule 1

From:

Identities:ANY_IDENTITY

To:
```

```
Projects =

All projects

Service =

Service name: All services
```

プライベートワーカープールを有効にする

プライベートワーカープールを有効にするには、ホスト接続でカスタムプロパティを次のように設定します。

1. Delivery Controller ホストから PowerShell ウィンドウを開くか、Remote PowerShell SDK を使用します。Remote PowerShell SDK の詳細については、「SDK と API」を参照してください。
2. 次のコマンドを実行します。
   a. `Add-PSSnapin citrix*`
   b. `cd XDHyp:\Connections\`
   c. `dir`
3. 接続から `CustomProperties` をメモ帳にコピーします。
4. プロパティ設定 `<Property xsi:type="StringProperty" Name="UsePrivateWorkerPool" Value="True"/>` を追加します。例:

   ```
   ```

   <CustomProperties xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
   xmlns="http://schemas.citrix.com/2014/xd/machinecreation">

   <Property xsi:type="StringProperty" Name="UsePrivateWorkerPool"
   Value="True"/>

   </CustomProperties>

   ```
   ```

5. PowerShell ウィンドウで、変更されたカスタムプロパティに変数を割り当てます。例: `$customProperty = '<CustomProperties…</CustomProperties>'`。

6. `$gcpServiceAccount = "<ENTER YOUR SERVICE ACCOUNT EMAIL HERE>"` を実行します。
7. `$gcpPrivateKey = "<ENTER YOUR SERVICE ACCOUNT PRIVATE KEY HERE AFTER REMOVING ALL INSTANCES OF \n >"` を実行します。
8. `$securePassword = ConvertTo-SecureString $gcpPrivateKey -AsPlainText -Force` を実行します。
9. 既存のホスト接続を更新するには、以下を実行します。

```
Set-Item -PassThru -Path @('XDHyp:\\Connections\\<ENTER YOUR CONNECTION NAME HERE>') -SecurePassword $securePassword -UserName $gcpServiceAccount -CustomProperties $customProperty
```

CMEK のグローバルキーとリージョンキーを指定する

> **注:**
>
> GCP での CMEK のサポートは現在プレビュー中です。

> GCP には、顧客管理の暗号化キー (CMEK) が 2 種類あります。

- リージョン：同じリージョン内のリソースのみが使用できる暗号化キー。
- グローバル：複数のリージョンのリソースが使用できる暗号化キー。

サービスアカウントがアクセスできるすべてのプロジェクトから、グローバルまたはリージョンの顧客管理の暗号化キー (CMEK) を参照して使用できます。その後、そのキーを使用して CMEK が有効な MCS マシンカタログを作成し、`Set-ProvScheme` コマンドを使用して既存の CMEK が有効な MCS マシンカタログを更新できます。PowerShell を使用して CMEK が有効なカタログを作成する方法については、「カスタムプロパティを使用して CMEK でカタログを作成する」を参照してください。

この機能には、次の 2 つのサービスアカウントに対する追加の権限が必要です。

- ホスティング接続が作成される現在のプロジェクトのサービスアカウント。
- 現在のプロジェクトのCompute Engineサービスエージェント (メールアドレス: `service-PROJECT_NUMBER@compute-system.iam.gserviceaccount.com` を持つもの)。詳細については、Compute Engine Service Agent を参照してください。

サービスアカウントでは、使用したい暗号鍵を持つプロジェクト (例: 共有プロジェクト) に、次のロールを割り当てる必要があります。

- Cloud KMS閲覧者
- Cloud KMS クリプトキー 暗号化担当者/復号担当者

ロールを割り当てない場合は、次の権限があることを確認してください。

- resourcemanager.projects.get
- cloudkms.keyRings.list
- cloudkms.keyRings.get
- cloudkms.cryptoKeys.get
- cloudkms.cryptoKeys.list
- cloudkms.cryptoKeyVersions.useToDecrypt
- cloudkms.cryptoKeyVersions.useToEncrypt

暗号化キーを一覧表示する

PowerShellコマンドを使用して、同じプロジェクト内およびアクセス可能な他のすべてのプロジェクト内のグローバルおよびリージョンの暗号化キーを一覧表示できます。これを行うには:

1. Delivery Controller™ホストまたはリモートPowerShellからPowerShellウィンドウを開きます。
2. Citrix固有のPowerShellモジュールをロードするには、`asnp citrix*`コマンドを実行します。
3. 暗号化キーを一覧表示するには、次のコマンドを実行します。例:
   - `encryptionKeys`フォルダーの内容を一覧表示するには:

     ```
     Get-ChildItem XDHyp:\HostingUnits\my-
     hostingunit\encryptionKeys.folder
     ```

   - 同じプロジェクト内のグローバル暗号化キーを取得するには:

     ```
     Get-Item XDHyp:\HostingUnits\my-
     hostingunit\encryptionKeys.folder\myglobalkeyring.globalkeyring\mygl
     obalkey.cryptokey
     ```

   - 同じプロジェクト内のリージョン暗号化キーを取得するには:

```
Get-Item XDHyp:\HostingUnits\my-
hostingunit\encryptionKeys.folder\regional-ring.keyring\shared-
key.cryptokey
```

- 別のアクセス可能なプロジェクト（例: myanotherproject）からグローバル暗号化キーを取得するには:

```
Get-Item XDHyp:\HostingUnits\my-
hostingunit\encryptionKeys.folder\myanotherproject.project\shared-
global-ring.globalkeyring\shared-key.cryptokey
```

- 別のアクセス可能なプロジェクト（例: myanotherproject）からリージョン暗号化キーを取得するには:

```
Get-Item XDHyp:\HostingUnits\my-
hostingunit\encryptionKeys.folder\myanotherproject .project.project\
shared-uscentral.keyring\shared-uscentral-key.cryptokey
```

注:

- グローバルキーリングのキーリングインベントリアイテムの拡張子は`.globalkeyring`です。
- グローバルキーリングのIDには、`global`という単語が含まれています。

必要なGCP権限

このセクションには、GCP権限の完全なリストが含まれています。機能が正しく動作するように、このセクションに記載されている権限の完全なセットを使用してください。

注:

GCP は、April 29, 2024 以降、Cloud Build Services のデフォルトの動作とサービスアカウントの使用に変更を導入しています。詳細については、Cloud Build Service Account Change を参照してください。April 29, 2024 より前に Cloud Build API が有効になっている既存の Google プロジェクトは、この変更の影響を受けません。ただし、April 29 以降も既存の

> Cloud Build Service の動作を維持したい場合は、API を有効にする前に、制約の適用を無効にする組織ポリシーを作成または適用できます。新しい組織ポリシーを設定した場合、このセクションの既存の権限と、**Before Cloud Build Service Account Change** とマークされている項目を引き続き使用できます。そうでない場合は、既存の権限と、**After Cloud Build Service Account Change** とマークされている項目に従ってください。

ホスト接続の作成

- プロビジョニングプロジェクトのCitrix Cloudサービスアカウントに必要な最小限の権限：

```
compute.instanceTemplates.list

compute.instances.list

compute.networks.list

compute.projects.get

compute.regions.list

compute.subnetworks.list

compute.zones.list

resourcemanager.projects.get
```

  次のGoogle定義のロールは、上記に記載されている権限を持ちます:

  - Compute 管理者
  - クラウド データストア ユーザー

- 共有 VPC プロジェクト内の Citrix Cloud サービスアカウントの共有 VPC に必要な追加の権限:

```
compute.networks.list

compute.subnetworks.list

resourcemanager.projects.get
```

  次のGoogle定義のロールは、上記に記載されている権限を持ちます:

    - コンピュートネットワークユーザー

- サービスアカウントでは、使用したい暗号鍵を持つプロジェクト (例: 共有プロジェクト) に次のロールを割り当てる必要があります:

    - Cloud KMS 閲覧者
    - クラウド KMS 暗号鍵暗号化/復号者

    ロールを割り当てない場合は、次の権限があることを確認してください:

    - resourcemanager.projects.get
    - cloudkms.keyRings.list
    - cloudkms.keyRings.get
    - cloudkms.cryptoKeys.get
    - cloudkms.cryptoKeys.list
    - cloudkms.cryptoKeyVersions.useToDecrypt
    - cloudkms.cryptoKeyVersions.useToEncrypt

仮想マシンの電源管理

電源管理のみのカタログの場合に、プロビジョニングプロジェクトのCitrix Cloudサービスアカウントに必要な最小限の権限:

```
compute.instanceTemplates.list

compute.instances.list

compute.instances.get

compute.instances.reset

compute.instances.resume

compute.instances.start

compute.instances.stop

compute.instances.suspend

compute.networks.list
```

```
compute.projects.get

compute.regions.list

compute.subnetworks.list

compute.zones.list

resourcemanager.projects.get

compute.zoneOperations.get
```

次のGoogle定義のロールは、上記の権限を持っています:

- Compute 管理者
- クラウド データストア ユーザー

仮想マシンの作成、更新、または削除

- プロビジョニングプロジェクトのCitrix Cloudサービスアカウントに必要な最小限の権限:

```
cloudbuild.builds.create

cloudbuild.builds.get

cloudbuild.builds.list

compute.acceleratorTypes.list

compute.diskTypes.get

compute.diskTypes.list

compute.disks.create

compute.disks.createSnapshot

compute.disks.delete

compute.disks.get

compute.disks.list
```

```
compute.disks.setLabels

compute.disks.use

compute.disks.useReadOnly

compute.firewalls.create

compute.firewalls.delete

compute.firewalls.list

compute.globalOperations.get

compute.images.create

compute.images.delete

compute.images.get

compute.images.list

compute.images.setLabels

compute.images.useReadOnly

compute.instanceTemplates.create

compute.instanceTemplates.delete

compute.instanceTemplates.get

compute.instanceTemplates.list

compute.instanceTemplates.useReadOnly

compute.instances.attachDisk

compute.instances.create

compute.instances.delete

compute.instances.detachDisk
```

```
compute.instances.get

compute.instances.getSerialPortOutput

compute.instances.list

compute.instances.reset

compute.instances.resume

compute.instances.setDeletionProtection

compute.instances.setLabels

compute.instances.setMetadata

compute.instances.setServiceAccount

compute.instances.setTags

compute.instances.start

compute.instances.stop

compute.instances.suspend

compute.machineTypes.get

compute.machineTypes.list

compute.networks.list

compute.networks.updatePolicy

compute.nodeGroups.list

compute.nodeTemplates.get

compute.projects.get

compute.regions.list

compute.snapshots.create
```

```
compute.snapshots.delete

compute.snapshots.list

compute.snapshots.get

compute.snapshots.setLabels

compute.snapshots.useReadOnly

compute.subnetworks.get

compute.subnetworks.list

compute.subnetworks.use

compute.zoneOperations.get

compute.zoneOperations.list

compute.zones.get

compute.zones.list

iam.serviceAccounts.actAs

resourcemanager.projects.get

storage.buckets.create

storage.buckets.delete

storage.buckets.get

storage.buckets.list

storage.buckets.update

storage.objects.create

storage.objects.delete

storage.objects.get
```

```
storage.objects.list

compute.networks.get

compute.resourcePolicies.use
```

以下のGoogle定義ロールには、上記にリストされている権限があります:

- Compute 管理者
- Storage 管理者
- Cloud Build 編集者
- サービスアカウント ユーザー
- クラウド データストア ユーザー

- Shared VPCプロジェクト内のVPCとサブネットワークを使用してホスティングユニットを作成するために、Shared VPCのCitrix Cloud Service Accountに必要な追加の権限:

```
compute.firewalls.list

compute.networks.list

compute.projects.get

compute.regions.list

compute.subnetworks.get

compute.subnetworks.list

compute.subnetworks.use

compute.zones.list

resourcemanager.projects.get
```

以下のGoogle定義ロールには、上記にリストされている権限があります:

- コンピュートネットワーク ユーザー

- クラウドデータストア ユーザー

MCSに準備指示ディスクをダウンロードする際に必要な最小限の権限:

- (Cloud Build Service Accountの変更前): これらの権限をProvisioningプロジェクトのCloud Build Service Accountに割り当てます。
- (Cloud Build Service Accountの変更後): これらの権限をProvisioningプロジェクトのCloud Compute Service Accountに割り当てます。

```
compute.disks.create

compute.disks.delete

compute.disks.get

compute.disks.list

compute.disks.setLabels

compute.disks.use

compute.disks.useReadOnly

compute.images.get

compute.images.list

compute.images.useReadOnly

compute.instances.create

compute.instances.delete

compute.instances.get

compute.instances.getSerialPortOutput

compute.instances.list

compute.instances.setLabels

compute.instances.setMetadata
```

```
compute.instances.setServiceAccount

compute.machineTypes.list

compute.networks.get

compute.networks.list

compute.projects.get

compute.subnetworks.list

compute.subnetworks.use

compute.subnetworks.useExternalIp

compute.zoneOperations.get

compute.zones.list

iam.serviceAccounts.actAs

logging.logEntries.create

pubsub.topics.publish

resourcemanager.projects.get

source.repos.get

source.repos.list

storage.buckets.create

storage.buckets.get

storage.buckets.list

storage.objects.create

storage.objects.delete

storage.objects.get
```

```
storage.objects.list
```

以下のGoogle定義ロールには、上記にリストされている権限があります:

- Cloud Build サービスアカウント (Cloud Build サービスアカウントの変更後、Cloud Compute サービスアカウントになります)
- Compute Instance 管理者
- サービスアカウントユーザー

- 準備指示ディスクをMCSにダウンロードする際に、Google Cloud Buildサービスによって ProvisioningプロジェクトのCloud Compute Service Accountに必要とされる最小限の権限:

```
resourcemanager.projects.get

storage.objects.create

storage.objects.get

storage.objects.list
```

以下のGoogle定義ロールには、上記にリストされている権限があります:

- コンピューティング ネットワーク ユーザー
- ストレージアカウントユーザー
- Cloud Datastore 利用者

MCS に準備指示ディスクをダウンロードする際に Shared VPC で必要となる追加の権限:

- (Cloud Build サービスアカウントの変更前): これらの権限をプロビジョニングプロジェクトの Cloud Build サービスアカウントに割り当てます。
- (Cloud Build サービスアカウントの変更後): これらの権限をプロビジョニングプロジェクトの Cloud Compute サービスアカウントに割り当てます。

```
compute.firewalls.list

compute.networks.list

compute.subnetworks.list
```

```
compute.subnetworks.use

resourcemanager.projects.get
```

次の Google 定義ロールには、上記にリストされている権限があります。

- Compute Network 利用者
- ストレージアカウントユーザー
- Cloud Datastore 利用者

- プロビジョニングプロジェクトの Citrix Cloud サービスアカウントの Cloud Key Management Service (KMS) に必要となる追加の権限:

```
cloudkms.cryptoKeys.get

cloudkms.cryptoKeys.list

cloudkms.keyRings.get

cloudkms.keyRings.list
```

次の Google 定義ロールには、上記にリストされている権限があります。

- Compute KMS ビューアー

一般的な権限

以下は、MCS でサポートされているすべての機能について、プロビジョニングプロジェクトの Citrix Cloud サービスアカウントの権限です。これらの権限は、今後の最適な互換性を提供します。

```
resourcemanager.projects.get

cloudbuild.builds.create

cloudbuild.builds.get

cloudbuild.builds.list

compute.acceleratorTypes.list
```

```
compute.diskTypes.get

compute.diskTypes.list

compute.disks.create

compute.disks.createSnapshot

compute.disks.delete

compute.disks.get

compute.disks.setLabels

compute.disks.use

compute.disks.useReadOnly

compute.firewalls.create

compute.firewalls.delete

compute.firewalls.list

compute.globalOperations.get

compute.images.create

compute.images.delete

compute.images.get

compute.images.list

compute.images.setLabels

compute.images.useReadOnly

compute.instanceTemplates.create

compute.instanceTemplates.delete

compute.instanceTemplates.get
```

```
compute.instanceTemplates.list

compute.instanceTemplates.useReadOnly

compute.instances.attachDisk

compute.instances.create

compute.instances.delete

compute.instances.detachDisk

compute.instances.get

compute.instances.getSerialPortOutput

compute.instances.list

compute.instances.reset

compute.instances.resume

compute.instances.setDeletionProtection

compute.instances.setLabels

compute.instances.setMetadata

compute.instances.setTags

compute.instances.start

compute.instances.stop

compute.instances.suspend

compute.instances.update

compute.instances.updateAccessConfig

compute.instances.updateDisplayDevice

compute.instances.updateSecurity
```

```
compute.instances.updateShieldedInstanceConfig

compute.instances.updateShieldedVmConfig

compute.machineTypes.get

compute.machineTypes.list

compute.networks.list

compute.networks.updatePolicy

compute.nodeGroups.list

compute.nodeTemplates.get

compute.projects.get

compute.regions.list

compute.snapshots.create

compute.snapshots.delete

compute.snapshots.list

compute.snapshots.get

compute.snapshots.setLabels

compute.snapshots.useReadOnly

compute.subnetworks.get

compute.subnetworks.list

compute.subnetworks.use

compute.subnetworks.useExternalIp

compute.zoneOperations.get

compute.zoneOperations.list
```

```
compute.zones.get

compute.zones.list

resourcemanager.projects.get

storage.buckets.create

storage.buckets.delete

storage.buckets.get

storage.buckets.list

storage.buckets.update

storage.objects.create

storage.objects.delete

storage.objects.get

storage.objects.list

cloudkms.cryptoKeys.get

cloudkms.cryptoKeys.list

cloudkms.keyRings.get

cloudkms.keyRings.list

compute.disks.list

compute.instances.setServiceAccount

compute.networks.get

compute.networks.use

compute.networks.useExternalIp

iam.serviceAccounts.actAs
```

```
compute.resourcePolicies.use

cloudkms.cryptoKeyVersions.useToDecrypt

cloudkms.cryptoKeyVersions.useToEncrypt
```

次のステップ

- 初期展開プロセス中の場合は、マシンカタログの作成を参照してください。
- Google Cloud Platform (GCP) 固有の情報については、Google Cloud Platformカタログの作成を参照してください。

詳細情報

- 接続とリソース
- マシンカタログの作成

HPE Moonshotへの接続

「接続とリソースの作成と管理」(/ja-jp/citrix-virtual-apps-desktops/2503/install-configure/connections.html)では、接続を作成するウィザードについて説明します。以下の情報は、HPE Moonshotに固有の詳細を説明しています。

注:

HPE Moonshotへの接続を作成する前に、まずHPEアカウントの設定を完了する必要があります。「HPE Moonshot仮想化環境」(/ja-jp/citrix-virtual-apps-desktops/2503/install-configure/install-prepare/hpe-moonshot.html)を参照してください。

接続を作成する

HPE Moonshotへの接続は、以下を使用して作成できます。

- ウェブスタジオ
- PowerShellコマンド

Web Studioを使用して接続を作成する

1. **接続とリソースの追加**ページで、接続の種類として**HPE Moonshot**を選択します。

2. Moonshot iLO Chassis Managerの接続アドレスを入力します。アドレスには、IPアドレス、ホスト名、またはFQDNを使用できます。
3. シャーシの管理資格情報と、わかりやすい接続名を入力します。

接続設定は、次のいずれかの状況で停止します。

- Citrix Virtual Apps and Desktops™がエラーのある公開CA署名証明書を受信した場合：エラーメッセージが表示されます。画面の指示に従って問題を修正してください。そうしないと、接続の作成に進むことはできません。
- Citrix Virtual Apps and DesktopsがプライベートCA署名証明書を受信した場合。警告ページが表示されます。受信したサムプリントをサーバーのものと比較して、証明書の有効性を確認します。有効な場合は、**証明書を信頼する**を選択し、**OK**をクリックして接続の作成に進みます。その後、Citrix Virtual Apps and Desktopsは証明書を信頼し、将来の検証のためにサムプリントを保存します。

PowerShellコマンドを使用して接続を作成する

PowerShellコマンドを使用して接続を作成する場合、次の情報を提供します。

- IP: HPEサーバーのIPアドレス
- ユーザー名: HPEユーザー名
- パスワード: HPEパスワード

例:

```
New-Item -ConnectionType "Custom" -HypervisorAddress $IP -Metadata
@{"Citrix_Orchestration_Hypervisor_Secret_Allow_Edit"="false"} -Path
@("XDHyp:\Connections\$connectionName") -Persist -PluginId
"HPMoonshotFactory" -Scope @() -SecurePassword $Password -UserName
$UserName -sslthumbprint $SslThumbprint New-BrokerHypervisorConnection
-HypHypervisorConnectionUid $HypervisorConnectionID
```

注:

`sslthumbprint`パラメーターは、プライベートCA署名付き証明書の場合にのみ必要です。

証明書とサムプリントの検証

HPE Moonshot への接続を正常に作成するには、証明書にエラーがなく、サムプリントが正しい値である必要があります。証明書とサムプリントの検証に関連するユースケースは次のとおりです。

- パブリックCA署名付き証明書にエラーがあります。接続は正常に作成されません。エラーの詳細を確認し、問題を解決してください。
- エラーのないパブリックCA署名付き証明書。接続は正常に作成され、`SslThumbprints` の値は **Null** です。
- エラーがなく、`sslthumbprint` の値を持つプライベートCA署名付き証明書。接続は正しい `SslThumbprints` の値で正常に作成されます。
- 不正確なサムプリント値を持つプライベートCA署名付き証明書。接続は正常に作成されません。
- エラーのないプライベートCA署名付き証明書。接続は正常に作成されます。接続作成時に `SSlThumbprints` は **Null** です。`SSlThumbprints` の値はサイトサービスによって値に更新されます。

> **注：**
>
> Citrix Database と Moonshot サーバー間の証明書サムプリントの不一致は、Web Studio で警告をトリガーします。ただし、この警告はMMCベースのStudioには表示されません。

接続の管理

このセクションでは、接続を管理する方法について詳しく説明します。

- Web Studioを使用して証明書の問題を修正する
- PowerShellコマンドを使用してサムプリント値を更新する

証明書の問題を修正する

証明書の問題が発生すると、Citrix Virtual Apps and DesktopsはHPE Moonshot接続をブロックし、関連するHPE Moonshotノードでのワークロードの配信と管理ができなくなります。**ホスト接続**リストの接続の横にエラーアイコンが表示されます。特定の課題と解決策については、次の表を参照してください。

課題	解決策
公開CA署名証明書に証明書エラーが発生する	接続をクリックし、**トラブルシューティング**タブを選択します。エラーの詳細を表示し、問題を解決します。
受信した証明書はプライベートCA署名であるか、期限切れです。	ホスト接続を編集して、証明書のサムプリントを更新します。詳細な手順： 1. 接続を選択し、**接続の編集**をクリックします。 2. **接続プロパティ**ページで、**設定の編集**をクリックします。 3. HPE Moonshotシャーシに接続するためのパスワードを入力し、**保存**をクリックします。 4. 表示される「**警告**」ページで、受信したサムプリントをサーバーのものと比較して、証明書の有効性を確認します。 5. 同じである場合は、**証明書を信頼する**を選択し、**OK**をクリックします。

サムプリント値の更新

接続を作成した後、`Set-Item` PowerShellコマンドを使用して接続のサムプリント値を更新できます。たとえば、次のコマンドを実行します。

1. 接続の詳細を取得します。例：

```
Get-Item -LiteralPath xdhyp:\connections\SinMoonshot-101
```

2. サムプリント値を更新します。例:

```
Set-Item -LiteralPath xdhyp:\connections\SinMoonshot-101 -Username
Administrator -SslThumbprint xxxxxxxxxxx12AD048480631BB7AB10D69xxxxx
```

3. 更新されたサムプリント値を確認します。例:

```
Get-Item -LiteralPath xdhyp:\connections\SinMoonshot-101
```

注:

`Set-Item`コマンドで誤ったサムプリント値を指定すると、更新は失敗します。

次のステップ

- 初期展開プロセスの場合は、マシンカタログの作成を参照してください。
- AWS固有の情報については、HPE Moonshotマシンカタログの作成を参照してください。

詳細情報

- 接続とリソース
- マシンカタログの作成

Microsoft Azure への接続

注:

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

接続とリソースの作成および管理では、接続を作成するウィザードについて説明しています。以下の情報は、Azure Resource Managerクラウド環境に固有の詳細を扱っています。

注:

> Microsoft Azureへの接続を作成する前に、Azureアカウントをリソースの場所として設定を完了する必要があります。Microsoft Azure Resource Managerクラウド環境を参照してください。

サービスプリンシパルと接続の作成

接続を作成する前に、接続がAzureリソースにアクセスするために使用するサービスプリンシパルを設定する必要があります。接続は次の2つの方法で作成できます。

- Web Studioを使用してサービスプリンシパルと接続を同時に作成する
- 以前に作成したサービスプリンシパルを使用して接続を作成する

このセクションでは、次のタスクを完了する方法を示します。

- Web Studioを使用してサービスプリンシパルと接続を作成する
- PowerShellを使用してサービスプリンシパルを作成する
- Azureでアプリケーションシークレットを取得する
- 既存のサービスプリンシパルを使用して接続を作成する

考慮事項

- Citrix® は、共同作成者ロールを持つサービスプリンシパルの使用を推奨しています。ただし、最小限の権限のリストについては、(#minimum-permissions)セクションの「最小限の権限」を参照してください。
- 最初の接続を作成するとき、Azure は必要な権限を付与するように求めます。今後の接続では引き続き認証が必要ですが、Azure は以前の同意を記憶しており、プロンプトを再度表示することはありません。
- 認証に使用されるアカウントは、Azure RBAC を使用してサブスクリプション内でロールを割り当てる権限を持っている必要があります。例として、サブスクリプションの所有者、ロールベースのアクセス制御管理者、またはユーザーアクセス管理者などです。
- 認証に使用されるアカウントは、サブスクリプションのディレクトリのメンバーである必要があります。注意すべきアカウントには、「職場または学校」と「個人用 Microsoft アカウント」の2種類があります。詳細については、CTX219211を参照してください。
- 既存の Microsoft アカウントをサブスクリプションのディレクトリのメンバーとして追加して使用することはできますが、ユーザーが以前にディレクトリのリソースのいずれかへのゲストアクセスを許可されていた場合、問題が発生する可能性があります。この場合、ディレクトリ

内に必要な権限を付与しないプレースホルダーエントリが存在し、エラーが返される可能性があります。

ディレクトリからリソースを削除し、明示的に追加し直すことで、これを修正します。ただし、このオプションは、アカウントがアクセスできる他のリソースに意図しない影響を与える可能性があるため、慎重に実行してください。

- 特定のアカウントが実際にはメンバーであるにもかかわらず、ディレクトリゲストとして検出される既知の問題があります。このような構成は、通常、古くから確立されたディレクトリアカウントで発生します。回避策: ディレクトリにアカウントを追加し、適切なメンバーシップ値を取得します。
- リソースグループは単にリソースのコンテナであり、自身のリージョン以外のリージョンからのリソースを含むことができます。これは、リソースグループのリージョンに表示されるリソースが利用可能であると期待している場合、混乱を招く可能性があります。
- 必要な数のマシンをホストするのに十分な大きさのネットワークとサブネットがあることを確認してください。これにはある程度の先見性が必要ですが、Microsoft はアドレス空間の容量に関するガイダンスを提供し、適切な値を指定するのに役立ちます。

Web Studio を使用してサービスプリンシパルと接続を作成する

> **重要:**
>
> この機能は、Azure China サブスクリプションではまだ利用できません。

> Web Studio を使用すると、単一のワークフローでサービスプリンシパルと接続の両方を作成できます。サービスプリンシパルは、接続に Azure リソースへのアクセスを許可します。サービスプリンシパルを作成するために Azure に認証すると、Azure にアプリケーションが登録されます。登録されたアプリケーションには、秘密鍵（クライアントシークレットまたはアプリケーションシークレットと呼ばれます）が作成されます。登録されたアプリケーション（この場合は接続）は、クライアントシークレットを使用して Azure AD に認証します。

開始する前に、以下の前提条件を満たしていることを確認してください。

- サブスクリプションのAzure Active Directoryテナントにユーザーアカウントがあること。
- 認証に使用されるアカウントには、Azure RBACを使用してサブスクリプションでロールを割り当てる権限が必要です。例として、サブスクリプションの所有者、ロールベースのアクセス制御管理者、またはユーザーアクセス管理者などです。

- 認証のために、グローバル管理者、アプリケーション管理者、またはアプリケーション開発者の権限を持っていること。これらの権限は、ホスト接続を作成した後に取り消すことができます。ロールの詳細については、「Azure AD の組み込みロール」を参照してください。

サービスプリンシパルと接続を同時に作成するには、**接続とリソースの追加**ウィザードを使用します。

1. **接続**ページで、**新しい接続の作成**、**Microsoft Azure**接続タイプ、およびAzure環境を選択します。
2. 仮想マシンを作成するために使用するツールを選択し、**次へ**を選択します。
3. **接続の詳細**ページで、AzureサブスクリプションIDと接続の名前を入力します。サブスクリプションIDを入力すると、**新規作成**ボタンが有効になります。

   > **注：**
   >
   > 接続名には1～64文字を含めることができ、空白のみ、または文字 `\/;:#.*?=<>|[]{}"'()'` を含めることはできません。

4. **新規作成**を選択し、Azure Active Directoryアカウントのユーザー名とパスワードを入力します。
5. **サインイン**を選択します。
6. **同意する**を選択して、Citrix Virtual Apps and Desktops™にリストされている権限を付与します。Citrix Virtual Apps and Desktopsは、指定されたユーザーに代わってAzureリソースを管理できるサービスプリンシパルを作成します。
7. **同意する**を選択すると、ウィザードの**接続**ページに戻ります。

   > **注：**
   >
   > Azureへの認証が成功すると、**新規作成**ボタンと**既存を使用**ボタンは表示されなくなります。緑色のチェックマークとともに**接続に成功しました**というテキストが表示され、Azureサブスクリプションへの接続が成功したことを示します。

8. ページで、 を選択します。

   > **注：**

> Azureへの認証に成功し、必要な権限の付与に同意するまで、次のページに進むことはできません。

9. 接続のリソースを構成します。リソースは、リージョンとネットワークで構成されます。
   - ページで、リージョンを選択します。
   - ページで、以下を実行します。
     - リージョンとネットワークの組み合わせを識別するために、1〜64文字のリソース名を入力します。リソース名には、空白のみ、または文字 `\/;:#.*?=<>|[]{}"'()'` を含めることはできません。
     - 仮想ネットワーク/リソースグループのペアを選択します。（同じ名前の仮想ネットワークが複数ある場合、ネットワーク名とリソースグループをペアにすることで、一意の組み合わせが提供されます。）前のページで選択したリージョンに仮想ネットワークがない場合は、そのページに戻り、仮想ネットワークがあるリージョンを選択してください。
10. ページで、設定の概要を確認し、 を選択してセットアップを完了します。

アプリケーションIDを表示する

接続を作成した後、その接続がAzureリソースへのアクセスに使用するアプリケーションIDを表示できます。

リストで、接続を選択して詳細を表示します。 タブにアプリケーションIDが表示されます。

PowerShellを使用してサービスプリンシパルを作成する

PowerShellを使用してサービスプリンシパルを作成するには、Azure Resource Managerサブスクリプションに接続し、以下のセクションで提供されているPowerShellコマンドレットを使用します。

以下の項目が準備されていることを確認してください。

- **SubscriptionId:** VDAをプロビジョニングするサブスクリプションのAzure Resource Manager `SubscriptionID`。
- 「**ActiveDirectoryID**」: Azure AD に登録したアプリケーションのテナントID。
- 「**ApplicationName**」: Azure AD で作成するアプリケーションの名前。

詳細な手順は次のとおりです。

Azure Resource Manager サブスクリプションに接続します。

```
`Connect-AzAccount`
```

1. サービスプリンシパルを作成する Azure Resource Manager サブスクリプションを選択します。

   ```
   Get-AzSubscription -SubscriptionId $subscriptionId | Select-AzSubscription
   ```

2. AD テナントにアプリケーションを作成します。

   ```
   $AzureADApplication = New-AzADApplication -DisplayName $ApplicationName
   ```

3. サービスプリンシパルを作成します。

   ```
   New-AzADServicePrincipal -ApplicationId $AzureADApplication.AppId
   ```

4. サービスプリンシパルにロールを割り当てます。

   ```
   New-AzRoleAssignment -RoleDefinitionName Contributor -ServicePrincipalName $AzureADApplication.AppId –scope /subscriptions/$SubscriptionId
   ```

5. PowerShell コンソールの出力ウィンドウから ApplicationId をメモします。ホスト接続を作成する際に、その ID を指定します。

Azure でアプリケーションシークレットを取得する

既存のサービスプリンシパルを使用して接続を作成するには、まず Azure portal でサービスプリンシパルのアプリケーションIDとシークレットを取得する必要があります。

詳細な手順は次のとおりです。

1. Web Studio から、または PowerShell を使用して「**Application ID**」を取得します。
2. Azureポータルにサインインします。
3. Azure で、「**Azure Active Directory**」を選択します。
4. Azure AD の「**App registrations**」から、アプリケーションを選択します。
5. **証明書とシークレット**に移動します。
6. **クライアントシークレット**をクリックします。

既存のサービスプリンシパルを使用して接続を作成する

サービスプリンシパルをすでに持っている場合は、それを使用してWeb Studioで接続を作成できます。

次の項目を用意してください。

- SubscriptionId
- ActiveDirectoryID (テナントID)
- アプリケーションID
- アプリケーションシークレット

  詳細については、「アプリケーションシークレットの取得」を参照してください。
- シークレットの有効期限

詳細な手順は次のとおりです。

接続とリソースの追加ウィザードで、次の手順を実行します。

1. **接続**ページで、**新しい接続の作成**、**Microsoft Azure**接続タイプ、およびAzure環境を選択します。
2. 仮想マシンを作成するために使用するツールを選択し、**次へ**を選択します。
3. 「**接続の詳細**」ページで、Azure サブスクリプション ID と接続の名前を入力します。

   > **注:**
   >
   > 接続名には 1～64 文字を含めることができ、空白のみ、または文字 `\/;:#.*?=<>|[]{}"'()'` を含めることはできません。

4. **既存を使用**を選択します。**既存のサービスプリンシパルの詳細**ウィンドウで、既存のサービスプリンシパルに対して次の設定を入力します。詳細を入力すると、**保存**ボタンが有効になります。**保存**を選択します。有効な詳細情報を提供するまで、このページから先に進むことはできません。

   - **サブスクリプションID**。AzureサブスクリプションIDを入力します。サブスクリプションIDを取得するには、Azureポータルにサインインし、**サブスクリプション > 概要**に移動します。
   - **Active Directory ID**（テナントID）。Azure ADに登録したアプリケーションのディレクトリ（テナント）IDを入力します。
   - **アプリケーションID**。Azure ADに登録したアプリケーションのアプリケーション（クライアント）IDを入力します。

- **アプリケーションシークレット**。シークレットキー（クライアントシークレット）を作成します。登録されたアプリケーションは、このキーを使用してAzure ADに認証します。セキュリティ上の理由から、定期的にキーを変更することをお勧めします。キーは後で取得できないため、必ず保存してください。
- **シークレットの有効期限**。アプリケーションシークレットの有効期限が切れる日付を入力します。シークレットキーの有効期限が切れる14日前から、**ホスティング**ノードの特定のホスト接続に警告アイコンが表示されます。ただし、シークレットキーの有効期限が切れると、エラーが発生します。

> **注記:**
>
> セキュリティ上の理由から、有効期限は現在から2年を超えることはできません。

- **認証 URL**。このフィールドは自動的に入力され、編集できません。
- **管理 URL**。このフィールドは自動的に入力され、編集できません。
- **ストレージサフィックス**。このフィールドは自動的に入力され、編集できません。
- **ディスクまたはスナップショットをアップロードまたはダウンロードするためのAzure BLOBストレージエンドポイント**。このフィールドは自動的に入力され、編集できません。
- **Key Vaultサービス**。このフィールドは自動的に入力され、編集できません。
- **サービスバスサフィックス**。このフィールドは自動的に入力され、編集できません。

  AzureでMCSカタログを作成するには、以下のエンドポイントへのアクセスが必要です。これらのエンドポイントへのアクセスにより、ネットワークとAzureポータルおよびそのサービス間の接続が最適化されます。

  - 認証URL: `https://login.microsoftonline.com`
  - 管理URL: `https://management.azure.com`。これはAzure Resource Managerプロバイダー APIのリクエストURLです。管理用のエンドポイントは環境によって異なります。たとえば、Azure Globalの場合は`https://management.azure.com`、Azure US Governmentの場合は`https://management.usgovcloudapi.net`です。
  - ストレージサフィックス: `https://*.core.windows.net`。この (*) はストレージサフィックスのワイルドカード文字です。例: `https://demo.table.core.windows.net`。

- ディスクまたはスナップショットをアップロードまたはダウンロードするためのAzure BLOBストレージエンドポイント: `https://*.storage.azure.net`。この (*) はBLOBストレージのインポートおよびエクスポート操作のワイルドカード文字です。例: `https://md-impexp-xxxxx.z[00-50].blob.storage.azure.net`。
- Key Vaultサービス: `https://*.vault.azure.net`。この (*) はキーコンテナー名のワイルドカード文字です。例: `https://<your-key-vault-name>.vault.azure.net`。
- サービスバスサフィックス: `https://*.servicebus.windows.net`。この (*) はグローバルAzureクラウドで作成された名前空間のワイルドカード文字です。例: `https://{serviceNamespace}.servicebus.windows.net/{path}`。

5. 「**保存**」を選択すると、「**接続の詳細**」ページに戻ります。「**次へ**」を選択して次のページに進みます。
6. 接続のリソースを構成します。リソースはリージョンとネットワークで構成されます。
   - 「**地域**」ページで、地域を選択します。
   - 「**ネットワーク**」ページで、次の操作を行います。
     - リージョンとネットワークの組み合わせを識別しやすくするため、1〜64文字のリソース名を入力します。リソース名には空白のみを含めることはできません。また、`\/;:#.*?=<>|[]{}"'()'`の文字を含めることもできません。
     - 仮想ネットワーク/リソースグループのペアを選択します。（同じ名前の仮想ネットワークが複数ある場合、ネットワーク名とリソースグループをペアにすることで一意の組み合わせが提供されます。）前のページで選択したリージョンに仮想ネットワークがない場合は、そのページに戻り、仮想ネットワークがあるリージョンを選択してください。
7. 「**概要**」ページで、設定の概要を表示し、「**完了**」を選択してセットアップを完了します。

サービスプリンシパルと接続を管理する

このセクションでは、サービスプリンシパルと接続を管理する方法について詳しく説明します。

- Azureの調整設定を構成する
- Azureでイメージ共有を有効にする
- Web Studioを使用して共有テナントを接続に追加する
- PowerShellを使用してイメージ共有を実装する
- アプリケーションシークレットとシークレットの有効期限を管理する

Azureの調整設定を構成する

Azure Resource Managerは、サブスクリプションとテナントのリクエストをスロットルし、プロバイダーの特定のニーズに合わせて調整された定義済みの制限に基づいてトラフィックをルーティングします。詳細については、MicrosoftサイトのResource Managerリクエストのスロットリングを参照してください。サブスクリプションとテナントには制限があり、多数のマシンを管理すると問題が発生する可能性があります。たとえば、多数のマシンを含むサブスクリプションでは、電源操作に関連するパフォーマンスの問題が発生する可能性があります。

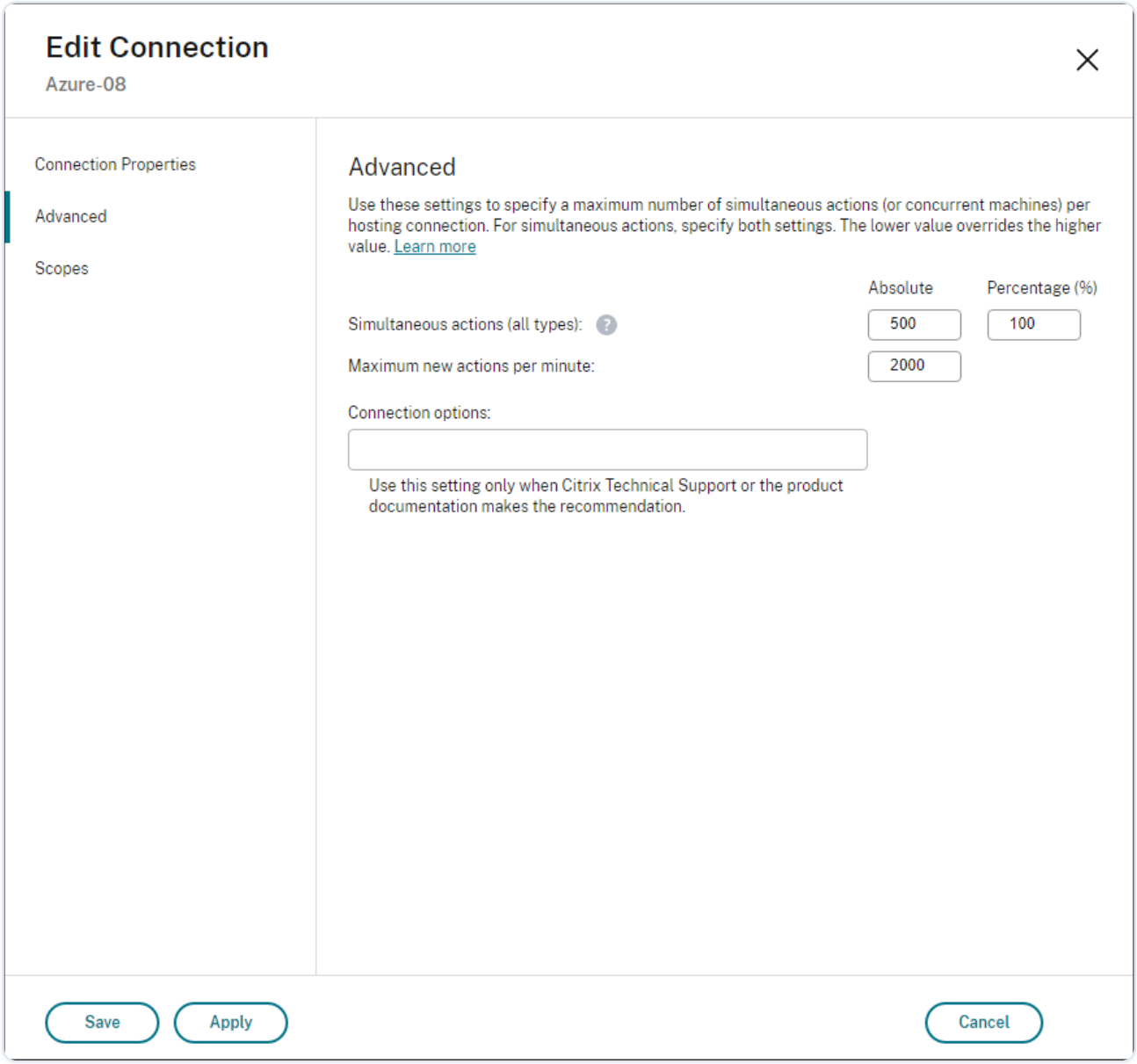
> **ヒント：**
>
> 詳細については、「Machine Creation ServicesによるAzureパフォーマンスの向上」を参照してください。
>
> これらの問題を軽減するために、MCSの内部スロットリングを削除して、Azureから利用可能なリクエストクォータをより多く使用できます。

大規模なサブスクリプション（たとえば、1,000台のVMを含むもの）でVMの電源をオンまたはオフにする場合は、次の最適な設定をお勧めします。

- 絶対同時操作数：500
- 1分あたりの最大新規操作数：2000
- 操作の最大同時実行数：500

Web Studioを使用して、特定のAzure接続のAzure操作を構成します。

1. Web Studioで、左側のペインの**ホスティング**を選択します。
2. 接続を選択します。
3. **接続の編集**ウィザードで、**詳細**を選択します。
4. **詳細**ページで、構成オプションを使用して、同時実行アクションの数、1分あたりの最大新規アクション数、および追加の接続オプションを指定します。



MCSは、デフォルトで最大500の同時操作をサポートします。または、Remote PowerShell SDKを使用して、同時操作の最大数を設定することもできます。

PowerShell プロパティ `MaximumConcurrentProvisioningOperations` を使用して、Azure プロビジョニングの同時操作の最大数を指定します。このプロパティを使用する際は、以下を考慮してください。

- `MaximumConcurrentProvisioningOperations` のデフォルト値は 500 です。
- PowerShell コマンド `Set-item` を使用して、`MaximumConcurrentProvisioningOperations` パラメーターを構成します。

Azure でのイメージ共有を有効にする

マシンカタログを作成または更新する際、異なるAzureテナントやサブスクリプションから共有イメージ（Azure Compute Galleryを介して共有）を選択できます。テナント内またはテナント間でイメージ共有を有効にするには、Azureで必要な設定を行う必要があります。

- テナント内でのイメージ共有（サブスクリプション間）
- テナント間でのイメージ共有

テナント内でのイメージ共有（サブスクリプション間）

異なるサブスクリプションに属するAzure Compute Galleryのイメージを選択するには、そのイメージをそのサブスクリプションのサービスプリンシパル（SPN）と共有する必要があります。

たとえば、Studioで次のように構成されているサービスプリンシパル（SPN 1）がある場合：

サービスプリンシパル: SPN 1

サブスクリプション: subscription 1

テナント: tenant 1

イメージは別のサブスクリプションにあり、Studioで次のように構成されています。

サブスクリプション: subscription 2

テナント: tenant 1

subscription 2のイメージをsubscription 1 (SPN 1) と共有したい場合は、subscription 2に移動し、リソースグループをSPN1と共有します。

イメージは、Azure ロールベースのアクセス制御 (RBAC) を使用して、別の SPN と共有する必要があります。Azure RBAC は、Azure リソースへのアクセスを管理するために使用される承認システムです。Azure RBAC の詳細については、Microsoft ドキュメント「Azure ロールベースのアクセス制御 (Azure RBAC) とは」を参照してください。アクセスを許可するには、リソースグループスコープで共同作成者ロールを持つサービスプリンシパルにロールを割り当てます。Azure ロールを割り当てるには、ユーザーアクセス管理者や所有者などの `Microsoft.Authorization/roleAssignments/write` 権限が必要です。別の SPN とイメージを共有する方法の詳細については、Microsoft ドキュメント「Azure portal を使用して Azure ロールを割り当てる」を参照してください。

PowerShell コマンドを使用して別のサブスクリプションからイメージを選択する方法については、「別のサブスクリプションからイメージを選択する」を参照してください。

テナント間で画像を共有する

Azure Compute Gallery を使用してテナント間でイメージを共有するには、アプリケーション登録を作成します。

たとえば、2 つのテナント (テナント 1 とテナント 2) があり、イメージギャラリーをテナント 1 と共有したい場合は、次の手順を実行します。

1. テナント 1 のアプリケーション登録を作成します。詳細については、「アプリ登録を作成する」を参照してください。
2. ブラウザを使用してサインインを要求することで、テナント 2 にアプリケーションへのアクセスを許可します。`Tenant2 ID` をテナント 1 のテナント ID に置き換えます。`Application (client) ID` を作成したアプリケーション登録のアプリケーション ID に置き換えます。置き換えが完了したら、URL をブラウザに貼り付け、サインインプロンプトに従ってテナント 2 にサインインします。例:

   ```
   https://login.microsoftonline.com/<Tenant 2 ID>/oauth2/authorize?
   client_id=<Application (client)
   ID>&response_type=code&redirect_uri=https%3A%2F%2Fwww.microsoft.com%2F
   ```

   詳細については、「テナント 2 にアクセスを許可する」を参照してください。
3. アプリケーションにテナント 2 のリソースグループへのアクセスを許可します。テナント 2 としてサインインし、ギャラリーイメージを持つリソースグループにアプリケーション登録アクセスを許可します。詳細については、「テナント間で要求を認証する」を参照してください。

PowerShell コマンドを使用して別のテナントのイメージからカタログを作成するには:

1. 共有テナント ID でホスティング接続のカスタムプロパティを更新する。
2. 別のテナントからイメージを選択する。

Web Studio を使用して共有テナントを接続に追加する

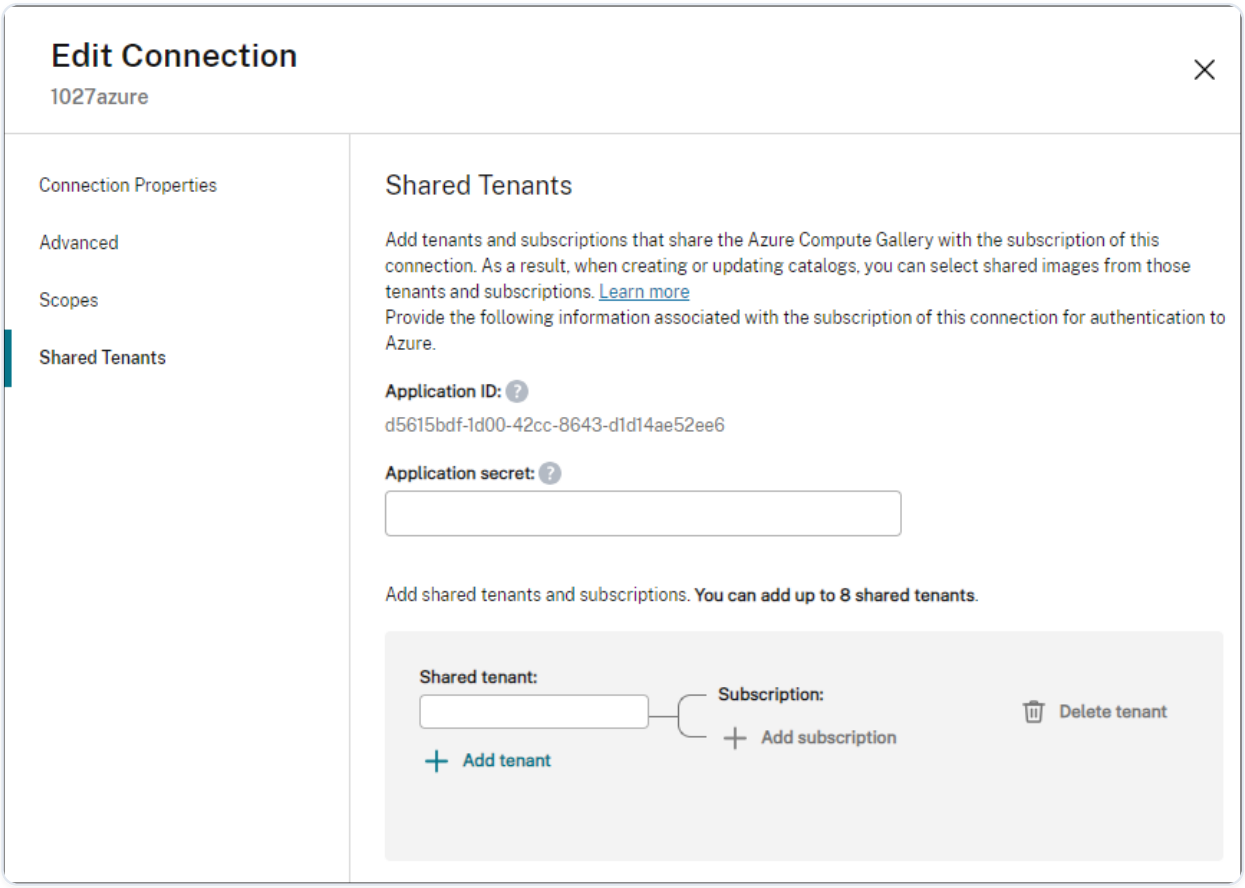
Web Studio でマシンカタログを作成または更新する際、異なる Azure テナントおよびサブスクリプション (Azure Compute Gallery を介して共有) から共有イメージを選択できます。この機能では、関連するホスト接続の共有テナントおよびサブスクリプション情報を提供する必要があります。

> **注:**
>
> テナント間でイメージ共有を有効にするために、Azure で必要な設定が構成されていることを確認してください。詳細については、「テナント間で画像を共有する」を参照してください。

接続に対して、次の手順を実行します。

1. Web Studio で、左側のペインの を選択します。

2. 接続を選択し、アクションバーで**接続の編集**を選択します。



3. 「**共有テナント**」で、以下を実行します。

   - 接続のサブスクリプションに関連付けられているアプリケーション ID とアプリケーションシークレットを指定します。Citrix Virtual Apps and Desktops は、この情報を使用して Azure AD に対して認証を行います。
   - 接続のサブスクリプションと Azure Compute Gallery を共有するテナントとサブスクリプションを追加します。テナントごとに最大8つの共有テナントと8つのサブスクリプションを追加できます。

4. 完了したら、**適用**を選択して行った変更を適用し、ウィンドウを開いたままにするか、**OK**を選択して変更を適用し、ウィンドウを閉じます。

PowerShellを使用したイメージ共有の実装

このセクションでは、PowerShellを使用してイメージを共有するプロセスについて説明します。

- 別のサブスクリプションからイメージを選択する
- 共有テナントIDでホスティング接続のカスタムプロパティを更新する
- 別のテナントからイメージを選択する

別のサブスクリプションからイメージを選択する

同じAzureテナント内の別の共有サブスクリプションに属するAzure Compute Galleryのイメージを選択して、PowerShellコマンドを使用してMCSカタログを作成および更新できます。

1. ホスティングユニットのルートフォルダーに、Citrixは`sharedsubscription`という新しい共有サブスクリプションフォルダーを作成します。
2. テナント内のすべての共有サブスクリプションを一覧表示します。

```
Get-ChildItem -Path "XDhyp:
\HostingUnits\azres\sharedsubscription.folder"
```

3. 1つの共有サブスクリプションを選択し、その共有サブスクリプションのすべての共有リソースグループを一覧表示します。

```
Get-ChildItem -Path "XDhyp:
\HostingUnits\azres\image.folder\abc123.sharedsubscription"
```

4. リソースグループを選択し、そのリソースグループのすべてのギャラリーを一覧表示します。

```
Get-ChildItem -Path "XDhyp:
\HostingUnits\azres\image.folder\abc123.sharedsubscription\
xyz.resourcegroup"
```

5. ギャラリーを選択し、そのギャラリーのすべてのイメージ定義を一覧表示します。

```
Get-ChildItem -Path "XDhyp:
\HostingUnits\azres\image.folder\abc123.sharedsubscription\xyz.resource
group\testgallery.gallery"
```

6. 1つのイメージ定義を選択し、そのイメージ定義のすべてのイメージバージョンを一覧表示します。

```
Get-ChildItem -Path "XDhyp:
\HostingUnits\azres\image.folder\abc123.sharedsubscription\xyz.resource
group\sigtestdef.imagedefinition"
```

7. 次の要素を使用してMCSカタログを作成および更新します。

   - リソースグループ

- ギャラリー
- ギャラリーイメージ定義
- ギャラリーイメージバージョン

Remote PowerShell SDK を使用したカタログの作成方法については、`<https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/>` を参照してください。

共有テナントIDでホスティング接続のカスタムプロパティを更新する

`Set-Item` を使用して、共有テナントIDとサブスクリプションIDでホスティング接続のカスタムプロパティを更新します。`CustomProperties` にプロパティ `SharedTenants` を追加します。`Shared Tenants` の形式は次のとおりです。

```
[{"Tenant":"94367291-119e-457c-bc10-25337231f7bd","Subscriptions":
["7bb42f40-8d7f-4230-a920-be2781f6d5d9"]},{"Tenant":"50e83564-c4e5-4209-
b43d-815c45659564","Subscriptions":["06ab8944-6a88-47ee-
a975-43dd491a37d0"]}]
```

例：

```
Set-Item -CustomProperties "<CustomProperties xmlns=`"http://
schemas.citrix.com/2014/xd/machinecreation`" xmlns:xsi=`"http://
www.w3.org/2001/XMLSchema-instance`">

<Property xsi:type=`"StringProperty`" Name=`"SubscriptionId`"
Value=`"123`" />

<Property xsi:type=`"StringProperty`" Name=`"ManagementEndpoint`"
Value=`"https://management.azure.com/`" />

<Property xsi:type=`"StringProperty`" Name=`"AuthenticationAuthority`"
Value=`"https://login.microsoftonline.com/`" />

<Property xsi:type=`"StringProperty`" Name=`"StorageSuffix`"
Value=`"core.windows.net`" />

<Property xsi:type=`"StringProperty`" Name=`"TenantId`" Value=`"123abc`" /
>

<Property xsi:type=`"StringProperty`" Name=`"SharedTenants`"
Value=`"`[ { 'Tenant':'123abc', 'Subscriptions':['345', '567'] } ]`"` />
```

```
</CustomProperties>"

-LiteralPath @("XDHyp:\Connections\aazure") -PassThru -UserName "advc345"
-SecurePassword

$psd
```

注：

複数のテナントを追加できます。各テナントは複数のサブスクリプションを持つことができます。

別のテナントからイメージを選択する

PowerShellコマンドを使用してMCSカタログを作成および更新するために、別のAzureテナントに属するAzure Compute Galleryのイメージを選択できます。

1. ホスティングユニットのルートフォルダーに、Citrixは`sharedsubscription`という新しい共有サブスクリプションフォルダーを作成します。
2. すべての共有サブスクリプションを一覧表示します。

   ```
   Get-ChildItem XDHyp:\HostingUnits\azres\sharedsubscription.folder
   ```

3. 共有サブスクリプションを1つ選択し、その共有サブスクリプションのすべての共有リソースグループを一覧表示します。

   ```
   Get-ChildItem XDHyp:
   \HostingUnits\azres\image.folder\abc123.sharedsubscription
   ```

4. リソースグループを選択し、そのリソースグループのすべてのギャラリーを一覧表示します。

   ```
   Get-ChildItem XDHyp:
   \HostingUnits\azres\image.folder\abc123.sharedsubscription\
   xyz.resourcegroup
   ```

5. ギャラリーを選択し、そのギャラリーのすべてのイメージ定義を一覧表示します。

```
Get-ChildItem XDHyp:
\HostingUnits\azres\image.folder\abc123.sharedsubscription\xyz.resource
group\efg.gallery
```

6. イメージ定義を1つ選択し、そのイメージ定義のすべてのイメージバージョンを一覧表示します。

```
Get-ChildItem XDHyp:
\HostingUnits\azres\image.folder\abc123.sharedsubscription\xyz.resource
group\efg.gallery\hij.imagedefinition
```

7. 次の要素を使用してMCSカタログを作成および更新します。

   - リソースグループ
   - ギャラリー
   - ギャラリーイメージ定義
   - ギャラリーイメージバージョン

   Remote PowerShell SDK を使用したカタログの作成方法については、`<https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/>` を参照してください。

アプリケーションシークレットとシークレットの有効期限を管理する

シークレットの有効期限が切れる前に、接続のアプリケーションシークレットを必ず変更してください。シークレットキーの有効期限が切れる14日前から、**Hosting** ノードの特定のホスト接続に警告アイコンが表示されます。ただし、シークレットキーの有効期限が切れると、エラーが発生します。

AZURE でアプリケーションシークレットを作成する

Azure ポータルを通じて、接続のアプリケーションシークレットを作成できます。

1. **Azure Active Directory** を選択します。
2. Azure AD の **App registrations** から、アプリケーションを選択します。
3. **Certificates & secrets** に移動します。
4. **Client secrets > New client secret** をクリックします。
5. シークレットの説明を入力し、期間を指定します。完了したら、**Add** を選択します。

> **注:**
>
> クライアントシークレットは後で取得できないため、必ず保存してください。

6. クライアントシークレットの値と有効期限をコピーします。
7. Web Studio で、対応する接続を編集し、**Application secret** および **Secret expiration date** フィールドの内容をコピーした値に置き換えます。

シークレットの有効期限を変更する

Web Studio を使用して、使用中のアプリケーションシークレットの有効期限を追加または変更できます。

> **注:**
>
> シークレットキーの有効期限が切れる14日前から、**Hosting** ノードの特定のホスト接続に警告アイコンが表示されます。

1. **接続とリソースの追加**ウィザードで、接続を右クリックし、**接続の編集**をクリックします。
2. **接続プロパティ**ページで、**シークレットの有効期限**をクリックして、使用中のアプリケーションシークレットの有効期限を追加または変更します。

事前作成されたネットワークセキュリティグループを使用する

CitrixにNSGの作成と変更を要求する代わりに、イメージ準備用のDeny-Allネットワークセキュリティグループを作成します。PowerShellコマンド `Set-Item` を使用してホスティングユニットのカスタムプロパティを編集し、Deny-Allネットワークセキュリティグループを提供するためのパラメーター `NsgForPreparation` を含めます。

前提条件

サービスプリンシパルに必要な次のアクセス許可を構成します。

- `Microsoft.Network/networkSecurityGroups/join/action`: ネットワークセキュリティグループをサブネットまたはネットワークインターフェイスに関連付ける
- `Microsoft.Network/networkSecurityGroups/read`: ネットワークセキュリティグループを取得する
- `Microsoft.Network/networkSecurityGroups/securityRules/read`: ルールを取得する

事前作成されたDeny-Allネットワークセキュリティグループを追加する

事前作成されたDeny-Allネットワークセキュリティグループを追加するには、ホスティングユニットでカスタムプロパティを次のように設定します。

1. Remote PowerShell SDKを使用してPowerShellウィンドウを開きます。
2. 次のコマンドを実行します。

```
Add-PSSnapin citrix*.

cd XDHyp:\HostingUnits\

Dir
```

3. 詳細を取得するホスティングユニットを選択します。

```
Get-Item "XDHyp:\HostingUnits\<hostingunitname>"
```

4. CustomPropertiesをメモ帳にコピーし、プロパティ設定 `<Property xsi:type="StringProperty` " Name= `"NsgForPreparation` " Value= `"{ResourceGroupName}/{NetworkSecurityGroupName}"/>` を追加します。例:

```
<CustomProperties xmlns=`"http://schemas.citrix.com/2014/xd/
machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`"><Property xsi:type=`"StringProperty`"
Name=`"NsgForPreparation`" Value=`{ResourceGroupName}/
{NetworkSecurityGroupName}`"/></CustomProperties>
```

5. PowerShellウィンドウで、変更されたカスタムプロパティに変数を割り当てます。例:

```
$customProperty = "<CustomProperties xmlns=`"http://schemas.citrix.com/
2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`"><Property xsi:type=`"StringProperty`"
Name=`"NsgForPreparation`" Value=`"{ResourceGroupName}/
{NetworkSecurityGroupName}`"/></CustomProperties>"
```

6. `$cred = Get-Credential` を実行します。プロンプトが表示されたら、接続資格情報を入力します。資格情報は Azure アプリケーション ID とシークレットです。
7. 次のコマンドを実行します。

```
Set-Item -PSPath XDHyp:\HostingUnits\<hostingunitname>
-CustomProperties $customProperty -username $cred.username
-Securepassword $cred.password
```

重要:

SubscriptionIdが見つからないというメッセージが表示された場合は、カスタムプロパティ内のすべての二重引用符（“）をバッククォートと二重引用符（`”）に置き換えます。

8. 更新された `CustomProperties` 設定を確認するには、`dir` を実行します。

注:

更新が反映されるまでに1分以上かかります。

ネットワークセキュリティグループの詳細を取得する

ネットワークセキュリティグループの詳細を取得するには、まずネットワークセキュリティグループを含むリソースグループを取得し、次にリソースグループ名に基づいてネットワークセキュリティグループを取得します。

1. ネットワークセキュリティグループを含むリソースグループを取得します。例：

```
Get-HypInventoryItem -LiteralPath "XDHyp:
\HostingUnits\ctx04con01unit01" -ResourceType resourceGroup -MaxRecords
5 -AdditionalDataFilter '{"containedresourcetypes":
["networksecuritygroup"]}'
```

2. リソースグループ名に基づいてネットワークセキュリティグループを取得します。例：

```
Get-HypInventoryItem -LiteralPath "XDHyp:
\HostingUnits\ctx04con01unit01" -ResourceType securitygroup -MaxRecords
5 -AdditionalDataFilter '{"location": ["eastus", "westus"],
"resourcegroup":["resourcegroupname"]}'
```

空のリソースグループをフィルターする

マシンカタログ作成時にマスターイメージ、マシンプロファイル、または準備済みイメージを選択する際に、PowerShellコマンド`Get-HypInventoryItem`を使用して空のリソースグループをフィルターします。

例:

- 1ページあたりの最大レコード数を取得します。

```
Get-HypInventoryItem -LiteralPath "XDHyp:
\HostingUnits\ctx04con01unit01" -ResourceType resourceGroup -MaxRecords
5
```

- 1ページあたりの最大レコード数を取得し、特定の資源を持つリソースコンテナを見つけるためにフィルターします。

```
Get-HypInventoryItem -LiteralPath "XDHyp:
\HostingUnits\ctx04con01unit01" -ResourceType resourceGroup -MaxRecords
5 -AdditionalDataFilter '{"containedresourcetypes": ["vm",
"manageddisk", "snapshot", "imageversion", "storageaccount"]}'
```

- スキップを使用してページを直接指定して取得し、特定の資源を持つリソースコンテナを見つけるためにフィルターします。

```
Get-HypInventoryItem -LiteralPath "XDHyp:
\HostingUnits\ctx04con01unit01" -ResourceType resourceGroup -MaxRecords
5 -skip 20 -AdditionalDataFilter '{"containedresourcetypes": ["vm",
"manageddisk", "snapshot", "imageversion", "storageaccount"]}'
```

- トークンを使用して次のページを取得し、特定の資源を持つリソースコンテナを見つけるためにフィルターします。

```
Get-HypInventoryItem -LiteralPath "XDHyp:
\HostingUnits\ctx04con01unit01" -ResourceType resourceGroup -MaxRecords
5 -AdditionalDataFilter '{"containedresourcetypes": ["vm",
"manageddisk", "snapshot", "imageversion", "storageaccount"]}'
-ContinuationToken
'ew0KICAiJGlkIjogIjEiLA0KICAiTWF4Um93cyI6IDUsDQogICJSb3dzVG9Ta2lwIjogMj
```

```
UsDQogICJLdXN0b0NsdXN0ZXJVcmwiOiAiaHR0cHM6Ly9hcmctbmV1LTEzLXNmLmFyZy5jb
3JlLndpbmRvd3MubmV0Ig0KfQ=='
```

- タグ「Citrix internal tag」を持つすべてのリソースグループを取得し、`MaxRecords` で最大レコード数を制限します。

```
Get-HypInventoryItem -LiteralPath "XDHyp:
\HostingUnits\ctx04con01unit01" -ResourceType resourceGroup -MaxRecords
5
```

- タグ「Citrix internal tag」を持つマシンプロファイル（マスターイメージ）をフィルターし、`MaxRecords` で最大レコード数を制限します。

```
Get-HypInventoryItem -LiteralPath "XDHyp:
\HostingUnits\ctx04con01unit01" -ResourceType resourceGroup -MaxRecords
5 -AdditionalDataFilter '{"containedresourcetypes": ["vm",
"templatespecversion"]}'
```

- タグ「Citrix internal tag」を持つ準備済みイメージをフィルターし、`MaxRecords` で最大レコード数を制限します。

```
Get-HypInventoryItem -LiteralPath "XDHyp:
\HostingUnits\ctx04con01unit01" -ResourceType resourceGroup -MaxRecords
5 -AdditionalDataFilter '{"containedresourcetypes": ["manageddisk",
"snapshot", "imageversion"]}'
```

- タグ「Citrix internal tag」を持つマシンプロファイル（準備済みイメージ）をフィルターし、`MaxRecords` で最大レコード数を制限します。

```
Get-HypInventoryItem -LiteralPath "XDHyp:
\HostingUnits\ctx04con01unit01" -ResourceType resourceGroup -MaxRecords
5 -AdditionalDataFilter '{"containedresourcetypes": ["vm",
"templatespecversion"]}'
```

- タグ「Citrix internal tag」を持つイメージをフィルターし、`MaxRecords` と場所で最大レコード数を制限します。

```
Get-HypInventoryItem -LiteralPath "XDHyp:
\HostingUnits\ctx04con01unit01" -ResourceType resourceGroup -MaxRecords
5 -AdditionalDataFilter '{"containedresourcetypes": ["manageddisk",
"snapshot", "imageversion", "storageaccount"], "location": ["eastus",
"westus"]}'
```

- タグを考慮せずにすべてのリソースグループを取得します `CitrixResource`。

```
Get-HypInventoryItem -LiteralPath "XDHyp:
\HostingUnits\ctx04con01unit01" -ResourceType resourceGroup -MaxRecords
50 -AdditionalDataFilter '{"containedresourcetypes": ["manageddisk",
"snapshot", "imageversion", "storageaccount"]}' -Force $true
```

Azure Sovereign Airgapクラウド環境に接続する

Azure Sovereign Airgapクラウド環境は、分離されたネットワークドメイン上にある必要がある極秘のワークロードに適しています。ホスト接続の作成時に、カスタムプロパティ `DisableInstanceDiscovery` を使用してAzure Sovereign Airgapクラウド環境に接続できます。

```
<Property xsi:type="StringProperty" Name="DisableInstanceDiscovery"
Value="true" />
```

Azureホスト接続の作成の詳細については、Create-HostingConnection.ps1 を参照してください。

必要なAzure権限

このセクションには、Azureに必要な最小限の一般的な権限が含まれています。

最小限の権限

最小限の権限は、より優れたセキュリティ制御を提供します。ただし、追加の権限を必要とする新機能は、最小限の権限のみを使用しているため失敗します。

ホスト接続の作成

Azureから取得した情報を使用して、新しいホスト接続を追加します。

```
"Microsoft.Network/virtualNetworks/read",

"Microsoft.Compute/virtualMachines/read",

"Microsoft.Compute/disks/read",
```

```
"Microsoft.Resources/providers/read",

"Microsoft.Resources/subscriptions/locations/read",

"Microsoft.Resources/tenants/read",

"Microsoft.Network/networkSecurityGroups/join/action",

"Microsoft.Network/networkSecurityGroups/read",

"Microsoft.Network/networkSecurityGroups/securityRules/read"
```

VMの電源管理

マシンインスタンスの電源をオンまたはオフにします。

```
"Microsoft.Compute/virtualMachines/read",

"Microsoft.Resources/subscriptions/resourceGroups/read",

"Microsoft.Compute/virtualMachines/deallocate/action",

"Microsoft.Compute/virtualMachines/start/action",

"Microsoft.Compute/virtualMachines/restart/action",

"Microsoft.Insights/diagnosticsettings/delete",

"Microsoft.Insights/diagnosticsettings/read",

"Microsoft.Insights/diagnosticsettings/write",
```

VMの作成、更新、または削除

マシンカタログを作成し、マシンを追加、削除、更新し、マシンカタログを削除します。

以下は、マスターイメージがマネージドディスクである場合、またはスナップショットがホスティング接続と同じリージョンにある場合に必要となる最小限の権限のリストです。

```
"Microsoft.Resources/subscriptions/resourceGroups/read",

"Microsoft.Resources/deployments/validate/action",
```

```
"Microsoft.Resources/tags/read",

"Microsoft.Resources/tags/write",

"Microsoft.Compute/virtualMachines/read",

"Microsoft.Compute/virtualMachines/write",

"Microsoft.Compute/virtualMachines/delete",

"Microsoft.Compute/virtualMachines/deallocate/action",

"Microsoft.Compute/snapshots/read",

"Microsoft.Compute/snapshots/write",

"Microsoft.Compute/snapshots/delete",

"Microsoft.Compute/snapshots/beginGetAccess/action",

"Microsoft.Compute/snapshots/endGetAccess/action",

"Microsoft.Compute/disks/read",

"Microsoft.Compute/disks/write",

"Microsoft.Compute/disks/delete",

"Microsoft.Compute/disks/beginGetAccess/action",

"Microsoft.Compute/disks/endGetAccess/action",

"Microsoft.Compute/locations/publishers/artifacttypes/types/versions/
read",

"Microsoft.Compute/skus/read",

"Microsoft.Compute/virtualMachines/extensions/read",

"Microsoft.Compute/virtualMachines/extensions/write",

"Microsoft.Features/providers/features/read",
```

```
"Microsoft.Network/virtualNetworks/read",

"Microsoft.Network/virtualNetworks/subnets/join/action",

"Microsoft.Network/virtualNetworks/subnets/read",

"Microsoft.Network/networkSecurityGroups/read",

"Microsoft.Network/networkSecurityGroups/write",

"Microsoft.Network/networkSecurityGroups/delete",

"Microsoft.Network/networkSecurityGroups/join/action",

"Microsoft.Network/networkInterfaces/read",

"Microsoft.Network/networkInterfaces/write",

"Microsoft.Network/networkInterfaces/delete",

"Microsoft.Network/networkInterfaces/join/action",

"Microsoft.Network/locations/usages/read",

"Microsoft.Compute/capacityReservationGroups/capacityReservations/read"
```

以下の機能の最小限の権限に基づいて、以下の追加の権限が必要です。

- マスターイメージが、ホスティング接続と同じリージョンにあるストレージアカウント内のVHDである場合:

```
"Microsoft.Storage/storageAccounts/read",

"Microsoft.Storage/storageAccounts/listKeys/action",
```

- マスターイメージが共有イメージギャラリーのImageVersionである場合:

```
"Microsoft.Compute/galleries/read",

"Microsoft.Compute/galleries/images/read",
```

```
"Microsoft.Compute/galleries/images/versions/read",
```

- マスターイメージがマネージドディスクであり、スナップショットまたはVHDがホスティング接続のリージョンとは異なるリージョンにある場合:

```
"Microsoft.Storage/storageAccounts/read",

"Microsoft.Storage/storageAccounts/listKeys/action",

"Microsoft.Storage/storageAccounts/write",

"Microsoft.Storage/storageAccounts/delete",

"Microsoft.Storage/checknameavailability/read",

"Microsoft.Storage/locations/usages/read",

"Microsoft.Storage/skus/read",
```

- Citrix管理のリソースグループを使用する場合:

```
"Microsoft.Resources/subscriptions/resourceGroups/write",

"Microsoft.Resources/subscriptions/resourceGroups/delete",
```

- マスターイメージを共有テナントまたはサブスクリプションのAzure Compute Gallery (旧 Shared Image Gallery) に配置する場合:

```
"Microsoft.Compute/galleries/write",

"Microsoft.Compute/galleries/images/write",

"Microsoft.Compute/galleries/images/versions/write",

"Microsoft.Compute/galleries/read",

"Microsoft.Compute/galleries/images/read",

"Microsoft.Compute/galleries/images/versions/read",
```

```
"Microsoft.Compute/galleries/delete",
"Microsoft.Compute/galleries/images/delete",
"Microsoft.Compute/galleries/images/versions/delete",
"Microsoft.Resources/subscriptions/read",
```

- Azure専用ホストサポートを使用する場合:

```
"Microsoft.Compute/hostGroups/read",
"Microsoft.Compute/hostGroups/write",
"Microsoft.Compute/hostGroups/hosts/read",
```

- 顧客管理キー (CMK) を使用したサーバー側暗号化 (SSE) を使用する場合:

```
"Microsoft.Compute/diskEncryptionSets/read",
```

- ARMテンプレート (マシンプロファイル) を使用してVMを展開する場合:

```
"Microsoft.Resources/deployments/write",
"Microsoft.Resources/deployments/operationstatuses/read",
"Microsoft.Resources/deployments/read",
"Microsoft.Resources/deployments/delete",
"Microsoft.Insights/DataCollectionRuleAssociations/Read",
"Microsoft.Insights/dataCollectionRules/read",
```

- Azureテンプレート仕様をマシンプロファイルとして使用する場合:

```
"Microsoft.Resources/templateSpecs/read",
"Microsoft.Resources/templateSpecs/versions/read",
```

アンマネージドディスクを使用したマシンの作成、更新、削除

マスターイメージが VHD であり、管理者が提供するリソースグループを使用する場合に必要となる最小限の権限のリストは次のとおりです。

```
"Microsoft.Resources/subscriptions/resourceGroups/read",

"Microsoft.Resources/tags/read",

"Microsoft.Resources/tags/write",

"Microsoft.Storage/storageAccounts/delete",

"Microsoft.Storage/storageAccounts/listKeys/action",

"Microsoft.Storage/storageAccounts/read",

"Microsoft.Storage/storageAccounts/write",

"Microsoft.Storage/checknameavailability/read",

"Microsoft.Storage/locations/usages/read",

"Microsoft.Storage/skus/read",

"Microsoft.Compute/virtualMachines/deallocate/action",

"Microsoft.Compute/virtualMachines/delete",

"Microsoft.Compute/virtualMachines/read",

"Microsoft.Compute/virtualMachines/write",

"Microsoft.Resources/deployments/validate/action",

"Microsoft.Network/networkInterfaces/delete",

"Microsoft.Network/networkInterfaces/join/action",

"Microsoft.Network/networkInterfaces/read",

"Microsoft.Network/networkInterfaces/write",

"Microsoft.Network/networkSecurityGroups/delete",
```

```
"Microsoft.Network/networkSecurityGroups/join/action",

"Microsoft.Network/networkSecurityGroups/read",

"Microsoft.Network/networkSecurityGroups/write",

"Microsoft.Network/virtualNetworks/subnets/read",

"Microsoft.Network/virtualNetworks/read",

"Microsoft.Network/virtualNetworks/subnets/join/action",

"Microsoft.Network/locations/usages/read",
```

一般権限

共同作成者ロールは、すべてのリソースを管理するためのフルアクセス権を持っています。この権限セットは、新機能の取得を妨げるものではありません。

以下の権限セットは、現在の機能セットで必要とされる以上の権限が含まれていますが、今後も最高の互換性を提供します。

```
"Microsoft.Compute/diskEncryptionSets/read",

"Microsoft.Compute/disks/beginGetAccess/action",

"Microsoft.Compute/disks/delete",

"Microsoft.Compute/disks/endGetAccess/action",

"Microsoft.Compute/disks/read",

"Microsoft.Compute/disks/write",

"Microsoft.Compute/galleries/delete",

"Microsoft.Compute/galleries/images/delete",

"Microsoft.Compute/galleries/images/read",

"Microsoft.Compute/galleries/images/versions/delete",
```

```
"Microsoft.Compute/galleries/images/versions/read",

"Microsoft.Compute/galleries/images/versions/write",

"Microsoft.Compute/galleries/images/write",

"Microsoft.Compute/galleries/read",

"Microsoft.Compute/galleries/write",

"Microsoft.Compute/hostGroups/hosts/read",

"Microsoft.Compute/hostGroups/read",

"Microsoft.Compute/hostGroups/write",

"Microsoft.Compute/snapshots/beginGetAccess/action",

"Microsoft.Compute/snapshots/delete",

"Microsoft.Compute/snapshots/endGetAccess/action",

"Microsoft.Compute/snapshots/read",

"Microsoft.Compute/snapshots/write",

"Microsoft.Compute/virtualMachines/deallocate/action",

"Microsoft.Compute/virtualMachines/delete",

"Microsoft.Compute/virtualMachines/read",

"Microsoft.Compute/virtualMachines/restart/action",

"Microsoft.Compute/virtualMachines/start/action",

"Microsoft.Compute/virtualMachines/write",

"Microsoft.Compute/locations/publishers/artifacttypes/types/versions/
read",

"Microsoft.Compute/skus/read",
```

```
"Microsoft.Compute/virtualMachines/extensions/read",

"Microsoft.Compute/virtualMachines/extensions/write",

"Microsoft.Network/networkInterfaces/delete",

"Microsoft.Network/networkInterfaces/join/action",

"Microsoft.Network/networkInterfaces/read",

"Microsoft.Network/networkInterfaces/write",

"Microsoft.Network/networkSecurityGroups/delete",

"Microsoft.Network/networkSecurityGroups/join/action",

"Microsoft.Network/networkSecurityGroups/read",

"Microsoft.Network/networkSecurityGroups/write",

"Microsoft.Network/virtualNetworks/subnets/read",

"Microsoft.Network/virtualNetworks/read",

"Microsoft.Network/virtualNetworks/subnets/join/action",

"Microsoft.Network/locations/usages/read",

"Microsoft.Resources/deployments/operationstatuses/read",

"Microsoft.Resources/deployments/read",

"Microsoft.Resources/deployments/validate/action",

"Microsoft.Resources/deployments/write",

"Microsoft.Resources/deployments/delete",

"Microsoft.Resources/subscriptions/resourceGroups/read",

"Microsoft.Resources/subscriptions/resourceGroups/write",

"Microsoft.Resources/subscriptions/resourceGroups/delete",
```

```
"Microsoft.Resources/providers/read",
"Microsoft.Resources/subscriptions/locations/read",
"Microsoft.Resources/subscriptions/read",
"Microsoft.Resources/tags/read",
"Microsoft.Resources/tags/write",
"Microsoft.Resources/tenants/read",
"Microsoft.Resources/templateSpecs/read",
"Microsoft.Resources/templateSpecs/versions/read",
"Microsoft.Storage/storageAccounts/delete",
"Microsoft.Storage/storageAccounts/listKeys/action",
"Microsoft.Storage/storageAccounts/read",
"Microsoft.Storage/storageAccounts/write",
"Microsoft.Storage/checknameavailability/read",
"Microsoft.Storage/locations/usages/read",
"Microsoft.Storage/skus/read",
"Microsoft.Features/providers/features/read",
"Microsoft.Insights/DataCollectionRuleAssociations/Read",
"Microsoft.Insights/dataCollectionRules/read",
"Microsoft.Insights/diagnosticsettings/delete",
"Microsoft.Insights/diagnosticsettings/read",
"Microsoft.Insights/diagnosticsettings/write",
"Microsoft.Network/networkSecurityGroups/join/action",
```

```
"Microsoft.Network/networkSecurityGroups/read",

"Microsoft.Network/networkSecurityGroups/securityRules/read",

"Microsoft.Compute/capacityReservationGroups/capacityReservations/read"
```

Azure 非シークレット環境でのホスト接続の検証

MCS マシンカタログの作成と管理に関連するタスクを実行するために、ホスト接続のアクセス許可を検証できます。この実装は、VM の作成、削除、更新、VM の電源管理など、さまざまなシナリオで必要な不足しているアクセス許可を事前に特定するのに役立ち、重要な時期にブロックされるのを回避できます。

PowerShell コマンド `Test-HypHypervisorConnection` を使用して、ホスト接続のアクセス許可を検証できます。コマンドの結果はリストとしてキャプチャされ、リストの各項目は3つのセクションに分かれています。

- カテゴリ: ユーザーが MCS マシンカタログを作成および管理するために実行できるアクションまたはタスク。
- 修正措置: 管理者がユーザーの不足しているアクセス許可の不一致を解決するために実行する必要がある手順。
- 不足しているアクセス許可: カテゴリの不足しているアクセス許可のリスト。

アクセス許可を検証するには、次の手順を実行します。

1. Azure へのホスト接続を作成します。
2. Delivery Controller™ ホストから PowerShell ウィンドウを開きます。
3. Citrix 固有の PowerShell モジュールをロードするには、`asnp citrix*` を実行します。
4. 接続をテストするために必要なアクセス許可があるかどうかを確認するには、次のコマンドを実行します。

   ```
   Test-HypHypervisorConnection -LiteralPath "XDHyp:\Connections\AzureCon"
   ```

   SPN に必要なロールレベルのアクセス許可:

   - Microsoft.Authorization/roleDefinitions/read (サブスクリプションレベル、またはリソースグループが指定されている場合はリソースグループレベル)

- Microsoft.Authorization/roleAssignments/read (サブスクリプションレベル、またはリソースグループが指定されている場合はリソースグループレベル)

SPN に必要な API レベルのアクセス許可:

Microsoft.Graph:

- Application.Read.All
- Directory.Read.All
- ServicePrincipalEndpoint.Read.All

5. 権限を検索するために必要な不足している権限を追加した後、次のコマンドを実行して、さまざまなカテゴリで権限があるかどうかを確認します。

   例:

   より高いレベルの承認が必要なサブスクリプションレベルで接続をテストするには:

   ```
   Test-HypHypervisorConnection -LiteralPath XDHyp:\Connections\ AzureCon
   -SecurePassword $password -UserName 922e65d5-38ae-4cf5-xxxx-xxxxxxxxx
   ```

   例:

   高レベルの承認なしでリソースグループレベルで接続をテストするには:

   ```
   Test-HypHypervisorConnection -LiteralPath XDHyp:\Connections\testles
   -CustomProperties $customProperties | Format-List
   ```

   注:

   CustomProperties パラメーターは、リソースグループが接続固有の情報であるため、リソースグループレベルを提供するために使用されます。

   例:

   リソースグループレベルでより高いレベルの承認を使用して接続をテストするには:

```
Test-HypHypervisorConnection -LiteralPath XDHyp:\Connections\testles
-SecurePassword $password -UserName
922e65d5-38ae-4cf5-832b-54122196b7dd -CustomProperties
$customProperties
```

権限の詳細については、「必要な Azure 権限」を参照してください。

Azure シークレット環境でホスト接続を検証する

ホスト接続がAzureシークレット環境で必要な権限を持っているかどうかを、PowerShellコマンド `Test-HypHypervisorConnection` を使用して検証できます。

ただし、検証結果を正常に取得するには、既存のホスト接続を作成または更新して、カスタムプロパティ `AuthenticationObjectId` を持つようにします。このプロパティには、ホスティング接続に関連付けられたサービスプリンシパルのオブジェクトIDが格納されます。

注:

Azureポータルからサービスプリンシパルのオブジェクトを取得します。アプリケーションのIDは使用しないでください。

AuthenticationObjectId を含めるようにホスト接続を作成または更新する

`New-Item` を使用してホスト接続を作成し、`AuthenticationObjectId` をカスタムプロパティとして追加します。例：

```
New-Item -ConnectionType 'Azure' -HypervisorAddress @('http://
hypervisorhost1.example.com','http://hypervisorhost2.example.com')`

    -LoggingId $loggingId -Path @('XDHyp:\\Connections\\Example') -Persist
-Scope @() `

    -Password 'Password' -UserName 'root' -CustomProperties <Property
xsi:type="StringProperty" Name="AuthenticationObjectId" Value="Object ID
of the service principal"/>
```

`Set-Item` を使用して既存のホスト接続を更新し、`AuthenticationObjectId` をカスタムプロパティとして追加します。手順は次のとおりです。

1. Remote PowerShell SDKを使用してPowerShellウィンドウを開きます。

2. 次のコマンドを実行します。

```
Add-PSSnapin citrix*.

cd XDHyp:\Connections\

dir
```

3. 接続から `CustomProperties` をメモ帳にコピーし、プロパティ設定 `<Property xsi:type="StringProperty" Name="AuthenticationObjectId" Value="Object ID of the service principal"/>` を `CustomProperties` に追加します。
4. PowerShellウィンドウで、変更されたカスタムプロパティに変数を割り当てます。
5. `$cred = Get-Credential` を実行します。プロンプトが表示されたら、接続資格情報を入力します。資格情報はAzureアプリケーションIDとシークレットです。
6. `Set-Item -PSPath XDHyp:\Connections\<Connection_Name> -CustomProperties $customProperty -username $cred.username -Securepassword $cred.password` を実行します。
7. 更新された `CustomProperties` 設定を確認するには、`dir` を実行します。

```
Set-Item -PSPath XDHyp:\Connections\$connName -CustomProperties
<Property xsi:type="StringProperty" Name="AuthenticationObjectId"
Value="Object ID of the service principal"/> -username $cred.username
-Securepassword $cred.password
```

権限のホスト接続を検証する

必要なロールと権限のホスト接続を検証するには、次のコマンドを実行します。

- サブスクリプションレベルでロールと権限が割り当てられている場合:

```
Test-HypHypervisorConnection -LiteralPath XDHyp:\Connections\<Your-
HostingConnection>
```

- リソースグループレベルでロールと権限が割り当てられている場合:

```
Test-HypHypervisorConnection -LiteralPath XDHyp:\Connections\<Your-
HostingConnection>  -CustomProperties $CustomProperties
```

```
$CustomProperties = '<CustomProperties xmlns:xsi="http://www.w3.org/
2001/XMLSchema-instance" xmlns="http://schemas.citrix.com/2014/xd/
machinecreation">'`

+ '<Property xsi:type="StringProperty" Name="ResourceGroups"
Value="ExampleResourceGroup" />'`

+ '</CustomProperties>'
```

次のステップ

- 初期展開プロセス中の場合は、「マシンカタログの作成」を参照してください。
- Azure固有の情報については、「Microsoft Azureカタログの作成」を参照してください。

詳細情報

- 接続とリソース
- マシンカタログの作成

Microsoft System Center バーチャル マシン マネージャー への接続

接続とリソースの作成および管理では、接続を作成するウィザードについて説明します。以下の情報は、Microsoft System Center Virtual Machine Manager (VMM) に固有の詳細を扱います。

注：

VMM への接続を作成する前に、まず VMM アカウントをリソースの場所として設定を完了する必要があります。Microsoft System Center Virtual Machine Manager 仮想化環境を参照してください。

接続を作成する

MCSを使用してVMをプロビジョニングした場合は、接続作成ウィザードで次の操作を行います。

- ホストサーバーの完全修飾ドメイン名としてアドレスを入力します。
- 以前に設定した管理者アカウントの資格情報を入力します。このアカウントには、新しいVMを作成する権限が必要です。
- 「ホストの詳細」ダイアログボックスで、VMの作成時に使用するクラスターまたはスタンドアロンホストを選択します。

> **重要**
>
> 単一のHyper-Vホスト展開を使用している場合でも、クラスターまたはスタンドアロンホストを参照してください。

次のステップ

- 初期展開プロセス中の場合は、マシンカタログの作成を参照してください。
- SMB 3 ファイル共有で MCS を使用してマシンカタログを作成する場合は、Microsoft System Center Virtual Machine Manager カタログの作成を参照してください。

詳細情報

- 接続とリソース
- マシンカタログの作成

Nutanixへの接続

接続とリソースの作成および管理では、接続を作成するウィザードについて説明しています。以下の情報は、Nutanixに固有の詳細を扱っています。

> **注:**
>
> Nutanixへの接続を作成する前に、まず、Nutanixアカウントをリソースの場所として設定を完了する必要があります。「Nutanix仮想化環境」を参照してください。

Nutanixへの接続を作成する

以下の情報は、「接続とリソース」のガイダンスを補足するものです。Nutanix接続を作成するには、その記事の一般的なガイダンスに従い、Nutanixに固有の詳細に注意してください。

接続とリソースの追加ウィザードで、**接続**ページでNutanix接続の種類を選択し、アドレスと資格情報、および接続の名前を指定します。**ネットワーク**ページで、ホスティングユニットのネットワークを選択します。

選択できる接続の種類は、**Nutanix AHV**、**Nutanix AHV DRaaS**、**Nutanix AHV PC**です。

- **Nutanix AHV**の場合、Prism Element（PE）クラスターのアドレスと資格情報を指定します。

- **Nutanix AHV PC**の場合、Prism Central（PC）のアドレスと資格情報を指定します。

> **注:**
>
> 現在、Nutanix AHV PC接続タイプは、Azure上のNutanix Cloud Cluster (NC2) への接続を作成する場合にのみ使用されます。また、マシンカタログは、Azure接続上のNC2内の単一クラスターでのみホストできます。

- **Nutanix AHV DRaaS**の場合、DRaaSテナントのアドレスとユーザー名を指定します。プライベートおよびパブリックのNutanix DRaaS資格情報ファイル (`.pem`) をインポートします。

> **ヒント:**
>
> Nutanix AHV (Prism Element) をリソースとして使用してマシンを展開する場合、仮想マシンのディスクが存在するコンテナを選択します。

次のステップ

- 初期展開プロセス中の場合は、「マシンカタログの作成」(/ja-jp/citrix-virtual-apps-desktops/2503/install-configure/machine-catalogs-create.html) を参照してください。
- Nutanix固有の情報については、「Nutanixカタログの作成」(/ja-jp/citrix-virtual-apps-desktops/2503/install-configure/machine-catalogs-create/create-machine-catalog-nutanix.html) を参照してください。

詳細情報

- 「接続とリソース」(/ja-jp/citrix-virtual-apps-desktops/2503/manage-deployment/connections.html)
- 「マシンカタログの作成」(/ja-jp/citrix-virtual-apps-desktops/2503/install-configure/machine-catalogs-create.html)

Nutanix クラウドおよびパートナーソリューションへの接続

(/ja-jp/citrix-virtual-apps-desktops/2503/install-configure/connections.html)では、接続を作成するウィザードについて説明します。以下の情報は、Nutanix クラウドおよびパートナーソリューションに固有の詳細を扱っています。

Citrix Virtual Apps and Desktops™ は、以下の Nutanix クラウドおよびパートナーソリューションをサポートしています。

- AWS 上のニュータニックス・クラウド・クラスター

> **注：**
>
> Nutanix クラウドおよびパートナーソリューションへの接続を作成する前に、まずリソースの場所としてそれぞれのアカウントの設定を完了する必要があります。(/ja-jp/citrix-virtual-apps-desktops/2503/install-configure/install-prepare/nutanix-cloud-patrner-solutions.html)を参照してください。

Nutanix Prismへの接続

Nutanix クラスターを作成したら、Nutanix Prism に接続します。

Nutanix Prism に接続するには：

1. 10.0.129.0/24 サブネットに踏み台 VM を作成します。
2. 踏み台 VM に RDP 接続し、前のセクションでコピーした **Prism Element** の URL に移動します。
3. デフォルトの資格情報 `admin:nutanix/4u` を使用してログインします。パスワードを変更することを忘れないでください。

Nutanixクラスター上にVMを作成する

Nutanix Prism に接続した後、Nutanix クラスター上の VM を作成します。

VM にインターネットアクセスが必要な場合

1. AWSコンソールに移動します。
2. Nutanix CFS によって作成された VPC と同じ VPC に、新しいサブネット 10.0.130.0/24 を作成します。
3. このサブネットのルートテーブルにルートを追加し、すべての非ローカルトラフィックを上記のNATゲートウェイに転送するようにします。
4. 踏み台VMにRDP接続し、前のセクションでコピーした**Prism Element**のURLにアクセスしてログインします。
5. 新しいネットワークを追加します。**Settings>Network Configuration>Create Subnet**に移動します。AWSで使用したのと同じサブネット10.0.130.0/24を使用します。

6. その新しいサブネットにすべてのVM（AD、CC、VDAなど）を作成します。

VM がインターネットアクセスを必要としない場合

1. 踏み台VMにRDP接続し、前のセクションでコピーした**Prism Element**のURLにアクセスしてログインします。
2. 新しいネットワークを追加します。**Settings>Network Configuration>Create Subnet**に移動します。サブネット10.0.129.0/24を使用します。
3. そのサブネットにすべてのVM（AD、CC、VDAなど）を作成します。

> **ヒント:**

> VM の時刻とタイムゾーン情報が正しく設定されていることを確認してください。これは特に AD に当てはまります。

ホスト接続を作成

1. Web Studioを起動します。
2. ホスティングノードを選択し、**Add Connection and Resources**をクリックします。
3. 「**接続**」画面で、「**新しい接続の作成**」を選択し、「**接続アドレス**」に`https://xxx.xxx.xxx.xxx:9440`と入力します。
4. UIに従ってウィザードを完了します。

> 「**注：**」:

> Web StudioでNutanixのオプションを表示するには、すべてのコネクタVMにNutanixプラグインがインストールされている必要があります。これは、Nutanixゾーンで使用されていない場合でも同様です。

次のステップ

- 初期展開プロセス中の場合は、「マシンカタログの作成」を参照してください。
- Nutanix 固有の情報については、「Nutanix カタログの作成」を参照してください。(/ja-jp/citrix-virtual-apps-desktops/2503/install-configure/machine-catalogs-create/create-machine-catalog-nutanix.html)

詳細情報

- 「接続とリソース」
- 「マシンカタログの作成」

Red Hat OpenShift への接続 (プレビュー)

(/ja-jp/citrix-virtual-apps-desktops/2503/install-configure/connections.html) は、接続を作成するウィザードについて説明しています。以下の情報は、Red Hat OpenShift に固有の詳細を扱っています。

> **注:**
>
> Red Hat OpenShift への接続を作成する前に、まず Red Hat OpenShift のセットアップを完了する必要があります。Red Hat OpenShift 仮想化環境 を参照してください。

接続を作成する

Red Hat OpenShift クラスターへの接続は、以下を使用して作成できます。

- Webスタジオ
- PowerShell

Web Studio を使用して接続を作成する

1. Web Studio で、**ホスティング > 接続とリソースの追加** を開きます。
2. **接続** ページで、以下の手順に従って接続を構成します。
    a. **新しい接続を作成** を選択します。
    b. 接続の種類として **Red Hat OpenShift** を選択します。
    c. **接続アドレス** フィールドに、OpenShift サーバーの IP アドレス、ホスト名、または FQDN を入力します。
    d. サービスアカウントトークンと、わかりやすい接続名を入力します。
    e. 「**ゾーン**」設定はデフォルトのままにします。
3. **次へ**をクリックします。接続設定が開始されます。

    自己署名証明書が検出された場合、証明書のサムプリントを含む警告ページが表示されます。続行するには：

a. サムプリントをサーバーのものと比較して、証明書の有効性を確認します。

b. 有効な場合は、**証明書を信頼する**を選択し、**OK**をクリックして接続設定を完了します。

証明書は信頼済みとしてマークされ、サムプリントは今後の検証のために保存されます。

PowerShellコマンドを使用した接続の作成

PowerShellコマンドを使用して接続を作成する場合、次の情報を提供します。

- ホスティング接続名
- クラスターAPIアドレス
- ユーザー名
- パスワード（サービスアカウントトークン）
- SSLThumbprint：これはCA証明書のサムプリントであり、APIサーバーのサムプリントではありません。サムプリントを指定せずにホスティング接続を作成しようとすると、サーバーがCA証明書のサムプリントを提供します。
- ZoneUid

1. PowerShellウィンドウを開きます。
2. `add-pssnapin citrix*` を実行します。
3. ホスティング接続を作成するには、次のコマンドを実行します。

   サムプリントを指定せずにホスティング接続を作成しようとすると、サーバーがCA証明書のサムプリントを提供します。例:

```
$newItemParameters = @{

ConnectionType= "Custom"

PluginId= "OpenShiftPluginFactory"

HypervisorAddress = "https://
api.myopenshiftclusteraddress.mydomain.local:6443"

Path= "XDHyp:\Connections\OpenShiftConnectionName"

Persist= $true

UserName= "__ServiceAccount__"
```

```
Password= "<service account token>"

ErrorVariable= "connectionError"

 }



& New-Item @newItemParameters




$newItemParameters["SSLThumbprint"] =
$connectionError[0].ErrorData.Thumbprint

$connection = & New-Item @newItemParameters

$brokerConnection = New-BrokerHypervisorConnection
-HypHypervisorConnectionUid $connection.HypervisorConnectionUid
```

ホスティングユニットの作成

ホスティングユニットは、VMが作成される環境を表します。ホスティングユニットを作成するには、OpenShiftから次の入力が必要です。

- 名前空間
- ストレージクラス
- ネットワークアタッチメント定義

ホスティングユニットは名前空間にバインドされます。これは、1つのホスティングユニットが1つの名前空間のみにアクセスでき、その名前空間下のVMを管理することを意味します。

現在、PowerShellのみを使用してホスティングユニットを作成できます。

PowerShellコマンドを使用してホスティングユニットを作成する場合、次の情報を提供します。

- ホスティング接続名
- ホスティングユニット名
- ターゲットの名前空間名

- ストレージクラス名
- NetworkAttachmentDefinition 名

1. PowerShell ウィンドウを開きます。
2. `add-pssnapin citrix*` を実行します。
3. PowerShell コマンドを実行してホスティングユニットを作成します。例:

```
$HostingConnectionName = "OpenShiftConnectionName"

$HostingUnitName = "HostingUnitName"

$TargetNamespace = "TargetNamespaceName"

$StorageClassToUse = "YourStorageClassesName"

$NetworkAttachmentDefinition = "YourNetworkAttachmentDefinitionName"

New-HypStorage `

-StoragePath @("XDHyp:\Connections\$HostingConnectionName\
$TargetNamespace.namespace\$StorageClassToUse.storage") `

-StorageType "TemporaryStorage"

New-Item `

-CustomProperties "" `

-HypervisorConnectionName $HostingConnectionName `

-NetworkPath @("XDHyp:\Connections\$HostingConnectionName\
$TargetNamespace.namespace\$NetworkAttachmentDefinition.network") `

-Path @("XDHyp:\HostingUnits\$HostingUnitName") -RootPath "XDHyp:
\Connections\$HostingConnectionName\$TargetNamespace.namespace" `

-StoragePath @("XDHyp:\Connections\$HostingConnectionName\
$TargetNamespace.namespace\$StorageClassToUse.storage")
```

次のステップ

- 初期展開プロセスの場合は、マシンカタログの作成 を参照してください。

- Red Hat OpenShift 固有の情報については、Red Hat OpenShift カタログの作成 を参照してください。

詳細情報

- 接続とリソース
- マシンカタログの作成

VMwareへの接続

接続とリソースの作成および管理では、接続を作成するウィザードについて説明します。以下の情報は、VMware仮想化環境に固有の詳細を扱います。

> **注:**
>
> VMwareへの接続を作成する前に、まずVMwareアカウントをリソースの場所として設定を完了する必要があります。VMware仮想化環境を参照してください。

接続を作成する

接続作成ウィザードで：

1. VMware接続の種類を選択します。
2. vCenter SDKのアクセスポイントのアドレスを指定します。
3. 以前に設定した、VMを作成する権限を持つVMwareユーザーアカウントの資格情報を指定します。ユーザー名はdomain/usernameの形式で指定します。

VMware SSLサムプリント

VMware SSLサムプリント機能により、VMware vSphereハイパーバイザーへのホスト接続を手動で作成する必要がなくなります。接続を作成する前に、サイト内のDelivery Controllerとハイパーバイザーの証明書との間に信頼関係を手動で作成する必要はなくなりました。

VMware SSLサムプリント機能は、信頼されていない証明書のサムプリントをサイトデータベースに保存します。この構成により、コントローラーによって信頼されていなくても、ハイパーバイザーがCitrix Virtual Apps and Desktops™によって継続的に信頼されていると識別されることが保証されます。

StudioでvSphereホスト接続を作成する際、接続先のコンピューターの証明書を表示できるダイアログボックスが表示されます。その後、それを信頼するかどうかを選択できます。

必要な権限

VMwareユーザーアカウントと、この記事に記載されている権限の一部またはすべてを持つ1つ以上のVMwareロールを作成します。ロールの作成は、ユーザーがいつでもさまざまなCitrix DaaS™操作を要求するために必要な権限の特定の粒度レベルに基づいて行います。特定の時点でユーザー固有の権限を付与するには、**子に伝播**オプションを選択して、少なくともデータセンターレベルでそれぞれのロールに関連付けます。ただし、`StorageProfile`権限と特定の`Tags`権限については、**子に伝播**なしで、ルートvCenter Serverレベルで権限を適用します。各テーブルの注記を参照してください。

以下の表は、Citrix Virtual Apps and Desktops の操作と、必要な最小限の VMware 権限とのマッピングを示しています。

> **注:**
>
> 権限リストの表示名、特に *ユーザーインターフェイス* は、一部の vSphere バージョンで異なります。たとえば、vSphere 6.7 では、*ユーザーインターフェイス* 権限は、このページに記載されている必要な権限で説明されている **Settings** および **Memory** ではなく、**Change Memory** および **Change Settings** です。

接続とリソースを追加する

SDK	ユーザーインターフェイス
System. 匿名、System. 読み取り、および System. 表示	自動的に追加されます。組み込みの読み取り専用ロールを使用できます。

電源管理

SDK	ユーザーインターフェイス
VirtualMachine.Interact.PowerOff	仮想マシン > インタラクション > 電源オフ
VirtualMachine.Interact.PowerOn	仮想マシン > インタラクション > 電源オン
VirtualMachine.Interact.Reset	仮想マシン > インタラクション > リセット
VirtualMachine.Interact.Suspend	仮想マシン > インタラクション > サスペンド
Datastore.Browse	データストア > データストアの参照

マシンのプロビジョニング (Machine Creation Services™)

MCS を使用してマシンをプロビジョニングするには、次の権限が必要です。

SDK	ユーザーインターフェイス
Datastore.AllocateSpace	データストア > スペースの割り当て
Datastore.Browse	データストア > データストアの参照
Datastore.FileManagement	データストア > 低レベルファイル操作
Network.Assign	ネットワーク > ネットワークの割り当て
Resource.AssignVMToPool	リソース > 仮想マシンをリソースプールに割り当てる
VirtualMachine.Config.AddExistingDisk	仮想マシン > 構成 > 既存のディスクを追加
VirtualMachine.Config.AddNewDisk	仮想マシン > 構成 > 新しいディスクを追加
仮想マシン.構成.デバイスの追加または削除	仮想マシン > 構成 > デバイスの追加または削除
VirtualMachine.Config.AdvancedConfig	仮想マシン > 構成 > 詳細設定
VirtualMachine.Config.RemoveDisk	仮想マシン > 構成 > ディスクの削除
VirtualMachine.Config.CPUCount	仮想マシン > 構成 > CPUカウントの変更
VirtualMachine.Config.Memory	仮想マシン > 構成 > メモリの変更
VirtualMachine.Config.Settings	仮想マシン > 構成 > 設定の変更
VirtualMachine.Interact.PowerOff	仮想マシン > 操作 > 電源オフ
VirtualMachine.Interact.PowerOn	仮想マシン > 操作 > 電源オン
VirtualMachine.Interact.Reset	仮想マシン > 操作 > リセット
VirtualMachine.Interact.Suspend	仮想マシン > 操作 > サスペンド
VirtualMachine.Inventory.CreateFromExisting	仮想マシン > インベントリ > 既存から作成
VirtualMachine.Inventory.Create	仮想マシン > インベントリ > 新規作成

SDK	ユーザーインターフェイス
VirtualMachine.Inventory.Delete	仮想マシン > インベントリ > 削除
VirtualMachine.Provisioning.Clone	仮想マシン > プロビジョニング > 仮想マシンのクローン作成
VirtualMachine.State.CreateSnapshot	vSphere 5.0、Update 2、vSphere 5.1、Update 1、および vSphere 6.x、Update 1: 仮想マシン > 状態 > スナップショットの作成; vSphere 5.5: 仮想マシン > スナップショット管理 > スナップショットの作成

イメージの更新とロールバック

SDK	ユーザーインターフェイス
Datastore.AllocateSpace	データストア > スペースの割り当て
Datastore.Browse	データストア > データストアの参照
Datastore.FileManagement	データストア > 低レベルファイル操作
Network.Assign	ネットワーク > ネットワークの割り当て
Resource.AssignVMToPool	リソース > 仮想マシンをリソースプールに割り当て
VirtualMachine.Config.AddExistingDisk	仮想マシン > 構成 > 既存のディスクを追加
VirtualMachine.Config.AddNewDisk	仮想マシン > 構成 > 新しいディスクを追加
VirtualMachine.Config.AdvancedConfig	仮想マシン > 構成 > 詳細設定
VirtualMachine.Config.RemoveDisk	仮想マシン > 構成 > ディスクの削除
VirtualMachine.Interact.PowerOff	仮想マシン > 操作 > 電源オフ
VirtualMachine.Interact.PowerOn	仮想マシン > 操作 > 電源オン
VirtualMachine.Interact.Reset	仮想マシン > 操作 > リセット
VirtualMachine.Inventory.CreateFromExisting	仮想マシン > インベントリ > 既存から作成

SDK	ユーザーインターフェイス
VirtualMachine.Inventory.Create	仮想マシン > インベントリ > 新規作成
VirtualMachine.Inventory.Delete	仮想マシン > インベントリ > 削除
VirtualMachine.Provisioning.Clone	仮想マシン > プロビジョニング > 仮想マシンのクローン作成

プロビジョニングされたマシンの削除

SDK	ユーザーインターフェイス
Datastore.Browse	データストア > データストアの参照
Datastore.FileManagement	Datastore > 低レベルファイル操作
VirtualMachine.Config.RemoveDisk	仮想マシン > 構成 > ディスクの削除
VirtualMachine.Interact.PowerOff	仮想マシン > 操作 > 電源オフ
VirtualMachine.Inventory.Delete	仮想マシン > インベントリ > 削除

ストレージプロファイル (vSAN)

vSANデータストアでカタログ作成中にストレージポリシーを表示、作成、または削除するには、以下の権限が必要です。

SDK	ユーザーインターフェイス
StorageProfile.Update	プロファイル駆動型ストレージ > プロファイル駆動型ストレージの更新。vSphere 8 の場合: VMストレージポリシー > VMストレージポリシーの更新
StorageProfile.View	PROFILE-DRIVEN STORAGE > プロファイル駆動型ストレージビュー。vSphere 8 の場合: VM ストレージポリシー > VM ストレージポリシーの表示

注記:

ストレージプロファイルの権限は、**子オブジェクトに伝播**せずに、ルートvCenter Serverレベルで適用してください。

タグとカスタム属性

タグとカスタム属性を使用すると、vSphereインベントリで作成されたVMにメタデータを添付し、これらのオブジェクトの検索とフィルタリングを容易にすることができます。タグまたはカテゴリを作成、編集、割り当て、削除するには、次の権限が必須です。

SDK	ユーザーインターフェイス
InventoryService.Tagging.CreateTag	vSphere タグ付け > vSphere タグの作成
InventoryService.Tagging.CreateCategory	vSphere タグ付け > vSphere タグカテゴリの作成
InventoryService.Tagging.EditTag	vSphere タグ付け > vSphere タグの編集
InventoryService.Tagging.EditCategory	vSphere タグ付け > vSphere タグカテゴリの編集
InventoryService.Tagging.DeleteTag	vSphere タグ付け > vSphere タグの削除
InventoryService.Tagging.DeleteCategory	vSphere タグ付け > vSphere タグカテゴリの削除
InventoryService.Tagging.AttachTag	vSphere タグ付け > vSphere タグの割り当てまたは割り当て解除
InventoryService.Tagging.ObjectAttachable	vSphere タグ付け > オブジェクトへの vSphere タグの割り当てまたは割り当て解除
Global.ManageCustomFields	グローバル > カスタム属性の管理
Global.SetCustomField	グローバル > カスタム属性の設定

注:

- MCS がマシンカタログを作成すると、ターゲット VM に特別な名前タグが付けられます。これらのタグは、マスターイメージを MCS で作成された VM と区別し、MCS で作

成された VM がイメージ準備に使用されるのを防ぎます。vCenter の `XdProvisioned` 属性の値によって違いを識別できます。MCS が VM を作成した場合、この属性は **True** に設定されます。

- **子に伝播**せずに、ルート vCenter Server レベルで `InventoryService.Tagging.AttachTag` 権限を適用します。

暗号化操作

暗号化操作の権限は、誰がどの種類のオブジェクトに対してどの種類の暗号化操作を実行できるかを制御します。vSphere Native Key Provider は `Cryptographer.*` 権限を使用します。暗号化操作には、次の最小限の権限が必要です。

注:

これらの権限は、vTPM を搭載した VM を使用して MCS マシンカタログを作成するために必要です。

SDK	ユーザーインターフェイス
Cryptographer.Access	権限 > すべての権限 > 暗号化操作 > 直接アクセス
Cryptographer.AddDisk	権限 > すべての権限 > 暗号化操作 > ディスクの追加
Cryptographer.Clone	特権 > すべての特権 > 暗号化操作 > クローン
Cryptographer.Encrypt	特権 > すべての特権 > 暗号化操作 > 暗号化
Cryptographer.EncryptNew	特権 > すべての特権 > 暗号化操作 > 新規暗号化
Cryptographer.Decrypt	特権 > すべての特権 > 暗号化操作 > 復号化
Cryptographer.Migrate	特権 > すべての特権 > 暗号化操作 > 移行

SDK	ユーザーインターフェイス
Cryptographer.ReadKeyServersInfo	特権 > すべての特権 > 暗号化操作 > KMS情報の読み取り

マシンのプロビジョニング (Citrix Provisioning™)

Citrix Provisioningコンソールを介してCitrix Virtual Apps and Desktopsセットアップウィザードおよびデバイスのエクスポートウィザードを使用してVMをプロビジョニングするには、テンプレートをクローンおよび展開するためのこれらの権限が必要です。ホスティング接続の作成時に権限を設定します。マシンのプロビジョニング（Machine Creation Services）のすべての権限と、以下の権限が必要です。

SDK	ユーザーインターフェイス
VirtualMachine.Config.AddRemoveDevice	仮想マシン > 構成 > デバイスの追加または削除
VirtualMachine.Config.CPUCount	仮想マシン > 構成 > CPU数の変更
VirtualMachine.Config.Memory	仮想マシン > 構成 > メモリ
VirtualMachine.Config.Settings	仮想マシン > 構成 > 設定
VirtualMachine.Provisioning.CloneTemplate	仮想マシン > プロビジョニング > テンプレートのクローン作成
VirtualMachine.Provisioning.DeployTemplate	仮想マシン > プロビジョニング > テンプレートの展開
VApp.Export	vApp > エクスポート

注:

`VApp.Export` は、マシンプロファイルを使用して MCS マシンカタログを作成するために必要です。

証明書を取得してインポートする

vSphere 通信を保護するため、Citrix® は HTTP ではなく HTTPS を使用することを推奨します。

HTTPS にはデジタル証明書が必要です。組織のセキュリティポリシーに準拠した認証局から発行されたデジタル証明書を使用してください。

認証局から発行されたデジタル証明書を使用できない場合は、VMware がインストールした自己署名証明書を使用できます。この方法は、組織のセキュリティポリシーで許可されている場合にのみ使用してください。VMware vCenter 証明書を各 Delivery Controller に追加します。

1. vCenter Server を実行しているコンピューターの完全修飾ドメイン名 (FQDN) を、そのサーバーのホストファイルに `%SystemRoot%/WINDOWS/system32/Drivers/etc/` で追加します。この手順は、vCenter Server を実行しているコンピューターの FQDN がドメインネームシステムにまだ存在しない場合にのみ必要です。
2. 以下の3つの方法のいずれかを使用して vCenter 証明書を取得します。

   vCenter サーバーから。

   a. rui.crt ファイルを vCenter サーバーから Delivery Controller でアクセス可能な場所にコピーします。
   b. Controller で、エクスポートされた証明書の場所に移動し、rui.crt ファイルを開きます。

   Web ブラウザーを使用して証明書をダウンロードします。 Internet Explorer を使用している場合は、Internet Explorer を右クリックし、**管理者として実行** を選択して証明書をダウンロードまたはインストールします。

   a. Web ブラウザーを開き、vCenter サーバーへの安全な Web 接続を行います (例: `<https://server1.domain1.com)>`。
   b. セキュリティ警告を承認します。
   c. 証明書エラーが表示されているアドレスバーをクリックします。
   d. 証明書を表示し、 タブをクリックします。
   e. 「**ファイルにコピーして.CER形式でエクスポート**」を選択し、プロンプトが表示されたら名前を指定します。
   f. エクスポートされた証明書を保存します。
   g. エクスポートされた証明書の場所に移動し、.CERファイルを開きます。

   「**管理者として実行しているInternet Explorerから直接インポートします。**」.

   - Webブラウザを開き、vCenterサーバーへの安全なWeb接続を確立します (例: `<https://server1.domain1.com)>`)。
   - セキュリティ警告を承諾します。

- 証明書エラーが表示されているアドレスバーをクリックします。
- 証明書を表示します。

3. 各Controllerの証明書ストアに証明書をインポートします。

   a. 「**証明書のインストール**」オプションをクリックし、「**ローカルコンピューター**」を選択して、「**次へ**」をクリックします。

   b. 「**証明書をすべて次のストアに配置する**」を選択し、「**参照**」をクリックします。「**信頼されたユーザー**」を選択し、「**OK**」をクリックします。「**次へ**」をクリックし、「**完了**」をクリックします。

   インストール後にvSphereサーバーの名前を変更した場合は、新しい証明書をインポートする前に、そのサーバーで新しい自己署名証明書を生成する必要があります。

次のステップ

- 初期展開プロセス中の場合は、「マシンカタログの作成」を参照してください。
- VMware固有の情報については、「VMwareカタログの作成」を参照してください。

詳細情報

- 接続とリソース
- マシンカタログの作成

VMware クラウドおよびパートナーソリューションへの接続

Azure VMware Solution (AVS) cluster、Google Cloud VMware Engine、およびVMware cloud on AWSをセットアップした後、接続を作成します。接続の作成については、Connection to VMwareを参照してください。

次のステップ

- 初期展開プロセス中の場合は、Create machine catalogsを参照してください。
- VMware固有の情報については、Create a VMware catalogを参照してください。

詳細情報

- 接続とリソース
- マシンカタログの作成

マシンID管理のためのサービスアカウント

サービスアカウントは、保存された資格情報のコンテナであり、ユーザーの操作なしにマシンID関連の操作を実行するように構成および使用されます。マシンID管理の権限を必要とする操作の前に、サービスアカウントを作成してください。

MCSマシンカタログを構成して、サービスアカウントを次の目的で使用できます。

- Active Directoryでコンピューターアカウントを作成または削除する際に、毎回ドメイン資格情報を入力する必要がない。
- 古くなったAzure AD参加済みデバイスまたはMicrosoft Intune登録済みデバイスを、Azure ADまたはIntuneポータルから手動で削除することなく管理する。

サポートされているサービスアカウントの種類

Citrix®では、IDプロバイダーの種類に基づいて、以下のサービスアカウントを作成できます。

IDプロバイダーの種類	説明	資格情報
オンプレミスActive Directoryサービスアカウント	マシンカタログとコンピューターアカウントを、毎回ドメイン資格情報を入力することなく管理します。	オンプレミスActive Directoryユーザーアカウントのユーザー名とパスワード。

資格情報の保護

Citrixは、サービスアカウントの資格情報を顧客のサイトデータベースに保存します。DaaSでは、サイトデータベースはテナント（顧客）ごとのデータベースであり、顧客向けに実行されているサービスのみがアクセス可能です。

保存された資格情報を保護するために、以下の対策も実施されています。

- 資格情報は、データベースに保存される前に、**AES 256**暗号化を使用して暗号化されます。
- 暗号化キーはサイトごとに生成され、Delivery Controller™にローカルに保存されます。これは、お客様専用のサービスのみがアクセスできます。
- データベースへの接続は、TLS 1.2プロトコルを使用して暗号化されます。

オンプレミス Active Directory サービスアカウント

オンプレミス Active Directory サービスアカウントは、特権ドメインユーザーアカウントのユーザー名とパスワードを保存するためのコンテナです。このユーザーアカウントは、Active Directory でコンピューターアカウントを管理するのに十分な権限を持っている必要があります。

Machine Creation Service は、このサービスアカウントを使用して、毎回ドメイン資格情報を入力することなく、コンピューターアカウント関連の操作を実行できます。

オンプレミス Active Directory サービスアカウントを作成する

Studio または PowerShell を使用して、オンプレミス Active Directory サービスアカウントを作成します。

前提条件

オンプレミス Active Directory サービスアカウントを作成するには、次のタスクを完了していることを確認してください。

- Active Directory または特定の OU でコンピューターオブジェクトを作成、更新、削除するのに十分な権限を持つドメインユーザーアカウントを Active Directory に作成します。

Web Studio を使用する

1. **DaaS** タイルで、**管理**をクリックします。
2. 左側のペインで、**管理者**を選択します。
3. **サービスアカウント**タブで、**サービスアカウントの作成**をクリックします。
4. **IDの種類**ページで、**オンプレミス Active Directory**を選択します。**次へ**をクリックします。
5. **資格情報**ページで、**資格情報の入力**をクリックして、サービスアカウントとして使用する特権ドメインユーザーアカウントのユーザー名とパスワードを入力します。
6. パスワードの有効期限を設定するか、期限なしのままにします。
7. このサービスアカウントのスコープを1つ以上選択します。
8. サービスアカウントのフレンドリ名と説明（オプション）を入力します。
9. 作成を完了するには、**「完了」**をクリックします。

PowerShell を使用する

PowerShellコマンドを使用して、オンプレミスのActive Directoryサービスを作成できます。例：

```
$credential = ConvertTo-SecureString -String $password -AsPlainText -Force

New-AcctServiceAccount -IdentityProviderType ActiveDirectory
-IdentityProviderIdentifier test.local -AccountId test\svcacct_mcs
-AccountSecret $credential -SecretExpiryTime 2030/08/15 -DisplayName
'scvacct_mcs' -Description 'Service account for test.local'
```

> **注:**
>
> `$password` は、指定されたドメインユーザーアカウントの一致するパスワードです。

マシンのID関連のアクションを実行する

Active Directory またはハイブリッド Azure AD ベースのIDプールがサービスアカウントに関連付けられると、ドメイン資格情報を入力することなく、さまざまなマシンID関連のアクションを実行できます。

- サービスアカウントを使用して新しいIDアカウントを作成するには

```
New-AcctADAccount -IdentityPoolName MyPool -Count 2 -UseServiceAccount
```

- サービスアカウントを使用してIDアカウントを修復するには

```
Repair-AcctADAccount -ADAccountName "Domain\account","Domain\account2"
-UseServiceAccount
```

- サービスアカウントを使用してIDアカウントを削除するには

```
Remove-AcctADAccount -IdentityPoolName MyPool -RemovalOption Delete
-ADAccountName "Domain\account","domain\account2" -UserServiceAccount
```

次のステップ

- オンプレミスのActive Directory参加済みカタログを作成するには、「オンプレミスのActive Directory参加済みマシンIDのIDプール」を参照してください。
- サービスアカウントを管理するには、「サービスアカウントの管理」を参照してください。

サービスアカウントを管理する

サービスアカウントの管理は、それらが健全な状態を保ち、資格情報が最新であることを保証するための重要な側面です。この記事では、サービスアカウントの表示、名前変更、編集、テスト、および削除の手順について説明します。

サービスアカウントの詳細を表示する

1. **DaaS**タイルで、**管理**をクリックします。

2. 左ペインで、**管理者**を選択します。
3. **サービスアカウント**タブを選択します。
4. サービスアカウントを選択し、下部パネルでその詳細を表示します。各サービスアカウントのプロパティ、関連するマシンカタログ、およびトラブルシューティングのヒントを下部パネルで確認します。

次の場合、サービスアカウントの横にエラーまたは警告アイコンが表示されます。

- サービスアカウントが異常な状態である場合。
- サービスアカウントの資格情報の有効期限が近づいている場合。

トラブルシューティングタブには、問題を診断して修正するための情報が提供されます。

> **注:**
>
> 問題を修正した後、サービスアカウントテストを実行してステータスを更新します。詳細については、「サービスアカウントをテストする」を参照してください。

サービスの名前を変更する

1. 「**DaaS**」タイルで、「**管理**」をクリックします。
2. 左側のペインで、「**管理者**」を選択します。
3. **サービスアカウント**タブを選択します。
4. サービスアカウントを選択し、**名前の変更**をクリックします。

サービスアカウントを編集する

1. 「**DaaS**」タイルで、「**管理**」をクリックします。
2. 左側のペインで、「**管理者**」を選択します。
3. **サービスアカウント**タブを選択します。
4. サービスアカウントを選択し、**編集**をクリックします。

サービスアカウントをテストする

1. 「**DaaS**」タイルで、「**管理**」をクリックします。
2. 左側のペインで、「**管理者**」を選択します。
3. **サービスアカウント**タブを選択します。

4. サービスアカウントを選択し、**サービスアカウントのテスト**をクリックします。

- オンプレミスのActive Directoryサービスアカウントの場合、テスト中に資格情報が検証されます。
- Azure ADサービスアカウントの場合、アプリケーションIDとシークレット、および必要な権限はテスト中に検証されます。

推奨事項に従って問題を特定し、修正します。**トラブルシューティング**タブには、問題を診断して修正するための情報が提供されます。問題を修正した後、サービスアカウントをテストします。

サービスアカウントを削除する

サービスアカウントを削除する前に、そのサービスアカウントがどのMCSマシンカタログでも使用されていないことを確認してください。

1. 「**DaaS**」タイルで、「**管理**」をクリックします。
2. 左側のペインで、「**管理者**」を選択します。
3. **サービスアカウント**タブを選択します。
4. サービスアカウントを選択し、**削除**をクリックします。

イメージ管理

はじめに

MCSカタログの作成または更新プロセスには、次の2つのフェーズがあります。

- マスタリング: ソースイメージが公開イメージに変換されます
- クローニング: 公開イメージから新しいVMが作成されます

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

単一のソースイメージからさまざまなMCSイメージバージョン（準備済みイメージ）を準備し、複数の異なるMCSマシンカタログでそれを使用できます。また、同じホスト接続内のホスティングユニット間で準備済みイメージバージョンを共有することもできます。この実装により、ストレージと時間のコストが大幅に削減され、VMの展開とイメージ更新プロセスが簡素化されます。

このイメージ管理機能を使用する利点は次のとおりです。

- カタログを作成せずに、準備済みイメージを事前に生成します。
- カタログの作成や更新など、複数のシナリオで準備済みイメージを再利用します。

- カタログの作成または更新時間を大幅に短縮します。
- 同じホスト接続内のホスティングユニット間で準備済みイメージバージョンを共有します。

> **注：**
>
> - この機能は現在、AzureおよびVMware仮想化環境に適用できます。
> - 準備済みイメージを使用せずにMCSマシンカタログを作成できます。その場合、この機能の利点を得ることはできません。

ユースケース

イメージ管理機能のユースケースの一部を次に示します。

- *バージョン管理*: イメージバージョンを使用すると、次のことができます。
  - 特定のイメージに対するさまざまなイテレーションや更新を管理する。
  - さまざまな目的のために、イメージの複数のバージョンを維持する。
- *論理的なグループ化*: 複数のイメージ定義を作成して、次のことができます。
  - プロジェクト、部署、アプリケーション、デスクトップの種類など、さまざまな基準に基づいてイメージバージョンを論理的にグループ化する。
  - 組織内でイメージをより効率的に管理する。
- *イメージ共有*: 同じホスト接続内のホスティングユニット間で準備されたイメージバージョンを共有して、次のことができます。
  - 異なるホスティングユニット間でイメージの一貫性と均一性を確保する。

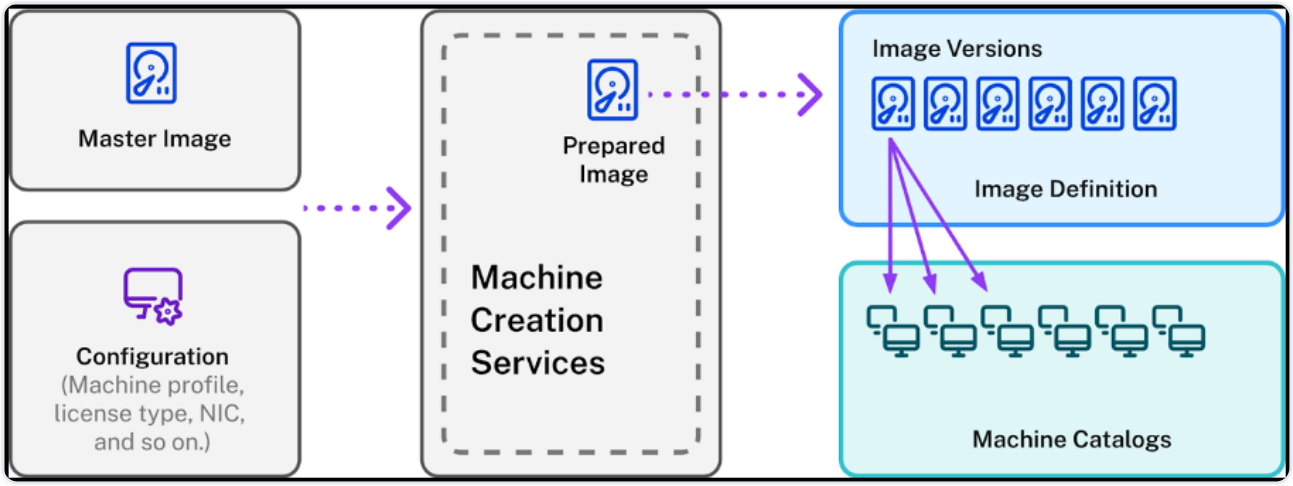
準備されたイメージとは何ですか?

イメージ管理機能により、MCSはマスタリングフェーズをカタログ作成または更新ワークフロー全体から切り離し、プロセスを2つの段階に分けます。

1. 単一のソースイメージから準備されたイメージを作成する。
2. 準備されたイメージを使用して、MCSマシンカタログを作成または更新する。

準備されたイメージは事前に作成できます。単一の準備されたイメージを使用して、複数のMCSプロビジョニング済みマシンカタログを作成または更新できます。

準備されたイメージが、イメージからWeb Studioを使用する際に、複数のMCSマシンカタログでどのように使用されるかを理解します。



イメージ定義: イメージ定義は、イメージのバージョンの論理的なグループ化です。イメージ定義には、次の情報が含まれます。

- イメージが作成された理由
- どのOS用であるか
- イメージの使用に関するその他の情報。

カタログはイメージ定義から作成されるのではなく、イメージ定義に基づいて作成されたイメージバージョンから作成されます。

イメージバージョン: イメージバージョンは、イメージ定義のバージョン管理を行います。1つのイメージ定義には複数のイメージバージョンを含めることができます。イメージバージョンを準備済みイメージとして使用して、カタログを作成または更新します。AzureおよびVMware仮想化環境では、同じホスト接続内のホスティングユニット間でイメージバージョンを共有できます。

あるいは、PowerShellコマンドを使用してプロビジョニングスキームを作成し、カタログを作成または更新する場合は、環境に応じてマスターイメージバージョン仕様に基づいて準備されたイメージバージョン仕様を作成する必要があります。準備されたイメージバージョン仕様は、同じホスティング接続内の別のホスティングユニットと共有することもできます。

要件

- Windowsマスターイメージの場合、VDAイメージバージョン2311以降のみがサポートされます。MCS/IOコンポーネントは明示的に選択してインストールする必要があります。MCS I/O構成の有効化または無効化は、デフォルトでは有効になっていないため、マシンカタログの作成または更新時に決定する必要があります。

制限事項

現在、この機能は以下をサポートしていません。

- Azureでの複数のNIC
- 永続データディスク機能
- マルチセッションの休止状態
- イメージタイプの変更
- Azureのホスティングユニット間で準備済みイメージバージョンを共有する場合、以下の共有方法は許可されていません。
  - 直接共有
  - パブリックコミュニティギャラリーへの共有
- 現在、イメージ管理ではAzure機密VMはサポートされていません。

Web Studioを使用したイメージライフサイクル管理

Web Studioを使用する場合のイメージのライフサイクルは次のとおりです。

1. 準備済みイメージの作成: イメージ定義とその初期イメージバージョンを作成します。
2. 初期イメージバージョンからイメージバージョンを作成します。
3. 他のホスティングユニットでイメージバージョンを使用したい場合は、同じホスティング接続内の別のホスティングユニットとイメージバージョンを共有します。
4. イメージバージョンを準備済みイメージとして使用してカタログを作成します。
5. 異なる準備済みイメージでマシンカタログを更新します。
6. イメージ定義とバージョンを管理する: イメージバージョンの名前と説明、およびイメージ定義の説明を編集します。
7. イメージバージョンを削除します。
8. イメージ定義を削除する。

あるいは、PowerShell を使用してイメージを管理することもできます。PowerShell を使用したイメージのライフサイクル管理を参照してください。

PowerShell を使用したイメージのライフサイクル管理

PowerShell コマンドを使用してプロビジョニングスキームを作成する場合は、環境の必要に応じて、マスターイメージバージョン仕様に基づいて準備済みイメージバージョン仕様を作成する必要があります。

マスターイメージバージョン仕様: マスターイメージバージョン仕様は、イメージバージョン下に追加または作成された特定のイメージです。ハイパーバイザー内の既存のイメージをマスターイメージバージョン仕様として追加したり、環境の必要に応じてマスターイメージバージョン仕様に基づいて準備済みイメージバージョン仕様を作成したりできます。準備済みイメージバージョン仕様は、複数のプロビジョニングスキームに使用できます。

AzureおよびVMware環境では、同じホスティング接続内のホスティングユニット間で準備済みイメージバージョン仕様を共有することもできます。Azureでは、Azure Compute Gallery (ACG) のディスク共有機能を使用して共有が実現されます。

PowerShellコマンドを使用する場合のイメージのライフサイクルは次のとおりです。

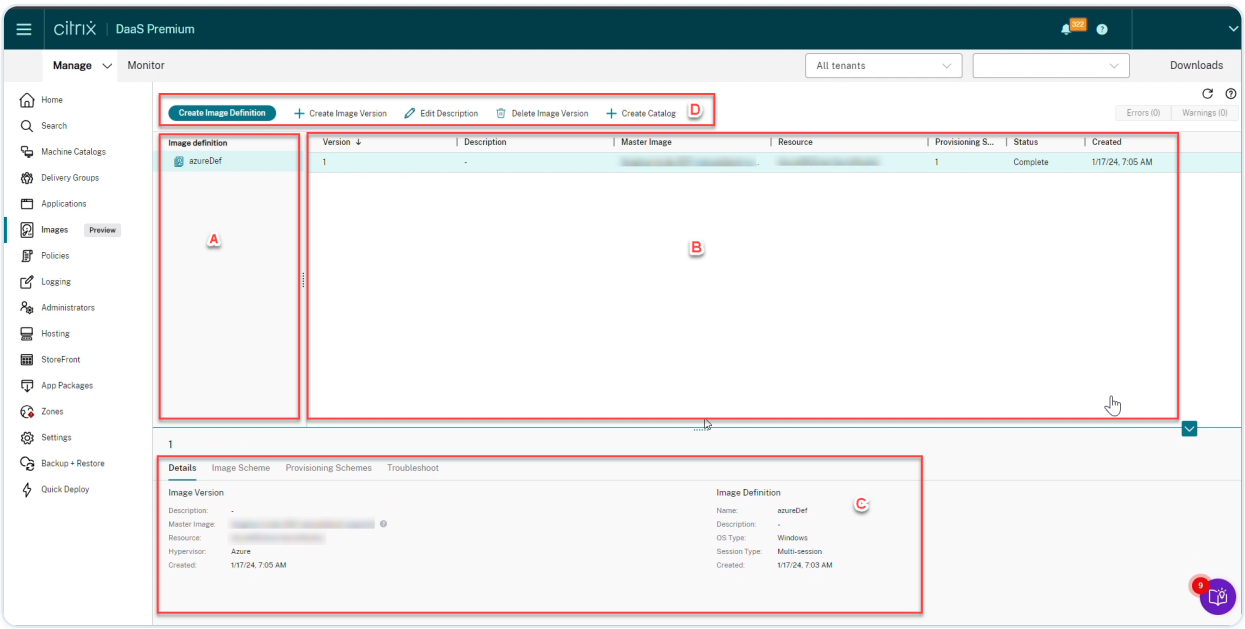
1. イメージを作成する:
    a. イメージ定義を作成する。
    b. 指定されたホスティング接続にイメージ定義の新しい構成を追加する。
    c. イメージバージョンを作成する。
    d. マスターイメージバージョン仕様を追加する。
    e. 準備済みイメージバージョン仕様を作成する。
2. 他のホスティングユニットでイメージバージョンを使用する場合は、同じホスティング接続内の別のホスティングユニットと準備済みイメージバージョン仕様を共有します。
3. 準備済みイメージバージョン仕様を使用して MCS マシンカタログを作成する:
    a. ブローカーカタログを作成します。
    b. IDプールを作成します。
    c. `New-ProvScheme` コマンドを使用して、準備済みイメージバージョン仕様のUidパラメーターを持つプロビジョニングスキームを作成します。
    d. ブローカーカタログをプロビジョニングスキームにリンクします。
4. MCSマシンカタログにVMを作成します。
5. `Set-ProvScheme` コマンドを使用して、プロビジョニングスキームの準備済みイメージバージョン仕様を変更します。
6. イメージ定義とバージョンを管理します: イメージバージョンとイメージ定義を編集します。
7. MCSマシンカタログを削除します: 削除順序は次のとおりです: マシンカタログ > 共有準備済みイメージバージョン仕様 (イメージ共有の場合) > 準備済みイメージバージョン仕様 > マスターイメージバージョン仕様 > イメージバージョン > 指定されたホスティング接続内のイメージ定義の構成 > イメージ定義。イメージバージョン仕様を削除する前に、準備済みイメージ

バージョン仕様がどのMCSマシンカタログにも関連付けられていないことを確認してください。

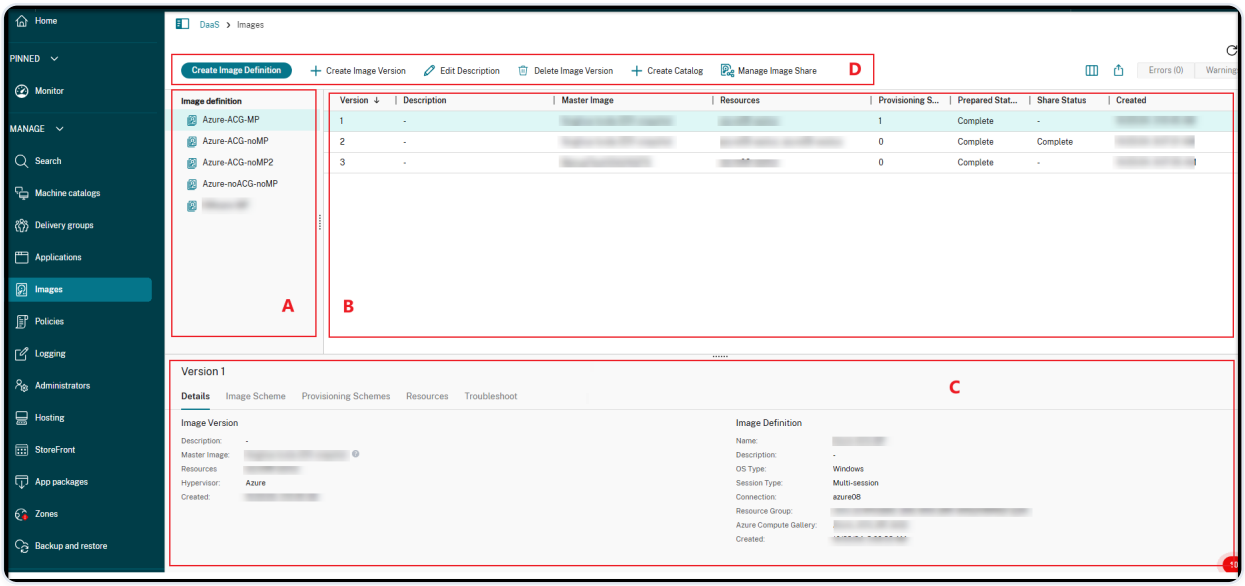
「イメージ」ノードについて

イメージノードを使用して、MCSで準備されたイメージを作成および管理します。そのメインビューは4つの部分に分かれています。

- ホストユニット間で準備済みイメージが共有されていない場合



- ホストユニット間で準備済みイメージが共有されている場合:



ラベル	部分	説明
A	イメージ定義	以前に作成されたイメージ定義を一覧表示します。
B	イメージバージョン	選択したイメージ定義のイメージバージョンを表示します。
C	詳細	• **詳細**タブには、選択したイメージ定義またはバージョンに関する詳細情報（マスターイメージ、リソース、ハイパーバイザー、イメージ定義名、OS タイプ、セッションタイプなど）が表示されます。 • **イメージスキーム**タブには、ハードディスク、マシンサイズ、ライセンスタイプ、ディスク暗号化セット、マシンプロファイルなど、イメージの準備に使用されるテンプレートに関

ラベル	部分	説明	
		する情報が表示されます。 • 「**プロビジョニングスキーム**」タブには、カタログの作成に使用されたプロビジョニングスキーム名が表示されます。 • 「**トラブルシューティング**」タブには、選択したイメージバージョンのエラー状態が表示されます。 • イメージ共有の場合：「**リソース**」タブには、イメージバージョンの共有ステータスが表示されます。	
D	アクションバー	イメージ定義およびバージョンに対して実行できるアクション（**イメージバージョンの作成**、**説明の編集**、**イメージ共有の管理**（準備済みイメージ共有の場合）、**イメージバージョンの削除**、**カタ**	

ラベル	部分	説明
		ログの作成など）を一覧表示します。

次のステップ

準備済みイメージマシンカタログを作成する(/ja-jp/citrix-virtual-apps-desktops/2503/install-configure/create-prepared-image-machine-catalogs.html)

- Azure で準備済みイメージマシンカタログを作成する(/ja-jp/citrix-virtual-apps-desktops/2503/install-configure/create-prepared-image-machine-catalogs-azure.html)
- VMware で準備済みイメージマシンカタログを作成する(/ja-jp/citrix-virtual-apps-desktops/2503/install-configure/create-prepared-image-machine-catalogs-vmware.html)

準備済みイメージのマシンカタログを作成する

準備済みイメージを作成し、その準備済みイメージを使用して、次の方法でMCSマシンカタログを作成します。

- ウェブスタジオ
- PowerShellコマンド

現在、AzureおよびVMware仮想化環境で準備済みイメージマシンカタログを作成できます。

詳細情報

- イメージ管理

次のステップ

- Azureで準備済みイメージのマシンカタログを作成する
- VMwareで準備済みイメージのマシンカタログを作成する
- 準備済みイメージマシンカタログを管理する(/ja-jp/citrix-virtual-apps-desktops/2503/install-configure/manage-prepared-image-machine-catalogs.html)

Azure で準備済みイメージのマシンカタログを作成する

準備済みイメージを作成し、その準備済みイメージを使用して、次の方法でMCSマシンカタログを作成します。

- ウェブスタジオ

- PowerShell コマンド

準備済みイメージを使用して MCS マシンカタログを作成する主な手順は次のとおりです。

1. イメージ定義と初期イメージバージョンを作成します。
2. イメージバージョンを準備済みイメージとして使用してカタログを作成します。

Web Studio を使用する

イメージ定義と初期イメージバージョンを作成する

イメージ定義と初期イメージバージョンを作成するには、次の手順を実行します。

1. Web Studio から、**イメージ**ノードに移動し、**イメージ定義の作成**をクリックします。**はじめに**ページで**次へ**をクリックします。
2. **イメージ定義**ページで、イメージ定義の**OSタイプ**と**セッションタイプ**を指定します。
3. 既存のリソースグループを選択するか、イメージリソースを保持するための新しいリソースグループを作成します。イメージ共有を有効にするには、Azure Compute Gallery で**イメージバージョンを配置**を選択し、新しいギャラリーを作成するか、既存のギャラリーを使用してイメージバージョンを保持するかを選択します。
4. **イメージ**ページで、**リソース**（設定された接続に適用可能なリソースのみが一覧表示されます）と、イメージバージョンを作成するためのテンプレートとして使用するマスターイメージを選択します。**マシンプロファイルを使用**チェックボックスをオンにして、マシンプロファイルを選択できます。

   注:

   イメージを選択する前に、マスターイメージにVDA 2311以降がインストールされており、MCSIOドライバーがVDAにインストールされていることを確認してください。

5. **ストレージとライセンスの種類**ページで、イメージ準備プロセスの一部として使用するストレージとライセンスの種類を選択します。

   注:

   イメージページでマシンプロファイルを選択した場合、マシンプロファイルのライセンスの種類はプロファイル設定に基づいて事前に選択されます。

6. **マシン仕様**ページで、マシンサイズを選択します。**イメージ**ページでマシンプロファイルを選択した場合、マシンプロファイルのマシンサイズがデフォルトで選択されます。
7. **NIC**ページで、準備イメージ用のNICを選択または追加します。各NICについて、関連する仮想ネットワークを選択します。
8. **ディスク設定**ページで、顧客管理の暗号化キー（CMEK）を選択します。マシンプロファイルにCMEKがないが、マスターイメージにある場合、マスターイメージからCMEKが事前に選択されます。
9. **バージョン説明**ページで、作成された初期イメージバージョンの説明を入力します。
10. **概要**ページで、イメージ定義と作成された初期イメージバージョンの詳細を確認します。イメージ定義の名前と説明を入力します。**完了**をクリックします。

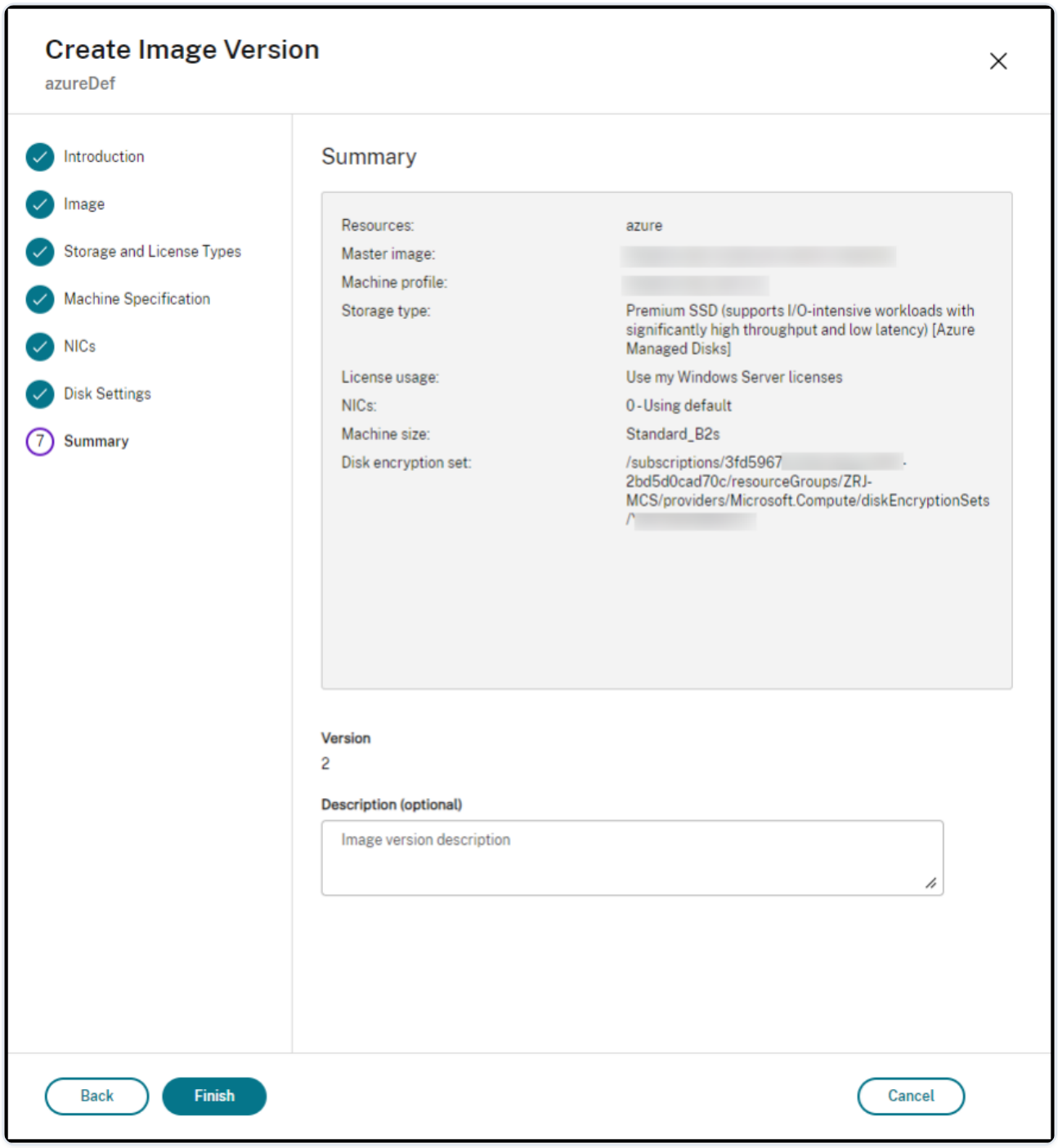
イメージバージョンを作成する

イメージバージョンを使用すると、特定のイメージに対するさまざまなイテレーションや更新を管理できます。この機能により、さまざまな目的のためにイメージの複数のバージョンを維持できます。

初期イメージバージョンからイメージバージョンを作成するには、次の手順を実行します。

> **注:**
>
> すべてのイメージバージョンのホスティングユニットは同じである必要があります。

1. **イメージ**ノードに移動し、イメージバージョンまたはイメージ定義を選択して、**イメージバージョンを作成**をクリックします。
2. 「イメージ定義」ページで、ホスティングユニットを変更し、そのイメージバージョン用のマスターイメージとマシンプロファイルを再選択できます。
3. イメージバージョンの構成を、最初に構成されたイメージバージョンと異なるものにしたい場合は、「**イメージバージョンの作成**」ダイアログの「**ストレージとライセンスの種類**」、「**マシン仕様**」、「**NIC**」、「**ディスク設定**」ページで設定を構成します。
4. イメージバージョンの説明を追加します。「**完了**」をクリックします。



注:

何らかの理由でイメージバージョンの作成に失敗した場合、下部にある「**トラブルシューティング**」タブに「**再試行**」オプションが表示されます。

共有準備済みイメージ

Azure の異なるホストユニット間で準備済みイメージを共有するには、次の手順に従います。

1. イメージバージョンを右クリックし、「**イメージ共有の管理**」を選択します。選択した接続下のすべてのホストユニットが一覧表示されます。イメージバージョンが作成されたリソースは、すべてのアクションに対して無効になっています。
2. イメージを共有するホストユニットを選択し、「**保存**」をクリックします。「**共有ステータス**」列に「進行中」と表示されます。
3. 共有ステータスの詳細については、「**リソース**」タブをクリックしてください。

> **注:**
>
> イメージバージョンの共有のステータスが進行中の場合、**イメージバージョンの削除**または**イメージ共有の管理**のオプションは無効になります。

イメージノードからマシンカタログを作成する

「**イメージ**」ノードの「**カタログの作成**」オプションを使用して、イメージバージョンでカタログを作成します。

あるいは、**マシンカタログ**ノードでカタログを作成する際にバージョンを選択し、カタログ作成ワークフローの準備済みイメージオプションにリンクすることもできます。詳細については、「マシンカタログノードからマシンカタログを作成する」を参照してください。

「**イメージ**」ノードからMCSマシンカタログを作成するには、次の手順を実行します。

1. イメージバージョンを選択し、**カタログの作成**をクリックします。**はじめに**ページで**次へ**をクリックします。
2. **デスクトップエクスペリエンス**ページで、必要なデスクトップエクスペリエンスを選択します。
3. **イメージ**ページから**ディスク設定**ページまで、設定は選択したイメージバージョンに基づいて事前に選択されています。
4. **リソースグループ**ページで、新しいリソースグループを作成するか、既存のリソースグループを使用してこのカタログのリソースを配置するかを選択できます。
5. 次のページで設定を完了します。
6. **概要**ページで、マシンカタログの詳細を確認します。マシンカタログの名前と説明を入力します。**完了**をクリックします。
7. **マシンカタログ**ノードに移動して、作成されたマシンカタログを確認します。

「マシンカタログ」ノードからマシンカタログを作成する

マシンカタログノードからMCSマシンカタログを作成するには、次の手順を実行します。

1. 左側のナビゲーションペインで**マシンカタログ**をクリックします。
2. **マシンカタログの作成**をクリックします。**マシンカタログのセットアップ**ページが表示されます。**はじめに**、**マシンの種類**、**マシン管理**の各ページで**次へ**をクリックします。
3. **マシン管理**ページで、次の設定を選択します。
    a. **電源管理されているマシン（仮想マシンやブレードPCなど）**を選択します。
    b. 「**Citrixプロビジョニングテクノロジー**」を選択します。次に、「**Citrix Machine Creation Services™**」を選択します。
    c. 「**リソース**」フィールドには、異なるゾーンに属するリソースが一覧表示されます。任意のAzureネットワークリソースを選択し、「**次へ**」をクリックします。
4. 「**イメージ**」ページで、マスターイメージタイプの場合は、次の手順に従います。
    a. マスターイメージを選択します。
    b. マスターイメージの下で、イメージを選択します。ブレードには、リソースと同じリージョンに属するすべてのイメージが一覧表示されます。
    c. 「**完了**」をクリックします。
    d. 準備済みイメージタイプの場合は、「**準備済みイメージ**」を選択します。
    e. 「**準備済みイメージ**」の下で、イメージ定義のイメージバージョンを選択します。
    f. イメージバージョン名をクリックします。選択したイメージバージョンの詳細を表示するには、下線が引かれているバージョン番号をクリックします。
    g. 選択したイメージバージョンがマシンプロファイルで構成されている場合は、マシンプロファイルを選択します。選択したイメージバージョンがマシンプロファイルで構成されていない場合、マシンプロファイルを使用することはできません。
5. 次のページで設定を構成します。
6. 「**ディスク設定**」ページで、選択した準備済みイメージがディスク暗号化セットを使用している場合、その暗号化セットを削除することはできませんが、キーを別の暗号化キーに変更することはできます。
7. 「**リソースグループ**」ページで、新しいリソースグループを作成するか、既存のリソースグループを使用してこのカタログのリソースを配置するかを選択できます。
8. 次のページで設定を完了します。

9. 「**概要**」ページで、マシンカタログの詳細を確認します。マシンカタログの名前と説明を入力します。「**完了**」をクリックします。

PowerShellを使用する

準備されたイメージを作成する

準備されたイメージバージョン仕様を作成するための詳細なPowerShellコマンドは次のとおりです。

1. `Test-ProvImageDefinitionNameAvailable command`を使用して、利用可能なイメージ定義名を確認します。例：

   ```
   Test-ProvImageDefinitionNameAvailable -ImageDefinitionName <string[]>
   ```

2. `New-ProvImageDefinition`コマンドを使用してイメージ定義を作成します。例：

   ```
   New-ProvImageDefinition -ImageDefinitionName image1 -OsType Windows
   -VdaSessionSupport MultiSession
   ```

3. `Add-ProvImageDefinitionConnection`コマンドを使用して、指定されたホスティング接続でイメージ定義の新しい構成を作成します。

   `Add-ProvImageDefinitionConnection`の`CustomProperties`には、次のものが含まれます。パラメーターを使用しない場合、デフォルト値が使用されます。

   - `ResourceGroups`：ベースディスクを持つリソースグループ。
   - `UseSharedImageGallery`：ベースディスクの種類のインジケーター。ACG（イメージ共有）には`true`を、スナップショットには`false`を使用します。
   - `ImageGallery`：ベースディスクがACGイメージバージョンの場合のギャラリー名。

   例:

   - スナップショットおよび顧客が提供するリソースグループの場合：

     ```
     $CustomerOwnRsourceGroupProperties = @"

     <CustomProperties xmlns="http:// schemas.citrix.com/2014/xd/
     machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
     instance">
     ```

```
<Property xsi:type="StringProperty" Name="ResourceGroups"
Value="yangj_image" />

</CustomProperties>

"@
```

- ACGおよび顧客が提供するリソースグループとイメージギャラリーの場合：

```
$CustomerOwnAllProperties = @"

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="UseSharedImageGallery"
Value="true" />

<Property xsi:type="StringProperty" Name="ResourceGroups"
Value="rg" />

<Property xsi:type="StringProperty" Name="ImageGallery"
Value="gallery" />

</CustomProperties>

"@
```

- ACGおよび顧客が提供するリソースグループのみの場合：

```
$CustomerOwnResourceGroupProperties = @"

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="UseSharedImageGallery"
Value="true" />

<Property xsi:type="StringProperty" Name="ResourceGroups"
Value="rg" />
```

```
</CustomProperties>

"@
```

- ACGおよびCitrixが管理するリソースグループとイメージギャラリーの場合：

```
$CustomerOwnResourceGroupNothingProperties = @"

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="UseSharedImageGallery"
Value="true" />

</CustomProperties>

"@
```

```
Add-ProvImageDefinitionConnection -ImageDefinitionName image1
-HypervisorConnectionName Azure28 [-CustomProperties $CustomProperties]
```

4. `New-ProvImageVersion` コマンドを使用してイメージバージョンを作成します。例:

```
New-ProvImageVersion -ImageDefinitionName image1 -Description "version
1"
```

5. `Add-ProvImageVersionSpec` コマンドを使用して、マスターイメージバージョン仕様をイメージバージョンに追加します。例:

```
Add-ProvImageVersionSpec -ImageDefinitionName  image1  -
ImageVersionNumber  1 -HostingUnitName azure -MasterImagePath "XDHyp:
\HostingUnits\azure\image.folder\azureresourcegroup.resourcegroup\win20
22-snapshot.snapshot"
```

注:

> ホスティングユニットのイメージバージョンには、マスターイメージバージョン仕様を1つだけ追加できます。

6. `New-ProvImageVersionSpec`コマンドを使用して、マスターイメージバージョン仕様から準備済みイメージバージョン仕様を作成します。例：

```
New-ProvImageVersionSpec

-SourceImageVersionSpecUid  c6e7384c-b2f8-46d6-9519-29a2c57ed3cb

-NetworkMapping @{"0"="XDHyp:
\HostingUnits\azure\virtualprivatecloud.folder\azureresourcegroup.resou
rcegroup\azure-vnet-eastus.virtualprivatecloud\dev.network"}

-ServiceOffering"XDHyp:
\HostingUnits\azure\serviceoffering.folder\Standard_B2ms.serviceofferin
g" -CustomProperties "<CustomProperties xmlns=`"http://
schemas.citrix.com/2014/xd/machinecreation`" xmlns:xsi=`"http://
www.w3.org/2001/XMLSchema-instance`"></CustomProperties>"
-RunAsynchronously
```

7. 同じホスティング接続内の別のホスティングユニットと、準備されたイメージバージョンの仕様を`Add-ProvImageVersionSpecHostingUnit`コマンドを使用して共有することもできます。例:

```
Add-ProvImageVersionSpecHostingUnit -ImageVersionSpecUid xxxxxxx
-HostingUnitName AzureWest
```

> **注:**
>
> 1つのホスティングユニットと準備タイプには、準備済みインスタンスを1つしか持つことができません。

イメージ定義、イメージバージョン、および準備済みイメージバージョン仕様を作成するためのPowershellコマンドの完全なセットの例:

```
New-ProvImageDefinition -ImageDefinitionName image1 -OsType Windows
-VdaSessionSupport MultiSession



$CustomProperties = @"

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

    <Property xsi:type="StringProperty" Name="UseSharedImageGallery"
Value="true" />

    <Property xsi:type="StringProperty" Name="ResourceGroups" Value="rg" /
>

    <Property xsi:type="StringProperty" Name="ImageGallery"
Value="gallery" />

</CustomProperties>

"@



Add-ProvImageDefinitionConnection -ImageDefinitionName image1
-HypervisorConnectionName Azure28 -CustomProperties $CustomProperties



$imageVersion = New-ProvImageVersion -ImageDefinitionName image1
-Description "version 1"



$SourceImageVersionSpec = Add-ProvImageVersionSpec -ImageVersionUid
$imageVersion.ImageVersionUid `

    -HostingUnitUid $hostingunit.HostingUnitUid `

    -MasterImagePath "XDHyp:
\HostingUnits\azure28\image.folder\abc.resourcegroup\def-
snapshot.snapshot"
```

```
New-ProvImageVersionSpec -NetworkMapping @{"0" = "XDHyp:
\HostingUnits\azure28\virtualprivatecloud.folder\East
US.region\virtualprivatecloud.folder\studio-mcs-
infrastructure.resourcegroup\studio-mcs-vnet-
eastus.virtualprivatecloud\mcs-dev.network" } -CustomProperties
"<CustomProperties xmlns=`"http://schemas.citrix.com/2014/xd/
machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`"><Property xsi:type=`"StringProperty`" Name=`"LicenseType`"
Value=`"Windows_Server`" /></CustomProperties>" -ServiceOffering "XDHyp:
\HostingUnits\azure28\serviceoffering.folder\Standard_B2s.serviceoffering"
-SourceImageVersionSpecUid $SourceImageVersionSpec.ImageVersionSpecUid

Add-ProvImageVersionSpecHostingUnit -ImageVersionSpecUid xxxxxxx
-HostingUnitName AzureWest

$PreparedImageVersionSpec = Get-ProvImageVersionSpec -ImageVersionUid
$imageVersion.ImageVersionUid | Where SourceImageVersionSpecUid-eq
$SourceImageVersionSpec.ImageVersionSpecUid
```

注:

- イメージ定義内のすべてのイメージバージョン仕様は、同じホスティングユニットに属している必要があります。
- イメージバージョンには、マスターイメージバージョン仕様を1つと、準備済みイメージバージョン仕様を1つしか持つことができません。
- すべてのイメージバージョン仕様は、マシンプロファイルを持つか、またはどのイメージバージョン仕様もマシンプロファイルを持たないかのいずれかである必要があります。

準備済みイメージバージョン仕様を使用してカタログを作成する

`New-ProvScheme` コマンドを使用して、準備済みイメージバージョン仕様から MCS マシンカタログを作成します。例:

```
New-ProvScheme -ProvisioningSchemeName <string> -ImageVersionSpecUid
<Guid> -HostingUnitUid <Guid> -IdentityPoolUid <Guid> [-VMCpuCount <int>]
[-VMMemoryMB <int>] [-UseWriteBackCache] [-NetworkMapping <Hashtable>] [-
CleanOnBoot] [-Scope <string[]>] [-Metadata <Hashtable>] [-ServiceOffering
<string>] [-SecurityGroup <string[]>] [-TenancyType <string>] [-
MachineProfile <string>] [-CustomProperties <string>] [-
ResetAdministratorPasswords] [-UseFullDiskCloneProvisioning] [-
RunAsynchronously] [-PurgeJobOnSuccess] [-ProvisioningSchemeType
<ProvisioningSchemeType>]
```

または、,

```
New-ProvScheme -ProvisioningSchemeName <string> -ImageVersionSpecUid
<Guid> -HostingUnitName <string> -IdentityPoolName <string> [-VMCpuCount
<int>] [-VMMemoryMB <int>] [-UseWriteBackCache] [-NetworkMapping
<Hashtable>] [-CleanOnBoot] [-Scope <string[]>] [-Metadata <Hashtable>] [-
ServiceOffering <string>] [-SecurityGroup <string[]>] [-TenancyType
<string>] [-MachineProfile <string>] [-CustomProperties <string>] [-
ResetAdministratorPasswords] [-UseFullDiskCloneProvisioning] [-
RunAsynchronously] [-PurgeJobOnSuccess] [-ProvisioningSchemeType
<ProvisioningSchemeType>]
```

ACGイメージバージョン仕様を使用したい場合は、`UseSharedImageGallery`を`true`として設定します。例えば、,

```
$provSchemeCustomProperties= @"

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

    <Property xsi:type="StringProperty" Name="UseSharedImageGallery"
Value="true" />

    <Property xsi:type="StringProperty" Name="StorageAccountType"
Value="StandardSSD_LRS" />

</CustomProperties>

"@

New-ProvScheme -ProvisioningSchemeName assignimage -ImageVersionSpecUid
```

```
$PreparedImageVersionSpec.ImageVersionSpecUid `

    -HostingUnitUid $hostingunit.HostingUnitUid `

    -IdentityPoolUid $IdentityPool.IdentityPoolUid `

    -CleanOnBoot -Scope @() -SecurityGroup @() `

    -ServiceOffering "XDHyp:
\HostingUnits\azure28\serviceoffering.folder\Standard_B2s.serviceoffering"
`

    -NetworkMapping @{"0"="XDHyp:
\HostingUnits\azure28\virtualprivatecloud.folder\East
US.region\virtualprivatecloud.folder\studio-mcs-
infrastructure.resourcegroup\studio-mcs-vnet-
eastus.virtualprivatecloud\mcs-dev.network"} `

    -CustomProperties $provSchemeCustomProperties
```

カタログを作成するためのPowershellコマンドの完全なセットの例：

```
$Catalog = New-BrokerCatalog  -AllocationType "Random"  -IsRemotePC $False
 -MinimumFunctionalLevel "L7_20" -Name "azurecatalog" -PersistUserChanges
"Discard" -ProvisioningType "MCS" -Scope @() -SessionSupport
"MultiSession"



$IdentityPool = New-AcctIdentityPool  -AllowUnicode  -Domain "azure.local"
-IdentityPoolName "azurecatalog" -IdentityType "ActiveDirectory"  -
NamingScheme "azure##" -NamingSchemeType "Numeric" -Scope @()



$PreparedImageVersionSpec = Get-ProvImageVersionSpec -ImageDefinitionName
image1 -ImageVersionNumber 1 -Filter "PreparationType -eq 'Mcs'"



$Task = New-ProvScheme -ProvisioningSchemeName azurecatalog
-ImageVersionSpecUid $PreparedImageVersionSpec.ImageVersionSpecUid
-HostingUnitName azure -IdentityPoolName azurecatalog -CleanOnBoot -Scope
```

```
@() -SecurityGroup @() -ServiceOffering "XDHyp:
\HostingUnits\azure\serviceoffering.folder\Standard_B2s.serviceoffering"
-NetworkMapping @{"0"="XDHyp:
\HostingUnits\azure\virtualprivatecloud.folder\azureresourcegroup.resource
group\azure-vnet-eastus.virtualprivatecloud\dev.network"}
-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com/
2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`">    <Property xsi:type="StringProperty"
Name="UseSharedImageGallery" Value="true" /><Property
xsi:type=`"StringProperty`" Name=`"StorageAccountType`"
Value=`"StandardSSD_LRS`" /></CustomProperties>" -RunAsynchronously



Get-ProvTask -TaskId $Task.TaskId

$ProvScheme = Get-ProvScheme -ProvisioningSchemeName azurecatalog



Set-BrokerCatalog -Name $Catalog.Name -ProvisioningSchemeId
$ProvScheme.ProvisioningSchemeUid
```

詳細情報

- イメージ管理

次のステップ

- 準備済みイメージマシンカタログを管理する(/ja-jp/citrix-virtual-apps-desktops/2503/install-configure/manage-prepared-image-machine-catalogs.html)

VMware で準備済みイメージのマシンカタログを作成する

準備済みイメージを作成し、その準備済みイメージを使用して、次の方法で MCS マシンカタログを作成します。

- ウェブスタジオ
- PowerShell コマンド

準備済みイメージを使用して MCS マシンカタログを作成する主な手順は次のとおりです。

1. イメージ定義と初期イメージバージョンを作成します。

2. イメージバージョンを準備済みイメージとして使用してカタログを作成します。

Web Studio を使用する

イメージ定義と初期イメージバージョンを作成する

イメージ定義と初期イメージバージョンを作成するには、次の手順を実行します。

1. Studioから、**イメージ**ノードに移動し、**イメージ定義の作成**をクリックします。**はじめに**ページで**次へ**をクリックします。
2. **イメージ定義**ページで、イメージ定義の**OSタイプ**と**セッションタイプ**を指定します。
3. **［イメージ］ページで、［リソース］**（設定された接続に適用可能なリソースのみが一覧表示されます）と、イメージバージョンを作成するためのテンプレートとして使用するマスターイメージを選択します。**［マシンプロファイルを使用する］**チェックボックスをオンにして、マシンプロファイルを選択できます。

   > **注:**
   >
   > イメージを選択する前に、マスターイメージにVDA 2311以降がインストールされており、MCSIOドライバーがVDAにインストールされていることを確認してください。

4. 「**マシン仕様**」ページで、マシンサイズを選択します。マシンプロファイルを選択した場合、マシンプロファイルから派生した仮想CPUカウントが表示され、変更できません。マシンプロファイルを選択しない場合、マスターイメージから派生したメモリサイズのみが表示されます。
5. 「**NIC**」ページで、準備イメージ用のNICを選択または追加します。各NICについて、関連する仮想ネットワークを選択します。マシンプロファイルを選択しない場合、マスターイメージに関連付けられたNICがデフォルトで選択されます。マシンプロファイルを選択した場合、NICはマシンプロファイルから派生し、その数は変更できません。
6. 「**バージョン説明**」ページで、作成された初期イメージバージョンの説明を入力します。
7. 「**概要**」ページで、イメージ定義と作成された初期イメージバージョンの詳細を確認します。イメージ定義の名前と説明を入力します。「**完了**」をクリックします。

イメージバージョンを作成する

イメージバージョンを使用すると、特定のイメージに対するさまざまなイテレーションや更新を管理できます。この機能により、さまざまな目的のためにイメージの複数のバージョンを維持できます。

初期イメージバージョンからイメージバージョンを作成するには、次の手順を実行します。

1. 「**イメージ**」ノードに移動し、イメージバージョンまたはイメージ定義を選択して、「**イメージバージョンの作成**」をクリックします。
2. 「**イメージ**」ページで、同じホスティング接続内のホスティングユニットを変更し、そのイメージバージョンのマスターイメージとマシンプロファイルを再選択できます。
3. イメージバージョンの構成を、最初に構成されたイメージバージョンと異なるものにしたい場合は、「**イメージバージョンの作成**」ダイアログの「**マシン仕様**」ページと「**NIC**」ページで設定を構成します。
4. イメージバージョンの説明を追加します。「**完了**」をクリックします。

> **注:**
>
> 何らかの理由でイメージバージョンの作成に失敗した場合、下部にある**トラブルシューティング**タブに**再試行**オプションが表示されます。

準備済みイメージを共有する

前提条件

準備済みイメージの共有では、コールドマイグレーションを使用してvCenter Serverインスタンス間でイメージが複製されます。異なるホスティング接続に属するホスティングユニットには、次の前提条件が適用されます。

- vCenter Server間のコールドマイグレーション：コールドマイグレーションには、両方の環境でクロスvCenterマイグレーションのサポートが必要です。
  - 両方のvCenter ServerはvSphere 7.0以降を実行している必要があります（vSphere 8.0以降を推奨）。
  - 拡張リンクモードは不要です。

  ポート要件：マイグレーションのために次のポートが開いていることを確認してください。

送信元	宛先	ポート	プロトコル	目的
送信元vCenter Server	ターゲットvCenter Server	443	TCP	vCenter間のAPI通信

送信元	宛先	ポート	プロトコル	目的
ソースESXiホスト	ターゲットESXiホスト	902	TCP	NFC (Network File Copy) データ転送
ソースESXiホスト	ターゲットESXiホスト	8000	TCP	vMotionトラフィック

注：

ポートは双方向に開いている必要があります。移行では主に、データにNFC (ポート902) を、管理にポート443を使用します。パスによってはポート8000が使用される場合があります。ソースvCenterは、クローン操作中にターゲットのSSL証明書のサムプリントを検証する必要があります。

VMkernelアダプターの構成：

ESXIホスト	必要なサービス
ソースESXiホスト	プロビジョニングまたは管理
ターゲットESXiホスト	ソースと同じサービス (プロビジョニングまたは管理)

両側でVMkernelアダプターに同じトラフィックサービス（プロビジョニングまたは管理）を有効にする必要があります。不一致は移行の失敗を引き起こします。

vSphere Clientで、**ホスト > 構成 > ネットワーク > VMkernel アダプター**の下を確認します。

既知の制限事項：カスタムストレージポリシーは、vCenter間レプリケーション中に保持されません。ターゲットデータストアのデフォルトストレージポリシーが適用されます。

- vTPM対応マシンプロファイル：キープロバイダーの互換性。vTPMを持つプロファイルの場合、両方のvCenter Serverが互換性のあるキープロバイダーにアクセスできる必要があります。

要件	詳細
同じキープロバイダーへのアクセス	宛先vCenterは、ソースと同じキープロバイダーにアクセスできるか、Native Key Providerをブリッジとして使用できる必要があります。
キーマテリアル	外部KMSの場合：両方のvCenterは同じKMSクラスター（またはキーマテリアルを共有するKMSクラスター）に登録されている必要があります。
ネイティブキープロバイダー	両方のvCenter Serverでネイティブキープロバイダーを構成します。各vCenterのネイティブキープロバイダーは独立していますが、vSphereはこの組み合わせをvCenter間操作で受け入れます。ネイティブキープロバイダーは、ソースと宛先が外部KMSを共有していない場合でも、ブリッジとして機能できます。ネイティブキープロバイダーは、使用する前に両方のvCenterでバックアップする必要があります。

注:

ネイティブキープロバイダーは最も簡単なオプションです。両方のサーバーで構成し、バックアップしてください。外部KMSを使用する場合は、両方のvCenterが同じクラスターまたはキーマテリアルを共有していることを確認してください。vTPM対応カタログのイメージ共有を有効にする前に、**vSphere ClientのvCenter > 構成 > セキュリティ > キープロバイダー**でキープロバイダーの構成を確認してください。

準備済みイメージを異なるホストユニット間で共有する

準備済みイメージを異なるホストユニット間で共有するには、次の手順に従います。

1. イメージバージョンを右クリックし、**イメージ共有の管理**を選択します。選択した接続下のすべてのホストユニットが一覧表示されます。イメージバージョンが作成されたリソースは、いかなる操作も無効になっています。
2. イメージを共有するホストユニットを選択し、**保存**をクリックします。 **共有ステータス**列に**進行中**と表示されます。

3. 下部にある**リソース**タブをクリックして、共有ステータスの詳細を確認します。

> **注:**
>
> イメージバージョンの共有のステータスが進行中の場合、**イメージバージョンの削除**または**イメージ共有の管理**のオプションは無効になります。

「イメージ」ノードからマシンカタログを作成する

「**イメージ**」ノードの「**カタログの作成**」オプションを使用して、イメージバージョンでカタログを作成します。

または、**マシンカタログ**ノードでカタログを作成する際にバージョンを選択し、カタログ作成ワークフローで準備済みイメージオプションにリンクできます。「マシンカタログノードからマシンカタログを作成する」を参照してください。(#create-a-machine-catalog-from-the-machine-catalogs-node)

「**イメージ**」ノードからMCSマシンカタログを作成するには、次の手順を実行します。

1. イメージバージョンを選択し、**カタログの作成**をクリックします。**はじめに**ページで**次へ**をクリックします。
2. 「**デスクトップエクスペリエンス**」ページで、必要なデスクトップエクスペリエンスを選択します。
3. 「**イメージ**」ページから「**仮想マシン**」ページまで、設定は選択したイメージバージョンに基づいて事前に選択されています。
4. 以下のページで設定を完了します。
5. 「**概要**」ページで、マシンカタログの詳細を確認します。マシンカタログの名前と説明を入力します。「**完了**」をクリックします。
6. 「**マシンカタログ**」ノードに移動して、作成されたマシンカタログを表示します。

「マシンカタログ」ノードからマシンカタログを作成する

マシンカタログノードからMCSマシンカタログを作成するには、次の手順を実行します。

1. 左側のナビゲーションペインで「**マシンカタログ**」をクリックします。
2. 「**マシンカタログの作成**」をクリックします。「**マシンカタログのセットアップ**」ページが表示されます。「**はじめに**」、「**マシンの種類**」、「**マシン管理**」の各ページで「**次へ**」をクリックします。

3. 「**イメージ**」ページで:
    a. 「**準備済みイメージ**」を選択します。
    b. 「**準備済みイメージ**」の下で、イメージ定義のイメージバージョンを選択します。
    c. イメージバージョン名をクリックします。選択したイメージバージョンの詳細を表示するには、下線が引かれているバージョン番号をクリックします。
    d. 選択したイメージバージョンがマシンプロファイルで構成されている場合は、マシンプロファイルを選択します。選択したイメージバージョンがマシンプロファイルで構成されていない場合、マシンプロファイルを使用することはできません。
4. 次のページで設定を構成します。
5. **概要**ページで、マシンカタログの詳細を確認します。マシンカタログの名前と説明を入力します。**完了**をクリックします。

PowerShell を使用する

準備済みイメージを作成する

準備済みイメージバージョン仕様を作成するための詳細な PowerShell コマンドは次のとおりです。

1. `Test-ProvImageDefinitionNameAvailable command` を使用して、利用可能なイメージ定義名を確認します。例:

```
Test-ProvImageDefinitionNameAvailable -ImageDefinitionName <string[]>
```

2. `New-ProvImageDefinition` コマンドを使用してイメージ定義を作成します。例:

```
New-ProvImageDefinition -ImageDefinitionName image2 -OsType Windows
-VdaSessionSupport SingleSession
```

3. `Add-ProvImageDefinitionConnection`コマンドを使用して、指定されたホスティング接続でイメージ定義の新しい構成を作成します。例：

```
Add-ProvImageDefinitionConnection -ImageDefinitionName image2
-HypervisorConnectionName VMware
```

4. `New-ProvImageVersion` コマンドを使用してイメージバージョンを作成します。例:

```
New-ProvImageVersion -ImageDefinitionName
$ImageDefintion.ImageDefinitionName -Description "version 1"
```

5. `Add-ProvImageVersionSpec` コマンドを使用して、マスターイメージバージョン仕様をイメージバージョンに追加します。例:

```
$MasterImagePath = "XDHyp:\HostingUnits\vmware\win10-master.vm\win10-
master-snap.snapshot"

$SourceImageVersionSpec = Add-ProvImageVersionSpec -ImageDefinitionName
$ImageVersion.ImageDefinitionName -ImageVersionNumber
$ImageVersion.ImageVersionNumber -HostingUnitName vmware
-MasterImagePath $MasterImagePath
```

注:

ホスティングユニットのイメージバージョンには、マスターイメージバージョン仕様を1つだけ追加できます。

6. `New-ProvImageVersionSpec`コマンドを使用して、マスターイメージバージョン仕様から準備済みイメージバージョン仕様を作成します。例：

```
New-ProvImageVersionSpec -SourceImageVersionSpecUid
 $SourceImageVersionSpec.ImageVersionSpecUid -NetworkMapping
@{"0"="XDHyp:\HostingUnits\vmware\\DSwitch-VM Network.network"}
-VMCpuCount 2 -VMMemoryMB 4096 -RunAsynchronously
```

7. 同じホスティング接続内の別のホスティングユニットと、準備されたイメージバージョンの仕様を`Add-ProvImageVersionSpecHostingUnit`コマンドを使用して共有することもできます。例:

```
Add-ProvImageVersionSpecHostingUnit -ImageVersionSpecUid xxxxxxx
-HostingUnitName VMwareabc
```

イメージ定義、イメージバージョン、および準備済みイメージバージョン仕様を作成するための PowerShell コマンドの完全なセットの例:

```
New-ProvImageDefinition -ImageDefinitionName image2 -OsType Windows
-VdaSessionSupport Single



Add-ProvImageDefinitionConnection -ImageDefinitionName image2
-HypervisorConnectionName VMware



$imageVersion = New-ProvImageVersion -ImageDefinitionName image2



$SourceImageVersionSpec = Add-ProvImageVersionSpec -ImageVersionUid
$imageVersion.ImageVersionUid `

    -HostingUnitUid $hostingunit.HostingUnitUid `

    -MasterImagePath "XDHyp:\HostingUnits\vmware\shuaiz-win10-
master.vm\shuaiz-win10-master-snap.snapshot"



New-ProvImageVersionSpec -SourceImageVersionSpecUid
$SourceImageVersionSpec.ImageVersionSpecUid `

    -NetworkMapping @{"0"="XDHyp:\HostingUnits\vmware\\DSwitch-
VMNetwork.network"} `

    -VMCpuCount 2 -VMMemoryMB 4096







Add-ProvImageVersionSpecHostingUnit -ImageVersionSpecUid xxxxxxx
-HostingUnitName VMwareabc

 $PreparedImageVersionSpec = Get-ProvImageVersionSpec -ImageVersionUid
$imageVersion.ImageVersionUid | Where SourceImageVersionSpecUid-eq
$SourceImageVersionSpec.ImageVersionSpecUid
```

注:

- イメージ定義内のすべてのイメージバージョン仕様は、同じホスティングユニットに属している必要があります。
- イメージバージョンには、マスターイメージバージョン仕様を1つと、準備済みイメージバージョン仕様を1つのみ持つことができます。
- すべてのイメージバージョン仕様はマシンプロファイルを持つか、またはどのイメージバージョン仕様もマシンプロファイルを持たないかのいずれかである必要があります。

準備済みイメージバージョン仕様を使用してカタログを作成する

`New-ProvScheme` コマンドを使用して、準備済みイメージバージョン仕様から MCS マシンカタログを作成します。例:

```
New-ProvScheme -ProvisioningSchemeName <string> -ImageVersionSpecUid
<Guid> -HostingUnitUid <Guid> -IdentityPoolUid <Guid> [-VMCpuCount <int>]
[-VMMemoryMB <int>] [-UseWriteBackCache] [-NetworkMapping <Hashtable>] [-
CleanOnBoot] [-Scope <string[]>] [-Metadata <Hashtable>] [-ServiceOffering
<string>] [-SecurityGroup <string[]>] [-TenancyType <string>] [-
MachineProfile <string>] [-CustomProperties <string>] [-
ResetAdministratorPasswords] [-UseFullDiskCloneProvisioning] [-
RunAsynchronously] [-PurgeJobOnSuccess] [-ProvisioningSchemeType
<ProvisioningSchemeType>]
```

または、,

```
New-ProvScheme -ProvisioningSchemeName <string> -ImageVersionSpecUid
<Guid> -HostingUnitName <string> -IdentityPoolName <string> [-VMCpuCount
<int>] [-VMMemoryMB <int>] [-UseWriteBackCache] [-NetworkMapping
<Hashtable>] [-CleanOnBoot] [-Scope <string[]>] [-Metadata <Hashtable>] [-
ServiceOffering <string>] [-SecurityGroup <string[]>] [-TenancyType
<string>] [-MachineProfile <string>] [-CustomProperties <string>] [-
ResetAdministratorPasswords] [-UseFullDiskCloneProvisioning] [-
RunAsynchronously] [-PurgeJobOnSuccess] [-ProvisioningSchemeType
<ProvisioningSchemeType>]
```

VMwareで準備されたイメージバージョンの仕様を使用してカタログを作成する例:

```
New-ProvScheme -ProvisioningSchemeName assignimage -ImageVersionSpecUid
$PreparedImageVersionSpec.ImageVersionSpecUid `

    -HostingUnitName $hostingunit.c-IdentityPoolName
$IdentityPool.IdentityPoolName `

    -CleanOnBoot -Scope @() -SecurityGroup @() -VMCpuCount 2 -VMMemoryMB
8192 `

    -NetworkMapping @{"0"="XDHyp:\HostingUnits\vmware\\DSwitch-VM
Network.network"}
```

カタログを作成するためのPowershellコマンドの完全なセットの例：

```
$Catalog = New-BrokerCatalog  -AllocationType "Random"  -IsRemotePC $False
 -MinimumFunctionalLevel "L7_20" -Name "vmwarecatalog" -PersistUserChanges
"Discard" -ProvisioningType "MCS" -Scope @() -SessionSupport
"MultiSession"

$IdentityPool = New-AcctIdentityPool  -AllowUnicode  -Domain
"vmware.local" -IdentityPoolName "vmwarecatalog" -IdentityType
"ActiveDirectory"  -NamingScheme "vmware##" -NamingSchemeType "Numeric"
-Scope @()

$PreparedImageVersionSpec = Get-ProvImageVersionSpec -ImageDefinitionName
image2 -ImageVersionNumber 1 -Filter "PreparationType -eq 'Mcs'"

$Task = New-ProvScheme -ProvisioningSchemeName vmwarecatalog
-ImageVersionSpecUid $PreparedImageVersionSpec.ImageVersionSpecUid
-HostingUnitName vmware -IdentityPoolName vmwarecatalog -CleanOnBoot
-Scope @() -SecurityGroup @() -NetworkMapping @{"0"="XDHyp:
\HostingUnits\vmware\\DSwitch-VM Network.network"} -VMCpuCount 2
-VMMemoryMB 4096 -RunAsynchronously

Get-ProvTask -TaskId $Task.TaskId

$ProvScheme = Get-ProvScheme -ProvisioningSchemeName vmwarecatalog

Set-BrokerCatalog -Name $Catalog.Name -ProvisioningSchemeId
$ProvScheme.ProvisioningSchemeUid
```

詳細情報

- イメージ管理

次のステップ

- 準備済みイメージマシンカタログを管理する

準備済みイメージのマシンカタログを管理する

既存のMCSマシンカタログを別の準備済みイメージで更新し、イメージ定義とバージョンを管理するには、以下を使用します。

- ウェブスタジオ
- PowerShell

Web Studioを使用する

マシンカタログを別の準備済みイメージで更新する

既存のMCSマシンカタログを別の準備済みイメージで更新するには、次の手順を実行します。

1. 左側のナビゲーションペインで をクリックし、更新するマシンカタログを選択します。右クリックして を選択します。
2. **イメージ**ページで、準備済みイメージを選択します。

> **注:**
>
> Azureに適用可能：ACGが有効になっていないイメージを選択し、後で チェックボックスをオンにして、イメージをギャラリーに配置することもできます。

3. **ロールアウト戦略**ページで、選択した準備済みイメージでこのカタログを更新するタイミングを選択します。
4. ページで詳細を確認します。 をクリックします。

カタログに加えられたイメージ変更の履歴を確認できます。履歴を確認するには、次の手順を実行します。

1. マシンカタログを選択します。

2. 「**準備済みイメージ**」フィールドの「**テンプレートプロパティ**」タブで、「**イメージ履歴の表示**」をクリックします。

イメージ定義とバージョンを管理する

作成されたさまざまなイメージバージョンと定義の使用を管理するために、イメージ定義とバージョンを編集および削除できます。

イメージ定義を編集する

イメージ定義の名前と説明を編集できます。

イメージ定義を編集するには、次の手順を実行します。

1. **イメージ**ノードに移動し、イメージ定義を選択して、**イメージ定義の編集**を選択します。

イメージバージョンを編集する

そのイメージバージョンの目的を指定するために、イメージバージョンの説明を編集できます。

イメージバージョンを編集するには、次の手順を実行します。

1. **イメージ**ノードに移動し、イメージバージョンを選択して、**説明の編集**を選択します。

イメージバージョンを削除する

イメージバージョンを削除するには、次の手順を実行します。

1. **イメージ**ノードに移動し、イメージバージョンを選択して、**イメージバージョンの削除**を選択します。

> 「**注：**」:

> マシンカタログで使用されているイメージバージョンは削除できません。

イメージ定義を削除する

イメージ定義を削除するには、次の手順を実行します。

1. **イメージ**ノードに移動し、イメージ定義を選択して、**イメージ定義の削除**を選択します。

> **注：**

> イメージバージョンが含まれているイメージ定義は削除できません。

PowerShell を使用する

準備済みイメージバージョン仕様を使用してカタログを更新する

`Set-ProvSchemeImage` コマンドを使用してカタログを更新できます。例:

```
Set-ProvSchemeImage -ProvisioningSchemeUid <Guid> -ImageVersionSpecUid
<Guid> [-DoNotStoreOldImage] [-RunAsynchronously] [-PurgeJobOnSuccess]
```

または、,

```
Set-ProvSchemeImage -ProvisioningSchemeName <string> -ImageVersionSpecUid
<Guid> [-DoNotStoreOldImage] [-RunAsynchronously] [-PurgeJobOnSuccess]
```

カタログを更新するためのPowershellコマンドの完全なセットの例：

```
$PreparedImageVersionSpec = Get-ProvImageVersionSpec -ImageDefinitionName
image1 -ImageVersionNumber 2 -Filter "PreparationType -eq 'Mcs'"



Set-ProvSchemeImage -ProvisioningSchemeName azurecatalog
-ImageVersionSpecUid $PreparedImageVersionSpec.ImageVersionSpecUid
-RunAsynchronously
```

イメージ定義、イメージバージョン、および準備済みイメージバージョン仕様を削除する

イメージ定義、イメージバージョン、および準備済みイメージバージョン仕様を削除する前に、以下を考慮してください。

- イメージバージョンが含まれているイメージ定義は削除できません。
- イメージバージョン仕様が含まれているイメージバージョンは削除できません。
- マスターイメージバージョン仕様は、他の準備済みイメージバージョン仕様で使用されている場合、削除できません。
- 準備済みイメージバージョン仕様は、MCSマシンカタログで使用されている場合、削除できません。
- ホスティングユニットは、他の準備済みイメージバージョン仕様で使用されている場合、削除できません。

詳細な手順は次のとおりです。

1. マシンカタログを削除します。例:

```
Remove-ProvScheme -ProvisioningScheneName decouplingCatalog
```

2. 共有準備済みイメージバージョン仕様を削除します。例:

```
Remove-ProvImageVersionSpecHostingUnit -ImageVersionSpecUid <uid>
-HostingUnitName AzureWest
```

3. 準備済みイメージバージョン仕様を削除します。例:

```
$PreparedImageVersionSpec = Get-ProvImageVersionSpec
-ImageDefinitionName image1 -ImageVersionNumber 1 -Filter
"PreparationType -eq 'Mcs'"



Remove-ProvImageVersionSpec -ImageVersionSpecUid
$PreparedImageVersionSpec.ImageVersionSpecUid -RunAsynchronously
```

4. マスターイメージバージョン仕様を削除します。例:

```
$MasterImageVersionSpec = Get-ProvImageVersionSpec -ImageDefinitionName
image1 -ImageVersionNumber 1 -Filter "PreparationType -eq 'None'"



Remove-ProvImageVersionSpec -ImageVersionSpecUid
$PreparedImageVersionSpec.ImageVersionSpecUid -RunAsynchronousl
```

> **注:**
>
> マスターイメージバージョン仕様は、関連付けられた準備済みイメージバージョン仕様がない場合にのみ削除できます。

5. イメージバージョンを削除します。例:

```
Remove-ProvImageVersion -ImageDefinitionName image1 -ImageVersionNumber
1
```

6. 指定されたホスティング接続のイメージ定義の構成を削除します。例:

```
Remove-ProvImageDefinitionConnection -ImageDefinitionName xx
-HypervisorConnectionName xxx
```

7. イメージ定義を削除します。例:

```
Remove-ProvImageDefinition -ImageDefinitionName image1
```

準備済みイメージがホストユニット間で共有されていない場合のPowerShellコマンドの完全なセットの例:

```
Remove-ProvScheme -ProvisioningSchemeName decouplingCatalog



$PreparedImageVersionSpec = Get-ProvImageVersionSpec -ImageDefinitionName
image1 -ImageVersionNumber 1 -Filter "PreparationType -eq 'Mcs'"



Remove-ProvImageVersionSpec -ImageVersionSpecUid
$PreparedImageVersionSpec.ImageVersionSpecUid -RunAsynchronously



$MasterImageVersionSpec = Get-ProvImageVersionSpec -ImageDefinitionName
image1 -ImageVersionNumber 1 -Filter "PreparationType -eq 'None'"



Remove-ProvImageVersionSpec -ImageVersionSpecUid
$MasterImageVersionSpec.ImageVersionSpecUid -RunAsynchronously



Remove-ProvImageVersion -ImageDefinitionName image1 -ImageVersionNumber 1
```

```
Remove-ProvImageDefinition -ImageDefinitionName image1
```

準備済みイメージがホストユニット間で共有されている場合のPowerShellコマンドの完全なセットの例:

```
Remove-ProvScheme -ProvisioningSchemeName decouplingCatalog



Remove-ProvImageVersionSpecHostingUnit -ImageVersionSpecUid <uid>

-HostingUnitName AzureWest



$PreparedImageVersionSpec = Get-ProvImageVersionSpec -ImageDefinitionName
image1 -ImageVersionNumber 1 -Filter "PreparationType -eq 'Mcs'"



Remove-ProvImageVersionSpec -ImageVersionSpecUid
$PreparedImageVersionSpec.ImageVersionSpecUid -RunAsynchronously



$MasterImageVersionSpec = Get-ProvImageVersionSpec -ImageDefinitionName
image1 -ImageVersionNumber 1 -Filter "PreparationType -eq 'None'"



Remove-ProvImageVersionSpec -ImageVersionSpecUid
$MasterImageVersionSpec.ImageVersionSpecUid -RunAsynchronously



Remove-ProvImageVersion -ImageDefinitionName image1 -ImageVersionNumber 1



Remove-ProvImageDefinitionConnection -ImageDefinitionName xx
-HypervisorConnectionName xxx
```

```
Remove-ProvImageDefinition -ImageDefinitionName image1
```

イメージ定義とイメージバージョンの管理

イメージ定義の名前変更と編集、およびイメージバージョンの編集が可能です。

- `Rename-ProvImageDefinition`コマンドを使用してイメージ定義の名前を変更します。例:

  ```
  Rename-ProvImageDefinition -ImageDefinitionUid <Guid>
  -NewImageDefinitionName <string>
  ```

  または、,

  ```
  Rename-ProvImageDefinition -ImageDefinitionName <string>
  -NewImageDefinitionName <string>
  ```

- `Set-ProvImageDefinition`コマンドを使用してイメージ定義を編集します。例:

  ```
  Set-ProvImageDefinition -ImageDefinitionUid <Guid> [-Description
  <string>]
  ```

  または、,

  ```
  Set-ProvImageDefinition -ImageDefinitionName <string> [-Description
  <string>]
  ```

- `Set-ProvImageVersion`コマンドを使用してイメージバージョンを編集します。例:

  ```
  Set-ProvImageVersion -ImageVersionUid <Guid> [-Description <string>]
  ```

  または、,

  ```
  Set-ProvImageVersion -ImageDefinitionName <string> -ImageVersionNumber
  <int> [-Description <string>]
  ```

イメージ定義、イメージバージョン、準備されたイメージバージョンの仕様、およびプロビジョニングスキームの詳細を取得する

- `Get-ProvImageDefinition`コマンドを使用してイメージ定義の詳細を取得します。例:

```
Get-ProvImageDefinition [-ImageDefinitionName <string>] [-
ImageDefinitionUid <Guid>] [-ReturnTotalRecordCount] [-MaxRecordCount
<int>] [-Skip <int>] [-SortBy <string>] [-Filter <string>]
```

- `Get-ProvImageVersion`コマンドを使用してイメージバージョンの詳細を取得します。例:
  - イメージ定義内のイメージバージョンを一覧表示するには、,

    ```
    Get-ProvImageVersion -ImageDefinitionUid <Guid>
    ```

    または、,

    ```
    Get-ProvImageVersion -ImageDefinitionName <string>
    ```

  - イメージバージョンの詳細を取得するには、,

    ```
    Get-ProvImageVersion -ImageVersionUid <Guid>
    ```

    または、,

    ```
    Get-ProvImageVersion -ImageDefinitionName <string>
    -ImageVersionNumber <int>
    ```

- `Get-ProvImageVersionSpec`コマンドを使用して、準備済みイメージバージョン仕様を取得します。例:
  - イメージバージョン内のすべての準備済みイメージバージョン仕様を一覧表示するには、,

    ```
    Get-ProvImageVersionSpec -ImageVersionUid <Guid>
    ```

  - 準備済みイメージバージョン仕様内のマスターイメージバージョン仕様を一覧表示するには、,

```
Get-ProvImageVersionSpec -ImageVersionUid <Guid> -Filter
'PreparationType -eq "None"'
```

  - マスターイメージに関連付けられているイメージバージョン内の準備済みイメージバージョン仕様を一覧表示するには、,

```
Get-ProvImageVersionSpec -ImageVersionUid <Guid> -Filter
'PreparationType -eq "MCS" -and SourceImageVersionSpecUid -eq
"xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"'
```

  - イメージバージョン内の成功した準備済みイメージバージョン仕様を取得するには、,

```
Get-ProvImageVersionSpec -ImageVersionUid <Guid> -Filter
'PreparationType -eq "MCS" -and SourceImageVersionSpecUid -eq
"xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" -and ImageVersionSpecStatus
-eq "Complete"'
```

  - 準備済みイメージバージョン仕様の詳細を取得するには、,

```
Get-ProvImageVersionSpec -ImageVersionSpecUid <Guid>
```

- `Get-ProvScheme`コマンドを使用して、プロビジョニングスキームの詳細を取得します。例:

```
Get-ProvScheme [[-ProvisioningSchemeName] <String>] [-
ProvisioningSchemeUid <Guid>] [-ScopeId <Guid>] [-ScopeName <String>]
[-ReturnTotalRecordCount] [-MaxRecordCount <Int32>] [-Skip <Int32>] [-
SortBy <String>] [-Filter <String>] [-FilterScope <Guid>]
```

- `Get-ProvSchemeImageVersionSpecHistory`コマンドを使用して、プロビジョニングスキームの準備済みイメージバージョン仕様の履歴を取得します。例:

```
Get-ProvSchemeImageVersionSpecHistory [-ProvisioningSchemeName
<String>] [-ProvisioningSchemeUid <Guid>] [-ImageVersionSpecUid <Guid>]
[-ImageVersionSpecHistoryUid <Guid>] [-ReturnTotalRecordCount] [-
MaxRecordCount <Int32>] [-Skip <Int32>] [-SortBy <String>] [-Filter
<String>] [-FilterScope <Guid>]
```

詳細情報

- イメージ管理

マシンカタログを作成する

> **重要：**

> Citrix Virtual Apps and Desktops™ 7 2006以降、現在の展開で以下のいずれかのテクノロジーを使用している場合、それらのテクノロジーを使用するサポート終了（EOL）項目を削除した後にのみ、現在のリリースにアップグレードできます。

> - パーソナルvDisk (PvDs)
> - AppDisks™
> - パブリッククラウドホストの種類：Citrix CloudPlatform、Microsoft Azure Classic

> 詳細については、「PvD、AppDisks、およびサポートされていないホストの削除」を参照してください。

> **注：**

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

> 展開にパブリッククラウドホスト接続を使用する場合は、新規インストールを完了するか、現在のリリースにアップグレードするためにHybrid Rights Licenseが必要です。

インストーラーがサポートされていないテクノロジーのいずれか、またはHybrid Rights Licenseなしのホスト接続を検出すると、アップグレードは一時停止または停止します。説明メッセージが表示されます。インストーラーログには詳細が含まれています。詳細については、「展開をアップグレードする」を参照してください。

はじめに

物理マシンまたは仮想マシンのコレクションは、マシンカタログと呼ばれる単一のエンティティとして管理されます。カタログ内のすべてのマシンは、マルチセッションOSまたはシングルセッションOS、およびWindowsまたはLinuxマシンという同じ種類のオペレーティングシステムを持っています。

Web Studioは、サイトを作成した後、最初のマシンカタログを作成するようにガイドします。最初のカタログを作成した後、Web Studioは最初のデリバリーグループを作成するようにガイドします。その後、作成したカタログを変更したり、さらにカタログを作成したりできます。

> **ヒント：**
>
> 既存の展開をアップグレードすると、Machine Creation Services (MCS) ストレージ最適化 (MCS I/O) 機能が有効になり、追加の構成は不要です。Virtual Delivery Agent (VDA) と Delivery Controller のアップグレードが MCS I/O のアップグレードを処理します。

概要

VM のカタログを作成するときに、それらの VM をプロビジョニングする方法を指定します。Machine Creation Services™ (MCS) を使用できます。または、独自のツールを使用してマシンを提供することもできます。

考慮事項:

- MCS は、仮想マシンイメージからの単一のシステムディスクをサポートします。そのイメージに接続されている残りのデータディスクは無視されます。
- MCS を使用して VM をプロビジョニングする場合、カタログに同一の VM を作成するためにマスターイメージ（またはイメージのスナップショット）を提供します。カタログを作成する前に、まずツールを使用してマスターイメージを作成および構成します。このプロセスには、イメージに Virtual Delivery Agent (VDA) をインストールすることが含まれます。その後、Web Studio でマシンカタログを作成します。そのイメージ（またはスナップショット）を選択し、カタログに作成する VM の数を指定し、追加情報を構成します。
- マシンがすでに利用可能な場合でも、それらのマシン用に1つ以上のマシンカタログを作成する必要があります。
- PowerShell SDK を直接使用してカタログを作成する場合、イメージやスナップショットではなく、ハイパーバイザーテンプレート（**VMTemplates**）を指定できます。

- テンプレートを使用してカタログをプロビジョニングすることは、実験的な機能と見なされます。この方法を使用すると、仮想マシンの準備が失敗する可能性があります。その結果、テンプレートを使用してカタログを公開することはできません。

MCS または Citrix Provisioning™ を使用して最初のカタログを作成する場合、サイトを作成したときに構成したホスト接続を使用します。後で（最初のカタログとデリバリーグループを作成した後）、その接続に関する情報を変更したり、さらに接続を作成したりできます。

カタログ作成ウィザードを完了すると、正しく構成されていることを確認するためにテストが自動的に実行されます。テストが完了すると、テストレポートを表示できます。Web Studio からいつでもテストを実行できます。

> **注:**
>
> MCSはWindows 10 IoT CoreおよびWindows 10 IoT Enterpriseをサポートしていません。詳細については、Microsoftサイトを参照してください。

> Citrix Provisioning ツールの技術的な詳細については、Citrix Virtual Apps and Desktops Image Management を参照してください。

RDS ライセンスチェック

Web Studio は現在、Windows マルチセッションOSマシンを含むマシンカタログの作成中に、有効なMicrosoft RDSライセンスのチェックを実行しません。Windows **マルチセッションOSマシン**のMicrosoft RDSライセンスのステータスを表示するには、Citrix Directorに移動します。Microsoft RDSライセンスのステータスは、**マシン詳細** パネルで確認できます。このパネルは、**マシン詳細とユーザー詳細** ページにあります。詳細については、「Microsoft RDSライセンスの健全性」を参照してください。

VDA登録

ブローカーセッションを起動する際には、VDAをDelivery Controller™に登録する必要があります。未登録のVDAは、利用可能なリソースの利用率低下につながる可能性があります。VDAが登録されない理由はさまざまであり、その多くは管理者がトラブルシューティングできます。Web Studioは、カタログ作成ウィザードで、またカタログからデリバリーグループにマシンを追加した後で、トラブルシューティング情報を提供します。

ウィザードを使用して既存のマシンを追加すると、コンピューターアカウント名のリストに、各マシンがカタログへの追加に適しているかどうかが表示されます。各マシンの横にあるアイコンにマウスカーソルを合わせると、そのマシンに関する情報メッセージが表示されます。

メッセージで問題のあるマシンが特定された場合は、そのマシンを削除するか、追加します。たとえば、マシンに関する情報が取得できない可能性があることを示すメッセージが表示された場合でも、そのマシンを追加してください。

詳細については、以下を参照してください。

- VDA登録のトラブルシューティングガイダンスについては、CTX136668
- VDAのバージョンと機能レベル
- VDA登録方法

MCSカタログ作成の概要

カタログ作成ウィザードで情報を提供した後の、デフォルトのMCSアクションの概要を以下に示します。

- マスターイメージ（スナップショットではなく）を選択した場合、MCSはスナップショットを作成します。
- MCSはスナップショットの完全なコピーを作成し、そのコピーをホスト接続で定義されている各ストレージの場所に配置します。
- MCSはマシンをActive Directoryに追加し、一意のIDを作成します。
- MCSは、ウィザードで指定された数のVMを作成し、各VMに2つのディスクを定義します。各VMの2つのディスクに加えて、マスターも同じストレージの場所に保存されます。複数のストレージの場所が定義されている場合、それぞれに次のディスクタイプが割り当てられます。
    - スナップショットの完全なコピーで、読み取り専用であり、作成されたばかりのVM間で共有されます。
    - 各VMに一意のIDを付与する、一意の16 MBのIDディスク。各VMはIDディスクを取得します。
    - VMへの書き込みを保存するための一意の差分ディスク。このディスクはシンプロビジョニングされており（ホストストレージでサポートされている場合）、必要に応じてマスターイメージの最大サイズまで増加します。各VMは差分ディスクを取得します。差分ディスクはセッション中に行われた変更を保持します。専用デスクトップの場合は永続的です。プールされたデスクトップの場合、デリバリーコントローラーを介した再起動ごとに削除され、新しいものが作成されます。

あるいは、静的デスクトップを提供するVMを作成する際、カタログ作成ウィザードの**マシン**ページで、シック（完全コピー）VMクローンを指定できます。完全クローンは、すべてのデータストアでマスターイメージを保持する必要はありません。各VMは独自のファイルを持ちます。

MCSストレージに関する考慮事項

MCSのストレージソリューション、構成、容量を決定する際には、多くの要因があります。以下の情報は、ストレージ容量に関する適切な考慮事項を提供します。

容量に関する考慮事項:

- ディスク

  DeltaまたはDifferencing (Diff) ディスクは、ほとんどのMCS展開において、各VMで最大のスペースを消費します。MCSによって作成される各VMには、作成時に最低2つのディスクが割り当てられます。

  - Disk0 = 差分ディスク: マスターベースイメージからコピーされたOSが含まれます。
  - Disk1 = IDディスク: 16 MB - 各VMのActive Directoryデータが含まれます。

  製品の進化に伴い、特定のユースケースや機能の消費を満たすために、さらにディスクを追加する必要がある場合があります。例:

  - MCS Storage Optimizationは、各VMにライトキャッシュスタイルのディスクを作成します。XenServer、VMware、およびSCVMM仮想化環境では、ホスト接続の作成時に利用可能なOSストレージリストと利用可能な一時ストレージリストを同じように構成した場合、MCSはライトバックキャッシュ（WBC）ディスクをOSディスクと同じストレージ場所に配置します。
  - MCSは、前のセクションで説明したデルタディスクのシナリオとは対照的に、フルクローンを使用する機能を追加しました。

  ハイパーバイザーの機能も考慮に入れる必要があるかもしれません。例:

  - XenServer IntelliCacheは、各XenServerのローカルストレージに読み取りディスクを作成します。このオプションにより、共有ストレージの場所に保持されている可能性のあるマスターイメージに対するIOPSを節約できます。

- ハイパーバイザーのオーバーヘッド

  異なるハイパーバイザーは、VMのオーバーヘッドを発生させる特定のファイルを使用します。ハイパーバイザーは、管理および一般的なログ記録操作にもストレージを使用します。オーバーヘッドを含めるためのスペースを計算します。

  - ログファイル
  - ハイパーバイザー固有のファイル。例:

    - VMwareは、**VMストレージ**フォルダーにファイルを追加します。VMwareのベストプラクティスを参照してください。
    - 仮想マシンの合計サイズ要件を計算します。仮想ディスクに20 GB、スワップファイルに16 GB、ログファイルに100 MBを使用し、合計36.1 GBを消費する仮想マシンを考慮してください。
  - XenServerのスナップショット; VMwareのスナップショット。

- プロセスオーバーヘッド

  カタログの作成、マシンの追加、カタログの更新には、それぞれ固有のストレージへの影響があります。例:

  - 初期カタログ作成では、ベースディスクのコピーを各ストレージの場所にコピーする必要があります。
  - マシンの追加をカタログに追加する場合、ベースディスクを各ストレージの場所にコピーする必要はありません。カタログの作成は、選択した機能によって異なります。
  - カタログの更新により、各ストレージの場所に余分なベースディスクが作成されます。カタログの更新では、カタログ内の各VMが一定期間2つの差分ディスクを持つため、一時的なストレージピークも発生します。

その他の考慮事項：

- **RAMサイジング：** I/O最適化ディスク、ライトキャッシュ、スナップショットファイルなど、特定のハイパーバイザーファイルとディスクのサイズに影響します。
- **シンプロビジョニング/シックプロビジョニング:** シンプロビジョニング機能があるため、NFSストレージが推奨されます。

Machine Creation Services (MCS) ストレージ最適化

Machine Creation Services (MCS) ストレージ最適化機能は、MCS I/O とも呼ばれます。この機能は、Azure、GCP、XenServer、VMware、AWS、および SCVMM でのみ利用可能です。

- 書き込みキャッシュコンテナは、Citrix Provisioning と同じ機能である *ファイルベース* です。たとえば、Citrix Provisioning の書き込みキャッシュファイル名は `D:\vdiskdif.vhdx` で、MCS I/O の書き込みキャッシュファイル名は `D:\mcsdif.vhdx` です。
- 書き込みキャッシュディスクに書き込まれた Windows クラッシュダンプファイルのサポートを含めることで、診断の改善を実現します。
- MCS I/O は、最適な多層書き込みキャッシュソリューションを提供するために、*RAM 内キャッシュとハードディスクへのオーバーフロー* というテクノロジーを保持しています。この

機能により、管理者は各層（RAM とディスク）のコストとパフォーマンスのバランスを取り、目的のワークロード要件を満たすことができます。

書き込みキャッシュ方式を *ディスクベース* から *ファイルベース* に更新するには、次の変更が必要です。

1. MCS I/O は、RAMのみのキャッシュをサポートしなくなりました。マシンカタログ作成時にWeb Studioでディスクサイズを指定します。
2. VM の書き込みキャッシュディスクは、VM を初めて起動するときに自動的に作成およびフォーマットされます。VM が起動すると、書き込みキャッシュファイル `mcsdif.vhdx` がフォーマットされたボリューム `MCSWCDisk` に書き込まれます。
3. ページファイルはこのフォーマットされたボリューム `MCSWCDisk` にリダイレクトされます。その結果、このディスクサイズはディスク領域の合計量を考慮します。これには、ディスクサイズと生成されたワークロードの差分にページファイルサイズを加えたものが含まれます。これは通常、VM の RAM サイズに関連付けられています。

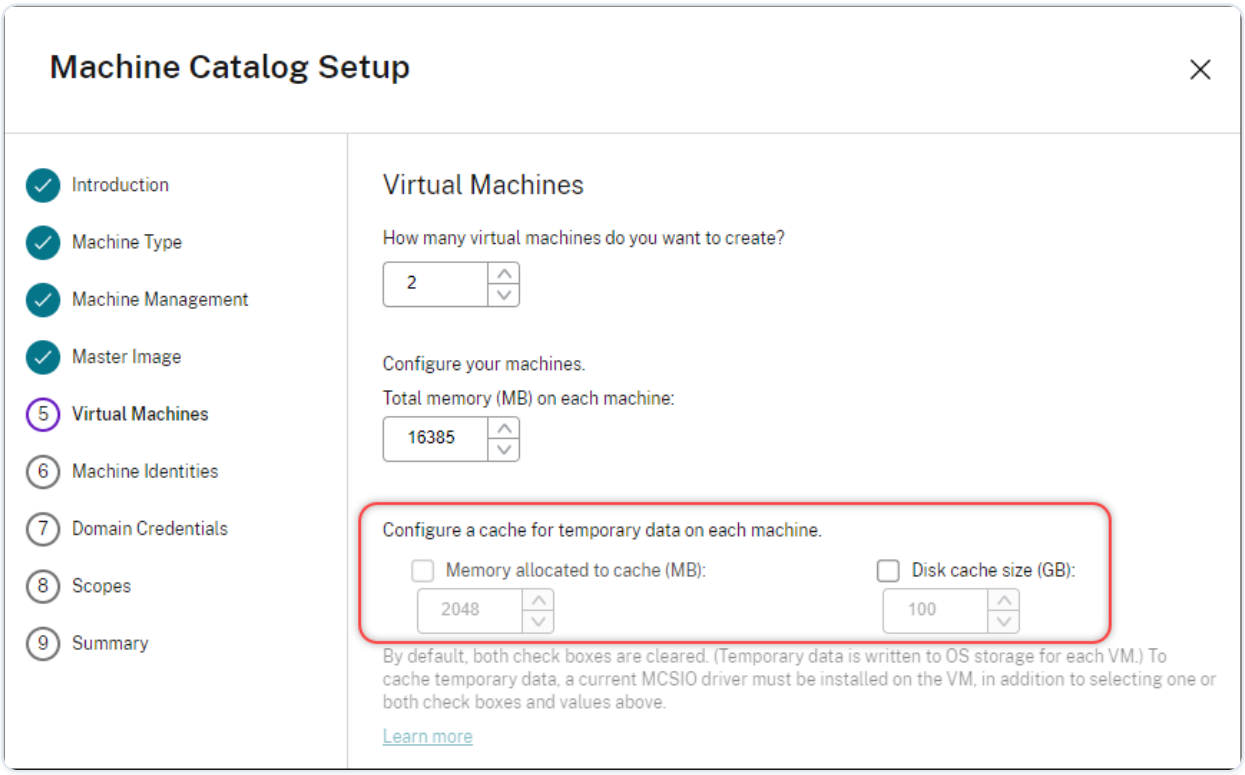
MCS ストレージ最適化の更新の有効化

MCS I/O ストレージ最適化機能を有効にするには、Delivery Controller と VDA を Citrix Virtual Apps and Desktops の最新バージョンにアップグレードしてください。

> **注:**
>
> MCS I/O が有効になっている既存の展開をアップグレードする場合、追加の構成は不要です。VDA と Delivery Controller のアップグレードによって MCS I/O のアップグレードが処理されます。

> MCS ストレージ最適化の更新を有効にする際は、次の点を考慮してください。

- マシンカタログを作成する際、管理者は RAM とディスクサイズを構成できます。



- 既存のマシンカタログを、バージョン1903用に構成されたVDAを含む新しいVMスナップショットに更新すると、次の動作が発生します。新しいスナップショットは、既存のカタログのRAMおよびディスクサイズに対するMCS I/O設定を引き続き使用します。既存の生ディスクはフォーマットされます。

重要:

MCSストレージ最適化は、Citrix Virtual Apps and Desktopsバージョン1903で変更されました。このリリースでは、ファイルベースのライトキャッシュテクノロジーがサポートされ、パフォーマンスと安定性が向上します。MCS I/Oによって提供される新しい機能は、以前のCitrix Virtual Apps and Desktopsリリースと比較して、より高いライトキャッシュストレージ要件を必要とする場合があります。Citrixは、割り当てられたワークフローと追加のページファイルサイズに対して十分なディスク容量があることを確認するために、ディスクサイズを再評価することを推奨します。ページファイルサイズは通常、システムRAMの量に関連しています。既存のカタログディスクサイズが不十分な場合は、マシンカタログを作成し、より大きなライトキャッシュディスクを割り当ててください。

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

MCS I/Oライトバックキャッシュディスクに特定のドライブ文字を割り当てることができます。この実装により、使用するアプリケーションのドライブ文字とMCS I/Oライトバックキャッシュディスクのドライブ文字との間の競合を回避できます。MCS I/Oライトバックキャッシュディスクにドライブ文字を割り当てるには、PowerShellコマンドを使用できます。サポートされているハイパーバイザーは、Azure、GCP、VMware、SCVMM、およびXenServerです。

> **注:**
>
> この機能には、VDAバージョン2305以降が必要です。

制限事項

- Windowsオペレーティングシステムのみに適用
- ライトバックキャッシュディスクに適用可能なドライブ文字：`E`から`Z`
- Azure一時ディスクがライトバックキャッシュディスクとして使用されている場合は適用されません
- 新しいマシンカタログを作成する場合にのみ適用されます

ライトバックキャッシュディスクにドライブ文字を割り当てる

ライトバックキャッシュディスクにドライブ文字を割り当てるには：

1. **PowerShell**ウィンドウを開きます。
2. `asnp citrix*`を実行します。
3. まだ作成されていない場合は、IDプールを作成します。
4. プロパティ`WriteBackCacheDriveLetter`を指定して、`New-ProvScheme`コマンドを使用してプロビジョニングスキームを作成します。例：

```
New-ProvScheme -CleanOnBoot `

-HostingUnitName "<name>" `

-IdentityPoolName $schemeName `

-ProvisioningSchemeName $schemeName `
```

```
-InitialBatchSizeHint 1 `

-UseWriteBackCache -WriteBackCacheDiskSize 127
-WriteBackCacheMemorySize 256 -WriteBackCacheDriveLetter E `

-MasterImageVM "XDHyp:\HostingUnits\<name>\image.folder\abcd-
resources.resourcegroup\MCSIOMasterVm_OsDisk_1_d3e2d6352xxxxxxxxx2130aa
145ec77.manageddisk" `

-NetworkMapping @{"0"="XDHyp:\\HostingUnits\\name\
\virtualprivatecloud.folder\\East US.region\
\virtualprivatecloud.folder\\abcd-resources.resourcegroup\\abcd-
resources-vnet.virtualprivatecloud\\default.network"} `

-ServiceOffering "XDHyp:\\HostingUnits\\<name>\\serviceoffering.folder\
\Standard_D2s_v5.serviceoffering" `

-CustomProperties '<CustomProperties xmlns="http://schemas.citrix.com/
2014/xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks"
Value="true" />

<Property xsi:type="StringProperty" Name="OsType" Value="Windows" />

<Property xsi:type="StringProperty" Name="StorageType"
Value="Premium_LRS"/>

<Property xsi:type="StringProperty" Name="PersistWBC" Value="false" />

<Property xsi:type="StringProperty" Name="PersistOsDisk"
Value="false" />

<Property xsi:type="StringProperty" Name="PersistVm" Value="false" />

<Property xsi:type="StringProperty" Name="WBCDiskStorageType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="UseTempDiskForWBC"
Value="false" />

<Property xsi:type="StringProperty" Name="ResourceGroups" Value="abcd-
```

```
group1" />

<Property xsi:type="StringProperty" Name="LicenseType"
Value="Windows_Client" />

<Property xsi:type="StringProperty" Name="SchemaVersion" Value="2" />

</CustomProperties>'
```

5. カタログの作成を完了します。詳細については、`<https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/>`を参照してください。

マスターイメージを準備する

接続ホストの作成については、接続とリソース を参照してください。

マスターイメージには、オペレーティングシステム、仮想化されていないアプリケーション、VDA、およびその他のソフトウェアが含まれています。

知っておくと良いこと:

- マスターイメージは、クローンイメージ、ゴールデンイメージ、ベースVM、またはベースイメージとも呼ばれることがあります。ホストベンダーは異なる用語を使用します。
- ホストが、作成されるマシンの数に対応できる十分なプロセッサ、メモリ、ストレージを備えていることを確認してください。
- デスクトップとアプリケーションに必要なハードディスク容量を正しく構成します。この値は後で、またはマシンカタログ内で変更することはできません。
- Remote PC Access マシンカタログはマスターイメージを使用しません。

マスターイメージに次のソフトウェアをインストールして構成します。

- ハイパーバイザー用の統合ツール（Citrix VM Tools、Hyper-V Integration Services、VMware toolsなど）。この手順を省略すると、アプリケーションやデスクトップが正しく機能しない可能性があります。
- VDA。Citrixでは、最新機能にアクセスできるように、最新バージョンをインストールすることをお勧めします。マスターイメージにVDAをインストールしないと、カタログの作成が失敗します。

- 必要に応じて、ウイルス対策ソフトウェアや電子ソフトウェア配布エージェントなどのサードパーティ製ツール。ユーザーとマシンタイプに適した設定（更新機能など）でサービスを構成します。
- 仮想化しないサードパーティ製アプリケーション。Citrixでは、アプリケーションを仮想化することをお勧めします。仮想化により、アプリケーションの追加または再構成後にマスターイメージを更新する必要がなくなるため、コストが削減されます。また、インストールされるアプリケーションが少ないほど、マスターイメージのハードディスクのサイズが小さくなり、ストレージコストを節約できます。
- App-Vアプリケーションを公開する予定がある場合は、推奨設定のApp-Vクライアント。App-VクライアントはMicrosoftから入手できます。
- MCSを使用する場合、Microsoft Windowsをローカライズする場合は、ロケールと言語パックをインストールします。プロビジョニング中にスナップショットが作成されると、プロビジョニングされたVMはインストールされているロケールと言語パックを使用します。

重要：

MCSを使用している場合は、マスターイメージでSysprepを実行しないでください。

マスターイメージを準備するには：

1. ハイパーバイザーの管理ツールを使用してマスターイメージを作成し、オペレーティングシステム、すべてのサービスパック、および更新プログラムをインストールします。vCPUの数を指定します。PowerShellを使用してマシンカタログを作成する場合も、vCPUの値を指定できます。Web Studioを使用してカタログを作成する場合、vCPUの数を指定することはできません。デスクトップとアプリケーションに必要なハードディスク容量を構成します。この値は後で変更したり、カタログ内で変更したりすることはできません。
2. ハードディスクがデバイスロケーション0に接続されていることを確認します。ほとんどの標準マスターイメージテンプレートでは、このロケーションがデフォルトで構成されていますが、一部のカスタムテンプレートではそうでない場合があります。
3. 上記のソフトウェアをマスターイメージにインストールして構成します。
4. MCSを使用していない場合は、マスターイメージをアプリケーションとデスクトップが属するドメインに参加させます。マスターイメージがマシンが作成されるホストで利用可能であることを確認します。MCSを使用している場合、マスターイメージをドメインに参加させる必要はありません。プロビジョニングされたマシンは、カタログ作成ウィザードで指定されたドメインに参加します。

5. Citrixでは、マスターイメージのスナップショットを作成して名前を付けることをお勧めします。カタログ作成時にスナップショットではなくマスターイメージを指定した場合、Web Studioはスナップショットを作成します。そのスナップショットに名前を付けることはできません。

ボリュームライセンス認証

MCS は、Windows オペレーティングシステムと Microsoft Office のアクティベーションを自動化および管理するためのボリュームライセンス認証をサポートしています。MCS がサポートするボリュームライセンス認証の 3 つのモデルは次のとおりです。

- キー管理サービス (KMS)
- Active Directoryベースのアクティベーション (ADBA)
- 複数ライセンス認証キー (MAK)

マシンカタログを作成した後で、アクティベーション設定を変更できます。

キー管理サービス (KMS)

KMS は、専用のシステムを必要とせず、他のサービスを提供するシステム上で簡単に共存できる軽量なサービスです。この機能は、Citrix がサポートするすべての Windows バージョンでサポートされています。イメージ準備中に、MCS は Microsoft Windows および Microsoft Office の KMS リアームを実行します。コマンド `Set-Provserviceconfigurationdata` を実行することで、リアームをスキップできます。KMS アクティベーションの詳細については、「キー管理サービスを使用したアクティベーション」を参照してください。

> **注：**
>
> コマンド `Set-Provserviceconfigurationdata` の実行後に作成されたすべてのマシンカタログは、そのコマンドで指定された設定と同じ設定になります。

Active Directory ベースのアクティベーション (ADBA)

ADBA を使用すると、ドメイン接続を介してマシンをアクティベートできます。マシンはドメインに参加するとすぐにアクティベートされます。これらのマシンは、ドメインに参加しており、ドメインと通信している限りアクティベートされたままになります。この機能は、Citrix がサポートするすべての Windows バージョンでサポートされています。Active Directory ベースのアクティベーションの詳細については、「Active Directory ベースのアクティベーション を使用したアクティベーション」を参照してください。

マルチプルアクティベーションキー (MAK)

MAK は、Microsoft サーバーの助けを借りて、ボリュームをアクティベートし、Windows システムを認証する方法です。Microsoft から MAK キーを購入する必要があります。このキーには、固定されたアクティベーションカウントが割り当てられています。Windows システムがアクティベートされるたびに、アクティベーションカウントが減少します。システムをアクティベートする方法は 2 つあります。

- オンラインアクティベーション：アクティベートする Windows システムがインターネットにアクセスできる場合、プロダクトキーをインストールするとシステムは自動的に Windows をアクティベートします。このプロセスにより、対応する MAK のアクティベーションカウントが 1 減少します。
- オフラインアクティベーション：Windows システムがインターネットに接続してオンラインアクティベーションを実行できない場合、MCS は Microsoft サーバーから確認 ID とインストール ID を取得して Windows システムをアクティベートします。このアクティベーション方法は、非永続マシンカタログに役立ちます。

注:

コマンド `Set-Provserviceconfigurationdata` の実行後に作成されたすべてのマシンカタログは、コマンドで指定されたものと同じ設定になります。

Active Directoryベースのアクティベーション (ADBA)

ADBAを使用すると、マシンのドメイン接続を介してアクティベートできます。マシンはドメインに参加するとすぐにアクティベートされます。これらのマシンは、ドメインに参加し、ドメインと連絡を取り合っている限り、アクティベートされたままになります。この機能は、Citrixがサポートするすべてのバージョンでサポートされています。Active Directoryベースのアクティベーションの詳細については、「Active Directoryベースのアクティベーション」を参照してください。

マルチプルアクティベーションキー (MAK)

MAKは、Microsoftサーバーの助けを借りて、ボリュームをアクティベートし、Windowsシステムを認証する方法です。MicrosoftからMAKキーを購入する必要があります。このキーには、固定されたアクティベーションカウントが割り当てられています。Windowsシステムがアクティベートされるたびに、アクティベーションカウントが減少します。システムをアクティベートする方法は2つあります。

- オンラインアクティベーション: アクティベートしたいWindowsシステムがインターネットアクセスを持っている場合、製品キーをインストールするとシステムは自動的にWindowsをアクティベートします。このプロセスにより、対応するMAKのアクティベーションカウントが1減少します。
- オフラインアクティベーション: Windowsシステムがオンラインアクティベーションを行うためにインターネットに接続できない場合、MCSはMicrosoftサーバーから確認IDとインストールIDを取得し、Windowsシステムをアクティベートします。このアクティベーション方法は、非永続的なマシンカタログに役立ちます。

> **注:**
>
> - MCSはMAKを使用したMicrosoft Officeのアクティベーションをサポートしていません。
> - 必要なVDAの最小バージョンは2303です。

主な要件

- Delivery Controller はインターネットにアクセスできる必要があります。
- 更新する新しいイメージの MAK キーが元のイメージと異なる場合は、新しいカタログを作成します。
- マスターイメージに MAK キーをインストールします。Windows システムに MAK キーをインストールする手順については、MAK アクティベーションの展開 を参照してください。
- イメージ準備を使用しない場合:

  a. レジストリ DWORD 値 `Manual` を `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform\Activation` の下に追加します。

  b. 値を `1` に設定します。

アクティベーション数

MAK キーの残りのアクティベーション数を表示したり、VM が 2 つ以上のアクティベーションを消費しているかどうかを確認したりするには、ボリュームアクティベーション管理ツール (VAMT) を使用します。VAMT のインストール を参照してください。

MAKを使用してWindowsシステムをアクティベートする

MAKを使用してWindowsシステムをアクティベートするには：

1. マスターイメージにプロダクトキーをインストールします。この手順で、1 つのアクティベーションカウントが消費されます。
2. MCSマシンカタログを作成します。
3. イメージ準備を使用しない場合:

   a. `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform\Activation`の下にレジストリDWORD値`Manual`を追加します。

   b. 値を`1`に設定します。

   この方法では、オンラインアクティベーションのオプションが無効になります。
4. マシンカタログにVMを追加します。
5. VMの電源をオンにします。
6. オンラインアクティベーションかオフラインアクティベーションかに応じて、Windowsシステムがアクティベートされます。

   - アクティベーションがオンラインの場合、プロダクトキーのインストール後にWindowsシステムがアクティベートされます。
   - アクティベーションがオフラインの場合、MCSはプロビジョニングされたVMと通信してWindowsシステムのアクティベーションステータスを取得します。その後、MCSはMicrosoftサーバーから確認IDとインストール済みIDを取得します。これらのIDはWindowsシステムのアクティベートに使用されます。

トラブルシューティング

プロビジョニングされたVMがインストール済みのMAKキーでアクティベートされていない場合は、PowerShellウィンドウで`Get-ProvVM`または`Get-ProvScheme`コマンドを実行します。

- `Get-ProvScheme`コマンド: 最新のマスターイメージからMCSマシンカタログに関連付けられているパラメーター`WindowsActivationType`を参照してください。
- `Get-ProvVM`コマンド。パラメーター`WindowsActivationType`、`WindowsActivationStatus`、`WindowsActivationStatusErrorCode`、および`WindowsActivationStatusError`を参照してください。

エラーを確認し、問題を解決するための手順を検証できます。

Web Studio を使用してマシンカタログを作成する

カタログを作成する前に:

- このセクションを確認して、選択する項目と提供する情報について学習してください。
- ハイパーバイザー、クラウドサービス、およびマシンをホストするその他のリソースへの接続が作成されていることを確認してください。
- マシンをプロビジョニングするためのマスターイメージを作成した場合は、そのイメージにVDAがインストールされていることを確認してください。

カタログ作成ウィザードを開始するには：

1. これが最初に作成するカタログである場合、適切な選択肢（「マシンをセットアップし、アプリとデスクトップを実行するためのマシンカタログを作成する」など）に誘導されます。カタログ作成ウィザードが開きます。
2. すでにカタログを作成しており、別のカタログを作成したい場合は、次の手順に従ってください:

    a. Web Studioにサインインし、左ペインで**マシンカタログ**を選択し、アクションバーで**マシンカタログの作成**を選択します。

    b. フォルダーを使用してカタログを整理するには、デフォルトの**マシンカタログ**フォルダーの下にフォルダーを作成します。詳しくは、カタログフォルダーの作成を参照してください。

    c. カタログを作成したいフォルダーを選択し、**マシンカタログの作成**をクリックします。カタログ作成ウィザードが開きます。

ウィザードは次の項目について説明します。表示されるウィザードページは、選択内容によって異なります。

オペレーティングシステム

各カタログには、1種類のマシンのみが含まれます。1つ選択してください。

- **マルチセッションOS:** マルチセッションOSカタログは、ホストされた共有デスクトップを提供します。マシンはサポートされているバージョンのWindowsまたはLinuxオペレーティングシステムを実行できますが、カタログに両方を含めることはできません。（そのOSの詳細については、Linux VDAのドキュメントを参照してください。）
- **シングルセッションOS:** シングルセッションOSカタログは、さまざまなユーザーに割り当てることができるVDIデスクトップを提供します。
- **Remote PC Access:** Remote PC Accessカタログは、ユーザーに物理的なオフィスデスクトップマシンへのリモートアクセスを提供します。Remote PC Accessは、セキュリティを提供するためにVPNを必要としません。

マシン管理

このページは、リモートPCアクセスカタログを作成する際には表示されません。

マシン管理ページには、マシンの管理方法と、マシンを展開するために使用するツールが表示されます。

カタログ内のマシンがWeb Studioを介して電源管理されるかどうかを選択します。

- マシンはWeb Studioを介して電源管理されます（例: VMまたはブレードPC）。このオプションは、ホストへの接続をすでに構成している場合にのみ利用可能です。
- マシンはWeb Studioを介して電源管理されません（例: 物理マシン）。

マシンがWeb Studioを介して電源管理されることを示した場合は、VMの作成に使用するツールを選択します。

- Citrix Provisioningテクノロジー
  - **Citrix Machine Creation Services (MCS)** MCSを使用してプロビジョニングおよびイメージ化されたVMのカタログを作成します。MCSは、マスターイメージからクローンされたイメージをこれらのVMにコピーします。
  - **Citrix Provisioning Services (PVS)** MCSを使用してプロビジョニングされ、PVSを使用してイメージ化されたVMのカタログを作成します。これらのVMはPVSターゲットデバイスとして機能し、PVSサーバーは単一の共有ディスクイメージをそれらにストリーミングできます。

> **注:**
>
> - このオプションは、Citrix Cloud™に登録されているPVSサイトでのみ利用可能であり、現在はAzureリソースに限定されています。
> - Citrix Provisioningカタログを作成する際に、**ターゲットデバイス**ページで、プロビジョニングするマシンのファームとサイトを選択するドロップダウンメニューに、存在しないファームとサイトがリストされている場合があります。回避策として、PowerShellコマンド `Unregister-HypPvsSite` を実行して、データベースからファームとサイトを削除できます。PowerShellコマンドの詳細については、Unregister-HypPvsSite を参照してください。

- **その他のサービスまたはテクノロジー** データセンターにすでに存在するマシンを管理するツール。Citrixでは、カタログ内のマシンの一貫性を確保するために、Microsoft System Center Configuration Managerまたはその他のサードパーティ製アプリケーションを使用することをお勧めします。

デスクトップの種類（デスクトップエクスペリエンス）

> **注:**
>
> **デスクトップエクスペリエンス**ページで利用できるオプションは、**マシンタイプ**ページで選択したマシンタイプによって異なります。

- **マルチセッションOS**マシンでは、ユーザーはログオンするたびにランダムなデスクトップを割り当てられます。次のいずれかのオプションを選択してください。
  - **はい、仮想デスクトップをホストするマシンのローカルディスクに変更を保存します。**（永続的）
  - **いいえ、すべての変更を破棄し、ユーザーがログオフするときに仮想デスクトップをクリアします。**（非永続的）

  > **注:**
  >
  > 永続的なマルチセッションマシンでは、ユーザーがデスクトップに行った変更は保存され、すべての承認済みユーザーがアクセスできます。

- **シングルセッションOS**マシンでは、**デスクトップエクスペリエンス**ページで次のオプションが表示されます。
  - **ユーザーがログオンするたびに、新しい（ランダムな）デスクトップに接続するようにします。**
  - **ユーザーがログオンするたびに、同じ（静的な）デスクトップに接続するようにします。**

    静的デスクトップの場合、ユーザーが行った変更をログオフ後に保存するか破棄するかをさらに決定できます。

仮想デスクトップをホストするマシンのローカルディスクに変更を保存する：永続的を選択した場合、**仮想マシン**ページで仮想マシンコピーモードの高速コピーまたは完全コピーオプションが利用可能です。

すべての変更を破棄し、ユーザーがログオフするときに仮想デスクトップをクリアする: 非永続的を選択した場合、**仮想マシン**ページで仮想マシンコピーモードを構成することはできません。

イメージとマシンプロファイル

このページは、MCSを使用してVMを作成している場合にのみ表示されます。

1. マシンカタログのイメージタイプを選択し、イメージを選択します。利用可能なイメージタイプは次の2種類です。

   - **マスターイメージ。** イメージ準備プロセスをまだ経ていないイメージです。イメージ準備プロセスは、カタログ作成が開始されると自動的に開始されます。

     > **注:**
     >
     > - MCS を使用している場合、マスターイメージで Sysprep を実行しないでください。
     > - スナップショットではなくマスターイメージを指定した場合、Web Studio はスナップショットを作成しますが、名前を付けることはできません。

   - **準備済みイメージ。** イメージ準備プロセスを完了し、VM 作成に直接使用できるイメージ。カタログ作成時にマスターイメージではなく準備済みイメージを選択すると、マシンカタログの作成がより高速かつ信頼性の高いものになり、イメージのライフサイクル管理も効率化されます。

     > **注:**
     >
     > - 準備されたイメージを使用して作成されたVMは、ハイバネーションをサポートしていません。
     > - 現在、準備されたイメージを使用してカタログを作成することは、AzureおよびVMware環境でのみ利用可能です。

準備済みイメージの作成方法について詳しくは、「イメージ管理（プレビュー）」を参照してください。

イメージを選択する際、必要に応じて、選択したイメージにメモを追加できます。

最新の製品機能を使用できるようにするには、マスターイメージに最新のVDAバージョンがインストールされていることを確認してください。デフォルトの最小VDA選択を変更しないでください。ただし、以前のVDAバージョンを使用する必要がある場合は、VDA versions and functional levelsを参照してください。

ウィザードで以前に選択したマシン管理テクノロジと互換性のないスナップショットまたはVM を選択すると、エラーメッセージが表示されます。

2. 既存のVMをマシンプロファイルとして使用するには、**Use a machine profile**を選択し、その後、VMを選択します。

> **注:**
>
> 現在、マシンプロファイルの使用は、Azure、AWS、GCP、およびVMwareのVMに制限されています。

> VMwareの展開の場合、マシンプロファイルを使用してマシンカタログを作成する際、仮想マシンを保持するフォルダーを指定する必要があります。

仮想マシンフォルダーの場所を指定するには、カタログ作成ウィザードで**Virtual Machines**ページに移動し、**Select a folder to place the machines**セクションに移動して仮想マシンフォルダーの場所を選択します。指定されていない場合、システムは選択されたマシンプロファイルのフォルダーをデフォルトの場所と見なします。

3. AWSの展開の場合、起動テンプレートをマシンプロファイルとして選択できます。
4. カタログの最小機能レベルを選択します。最新の製品機能を使用できるようにするには、マスターイメージに最新のVDAバージョンがインストールされていることを確認してください。

マシン

リモートPCアクセス カタログを作成している場合、このページは表示されません。

このページのタイトルは、**マシン管理**ページで選択した内容（**マシン**、**仮想マシン**、または**VMとユーザー**）によって異なります。

MCSを使用する場合：

- 作成する仮想マシンの数を指定します。作成しない場合は**0**（ゼロ）を入力します。後で、**Add machines**を実行して、空のカタログにVMを作成できます。
- 各 VM が持つメモリ量 (MB 単位) を選択します。
- 作成された各VMにはハードディスクがあります。そのサイズはマスターイメージで設定されます。カタログでハードディスクのサイズを変更することはできません。
- 展開に複数のゾーンが含まれている場合、カタログのゾーンを選択できます。
- 静的デスクトップVMを作成している場合は、仮想マシンコピーモードを選択します。詳細については、「仮想マシンコピーモード」を参照してください。
- vDiskを使用しないランダムデスクトップVMを作成している場合は、各マシンの一時データに使用するキャッシュを構成できます。詳細については、「一時データ用のキャッシュの構成」を参照してください。

その他のツールを使用する場合：

Active Directoryマシンアカウント名を追加（またはリストをインポート）します。VMを追加/インポートした後で、そのVMのActive Directoryアカウント名を変更できます。**Desktop Experience**ページで静的マシンを指定した場合、追加する各VMのActive Directoryユーザー名をオプションで指定できます。

名前を追加またはインポートした後、このページにいる間は、**削除**ボタンを使用してリストから名前を削除できます。

他のツールを使用する場合（ただしMCSではない場合）：

追加（またはインポート）された各マシンに表示されるアイコンとツールヒントは、カタログに追加できない可能性のあるマシン、またはDelivery Controllerに登録できない可能性のあるマシンを特定するのに役立ちます。詳細については、「VDAのバージョンと機能レベル」を参照してください。

仮想マシン作成時にSIDを追加する

新しい仮想マシンを作成する際に、マシンを一意に識別するためにパラメーター`ADAccountSid`を追加できるようになりました。

これを行うには：

1. サポートされているIDタイプでカタログを作成します。
2. `NewProvVM`を使用してカタログにマシンを追加します。例：

```
New-ProvVM  -ProvisioningSchemeName "name"  -ADAccountSid @("SID ")  -
RunAsynchronously
```

ただし、次の条件のいずれかに該当するマシンをプロビジョニングすることはできません。

- カタログIDプールにないADアカウント
- 利用可能な状態ではないADアカウント

仮想マシンのコピーモード

「**マシン**」ページで指定するコピーモードによって、MCSがマスターイメージからシン（高速コピー）クローンを作成するか、シック（完全コピー）クローンを作成するかが決まります。（デフォルト = シンクローン）

- より効率的なストレージ使用とより高速なマシン作成のために、高速コピーのクローンを使用します。
- より優れたデータ回復と移行のサポートのために、完全コピーのクローンを使用します。これにより、マシン作成後のIOPSを潜在的に削減できます。

> 「**注：**」:

> 完全コピーのクローン方式は、マルチセッションまたはシングルセッションOS上の永続VMのプロビジョニングにのみ利用可能です。

VDAのバージョンと機能レベル

カタログの機能レベルは、カタログ内のマシンで利用できる製品機能を制御します。新しい製品バージョンで導入された機能を使用するには、新しいVDAが必要です。 ただし、以前のVDAバージョンを使用しているカタログ内のマシンは登録できません。

「**マシン**」（または「**デバイス**」）ページの下部にあるメニューで、最小VDAレベルを選択できます。これにより、カタログの最小機能レベルが設定されます。デフォルトでは、オンプレミス展開の場合、最新の機能レベルが選択されます。Citrixの推奨に従って、常にVDAとコアコンポーネントを最新バージョンにインストールおよびアップグレードする場合は、この選択を変更する必要はありません。ただし、古いVDAバージョンを使い続ける必要がある場合は、正しい値を選択してください。

Citrix Virtual Apps and Desktopsのリリースに新しいVDAバージョンが含まれていない場合や、新しいVDAが機能レベルに影響を与えない場合があります。そのような場合、機能レベルは、インストールまたはアップグレードされたコンポーネントよりも古いVDAバージョンを示すことがあります。各リリースの新機能の記事には、デフォルトの機能レベルの変更が示されています。

選択された機能レベルは、その上にあるマシンのリストに影響します。リストでは、各エントリの横にあるツールチップが、その機能レベルでマシンのVDAがカタログと互換性があるかどうかを示します。

各マシンのVDAが選択された最小機能レベルを満たしていないか、それを超えていない場合、ページにメッセージが表示されます。ウィザードを続行できます。これらのマシンは、後でControllerに登録できない可能性があります。または、次のことができます。

- 古いVDAを含むマシンをリストから削除し、VDAをアップグレードしてから、カタログに再度追加します。
- 最新の製品機能へのアクセスを妨げる、より低い機能レベルを選択します。

マシンが間違ったマシンタイプであるためにカタログに追加されなかった場合も、メッセージが表示されます。例としては、サーバーをシングルセッションOSカタログに追加しようとしたり、ランダム割り当て用に作成されたシングルセッションOSマシンを静的マシンのカタログに追加したりする場合があります。

> **重要:**
>
> リリース1811で、追加の機能レベルである**1811 (またはそれ以降)**が追加されました。このレベルは、将来のCitrix Virtual Apps and Desktopsの機能で使用することを目的としています。**7.9 (またはそれ以降)**の選択はデフォルトのままです。このデフォルトは、現在のすべての展開で有効です。

> **1811 (またはそれ以降)**を選択した場合、そのカタログ内の以前のVDAバージョンはControllerに登録できません。ただし、カタログにバージョン1811以降のサポートされているVDAのみが含まれている場合、それらはすべて登録可能です。これには、バージョン1903や現在のリリース以前の他の19XXリリースを含む、後のCitrix Virtual Apps and Desktopsリリース用に構成されたVDAを含むカタログが含まれます。

一時データのキャッシュを構成する

カタログ内のランダムな非永続マシンをMCSで管理する場合、I/Oパフォーマンスを向上させるために、マシンに対してライトバックキャッシュを有効にできます。

ライトバックキャッシュはMCSIOと呼ばれます。詳細については、こちらのブログ記事を参照してください。

前提条件

ライトバックキャッシュを有効にするには、カタログは次の要件を満たす必要があります。

- 一時データ用のストレージを指定する接続を使用していること。詳細については、接続とリソースを参照してください。
- VDAはバージョン7.9以降であり、最新のMCSIOドライバーがインストールされている必要があります。

> **注：**
>
> このドライバーのインストールは、VDAをインストールまたはアップグレードする際のオプションです。デフォルトでは、このドライバーはインストールされません。

- ディスクキャッシュのドライブ文字割り当てを有効にするには、VMは次の追加要件を満たす必要があります。
  - オペレーティングシステム: Windows
  - VDAバージョン: 2305以降

考慮事項

- ライトバックキャッシュには、*メモリ*キャッシュと*ディスク*キャッシュがあります。デフォルトでは、接続タイプによってデフォルト値が異なります。一般的に、ほとんどの場合、デフォルト値で十分ですが、以下のために必要な領域を考慮してください。
  - Windows自体によって作成される一時データファイル（Windowsページファイルを含む）。
  - ユーザープロファイルデータ。
  - ユーザーセッションに同期されるShareFileデータ。
  - セッションユーザーによって作成またはコピーされる可能性のあるデータ、またはユーザーがセッション内にインストールする可能性のあるアプリケーション。

ストレージイメージ(/en-us/citrix-virtual-apps-desktops/2503/media/storage-temp2.png)

- ディスクキャッシュがあり、メモリキャッシュがないライトバックキャッシュの構成は削除されました。一時データのキャッシュを有効にするには、**ディスクキャッシュサイズ (GB)** と **キャッシュに割り当てられるメモリ (MB)** を選択し、メモリキャッシュに0より大きいサイズを指定することをお勧めします。一時データは最初にメモリキャッシュに書き込まれます。メモリキャッシュが構成された制限に達すると、最も古いデータは一時データキャッシュディスクに移動されます。
- メモリキャッシュは、各マシン上のメモリの総量の一部です。したがって、**メモリキャッシュサイズ (MB) (推奨)** チェックボックスを有効にする場合は、各マシン上のメモリの総量を増やすことを検討してください。
- **メモリキャッシュサイズ (MB) (推奨)** チェックボックスをオフのままにすると、一時データは、最小限のメモリを使用して、ディスクキャッシュに直接書き込まれます。
- **ディスクキャッシュサイズ (GB)** をデフォルト値から変更すると、パフォーマンスに影響を与える可能性があります。サイズは、ユーザーの要件とマシンにかかる負荷に合わせる必要があります。

> **重要:**
>
> ディスクキャッシュの容量が不足すると、ユーザーセッションは使用できなくなります。

- **ディスクキャッシュサイズ** チェックボックスをオフにすると、キャッシュディスクは作成されません。この場合、すべての一時データを保持するのに十分な大きさの **キャッシュに割り当てられるメモリ** の値を指定します。これは、各VMに割り当てるための大量のRAMが利用可能な場合にのみ実現可能です。
- 両方のチェックボックスをオフにすると、一時データはキャッシュされません。各VMの差分ディスク（OSストレージにあります）に書き込まれます。（これは、7.9より前のリリースでのプロビジョニングアクションです。）
- このカタログを使用してAppDiskを作成する予定がある場合は、キャッシュを有効にしないでください。
- マシンカタログの作成後に、キャッシュ値を変更することはできません。

NIC (NIC)

このページは、Remote PC Accessカタログを作成しているときには表示されません。

複数のNICを使用する予定がある場合は、各カードに仮想ネットワークを関連付けます。たとえば、一方のカードを特定のセキュアネットワークへのアクセスに割り当て、もう一方のカードをより一般的に使用されるネットワークへのアクセスに割り当てることができます。このページからNICを追加または削除することもできます。

マシンアカウント

このページは、Remote PC Accessカタログを作成している場合にのみ表示されます。

「**マシンアカウント**」ページで、ユーザーまたはユーザーグループに対応するActive Directoryマシンアカウントまたは組織単位 (OU) を追加するように指定します。OU名にスラッシュ (/) を使用しないでください。

OUを追加するときに、ドメインがリストに表示されない場合は、次の操作を実行できます。

- 完全一致を使用して検索します。
- すべてのドメインを参照して見つけます。

以前に構成した電源管理接続を選択するか、電源管理を使用しないことを選択できます。電源管理を使用したいが、適切な接続がまだ構成されていない場合は、後でその接続を作成し、マシンカタログを編集して電源管理設定を更新できます。

マシンID

このページは、MCSを使用してVMを作成する場合にのみ表示されます。

カタログ内の各マシンは一意のIDを持つ必要があります。このページでは、カタログ内のマシンのIDを構成できます。マシンはプロビジョニング後にIDに結合されます。カタログを作成した後でIDタイプを変更することはできません。

このページで設定を構成するための一般的なワークフローは次のとおりです。

1. リストからIDを選択します。
2. アカウントを作成するか既存のアカウントを使用するか、およびそれらのアカウントの場所（ドメイン）を指定します。

次のいずれかのオプションを選択できます。

- **オンプレミスActive Directory**。組織が所有し、その組織に属するActive Directoryアカウントでサインインするマシン。これらはオンプレミスに存在します。

- **ハイブリッドAzure Active Directory参加済み**。組織が所有し、その組織に属するActive Directory Domain Servicesアカウントでサインインするマシン。これらはクラウドとオンプレミスに存在します。要件、制限、考慮事項については、「ハイブリッドAzure Active Directory参加済み」を参照してください。

  注:

  - ハイブリッドAzure Active Directory参加を使用する前に、Azure環境が前提条件を満たしていることを確認してください。「Microsoft Entraハイブリッド参加の構成」を参照してください。
  - このオプションでは、マスターイメージがオペレーティングシステムの前提条件を満たしている必要があります。詳しくは、「Microsoft Entraハイブリッド参加済みデバイス」を参照してください。

- **ドメイン非参加**。どのドメインにも参加していないマシン。要件と制限については、「ドメイン非参加」を参照してください。

重要:

- IDの種類として**オンプレミスActive Directory**または**ハイブリッドAzure Active Directory参加済み**を選択した場合、カタログ内の各マシンには対応するActive Directoryコンピューターアカウントが必要です。
- IDタイプが**Non-domain-joined**の場合、カタログの最小機能レベルとしてVDAバージョン2311以降が必要です。利用可能にするには、最小機能レベルを更新してください。

アカウントを作成する場合、マシンが存在するOUにコンピューターアカウントを作成する権限が必要です。カタログ内の各マシンには一意の名前が必要です。作成するマシンのアカウント命名スキームを指定します。詳しくは、「マシンアカウント命名スキーム」を参照してください。

注:

OU名にスラッシュ（`/`）を使用しないようにしてください。

> 既存のアカウントを使用する場合は、アカウントを参照するか、**インポート**をクリックしてアカウント名を含む.csvファイルを指定します。インポートするファイルの内容は、次の形式を使用する必要があります。

- ADcomputeraccountname.domain

追加するすべてのマシンに対して十分なアカウントがあることを確認してください。Web Studioインターフェイスがこれらのアカウントを管理します。したがって、そのインターフェイスですべてのアカウントのパスワードをリセットできるようにするか、すべてのアカウントで同じである必要があるアカウントパスワードを指定してください。

物理マシンまたは既存のマシンを含むカタログの場合、既存のアカウントを選択またはインポートし、各マシンをActive Directoryコンピューターアカウントとユーザーアカウントの両方に割り当てます。

マシンアカウントの命名規則

カタログ内の各マシンには、一意の名前が必要です。カタログを作成する際には、マシンアカウントの命名規則を指定する必要があります。名前に表示される連番または文字のプレースホルダーとして、ワイルドカード（ハッシュマーク）を使用します。

命名規則を指定する際は、以下のルールに注意してください。

- 命名規則には少なくとも1つのワイルドカードを含める必要があります。すべてのワイルドカードはまとめて配置する必要があります。
- ワイルドカードを含む名前全体は、2文字以上15文字以下である必要があります。少なくとも1つの非数字文字と1つの#（ワイルドカード）文字を含める必要があります。
- 名前にスペースや次の文字を含めることはできません: `,~!@'$%\^&.(){}{\/*?"<>|=+[];:_".`。
- 名前をハイフン（-）で終わらせることはできません。

また、命名規則を指定する際には、拡張のための十分な余地を残してください。例を挙げます。「veryverylong#」というスキームで1,000個のマシンアカウントを作成した場合、最後に作成されるアカウント名（veryverylong1000）は16文字になります。したがって、この命名規則では、最大15文字を超えるマシン名が1つ以上生成されることになります。

シーケンシャル値が数字（0-9）か文字（A-Z）かを示すことができます。

- **0-9**。選択した場合、指定されたワイルドカードは連番に解決されます。

> **注:**
>
> ワイルドカード（#）が1つの場合、アカウント名は1から始まります。2つの場合、アカウント名は01から始まります。3つの場合、アカウント名は001から始まり、以降同様です。

- **A-Z**。選択した場合、指定されたワイルドカードは連続する文字に解決されます。

たとえば、PC-Sales-##（**0-9**を選択）という命名スキームでは、PC-Sales-01、PC-Sales-02、PC-Sales-03などのアカウント名が生成されます。

必要に応じて、アカウント名の開始文字を指定できます。

- **0-9**を選択した場合、アカウントは指定された数字から順に命名されます。前のフィールドで使用するワイルドカードの数に応じて、1桁以上の数字を入力します。たとえば、2つのワイルドカードを使用する場合は、2桁以上の数字を入力します。
- **A-Z**を選択した場合、アカウントは指定された文字から順に命名されます。前のフィールドで使用するワイルドカードの数に応じて、1文字以上の文字を入力します。たとえば、2つのワイルドカードを使用する場合は、2文字以上の文字を入力します。

ドメイン資格情報

アカウント操作を実行する権限を持つ管理者の資格情報を入力します。詳細な手順は次のとおりです。

1. をクリックします。Windowsセキュリティページが表示されます。
2. フィールドに、管理者のSamName、ユーザー名、またはユーザーSIDを入力します。
   - SamNameを入力すると、 フィールドが自動的に入力されます。
   - ユーザー名またはSIDを入力する場合、 フィールドにドメイン名またはSIDを入力することで、特定のドメインにユーザー検索を限定できます。
3. をクリックして、ユーザー名が有効または一意であるかを確認します。
4. フィールドに、管理者のドメインパスワードを入力します。
5. 「**完了**」をクリックします。

> **注:**

> 「**マシンID**」で選択したIDタイプが「**Hybrid Azure Active Directory joined**」の場合、入力する資格情報には、`Write userCertificate`権限が付与されている必要があります。

概要、名前、および説明

「**概要**」ページで、指定した設定を確認します。カタログの名前と説明を入力します。この情報はWeb Studioに表示されます。

完了したら、**「完了」をクリックしてカタログの作成を開始します。 完了したら、**「完了」**を選択してカタログの作成を開始します。

マシンカタログに、新しいカタログがインラインの進行状況バーとともに表示されます。

作成の進行状況の詳細を表示するには：

1. マシンカタログにマウスを合わせます。
2. 表示されるツールヒントで、**詳細の表示**をクリックします。

   以下の項目を確認できるステップバイステップの進行状況グラフが表示されます。

   - ステップの履歴
   - 現在のステップの進行状況と実行時間
   - 残りのステップ

MCSの時刻同期

タイム同期は、マスターイメージと、参加しているマシンIDカタログのタイプによって決定されます。マスターイメージとカタログに応じて、以下のタイム同期方法が得られます。

マスターイメージ	カタログ	結果のタイム同期方法
NDJ	ADまたはハイブリッドAzure AD	デフォルトでは、NT5DSです。マスターイメージのレジストリ設定を使用して、MCSがタイム同期設定を変更するのを無効にできます。
NDJ	NDJまたはAzure AD	元のタイム同期設定と同じ
ADまたはハイブリッドAzure AD	ADまたはハイブリッドAzure AD	元のタイム同期設定と同じ

マスターイメージ	カタログ	結果のタイム同期方法
アジュール AD	アジュール AD	元の時刻同期設定と同じ

注:

元の時刻同期は、以下のレジストリ設定によって制御されており、変更できません。

- Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Config

値: MaxAllowedPhaseOffset、MaxNegPhaseCorrection、およびMaxPosPhaseCorrection

- Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Parameters

値: Type

MCSが時刻同期設定を変更しないようにするには、マスターイメージで以下のレジストリ設定の値を設定します。

- `Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix`
- 名前：TimeSyncMethodKeep
- 種類：DWORD
- 0（または、値TimeSyncMethodKeepが構成されていない場合）：元の時刻同期設定を保持しません。
- 1：元の時刻同期設定とデフォルトのパラメーター値を保持します。

カスタムプロパティの設定に関する重要な考慮事項

GCPおよびAzure環境では、カスタムプロパティを`New-ProvScheme`と`Set-ProvScheme`で正しく設定する必要があります。存在しないカスタムプロパティを指定すると、以下のエラーメッセージが表示され、コマンドの実行に失敗します。

- Azure で: `Invalid property found: <invalid property>. Ensure that the CustomProperties parameter supports the property.`.

- GCP で: `Invalid property found: <invalid property>. Ensure that the value supplied for the property is supported in the Hypervisor.`.

トラブルシューティング

> **重要:**

> Web Studio を使用してマシンカタログを作成した後、マシンカタログ作成に関連するタスクを取得するために `Get-ProvTask` PowerShell コマンドを使用することはできません。この制限は、カタログが正常に作成されたかどうかにかかわらず、Web Studio がマシンカタログ作成後にそれらのタスクを削除するためです。

> Citrix は、サポートチームが解決策を提供できるよう、ログを収集することをお勧めします。Citrix Provisioning を使用している場合は、ログファイルを生成するために次の手順を使用してください。

1. マスターイメージで、値 1 (DWORD (32 ビット) 値として) を持つ次のレジストリキーを作成します: `HKLM\Software\Citrix\MachineIdentityServiceAgent\LOGGING`。
2. マスターイメージをシャットダウンし、スナップショットを作成します。
3. Delivery Controller で、次の PowerShell コマンドを実行します: `Set-ProvServiceConfigurationData -Name ImageManagementPrep_NoAutoShutdown -Value $True`。
4. そのスナップショットに基づいてカタログを作成します。
5. ハイパーバイザー上に準備 VM が作成されたら、ログインして C:\\ のルートから次のファイル (Image-prep.log および PvsVmAgentLog.txt) を抽出します。
6. マシンをシャットダウンすると、その時点で障害が報告されます。
7. イメージ準備マシンの自動シャットダウンを再度有効にするには、次の PowerShell コマンドを実行します: `Remove-ProvServiceConfigurationData -Name ImageManagementPrep_NoAutoShutdown`。

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

MCS I/O ライトバックキャッシュディスクに特定のドライブ文字を割り当てることができます。この実装により、使用するアプリケーションのドライブ文字と MCS I/O ライトバックキャッシュディスクのドライブ文字との間の競合を回避できます。これを行うには、PowerShell コマンドを

使用できます。サポートされているハイパーバイザーは、Azure、GCP、VMware、SCVMM、および XenServer です。

> **注:**
>
> この機能には、VDAバージョン2305以降が必要です。

制限事項

- Windowsオペレーティングシステムのみに適用可能
- ライトバックキャッシュディスクに適用可能なドライブ文字: `E` から `Z`
- Azure一時ディスクがライトバックキャッシュディスクとして使用されている場合は適用されません
- 新しいマシンカタログを作成する場合にのみ適用可能

ライトバックキャッシュディスクにドライブ文字を割り当てる

ライトバックキャッシュディスクにドライブ文字を割り当てるには:

1. **PowerShell**ウィンドウを開きます。
2. `asnp citrix*` を実行します。
3. まだ作成されていない場合は、IDプールを作成します。詳細については、「カタログの作成」を参照してください。
4. プロパティ `WriteBackCacheDriveLetter` を指定して、`New-ProvScheme` コマンドを使用してプロビジョニングスキームを作成します。例：

```
New-ProvScheme -CleanOnBoot `

-HostingUnitName "<name>" `

-IdentityPoolName $schemeName `

-ProvisioningSchemeName $schemeName `

-InitialBatchSizeHint 1 `

-UseWriteBackCache -WriteBackCacheDiskSize 127
-WriteBackCacheMemorySize 256 -WriteBackCacheDriveLetter E `
```

```
-MasterImageVM "XDHyp:\HostingUnits\<name>\image.folder\abcd-
resources.resourcegroup\MCSIOMasterVm_OsDisk_1_d3e2d6352xxxxxxxxx2130aa
145ec77.manageddisk" `

-NetworkMapping @{"0"="XDHyp:\\HostingUnits\\name\
\virtualprivatecloud.folder\\East US.region\
\virtualprivatecloud.folder\\abcd-resources.resourcegroup\\abcd-
resources-vnet.virtualprivatecloud\\default.network"} `

-ServiceOffering "XDHyp:\\HostingUnits\\<name>\\serviceoffering.folder\
\Standard_D2s_v5.serviceoffering" `

-CustomProperties '<CustomProperties xmlns="http://schemas.citrix.com/
2014/xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks"
Value="true" />

<Property xsi:type="StringProperty" Name="OsType" Value="Windows" />

<Property xsi:type="StringProperty" Name="StorageType"
Value="Premium_LRS"/>

<Property xsi:type="StringProperty" Name="PersistWBC" Value="false" />

<Property xsi:type="StringProperty" Name="PersistOsDisk"
Value="false" />

<Property xsi:type="StringProperty" Name="PersistVm" Value="false" />

<Property xsi:type="StringProperty" Name="WBCDiskStorageType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="UseTempDiskForWBC"
Value="false" />

<Property xsi:type="StringProperty" Name="ResourceGroups" Value="abcd-
group1" />

<Property xsi:type="StringProperty" Name="LicenseType"
Value="Windows_Client" />
```

```
<Property xsi:type="StringProperty" Name="SchemaVersion" Value="2" />

</CustomProperties>'
```

5. カタログの作成を完了します。

MCSマシンカタログを作成する前に構成を検証する

MCSマシンカタログを作成する前に、`New-ProvScheme`コマンドの`-validate`パラメーターを使用して構成設定を検証できます。このPowerShellコマンドをパラメーターと共に実行すると、誤ったパラメーターが使用されている場合や、パラメーターが他のパラメーターと競合している場合に、適切なエラーメッセージが表示されます。その後、エラーメッセージを使用して問題を解決し、PowerShellを使用してMCSマシンカタログを正常に作成できます。現在、この機能はAWS、Azure、GCP、およびVMwareの仮想化環境に適用できます。

注:

検証中は、実際のMCSマシンカタログを作成してはなりません。コマンドの結果を使用してエラーを修正し、その後、正常なカタログを作成する必要があります。したがって、`New-ProvScheme`コマンドを実行する際は、偽のIDプール名を使用してください。

構成を検証するには、次の手順を実行します。

1. Delivery ControllerホストからPowerShellウィンドウを開きます。
2. Citrix固有のPowerShellモジュールをロードするには、`asnp citrix*`を実行します。
3. `New-ProvScheme`コマンドを実行し、`-validate`パラメーターを使用します。コマンドが機能するように、偽のIDプール名を提供します。例：

```
$result =New-ProvScheme  -CleanOnBoot -HostingUnitName "vSanRg"
-IdentityPoolName "mptmpcatalogdemo" -InitialBatchSizeHint 1  -
MasterImageVM "XDHyp:
\HostingUnits\vSanRg\Windows19MasterImage.vm\Citrix_XD_NonMachineProfil
eWin19Machines.snapshot" -NetworkMapping @{"0"="XDHyp:
\HostingUnits\vSanRg\\VM Network.network"} -ProvisioningSchemeName
"MachineProfileW10Machines"  -Scope @()

-VMCpuCount 2  -VM
```

```
MemoryMB 6143 -MachineProfile "XDHyp:\HostingUnits\vSanRg\TRW-Win11-
tpm-BL-TEMPLATE.template" -TenancyType Shared  -FunctionalLevel "L7_20"
-Validate

$result.TerminatingError | Format-List -Property *
```

エラーメッセージ：

```
ErrorData    : {[[ValidationFailureCount, xxx], [InvalidMemoryValue,
The memory size provided 6143 must be a multiple of 4 MB and must be
greater than or equal to 4 MB.], [InconsistentGuestOsSetting, The
GuestOs setting - windows9_64Guest of the selected machine profile does
not match with the setting - windows2019srv_64Guest of master image.
Please select a machine profile that matches the GuestOs setting of the
master image.], [InconsistentVtpmSetting, The vTPM setting of the
selected machine profile does not match with the selected master image.
Please select a machine profile that matches the vTPM setting of the
master image.], [InconsistentFirmwareSetting, The firmware setting -
efi of the selected machine profile does not match with the setting -
bios of master image. Please select a machine profile that matches the
firmware setting of the master image ErrorId      : ValidationFailure

ErrorMessage : ValidationFailure

Operation    : ValidatingInputs
```

4. 構成設定を検証した後、実際のIDプール名と正しいパラメーターを使用してMCSマシンカタログを作成できます。

次のステップ

特定のクラウドサービスカタログの作成については、以下を参照してください。

- AWS カタログを作成する
- XenServerカタログを作成する
- Google Cloud Platformカタログを作成する
- Microsoft Azureカタログを作成する
- Microsoft System Center Virtual Machine Managerカタログを作成する
- Nutanixカタログを作成する

- VMwareカタログを作成する

これが最初に作成されたカタログである場合、Web Studioはデリバリーグループを作成するように案内します。

設定プロセス全体を確認するには、インストールと構成を参照してください。

Web StudioとPowerShellを使用してCitrix Provisioningカタログを作成できます。 この実装には、次の利点があります。

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

現在、この機能はAzureおよびVMwareワークロードでのみ利用可能です。ただし、VMware環境では、現在PowerShellコマンドのみを使用してカタログを作成できます。詳細については、Citrix StudioでCitrix Provisioningカタログを作成するを参照してください。

詳細情報

- 接続とリソースの作成と管理
- 異なる参加タイプのカタログを作成する
- マシンカタログを管理する

AWSカタログを作成する

マシンカタログの作成では、マシンカタログを作成するウィザードについて説明しています。以下の情報は、AWS仮想化環境に固有の詳細を扱っています。

> **注:**
>
> AWSカタログを作成する前に、AWSへの接続の作成を完了する必要があります。AWSへの接続を参照してください。

制限事項

Citrix Virtual Apps and Desktops™ 2203 LTSR以降、MCS AWSプラグインは `DescribeInstanceTypes` AWS API呼び出しを実行し、それが成功すると、MCSはAPI応答から作成されたインベントリ名を使用します。

したがって、Citrix Virtual Apps and Desktops 1912から2203以降にアップグレードする場合、AWSで `DefineInstanceType` 権限を無効にし、その後、 `Set-ProvScheme` コマンドを使用して既存のカタログを更新し、AWSの命名規則に合わせます。その後、カタログの更新が完了し、サービス提供がAWSの命名規則に一致したら、 `DescribeInstanceType` 権限を再度追加します。

イメージ準備中のネットワーク設定

イメージ準備中、元のVMに基づいて準備用仮想マシン（VM）が作成されます。この準備用VMはネットワークから切断されます。準備用VMからネットワークを切断するために、すべてのインバウンドおよびアウトバウンドトラフィックを拒否するネットワークセキュリティグループが作成されます。このネットワークセキュリティグループは永続化され、再利用されます。ネットワークセキュリティグループの名前は `Citrix.XenDesktop.IsolationGroup-GUID` で、GUIDはランダムに生成されます。

AWSテナンシーの構成

AWSは以下のテナンシーオプションを提供します。

- 共有テナンシー（デフォルトタイプ）：異なる顧客からの複数のAmazon EC2インスタンスが、同じ物理ハードウェア上に存在する可能性があります。
- 専用テナンシー：お客様のEC2インスタンスは、お客様がデプロイした他のインスタンスと同じハードウェア上でのみ実行されます。他の顧客は同じハードウェアを使用しません。

PowerShellを使用して、MCSでAWS専用ホストをプロビジョニングできます。

PowerShellを使用したAWS専用ホストテナンシーの構成

PowerShellを介してホストテナンシーが定義されたマシンカタログを作成できます。

Amazon 専用ホストは、インスタンス容量を持つ完全に専用の物理サーバーであり、既存のソケットごと、またはVMごとのソフトウェアライセンスを使用できます。

専用ホストは、インスタンスタイプに基づいて事前設定された利用率を持っています。たとえば、C4 Large インスタンスタイプの単一の割り当てられた専用ホストは、16 インスタンスの実行に制限されます。詳細については、AWS サイト を参照してください。

AWSホストへのプロビジョニングの要件は次のとおりです。

- インポートされたBYOL（bring your own license）イメージ（AMI）。専用ホストでは、既存のライセンスを使用および管理します。
- プロビジョニング要求を満たすのに十分な利用率を持つ専用ホストの割り当て。

- **自動配置**を有効にします。

PowerShell を使用して AWS の専用ホストにプロビジョニングするには、**New-ProvScheme** コマンドレットでパラメーター `TenancyType` を *Host* に設定して使用します。

詳細については、Citrix Developer Documentation を参照してください。

マシンプロファイルからマシンプロパティをキャプチャする

MCS を使用して AWS マシンをプロビジョニングするためのカタログを作成する際、マシンプロファイルを使用して特定のマシンプロパティ設定を事前設定できます。

これを行うには、次の手順に従います。

1. マシンプロファイルを、このカタログを作成するリソースと同じアベイラビリティゾーンに保存します。
2. カタログ作成ウィザードの**マシンのテンプレート**ページで、**マシンプロファイルを使用**を選択します。選択したリソースと同じアベイラビリティゾーンにあるマシンプロファイルが表示されます。
3. 必要に応じてマシンプロファイルを選択します。

AWS オペレーションリソースのタグ付け

MCS を使用して AWS でマシンをプロビジョニングするためのカタログを作成する際、IAM ロールとタグのプロパティをそれらのマシンに適用するかどうかを制御できます。また、マシンのタグをオペレーションリソースに適用するかどうかも制御できます。

Amazon マシンイメージ (AMI) は、Amazon Cloud 環境内で仮想マシンを作成するために使用される仮想アプライアンスの一種であり、一般に EC2 と呼ばれます。AMI を使用して、EC2 環境を使用するサービスを展開します。AWS 用の MCS を使用してマシンをプロビジョニングするためのカタログを作成する際、そのカタログのゴールデンイメージとして機能する **AMI** を選択します。

> **重要:**
>
> オペレーションリソースのタグ付けを使用するには、マシンプロファイルと起動テンプレートの両方を使用してカタログを作成する必要があります。

> AWS カタログを作成するには、まずゴールデンイメージとするインスタンスの AMI を作成する必要があります。MCS はそのインスタンスからタグを読み取り、起動テンプレートに組

> み込みます。その後、起動テンプレートのタグは、AWS 環境で作成されたすべての Citrix® リソースに適用されます。これには以下が含まれます。

- 仮想マシン
- VM ディスク
- VM ネットワークインターフェイス
- S3 バケット
- S3 オブジェクト
- 起動テンプレート
- AMI

Web Studio を使用したオペレーションリソースのタグ付け

MCS を使用して AWS でマシンをプロビジョニングするためのカタログを作成する際、**Machine Template** ページで **Apply machine tags to operational resources** オプションを選択することで、マシンのタグをオペレーションリソースに適用するかどうかを制御できます。

このオプションは、マシンのプロビジョニングを容易にするAWS環境で作成されたすべての項目にマシンタグを適用するかどうかを制御します。オペレーションリソースは、カタログ作成の副産物として作成されます。これらには、準備用VMインスタンスやAMIなどの一時的および永続的なリソースが含まれます。

PowerShellを使用してオペレーションリソースにタグを付ける

PowerShell を使用してリソースにタグを付けるには：

1. DDC ホストから PowerShell ウィンドウを開きます。
2. コマンド `asnp citrix` を実行して、Citrix固有のPowerShellモジュールをロードします。

プロビジョニングされた VM のリソースにタグを付けるには、カスタムプロパティ `AwsOperationalResourcesTagging` を使用します。例：

```
New-ProvScheme -ProvisioningSchemeName test

-CustomProperties “AwsOperationalResourcesTagging,true”

-MachineProfile "XDHyp:\HostingUnits\xxxx-ue1a\machineprofiletest
(lt-01xxxxx).launchtemplate\lt-01xxxxx (1).launchtemplateversion"
```

```
... <Other <standard provscheme parameters>
```

VM上のタグをコピーする

マシンプロファイルで指定されたNICおよびディスク（IDディスク、ライトバックキャッシュディスク、OSディスク）のタグを、MCSマシンカタログで新しく作成されたVMにコピーできます。これらのタグは、マシンプロファイルのソース（AWS VMインスタンスまたはAWS起動テンプレートバージョン）のいずれかで指定できます。この機能は、永続的および非永続的なマシンカタログとVMに適用されます。

注:

- AWS EC2コンソールでは、**Launch Template Version Resource Tags**の下に**Tag Network Interfaces**の値が表示されません。ただし、PowerShellコマンド `aws ec2 describe-launch-template-versions --launch-template-id lt-0bb652503d45dcbcd --versions 12` を実行してタグの仕様を確認できます。
- マシンプロファイルソース（VMまたは起動テンプレートバージョン）に2つのネットワークインターフェイス（eni-1とeni-2）があり、eni-1にタグt1、eni-2にタグt2がある場合、VMは両方のネットワークインターフェイスのタグを取得します。

マシンプロファイルを使用してカタログを作成する

マシンプロファイルを使用して、EC2インスタンス（VM）または起動テンプレートバージョンからハードウェアプロパティをキャプチャし、プロビジョニングされたマシンに適用できます。キャプチャされるプロパティには、たとえば、EBSボリュームプロパティ、インスタンスタイプ、EBS最適化、CPUオプション、テナンシータイプ、ハイバネーション機能、その他のサポートされているAWS構成が含まれます。

マシンプロファイルの入力として、AWS EC2インスタンス（VM）またはAWS起動テンプレートバージョンを使用できます。

注:

- EBSボリュームのプロパティは、マシンプロファイルからのみ派生します。

- MCSは、GP3ボリュームタイプのIDディスクを持つVMをプロビジョニングします。GP3ボリュームタイプはAWSが提供する最も安価なオプションであるため、この機能はコストを最小限に抑えます。この実装は、新しいカタログに追加されたVMと、既存のカタログに追加された新しいVMにのみ適用されます。この機能より前に作成された既存のVMは、IDディスクがリセットされない限り、GP2ボリュームタイプのIDディスクを引き続き使用します。

重要な考慮事項

MCSマシンカタログを作成する際の重要な考慮事項：

- `New-ProvScheme`および`Set-ProvScheme`コマンドでマシンハードウェアプロパティパラメータを追加すると、パラメータで指定された値がマシンプロファイルの値よりも優先されます。
- `AwsCaptureInstanceProperties`を`true`として設定し、`MachineProfile`プロパティを設定しない場合、IAMロールとタグのみがキャプチャされます。
- `AwsCaptureInstanceProperties`と`MachineProfile`を同時に設定することはできません。

> **注：**
>
> `AwsCaptureInstanceProperties` は非推奨です。

- マシンプロファイルが指定されていない場合は、次のプロパティの値を明示的に指定する必要があります。
  - セキュリティグループ
  - ENI または仮想ネットワーク
- `AwsOperationalResourcesTagging` は、`AwsCaptureInstanceProperties` を有効にするか、マシンプロファイルを指定した場合にのみ有効にできます。

MCSマシンカタログ作成後の重要な考慮事項：

- マシンプロファイルベースのカタログを、マシンプロファイルベースではないカタログに変更することはできません。

マシンプロファイルを使用してマシンカタログを作成する

マシンプロファイルを使用してマシンカタログを作成するには：

1. **PowerShell** ウィンドウを開きます。
2. Citrix固有のPowerShellモジュールをロードするために`asnp citrix*`を実行します。
3. まだ作成されていない場合は、IDプールを作成します。例：

```
New-AcctIdentityPool -IdentityPoolName idPool -NamingScheme ms##
-Domain abcdf -NamingSchemeType Numeric
```

4. New-ProvSchemeコマンドを実行します。例：

```
New-ProvScheme -ProvisioningSchemeName demet-test-1

-HostingUnitUid aa633238-9xxd-4cf6-80e8-232a758a1xx1

-IdentityPoolUid 34d5b088-e312-416f-907d-16573xxxxxc4

-CleanOnBoot

-MasterImageVM 'XDHyp:\HostingUnits\cvad-test-scalestress\citrix-demet-
ami.0 (ami-0ca813xxxxxx061ef).template'

-MachineProfile 'XdHyp:\HostingUnits\cvad-test-scalestress\us-
east-1a.availabilityzone\machine-profile-instance i (i-0xxxxxxxx).vm'
```

5. カタログの作成を完了します。詳細については、Citrix PowerShell SDKを参照してください。

マシンプロファイルを更新する

マシンプロファイルで最初にプロビジョニングされたカタログのマシンプロファイルを更新するには、次の手順を実行します。MCSマシンカタログを編集する際に、マシンプロファイルソースのテナンシータイプとハイバネーション機能を変更することもできます。

1. `Set-ProvScheme`コマンドを実行します。例：

```
Set-ProvScheme `

-ProvisioningSchemeUid "<ID" `

-MachineProfile "XDHyp:\HostingUnits\abc\us-
```

```
east-1a.availabilityzone\citrix-cvad-machineprofile-instance
(i-0xxxxxxxx).vm"
```

起動テンプレートバージョンでカタログを作成する

起動テンプレートバージョンをマシンプロファイルの入力として使用して、MCSマシンカタログを作成できます。また、マシンプロファイルカタログの入力をVMから起動テンプレートバージョンに、または起動テンプレートバージョンからVMに更新することもできます。

AWS EC2コンソールでは、起動テンプレートのインスタンス構成情報をバージョン番号とともに提供できます。マシンカタログの作成または更新時に起動テンプレートバージョンをマシンプロファイルの入力として指定すると、そのバージョンの起動テンプレートのプロパティがプロビジョニングされたVDA VMにコピーされます。

以下のプロパティは、マシンプロファイルの入力として、または`New-ProvScheme`または`Set-ProvScheme`コマンドのパラメーターとして明示的に指定できます。`New-ProvScheme`または`Set-ProvScheme`コマンドで指定された場合、これらのプロパティのマシンプロファイル値よりも優先されます。

- サービスオファリング
- ネットワーク
- セキュリティグループ
- テナンシータイプ

注:

マシンプロファイルの起動テンプレートでサービス提供が指定されていない場合、または`New-ProvScheme`コマンドのパラメータとして指定されていない場合、適切なエラーが発生します。

マシンプロファイルの入力として起動テンプレートバージョンを使用してカタログを作成するには:

1. **PowerShell**ウィンドウを開きます。
2. Citrix固有のPowerShellモジュールをロードするために`asnp citrix*`を実行します。
3. 起動テンプレートの起動テンプレートバージョンの一覧を取得します。例:

```
XDHyp:\HostingUnits\test\test-mp-sard (lt-01xxxxx).launchtemplate> ls |
Select FullPath
```

4. 作成されていない場合は、IDプールを作成します。例:

```
New-AcctIdentityPool `

-IdentityPoolName "abc11" `

-NamingScheme "abc1-##" `

-NamingSchemeType Numeric `

-Domain "citrix-xxxxxx.local" `

-ZoneUid "xxxxxxxx" `
```

5. マシンプロファイルの入力として起動テンプレートバージョンを使用してプロビジョニングスキームを作成します。例:

```
New-ProvScheme `

-ProvisioningSchemeName "MPLT1" `

-HostingUnitUid "c7f71f6a-3f45-4xxx-xxxx-xxxxxxxxxx" `

-IdentityPoolUid "bf3a6ba2-1f80-4xxx-xxxx-xxxxxxxxx" `

-MasterImageVM "XDHyp:\HostingUnits\xxxd-ue1a\apollo-non-persistent-
vda-win2022 (ami-0axxxxxxxxxx).template" `

-CleanOnBoot `

-MachineProfile "XDHyp:\HostingUnits\xxxx-ue1a\machineprofiletest
(lt-01xxxxx).launchtemplate\lt-01xxxxx (1).launchtemplateversion"
```

6. プロビジョニングスキームをブローカーカタログとして登録します。例：

```
New-BrokerCatalog -Name "MPLT1" `

-AllocationType Random `

-Description "Machine profile catalog" `

-ProvisioningSchemeId fe7df345-244e-4xxxx-xxxxxxxxx `

-ProvisioningType Mcs `

-SessionSupport MultiSession `

-PersistUserChanges Discard
```

7. カタログの作成を完了します。詳細については、Citrix PowerShell SDKを参照してください。

マシンプロファイルカタログの入力を、VMから起動テンプレートバージョンへ、または起動テンプレートバージョンからVMへ更新することもできます。例:

- マシンプロファイルカタログの入力をVMから起動テンプレートバージョンに更新するには:

```
Set-ProvScheme -ProvisioningSchemeName "CloudServiceOfferingTest" `

-MachineProfile "XDHyp:\HostingUnits\xxxx-ue1a\machineprofiletest
(lt-0bxxxxxxxxxxxx).launchtemplate\lt-0bxxxxxxxxxxxx
(1).launchtemplateversion"
```

- マシンプロファイルカタログの入力を起動テンプレートバージョンからVMに更新するには:

```
Set-ProvScheme -ProvisioningSchemeName "CloudServiceOfferingTest" `

-MachineProfile "XDHyp:\HostingUnits\sard-ue1a\us-
east-1a.availabilityzone\apollo-non-persistent-vda-win2022-2
(i-08xxxxxxxx).vm"
```

MCSIO対応カタログ

MCS Storage Optimization (MCSIO) は、ディスク操作をメモリまたは小型の高速ディスクにキャッシュすることで、VMのパフォーマンスを向上させます。PowerShellコマンドを使用して、MCSIO対応の非永続カタログを作成できます。このようなカタログを作成するには、AMIインス

タンスの準備中にVDAをインストールまたはアップグレードする際に、MCSIOドライバーをインストールする必要があります。デフォルトでは、このドライバーはインストールされていません。

MCSIO AMIが準備されたら、MCSIO対応の非永続カタログを作成できます。

MCSIO対応カタログの作成

New-ProvScheme PowerShellコマンドに追加される4つのパラメーターは次のとおりです。

- `UseWriteBackCache`: 指定されたプロビジョニングスキームに対してキャッシュ（ライトバックキャッシュ）を有効にします
- `WriteBackCacheDiskSize`: キャッシュに使用される一時ディスクのGB単位のサイズを指定します
- `WriteBackCacheMemorySize`: キャッシュに使用するMB単位のメモリ量を指定します。これはオプションのパラメーターです。
- `WriteBackCacheDriverLetter`: キャッシュストレージディスクに割り当てるドライブ文字を指定します。これはオプションのパラメーターです。

> **注:**
>
> - 少なくとも1 GBのキャッシュディスクストレージが必要なため、`WriteBackCacheDiskSize`の値はゼロより大きくする必要があります。キャッシュディスクサイズはOSディスクサイズより大きくしてはいけません。
> - `WriteBackCacheMemorySize`の値はゼロ以外で、マシンカタログのメモリサイズよりも小さくする必要があります。

MCSIOに影響するカスタムプロパティは次のとおりです。

- `WBCDiskStorageType`: AWSで一時ディスクに使用されるボリュームタイプを定義します。このパラメーターは、`volume-type[:iops][:throughput]`の形式で文字列引数を取ります。ボリュームタイプは次のとおりです。
  - gp2: このボリュームタイプにはiopsおよびスループットパラメータを使用しないでください。
  - gp3: このボリュームタイプにはiopsおよびスループットパラメータを使用してください。
  - io1: このボリュームタイプにはiopsパラメータのみを使用してください。
  - io2: このボリュームタイプにはiopsパラメータのみを使用してください。

デフォルトのボリュームタイプは **gp2** です。

- `PersistWBC`: AWSインスタンスの電源がオフになったときに、キャッシュディスクを保持するか破棄するかを制御します。`true`に設定すると、キャッシュディスクは保持されます。`false`（デフォルト）に設定すると、キャッシュディスクはAMIインスタンスの電源がオンになっている間のみ作成および保持されます。
- `PersistOSDisk`: AWSインスタンスの電源がオフになったときに、OSディスクを保持するか破棄するかを制御します。`true`に設定すると、OSディスクは保持されます。`false`（デフォルト）に設定すると、OSディスクはAMIインスタンスの電源がオンになっている間のみ作成および保持されます。

MCSIOが有効な非永続カタログを作成するには、PowerShellウィンドウで次の手順を実行します。

1. PowerShellウィンドウを開きます。
2. Citrix固有のPowerShellモジュールをロードするために`asnp citrix*`を実行します。
3. ブローカーカタログとIDプールを作成します。
4. プロビジョニングスキームを作成します。例：

```
$HostingUnitUid = '0xxxx1d9-bbfc-xxxf-bxxb-exxxxxe008b2'

$MasterImageVM = 'XDHyp:\HostingUnits\ctx-test\aws-apollo-non-
persistent-multi-mcsio-vda-win2022 (ami-0bf1810488acbxxxb).template'

$NetworkMap = @{ 'NetworkPath' = 'XDHyp:\HostingUnits\ctx-test\us-
east-1a.availabilityzone\10.0.128.0`/17
(vpc-0fa6e41d72507fxxx).network' }

$SecurityGroup = $( 'XDHyp:\HostingUnits\ctx-test\us-
east-1a.availabilityzone\private.securitygroup' )

$ServiceOffering = 'XDHyp:\HostingUnits\ctx-test\T3 Medium
Instance.serviceoffering'

$CustomProperties = 'WBCDiskStorageType,gp3:6000:250;PersistWBC,false'




$provScheme = New-ProvScheme -ProvisioningSchemeName $CatalogName
```

```
-HostingUnitUid $HostingUnitUid `

-IdentityPoolUid $acctPool.IdentityPoolUid -CleanOnBoot `

- MasterImageVM $MasterImageVM `

-NetworkMap $NetworkMap `

-ServiceOffering $ServiceOffering `

-SecurityGroup $SecurityGroup `

-CustomProperties $CustomProperties `

-UseWriteBackCache -WriteBackCacheDiskSize 16 -WriteBackCacheMemorySize
256
```

5. カタログにVMを追加します。

MCSIOで起動パフォーマンスを向上させる

MCSIOを有効にし、`PersistWBC`と`PersistOSDisk`のカスタムプロパティを`true`として設定すると、VMの起動パフォーマンスを向上させることができます。この設定により、VMは新しいキャッシュディスクを初期化したり、テンプレートからルートディスクを再作成したりする必要がないため、より高速に起動できます。

OS、ID、およびWBCディスクを暗号化する

OSディスク、IDディスク（ID）、およびライトバックキャッシュディスク（WBC）の暗号化に使用できるAWS KMSキー（カスタマーマネージドキーおよびAWSマネージドキー）を使用して、永続および非永続VMカタログを作成できます。

- AWSマネージドキーは毎年自動的にローテーションされます。
- カスタマーマネージドキーは自動ローテーションのオプションであり、手動で管理できます。

KMSキーの詳細については、以下のAWSドキュメントを参照してください。

- AWS KMSの概念
- 自動キーローテーションの仕組み

OS、ID、およびWBCディスクの暗号化には、次のいずれかを構成します。

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

制限事項

次の制限事項を考慮してください。

- MCSは現在、マスターイメージAMI上のディスクを1つのみサポートしています。
- 既存の暗号化されていないEBSボリュームまたはスナップショットを直接暗号化したり、既存の暗号化されたボリュームのKMSキーを変更したりすることはできません。これを行うには、次の手順を実行する必要があります。

  a. そのボリュームの新しいスナップショットを作成します。

  b. そのスナップショットから新しいボリュームを作成します。

  c. 新しいボリュームを暗号化します。

以下の AWS ドキュメントを参照してください。

- 暗号化されていないリソースを暗号化する
- EBSボリュームの自動またはデフォルト暗号化の制限：既存および新規のAmazon EBSボリュームを自動的に暗号化する。

ディスク暗号化を使用してカタログを作成する

ディスク暗号化を使用して MCS マシンカタログを作成するには、次の方法があります。

- マスターイメージ
- マシンプロファイル

マシンプロファイル入力を使用する際の考慮事項は次のとおりです。

- マシンプロファイル入力のKMSキーは、マスターイメージのKMSキーよりも優先されます。
- マシンプロファイル入力が提供されない場合、マスターイメージAMIのKMSキーがカタログVMのディスクを暗号化するために使用されます。
- マシンプロファイルにブロックデバイスマッピングが存在する場合、マスターイメージテンプレート（AMI）とマシンプロファイルに存在するブロックデバイスは一致する必要があります。たとえば、AMIに`/dev/sda1`で定義されたデバイスがある場合、マシンプロファイルにも`/dev/sda1`で定義されたデバイスが必要です。

- マシンプロファイルソースにキーがなく、マスターイメージが暗号化されていない場合、カタログVMのディスクは暗号化されません。
- マスターイメージが暗号化されている場合、マシンプロファイルソースVMまたは起動テンプレートには、有効な入力と見なされるために暗号化されたルートボリュームが必要です。

既存のカタログを変更する

`Set-ProvScheme` PowerShellコマンドを使用して、既存のカタログを次のように変更できます。

- 新しいKMSキーを含むボリュームを持つマシンプロファイル入力。
- 新しいKMSキーで暗号化されたマスターイメージテンプレートAMI。

重要な考慮事項：

- カタログに追加された新しいVMのボリュームは、新しいKMSキーで暗号化されます。
- 既存のマシンプロファイルがある場合に暗号化設定を更新するには、新しいマシンプロファイルで`Set-ProvScheme`を実行します。
- 既存のカタログを、暗号化されたボリュームから暗号化されていないボリュームに変更することはできません。 暗号化されたマスターAMIから暗号化されていないマスターAMIへのイメージ更新はできません。

VMインスタンスでNitroTPMとUEFIセキュアブートを有効にする

カタログを作成する際、NitroTPMおよび/またはUEFIセキュアブートが有効なマスターイメージ(AMI) を選択できるようになりました。これにより、カタログ内のプロビジョニングされたVMもNitroTPMおよび/またはUEFIセキュアブートが有効になります。この実装により、VMが保護され、信頼できるものになります。NitroTPMおよびUEFIセキュアブートの詳細については、Amazonドキュメントを参照してください。

制限事項

- 現在、中国を除くすべてのAWSリージョン（AWS GovCloud (US) リージョンを含む）で、NitroTPMとセキュアブートの両方を使用できます。
- 既存のカタログでNitroTPMとUEFIセキュアブートを有効にすることはできません。NitroTPMとUEFIセキュアブートが有効なカタログが必要な場合は、新しいカタログを作成してください。

主な手順

1. AWS環境をセットアップします。
2. AWSへの接続を作成します。

3. NitroTPMおよび/またはUEFIセキュアブートが有効なマスターイメージ (AMI) を作成します (#create-an-ami-that-supports-nitrotpm-and-uefi-secure-boot)。
4. Web StudioのカタログメニューでNitroTPMとUEFIセキュアブートが有効なマスターイメージを選択するか、PowerShellコマンドを使用してプロビジョニングスキームを作成することで、マシンカタログを作成します。

作成されたカタログに追加されたVMは、NitroTPMとUEFIセキュアブートが有効になっています。

NitroTPMとUEFIセキュアブートをサポートするAMIを作成する

1. NitroTPMおよび/またはUEFIセキュアブートが有効なVMからAMIを作成できます。
   a. AWS Marketplaceイメージを使用してインスタンスを作成します。例: `TPM-Windows_Server-2022-English-Full-Base on the aws-marketplace`を検索します。
   b. シングルセッションまたはマルチセッションVDAをダウンロードします。
   c. そのVMからAMIを作成します。
2. register-image コマンドを使用します:

```
--boot-mode (string)

--tpm-support (string)
```

   詳しくは、register-imageを参照してください。

以下の AWS ドキュメントを参照してください。

- EC2インスタンスタイプのサポートされているブートモードを決定する
- Amazon EC2インスタンスでNitroTPMを使用するための要件/。

Delivery Controller™ ホストからPowerShellウィンドウを開き、特定の項目を確認できます:

- サービスオファリングがNitroTPMまたはUEFIセキュアブートをサポートしているか

```
(Get-Item -Path “XDHyp:\HostingUnits\aws\T3 Medium
Instance.serviceoffering”).AdditionalData.BootMode

(Get-Item -Path “XDHyp:\HostingUnits\aws\T3 Medium
Instance.serviceoffering”).AdditionalData.NitroTpmSupportVersions
```

- テンプレートがNitroTPMまたはUEFIセキュアブートをサポートしているか

```
(Get-HypInventoryItem -LiteralPath “XDHyp:\HostingUnits\aws”
-ResourceType “template -Id “ID”).AdditionalData.BootMode



(Get-HypInventoryItem -LiteralPath “XDHyp:\HostingUnits\aws”
-ResourceType “template -Id “ID”).AdditionalData.TpmSupport
```

既存のカタログのサービスオファリングを更新する

`Set-ProvScheme`を使用して、既存のカタログのサービスオファリングを変更できます。この変更は、新しく追加されたVMに適用されます。ただし、以下のシナリオではエラーが発生します:

AMIのブートモード	AMIはNITRO TPMをサポートしていますか？	サービスオファリングはNITROTPMとUEFIセキュアブートをサポートしていますか？
UEFI	いいえ	いいえ
レガシーBIOS	はい	いいえ
UEFI	はい	いいえ
UEFI優先	はい	いいえ

VMインスタンスをフィルタリングする

マシンプロファイルVMとして使用するAWS EC2インスタンスは、マシンカタログが正しく作成され機能するために互換性がある必要があります。マシンプロファイルの入力VMとして使用できるAWS EC2インスタンスを一覧表示するには、`Get-HypInventoryItem`コマンドを使用します。このコマンドは、ホスティングユニットで利用可能なVMのインベントリをページングおよびフィルタリングできます。

ページネーション:

Get-HypInventoryItemは、2つのページネーションモードをサポートしています。

- ページングモードでは、`-MaxRecords`と`-Skip`パラメーターを使用してアイテムのセットを返します。
    - `-MaxRecords`: デフォルトは**1**です。これは、返されるアイテムの数を制御します。

  - `-Skip`: デフォルトは**0**です。これは、ハイパーバイザー内のリストの絶対的な先頭（または絶対的な末尾）からスキップするアイテムの数を制御します。

- スクロールモードでは、`-MaxRecords`、`-ForwardDirection`、および`-ContinuationToken`パラメーターを使用してレコードのスクロールを可能にします。

  - `-ForwardDirection`: デフォルトは**True**です。これは`-MaxRecords`と組み合わせて使用され、一致するレコードの次のセットまたは前のセットのいずれかを返します。
  - `-ContinuationToken`: `ContinuationToken`で指定されたアイテムを含まず、その直後（`ForwardDirection`が**false**の場合は直前）のアイテムを返します。

ページネーションの例:

- 最も名前の小さいマシンテンプレートの単一レコードを返します。`AdditionalData`フィールドには`TotalItemsCount`と`TotalFilteredItemsCount`があります。

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template
```

- 最も名前の小さいマシンテンプレートのレコードを10件返します。

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template -MaxRecords 10 | select Name
```

- 最も名前の大きいレコードで終わるレコードの配列を返します。

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template -ForwardDirection $False -MaxRecords 10 | select
Name
```

- 指定された`ContinuationToken`に関連付けられたマシンテンプレートから始まるレコードの配列を返します。

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template -ContinuationToken "ami-07xxxxxxxxx"
-MaxRecords 10
```

フィルタリング:

フィルタリングには、以下の追加のオプションパラメーターがサポートされています。これらのパラメーターは、ページネーションオプションと組み合わせることができます。

- `-ContainsName "my_name"`: 指定された文字列がAMI名の一部と一致する場合、そのAMIは `Get` の結果に含まれます。例:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template -MaxRecords 100 -ContainName ‘apollo’ | select
Name
```

- `-Tags '{ "Key0": "Value0", "Key1": "Value1", "Key2": "Value2" }'`: AMIがこれらのタグの少なくとも1つを持っている場合、そのAMIは `Get` の結果に含まれます。例:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template -MaxRecords 100 -Tags '{"opex owner": "Not
tagged"}' | select Name
```

> **注:**
>
> 2つのタグ値がサポートされています。「**Not Tagged**」タグ値は、タグのリストに指定されたタグがない項目と一致します。「**All values**」タグ値は、タグの値に関係なくタグを持つ項目と一致します。それ以外の場合、一致は、項目がタグを持ち、その値がフィルターで指定された値と等しい場合にのみ発生します。

- `-Id "ami-0a2d913927e0352f3"`: AMIが指定されたIDと一致する場合、そのAMIは `Get` の結果に含まれます。例:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
-ResourceType template -Id ami-xxxxxxxxxxxx
```

AdditionalData パラメーターでのフィルタリング:

`AdditionalData` フィルターパラメーターは、テンプレートまたはVMを、その機能、サービス提供、またはAdditionalDataにある任意のプロパティに基づいてリストします。例:

```
(Get-HypInventoryItem -ResourceType "launchtemplateversion" -LiteralPath
"XDHyp:\HostingUnits\aws" -MaxRecords 200).AdditionalData
```

互換性のないVMを示すために、`-Warn` パラメーターを追加することもできます。VMは、**Warning** という名前の `AdditionalData` フィールドとともに含まれます。例:

```
(Get-HypInventoryItem -ResourceType "launchtemplateversion" -LiteralPath
"XDHyp:\HostingUnits\aws" -MaxRecords 200 -Template "ami-015xxxxxxxx"
-Warn $true).AdditionalData
```

VMのバックアップSKUリスト

パブリッククラウドでは、特定のEC2インスタンスタイプ（**プライマリSKU**）の容量が不足することがあります。プライマリVM構成が利用できない場合、VMを起動できず、時間の損失やビジネスの中断につながります。このようなシナリオに対処するため、容量関連の問題が発生した場合にMCSがフォールバックできるバックアップEC2インスタンスタイプ（**バックアップSKU**）のリストを提供します。

MCSマシンカタログの作成または更新時に、カスタムプロパティ `BackupVmConfiguration` を使用して、バックアップEC2インスタンスタイプ（**バックアップSKUリスト**）のリストを提供します。

プライマリEC2インスタンスが失敗した場合、MCSは指定された順序でバックアップEC2インスタンスタイプへのフォールバックを試行します。MCSが提供されたバックアップEC2インスタンスタイプのいずれにもフォールバックできない場合、エラーメッセージが表示されます。その後、プライマリEC2インスタンスの電源を再度オンにしてみてください。これが失敗した場合、MCSはバックアップEC2インスタンスタイプを再試行します。

バックアップSKUリストには、オンデマンドインスタンスを含めることができます。

この機能は、永続的および非永続的なMCSマシンカタログの両方に適用できます。

重要な考慮事項

- バックアップSKUリストには、複数のバックアップEC2インスタンスタイプを指定できます。
- バックアップSKUリストは一意である必要があります。
- バックアップEC2インスタンスは、プライマリEC2インスタンスと同じにすることはできません。
- バックアップEC2インスタンスは、有効なAWSインスタンスタイプである必要があります。
- 重複するサービスオファリングを指定しないでください。例: `BackupVmConfiguration,t2.small|t3.small|t2.small` は無効です。

- リストで指定されたサービスオファリングは、マシンカタログ構成と互換性がある必要があります。たとえば、カタログがUEFIを使用しており、バックアップリストで指定されたサービスオファリングがそれをサポートしていない場合、カタログの作成または更新はプレフライト中に失敗します。
- 既存のカタログのバックアップSKUリストは、`Set-ProvScheme` PowerShellコマンドを使用して変更できます。既存のVMは、`Set-ProvVM` および `Set-ProvVMUpdateTimeWindow` PowerShellコマンドを使用して変更できます。

バックアップ EC2 インスタンスを構成する

1. PowerShell ウィンドウを開きます。
2. Citrix固有のPowerShellモジュールをロードするために`asnp citrix*`を実行します。
3. ブローカーカタログを作成します。
4. IDプールを作成します。
5. カスタムプロパティ`BackupVmConfiguration`を使用してバックアップEC2インスタンスリストを追加し、プロビジョニングスキームを作成します。例：

```
$serviceOffering = "XDHyp:\HostingUnits\$hostingUnitName\T3 Medium
Instance.serviceoffering"

$customProperties =
"AwsCaptureInstanceProperties,false;AwsOperationalResourcesTagging,fals
e;BackupVmConfiguration,t2.small|t2.large|t3.small|t3.large;"

$createdProvScheme = New-ProvScheme -ProvisioningSchemeName
$provisioningSchemeName -HostingUnitName $hostingUnitName
-IdentityPoolName $provisioningSchemeName -NetworkMapping
$networkMapping -SecurityGroup $securityGroupPath -ServiceOffering
$serviceOffering -MasterImageVM $masterImageVm -CustomProperties
$customProperties
```

6. プロビジョニングスキームの一意の ID で BrokerCatalog を更新します。
7. カタログにVMを作成して追加します。

次のステップ

- これが最初に作成されたカタログである場合、Web Studioはデリバリーグループの作成を案内します。
- 構成プロセス全体を確認するには、インストールと構成を参照してください。

- カタログを管理するには、マシンカタログの管理およびAWSカタログの管理を参照してください。

詳細情報

- 接続とリソースの作成および管理
- AWSへの接続
- マシンカタログの作成

XenServer®カタログを作成する

マシンカタログの作成では、マシンカタログを作成するウィザードについて説明します。以下の情報は、XenServer仮想化環境に固有の詳細を扱います。

> **注:**
>
> XenServerカタログを作成する前に、XenServerへの接続の作成を完了する必要があります。XenServerへの接続を参照してください。

XenServer接続を使用してマシンカタログを作成する

GPU対応マシンには専用のマスターイメージが必要です。これらのVMには、GPUをサポートするビデオカードドライバーが必要です。GPU対応マシンを構成して、GPUを操作に使用するソフトウェアでVMが動作できるようにします。

1. XenCenter®で、標準VGA、ネットワーク、およびvCPUを備えたVMを作成します。
2. VM構成を更新してGPUの使用を有効にします（パススルーまたはvGPUのいずれか）。
3. サポートされているオペレーティングシステムをインストールし、RDPを有効にします。
4. Citrix VM ToolsおよびNVIDIAドライバーをインストールします。
5. Virtual Network Computing (VNC) 管理コンソールをクリアしてパフォーマンスを最適化し、VMを再起動します。
6. RDPを使用するように求められます。RDPを使用してVDAをインストールし、VMを再起動します。
7. 必要に応じて、他のGPUマスターイメージのベースラインテンプレートとしてVMのスナップショットを作成します。
8. RDPを使用して、XenCenterで構成され、GPU機能を使用する顧客固有のアプリケーションをインストールします。

制限事項

- Citrix Hypervisor 8.2 Cumulative Update 1上にVMがホストされているCitrix Virtual Apps and Desktops展開で、単一のMCSカタログに複数のGFS2 SRを使用している場合、カタログ内のVMは展開中にVDIにアクセスできません。「VDI is currently in use」というエラーが報告されます。
- Citrix Hypervisor 8.2 Cumulative Update 1は、GFS2 SRを使用したMCSフルクローンVMをサポートしていません。

詳細については、「Constraints」を参照してください。

これらの制約は、XenServer 8 以降には適用されません。

マシンプロファイルを使用してマシンカタログを作成する

MCSを使用してマシンをプロビジョニングするためのカタログを作成する際、マシンプロファイルを使用して仮想マシンからハードウェアプロパティをキャプチャし、カタログ内の新しくプロビジョニングされたVMに適用できます。`MachineProfile`パラメーターが使用されていない場合、ハードウェアプロパティはマスターイメージVMまたはスナップショットからキャプチャされます。

> **注:**
>
> 現在、マシンプロファイルの入力としてVMのみを使用できます。

> MCSIO が有効になっている場合、MCS カタログの作成後にメモリとディスクキャッシュのサイズを更新できます。マシンプロファイル入力のパラメーターの値を上書きするために、次のパラメーターを明示的に構成できます。

- `VMCpuCount`
- `VMMemory`
- `NetworkMapping`

マシンプロファイルを使用してカタログを作成するには：

1. PowerShellウィンドウを開きます。
2. `asnp citrix*`を実行します。
3. ID プールを作成します。ID プールは、作成する VM の Active Directory (AD) アカウントのコンテナです。例：

```
New-AcctIdentityPool -Domain "citrix-xxxxxx.local" -IdentityPoolName
"ExampleIdentityPool" -NamingScheme "abc1-##" -NamingSchemeType
"Numeric" -Scope @() -ZoneUid "xxxxxxxx"
```

4. 必要なADコンピューターアカウントをActive Directoryに作成します。

```
$password = "password123" | ConvertTo-SecureString -AsPlainText -Force

New-AcctIdentity -IdentityPoolName "ExampleIdentityPool" -Count 10
-ADUserName "citrix-xxxxxx\admin1" -ADPassword $password

Set-AcctAdAccountUserCert -IdentityPoolName "ExampleIdentityPool"
-ADUserName "citrix-xxxxxx\admin1" -ADPassword $password
```

5. カタログを作成するには、`New-ProvScheme`コマンドを実行します。例:

```
New-ProvScheme -CleanOnBoot -HostingUnitName "ExampleHostingUnit"
-IdentityPoolName "ExampleIdentityPool" -InitialBatchSizeHint 2
-CustomProperties '<CustomProperties xmlns="http://schemas.citrix.com/
2014/xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks"
Value="true" />

</CustomProperties>'

-MasterImageVM "XDHyp:
\HostingUnits\ExampleHostingUnit\ExampleVDA.vm\ExampleVDA.snapshot"
-ProvisioningSchemeName "ExampleCatalog" -Scope @() -SecurityGroup @()

-MachineProfile "XDHyp:
\HostingUnits\ExampleHostingUnit\ExampleMachineProfile.vm"
```

6. プロビジョニングスキームをブローカーカタログとして登録します。例：

```
$ConfigZone = Get-ConfigZone | Where-Object { $_.Name -eq "xxxxxx" }

New-BrokerCatalog -Name "MPLT1" -AllocationType Random -Description
"Machine profile catalog" -ProvisioningSchemeId fe7df345-244e-4xxxx-
```

```
xxxxxxxxx -ProvisioningType Mcs -SessionSupport MultiSession
-PersistUserChanges Discard -ZoneUid ($ConfigZone.Uid)
```

7. カタログにVMを追加します。

新しいマシンプロファイルでカタログを更新するには：

1. `Set-ProvScheme`コマンドを実行します。例：

```
Set-ProvScheme -ProvisioningSchemeName "ExampleCatalog" -MachineProfile
"XDHyp:
\HostingUnits\ExampleHostingUnit\ExampleMachineProfileVm.vm\ExampleMach
ineProfileSnapshot.snapshot"
```

   Set-ProvSchemeコマンドの詳細については、「Set-ProvScheme」を参照してください。

注:

- この場合、`Set-ProvScheme` コマンドはカタログ内の既存の VM のマシンプロファイルを変更しません。カタログに追加された新しく作成された VM のみが新しいマシンプロファイルを持ちます。
- マシンプロファイルベースのマシンカタログを、非マシンプロファイルベースのマシンカタログに変換することはできません。

次のステップ

- これが最初に作成されたカタログである場合、Web Studioはデリバリーグループの作成を案内します。
- 構成プロセス全体を確認するには、「インストールと構成」を参照してください。
- カタログを管理するには、「マシンカタログの管理」および「XenServerカタログの管理」を参照してください。

詳細情報

- 接続とリソースの作成および管理
- XenServerへの接続
- マシンカタログの作成

Google Cloud Platformカタログを作成する

「(/ja-jp/citrix-virtual-apps-desktops/2503/install-configure/machine-catalogs-create.html)」では、マシンカタログを作成するウィザードについて説明します。以下の情報は、Google Cloud環境に固有の詳細を扱っています。

> **注:**
>
> Google Cloud Platform (GCP) カタログを作成する前に、GCPへの接続の作成を完了する必要があります。「(/ja-jp/citrix-virtual-apps-desktops/2503/install-configure/connections/connection-gcp.html)」を参照してください。

マスターVMインスタンスと永続ディスクを準備する

> **ヒント:**
>
> 永続ディスクは、仮想ディスクを指すGoogle Cloudの用語です。

> マスターVMインスタンスを準備するには、計画しているマシンカタログ内のクローンVDAインスタンスに求める構成と一致するプロパティを持つVMインスタンスを作成および構成します。この構成は、インスタンスのサイズとタイプにのみ適用されるわけではありません。メタデータ、タグ、GPU割り当て、ネットワークタグ、サービスアカウントのプロパティなどのインスタンス属性も含まれます。

マスタリングプロセスの一環として、MCSはマスターVMインスタンスを使用してGoogle Cloudの*インスタンステンプレート*を作成します。このインスタンステンプレートは、マシンカタログを構成するクローンVDAインスタンスの作成に使用されます。クローンインスタンスは、インスタンステンプレートが作成されたマスターVMインスタンスのプロパティ（VPC、サブネット、永続ディスクのプロパティを除く）を継承します。

マスターVMインスタンスのプロパティを特定の要件に合わせて構成したら、インスタンスを起動し、そのインスタンスの永続ディスクを準備します。

ディスクのスナップショットまたはディスクのイメージを手動で作成することをお勧めします。これにより、意味のある命名規則を使用してバージョンを追跡し、マスターイメージの以前のバージョンを管理するためのより多くのオプションが得られ、マシンカタログ作成の時間を節約できます。独自のスナップショットを作成しない場合、MCSは一時的なスナップショットを作成しま

す（これはプロビジョニングプロセスの終了時に削除されます）。OSディスクまたはイメージのマルチリージョンスナップショットを手動で作成すると、異なるGCPリージョンのマシンカタログに同じマスターイメージを使用することもできます。

マシンカタログを作成する

マシンカタログは、次の2つの方法で作成できます。

- 「(#create-a-machine-catalog-using-web-studio)」
- 「(#create-a-machine-catalog-using-powershell)」

Web Studio を使用してマシンカタログを作成する

> **注:**
>
> マシンカタログを作成する前に、リソースを作成してください。マシンカタログを構成する際は、Google Cloud で確立された命名規則を使用してください。詳細については、「バケットとオブジェクトの命名ガイドライン」を参照してください。

(/ja-jp/citrix-virtual-apps-desktops/2503/install-configure/machine-catalogs-create.html)のガイダンスに従ってください。以下の説明は、Google Cloud カタログに固有のものです。

1. Web Studio にサインインし、左側のペインで を選択します。
2. アクションバーで を選択します。
3. ページで、 を選択し、 を選択します。
    - Citrix Virtual Apps and Desktops™ は、シングルセッションOSもサポートしています。
4. ページで、 と オプションを選択し、 を選択します。複数のリソースがある場合は、メニューから1つ選択します。
5. ページで、必要に応じてこれらの手順を完了し、 をクリックします。
    a. マスターイメージを選択します。次のイメージタイプを選択できます。
        - 仮想マシン (リージョンが選択されたホスティングユニットと同じもの)。
        - スナップショット (マルチリージョンスナップショットをサポート)。
        - OSイメージ (マルチリージョンのパブリックイメージと非パブリックイメージをサポート)。 単一テナンシー機能を使用する場合は、ノードグループプロパティが正しく

構成されているイメージを選択してください。「ゾーン選択の有効化」を参照してください。

b. マシンプロファイルからマシンプロパティを継承するには、 を選択し、 タブまたは タブからプロファイルを選択します。

> **注:**
>
> - 現在、このカタログ内のVMは、選択されたマシンプロファイルからストレージ、マシンタイプ、およびディスク暗号化の設定を継承します。
> - インスタンステンプレートをマシンプロファイルとして選択した場合、すべてのゾーンがデフォルトで選択されます。必要に応じてゾーンを選択できます。

c. カタログの最小機能レベルを選択します。

6. **ストレージの種類**ページで、このマシンカタログのオペレーティングシステムを格納するために使用されるストレージの種類を選択します。以下の各ストレージオプションには、独自の価格とパフォーマンス特性があります。（IDディスクは常にゾーン標準永続ディスクを使用して作成されます。）

   - 標準永続ディスク
   - バランス永続ディスク
   - SSD永続ディスク

   Google Cloud のストレージオプションの詳細については、`<https://cloud.google.com/compute/docs/disks/>`を参照してください。

7. ページで、作成するVMの数を指定し、VMの詳細な仕様を表示してから、 を選択します。マシンカタログに単一テナントノードグループを使用する場合は、予約済みの単一テナントノードが利用可能なゾーン**のみ**を選択してください。ゾーン選択を有効にするを参照してください。

8. **ディスク設定**ページで、次の設定を構成できます。

   - ライトバックキャッシュを有効にするかどうかを選択します。ライトバックキャッシュを有効にした後、次のことができます。
     - 一時データをキャッシュするために使用されるディスクとRAMのサイズを構成します。詳細については、一時データのキャッシュを構成するを参照してください。

- ライトバックキャッシュディスクのストレージタイプを選択します。ライトバックキャッシュディスクに使用できるストレージオプションは次のとおりです。
  - 標準永続ディスク
  - バランス永続ディスク
  - SSD永続ディスク

  Google Cloudのストレージオプションの詳細については、「ストレージオプション」を参照してください。
- ライトバックキャッシュディスクの種類を選択します。
  - **非永続ライトバックキャッシュディスクを使用する**。選択した場合、ライトバックキャッシュディスクはプロビジョニングされたVMに永続しません。ディスクは電源サイクル中に削除され、ディスクにリダイレクトされたデータはすべて失われます。
  - **永続ライトバックキャッシュディスクを使用する**。選択した場合、ライトバックキャッシュディスクはプロビジョニングされたVMに永続します。このオプションを有効にすると、ストレージコストが増加します。

- MCSストレージ最適化（MCS I/O）が有効になっている場合、次のいずれかを実行できます。
  - 電源サイクル中にVDAのシステムディスクを保持するかどうかを選択します。詳細については、「MCSストレージ最適化の更新を有効にする」を参照してください。
  - メモリとディスクキャッシュのサイズを更新します。
- ディスクの内容を保護するために独自のキーを使用するかどうかを選択します。この機能を使用するには、まず独自の顧客管理暗号化キー（CMEK）を作成する必要があります。詳細については、「顧客管理暗号化キー（CMEK）を使用する」を参照してください。

> **注:**
>
> Studioインターフェイスでのみ利用可能です。

> キーを作成した後、リストからいずれかのキーを選択できます。カタログを作成した後は、キーを変更できません。Google Cloudは、既存の永続ディスクまたはイメージでのキーのローテーションをサポートしていません。したがって、カタログをプロビジョニングした後、カタログは特定のバージョンのキーに紐付けられます。そのキー

> が無効化または破棄された場合、そのキーで暗号化されたインスタンスとディスクは、キーが再度有効化または復元されるまで使用できなくなります。

9. ページで、Active Directory アカウントを選択し、 を選択します。
   - **新しいActive Directoryアカウントを作成する**を選択した場合、ドメインを選択し、Active Directoryで作成されるプロビジョニング済みVMコンピューターアカウントの命名スキームを表す文字のシーケンスを入力します。アカウント命名スキームは1〜64文字で構成でき、空白スペース、非ASCII文字、または特殊文字を含めることはできません。
   - 「**既存のActive Directoryアカウントを使用する**」を選択した場合、「**参照**」を選択して、選択したマシンの既存のActive Directoryコンピューターアカウントに移動します。
10. **ドメイン資格情報**ページで、**資格情報を入力**を選択し、ユーザー名とパスワードを入力して、**保存**を選択し、**次へ**を選択します。
    - 入力する資格情報には、Active Directoryアカウント操作を実行する権限が必要です。
11. **概要**ページで、情報を確認し、カタログの名前を指定して、**完了**を選択します。

> **注:**
>
> バージョン2402以降、GCPカタログ名は以下の規則に準拠する必要があります。
>
> - 小文字で始まること。
> - 小文字 (a-z)、数字、ハイフンのみを含めること。
> - 小文字または数字で終わること。 これらの規則に準拠していない既存のGCPカタログの名前を変更しようとすると、エラーメッセージが表示され、更新された規則に従って名前を変更するように案内されます。

マシンカタログの作成には時間がかかる場合があります。マシンがターゲットノードグループに作成されていることを確認するには、Google Cloudコンソールに移動します。

手動で作成されたGoogle Cloudマシンをインポートする

Google Cloudへの*接続を作成*し、その後、Google Cloudマシンを含む*カタログを作成*できます。その後、Citrix Virtual Apps and Desktopsを介してGoogle Cloudマシンを手動で電源サイクルできます。この機能を使用すると、次のことができます。

- 手動で作成されたGoogle CloudマルチセッションOSマシンをCitrix Virtual Apps and Desktopsマシンカタログにインポートする。
- 手動で作成されたGoogle CloudマルチセッションOSマシンをCitrix Virtual Apps and Desktopsカタログから削除する。
- 既存のCitrix Virtual Apps and Desktopsの電源管理機能を使用して、Google Cloud WindowsマルチセッションOSマシンを電源管理します。たとえば、それらのマシンの再起動スケジュールを設定します。

この機能は、既存のCitrix Virtual Apps and Desktopsプロビジョニングワークフローの変更や、既存の機能の削除を必要としません。手動で作成したGoogle Cloudマシンをインポートする代わりに、Web StudioでMCSを使用してマシンをプロビジョニングすることをお勧めします。

共有仮想プライベートクラウド

共有仮想プライベートクラウド (VPC) は、共有サブネットが利用可能になるホストプロジェクトと、そのリソースを使用する1つ以上のサービスプロジェクトで構成されます。共有VPCは、共有企業Googleクラウド資産の一元的な制御、使用、管理を提供するため、大規模なインストールにとって望ましいオプションです。詳細については、Googleドキュメントサイトを参照してください。

この機能により、Machine Creation Services (MCS) は、共有VPCに展開されたマシンカタログのプロビジョニングと管理をサポートします。このサポートは、現在ローカルVPCで提供されているサポートと機能的に同等ですが、次の2つの点で異なります。

1. ホスト接続の作成に使用されるサービスアカウントに追加の権限を付与する必要があります。このプロセスにより、MCSは共有VPCリソースにアクセスして使用できるようになります。
2. イングレスとエグレス用にそれぞれ1つずつ、2つのファイアウォールルールを作成する必要があります。これらのファイアウォールルールは、イメージマスタリングプロセス中に使用されます。

必要な新しい権限

ホスト接続を作成する際には、特定の権限を持つGoogle Cloudサービスアカウントが必要です。これらの追加権限は、共有VPCベースのホスト接続の作成に使用されるすべてのサービスアカウントに付与する必要があります。

> **ヒント:**

> これらの追加の権限は、Citrix Virtual Apps and Desktopsにとって新しいものではありません。これらはローカルVPCの実装を容易にするために使用されます。共有VPCでは、これらの追加の権限により、他の共有VPCリソースへのアクセスが可能になります。

> Shared VPCをサポートするために、ホスト接続に関連付けられたサービスアカウントに最大4つの追加権限を付与する必要があります。

1. **compute.firewalls.list** - この権限は必須です。これにより、MCSは共有VPCに存在するファイアウォールルールの一覧を取得できます。
2. **compute.networks.list** - この権限は必須です。これにより、MCSはサービスアカウントが利用できる共有VPCネットワークを識別できます。
3. **compute.subnetworks.list** – この権限は、VPCの使用方法によってオプションです。これにより、MCSは表示可能な共有VPC内のサブネットを識別できます。この権限はローカルVPCを使用する場合にすでに必要ですが、共有VPCホストプロジェクトでも割り当てる必要があります。
4. **compute.subnetworks.use** - この権限は、VPC の使用方法によってオプションです。プロビジョニングされたマシンカタログでサブネットリソースを使用するために必要です。この権限はローカル VPC を使用する場合にすでに必要ですが、共有 VPC ホストプロジェクトにも割り当てる必要があります。

これらの権限を使用する際には、マシンカタログの作成に使用される権限の種類に基づいて異なるアプローチがあることを考慮してください。

- プロジェクトレベルの権限:
  - ホストプロジェクト内のすべてのShared VPCへのアクセスを許可します。
  - 権限 #3 と #4 をサービスアカウントに割り当てる必要があります。
- サブネットレベルの権限:
  - Shared VPC内の特定のサブネットへのアクセスを許可します。
  - 権限 #3 と #4 はサブネットレベルの割り当てに固有のものであるため、サービスアカウントに直接割り当てる必要はありません。

組織のニーズとセキュリティ基準に合ったアプローチを選択してください。

> **ヒント:**

> プロジェクトレベルとサブネットレベルの権限の違いについて詳しくは、Google Cloud ドキュメントを参照してください。

ファイアウォールルール

マシンカタログの準備中に、カタログのマスターイメージシステムディスクとして機能するマシンイメージが準備されます。このプロセスが発生すると、ディスクは一時的に仮想マシンに接続されます。このVMは、すべてのインバウンドおよびアウトバウンドネットワークトラフィックを防止する分離された環境で実行する必要があります。これは、イングレス用とエグレス用の2つのすべて拒否ファイアウォールルールによって実現されます。Google CloudローカルVPCを使用する場合、MCSはこのファイアウォールをローカルネットワークに作成し、マスタリング用のマシンに適用します。マスタリングが完了すると、ファイアウォールルールはイメージから削除されます。

共有 VPC を使用するために必要な新しい権限の数を最小限に抑えることをお勧めします。共有 VPC はより高レベルの企業リソースであり、通常、より厳格なセキュリティプロトコルが導入されています。このため、共有 VPC リソースのホストプロジェクトに、インバウンド用とアウトバウンド用の 2 つのファイアウォールルールを作成します。それらに最高の優先順位を割り当てます。次の値を使用して、これらの各ルールに新しいターゲットタグを適用します。

`citrix-provisioning-quarantine-firewall`

MCS はマシンカタログを作成または更新する際に、このターゲットタグを含むファイアウォールルールを検索します。次に、ルールの正確性を確認し、カタログのマスターイメージの準備に使用されるマシンに適用します。ファイアウォールルールが見つからない場合、またはルールが見つかってもルールやその優先順位が正しくない場合は、次のようなメッセージが表示されます。

`"Unable to find valid INGRESS and EGRESS quarantine firewall rules for VPC <name> in project <project>. " Please ensure you have created 'deny all' firewall rules with the network tag 'citrix-provisioning-quarantine-firewall' and proper priority." "Refer to Citrix Documentation for details."`

共有 VPC の構成

Web Studio で共有 VPC をホスト接続として追加する前に、プロビジョニングするプロジェクトからサービスアカウントを追加するために、次の手順を完了してください。

1. IAM ロールを作成します。
2. CVAD ホスト接続の作成に使用するサービスアカウントを、共有 VPC ホストプロジェクトの IAM ロールに追加します。
3. プロビジョニングするプロジェクトの Cloud Build サービスアカウントを、共有 VPC ホストプロジェクトの IAM ロールに追加します。

4. ファイアウォールルールを作成します。

IAM ロールの作成

ロールのアクセスレベルを決定します — *プロジェクトレベルアクセス*、またはより制限されたモデルである *サブネットレベルアクセス* を使用します。

IAMロールのプロジェクトレベルアクセス。プロジェクトレベルのIAMロールには、次の権限を含めます。

- compute.firewalls.list
- compute.networks.list
- compute.subnetworks.list
- compute.subnetworks.use

プロジェクトレベルのIAMロールを作成するには：

1. Google Cloudコンソールで、**IAMと管理 > ロール**に移動します。
2. 「**ロール**」ページで、「**ロールを作成**」を選択します。
3. 「**ロールを作成**」ページで、ロール名を指定します。「**権限を追加**」を選択します。
    a. **権限の追加**ページで、ロールに権限を個別に追加します。権限を追加するには、**テーブルをフィルタリング**フィールドに権限の名前を入力します。権限を選択し、**追加**を選択します。
    b. 「**作成**」を選択します。

サブネットレベルのIAMロール。このロールは、**ロールを作成**を選択した後に、権限`compute.subnetworks.list`と`compute.subnetworks.use`の追加を省略します。このIAMアクセスレベルの場合、権限`compute.firewalls.list`と`compute.networks.list`を新しいロールに適用する必要があります。

サブネットレベルのIAMロールを作成するには：

1. Google Cloudコンソールで、**VPCネットワーク** > **共有VPC** に移動します。**共有VPC** ページが表示され、ホストプロジェクトに含まれる共有VPCネットワークのサブネットが表示されます。
2. ページで、アクセスするサブネットを選択します。
3. 右上隅で、 を選択してサービスアカウントを追加します。
4. ページで、次の手順を実行します。

a. フィールドにサービスアカウントの名前を入力し、メニューからサービスアカウントを選択します。
b. フィールドを選択し、 を選択します。
c. を選択します。

5. Google Cloud コンソールで、**IAM と管理** > **ロール**に移動します。
6. **ロール**ページで、**ロールを作成**を選択します。
7. **ロールを作成**ページで、ロール名を指定します。**権限を追加**を選択します。

a. **権限を追加**ページで、ロールに権限を個別に追加します。権限を追加するには、**テーブルをフィルタリング**フィールドに権限の名前を入力します。権限を選択し、**追加**を選択します。
b. **作成**を選択します。

ホストプロジェクトのIAMロールにサービスアカウントを追加する

IAMロールを作成したら、ホストプロジェクトのサービスアカウントを追加するために次の手順を実行します。

1. Google Cloud コンソールで、ホストプロジェクトに移動し、次に**IAM と管理 > IAM**に移動します。
2. **IAM**ページで、**追加**を選択してサービスアカウントを追加します。
3. **メンバーを追加**ページで、:

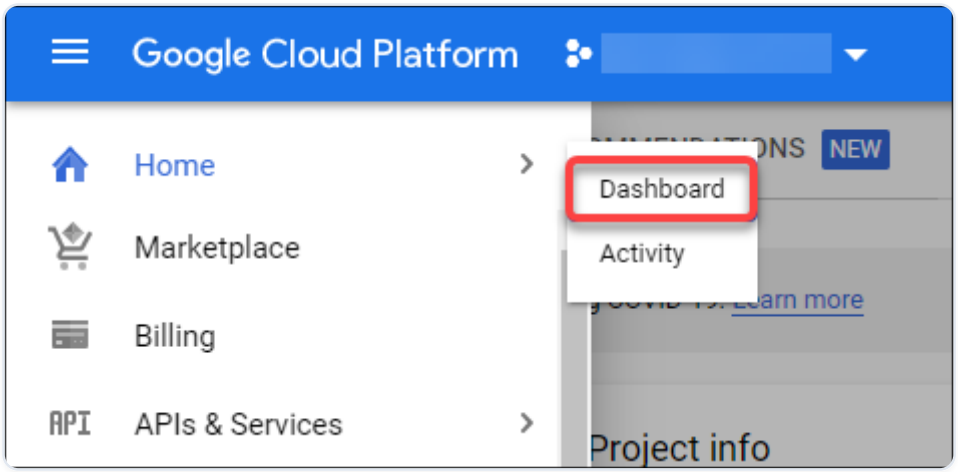
a. **新しいメンバー**フィールドにサービスアカウントの名前を入力し、メニューでサービスアカウントを選択します。
b. ロールフィールドで、作成したIAMロールを入力し、メニューでそのロールを選択します。
c. **保存**を選択します。

サービスアカウントがホストプロジェクト用に設定されました。

CLOUD BUILD サービスアカウントを共有VPCに追加する

すべてのGoogle Cloudサブスクリプションには、プロジェクトID番号の後に`cloudbuild.gserviceaccount`が続くサービスアカウントがあります。例: `705794712345@cloudbuild.gserviceaccount`。

Google Cloudコンソールで**ホーム**と**ダッシュボード**を選択すると、プロジェクトのプロジェクトID番号を確認できます。



画面の**プロジェクト情報**領域の下にある**プロジェクト番号**を見つけます。

Cloud Buildサービスアカウントを共有VPCに追加するには、次の手順を実行します。

1. Google Cloudコンソールで、ホストプロジェクトに移動し、**IAM と管理** > **IAM**に移動します。
2. **権限**ページで、**追加**を選択してアカウントを追加します。
3. **メンバーの追加**ページで、次の手順を実行します。
    a. **新しいメンバー**フィールドにCloud Buildサービスアカウントの名前を入力し、メニューからサービスアカウントを選択します。
    b. **ロールを選択**フィールドを選択し、`Computer Network User`と入力して、メニューからロールを選択します。
    c. **保存**を選択します。

ファイアウォールルールを作成する

マスタリングプロセスの一環として、MCS は選択されたマシンイメージをコピーし、それを使用してカタログ用のマスターイメージシステムディスクを準備します。マスタリング中、MCS はディスクを一時的な仮想マシンに接続し、その仮想マシンが準備スクリプトを実行します。この VM は、すべてのインバウンドおよびアウトバウンドネットワークトラフィックを禁止する分離された環境で実行する必要があります。分離された環境を作成するために、MCS は2つの *すべて拒否* ファイアウォールルール（イングレスルールとエグレスルール）を必要とします。したがって、*ホストプロジェクト* に次の2つのファイアウォールルールを作成します。

1. Google Cloudコンソールで、ホストプロジェクトに移動し、**VPC ネットワーク > ファイアウォール**に移動します。
2. **ファイアウォール**ページで、**ファイアウォールルールを作成**を選択します。
3. 「**ファイアウォールルールの作成**」ページで、以下を完了します。
    - **名前**。ルールの名前を入力します。

- **ネットワーク**。イングレスファイアウォールルールを適用する共有VPCネットワークを選択します。
- **優先度**。値が小さいほど、ルールの優先度が高くなります。小さい値（例: 10）をお勧めします。
- **トラフィックの方向**。**イングレス** を選択します。
- **一致時のアクション**。**拒否** を選択します。
- **ターゲット**。デフォルトの **指定されたターゲットタグ** を使用します。
- **ターゲットタグ**。`citrix-provisioning-quarantine-firewall` と入力します。
- **ソースフィルター**。デフォルトの **IP 範囲** を使用します。
- **ソース IP 範囲**。すべてのトラフィックに一致する範囲を入力します。`0.0.0.0/0` と入力します。
- **プロトコルとポート**。「**すべて拒否**」を選択します。

4. 「**作成**」を選択してルールを作成します。
5. 手順1〜4を繰り返して別のルールを作成します。「**トラフィックの方向**」には「**エグレス**」を選択します。

接続の追加

Google Cloud環境への接続を追加します。「」を参照してください(/ja-jp/citrix-virtual-apps-desktops/2503/install-configure/connections/connection-gcp.html#add-a-connection)。

ゾーン選択を有効にする

Citrix Virtual Apps and Desktopsはゾーン選択をサポートしています。ゾーン選択を使用すると、VMを作成するゾーンを指定できます。ゾーン選択を使用すると、管理者は選択したゾーンに単一テナントノードを配置できます。単一テナンシーを構成するには、Google Cloudで以下を完了する必要があります。

- Google Cloud の単一テナントノードを予約する
- VDA マスターイメージを作成する

Google Cloud の単一テナントノードを予約する

単一テナントノードを予約するには、Google Cloud のドキュメントを参照してください。

> **重要：**

ノードテンプレートは、ノードグループに予約されているシステムのパフォーマンス特性を示すために使用されます。これらの特性には、vGPU の数、ノードに割り当てられるメモリ量、およびノード上に作成されるマシンに使用されるマシンタイプが含まれます。詳細については、Google Cloud のドキュメントを参照してください。

VDA マスターイメージの作成

単一テナントノードにマシンを正常に展開するには、マスター VM イメージを作成する際に追加の手順を実行する必要があります。Google Cloud のマシンインスタンスには、*ノードアフィニティラベル*と呼ばれるプロパティがあります。単一テナントノードに展開されるカタログのマスターイメージとして使用されるインスタンスには、**ターゲットノードグループ**の名前と一致する*ノードアフィニティラベル*が必要です。これを実現するには、次の点に留意してください。

- 新しいインスタンスの場合、インスタンス作成時にGoogle Cloudコンソールでラベルを設定します。詳細については、単一テナントVMのプロビジョニングを参照してください。
- 既存のインスタンスの場合、**gcloud**コマンドラインを使用してラベルを設定します。詳細については、ノードアフィニティラベルの構成を参照してください。

注：

共有 VPC で単一テナンシーを使用する場合は、共有仮想プライベートクラウドを参照してください。

マシンカタログを作成する

ノードアフィニティラベルを設定したら、マシンカタログを構成します。

顧客管理の暗号化キー (CMEK)

MCSカタログには、顧客管理の暗号化キー (CMEK) を使用できます。この機能を使用する場合、Google Cloud Key Management Service `CryptoKey Encrypter/Decrypter` ロールをCompute Engine Service Agentに割り当てます。Citrix Virtual Apps and Desktopsアカウントは、キーが保存されているプロジェクトで適切な権限を持っている必要があります。詳細については、Cloud KMS キーを使用してリソースを保護する を参照してください。

お使いのCompute Engine Service Agentは、次の形式です: `service-<Project_Number>@compute-system.iam.gserviceaccount.com`。この形式は、デフォルトのCompute Engine Service Accountとは異なります。

注:

このCompute Engine Service Accountは、Google Consoleの**IAM権限**表示に表示されない場合があります。そのような場合は、Cloud KMSキーを使用してリソースを保護する で説明されているように、`gcloud` コマンドを使用してください。

Citrix Virtual Apps and Desktops アカウントに権限を割り当てる

Google Cloud KMSの権限は、さまざまな方法で構成できます。*プロジェクトレベル*のKMS権限または*リソースレベル*のKMS権限のいずれかを提供できます。詳細については、権限とロール を参照してください。

プロジェクトレベルの権限

1つのオプションは、Citrix Virtual Apps and Desktopsアカウントに、Cloud KMSリソースを参照するためのプロジェクトレベルの権限を提供することです。これを行うには、カスタムロールを作成し、次の権限を追加します。

- `cloudkms.keyRings.list`
- `cloudkms.keyRings.get`
- `cloudkms.cryptokeys.list`
- `cloudkms.cryptokeys.get`

このカスタムロールをCitrix Virtual Apps and Desktopsに割り当てます。これにより、インベントリ内の関連プロジェクトでリージョンキーを参照できるようになります。

リソースレベルの権限

もう1つのオプションであるリソースレベルの権限については、Google Cloudコンソールで、MCSプロビジョニングに使用する`cryptoKey`に移動します。Citrix Virtual Apps and Desktopsアカウントを、カタログプロビジョニングに使用するキーリングまたはキーに追加します。

ヒント:

このオプションでは、Citrix Virtual Apps and DesktopsアカウントにCloud KMSリソースに対するプロジェクトレベルのリスト権限がないため、インベントリでプロジェクトのリージョンキーを参照することはできません。ただし、以下で説明するように、`ProvScheme`カスタムプロパティで正しい`cryptoKeyId`を指定することで、CMEKを使用してカタログをプロビジョニングすることは可能です。

カスタムプロパティを使用したCMEKによるプロビジョニング

PowerShellでプロビジョニングスキームを作成するときに、`ProvScheme CustomProperties`で`CryptoKeyId`プロパティを指定します。例：

```
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

    <Property xsi:type="StringProperty" Name="CryptoKeyId"
Value="<yourCryptoKeyId>" />

</CustomProperties>'
```

`cryptoKeyId`は次の形式で指定する必要があります。

`projectId:location:keyRingName:cryptoKeyName`

たとえば、リージョン`us-east1`のキーリング`my-example-key-ring`にあるキー`my-example-key`を、IDが`my-example-project-1`のプロジェクトで使用する場合、`ProvScheme`カスタム設定は次のようになります。

```
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

    <Property xsi:type="StringProperty" Name="CryptoKeyId" Value="my-
example-project-1:us-east1:my-example-key-ring:my-example-key" />

</CustomProperties>'
```

このプロビジョニングスキームに関連するすべてのMCSプロビジョニング済みディスクとイメージは、この顧客管理の暗号化キーを使用します。

ヒント:

グローバルキーを使用する場合、カスタムプロパティの場所は、上記の例の**us-east1**のような**リージョン**名ではなく、`global`と記述する必要があります。例：`<Property xsi:type="StringProperty" Name="CryptoKeyId" Value="my-example-project-1:global:my-example-key-ring:my-example-key" />`。

顧客管理キーのローテーション

Google Cloudは、既存の永続ディスクまたはイメージでのキーのローテーションをサポートしていません。マシンがプロビジョニングされると、作成時に使用されていたキーのバージョンに紐付けられます。ただし、新しいバージョンのキーを作成でき、その新しいキーは、新しくプロビジョニングされたマシンや、新しいマスターイメージでカタログが更新されたときに作成されるリソースに使用されます。

キーリングに関する重要な考慮事項

キーリングは名前変更または削除できません。また、設定時に予期せぬ料金が発生する場合があります。キーリングを削除または削除すると、Google Cloud はエラーメッセージを表示します。

```
Sorry, you can't delete or rename keys or key rings. We were concerned
about the security implications of allowing multiple keys or key versions
over time to have the same resource name, so we decided to make names
immutable. (And you can't delete them, because we wouldn't be able to do a
true deletion--there would still have to be a tombstone tracking that this
name had been used and couldn't be reused).

We're aware that this can make things untidy, but we have no immediate
plans to change this.

If you want to avoid getting billed for a key or otherwise make it
unavailable, you can do so by deleting all the key versions; neither keys
nor key rings are billed for, just the active key versions within the
keys.
```

ヒント:

詳細については、「コンソールからキーリングを編集または削除する」を参照してください。

均一なバケットレベルのアクセス互換性

Citrix Virtual Apps and Desktops は、Google Cloud の均一なバケットレベルのアクセス制御ポリシーと互換性があります。この機能は、ストレージバケットを含むリソースの操作を許可するためにサービスアカウントに権限を付与する IAM ポリシーの使用を強化します。均一なバケットレベルのアクセス制御により、Citrix Virtual Apps and Desktops では、アクセス制御リスト (ACL) を使用して、ストレージバケットまたはそこに保存されているオブジェクトへのアクセスを制御できます。Google Cloud の均一なバケットレベルのアクセスに関する概要情報については、「均一なバ

ケットレベルのアクセス」を参照してください。構成情報については、「均一なバケットレベルのアクセスを要求する」を参照してください。

PowerShell を使用してマシンカタログを作成する

このセクションでは、PowerShell を使用してカタログを作成する方法について詳しく説明します。

- 永続的なライトバックキャッシュディスクを持つカタログを作成する
- MCSIO で起動パフォーマンスを向上させる
- マシンプロファイルを使用してマシンカタログを作成する
- インスタンステンプレートとしてマシンプロファイルを持つマシンカタログを作成する
- PowerShell を使用してシールドされた VM を持つカタログを作成する
- 単一テナントノードに Windows 11 VM を作成する

永続的なライトバックキャッシュディスクを持つカタログを作成する

永続的なライトバックキャッシュディスクを持つカタログを構成するには、PowerShell パラメーター `New-ProvScheme` `CustomProperties` を使用します。

> **ヒント:**
>
> ここでPowerShellパラメーターを使用するのは、クラウドベースのホスティング接続の場合のみです。オンプレミスソリューション（XenServer®など）で永続的なライトバックキャッシュディスクを使用してマシンをプロビジョニングする場合、ディスクは自動的に永続化されるため、PowerShellは必要ありません。

> このパラメーターは、MCSでプロビジョニングされたマシンに対してライトバックキャッシュディスクがどのように永続化されるかを決定するために使用される追加プロパティ `PersistWBC` をサポートします。`PersistWBC` プロパティは、`UseWriteBackCache` パラメーターが指定され、`WriteBackCacheDiskSize` パラメーターがディスクが作成されることを示すように設定されている場合にのみ使用されます。

> **注:**

この動作は、AzureとGCPの両方に適用されます。これらの環境では、デフォルトのMCSIOライトバックキャッシュディスクは電源サイクル時に削除され、再作成されます。ディスクを永続化することを選択すると、MCSIOライトバックキャッシュディスクの削除と再作成を回避できます。

`PersistWBC` プロパティを `true` に設定すると、Citrix Virtual Apps and Desktops 管理者が管理インターフェイスからマシンをシャットダウンしても、ライトバックキャッシュディスクは削除されません。

`PersistWBC` プロパティを `false` に設定すると、Citrix Virtual Apps and Desktops 管理者が管理インターフェイスからマシンをシャットダウンしたときに、ライトバックキャッシュディスクが削除されます。

注:

`PersistWBC` プロパティが省略されている場合、プロパティはデフォルトで `false` になり、マシンが管理インターフェイスからシャットダウンされるとライトバックキャッシュは削除されます。

たとえば、CustomPropertiesパラメーターを使用して `PersistWBC` を `true` に設定する場合：

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="ResourceGroups"
Value="benvaldev5RG3" />

<Property xsi:type="StringProperty" Name="PersistWBC" Value="true" />

</CustomProperties>
```

注:

`PersistWBC`プロパティは、`New-ProvScheme` PowerShellコマンドレットを使用してのみ設定できます。作成後にプロビジョニングスキームの`CustomProperties`を変更しようとしても、マシンカタログや、マシンがシャットダウンされたときのライトバックキャッシュディスクの永続性には影響しません。

たとえば、`New-ProvScheme`を使用してライトバックキャッシュを使用するように設定し、同時に`PersistWBC`プロパティを`true`に設定する場合：

```
New-ProvScheme

-CleanOnBoot

-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com/
2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`"><Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`"
Value=`"true`" /><Property xsi:type=`"StringProperty`"
Name=`"StorageAccountType`" Value=`"Premium_LRS`" /><Property
xsi:type=`"StringProperty`" Name=`"ResourceGroups`"
Value=`"benvaldev5RG3`" /><Property xsi:type=`"StringProperty`"
Name=`"PersistWBC`" Value=`"true`" /></CustomProperties>"

-HostingUnitName "adSubnetScale1"

-IdentityPoolName "BV-WBC1-CAT1"

-MasterImageVM "XDHyp:
\HostingUnits\adSubnetScale1\image.folder\GoldImages.resourcegroup\W10MCSI
O-01_OsDisk_1_a940e6f5bab349019d57ccef65d2c7e3.manageddisk"

-NetworkMapping @{"0"="XDHyp:\HostingUnits\adSubnetScale1\
\virtualprivatecloud.folder\CloudScale02.resourcegroup\adVNET.virtualpriva
tecloud\adSubnetScale1.network"}

-ProvisioningSchemeName "BV-WBC1-CAT1"

-ServiceOffering "XDHyp:
\HostingUnits\adSubnetScale1\serviceoffering.folder\Standard_D2s_v3.servic
eoffering"
```

```
-UseWriteBackCache

-WriteBackCacheDiskSize 127

-WriteBackCacheMemorySize 256
```

MCSIOで起動パフォーマンスを向上させる

MCSIOが有効になっている場合、AzureおよびGCPマネージドディスクの起動パフォーマンスを向上させることができます。この機能を構成するには、PowerShellの `New-ProvScheme` コマンドで `PersistOSDisk` カスタムプロパティを使用します。`New-ProvScheme` に関連するオプションは次のとおりです。

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="Resource ``````<!--NeedCopy-->

````````Groups" Value="benvaldev5RG3" />

<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="true" />

</CustomProperties>
```

この機能を有効にするには、`PersistOSDisk` カスタムプロパティを `true` に設定します。例：

```
New-ProvScheme

-CleanOnBoot

-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com/
2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`"><Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`"
Value=`"true`" /><Property xsi:type=`"StringProperty`"
Name=`"StorageAccountType`" Value=`"Premium_LRS`" /><Property
xsi:type=`"StringProperty`" Name=`"ResourceGroups`"
```
```

```
Value=`"benvaldev5RG3`" /><Property xsi:type=`"StringProperty`"
Name=`"PersistOsDisk`" Value=`"true`" /></CustomProperties>"

-HostingUnitName "adSubnetScale1"

-IdentityPoolName "BV-WBC1-CAT1"

-MasterImageVM "XDHyp:
\HostingUnits\adSubnetScale1\image.folder\GoldImages.resourcegroup\W10MCSI
O-01_OsDisk_1_a940e6f5bab349019d57ccef65d2c7e3.manageddisk"

-NetworkMapping @{"0"="XDHyp:\HostingUnits\adSubnetScale1\
\virtualprivatecloud.folder\CloudScale02.resourcegroup\adVNET.virtualpriva
tecloud\adSubnetScale1.network"}

-ProvisioningSchemeName "BV-WBC1-CAT1"

-ServiceOffering "XDHyp:
\HostingUnits\adSubnetScale1\serviceoffering.folder\Standard_D2s_v3.servic
eoffering"

-UseWriteBackCache

-WriteBackCacheDiskSize 127

-WriteBackCacheMemorySize 256
```

マシンプロファイルを使用してマシンカタログを作成する

Machine Creation Services (MCS) を使用してマシンをプロビジョニングするカタログを作成する場合、マシンプロファイルを使用して、仮想マシンからハードウェアプロパティをキャプチャし、カタログ内の新しくプロビジョニングされたVMに適用できます。`MachineProfile` パラメータが使用されていない場合、ハードウェアプロパティはマスターイメージVMまたはスナップショットからキャプチャされます。 たとえば、`StorageType`、`CatalogZones`、`CryptoKeyIs` など、明示的に定義する一部のプロパティは、マシンプロファイルから無視されます。

- マシンプロファイルを使用してカタログを作成するには、`New-ProvScheme` コマンドを使用します。例: `New-ProvScheme –MachineProfile "path to VM"`。`MachineProfile` パラメータを指定しない場合、ハードウェアプロパティはマスターイメージVMからキャプチャされます。

- 新しいマシンプロファイルでカタログを更新するには、`Set-ProvScheme` コマンドを使用します。例: `Set-ProvScheme –MachineProfile "path to new VM"`。このコマンドは、カタログ内の既存のVMのマシンプロファイルを変更しません。カタログに追加された新しく作成されたVMのみが新しいマシンプロファイルを持ちます。
- マスターイメージを更新することもできますが、マスターイメージを更新してもハードウェアプロパティは更新されません。ハードウェアプロパティを更新したい場合は、`Set-ProvScheme` コマンドを使用してマシンプロファイルを更新する必要があります。これらの変更は、カタログ内の新しいマシンにのみ適用されます。既存のマシンのハードウェアプロパティを更新するには、`-StartsNow` および `-DurationInMinutes -1` パラメータを指定して `Set-ProvVMUpdateTimeWindow` コマンドを使用できます。

> **注:**
>
> - `StartsNow` は、スケジュールされた開始時刻が現在の時刻であることを示します。
> - 負の数（例: –1）を指定した `DurationInMinutes` は、スケジュールの時間枠に上限がないことを示します。

マシンプロファイルをインスタンステンプレートとして使用してマシンカタログを作成する

マシンプロファイルの入力としてGCPインスタンステンプレートを選択できます。インスタンステンプレートはGCPの軽量リソースであるため、非常に費用対効果が高いです。

マシンプロファイルをインスタンステンプレートとして使用して新しいマシンカタログを作成する

1. PowerShellウィンドウを開きます。
2. `asnp citrix*` を実行して、Citrix固有のPowerShellモジュールをロードします。
3. 次のコマンドを使用して、GCPプロジェクトでインスタンステンプレートを見つけます。

```
cd XDHyp:\HostingUnits\<HostingUnitName>\instanceTemplates.folder
```

4. NewProvSchemeコマンドを使用して、インスタンステンプレートとしてマシンプロファイルを持つ新しいマシンカタログを作成します。

```
New-ProvScheme -ProvisioningSchemeName <CatalogName>  -HostingUnitName
<HostingUnitName> -IdentityPoolName <identity pool name> -MasterImageVM

XDHyp:\HostingUnits\<HostingUnitName> \Base.vm\Base.snapshot
-MachineProfile XDHyp:
\HostingUnits\<HostingUnitName>\instanceTemplates.folder\mytemplate.tem
plate
```

New-ProvSchemeコマンドの詳細については、https://developer-docs.citrix.com/projects/citrix-daas-sdk/en/latest/MachineCreation/New-ProvScheme/を参照してください。

5. PowerShellコマンドを使用してマシンカタログの作成を完了します。Remote PowerShell SDKを使用したカタログの作成方法については、https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/を参照してください。

既存のマシンカタログのマシンプロファイルをインスタンステンプレートに変更する

既存のマシンカタログのマシンプロファイルをインスタンステンプレートに変更する詳細な手順は次のとおりです。

1. PowerShellウィンドウを開きます。
2. Citrix固有のPowerShellモジュールをロードするには、`asnp citrix*`を実行します。
3. 次のコマンドを実行します。

```
Set-ProvScheme -ProvisioningSchemeName  <CatalogName> -MachineProfile
XDHyp:
\HostingUnits\<HostingUnitName>\instanceTemplates.folder\<TemplateName>
.template
```

Set-ProvSchemeコマンドの詳細については、https://developer-docs.citrix.com/projects/citrix-daas-sdk/en/latest/MachineCreation/Set-ProvScheme/を参照してください。

PowerShellを使用してシールドされたVMでカタログを作成する

シールドされたVMプロパティを持つMCSマシンカタログを作成できます。シールドされた仮想マシンは、セキュアブート、仮想トラステッドプラットフォームモジュール、UEFIファームウェア、整合性監視などの高度なプラットフォームセキュリティ機能を使用して、Compute Engineインスタンスの検証可能な整合性を提供する一連のセキュリティ制御によって強化されています。

MCSは、マシンプロファイルワークフローを使用してカタログを作成することをサポートしています。マシンプロファイルワークフローを使用する場合、VMインスタンスのシールドされたVMプ

ロパティを有効にする必要があります。その後、このVMインスタンスをマシンプロファイルの入力として使用できます。

マシンプロファイルワークフローを使用して、シールドされたVMを持つMCSマシンカタログを作成するには。

1. Google CloudコンソールでVMインスタンスのシールドされたVMオプションを有効にします。「クイックスタート: シールドされたVMオプションを有効にする」を参照してください。
2. VMインスタンスを使用して、マシンプロファイルワークフローでMCSマシンカタログを作成します。

    a. PowerShell ウィンドウを開きます。

    b. Citrix 固有の PowerShell モジュールをロードするには、`asnp citrix*` を実行します。

    c. まだ作成されていない場合は、ID プールを作成します。

    d. `New-ProvScheme` コマンドを実行します。例:

    ```
    New-ProvScheme -ProvisioningSchemeName <catalog-name>

    -HostingUnitName gcp-hostint-unit

    -MasterImageVM XDHyp:\HostingUnits\gcp-hostint-unit\catalog-vda.vm

    -MachineProfile XDHyp:\HostingUnits\gcp-hostint-unit\catalog-
    machine.vm
    ```

3. マシンカタログの作成を完了します。

新しいマシンプロファイルでマシンカタログを更新するには:

1. `Set-ProvScheme` コマンドを実行します。例:

    ```
    Set-ProvScheme -ProvisioningSchemeName <catalog-name>

    -MasterImageVM XDHyp:\HostingUnits\<hostin-unit>\catalog-vda.vm

    -MachineProfile "DHyp:\HostingUnits\<hostin-unit>\catalog-machine.vm
    ```

`Set-ProvScheme` で行われた変更を既存の VM に適用するには、`Set-ProvVMUpdateTimeWindow` コマンドを実行します。

1. `Set-ProvVMUpdateTimeWindow` コマンドを実行します。例:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog -VMName
<List-Of-Vm-Names> -StartsNow -DurationInMinutes -1
```

2. VM を再起動します。

シングルテナントノードに Windows 11 VM を作成する

GCP で Windows 11 VM を作成できます。ただし、マスターイメージに Windows 11 をインストールする場合は、マスターイメージ作成プロセス中に vTPM を有効にする必要があります。また、マシンプロファイルソース (VM またはインスタンステンプレート) で vTPM を有効にする必要があります。

シングルテナントノードに Windows 11 VM を作成するための主要な手順は次のとおりです。

1. Google Cloud 仮想化環境をセットアップします。詳細については、「Google Cloud environments」を参照してください。
2. VDA をインストールします。「Install VDAs」を参照してください。
3. Google Cloud環境への接続を作成します。詳細については、「Google Cloud環境への接続」を参照してください。
4. Windows 11 Bring Your Own License (BYOL) マスターイメージを作成し、そのイメージをGoogle Cloudにインポートします。「Windows 11 BYOLマスターイメージの作成」を参照してください。
5. マシンプロファイルソースを作成します: 専用テナントノードにVMをプロビジョニングし、ソースマシンプロファイルのvTPMを有効にします。「専用テナントノードでのVMのプロビジョニング」を参照してください。
6. vTPMが有効なWindows 11マシンプロファイルソースを使用してMCSマシンカタログを作成します。マシンプロファイルソースは、専用テナントノードで説明されているものと同じインスタンスタイプである必要があります。「Windows 11マシンプロファイルソースを使用したMCSマシンカタログの作成」を参照してください。

Windows 11 BYOLマスターイメージの作成

Windows 11 BYOLマスターイメージを作成し、そのマスターイメージをGoogle Cloudにインポートするには、次の2つのオプションがあります。

- Google Cloud Cloud Build Tools を使用する
- 他のハイパーバイザーでマスターイメージを作成する

GOOGLE CLOUD CLOUD BUILD TOOLS を使用する

1. Windows 11 ISO、GCP SDK、.NET framework、およびPowerShellインストーラーファイルをGCPストレージバケットにアップロードします。
2. クラウドビルド`.yaml`ファイルでファイルの場所をパラメーターとして指定します。
3. コマンドラインから次のCloud Buildを実行して、最終的なWindows 11イメージをビルドします。GCPは、GCPのDaisyワークフローを使用して、選択したプロジェクトでマスターイメージをブートストラップして作成し、マスターイメージはGCPにインポートされます。

```
gcloud compute instances import INSTANCE-NAME--source-uri=gs://BUCKET/
IMAGE-OVF-FILE.ovf --guest-os-features=UEFI_COMPATIBLE --byol --
machine-type=MACHINE-TYPE --zone=ZONE
```

> **注:**
>
> すべての大文字のテキストを実際のリソースの詳細に置き換えてください。

詳細については、「カスタム Windows BYOL イメージの作成」を参照してください。

他のハイパーバイザーでマスターイメージを作成する

1. 他のハイパーバイザーを使用して Windows 11 マスターイメージを作成します。
2. マスターイメージを OVF 形式でローカルマシンにエクスポートします。
3. ローカルの gcloud CLI を使用して、OVF ファイルを GCP ストレージバケットにアップロードします。

```
gsutil cp LOCAL_IMAGE_PATH_OVF_FILES gs://BUCKET_NAME/
```

4. コマンドラインから以下のCloud Buildを実行して、最終的なWindows 11イメージを構築します。GCPは、GCPのDaisyワークフローを使用して、選択したプロジェクトでマスターイメージをブートストラップして作成し、マスターイメージはGCPにインポートされます。

```
gcloud compute instances import INSTANCE-NAME --source-uri=gs://BUCKET/
IMAGE-OVF-FILE.ovf --guest-os-features=UEFI_COMPATIBLE --byol --
machine-type=MACHINE-TYPE --zone=ZONE
```

> **注:**
>
> すべての大文字のテキストを実際のリソースの詳細に置き換えます。

単一テナントノードでのVMのプロビジョニング

シングルテナントノードを使用すると、VMを他のプロジェクトのVMから物理的に分離したり、同じホストハードウェア上にVMをグループ化したりできます。シングルテナントノードの詳細については、GCPドキュメントのシングルテナンシーの概要を参照してください。

単一テナントノードでのVM（マシンプロファイルソース）のプロビジョニングについては、GCPドキュメント「Provision VMs on sole-tenant nodes」を参照してください。

> **注:**
>
> - ノードグループと同じインスタンスタイプとリージョンを選択します。
> - シールドされたVMセクションでvTPMを有効にします。詳細については、クイックスタート：シールドされたVMオプションを有効にするを参照してください。
> - ソースVMでBitlockerを無効にします。

Windows 11のマシンプロファイルソースを使用してMCSマシンカタログを作成する

Web StudioまたはPowerShellコマンドを使用して、Windows 11 VMを作成するためのMCSマシンカタログを作成できます。

> **注:**
>
> - マスターイメージには、Windows 11のスナップショットまたはVMを選択します。
> - マシンプロファイルソースには、Windows 11 VMをマシンプロファイルとして選択します。マシンプロファイルソースは、単一テナントノードで説明されているものと同じインスタンスタイプである必要があります。

> Web Studioの使用方法については、「Web Studioを使用してマシンカタログを作成する」を参照してください。

PowerShellコマンドについては、「マシンプロファイルを使用してマシンカタログを作成する」を参照してください。

カタログを作成し、VM の電源をオンにすると、Google Cloud コンソールで単一テナントノード上で実行されている Windows 11 VM を確認できます。

継承されたラベルを持つ VM とディスク

MCSマシンカタログのVMとディスク（Identity Disk、Write-cache Back Disk、OS disk）は、マシンプロファイルソース（GCP VMインスタンスまたはインスタンステンプレート）のラベルを継承できます。これらのラベルを使用して、異なるチーム（例：team:researchおよびteam:analytics）が所有するインスタンスを区別し、さらにコスト計算や予算編成に利用できます。ラベルの詳細については、GCPドキュメント「ラベルを使用してリソースを整理する」を参照してください。

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

この機能は、永続的および非永続的な MCS マシンカタログに適用されます。

次のことができます。

- 継承されたラベルを持つカタログを作成する
- 継承されたラベルを持つ既存のカタログを更新する
- 継承されたラベルを持つ既存のVMを更新する
- VMとブートディスクのラベルの情報を取得する(#retrieve-information-for-vm-and-boot-disk-labels)
- VMを削除する(#remove-a-vm)

継承されたラベルを持つカタログを作成する

VM とディスクがマシンプロファイルソースからラベルを継承する MCS マシンカタログを作成するには、次の手順を実行します。

1. ラベル付きのマシンプロファイルソース（VMインスタンスまたはインスタンステンプレート）を作成します。ラベル付きVMの作成については、GCPドキュメント「Create resources with labels」を参照してください。インスタンステンプレートはVMから作成され、VMで定義されたラベルを引き継ぎます。
2. Web StudioまたはPowerShellコマンドを使用してMCSカタログを作成します。
3. Web Studioを使用している場合は、**イメージ**ページで**マシンプロファイルを使用**を選択し、VMまたはテンプレートを選択します。

4. PowerShellコマンドを使用している場合、次の操作を行います。

   a. PowerShellウィンドウを開きます。

   b. asnp citrix* を実行します。

   c. IDプールを作成します。IDプールは、作成されるVMのActive Directory (AD) アカウントのコンテナです。

   d. Active Directoryで必要なADコンピューターアカウントを作成します。

   e. カタログを作成するには、`New-ProvScheme`コマンドを実行します。例:

      マシンプロファイル入力としてテンプレートを使用するNew-ProvScheme (永続カタログ):

      ```
      New-ProvScheme `

      -ProvisioningSchemeName "catalog-name" `

      -HostingUnitUid "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" `

      -IdentityPoolUid "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" `

      -MasterImageVM "XDHyp:\HostingUnits\hosting-unit-name\vm-name.vm" `

      -MachineProfile "XDHyp:\HostingUnits\hosting-unit-
      name\instanceTemplates.folder\instance-template-name.template" `
      ```

      マシンプロファイル入力としてインスタンステンプレートを使用するNew-ProvScheme (非永続カタログ):

      ```
      New-ProvScheme `

      -ProvisioningSchemeName "catalog-name" `

      -HostingUnitUid "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" `

      -IdentityPoolUid "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" `

      -MasterImageVM "XDHyp:\HostingUnits\hosting-unit-name\vm-name.vm" `

      -MachineProfile "XDHyp:\HostingUnits\hosting-unit-
      name\instanceTemplates.folder\instance-template-name.template" `
      ```

```
-CleanOnBoot
```

New-ProvScheme と VM インスタンスをマシンプロファイル入力として使用（永続カタログ）：

```
New-ProvScheme `

-ProvisioningSchemeName "catalog-name" `

-HostingUnitUid "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" `

-IdentityPoolUid "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" `

-MasterImageVM "XDHyp:\HostingUnits\hosting-unit-name\vm-name.vm" `

-MachineProfile "XDHyp:\HostingUnits\hosting-unit-name\vm-name.vm" `
```

New-ProvScheme と VM インスタンスをマシンプロファイル入力として使用（非永続カタログ）：

```
New-ProvScheme `

-ProvisioningSchemeName "catalog-name" `

-HostingUnitUid "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" `

-IdentityPoolUid "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" `

-MasterImageVM "XDHyp:\HostingUnits\hosting-unit-name\vm-name.vm" `

-MachineProfile "XDHyp:\HostingUnits\hosting-unit-name\vm-name.vm" `

-CleanOnBoot
```

f. プロビジョニングスキームをブローカーカタログとして登録します。

g. カタログにVMを追加します。

継承されたラベルで既存のカタログを更新する

既存のカタログを新しいマシンプロファイルを持つように更新するには、Set-ProvScheme コマンドを実行します。このコマンドを実行すると、カタログに追加されたすべての新しいVMは、新しいマシンプロファイルソースのラベルを持つようになります。非永続カタログは、次回の電源投入時に更新されます。

例:

Set-ProvScheme とインスタンステンプレートをマシンプロファイル入力として使用：

```
Set-ProvScheme `

-ProvisioningSchemeName "catalog-name" `

-MachineProfile "XDHyp:\HostingUnits\hosting-unit-
name\instanceTemplates.folder\instance-template-name.template" `
```

Set-ProvScheme と VM インスタンスをマシンプロファイル入力として使用：

```
Set-ProvScheme `

-ProvisioningSchemeName "catalog-name" `

-MachineProfile "XDHyp:\HostingUnits\hosting-unit-name\vm-name.vm" `
```

継承されたラベルで既存のVMを更新する

更新されたマシンプロファイルソースで既存のVMを更新するには、次のコマンドを実行します：

1. `Set-ProvScheme`
2. `Set-ProvVMUpdateTimeWindow`。例：

   ```
   Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog -VMName
   <List-Of-Vm-Names> -StartsNow -DurationInMinutes -1
   ```

3. VMを再起動します。

VMおよびブートディスクラベルの情報を取得する

VMを作成した後、`AdditionalData`パラメーターを指定して`Get-Item`コマンドを使用すると、VMおよびブートディスクラベルの情報を取得できます。

VMラベルの情報を取得するには、次のコマンドを実行します。

```
(Get-Item XDHyp:\HostingUnits\hosting-unit-
name\vm_name.vm).AdditionalData.Tags
```

ブートディスクラベルの情報を取得するには、次のコマンドを実行します。

```
(Get-Item XDHyp:\HostingUnits\hosting-unit-name\vm_name.vm\bootdisk-
name.attacheddisk).AdditionalData.Tags
```

注:

さまざまなハイパーバイザー間で一貫性を保つため、GCPラベルを表示するために「タグ」という用語を使用しています。

VMを削除する

カタログからVMを削除することはできますが、GCPからVMを削除しないように選択できます。この場合、Citrixラベルのみがから削除されます。追加された他のすべてのラベルはVMから削除されません。Web StudioまたはPowerShellコマンドを使用してVMを削除できます。

WEB STUDIOを使用する

1. VMを選択して右クリックします。
2. **削除**」をクリックします。
3. **仮想マシンをカタログから削除しますが、仮想マシンは削除しません**を選択します。

POWERSHELLコマンドを使用する

`ForgetVM`パラメーターを指定して`Remove-ProvVM`を実行します。詳細については、SDKドキュメントのRemove-ProvVMを参照してください。

Google Cloud マーケットプレイス

Citrixが**Google Cloud Marketplace**で提供するイメージを参照して選択し、マシンカタログを作成できます。現在、MCSはこの機能に対してマシンプロファイルワークフローのみをサポートしています。

Google Cloud MarketplaceでCitrix VDA VM製品を検索するには、https://console.cloud.google.com/marketplaceにアクセスしてください。

Google Cloud MarketplaceでカスタムイメージまたはCitrix ready®イメージを使用して、マシンカタログのイメージを更新できます。

> **注:**
>
> マシンプロファイルにストレージタイプ情報が含まれていない場合、値はカスタムプロパティから派生します。

> サポートされているGoogle Cloud Marketplaceイメージは次のとおりです。

- Windows 2019シングルセッション
- Windows 2019 マルチセッション
- ウブントゥ

Citrix対応イメージをマシンカタログ作成のソースとして使用する例:

```
New-ProvScheme -ProvisioningSchemeName GCPCatalog \

-HostingUnitName GcpHu -IdentityPoolName gcpPool -CleanOnBoot \

-MasterImageVM XDHyp:\HostingUnits\GcpHu\images.folder\citrix-daas-
win2019-single-vda-v20220819.publicimage \

-MachineProfile XDHyp:\HostingUnits\GcpHu\Base.vm
```

次のステップ

- これが最初に作成されたカタログである場合、Web Studioはデリバリーグループを作成するようにガイドします。
- 構成プロセス全体を確認するには、インストールと構成を参照してください。
- カタログを管理するには、マシンカタログを管理するおよびGoogle Cloud Platformカタログを管理するを参照してください。

詳細情報

- 接続とリソースの作成と管理
- Google Cloud環境への接続(/ja-jp/citrix-virtual-apps-desktops/2503/install-configure/connections/connection-gcp.html)

- マシンカタログの作成(/ja-jp/citrix-virtual-apps-desktops/2503/install-configure/machine-catalogs-create.html)

HPE Moonshotマシンカタログを作成する

マシンカタログを作成するウィザードについては、マシンカタログの作成で説明しています。以下の情報は、HPE Moonshot環境に固有の詳細を扱っています。

> **注:**
>
> - HPE Moonshotへの接続を作成する
> - 1つ以上のHPE Moonshotノードが利用可能であることを確認し、それらのノードにVDAをインストールしてください。
> - 最初のHPE Moonshotカートリッジイメージの作成については、OS Deployment on Moonshot User Guideを参照してください。

HPE Moonshotマシンカタログは、以下を使用して作成できます。

- ウェブスタジオ
- PowerShellコマンド

Web Studioを使用してマシンカタログを作成する

マシンカタログセットアップウィザードで：

1. **オペレーティングシステム**ページで、**マルチセッションOS**または**シングルセッションOS**を選択します。
2. **マシン管理**ページで、**電源管理されているマシン**と**別のサービスまたはテクノロジー**を選択します。
3. **仮想マシン**ページで、マシンとそのActive Directoryマシンアカウントを追加します。以下のいずれかを実行できます。
    - **マシンの追加**をクリックして、マシンを手動で追加します。**VMの選択**ウィンドウが表示されます。以前に作成したHPE Moonshotシャーシ接続を展開し、追加するノード（VM）を選択します。次に、関連するマシンアカウント名を追加します。

- 「**CSVファイルの追加**」をクリックして、マシンを一括追加します。CSVファイルを使用してマシンを追加する方法については、「CSVファイルを使用してマシンをカタログに一括追加する」を参照してください。

スコープページと**概要**ページには、HPE Moonshot固有の情報は含まれていません。

PowerShellコマンドを使用してマシンカタログを作成する

ブローカーカタログを作成し、マシンをブローカーカタログにインポートするには、`New-BrokerCatalog`および`New-BrokerMachine` PowerShellコマンドを実行します。

例:

```
New-BrokerCatalog  -AdminAddress "MyDDC.MyDomain.local" -AdminClientIP
"103.14.252.249" -AllocationType "Random" -IsRemotePC $False
-MachinesArePhysical $False -MinimumFunctionalLevel "L7_20" -Name "BurMC"
-PersistUserChanges "OnLocal" -ProvisioningType "Manual" -Scope @()
-SessionSupport "MultiSession" -ZoneUid "e166e2cb-25dc-4578-bc07-
bcf2a82d1463"

New-BrokerMachine  -AdminAddress "MyDDC.MyDomain.local" -AdminClientIP
"103.14.252.249" -CatalogUid 3 -HostedMachineId "c10n1"
-HypervisorConnectionUid 4 -IsReserved $False -MachineName
"S-1-5-21-2589939477-3963209805-1860259709-1121"
```

次のステップ

- これが最初に作成されたカタログである場合、Web Studioはデリバリーグループの作成を案内します。
- 構成プロセス全体を確認するには、「インストールと構成」を参照してください。
- カタログを管理するには、「マシンカタログの管理」および「HPE Moonshotカタログの管理」を参照してください。

詳細情報

- 接続とリソースの作成および管理
- HPE Moonshotへの接続
- マシンカタログの作成

Microsoft Azureカタログの作成

注:

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

マシンカタログを作成するウィザードについては、(/ja-jp/citrix-virtual-apps-desktops/2503/install-configure/machine-catalogs-create.html)で説明しています。以下の情報は、Microsoft Azure Resource Managerクラウド環境に固有の詳細を扱っています。

注:

Microsoft Azureカタログを作成する前に、Microsoft Azureへの接続の作成を完了する必要があります。(/ja-jp/citrix-virtual-apps-desktops/2503/install-configure/connections/connection-azure-resource-manager.html)を参照してください。

マシンカタログの作成

マシンカタログは、次の2つの方法で作成できます。

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

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

イメージとは、ディスク、スナップショット、またはAzure Compute Gallery内のイメージ定義のイメージバージョンであり、マシンカタログ内のVMを作成するために使用されます。マシンカタログを作成する前に、Azure Resource Managerでイメージを作成します。イメージに関する一般的な情報については、(/ja-jp/citrix-virtual-apps-desktops/2503/install-configure/machine-catalogs-create.html)を参照してください。

注:

ホスト接続で構成されているリージョンとは異なるリージョンからのマスターイメージの使用は非推奨です。Azure Compute Galleryを使用して、マスターイメージを目的のリージョンにレプリケートしてください。

> MCSマシンカタログを作成すると、DHCPの有効化やライセンスの再アクティブ化などの準備タスクを実行するために、元のVMに基づいて一時的なVMが作成されます。この一時的なVMは準備VMと呼ばれます。この準備VMの名前は**Preparati-84x9n**という形式に従い、最後の5文字は重複を避けるためにランダムに生成されます。この準備VMの命名規則は固定されており、カスタマイズできません。準備タスクが完了すると、準備VMは破棄されます。

準備用VMからネットワークを切断するために、すべてのインバウンドおよびアウトバウンドトラフィックを拒否するネットワークセキュリティグループが作成されます。ネットワークセキュリティグループは、カタログごとに1回自動的に作成されます。ネットワークセキュリティグループの名前は`Citrix-Deny-All-a3pgu-GUID`で、GUIDはランダムに生成されます。例: `Citrix-Deny-All-a3pgu-3f161981-28e2-4223-b797-88b04d336dd1`。

マシンカタログ作成ウィザードで:

- **マシンタイプ**ページと**マシン管理**ページには、Azure固有の情報は含まれていません。マシンカタログの作成の記事のガイダンスに従ってください。
- **イメージ**ページで、このカタログにマシンを作成するためのテンプレートとして使用するイメージを選択します。

  使用するイメージタイプとして**マスターイメージ**を選択する場合は、**イメージの選択**をクリックし、必要に応じてマスターイメージを選択するために次の手順に従います。

  a. (テナント内またはテナント間で共有イメージが構成されている接続にのみ適用) イメージが存在するサブスクリプションを選択します。

  b. リソースグループを選択します。

  c. Azure VHD、Azure Compute Gallery、またはAzureイメージバージョンに移動します。必要に応じて、選択したイメージにメモを追加します。

  イメージを選択する際は、次の点を考慮してください。

  - イメージにCitrix VDAがインストールされていることを確認します。
  - VMに接続されているVHDを選択する場合は、次の手順に進む前にVMをシャットダウンする必要があります。

> **注:**
>
> - カタログ内のマシンを作成した接続（ホスト）に対応するサブスクリプションは、緑色の点で示されます。その他のサブスクリプションは、Azure Compute Galleryがそ

のサブスクリプションと共有されているものです。これらのサブスクリプションでは、共有ギャラリーのみが表示されます。共有サブスクリプションの構成方法については、テナント内（サブスクリプション間）でイメージを共有するおよびテナント間でイメージを共有するを参照してください。

- Trusted Launchが有効になっているイメージまたはスナップショットを選択する場合、**セキュリティの種類**としてTrusted Launchを使用するマシンプロファイルの使用が必須です。その後、マシンプロファイルでSecureBootとvTPMの値を指定することで、それらを有効または無効にできます。Trusted LaunchはShared Image Galleryではサポートされていません。Azure Trusted Launchの詳細については、`<https://docs.microsoft.com/ja-jp/azure/virtual-machines/trusted-launch>`を参照してください。
- Trusted Launchが有効なWindowsでエフェメラルOSディスクを使用してプロビジョニングスキームを作成できます。Trusted Launchが有効なイメージを選択する場合、vTPMが有効なTrusted Launchを使用するマシンプロファイルを選択する必要があります。エフェメラルOSディスクを使用してマシンカタログを作成する方法については、エフェメラルOSディスクを使用してマシンを作成する方法を参照してください。
- イメージのレプリケーションが進行中の場合でも、続行してそのイメージをマスターイメージとして選択し、セットアップを完了できます。ただし、イメージのレプリケーション中は、カタログの作成に時間がかかる場合があります。MCSでは、カタログ作成から1時間以内にレプリケーションが完了する必要があります。レプリケーションがタイムアウトすると、カタログ作成は失敗します。Azureでレプリケーションステータスを確認できます。レプリケーションがまだ保留中の場合、またはレプリケーションが完了した後に再試行してください。
- Azureでマシンカタログのマスターイメージを選択すると、MCSは選択したマスターイメージとマシンプロファイルに基づいてOSタイプを識別します。MCSが識別できない場合は、マスターイメージに一致するOSタイプを選択してください。
- Gen2イメージを使用してGen2 VMカタログをプロビジョニングすると、起動時間のパフォーマンスが向上します。ただし、Gen1イメージを使用してGen2マシンカタログを作成することはサポートされていません。同様に、Gen2イメージを使用してGen1マシンカタログを作成することもサポートされていません。また、世代情報を持たない古いイメージはすべてGen1イメージです。

使用するイメージの種類として**準備済みイメージ**を選択する場合は、**イメージの選択**をクリックし、必要に応じて準備済みイメージを選択します。

VMの作成を成功させるには、イメージにCitrix VDA 2311以降がインストールされており、VDAにMCSIOが存在することを確認してください。

イメージを選択すると、**マシンプロファイルを使用する（Azure Active Directoryに必須）**チェックボックスが自動的に選択されます。**マシンプロファイルの選択**をクリックして、リソースグループのリストからVMまたはARMテンプレート仕様を参照します。カタログ内のVMは、選択したマシンプロファイルから構成を継承できます。

ARMテンプレート仕様がマシンカタログを作成するためのマシンプロファイルとして使用できることを確認するために検証します。ARMテンプレート仕様を検証する方法は2つあります。

- リソースグループリストからARMテンプレート仕様を選択した後、**次へ**をクリックします。ARMテンプレート仕様にエラーがある場合、エラーメッセージが表示されます。
- 次のPowerShellコマンドのいずれかを実行します。
  - `Test-ProvInventoryItem -HostingUnitName <string> -InventoryPath <string>`
  - `Test-ProvInventoryItem -HostingUnitUid <Guid> -InventoryPath <string>`

VMがマシンプロファイルから継承できる構成の例を次に示します。

- アクセラレーテッドネットワーク
- ブート診断
- ホストディスクキャッシュ (OSおよびMCSIOディスクに関連)
- マシンサイズ (別途指定がない限り)
- VMに配置されたタグ

カタログを作成した後、イメージがマシンプロファイルから継承する構成を表示できます。**マシンカタログ**ノードでカタログを選択し、下部のペインで詳細を表示します。次に、**テンプレートプロパティ**タブをクリックして、マシンプロファイルのプロパティを表示します。**タグ**セクションには最大3つのタグが表示されます。VMに配置されているすべてのタグを表示するには、**すべて表示**をクリックします。

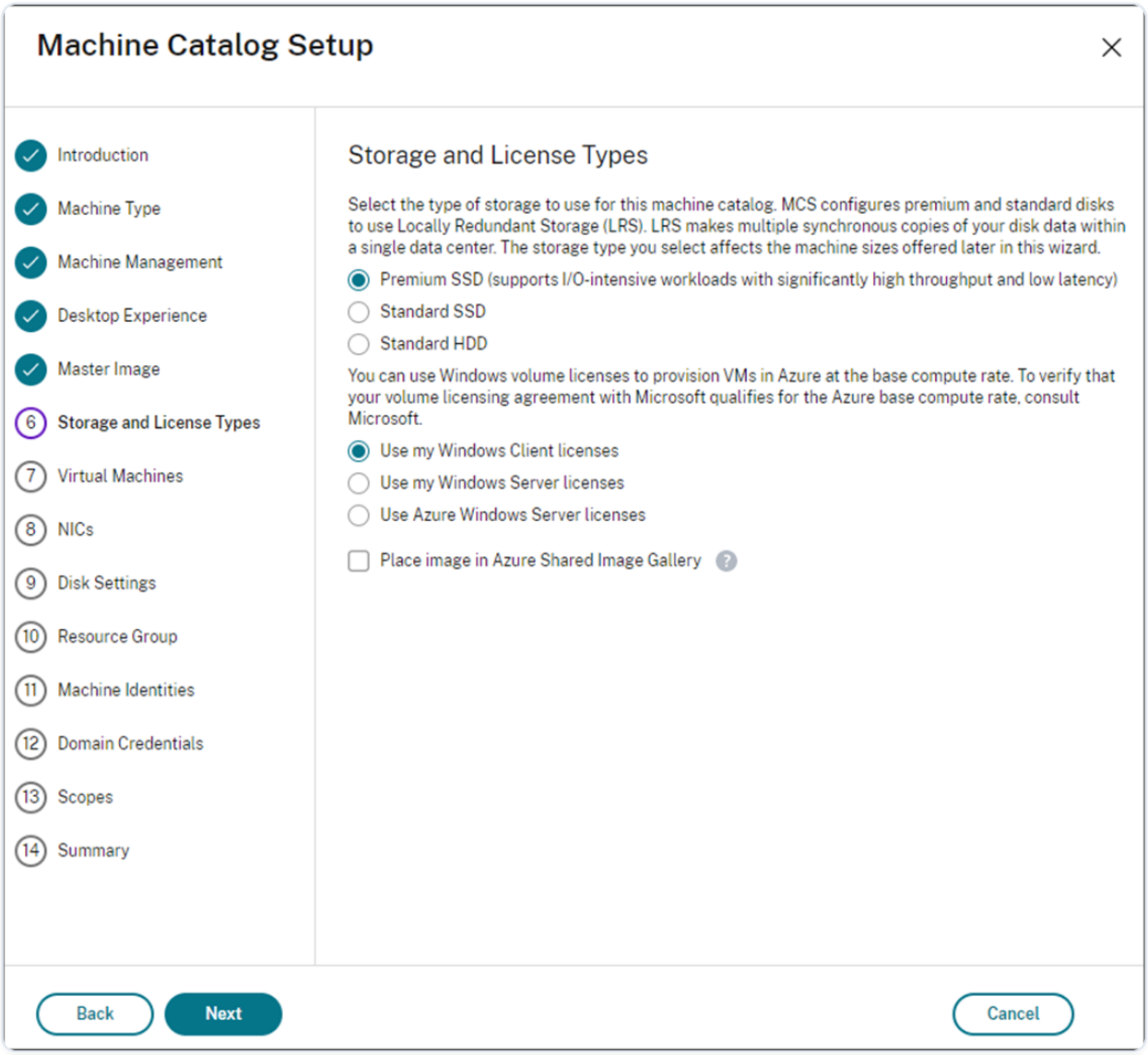
MCSでAzure専用ホストにVMをプロビジョニングする場合は、**専用ホストグループを使用**チェックボックスを有効にしてから、リストからホストグループを選択します。ホストグループは、専用ホストのコレクションを表すリソースです。専用ホストは、1つ以上のVMをホストする物理サーバーを提供するサービスです。サーバーはAzureサブスクリプション専用であり、他のサブスクライバーと共有されることはありません。専用ホストを使用すると、AzureはVMがそのホストで実行されている唯一のマシンであることを保証します。この機能は、規

制要件または内部セキュリティ要件を満たす必要があるシナリオに適しています。ホストグループとその使用に関する考慮事項の詳細については、「Azure 専用ホスト」を参照してください。

重要:

- Azureの自動配置が有効になっているホストグループのみが表示されます。
- ホストグループを使用すると、ウィザードの後半で提供される**仮想マシン**ページが変更されます。そのページには、選択したホストグループに含まれるマシンサイズのみが表示されます。また、可用性ゾーンは自動的に選択され、選択できません。

- **ストレージとライセンスの種類**ページは、Azure Resource Managerイメージを使用する場合にのみ表示されます。



マシンカタログで使用できるストレージの種類は次のとおりです。

- **プレミアム SSD**。I/O集中型ワークロードを持つVMに適した、高性能で低遅延のディスクストレージオプションを提供します。
- **Standard SSD**。低いIOPSレベルで一貫したパフォーマンスを必要とするワークロードに適した、費用対効果の高いストレージオプションを提供します。
- **Standard HDD**。遅延に影響されないワークロードを実行するVMに適した、信頼性の高い低コストのディスクストレージオプションを提供します。
- **Azureエフェメラルosディスク**。VMのローカルディスクを再利用してオペレーティングシステムディスクをホストする、費用対効果の高いストレージオプションを提供します。あるいは、PowerShellを使用してエフェメラルOSディスクを使用するマシンを作成することもできます。詳細については、「Azure エフェメラルディスク」を参照してください。エフェメラルOSディスクを使用する際の以下の考慮事項に注意してください。
  - AzureエフェメラルOSディスクとMCS I/Oは同時に有効にできません。
  - エフェメラルOSディスクを使用するマシンを更新するには、VMのキャッシュディスクまたは一時ディスクのサイズを超えないイメージを選択する必要があります。
  - ウィザードの後半で提供される**電源サイクル中にVMとシステムディスクを保持する**オプションは使用できません。

> **注:**
>
> 選択したストレージの種類に関係なく、IDディスクは常にStandard SSDを使用して作成されます。

> ストレージの種類によって、ウィザードの**仮想マシン**ページで提供されるマシンのサイズが決まります。MCSは、プレミアムディスクと標準ディスクをローカル冗長ストレージ（LRS）を使用するように構成します。LRSは、単一のデータセンター内でディスクデータの複数の同期コピーを作成します。AzureエフェメラルOSディスクは、VMのローカルディスクを使用してオペレーティングシステムを保存します。Azureストレージの種類とストレージレプリケーションの詳細については、以下を参照してください。

- `<https://docs.microsoft.com/ja-jp/azure/storage/common/storage-introduction/>`
- `<https://docs.microsoft.com/ja-jp/azure/virtual-machines/premium-storage-performance/>`

- `<https://docs.microsoft.com/ja-jp/azure/storage/common/storage-redundancy/>`

既存のWindowsライセンスまたはLinuxライセンスを使用するかどうかを選択します。

- Windowsライセンス：WindowsライセンスをWindowsイメージ（Azureプラットフォームサポートイメージまたはカスタムイメージ）とともに使用すると、AzureでWindows VMを低コストで実行できます。ライセンスには次の2種類があります。
  - **Windows Serverライセンス**。Windows ServerまたはAzure Windows Serverライセンスを使用でき、Azureハイブリッド特典を利用できます。詳細については、`<https://azure.microsoft.com/ja-jp/pricing/hybrid-benefit/>`を参照してください。Azureハイブリッド特典は、AzureでのVMの実行コストを基本コンピューティング料金に削減し、Azureギャラリーからの追加のWindows Serverライセンスのコストを免除します。
  - **Windowsクライアントライセンス**。Windows 10およびWindows 11ライセンスをAzureに持ち込むことができ、追加のライセンスなしでAzureでWindows 10およびWindows 11 VMを実行できます。詳細については、「クライアントアクセスライセンスと管理ライセンス」を参照してください。

プロビジョニングされたVMがライセンス特典を使用しているかどうかは、次のPowerShellコマンドを実行して確認できます: `Get-AzVM -ResourceGroup MyResourceGroup -Name MyVM`。

- Windows Serverライセンスタイプの場合、ライセンスタイプが **Windows_Server** であることを確認します。詳細な手順は `<https://docs.microsoft.com/ja-jp/azure/virtual-machines/windows/hybrid-use-benefit-licensing/>` で入手できます。
- Windows Clientライセンスタイプの場合、ライセンスタイプが **Windows_Client** であることを確認します。詳細な手順は `<https://docs.microsoft.com/ja-jp/azure/virtual-machines/windows/windows-desktop-multitenant-hosting-deployment/>` で入手できます。

あるいは、`Get-Provscheme` PowerShell SDKを使用して検証を行うこともできます。例: `Get-Provscheme -ProvisioningSchemeName "My Azure Catalog"`。このコマンドレットの詳細については、`<https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/MachineCreation/Get-ProvScheme/>` を参照してください。

- Linuxライセンス: BYOS (bring-your-own-subscription) Linuxライセンスでは、ソフトウェアの料金を支払う必要はありません。BYOSの料金には、コンピューティングハードウェア料金のみが含まれます。ライセンスには次の2種類があります。
  - **RHEL_BYOS**: RHEL_BYOSタイプを正常に使用するには、AzureサブスクリプションでRed Hat Cloud Accessを有効にします。
  - **SLES_BYOS**: SLESのBYOSバージョンには、SUSEからのサポートが含まれています。

LicenseTypeの値を、`New-ProvScheme` および `Set-ProvScheme` のLinuxオプションに設定できます。

`New-ProvScheme` でLicenseTypeをRHEL_BYOSに設定する例:

```
New-ProvScheme -CleanOnBoot -ProvisioningSchemeName "azureCatalog"
-RunAsynchronously -Scope @() -SecurityGroup @() -CustomProperties
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance"><Property xsi:type="StringProperty" Name="UseManagedDisks"
Value="true" /><Property xsi:type="StringProperty"
Name="StorageAccountType" Value="StandardSSD_LRS" /><Property
xsi:type="StringProperty" Name="ResourceGroups" Value="hu-dev-mcs" /
><Property xsi:type="StringProperty" Name="OsType" Value="Linux" /
><Property xsi:type="StringProperty" Name="LicenseType"
Value="RHEL_BYOS" /></CustomProperties>'
```

`Set-ProvScheme` でLicenseTypeをSLES_BYOSに設定する例:

```
Set-ProvScheme -ProvisioningSchemeName "azureCatalog"
-CustomProperties '<CustomProperties xmlns="http://
schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance"><Property
xsi:type="StringProperty" Name="UseManagedDisks" Value="true" /
><Property xsi:type="StringProperty" Name="StorageAccountType"
Value="StandardSSD_LRS" /><Property xsi:type="StringProperty"
Name="ResourceGroups" Value="hu-dev-mcs" /><Property
xsi:type="StringProperty" Name="OsType" Value="Linux" /><Property
xsi:type="StringProperty" Name="LicenseType" Value="SLES_BYOS" /></
CustomProperties>'
```

> **注:**
>
> `LicenseType` の値が空の場合、デフォルト値はOsTypeの値に応じて、Azure Windows Server LicenseまたはAzure Linux Licenseになります。

> LicenseType を空に設定する例:

```
Set-ProvScheme -ProvisioningSchemeName "azureCatalog"
-CustomProperties '<CustomProperties xmlns="http://
schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance"><Property
xsi:type="StringProperty" Name="UseManagedDisks" Value="true" /
><Property xsi:type="StringProperty" Name="StorageAccountType"
Value="StandardSSD_LRS" /><Property xsi:type="StringProperty"
Name="ResourceGroups" Value="hu-dev-mcs" /><Property
xsi:type="StringProperty" Name="OsType" Value="Linux" /></
CustomProperties>'
```

ライセンスの種類とその利点については、以下のドキュメントを参照してください。

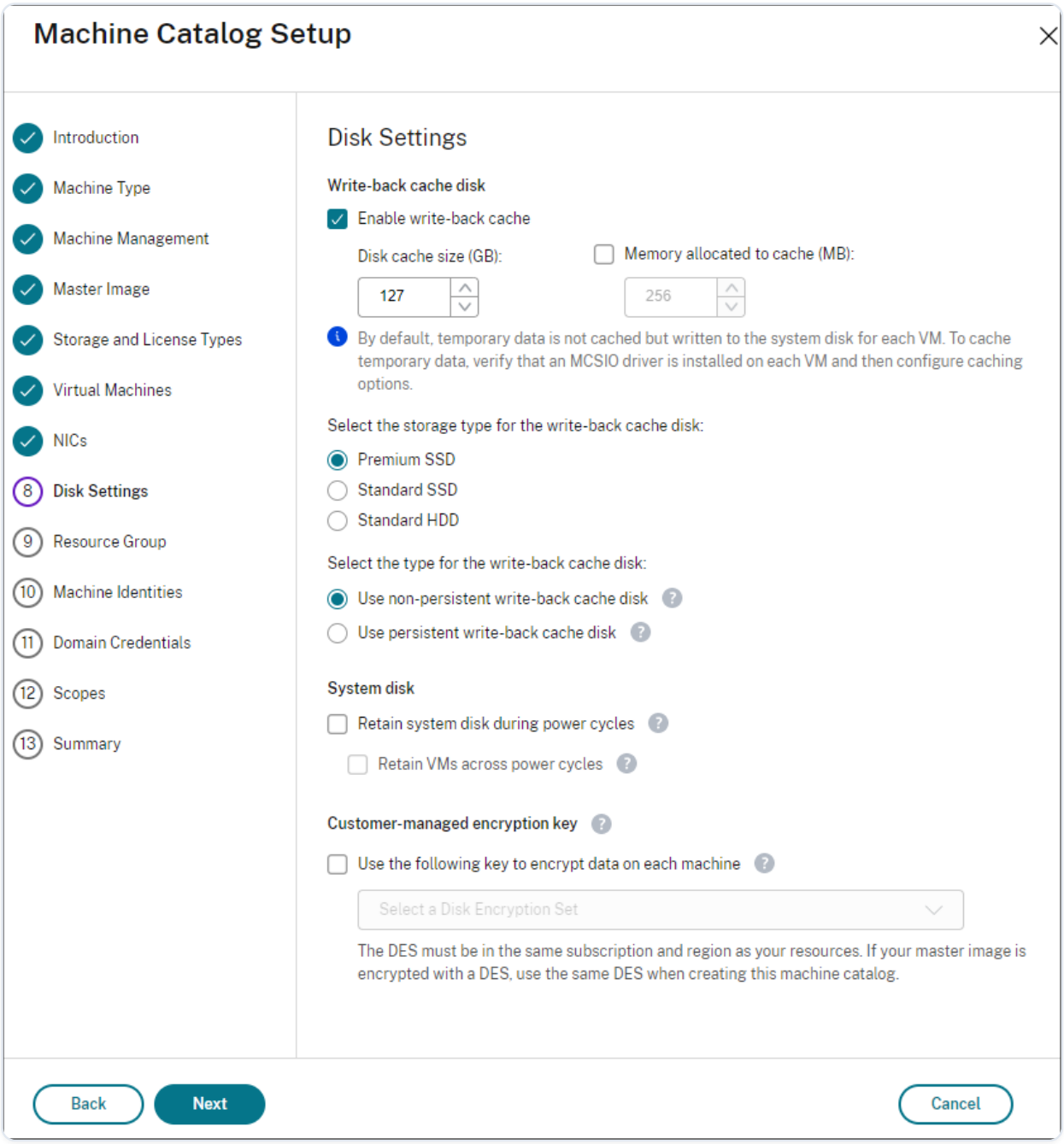
- `<https://docs.microsoft.com/ja-jp/dotnet/api/microsoft.azure.management.compute.models.virtualmachine.licensetype?view=azure-dotnet>`
- `<https://docs.microsoft.com/ja-jp/azure/virtual-machines/linux/azure-hybrid-benefit-linux>`

Azure Compute Gallery (旧称 Azure Shared Image Gallery) は、イメージを管理および共有するためのリポジトリです。これにより、組織全体でイメージを利用できるようになります。大規模な非永続マシンカタログを作成する際には、VDA OSディスクのリセットが高速化されるため、イメージをSIGに保存することをお勧めします。 を選択すると、 セクションが表示され、Azure Compute Gallery の詳細設定を指定できます。

- **仮想マシンとイメージレプリカの比率**。Azureが保持する仮想マシンとイメージレプリカの比率を指定できます。デフォルトでは、Azureは非永続マシン40台ごとに1つのイメージレプリカを保持します。永続マシンの場合、この数はデフォルトで1,000です。
- **最大レプリカ数**。Azure に保持させるイメージレプリカの最大数を指定できます。デフォルトは 100 です。

> **注:**
>
> イメージを保存するために、ACG にギャラリーが作成されます。このギャラリーは、VM 作成のために MCS からのみアクセス可能であり、**イメージの選択**ページには表示されません。

- **仮想マシン**ページで、作成するVMの数を指定します。少なくとも1つを指定し、マシンサイズを選択する必要があります。カタログ作成後、カタログを編集することでマシンサイズを変更できます。
- **NIC**ページには、Azure固有の情報は含まれていません。(/ja-jp/citrix-virtual-apps-desktops/2503/install-configure/machine-catalogs-create.html#nic)の記事のガイダンスに従ってください。
- **ディスク設定**ページで、ライトバックキャッシュを有効にするかどうかを選択します。MCS ストレージ最適化機能が有効になっている場合、カタログ作成時に以下の設定を構成できます。これらの設定は、Azure と GCP の両方の環境に適用されます。



ライトバックキャッシュを有効にすると、次のことができます。

- 一時データのキャッシュに使用されるディスクとRAMのサイズを構成します。詳しくは、(/ja-jp/citrix-virtual-apps-desktops/2503/install-configure/machine-catalogs-create.html#configure-cache-for-temporary-data)を参照してください。
- ライトバックキャッシュディスクのストレージタイプを選択します。ライトバックキャッシュディスクに使用できるストレージオプションは次のとおりです。
  - プレミアム SSD
  - スタンダード SSD
  - スタンダード HDD

- プロビジョニングされたVMに対してライトバックキャッシュディスクを永続化するかどうかを選択します。オプションを有効にするには、**ライトバックキャッシュを有効にする**を選択します。デフォルトでは、**非永続ライトバックキャッシュディスクを使用する**が選択されています。
- ライトバックキャッシュディスクの種類を選択します。
  - **非永続的なライトバックキャッシュディスクを使用する**。選択した場合、ライトバックキャッシュディスクは電源サイクル中に削除されます。そこにリダイレクトされたデータはすべて失われます。VMの一時ディスクに十分な空き容量がある場合、コストを削減するためにライトバックキャッシュディスクをホストするために使用されます。カタログ作成後、プロビジョニングされたマシンが一時ディスクを使用しているかどうかを確認できます。そのためには、カタログをクリックし、**テンプレートプロパティ**タブの情報を確認します。一時ディスクが使用されている場合、**非永続的なライトバックキャッシュディスク**と表示され、その値は**はい（VMの一時ディスクを使用）**となります。そうでない場合、非永続的なライトバックキャッシュディスクと表示され、その値は**いいえ（VMの一時ディスクを使用しない）**となります。
  - **永続的なライトバックキャッシュディスクを使用する**。選択した場合、ライトバックキャッシュディスクはプロビジョニングされたVMに対して永続化されます。このオプションを有効にすると、ストレージコストが増加します。
- 電源サイクル中にVDAのVMとシステムディスクを保持するかどうかを選択します。

  電源サイクル中にVMとシステムディスクを保持する。ライトバックキャッシュを有効にするを選択した場合に利用可能です。デフォルトでは、VMとシステムディスクはシャットダウン時に削除され、起動時に再作成されます。VMの再起動時間を短縮したい場合は、このオプションを選択します。このオプションを有効にすると、ストレージコストも増加することに注意してください。
- **ストレージコストの節約**を有効にするかどうかを選択します。有効にすると、VMがシャットダウンしたときにストレージディスクをStandard HDDにダウングレードすることで、ストレージコストを節約できます。VMは再起動時に元の設定に戻ります。このオプションは、ストレージディスクとライトバックキャッシュディスクの両方に適用されます。または、PowerShellを使用することもできます。VMシャットダウン時にストレージタイプを下位層に変更するを参照してください。

> **注:**

> Microsoftは、VMシャットダウン中のストレージタイプの変更に制限を課しています。また、Microsoftが将来的にストレージタイプの変更をブロックする可能性もあります。詳細については、このMicrosoftの記事を参照してください。

- このカタログ内のマシン上のデータを暗号化するかどうか、およびどの暗号化キーを使用するかを選択します。顧客管理キー（CMK）によるサーバー側暗号化を使用すると、マネージドディスクレベルで暗号化を管理し、カタログ内のマシン上のデータを保護できます。デフォルト設定は、マシンプロファイルまたはマスターイメージのいずれかから継承され、プロファイルが優先されます。
  - *CMK*を使用する*マシンプロファイル*を使用している場合、**各マシン上のデータを暗号化するために次のキーを使用する**オプションが自動選択され、*マシンプロファイル*からのキーがデフォルトになります。
  - プラットフォーム管理キー（PMK）を使用する*マシンプロファイル*を使用しており、*マスターイメージ*が*CMK*で暗号化されている場合、**各マシン上のデータを暗号化するために次のキーを使用する**オプションが自動選択され、マスターイメージからのキーがデフォルトになります。
  - *マシンプロファイル*を*使用していない*場合、および*マスターイメージ*が*CMK*で暗号化されている場合、**各マシン上のデータを暗号化するために次のキーを使用する**オプションが自動選択され、*マスターイメージ*からのキーがデフォルトになります。

  詳細については、Azureサーバー側暗号化を参照してください。

- **リソースグループ** ページで、リソースグループを作成するか、既存のグループを使用するかを選択します。
  - リソースグループを作成することを選択した場合は、**次へ**を選択します。
  - 既存のリソースグループを使用することを選択した場合は、**利用可能なプロビジョニングリソースグループ**リストからグループを選択します。**注意**: カタログで作成するマシンを収容するのに十分なグループを選択してください。選択が少なすぎるとメッセージが表示されます。後でカタログにVMを追加する予定がある場合は、必要最小限よりも多く選択することをお勧めします。カタログ作成後に、カタログにリソースグループを追加することはできません。

  詳細については、「Azure リソースグループ」を参照してください。

- **マシンID**ページで、IDタイプを選択し、このカタログ内のマシン用のIDを構成します。VM を **Azure Active Directory に参加済み**として選択した場合、それらを Azure AD セキュリティグループに追加できます。詳細な手順は次のとおりです。

a. **IDの種類**フィールドから、**Azure Active Directory参加済み**を選択します。**Azure ADセキュリティグループ (オプション)**オプションが表示されます。

b. **Azure ADセキュリティグループ: 新規作成**をクリックします。

c. グループ名を入力し、**作成**をクリックします。

d. 画面の指示に従って Azure にサインインします。 グループ名が Azure に存在しない場合、緑色のアイコンが表示されます。それ以外の場合は、新しい名前を入力するよう求めるエラーメッセージが表示されます。

e. VM のマシンアカウントの命名スキームを入力します。

カタログ作成後、Citrix Virtual Apps and Desktops™はユーザーに代わってAzureにアクセスし、セキュリティグループとグループの動的メンバーシップルールを作成します。このルールに基づいて、このカタログで指定された命名スキームを持つVMは自動的にセキュリティグループに追加されます。

異なる命名スキームを持つVMをこのカタログに追加するには、Azureにサインインする必要があります。Citrix Virtual Apps and Desktopsは、Azureにアクセスして、新しい命名スキームに基づいて動的メンバーシップルールを作成できます。

このカタログを削除する際、Azure からセキュリティグループを削除するには、Azure へのサインインも必要です。

- **ドメイン資格情報**および**概要**ページには、Azure固有の情報は含まれていません。「マシンカタログの作成」の記事のガイダンスに従ってください。

ウィザードを完了します。

Azure一時ディスクがライトバックキャッシュディスクとして適格であるための条件

Azure一時ディスクをライトバックキャッシュディスクとして使用できるのは、以下のすべての条件が満たされている場合のみです。

- Azure一時ディスクは永続的なデータに適していないため、ライトバックキャッシュディスクは非永続的である必要があります。
- 選択したAzure VMサイズには一時ディスクが含まれている必要があります。
- エフェメラルOSディスクを有効にする必要はありません。
- ライトバックキャッシュファイルをAzure一時ディスクに配置することを受け入れます。
- Azure一時ディスクのサイズは、（ライトバックキャッシュディスクサイズ + ページングファイル用の予約スペース + 1 GBのバッファースペース）の合計サイズよりも大きい必要があります。

非永続的なライトバックキャッシュディスクのシナリオ

次の表は、マシンカタログの作成時に一時ディスクをライトバックキャッシュに使用する場合の3つの異なるシナリオについて説明しています。

シナリオ	結果
ライトバックキャッシュに一時ディスクを使用するためのすべての条件が満たされています。	WBCファイル `mcsdif.vhdx` は一時ディスクに配置されます。
一時ディスクには、ライトバックキャッシュの使用に十分なスペースがありません。	VHDディスク `MCSWCDisk` が作成され、WBCファイル `mcsdif.vhdx` がこのディスクに配置されます。
一時ディスクにはライトバックキャッシュの使用に十分なスペースがありますが、`UseTempDiskForWBC` が **false** に設定されています。	VHDディスク `MCSWCDisk` が作成され、WBCファイル `mcsdif.vhdx` がこのディスクに配置されます。

Azure テンプレート仕様を作成する

Azure ポータルで Azure テンプレート仕様を作成し、Web Studio および PowerShell コマンドで使用して、MCS マシンカタログを作成または更新できます。

既存のVMのAzureテンプレートスペックを作成するには：

1. Azure portalに移動します。リソースグループを選択し、VMとネットワークインターフェイスを選択します。上部の**...**メニューから、**テンプレートのエクスポート**をクリックします。
2. カタログプロビジョニング用のテンプレートスペックを作成する場合は、**パラメーターを含める**チェックボックスをオフにします。JSONファイルで `parameters` および `variables` セクションが次のようになっていることを確認します。

   ```
   "parameters": {},

   "variables": {}
   ```

3. **ダウンロード**をクリックして、テンプレートをJSONファイルとして保存します。
4. Azureポータルで、**テンプレートスペック**を選択し、**テンプレートのインポート**をクリックします。

5. コンピューターに保存されているマシンプロファイル（JSON形式）を参照してインポートします。
6. **名前、サブスクリプション、リソースグループ、場所、バージョン**を指定します。**次へ: テンプレートの編集**をクリックします。
7. **確認と作成**を作成し、テンプレートスペックを作成します。
8. **テンプレートスペック**ページで、作成したばかりのテンプレートスペックを確認します。テンプレートスペックをクリックします。左側のパネルで、**バージョン**をクリックします。
9. **新しいバージョンの作成**をクリックして、新しいバージョンを作成できます。新しいバージョン番号を指定し、現在のテンプレートスペックに変更を加え、**確認と作成**をクリックして、テンプレートスペックの新しいバージョンを作成します。

以下のPowerShellコマンドを使用して、テンプレートスペックとテンプレートバージョンの情報を取得できます。

- テンプレートスペックの情報を取得するには、以下を実行します。

```
get-item XDHyp:
\HostingUnits\East\machineprofile.folder\abc.resourcegroup\bggTemplateS
pec.templatespec
```

- テンプレートスペックバージョンの情報を取得するには、以下を実行します。

```
get-item XDHyp:
\HostingUnits\East\machineprofile.folder\abc.resourcegroup\bggTemplateS
pec.templatespec\bgg1.0.templatespecversion
```

カタログの作成または更新でのテンプレートスペックの使用

テンプレート仕様をマシンプロファイル入力として使用して、MCSマシンカタログを作成または更新できます。これを行うには、Web StudioまたはPowerShellコマンドを使用します。

- Web Studioについては、「Web StudioでAzure Resource Managerイメージを使用してマシンカタログを作成する」を参照してください。
- PowerShellについては、「PowerShellを使用してカタログを作成または更新する際にテンプレート仕様を使用する」を参照してください。

Azureサーバー側暗号化

Citrix Virtual Apps and Desktopsは、Azure Key Vaultを介したAzureマネージドディスクの顧客管理暗号化キーをサポートしています。このサポートにより、独自の暗号化キーを使用してマシンカタログのマネージドディスクを暗号化することで、組織およびコンプライアンス要件を管理できます。詳しくは、「Azure Disk Storageのサーバー側暗号化」を参照してください。

マネージドディスクでこの機能を使用する場合：

- ディスクの暗号化に使用するキーを変更するには、`DiskEncryptionSet` で現在のキーを変更します。その `DiskEncryptionSet` に関連付けられているすべてのリソースは、新しいキーで暗号化されるように変更されます。
- キーを無効にするか削除すると、そのキーを使用しているディスクを持つVMは自動的にシャットダウンします。シャットダウン後、キーが再度有効になるか、新しいキーを割り当てない限り、VMは使用できません。そのキーを使用しているカタログは電源をオンにできず、VMを追加することもできません。

顧客管理暗号化キーを使用する際の重要な考慮事項

この機能を使用する際は、次の点を考慮してください。

- 顧客管理キーに関連するすべてのリソース（Azure Key Vault、ディスク暗号化セット、VM、ディスク、スナップショット）は、同じサブスクリプションとリージョンに存在する必要があります。
- 顧客管理キーで暗号化されたディスク、スナップショット、およびイメージは、別のリソースグループやサブスクリプションに移動できません。
- リージョンごとのディスク暗号化セットの制限については、Microsoftサイトを参照してください。

> **注:**
>
> Azureサーバー側暗号化の構成については、「クイックスタート: Azureポータルを使用してKey Vaultを作成する」を参照してください。

Azureカスタマーマネージド暗号化キー

マシンカタログを作成する際、カタログでプロビジョニングされたマシン上のデータを暗号化するかどうかを選択できます。顧客管理の暗号化キーによるサーバー側暗号化を使用すると、マネージドディスクレベルで暗号化を管理し、カタログ内のマシン上のデータを保護できます。ディスク

暗号化セット (DES) は、顧客管理キーを表します。この機能を使用するには、まずAzureでDESを作成する必要があります。DESは次の形式です:

- `/subscriptions/12345678-1234-1234-1234-123456789012/resourceGroups/Sample-RG/providers/Microsoft.Compute/diskEncryptionSets/SampleEncryptionSet`

リストからDESを選択します。選択するDESは、リソースと同じサブスクリプションおよびリージョンにある必要があります。

を参照してください(#create-a-machine-catalog-with-customer-managed-encryption-key)。

Azure ホストでのディスク暗号化

ホストでの暗号化機能を持つMCSマシンカタログを作成できます。現在、MCSはこの機能に対してマシンプロファイルワークフローのみをサポートしています。マシンプロファイルの入力として、VMまたはテンプレート仕様を使用できます。

この暗号化方法は、Azureストレージを介してデータを暗号化しません。VMをホストするサーバーがデータを暗号化し、その後、暗号化されたデータがAzureストレージサーバーを介して流れます。したがって、この暗号化方法はデータをエンドツーエンドで暗号化します。

制限事項：

Azure ホストでのディスク暗号化は次のとおりです:

- すべてのAzureマシンサイズでサポートされているわけではありません
- Azure ディスク暗号化と互換性がありません

ホストでの暗号化機能を持つマシンカタログを作成するには:

1. サブスクリプションでホストでの暗号化機能が有効になっているかどうかを確認します。これを行うには、`<https://learn.microsoft.com/ja-jp/rest/api/resources/features/get?tabs=HTTP/>`を参照してください。有効になっていない場合は、サブスクリプションでこの機能を有効にする必要があります。サブスクリプションで機能を有効にする方法については、`<https://learn.microsoft.com/ja-jp/azure/virtual-machines/disks-enable-host-based-encryption-portal?tabs=azure-powershell#prerequisites/>`を参照してください。
2. 特定のAzure VMサイズがホストでの暗号化をサポートしているかどうかを確認します。これを行うには、PowerShellウィンドウで次のいずれかを実行します:

```
PS XDHyp:\Connections\<your connection>\east
us.region\serviceoffering.folder>
```

```
PS XDHyp:\HostingUnits\<your hosting unit>\serviceoffering.folder>
```

3. Azure portal で、ホストでの暗号化を有効にして、マシンプロファイルの入力としてVMまたはテンプレート仕様を作成します。
   - VMを作成する場合は、ホストでの暗号化をサポートするVMサイズを選択します。VMを作成すると、VMプロパティの**Encryption at host**が有効になります。
   - テンプレート仕様を使用する場合は、`securityProfile`内でパラメーター`Encryption at Host`を**true**として割り当てます。
4. VMまたはテンプレート仕様のいずれかを選択して、マシンプロファイルワークフローでMCSマシンカタログを作成します。
   - OSディスク/データディスク：顧客管理キーとプラットフォーム管理キーを介して暗号化されます
   - エフェメラルOSディスク：プラットフォーム管理キーのみを介して暗号化されます
   - キャッシュディスク: 顧客管理キーとプラットフォーム管理キーによって暗号化されます

   Web Studioを使用するか、PowerShellコマンドを実行して、マシンカタログを作成できます。

マシンプロファイルからホストでの暗号化情報を取得する

`AdditionalData` パラメーターを指定して PowerShell コマンドを実行すると、マシンプロファイルからホストでの暗号化情報を取得できます。`EncryptionAtHost` パラメーターが **True** の場合、そのマシンプロファイルでホストでの暗号化が有効になっていることを示します。

例: マシンプロファイルの入力が VM の場合、次のコマンドを実行します。

```
(get-item XDHyp:
\HostingUnits\myAzureNetwork\machineprofile.folder\abc.resourcegroup\def.v
m).AdditionalData
```

例: マシンプロファイルの入力がテンプレート仕様の場合、次のコマンドを実行します。

```
(get-item XDHyp:
\HostingUnits\myAzureNetwork\machineprofile.folder\abc.resourcegroup\def_t
emplatespec.templatespec\EncryptionAtHost.templatespecversion).AdditionalD
ata
```

マネージドディスクでの二重暗号化

二重暗号化を使用してマシンカタログを作成できます。この機能で作成されたカタログはすべて、プラットフォームキーと顧客管理キーの両方でサーバー側で暗号化されたディスクを持ちます。Azure Key Vault、Encryption Key、およびDisk Encryption Sets (DES) はお客様が所有および管理します。

二重暗号化は、プラットフォーム側暗号化（デフォルト）と顧客管理暗号化（CMEK）です。したがって、暗号化アルゴリズム、実装、または侵害されたキーに関連するリスクを懸念するセキュリティ意識の高いお客様は、この二重暗号化を選択できます。永続OSディスクとデータディスク、スナップショット、およびイメージはすべて、二重暗号化によって保存時に暗号化されます。

注記：

- Web Studio および PowerShell コマンドを使用して、二重暗号化されたマシンカタログを作成および更新できます。PowerShell コマンドについては、「二重暗号化されたマシンカタログの作成」を参照してください。
- 二重暗号化されたマシンカタログを作成または更新するには、マシンプロファイルに基づかないワークフローまたはマシンプロファイルに基づくワークフローを使用できます。
- マシンプロファイルに基づかないワークフローを使用してマシンカタログを作成する場合、保存されている `DiskEncryptionSetId` を再利用できます。
- マシンプロファイルを使用する場合、VM またはテンプレート仕様をマシンプロファイルの入力として使用できます。

制限事項：

- 二重暗号化は、Ultra Disks または Premium SSD v2 ディスクではサポートされていません。
- 二重暗号化は、アンマネージドディスクではサポートされていません。
- カタログに関連付けられている DiskEncryptionSet キーを無効にすると、そのカタログの VM は無効になります。

- お客様が管理するキーに関連するすべてのリソース (Azure Key Vault、ディスク暗号化セット、VM、ディスク、およびスナップショット) は、同じサブスクリプションおよびリージョンにある必要があります。
- サブスクリプションあたり、リージョンあたりで作成できるディスク暗号化セットは最大 50 個です。

Azure リソースグループ

Azure プロビジョニングリソースグループは、ユーザーにアプリケーションとデスクトップを提供する VM をプロビジョニングする方法を提供します。MCS マシンカタログで VM をプロビジョニングするために、リソースグループを作成するか、既存のリソースグループを使用できます。複数のマシンカタログで同じリソースグループを使用できます。Azure リソースグループの詳細については、Microsoft ドキュメント を参照してください。

Azure リソースグループの使用状況

Azure リソースグループあたりの仮想マシン、マネージドディスク、スナップショット、およびイメージの数に制限はありません。(Azure リソースグループあたり 800 個のマネージドディスクあたり 240 個の VM という制限は削除されました。)

- フルスコープのサービスプリンシパルを使用してマシンカタログを作成する場合、MCS は 1 つの Azure リソースグループのみを作成し、そのグループをカタログに使用します。
- ナロースコープのサービスプリンシパルを使用してマシンカタログを作成する場合、空の、事前に作成された Azure リソースグループをカタログに提供する必要があります。

Azureエフェメラルディスク

An Azure エフェメラルディスク を使用すると、キャッシュディスクまたは一時ディスクを再利用して、Azure 対応仮想マシンの OS ディスクを保存できます。この機能は、標準の HDD ディスクよりも高性能な SSD ディスクを必要とする Azure 環境で役立ちます。Azure エフェメラルディスクを使用してカタログを作成する方法については、Azure エフェメラルディスクを使用してカタログを作成する を参照してください。

> **注:**
>
> 永続カタログはエフェメラルOSディスクをサポートしていません。

> エフェメラル OS ディスクには、プロビジョニングスキームでマネージドディスクと共有イメージギャラリーを使用する必要があります。

エフェメラルOS一時ディスクの保存

エフェメラルOSディスクをVMの一時ディスクまたはリソースディスクに保存するオプションがあります。この機能により、キャッシュがない、またはキャッシュが不十分なVMでエフェメラルOSディスクを使用できます。このようなVMには、`Ddv4`などのエフェメラルOSディスクを保存するための一時ディスクまたはリソースディスクがあります。

次の点を考慮してください。

- エフェメラルディスクは、VM キャッシュディスクまたは VM の一時 (リソース) ディスクのいずれかに保存されます。キャッシュディスクが OS ディスクの内容を保持するのに十分な大きさでない限り、一時ディスクよりもキャッシュディスクが優先されます。
- 更新の場合、キャッシュディスクより大きく、一時ディスクより小さい新しいイメージは、エフェメラル OS ディスクを VM の一時ディスクに置き換えることになります。

AzureエフェメラルディスクとMachine Creation Services (MCS) ストレージ最適化 (MCS I/O)

AzureエフェメラルOSディスクとMCS I/Oは同時に有効にできません。

重要な考慮事項は次のとおりです。

- エフェメラルOSディスクとMCS I/Oの両方を同時に有効にしてマシンカタログを作成することはできません。
- PowerShellパラメーター (`UseWriteBackCache` および `UseEphemeralOsDisk`) を `New-ProvScheme` または `Set-ProvScheme` で**true**に設定すると、適切なエラーメッセージが表示されて失敗します。
- 両方の機能が有効になっている既存のマシンカタログについては、引き続き以下を行うことができます。
  - マシンカタログを更新する。
  - VMを追加または削除する。
  - マシンカタログを削除する。

Azure コンピュート ギャラリー

Azure Compute Gallery (旧称 Azure Shared Image Gallery) を、AzureでMCSプロビジョニングされたマシンの公開イメージリポジトリとして使用します。公開イメージをギャラリーに保存することで、OSディスクの作成とハイドレーションを高速化し、非永続VMの起動時間とアプリケーション起動時間を改善できます。共有イメージギャラリーには、次の3つの要素が含まれています。

- *ギャラリー*: イメージはここに保存されます。MCSは、マシンカタログごとに1つのギャラリーを作成します。

- *ギャラリーイメージ定義*: この定義には、公開イメージに関する情報 (オペレーティングシステムの種類と状態、Azureリージョン) が含まれます。MCSは、カタログ用に作成されたイメージごとに1つのイメージ定義を作成します。
- *ギャラリーイメージバージョン*: 共有イメージギャラリー内の各イメージは複数のバージョンを持つことができ、各バージョンは異なるリージョンに複数のレプリカを持つことができます。各レプリカは、公開イメージの完全なコピーです。

> **注:**
>
> 共有イメージギャラリー機能は、マネージドディスクとのみ互換性があります。レガシーマシンカタログでは使用できません。

> 詳しくは、「Azure Compute Galleryの概要」を参照してください。

PowerShell を使用して Azure Compute Gallery イメージでマシンカタログを作成または更新する方法については、「Azure Compute Gallery イメージを使用してマシンカタログを作成または更新する」を参照してください。

Azure 機密 VM

Azure 機密コンピューティング VM は、仮想デスクトップがメモリ内で暗号化され、使用中に保護されることを保証します。

MCS を使用して、Azure 機密 VM を含むカタログを作成できます。このようなカタログを作成するには、マシンプロファイルワークフローを使用する必要があります。マシンプロファイルの入力として、VM と ARM テンプレート仕様の両方を使用できます。

機密 VM に関する重要な考慮事項

サポートされている VM サイズと機密 VM を使用したマシンカタログの作成に関する重要な考慮事項は次のとおりです。

- サポートされている VM サイズ: 機密 VM は、次の VM サイズをサポートしています。
  - DCasv5 シリーズ
  - DCadsv5 シリーズ
  - ECasv5 シリーズ
  - ECadsv5 シリーズ
- 機密 VM を使用してマシンカタログを作成します。

- Web Studio および PowerShell コマンドを使用して、Azure 機密 VM を含むマシンカタログを作成できます。
- Azure 機密 VM を含むマシンカタログを作成するには、マシンプロファイルベースのワークフローを使用する必要があります。マシンプロファイルの入力として、VM またはテンプレート仕様を使用できます。
- マスターイメージとマシンプロファイルの入力は、両方とも同じ機密セキュリティタイプで有効にする必要があります。セキュリティタイプは次のとおりです。
  - **VMGuestStateOnly**: VM ゲストの状態のみが暗号化された機密 VM
  - **DiskWithVMGuestState**: OSディスクとVMゲスト状態の両方がプラットフォームマネージドキーまたはカスタマーマネージドキーで暗号化された機密VM。通常のOSディスクとエフェメラルOSディスクの両方を暗号化できます。
- マネージドディスク、スナップショット、Azure Compute Galleryイメージ、VM、ARMテンプレート仕様など、さまざまなリソースタイプの機密VM情報を、AdditionalDataパラメーターを使用して取得できます。例:

  ```
  PS C:\Users\username> (get-item XDHyp:
  \HostingUnits\mynetwork\image.folder\username-dev-testing-
  rg.resourcegroup\username-dev-tsvda.vm).AdditionalData
  ```

  追加データフィールドは次のとおりです。
  - DiskSecurityType
  - ConfidentialVMDiskEncryptionSetId
  - DiskSecurityProfiles

  マシンサイズの機密コンピューティングプロパティを取得するには、次のコマンドを実行します: `(Get-Item -path "XDHyp:\Connections\my-connection-name\East US.region\serviceoffering.folder\abc.serviceoffering").AdditionalData`

  追加データフィールドは`ConfidentialComputingType`です。
- マスターイメージまたはマシンプロファイルを、機密から非機密セキュリティタイプへ、あるいは非機密から機密セキュリティタイプへ変更することはできません。
- 不適切な構成の場合、適切なエラーメッセージが表示されます。

マスターイメージとマシンプロファイルを準備する

一連の機密VMを作成する前に、次の手順に従ってそれらのマスターイメージとマシンプロファイルを準備します。

1. Azureポータルで、次のような特定の構成で機密VMを作成します。
   - **セキュリティの種類**: 機密仮想マシン
   - **機密OSディスク暗号化**: 有効。
   - **キー管理**: プラットフォーム管理キーによる機密ディスク暗号化 機密VMの作成に関する詳細については、こちらのMicrosoft記事を参照してください。
2. 作成したVMでマスターイメージを準備します。作成したVMに必要なアプリケーションとVDAをインストールします。

   > **注:**
   >
   > VHDを使用した機密VMの作成はサポートされていません。代わりに、Azure Compute Gallery、マネージドディスク、またはスナップショットを使用してください。

3. 次のいずれかの方法でマシンプロファイルを作成します。
   - ステップ1で作成した既存のVMが必要なマシンプロパティを持っている場合は、それを使用します。
   - マシンプロファイルとしてARMテンプレート仕様を選択する場合は、必要に応じてテンプレート仕様を作成します。具体的には、*SecurityEncryptionType* や *diskEncryptionSet* (顧客管理キーの場合) など、機密VMの要件を満たすパラメーターを構成します。詳細については、(/ja-jp/citrix-virtual-apps-desktops/2503/install-configure/machine-catalogs-create/create-machine-catalog-citrix-azure#create-an-azure-template-spec)を参照してください。

     > **注:**
     >
     > - マスターイメージとマシンプロファイルが同じセキュリティキータイプであることを確認してください。
     > - 顧客管理キーによる機密OSディスク暗号化を必要とする機密VMを作成するには、マスターイメージとマシンプロファイルの両方でディスク暗号化セットIDが同じであることを確認してください。

Web Studio または PowerShell コマンドを使用して機密VMを作成する

機密VMのセットを作成するには、マスターイメージと、目的の機密VMから派生したマシンプロファイルを使用してマシンカタログを作成します。

Web Studioを使用してカタログを作成するには、(/ja-jp/citrix-virtual-apps-desktops/2503/install-configure/machine-catalogs-create)に記載されている手順に従ってください。以下の点を考慮してください。

- **イメージ**ページで、機密VM作成のために準備したマスターイメージとマシンプロファイルを選択します。マシンプロファイルの選択は必須であり、選択したマスターイメージと同じセキュリティ暗号化タイプに一致するプロファイルのみが選択可能です。
- **仮想マシン**ページでは、機密VMをサポートするマシンサイズのみが選択肢として表示されます。
- 「**ディスク設定**」ページでは、選択したマシンプロファイルから継承されるため、ディスク暗号化セットを指定できません。

起動整合性監視

VMでセキュアブートと仮想トラステッドプラットフォームモジュール（vTPM）が有効になっており、`GuestAttestation`拡張機能がインストールされている場合、Microsoft Defender for Cloudは、VMが正常に起動することをリモートで検証できます。この監視は**ブート整合性監視**と呼ばれます。ブート整合性監視の詳細については、「ブート整合性監視の概要」を参照してください。

マシンプロファイル（VMまたはテンプレート仕様）を使用して、MCSマシンカタログVM（永続VMおよび非永続VM）のブート整合性監視を有効にできます。ブート整合性監視は、信頼できる起動と機密VMでのみサポートされます。

`Set-ProvScheme`を使用して、既存のカタログを更新し、ブート整合性が有効なマシンプロファイルを指すようにできます。カタログに追加された新しいVMは、整合性監視が有効になります。

`Set-ProvVmUpdateTimeWindow`、`Set-ProvVm`、または`Maintenance Cycles`を使用して、カタログ内の既存のVMを更新することもできます。次のように変換できます。

- 整合性監視なしのVMを整合性監視ありにする
- 整合性監視ありのVMを整合性監視なしにする

整合性監視が有効なマシンカタログを作成する

必要な権限：

次の権限があることを確認してください。

- `Microsoft.Compute/virtualMachines/extensions/read`
- `Microsoft.Compute/virtualMachines/extensions/write`

整合性監視が有効なMCSマシンカタログを作成するには、次の手順を実行します。

1. `GuestAttestation`拡張機能がインストールされたマシンプロファイル（VMまたはテンプレート仕様）を作成します。（以下のコンテンツへのリンク）
2. Web StudioまたはPowerShellコマンドを使用して、マシンプロファイル入力を利用したMCSマシンカタログを作成します。

   > **注：**
   >
   > `Get-Item` PowerShellコマンドを`AdditionalData`パラメーターとともに使用して、VMまたはテンプレート仕様の`GuestAttestationExtensionEnabled`ステータスを確認できます。

3. カタログにVMを追加します。

GUESTATTESTATION拡張機能がインストールされた状態で有効化されたマシンプロファイルを作成する

整合性監視が有効になっているVMまたはテンプレート仕様をマシンプロファイル入力として作成します。これは、GuestAttestation拡張機能がインストールされていることを意味します。

整合性監視が有効なVMを作成するには、次の手順を実行します。

1. Azureポータルにサインインします。
2. 新しいVMを作成している場合：
   a. **セキュリティの種類**として、**信頼された起動仮想マシン**または**機密仮想マシン**を選択します。
   b. **セキュリティ機能の構成**をクリックし、**整合性監視**チェックボックスを選択します。

      > **注：**
      >
      > 整合性監視には、セキュアブートとvTPMを有効にする必要があります。

3. **概要**ページで、**セキュリティの種類**セクションに移動し、**セキュリティの種類**が**信頼された起動**または**機密仮想マシン**であり、**整合性監視**が有効になっていることを確認します。
4. **拡張機能 + アプリケーション**ページに移動して、`GuestAttestation`がインストールされていることを確認します。

既存のVMの整合性監視を有効にするには、「整合性監視を有効にする - Azure portal」を参照してください。

`GuestAttestation`拡張機能がインストールされたテンプレート仕様を作成するには:

- テンプレート仕様を使用してGuestAttestationをインストールできます。「整合性監視を有効にする - テンプレート仕様」を参照してください。

> **注：**
>
> `Get-Item` PowerShell コマンドを `AdditionalData` パラメーターとともに使用して、VM またはテンプレート仕様の `GuestAttestationExtensionEnabled` ステータスを確認できます。

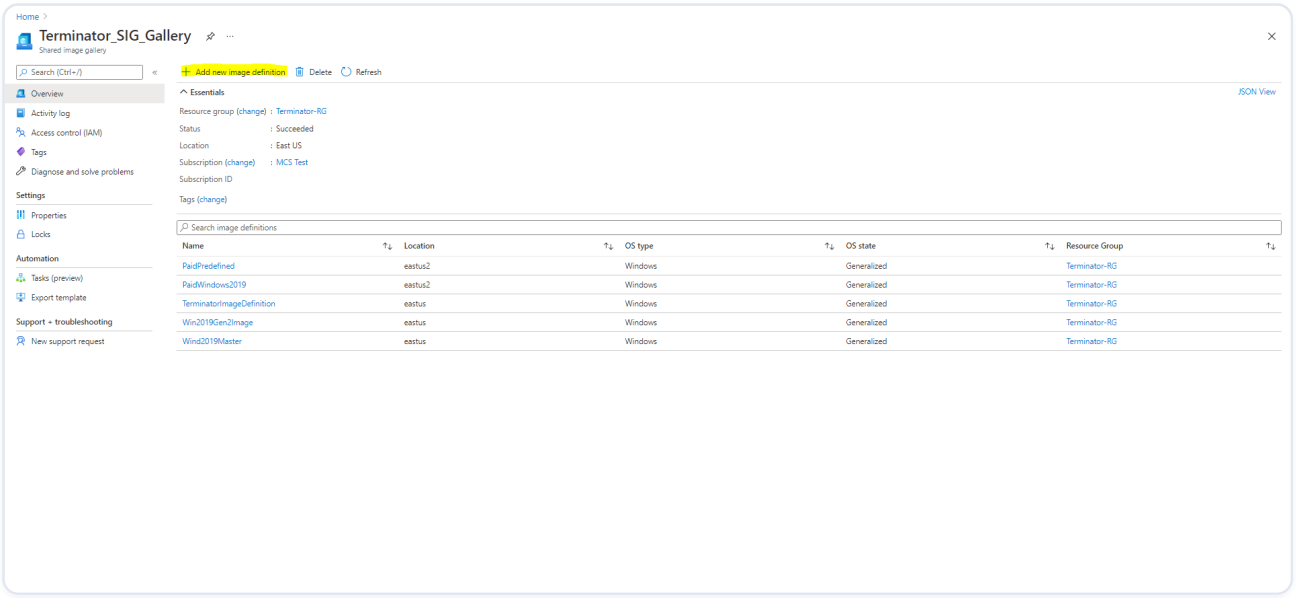
アジュール マーケットプレイス

Citrix Virtual Apps and Desktopsは、マシンカタログを作成するためのプラン情報を含むAzure上のマスターイメージの使用をサポートしています。詳しくは、「Microsoft Azure Marketplace」を参照してください。

> **ヒント：**
>
> 標準のWindows Serverイメージなど、Azure Marketplaceで見つかる一部のイメージには、プラン情報が追加されていません。Citrix Virtual Apps and Desktops の機能は、有料イメージ向けです。

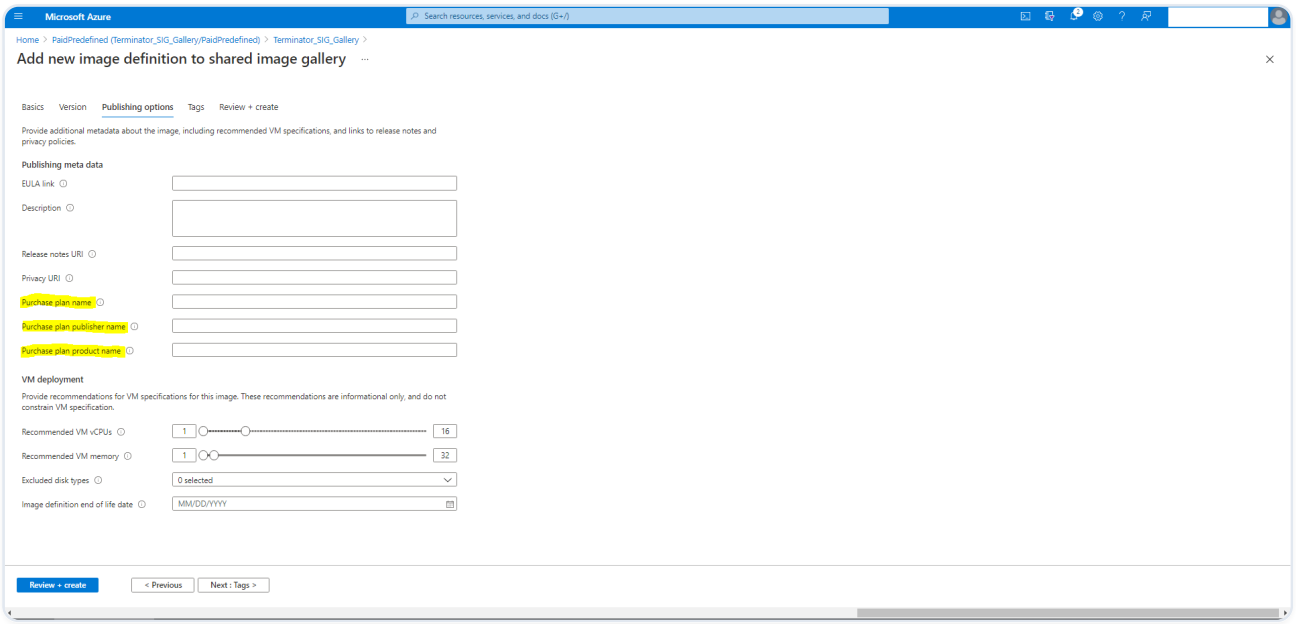
共有イメージギャラリーで作成されたイメージにAzureプラン情報が含まれていることを確認する

このセクションの手順を使用して、Web Studioで共有イメージギャラリーのイメージを表示します。これらのイメージは、オプションでマスターイメージとして使用できます。イメージを共有イメージギャラリーに入れるには、ギャラリーでイメージ定義を作成します。

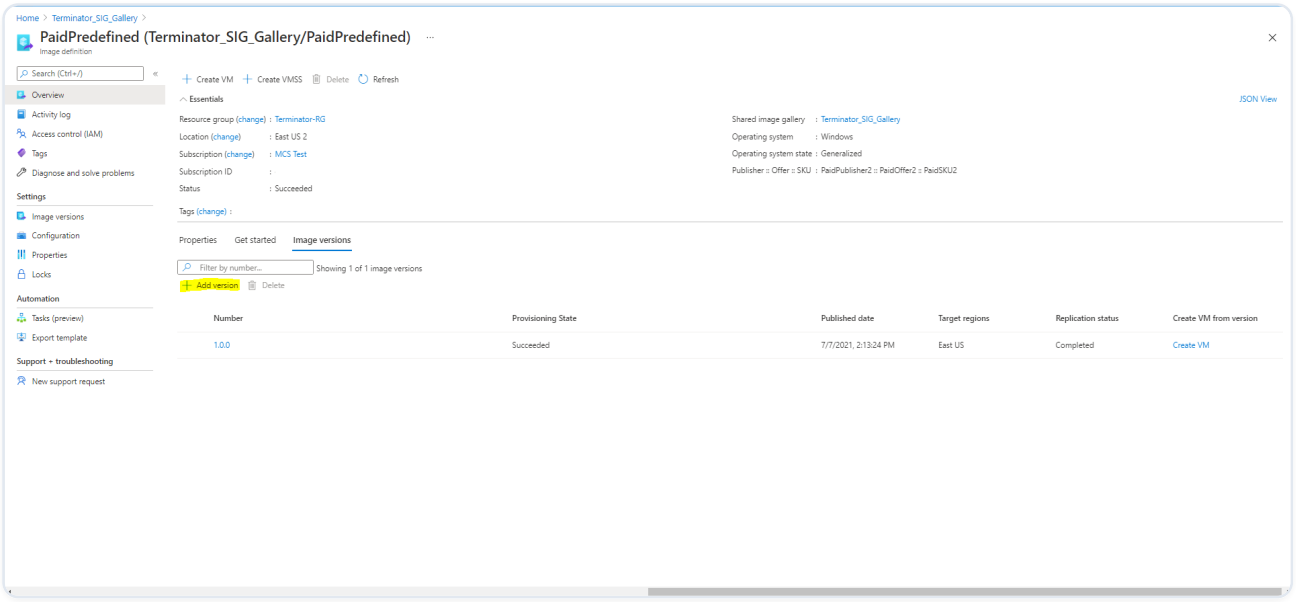


公開オプションページで、購入プラン情報を確認します。

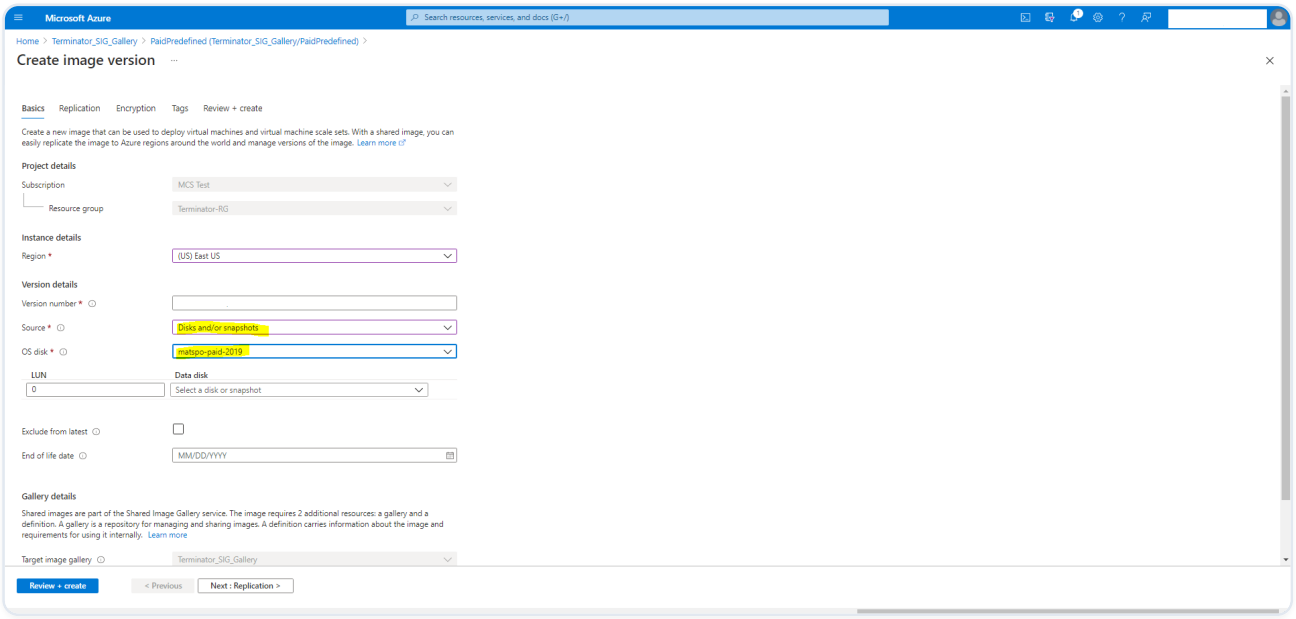
購入プラン情報フィールドは最初は空です。これらのフィールドに、イメージに使用する購入プラン情報を入力します。購入プラン情報を入力しないと、マシンカタログのプロセスが失敗する可能性があります。



購入プラン情報を確認後、定義内にイメージバージョンを作成します。これはマスターイメージとして使用されます。「**バージョンを追加**」をクリックします。



バージョン詳細セクションで、イメージスナップショットまたはマネージドディスクをソースとして選択します。



オンデマンド容量予約VMのカタログを作成する

オンデマンド容量予約を使用すると、Azureリージョンまたは可用性ゾーンで任意の期間、コンピューティング容量を予約できます。Azureオンデマンド容量予約の詳細については、Microsoftドキュメント「オンデマンド容量予約」を参照してください。

マシンプロファイル（VMまたはテンプレート仕様）を使用して、オンデマンド容量予約付きのAzure VMのMCSマシンカタログを作成できます。また、既存のマシンカタログと既存のVMを更新して、オンデマンド容量予約を追加または削除することもできます。

この機能は、永続および非永続マシンカタログに適用されます。

制限事項

この機能は、以下には適用されません。

- スポットVM
- ホストグループ
- 休止状態が有効なVM

制限事項の詳細については、Microsoftドキュメントの「制限事項」を参照してください。

オンデマンド容量予約VMのカタログを作成する手順

1. マシンプロファイルソース（VMまたはARMテンプレート仕様）を作成します。VMまたはARMテンプレート仕様の作成については、「キャパシティ予約グループへのVMの関連付け」を参照してください。
2. マシンプロファイルでオンデマンドキャパシティ予約が有効になっているかどうかを確認するには、次のPowerShellコマンドを実行します。マシンプロファイルでオンデマンドキャパシティ予約が有効になっている場合、`capacityReservationGroup id`を取得します。

   例：

   マシンプロファイルソースがVMの場合、次のコマンドを実行します。

   ```
   (Get-Item "XDHyp:\HostingUnits\azure-res-
   conn2\machineprofile.folder\fifthcolumn.resourcegroup\demand-
   capacity.vm").AdditionalData
   ```

   マシンプロファイルソースがテンプレート仕様の場合、次のコマンドを実行します。

   ```
   (Get-Item "XDHyp:\HostingUnits\azure-res-
   conn2\machineprofile.folder\fifthcolumn.resourcegroup\fc-aeh-
   templatespec.templatespec\14.0.0-capacity-
   reservation.templatespecversion").AdditionalData
   ```

3. Web StudioまたはPowerShellコマンドを使用して、マシンプロファイルを使用してマシンカタログを作成します。

`Set-ProvScheme`コマンドを使用してカタログを更新できます。PowerShellコマンド`Set-ProvVmUpdateTimeWindow`を使用して既存のVMを更新することもできます。マシンプロファイルは次回の電源投入時に更新されます。

入れ子になった仮想化

マスターVMを入れ子になった仮想化が有効になるように構成すると、そのマスターVMを使用して作成されたMCSマシンカタログ内のすべてのVMで入れ子になった仮想化が有効になります。この機能は、永続VMと非永続VMの両方に適用されます。既存のMCSマシンカタログと既存のVMをイメージ更新によって入れ子になった仮想化を有効にするように更新できます。

現在、Dv3およびEv3 VMサイズのみが入れ子になった仮想化をサポートしています。

入れ子になった仮想化の詳細については、Microsoftのブログ「Azureにおける入れ子になった仮想化」を参照してください。

NVMeのみのSKU

通常、汎用、メモリ最適化、およびコンピューティング最適化VMの古い世代（D/Ev5またはFv2以前）はSCSIをサポートしています。新しい世代（Da/Ea/Fav6以降）は通常、NVMeストレージインターフェイスのみをサポートしています。MCSは、Azureの新しいVM SKUをサポートするためにNVMeストレージコントローラータイプをサポートしています。

NVMeの詳細については、Microsoftのドキュメント「NVMeに関する一般的なFAQ」を参照してください。

次のサービスオファリングを使用して MCS カタログを作成できます。

- SCSIとNVMeの両方をサポートしています。詳細については、「SCSIとNVMeの両方をサポートするサービスオファリングを使用したカタログの作成」を参照してください。
- NVMeのみをサポートしています。詳細については、「NVMeのみをサポートするサービスオファリングを使用したカタログの作成」を参照してください。

制限事項

- NVMeをサポートするすべてのサービスオファリングは、同時にTrusted Launchをサポートしていません。
- NVMeはGen 1 VMではサポートされていません。
- 一部のOSイメージはNVMeをサポートしていない場合があります。その場合、Azure UIではNVMeオプションがグレー表示されます。

SCSIとNVMeの両方をサポートするサービスオファリングを使用したカタログの作成

1. マスターイメージとして使用する VM を作成します。

a. NVMeをサポートするマーケットプレイスイメージを使用します。NVMeをサポートするAzure Marketplaceイメージのリストは、「リモートNVMeでサポートされているOSイメージ」で確認できます。

b. VMのOSディスクのスナップショットを取得し、`New-ProvScheme`コマンドの`MasterImageVM`パラメーターで使用するか、マネージドディスクを直接使用します。

   マスターイメージがNVMeをサポートしているかどうかを、以下のいずれかの方法で確認します。

   - `Get-Item`の`AdditionalData`フィールドにある`SupportedDiskControllerTypes`を確認します。例：

     ```
     (get-item XDHyp:
     \HostingUnits\mynetwork\image.folder\abc.resourcegroup\deg-
     snapshot).AdditionalData
     ```

     `SupportedDiskControllerTypes`は`SCSI, NVMe`である必要があります。

   - Azure CLIとPowerShellを使用する

2. NVMeとSCSIの両方をサポートするサービスオファリングを使用します。
3. NVMeが有効になっているマシンプロファイルとして、VMまたはテンプレート仕様を使用します。`DiskControllerType`がNVMeに設定されている任意のVMを使用します。VMをマシンプロファイルとして直接使用するか、テンプレートをエクスポートしてテンプレート仕様をマシンプロファイルとして使用します。

NVMeのみをサポートするサービスオファリングを使用してカタログを作成する

1. マスターイメージとして使用するVMを作成します。NVMeをサポートするマーケットプレイスイメージを使用します。NVMeをサポートするAzure Marketplaceイメージのリストは、リモートNVMeでサポートされるOSイメージで確認できます。
2. NVMeのみをサポートするサービスオファリングを使用します。

> **注:**
>
> サービスオファリングがNVMeをサポートしているため、カタログでNVMeを有効にするために`NVMe`に設定された`DiskControllerType`を持つマシンプロファイルは必要ありません。ただし、マシンプロファイルを使用する場合は、`DiskControllerType`が`NVMe`に設定されているか、空白であるか、指定されていない必要があります。

既存の永続VMを変更する

NVMe構成は、VMが作成された後に変更することはできません。永続VMのNVMe構成を変更する方法は、VMを再デプロイすることです。これを行うロジックは次のとおりです。

1. VMの現在の状態を保存します。
2. 既存のVMの電源をオンにした後、VMが再デプロイを必要とするかどうかを検出します。
    a. 構成変更がNVMeからNVMe、またはSCSIからSCSIである場合、VMの再展開は不要です。
    b. 構成変更がSCSIからNVMe、またはその逆である場合、VMを再展開して再作成します。

PowerShellを使用してマシンカタログを作成する

このセクションでは、PowerShell を使用してカタログを作成する方法について詳しく説明します。

- 非永続的なライトバックキャッシュディスクを持つカタログを作成する
- 永続的なライトバックキャッシュディスクを持つカタログを作成する
- MCSIO で起動パフォーマンスを向上させる
- PowerShell を使用してカタログを作成または更新する際にテンプレート仕様を使用する
- トラステッド起動によるマシンカタログ
- マシンプロファイルプロパティ値を使用する
- 顧客管理の暗号化キーを使用してマシンカタログを作成する
- 二重暗号化を使用してマシンカタログを作成する
- Azure エフェメラルディスクを使用してカタログを作成する
- Azure 専用ホスト
- Azure Compute Gallery イメージを使用してマシンカタログを作成または更新する
- 共有イメージギャラリーを構成する
- 指定された可用性ゾーンにマシンをプロビジョニングする
- ストレージの種類
- Azure Spot VM を使用してカタログを作成する
- バックアップ VM サイズを構成する
- すべてのリソースにタグをコピー(#copy-tags-on-all-resources)

- Azure Monitor Agentがインストールされたカタログ VMをプロビジョニング(#provision-catalog-vms-with-azure-monitor-agent-installed)

非永続的なライトバックキャッシュディスクを持つカタログの作成

非永続的なライトバックキャッシュディスクを持つカタログを構成するには、PowerShellパラメーター`New-ProvScheme CustomProperties`を使用します。カスタムプロパティ`UseTempDiskForWBC`は、ライトバックキャッシュファイルを保存するためにAzure一時ストレージの使用を許可するかどうかを示します。一時ディスクをライトバックキャッシュディスクとして使用する場合は、`New-ProvScheme`の実行時にこれをtrueに構成する必要があります。このプロパティが指定されていない場合、パラメーターはデフォルトで**False**に設定されます。

例えば、`CustomProperties`パラメーターを使用して`UseTempDiskForWBC`を**true**に設定する場合：

```
-CustomProperties '<CustomProperties xmlns=" http://schemas.citrix.com/
2014/xd/machinecreation" xmlns:xsi=" http://www.w3.org/2001/XMLSchema-
instance"> `

<Property xsi:type="StringProperty" Name="PersistWBC" Value="false"/> `

<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="false"/> `

<Property xsi:type="StringProperty" Name="PersistVm" Value="false"/> `

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="Premium_LRS"/> `

<Property xsi:type="StringProperty" Name="WBCDiskStorageType"
Value="Premium_LRS"/> `

<Property xsi:type="StringProperty" Name="LicenseType"
Value="Windows_Client"/> `

<Property xsi:type="StringProperty" Name="UseTempDiskForWBC" Value="true"/
> `

</CustomProperties>'
```

注:

> ライトバックキャッシュファイルにAzureローカル一時ストレージを使用するようにマシンカタログをコミットした後、後でVHDを使用するように変更することはできません。

永続的なライトバックキャッシュディスクを持つカタログを作成する

永続的なライトバックキャッシュディスクを持つカタログを構成するには、PowerShellパラメーター`New-ProvScheme CustomProperties`を使用します。このパラメーターは、MCSプロビジョニングされたマシンに対してライトバックキャッシュディスクがどのように永続化するかを決定するために使用される追加のプロパティ`PersistWBC`をサポートします。`PersistWBC`プロパティは、`UseWriteBackCache`パラメーターが指定され、`WriteBackCacheDiskSize`パラメーターがディスクが作成されることを示すように設定されている場合にのみ使用されます。

`PersistWBC`をサポートする前の`CustomProperties`パラメーターに見られるプロパティの例を次に示します。

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="ResourceGroups"
Value="benvaldev5RG3" />

</CustomProperties>
```

これらのプロパティを使用する場合、`CustomProperties`パラメーターからプロパティが省略されていると、それらはデフォルト値を含むことに注意してください。`PersistWBC`プロパティには、**true**または**false**の2つの可能な値があります。

`PersistWBC`プロパティを**true**に設定すると、Citrix Virtual Apps and Desktops管理者がWeb Studioを使用してマシンをシャットダウンしても、ライトバックキャッシュディスクは削除されません。

`PersistWBC`プロパティを**false**に設定すると、Citrix Virtual Apps and Desktops管理者がWeb Studioを使用してマシンをシャットダウンしたときに、ライトバックキャッシュディスクが削除されます。

注:

`PersistWBC`プロパティが省略された場合、プロパティはデフォルトで**false**になり、Web Studioを使用してマシンがシャットダウンされるとライトバックキャッシュは削除されます。

例えば、`CustomProperties` パラメーターを使用して `PersistWBC` を true に設定する場合:

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="ResourceGroups"
Value="benvaldev5RG3" />

<Property xsi:type="StringProperty" Name="PersistWBC" Value="true" />

</CustomProperties>
```

重要:

`PersistWBC` プロパティは、`New-ProvScheme` PowerShell コマンドレットを使用してのみ設定できます。プロビジョニングスキームの `CustomProperties` を作成後に変更しようとしても、マシンカタログには影響せず、マシンがシャットダウンされたときのライトバックキャッシュディスクの永続性にも影響しません。

例えば、`New-ProvScheme` を使用してライトバックキャッシュを使用するように設定し、同時に `PersistWBC` プロパティを true に設定する場合:

```
New-ProvScheme

-CleanOnBoot
```

```
-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com/
2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`"><Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`"
Value=`"true`" /><Property xsi:type=`"StringProperty`"
Name=`"StorageAccountType`" Value=`"Premium_LRS`" /><Property
xsi:type=`"StringProperty`" Name=`"ResourceGroups`"
Value=`"benvaldev5RG3`" /><Property xsi:type=`"StringProperty`"
Name=`"PersistWBC`" Value=`"true`" /></CustomProperties>"

-HostingUnitName "adSubnetScale1"

-IdentityPoolName "BV-WBC1-CAT1"

-MasterImageVM "XDHyp:
\HostingUnits\adSubnetScale1\image.folder\GoldImages.resourcegroup\W10MCSI
O-01_OsDisk_1_a940e6f5bab349019d57ccef65d2c7e3.manageddisk"

-NetworkMapping @{"0"="XDHyp:\HostingUnits\adSubnetScale1\
\virtualprivatecloud.folder\CloudScale02.resourcegroup\adVNET.virtualpriva
tecloud\adSubnetScale1.network"}

-ProvisioningSchemeName "BV-WBC1-CAT1"

-ServiceOffering "XDHyp:
\HostingUnits\adSubnetScale1\serviceoffering.folder\Standard_D2s_v3.servic
eoffering"

-UseWriteBackCache

-WriteBackCacheDiskSize 127

-WriteBackCacheMemorySize 256
```

MCSIOで起動パフォーマンスを向上させる

MCSIO が有効になっている場合、Azure および GCP マネージドディスクの起動パフォーマンスを向上させることができます。この機能を構成するには、`New-ProvScheme` コマンドで PowerShell の `PersistOSDisk` カスタムプロパティを使用します。`New-ProvScheme` に関連するオプションは次のとおりです。

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="Resource ``````<!--NeedCopy-->

````````Groups" Value="benvaldev5RG3" />

<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="true" />

</CustomProperties>
```

この機能を有効にするには、`PersistOSDisk` カスタムプロパティを `true` に設定します。例:

```
New-ProvScheme

-CleanOnBoot

-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com/
2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`"><Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`"
Value=`"true`" /><Property xsi:type=`"StringProperty`"
Name=`"StorageAccountType`" Value=`"Premium_LRS`" /><Property
xsi:type=`"StringProperty`" Name=`"ResourceGroups`"
Value=`"benvaldev5RG3`" /><Property xsi:type=`"StringProperty`"
Name=`"PersistOsDisk`" Value=`"true`" /></CustomProperties>"

-HostingUnitName "adSubnetScale1"

-IdentityPoolName "BV-WBC1-CAT1"

-MasterImageVM "XDHyp:
\HostingUnits\adSubnetScale1\image.folder\GoldImages.resourcegroup\W10MCSI
O-01_OsDisk_1_a940e6f5bab349019d57ccef65d2c7e3.manageddisk"

-NetworkMapping @{"0"="XDHyp:\HostingUnits\adSubnetScale1\
\virtualprivatecloud.folder\CloudScale02.resourcegroup\adVNET.virtualpriva
tecloud\adSubnetScale1.network"}
```
```

```
-ProvisioningSchemeName "BV-WBC1-CAT1"

-ServiceOffering "XDHyp:
\HostingUnits\adSubnetScale1\serviceoffering.folder\Standard_D2s_v3.servic
eoffering"

-UseWriteBackCache

-WriteBackCacheDiskSize 127

-WriteBackCacheMemorySize 256
```

PowerShell を使用してカタログを作成または更新する際にテンプレート仕様を使用する

マシンプロファイルの入力としてテンプレート仕様を使用して、MCS マシンカタログを作成または更新できます。これを行うには、Web Studio または PowerShell コマンドを使用します。

Web Studio の場合は、「Web Studio で Azure Resource Manager イメージを使用してマシンカタログを作成する」を参照してください。

PowerShell コマンドを使用する場合:

1. **PowerShell** ウィンドウを開きます。
2. `asnp citrix*` を実行します。
3. カタログを作成または更新します。
    - カタログを作成するには:
        a. `New-ProvScheme` コマンドをテンプレート仕様とともにマシンプロファイル入力として使用します。例:

```
New-ProvScheme -MasterImageVM "XDHyp:/HostingUnits/azure/
image.folder/fgthj.resourcegroup/nab-ws-
vda_OsDisk_1_xxxxxxxxxxa.manageddisk"

MachineProfile "XDHyp:/HostingUnits/azure/machineprofile.folder/
fgthj.resourcegroup/test.templatespec/V1.templatespecversion"

-ProvisioningSchemeName <String>

-HostingUnitName <String>
```

```
-IdentityPoolName <String>

[-ServiceOffering <String>][-CustomProperties <String>

[-LoggingId <Guid>]

[-BearerToken <String>][-AdminAddress <String>]

[<CommonParameters>]
```

b. カタログの作成を完了します。

- カタログを更新するには、`Set-ProvScheme` コマンドをテンプレート仕様とともにマシンプロファイル入力として使用します。例:

```
Set-ProvScheme -MasterImageVm 'XDHyp://Connections/Azure/East
Us.region/vm.folder/MasterDisk.vm'

MachineProfile 'XDHyp:/HostingUnits/azure/machineprofile.folder/
fgthj.resourcegroup/testing.templatespec/V1.templatespecversion'

[-ProvisioningSchemeName] <String>

[-CustomProperties <String>][-ServiceOffering <String>] [-PassThru]

[-LoggingId <Guid>] [-BearerToken <String>][-AdminAddress <String>]
[<CommonParameters>]
```

Trusted Launch を使用したマシンカタログ

Trusted Launch を使用してマシンカタログを正常に作成するには、以下を使用します。

- Trusted Launch が有効なマスターイメージ。マシンプロファイルを使用する必要がありますが、マシンプロファイルが Trusted Launch 対応である必要はありません。Trusted Launch が有効なマスターイメージと、Trusted Launch が有効でないマシンプロファイルを使用すると、マスターイメージとマシンプロファイルの Trusted Launch 構成が一致しないため、警告メッセージが表示されます。
- Trusted Launch をサポートするVMサイズ
- Trusted Launch をサポートするWindows VMバージョン。現在、Windows 10、Windows 11、Windows Server 2016、2019、2022 が Trusted Launch をサポートしています。

Citrix Virtual Apps and Desktops の提供インベントリアイテムを表示し、VMサイズが Trusted Launch をサポートしているかどうかを判断するには、次のコマンドを実行します。

1. PowerShellウィンドウを開きます。
2. Citrix固有のPowerShellモジュールをロードするには、**asnp citrix*** を実行します。
3. 次のコマンドを実行します。

```
$s = (ls XDHyp:\HostingUnits\<name of hosting
unit>\serviceoffering.folder\"<VM size>.serviceoffering)
```

4. `$s | select -ExpandProperty Additionaldata` を実行します。
5. `SupportsTrustedLaunch` 属性の値を確認します。
   - `SupportsTrustedLaunch` が **True** の場合、VMサイズは Trusted Launch をサポートしています。
   - `SupportsTrustedLaunch` が **False** の場合、VM サイズは Trusted Launch をサポートしていません。

Azure の PowerShell によると、Trusted Launch をサポートする VM サイズを特定するには、次のコマンドを使用できます。

```
(Get-AzComputeResourceSku | where {$_.Locations.Contains($region) -and
($_.Name -eq "<VM size>") })[0].Capabilities
```

Azure PowerShell コマンドを実行した後、VM サイズが Trusted Launch をサポートしているかどうかを説明する例を次に示します。

- *例 1*: Azure VM が Generation 1 のみをサポートしている場合、その VM は Trusted Launch をサポートしていません。したがって、Azure PowerShell コマンドを実行しても `TrustedLaunchDisabled` 機能は表示されません。
- *例 2*: Azure VM が Generation 2 のみをサポートしており、`TrustedLaunchDisabled` 機能が **True** の場合、Generation 2 VM サイズは Trusted Launch でサポートされません。
- *例 3*: Azure VM が Generation 2 のみをサポートしており、PowerShell コマンドを実行しても `TrustedLaunchDisabled` 機能が表示されない場合、Generation 2 VM サイズは Trusted Launch でサポートされます。

Azure 仮想マシンの Trusted Launch の詳細については、Microsoft ドキュメント「Trusted Launch for Azure virtual machines」を参照してください。

Trusted Launch を使用してマシンカタログを作成する

1. Trusted Launch が有効なマスターイメージを作成します。Microsoft ドキュメント「Trusted Launch VM Images」を参照してください。
2. セキュリティの種類を **trusted launch virtual machines** として VM またはテンプレート仕様を作成します。VM またはテンプレート仕様の作成の詳細については、Microsoft ドキュメント「Deploy a trusted launch VM」を参照してください。
3. Web Studio または PowerShell コマンドを使用してマシンカタログを作成します。

   - Web Studio を使用する場合は、「Web Studio で Azure Resource Manager イメージを使用してマシンカタログを作成する」を参照してください。
   - PowerShell コマンドを使用する場合は、VM またはテンプレート仕様をマシンプロファイル入力として `New-ProvScheme` コマンドを使用します。カタログを作成するためのコマンドの完全なリストについては、「カタログの作成」を参照してください。

     VM をマシンプロファイル入力とする `New-ProvScheme` の例:

     ```
     New-ProvScheme -CleanOnBoot -HostingUnitName "name"
     -IdentityPoolName "name" -InitialBatchSizeHint 1

     -MasterImageVM "XDHyp:/HostingUnits/azure/image.folder/
     fgthj.resourcegroup/nab-ws-vda_OsDisk_1_xxxxxxxxxxa.manageddisk"

     -MachineProfile "XDHyp:
     \HostingUnits\<adnet>\machineprofile.folder\<def.resourcegroup>\<mac
     hine profile vm.vm>"

     -ProvisioningSchemeName <String>

     -HostingUnitName <String>

     -IdentityPoolName <String>

     [-ServiceOffering <String>][-CustomProperties <String>]

     [<CommonParameters>]
     ```

     テンプレート仕様をマシンプロファイル入力とする `New-ProvScheme` の例:

```
New-ProvScheme -CleanOnBoot -HostingUnitName "name"
-IdentityPoolName "name" -InitialBatchSizeHint 1

-MasterImageVM "XDHyp:/HostingUnits/azure/image.folder/
fgthj.resourcegroup/nab-ws-vda_OsDisk_1_xxxxxxxxxxa.manageddisk"

MachineProfile "XDHyp:/HostingUnits/azure/machineprofile.folder/
fgthj.resourcegroup/test.templatespec/V1.templatespecversion"

-ProvisioningSchemeName <String>

-HostingUnitName <String>

-IdentityPoolName <String>

[-ServiceOffering <String>][-CustomProperties <String>]

[<CommonParameters>]
```

トラステッド起動でマシンカタログを更新する

永続および非永続の両方のマシンカタログを更新できます。

永続マシンカタログの場合:

永続マシンカタログを Trusted Launch で更新する (/en-us/citrix-virtual-apps-desktops/2503/media/persistent-update-trusted-launch.png)

非永続マシンカタログの場合:

非永続マシンカタログを Trusted Launch で更新する (/en-us/citrix-virtual-apps-desktops/2503/media/non-persistent-update-trusted-launch.jpg)

トラステッド起動でマシンカタログを作成する際のエラー

トラステッド起動でマシンカタログを作成する際に、以下のシナリオで適切なエラーが発生します。

シナリオ	エラー
アンマネージドカタログの作成中にマシンプロファイルを選択した場合	`MachineProfileNotSupportedForUnmanagedCatalog`

シナリオ	エラー
セキュリティの種類として Trusted Launch を使用するマスターイメージソースでマネージドカタログを作成する際に、マシンプロファイルを選択しなかった場合	`MachineProfileNotFoundForTrustedLaunchMasterImage`
マスターイメージのセキュリティの種類とは異なるセキュリティ種類のマシンプロファイルを選択した場合	`SecurityTypeConflictBetweenMasterImageAndMachineProfile`
カタログ作成時に、Trusted Launchをサポートしないサイズを選択したが、Trusted Launchをサポートするマスターイメージを使用した場合	`MachineSizeNotSupportTrustedLaunch`

マシンプロファイルプロパティ値の使用

マシンカタログは、カスタムプロパティで定義されている次のプロパティを使用します。

- アベイラビリティゾーン
- 専用ホストグループID
- ディスク暗号化セットID
- OSの種類
- ライセンスの種類
- ストレージの種類

これらのカスタムプロパティが明示的に定義されていない場合、プロパティ値は、マシンプロファイルとして使用されるARMテンプレート仕様またはVMから設定されます。さらに、`ServiceOffering`が指定されていない場合、マシンプロファイルから設定されます。

> **注:**
>
> マシンプロファイルに一部のプロパティが欠落しており、カスタムプロパティで定義されていない場合、該当する場所ではプロパティのデフォルト値が適用されます。

> 次のセクションでは、`New-ProvScheme`と`Set-ProvScheme`におけるいくつかのシナリオについて説明します。この場合、`CustomProperties`はすべてのプロパティを定義しているか、値がMachineProfileから派生しています。

- New-ProvSchemeのシナリオ
  - MachineProfileにすべてのプロパティがあり、CustomPropertiesが定義されていない場合。
    例:

    `New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit\machineprofile.folder\azure.resourcegroup\mpA.vm"`

    以下の値がカタログのカスタムプロパティとして設定されます:

    ```
    Get-ProvScheme | select CustomProperties

    <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
    machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
    instance">

    <Property xsi:type="StringProperty" Name="StorageAccountType"
    Value="<mpA-value>"/>

    <Property xsi:type="StringProperty" Name="OSType" Value="<mpA-
    value>"/>

    <Property xsi:type="StringProperty" Name="LicenseType" Value="<mpA-
    value>"/>

    <Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
    Value="<mpA-value>"/>

    <Property xsi:type="StringProperty" Name="DedicatedHostGroupId"
    Value="<mpA-value>"/>

    <Property xsi:type="StringProperty" Name="Zones" Value="<mpA-
    value>"/>

    </CustomProperties>
    ```

  - MachineProfileに一部のプロパティがあり、CustomPropertiesが定義されていない場合。
    例: MachineProfileにはLicenseTypeとOsTypeのみがあります。

`New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit\machineprofile.folder\azure.resourcegroup\mpA.vm"`

以下の値がカタログのカスタムプロパティとして設定されます:

```
Get-ProvScheme | select CustomProperties

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="OSType" Value="<mpA-
value>"/>

<Property xsi:type="StringProperty" Name="LicenseType" Value="<mpA-
value>"/>

</CustomProperties>
```

- MachineProfile と CustomProperties の両方がすべてのプロパティを定義している場合。例:

`New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit\machineprofile.folder\azure.resourcegroup\mpA.vm" -CustomProperties $CustomPropertiesA`

カスタムプロパティが優先されます。以下の値がカタログのカスタムプロパティとして設定されます:

```
Get-ProvScheme | select CustomProperties

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="<CustomPropertiesA-value>"/>

<Property xsi:type="StringProperty" Name="OSType"
Value="<CustomPropertiesA-value>"/>

<Property xsi:type="StringProperty" Name="LicenseType"
Value="<CustomPropertiesA-value>"/>
```

```
<Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
Value="<CustomPropertiesA-value>"/>

<Property xsi:type="StringProperty" Name="DedicatedHostGroupId"
Value="<CustomPropertiesA-value>"/>

<Property xsi:type="StringProperty" Name="Zones"
Value="<CustomPropertiesA-value>"/>

</CustomProperties>
```

- MachineProfileで一部のプロパティが定義され、CustomPropertiesで一部のプロパティが定義されている場合。例:
  - CustomProperties は LicenseType と StorageAccountType を定義します
  - MachineProfile は LicenseType、OsType、および Zones を定義します

`New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit\machineprofile.folder\azure.resourcegroup\mpA.vm" -CustomProperties $CustomPropertiesA`

以下の値がカタログのカスタムプロパティとして設定されます:

```
Get-ProvScheme | select CustomProperties

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="<CustomPropertiesA-value>"/>

<Property xsi:type="StringProperty" Name="OSType" Value="<mpA-
value>"/>

<Property xsi:type="StringProperty" Name="LicenseType"
Value="<CustomPropertiesA-value>"/>

<Property xsi:type="StringProperty" Name="Zones" Value="<mpA-
value>"/>
```

```
</CustomProperties>
```

- 一部のプロパティはMachineProfileで定義されており、一部のプロパティはCustomPropertiesで定義されています。さらに、ServiceOfferingは定義されていません。
  例:
  - CustomProperties は StorageType を定義します
  - MachineProfile は LicenseType を定義します

```
New-ProvScheme -MachineProfile "XDHyp:
\HostingUnits\azureunit\machineprofile.folder\azure.resourcegroup\mp
.vm"

-ServiceOffering "XDHyp:
\HostingUnits\azureunit\serviceoffering.folder\<explicit-machine-
size>.serviceoffering"
```

カタログのカスタムプロパティとして、次の値が設定されます。

```
Get-ProvScheme | select ServiceOffering

serviceoffering.folder\<explicit-machine-size>.serviceoffering



Get-ProvScheme | select CustomProperties

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="explicit-storage-type"/>

<Property xsi:type="StringProperty" Name="LicenseType" Value="value-
from-machineprofile"/>

</CustomProperties>
```

- OsTypeがCustomPropertiesにもMachineProfileにもない場合、次のようになります。

    - 値はマスターイメージから読み取られます。
    - マスターイメージがアンマネージドディスクの場合、OsType は Windows に設定されます。例:

`New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit\machineprofile.folder\azure.resourcegroup\mpA.vm" -MasterImageVM "XDHyp:\HostingUnits\azureunit\image.folder\linux-master-image.manageddisk"`

マスターイメージからの値はカスタムプロパティに書き込まれます。この場合、Linuxです。

```
Get-ProvScheme | select CustomProperties

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="OSType" Value="Linux"/>

</CustomProperties>
```

- Set-ProvScheme シナリオ
    - 既存のカタログ (以下を含む):
        - `StorageAccountType` とOsTypeのカスタムプロパティ
        - ゾーンを定義するMachineProfile `mpA.vm`
    - 更新:
        - StorageAccountTypeを定義するマシンプロファイル mpB.vm
        - LicenseType と OsType を定義する新しいカスタムプロパティセット $CustomPropertiesB

`Set-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit\machineprofile.folder\azure.resourcegroup\mpB.vm" -CustomProperties $CustomPropertiesB`

カタログのカスタムプロパティとして、次の値が設定されます。

```
Get-ProvScheme | select CustomProperties

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="<mpB-value>"/>

<Property xsi:type="StringProperty" Name="OSType"
Value="<CustomPropertiesB-value>"/>

<Property xsi:type="StringProperty" Name="LicenseType"
Value="<CustomPropertiesB-value>"/>

    </CustomProperties>
```

- 既存のカタログ (以下を含む):
  - S`torageAccountType` と OsType の CustomProperties
  - StorageAccountType と LicenseType を定義する MachineProfile `mpA.vm`
- 更新:
  - StorageAccountType と OsType を定義する新しいカスタムプロパティセット $CustomPropertiesB。

`Set-ProvScheme -CustomProperties $CustomPropertiesB`

カタログのカスタムプロパティとして、次の値が設定されます。

```
Get-ProvScheme | select CustomProperties

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="<CustomPropertiesB-value>"/>

<Property xsi:type="StringProperty" Name="OSType"
Value="<CustomPropertiesB-value>"/>
```

```
<Property xsi:type="StringProperty" Name="LicenseType" Value="<mp-A-value>"/>

</CustomProperties>
```

- 既存のカタログ (以下を含む):
  - `StorageAccountType` と OsType の CustomProperties
  - Zones を定義する MachineProfile `mpA.vm`
- 更新:
  - StorageAccountType と LicenseType を定義する MachineProfile mpB.vm
  - `ServiceOffering` が指定されていません

`Set-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit\machineprofile.folder\azure.resourcegroup\mpB.vm"`

カタログのカスタムプロパティとして、以下の値が設定されます:

```
Get-ProvScheme | select ServiceOffering

serviceoffering.folder\<value-from-machineprofile>.serviceoffering



Get-ProvScheme | select CustomProperties

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="StorageAccountType" Value="<mpB-value>"/>

<Property xsi:type="StringProperty" Name="OSType" Value="<prior-CustomProperties-value>"/>

<Property xsi:type="StringProperty" Name="LicenseType" Value="<mpB-value>"/>
```

```
</CustomProperties>
```

VMごとに複数のNICを持つカタログを作成または更新する

MCSはVMごとに複数のNICをサポートしています。VM上の複数のNICを複数のサブネットに関連付けることができますが、それらのサブネットは同じ仮想ネットワーク (VNet) 内にある必要があります。PowerShellコマンドを使用して、以下を実行できます。

- VM上に複数のNICを持つカタログを作成する(#create-a-catalog-with-multiple-nics-on-a-vm)
- 既存のカタログ構成を更新して、VM上に複数のNICを持たせ、新しく作成されるVMが複数のNICを持つようにする(#update-a-catalog-to-have-multiple-nics-on-a-vm)
- 既存のVMを更新して、複数のNICを持つようにする(#update-an-existing-vm-to-have-multiple-nics-on-a-vm)

マシンプロファイルに基づかないマシンカタログと、マシンプロファイルに基づくマシンカタログを作成または更新して、VM上に複数のNICを持たせることができます。現在、マシンプロファイルに基づくマシンカタログの場合、マシンプロファイルソースで指定されたNICの数と同じ数しか持つことができません。

アクセラレーテッドネットワーキングなどのプロパティは、マシンプロファイルソースから派生します。

注:

VMサイズは、同じ数のNICと対応するアクセラレーテッドネットワーキングをサポートしている必要があります。そうでない場合、エラーが発生します。

選択したVMサイズに関連付けられているNICの最大数を取得できます。PowerShellコマンド `get-item` を `AdditionalData` パラメーターとともに実行すると、`MaxNetworkInterfaces` というPowerShellプロパティが最大NIC数を表示します。

最大NIC数を取得する

最大NIC数を取得するには:

1. Delivery Controller™ホストから**PowerShell**ウィンドウを開きます。
2. Citrix固有のPowerShellモジュールをロードするには、`asnp citrix*` を実行します。

3. 利用可能なすべてのVMサイズを一覧表示するには、`Get-ChildItem -Path "XDHyp:\Connections\abc-connection\East US.region\serviceoffering.folder"`を実行します。
4. `get-item -Path "XDHyp:\Connections\abc-connection\East US.region\serviceoffering.folder\Standard_M416ms_v2.serviceoffering").AdditionalData`を実行します。
5. `MaxNetworkInterfaces`を確認して、最大NIC数を把握します。

VM上に複数のNICを持つカタログを作成する

VM上に複数のNICを持つカタログを作成するには、次の手順を実行します。

1. Delivery ControllerホストからPowerShellウィンドウを開きます。
2. Citrix固有のPowerShellモジュールをロードするには、`asnp citrix*`を実行します。
3. まだ作成されていない場合は、IDプールを作成します。
4. プロビジョニングスキームを作成します。

   - マシンプロファイルに基づかないマシンカタログを作成する場合は、`NetworkMappings`パラメーターを指定して`New-ProvScheme`コマンドを実行します。`NetworkMappings`パラメーターに複数のサブネットを追加できます。例：

     ```
     New-Provscheme -NetworkMappings
     @{"0"="subnetpath1";"1"="subnetpath1"}
     ```

   - マシンプロファイルに基づいたマシンカタログを作成する場合:

     a. 複数のNICを持つVMをAzureに作成します。詳しくは、複数のNICを持つWindows仮想マシンの作成と管理を参照してください。新しいVMを作成し、Azureポータルの Networkingページでネットワークインターフェイスをアタッチすることもできます。

     b. VMをマシンプロファイルの入力として使用して、`New-ProvScheme`コマンドを実行します。

     > **注：**
     >
     > マシンプロファイルベースのマシンカタログを作成する場合、`NetworkMappings`の数は、マシンプロファイルの`NetworkInterfaceCount`と同じである必要があり

> ます。`NetworkInterfaceCount` は、`Get-item -Path "machine profile path"` の `AdditionalData` から取得できます。

5. カタログの作成を完了します。

VM上に複数のNICを持つようにカタログを更新する

VM上に複数のNICを持つようにカタログを更新するには、次の手順を実行します。

1. Delivery Controllerホストから**PowerShell**ウィンドウを開きます。
2. Citrix固有のPowerShellモジュールをロードするには、`asnp citrix*` を実行します。
3. プロビジョニングスキームを更新します。

   - マシンプロファイルに基づかないマシンカタログを作成する場合は、`NetworkMappings` パラメーターを指定して `Set-ProvScheme` コマンドを実行します。パラメーター `NetworkMappings` に複数のサブネットを追加できます。例：

     ```
     Set-Provscheme -NetworkMappings
     @{"0"="subnetpath1";"1"="subnetpath1"}
     ```

   - マシンプロファイルに基づいてマシンカタログを作成する場合：

     a. 複数の NIC を持つ VM を Azure に作成します。詳しくは、「複数の NIC を持つ Windows 仮想マシンの作成と管理」を参照してください。

     b. VM をマシンプロファイルの入力として使用して `Set-ProvScheme` コマンドを実行します。

既存の VM を更新して、VM に複数の NIC を持たせる

`Set-ProvVMUpdateTimeWindow` を使用して既存のVMを更新したり、更新時間枠中に既存のVMでパワーサイクルを実行したりすることもできます。

Azure Monitor エージェントがインストールされたカタログ VM をプロビジョニングする

Azure監視は、Azureおよびオンプレミス環境からのテレメトリデータを収集、分析し、それに基づいて行動するために使用できるサービスです。

Azure Monitor Agent (AMA) は、仮想マシンなどのコンピューティングリソースから監視データを収集し、そのデータを Azure Monitor に配信します。現在、イベントログ、Syslog、パフォーマンスメトリックの収集をサポートしており、Azure Monitor Metrics および Azure Monitor Logs データソースに送信します。

監視データ内の VM を一意に識別して監視を有効にするには、AMA を拡張機能としてインストールした MCS マシンカタログの VM をプロビジョニングできます。

要件

- 権限: 必要な Azure 権限 に指定されている最小限の Azure 権限と、Azure Monitor を使用するための以下の権限があることを確認してください。
  - `Microsoft.Compute/virtualMachines/extensions/read`
  - `Microsoft.Compute/virtualMachines/extensions/write`
  - `Microsoft.Insights/DataCollectionRuleAssociations/Read`
  - `Microsoft.Insights/dataCollectionRuleAssociations/write`
  - `Microsoft.Insights/DataCollectionRules/Read`
- データ収集ルール: Azure portal でデータ収集ルールを設定します。DCR の設定については、「データ収集ルールを作成する」を参照してください。DCR はプラットフォーム固有 (Windows または Linux) です。必要なプラットフォームに応じて DCR を作成してください。AMA は、データ収集ルール (DCR) を使用して、VM などのリソースと、Azure Monitor Metrics や Azure Monitor Logs などのデータソース間のマッピングを管理します。
- デフォルトワークスペース: Azure portal でワークスペースを作成します。ワークスペースの作成については、「Log Analytics ワークスペースを作成する」を参照してください。ログとデータを収集すると、その情報はワークスペースに保存されます。ワークスペースには一意のワークスペース ID とリソース ID があります。ワークスペース名は、特定のリソースグループに対して一意である必要があります。ワークスペースを作成したら、データソースとソリューションを設定して、データをワークスペースに保存します。
- 監視拡張機能のホワイトリスト登録: 拡張機能 `AzureMonitorWindowsAgent` および `AzureMonitorLinuxAgent` は、Citrix が定義したホワイトリスト登録済みの拡張機能です。ホワイトリスト登録済みの拡張機能のリストを表示するには、PoSH コマンド `Get-ProvMetadataConfiguration` を使用します。
- マスターイメージ: Microsoft は、既存のマシンから新しいマシンを作成する前に、既存のマシンから拡張機能を削除することを推奨しています。拡張機能が削除されない場合、残存ファイルや予期しない動作につながる可能性があります。詳細については、「VM が既存の VM から再作成された場合」を参照してください。

AMA を有効にしてカタログ VM をプロビジョニングするには:

1. マシンプロファイルテンプレートを設定します。
   - VM をマシンプロファイルテンプレートとして使用する場合:

a. Azure ポータルで VM を作成します。

b. VM の電源を入れます。

c. **Resources** の下のデータ収集ルールに VM を追加します。これにより、テンプレート VM にエージェントのインストールが呼び出されます。

注:

Linux カタログを作成する必要がある場合は、Linux マシンを設定します。

- テンプレート仕様をマシンプロファイルテンプレートとして使用する場合:

a. テンプレート仕様を設定します。

b. 生成されたテンプレート仕様に、次の拡張機能とデータ収集ルール関連付けを追加します。

```
{

"type": "Microsoft.Compute/virtualMachines/extensions",

"apiVersion": "2022-03-01",

"name": "<vm-name>/AzureMonitorWindowsAgent",

"dependsOn": [

    "Microsoft.Compute/virtualMachines/<vm-name>"

],

"location": "<azure-region>",

"properties": {

    "publisher": "Microsoft.Azure.Monitor",

    "type": "AzureMonitorWindowsAgent",

    "typeHandlerVersion": "1.0",

    "autoUpgradeMinorVersion": true,
```

```
    "enableAutomaticUpgrade": true

}

},

 {

    "type": "Microsoft.Insights/dataCollectionRuleAssociations",

    "apiVersion": "2021-11-01",

    "name": "<associatio-name>",

    "scope": "Microsoft.Compute/virtualMachines/<vm-name>",

    "dependsOn": [

     "Microsoft.Compute/virtualMachines/<vm-name>",

    "Microsoft.Compute/virtualMachines/<vm-name>/extensions/
AzureMonitorWindowsAgent"

    ],

    "properties": {

       "description": "Association of data collection rule.
Deleting this association will break the data collection for this
Arc server.",

     "dataCollectionRuleId": "/subscriptions/<azure-
subscription>/resourcegroups/<azure-resource-group>/providers/
microsoft.insights/datacollectionrules/<azure-data-collection-
rule>"

     }

    }
```

2. 既存の MCS マシンカタログを作成または更新します。

- 新しい MCS カタログを作成するには:
  a. Web Studio で、その VM またはテンプレート仕様をマシンプロファイルとして選択します。
  b. カタログを作成するための次の手順に進みます。
- 既存の MCS カタログを更新するには、次の PoSH コマンドを使用します。
  - 新しいVMに更新されたマシンプロファイルテンプレートを適用するには、次のコマンドを実行します。

```
Set-ProvScheme -ProvisioningSchemeName "name"

-MachineProfile "XDHyp:
\HostingUnits\Unit1\machineprofile.folder\abc.resourcegroup\ab-
machine-profile.vm"
```

  - 既存の VM を更新されたマシンプロファイルテンプレートで更新するには：

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
-StartsNow -DurationInMinutes -1
```

3. カタログVMの電源を入れます。
4. Azure portal に移動し、モニター拡張機能が VM にインストールされていること、および VM が DCR のリソースの下に表示されていることを確認します。数分後、監視データが Azure Monitor に表示されます。

トラブルシューティング

Azure Monitor Agentのトラブルシューティングガイダンスについては、以下を参照してください。

- https://learn.microsoft.com/ja-jp/azure/azure-monitor/agents/azure-monitor-agent-troubleshoot-windows-vm/
- https://learn.microsoft.com/ja-jp/azure/azure-resource-manager/troubleshooting/create-troubleshooting-template/

顧客管理の暗号化キーでマシンカタログを作成する

顧客管理の暗号化キーを使用してマシンカタログを作成する詳細な手順は次のとおりです。

1. PowerShellウィンドウを開きます。

2. Citrix固有のPowerShellモジュールをロードするには、`asnp citrix*`を実行します。
3. `cd xdhyp:/`と入力します。
4. `cd .\HostingUnits\(your hosting unit)`と入力します。
5. `cd diskencryptionset.folder`と入力します。
6. `dir` を入力して、ディスク暗号化セットのリストを取得します。
7. ディスク暗号化セットのIDをコピーします。
8. ディスク暗号化セットのIDを含めるカスタムプロパティ文字列を作成します。例：

```
$customProperties = "<CustomProperties xmlns=`"http://
schemas.citrix.com/2014/xd/machinecreation`" xmlns:xsi=`"http://
www.w3.org/2001/XMLSchema-instance`">

<Property xsi:type=`"StringProperty`" Name=`"StorageAccountType`"
Value=`"Standard_LRS`" />

<Property xsi:type=`"StringProperty`" Name=`"persistWBC`"
Value=`"False`" />

<Property xsi:type=`"StringProperty`" Name=`"PersistOsDisk`"
Value=`"false`" />

<Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`"
Value=`"true`" />

<Property xsi:type=`"StringProperty`" Name=`"DiskEncryptionSetId`"
Value=`"/subscriptions/0xxx4xxx-xxb-4bxx-xxxx-xxxxxxxx/resourceGroups/
abc/providers/Microsoft.Compute/diskEncryptionSets/abc-des`"/>

</CustomProperties>
```

9. まだ作成されていない場合は、IDプールを作成します。例：

```
New-AcctIdentityPool -IdentityPoolName idPool -NamingScheme ms##
-Domain def.local -NamingSchemeType Numeric
```

10. New-ProvSchemeコマンドを実行します: 例:

```
New-ProvScheme -CleanOnBoot -HostingUnitName "name" -IdentityPoolName
"name" -InitialBatchSizeHint 1

-MasterImageVM "XDHyp:\HostingUnits\azure-
res2\image.folder\def.resourcegroup\def.snapshot"

-NetworkMapping @{"0"="XDHyp:\HostingUnits\azure-res2\
\virtualprivatecloud.folder\def.resourcegroup\def-
vnet.virtualprivatecloud\subnet1.network"}

-ProvisioningSchemeName "name"

-ServiceOffering "XDHyp:\HostingUnits\azure-
res2\serviceoffering.folder\Standard_DS2_v2.serviceoffering"

-MachineProfile "XDHyp:
\HostingUnits\<adnet>\machineprofile.folder\<def.resourcegroup>\<machin
e profile vm.vm>"

-CustomProperties $customProperties
```

11. マシンカタログの作成を完了します。

二重暗号化でマシンカタログを作成する

Web StudioとPowerShellコマンドを使用して、二重暗号化されたマシンカタログを作成および更新できます。

二重暗号化されたマシンカタログを作成する方法に関する詳細な手順は次のとおりです。

1. プラットフォーム管理キーと顧客管理キーを使用して、Azure Key VaultとDESを作成します。Azure Key VaultとDESの作成方法については、Azureポータルを使用してマネージドディスクの保存時の二重暗号化を有効にするを参照してください。
2. ホスティング接続で利用可能なDiskEncryptionSetsを参照するには:
    a. **PowerShell**ウィンドウを開きます。
    b. 次のPowerShellコマンドを実行します:
        i. `asnp citrix*`
        ii. `cd xdhyp:`:
        iii. `cd HostingUnits`

iv. `cd YourHostingUnitName` (例えば azure-east)

v. `cd diskencryptionset.folder`

vi. `dir`

カスタムプロパティを使用してカタログを作成または更新するには、`DiskEncryptionSet` の ID を使用できます。

3. マシンプロファイルワークフローを使用する場合は、VM またはテンプレート仕様をマシンプロファイル入力として作成します。

   - VM をマシンプロファイル入力として使用する場合:

     a. Azure Portal で VM を作成します。

     b. **ディスク > キー管理** に移動して、任意の `DiskEncryptionSetID` で VM を直接暗号化します。

   - テンプレート仕様をマシンプロファイル入力として使用する場合:

     a. テンプレートの `properties>storageProfile>osDisk>managedDisk` の下に、`diskEncryptionSet` パラメーターを追加し、二重暗号化 DES の ID を追加します。

4. マシンカタログを作成します。

   - Web Studio を使用する場合は、マシンカタログの作成 の手順に加えて、次のいずれかを実行します。

     ◦ マシンプロファイルベースのワークフローを使用しない場合は、**ディスク設定** ページで、**各マシンのデータを暗号化するために次のキーを使用する** を選択します。次に、ドロップダウンメニューから二重暗号化 DES を選択します。カタログの作成を続行します。

     ◦ マシンプロファイルワークフローを使用する場合は、**イメージ** ページでマスターイメージとマシンプロファイルを選択します。マシンプロファイルのプロパティにディスク暗号化セット ID があることを確認してください。

     カタログで作成されたすべてのマシンは、選択した DES に関連付けられたキーによって二重に暗号化されます。

   - PowerShellコマンドを使用する場合は、次のいずれかを実行します。

     ◦ マシンプロファイルベースのワークフローを使用しない場合は、`New-ProvScheme` コマンドにカスタムプロパティ `DiskEncryptionSetId` を追加します。例:

```
New-ProvScheme -CleanOnBoot -CustomProperties '<CustomProperties
xmlns="http://schemas.citrix.com/2014/xd/machinecreation"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks"
Value="true" />

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
Value="/subscriptions/12345678-xxxx-1234-1234-123456789012/
resourceGroups/Sample-RG/providers/Microsoft.Compute/
diskEncryptionSets/SampleEncryptionSet" />

</CustomProperties>'

-HostingUnitName "Redacted"

-IdentityPoolName "Redacted"

-InitialBatchSizeHint 1

-MasterImageVM "Redacted"

-NetworkMapping @{"0"="Redacted"}

-ProvisioningSchemeName "Redacted"

-ServiceOffering "Redacted"
```

- マシンプロファイルベースのワークフローを使用する場合は、`New-ProvScheme`コマンドでマシンプロファイル入力を使用します。例:

```
New-ProvScheme -CleanOnBoot

-HostingUnitName azure-east

-IdentityPoolName aio-ip

-InitialBatchSizeHint 1
```

```
-MasterImageVM XDHyp:\HostingUnits\azure-
east\image.folder\abc.resourcegroup\fgb-vda-snapshot.snapshot

-NetworkMapping @{"0"="XDHyp:\HostingUnits\azure-
east\virtualprivatecloud.folder\apa-
resourceGroup.resourcegroup\apa-resourceGroup-
vnet.virtualprivatecloud\default.network"}

-ProvisioningSchemeName aio-test

-MachineProfile XDHyp:\HostingUnits\azure-
east\machineprofile.folder\abc.resourcegroup\abx-
mp.templatespec\1.0.0.templatespecversion
```

5. リモートPowerShell SDKを使用してカタログの作成を完了します。リモートPowerShell SDKを使用してカタログを作成する方法については、https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/を参照してください。カタログで作成されたすべてのマシンは、選択したDESに関連付けられたキーによって二重に暗号化されます。

暗号化されていないカタログを二重暗号化を使用するように変換する

マシンカタログの暗号化タイプ（カスタムプロパティまたはマシンプロファイルを使用）を更新できます。

- マシンプロファイルベースのワークフローを使用しない場合は、`Set-ProvScheme`コマンドにカスタムプロパティDiskEncryptionSetIdを追加します。例:

```
Set-ProvScheme -ProvisioningSchemeName "SampleProvSchemeName"

-CustomProperties '<CustomProperties xmlns="http://schemas.citrix.com/
2014/xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="DiskEncryptionSetId" Value="/
subscriptions/12345678-xxxx-1234-1234-123456789012/resourceGroups/
Sample-RG/providers/Microsoft.Compute/diskEncryptionSets/
SampleEncryptionSet" />

</CustomProperties>'
```

- マシンプロファイルベースのワークフローを使用する場合は、`Set-ProvScheme`コマンドでマシンプロファイル入力を使用します。例:

```
Set-ProvScheme -ProvisioningSchemeName mxiao-test -MachineProfile
XDHyp:\HostingUnits\azure-
east\machineprofile.folder\aelx.resourcegroup\elx-
mp.templatespec\1.0.0.templatespecversion
```

成功すると、カタログに追加するすべての新しいVMは、選択したDESに関連付けられたキーによって二重暗号化されます。

カタログが二重暗号化されていることを確認する

- ウェブスタジオで:

  a. **マシンカタログ**に移動します。

  b. 確認するカタログを選択します。画面下部にある**テンプレートプロパティ**タブをクリックします。

  c. **Azureの詳細**で、**ディスク暗号化セット**のディスク暗号化セットIDを確認します。カタログのDES IDが空白の場合、カタログは暗号化されていません。

  d. Azure Portalで、DES IDに関連付けられたDESの暗号化タイプがプラットフォーム管理キーと顧客管理キーであることを確認します。

- PowerShellコマンドの使用:

  a. **PowerShell**ウィンドウを開きます。

  b. Citrix固有のPowerShellモジュールをロードするには、`asnp citrix*`を実行します。

  c. マシンカタログの情報を取得するには、`Get-ProvScheme`を使用します。例:

```
Get-ProvScheme -ProvisioningSchemeName "SampleProvSchemeName"
```

  d. マシンカタログのDES IDカスタムプロパティを取得します。例:

```
<Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
Value="/subscriptions/12345678-1234-1234-1234-123456789012/
resourceGroups/Sample-RG/providers/Microsoft.Compute/
diskEncryptionSets/SampleEncryptionSet" />
```

e. Azure Portalで、DES IDに関連付けられたDESの暗号化タイプがプラットフォーム管理キーと顧客管理キーであることを確認します。

Azureエフェメラルディスクでカタログを作成する

エフェメラルディスクを使用するには、`New-ProvScheme`の実行時にカスタムプロパティ`UseEphemeralOsDisk`を**true**に設定する必要があります。

> **注:**
>
> カスタムプロパティ`UseEphemeralOsDisk`が**false**に設定されているか、値が指定されていない場合、プロビジョニングされたすべてのVDAはプロビジョニングされたOSディスクを引き続き使用します。

以下は、プロビジョニングスキームで使用するカスタムプロパティのセットの例です。

```
"CustomProperties": [

            {

                "Name": "UseManagedDisks",

                "Value": "true"

            },

            {

                "Name": "StorageType",

                "Value": "Standard_LRS"

            },

            {

                "Name": "UseSharedImageGallery",

                "Value": "true"

            },
```

```
            {
                "Name": "SharedImageGalleryReplicaRatio",
                "Value": "40"
            },
            {
                "Name": "SharedImageGalleryReplicaMaximum",
                "Value": "10"
            },
            {
                "Name": "LicenseType",
                "Value": "Windows_Server"
            },
            {
                "Name": "UseEphemeralOsDisk",
                "Value": "true"
            }
        ],
```

カタログのエフェメラルディスクを構成する

カタログのAzureエフェメラルOSディスクを構成するには、`Set-ProvScheme`で`UseEphemeralOsDisk`パラメーターを使用します。`UseEphemeralOsDisk`パラメーターの値を**true**に設定します。

> **注:**

> この機能を使用するには、`UseManagedDisks`と`UseSharedImageGallery`のパラメーターも有効にする必要があります。

> 例:

```
Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="UseSharedImageGallery"
Value="true" />

<Property xsi:type="StringProperty" Name="UseEphemeralOsDisk"
Value="true" />

</CustomProperties>'
```

エフェメラルディスクに関する重要な考慮事項

`New-ProvScheme`を使用してエフェメラルOSディスクをプロビジョニングするには、次の制約を考慮してください。

- カタログに使用されるVMサイズは、エフェメラルOSディスクをサポートしている必要があります。
- VMサイズに関連付けられているキャッシュまたは一時ディスクのサイズは、OSディスクのサイズ以上である必要があります。
- 一時ディスクのサイズは、キャッシュディスクのサイズよりも大きくする必要があります。

また、以下の状況ではこれらの問題も考慮してください。

- プロビジョニングスキームを作成する際。
- プロビジョニングスキームを変更する際。
- イメージを更新する際。

Azure専用ホスト

MCSを使用して、Azure専用ホストにVMをプロビジョニングできます。Azure専用ホストにVMをプロビジョニングする前に:

- ホストグループを作成します。
- そのホストグループ内にホストを作成します。
- カタログと仮想マシンを作成するために、十分なホスト容量が確保されていることを確認してください。

次のPowerShellスクリプトを使用して、ホストテナンシーが定義されたマシンのカタログを作成できます。

```
New-ProvScheme <otherParameters> -CustomProperties '<CustomProperties
xmlns="http://schemas.citrix.com/2014/xd/machinecreation"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

 <Property xsi:type="StringProperty" Name="HostGroupId"
Value="myResourceGroup/myHostGroup" />

 ...other Custom Properties...

 </CustomProperties>
```

MCSを使用してAzure専用ホストに仮想マシンをプロビジョニングする場合、以下を考慮してください。

- *専用ホスト*はカタログのプロパティであり、カタログ作成後に変更することはできません。専用テナンシーは現在、Azureではサポートされていません。
- ホスティングユニットのリージョンに、事前に構成されたAzureホストグループが、`HostGroupId` パラメータを使用する際に必要です。
- Azureの自動配置が必要です。この機能は、ホストグループに関連付けられたサブスクリプションをオンボードする要求を行います。詳細については、「VM Scale Set on Azure Dedicated Hosts - Public Preview」を参照してください。自動配置が有効になっていない場合、MCSはカタログ作成中にエラーをスローします。

Azure Compute Galleryイメージを使用してマシンカタログを作成または更新する

マシンカタログの作成に使用するイメージを選択する際、Azure Compute Gallery で作成したイメージを選択できます。

これらのイメージを表示するには、次の操作を行う必要があります。

1. Citrix Virtual Apps and Desktopsサイトを構成します。
2. Azure Resource Managerに接続します。

3. Azureポータルで、リソースグループを作成します。詳細については、「Create an Azure Compute Gallery using the portal」を参照してください。
4. リソースグループ内で、Azure Compute Galleryを作成します。
5. Azure Compute Gallery内で、イメージ定義を作成します。
6. イメージ定義内で、イメージバージョンを作成します。

Azure Compute Gallery のイメージを使用してマシンカタログを作成または更新するには、次の PowerShell コマンドを使用します。

1. PowerShell ウィンドウを開きます。
2. Citrix固有のPowerShellモジュールをロードするために`asnp citrix*`を実行します。
3. リソースグループを選択し、そのリソースグループのすべてのギャラリーを一覧表示します。

```
Get-ChildItem -LiteralPath @("XDHyp:
\HostingUnits\testresource\image.folder\sharedImageGalleryTest.resource
group")
```

4. ギャラリーを選択し、そのギャラリーのすべてのイメージ定義を一覧表示します。

```
Get-ChildItem -LiteralPath @("XDHyp:
\HostingUnits\testresource\image.folder\sharedImageGalleryTest.resource
group\sharedImageGallery.sharedimagegallery")
```

5. 1つのイメージ定義を選択し、そのイメージ定義のすべてのイメージバージョンを一覧表示します。

```
Get-ChildItem -LiteralPath @("XDHyp:
\HostingUnits\testresource\image.folder\sharedImageGalleryTest.resource
group\sharedImageGallery.sharedimagegallery\sigtestimage.imagedefinitio
n")
```

6. 次の要素を使用して、MCSカタログを作成および更新します。
   - リソースグループ
   - ギャラリー
   - ギャラリーイメージ定義
   - ギャラリーイメージバージョン

Remote PowerShell SDK を使用してカタログを作成する方法については、https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/ を参照してください。

共有イメージギャラリーの構成

`New-ProvScheme` コマンドを使用して、Shared Image Gallery をサポートするプロビジョニングスキームを作成します。`Set-ProvScheme` コマンドを使用して、プロビジョニングスキームのこの機能を有効または無効にし、レプリカ比率とレプリカの最大値を変更します。

Shared Image Gallery 機能をサポートするために、プロビジョニングスキームに3つのカスタムプロパティが追加されました。

`UseSharedImageGallery`

- 公開されたイメージを保存するためにShared Image Galleryを使用するかどうかを定義します。**True**に設定されている場合、イメージはShared Image Galleryイメージとして保存され、それ以外の場合はスナップショットとして保存されます。
- 有効な値は**True**と**False**です。
- プロパティが定義されていない場合、デフォルト値は**False**です。

`SharedImageGalleryReplicaRatio`

- マシンとギャラリーイメージバージョンレプリカの比率を定義します。
- 有効な値は0より大きい整数です。
- プロパティが定義されていない場合、デフォルト値が使用されます。永続OSディスクのデフォルト値は1000、非永続OSディスクのデフォルト値は40です。

`SharedImageGalleryReplicaMaximum`

- 各ギャラリーイメージバージョンに対するレプリカの最大数を定義します。
- プロパティが定義されていない場合、デフォルト値は100です。
- プロパティが定義されていない場合、デフォルト値は100です。

> **ヒント:**

> MCSプロビジョニングされたカタログの公開イメージを保存するためにShared Image Galleryを使用する場合、MCSはカタログ内のマシンの数、レプリカ比率、およびレプリカの最大値に基づいてギャラリーイメージバージョンのレプリカ数を設定します。レプリカ数

は、カタログ内のマシンの数をレプリカ比率で割って（最も近い整数値に切り上げて）、その値を最大レプリカ数で上限を設けることによって計算されます。たとえば、レプリカ比率が20で最大値が5の場合、0〜20台のマシンには1つのレプリカが作成され、21〜40台には2つのレプリカ、41〜60台には3つのレプリカ、61〜80台には4つのレプリカ、81台以上には5つのレプリカが作成されます。

ユースケース: Shared Image Galleryのレプリカ比率とレプリカ最大値を更新する

既存のマシンカタログはShared Image Galleryを使用しています。カタログ内の既存のすべてのマシンおよび今後のマシンのカスタムプロパティを更新するには、`Set-ProvScheme`コマンドを使用します。

```
Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<Property xsi:type="StringProperty" Name="StorageType"
Value="Standard_LRS"/> <Property xsi:type="StringProperty"
Name="UseManagedDisks" Value="True"/> <Property xsi:type="StringProperty"
Name="UseSharedImageGallery" Value="True"/> <Property
xsi:type="IntProperty" Name="SharedImageGalleryReplicaRatio" Value="30"/>
<Property xsi:type="IntProperty" Name="SharedImageGalleryReplicaMaximum"
Value="20"/></CustomProperties>'
```

ユースケース：スナップショットカタログを Shared Image Gallery カタログに変換する

このユースケースの場合:

1. `UseSharedImageGallery`フラグを**True**に設定して`Set-ProvScheme`を実行します。オプションで、`SharedImageGalleryReplicaRatio`および`SharedImageGalleryReplicaMaximum`プロパティを含めます。
2. カタログを更新します。
3. マシンの電源を入れ直して、強制的に更新します。

例:

```
Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<Property xsi:type="StringProperty" Name="StorageType"
Value="Standard_LRS"/> <Property xsi:type="StringProperty"
Name="UseManagedDisks" Value="True"/> <Property xsi:type="StringProperty"
```

```
Name="UseSharedImageGallery" Value="True"/> <Property
xsi:type="IntProperty" Name="SharedImageGalleryReplicaRatio" Value="30"/>
<Property xsi:type="IntProperty" Name="SharedImageGalleryReplicaMaximum"
Value="20"/></CustomProperties>'
```

ヒント:

パラメーター`SharedImageGalleryReplicaRatio`と`SharedImageGalleryReplicaMaximum`は必須ではありません。`Set-ProvScheme`コマンドが完了しても、Shared Image Galleryイメージはまだ作成されていません。カタログがギャラリーを使用するように構成されると、次回のカタログ更新操作で公開されたイメージがギャラリーに保存されます。カタログ更新コマンドは、ギャラリー、ギャラリーイメージ、およびイメージバージョンを作成します。マシンの電源を入れ直すと更新され、必要に応じてレプリカ数が更新されます。それ以降、既存のすべての非永続マシンはShared Image Galleryイメージを使用してリセットされ、新しくプロビジョニングされたすべてのマシンはイメージを使用して作成されます。古いスナップショットは数時間以内に自動的にクリーンアップされます。

ユースケース: 共有イメージギャラリーカタログをスナップショットカタログに変換する

このユースケースの場合:

1. `UseSharedImageGallery`フラグを**False**に設定するか、未定義のままにして`Set-ProvScheme`を実行します。
2. カタログを更新します。
3. マシンの電源を入れ直して、強制的に更新します。

例:

```
Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<Property xsi:type="StringProperty" Name="StorageType"
Value="Standard_LRS"/> <Property xsi:type="StringProperty"
Name="UseManagedDisks" Value="True"/> <Property xsi:type="StringProperty"
Name="UseSharedImageGallery" Value="False"/></CustomProperties>'
```

ヒント:

スナップショットから共有イメージギャラリーカタログへの更新とは異なり、各マシンのカスタムデータはまだ新しいカスタムプロパティを反映するように更新されていません。元の共有イメージギャラリーカスタムプロパティを表示するには、次のコマンドを実行します: `Get-ProvVm -ProvisioningSchemeName catalog-name`。`Set-ProvScheme` コマンドが完了しても、イメージスナップショットはまだ作成されていません。カタログがギャラリーを使用しないように構成されると、次回のカタログ更新操作で公開されたイメージがスナップショットとして保存されます。その時点から、既存のすべての非永続マシンはスナップショットを使用してリセットされ、新しくプロビジョニングされたすべてのマシンはスナップショットから作成されます。マシンの電源を入れ直すと更新され、その時点でカスタムマシンデータが更新され、`UseSharedImageGallery` が **False** に設定されていることが反映されます。古い共有イメージギャラリーアセット（ギャラリー、イメージ、バージョン）は、数時間以内に自動的にクリーンアップされます。

指定された可用性ゾーンにマシンをプロビジョニングする

Azure環境では、特定の可用性ゾーンにマシンをプロビジョニングできます。これはPowerShellを使用して実現できます。

注:

ゾーンが指定されていない場合、MCSはAzureにリージョン内にマシンを配置させます。複数のゾーンが指定されている場合、MCSはそれらのゾーンにマシンをランダムに分散します。

PowerShellによる可用性ゾーンの構成

PowerShellを使用して、`Get-Item` で提供されるインベントリアイテムを表示できます。たとえば、*米国東部リージョン*の `Standard_B1ls` サービス提供を表示するには:

```
$serviceOffering = Get-Item -path "XDHyp:\Connections\my-connection-
name\East US.region\serviceoffering.folder\Standard_B1ls.serviceoffering"
```

ゾーンを表示するには、アイテムの`AdditionalData`パラメーターを使用します:

`$serviceOffering.AdditionalData`

可用性ゾーンが指定されていない場合、マシンのプロビジョニング方法に変更はありません。

PowerShellを介して可用性ゾーンを構成するには、`New-ProvScheme`操作で利用可能な**Zones**カスタムプロパティを使用します。**Zones**プロパティは、マシンをプロビジョニングする可用性ゾーンのリストを定義します。これらのゾーンには、1つ以上の可用性ゾーンを含めることができます。たとえば、ゾーン1および3の`<Property xsi:type="StringProperty" Name="Zones" Value="1, 3"/>`です。

プロビジョニングスキームのゾーンを更新するには、`Set-ProvScheme`コマンドを使用します。

無効なゾーンが提供された場合、プロビジョニングスキームは更新されず、無効なコマンドを修正する方法に関する指示を提供するエラーメッセージが表示されます。

> **ヒント:**
>
> 無効なカスタムプロパティを指定すると、プロビジョニングスキームは更新されず、関連するエラーメッセージが表示されます。

ストレージの種類

MCSを使用するAzure環境の仮想マシンに対して、異なるストレージの種類を選択します。ターゲットVMの場合、MCSは以下をサポートします。

- OSディスク: プレミアムSSD、SSD、またはHDD
- ライトバックキャッシュディスク: プレミアムSSD、SSD、またはHDD

これらのストレージの種類を使用する場合、以下を考慮してください。

- 選択したストレージの種類をVMがサポートしていることを確認してください。
- 構成でAzureエフェメラルディスクを使用している場合、ライトバックキャッシュディスク設定のオプションは表示されません。

> **ヒント:**
>
> `StorageType`はOSタイプとストレージアカウント用に構成されます。`WBCDiskStorageType`はライトバックキャッシュストレージタイプ用に構成されます。通常のカタログの場合、`StorageType`が必要です。`WBCDiskStorageType`が構成されていない場合、`StorageType`が`WBCDiskStorageType`のデフォルトとして使用されます。

> WBCDiskStorageType が構成されていない場合、StorageType が WBCDiskStorageType のデフォルトとして使用されます。

ストレージの種類を構成する

VMのストレージタイプを構成するには、`New-ProvScheme` の `StorageType` パラメーターを使用します。`StorageType` パラメーターの値をサポートされているストレージタイプのいずれかに設定します。

以下は、プロビジョニングスキームにおける `CustomProperties` パラメーターの設定例です。

```
Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="StorageType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="LicenseType"
Value="Windows_Client" />

</CustomProperties>'
```

ゾーン冗長ストレージを有効にする

カタログ作成時にゾーン冗長ストレージを選択できます。これは、Azure マネージドディスクを複数の可用性ゾーンに同期的にレプリケートし、あるゾーンでの障害発生時に他のゾーンの冗長性を利用して回復できるようにします。

ストレージタイプのカスタムプロパティで **Premium_ZRS** と **StandardSSD_ZRS** を指定できます。ZRS ストレージは、既存のカスタムプロパティまたは **MachineProfile** テンプレートを使用して設定できます。ZRS ストレージは、`-StartsNow` および `-DurationInMinutes -1` パラメータを持つ `Set-ProvVMUpdateTimeWindow` コマンドでもサポートされており、既存のマシンを LRS から ZRS ストレージに変更できます。

制限事項:

- マネージドディスクのみをサポート
- プレミアムおよび標準ソリッドステートドライブ (SSD) のみでサポート
- `StorageTypeAtShutdown` には対応していません

- 一部のリージョンでのみ利用可能です。
- 大規模にZRSディスクを作成すると、Azureのパフォーマンスが低下します。そのため、最初の電源投入時には、マシンをより小さなバッチ（一度に300台未満のマシン）で起動してください。

ゾーン冗長ストレージをディスクストレージタイプとして設定する

初期カタログ作成時にゾーン冗長ストレージを選択することも、既存のカタログでストレージタイプを更新することもできます。

POWERSHELLコマンドを使用してゾーン冗長ストレージを選択する

`New-ProvScheme` PowerShellコマンドを使用してAzureで新しいカタログを作成する場合、`StorageAccountType`の値として`Standard_ZRS`を使用します。 例:

```
<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="StandardSSD_ZRS" />
```

この値を設定すると、それが適切に使用できるかどうかを判断する動的APIによって検証されます。ZRSの使用がカタログに対して有効でない場合、以下の例外が発生する可能性があります。

- **StorageTypeAtShutdownNotSupportedForZrsDisks**: StorageTypeAtShutdownカスタムプロパティはZRSストレージでは使用できません。
- **StorageAccountTypeNotSupportedInRegion**: この例外は、ZRSをサポートしていないAzureリージョンでZRSストレージを使用しようとすると発生します。
- **ZrsRequiresManagedDisks**: ゾーン冗長ストレージはマネージドディスクでのみ使用できます。

以下のカスタムプロパティを使用して、ディスクストレージタイプを設定できます。

- `StorageType`
- `WBCDiskStorageType`
- `IdentityDiskStorageType`

注:

カタログ作成時に、カスタムプロパティが設定されていない場合、マシンプロファイルのOSディスク`StorageType`が使用されます。

マシンプロファイルからVMとNICの診断設定をキャプチャする

マシンカタログの作成時、既存のマシンカタログの更新時、および既存のVMの更新時に、マシンプロファイルからVMとNICの診断設定をキャプチャできます。

VMまたはテンプレート仕様をマシンプロファイルのソースとして作成できます。

主な手順

1. Azureで必要なIDを設定します。これらのIDはテンプレート仕様で指定する必要があります。
    - ストレージアカウント
    - Log Analyticsワークスペース
    - 標準ティアの価格設定のEvent Hub名前空間
2. マシンプロファイルソースを作成します。
3. 新しいマシンカタログを作成するか、既存のカタログを更新するか、既存のVMを更新します。

Azureで必要なIDを設定します

Azureで次のいずれかを設定します。

- ストレージアカウント
- ログ分析ワークスペース
- Standardティアの価格設定を持つイベントハブ名前空間

ストレージアカウントを設定します

Azureで標準ストレージアカウントを作成します。テンプレート仕様で、ストレージアカウントの完全なresourceIdを`storageAccountId`として指定します。

VMがストレージアカウントにデータをログ記録するように設定されると、データは`insights-metrics-pt1m`コンテナの下にあります。

LOG ANALYTICSワークスペースを設定します

Log Analyticsワークスペースを作成します。テンプレート仕様で、Log Analyticsワークスペースの完全なresourceIdをworkspaceIdとして指定します。

VMがワークスペースにデータをログ記録するように設定されると、Azureのでデータをクエリできます。Azureので次のコマンドを実行して、リソースによってログ記録されたすべてのメトリックの数を表示できます。

```
AzureMetrics | summarize Count=count() by ResourceId
```

イベントハブを設定します

Azureポータルでイベントハブを設定するには、次の手順を実行します。

1. 標準ティアの価格でイベントハブの名前空間を作成します。
2. 名前空間の下にイベントハブを作成します。
3. イベントハブの下にある に移動します。トグルをオンにして、Avro 出力タイプでキャプチャします。
4. ログをキャプチャするために、既存のストレージアカウントに新しいコンテナを作成します。
5. テンプレート仕様で、`eventHubAuthorizationRuleId` を次の形式で指定します: `/subscriptions/093f4c12-704b-4b1d-8339-f339e7557f60/resourcegroups/matspo/providers/Microsoft.EventHub/namespaces/matspoeventhub/authorizationrules/RootManageSharedAccessKey`
6. イベントハブの名前を指定します。

VMがイベントハブにデータをログするように設定されると、データは構成されたストレージコンテナにキャプチャされます。

マシンプロファイルソースを作成する

VMまたはテンプレートスペックをマシンプロファイルソースとして作成できます。

診断設定を含むVMベースのマシンプロファイルを作成する

VMをマシンプロファイルとして作成する場合は、まずテンプレートVM自体に診断設定をセットアップします。詳細な手順については、MicrosoftドキュメントのAzure Monitorの診断設定を参照してください。

VMまたはNICに関連付けられた診断設定が現在存在することを確認するには、次のコマンドを実行できます。

```
az monitor diagnostic-settings list --resource-group matspo --resource
matspo-tog-cc2659 --resource-type microsoft.network/networkInterfaces
```

```
az monitor diagnostic-settings list --resource-group matspo --resource
matspo-tog-cc2 --resource-type microsoft.compute/virtualMachines
```

診断設定を含むテンプレートスペックベースのマシンプロファイルを作成する

診断設定がすでに有効になっているVMを使用し、それをARMテンプレートスペックにエクスポートする場合、これらの設定はテンプレートに自動的に含まれません。ARMテンプレート内で診断設定を手動で追加または変更する必要があります。

ただし、VMをマシンプロファイルとして使用する場合、MCSは、重要な診断設定が正確にキャプチャされ、MCSカタログ内のリソースに適用されることを保証します。

1. VM と NIC を定義する標準テンプレート仕様を作成します。
2. 診断設定を仕様に従って展開するための追加リソースを追加します: Microsoft.Insights diagnosticSettings。スコープについては、テンプレート内の VM または NIC を部分的な ID を持つ名前で参照します。たとえば、テンプレート仕様で test-VM という名前の VM にアタッチされた診断設定を作成する場合、スコープを次のように指定します。

   ```
   "scope": "microsoft.compute/virtualMachines/test-VM",
   ```

3. テンプレート仕様をマシンプロファイルのソースとして使用します。

診断設定を含むカタログを作成または更新する

マシンプロファイルソースを作成した後、`New-ProvScheme` コマンドを使用してマシンカタログを作成し、`Set-ProvScheme` コマンドを使用して既存のマシンカタログを更新し、`Request-ProvVMUpdate` コマンドを使用して既存のVMを更新できます。

ページファイルの場所の決定

ページファイルの場所は、次のシナリオに従って決定されます。

注:

デフォルトのページファイルの場所は OS ディスクです。

シナリオ	場所
ページファイル設定がカスタムプロパティで指定されている	カスタムプロパティで指定されているとおり

シナリオ	場所
エフェメラル OS ディスクまたはハイバネーションが有効になっている	OSディスク
VMに一時ディスクがある	一時ディスク
MCS I/O が有効になっています	WBCディスク

ページファイル設定のシナリオ

次の表は、イメージ準備中およびプロビジョニングスキームの更新中に考えられるページファイル設定のシナリオの一部を示しています。

期間	シナリオ	結果
イメージ準備	プロビジョニングスキームで指定するVMサイズに一時ディスクがないにもかかわらず、ソースイメージのページファイルを一時ディスクに設定する	ページファイルはOSに配置される
イメージ準備	プロビジョニングスキームで指定するVMサイズに一時ディスクがあるにもかかわらず、ソースイメージのページファイルをOSディスクに設定する	ページファイルは一時ディスクに配置されます
イメージの準備	プロビジョニングスキームで、ソースイメージのページファイルを一時ディスクに設定し、エフェメラルOSディスクを有効にします	ページファイルはOSディスクに配置されます
プロビジョニングスキームの更新	VDAバージョンが2311より前のときにプロビジョニングスキームを更新しようとします	警告とともにページファイル設定を変更します

期間	シナリオ	結果
プロビジョニングスキームの更新	VDAバージョンが2311以降のときにプロビジョニングスキームを更新しようとします	ページファイルの場所の決定に従ってページファイルの場所を決定します

ページファイル設定の指定

PowerShellコマンドを使用して、場所やサイズを含むページファイル設定を指定できます。これにより、ページファイルの場所の決定に従ってMCSによって決定されたページファイル設定が上書きされます。これは、マシンカタログ作成中に次の`New-ProvScheme`コマンドを実行することで行えます。

重要な考慮事項

カタログ作成を進める前に、以下を考慮してください。

- すべてのカスタムプロパティ（'PageFileDiskDriveLetterOverride'、'InitialPageFileSizeInMB'、'MaxPageFileSizeInMB'）を`New-ProvScheme`コマンドで指定するか、または何も指定しないでください。
- この機能はCitrix Studioではサポートされていません。
- 初期ページファイルサイズは16 MBから16777216 MBの間である必要があります。
- 最大ページファイルサイズは、初期ページファイルサイズ以上で、かつ16777216 MB未満である必要があります。
- 初期ページファイルサイズと最大ページファイルサイズの両方を同時にゼロに設定できます。

注:

既存のカタログに新しく追加されたVMのページファイル設定は、マスターイメージを更新することなく変更できます。ページファイル設定を変更するには、VDAバージョン2311以降が必要です。PowerShellコマンドを使用してページファイル設定を変更できます。詳細については、「ページファイル設定の変更」を参照してください。

```
New-ProvScheme -CleanOnBoot `

-HostingUnitName "zijinnet" `

-IdentityPoolName "PageFileSettingExample" `
```

```
-ProvisioningSchemeName "PageFileSettingExample" `

-InitialBatchSizeHint 1 `

-MasterImageVM "XDHyp:\HostingUnits\zijinnet\image.folder\neal-zijincloud-
resources.resourcegroup\CustomWin10VDA_OsDisk_1_9473d7c8a6174b2c8284c7d3ef
eea88f.manageddisk" `

-NetworkMapping @{"0"="XDHyp:\\HostingUnits\\zijinnet\
\virtualprivatecloud.folder\\East US.region\\virtualprivatecloud.folder\
\neal-zijincloud-resources.resourcegroup\\neal-zijincloud-resources-
vnet.virtualprivatecloud\\default.network"} `

-ServiceOffering "XDHyp:\\HostingUnits\\zijinnet\\serviceoffering.folder\
\Standard_B2ms.serviceoffering" `

-CustomProperties '<CustomProperties xmlns=" http://schemas.citrix.com/
2014/xd/machinecreation" xmlns:xsi=" http://www.w3.org/2001/XMLSchema-
instance"> `

<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="false"/> `

<Property xsi:type="StringProperty" Name="PersistVm" Value="false"/> `

<Property xsi:type="StringProperty" Name="PageFileDiskDriveLetterOverride"
Value="d"/> `

<Property xsi:type="StringProperty" Name="InitialPageFileSizeInMB"
Value="2048"/> `

<Property xsi:type="StringProperty" Name="MaxPageFileSizeInMB"
Value="8196"/> `

<Property xsi:type="StringProperty" Name="StorageAccountType"
Value="Premium_LRS"/> `

<Property xsi:type="StringProperty" Name="LicenseType"
Value="Windows_Client"/> `

</CustomProperties>'
```

ページファイル設定の変更

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

ページファイル設定を変更するには、VDAバージョン2311以降が必要です。PowerShellコマンドを使用してページファイル設定を変更できます。

Azure環境で変更できるページファイル設定は次のとおりです。

- `PageFileDiskDriveLetterOverride`
- `InitialPageFileSizeInMB`
- `MaxPageFileSizeInMB`

既存のカタログのページファイル設定を変更する

既存のマシンカタログのページファイル設定を変更するには、`Set-ProvScheme`コマンドを実行します。この場合、更新はカタログに追加された新しいVMにのみ適用されます。例:

```
Set-ProvScheme -ProvisioningSchemeName $schemeName -CustomProperties
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="OsType" Value="Windows" />

<Property xsi:type="StringProperty" Name="StorageType"
Value="StandardSSD_LRS" />

<Property xsi:type="StringProperty" Name="PageFileDiskDriveLetterOverride"
Value="D" />

<Property xsi:type="StringProperty" Name="InitialPageFileSizeInMB"
Value="2048" />

<Property xsi:type="StringProperty" Name="MaxPageFileSizeInMB"
Value="8196" />

<Property xsi:type="StringProperty" Name="LicenseType"
Value="Windows_Client" />

<Property  xsi:type="StringProperty" Name="Zones" Value="1" />
```

```
<Property xsi:type="StringProperty" Name="ResourceGroups" Value="neal-
test-group1" />

<Property xsi:type="StringProperty" Name="SchemaVersion" Value="2" />

</CustomProperties>'
```

注：

ライトバックキャッシュを有効にして、PowerShellコマンドを使用して `PageFileDiskDriveLetterOverride` を `C:` に設定しようとすると、MCS IOドライバーはページファイルを正しいディスクドライブに自動的にリダイレクトし、`C:` にはリダイレクトしません。

Azure Spot VMを使用してカタログを作成する

Azure Spot VMを使用すると、Azureの未使用のコンピューティング能力を大幅なコスト削減で活用できます。ただし、Azure Spot VMを割り当てる機能は、現在の容量と価格設定によって異なります。そのため、Azureは強制排除ポリシーに従って、実行中のVMを強制排除したり、VMの作成に失敗したり、VMの電源投入に失敗したりする可能性があります。したがって、Azure Spot VMは、一部の重要でないアプリケーションやデスクトップに適しています。詳細については、Azure Spot Virtual Machinesの使用を参照してください。

制限事項

- すべてのVMサイズがAzure Spot VMでサポートされているわけではありません。詳細については、制限事項を参照してください。

  VMサイズがSpot VMをサポートしているかどうかを確認するには、次のPowerShellコマンドを実行します。VMサイズがSpot VMをサポートしている場合、`SupportsSpotVM` は**True**です。

  ```
  (Get-Item "XDHyp:\HostingUnits\azure-res-
  conn2\serviceoffering.folder\Standard_D2ds_v4.serviceoffering").
  AdditionalData
  ```

- 現在、Azure Spot VMは休止状態をサポートしていません。

要件

Azure Spot VMカタログの仮想マシンプロファイルソース（VMまたはテンプレート仕様）を作成する際、Azure Spotインスタンスを選択するか（VMを使用する場合）、`priority`を`Spot`に設定する必要があります（テンプレート仕様を使用する場合）。

Azure Spot VMを使用してカタログを作成する手順

1. 仮想マシンプロファイルソース（VMまたは起動テンプレート）を作成します。

   - Azureポータルを使用してVMを作成する方法については、Azureポータルを使用してAzure Spot Virtual Machinesを展開するを参照してください。
   - テンプレート仕様を作成するには、テンプレート仕様の**resources > type: Microsoft.Compute/virtualMachines > properties**の下に次のプロパティを追加します。例：

     ```
     "priority": "Spot",

     "evictionPolicy": "Deallocate",

     "billingProfile": {

     "maxPrice": 0.01

     }
     ```

注：

- 立ち退きポリシーは、**割り当て解除**または**削除**にすることができます。
- 非永続VMの場合、MCSは常に立ち退きポリシーを**削除**に設定します。VMが立ち退きになると、非永続ディスク（例: OSディスク）とともに削除されます。永続ディスク（例: IDディスク）は削除されません。ただし、カタログタイプが永続的であるか、`PersistOsDisk`カスタムプロパティがTrueに設定されている場合、OSディスクは永続的です。同様に、`PersistWbc`カスタムプロパティが**True**に設定されている場合、WBCディスクは永続的です。
- 永続VMの場合、MCSは常に立ち退きポリシーを割り当て解除に設定します。VMが立ち退きになると、割り当て解除されます。ディスクに変更は加えられません。

- 最大価格は、1時間あたりに支払う意思のある価格です。**容量のみ**を使用している場合、これは**-1**です。最大価格は、null、-1、またはゼロより大きい小数のみにすることができます。詳細については、価格設定を参照してください。

2. マシンプロファイルでAzure Spot VMが有効になっているかどうかを確認するには、次のPowerShellコマンドを実行します。`SpotEnabled` パラメーターが**True**で、`SpotEvictionPolicy` が**割り当て解除**または**削除**に設定されている場合、マシンプロファイルでAzure Spot VMが有効になっています。例：

   - マシンプロファイルのソースがVMの場合、次のコマンドを実行します。

     ```
     (Get-Item "XDHyp:\HostingUnits\azure-res-
     conn2\machineprofile.folder\fifthcolumn.resourcegroup\kb-spot-
     delete.vm"). AdditionalData
     ```

   - マシンプロファイルのソースがテンプレート仕様の場合、次のコマンドを実行します。

     ```
     (Get-Item "XDHyp:\HostingUnits\azure-res-
     conn2\machineprofile.folder\fifthcolumn.resourcegroup\fc-aeh-
     templatespec.templatespec\14.0.0-spot-
     delete.templatespecversion").AdditionalData
     ```

3. `New-ProvScheme` PowerShellコマンドを使用して、マシンプロファイルでマシンカタログを作成します。

`Set-ProvScheme` コマンドを使用してカタログを更新できます。PowerShellコマンド `Set-ProvVmUpdateTimeWindow` を使用して既存のVMを更新することもできます。マシンプロファイルは次回の電源投入時に更新されます。

実行中のAzure Spot VMでの強制排除

コンピューティング容量が利用できない場合、または1時間あたりの価格が構成されている最大価格よりも高い場合、Azureは実行中のSpot VMを立ち退かせます。デフォルトでは、立ち退きの通知はされません。VMは単にフリーズし、立ち退きになります。Microsoftは、立ち退きを監視するためにスケジュールされたイベントを使用することを推奨しています。立ち退きを継続的に監視するを参照してください。立ち退きの前に通知を受け取るために、VM内からスクリプトを実行することもできます。たとえば、MicrosoftはPythonでポーリングスクリプトScheduledEvents.csを提供しています。

トラブルシューティング

- `Get-ProvVM` コマンドを使用して、プロビジョニングされたVMのcustomMachineDataでSpot VMプロパティを確認できます。優先度フィールドが**Spot**に設定されている場合、Spotが使用中です。
- AzureポータルでVMがSpotを使用しているかどうかを確認できます。

  a. Azureポータルで VMを見つけます。

  b. 「**概要**」ページに移動します。

  c. 下までスクロールし、「**Azure Spot**」セクションを見つけます。

    - Spotが使用されていない場合、このフィールドは空です。
    - Spotが使用されている場合、「**Azure Spot**」と「**Azure Spot eviction policy**」フィールドが設定されます。

1. 構成ページで、VMの課金プロファイルまたは1時間あたりの最大価格を確認できます。

バックアップVMサイズを構成する

パブリッククラウドでは、特定のVMサイズで容量が不足する場合があります。また、Azure Spot VMを使用している場合、Azureの容量要件に基づいてVMはいつでも強制終了されます。Azureの容量不足またはSpot VMの電源投入失敗の場合、MCSはバックアップVMサイズにフォールバックします。MCSマシンカタログの作成または更新時に、カスタムプロパティ `BackupVmConfiguration` を使用してバックアップVMサイズのリストを提供できます。MCSは、リストで指定された順序でバックアップVMサイズにフォールバックしようとします。

MCSがVMに特定のバックアップ構成を使用する場合、次回のシャットダウンまでその構成を使い続けます。次回の電源投入時には、MCSはプライマリVM構成を起動しようとします。失敗した場合、MCSはリストに従ってバックアップVMサイズ構成を再度起動しようとします。

この機能は以下をサポートしています。

- マシンプロファイルを使用するカタログ
- 永続的および非永続的なMCSマシンカタログ
- 現在のAzure環境

重要な考慮事項

- リストには複数のバックアップVMサイズを指定できます。
- リストは一意である必要があります。

- リスト内の各VMにインスタンスタイププロパティを追加できます。タイプは**Spot**または**Regular**のいずれかです。タイプが指定されていない場合、MCSはVMを**Regular**と見なします。
- 既存のカタログのバックアップVMサイズリストは、`Set-ProvScheme` PowerShellコマンドを使用して変更できます。
- カタログに関連付けられたプロビジョニングスキームから作成された既存のVMは、`Set-ProvVMUpdateTimeWindow` コマンドを使用して更新できます。
- 選択した数の既存のMCS VMのバックアップVMサイズリストは、`Set-ProvVM` コマンドを使用して構成できます。ただし、更新を適用するには、`Set-ProvVMUpdateTimeWindow` を使用してVMの更新時間枠を設定し、その時間枠内にVMを起動します。VMで`Set-ProvVm` コマンドが使用された場合、プロビジョニングスキーム上のリストが後で更新されても、VMはその特定のVMに設定されたバックアップVMサイズリストを引き続き使用します。VMにプロビジョニングスキーム上のバックアップリストを使用させるには、`Set-ProvVM` と `-RevertToProvSchemeConfiguration` を使用できます。

バックアップVMサイズでカタログを作成する

> **注:**
>
> Studio UI のフリーズの問題に対処するには、PowerShell コマンドを実行する際に、すべてのシングルクォートを `"` に置き換えてください。

1. **PowerShell**ウィンドウを開きます。
2. Citrix固有のPowerShellモジュールをロードするには、`asnp citrix*` を実行します。
3. ブローカーカタログを作成します。このカタログには、これから作成されるマシンが格納されます。
4. IDプールを作成します。これは、作成されるマシン用に作成されたADアカウントのコンテナになります。
5. マシンプロファイルを使用してプロビジョニングスキームを作成します。「バックアップ構成の構成方法」を参照してください。
6. プロビジョニングスキームの一意のIDでBrokerCatalogを更新します。
7. VMを作成し、カタログに追加します。

既存のカタログを更新する

`Set-ProvScheme`コマンドを使用してプロビジョニングスキームを更新できます。バックアップ構成を構成する方法を参照してください。

既存のVMを更新する

`Set-ProvVMUpdateTimeWindow` PowerShellコマンドを使用して、カタログ内の既存のVMを更新できます。このコマンドは、指定された時間枠内で次回の電源投入時に、カタログに関連付けられたプロビジョニングスキームから作成されたVMを更新します。例:

- `Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName azure-catalog -StartTimeInUTC "3/12/2022 3am" -DurationInMinutes 60`
- `Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName azure-catalog -StartsNow -DurationInMinutes 60`

注:

`StartsNow`はスケジュールされた開始時間を示します。`DurationInMinutes`はスケジュールの時間枠です。

`Set-ProvVM`コマンドを使用して、選択した既存のMCS VMのバックアップVMサイズリストを構成できます。ただし、更新を適用するには、`Set-ProvVMUpdateTimeWindow`を使用してVMの更新時間枠を設定し、その時間枠内でVMを起動する必要があります。例:

1. `Set-ProvVM`コマンドを実行して、選択した既存のMCS VMのバックアップVMサイズリストを構成します。例:

```
Set-ProvVM -ProvisioningSchemeName "name" -VMName "Vm-001"

-CustomProperties

"<CustomProperties xmlns=`"http://schemas.citrix.com/2014/xd/
machinecreation`"xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`">

<Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`"
Value=`"true`" />

<Property xsi:type=`"StringProperty`" Name=`"StorageAccountType`"
```

```
Value=`"Premium_LRS`" />

<Property xsi:type=`"StringProperty`" Name=`"LicenseType`"
Value=`"Windows_Server`"/>

<Property xsi:type=`"StringProperty`" Name=`"PersistWBC`"
Value=`"true`"/>

<Property xsi:type=`"StringProperty`" Name=`"BackupVmConfiguration`"
Value=`"[{&quot;ServiceOffering&quot;: &quot;Standard_D2as_v4&quot;,
&quot;Type&quot;: &quot;Spot&quot;}, {&quot;ServiceOffering&quot;:
&quot;Standard_D2s_v3&quot;, &quot;Type&quot;: &quot;Regular&quot;},
{&quot;ServiceOffering&quot;: &quot;Standard_D2s_v3&quot;,
&quot;Type&quot;: &quot;Spot&quot;}]`"/>

</CustomProperties>"
```

2. `Set-ProvVMUpdateTimeWindow`コマンドを実行して更新を適用します。例:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName azure-catalog
-StartsNow -DurationInMinutes 60
```

すべてのリソースにタグをコピーする

マシンプロファイルで指定されたタグを、マシンカタログ内の新しいVMまたは既存のVMの複数のNICやディスク（OSディスク、IDディスク、ライトバックキャッシュディスクなど）といったすべてのリソースにコピーできます。マシンプロファイルのソースは、VMまたはARMテンプレート仕様にすることができます。

注:

タグに関するポリシーを追加するか（タグコンプライアンスのポリシー定義を割り当てるを参照）、またはマシンプロファイルソースにタグを追加して、リソース上のタグを保持する必要があります。

前提条件

マシンプロファイルソース（VMまたはARMテンプレート仕様）を作成し、そのVMのVM、ディスク、NICにタグを付けます。

- VMをマシンプロファイルの入力として使用する場合は、AzureポータルでVMとすべてのリソースにタグを適用します。「Azureポータルでタグを適用する」を参照してください。
- ARMテンプレート仕様をマシンプロファイルの入力として使用する場合は、各リソースの下に次のタグブロックを追加します。

```
 "tags": {

"TagC": "Value3"

},
```

注:

テンプレート仕様には、最大1つのディスクと少なくとも1つのNICを含めることができます。

新しいマシンカタログ内のVMのリソースにタグをコピーする

1. VMまたはARMテンプレート仕様をマシンプロファイルの入力として使用して、非永続または永続カタログを作成します。
2. カタログにVMを追加して電源をオンにします。マシンプロファイルで指定されたタグが、そのVMの対応するリソースにコピーされていることを確認する必要があります。

注:

マシンプロファイルで提供されるNICの数と、VMで使用するNICの数に不一致がある場合、エラーが発生します。

既存のVMのリソース上のタグを変更する

1. すべてのリソースにタグを付けたマシンプロファイルを作成します。
2. 既存のマシンカタログを、更新されたマシンプロファイルで更新します。例：

```
Set-ProvScheme -ProvisioningSchemeName <YourCatalogName>
-MachineProfile <PathToYourMachineProfile>
```

3. 更新を適用したいVMの電源をオフにします。
4. VMのスケジュールされたアップデートを要求します。例:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName <YourCatalogName>  -
VMName machine1 -StartsNow -DurationInMinutes -1
```

5. VM を起動します。
6. マシンプロファイルで指定されたタグが、対応するリソースにコピーされていることを確認する必要があります。

注：

マシンプロファイルで提供される NIC の数と、`Set-ProvScheme` で提供される NIC の数の間に不一致がある場合、エラーが発生します。

事前フォーマットされたWBCディスクカタログを作成する

プロビジョニングされたマシンの起動パフォーマンスを向上させるために、事前フォーマットされた WBC ディスクカタログを作成できます。この機能を実装するには、WBC が有効な Azure カタログを作成し、追加のカスタムプロパティ `PreformatWriteBackCache` を `True` として含めます。

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

この機能は、MCS がマスタリングフェーズを全体のプロビジョニングワークフローから分離するイメージ管理ワークフローと互換性があります。イメージ管理の詳細については、「イメージ管理」を参照してください。

WBC を有効にし、`PreformatWriteBackCache` を `True` として設定した Azure カタログを作成する例：

```
$customProperties = @'

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="PreformatWriteBackCache"
Value="true" />
```

```
</CustomProperties>

'@



New-ProvScheme -CleanOnBoot `

-ProvisioningSchemeName "provisioningschemename" `

-HostingUnitName "hostingunitname" `

-IdentityPoolName "identitypoolnamename" `

-MasterImageVM "XDHyp:
\HostingUnits\AzureHostingUnit\image.folder\rg.resourcegroup\masterImage.m
anageddisk" `

-CustomProperties $customProperties `

-NetworkMapping $networkMapping `

-UseWriteBackCache `

-WriteBackCacheDiskSize 30
```

既存のカタログの WBC ディスクキャッシュサイズを更新する例：

```
Set-ProvScheme -ProvisioningSchemeName provisioningschemename
-WriteBackCacheDiskSize 127
```

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

Azure で MCS プロビジョニングされた Citrix Provisioning カタログを作成する際に、WBC ディスクを非永続的 (`PersistWBC` を False) にプロビジョニングできます。この構成により、Azure で MCS プロビジョニングされた Citrix Provisioning カタログの VM をシャットダウンした後、ライトバックキャッシュ (WBC) ディスクを削除できます。

条件：

この機能が動作するには、カスタムプロパティ `PreformatWriteBackCache` を `True` として設定する必要があります。

`PersistWBC` を `False`、`PreformatWriteBackCache` を `True` として設定した Azure カタログを作成する例：

```
$customProperties = @'

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="PersistWBC" Value="false" />

<Property xsi:type="StringProperty" Name="PreformatWriteBackCache"
Value="true" />

</CustomProperties>

'@



New-ProvScheme -CleanOnBoot `

-ProvisioningSchemeName "provisioningschemename" `

-HostingUnitName "hostingunitname" `

-IdentityPoolName "identitypoolnamename" `

-MasterImageVM "XDHyp:
\HostingUnits\AzureHostingUnit\image.folder\rg.resourcegroup\masterImage.m
anageddisk" `

-CustomProperties $customProperties `

-NetworkMapping $networkMapping `

-UseWriteBackCache `

-WriteBackCacheDiskSize 30
```

`Set-ProvScheme`コマンドを使用して`PersistWBC`カスタムプロパティを更新することで、既存のカタログを更新することもできます。

次のステップ

- これが最初に作成されたカタログである場合、Web Studioはデリバリーグループを作成するように案内します
- 構成プロセス全体を確認するには、インストールと構成を参照してください
- カタログを管理するには、マシンカタログの管理およびMicrosoft Azureカタログの管理を参照してください

詳細情報

- 接続とリソースの作成および管理
- Microsoft Azure Resource Managerへの接続について
- マシンカタログの作成

Microsoft System Center Virtual Machine Managerカタログを作成する

マシンカタログの作成では、マシンカタログを作成するウィザードについて説明します。以下の情報は、Microsoft System Center Virtual Machine Manager (VMM) 仮想化環境に固有の詳細を扱っています。

> **注:**
>
> VMMカタログを作成する前に、VMMへの接続の作成を完了する必要があります。Microsoft System Center Virtual Machine Managerへの接続を参照してください。

マスターVMを作成する

1. マスターVMにVDAをインストールし、パフォーマンスを向上させるためにデスクトップを最適化するオプションを選択します。
2. バックアップとして使用するために、マスターVMのスナップショットを作成します。
3. 仮想デスクトップを作成します。

SMB 3ファイル共有上のMCS

VMストレージ用のSMB 3ファイル共有でMCSを使用して作成されたマシンカタログの場合、資格情報が次の要件を満たしていることを確認してください。これらの要件により、ControllerのHypervisor Communications Library（HCL）からの呼び出しがSMBストレージに正常に接続されます。

- VMMユーザーの資格情報には、SMBストレージへの完全な読み取り/書き込みアクセス権が含まれている必要があります。
- VMライフサイクルイベント中のストレージ仮想ディスク操作は、VMMユーザー資格情報を使用してHyper-Vサーバー経由で実行されます。

SMBストレージを使用する場合、Controllerから個々のHyper-VマシンへのAuthentication Credential Security Support Provider (CredSSP) を有効にします。このプロセスは、Windows Server 2012上のHyper-VとVMM 2012 SP1で使用します。詳細については、CTX137465を参照してください。

HCLは`CredSSP`を使用してHyper-Vマシンへの接続を開きます。この機能は、Kerberos暗号化されたユーザー資格情報をHyper-Vマシンに渡します。リモートHyper-Vマシン上のセッションでの**PowerShell**コマンドは、提供された資格情報で実行されます。この場合、ストレージへの通信コマンドが正しく機能するように、VMMユーザーの資格情報が使用されます。

次のタスクでは、HCLで生成され、SMB 3.0ストレージに対して動作するためにHyper-Vマシンに送信されるPowerShellスクリプトを使用します。

- **マスターイメージの統合**: マスターイメージは、MCSプロビジョニングスキーム（マシンカタログ）を作成します。マスターVMを複製してフラット化し、新しく作成されたディスクからVMを作成できるようにします（元のマスターVMへの依存関係を削除します）。

  root\\virtualization\\v2名前空間のConvertVirtualHardDisk

  例:

```
$ims = Get-WmiObject -class $class -namespace "root\\virtualization\\v2";

$result = $ims.ConvertVirtualHardDisk($diskName, $vhdastext)

$result
```

- **差分ディスクの作成:** マスターイメージを統合して生成されたマスターイメージから差分ディスクを作成します。その後、差分ディスクは新しいVMに接続されます。

root\\virtualization\\v2名前空間のCreateVirtualHardDisk

例:

```
$ims = Get-WmiObject -class $class -namespace "root\\virtualization\\v2";

$result = $ims.CreateVirtualHardDisk($vhdastext);

$result
```

- **IDディスクのアップロード**: HCLはIDディスクをSMBストレージに直接アップロードできません。そのため、Hyper-VマシンがIDディスクをアップロードしてストレージにコピーする必要があります。Hyper-Vマシンはコントローラーからディスクを読み取ることができないため、HCLはまず次のようにHyper-Vマシンを介してIDディスクをコピーする必要があります。

  a. HCLは、管理者共有を介してIDをHyper-Vマシンにアップロードします。

  b. Hyper-Vマシンは、PowerShellリモートセッションで実行されているPowerShellスクリプトを介して、ディスクをSMBストレージにコピーします。Hyper-Vマシン上にフォルダーが作成され、そのフォルダーのアクセス許可はVMMユーザーのみにロックされます（リモートPowerShell接続を介して）。

  c. HCLは管理者共有からファイルを削除します。

  d. HCLがIDディスクをHyper-Vマシンへのアップロードを完了すると、リモートPowerShellセッションはIDディスクをSMBストレージにコピーします。その後、Hyper-Vマシンから削除します。

  IDディスクフォルダーは、削除された場合でも再利用できるように再作成されます。

- **IDディスクのダウンロード:** アップロードと同様に、IDディスクはHyper-Vマシンを経由してHCLに渡されます。次のプロセスでは、Hyper-Vサーバー上にVMMユーザー権限のみを持つフォルダーが存在しない場合に作成します。

  a. Hyper-Vマシンは、PowerShellスクリプトを介してSMBストレージからローカルのHyper-Vストレージにディスクをコピーします。このスクリプトはPowerShell V3リモートセッションで実行されます。

  b. HCLは、Hyper-Vマシンの管理者共有からディスクをメモリに読み込みます。

  c. HCL は管理者共有からファイルを削除します。

マシンプロファイルを使用してカタログを作成する

System Center Virtual Machine Manager (SCVMM) 環境では、マシンプロファイルを使用して MCS マシンカタログを作成および更新できます。vTPM を有効にできます。また、マシンプロファイル VM のカスタムタグをプロビジョニングされた VM に追加することもできます。

重要な考慮事項

- マスターイメージはスナップショットのみであり、VM ではありません。
- マシンプロファイルのソースとして使用できるのは VM のみです。
- Hyper-V コンソールから VTPM を構成できますが、SCVMM コンソールからは構成できません。
- マスターイメージで vTPM が有効になっている場合は、マシンプロファイルソースで vTPM を有効にする必要があります。
- vTPM は第2世代のマシンでのみサポートされています。
- 次のパラメーターは、個別に指定された場合、マシンプロファイルでキャプチャされた値を上書きします。
  - VMCpuCount
  - VMMemoryMB
  - ディスクストレージ
- カスタムタグは、マスターイメージからではなく、マシンプロファイルからのみ継承されます。`CitrixProvisioningSchemeId` タグは、デフォルトでVMに追加されます。`CitrixProvisioningSchemeId` タグを含めたくない場合は、ホスティングユニットの作成時に `-NoVmTagging` パラメーターを追加します。例:

```
New-Item -HypervisorConnectionName  $ConnectionName `

    -NetworkPath @($NetworkPath) `

    -Path @($HostingUnitPath) `

    -PersonalvDiskStoragePath @() `

    -RootPath $RootPath `

    -StoragePath @($StoragePath) `

    -NoVmTagging
```

```
```

- `Set-ProvScheme` コマンドを使用して既存のカタログを更新できます。
- MCSIOが有効な場合、MCSカタログの作成後にメモリとディスクキャッシュのサイズを更新できます。

マシンプロファイルを使用してマシンカタログを作成する

1. マシンプロファイルのソースとなるVMを作成します。詳細については、「VMMファブリックで仮想マシンをプロビジョニングする」を参照してください。**世代**は一度選択すると変更できません。SCVMMでは、次のことができます。
   - vTPMを有効にするには：
     a. VMを作成したら、Hyper-Vホストにログオンし、**Hyper-Vマネージャー**でVMを見つけます。
     b. VMを右クリックし、**設定**に移動します。
     c. **セキュリティ**で、**トラステッドプラットフォームモジュールを有効にする**チェックボックスをオンにします。
2. **PowerShell**ウィンドウを開きます。
3. Citrix固有のPowerShellモジュールをロードするには、`asnp citrix*` を実行します。
4. ブローカーカタログを作成します。このカタログには、これから作成されるマシンが格納されます。
5. IDプールを作成します。これは、作成されるマシン用に作成されたADアカウントのコンテナになります。
6. マシンプロファイルを使用してプロビジョニングスキームを作成します。例：

```
New-ProvScheme -HostingUnitName "<hostingunit name>"

-IdentityPoolName "ID1" -MasterImageVM "XDHyp:\HostingUnits\HU1\<path
to the checkpoint/snapshot>"

-ProvisioningSchemeName "<catalogname>"  -MachineProfile "XDHyp:\<path
to the machine profile VM>"
```

7. プロビジョニングスキームの一意のIDでブローカーカタログを更新します。

8. VMを作成してカタログに追加します。

既存のカタログを更新する

既存のカタログは、Set-ProvSchemeコマンドを使用して更新できます。例：

```
Set-ProvScheme -ProvisioningSchemeName "<catalogname>" -MachineProfile
"XDHyp:\<path to the machine profile VM>"
```

VMを削除する

カタログからVMを削除し、SCVMMからVMを削除しないことを選択できます。この場合、`CitrixProvisioningSchemeId`タグはVMからのみ削除されます。カスタムタグはVMから削除されません。Web StudioまたはPowerShellコマンドを使用してVMを削除できます。

WEB STUDIO を使用して VM を削除する

1. VMを選択して右クリックします。
2. **「削除」**をクリックします。
3. **「仮想マシンをカタログから削除するが、仮想マシンは削除しない」**を選択します。

POWERSHELLコマンドの使用

`ForgetVM`パラメーターを指定した`Remove-ProvVM`。詳しくは、以下を参照してください。

- タグを削除する
- ハイパーバイザーアクセスなしでマシンを削除する

次のステップ

- これが最初に作成されたカタログである場合、Web Studioはデリバリーグループを作成するようにガイドします。
- 構成プロセス全体を確認するには、「インストールと構成」を参照してください。
- カタログを管理するには、「マシンカタログを管理する」および「Microsoft System Center Virtual Machine Managerカタログを管理する」を参照してください。

詳細情報

- 接続とリソースの作成および管理
- マイクロソフト システムセンター バーチャルマシンマネージャー への接続
- マシンカタログの作成

Nutanixカタログを作成する

マシンカタログを作成するウィザードについては、マシンカタログの作成で説明しています。以下の情報は、Nutanix仮想化環境に固有の詳細を扱っています。

> **注:**
>
> Nutanixカタログを作成する前に、Nutanixへの接続の作成を完了する必要があります。Nutanixへの接続を参照してください。

Nutanixスナップショットを使用してマシンカタログを作成する

選択したスナップショットは、カタログ内のVMを作成するために使用されるテンプレートです。カタログを作成する前に、Nutanixでイメージとスナップショットを作成してください。詳細については、Nutanixのドキュメントを参照してください。

カタログ作成ウィザードで：

- **オペレーティングシステム**および**マシン管理**ページには、Nutanix固有の情報は含まれていません。
- **コンテナ**または**クラスターとコンテナ**ページはNutanix固有です。

  Nutanix AHV XIをリソースとして使用してマシンを展開する場合、**コンテナ**ページが表示されます。VMのIDディスクが配置されるコンテナを選択します。

  Nutanix AHV Prism Central (PC)をリソースとして使用してマシンを展開する場合、**クラスターとコンテナ**ページが表示されます。VMの展開に使用するクラスターを選択し、次にコンテナを選択します。
- **イメージ**ページで、イメージスナップショットを選択します。Citrix Virtual Apps and Desktopsで使用するには、Acropolisスナップショット名に「XD_」というプレフィックスを付ける必要があります。必要に応じて、Acropolisコンソールを使用してスナップショットの名前を変更してください。スナップショットの名前を変更した場合は、カタログ作成ウィザードを再起動して、更新されたリストを表示してください。
- **仮想マシン**ページで、仮想CPUの数とvCPUあたりのコア数を指定します。
- **ネットワークカード**ページで、関連するネットワークをフィルタリングするNICタイプを選択します。NICタイプには**VLAN**と**OVERLAY**の2種類があります。マスターイメージに含まれるNICを1つ以上選択し、次に各NICに関連付けられた仮想ネットワークを選択します。

- **マシンID**、**ドメイン資格情報**、**スコープ**、および**概要**ページには、Nutanix固有の情報は含まれていません。

制限事項

Nutanixホスト接続（具体的にはNutanix AHVプラグイン2.7.1）を使用してMCSカタログを作成すると、プロビジョニングされたVMのハードディスクサイズがWeb Studioで誤って表示されます。表示されるサイズは、実際のストレージサイズ（50 GB）よりもはるかに小さい（1 GB）です。ハードディスクサイズはNutanixコンソールに正しく表示されます。

次のステップ

- これが最初に作成されたカタログである場合、Web Studioはデリバリーグループの作成に誘導します
- 構成プロセス全体を確認するには、インストールと構成を参照してください
- カタログを管理するには、マシンカタログの管理を参照してください

詳細情報

- 接続とリソースの作成および管理
- Nutanixへの接続
- Nutanixクラウドおよびパートナーソリューションへの接続
- マシンカタログの作成

Red Hat OpenShiftカタログを作成する

マシンカタログの作成では、マシンカタログを作成するウィザードについて説明します。以下の情報は、Red Hat OpenShift仮想化環境に固有の詳細を扱います。

> **注:**
>
> Red Hat OpenShiftカタログを作成する前に、Red Hat OpenShiftへの接続とホスティングユニットの作成を完了してください。「(/ja-jp/citrix-virtual-apps-desktops/2503/install-configure/connections/connection-redhat-openshift.html)」を参照してください。

マスターイメージVMを作成する

マシンカタログを作成するには、マスターイメージVMが必要です。

1. ログインIDを使用してOpenShiftコンソールにアクセスします。

2. **Virtualization > VirtualMachines**に移動して、マスターイメージVMを含むVMのリストを表示します。
3. マスターイメージを作成します。マスターイメージを作成する際は、マスターイメージVMにストレージデバイスが1つだけであることを確認してください。

注:

- マスターイメージVMの作成時に自動的にアタッチされる、Masqueradeタイプとポッドネットワーキングを持つデフォルトのネットワークアタッチメント定義（NAD）を削除します。さらに、クラスター環境に対する顧客の要件に従って、ルーティング可能なNADがマスターイメージVMに追加されていることを確認してください。
- マスターイメージがドメインに参加している場合、カタログ作成に使用された後にドメイン信頼が失われる可能性があります。この問題は、OpenShift環境の制限により、Citrix Virtual Apps and Desktops™ 2503に影響します。回避策は、マスターイメージでドメインに参加しないことです。CitrixはRed Hatと協力して、ネットワーク分離機能の強化に取り組んでいます。
- Red Hat OpenShift仮想化環境でMCSマシンカタログを作成する場合、異なるオペレーティングシステムタイプを持つマスターイメージとマシンプロファイルを使用することはできません。これは、Red Hat OpenShiftが各OSタイプを管理する方法によるものです。したがって、Windows VMをマスターイメージとして使用し、非Windows（例：Linux）VMをマシンプロファイルとして使用すること、またはその逆はサポートされていません。
- 現在、`InstanceType`を使用して作成されたVMは、マスターイメージとしてサポートされていません。

カタログを作成する

OpenShift環境でマシンを作成、配信、電源管理するためにOpenShiftカタログを作成できます。

- Web Studioを使用してカタログを作成する(#create-a-catalog-using-web-studio): 現在、Web Studioを使用して、マシンの配信と電源管理のみを目的としたOpenShiftカタログを作成できます。
- PowerShellコマンドを使用してカタログを作成する(#create-a-catalog-using-powershell-commands): PowerShellを使用して、マシンの作成、配信、および電源管理を目的としたOpenShiftカタログを作成します。

Web Studioを使用してカタログを作成する

現在、Studioを使用してOpenShiftカタログを作成し、OpenShift環境内の既存のマシンの配信と電源管理を行うことができます。

マシンカタログセットアップウィザードで：

1. **オペレーティングシステム**ページで、**マルチセッションOSまたはシングルセッションOS**を選択します。
2. **マシン管理**ページで、**電源管理されているマシンと別のサービスまたはテクノロジ**を選択します。
3. 「**仮想マシン**」ページで、マシンとそれらのActive Directoryマシンアカウントを追加します。次のことができます。
   - *マシンを手動で追加する*：「**マシンを追加**」をクリックして、マシンを手動で追加します。「**VMの選択**」ウィンドウが表示されます。以前に作成したOpenShift接続を展開し、追加するノード（VM）を選択します。次に、関連するマシンアカウント名を追加します。
   - *CSVファイルを使用してマシンを追加する*：「**CSVファイルを追加**」をクリックして、マシンを一括で追加します。CSVファイルを使用してマシンを追加する方法については、「CSVファイルを使用してマシンをカタログに一括追加する」を参照してください。
4. 画面の指示に従って、OpenShift固有の情報を含まない残りの手順を完了します。

PowerShellコマンドを使用してカタログを作成する

現在、Red Hat OpenShift環境でMCSマシンカタログを作成するには、PowerShellコマンドのみを使用できます。マシンプロファイルを使用しても使用しなくても、マシンカタログを作成できます。VMはマシンプロファイルの入力として使用されます。

1. PowerShellウィンドウを開きます。
2. `asnp citrix*` を実行します。
3. PowerShellコマンドを実行して
   a. IDプールを作成します
   b. ADアカウントを作成します
   c. マシンプロファイルの有無にかかわらず、永続VMを持つMCSマシンカタログを作成します。
   d. カタログにVMを追加します
   e. ブローカーカタログを作成します

f. 新しいVMにブローカーマシンを追加します

以下はスクリプトの例です:

IDプールを作成します

```
New-AcctIdentityPool `

    -IdentityPoolName "IdentityPoolName" `

    -ZoneUid "00000000-0000-0000-0000-000000000000" `

    -NamingScheme "vm###" `

    -NamingSchemeType "Numeric" `

    -AllowUnicode `

    -Domain "MyDomain.local" `

    -AdminAddress "MyDDC.MyDomain.Local"
```

ADアカウントを作成します

```
New-AcctADAccount `

    -IdentityPoolUid "11111111-1111-1111-1111-111111111111" `

    -ADUserName "MyDomain\MyUserName" `

    -ADPassword SecurePassword `

    -Count 1 `

    -AdminAddress "MyDDC.MyDomain.Local"
```

永続マシンを持つプロビジョニングスキームを作成します (マシンプロファイルなし)

```
New-ProvScheme `

    -ProvisioningSchemeName "ProvisioningSchemeName" `

    -HostingUnitName "HostingUnitName" `
```

```
    -IdentityPoolName "IdentityPoolName" `

    -ProvisioningSchemeType "MCS" `

    -MasterImageVM "XDHyp:
\HostingUnits\HostingUnitName\TargetNamespace.namespace\MasterImageVM.vm"
`

    -NetworkMapping @{"0" = "XDHyp:
\HostingUnits\HostingUnitName\TargetNamespace.namespace\MyNetwork.network"
 } `

    -VMCpuCount 1 `

    -VMMemoryMB 4096 `

    -InitialBatchSizeHint 1 `

    -AdminAddress "MyDDC.MyDomain.Local"
```

永続マシンを持つプロビジョニングスキームを作成します (マシンプロファイルあり)

```
New-ProvScheme `

    -ProvisioningSchemeName "ProvisioningSchemeName" `

    -HostingUnitName "HostingUnitName" `

    -IdentityPoolName "IdentityPoolName" `

    -ProvisioningSchemeType "MCS" `

    -MasterImageVM "XDHyp:
\HostingUnits\HostingUnitName\TargetNamespace.namespace\MasterImageVM.vm"
`

    -NetworkMapping @{"0" = "XDHyp:
\HostingUnits\HostingUnitName\TargetNamespace.namespace\MyNetwork.network"
 } `

    -VMCpuCount 1 `
```

```
    -VMMemoryMB 4096 `

    -InitialBatchSizeHint 1 `

    -AdminAddress "MyDDC.MyDomain.Local" `

    -MachineProfile "XDHyp:
\HostingUnits\HostingUnitName\TargetNamespace.namespace\MachineProfileVM.v
m"
```

新しいPROVVMを作成します

```
New-ProvVM `

    ProvisioningSchemeName "ProvisioningSchemeName" `

    ADAccountName "MyDomain\vm001" `

    AdminAddress "MyDDC.MyDomain.Local"



Lock-ProvVM `

    -ProvisioningSchemeName "ProvisioningSchemeName" `

    -Tag "Brokered" `

    -VMID "TargetNamespace:vm001"
```

新しいブローカーカタログを作成します

```
New-BrokerCatalog `

    -Name "ProvisioningSchemeName" `

    -ProvisioningType "MCS" `

    -SessionSupport "MultiSession" `

    -AllocationType "Random" `
```

```
    -PersistUserChanges "OnLocal" `

    -ZoneUid "00000000-0000-0000-0000-000000000000" `

    -AdminAddress "MyDDC.MyDomain.Local"
```

ブローカーカタログのメタデータを設定する

```
Set-BrokerCatalogMetadata `

    -CatalogId "1" `

    -Name "Citrix_DesktopStudio_IdentityPoolUid" `

    -Value "11111111-1111-1111-1111-111111111111"



Set-BrokerCatalog `

    -Name "ProvisioningSchemeName " `

    -ProvisioningSchemeId "22222222-2222-2222-2222-222222222222"
```

新しいPROVVM用のブローカーマシンを作成する

```
New-BrokerMachine `

    -CatalogUid "33333333-3333-3333-3333-333333333333" `

    -AdminAddress "MyDDC.MyDomain.Local" `

    -MachineName "S-0-0-00-0000000000-0000000000-000000000-000000"
```

次のステップ

- これが最初に作成されたカタログである場合、Web Studioは(/ja-jp/citrix-virtual-apps-desktops/2503/install-configure/delivery-groups-create.html)に誘導します
- 構成プロセス全体を確認するには、(/ja-jp/citrix-virtual-apps-desktops/2503/install-configure.html)を参照してください

- 電源管理については、(/ja-jp/citrix-virtual-apps-desktops/2503/install-configure/power-management/power-manage-openshift-vms.html)を参照してください

詳細情報

- 接続とリソースを作成および管理する
- Red Hat OpenShiftへの接続
- マシンカタログを作成する

VMwareカタログを作成する

「(/ja-jp/citrix-virtual-apps-desktops/2503/install-configure/machine-catalogs-create.html)」では、マシンカタログを作成するウィザードについて説明します。以下の情報は、VMware仮想化環境に固有の詳細を扱います。

> **注:**
>
> VMwareカタログを作成する前に、VMwareへの接続の作成を完了する必要があります。「(/ja-jp/citrix-virtual-apps-desktops/2503/install-configure/connections/connection-vmware-virtualization-environments.html)」を参照してください。

マスターVMを作成する

マスターVMを使用して、マシンカタログでユーザーデスクトップとアプリケーションを提供します。ハイパーバイザーで、次の操作を行います。

1. マスターVMにVDAをインストールし、デスクトップを最適化するオプションを選択して、パフォーマンスを向上させます。
2. バックアップとして使用するために、マスターVMのスナップショットを取得します。

> **注:**
>
> MCSを使用して、vSAN 8.0環境でVMをプロビジョニングできます。

マシンプロファイルを使用してマシンカタログを作成する

マシンプロファイルを使用してMCSマシンカタログを作成できます。マシンプロファイルの入力元はVMwareテンプレートです。マシンプロファイルは、VMwareテンプレートからハードウェアプロパティを取得し、カタログ内の新しくプロビジョニングされたVMに適用します。

注:

- マスターイメージ入力（スナップショット）とマシンプロファイル入力（VMwareテンプレート）は、両方ともvTPMが有効であるか、両方ともvTPMが無効である必要があります。このルールは、`New-ProvScheme`と`Set-ProvScheme`の両方に適用されます。
- マスターイメージでvTPMが有効になっている場合、VMwareテンプレートはマスターイメージと同じVMソースからのみ取得できます。
- 暗号化ストレージポリシーはフルクローンのみサポートします。
- マシンプロファイルベースのカタログは、提供されたVMwareテンプレートを利用してストレージコントローラー情報を収集し、接続された仮想ディスクに依存します。テンプレートには、仮想マシンの仮想ディスクを構成するために使用されるストレージコントローラー情報を取得するために必要な仮想ディスクが含まれている必要があります。

マシンプロファイル内のVMwareテンプレートは、カタログへのVMのプロビジョニングを可能にするために、カタログのライフサイクル中に存在している必要があります。VMwareテンプレートがないと、新しいVMをプロビジョニングできません。VMwareテンプレートが削除された場合は、`Set-ProvScheme`コマンドを使用して新しいテンプレートを提供する必要があります。

- MCSはVMwareテンプレートのプロパティをキャプチャします。Get-Provschemeコマンドを使用して、VMwareテンプレートの保存されたプロパティを参照する新しいVMwareテンプレートを作成できます。
- あるいは、マシンカタログとプロビジョニングされたVMが存在する場合、MCSでプロビジョニングされたマシンを使用して新しいVMwareテンプレートを作成することもできます。
- MCSIOが有効な場合、MCSカタログ作成後にメモリとディスクキャッシュのサイズを更新できます。

異なるOSに基づいて、異なる構成でマシンカタログを作成できます。

- マスターイメージにWindows 11がインストールされている場合、マスターイメージでvTPMを有効にすることが要件となります。したがって、マシンプロファイルのソースであるVMwareテンプレートには、vTPMがアタッチされている必要があります。
- vTPMがアタッチされていないマスターイメージにWindows 10がインストールされている場合、マシンプロファイルのソースとしてvTPMなしのVMwareテンプレートを使用してマシンカタログを作成できます。

別の構成として、暗号化ストレージポリシーが適用されたマシンプロファイルテンプレートでフルコピーディスクモードを使用してマシンカタログを作成できます。

マシンプロファイルを入力としてPowerShellコマンドを使用してマシンカタログを作成するには:

1. **PowerShell**ウィンドウを開きます。
2. `asnp citrix*`を実行します。
3. 次のコマンドを実行します。
    - vTPMがアタッチされたVMwareテンプレートをマシンプロファイル入力のソースとして、Windows 11がインストールされたマスターイメージでマシンカタログを作成するには：

```
$identityPool = New-AcctIdentityPool  -IdentityPoolName "<string>"

-NamingScheme "<string>-###"

-NamingSchemeType Numeric

-Domain "<domain name"

-ZoneUid "<Uid>"  -Scope @()
```

```
$provScheme =New-ProvScheme  -CleanOnBoot

-HostingUnitName "vSanRg"

-IdentityPoolName "<string>"

-InitialBatchSizeHint 1

-MasterImageVM "XDHyp:\HostingUnits\<hosting unit name>\<snapshot
name>.snapshot"

-NetworkMapping @{"0"="XDHyp:\HostingUnits\<hosting unit name>\
```

```
\<network name>.network"}

-ProvisioningSchemeName "<string>"

-Scope @() -VMCpuCount 4

-VMMemoryMB 6144

-MachineProfile "XDHyp:\HostingUnits\<hosting unit name>\<template
name>.template" -TenancyType Shared

-FunctionalLevel "L7_20"
```

```
$catalog = New-BrokerCatalog

-AllocationType "Static"

-PersistUserChanges  "OnLocal"

-Description "<string>"

-IsRemotePC $False

-MinimumFunctionalLevel 'L7_9'

-Name "<catalog name>"

-ProvisioningType 'MCS'

-Scope @()

-SessionSupport "SingleSession" -ZoneUid "<Uid>"
```

```
Set-BrokerCatalog -Name "<string>"

-ProvisioningSchemeId $provScheme.ProvisioningSchemeUid.Guid
```

- 非vTPM VMwareテンプレートをマシンプロファイルのソースとして、Windows 10がインストールされたマスターイメージでマシンカタログを作成するには：

```
$identityPool = New-AcctIdentityPool

-IdentityPoolName "<string>"

-NamingScheme "<string>-###" -NamingSchemeType Numeric

-Domain "<domain name>"

-ZoneUid "<Uid>"  -Scope @()
```

```
$provScheme =New-ProvScheme

-CleanOnBoot -HostingUnitName "<string>"

-IdentityPoolName "<string>"

-InitialBatchSizeHint 1

-MasterImageVM "XDHyp:\HostingUnits\<hosting unit name>\<snapshot
name>.snapshot

-NetworkMapping @{"0"="XDHyp:\HostingUnits\<hosting unit name>\
\<string>.network"}

-ProvisioningSchemeName "<string>"  -Scope @() -VMCpuCount 4  -
VMMemoryMB 8192

-MachineProfile "XDHyp:\HostingUnits\<hosting unit name>\<template
name>.template"

-TenancyType Shared  -FunctionalLevel "L7_20"
```

```
$catalog = New-BrokerCatalog

-AllocationType "Static"

-PersistUserChanges  "OnLocal"

-Description "<string>"

-IsRemotePC $False
```

```
-MinimumFunctionalLevel 'L7_9' -Name "<string>" -ProvisioningType
'MCS' -Scope @()

-SessionSupport "SingleSession" -ZoneUid "<Uid"
```

```
Set-BrokerCatalog -Name "<string>"

-ProvisioningSchemeId $provScheme.ProvisioningSchemeUid.Guid
```

- 暗号化されたストレージポリシーが適用されたマシンプロファイルテンプレートを使用して、フルコピーディスクモードでマシンカタログを作成するには：

```
$identityPool = New-AcctIdentityPool

-IdentityPoolName "<string>"

-NamingScheme "<string>-###"

-NamingSchemeType Numeric

-Domain "<domain name>"

-ZoneUid "<Uid>"  -Scope @()
```

```
$provScheme =New-ProvScheme

-HostingUnitName "<string>"

-IdentityPoolName "<string>"

-InitialBatchSizeHint 1

-MasterImageVM "XDHyp:\HostingUnits\<hosting unit name>\<snapshot
name>.snapshot"

-NetworkMapping @{"0"="XDHyp:\HostingUnits\<hosting unit name>\
\<string>.network"}

-ProvisioningSchemeName "<string>"
```

```
-Scope @() -VMCpuCount 4  -VMMemoryMB 8192 -MachineProfile "XDHyp:
\HostingUnits\<hosting unit name>\<template name>.template"

-TenancyType Shared

-FunctionalLevel "L7_20" -UseFullDiskCloneProvisioning
```

```
$catalog = New-BrokerCatalog

-AllocationType "Static"

-PersistUserChanges  "OnLocal"

-Description "<string>"  -IsRemotePC $False

-MinimumFunctionalLevel 'L7_9'

-Name "<string>" -ProvisioningType 'MCS' -Scope @()

-SessionSupport "SingleSession" -ZoneUid "<Uid>"
```

```
Set-BrokerCatalog -Name "<string>"

-ProvisioningSchemeId $provScheme.ProvisioningSchemeUid.Guid
```

マシンプロファイルを更新するには、Set-ProvSchemeコマンドを使用します。例：

```
Set-ProvScheme -ProvisioningSchemeName 'name' -IdentityPoolName 'name'
-MachineProfile 'XDHyp:\HostingUnits\<hosting unit name>\<template
name>.template'
```

複数のNICの確認

マシンプロファイルを使用し、`New-ProvScheme`および`Set-ProvScheme`コマンドで`NetworkMapping`パラメーターを使用する場合、複数のNICの事前チェック中にさまざまなエラーメッセージが表示されます。

複数のNICの事前チェックリストは次のとおりです。

- マシンプロファイルテンプレートからのNIC数のみが使用され、検証されます。これらのNICが指すネットワークは、ホスティングユニットネットワークに対して使用または検証されません。
- マシンプロファイルテンプレートのNIC数がホスティングユニットのネットワーク数よりも多い場合、エラーメッセージが表示されます。
- マシンプロファイルテンプレートのNIC数がゼロの場合、エラーメッセージが表示されます。マシンプロファイルテンプレートのNIC数が1の場合：
  - `New-ProvScheme`または`Set-ProvScheme`コマンドでネットワークマッピングが指定されておらず、ホスティングユニットネットワークが1つの場合、そのホスティングユニットネットワークが使用されます。
  - ネットワークマッピングが指定されている場合、それが有効であれば、指定されたネットワークマッピングが使用されます。
- マシンプロファイルテンプレートのNIC数が1より大きい場合、またはホスティングユニットネットワーク数が1より大きい場合：
  - コマンドには有効なネットワークマッピングが必要であり、各NICのマッピングを提供する必要があります（つまり、NetworkMappingの数はマシンプロファイルのNIC数と同じである必要があります）。
  - 複数のNICをホスティングユニット内の同じネットワークにマッピングすることはできません。
  - `NetworkMapping`の数とマシンプロファイルのNIC数は、ホスティングユニットのネットワーク数以下である必要があります。
  - マシンプロファイルテンプレート内のネットワークアダプターの数をnとした場合、0からn-1までの各IDに`NetworkMapping`を指定する必要があります。

トラブルシューティング

カタログの作成に失敗した場合は、CTX294978を参照してください。

次のステップ

- これが最初に作成されたカタログである場合、Web Studioはデリバリーグループの作成を案内します。
- 構成プロセス全体を確認するには、インストールと構成を参照してください。
- カタログを管理するには、マシンカタログの管理とVMwareカタログの管理を参照してください。

詳細情報

- 接続とリソースの作成および管理
- VMwareへの接続
- マシンカタログの作成

異なるマシンID参加タイプのIDプール

オンプレミスActive Directoryに参加しているマシンIDのIDプール

この記事では、オンプレミスActive Directoryに参加しているマシンIDのIDプールを作成する方法について説明します。

Web Studioを使用する

以下の情報は、マシンカタログの作成に関するガイダンスを補足するものです。

1. **マシンID**ページで:
   a. IDタイプとして**オンプレミスActive Directory**を選択します。
   b. Active Directoryアカウントオプションを選択します:
      - **新しいActive Directoryアカウントを作成**:
        - **新しいActive Directoryアカウントを作成**を選択し、既存のIDプールを使用して新しいアカウントを作成する場合は、それらのアカウントのドメインを選択し、アカウント命名スキームを指定します。
        - **新しいActive Directoryアカウントを作成**を選択し、既存のIDプールを使用して新しいアカウントを作成する場合は、リストからIDプールを選択します。
      - **既存のActive Directoryアカウントを使用**: CSVファイルから参照またはインポートでき、パスワードをリセットするか、すべてのアカウントに同じパスワードを指定できます。
   c. **次へ**をクリックします。
2. **ドメイン資格情報**ページで、サービスアカウントを選択するか、資格情報を手動で入力します。サービスアカウントの詳細については、オンプレミスActive Directoryサービスアカウントを参照してください。

サービスアカウントの関連付けを変更する

関連付けられているサービスアカウントを変更するか、既存のMCSマシンカタログに新しい関連付けを追加するには、**マシンカタログの編集**ページを使用します。

- サービスアカウントを追加するには、「**サービスアカウント**」ページで「**サービスアカウントの選択**」をクリックします。
- サービスアカウントの関連付けを変更するには、「**サービスアカウント**」ページで編集アイコンをクリックします。

PowerShell を使用する

オンプレミスサービスアカウントをIDプールに関連付けることで、オンプレミスサービスアカウントをMCSで作成されたマシンカタログに関連付けることができます。IDプールを作成するか、既存のIDプールを更新して、サービスアカウントに関連付けることができます。

例：新しいIDプールを作成し、サービスアカウントに関連付けるには、以下を実行します。

```
New-AcctIdentityPool -IdentityType ActiveDirectory -IdentityPoolName
MyPool -NamingScheme Acc#### -Domain MyDomain.com -NamingSchemeType
Numeric -OU "CN=MyOU,DC=MyDomain,DC=com" -ServiceAccountUid
$serviceAccountUid
```

例：既存のIDプールを更新してサービスアカウントに関連付けるには、以下を実行します。

```
$identityPoolUid = (Get-ProvScheme -ProvisioningSchemeName
"MyProvScheme").IdentityPoolUid

Set-AcctIdentityPool -IdentityPoolUid $identityPoolUid -ServiceAccountUid
$serviceAccountUid
```

注：

`$serviceAccountUid`は、オンプレミスのActive Directoryサービスアカウントの有効なUIDである必要があります。

ハイブリッド Azure Active Directory 参加済みマシンIDのIDプール

注:

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

> この記事では、以下のIDプールを作成する方法について説明します。

- ハイブリッド Azure Active Directory (AD) 参加済みカタログ
- Microsoft Intuneに登録されているハイブリッド Azure AD 参加済みカタログ

要件、制限、考慮事項については、ハイブリッド Azure Active Directory 参加済みを参照してください。

ハイブリッド Azure Active Directory (AD) 参加済みカタログを作成する

Web Studioを使用する

以下の情報は、マシンカタログの作成のガイダンスを補足するものです。

カタログ作成ウィザードの**マシンID**ページで：

- **ハイブリッド Azure Active Directory 参加済み**を選択します。作成されたマシンは組織によって所有され、その組織に属するActive Directoryアカウントでサインインされます。
- デバイス管理のために作成されたマシンをMicrosoft Intune（Configuration Managerを含む）に登録するには、**Configuration Managerを使用してマシンをMicrosoft Intuneに登録する**を選択します。カタログ作成中のエラーを回避するには、マスターイメージが以下の要件を満たしていることを確認してください。
  - VDAバージョン2405以降がインストールされていること。
  - サイトコードが割り当てられていない**Configuration Managerクライアント**がインストールされていること。詳細については、このMicrosoftの記事を参照してください。

> **注:**
>
> 識別タイプとして**Hybrid Azure Active Directory joined**を選択した場合、カタログ内の各マシンには対応するADコンピューターアカウントが必要です。

PowerShellの使用

以下は、Web Studioでの操作に相当するPowerShellの手順です。Remote PowerShell SDKを使用してカタログを作成する方法については、`<https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/>`を参照してください。

オンプレミスAD参加済みカタログとハイブリッドAzure AD参加済みカタログの違いは、IDプールとマシンアカウントの作成にあります。

ハイブリッドAzure AD参加済みカタログ用のアカウントとともにIDプールを作成するには:

```
New-AcctIdentityPool -AllowUnicode -IdentityType "HybridAzureAD" -Domain
"corp.local" -IdentityPoolName "HybridAADJoinedCatalog" -NamingScheme
"HybridAAD-VM-##" -NamingSchemeType "Numeric" -OU
"CN=AADComputers,DC=corp,DC=local" -Scope @() -ZoneUid "81291221-
d2f2-49d2-ab12-bae5bbd0df05"

New-AcctIdentity -IdentityPoolName "HybridAADJoinedCatalog" -Count 10
-ADUserName "corp\admin1" -ADPassword $password

Set-AcctAdAccountUserCert -IdentityPoolName "HybridAADJoinedCatalog" -All
-ADUserName "corp\admin1" -ADPassword $password
```

注:

`$password`は、書き込み権限を持つADユーザーアカウントの一致するパスワードです。

ハイブリッドAzure AD参加済みカタログの作成に使用されるその他のすべてのコマンドは、従来のオンプレミスAD参加済みカタログの場合と同じです。

ハイブリッドAzure AD参加プロセスの状態を表示する

Web Studioでは、デリバリーグループ内のハイブリッドAzure AD参加済みマシンが電源オン状態の場合に、ハイブリッドAzure AD参加プロセスのステータスが表示されます。ステータスを表示するには、検索を使用してそれらのマシンを特定し、下部ペインの**詳細**タブで各マシンの**マシンID**を確認します。**マシンID**には次の情報が表示されます。

- ハイブリッドAzure AD参加済み
- Azure ADにまだ参加していません

注:

- マシンが最初に電源オンになったときに、ハイブリッドAzure AD参加が遅延する場合があります。これは、デフォルトのマシンID同期間隔（Azure AD Connectの30分）が原因です。マシンは、マシンIDがAzure AD Connectを介してAzure ADに同期された後にのみ、ハイブリッドAzure AD参加済み状態になります。
- マシンがハイブリッドAzure AD参加状態にならない場合、Delivery Controllerに登録されません。登録ステータスは**初期化中**と表示されます。

また、Web Studio を使用して、マシンが利用できない理由を確認できます。これを行うには、**検索** ノードでマシンをクリックし、下部ペインの **詳細** タブで **登録** を確認し、ツールチップを読んで追加情報を確認します。

トラブルシューティング

マシンがハイブリッド Azure AD 参加済みにならなかった場合は、次の操作を行います。

- Microsoft Azure ADポータルを通じて、マシンアカウントがAzure ADに同期されているか確認します。同期されている場合、**Azure ADにまだ参加していません**と表示され、登録が保留中であることを示します。

  マシンアカウントをAzure ADに同期するには、以下を確認してください。

  - マシンアカウントが、Azure ADと同期するように構成されているOU内にあること。**userCertificate**属性を持たないマシンアカウントは、同期するように構成されているOU内にあってもAzure ADに同期されません。
  - マシンアカウントに**userCertificate**属性が入力されていること。属性を表示するには、Active Directory Explorerを使用します。
  - マシンアカウントが作成された後、Azure AD Connectが少なくとも1回同期されている必要があります。同期されていない場合は、Azure AD ConnectマシンのPowerShellコンソールで`Start-ADSyncSyncCycle -PolicyType Delta`コマンドを手動で実行して、即時同期をトリガーします。

- ハイブリッドAzure AD参加用のCitrix管理デバイスキーペアがマシンに正しくプッシュされているか、**HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix** の下の **DeviceKeyPairRestored** の値をクエリして確認します。

  値が1であることを確認します。そうでない場合、考えられる理由は次のとおりです。

  - プロビジョニングスキームに関連付けられたIDプールの`IdentityType`が`HybridAzureAD`に設定されていません。これは`Get-AcctIdentityPool`を実行して確認できます。
  - マシンがマシンカタログと同じプロビジョニングスキームを使用してプロビジョニングされていない。
  - マシンがローカルドメインに参加していない。ローカルドメインへの参加は、ハイブリッドAzure AD参加の前提条件です。

- MCSでプロビジョニングされたマシンで`dsregcmd /status /debug`コマンドを実行して、診断メッセージを確認します。
  - ハイブリッドAzure AD参加が成功した場合、コマンドラインの出力で **AzureAdJoined** と **DomainJoined** が **YES** になります。
  - そうでない場合は、問題のトラブルシューティングのためにMicrosoftのドキュメントを参照してください: `<https://docs.microsoft.com/ja-jp/azure/active-directory/devices/troubleshoot-hybrid-join-windows-current>`。
  - エラーメッセージ「**Server Message: The user certificate is not found on the device with id: xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx**」が表示された場合は、ユーザー証明書を修復するために次のPowerShellコマンドを実行します。

    ```
    Repair-AcctIdentity -IdentityAccountName TEST\VM1 -Target
    UserCertificate
    ```

    ユーザー証明書の問題に関する詳細については、CTX566696を参照してください。

Microsoft Intuneに登録されたハイブリッドAzure AD参加カタログを作成する

Microsoft Intuneに登録されたハイブリッドAzure AD参加カタログに対して、永続的なシングルセッションおよびマルチセッションVM用の共同管理対応カタログを作成できます。共同管理対応カタログは、StudioとPowerShellの両方を使用して作成できます。

Web Studioを使用する

以下の情報は、マシンカタログの作成のガイダンスを補足するものです。

マシンカタログのセットアップウィザードで、:

- **マシンID**ページで、**ハイブリッドAzure Active Directory参加済み**を選択し、次に**Configuration Managerを使用してMicrosoft Intuneにマシンを登録**を選択します。このアク

ションを使用すると、Configuration ManagerとMicrosoft Intune（つまり、共同管理）がVMを管理します。

PowerShell を使用する

以下は、Studio の手順に相当する PowerShell の手順です。

Remote PowerShell SDKを使用してConfiguration ManagerでMicrosoft Intuneにマシンを登録するには、`New-AcctIdentityPool`で`DeviceManagementType`パラメーターを使用します。この機能には、カタログがハイブリッドAzure AD参加済みであり、Azure ADが適切なMicrosoft Intuneライセンスを所有している必要があります。

ハイブリッドAzure AD参加カタログと共同管理対応カタログの違いは、IDプールの作成にあります。例:

```
New-AcctIdentityPool -AllowUnicode -DeviceManagementType "IntuneWithSCCM"
IdentityType="HybridAzureAD" -IdentityPoolName "CoManagedCatalog"
-NamingScheme "CoManaged-VM-##" -NamingSchemeType "Numeric" -Scope @()
-ZoneUid "81291221-d2f2-49d2-ab12-bae5bbd0df05"
```

トラブルシューティング

マシンがMicrosoft Intuneへの登録に失敗したり、共同管理状態に到達しなかったりした場合は、以下を実行してください。

- Intuneライセンスを確認する

  Azure ADテナントに適切なIntuneライセンスが割り当てられているか確認します。Microsoft Intuneのライセンス要件については、Microsoft Intune licensingを参照してください。

- ハイブリッドAzure AD参加ステータスを確認する

  MCSでプロビジョニングされたマシンがハイブリッドAzure ADに参加しているか確認します。ハイブリッドAzure ADに参加していない場合、マシンは共同管理の対象になりません。ハイブリッドAzure AD参加の問題をトラブルシューティングするには、Troubleshootを参照してください。

- 共同管理の適格性を確認する

  - MCSでプロビジョニングされたマシンに、期待されるConfiguration Managerサイトが正しく割り当てられているか確認します。割り当てられたサイトを取得するには、影響を受けるマシンで次のPowerShellコマンドを実行します。

```
(New-Object -ComObject "Microsoft.SMS.Client").GetAssignedSite()
```

- VMにサイトが割り当てられていない場合は、次のコマンドを使用して、Configuration Managerサイトが自動的に検出できるか確認します。

```
(New-Object -ComObject "Microsoft.SMS.Client").AutoDiscoverSite()
```

- サイトコードが検出できない場合は、Configuration Manager環境で境界と境界グループが適切に構成されていることを確認してください。詳細については、Considerationsを参照してください。
- Configuration Managerクライアントサイトの割り当てに関する問題がないか、`C:\Windows\CCM\Logs\ClientLocation.log`を確認してください。
- マシンの共同管理状態を確認します。影響を受けるマシンで**Configuration Managerコントロールパネル**を開き、**全般**タブに移動します。共同管理プロパティの値は**有効**である必要があります。そうでない場合は、`C:\Windows\CCM\Logs\CoManagementHandler.log`の下のログを確認してください。

- Intune 登録を確認する

  すべての前提条件が満たされていても、マシンが Microsoft Intune への登録に失敗する場合があります。Intune 登録の問題については、**Application and Services Logs > Microsoft > Windows > DeviceManagement-Enterprise-Diagnostics-Provider** の下の Windows イベントログを確認してください。

非ドメイン参加型マシンIDのIDプール

この記事では、Citrix Virtual Apps and Desktopsを使用して、ドメインに参加していないカタログのIDプールを作成する方法について説明します。

要件、制限、考慮事項については、「ドメインに参加していない」を参照してください。

マシンカタログを作成する前に、以下が必要です。

1. 新しいリソースの場所

   - Citrix Cloud™管理UI > 左上のハンバーガーメニュー > **リソースの場所**に移動します。
   - **+ リソースの場所**をクリックします。
   - 新しいリソースの場所の名前を入力し、**保存**をクリックします。

2. ホスティング接続を作成します。詳細については、「接続の作成と管理」セクションを参照してください。

Citrix Virtual Apps and Desktopsを使用すると、ワークグループまたはドメインに参加していないマシンに基づいてカタログを作成できます。ドメインに参加していないマシンを作成するかどうかは、アカウントIDプールがどのように作成されるかによって異なります。アカウントIDプールは、カタログプロビジョニング中にMCSがマシン名を作成および追跡するために使用するメカニズムです。

Web Studioを使用する

以下の情報は、「マシンカタログの作成」のガイダンスを補足するものです。

カタログ作成ウィザードで：

- **マシンID**ページで、**ドメインに参加していない**を選択します。作成されたマシンはどのドメインにも参加しません。

> **注:**
>
> 「**ドメイン非参加**」のIDタイプには、カタログの最小機能レベルとしてVDAバージョン2311以降が必要です。利用可能にするには、必要に応じて最小機能レベルを更新してください。

PowerShell を使用する

Remote PowerShell SDKを使用して、ドメイン非参加カタログ用のIDプールを作成できます。

PowerShellパラメーターの**WorkgroupMachine**と**IdentityType**を使用して、ドメイン非参加カタログ用のIDプールを作成します。これらのパラメーターにより、ドメイン管理者資格情報を含むすべてのAD固有のパラメーターを指定する必要がなくなります。

```
New-AcctIdentityPool -AllowUnicode -IdentityType "Workgroup"
-WorkgroupMachine -IdentityPoolName "NonDomainJoinedCatalog" -NamingScheme
"NDJ-VM-##" -NamingSchemeType "Numeric" -Scope @() -ZoneUid "81291221-
d2f2-49d2-ab12-bae5bbd0df05"
```

非ドメイン参加型カタログの作成に使用されるその他のすべてのコマンドは、従来のオンプレミスActive Directory参加型カタログの場合と同じです。

マシンカタログを管理する

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

はじめに

マシンカタログへのマシンの追加または削除、名前の変更、説明の変更、カタログのActive Directoryコンピューターアカウントの管理を行うことができます。

カタログの保守には、各マシンに最新のOSアップデートが適用されていることを確認することも含まれます。これには、ウイルス対策の更新、オペレーティングシステムのアップグレード、または構成の変更が含まれます。

- Machine Creation Services™ (MCS) を使用して作成されたプールされたランダムマシンを含むカタログは、カタログで使用されるマスターイメージを更新し、その後マシンを更新することでマシンを保守します。この方法により、多数のユーザーマシンを効率的に更新できます。
- 静的で永続的に割り当てられたマシンを含むカタログ、およびリモートPCアクセス マシンカタログの場合、ユーザーマシンの更新はWeb Studioの外部で管理します。このタスクは、個別に、またはサードパーティのソフトウェア配布ツールを使用して一括で実行します。

ホストハイパーバイザーへの接続の作成と管理については、「接続とリソース」を参照してください。

> **注:**
>
> MCSはWindows 10 IoT CoreおよびWindows 10 IoT Enterpriseをサポートしていません。詳細については、Microsoftサイトを参照してください。

永続インスタンスについて

永続インスタンスまたは専用インスタンスを使用して作成されたMCSカタログを更新する場合、カタログ用に作成された新しいマシンは更新されたイメージを使用します。既存のインスタンス

は元のインスタンスを引き続き使用します。イメージの更新プロセスは、他の種類のカタログと同じ方法で行われます。以下を考慮してください。

- 永続ディスクカタログの場合、既存のマシンは新しいイメージに更新されませんが、カタログに追加された新しいマシンは新しいイメージを使用します。
- 非永続ディスクカタログの場合、マシンイメージはマシンがリセットされる次回のタイミングで更新されます。
- 永続的なマシンカタログでは、イメージを更新すると、それを使用するカタログインスタンスも更新されます。
- 永続的ではないカタログの場合、異なるマシンに異なるイメージを使用したい場合は、イメージは別々のカタログに存在する必要があります。

マシンカタログを管理する

マシンカタログは次の2つの方法で管理できます。

- Web Studioの使用
- PowerShellを使用する

Web Studioを使用する

このセクションでは、Web Studioを使用してカタログを管理する方法について詳しく説明します。

- マシンカタログの管理
  - はじめに
  - 永続インスタンスについて
- マシンカタログの管理
- Web Studioの使用
- カタログの詳細を表示
  - カタログにマシンを追加
  - カタログからマシンを削除する
- カタログを編集する
- カタログの名前を変更する
- カタログを別のゾーンに移動する

- カタログを削除する
- レガシーMCSカタログをマシンプロファイルベースのカタログに変換する(#convert-legacy-mcs-catalogs-to-machine-profile-based-catalogs)
- カタログ内のActive Directoryコンピューターアカウントを管理する
- カタログを更新する
    - マスターイメージを更新または作成する
    - マスターイメージを変更する
    - マスターイメージをロールバックする
- 機能レベルを変更するか、変更を元に戻す
- カタログをクローンする
- フォルダーを使用してカタログを整理する
    - カタログフォルダーを作成する
    - カタログを移動する
    - カタログフォルダーを管理する
- カタログ作成を再試行する
- トークンを使用してMCS以外でプロビジョニングされたVDAを登録する
- PowerShellを使用する
- カタログに関連付けられている警告とエラーを取得する
- イメージに説明を追加する
- OSディスクをリセットする
- 既存のプロビジョニングスキームのネットワーク設定を変更する
- マシンカタログのバージョンを管理する
- マシンプロファイルベースではないマシンカタログをマシンプロファイルベースのマシンカタログに変換する
- アクティブなコンピューターアカウントのID情報を修復する
    - 条件(#conditions)
    - IDディスクをリセットする(#reset-identity-disk)
- 既存のマシンカタログのキャッシュ構成を変更する(#change-cache-configuration-on-an-existing-machine-catalog)

    - 要件
    - キャッシュ構成を変更する
- ローカルファイル共有アクセスによるVDA更新のサポート
    - PowerShell コマンドレット
    - 前提条件
    - ファイル共有のアクセス許可を設定する方法
    - ローカルファイル共有からのVDA更新
- トラブルシューティング
- 次のステップ

カタログの詳細を表示

1. 特定のマシンカタログを見つけるには、検索機能を使用します。手順については、インスタンスの検索を参照してください。
2. 検索結果から、必要に応じてカタログを選択します。
3. カタログ列の説明については、次の表を参照してください。
4. このカタログに関する詳細情報については、下部の詳細ペインにあるタブをクリックしてください。

列	説明
マシンカタログ	カタログの名前と割り当ての種類。割り当ての種類は次のとおりです。 • ランダム: カタログ内のマシンはユーザーにランダムに割り当てられます。 • 永続: カタログ内のマシンはユーザーに永続的に割り当てられます。

列	説明
マシンタイプ	カタログ内のマシンでサポートされているセッションの種類。可能な値は次のとおりです。 • OSタイプ: マルチセッションOS (仮想); ユーザーデータ: 破棄。 • OSタイプ: マルチセッションOS (仮想); ユーザーデータ: ローカルディスク上 • OSタイプ: シングルセッションOS (リモートPCアクセス) • OSの種類: シングルセッションOS (仮想); ユーザーデータ: 破棄 • OSの種類: シングルセッションOS (仮想); ユーザーデータ: ローカルディスク上
マシン数	カタログ内のマシン数とプロビジョニング方法。可能なプロビジョニング方法には、マシン作成サービス (MCSマシン)、手動、Citrix Provisioning™サービスが含まれます。
割り当て済み数	デリバリーグループに割り当てられているカタログ内のマシン数。

列	説明
フォルダー	**マシンカタログ**ツリー内のカタログの場所。カタログが存在するフォルダーの名前 (末尾のバックスラッシュを含む) を表示します。カタログがルートレベルにある場合は `-` と表示されます。
VDAアップグレード	VDAアップグレードの状態。可能な値は、未構成、スケジュール済み、利用可能、最新です。
イメージステータス	カタログのイメージ更新ステータス。非永続マシンカタログにのみ適用されます。可能な値は、完全に更新済み、部分的に更新済み、更新保留中、準備中です。

マシンをカタログに追加する

開始する前に:

- 仮想化ホストに、追加のマシンを収容するのに十分なプロセッサ、メモリ、ストレージがあることを確認してください。
- 未使用のActive Directoryコンピューターアカウントが十分にあることを確認してください。既存のアカウントを使用している場合、追加できるマシンの数は利用可能なアカウントの数によって制限されます。
- Web Studioを使用して追加のマシン用のActive Directoryコンピューターアカウントを作成する場合、適切なドメイン管理者権限が必要です。

カタログにマシンを追加するには:

1. Web Studioにサインインします。
2. 左側のペインで**Machine Catalogs**を選択します。
3. マシンカタログを選択し、アクションバーで**Add machines**を選択します。
4. 追加する仮想マシンの数を選択します。

5. 追加するVMの数に対して既存のActive Directoryアカウントが不足している場合は、アカウントが作成されるドメインと場所を選択します。連続する数字または文字が表示される場所を示すには、ハッシュマークを使用してアカウントの命名スキームを指定します。OU名にスラッシュ（/）を使用しないでください。名前は数字で始めることはできません。たとえば、PC-Sales-##（0-9を選択）という命名スキームでは、PC-Sales-01、PC-Sales-02、PC-Sales-03などのコンピューターアカウントが作成されます。
6. 既存のActive Directoryアカウントを使用する場合は、アカウントを参照するか、**インポート**をクリックしてアカウント名を含む.csvファイルを指定します。追加するすべてのマシンに対して十分なアカウントがあることを確認してください。Web Studioはこれらのアカウントを管理します。Web Studioがすべてのアカウントのパスワードをリセットすることを許可するか、すべてのアカウントで同じである必要があるアカウントパスワードを指定します。

マシンはバックグラウンドプロセスとして作成され、多数のマシンを作成する場合は時間がかかることがあります。Web Studioを閉じても、マシンの作成は続行されます。

カタログからマシンを削除する

マシンカタログからマシンを削除すると、ユーザーはそのマシンにアクセスできなくなるため、マシンを削除する前に、以下を確認してください。

- ユーザーデータがバックアップされているか、不要になっていること。
- すべてのユーザーがログオフされます。メンテナンスモードをオンにすると、マシンへの新しい接続が停止します。
- マシンの電源がオフになります。

カタログからマシンを削除するには：

1. Web Studioにサインインします。
2. 左側のペインで**マシンカタログ**を選択します。
3. カタログを選択し、アクションバーで**マシンの表示**を選択します。
4. 1つ以上のマシンを選択し、アクションバーで**削除**を選択します。

削除するマシンを削除するかどうかを選択します。マシンを削除することを選択した場合、それらのマシンのActive Directoryアカウントを保持するか、無効にするか、削除するかを指定します。

カタログを編集する

1. **説明**ページで、カタログの説明を変更します。

2. 左側のペインで**マシンカタログ**を選択します。
3. カタログを選択し、アクションバーで**マシンカタログの編集**を選択します。
4. **スコープ**ページで、スコープを変更します。
5. **NIC**ページで、次のアクションを実行します。

   - NICのサブネットマッピングを変更するには、**関連ネットワーク**フィールドからネットワークを選択します。
   - サブネットマッピングを追加するには、**NICの追加**を選択し、**関連付けられたネットワーク**フィールドからネットワークを選択して、**保存**をクリックします。

   カタログに関連付けられているホストに存在するサブネットのみが、**関連付けられたネットワーク**フィールドに表示されます。

   マシンプロファイルのないAzureマシンカタログにのみNICを追加できます。

   > **注：**
   >
   > - AWSマシンカタログの場合、同じサブネットを複数のNICにマッピングすることはできません。
   > - マシンプロファイルを持つマシンカタログの場合、カタログ上のNICの数は、マシンプロファイル上のNICの数と等しくなければなりません。
   > - この機能は、IBM Cloudハイパーバイザーではサポートされていません。
   > - この機能は、Nutanixハイパーバイザーの場合、Nutanix Prism Elementでのみサポートされています。

6. カタログの種類によっては、他のページが表示される場合があります。

   Azure Resource Managerイメージを使用して作成されたカタログの場合、次のページが表示されます。行った変更は、後でカタログに追加するマシンにのみ適用されることに注意してください。既存のマシンは変更されません。

   - **仮想マシン**ページで、マシンを作成するマシンサイズとアベイラビリティゾーンを変更します。

     > **注：**

  - カタログがサポートするマシンサイズのみが表示されます。
  - 必要に応じて、**他のマシンカタログで使用されているマシンサイズのみを表示**を選択して、マシンサイズリストをフィルターします。

- **マシンプロファイル**ページで、マシンプロファイルを使用するか変更するかを選択します。
- (カタログが専用グループホストで構成されている場合にのみ表示されます) **専用ホストグループ**ページで、ホストグループを変更するかどうかを選択します。
- **ストレージとライセンスの種類**ページで、ストレージの種類、ライセンスの種類、およびAzure Computer Galleryの設定を変更するかどうかを選択します (**準備済みイメージをAzure Galleryに配置**が使用されている場合にのみ利用可能)。

注：

新しく選択した設定が現在のマシンサイズをサポートしていない場合、設定を変更するとマシンサイズの設定がリセットされることを示す警告ダイアログボックスが表示されます。続行を選択した場合、**仮想マシン**メニューの横に赤い点が表示され、新しいマシンサイズを選択するように促されます。

- **ライセンスの種類**ページで、WindowsライセンスまたはLinuxライセンスの設定を変更するかどうかを選択します。

Remote PC Accessカタログの場合、以下のページが表示されます。

- **電源管理**ページで、電源管理設定を変更し、電源管理接続を選択します。
- **組織単位**ページで、Active Directory OUを追加または削除します。

7. 加えた変更を適用するには、**適用**をクリックし、終了するには**保存**をクリックします。

カタログの名前を変更する

1. Web Studioにサインインします。
2. 左ペインで**マシンカタログ**を選択します。
3. カタログを選択し、アクションバーで**マシンカタログの名前を変更**を選択します。
4. 新しい名前を入力します。

カタログを別のゾーンに移動する

展開に複数のゾーンがある場合、カタログをあるゾーンから別のゾーンに移動できます。

カタログ内のVMを含むハイパーバイザーとは異なるゾーンにカタログを移動すると、パフォーマンスに影響します。

1. Web Studioにサインインします。
2. 左側のペインで**マシンカタログ**を選択します。
3. カタログを選択し、アクションバーで**移動**を選択します。
4. カタログを移動するゾーンを選択します。

カタログを削除する

カタログを削除する前に、以下を確認してください。

- すべてのユーザーがログオフしており、切断されたセッションは実行されていません。
- カタログ内のすべてのマシンでメンテナンスモードがオンになっており、新しい接続が確立できないこと。
- カタログ内のすべてのマシンが電源オフになっていること。
- カタログはデリバリーグループに関連付けられていません。つまり、デリバリーグループにはそのカタログのマシンが含まれていません。

カタログを削除するには：

1. Web Studioにサインインします。
2. 左側のペインで**マシンカタログ**を選択します。
3. カタログを選択し、アクションバーで**マシンカタログの削除**を選択します。
4. カタログ内のマシンを削除するかどうかを指定します。マシンを削除することを選択した場合、それらのマシンのActive Directoryコンピューターアカウントを保持するか、無効にするか、削除するかを指定します。

レガシーMCSカタログをマシンプロファイルベースのカタログに変換する

マシンプロファイルベースではないマシンカタログをマシンプロファイルベースのマシンカタログに変換するには、次の手順を実行します。

1. **マシンカタログ**ページで、変換する**マシンカタログ**名を右クリックし、**マシンカタログの編集**を選択します。

2. **マシンカタログの編集 > マシンプロファイル**ページで、**マシンプロファイルを使用する（Azure Active Directoryでは必須）**チェックボックスをオンにします。
3. **マシンプロファイルの選択**をクリックします。
4. **マシンプロファイルの選択**ページで、マシンプロファイルとして使用する仮想マシンまたは起動テンプレートを選択します。
5. 現在の設定の一部が新しいマシンプロファイルの設定と異なる場合は、使用する設定に必要なオプションを選択し、**続行**をクリックします。
6. **適用**をクリックします。

> **注:**
>
> 現在、この機能はAzure、AWS、VMwareでのみ利用可能です。

カタログ内のActive Directoryコンピューターアカウントを管理する

マシンカタログ内のActive Directoryアカウントを管理するには、次の操作を実行できます。

- シングルセッションOSおよびマルチセッションOSカタログからActive Directoryコンピューターアカウントを削除して、未使用のマシンアカウントを解放します。これらのアカウントは、他のマシンに使用できます。
- カタログにマシンを追加する際に、コンピューターアカウントがすでに存在するようにアカウントを追加します。OU名にスラッシュ (/) を使用しないでください。

Active Directoryアカウントを管理するには：

1. Web Studioにサインインします。
2. 左ペインで**マシンカタログ**を選択します。
3. カタログを選択し、アクションバーで**ADアカウントの管理**を選択します。
4. コンピューターアカウントを追加するか削除するかを選択します。アカウントを追加する場合は、アカウントのパスワードをどうするかを指定します。すべてリセットするか、すべてのアカウントに適用されるパスワードを入力します。

   現在のアカウントパスワードが不明な場合は、パスワードをリセットできます。パスワードリセットを実行する権限が必要です。パスワードを入力すると、アカウントがインポートされる際にパスワードが変更されます。アカウントを削除する際は、Active Directory内のアカウントを保持するか、無効にするか、削除するかを選択します。

カタログからマシンを削除したり、カタログを削除したりする際に、Active Directoryアカウントを保持するか、無効にするか、削除するかを指定します。

カタログを更新する

カタログ内のマシンを更新する前に、マスターイメージのコピーまたはスナップショットを保存することをお勧めします。データベースは、各マシンカタログで使用されたマスターイメージの履歴レコードを保持します。カタログ内のマシンをロールバックまたは元に戻して、マスターイメージの以前のバージョンを使用します。ユーザーがデスクトップに展開した更新プログラムで問題が発生した場合に、このタスクを実行します。これにより、ユーザーのダウンタイムが最小限に抑えられます。マスターイメージを削除、移動、または名前変更しないでください。それらを使用してカタログを元に戻すことはできません。

マシンが更新されると、自動的に再起動します。

マスターイメージを更新または作成する

マシンカタログを更新する前に、既存のマスターイメージを更新するか、ホストハイパーバイザー上に新しいマスターイメージを作成します。

1. ハイパーバイザー上で、現在のVMのスナップショットを取得し、意味のある名前を付けます。このスナップショットは、必要に応じてカタログ内のマシンを元に戻す（ロールバックする）ために使用できます。
2. 必要に応じて、マスターイメージの電源を入れ、ログオンします。
3. マスターイメージに更新プログラムをインストールするか、必要な変更を加えます。
4. VMの電源を切ります。
5. VMのスナップショットを作成します。Web Studioでカタログが更新されたときに認識されるような意味のある名前を付けます。Web Studioでスナップショットを作成することもできますが、Citrixではハイパーバイザー管理コンソールを使用して作成することをお勧めします。その後、Web Studioでそのスナップショットを選択します。このプロセスにより、自動生成された名前ではなく、意味のある名前と説明を提供できます。GPUマスターイメージの場合、マスターイメージはXenServer®コンソールからのみ変更できます。

マスターイメージを変更する

カタログ内のすべてのマシンに更新プログラムを準備して展開するには：

1. Web Studioにサインインします。
2. 左側のペインで を選択します。
3. カタログを選択し、アクションバーで を選択します。

4. ページで、展開するホストとイメージを選択します。

> **ヒント：**
>
> MCSで作成されたカタログの場合、イメージにメモを追加して注釈を付けることができます。メモは最大500文字まで入力できます。マスターイメージを変更するたびに、メモを追加したかどうかにかかわらず、メモ関連のエントリが作成されます。メモを追加せずにカタログを更新した場合、エントリはnull (-) と表示されます。イメージのメモ履歴を表示するには、カタログを選択し、下部のペインで をクリックし、 をクリックします。

5. ページで、マシンカタログ内のマシンを新しいマスターイメージで更新するタイミング（次回のシャットダウン時または即時）を選択します。

> **注：**
>
> ページは、展開が非永続VMにのみ適用されるため、永続VMでは利用できません。

6. ページで情報を確認し、 をクリックします。各マシンは更新後に自動的に再起動します。

更新の進行状況を追跡するには、「**マシンカタログ**」でカタログを見つけ、インラインの進行状況バーと段階的な進行状況グラフを表示します。

Web StudioではなくPowerShell SDKを直接使用してカタログを更新する場合は、ハイパーバイザーテンプレート（**VMTemplates**）を指定します。これは、イメージまたはイメージのスナップショットの代替として使用します。

Azureベースのマシンカタログに新しいマスターイメージを展開するには：

1. Web Studioから、左ペインで**マシンカタログ**を選択します。
2. Azureカタログを選択し、アクションバーで**マスターイメージの変更**を選択します。
3. **マスターイメージの変更**ページで、マスターイメージの下にあるイメージを選択します。ブレードには、リソースと同じリージョンに属するすべてのイメージが一覧表示されます。

展開戦略：

次回のシャットダウン時にイメージを更新すると、現在使用されていないマシン、つまりアクティブなユーザーセッションがないマシンにすぐに影響します。使用中のシステムは、現在のアクティブセッションが終了したときに更新を受け取ります。以下を考慮してください。

- 適用可能なマシンでの更新が完了するまで、新しいセッションを起動することはできません。
- シングルセッションOSマシンでは、マシンが使用されていないとき、またはユーザーがログインしていないときに、マシンはすぐに更新されます。
- 子マシンを持つマルチセッションOSの場合、再起動は自動的に行われません。更新されたマスターイメージを適用するには、Studio、PowerShell、またはWorkspaceを使用してマシンを再起動します。マシンまたはハイパーバイザーからの再起動では、更新は適用されません。

> **ヒント:**
>
> ホスト接続の詳細設定を使用して、再起動されるマシンの数を制限します。これらの設定を使用して、特定のカタログに対して実行されるアクションを変更します。詳細設定はハイパーバイザーによって異なります。

マスターイメージをロールバックする

更新された、または新しいマスターイメージを展開した後、それをロールバックできます。このプロセスは、新しく更新されたマシンで問題が発生した場合に必要になることがあります。ロールバックすると、カタログ内のマシンは最後に動作していたイメージにロールバックされます。新しいイメージを必要とする新機能は利用できなくなります。展開と同様に、マシンをロールバックすると再起動が含まれます。

1. Web Studioにサインインします。
2. 左ペインで**マシンカタログ**を選択します。
3. カタログを選択し、アクションバーで**マスターイメージのロールバック**を選択します。
4. ロールアウト操作に関する前のセクションで説明されているように、以前のマスターイメージをマシンに適用するタイミングを指定します。

ロールバックは、元に戻す必要があるマシンにのみ適用されます。新しいまたは更新されたマスターイメージで更新されていないマシンは、通知メッセージを受信せず、強制的にログオフされることもありません。

ロールバックの進行状況を追跡するには、**マシンカタログ**でカタログを見つけて、インラインの進行状況バーと段階的な進行状況グラフを表示します。

機能レベルを変更または変更を元に戻す

マシンのVDAを新しいバージョンにアップグレードした後、マシンカタログの機能レベルを変更します。Citrixは、すべての最新機能にアクセスできるように、すべてのVDAを最新バージョンにアップグレードすることを推奨します。

マシンカタログの機能レベルを変更する前に、次の点に注意してください。

- アップグレードされたマシンを起動して、Controllerに登録させます。このプロセスにより、Web Studioはカタログ内のマシンがアップグレードを必要としていることを判断できます。

カタログの機能レベルを変更するには：

1. Web Studioにサインインします。
2. 左ペインで**マシンカタログ**を選択します。
3. カタログを選択します。下部のペインにある**詳細**タブにバージョン情報が表示されます。
4. **機能レベルの変更**を選択します。Web Studioがカタログのアップグレードが必要であると検出した場合、メッセージが表示されます。プロンプトに従います。1台以上のマシンをアップグレードできない場合、その理由を説明するメッセージが表示されます。すべてのマシンが正常に機能するように、Citrixは**変更**をクリックして続行する前に、マシンの問題を解決することをお勧めします。

カタログの変更が完了したら、カタログを選択し、アクションバーで を選択して、マシンを以前のVDAバージョンに戻すことができます。

カタログを複製する

カタログをクローンする前に、次の考慮事項に注意してください。

- オペレーティングシステム および マシン管理 に関連する設定は変更できません。クローンされたカタログは、元のカタログからこれらの設定を継承します。

> **注:**
>
> 複製するAzureカタログを選択し、マスターイメージを選択した場合、ブレードにはリソースと同じリージョンに属するすべてのイメージが一覧表示されます。

- カタログのクローンには時間がかかる場合があります。必要に応じて、 を選択して、バックグラウンドでクローンを実行します。

- クローンされたカタログは元のカタログの名前を継承し、サフィックス `Copy` が付きます。名前は変更できます。「カタログの名前を変更する」を参照してください。
- クローンが完了したら、クローンされたカタログをデリバリーグループに割り当ててください。

1. Web Studioにサインインし、左側のペインで を選択します。
2. カタログを選択し、アクションバーで を選択します。
3. ウィンドウで、クローンされたカタログの設定を表示し、必要に応じて設定を構成します。 を選択して次のページに進みます。
4. ページで、設定の概要を表示し、 を選択してクローンを開始します。
5. 必要に応じて、 を選択して、バックグラウンドでクローンを実行します。

フォルダーを使用してカタログを整理する

フォルダーを作成してカタログを整理し、簡単にアクセスできるようにすることができます。たとえば、イメージの種類別または組織構造別にカタログを整理できます。

> **ヒント:**
>
> アクションバーの右上にある**フォルダー**アイコンをクリックすると、マシンカタログノードの優先デフォルトビュー（フォルダービューまたはリストビュー）を設定できます。

カタログフォルダーを作成する

開始する前に、まずカタログの整理方法を計画してください。次の点を考慮してください。

- フォルダーは最大5レベルまでネストできます（デフォルトのルートフォルダーを除く）。
- カタログフォルダーには、カタログとサブフォルダーを含めることができます。
- Web Studioのすべてのノード（**マシンカタログ**、**デリバリーグループ**、**アプリケーション**、**アプリケーショングループ**など）は、バックエンドで同じフォルダーツリーを共有します。フォルダーの名前変更や移動の際に名前の競合を避けるため、異なるノード間で最上位フォルダーには一意の名前を使用してください。

  `New-BrokerAdminFolder` SDKコマンドレットを使用してフォルダーを作成し、それを**マシンカタログ**ノードの下に表示させたい場合は、`Set-BrokerAdminFolderMetadata` コマンドレットを使用して`ContainsMachineCatalogs` メタデータを追加する必要があります。

  例:

```
Set-BrokerAdminFolderMetadata -AdminFolderId {adminFolderUid} -Name
ContainsMachineCatalogs -Value true
```

カタログフォルダーを作成するには、次の手順に従います。

1. 左側のペインで**Machine Catalogs**を選択します。
2. フォルダー階層でフォルダーを選択し、**アクション**バーで**フォルダーの作成**を選択します。
3. 新しいフォルダーの名前を入力し、**完了**をクリックします。

ヒント:

意図しない場所にフォルダーを作成した場合でも、正しい場所にドラッグして移動できます。

カタログを移動する

カタログはフォルダー間で移動できます。詳細な手順は次のとおりです。

1. 左側のペインで**マシンカタログ**を選択します。
2. フォルダー別にカタログを表示します。フォルダー階層の上にある**すべて表示**をオンにすると、すべてのカタログを一度に表示することもできます。
3. カタログを右クリックし、**マシンカタログの移動**を選択します。
4. カタログの移動先のフォルダーを選択し、**完了**をクリックします。

ヒント:

カタログをフォルダーにドラッグできます。

カタログフォルダーの管理

カタログフォルダーを削除、名前変更、移動できます。

フォルダーとそのサブフォルダーにカタログが含まれていない場合にのみ、フォルダーを削除できます。

フォルダーを管理するには、以下の手順に従います。

1. 左側のペインで**マシンカタログ**を選択します。
2. フォルダー階層でフォルダーを選択し、必要に応じて**アクション**バーでアクションを選択します。
   - フォルダーの名前を変更するには、 を選択します。
   - フォルダーを削除するには、 を選択します。
   - フォルダーを移動するには、 を選択します。
3. 画面の指示に従って、残りの手順を完了します。

カタログ作成を再試行する

> **注:**
>
> この機能はMCSカタログにのみ適用されます。

> 失敗したカタログにはエラーアイコンが表示されます。詳細を確認するには、各カタログのタブに移動します。カタログ作成を再試行する前に、以下の考慮事項に注意してください。

- まずトラブルシューティング情報を確認し、問題を解決してください。この情報には、検出された問題とその解決策に関する推奨事項が記載されています。
- Operating system および machine management に関連付けられた設定は変更できません。カタログは、元の設定を継承します。
- 作成には時間がかかる場合があります。必要に応じて、 を選択して、バックグラウンドで作成を実行します。

カタログの作成を再試行するには、次の手順を実行します。

1. Web Studioで、左側のペインの を選択します。
2. カタログを選択し、その タブに移動します。
3. 再試行ハイパーリンクをクリックして、カタログの作成を再試行します。
4. 表示されるウィザードで、必要に応じて設定を変更します。変更する必要がない場合は、直接**概要**ページに進むことができます。
5. 完了したら、**完了**を選択して作成を開始します。

トークンを使用してMCS以外のプロビジョニング済みVDAを登録する

MCSでプロビジョニングされていないVDAの登録トークンを生成および管理できるようになりました。この実装により、MCSでVDAをプロビジョニングすることなく、WebSocket経由でVDAを登録できます。この機能は、Linux Virtual Delivery Agent、macOS用Citrix Virtual Delivery Agent、およびCitrix Virtual Apps and Desktopsを使用するドメインに参加していないVDAもサポートしています。

始める前に

1. サイトを構成します。詳しくは、サイトの作成を参照してください。
2. Delivery ControllerにTLS証明書をインストールします。詳しくは、ControllerにTLSサーバー証明書をインストールするを参照してください。
3. Delivery Controllerを信頼するために、VDAにルートCAと中間CAをインストールします。
4. Delivery ControllerでWebSocket接続を有効にします。サイト上の各Delivery Controllerで次のコマンドを実行します。

```
New-ItemProperty "HKLM:\SOFTWARE\Citrix\DesktopServer\WorkerProxy"
-Name "WebSocket_Enabled" -PropertyType "DWord" -Value 1 -Force
```

> **注:**
>
> WebSocketを有効にした後、Delivery Controllerを再起動してください。

登録トークンを生成する

Citrix以外でプロビジョニングされたマシン向けにトークンベースの登録を有効にすることを決定したら、まずマシンカタログごとにトークンを生成し、その後、VDAインストール管理者と共有する必要があります。

登録トークンの特徴：

- 登録範囲：1〜5000台のVDAマシン
- 有効期間：最大14日間

Web Studioを使用してカタログのトークンを生成するには、次の手順に従います。

1. **Web Studio > マシンカタログ**で、**マシン数**列に**プロビジョニング方法：手動**と表示されている、MCSでプロビジョニングされていないカタログを見つけます。

2. カタログを右クリックし、**登録トークンの管理**を選択します。
3. 表示される**登録トークンの生成**ページで、次のトークン情報を提供します。
   - トークンの名前を入力します。
   - 有効期間を入力します。期間は14日以内である必要があります。トークンは指定された期間のみ有効です。
   - （オプション）トークンで登録されたVDAの電源管理のためにホスト接続を選択します。オプションには、このカタログのゾーン下のすべてのホスト接続が含まれます。
   - トークンの使用制限（1〜5000）を入力します。
4. **生成**をクリックします。
5. 表示される**トークンが正常に生成されました**ウィンドウで、トークンをコピーして安全な場所に保存するか、**ダウンロード**をクリックして**ダウンロード**フォルダーにダウンロードします。

   トークンリストにトークンレコードが表示されます。

   トークン生成(/en-us/citrix-virtual-apps-desktops/2503/media/token-based-enrollment.png)
6. トークンをVDAインストール管理者と共有します。

   マシンにVDAとトークンをインストールする方法の詳細については、「VDAのインストール」を参照してください。

トークンの管理

トークンを取り消してVDA登録に使用できないようにするには、次の2つのオプションがあります。

- 取り消し：トークンを取り消しますが、ログ記録のためにリストに残します。
- 削除：トークンを取り消し、リストから削除します。

> **注：**
>
> 期限切れのトークンは14日後に自動的に削除されます。

WebSocket VDA登録ツールを使用してマシンをカタログに登録する

WebSocket VDA登録ツールは、VDAマシン向けのトークンベースの登録を容易にします。このツールは、登録トークンを使用してVDAをマシンカタログに追加することで、接続をWebSocket接続に変換するのに役立ちます。

注：

このツールは、どのマシンカタログにも登録されていないVDAマシンを登録するために設計されています。

登録ツールを実行するには、以下の手順に従ってください。

1. VDAにログオンします。
2. `C:\Program Files\Citrix\Virtual Desktop Agent\Web Socket Vda Enrollment Tool` でツール `EnrollMachine.exe` を見つけます。
3. 適切な入力パラメーターを指定してツールを実行します。例： `EnrollMachine.exe -websocket_token_string:xxxxxxxxx`

次の表は、登録ツールの入力パラメータについて説明しています。

パラメータ名	必須	説明	例
`-websocket_token_stdin`	はい	登録トークンを読み取ります。	`.\EnrollMachine.exe -websocket_token_stdin`
`-websocket_token_string`		コマンドラインパラメータから登録トークンを直接読み取ります。	`.\EnrollMachine.exe -websocket_token_string:<token>`
`-websocket_token_file:[token-file-path]`		指定されたパスから登録トークンを読み取ります。	`.\EnrollMachine.exe -websocket_token_file:C:\token\test2.txt`
`log:[log-file-path]`	いいえ	登録ツールのログを表示します。	`.\EnrollMachine.exe log:[C:`

パラメータ名	必須	説明	例
			`\ProgramData\Citrix\EnrollMachine\EnrollMachine.txt]`
`-help`	いいえ	短いヘルプテキストを表示します。	`.\EnrollMachine.exe -help`

登録が成功すると、ツールとログに成功メッセージが表示されます。Web Studioにサインインして、VDAマシンがカタログに追加され、マシンのステータスが登録済みであることを確認してください。

トラブルシューティング

デフォルトでは、登録ツールのログは次の場所にあります。

`C:\ProgramData\Citrix\EnrollMachine\EnrollMachine.txt`

ログに別のパスを指定した場合は、`log:[log-file-path]` を使用してログを取得できます。

次の表に、登録ツールによって返されるコードを示します。

コード	文字列	説明
0	成功	VDAがマシンカタログに正常に追加されました。
-1	無効な引数	登録トークンの入力パラメーターが無効です。
-2	ブローカーエージェントが見つかりません	ブローカーエージェントサービスが見つかりません。
-3	トークンが無効です	入力されたトークンが無効です。
-4	TokenMissingRequiredClaims	トークンに必要なクレーム（例：CustomerId、登録URI）が不足しています。

コード	文字列	説明
-5	InternalError	一般的なエラーが発生しました。
-6	TimedOut	タスクがタイムアウトしました。
-7	FailedToDetermineMachineADJoinedStatus	マシンのAD参加ステータスを返すサービスが失敗しました。
-8	ADMachineFailedToFindSid	ADマシンのSIDを返すサービスが失敗しました。
-9	EnrollRequestFailed	HTTPエラーが原因でリクエストが失敗しました。
-10	EnrollResponseMissingRequiredFields	登録ツールの応答にパラメータ `VirtualSiteId` がありません。
-11	InsufficientPermission	タスクを実行するために必要な権限がありません。
-12	FailedToDetermineMachineAadJoinedStatus	マシンのAD参加ステータスを確認するサービスがエラーをスローしました。
-13	AadMachineFailedToFindDeviceId	システムによって追加された追加パラメータ `AAD device id` が空です。
-14	AadDeviceIdNotValid	システムによって追加された追加パラメーター `AAD device id` は、有効な GUID ではありません。
-15	NoValidMacAddress	無効な MAC アドレスです。
-16	FailedToGetComputerHostNameForVdaInstanceName	追加パラメーター `VdaInstanceName` を設定するためのコンピューターホ

コード	文字列	説明
		スト名の取得に失敗しました。
-17	VirtualDesktopAgentRegistryKeyFailedToOpen	デリバリーコントローラーのリストを書き込むためのVDA レジストリキーを開けませんでした。
-18	失敗したトークンが最大数に達しました	失敗したトークンが最大数に達しました。

PowerShell を使用する

このセクションでは、PowerShellを使用してカタログを管理する方法について詳しく説明します。

- カタログに関連付けられている警告とエラーの取得
- イメージに説明を追加
- OS ディスクのリセット
- 既存のプロビジョニングスキームのネットワーク設定を変更
- マシンカタログのバージョンを管理
- マシンプロファイルベースではないマシンカタログをマシンプロファイルベースのマシンカタログに変換
- アクティブなコンピューターアカウントのID情報を修復
- 既存のマシンカタログのキャッシュ構成を変更
- ローカルファイル共有アクセスによるVDA更新のサポート

カタログに関連付けられている警告とエラーの取得

履歴エラーと警告を取得して、MCS マシンカタログの問題を把握し、それらの問題を修正できます。

PowerShell コマンドを使用すると、次のことができます。

- エラーまたは警告のリストを取得する
- 警告の状態を**新規**から**確認済み**に変更する
- エラーまたは警告を削除する

PowerShellコマンドを実行するには:

1. PowerShell ウィンドウを開きます。
2. Citrix 固有の PowerShell モジュールをロードするには、`asnp citrix*` を実行します。

エラーと警告のリストを取得するには：

`Get-ProvOperationEvent` コマンドを実行します。

- パラメーターなしの場合：すべてのエラーと警告を取得します
- `LinkedObjectType` および `LinkedObjectUid` パラメーターを使用する場合：特定のプロビジョニングスキームに関連付けられているすべてのエラーと警告を取得します
- `EventId` パラメーターを使用する場合：このイベントIDに一致する特定のエラーまたは警告を取得します
- `Filter` パラメーターを使用する場合：カスタマイズされたフィルターによってエラーまたは警告を取得します

エラーまたは警告の状態を **New** から **Acknowledged** に変更するには：

`Confirm-ProvOperationEvent` コマンドを実行します。

- `EventId` パラメーターを使用する場合：このイベントIDに一致する特定のエラーまたは警告の状態を設定します。特定のエラーまたは警告の `EventId` は、`Get-ProvOperationEvent` コマンドの出力として取得できます。
- `LinkedObjectType` および `LinkedObjectUid` パラメーターを使用する場合：特定のプロビジョニングスキームに関連付けられているすべてのエラーと警告の状態を設定します
- `All` パラメーターを使用すると、すべてのエラーと警告の状態が**確認済み**に設定されます。

エラーまたは警告を削除するには：

`Remove-ProvOperationEvent` コマンドを実行します。

- `EventId` パラメーターを使用すると、このイベントIDに一致する特定のエラーまたは警告が削除されます。特定の `EventId` エラーまたは警告は、`Get-ProvOperationEvent` コマンドの出力として取得できます。
- `LinkedObjectType` と `LinkedObjectUid` パラメーターを使用すると、特定のプロビジョニングスキームに関連付けられているすべてのエラーと警告が削除されます。
- `All` パラメーターを使用すると、すべてのエラーと警告が削除されます。

詳しくは、Citrix PowerShell SDKを参照してください。

ハイパーバイザーアクセスなしでマシンを削除する

VMまたはプロビジョニングスキームを削除する際、MCSはVMから、場合によってはベースディスクからもタグを削除する必要があります。これにより、削除オプションに含まれるリソースがMCSによって追跡または識別されなくなります。ただし、これらのリソースの一部はハイパーバイザーを介してのみアクセス可能です。ハイパーバイザーアクセスがない場合でも、`Remove-ProvVM` PowerShell の `PurgeDBOnly` オプションを使用して、VM、ベースディスク、ACG内のイメージなどのVMリソースオブジェクトをデータベースから削除します。

このオプションは、以下で有効になります。

- サポートされているすべてのハイパーバイザー
- 永続VMおよび非永続VM

制限事項

-PurgeDBOnly コマンドと -ForgetVM コマンドを同時に使用することはできません。

PurgeDBOnly コマンドを使用する

PowerShell コマンド `Remove-ProvVM -ProvisioningSchemeName SCVMM-MC -VMName SCVMM01 -ForgetVM` を実行すると、以下のシナリオで削除操作が失敗する可能性があります。

- ホスト接続がメンテナンスモードになっている
- 無効な資格情報
- 認証の失敗
- 不正な操作
- ハイパーバイザーに到達できない

> **注：**
>
> Remove-provVM -ForgetVM は永続的なVMのみを対象とします。リスト内のVMのいずれかが非永続的である場合、操作は失敗します。

> ハイパーバイザーに到達できないために操作が失敗すると、次のプロンプトが表示されます。

`Try to use -PurgeDBOnly option to clean DDC database.`.

MCSデータベースからVMの参照を削除するには、`Remove-ProvVM` PowerShell コマンドで `-PurgeDBOnly` オプションを使用します。例：

```
Remove-ProvVM -ProvisioningSchemeName SCVMM-MC -VMName SCVMM01 -PurgeDBOnly
```

イメージに説明を追加する

マシンカタログのイメージ更新に関連する変更について、情報を提供する説明を追加できます。この機能を使用して、カタログの作成時、またはカタログの既存のマスターイメージを更新する際に説明を追加します。カタログ内の各マスターイメージの情報を表示することもできます。イメージの説明を追加または表示するには、次のコマンドを使用します。

- マスターイメージを使用してマシンカタログを作成する際にメモを追加するには、`NewProvScheme`コマンドで`MasterImageNote`パラメーターを使用します。例：

  ```
  C:\PS>New-ProvScheme -ProvisioningSchemeName <name> -HostingUnitName
  <name> -IdentityPoolName <name> -MasterImageVM

  XDHyp:\HostingUnits\<hosting unit name>\<vm name>.vm\Base.snapshot
  -MasterImageNote "Note"
  ```

- マシンカタログに関連付けられたマスターイメージを更新するには、`Publish-ProvMasterVMImage`コマンドでパラメータ`MasterImageNote`を使用します。例:

  ```
  C:\PS>Publish-ProvMasterVMImage -ProvisioningSchemeName <name>
  -MasterImageVM XDHyp:\HostingUnits\<hosting unit name>\<vm
  name>.vm\base.snapshot -MasterImageNote "Note"
  ```

- 各イメージの情報を表示するには、Get-ProvSchemeMasterVMImageHistoryコマンドを使用します。例:

  ```
  C:\PS>Get-ProvSchemeMasterVMImageHistory -ProvisioningSchemeName
  MyScheme -Showall
  ```

ロールバックの進行状況を追跡するには、**マシンカタログ**でカタログを見つけ、インラインの進行状況バーと段階的な進行状況グラフを表示します。

次のような特定のシナリオでは、ロールバックできません。（**マスターイメージのロールバック**オプションは表示されません）。

- ロールバックする権限がありません。
- カタログがMCSを使用して作成されていません。
- カタログがOSディスクのイメージを使用して作成されています。
- カタログの作成に使用されたスナップショットが破損しています。
- カタログ内のマシンに対するユーザーの変更が保持されません。
- カタログ内のマシンが実行中です。

OSディスクをリセットする

MCSで作成されたマシンカタログ内の永続VMのOSディスクをリセットするには、PowerShellコマンド`Reset-ProvVMDisk`を使用します。現在、この機能はAWS、Azure、XenServer、Google Cloud、SCVMM、およびVMwareの仮想化環境に適用できます。

PowerShellコマンドを正常に実行するには、以下を確認してください。

- ターゲットVMが永続的なMCSカタログにあります。
- MCSマシンカタログが正常に機能しています。
- これは、プロビジョニングスキームとホストが存在し、プロビジョニングスキームに正しいエントリがあることを意味します。
- ハイパーバイザーがメンテナンスモードではないこと。
- ターゲットVMが電源オフでメンテナンスモードであること。

OSディスクをリセットするには、次の手順を実行します。

1. PowerShellウィンドウを開きます。
2. **asnp citrix*** を実行して、Citrix固有のPowerShellモジュールをロードします。
3. 次のいずれかの方法でPowerShellコマンド `Reset-ProvVMDisk` を実行します。

    - VMのリストをコンマ区切りで指定し、各VMでリセットを実行します。

    ```
    Reset-ProvVMDisk -ProvisioningSchemeName "xxx" -VMName ("abc","def")
    -OS
    ```

    - `Get-ProvVM`コマンドからの出力としてVMのリストを指定し、各VMでリセットを実行します。

```
(Get-ProvVM -ProvisioningSchemeName "xxx") | Reset-ProvVMDisk "abc"
-OS
```

- 名前で単一のVMを指定します。

```
Reset-ProvVMDisk -ProvisioningSchemeName "xxx" -VMName "abc" -OS
```

- `Get-ProvVM`コマンドによって返されるVMごとに個別のリセットタスクを作成します。各タスクは、ハイパーバイザーの機能チェック、各VMの接続チェックなど、同じ冗長なチェックを実行するため、これは効率的ではありません。

```
Get-ProvVM -ProvisioningSchemeName "xxx" | Reset-ProvVMDisk
-ProvisioningSchemeName "xxx" -OS
```

4. リセットされるVMのリストと、回復不能な操作であるという警告メッセージが表示された確認プロンプトが表示されます。回答を入力せずに **Enter** キーを押すと、それ以上の操作は行われません。

> **注:**
>
> リセットプロセスが完了するまで、VMをメンテナンスモードから解除したり、電源をオンにしたりしないでください。

> PowerShellコマンド `-WhatIf` を実行して、実行されるアクションを表示し、アクションを実行せずに終了することができます。

確認プロンプトをバイパスするには、以下のいずれかの方法を使用することもできます。

- `-Force` パラメーターを指定します。

```
Reset-ProvVMDisk -ProvisioningSchemeName "xxx" -VMName "abc" -OS
-Force
```

- `-Confirm:$false`パラメーターを指定します。

```
Reset-ProvVMDisk -ProvisioningSchemeName "xxx" -VMName "abc" -OS
-Confirm:$false
```

- `Reset-ProvVMDisk`を実行する前に、`$ConfirmPreference`を**None**に変更します。

```
PS C:\Windows\system32> $ConfirmPreference='None'

PS C:\Windows\system32> $ConfirmPreference

None

PS C:\Windows\system32> Reset-ProvVMDisk -ProvisioningSchemeName
"xxx" -VMName "abc" -OS
```

5. `Reset-ProvVMDisk`コマンドによって返されるタスクのステータスを取得するには、`Get-ProvTask`を実行します。

既存のプロビジョニングスキームのネットワーク設定を変更する

既存のプロビジョニングスキームのネットワーク設定を変更して、新しいVMが新しいサブネットワーク上に作成されるようにすることができます。ネットワーク設定を変更するには、`Set-ProvScheme`コマンドで`-NetworkMapping`パラメーターを使用します。

注:

この機能は、Citrix Virtual Apps and Desktops 2203 LTSR CU3以降のバージョンでサポートされています。

既存のプロビジョニングスキームのネットワーク設定を変更するには、次の手順を実行します。

1. PowerShellウィンドウで、コマンド`asnp citrix*`を実行してPowerShellモジュールをロードします。
2. 変更するネットワークパスに移動するには、`(Get-Provscheme -ProvisioningSchemeName "name").NetworkMaps`を実行します。
3. 新しいネットワーク設定に変数を割り当てます。例：

```
$NewNetworkMap = @{"0"= "XDHYP:\HostingUnits\MyNetworks\Network
0.network"}
```

4. `Set-ProvScheme -ProvisioningSchemeName "name" -NetworkMapping $NewNetworkMap` を実行します。
5. 既存のプロビジョニングスキームの新しいネットワーク設定を確認するには、`(Get-Provscheme -ProvisioningSchemeName "name").NetworkMaps` を実行します。

マシンカタログのバージョンを管理する

MCSマシンカタログが`Set-ProvScheme`コマンドで更新されると、現在の構成がバージョンとして保存されます。その後、PowerShellコマンドを使用して、マシンカタログのさまざまなバージョンを管理できます。次のことができます。

- マシンカタログのバージョンリストを表示する
- 以前のバージョンを使用してマシンカタログを更新する
- そのマシンカタログのVMで使用されていないバージョンは手動で削除する
- マシンカタログで保持される最大バージョン数を変更する（デフォルトは99）

バージョンには、マシンカタログの次の情報が含まれます。

- VMCpuCount
- VMMemoryMB
- CustomProperties
- ServiceOffering
- MachineProfile
- NetworkMapping
- SecurityGroup

マシンカタログのさまざまなバージョンを管理するには、次のコマンド（例として提供）を実行します。

- マシンカタログのさまざまなバージョンの構成詳細を表示するには：

```
Get-ProvSchemeVersion -ProvisioningSchemeName AzureCatalog
```

- マシンカタログの特定のバージョンの構成詳細を表示するには：

```
Get-ProvSchemeVersion -ProvisioningSchemeName AzureCatalog -Version 2
```

- マシンカタログに関連付けられているバージョンの総数を確認するには：

```
(Get-ProvSchemeVersion -ProvisioningSchemeName AzureCatalog).Count
```

- 以前のバージョンを使用してマシンカタログを更新するには：

```
Set-ProvScheme -ProvisioningSchemeName AzureCatalog -Version 2
```

- マシンカタログのVMで使用されていないバージョンを手動で削除するには:

```
Remove-ProvSchemeVersion -ProvisioningSchemeName AzureCatalog -Version
3
```

- マシンカタログが保持する最大バージョン数を設定するには（デフォルトは99）。この設定はすべてのカタログに適用されます。たとえば、この場合、すべてのMCSプロビジョニング済みカタログに対して最大15バージョンが保持されます。

```
Set-ProvServiceConfigurationData -Name "MaxProvSchemeVersions" -Value
15
```

バージョン数が最大バージョン数に達した場合、マシンカタログ内のいずれかのVMで古いバージョンが使用されていると、新しいバージョンを作成できません。その場合は、次のいずれかを実行してください。

- マシンカタログによって保持される最大バージョン数の制限を増やします。
- 古いバージョンを使用している一部のVMを更新して、それらの古いバージョンがどのVMからも参照されなくなり、削除できるようにします。

マシンプロファイルベースではないマシンカタログをマシンプロファイルベースのマシンカタログに変換する

VM、テンプレート仕様（Azureの場合）、起動テンプレート（AWSの場合）、またはVMwareテンプレート（VMwareの場合）をマシンプロファイルの入力として使用して、マシンプロファイルに基づかないマシンカタログをマシンプロファイルに基づくマシンカタログに変換できます。カ

タログに追加された新しいVMは、明示的なカスタムプロパティによって上書きされない限り、マシンプロファイルからプロパティ値を取得します。

> **注:**
>
> 既存のマシンプロファイルベースのマシンカタログを、マシンプロファイルベースではないマシンカタログに変更することはできません。

これを行うには：

1. VMを含み、マシンプロファイルを含まない永続または非永続マシンカタログを作成します。
2. **PowerShell**ウィンドウを開きます。
3. マシンプロファイルからマシンカタログに追加された新しいVMにプロパティ値を適用するには、`Set-ProvScheme`コマンドを実行します。例:

   - Azureの場合:

     ```
     Set-ProvScheme -ProvisioningSchemeName xxxx -MachineProfile XDHyp:
     \HostingUnits\<HostingUnitName>\machineprofile.folder\<ResourceGroup
     Name>\<TemplateSpecName>\<VersionName>
     ```

   - AWSの場合:

     ```
     Set-ProvScheme -ProvisioningSchemeName xxxx -MachineProfile "XDHyp:
     \HostingUnits\<hosting-unit>\<launch-
     template>.launchtemplate\<launch-template-
     version>.launchtemplateversion"
     ```

   - VMwareの場合:

     ```
     Set-ProvScheme -ProvisioningSchemeName "my-prov-scheme"
     -MachineProfile "XDHyp:\HostingUnits\my-hosting-unit\my-
     template.template"
     ```

     > **注:**

> VMwareテンプレートから`FolderID`が派生するのを避けるために、`FolderID`をカスタムプロパティとして設定します。

アクティブなコンピューターアカウントのID情報を修復する

ID関連の問題があるアクティブなコンピューターアカウントのID情報をリセットできます。マシンパスワードと信頼キーのみをリセットするか、IDディスクのすべての構成をリセットするかを選択できます。この実装は、永続および非永続MCSマシンカタログの両方に適用できます。

> **注:**
>
> 現在、この機能はAWS、GCP、Azure、SCVMM、XenServer、およびVMwareの仮想化環境でサポートされています。

条件

IDディスクを正常にリセットするには、以下を確認してください:

- VMをシャットダウンし、メンテナンスモードに設定する
- PowerShellコマンドにパラメーター-OSを含めない

IDディスクのリセット

IDディスクをリセットするには：

1. **PowerShell**ウィンドウを開きます。
2. Citrix固有のPowerShellモジュールをロードするために`asnp citrix*`を実行します。
3. ID情報をリセットします。
   - マシンパスワードと信頼キーのみをリセットするには、次のコマンドを実行します。

     ```
     Repair-AcctIdentity -IdentityAccountName TEST\VM1
     -PrivilegedUserName TEST\admin1 -PrivilegedUserPassword $password
     -Target IdentityInfo
     ```

     コマンドで使用されるパラメーターの説明は次のとおりです。

     - IdentityAccountName: 修復する必要があるIDアカウントの名前。

  - PrivilegedUserName: IDプロバイダー (ADまたはAzureAD) に対する書き込み権限を持つユーザーアカウント。
  - PrivilegedUserPassword: PrivilegedUserNameのパスワード。
  - ターゲット：修復アクションのターゲット。アカウントパスワード/信頼キーを修復する場合はIdentityInfo、ハイブリッドAzureAD参加済みマシンIDのユーザー証明書属性を修復する場合はUserCertificateを指定できます。

- IDディスクのすべての構成をリセットするには、次のコマンドを次の順序で実行します。

```
Repair-AcctIdentity -IdentityAccountName TEST\VM1
-PrivilegedUserName TEST\admin1 -PrivilegedUserPassword $password
-Target IdentityInfo
```

```
Reset-ProvVMDisk ProvisioningSchemeName <name> -VMName <name>  -
Identity
```

- IDディスクを完全に再作成するには:

```
Reset-ProvVMDisk -ProvisioningSchemeName <name> -VMname <name>
-Identity -Recreate
```

4. アクションを確定するには「**y**」と入力します。`-Force` パラメーターを使用して確認プロンプトをスキップすることもできます。例:

```
Reset-ProvVMDisk -ProvisioningSchemeName <name> -VMName <name>
-Identity -Force
```

5. 更新されたIDディスク設定を確認するには、`Get-ProvVM -ProvisioningSchemeName <name -VMName <name>` を実行します。IDディスクの属性 (例: `IdentityDiskId`) は更新されている必要があります。`StorageId` と `IdentityDiskIndex` は変更されていてはなりません。

既存のマシンカタログのキャッシュ構成を変更する

MCSIOを有効にして非永続カタログを作成した後、Set-ProvSchemeコマンドを使用して以下のパラメータを変更できます。

- WriteBackCacheMemorySize
- WriteBackCacheDiskSize

この機能は現在、以下に適用されます。

- GCPおよびMicrosoft Azure環境、および
- MCSIOが有効な非永続カタログ

要件

キャッシュ構成を変更するための要件は次のとおりです。

- 最新バージョンのVDA（2308以降）に更新します。
- 既存のマシンカタログに対してパラメーター `UseWriteBackCache` を有効にします。`UseWriteBackCache` を有効にしてマシンカタログを作成するには、`New-ProvScheme` を使用します。例：

```
New-ProvScheme -ProvisioningSchemeName $CatalogName -HostingUnitUid
$HostingUnitUid `

-IdentityPoolUid $acctPool.IdentityPoolUid -CleanOnBoot `

-MasterImageVM $MasterImage `

-ServiceOffering $ServiceOffering `

-NetworkMap $NetworkMap `

-SecurityGroup $SecurityGroup `

-UseWriteBackCache -WriteBackCacheDiskSize 8
```

キャッシュ構成を変更する

Set-ProvSchemeコマンドを実行します。例:

```
Set-ProvScheme -ProvisioningSchemeName $provScheme.ProvisioningSchemeName
-WriteBackCacheDisk32 -WriteBackCacheMemorySize 128
```

注:

- `WriteBackCacheDiskSize` の値はゼロより大きい必要があります。これは、少なくとも1 GBのキャッシュディスクストレージが必要なためです。
- `WriteBackCacheMemorySize` の値は、マシンカタログのメモリサイズよりも小さくする必要があります。
- これらの変更は、変更後にカタログに追加された新しい VM にのみ影響します。既存の VM はこれらの変更の影響を受けません。

ローカルファイル共有アクセスによるVDAアップデートのサポート

PowerShellコマンドレットを介してVDAインストーラーの場所を指定することで、各VDAがCitrix Managed Azure CDNから新しいVDAインストーラーを取得できるようにするためのネットワークルールを提供する手間を省くことができます。

PowerShellコマンドレット

ローカルファイル共有からインストーラーを使用できるようにする、**New-VusCatalogSchedule** および **New-VusMachineUpgrade** コマンドレットに2つの新しいオプションパラメータが追加されました。

- **VdaWorkstationPackageUri** - ワークステーションOS VDAインストーラーへのUNCパスを指定します。
- **VdaServerPackageUri** - サーバーOS VDAインストーラーへのUNCパスを指定します。

前提条件

- VDA 2311に付属するVUSエージェントインストーラー
- VDAアップグレードエージェントをバージョン7.40.0.35以降にアップグレード（VDAインストーラーバージョン2311以降を使用）
- Virtual Apps and Desktops Remote PowerShell SDK バージョン 7.40 以降 (Jan 10, 2024 以降にリリース)

ファイル共有のアクセス許可を設定する方法

VDAインストーラーパッケージを含むネットワーク共有には、Local System (NT AUTHORITY\SYSTEMプリンシパル) として実行されるVDAアップグレードエージェントサービスに対する読み取りアクセス権が必要です。

- **ドメイン参加済みファイル共有のアクセス許可**

VDAマシンがドメインに参加している場合、**ローカルシステム**アカウント（VUAはローカルシステムとして実行されます）は、ネットワーク共有にアクセスする際にコンピューターの資格情報を使用します。

最小特権のアクセス許可は、Domain Computers に **読み取り** アクセスを付与することで設定できます。

a. ファイルを共有するネットワーク上のユーザーを選択します。
b. **詳細な共有設定** をクリックし、**ファイルとプリンターの共有** をオンにします。

- **ドメインに参加していないファイル共有のアクセス許可**

VDA マシンがドメインに参加していない場合、**ローカルシステム** アカウント (VUA はローカルシステムとして実行されます) は、ネットワーク共有にアクセスするときに **ANONYMOUS LOGON** を使用します。

a. 共有フォルダーを選択します。
b. パスワード保護を無効にします。
    a. フォルダーの**プロパティ**に移動します。
    b. **ネットワークと共有センター**を選択します。
    c. **パスワード保護共有**をオフにします。
c. **詳細な共有**をクリックして、共有アクセス許可を付与します。
    a. **アクセス許可**を選択します。
    b. **ANONYMOUS LOGON**に**読み取り**共有アクセス許可を付与します。
d. フォルダーのアクセス許可を付与するには、**セキュリティ**タブを選択します。
    a. 「**編集**」をクリックして、共有フォルダーにアクセス許可を追加します。
    b. 共有フォルダーを選択して、**ANONYMOUS LOGON** にフォルダーのアクセス許可を付与します。
e. 「**詳細設定**」をクリックして、**ファイルとプリンターの共有**をオンにします。
f. 共有フォルダー名を**ネットワークアクセスセキュリティポリシー**に追加します。

> **注:**
>
> 変更をすぐに有効にするには、マシンを再起動します。

ローカルファイル共有からのVDAアップデート

1. VDAインストーラーをダウンロードし、共有ファイルに配置します。

   注:

   Virtual Upgrade Serviceを使用すると、Current ReleaseトラックまたはLTSRトラックのいずれかを選択できます。

   例： マシンカタログがCurrent Release（2311）に設定されており、VDAバージョンが2305の場合、VDAをバージョン2311にアップグレードする必要があります。

   a. 弊社のWebサイトの**ダウンロード**ページに移動します。
   b. 製品として**Citrix Virtual Apps and Desktops**を選択します。
   c. **Citrix Virtual Apps and Desktops 7 2311, 全エディション**を選択します。
   d. 展開可能な**製品ISOに含まれるが個別にパッケージ化されているコンポーネント**からVDAインストーラーを選択します。

2. カタログの種類に基づいて、関連するVDAインストーラーを選択します。

   - カタログの種類が**マルチセッション**の場合は、**マルチセッションOS VDAインストーラー**をダウンロードします。
   - カタログの種類が**シングルセッション**の場合は、**シングルセッションOS VDAインストーラー**をダウンロードします。
   - カタログの種類が**Remote PC Access**の場合は、**シングルセッションOSコアサービスVDAインストーラー**をダウンロードします。

注:

ファイル共有インストーラーのバージョンは、VUSによってクラウドに公開された最新のインストーラーのバージョンと**完全に**一致している必要があります。

VMのストレージ移行

VMwareおよびXenServer環境では、既存のVMのディスクストレージを古いストレージから新しいストレージに移動できます。移行中、MCSは電源管理、OSディスクのリセットなどのVM機能を保持します。新しいディスクストレージを使用して、新しいVMをマシンカタログに追加することもできます。これを行うには、PowerShellコマンド`Move-ProvVMDisk`を使用します。

フルクローン永続VMと非永続VMを移行できます。

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

新しいストレージは、次の条件を満たす必要があります。

- 古いストレージと同じクラスター内にある必要があります。
- VMが実行されているホストは、古いデータストアと新しいデータストアの両方にアクセスできる必要があります。

ディスクストレージの移行

ディスクストレージを移行するには：

1. 既存のホスティングユニットに宛先ストレージを追加します。宛先ストレージを追加するには、PowerShellコマンド `Add-Hyphostingunitstorage` を実行します。

   古いストレージに新しいVMを追加したくない場合は、古いストレージを**Superseded**に変更します。これはStudioまたはPowerShellコマンドを使用して実行できます。Studioについては、ストレージの編集を参照してください。または、`Set-Hyphostingunitstorage`を実行し、`Superseded`を`true`に設定して、古いストレージでの新しいVM作成を無効にします。

   > **注:**
   >
   > 非永続VMの場合：
   >
   > - WBCを使用している場合は、ホスティングユニットでWBC宛先ストレージを構成します。

- OS宛先ストレージが構成されている場合、WBC（使用されている場合）はOS宛先ストレージと互換性がある必要があります。
- OS宛先ストレージが構成されていない場合、WBC（使用されている場合）は現在のOSストレージと互換性がある必要があります。

2. VMをシャットダウンし、**メンテナンスモード**をオンにします。
3. プロビジョニングスキーム、ホスティングユニット、OSディスクストレージ、およびWBCディスクストレージに関する情報を取得します。
   - OSストレージ情報については、`ProvResourceInStorage`を実行します。例：

     ```
     $result=Get-ProvSchemeResourceInStorage -ProvisioningSchemeName
     xxxxx

     $result

     $result.ProvResourceInStorage | Format-List -Property *
     ```

   - WBCストレージ情報については、`TemporaryStorageInfo`を実行します。例：

     ```
     $result=Get-ProvSchemeResourceInStorage -ProvisioningSchemeName
     xxxxx

     $result

     $result.TemporaryStorageInfo | Format-List -Property *
     ```

4. OSディスク、IDディスク、およびWBCディスク (非永続VMに適用) を`Move-ProvVMDisk` PowerShellコマンドを使用して宛先ストレージに移行します。

注:

- DiskTypeおよび`DestinationStorageId`パラメーターには、常にOSディスクとIDディスクを指定してください。
- OSディスクとIDディスクの`DestinationStorageId`は同じである必要があります。

例:

永続VM：

```
(Get-ProvVM -ProvisioningSchemeName xxxxx) | Move-ProvVMDisk
-ProvisioningSchemeName "myFullCloneProvScheme" -VMName "machine01"
-DiskType OS,Identity -DestinationStorageId datastore1,datastore1
```

重要:

永続VMの場合、すべてのディスクが移動されます。移動するディスクを選択することはできません。

非永続VM：

```
(Get-ProvVM -ProvisioningSchemeName xxxxx) | Move-ProvVMDisk
-ProvisioningSchemeName "myCleanOnBootProvScheme" -VMName "machine01"
-DiskType OS,Identity,WBC -DestinationStorageId None,None,datastore1
```

重要:

- 特定のディスクを移行したくない場合は、`DestinationStorageId`パラメーターの値を`None`として設定します。
- VMにWBCディスクがある場合は、WBCディスクを`DiskType`パラメーターに追加し、必要な情報を`DestinationStorageId`パラメーターに追加します。

既存のMCSプロビジョニング済みカタログを準備済みイメージマシンカタログに移行する

既存のMCSプロビジョニング済みマシンカタログは、PowerShellコマンド`Set-ProvSchemeImage`を使用して準備済みイメージマシンカタログに変換できます。ただし、移行後にレガシーカタログに戻すことはできません。現在、この機能はAzureおよびVMware仮想化環境に適用されます。

制限事項

次の制限事項を考慮してください。

- MCSカタログが永続データディスクを使用している場合、そのカタログを準備済みイメージを使用するように移行することはできません。
- MCSカタログがアンマネージドディスクを使用している場合、そのカタログを準備済みイメージを使用するように移行することはできません。

準備済みイメージマシンカタログへの移行

移行するには、次の手順を実行します。

1. StudioまたはPowerShellコマンドを使用して、イメージ定義とイメージバージョンを作成します。イメージ定義とイメージバージョンの作成手順については、以下を参照してください。
   - アジュール：
     - ウェブスタジオ
     - PowerShell
   - ヴイエムウェア：
     - ウェブスタジオ
     - PowerShell
2. プロビジョニングスキームのUIDを取得するには、`Get-ProvScheme` コマンドを実行します。例：

   ```
   Get-ProvScheme -ProvisioningSchemeName <name> | select
   ProvisioningSchemeName, ProvisioningSchemeUid
   ```

3. イメージ定義名、イメージバージョン仕様のUIDを取得するには、`Get-ProvImageVersionSpec` コマンドを実行します。例：

   ```
   Get-ProvImageVersionSpec -ImageDifinitionName <name> -Filter
   {IsPrepared -eq $true} | select ImageDefinitionName ImageVersionSpecUId
   ```

4. 既存のMCSプロビジョニング済みマシンカタログを準備済みイメージマシンカタログに移行するには、`Set-ProvSchemeImage` コマンドを実行します。例：

```
Set-ProvSchemeImage -ProvisioningSchemeName [ProvisioningSchemeName]
-ImageVersionSpecUid [ImageVersionSpecUid]
```

5. カタログが移行されたことを確認するには、`Get-ProvScheme` コマンドを実行します。例：

```
Get-ProvScheme -ProvisioningSchemeName <name> | select
ProvisioningSchemeName, ProvisioningSchemeUid, ImageVersionSpecUid
```

トラブルシューティング

- 「電源状態不明」ステータスのマシンについては、CTX131267 でガイダンスを参照してください。
- 継続的に不明な電源状態を示すVMを修正するには、継続的に不明な電源状態を示すVMを修正する方法を参照してください。

次のステップ

特定のクラウドサービスカタログの管理については、以下を参照してください。

- AWSカタログの管理(/ja-jp/citrix-virtual-apps-desktops/2503/install-configure/machine-catalogs-manage/manage-machine-catalog-aws.html)
- XenServerカタログの管理(/ja-jp/citrix-virtual-apps-desktops/2503/install-configure/machine-catalogs-manage/manage-machine-catalog-citrix-hypervisor.html)
- Google Cloud Platformカタログの管理(/ja-jp/citrix-virtual-apps-desktops/2503/install-configure/machine-catalogs-manage/manage-machine-catalog-gcp.html)
- Microsoft Azureカタログの管理(/ja-jp/citrix-virtual-apps-desktops/2503/install-configure/machine-catalogs-manage/manage-machine-catalog-azure.html)
- マイクロソフト システムセンター 仮想マシンマネージャー カタログの管理
- VMwareカタログの管理(/ja-jp/citrix-virtual-apps-desktops/2503/install-configure/machine-catalogs-manage/manage-machine-catalog-vmware.html)

AWSカタログを管理する

マシンカタログの管理では、マシンカタログを管理するウィザードについて説明します。以下の情報は、AWSクラウド環境に固有の詳細を扱っています。

> **注:**

> AWSカタログを管理する前に、AWSカタログの作成を完了する必要があります。AWSカタログを作成するを参照してください。

タグを削除する

カタログまたはVMを作成すると、MCSによって作成されたタグが以下のリソースに作成されます。

- 仮想マシン
- ルートディスクボリューム
- 識別ディスクボリューム
- NIC
- ルートディスクイメージ (AMI)
- 起動テンプレート
- AMIまたはルートディスクのスナップショット

Citrix®データベースからVMとマシンカタログを削除し、MCSによって作成されたタグを削除できます。以下を使用できます。

- `Remove-ProvVM`と`ForgetVM`パラメーターを使用して、マシンカタログから単一のVMまたはVMのリストからVMとMCSによって作成されたタグを削除します。
- Citrix データベースからマシンカタログを、マシンカタログからリソースを削除するには、`ForgetVM` パラメーターを指定して `Remove-ProvScheme` を使用します。

この機能は、永続VMにのみ適用されます。

これを行うには、次の手順を実行します。

1. **PowerShell** ウィンドウを開きます。
2. Citrix 固有の PowerShell モジュールをロードするには、`asnp citrix*` を実行します。
3. VM を削除する前に、VM のロックを解除します。例:

   ```
   Unlock-ProvVM -ProvisioningSchemeName "<name>" -VMID "<id"
   ```

4. VM、マシンカタログ、および MCS で作成されたタグをリソースから削除するには、次のいずれかのコマンドを実行します。

- Citrix データベースから VM を、VM からタグを削除するには、`ForgetVM` を指定して `Remove-ProvVM` を実行します。例:

```
Remove-ProvVM -ProvisioningSchemeName "<name>" -VMName "<name>"
-ForgetVM
```

- Citrix データベースからマシンカタログを、マシンカタログからリソースを削除するには、`Remove-ProvScheme` を実行します。例:

```
Run Remove-ProvScheme -ProvisioningSchemeName "<name>" -ForgetVM
```

5. VM が Delivery Controller™ から削除されているが、ハイパーバイザーからは削除されていないことを確認します。

   a. `Get-ProvVM -ProvisioningSchemeName "<name>" -VMName "<name>"` を実行します。何も返されないはずです。

   b. AWS EC2 コンソールに移動します。VM は表示されますが、タグは削除されています。以下のリソースからタグが削除されます。

      - 仮想マシン
      - ルートディスクボリューム
      - ID ディスクボリューム
      - NIC

6. マシンカタログを削除する場合は、カタログがデリバリーコントローラーから削除されていることを確認します。

   a. `Get-ProvScheme -ProvisioningSchemeName "forgetvmdemo"`を実行します。これはエラーを返すはずです。

   b. AWS EC2コンソールで、以下のリソースが削除されていることを確認します。

      - ルートディスクイメージ (AMI)
      - 起動テンプレート
      - AMIまたはルートディスクのスナップショット

MCSによって作成されたリソースを識別する

以下は、MCS がリソースに追加するタグです。表のタグは「"key":"value"」として表されます。

リソース名	タグ
IDディスク	"名前": "VMName_IdentityDisk"
	"Xd構成": "Xdプロビジョニング済み=true"
	"CitrixプロビジョニングスキームID": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
イメージ	"Xd構成": "Xdプロビジョニング済み=true"
	"CitrixプロビジョニングスキームID": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
NIC	"説明": "XD NIC"
	"Xd構成": "XdProvisioned=true"
	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
OSディスク	"名前": "VMName_rootDisk"
	"XdConfig": "XdProvisioned=True"
	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	[when AwsCaptureInstanceProperties = true] "Citrix リソース": ""
	[when AwsCaptureInstanceProperties = true and AwsOperationalResourcesTagging = true] "CitrixOperationalResource": ""
PrepVM	"名前": "準備 - CatalogName - xxxxxxxxxx"
	"XdConfig": "XdProvisioned=true"
	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	[when AwsCaptureInstanceProperties = true] "Citrix リソース": ""

リソース名	タグ
	[when AwsCaptureInstanceProperties = true and AwsOperationalResourcesTagging = true] "CitrixOperationalResource": ""
公開スナップショット	"XdConfig": "XdProvisioned=トゥルー"
	Volume Worker AMIのスナップショットでない場合、「CitrixProvisioningSchemeId」:「xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx」
テンプレート	[when AwsCaptureInstanceProperties = true] "XdConfig": "XdProvisioned=トゥルー"
	[when AwsCaptureInstanceProperties = true] "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	[when AwsCaptureInstanceProperties = true] "CitrixResource": ""
	[when AwsCaptureInstanceProperties = true and AwsOperationalResourcesTagging = true] "CitrixOperationalResource": ""
カタログ内のVM	"XdConfig": "XdProvisioned=true"
	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	[when AwsCaptureInstanceProperties = true] "CitrixResource": ""
	[when AwsCaptureInstanceProperties = true] "aws:ec2launchtemplate:id":"lt-xxxx" というタグ
	[when AwsCaptureInstanceProperties = true] "aws:ec2launchtemplate:version": "n" というタグ

リソース名	タグ
	[when AwsCaptureInstanceProperties = true and AwsOperationalResourcesTagging = true] "CitrixOperationalResource": ""
ボリュームワーカーAMI	"XdConfig": "XdProvisioned=true"
ボリュームワーカーブートストラッパー	"Name": "XenDesktop® 一時"
	"Xd設定": "XdProvisioned=true"
	"Citrixプロビジョニングスキーム ID": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	[when AwsCaptureInstanceProperties = true and AwsOperationalResourcesTagging = true] "CitrixVolumeWorkerBootstrapper": ""
ボリュームワーカーインスタンス	"Name": "Citrix.XD.Volumeworker-xxxx-xx-xx-xx-xxxx"
	"Xd設定": "XdProvisioned=true"

詳細情報

- 接続とリソースの作成および管理
- AWSへの接続
- マシンカタログの作成
- AWS カタログを作成する
- マシンカタログの管理

XenServer®カタログを管理する

マシンカタログを管理するは、マシンカタログを管理するウィザードについて説明しています。以下の情報は、XenServer仮想化環境に固有の詳細を扱っています。

> **注:**

> XenServerカタログを管理する前に、XenServerカタログの作成を完了する必要があります。「XenServerカタログを作成する(/ja-jp/citrix-virtual-apps-desktops/2503/install-configure/machine-catalogs-create/create-machine-catalog-citrix-hypervisor.html)」を参照してください。

MCSによって作成されたリソースを識別する

以下は、MCSがリソースに追加するタグです。表のタグは「"key":"value"」として表されます。

リソース名	タグ
公開されたベースディスクと、各ネットワークまたはローカルストレージ上のそのコピー	"Citrixプロビジョニングスキーム ID": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
IDディスク	"Citrixプロビジョニングスキーム ID": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
OSディスク	"Citrixプロビジョニングスキーム ID": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
準備VM	"Citrixプロビジョニングスキーム ID": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
カタログ内のVM	"Citrixプロビジョニングスキーム ID": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
WBCディスク	"Citrixプロビジョニングスキーム ID": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"

詳細情報

- 接続とリソースの作成および管理
- XenServerへの接続
- マシンカタログの作成
- XenServerカタログを作成する
- マシンカタログの管理

Google Cloud Platformカタログを管理する

マシンカタログの管理では、マシンカタログを管理するウィザードについて説明します。以下の情報は、Google Cloud環境に固有の詳細をカバーしています。

> **注：**
>
> Google Cloud Platformカタログを管理する前に、Google Cloud Platformカタログの作成を完了する必要があります。Google Cloud Platformカタログの作成を参照してください。

マシンカタログの管理

カタログへのマシンの追加、マシンの更新、および更新のロールバックについては、マシンカタログの管理を参照してください。

電源管理

Citrix DaaS™では、Google Cloudマシンの電源管理が可能です。左ペインの**検索**ノードを使用して、電源管理したいマシンを見つけます。以下の電源アクションが利用可能です。

- 削除
- 開始
- 再起動
- 強制再起動
- シャットダウン
- 強制シャットダウン
- デリバリーグループに追加
- タグの管理
- メンテナンスモードをオンにする

Autoscale を使用して Google Cloud マシンを電源管理することもできます。これを行うには、Google Cloud マシンをデリバリーグループに追加し、そのデリバリーグループで Autoscale を有効にします。Autoscale の詳細については、「Autoscale」を参照してください。

PowerShellを使用してプロビジョニングされたマシンを更新する

`Set-ProvScheme`コマンドはプロビジョニングスキームを変更しますが、既存のマシンには影響しません。PowerShellコマンド`Set-ProvVMUpdateTimeWindow`を使用すると、現在のプロビジョニングスキームを既存の永続マシンまたは非永続マシン、あるいはマシンセットに適用できるようになります。現在、GCPでは、この機能でサポートされているプロパティ更新はマシンプロファイルです。

更新できるもの:

- 単一のVM
- 特定のVMのリスト、またはプロビジョニングスキームIDに関連付けられている既存のすべてのVM
- プロビジョニングスキーム名に関連付けられた特定のVMのリスト、またはすべての既存のVM

既存のVMを更新するには：

1. 既存のマシンの構成を確認します。例えば、,

   ```
   Get-ProvScheme | select ProvisioningSchemeName,
   ProvisioningSchemeVersion
   ```

2. プロビジョニングスキームを更新します。例えば、,

   ```
   `Set-ProvScheme –ProvisioningSchemeName "my-catalog" –MachineProfile
   "XDHyp:\HostingUnits\<hosting-unit>\machineprofileinstance.vm"
   ```

3. VMの現在のプロパティが現在のプロビジョニングスキームと一致しているか、およびVMに保留中の更新アクションがあるかを確認します。例えば、,

   ```
   Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
   ProvisioningSchemeVersion
   ```

   特定のバージョンのマシンを見つけることもできます。例えば、,

   ```
   Get-ProvVM -Filter "ProvisioningSchemeVersion -eq 1" | select VMName,
   ProvisioningSchemeVersion
   ```

4. 既存のマシンを更新します。

   - すべての既存のマシンを更新するには：

     ```
     Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
     -StartsNow -DurationInMinutes -1
     ```

   - 特定のマシンのリストを更新するには：

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
-VMName <List-Of-Vm-Names> -StartsNow -DurationInMinutes -1
```

- `Get-ProvVM`の出力に基づいてマシンを更新するには：

```
Get-ProvVM -ProvisioningSchemeName "my-catalog" | Set-
ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog -StartsNow
-DurationInMinutes -1
```

5. 更新がスケジュールされているマシンを見つける。例：

```
Get-ProvVM -Filter "ProvisioningSchemeUpdateAfter" | select VMName,
ProvisioningSchemeUpdateAfter
```

6. マシンを再起動します。次回の電源投入時に、プロパティの変更が既存のマシンに適用されます。以下のコマンドを使用して更新されたステータスを確認できます。

```
Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
ProvisioningSchemeVersion
```

既存のカタログのディスク関連のカスタムプロパティを変更する

既存のカタログおよびカタログの既存のVMの、以下のディスク関連のカスタムプロパティを変更できます。

- `PersistOSDisk`
- `PersistWBC`
- `StorageType`
- `IdentityDiskStorageType`
- `WbcDiskStorageType`

注:

- `StorageType` プロパティは OS ディスク用です

- `PersistOsDisk` プロパティは、ライトバックキャッシュが有効な非永続カタログに対してのみ設定できます

この実装により、カタログ作成後でもディスクごとに異なるストレージタイプを選択できるようになり、さまざまなストレージタイプに関連する価格のバランスを取ることができます。

これを行うには、PowerShell コマンド `Set-ProvScheme` と `Set-ProvVMUpdateTimeWindow` を使用します。

1. **PowerShell** ウィンドウを開きます。
2. `asnp citrix*` を実行します。
3. カスタムプロパティを取得するには、`Get-ProvVM -VMName <VM name>` を実行します。
4. カスタムプロパティ文字列を変更します。
   a. カスタムプロパティをメモ帳にコピーし、カスタムプロパティを変更します。
   b. **PowerShell** ウィンドウで、メモ帳から変更したカスタムプロパティを貼り付け、変更したカスタムプロパティに変数を割り当てます。例:

```
$cp =  '<CustomProperties xmlns=http://schemas.citrix.com/2014/xd/
machinecreation xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<Property xsi:type="StringProperty" Name="CatalogZones" Value="" />

<Property xsi:type="StringProperty" Name="PersistWBC" Value="true" /
>

<Property xsi:type="StringProperty" Name="PersistOSDisk"
Value="true" />

<Property xsi:type="StringProperty" Name="WBCDiskStorageType"
Value="pd-standard" />

<Property xsi:type="StringProperty" Name="StorageType" Value="pd-
standard" />

</CustomProperties>'
```

5. 既存のカタログを更新します。例:

```
Set-ProvScheme -ProvisioningSchemeName <yourCatalogName>
-CustomProperties $cp
```

6. 既存の VM を更新します。例:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog -VMName
<List-Of-Vm-Names> -StartsNow -DurationInMinutes -1
```

7. VM を再起動します。次回の電源投入時に、カスタムプロパティの変更が既存の VM に適用されます。

誤ったマシン削除の防止

Citrix DaaS を使用すると、Google Cloud 上の MCS リソースを保護して、誤って削除されるのを防ぐことができます。プロビジョニングされた VM を構成するには、`deletionProtection` フラグを TRUE に設定します。

デフォルトでは、MCS または Google Cloud プラグインを介してプロビジョニングされた VM は、InstanceProtection が有効な状態で作成されます。この実装は、永続カタログと非永続カタログの両方に適用されます。非永続カタログは、インスタンスがテンプレートから再作成されるときに更新されます。既存の永続マシンについては、Google Cloud コンソールでフラグを設定できます。フラグの設定の詳細については、Google ドキュメントサイト を参照してください。永続カタログに追加された新しいマシンは、`deletionProtection` が有効な状態で作成されます。

`deletionProtection` フラグを設定した VM インスタンスを削除しようとすると、リクエストは失敗します。ただし、`compute.instances.setDeletionProtection` 権限が付与されているか、IAM の **Compute Admin** ロールが割り当てられている場合は、フラグをリセットしてリソースの削除を許可できます。

MCSによって作成されたリソースを識別する

以下は、MCS がリソースに追加するタグです。表のタグは「"key":"value"」として表されます。

リソース名	タグ
IDディスク	"CitrixResource": "内部"
	"Citrixプロビジョニングスキーム ID": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"

リソース名	タグ
イメージ	"CitrixResource": "内部"
	"CitrixプロビジョニングスキームID": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
OSディスク	"CitrixResource": "内部"
	"CitrixプロビジョニングスキームID": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
PrepVM	"CitrixResource": "内部"
	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
公開スナップショット	"CitrixResource": "内部"
ストレージバケット	"シトリックスリソース": "内部"
テンプレート	"CitrixResource": "内部"
	"CitrixプロビジョニングスキームID": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
カタログ内のVM	"CitrixResource": "内部"
	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx". プラグインは、MCSでプロビジョニングされたVMにこのラベルも追加します: "citrix-provisioning-scheme-id": "provSchemeId". このラベルを使用して、GCPコンソールでカタログ別にフィルタリングできます。
WBCディスク	"CitrixResource": "内部"
	CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"

注:

> MCSによって作成されたリソースとして識別するために**CitrixResource**タグが追加されている場合、VMはCitrixインベントリに表示されません。タグを削除または名前変更することで、表示させることができます。

詳細情報

- 接続とリソースの作成および管理
- Google Cloud環境への接続
- マシンカタログの作成
- Google Cloud Platform カタログを作成する
- マシンカタログの管理

HPE Moonshotカタログの管理

(/ja-jp/citrix-virtual-apps-desktops/2503/install-configure/machine-catalogs-manage.html)では、マシンカタログを管理するウィザードについて説明します。以下の情報は、HPE Moonshotカタログに固有の詳細を扱います。

> **注:**
>
> HPE Moonshotカタログを管理する前に、HPE Moonshotカタログの作成を完了する必要があります。

電源管理

Citrix Virtual Apps and Desktops™では、HPE Moonshotマシンの電源管理を行うことができます。電源管理したいマシンを見つけるには、ナビゲーションペインの**検索**ノードを使用します。以下の電源操作が利用可能です。

- 起動
- シャットダウン
- 強制シャットダウン
- 再起動
- リセット

> **注:**

一時停止および**再開**の電源操作はサポートされていません。

詳細情報

- 接続とリソースの作成および管理
- HPE Moonshotへの接続
- マシンカタログの作成
- HPE Moonshotマシンカタログの作成
- マシンカタログの管理

Microsoft Azureカタログを管理する

注:

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

マシンカタログの管理では、マシンカタログを管理するウィザードについて説明します。以下の情報は、Microsoft Azure Resource Managerクラウド環境に固有の詳細を扱います。

注:

Microsoft Azureカタログを管理する前に、Microsoft Azureカタログの作成を完了する必要があります。Microsoft Azureカタログの作成を参照してください。

VMのシャットダウン時にストレージタイプを下位層に変更する

VMをシャットダウンするときに、管理ディスクのストレージタイプを下位層に切り替えることで、ストレージコストを節約できます。これを行うには、`StorageTypeAtShutdown`カスタムプロパティを使用します。

VMをシャットダウンすると、ディスクのストレージタイプは下位層（`StorageTypeAtShutdown`カスタムプロパティで指定）に変更されます。VMの電源をオンにすると、ストレージタイプは元の状態（`StorageType`カスタムプロパティまたは`WBCDiskStorageType`カスタムプロパティで指定）に戻ります。

> **重要:**
>
> ディスクはVMが少なくとも一度電源オンになるまで存在しません。したがって、VMを最初に電源オンにしたときにストレージタイプを変更することはできません。

要件

- 管理ディスクに適用されます。これは、カスタムプロパティ`UseManagedDisks`をtrueに設定することを意味します。
- 永続OSディスクを持つ永続および非永続カタログに適用されます。これは、カスタムプロパティ`persistOsDisk`をtrueに設定することを意味します。
- 永続WBCディスクを持つ非永続カタログに適用されます。これは、カスタムプロパティ`persistWBC`をtrueに設定することを意味します。

制限

- Microsoftによると、ディスクの種類は1日2回しか変更できません。Microsoftドキュメントを参照してください。Citrixによると、VMの起動または割り当て解除アクションがあるたびに`StorageType`更新が行われます。したがって、VMあたりの電源アクションの数を1日2回に制限してください。たとえば、午前中にVMを起動するための電源アクションを1回、夕方にVMを割り当て解除するための電源アクションを1回行います。

ストレージの種類を下位層に変更する

手順に進む前に、要件と制限を参照してください。

1. カスタムプロパティ`StorageTypeAtShutdown`を追加し、値をStandard_LRS (HDD)に設定し、`New-ProvScheme`を使用してカタログを作成します。PowerShellを使用してカタログを作成する方法については、`<https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/>`を参照してください。

   > **注:**

`StorageTypeAtShutdown`が空またはStandard_LRS (HDD)以外の値を持つ場合、操作は失敗します。

永続カタログの作成中にカスタムプロパティを設定する例：

```
$customProperties='<CustomProperties xmlns="http://schemas.citrix.com/
2014/xd/machinecreation"

xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks"
Value="true" />

<Property xsi:type="StringProperty" Name="StorageType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="ResourceGroups" Value="" />

<Property xsi:type="StringProperty" Name="LicenseType"
Value="Windows_Client" />

<Property xsi:type="StringProperty" Name="SchemaVersion" Value="2" />

<Property xsi:type="StringProperty" Name="OsType" Value="Windows" />

<Property xsi:type="StringProperty" Name="StorageTypeAtShutdown"
Value="Standard_LRS" />

</CustomProperties>'
```

非永続カタログの作成中にカスタムプロパティを設定する例：

```
$customProperties='<CustomProperties xmlns="http://schemas.citrix.com/
2014/xd/machinecreation"

xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks"
Value="true" />

<Property xsi:type="StringProperty" Name="StorageType"
```

```
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="WbcDiskStorageType"
Value="Standard_SSD_LRS" />

<Property xsi:type="StringProperty" Name="ResourceGroups" Value="" />

<Property xsi:type="StringProperty" Name="LicenseType"
Value="Windows_Client" />

<Property xsi:type="StringProperty" Name="SchemaVersion" Value="2" />

<Property xsi:type="StringProperty" Name="OsType" Value="Windows" />

<Property xsi:type="BooleanProperty" Name="persistWBC" Value=true />

<Property xsi:type="BooleanProperty" Name="persistOsDisk" Value=true />

<Property xsi:type="StringProperty" Name="StorageTypeAtShutdown"
Value="Standard_LRS" />

</CustomProperties>'
```

注:

マシンプロファイルを使用する場合、カスタムプロパティは`MachineProfile`で定義されたプロパティよりも優先されます。

2. VMをシャットダウンし、AzureポータルでVMのストレージの種類を確認します。ディスクのストレージの種類は、`StorageTypeAtShutdown`カスタムプロパティで指定されたとおり、下位層に変更されます。
3. VMを起動します。ディスクのストレージの種類は、以下に記載されているストレージの種類に戻ります。
   - OSディスクの`StorageType`カスタムプロパティ
   - WBCディスクの`WBCDiskStorageType`カスタムプロパティ（`CustomProperties`で指定した場合のみ）。それ以外の場合は、`StorageType`に記載されているストレージの種類に戻ります。

既存のカタログに`StorageTypeAtShutdown`を適用する

手順を進める前に、要件と制限を参照してください。

既存のカタログにVMを追加するには、`Set-ProvScheme`を使用します。この機能は、`Set-ProvScheme`の実行後に追加された新しいVMに適用されます。既存のマシンには影響しません。

既存のカタログにVMを追加する際にカスタムプロパティを設定する例:

```
$customProperties='<CustomProperties xmlns="http://schemas.citrix.com/
2014/xd/machinecreation"

xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="StorageType"
Value="Premium_LRS" />

<Property xsi:type="StringProperty" Name="WbcDiskStorageType"
Value="Standard_SSD_LRS" />

<Property xsi:type="StringProperty" Name="ResourceGroups" Value="" />

<Property xsi:type="StringProperty" Name="LicenseType"
Value="Windows_Client" />

<Property xsi:type="StringProperty" Name="SchemaVersion" Value="2" />

<Property xsi:type="StringProperty" Name="OsType" Value="Windows" />

<Property xsi:type="BooleanProperty" Name="persistWBC" Value=true />

<Property xsi:type="BooleanProperty" Name="persistOsDisk" Value=true />

<Property xsi:type="StringProperty" Name="StorageTypeAtShutdown"
Value="Standard_LRS" />

</CustomProperties>'



$ProvScheme = Get-Provscheme -ProvisioningSchemeName $CatalogName
```

```
Set-ProvScheme -ProvisioningSchemeName $ProvScheme.ProvisioningSchemeName
-CustomProperties $customProperties
```

既存のVMのストレージタイプをシャットダウン時に下位層に変更する

手順を進める前に、要件と制限を参照してください。

VMがシャットダウンされたときに、既存のVMのストレージタイプを下位層に変更することで、ストレージコストを節約できます。これを行うには、`StorageTypeAtShutdown`カスタムプロパティを使用します。

VMがシャットダウンされたときに、カタログ内の既存のマシンのストレージタイプを下位層に変更するには:

1. PowerShellウィンドウを開きます。
2. Citrix固有のPowerShellモジュールをロードするために、`asnp citrix*`を実行します。
3. `Get-Provscheme -ProvisioningSchemeName $CatalogName`を実行します。
4. カスタムプロパティ文字列を変更します。

   ```
   $customProperties = '<CustomProperties xmlns="http://
   schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http://
   www.w3.org/2001/XMLSchema-instance">

   <Property xsi:type="StringProperty" Name="StorageTypeAtShutdown"
   Value="Standard_LRS" />

   </CustomProperties>'
   ```

5. 既存のカタログのプロビジョニングスキームを更新します。この更新は、`Set-ProvScheme`の実行後に追加された新しいVMに適用されます。

   ```
   Set-ProvScheme -ProvisioningSchemeName $CatalogName -CustomProperties
   $customProperties
   ```

6. 既存のVMを更新して`StorageTypeAtShutdown`を有効にします。

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName $CatalogName
-StartsNow -DurationInMinutes -1
```

7. 次回マシンを起動すると、マシンの`StorageTypeAtShutdown`プロパティが更新されます。ストレージタイプは次回のシャットダウン時に変更されます。
8. カタログ内の各VMの`StorageTypeAtShutdown`値を表示するには、次のコマンドを実行します。

```
Get-ProvVM -ProvisioningSchemeName <catalog-name> | foreach { $vmName =
$_.VMName; $storageTypeAtShutdown = ($_.CustomVmData | ConvertFrom-
Json).StorageTypeAtShutdown.DiskStorageAccountType; return New-Object
psobject -Property @{ "VMName" = $vmName; "StorageTypeAtShutdown" =
$storageTypeAtShutdown } }
```

プロビジョニングされたマシンを現在のプロビジョニングスキームの状態に更新する

`Set-ProvScheme`コマンドはプロビジョニングスキームを変更します。ただし、既存のマシンには影響しません。PowerShellコマンド`Set-ProvVMUpdateTimeWindow`を使用すると、現在のプロビジョニングスキームを既存の永続的または非永続的なマシン、またはマシンセットに適用できます。また、既存のMCSプロビジョニングされたマシンの構成更新のタイムスロットをスケジュールすることもできます。スケジュールされたタイムスロット中の電源オンまたは再起動は、スケジュールされたプロビジョニングスキームの更新をマシンに適用します。現在、Azureでは、`ServiceOffering`、`MachineProfile`、および次のカスタムプロパティを更新できます。

- `StorageType`
- `WBCDiskStorageType`
- `IdentityDiskStorageType`
- `LicenseType`
- `DedicatedHostGroupId`
- `PersistWBC`
- `PersistOsDisk`
- `PersistVm`

注:

- Azure環境でマネージドディスクを使用するカタログの場合、`StorageType`、`WBCDiskStorageType`、および`IdentityDiskStorageType`カスタムプロパティのみを更新できます。
- `Set-ProvVMUpdateTimeWindow`を2回実行した場合、最新のコマンドが有効になります。

更新できるもの:

- 単一のVM
- 特定のVMのリスト、またはプロビジョニングスキームIDに関連付けられている既存のすべてのVM
- 特定のVMのリスト、またはプロビジョニングスキーム名（マシンカタログ名）に関連付けられている既存のすべてのVM

プロビジョニングスキームに以下の変更を加えると、Azureの永続カタログの場合、VMインスタンスが再作成されます:

- `MachineProfile`を変更する
- 削除 `LicenseType`
- 削除 `DedicatedHostGroupId`

注:

既存のマシンのOSディスクとそのすべてのデータはそのまま残り、新しいVMがそのディスクに接続されます。

既存のVMを更新する前に:

1. 既存のマシンの構成を確認します。たとえば、,

```
Get-ProvScheme | select ProvisioningSchemeName,
ProvisioningSchemeVersion
```

2. プロビジョニングスキームを更新します。たとえば、,
   - マシンプロファイルの入力としてVMを使用する場合:

```
Set-ProvScheme -ProvisioningSchemeName "my-catalog" -MachineProfile
"XDHyp:\HostingUnits\<hosting-unit>\machineprofile.folder\<resource-
group>.resourcegroup\<virtual-machine>.vm"
```

- マシンプロファイルの入力としてテンプレート仕様を使用する場合:

```
Set-ProvScheme -ProvisioningSchemeName "my-catalog"

-MachineProfile "XDHyp:\HostingUnits\<hosting-
unit>\machineprofile.folder\<resource-
group>.resourcegroup\<template-spec>.templatespec\<template-spec-
version>.templatespecversion"

-ServiceOffering "XDHyp:\HostingUnits\<hosting-
unit>\serviceoffering.folder\<service-offering>.serviceoffering"
```

- サービス提供のみの場合:

```
Set-ProvScheme -ProvisioningSchemeName "my-catalog" -ServiceOffering
"XDHyp:\HostingUnits\<hosting-unit>\serviceoffering.folder\<service-
offering>.serviceoffering"
```

3. VMの現在のプロパティが現在のプロビジョニングスキームと一致しているか、およびVMに保留中の更新アクションがあるかを確認します。例えば、,

```
Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
ProvisioningSchemeVersion
```

特定のバージョンのマシンを見つけることもできます。例えば、,

```
Get-ProvVM -Filter "ProvisioningSchemeVersion -eq 1" | select VMName,
ProvisioningSchemeVersion
```

既存のマシンに次回の再起動時に適用される更新を要求するには:

1. 既存のマシンを更新し、次回の再起動時に更新を適用するには、以下のコマンドを実行します。

   - すべての既存のマシンを更新する場合。例：

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
-StartsNow -DurationInMinutes -1
```

- 特定のマシンのリストを更新する場合。例：

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
-VMName <List-Of-Vm-Names> -StartsNow -DurationInMinutes -1
```

- Get-ProvVMの出力に基づいてマシンを更新する場合。例：

```
Get-ProvVM -ProvisioningSchemeName "my-catalog" | Set-
ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog -StartsNow
-DurationInMinutes -1
```

注:

- `StartsNow` は、スケジュールされた開始時刻が現在の時刻であることを示します。
- 負の数（例：–1）を持つ `DurationInMinutes` は、スケジュールの時間枠に上限がないことを示します。

2. 更新がスケジュールされているマシンを見つける。例：

```
Get-ProvVM -Filter "ProvisioningSchemeUpdateAfter" | select VMName,
ProvisioningSchemeUpdateAfter
```

3. マシンを再起動します。次回の電源投入時に、プロパティの変更が既存のマシンに適用されます。以下のコマンドを使用して、更新されたステータスを確認できます。例：

```
Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
ProvisioningSchemeVersion
```

スケジュールされた時間枠内で次回起動時にVMが最新のプロビジョニング設定に更新されるようにスケジュールするには：

1. 以下のコマンドを実行します。

- 開始時刻を現在時刻として更新をスケジュールするには

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
-VMName vm1 -StartsNow -DurationInMinutes 120
```

- 週末に更新をスケジュールするには

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName “ my-catalog “
-VMName “vm1” -StartTimeInUTC “10/15/2022 9:00am” -DurationInMinutes
(New –TimeSpan –Days 2).TotalMinutes
```

注:

- `VMName` はオプションです。指定しない場合、更新はカタログ全体に対してスケジュールされます。
- `StartTimeInUTC` の代わりに `StartsNow` を使用して、スケジュール開始時刻が現在時刻であることを示します。
- `DurationInMinutes` はオプションです。デフォルトは120分です。負の数（例：–1）は、スケジュールの時間枠に上限がないことを示します。

2. 更新ステータスを確認します。

```
Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
ProvisioningSchemeUpdateUntil, ProvisioningSchemeVersion
```

3. VM の電源を入れます。スケジュールされた時間枠の後にマシンの電源を入れた場合、構成の更新は適用されません。スケジュールされた時間枠内にマシンの電源を入れた場合、,

- マシンの電源がオフの場合、かつ
  - マシンの電源を入れない場合、構成の更新は適用されません
  - マシンの電源を入れた場合、構成の更新が適用されます
- マシンの電源がオンの場合、かつ
  - マシンを再起動しない場合、構成の更新は適用されません

    - マシンを再起動した場合、構成の更新が適用されます

構成の更新をキャンセルするには：

単一のVM、複数のVM、またはカタログ全体の構成更新をキャンセルすることもできます。構成更新をキャンセルするには：

1. `Clear-ProvVMUpdateTimeWindow` を実行します。例:

    - 単一のVMにスケジュールされている構成の更新をキャンセルするには:

    ```
    Clear-ProvVMUpdateTimeWindow -ProvisioningSchemeName “ my-catalog “
    -VMName “vm1”
    ```

    - 複数のVMにスケジュールされている構成の更新をキャンセルするには:

    ```
    Clear-ProvVMUpdateTimeWindow -ProvisioningSchemeName "my-catalog"
    -VMName "vm1","vm2"
    ```

    > **注:**
    >
    > VM は同じカタログのものである必要があります。

個々のVMのプロパティを更新する

永続的なMCSマシンカタログ内の個々のVMのプロパティは、PowerShellコマンド `Set-ProvVM` を使用して更新できます。ただし、更新はすぐに適用されません。更新を適用するには、PowerShellコマンド `Set-ProvVMUpdateTimeWindow` を使用して時間枠を設定する必要があります。

この実装により、マシンカタログ全体を更新することなく、個々のVMを効率的に管理できます。現在、この機能はAzure環境でのみ適用可能です。

現在、更新できるプロパティは次のとおりです:

- `CustomProperties`
- `ServiceOffering`
- `MachineProfile`

この機能を使用すると、次のことができます:

- VMのプロパティを更新する
- マシンカタログが更新された後も、VMで更新されたプロパティを保持する
- VMに適用された構成の更新を元に戻す

VMのプロパティを更新する前に：

1. **PowerShell**ウィンドウを開きます。
2. `asnp citrix*`を実行して、Citrix固有のPowerShellモジュールをロードします。
3. 既存のマシンカタログの構成を確認します。例:

```
Get-ProvScheme -ProvisioningSchemeName AzureCatalog
```

4. 更新を適用するVMの構成を確認します。例:

```
Get-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
```

VMのプロパティを更新する

VMのプロパティを更新するには、次の手順を実行します:

1. 更新を適用するVMの電源を切ります。
2. VMのプロパティを更新します。たとえば、VMのストレージタイプ (`StorageType`) カスタムプロパティを更新する場合は、次を実行します:

```
Set-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
-CustomProperties "...<Property Name='StorageType'
Value='Premium_LRS' />..."
```

マシンカタログ内の2つのVMのプロパティを同時に更新できます。例:

```
Set-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
-CustomProperties "...<Property Name='StorageType'
Value='Premium_LRS' />..."
```

```
Set-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine2
-CustomProperties "...<Property Name='StorageType'
Value='StandardSSD_LRS' />..."
```

> **注:**
>
> 更新はすぐに適用されません。

3. 更新対象として指定されたプロパティのリストと構成バージョンを取得します。例:

```
Get-ProvVMConfiguration -ProvisioningSchemeName AzureCatalog -VMName
machine1
```

`Version`のプロパティ値と、更新するプロパティ (この場合は`StorageType`) を確認します。

4. 設定バージョンを確認します。例：

```
Get-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
```

`ProvVMConfigurationVersion` のプロパティ値を確認します。更新はまだ適用されていません。VM はまだ古い構成のままです。

5. スケジュールされた更新を要求します。例：

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName AzureCatalog
-StartsNow -DurationInMinutes -1
```

スケジュールされた更新の詳細については、プロビジョニングされたマシンを現在のプロビジョニングスキームの状態に更新する を参照してください。

> **注：**
>
> 保留中のプロビジョニングスキームの更新も適用されます。

6. VM を再起動します。例：

```
New-BrokerHostingPowerAction -MachineName machine1 -Action TurnOn
```

7. 設定バージョンを確認します。例：

```
Get-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
```

`ProvVMConfigurationVersion` のプロパティ値を確認します。更新が適用されました。VMは新しい構成になりました。

8. VMにさらに構成アップデートを適用するには、VMをオフにして、手順を繰り返します。

マシンカタログの更新後にVMで更新されたプロパティを保持する

VMで更新されたプロパティを保持するには、以下を実行します。

1. 更新を適用したいVMの電源をオフにします。
2. マシンカタログを更新します。たとえば、VMサイズ (`ServiceOffering`) とストレージタイプ (`StorageType`) を変更したい場合は、以下を実行します。

```
Set-ProvScheme -ProvisioningSchemeName AzureCatalog -ServiceOffering
Standard_E4_v3 -CustomProperties "...<Property Name='StorageType'
Value='StandardSSD_LRS' />..."
```

3. マシンカタログの構成詳細を取得します。例：

```
Get-ProvScheme -ProvisioningSchemeName AzureCatalog
```

`ProvisioningSchemeVersion` は1つ増えます。VMサイズとストレージタイプも更新されます。

4. VMのプロパティを更新します。たとえば、マシンプロファイルをVMに提供します。

```
Set-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
-MachineProfile "XDHyp:\HostingUnits\<hosting-
unit>\machineprofile.folder\<resource-group>.resourcegroup\<template-
spec>.templatespec\<template-spec-version>.templatespecversion"
```

注:

マシンプロファイルの入力には、タグと異なるVMサイズ（ `ServiceOffering` ）が指定されています。

5. VM上の構成更新とマシンカタログ更新をマージした後、VMが持つプロパティのリストを取得します。例：

```
Get-ProvVMConfigurationResultantSet -ProvisioningSchemeName
AzureCatalog -VMName machine1
```

> **注:**
>
> VMに対するすべてのアップデートは、マシンカタログで行われたアップデートを上書きします。

6. VMのスケジュールされたアップデートを要求します。例:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName AzureCatalog -VMName
machine1 -StartsNow -DurationInMinutes -1
```

7. VMを再起動します。例:

```
New-BrokerHostingPowerAction -MachineName machine1 -Action TurnOn
```

   VMは、マシンプロファイルから派生した更新済みのVMサイズを保持します。マシンプロファイルで指定されたタグ値もVMに適用されます。ただし、ストレージタイプは最新のプロビジョニングスキームから派生します。

8. VMの構成バージョンを取得します。例:

```
Get-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
```

   `ProvisioningSchemeVersion`と`ProvVMConfigurationVersion`に最新バージョンが表示されます。

VMに適用された構成の更新を元に戻す

1. VMに更新を適用した後、VMをシャットダウンします。
2. 次のコマンドを実行して、VMに適用された更新を削除します。例:

```
Set-ProvVM -RevertToProvSchemeConfiguration -ProvisioningSchemeName
AzureCatalog -VMName machine1
```

3. VMのスケジュールされた更新を要求します。例：

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName AzureCatalog -VMName
machine1 -StartsNow -DurationInMinutes -1
```

4. VMを再起動します。例：

```
New-BrokerHostingPowerAction -MachineName machine1 -Action TurnOn
```

5. VMの構成バージョンを確認します。例：

```
Get-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
```

`ProvVMConfigurationVersion` の値が、マシンカタログの構成バージョンになります。

ディスク暗号化の変更

Azure仮想化環境でディスク暗号化を変更し、次の操作を実行できます。

- マスターイメージのDESとは異なるディスク暗号化セット（DES）を使用してMCSマシンカタログを作成するには、`New-ProvScheme` コマンドを使用します。例：

```
$customProperties = @"

<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="DiskEncryptionSetId" Name="Zones" Value="/
subscriptions/XXXXXXXXXXXXXXXXXXXXXXXXXXXX/resourceGroups/testrsg/
providers/Microsoft.Compute/diskEncryptionSets/test-diskEncryptionSet"/
>

</CustomProperties>

"@

New-ProvScheme -CleanOnBoot `
```

```
-ProvisioningSchemeName $provisioningSchemeName `

-HostingUnitName $hostingUnitName `

-IdentityPoolName $identityPoolName `

-InitialBatchSizeHint $numberOfVms `

-masterImagePath $masterImagePath `

-NetworkMapping $networkMapping `

-CustomProperties $customProperties
```

- `Set-ProvScheme` および `Set-ProvVMUpdateTimeWindow` コマンドを使用して、既存のMCSマシンカタログと既存のVMのディスク暗号化タイプを、あるDESキーから別のDESキーに変更します。VMを再起動すると、更新されたDESキーが表示されます。例：

```
$customProperties = '<CustomProperties xmlns="http://
schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="DiskEncryptionSetId" Value="/
subscriptions/456c683e2ed7/resourceGroups/testrg/providers/
Microsoft.Compute/diskEncryptionSets/diskEncryptionSet1" />

</CustomProperties>'

Set-ProvScheme -ProvisioningSchemeName azure-catalog -CustomProperties
$customProperties

Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName azure-catalog
-VMName azu01, azu02 -StartsNow -DurationInMinutes -1
```

- 以前にCMEKが有効になっていなかったMCSマシンカタログとVMを、`Set-ProvScheme` および `Set-ProvVMUpdateTimeWindow` コマンドを使用して、顧客管理の暗号化キー（CMEK）暗号化（DES）、ホストでのディスク暗号化、または二重暗号化を持つように更新します。異なる暗号化タイプについては、Azure server side encryption、Azure disk encryption at host、および Double encryption on managed disk を参照してください。

- `Set-ProvScheme` および `Set-ProvVMUpdateTimeWindow` コマンドを使用して、以前に暗号化されていた既存のMCSマシンカタログとVMを非暗号化に更新します。例：

```
$customProperties = '<CustomProperties xmlns="http://
schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
Value="" />

</CustomProperties>'

Set-ProvScheme -ProvisioningSchemeName azure-catalog -CustomProperties
$customProperties

Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName azure-catalog
-VMName azu01, azu02 -StartsNow -DurationInMinutes -1
```

- プライベートエンドポイントを使用したディスク暗号化を有効にします（`ProxyHypervisorTrafficThroughConnector` で有効化されたホスト接続を使用したMCSマシンカタログ）。プライベートエンドポイントを使用したディスク暗号化を有効にする方法については、Enable disk encryption with private endpoint を参照してください。

プライベートエンドポイントを使用したディスク暗号化を有効にする

Azureの制限により、現在、プライベートエンドポイントに対して顧客管理キーによるサーバー側暗号化を使用することはできません。ただし、既存のMCSマシンカタログとプライベートエンドポイントを持つVMをDESキーで暗号化するように更新することはできます。

プライベートエンドポイントを持つ既存のマシンカタログを更新する

プライベートエンドポイントを持つ既存のマシンカタログを更新する詳細な手順は次のとおりです。

1. `ProxyHypervisorTrafficThroughConnector` を介してディスク暗号化なしでカタログを作成します。
2. `DiskEncryptionSetId` を使用してカタログを更新するには、`Set-ProvScheme` を実行します。

> **注:**

> `DiskEcryptionSetId` は `CustomProperties` または `MachineProfile` を介して構成できます。`CustomProperties` と `MachineProfile` の両方で定義されている場合、`CustomProperties` で定義されたプロパティが適用されます。

> `CustomProperties` を使用する場合の例:

```
$customProperties = '<CustomProperties xmlns="http://
schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="DiskEncryptionSetId" Value="/
subscriptions/456c683e2ed7/resourceGroups/testrg/providers/
Microsoft.Compute/diskEncryptionSets/diskEncryptionSet1"/>

</CustomProperties>'

Set-ProvScheme -ProvisioningSchemeName azure-catalog -CustomProperties
$customProperties
```

MachineProfileを使用する場合の例: ディスク暗号化が有効なVM、またはディスク暗号化設定を持つテンプレート仕様を使用します。

```
Set-ProvScheme -ProvisioningSchemeName azure-catalog -MachineProfile
"XDHyp:
\HostingUnits\azureunit\machineprofile.folder\testrg.resourcegroup\new-
template.vm"
```

または、Web Studioを使用してマシンプロファイルを更新することもできます。

3. 既存のカタログVMを更新するには、`Set-ProvVMUpdateTimeWindow` を実行します。例:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName azure-catalog
-VMName azu01, azu02 -StartsNow -DurationInMinutes -1
```

4. VM を再起動すると、Azure portal の VM のディスクで更新されたディスク暗号化を確認できます。
5. 新しいカタログ VM を追加する前にディスク暗号化を解除するには、`Set-ProvScheme` を実行します。

> **注:**
>
> プライベートエンドポイントカタログを更新しているため、この手順が必要です。この手順を実行しないと、新しいVMをカタログに追加しようとしたときにエラーが発生します。
>
> 例:

```
$customProperties = '<CustomProperties xmlns="http://
schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
Value="" />

</CustomProperties>'

Set-ProvScheme -ProvisioningSchemeName azure-catalog -CustomProperties
$customProperties
```

6. カタログに新しい VM を追加します。

個々のカタログ VM を更新する

個々のカタログ VM を更新する詳細な手順は次のとおりです。

1. `ProxyHypervisorTrafficThroughConnector`を介してディスク暗号化なしでカタログを作成します。
2. `DiskEncryptionSetId` を使用してカタログ VM を更新するには、`Set-ProvVM` を実行します。

> **注:**
>
> The `DiskEcryptionSetId` は、`CustomProperties` または `MachineProfile` のいずれかを使用して構成できます。
>
> `CustomProperties` を使用する場合の例:

```
$customProperties = '<CustomProperties xmlns="http://
schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="DiskEncryptionSetId" Value="/
subscriptions/456c683e2ed7/resourceGroups/testrg/providers/
Microsoft.Compute/diskEncryptionSets/diskEncryptionSet1" />

</CustomProperties>'

Set-ProvVM -ProvisioningSchemeName azure-catalog  -VMName azu01
-CustomProperties $customProperties
```

MachineProfile を使用する場合の例:

```
Set-ProvVM -ProvisioningSchemeName azure-catalog  -VMName azu01
-MachineProfile "XDHyp:
\HostingUnits\azureunit\machineprofile.folder\testrg.resourcegroup\new-
template.vm"
```

3. 既存のカタログVMを更新するには、`Set-ProvVMUpdateTimeWindow` を実行します。例:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName azure-catalog
-VMName azu01 -StartsNow -DurationInMinutes -1
```

4. VM を再起動すると、Azure portal の VM ディスクで更新されたディスク暗号化を確認できます。
5. 新しいVMをカタログに追加します。

既存のカタログのWBCディスクとして一時ディスクを使用する

既存のMCSマシンカタログのライトバックキャッシュディスク（WBC）ディスクとしてAzure一時ディスクを使用できます。既存のカタログとVMを更新するには、`Set-ProvScheme` PowerShellコマンドを使用します。

前提条件

既存のカタログは、次の条件を満たしている必要があります。

> **注:**

既存のカタログが次の要件を満たしていない場合、WBCディスクは一時ディスク内に配置されません。

- MCSIOが有効になっている: カスタムプロパティ `WriteBackCacheMemorySize`、`WriteBackCacheDiskSize`、および `UseWriteBackCache` が有効になっています。
- エフェメラルOSディスクが有効になっていない。
- WBCは非永続的である: `PersistWBC` は `false` です。
- `UseTempDiskForWBC` はnullまたはfalseです。
- 一時ディスクのサイズは、（ライトバックキャッシュディスクサイズ + ページングファイル用の予約済みスペース + 1 GBのバッファースペース）の合計サイズよりも大きくする必要があります。

重要:

一時ディスクを持つサービスオファリングから持たないサービスオファリングへの変更、またはその逆は許可されていません。

既存のカタログを更新する

既存のカタログを更新するには、次のコマンドを実行します。

1. 既存のカタログで `Set-ProvScheme` を実行して、`UseTempDiskForWBC` を `true` に更新します。例:

```
Set-ProvScheme -ProvisioningSchemeName name -CustomProperties
"<CustomProperties xmlns=`"http://schemas.citrix.com/2014/xd/
machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`"><Property xsi:type=`"StringProperty`"
Name=`"StorageAccountType`" Value=`"Standard_LRS`"/><Property
xsi:type=`"StringProperty`" Name=`"UseManagedDisks`" Value=`"True`"/
><Property xsi:type=`"StringProperty`" Name=`"ManagedDisksPreview`"
Value=`"False`"/><Property xsi:type=`"StringProperty`"
Name=`"PersistOsDisk`" Value=`"False`"/><Property
xsi:type=`"StringProperty`" Name=`"UseTempDiskForWBC`" Value=`"True`"/
><Property xsi:type=`"StringProperty`" Name=`"PersistWBC`"
Value=`"False`"/></CustomProperties>"
```

2. カタログに新しいマシンを追加して電源を入れます。新しい VM には、一時ディスク内に WBC ディスクがあります。

Azure VM、スナップショット、OS ディスク、およびギャラリーイメージ定義の情報を取得する

Azure VMの情報を表示できます。これには、OSディスクとタイプ、スナップショット、ギャラリーイメージ定義が含まれます。この情報は、マシンカタログが割り当てられたときにマスターイメージ上のリソースに対して表示されます。この機能を使用して、LinuxまたはWindowsイメージを表示および選択できます。PowerShellプロパティ`TemplateIsWindowsTemplate`が`AdditionDatafield`パラメーターに追加されました。このフィールドには、Azure固有の情報（VMタイプ、OSディスク、ギャラリーイメージ情報、OSタイプ情報）が含まれます。`TemplateIsWindowsTemplate`を**True**に設定するとOSタイプがWindowsであることを示し、`TemplateIsWindowsTemplate`を**False**に設定するとOSタイプがLinuxであることを示します。

> **ヒント:**
>
> `TemplateIsWindowsTemplate` PowerShellプロパティによって表示される情報は、Azure APIから取得されます。このフィールドが空の場合があります。たとえば、データディスクからのスナップショットには、OSタイプがスナップショットから取得できないため、`TemplateIsWindowsTemplate`フィールドが含まれていません。

> たとえば、PowerShell を使用して、Windows OS の種類に対して Azure VM `AdditionData` パラメーターを **True** に設定します。

```
PS C:\Users\username> (get-item XDHyp:
\HostingUnits\mynetwork\image.folder\username-dev-testing-
rg.resourcegroup\username-dev-tsvda.vm).AdditionalData

Key Value

ServiceOfferingDescription Standard_B2ms

HardDiskSizeGB 127

ResourceGroupName FENGHUAJ-DEV-TESTING-RG

ServiceOfferingMemory 8192
```

```
ServiceOfferingCores 2

TemplateIsWindowsTemplate True

ServiceOfferingWithTemporaryDiskSizeInMb 16384

SupportedMachineGenerations Gen1,Gen2
```

MCSによって作成されたリソースを識別する

以下は、MCSがリソースに追加するタグです。表のタグは「"key":"value"」として表されます。

リソース名	タグ
ID ディスク	"CitrixプロビジョニングスキームID" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	"CitrixResource" : "内部"
イメージ	"CitrixプロビジョニングスキームID" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	"CitrixResource" : "内部"
NIC	"CitrixProvisioningSchemeId" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	"CitrixResource" : "内部"
OSディスク	"CitrixProvisioningSchemeId" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	"CitrixResource" : "内部"
PrepVM	"CitrixプロビジョニングスキームID" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	"CitrixResource" : "内部"
公開スナップショット	"CitrixプロビジョニングスキームID" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	"CitrixResource" : "内部"

リソース名	タグ
リソースグループ	"CitrixResource" : "内部"
	CitrixSchemaVersion: 2.0
	"CitrixプロビジョニングスキームID" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
ストレージアカウント	"CitrixプロビジョニングスキームID" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	"CitrixResource" : "内部"
カタログ内のVM	"CitrixProvisioningSchemeId" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	"CitrixResource" : "内部"
WBCディスク	"CitrixProvisioningSchemeId" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	"CitrixResource" : "内部"

注:

MCSによって作成されたリソースとして識別するために**CitrixResource**タグが追加されている場合、VMはCitrixインベントリに表示されません。タグを削除または名前変更することで、表示させることができます。

タグを削除する

カタログまたはVMを作成すると、以下のリソースにタグが作成されます。

- リソースグループ
- 仮想マシン
- OSディスク
- 識別ディスク
- ネットワークインターフェイス

- ストレージアカウント

CitrixデータベースからVMとマシンカタログを削除し、タグを削除できます。次のものを使用できます。

- マシンカタログから単一のVMまたはVMのリストからVMとタグを削除するには、`ForgetVM` パラメーターを指定して`Remove-ProvVM`を使用します。
- Citrixデータベースからマシンカタログを削除し、マシンカタログ全体からタグを削除するには、`ForgetVM`パラメーターを指定して`Remove-ProvScheme`を使用します。

この機能は、永続VMにのみ適用されます。

これを行うには：

1. **PowerShell**ウィンドウを開きます。
2. Citrix固有のPowerShellモジュールをロードするには、**asnp citrix***を実行します。
3. CitrixデータベースからVMを削除し、VMからタグを削除するには、`Remove-ProvVM`を実行します。 例：

   ```
   Remove-ProvVM -ProvisioningSchemeName “ProvisioningSchemeName” -VMName “vmname” -ForgetVM
   ```

4. Citrixデータベースからマシンカタログを削除し、マシンカタログからタグを削除するには、`Remove-ProvScheme`を実行します。例：

   ```
   Remove-ProvScheme -ProvisioningSchemeName “ProvisioningSchemeName” -ForgetVM
   ```

   注:

   `Remove-ProvScheme`で`ForgetVM`パラメーターを使用すると、プロビジョニングスキームがBYORG（bring your own resource group）またはCitrix管理のリソースグループのいずれかに存在する場合、MCSはベースディスクスナップショットを含むすべてのスナップショットを削除します。

詳細情報

- 接続とリソースの作成および管理

- Microsoft Azureへの接続(/ja-jp/citrix-virtual-apps-desktops/2503/install-configure/connections/connection-azure-resource-manager.html)
- マシンカタログの作成(/ja-jp/citrix-virtual-apps-desktops/2503/install-configure/machine-catalogs-create.html)
- Microsoft Azureカタログの作成(/ja-jp/citrix-virtual-apps-desktops/2503/install-configure/machine-catalogs-create/create-machine-catalog-citrix-azure.html)
- マシンカタログの管理(/ja-jp/citrix-virtual-apps-desktops/2503/install-configure/machine-catalogs-manage.html)

Microsoft System Center Virtual Machine Manager カタログを管理する

マシンカタログの管理(/ja-jp/citrix-virtual-apps-desktops/2503/install-configure/machine-catalogs-manage.html)では、マシンカタログを管理するウィザードについて説明します。以下の情報は、Microsoft System Center Virtual Machine Manager (VMM) 仮想化環境に固有の詳細を扱います。

> **注:**
>
> VMMカタログを管理する前に、VMMカタログの作成を完了する必要があります。「Microsoft System Center Virtual Machine Managerカタログの作成(/ja-jp/citrix-virtual-apps-desktops/2503/install-configure/machine-catalogs-create/create-machine-catalog-mscvmm.html)」を参照してください。

MCSによって作成されたリソースを識別する

以下は、MCSがリソースに追加するタグです。表のタグは「"key":"value"」として表されます。

リソース名	タグ
準備VM	タグとして使用される文字列は: "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	カスタムプロパティエントリ: "XdConfig:"XdProvisioned=True"
カタログ内のVM	タグとして使用される文字列は: "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"

リソース名	タグ
	カスタムプロパティエントリ: "XdConfig:"XdProvisioned=True"

詳細情報

- 接続とリソースを作成および管理する(/ja-jp/citrix-virtual-apps-desktops/2503/install-configure/connections.html)
- Microsoft System Center バーチャル マシン マネージャー への接続
- マシンカタログを作成する(/ja-jp/citrix-virtual-apps-desktops/2503/install-configure/machine-catalogs-create.html)
- Microsoft System Center Virtual Machine Managerカタログを作成する(/ja-jp/citrix-virtual-apps-desktops/2503/install-configure/machine-catalogs-create/create-machine-catalog-mscvmm.html)
- マシンカタログを管理する(/ja-jp/citrix-virtual-apps-desktops/2503/install-configure/machine-catalogs-manage.html)

VMwareカタログの管理

マシンカタログの管理では、マシンカタログを管理するウィザードについて説明します。以下の情報は、VMware仮想化環境に固有の詳細を扱っています。

> **注:**
>
> VMwareカタログを管理する前に、VMwareカタログの作成を完了する必要があります。「VMwareカタログを作成する」を参照してください。

マシンカタログのフォルダーIDを更新する

MCSマシンカタログのフォルダーIDは、`Set-ProvScheme` コマンドのカスタムプロパティで `FolderId` を指定することで更新できます。フォルダーIDの更新後に作成されたVMは、この新しいフォルダーIDの下に作成されます。このプロパティが `CustomProperties` で指定されていない場合、VMはマスターイメージが配置されているフォルダーの下に作成されます。

マシンカタログのフォルダーIDを更新するには、次の手順を実行します。

1. Webブラウザーを開き、**vSphere Web Client**のURLを入力します。

2. 資格情報を入力し、**ログイン**をクリックします。
3. **vSphere Web Client**でVM配置フォルダーを作成します。
4. PowerShellウィンドウを開きます。
5. **asnp citrix®***を実行して、Citrix固有のPowerShellモジュールをロードします。
6. `Set-ProvScheme`の`CustomProperties`で`FolderID`を指定します。この例では、フォルダーIDの値は`group-v2406`です。

```
Set-ProvScheme -ProvisioningSchemeUid
"50bb319c-2e83-4a37-9ea1-94f630687372" -CustomProperties
"<CustomProperties xmlns=""http://schemas.citrix.com/2014/xd/
machinecreation"" xmlns:xsi=""http://www.w3.org/2001/XMLSchema-
instance""><Property xsi:type=""StringProperty"" Name=""FolderId""
Value=""group-v2406"" /></CustomProperties>"
```

7. Studioを使用してマシンカタログにVMを追加します。
8. vSphere Web Clientで新しいVMを確認します。新しいVMは新しいフォルダーの下に作成されます。

vSphereでフォルダーIDを見つける

任意のESXiまたはvCenterサーバーシステムでManaged Object Browser (MOB)にアクセスし、VMのフォルダーIDを見つけます。

MOBは、すべてのESX/ESXiおよびvCenterサーバーシステムに組み込まれているWebベースのサーバーアプリケーションです。このvSphereユーティリティを使用すると、VM、データストア、リソースプールなどのオブジェクトに関する詳細情報を表示できます。

1. Webブラウザーを開き、`http://x.x.x.x/mob`を入力します。ここで、x.x.x.xはvCenter ServerまたはESX/ESXiホストのIPアドレスです。例: `<https://10.60.4.70/mob>`。
2. MOBの**Home**ページで、**content**プロパティの値をクリックします。
3. **rootFolder**の値をクリックします。
4. **childEntity**の値をクリックします。
5. **vmFolder**の値をクリックします。
6. **childEntity**の値の中にフォルダーIDを見つけることができます。

MCSによって作成されたリソースを識別する

以下は、MCSがリソースに追加するタグです。表のタグは「"key":"value"」として表されます。

リソース名	タグ
準備VM	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	"XdConfig:"XdProvisioned=True"
カタログ内のVM	"Citrixプロビジョニングスキーム ID": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
	"Xd構成":"Xdプロビジョニング済み=True"

詳細情報

- 接続とリソースの作成および管理
- VMwareへの接続
- マシンカタログの作成
- VMwareカタログを作成する
- マシンカタログの管理

電源管理

Citrix Virtual Apps and Desktops™ を使用すると、さまざまなサポート対象のハイパーバイザーやクラウドサービスで、MCSプロビジョニングされたVMの電源を管理できます。電源管理操作により、以下が提供されます。

- 最適なユーザーエクスペリエンス
- コスト管理と電力節約

利用可能な電源操作は次のとおりです。

- 起動
- シャットダウン
- 再起動
- 一時停止
- 再開
- 強制再起動
- 強制シャットダウン

注:

- 非永続VMの場合、電源サイクル（シャットダウン/起動および再起動）によりOSディスクがリセットされます。
- 電源操作の機能と動作は、ハイパーバイザーまたはクラウドサービスによって異なります。

この記事では、特定のサポートされているハイパーバイザーに関連する主要な電源管理機能について説明します。

- AWS VMの電源管理
- Azure VMの電源管理

AWS VM の電源管理

必要な権限については、「必要なAWS権限」を参照してください。

インスタンスの休止

休止プロセスは、インスタンスのインメモリ状態と、プライベート IP アドレスおよび Elastic IP アドレスを保存し、中断したところから正確に再開できるようにします。

インスタンスに休止が指示されると、インメモリ状態をルート EBS ボリューム内のファイルに書き込み、その後シャットダウンします。Amazon EBS ボリュームは、インスタンスにアタッチできる耐久性のあるブロックレベルストレージデバイスです。ボリュームをインスタンスにアタッチすると、物理ハードドライブと同じように使用できます。インスタンスのルート EBS ボリュームを暗号化します。暗号化により、メモリから EBS ボリュームにコピーされる機密データが適切に保護されます。EBS 暗号化の詳細については、「Amazon EBS 暗号化」を参照してください。

サポートされているインスタンスの休止には、次の制限があります。

- 最大 150 GB までのインスタンスメモリ (RAM) のみがサポートされます
- UEFI ブートモードはサポートされていません
- 汎用 SSD とプロビジョンド IOPS SSD のみが EBS ボリュームタイプとしてサポートされます。

休止をサポートする VM の作成

休止をサポートする VM を作成するには：

1. ホスト接続を作成します。「AWS への接続」を参照してください。
2. EBSルートが暗号化され、**Stop-Hibernate**プロパティが有効になっているインスタンスを起動します。インスタンスの起動方法、ルートEBSボリュームの暗号化、および休止状態の有効化の詳細については、`<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/launching-instance.html/>`を参照してください。このインスタンスをマスターイメージとして使用してAMIを作成します。
3. マスターイメージを準備します。

   a. マスターイメージに VDA をインストールします。Citrix では、最新機能にアクセスできるように、最新バージョンをインストールすることをお勧めします。マスターイメージに VDA をインストールしないと、カタログ作成が失敗します。VDA のインストール方法の詳細については、「VDA のインストール」を参照してください。

   b. マスターイメージを、アプリケーションとデスクトップが属するドメインに参加させます。マスターイメージが、マシンが作成されるホストで利用可能であることを確認してください。

4. そのインスタンスから AMI を作成します。インスタンスから AMI を作成する方法については、「Amazon EC2 インスタンスから AMI を作成する」を参照してください。
5. `New-ProvScheme`コマンドを使用してマシンカタログを作成します。`AwsCaptureInstanceProperties`カスタムプロパティを**True**に設定します。Web StudioでAWSインスタンスプロパティを有効にする方法については、「**Web StudioでのAWSインスタンスプロパティの適用と運用リソースのタグ付け**」を参照してください。

```
New-ProvScheme  -AdminAddress "xxx" -CleanOnBoot

-CustomProperties "AwsCaptureInstanceProperties,true;"

-HostingUnitName "xxx" -IdentityPoolName $catalog_name
-InitialBatchSizeHint 1

-MasterImageVM "xyz.template" -NetworkMapping @{"0"="XDHyp:
\HostingUnits\MyConn\\us-east-2a.availabilityzone\10.0.0.0``/24
(vpc-0f1771e45671aedcd).network"}

-ProvisioningSchemeName $catalog_name

-RunAsynchronously -Scope @() -SecurityGroup @("xxx") -ServiceOffering
"xxx"
```

PowerShell コマンドを使用してマシンカタログを作成する方法については、`<https://developer-docs.citrix.com/projects/citrix-daas-sdk/en/latest/>` を参照してください。

ハイバネート可能な VM は、次の場合に作成されます。

- **Stop-Hibernate** プロパティが有効になっているマスターイメージから作成された AMI を選択した場合。
- マスター VM がドメインに参加しており、VDA がインストールされている場合。
- 休止状態を処理できる正しいVMサイズ（サービス提供）を選択します。

次の場合、**New-ProvScheme**コマンドは適切なエラーメッセージを表示して失敗します。

- マスターVMが休止状態を有効にしているが、サービスオファリングが休止状態を処理できない場合。
- マスターVMがドメインに参加しておらず、VDAがインストールされていない場合。

サービス提供とAMIの休止状態

サービス提供とAMI（テンプレート）の休止状態を取得するには、次のコマンドを実行します。

- `Get-HypConfigurationObjectForItem 'XDHyp:\HostingUnits\MyConn\WIN2016-ADDC-2021.09.10.145334-a1968709-10c4-47d5-9642-21e743159a7b (ami-0e6c5b33a52d2a6b6).template'`
- `Get-HypConfigurationObjectForItem 'XDHyp:\HostingUnits\MyConn\R6i Sixteen Extra Large Instance.serviceoffering'`

既存の休止状態対応プロビジョニングスキームのサービス提供を更新する

1. `Set-ProvScheme`コマンドを実行します。例：

```
Set-ProvScheme -ProvisioningSchemeName <String> -ServiceOffering
<String>
```

サービス提供に互換性がない場合、システムは例外メッセージを表示します。

休止状態をサポートするマシンカタログを作成する

マシンカタログを作成する際、休止状態をサポートするマシンプロファイルを使用できます。

1. カタログ作成ウィザードで、マシンプロファイルの選択まで指示に従います。

2. **マシンテンプレート**ページで、**マシンプロファイルの選択**をクリックし、マシンプロファイルを選択します。
3. 「**仮想マシン**」ページで、「**編集**」アイコンをクリックし、VMを選択します。

> **注:**
>
> マシンプロファイルでハイバネーションが有効になっている場合、システムはハイバネーション可能なVMのみを表示します。

4. 画面の指示に従ってすべての設定を完了します。「**概要**」ページにカタログの休止状態が表示されます。

> **注:**
>
> マシンカタログの編集で、マシンプロファイルを休止状態が有効なものに変更すると、それに応じてVMを再構成するように求められます。

休止状態をサポートするマシンカタログを更新する

既存のマシンカタログを休止状態をサポートしないマシンカタログで更新しようとすると、適切なエラーメッセージが表示されて更新が失敗します。

休止状態のVMの電源管理

休止状態のVMに対して、以下の電源管理操作を実行できます。

1. 実行状態からVMを一時停止する。
2. 一時停止状態からVMを再開する。
3. 一時停止状態からVMを再起動する。

Azure VM の電源管理

必要な権限については、「必要なAzure権限」を参照してください。

Azure オンデマンドプロビジョニング

Azure オンデマンドプロビジョニングでは、プロビジョニングが完了した後、Citrix Virtual Apps and Desktops™ が電源オンアクションを開始した場合にのみ VM が作成されます。

MCS を使用して Azure Resource Manager でマシンカタログを作成する場合、Azure オンデマンドプロビジョニング機能は次のことを行います。

- ストレージコストを削減します
- カタログ作成を高速化します

MCS カタログを作成すると、Azure portal にリソースグループ内のネットワークセキュリティグループ、ネットワークインターフェイス、ベースイメージ、およびIDディスクが表示されます。

Azure portal には、Citrix Virtual Apps and Desktops が電源オンアクションを開始するまで VM は表示されません。マシンには次の違いを持つ2つのタイプがあります。

- プールされたマシンの場合、オペレーティングシステムディスクとライトバックキャッシュは、VM が存在する場合にのみ存在します。コンソールでプールされたマシンをシャットダウンすると、Azure portal に VM は表示されません。定期的にマシンをシャットダウンする場合（たとえば、営業時間外）、ストレージコストを大幅に節約できます。
- 専用マシンの場合、オペレーティングシステムディスクは VM が最初に電源オンされたときに作成されます。Azure portal の VM は、マシンIDが削除されるまでストレージに残ります。コンソールで専用マシンをシャットダウンしても、Azure portal に VM は引き続き表示されます。

> **注：**

> オンデマンドプロビジョニング機能の前に作成されたAzureカタログ（「レガシー」カタログ）のサポートは非推奨です。したがって、Azureレガシーカタログ VMを再作成してください。カタログはオンデマンドとしてプロビジョニングされ、ストレージコストを節約できます。

電源サイクル時にプロビジョニングされた仮想マシンを保持する

電源サイクル時にプロビジョニングされた仮想マシンを保持するかどうかを選択します。PowerShell パラメーター `New-ProvScheme CustomProperties` を使用します。このパラメーターは、プロビジョニングされた仮想マシンが電源サイクル時に永続化するかどうかを決定するために使用される追加のプロパティ `PersistVm` をサポートします。電源オフ時に仮想マシンを永続化するには `PersistVm` プロパティを **true** に設定し、電源オフ時に仮想マシンが保持されないようにするには **false** に設定します。

> **注:**

`PersistVm` プロパティは、`CleanOnBoot` と `UseWriteBackCache` のプロパティが有効になっているプロビジョニングスキームにのみ適用されます。非永続仮想マシンに対して `PersistVm` プロパティが指定されていない場合、それらは電源オフ時にAzure環境から削除されます。

次の例では、`New-ProvScheme CustomProperties` パラメーターが `PersistVm` プロパティを **true** に設定します。

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />

<Property xsi:type="StringProperty" Name="StorageType"
Value="Standard_LRS" />

<Property xsi:type="StringProperty" Name="PersistWBC" Value="false" />

<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="true" />

<Property xsi:type="StringProperty" Name="PersistVm" Value="true" />

<Property xsi:type="StringProperty" Name="ResourceGroups" Value="demo-
resourcegroup" />

<Property xsi:type="StringProperty" Name="LicenseType"
Value="Windows_Client" />

</CustomProperties>
```

次の例では、`New-ProvScheme CustomProperties` パラメーターが `PersistVM` を **true** に設定することで、ライトバックキャッシュを保持します。

```
New-ProvScheme

-AzureAdJoinType "None"

-CleanOnBoot
```

```
 -CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com/
2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`"><Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`"
Value=`"true`" /><Property xsi:type=`"StringProperty`"
Name=`"StorageType`" Value=`"Standard_LRS`" /><Property
xsi:type=`"StringProperty`" Name=`"PersistWBC`" Value=`"false`" /
><Property xsi:type=`"StringProperty`" Name=`"PersistOsDisk`"
Value=`"true`" /><Property xsi:type=`"StringProperty`" Name=`"PersistVm`"
Value=`"true`" /><Property xsi:type=`"StringProperty`"
Name=`"ResourceGroups`" Value=`"demo-resourcegroup`" /><Property
xsi:type=`"StringProperty`" Name=`"LicenseType`"
Value=`"Windows_Client`" /></CustomProperties>"

 -HostingUnitName "demo"

 -IdentityPoolName "NonPersistent-MCSIO-PersistVM"

 -MasterImageVM "XDHyp:\HostingUnits\demo\image.folder\scale-
test.resourcegroup\demo-snapshot.snapshot"

 -NetworkMapping @ {"0"="XDHyp:\HostingUnits\demo\
\virtualprivatecloud.folder\East US.region\virtualprivatecloud.folder\ji-
test.resourcegroup\jitest-vnet.virtualprivatecloud\default.network"}

-ProvisioningSchemeName "NonPersistent-MCSIO-PersistVM"

 -ServiceOffering "XDHyp:
\HostingUnits\demo\serviceoffering.folder\Standard_B2ms.serviceoffering"
-UseWriteBackCache

 -WriteBackCacheDiskSize 127

 -WriteBackCacheMemorySize 256
```

ヒント:

`PersistVm` プロパティは、プロビジョニングされた仮想マシンを保持するかどうかを決定します。`PersistOsdisk` プロパティは、OSディスクを永続化するかどうかを決定します。プロビジョニングされた仮想マシンを保持するには、まずOSディスクを保持します。仮

> 想マシンを削除せずにOSディスクを削除しないでください。`PersistVm` パラメーターを指定せずに `PersistOsdisk` プロパティを使用できます。

ストレージタイプの変更失敗時の電源オン動作をカスタマイズする

電源オン時に、マネージドディスクのストレージタイプがAzureでの障害により目的のタイプに変更できない場合があります。このようなシナリオでは、VMはオフのままで、障害メッセージが送信されます。ただし、ストレージが構成されたタイプに復元できない場合でもVMの電源をオンにするか、VMをオフのままにするかを選択できます。

- カスタムプロパティ `FailSafeStorageType` を **true** (デフォルト設定) に構成した場合、または `New-ProvScheme` または `Set-ProvScheme` コマンドで指定しなかった場合：
  - 電源オン時に、VMは誤ったストレージタイプで電源オンになります。
  - シャットダウン時に、VMは誤ったストレージタイプでオフのままになります。
- `New-ProvScheme` または `Set-ProvScheme` コマンドでカスタムプロパティ `FailSafeStorageType` を **false** に構成した場合：
  - 電源オン時に、VMは誤ったストレージタイプでオフのままになります。
  - シャットダウン時、VMは誤ったストレージタイプでオフのままになります。

マシンカタログを作成するには：

1. PowerShellウィンドウを開きます。
2. Citrix固有のPowerShellモジュールをロードするには、`asnp citrix*`を実行します。
3. まだ作成されていない場合は、IDプールを作成します。
4. `New-ProvScheme`でカスタムプロパティを追加します。例：

```
New-ProvScheme -HostingUnitName "Azure-Resources-1" -IdentityPoolName
"name" -InitialBatchSizeHint 1

-MasterImageVM "XDHyp:\HostingUnits\Azure-
Resources-1\image.folder\abc.resourcegroup\def.snapshot"

-NetworkMapping @{"0"="XDHyp:\HostingUnits\Azure-
Resources-1\ght.folder\abc.resourcegroup\abc-
vnet.virtualprivatecloud\default.network"}

-ProvisioningSchemeName "name"
```

```
-ServiceOffering "XDHyp:\HostingUnits\Azure-
Resources-1\serviceoffering.folder\Standard_DS2_v2.serviceoffering"

-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com/
2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
instance`">

<Property xsi:type=`"StringProperty`" Name=`"StorageType`"
Value=`"Premium_LRS`" />

<Property xsi:type=`"StringProperty`" Name=`"StorageTypeAtShutdown`"
Value=`"Standard_LRS`" />

<Property xsi:type=`"StringProperty`" Name=`"FailSafeStorageType`"
Value=`"true`" />

</CustomProperties>"
```

5. マシンカタログを作成します。Remote PowerShell SDKを使用してカタログを作成する方法については、`<https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/>`を参照してください。

既存のマシンカタログを更新して、`FailSafeStorageType`カスタムプロパティを含めます。この更新は既存のVMには影響しません。

1. `Set-ProvScheme`コマンドでカスタムプロパティを更新します。例：

```
Set-ProvScheme -ProvisioningSchemeName <String> -CustomProperties "

<CustomProperties xmlns=`"http://schemas.citrix.com/2014/xd/
machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-instance`">

<Property xsi:type=`"StringProperty`" Name=`"StorageType`"
Value=`"Premium_LRS`" />

<Property xsi:type=`"StringProperty`" Name=`"IdentityDiskStorageType`"
Value=`"Premium_LRS`" />

<Property xsi:type=`"StringProperty`" Name=`"FailSafeStorageType`"
Value=`"false`" />
```

```
</CustomProperties>"
```

Set-ProvScheme で行われた変更を既存の VM に適用するには、`-StartsNow` および `-DurationInMinutes -1` パラメーターを指定して `Set-ProvVMUpdateTimeWindow` コマンドを実行します。

1. `-StartsNow` および `-DurationInMinutes -1` パラメーターを指定して `Set-ProvVMUpdateTimeWindow` コマンドを実行します。例:

   ```
   Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog -VMName
   <List-Of-Vm-Names> -StartsNow -DurationInMinutes -1
   ```

2. VMを再起動します。

休止状態対応VMを作成する

Azure環境では、休止状態をサポートするMCSマシンカタログを作成できます。この機能を使用すると、VMを中断し、ユーザーが再度サインインしたときにVMの以前の状態に再接続できます。

休止状態機能は以下に適用されます。

- シングルセッションOS
- 永続VMと非永続VM
- 静的およびランダム (プールされた) VDI デスクトップ

VDI デスクトップが静的かランダムかに関わらず、VM を休止状態にした後、同じセッションに再開できます。

このセクションでは、以下を参照してください。

- 前提条件
- 制限事項
- 休止状態対応マシンカタログの作成と管理
- 既存の休止状態対応VM用マシンカタログの作成
- 休止状態プロパティの確認
- VMの電源管理（手動および自動）

休止状態を使用するための前提条件

休止状態を使用するには、以下のタスクを完了していることを確認してください。

- WindowsとLinuxの両方のマスターイメージにAzure VMエージェントをインストールします。Windowsイメージのページファイルは一時ディスクに配置できます。マシンカタログで休止状態が有効になっている場合、MCSはページファイルの場所をベースディスクのC:ドライブに設定します。
- MCSは、生成されたリソースの休止状態プロパティを自動的に設定します。休止状態をサポートするために、マスターリソースのプロパティを設定する必要はありません。
- 休止状態をサポートするサブスクリプション内のVMサイズを使用してください。
- VMが休止状態機能を継承できるように、休止状態対応マシンプロファイル（VMまたはテンプレート仕様）を作成します。VMの作成については、休止状態の開始を参照してください。

> **注:**
>
> Microsoftによると、OSディスクから休止状態対応VMを展開できます。この機能は現在、特定のリージョンでサポートされており、近日中にすべてのリージョンで利用可能になります。詳細については、「OSディスクから休止状態対応VMを展開する」を参照してください。

> テンプレート仕様を作成するには、次の手順を実行します。

a. Azure Portalを開きます。テンプレートで使用する構成を持つVMを選択します。左ペインで**テンプレートのエクスポート**を選択します。

b. **パラメーターを含める**チェックボックスをオフにします。コンテキストをコピーし、JSONファイルとして保存します（例: `VMExportTemplate.json`）。

c. テンプレートでパラメーター`hibernationEnabled`が`true`であることを確認します。パラメーターが`true`でない場合は、使用したVM構成を確認してください。テンプレートファイルでサポートされているVMサイズを指定できます。ただし、カタログの作成時にマシンサイズを指定することもできます。

d. ネットワークインターフェースリソースのテンプレートをJSONファイル`VMExportTemplate.json`に追加します。その結果、2つのリソースを持つARMテンプレートファイルが作成されます。

e. **Azure Portal > テンプレート仕様 > テンプレートのインポート > ローカルテンプレートファイルの選択**を選択して、このテンプレートファイルをARMテンプレート仕様としてインポートします。

f. ARMテンプレート仕様が作成されたら、それをマシンプロファイルとして使用できます。

> **注:**
>
> Citrix Studioに同期されるまで数分かかる場合があります。

詳細については、Microsoftドキュメント休止状態を使用するための前提条件を参照してください。

制限事項

- シングルセッションOSマシンカタログ（永続的および非永続的）のみがサポートされています。
- エフェメラルOSディスクとMCS I/O機能はAzureの休止状態をサポートしていません。
- 休止状態は、自動Windowsアップデート中に失敗する可能性があります。
- Hyper-Vが有効な場合、信頼できる起動は休止状態の前提条件です。

詳細については、Microsoftドキュメントを参照してください。

休止状態対応のマシンカタログを作成および管理する

休止状態対応VMを作成するには、以下を使用して休止状態対応マシンカタログを作成および管理できます。

- Web Studio、または
- PowerShellコマンド

WEB STUDIOを使用してカタログを作成する

1. **マシンカタログの作成**を選択します。カタログ作成ウィザードが開きます。
2. **マシンタイプ**ページで、このカタログの**シングルセッションOS**マシンタイプを選択します。
3. **マシン管理**ページで、次のように設定を選択します。

   a. 「**電源管理されているマシン（仮想マシンやブレードPCなど）**」を選択します。

   b. 「**Citrix Machine Creation Services™ (MCS)**」を選択します。

4. **デスクトップエクスペリエンス**ページで、必要に応じてランダムまたは静的デスクトップエクスペリエンスを選択します。
5. **イメージ**ページで、マスターイメージを選択します。**マシンプロファイルを使用**チェックボックスをオンにし、休止状態をサポートするマシンプロファイルを選択します。ツールチップをクリックして、マシンプロファイルが休止状態をサポートしているかどうかを確認します。

> **注:**
>
> Azure マネージドマスターイメージを選択した場合、ブレードにはリソースと同じリージョンに属するすべてのイメージが一覧表示されます。

6. **Storage and License Types** ページで、このカタログに使用するストレージとライセンスを選択します。
7. **Virtual Machines** ページで、VM の数、VM サイズ、および可用性ゾーンを選択します。

> **注:**
>
> ハイバネーションをサポートするマシンサイズのみが選択肢として表示されます。

8. **NICs** ページで、VM に使用させる NIC を追加します。
9. **Disk Settings** ページで、ライトバックキャッシュディスクのストレージタイプとサイズを選択します。
10. **Resource Group** ページで、VM をプロビジョニングするリソースグループを選択します。
11. **Machine Identities** ページで、**Create new Active Directory accounts** を選択します。次に、アカウントの命名スキームを指定します。
12. **Domain Credentials** ページで、**Enter credentials** をクリックします。ターゲットの Active Directory ドメインでアカウント作成を実行するためのドメイン資格情報を入力します。
13. **Summary** ページで、マシンカタログの名前を入力し、**Finish** をクリックします。

MCS マシンカタログの作成が完了したら、カタログリストでカタログを見つけ、**Template Properties** タブをクリックします。パラメーター **Hibernation** の値は **Supported** である必要があります。

マシンカタログを編集する場合は、次の制限事項を考慮してください。

- 現在のマシンカタログが休止状態をサポートしている場合、次のことはできません。
  - VMサイズを休止状態に対応していないものに変更する。
  - マシンプロファイルを休止状態に対応していないものに変更する。
- 現在のマシンカタログが休止状態をサポートしていない場合、次のことはできません。
  - 現在、Web Studioを使用してマシンプロファイルを休止状態に対応したものに変更する。

既存の休止状態対応VMを管理するためのマシンカタログを作成する

すでに休止状態対応VMがあり、それらを一時停止および再開したい場合は、それらのVMを電源管理のためにインポートするマシンカタログを作成します。

> **注:**
>
> 休止状態に対応しているVMと対応していないVMの両方を含むマシンカタログを作成できます。ただし、休止状態関連の機能が必要な場合は、休止状態に対応しているVMのみでマシンカタログを作成する必要があります。

> Web Studioを使用して既存の休止状態対応VMのカタログを作成するには、画面の指示に従って手順を完了し、以下の主要な設定に注意してください。

1. **マシン管理**ページで、**電源管理されているマシン**を選択し、次に、マシンの展開方法として**その他のサービスまたはテクノロジー**を選択します。
2. **仮想マシン**ページで、休止状態に対応しているVMのみを追加またはインポートします。

POWERSHELLコマンドを使用してマシンカタログを作成する

休止状態を使用するためのすべての要件を満たした後、`New-ProvScheme`コマンドを使用して、休止状態対応のマシンカタログを作成できます。Remote PowerShell SDKを使用してカタログを作成する方法については、New-ProvSchemeを参照してください。

カタログの作成中に、以下のPowerShellコマンドを使用して、VMサイズとマシンプロファイルが休止状態をサポートしているかどうかを確認できます。

- VMサイズについては、次のコマンドを実行し、プロパティ`supportsHibernation`が**True**であるかどうかを確認します。例：

```
Get-ChildItem -AdminAddress "MyDDC.MyDomain.local" -LiteralPath
@("XDHyp:\HostingUnits\ <VirtualNetwork> \serviceoffering.folder") |
select Name, AdditionalData | ConvertTo-Json
```

- マシンプロファイルの場合、次のコマンドを実行し、プロパティ`supportsHibernation`が**True**であるかどうかを確認します。例：

```
Get-ChildItem -AdminAddress "MyDDC.MyDomain.local" -LiteralPath
@("XDHyp:\HostingUnits\ <VirtualNetwork>
\machineprofile.folder\abc.resourcegroup")|select Name, AdditionalData|
ConvertTo-Json
```

マシンカタログを編集する場合は、次の制限事項を考慮してください。

- 現在のマシンカタログが休止状態をサポートしている場合、次のことはできません。
  - VMサイズを休止状態非対応のものに変更する
  - マシンプロファイルを休止状態非対応のものに変更する
- 現在のマシンカタログが休止状態をサポートしていない場合、次のことはできません。
  - 現在、Web Studioを使用してマシンプロファイルを休止状態に対応したものに変更する。

Remote PowerShell SDKを使用してカタログのVMサイズとマシンプロファイルを変更する方法については、`<https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/MachineCreation/Set-ProvScheme/>`を参照してください。

休止状態プロパティの確認

PowerShellコマンドを使用して、マシンカタログ、VM、およびブローカーマシンの休止状態のプロパティを確認できます。

- プロビジョニングスキームの休止状態プロパティを確認するには、次のPowerShellコマンドを実行します。`HibernationEnabled`パラメーターは`True`である必要があります。

```
(Get-ProvScheme -provisioningSchemeName <YourSchemeName>).VMMetadata
-join "" |  ConvertFrom-Json | Select HibernationEnabled
```

- プロビジョニングVMの休止状態プロパティを確認するには、次のPowerShellコマンドを実行します。`SupportsHibernation`パラメーターは`True`である必要があります。

```
(Get-ProvVM -VMName <YourVMName>).CustomVmData | ConvertFrom-Json |
Select SupportsHibernation
```

- ブローカーマシンの休止状態容量を確認するには、次のPowerShellコマンドを実行します。**Suspend** および **Resume** の電源アクションは、休止状態機能を示します。

```
(Get-BrokerMachine -MachineName
<YourMachineName>).SupportedPowerActions
```

休止状態対応VMの電源管理

休止状態対応VMに対して、次の電源管理操作を実行できます。

- 実行状態からVMを**一時停止**する
- 一時停止状態からVMを**再開**する
- 一時停止状態からVMを**強制シャットダウン**する
- 一時停止状態からVMを**強制再起動**する

詳細については、以下を参照してください:

- 一時停止
- 再開

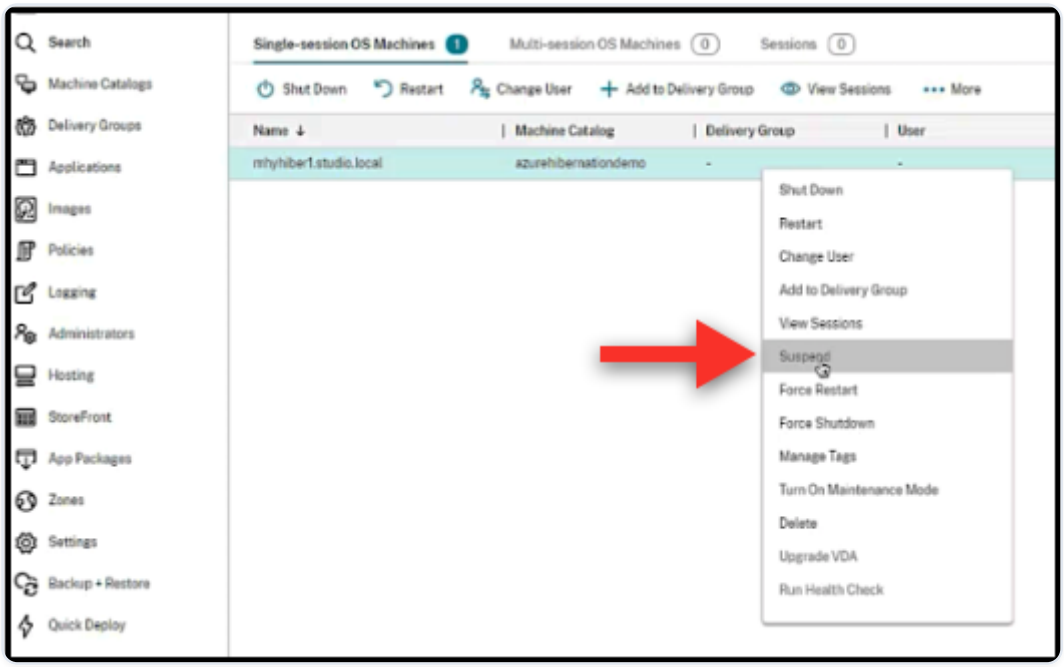
一時停止

VMを一時停止するには、次のいずれかの方法を使用できます:

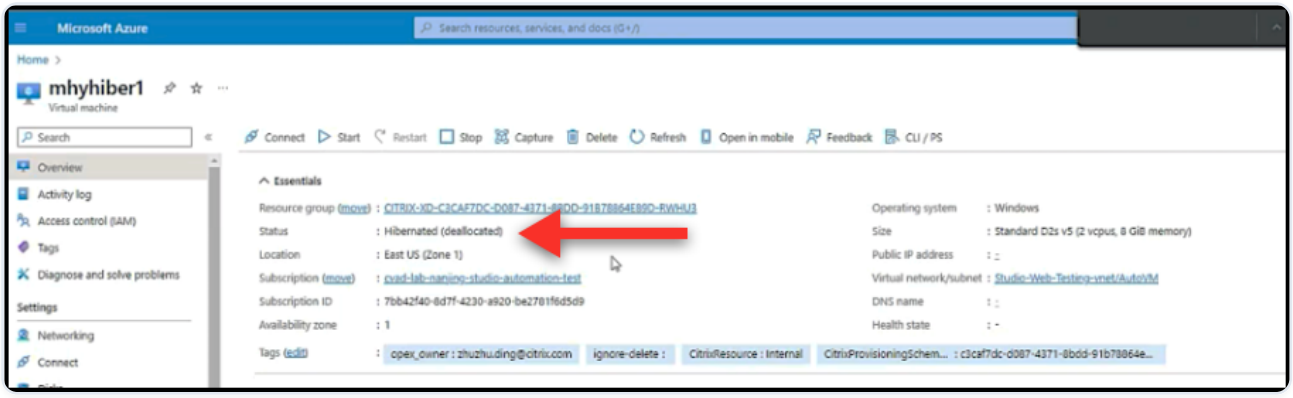
- Web Studioを使用して**手動で**
- タイムアウトポリシーを使用して**自動的に**: 詳細については、その他の設定を参照してください。

VMを手動で一時停止するには：

1. VMを右クリックし、**一時停止**を選択します。操作を確定するには、**はい**をクリックします。**電源状態**が**一時停止中**から**一時停止**に変わります。



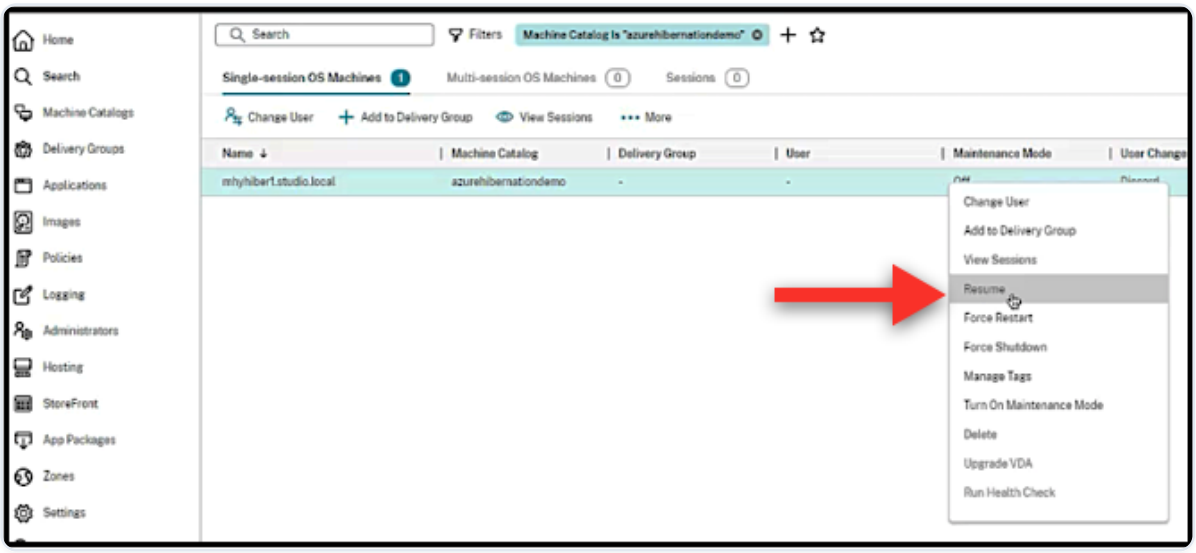
Azure portalでVMのステータスを確認できます。



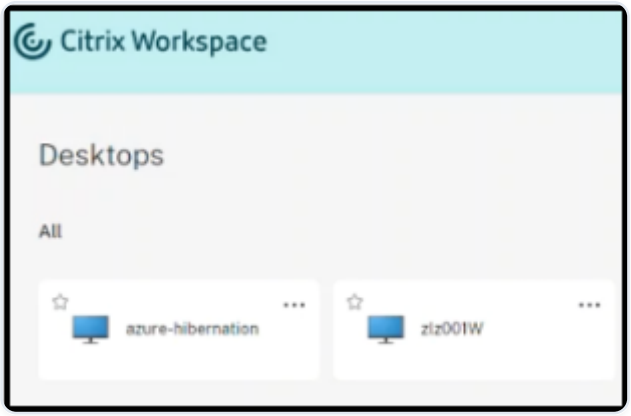
再開

休止状態のVMを再開するには、次のいずれかの方法を使用します。

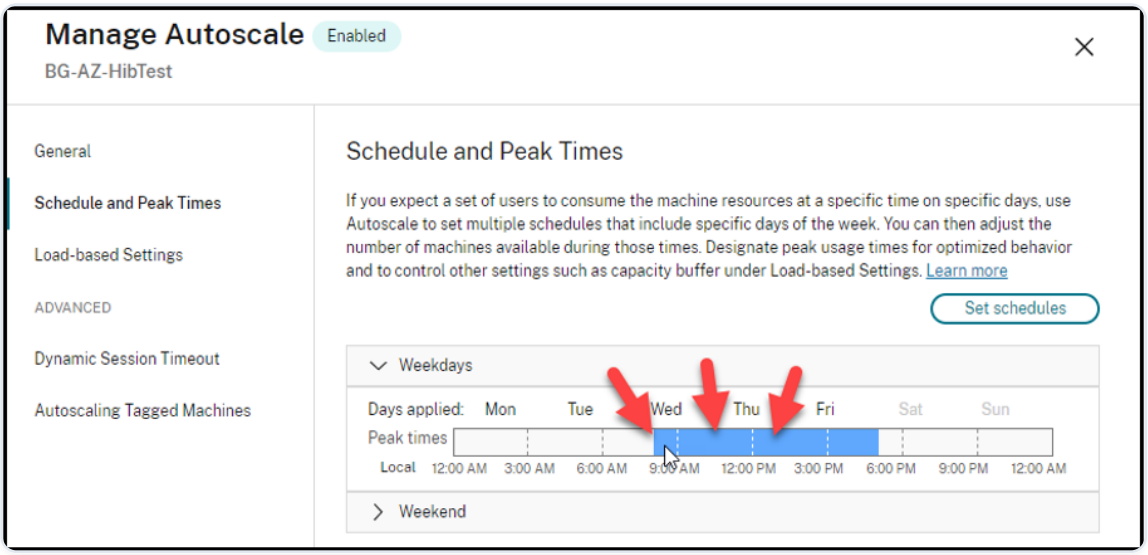
- **手動**:
  - 管理者はWeb Studioを使用してVMを再開できます。



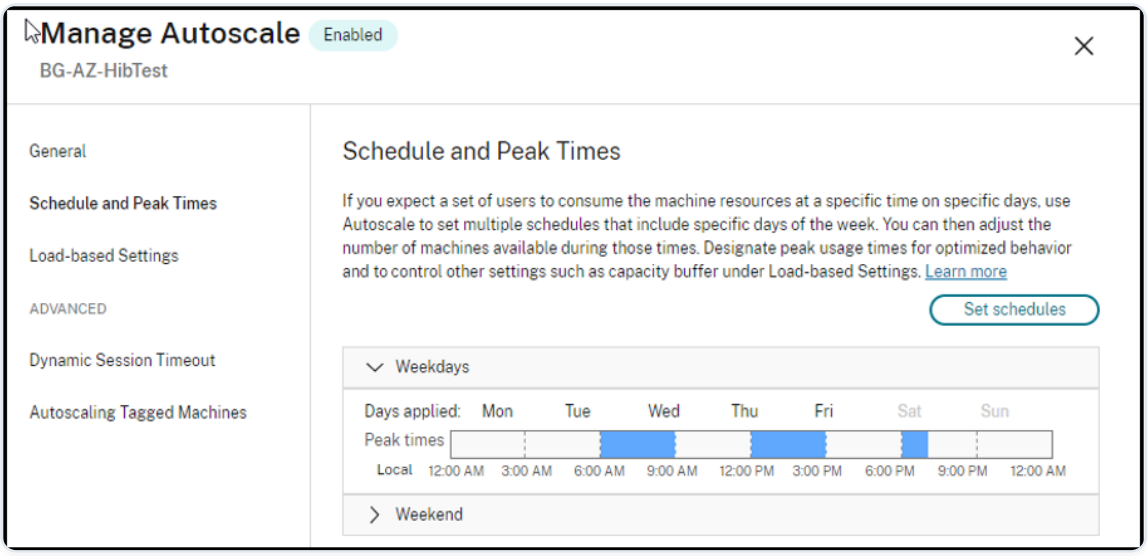
- エンドユーザーは、デスクトップアイコンをクリックすると、Citrix Workspace™メニューを使用してVMを起動できます。



- **自動**:
  - ピーク時間を正しく構成すると、Autoscale™は休止状態のマシンを自動的に電源オンにできます。タイムスケジュールをクリックして、ピーク時間を30分間隔で設定できます。各青いフレームは、ピーク時間としてマークされたタイムスロットを表します。ピーク時間には、連続したタイムスロットと連続しないタイムスロットの両方を含めることができます。
    - 連続したタイムスロット



- 連続しないタイムスロット



> **注:**
>
> 「**オートスケール管理 > 負荷ベース設定**」で、**アクション**が**サスペンド**に設定されている場合、そのデリバリーグループ内のすべてのVMが休止状態機能を備えていることを確認してください。そうでない場合、休止状態にできないVMは実行を継続します。

> オートスケール負荷ベース設定の管理(/en-us/citrix-virtual-apps-desktops/2503/media/azure-hibernation-autoscale.png)

休止状態の失敗に関する警告メッセージを取得する

MCSプロビジョニング済みおよび既存の休止状態対応VMの休止状態の失敗が発生した場合、PowerShellコマンド `Get-ProvOperationEvent` を使用して警告メッセージを取得できます。

PowerShellコマンドの詳細については、SDKドキュメントの Get-ProvOperationEvent を参照してください。

これを行うには：

1. PowerShellウィンドウを開きます。
2. Citrix固有のPowerShellモジュールをロードするために`asnp citrix*`を実行します。
3. 休止状態の失敗の場合に警告メッセージを取得するために`Get-ProvOperationEvent`を実行します。

```
Get-ProvOperationEvent -filter { OperationName -eq "Suspend" }
```

出力：

```
EventAdditionalData : Error code = OperationNotAllowed and Error
message = The Hibernate-Deallocate Operation cannot be performed on a
VM that has extension 'AzureHibernateExtension' in failed state. For
more information, see https://aka.ms/hibernate-resume/errors. Error
details from the extension : Enabling

                  hibernate failed. Response from the powercfg command.
Exit Code: 1. Error message:

                  Hibernation failed with the following error: The
request is not supported.



                  The following items are preventing hibernation on
this system.

                    The current Device Guard configuration has disabled
hibernation.

                    An internal system component has disabled
hibernation.

                            Hypervisor

                  Status: 409
```

```
                  ErrorCode: OperationNotAllowed



                  Content:

                  {

                    "error": {

                      "code": "OperationNotAllowed",

                      "message": "The Hibernate-Deallocate Operation
cannot be performed on a VM that has extension
'AzureHibernateExtension' in failed state. For more information, see
https://aka.ms/hibernate-resume/errors. Error details from the
extension : Enabling hibernate failed. Response from the

                  powercfg command. Exit Code: 1. Error message:
\nHibernation failed with the following error: The request is not
supported.\r\r\n\r\nThe following items are preventing hibernation on
this system.\r\n\tThe current Device Guard configuration has disabled
hibernation.\r\n\tAn internal system

                  component has disabled hibernation.
\r\n\t\tHypervisor"

                    }

                  }

EventCategory       : Warning

EventDateTime       : 1/11/2024 4:18:31 AM

EventId             : 0

EventMessage        : Failed to suspend machine my-resource-group/my-
vm.

EventSeverity       : Important

EventSource         : AzureRmPlugin
```

```
EventState          : New

LinkedObjectType    : ProvisioningScheme

LinkedObjectUid     : 589cb600-6e65-479f-9d47-9715c4732366

OperationName       : Suspend

OperationTargetName : my-resource-group/my-vm

OperationTargetType : VirtualMachine

OperationType       : PowerManagement

Recommendation      :
```

休止状態の問題のトラブルシューティング

休止状態と信頼できる起動VM機能の両方を有効にしようとすると、ゲストOSの設定が正しくない場合、次のエラーメッセージが表示されます。

エラーコード	エラーメッセージ
OperationNotAllowed	拡張機能「AzureHibernateExtension」が失敗状態にあるVMでは、休止状態解除操作を実行できません。詳細については、`<https://aka.ms/hibernate-resume/errors/>` を参照してください。拡張機能からのエラー詳細：休止状態の有効化に失敗しました。powercfgコマンドからの応答。終了コード：1。エラーメッセージ：次のエラーにより休止状態に失敗しました：要求はサポートされていません。次の項目がこのシステムでの休止状態を妨げています。**現在のDevice Guard構成により、休止状態が無効になっています。内部システムコンポーネントにより、休止状態が無効になっています。**

この問題を解決するには、ゲストVM内で仮想化が有効になっていることを確認してください。たとえば、Windows環境でHyper-Vが有効になっていることを確認します。

警告メッセージの詳細については、Microsoft ドキュメントのVM 休止状態のトラブルシューティングを参照してください。

> **注:**
>
> VMの再開失敗に関連するエラーメッセージは、将来のリリースで利用可能になります。

詳細情報

Citrix Azureの休止状態の詳細については、Citrix Tech Zoneの記事を参照してください。

セキュリティポリシー

この記事では、さまざまなサポート対象クラウドサービスにおけるセキュリティ機能について説明します。セキュリティ機能には、次のものがあります。

- セキュリティグループ(/ja-jp/citrix-virtual-apps-desktops/2503/install-configure/security-policies/security-group.html)
- セキュアブート(/ja-jp/citrix-virtual-apps-desktops/2503/install-configure/security-policies/secure-boot.html)
- 暗号化機能(/ja-jp/citrix-virtual-apps-desktops/2503/install-configure/security-policies/encryption-capabilities.html)

セキュリティグループ

セキュリティグループは、仮想ネットワーク内のリソース間のネットワークトラフィックをフィルタリングするための一連のセキュリティルールです。セキュリティルールは、いくつかの種類のリソースに対するインバウンドネットワークトラフィックまたはアウトバウンドネットワークトラフィックを許可または拒否します。各ルールは次のプロパティを指定します。

- 名前: ネットワークセキュリティグループ内で一意の名前
- 優先度: ルールは優先度順に処理され、数値が小さいほど優先度が高いため、数値が小さいものが数値が大きいものより先に処理されます
- 送信元または送信先: 任意、または個別のIPアドレス、クラスレスドメイン間ルーティング（CIDR）ブロック（例: 10.0.0.0/24）、サービスタグ、またはアプリケーションセキュリティグループ
- プロトコル: 各セキュリティグループのルールを追加する際のベースとなるプロトコル

- 方向: ルールがインバウンドトラフィックまたはアウトバウンドトラフィックのどちらに適用されるか
- ポート範囲: 個別のポートまたはポートの範囲を指定できます
- アクション: 許可または拒否

サポートされているハイパーバイザーの詳細については、以下を参照してください。

- AWS のセキュリティグループ
- Microsoft Azure のセキュリティグループ
- Google Cloud Platform のセキュリティグループ

AWS のセキュリティグループ

セキュリティグループは、VPC 内のインスタンスのトラフィックを制御する仮想ファイアウォールとして機能します。パブリックサブネット内のインスタンスがプライベートサブネット内のインスタンスと通信できるようにするルールをセキュリティグループに追加します。これらのセキュリティグループを VPC 内の各インスタンスに関連付けることもできます。インバウンドルールはインスタンスへの受信トラフィックを制御し、アウトバウンドルールはインスタンスからの送信トラフィックを制御します。

イメージ準備中のネットワーク設定の詳細については、イメージ準備中のネットワーク設定を参照してください。

インスタンスを起動するときに、1つ以上のセキュリティグループを指定できます。セキュリティグループを構成するには、セキュリティグループの構成を参照してください。

Microsoft Azure のセキュリティグループ

Citrix Virtual Apps and Desktops は、Azure のネットワークセキュリティグループをサポートしています。ネットワークセキュリティグループは、サブネットに関連付けられることが想定されています。詳細については、ネットワークセキュリティグループを参照してください。

イメージ準備中に作成されたネットワークセキュリティグループの詳細については、Azure Resource Managerイメージを使用したマシンカタログの作成を参照してください。

Google Cloud Platform のセキュリティグループ

マシンカタログの準備中に、カタログのマスターイメージシステムディスクとして機能するマシンイメージが準備されます。このプロセスが発生すると、ディスクは一時的に仮想マシンに接続されます。このVMは、すべてのインバウンドおよびアウトバウンドネットワークトラフィックを防止する分離された環境で実行する必要があります。これは、すべてのトラフィックを拒否するファイ

アウォールルールによって実現されます。詳細については、ファイアウォールルールを参照してください。

暗号化機能

暗号化機能は、共有仮想マシンホスト上の悪意のあるゲストによる攻撃や、ホスト上のすべての仮想マシンを管理するハイパーバイザー制御ソフトウェアによる攻撃から、仮想マシンのコンテンツを保護します。

サポートされているクラウドサービスの詳細については、以下を参照してください。

- AWS の暗号化機能
- Google Cloud Platform の暗号化機能
- Microsoft Azure の暗号化機能

AWS の暗号化機能

このセクションでは、AWS 仮想化環境における暗号化機能について説明します。

自動暗号化

アカウントで作成された新しい Amazon EBS ボリュームとスナップショットコピーの自動暗号化を有効にできます。詳細については、「自動暗号化」を参照してください。

Google Cloud Platform の暗号化機能

このセクションでは、Google Cloud Platform (GCP) 仮想化環境における暗号化機能について説明します。

Googleマネージド暗号化キーが許可する以上のキー操作を制御する必要がある場合は、顧客管理暗号化キーを使用できます。顧客管理暗号化キーを使用する場合、オブジェクトがバケットに保存されるときにCloud Storageによってキーで暗号化され、リクエスターに提供されるときにCloud Storageによって自動的に復号化されます。詳細については、顧客管理暗号化キーを参照してください。

MCSカタログに顧客管理暗号化キー (CMEK) を使用できます。詳細については、顧客管理暗号化キー (CMEK) の使用を参照してください。

Microsoft Azure の暗号化機能

このセクションでは、Azure仮想化環境における暗号化機能について説明します。

Azureサーバー側暗号化

ほとんどのAzureマネージドディスクは、サーバー側暗号化（SSE）を使用してデータを保護し、セキュリティとコンプライアンスのコミットメントを満たすのに役立つAzure Storage暗号化で暗号化されています。Citrix Virtual Apps and Desktopsは、Azure Key Vaultを介したAzureマネージドディスクの顧客管理暗号化キーをサポートしています。詳細については、Azureサーバー側暗号化を参照してください。

ホストでのAzureディスク暗号化

ホストでの暗号化機能を備えたMCSマシンカタログを作成できます。

この暗号化方法は、Azureストレージを介してデータを暗号化しません。VMをホストするサーバーがデータを暗号化し、その後、暗号化されたデータがAzureストレージサーバーを介して流れます。したがって、この暗号化方法はデータをエンドツーエンドで暗号化します。

ホストでの暗号化機能を持つMCSマシンカタログの作成に関する詳細については、ホストでのAzureディスク暗号化を参照してください。

Azure二重暗号化

二重暗号化は、プラットフォーム側暗号化（デフォルト）と顧客管理暗号化（CMEK）です。したがって、暗号化アルゴリズム、実装、または侵害されたキーに関連するリスクを懸念するセキュリティ意識の高いお客様は、この二重暗号化を選択できます。永続的なOSディスクとデータディスク、スナップショット、およびイメージはすべて、二重暗号化によって保存時に暗号化されます。詳細については、マネージドディスクの二重暗号化を参照してください。

Azure機密VM

Azure機密コンピューティングVMは、仮想デスクトップがメモリ内で暗号化され、使用中に保護されることを保証します。

MCSを使用して、Azure機密VMを含むカタログを作成できます。このようなカタログを作成するには、マシンプロファイルワークフローを使用する必要があります。マシンプロファイルの入力として、VMとARMテンプレート仕様の両方を使用できます。

詳細については、Azure機密VMを参照してください。

マシンの負荷分散

負荷分散は、組織が望むコストバランスを達成し、クラウドが提供するすべての利点を活用するのに役立ちます。負荷分散はデリバリーグループレベルで構成されます。

> **注:**

> 負荷分散は、マルチセッションOSマシンにのみ適用されます。

> 負荷分散には2つのオプションがあります。

- 水平負荷分散
- 垂直負荷分散

デフォルトでは、水平負荷分散が有効になっています。

水平負荷分散: 水平負荷分散モデルでは、受信ユーザーセッションは利用可能な最も負荷の低いマシンに割り当てられます。展開環境に2つのVDAがあると仮定した例を考えてみましょう。1つはアクティブなユーザーセッション（ユーザー1）を持ち、2番目のユーザー（ユーザー2）はセッションを待っています。水平負荷分散アルゴリズムは、より有利な負荷インデックスのため、ユーザー2をVDA 2に割り当てます。したがって、水平アルゴリズムはすべての利用可能なVDAにセッションを分散するため、負荷が減少したときにマシンがオフになるのを妨げる可能性があります。

垂直負荷分散: 垂直負荷分散モデルでは、セッションは最も高い負荷インデックスを持つVDAに割り当てられます。これにより、受信ユーザーセッションを他のユーザーがすでに使用しているVDAに集約し、電源をオンにしてユーザーセッションのために準備しておく必要があるVDAの数を減らすことができます。水平負荷分散で述べたのと同じ展開環境を考えてみましょう。ユーザー1はVDA 1に割り当てられ、ユーザー2のセッションには垂直負荷分散アルゴリズムが適用されます。負荷インデックスが高いのはVDA 1であるため、ユーザー2はVDA 1に割り当てられます。したがって、すべての受信セッションは、高負荷インデックスのウォーターマークに達するまで、最も負荷の高いVDAに割り当てられます。その後初めて、他のVDAがセッションの受信を開始します。

サイトレベルでの負荷分散設定

すべてのデリバリーグループに対して負荷分散を構成できます（サイト全体の構成）。

この機能をStudioから構成するには、左ペインで**Settings**を選択します。**Load Balancing Sessions on Machines**の下のオプションを選択します。

または、PowerShellを使用して、サイト全体で垂直負荷分散を有効または無効にできます。`Set-BrokerSite` コマンドレットで `UseVerticalScalingForRdsLaunches` 設定を使用しま

す。`UseVerticalScalingForRdsLaunches` 設定の値を表示するには `Get-BrokerSite` を使用します。詳細については、コマンドレットのヘルプを参照してください。

> **ヒント:**
>
> マシンがホストできるセッションの最大数を指定するには、最大セッション数 ポリシー設定を使用します。

デリバリーグループレベルでの負荷分散設定

ロードバランシングはデリバリーグループレベルで構成でき、サイトレベルから継承されたロードバランシング設定を上書きできます。

これは、デリバリーグループの作成時または既存のデリバリーグループの編集時に構成できます。「手順2. 負荷分散」を参照してください。

ロード管理

負荷管理はサーバーの負荷を測定し、現在の環境条件でどのサーバーを選択するかを決定します。この選択は、以下に基づいています。

- **サーバーメンテナンスモードの状態**: マルチセッションOSマシンは、メンテナンスモードがオフの場合にのみ負荷分散の対象となります。
- **サーバー負荷インデックス**: マルチセッションOSマシンを提供するサーバーが接続を受け入れる可能性を決定します。このインデックスは、セッション数やCPU、ディスク、メモリ使用量などのパフォーマンスメトリックの設定といった負荷評価子の組み合わせです。負荷評価子は、負荷管理ポリシー設定で指定されます。デフォルトでは、負荷インデックスは計算にセッション数のみを使用し、負荷管理ポリシー設定で構成されるまではCPU、ディスク、メモリは使用しません。ポリシー設定の詳細については、「負荷管理ポリシー設定」を参照してください。

  サーバー負荷インデックスが10000の場合、サーバーが完全に負荷されていることを示します。他に利用可能なサーバーがない場合、ユーザーはセッションを起動したときに、デスクトップまたはアプリケーションが現在利用できないというメッセージを受け取る可能性があります。 負荷インデックスは、Director（監視）、Studio検索、およびSDKで監視できます。

  コンソール表示で、**サーバー負荷インデックス**列（デフォルトでは非表示）を表示するには、マシンを選択し、列ヘッダーを右クリックして、**「列の選択」を選択します。「マシン」カテゴリ**で、**「負荷インデックス」**を選択します。

SDKでは、`Get-BrokerMachine`コマンドレットを使用します。詳細については、「CTX202150」を参照してください。

- **同時ログオン許容ポリシー設定**: サーバーへの同時ログオン要求の最大数。（この設定は、XenApp 6.xバージョンでのロードスロットリングに相当します。）

  すべてのサーバーが同時ログオン許容設定以上の場合、次のログオン要求は、保留中のログオンが最も少ないサーバーに割り当てられます。複数のサーバーがこれらの基準を満たす場合、負荷インデックスが最も低いサーバーが選択されます。「同時ログオン許容」を参照してください。

> **ヒント:**
>
> ログオン許容設定を適用し、指定された数を超える同時ログオンを失敗させるには、`Set-BrokerServiceConfigurationData Core.LogonToleranceIsHardLimit -SettingValue $true`を実行できます。

デリバリーグループの作成

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

> デリバリーグループは、1つ以上のマシンカタログから選択されたマシンの集合です。デリバリーグループは、どのユーザーがそれらのマシンにアクセスできるか、および利用可能なアプリケーションとデスクトップを定義します。

デリバリーグループの作成は、サイトとマシンカタログを設定した後の次のステップです。後で初期設定を変更したり、必要に応じて追加のデリバリーグループを作成したりできます。

一部の機能と設定は、既存のデリバリーグループを編集する場合にのみ構成できます。詳細については、「デリバリーグループの管理」を参照してください。

始める前に

デリバリーグループを作成する前に：

- 必要な選択肢と情報を理解するために、この記事を確認してください。
- ハイパーバイザー、クラウドサービス、またはマシンをホストするその他のリソースへの接続を作成済みであることを確認してください。
- 仮想マシンまたは物理マシンを含むマシンカタログが利用可能であることを確認してください。

デリバリーグループを作成するには：

1. サイトとマシンカタログを作成したがデリバリーグループを作成していない場合、Web Studioはデリバリーグループを作成するための正しい開始場所に案内します。

ウィザードのページ

サイトとマシンカタログを作成したがデリバリーグループを作成していない場合、Web Studioはデリバリーグループを作成するための正しい開始点に案内します。

既にデリバリーグループを作成済みで、別のグループを作成したい場合は、以下の手順に従ってください。

1. **デリバリーグループ**を選択します。
2. アクションペインで、**デリバリーグループの作成**を選択します。
3. デリバリーグループを整理するために、デフォルトの**デリバリーグループ**フォルダーの下にフォルダーを作成できます。詳しくは、フォルダーの作成を参照してください。
4. グループを作成したいフォルダーを選択し、**デリバリーグループの作成**をクリックします。グループ作成ウィザードが開きます。
5. ウィザードは**はじめに**ページから開始します。このページは、今後の起動時にスキップすることを選択できます。その後、以下の表に記載されているいくつかのページを案内します。各ページを完了したら、**次へ**をクリックして最終ページに進みます。

	マルチセッションOS	シングルセッションOS 静的（割り当て済み）	シングルセッションOS 共有（プール済み）	リモート PC アクセス
ページ	マシン	マシン	マシン	マシン

	マルチセッションOS	シングルセッションOS 静的（割り当て済み）	シングルセッションOS 共有（プール済み）	リモート PC アクセス
	負荷分散	デリバリーの種類	ユーザー	ユーザー
	ユーザー	ユーザー	アプリケーション	アプリケーション
	アプリケーション	アプリケーション	デスクトップ	デスクトップ割り当てルール
	デスクトップ	デスクトップ割り当てルール	アプリ保護	アプリ保護
	アプリ保護	アプリ保護	スコープ	スコープ
	スコープ	スコープ	ライセンス契約	ライセンス契約
	ライセンス契約	ライセンス契約	ポリシーセット	ポリシーセット
	ポリシーセット	ポリシーセット	ローカルホストキャッシュ	概要
	概要	概要	概要	

注:

- 選択したシングルセッションOS静的マシンカタログに利用可能な割り当て済みマシンがある場合、「**マシン割り当て**」ページ（「**マシン**」ページの直後）が表示されます。
- 電源管理されたシングルセッションのプールされたマシンを含むデリバリーグループでのみ、Local Host Cache settingページが利用可能です。

マシンページ

1. シングルセッションのサスペンド対応VMのみでデリバリーグループを作成するには、**このデリバリーグループにサスペンド機能を必須にする**を選択します。

> **注:**
>
> この機能は、シングルセッションのサスペンド対応マシンにのみ適用されます。

2. マシンカタログを選択し、そのカタログから使用するマシンの数を選択します。

重要な考慮事項

- カタログを選択する際、リストには少なくとも1つの未使用マシンがあるカタログのみが表示されます。
- 1つのカタログは、複数のデリバリーグループにマシンを提供できます。1つのマシンは、1つのデリバリーグループでのみ使用できます。デリバリーグループにマシンを追加すると、Web Studioはデフォルトで同じカタログを提案します。
- 1つのデリバリーグループは、複数のカタログのマシンを使用できます。ただし、それらのカタログには同じマシンタイプ（マルチセッションOS、シングルセッションOS、またはRemote PC Access）が含まれている必要があります。デリバリーグループ内のすべてのマシンは、同じ割り当てタイプ（プール型または静的）である必要があります。つまり、デリバリーグループ内でマシンタイプを混在させることはできません。
- Citrixは、すべてのマシンで最新のVDAバージョンを使用することを推奨します。
- **Remote PC Access**の場合、サイトを作成すると、「**Remote PC Access Machines**」という名前のカタログと、「**Remote PC Access Desktops**」という名前のデリバリーグループが自動的に作成されます。「**Remote PC Access Machines**」カタログ内の各マシンは、デリバリーグループに自動的に関連付けられます。
- 次の互換性チェックが実行されます。
    - MinimumFunctionalLevel は互換性がある必要があります
    - SessionSupport は互換性がある必要があります
    - AllocationType は SingleSession と互換性がある必要があります
    - Remote PC Access は Remote PC Access カタログとのみ互換性があります

マシンの割り当てページ

「**マシン割り当て**」ページは、「**マシン**」ページで選択したシングルセッションOS静的マシンカタログに、利用可能な割り当て済みマシンがある場合に利用できます。

このページを使用して、このデリバリーグループ内のマシンのユーザー割り当てとデスクトップ表示名を管理します。

- デスクトップ表示名を管理するには、**表示名**フィールドを使用します。
- **参照**をクリックして、ユーザーまたはグループを選択します。

負荷分散ページ

「**マシンの負荷分散セッション**」ページは、マルチセッションOSマシンで利用できます。

このページを使用して、このデリバリーグループで使用する負荷分散設定を構成します。デフォルトでは、デリバリーグループはサイト全体の負荷分散設定を使用します。

1. このデリバリーグループの負荷分散設定を構成するには、**サイト全体の設定を上書き**チェックボックスを選択します。
2. 必要に応じて、**水平負荷分散**または**垂直負荷分散**オプションを選択します。水平負荷分散と垂直負荷分散の方法については、「マシンの負荷分散」を参照してください。

デリバリーグループ作成時の負荷分散設定(/en-us/citrix-virtual-apps-desktops/2503/media/load-balancing.png)

「**垂直負荷分散**」を選択した場合、同時ログオン許容数と最大セッション数ポリシーが適切に構成されていることを確認してください。

配信の種類ページ

「**配信の種類**」ページは、シングルセッションOS静的（割り当て済み）マシンにのみ表示されます。

このページを使用して、カタログ内のマシンを構成し、デスクトップまたはアプリケーションをユーザーに配信します。

1. **アプリケーション**または**デスクトップ**のいずれかを選択します。両方を有効にすることはできません。

> **注:**
>
> マルチセッションOSまたはシングルセッションOSのランダム（プールされた）カタログからマシンを選択した場合、配信タイプはアプリケーションとデスクトップであると見なされます。アプリケーション、デスクトップ、またはその両方を配信できます。

ユーザーページ

ユーザーページはすべてのマシンタイプで利用できます。ただし、ページオプションはマシンタイプによって異なります。

このページを使用して、ユーザーがデリバリーグループ内のリソースにアクセスする方法を指定します。

ユーザーアクセス制御の仕組み

デリバリーグループでのユーザーアクセスは、アクセス設定を作成または編集する際に指定されたユーザーリストを通じて制御されます。

- 以下の *すべての* 条件を満たすユーザーは、デリバリーグループ内の**アプリケーション**にアクセスできます。
  - このデリバリーグループ内のリソース（アプリとデスクトップ）へのアクセス権を持っていること。デフォルトでは、アクセスは展開のユーザーアクセスリスト（Active Directory内のユーザー）によって決定され、これはStudioでは構成されません。デリバリーグループへのユーザーの追加または削除を参照してください。
  - このグループ内のアプリケーションへのアクセス権を持っていること。デフォルトでは、アプリケーションエンタイトルメントポリシー規則には全員が含まれます。詳細については、PowerShell SDK `BrokerAppEntitlementPolicyRule` コマンドレットを参照してください。
  - このアプリケーションを含むアプリケーショングループにアクセスできる。
- 以下の *両方* の条件を満たすユーザーは、デリバリーグループ内のデスクトップにアクセスできます。
  - このデリバリーグループ内のリソース（アプリとデスクトップ）にアクセスできる。デフォルトでは、アクセスは展開のユーザーアクセスリスト（Active Directory内のユーザー）によって決定され、これはStudioでは構成されません。デフォルトのユーザー範囲からユーザーを追加または削除できます。「デリバリーグループでのユーザーの追加または削除」を参照してください。
  - このグループ内のデスクトップにアクセスできる。詳細については、「デスクトップ（またはデスクトップ割り当てルールページ）」を参照してください。

構成手順

1. デリバリーグループ内のリソースの使用を許可または制限するオプションのいずれかを選択します。

- **認証済みユーザーによるリソースの使用を許可する:** アプリケーションとデスクトップにアクセスするには、指定したユーザーとグループメンバーが、スマートカードやユーザー名とパスワードなどの資格情報をStoreFront™またはCitrix Workspace™アプリに提示する必要があります。（シングルセッションOSマシンを含むデリバリーグループの場合、デリバリーグループを編集して後でユーザーデータ（ユーザーリスト）をインポートできます。）
- **リソースの使用を制限する:** または、ユーザーまたはユーザーグループを**許可リスト**に追加することで、デリバリーグループの使用を制限できます。**許可リスト**のユーザーのみが、デリバリーグループ内のアプリとデスクトップにアクセスできます。**ブロックリストの追加**をクリックして、ユーザーとユーザーグループをブロックリストに追加することもできます。これにより、選択したデリバリーグループ内のアプリとデスクトップをユーザーが使用できなくなります。ブロックリストは、許可リスト内のユーザーをブロックする場合にのみ意味があります。

2. マルチセッションOSマシンの場合、ユーザーがStoreFrontまたはCitrix Workspaceアプリに資格情報を提示せずにアプリケーションとデスクトップにアクセスできるようにする場合は、**認証されていない（匿名）ユーザーへのアクセスを許可する。資格情報は不要**を選択します。たとえば、キオスクではアプリケーションが資格情報を要求する場合がありますが、Citrixアクセスポータルとツールは要求しません。

   - 認証されていないユーザーアカウントは、セッションが起動されるとオンデマンドで作成され、AnonXYZという名前が付けられます。ここでXYZは一意の3桁の値です。
   - 認証されていないユーザーセッションには、デフォルトで10分間のアイドルタイムアウトがあり、クライアントが切断されると自動的にログオフされます。再接続、クライアント間のローミング、およびWorkspace Controlはサポートされていません。

3. ユーザーのホームゾーンに十分なリソースがある場合に、セッションが他の利用可能なゾーンにデフォルトで設定されるのを防ぐには、**セッションをユーザーのホームゾーンで起動することを要求する（構成されている場合）**を選択します。
4. デバイスや現在のセッションの有無にかかわらず、セッションを追跡させたい場合は、**ユーザーとともにクライアントデバイス間でセッションローミングを許可する**を選択します。「セッションローミング」を参照してください。

次の表は、**ユーザー**ページでの選択肢について説明しています。

アクセスを有効にする対象	ユーザーとユーザーグループを追加/割り当てますか？	「認証されていないユーザーにアクセスを許可する」チェックボックスを有効にしますか？
認証済みユーザーのみ	はい	いいえ
未認証ユーザーのみ	いいえ	はい
認証済みユーザーと未認証ユーザーの両方	はい	はい

アプリケーションページ

アプリケーションページは、すべてのマシンタイプで利用できます。ただし、追加できるアプリケーションは、マシンの種類によって異なります。

このページを使用して、このグループのデスクトップにパッケージ化されたアプリケーションを追加できます。

重要な考慮事項

- パッケージ化されたアプリケーションをデリバリーグループに追加できます。それらのアプリケーションを含むパッケージは、ユーザーがデスクトップまたはリモートPCにサインインするたびに自動的にマウントされます。
- デフォルトでは、追加する新しいアプリケーションはApplicationsという名前のフォルダーに配置されます。別のフォルダーを指定できます。詳細については、アプリケーションの記事を参照してください。
- アプリケーションをデリバリーグループに追加するとき、または後で、そのプロパティを変更できます。詳細については、アプリケーションの記事を参照してください。
- アプリケーションを追加しようとして、そのフォルダーに同じ名前のアプリケーションが存在する場合、追加しようとしているアプリケーションの名前を変更するよう求められます。拒否した場合、そのアプリケーションフォルダー内で一意になるようにサフィックスが付けられてアプリケーションが追加されます。
- アプリケーションを複数のデリバリーグループに追加する場合、それらのすべてのデリバリーグループでアプリケーションを表示する権限がないと、表示の問題が発生する可能性があります。そのような場合は、より高い権限を持つ管理者に相談するか、アプリケーションが追加されたすべてのデリバリーグループを含むようにスコープを拡張してください。

- 同じ名前の2つのアプリケーションを同じユーザーに公開する場合、アプリケーション名（ユーザー向け）プロパティを変更してください。そうしないと、ユーザーはCitrix Workspaceアプリで重複した名前を目にします。

構成手順

1. アプリケーションソースを表示するには、**追加**メニューを選択します。

   - **スタートメニューから:** アプリケーションは、デリバリーグループに割り当てられている現在登録済みのVDAのいずれかを介して検出されます。このソースを選択すると、検出されたアプリケーションのリストが表示された新しいページが起動します。追加するアプリケーションを選択し、**OK**を選択します。
   - **手動で:** デリバリーグループ内のVDAまたはネットワーク内の別の場所にあるアプリケーション。このソースを選択すると新しいページが開き、次の方法で追加するアプリケーションを指定します:
     - 実行可能ファイルへのパス、作業ディレクトリ、オプションのコマンドライン引数、および管理者とユーザーの表示名を入力します。
     - デリバリーグループ内のVDAからアプリケーションを選択します。これを行うには、**参照**をクリックし、VDAにアクセスするための資格情報を入力し、VDAに接続されるまで待ってから、VDAからアプリケーションを選択します。選択したアプリケーションのプロパティが、ページ上のフィールドに自動的に入力されます。
   - **既存:** 以前に展開に追加されたアプリケーション（別のデリバリーグループにある可能性もあります）。このソースを選択すると、検出されたアプリケーションのリストが表示された新しいページが起動します。追加するアプリケーションを選択し、**OK**を選択します。
   - **アプリケーションパッケージ:** App-V、MSIX、MSIX app attach、またはFlexAppアプリケーションパッケージ内のアプリケーション。このソースを選択すると、**パッケージからのアプリケーションの追加**ページが起動します。アプリケーションパッケージソースを選択し、表示された結果から追加するアプリケーションを選択し、**OK**を選択します。

     > **注:**
     >
     > - サイトにアプリケーションパッケージが構成されていない場合、このオプションは淡色表示されます。

> \> - MSIXまたはMSIXアプリ添付アプリを公開するには、デリバリーグループの機能レベルが2106以降である必要があります。FlexAppアプリの場合、機能レベルは2206以降である必要があります。機能レベルの要件が満たされていない場合、**Application package source**ドロップダウンリストの対応するオプションは淡色表示されます。

- **アプリケーショングループ:** 展開内に存在するアプリケーショングループ。

アプリケーションソースまたはアプリケーションが利用できないか無効な場合、表示されないか、選択できません。たとえば、展開にアプリケーションが追加されていない場合、**既存**のソースは利用できません。または、アプリケーションが選択されたマシンカタログ内のマシンのサポートされているセッションタイプと互換性がない場合があります。

デスクトップ（またはデスクトップ割り当てルール）ページ

このページのタイトルは、ウィザードで以前に選択したマシンカタログによって異なります。

- マルチセッションまたはプールされたシングルセッションマシンを含むカタログを選択した場合、このページは**デスクトップ**というタイトルになります。
- シングルセッションの静的マシンを含むカタログを選択し、**配信の種類**ページで「デスクトップ」を指定した場合、このページは**デスクトップ割り当てルール**というタイトルになります。

> **注:**
>
> シングルセッションの静的マシンを含むカタログを選択し、**配信の種類**ページで「アプリケーション」を指定した場合、このページは表示されません。

1. **追加**を選択します。ダイアログボックスで:
    a. **表示名**と**説明**フィールドに、Citrix Workspaceアプリに表示する情報を入力します。
    b. マルチセッションまたはプールされたシングルセッションOSマシン向け: デスクトップにタグ制限を追加するには、**このタグを持つマシンへの起動を制限する**を選択し、メニューからタグを選択します。
    c. ラジオボタンを使用して、次のいずれかを実行できます。
        i. **このデリバリーグループへのアクセス権を持つすべてのユーザーがデスクトップを使用できるようにする。** デリバリーグループ内のすべてのユーザーは、デスクトップを起動できます（プールされたマシンを持つグループの場合）、またはデスクトップを起

動したときにマシンを割り当てられます（シングルセッションの静的マシンを持つグループの場合）。

ii. **デスクトップの使用を制限**するには、ユーザーとユーザーグループを**許可リスト**に追加します。**許可リスト**上のユーザーのみがデスクトップにアクセスできます。**ブロックリストの追加、**をクリックして、ユーザーとユーザーグループをブロックリストに追加することもできます。これにより、選択したデリバリーグループ内のデスクトップをユーザーが使用できなくなります。ブロックリストは、許可リスト内のユーザーをブロックする場合にのみ意味があります。

d. グループにシングルセッションの静的マシンが含まれている場合、ユーザーあたりの最大デスクトップ数を指定します。これは1以上の値である必要があります。この設定は必須ではありません。マシンを手動で割り当てるか、RemotePCを使用してマシンを自動的に割り当てることができます。

e. デスクトップ（マルチセッションマシン用）またはデスクトップ割り当てルール（シングルセッション静的マシン用）を有効または無効にします。デスクトップを無効にすると、デスクトップの配信が停止します。デスクトップ割り当てルールを無効にすると、ユーザーへのデスクトップの自動割り当てが停止します。

f. ダイアログボックスでの作業が完了したら、**OK**を選択します。

サイト内のデスクトップの最大インスタンス数（PowerShellのみ）

サイト内のデスクトップの最大インスタンス数を構成するには（PowerShellのみ）：

- PowerShellで、適切なBrokerEntitlementPolicyRuleコマンドレットをMaxPerEntitlementInstancesパラメーターとともに使用します。たとえば、次のコマンドレットは、`tsvda-desktop`ルールを変更して、サイトで許可されるデスクトップの同時実行インスタンスの最大数を2に設定します。2つのデスクトップインスタンスが実行されているときに、3番目のサブスクライバーがデスクトップを起動しようとするとエラーが発生します。

  ```
  Set-BrokerEntitlementPolicyRule -Name tsvda-desktop
  -MaxPerEntitlementInstances 2
  ```

- ガイダンスについては、Get-Help コマンドレットを使用してください。たとえば、`Get-Help Set-BrokerEntitlementPolicyRule-Parameter MaxPerEntitlementInstances`。

アプリ保護ページ

アプリ保護ページは、すべてのマシンタイプで利用できます。

このページを使用して、Citrix公開アプリとデスクトップのセキュリティを強化できます。

次の情報は、Citrix Virtual Apps and Desktopsドキュメントのアプリ保護記事を補足するものです。

- 有効なアプリ保護エンタイトルメントが必要です。アプリ保護機能を購入するには、Citrixの営業担当者にお問い合わせください。
- アプリ保護にはXML信頼が必要です。XML信頼を有効にするには、**設定 > XML信頼を有効にする**に移動します。

保護は以下の条件で適用されます。

- **画面キャプチャ防止**：
  - WindowsおよびmacOSでは、保護されたコンテンツのウィンドウのみが空白になります。保護されたウィンドウが最小化されていない場合、アプリ保護がアクティブになります。
  - Linuxでは、キャプチャ全体が空白になります。保護されたウィンドウが最小化されているかどうかにかかわらず、アプリ保護がアクティブになります。
- **キーロギング防止**：保護されたウィンドウがフォーカスされている場合に有効になります。保護を無効にするには、別のウィンドウにフォーカスを変更します。

スコープページ

スコープページは、すべてのマシンタイプで利用できます。

このページを使用して、組織に関連する方法でオブジェクト（たとえば、接続、カタログ、デリバリーグループ）をグループ化します。

ライセンス割り当てページ

ライセンス割り当てページは、すべてのマシンタイプで利用できます。

このページを使用して、デリバリーグループで使用するライセンスを指定します。デフォルトでは、デリバリーグループはサイトライセンスを使用します。詳細については、「マルチタイプライセンス」を参照してください。

ポリシーセットページ

ポリシーセットページは、すべてのマシンタイプで利用できます。

このページを使用して、このデリバリーグループが使用するポリシーセットを指定します。

ローカルホストキャッシュ設定ページ

このページは、電源管理されたシングルセッションのプールされたマシンを含むデリバリーグループの場合にのみ利用できます。

デフォルトでは、電源管理されているプールされたマシンは、データ漏洩のリスクがあるため、ローカルホストキャッシュ (LHC) モードでは利用できません。このデフォルトの動作を変更し、LHCモードで新しいユーザー接続に利用できるようにするには、**リソースを維持する**を選択します。

または、PowerShellコマンドを使用してデフォルトの動作を変更できます。詳細については、アプリケーションとデスクトップのサポートを参照してください。

> **重要:**
>
> 電源管理されているシングルセッションのプールされたマシンへのアクセスを有効にすると、以前のユーザーセッションからのデータや変更が、後続のセッションに存在してしまう可能性があります。

ローカルホストキャッシュにおける1回限りの使用のプールされたデスクトップ

ローカルホストキャッシュ (LHC) の停止中、プールされたデスクトップは1回限り使用できます。これは、対応可能なVDAにハイジーンブロブを発行し、再起動を開始することで実現されます。このプロセスにより、停止からの復旧時にデスクトップのクリーンな状態が保証されます。対応できないマシンやレガシーマシンでは、再利用が明示的に有効になっている場合にのみ参加します。この機能は、停止中の可用性をよりシームレスにすることで、顧客満足度を向上させます。

前提条件

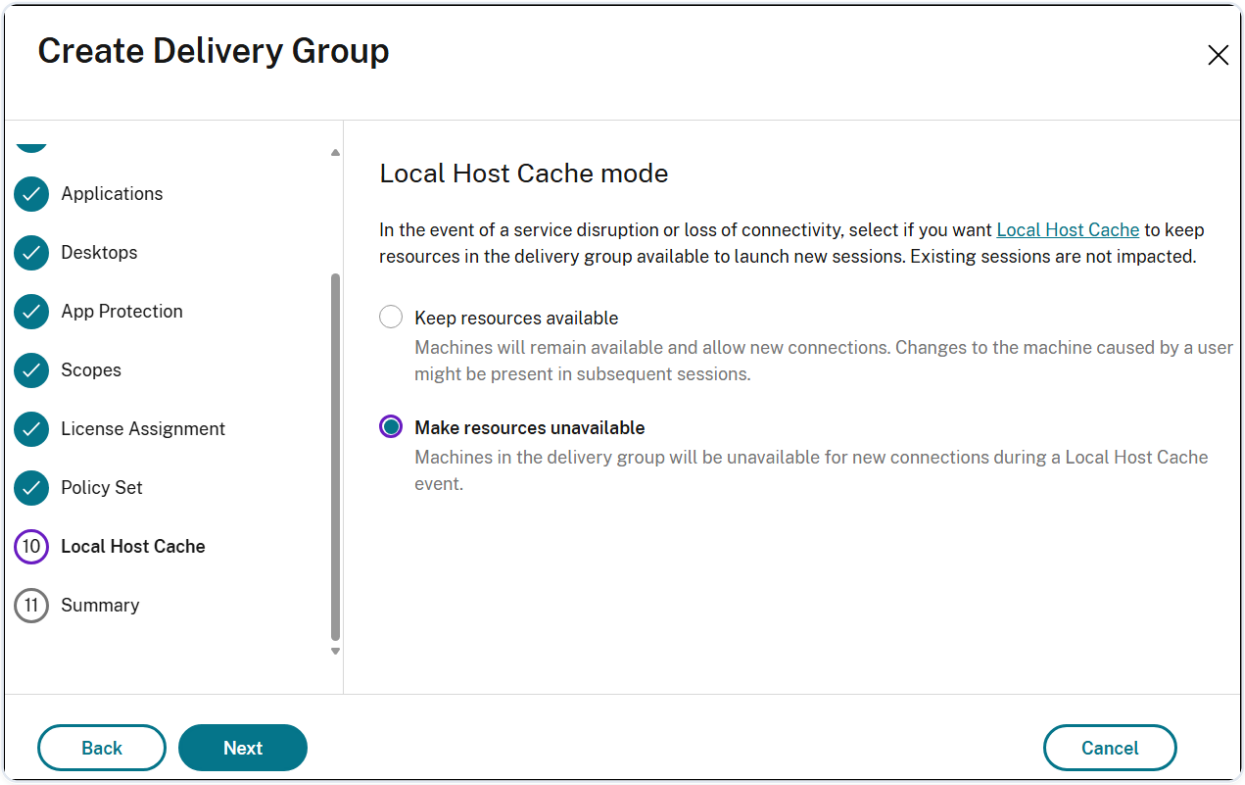
- 完全なハイジーン適用にはVDAバージョン2407以降。レガシーVDA (VDAバージョン2407以前) は、再利用が有効になっている場合にのみ使用できます。これらのVDAは、ハイジーンブロブや強制再起動を受け取りません。
- シングルセッションマシンを含むマシンカタログ。

プールされたデスクトップの1回限りの使用を構成する

1. VDAビルド2407以降を使用して、シングルセッションマシンを含むMCSカタログを作成します。
2. 対応するデリバリーグループを作成します。Remote PowerShellからデリバリーグループの `ReuseMachinesWithoutShutdownInOutage` デスクトップグループ設定を `false` に設定する

か、または、デリバリーグループの作成時にWeb Studioの**ローカルホストキャッシュモード**ページで**リソースを利用不可にする**を選択します。

```
Set-BrokerDesktopGroup -Name "name"
-ReuseMachinesWithoutShutdownInOutage $false
```



3. 構成が完了すると、LHC停止モード中に、マシンは1回限り使用できます。LHC停止モードから復旧すると、汚染されたマシンは再起動され、再度使用できるようになります。

> **注:**
>
> マシンは、最新の電源投入後にユーザーセッションが開始されると、汚染済みとして分類されます。汚染されていないマシンとは、最新の電源投入イベント以降、ユーザーセッションが起動されていないマシンを指します。

概要ページ

デリバリーグループの名前を入力します。オプションで、Citrix Workspaceアプリと Studioに表示される説明を入力することもできます。

概要情報を確認し、**「完了」**をクリックします。

制限事項

デスクトップをクライアントIPアドレスに割り当てる機能は、ごく限られたクライアントの種類と構成でのみ機能します。クライアントIPアドレスに基づいてアクセスフィルタリングを実行すると、クラウドクライアントにはパブリックIPアドレスが使用されます。

詳細情報

- デリバリーグループの管理
- アプリケーション

デリバリーグループの管理

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

はじめに

この記事では、管理コンソールからデリバリーグループを管理する手順について説明します。グループ作成時に指定した設定を変更するだけでなく、デリバリーグループの作成時には利用できないその他の設定も構成できます。

手順のカテゴリには、一般、ユーザー、マシン、セッションがあります。一部のタスクは複数のカテゴリにまたがります。たとえば、「ユーザーがマシンに接続できないようにする」はマシンのカテゴリで説明されていますが、ユーザーにも影響します。あるカテゴリでタスクが見つからない場合は、関連するカテゴリを確認してください。

その他の記事にも関連情報が含まれています。

- アプリケーションには、デリバリーグループ内のアプリケーションの管理に関する情報が含まれています。
- デリバリーグループの管理には、Delivery Group Administratorの組み込みロール権限が必要です。詳細については、委任管理を参照してください。

全般

- グループの詳細を表示
- デリバリーの種類を変更
- StoreFront™アドレスを変更
- 機能レベルを変更
- Remote PC Accessデリバリーグループを管理
- フォルダーを使用してデリバリーグループを整理する(#organize-delivery-groups-using-folders)
- アプリ保護を管理する(#manage-app-protection)
- デリバリーグループのサスペンド機能を変更する(#change-suspend-capability-for-a-delivery-group)

グループの詳細を表示

1. 検索機能を使用して特定のデリバリーグループを検索します。手順については、インスタンスの検索を参照してください。
2. 検索結果から、必要に応じてグループを選択します。
3. グループ列の説明については、次の表を参照してください。
4. このグループに関する詳細情報については、下部の詳細ペインにあるタブをクリックしてください。

列	説明
デリバリーグループ	グループ名とセッションの種類。セッションの種類には、シングルセッションOSとマルチセッションOSが含まれます。
配信中	このグループから配信されるリソースの種類。指定できる値には、アプリケーション、デスクトップ、アプリケーションとデスクトップがあります。デリバリーグループが専用マシンで構成されている場合、「静的マシン割り当て」が表示されます。
使用中のセッション	セットアップされているマシンの数と、切断状態にあるマシンの数。

列	説明
割り当て済み数	デリバリーグループに割り当てられているカタログ内のマシンの数。
フォルダー	**デリバリーグループ**ツリー内でのグループの場所。グループが存在するフォルダーの名前（末尾のバックスラッシュを含む）が表示されます。グループがルートレベルにある場合は `-` と表示されます。

デリバリーグループのデリバリーの種類を変更する

デリバリーの種類は、グループが提供できるもの（アプリケーション、デスクトップ、またはその両方）を示します。

アプリケーションのみまたは**デスクトップとアプリケーション**のタイプを**デスクトップのみ**のタイプに変更する前に、グループからすべてのアプリケーションを削除してください。

1. 左側のペインで**デリバリーグループ**を選択します。
2. グループを選択し、アクションバーで**編集**をクリックします。
3. **デリバリーの種類**ページで、目的のデリバリーの種類を選択します。
4. **適用**をクリックすると、行った変更が適用され、ウィンドウが開いたままになります。または、**保存**をクリックすると、変更が適用され、ウィンドウが閉じます。

StoreFrontアドレスを変更する

1. 左側のペインで**デリバリーグループ**を選択します。
2. グループを選択し、アクションバーで**編集**をクリックします。
3. 「**StoreFront**」ページで、StoreFront URLを選択または追加します。これらのURLは、デリバリーグループ内の各マシンにインストールされているCitrix Workspace™アプリによって使用されます。
4. 変更を適用してウィンドウを開いたままにするには、**［適用］をクリックします。または、変更を適用してウィンドウを閉じるには、**［保存］**をクリックします。

左側のペインで**［StoreFront］**を選択して、StoreFrontサーバーアドレスを指定することもできます。

機能レベルを変更する

デリバリーグループ内のマシン上のVDAと、デリバリーグループで使用されるマシンを含むマシンカタログをアップグレードした後、デリバリーグループの機能レベルを変更します。

開始する前に：

- Citrix Provisioning™（旧Provisioning Services）を使用している場合は、Citrix Provisioningコンソールで VDAバージョンをアップグレードします。
- アップグレードされたVDAを含むマシンを起動して、Delivery Controllerに登録できるようにします。このプロセスにより、デリバリーグループで何がアップグレードされる必要があるかがコンソールに通知されます。
- 以前のVDAバージョンを引き続き使用する必要がある場合、新しい製品機能は利用できません。詳しくは、アップグレードのドキュメントを参照してください。

デリバリーグループの機能レベルを変更するには：

1. 左側のペインで、**［デリバリーグループ］**を選択します。
2. グループを選択し、アクションバーの**機能レベルの変更**をクリックします。**機能レベルの変更**アクションは、アップグレードされたVDAが検出された場合にのみ表示されます。
3. **変更**をクリックします。

ディスプレイには、どのマシンが機能レベルに変更できないか、およびその理由が表示されます。その後、変更アクションをキャンセルし、マシンの問題を解決してから、変更アクションを再度実行できます。

変更が完了したら、マシンを以前の状態に戻すことができます。デリバリーグループを選択し、アクションバーで を選択します。

Remote PC Accessデリバリーグループの管理

Remote PC Accessマシンカタログ内のマシンが割り当てられていない場合、そのマシンは一時的にそのカタログに関連付けられたデリバリーグループに割り当てられます。この一時的な割り当てにより、後でマシンをユーザーに割り当てることができます。

デリバリーグループとマシンカタログの関連付けには、優先度値があります。優先度は、マシンがシステムに登録されるとき、またはユーザーがマシン割り当てを必要とするときに、マシンに割り当てられるデリバリーグループを決定します。値が小さいほど、優先度が高くなります。Remote PC Accessマシンカタログに複数のデリバリーグループ割り当てがある場合、ソフトウェアは最も優先度の高い一致を選択します。この優先度値を設定するには、PowerShell SDKを使用します。

リモートPCアクセス マシンカタログは、最初に作成されたときにデリバリーグループに関連付けられます。後でカタログに追加されたマシンアカウントまたは組織単位は、デリバリーグループに追加できます。この関連付けは、オン/オフを切り替えることができます。

デリバリーグループとのRemote PC Accessマシンカタログの関連付けを追加または削除するには：

1. 左ペインで**デリバリーグループ**を選択します。
2. Remote PC Accessグループを選択します。
3. **詳細**セクションで、**マシンカタログ**タブをクリックし、Remote PC Accessカタログを選択します。
4. 関連付けを追加または復元するには、**デスクトップの追加**をクリックします。関連付けを削除するには、**関連付けの削除**をクリックします。

フォルダーを使用したデリバリーグループの整理

フォルダーを作成してデリバリーグループを整理し、簡単にアクセスできるようにすることができます。

> **ヒント:**
>
> アクションバーの右上にある**フォルダー**アイコンをクリックして、デリバリーグループノードの優先するデフォルトビュー（フォルダービューまたはリストビュー）を設定できます。

必要な役割

デフォルトでは、デリバリーグループフォルダーを作成および管理するには、次の組み込み役割が必要です：Cloud Administrator、Full Administrator、またはDelivery Group Administrator。必要に応じて、デリバリーグループフォルダーの作成および管理のための役割をカスタマイズできます。詳しくは、「必要な権限」を参照してください。

デリバリーグループフォルダーを作成する

開始する前に、デリバリーグループの整理方法を計画してください。次の点を考慮してください。

- フォルダーは最大5レベルまでネストできます（デフォルトのルートフォルダーを除く）。
- フォルダーには、デリバリーグループとサブフォルダーを含めることができます。
- Web Studioのすべてのノード（**マシンカタログ**、**デリバリーグループ**、**アプリケーション**、**アプリケーショングループ**など）は、バックエンドで同じフォルダーツリーを共有します。フォ

ルダーの名前変更や移動時に名前の競合を避けるため、異なるノード間で最上位フォルダーには一意の名前を使用してください。

`New-BrokerAdminFolder` SDKコマンドレットを使用してフォルダーを作成し、それを**デリバリーグループ**ノードの下に表示させたい場合は、`Set-BrokerAdminFolderMetadata` コマンドレットを使用して`ContainsDeliveryGroups` メタデータを追加する必要があります。

例:

```
Set-BrokerAdminFolderMetadata -AdminFolderId {adminFolderUid} -Name
ContainsDeliveryGroups -Value true
```

デリバリーグループフォルダーを作成するには、次の手順に従います。

1. 左側のペインで**デリバリーグループ**を選択します。
2. フォルダー階層でフォルダーを選択し、**アクション**バーで**フォルダーの作成**を選択します。
3. 新しいフォルダーの名前を入力し、**完了**をクリックします。

ヒント:

意図しない場所にフォルダーを作成してしまった場合は、正しい場所にドラッグできます。

デリバリーグループを移動する

デリバリーグループはフォルダー間で移動できます。詳細な手順は次のとおりです。

1. 左側のペインで**デリバリーグループ**を選択します。
2. フォルダーごとにグループを表示します。フォルダー階層の上にある **View all** をオンにすると、すべてのグループを一度に表示することもできます。
3. グループを右クリックし、**Move Delivery Group** を選択します。
4. グループを移動するフォルダーを選択し、**Done** をクリックします。

ヒント:

グループをフォルダーにドラッグできます。

デリバリーグループフォルダーの管理

デリバリーグループフォルダーを削除、名前変更、移動できます。

フォルダーとそのサブフォルダーにデリバリーグループが含まれていない場合にのみ、フォルダーを削除できることに注意してください。

フォルダーを管理するには、次の手順に従います。

1. 左側のペインで**デリバリーグループ**を選択します。
2. フォルダー階層でフォルダーを選択し、必要に応じて**アクション**バーでアクションを選択します。
    - フォルダーの名前を変更するには、**Rename Folder**を選択します。
    - フォルダーを削除するには、**Delete Folder**を選択します。
    - フォルダーを移動するには、**Move Folder**を選択します。
3. 画面の指示に従って、残りの手順を完了します。

必要な権限

次の表に、デリバリーグループフォルダーに対してアクションを実行するために必要な権限を示します。

アクション	必要な権限
デリバリーグループフォルダーを作成する	デリバリーグループフォルダーの作成
デリバリーグループフォルダーを削除する	デリバリーグループフォルダーの削除
デリバリーグループフォルダーを移動する	デリバリーグループフォルダーの移動
デリバリーグループフォルダーの名前を変更する	デリバリーグループフォルダーの編集
デリバリーグループをフォルダーに移動する	デリバリーグループフォルダーの編集とデリバリーグループプロパティの編集

アプリ保護の管理

以下の情報は、アプリ保護(/ja-jp/citrix-virtual-apps-desktops/2503/secure/app-protection.html)の補足です。以下の点に注意してください:

- 有効なApp Protectionエンタイトルメントが必要です。App Protection機能を購入するには、Citrixの営業担当者にお問い合わせください。
- App ProtectionにはXML信頼が必要です。XML信頼を有効にするには、**設定 > XML信頼を有効にする**に移動します。
- 画面キャプチャ防止に関して:
  - WindowsおよびmacOSでは、保護されたコンテンツのウィンドウのみが空白になります。保護されたウィンドウが最小化されていない場合、App Protectionはアクティブになります。
  - Linuxでは、キャプチャ全体が空白になります。保護されたウィンドウが最小化されているかどうかにかかわらず、App Protectionはアクティブになります。

デリバリーグループのApp Protection方法を選択するには、次の手順に従います:

1. 左側のペインで**デリバリーグループ**を選択します。
2. グループを選択し、アクションバーで**編集**を選択します。
3. **App Protection**ページで、次のオプションが表示されます:

オプション	説明
適用しない	設定を適用しない場合は、このオプションを選択します。
このデリバリーグループに適用	**キーロギング対策**および/または**キーキャプチャ対策**オプションを選択します。これらの各設定にカーソルを合わせると、ツールチップに詳細が表示されます。
コンテキストに応じて適用	この設定を適用するには、**アクセスポリシー設定**ページでアクセスポリシーを構成します。
	1. 左ペインで**アクセスポリシー**をクリックし、**追加**をクリックします。
	1. **ポリシーの追加**ページで、次の操作を行います。
	- i. **ポリシー名**を入力し、必要に応じて設定を構成します。

オプション	説明
	- ii. **フィルター**フィールドと**値**フィールドに詳細を入力し、**完了**をクリックします。新しいポリシーは**アプリ保護**ページに表示されます。このポリシーに必要な設定を有効にします。
	- iii. **保存**をクリックします。

4. 「**デリバリーグループ**」ページで、「**デリバリーグループ**」を選択し、下部にある「**詳細**」タブをクリックします。適用された新しい「**アプリ保護**」設定が表示されます。

デリバリーグループのサスペンド機能を変更する

デリバリーグループのサスペンド機能を必須またはオプションにする：

- **必須** - デリバリーグループには、サスペンド可能なVMのみを含めることができます。
- **オプション** - デリバリーグループには、サスペンド可能なVMとサスペンド不可能なVMの両方を含めることができます。

始める前に

デリバリーグループ内のすべてのVMがサスペンド可能である場合にのみ、デリバリーグループのサスペンド機能を`Required`に変更できます。

デリバリーグループのサスペンド機能を変更するには：

1. Web Studioから、左ペインの**デリバリーグループ**に移動します。
2. グループを選択し、アクションバーで**中断機能の変更**をクリックします。
3. 「**はい**」をクリックして操作を確定します。

ユーザー

このセクションでは、次のトピックについて説明します。

- ユーザー設定の変更
- ユーザーの追加または削除
- ユーザー割り当ての管理

デリバリーグループのユーザー設定を変更する

このページの名前は、**ユーザー設定** または **基本設定** のいずれかで表示されます。

1. 左ペインで**デリバリーグループ**を選択します。
2. グループを選択し、アクションバーで**編集**をクリックします。
3. **ユーザー設定**（または**基本設定**）ページで、次の表の設定を変更します。
4. **適用**をクリックして変更を適用し、ウィンドウを開いたままにします。または、**保存**をクリックして変更を適用し、ウィンドウを閉じます。

設定	説明
説明	Citrix Workspace（またはStoreFront）が使用し、ユーザーに表示されるテキスト。
デリバリーグループを有効にする	デリバリーグループが有効になっているかどうか。
タイムゾーン	このデリバリーグループのマシンが存在する必要があるタイムゾーン。このオプションには、サイトでサポートされているタイムゾーンが一覧表示されます。**注：**デリバリーグループのタイムゾーンを変更すると、そのデリバリーグループ内のマシンが再起動される場合があります。これを回避するには、稼働時間外にタイムゾーン設定を変更してください。
Secure ICA® を有効にする	ICAプロトコルを暗号化するSecureICAを使用して、デリバリーグループ内のマシンとの通信を保護します。デフォルトのレベルは128ビットです。レベルはSDKを使用して変更できます。Citrixは、パブリックネットワークを通過する際にTLS暗号化などのより多くの暗号化方法を使用することを推奨しています。また、SecureICAはデータ整合性をチェックしません。

デリバリーグループ内のユーザーを追加または削除する

ユーザーに関する詳細については、「ユーザー」を参照してください。

1. 左側のペインで、 を選択します。
2. グループを選択し、アクションバーで をクリックします。
3. ページで：

- ユーザーを追加するには、**追加**をクリックし、追加するユーザーを指定します。
- ユーザーを削除するには、1人以上のユーザーを選択し、**削除**をクリックします。
- 認証されていないユーザーによるアクセスを許可するには、チェックボックスをオンまたはオフにします。

4. 変更を適用してウィンドウを開いたままにするには、**適用**をクリックします。または、変更を適用してウィンドウを閉じるには、**保存**をクリックします。

ユーザーリストをインポートまたはエクスポートする

物理的なシングルセッションOSマシンを含むデリバリーグループの場合、デリバリーグループの作成後に.csvファイルからユーザー情報をインポートできます。ユーザー情報を.csvファイルにエクスポートすることもできます。.csvファイルには、以前の製品バージョンのデータを含めることができます。

CSVファイルの最初の行には、コンマで区切られた2つの列ヘッダーが含まれている必要があります。最初のヘッダーが`Machine Account`で、2番目のヘッダーが`User Names`であることを確認してください。（追加のヘッダーを含めることはできますが、サポートされていません。）ファイルの以降の行には、コンマ区切りのデータが含まれます。`Machine Account`エントリは、コンピューターSID、FQDN、またはドメインとコンピューター名のペアにすることができます。

ユーザー情報をインポートまたはエクスポートするには：

1. 左側のペインで、 を選択します。
2. グループを選択し、アクションバーで**編集**をクリックします。
3. **マシン割り当て**ページで、**リストのインポート**または**リストのエクスポート**を選択し、ファイルの場所を参照します。
4. 加えた変更を適用してウィンドウを開いたままにするには、**適用**をクリックします。または、変更を適用してウィンドウを閉じるには、**保存**をクリックします。

ユーザー割り当ての管理

デリバリーグループ内のマシンのユーザー割り当てを管理します。デリバリーグループにデスクトップ割り当てルールが構成されている場合、マシンは最初のデスクトップ起動時にユーザーにランダムに割り当てられ、ユーザー割り当てが変更されない限り、ユーザーに割り当てられたままになります。割り当てられていないマシンを特定のユーザーに手動で割り当てる場合、またはマシンの既存のユーザー割り当てを変更する場合は、このトピックで説明されている手順に従って変更を行います。これらの手順を使用すると、ユーザーに割り当てられたマシンのCitrix Workspaceアプリに表示される名前を変更することもできます。

詳細な手順は次のとおりです。

1. コンソールで、左側のペインから**デリバリーグループ**を選択します。
2. グループを選択し、アクションバーで**編集**を選択します。
3. 左側のペインで、**マシン割り当て**を選択します。グループ内の各マシンの次の詳細が表示されます。

    - **マシン名:** マシンの名前が表示されます。
    - **表示名:** Citrix Workspaceアプリでのマシンの表示名が表示されます。
    - **ユーザー:** このマシンに割り当てられているユーザーが表示されます。デスクトップ割り当てルールが構成されている場合、マシンは最初のデスクトップ起動時にユーザーにランダムに割り当てられ、ユーザー割り当てが変更されない限り、ユーザーに割り当てられたままになります。

4. マシンを見つけ、それにユーザーを割り当てるか、ユーザー割り当てを変更します。

    - ユーザーを参照するには、**参照**をクリックします。
    - **ユーザー**列に、セミコロンで区切られたユーザー名のリストを入力します。
    - CSVファイルを使用して設定の詳細をインポートするには、「**CSVファイルからインポート**」をクリックします。

5. (オプション) マシンがユーザーに割り当てられている場合は、必要に応じて表示名を変更します。

> 「**注：**」:
>
> 表示名フィールドは、マシンがユーザーに割り当てられている場合にのみ有効になります。
>
> - マシンがデスクトップ割り当てルールに基づいてユーザーに割り当てられている場合、このフィールドにはそのルールで構成された表示名が表示されます。
> - マシンが手動でユーザーに割り当てられ、フィールドが空白のままの場合、デリバリーグループの公開名（指定されている場合）がマシンの表示名として使用されます。公開名が指定されていない場合は、デリバリーグループの名前が使用されます。デリバリーグループの公開名はPowerShellを介してのみ指定できることに注意してください。

6. 変更を適用してウィンドウを開いたままにするには、「**適用**」を選択します。または、変更を適用してウィンドウを閉じるには、「**OK**」を選択します。

マシン

- マシンからユーザーへの割り当てを変更する
- 電源管理されたシングルセッションのプールされたVDAでローカルホストキャッシュを有効にする
- ユーザーあたりの最大マシン数を変更する
- マシンを更新する
- デスクトップのタグ制限を追加、変更、または削除する
- マシンを削除する
- マシンへのアクセスを制限する
- ユーザーがマシンに接続できないようにする（メンテナンスモード）
- マシンのシャットダウンと再起動
- マシンの再起動スケジュールの作成と管理
- 1回限りの再起動スケジュールを有効にする
- 管理対象マシンの電源を管理する

デリバリーグループ内のマシンからユーザーへの割り当てを変更する

MCSでプロビジョニングされたシングルセッションOSマシンの割り当ては変更できます。マルチセッションOSマシンまたはCitrix Provisioningでプロビジョニングされたマシンの割り当ては変更できません。

1. 左ペインで**デリバリーグループ**を選択します。
2. グループを選択し、アクションバーで**編集**をクリックします。
3. **デスクトップ**または**デスクトップ割り当てルール**ページ（ページタイトルはデリバリーグループが使用するマシンカタログの種類によって異なります）で、新しいユーザーを指定します。
4. 加えた変更を適用してウィンドウを開いたままにするには、**適用**をクリックします。または、変更を適用してウィンドウを閉じるには、**保存**をクリックします。

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

デフォルトでは、電源管理されたシングルセッションプールマシンは、ローカルホストキャッシュモードでは利用できません。このデフォルトの動作は、デリバリーグループごとに上書きできます。詳細な手順は次のとおりです。

1. Studioから、左ペインで**デリバリーグループ**を選択します。

   グループリストで、MCSまたはCitrix Provisioningによってプロビジョニングされたシングルセッションプールマシンを含むグループには、警告アイコンが表示されます。
2. 必要に応じてグループを選択し、アクションバーの を選択します。
3. **ローカルホストキャッシュ**ページで、**リソースを常に利用可能にする**を選択します。
4. **適用**を選択して変更を適用し、ウィンドウを開いたままにします。または、**OK**を選択して変更を適用し、ウィンドウを閉じます。

または、PowerShellコマンドを使用してデフォルトの動作を上書きできます。詳細については、「アプリケーションとデスクトップのサポート」を参照してください。

> **重要：**
>
> 電源管理されたシングルセッションのプールされたマシンへのアクセスを有効にすると、以前のユーザーセッションからのデータと変更が、後続のセッションに存在してしまう可能性があります。

デリバリーグループ内のユーザーあたりの最大マシン数を変更する

1. 左ペインで**デリバリーグループ**を選択します。
2. グループを選択し、アクションバーで**編集**をクリックします。
3. **デスクトップ割り当てルール**ページで、ユーザーあたりの最大デスクトップ数を設定します。
4. 変更を適用してウィンドウを開いたままにするには、**適用**をクリックします。または、変更を適用してウィンドウを閉じるには、**保存**をクリックします。

デリバリーグループ内のマシンを更新する

1. 左ペインで**デリバリーグループ**を選択します。
2. グループを選択し、アクションバーで**マシンの表示**をクリックします。
3. マシンを選択し、アクションバーで**マシンの更新**をクリックします。

別のイメージを選択するには、**イメージ**を選択してからスナップショットを選択します。

変更を適用してマシンユーザーに通知するには、**エンドユーザーへのロールアウト通知**を選択します。次に、以下を指定します。

- マスターイメージを更新するタイミング: 今すぐ、または次回の再起動時
- 再起動の分散時間（グループ内のすべてのマシンの更新を開始するまでの合計時間）
- ユーザーに再起動が通知されるかどうか
- ユーザーが受信するメッセージ

デスクトップのタグ制限を追加、変更、または削除する

タグ制限の追加、変更、削除は、起動対象となるデスクトップに予期せぬ影響を与える可能性があります。タグの考慮事項と注意点を確認してください。

1. 左ペインで**デリバリーグループ**を選択します。
2. グループを選択し、アクションバーで**編集**をクリックします。
3. **デスクトップ**ページで、デスクトップを選択し、**編集**をクリックします。
4. タグ制限を追加するには、**タグを持つマシンへの起動を制限する**を選択し、タグを選択します。
5. タグ制限を変更または削除するには、次のいずれかの操作を行います。
    - 別のタグを選択します。
    - **このタグを持つマシンへの起動を制限する**のチェックを外して、タグ制限を削除します。
6. 加えた変更を適用してウィンドウを開いたままにするには、「**適用**」をクリックします。または、変更を適用してウィンドウを閉じるには、「**保存**」をクリックします。

デリバリーグループからマシンを削除する

マシンを削除すると、デリバリーグループから削除されます。デリバリーグループが使用するマシンカタログからは削除されません。したがって、そのマシンは別のデリバリーグループに割り当てることができます。

マシンを削除する前に、シャットダウンする必要があります。削除中にユーザーがマシンに接続するのを一時的に停止するには、シャットダウンする前に、マシンをメンテナンスモードにします。

マシンには個人データが含まれている可能性があるため、別のユーザーにマシンを割り当てる前に注意してください。マシンの再イメージングを検討してください。

1. 左ペインで「**デリバリーグループ**」を選択します。
2. グループを選択し、アクションバーで「**マシンの表示**」をクリックします。
3. マシンがシャットダウンされていることを確認します。
4. マシンを選択し、アクションバーで**デリバリーグループから削除**をクリックします。

マシンが使用する接続を介して、デリバリーグループからマシンを削除することもできます。

デリバリーグループ内のマシンへのアクセスを制限する

デリバリーグループ内のリソースへのアクセスを制限するために行った変更は、使用する方法に関係なく、以前の設定に優先します。次のことができます。

- **委任管理スコープを使用して管理者へのアクセスを制限する:** 管理者がすべてのアプリケーションにアクセスできるようにするスコープと、特定のアプリケーションにのみアクセスを提供する別のスコープを作成して割り当てることができます。詳細については、「委任管理」を参照してください。
- **スマートアクセス ポリシー式を介してユーザーのアクセスを制限する:** 特定のデリバリーグループへのユーザーアクセスを制御するために、アクセス ポリシー ルールを構成できます。例としては、次のものがあります。
  - ユーザーのサブセットへのアクセスを制限し、許可されたユーザーデバイスを指定します。
  - Workspace を介して接続されたユーザー (StoreFront ではなく) へのアクセスを制限します。
  - 特定の Workspace URL を介して接続されたユーザーへのアクセスを制限します。

このセクションでは、アクセスポリシー規則を使用してデリバリーグループへのユーザーアクセスを制限する方法について説明します。

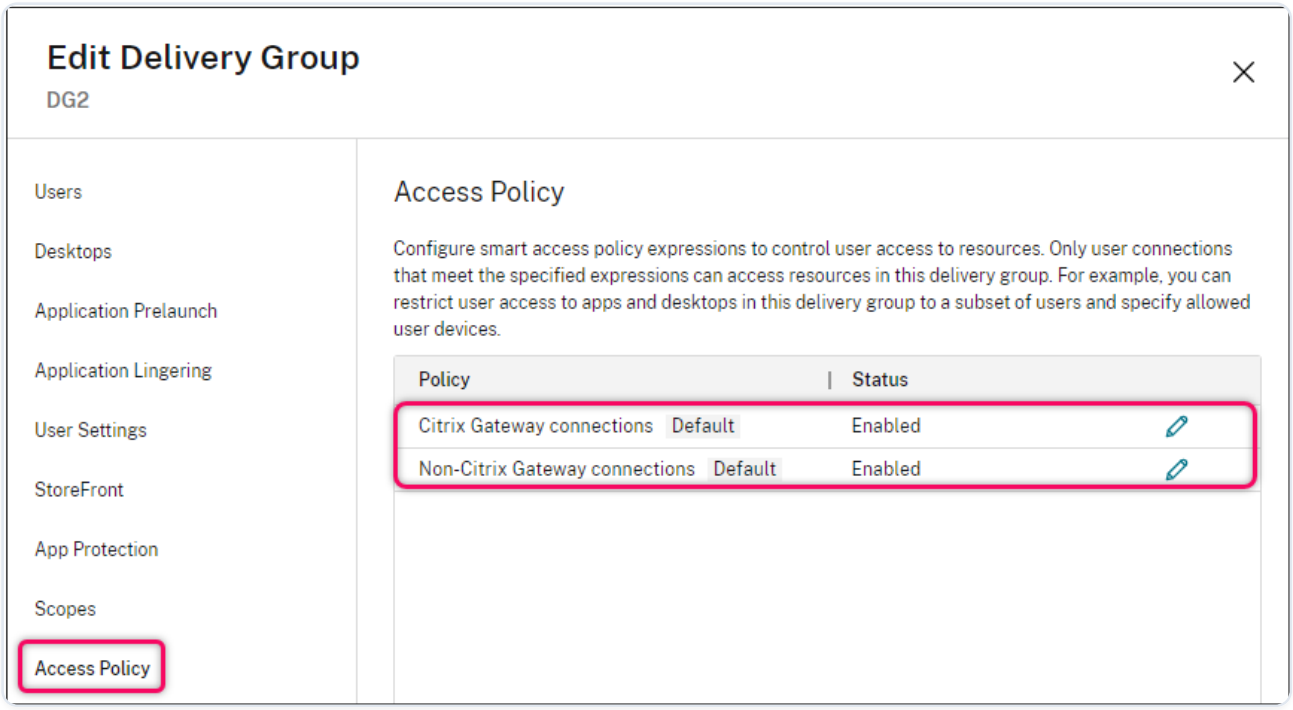
- アクセスポリシー規則について
- アクセスポリシー規則を追加する
- Web Studio を使用してアクセスポリシー規則を管理する
- PowerShell を使用してポリシー規則を追加および調整する

アクセスポリシー規則について

デリバリーグループに対して複数のアクセスポリシー規則を構成できます。デリバリーグループ内のアプリとデスクトップは、ユーザーの接続がデリバリーグループに対して定義したアクセスポ

リシー規則のいずれかに一致する場合に、順序に関係なくユーザーの StoreFront または Workspace に表示されます。

各規則は個別に有効または無効にできます。無効な規則は、アクセスポリシーが評価されるときに無視されます。



Web Studio のアクセスポリシーリストには、以下のデフォルトの SmartAccess ポリシー規則が含まれています。必要に応じて追加できます。

- **Citrix Gateway 接続。** このポリシーでは、Citrix Gateway を介して行われたユーザー接続のみがデリバリーグループ内のリソースにアクセスできます。デバイスポスチャまたはネットワークロケーション機能のいずれかが有効になっている場合に Workspace を介して行われたユーザー接続も、Citrix Gateway を介した接続と見なされます。
- **Citrix Gateway 以外の接続。** このポリシーでは、Citrix Gateway を介して行われていないユーザー接続のみがデリバリーグループ内のリソースにアクセスできます。

注:

- デフォルトのルールが新しく構成されたルールを上書きしないようにするには、デフォルトのルールを無効にするか、新しいポリシーで使用されているフィルターを除外するように調整する必要があります。

- デフォルトのポリシーは削除できませんが、無効にすることはできます。ポリシーを無効にするには、**［編集］**アイコンをクリックし、**［ポリシーの状態］**を**［無効］**に変更します。
- ポリシーリストには、PowerShellコマンドを使用して追加されたルールも表示されます。これらのポリシーは削除できますが、Web Studioで編集することはできません。

Web Studioを使用してアクセスポリシールールを追加する

アクセスポリシールールは、一連のフィルターで構成されます。フィルターについて詳しくは、この記事を参照してください。アクセスポリシールールを追加するときは、必要に応じて複数の条件フィルターをルールに追加します。

Web Studio を使用してデリバリーグループのポリシーを追加するには、次の手順に従います。

1. コンソールで、左ペインの**［デリバリーグループ］**を選択します。
2. グループを選択し、アクションバーの**［編集］**をクリックします。
3. **［アクセスポリシー］**ページで、**［追加］**をクリックします。**［ポリシーの追加］**ページが表示されます。

   (/en-us/citrix-virtual-apps-desktops/2503/media/delivery-groups-access-control.png)
4. **［ポリシー名］**フィールドに、ポリシーのわかりやすい名前を入力します。この名前は展開内で一意である必要があります。
5. 許可されるユーザー接続の基準を定義するには、次の手順に従います。

   a. **［次の条件を満たす接続］**を選択します。

   b. **［条件の追加］**をクリックします。

   c. **［フィルター］**フィールドに、使用するフィルターの名前を入力します。**［値］**フィールドに、フィルターの目的の値を入力します。たとえば、Workspace（StoreFrontではなく）を介して接続されたユーザーのみがこのデリバリーグループのリソースにアクセスできるようにするには、**［フィルター］**に`Citrix-Via-Workspace`、**［値］**に`True`と入力します。

   d. さらに条件を追加するには、手順b～cを繰り返します。

   e. 条件間の関係を選択します。

      - **いずれかに一致**。受信ユーザー接続が構成されたフィルター条件のいずれかを満たす場合にのみアクセスを許可します。

- **すべてに一致**。受信ユーザー接続が構成されたフィルター条件のすべてを満たす場合にのみアクセスを許可します。

6. 禁止されたユーザー接続の条件を定義するには、次の手順に従います。

   a. **次の条件のいずれも満たさない接続**を選択します。

   b. **条件の追加**をクリックします。

   c. 「**フィルター**」フィールドに、使用するフィルターの名前を入力します。「**値**」フィールドに、フィルターの目的の値を入力します。たとえば、`example.cloud.com` Workspace URL を介して接続しているユーザーがこのデリバリーグループのリソースにアクセスするのを禁止するには、「**フィルター**」に`Citrix.Workspace.UsingDomain`、「**値**」に`example.cloud.com`と入力します。

   d. さらに条件を追加するには、手順b～cを繰り返します。

   > **注:**
   >
   > 構成された条件のいずれかを満たすユーザー接続は、このデリバリーグループのリソースへのアクセスが禁止されます。

7. **完了**をクリックします。

   新しいポリシーがポリシーリストに表示されます。

8. この新しいポリシーでカバーされる接続との意図しない重複を避けるために、デフォルトのポリシー規則を確認し、調整してください。既存のポリシーを調整するには、以下の方法を使用します。

   - デフォルトのポリシー規則を無効にします。
   - 新しいポリシーの包含条件に追加したSmartAccessフィルターを除外するように、デフォルトのポリシー規則を構成します。詳細については、「Web Studioを使用したポリシー規則の管理」および「PowerShellを使用したアクセスポリシー規則の追加と管理」を参照してください。

> **重要:**
>
> 「アクセスポリシー規則について」で説明されているように、ユーザーの接続がデリバリーグループ内の1つ以上のポリシー規則に一致すると、ユーザーはそのリソースにアク

> セスできるようになります。したがって、規則を作成した後、新しい規則でカバーされる接続との意図しない重複を避けるために、既存の規則を慎重に確認し、調整する必要があります。

Web Studioを使用したアクセスポリシー規則の管理

包含条件と除外条件を使用して、デフォルトのポリシーを調整できます。たとえば、それらの接続のサブセットへのアクセスを制限するには、次の手順に従います。

1. デフォルトポリシーを編集します。
2. **［次のいずれかの条件を満たす接続］** を選択します。
3. 許可されたユーザーアクセスシナリオのSmartAccessポリシー式を追加、編集、または削除します。

詳しくは、Citrix Gatewayのドキュメントを参照してください。

PowerShellを使用したアクセスポリシー規則の追加と管理

デリバリーグループのアクセスポリシー規則を追加および管理するには、次のPowerShellコマンドレットを使用できます。

- New-BrokerAccessPolicyRule
- Get-BrokerAccessPolicyRule
- Set-BrokerAccessPolicyRule
- リネーム-ブローカーアクセスポリシールール
- リムーブ-ブローカーアクセスポリシールール

詳細については、Citrix Developer Documentationの関連記事を参照してください。

デリバリーグループ内のマシンへのユーザー接続を防止する（メンテナンスモード）

マシンへの新しい接続を一時的に停止する必要がある場合は、デリバリーグループ内の1台またはすべてのマシンでメンテナンスモードをオンにできます。これは、パッチを適用したり、管理ツールを使用したりする前に行うことがあります。

- マルチセッションOSマシンがメンテナンスモードの場合、ユーザーは既存のセッションに接続できますが、新しいセッションを開始することはできません。
- シングルセッションOSマシン（またはリモートPCアクセスを使用するPC）がメンテナンスモードの場合、ユーザーは接続または再接続できません。現在の接続は、切断またはログオフするまで接続されたままになります。

メンテナンスモードをオンまたはオフにするには：

1. 左側のペインで を選択します。
2. グループを選択します。
3. デリバリーグループ内のすべてのマシンでメンテナンスモードをオンにするには、アクションバーの をクリックします。

   1台のマシンでメンテナンスモードをオンにするには、アクションバーの をクリックします。マシンを選択し、アクションバーの をクリックします。
4. デリバリーグループ内の1台またはすべてのマシンでメンテナンスモードをオフにするには、上記の手順に従い、アクションバーの をクリックします。

Windowsリモートデスクトップ接続（RDC）の設定も、マルチセッションOSマシンがメンテナンスモードであるかどうかに影響します。メンテナンスモードは、次のいずれかが発生した場合にオンになります。

- 前述のように、メンテナンスモードがオンに設定されている。
- RDCが に設定されている。
- RDCが**このコンピューターへの接続を許可しない**に設定されていないこと。**リモートホスト構成ユーザーログオンモード**設定が、**再接続を許可するが、新しいログオンは禁止する**、または**再接続を許可するが、サーバーが再起動されるまで新しいログオンは禁止する**のいずれかであること。

メンテナンスモードは、次のものに対してもオン/オフを切り替えることができます。

- 接続。その接続を使用しているマシンに影響します。
- マシンカタログ。そのカタログ内のマシンに影響します。

デリバリーグループ内のマシンのシャットダウンと再起動

この手順は、Remote PC Accessマシンではサポートされていません。

1. 左ペインで**デリバリーグループ**を選択します。
2. グループを選択し、アクションバーで**マシンの表示**をクリックします。
3. マシンを選択し、アクションバーで次のいずれかのエントリをクリックします。

   - **強制シャットダウン:** マシンの電源を強制的にオフにし、マシンの一覧を更新します。
   - **再起動:** オペレーティングシステムにシャットダウンを要求し、その後マシンを再起動します。オペレーティングシステムがこれに応じられない場合、マシンは現在の状態のままになります。

- **強制再起動:** オペレーティングシステムを強制的にシャットダウンし、その後マシンを再起動します。
- **一時停止:** マシンをシャットダウンせずに一時停止し、マシンの一覧を更新します。
- **シャットダウン:** オペレーティングシステムにシャットダウンを要求します。

強制ではないアクションの場合、マシンが10分以内にシャットダウンしないと、電源がオフになります。シャットダウン中にWindowsが更新プログラムのインストールを試みると、更新が完了する前にマシンの電源がオフになるリスクがあります。

Citrixでは、シングルセッションOSマシンのユーザーがセッション内で**シャットダウン**を選択できないようにすることをお勧めします。詳細については、Microsoftのポリシーに関するドキュメントを参照してください。

接続でマシンをシャットダウンして再起動することもできます。

デリバリーグループ内のマシンの再起動スケジュールを作成および管理する

> **注:**
>
> - Autoscale™が有効なデリバリーグループに再起動スケジュールが適用されると、そのグループのマシンは電源がオフにされるだけで、Autoscaleが電源をオンにするまでそのままになります。
> - ランダムなシングルセッションマシンに再起動スケジュールが適用されると、コスト削減のため、それらのマシンは再起動されるのではなく電源がオフになります。マシンの電源をオンにするには、Autoscaleを使用することをお勧めします。
> - デリバリーグループのタイムゾーンを変更すると、そのデリバリーグループ内のマシンが再起動される場合があります。これを避けるには、稼働時間外にタイムゾーン設定を変更するようにしてください。

再起動スケジュールは、デリバリーグループ内のマシンが定期的に再起動されるタイミングを指定します。デリバリーグループに対して1つ以上のスケジュールを作成できます。スケジュールは次のいずれかに影響します。

- グループ内のすべてのマシン。

- グループ内の1つ以上の（ただしすべてではない）マシン。マシンは、そのマシンに適用するタグによって識別されます。これはタグ制限と呼ばれます。タグは、そのタグを持つアイテムのみにアクションを制限するためです。

たとえば、すべてのマシンが1つのデリバリーグループにあるとします。すべてのマシンを週に1回再起動し、経理チームが使用するマシンを毎日再起動したいとします。これを実現するには、すべてのマシンに対して1つのスケジュールを設定し、経理部門のマシンのみに対して別のスケジュールを設定します。

スケジュールには、再起動が開始される曜日と時刻、および期間が含まれます。

スケジュールを有効または無効にできます。スケジュールを無効にすることは、テスト中、特別な期間中、または必要になる前にスケジュールを準備する際に役立ちます。

管理コンソールから自動電源オンまたはシャットダウンにスケジュールを使用することはできません。再起動のみに使用できます。

スケジュールの重複

複数のスケジュールが重複する可能性があります。上記の例では、両方のスケジュールが経理部門の仮想マシンに影響を与えます。これらのマシンは日曜日に2回再起動される可能性があります。スケジューリングコードは、意図したよりも頻繁に同じマシンを再起動しないように設計されていますが、保証はできません。

- スケジュールが開始時刻と期間で正確に一致する場合、マシンが再起動されるのは1回のみである可能性が高くなります。
- スケジュールが開始時刻と期間で異なるほど、複数回の再起動が発生する可能性が高くなります。
- スケジュールによって影響を受けるマシンの数も、重複の可能性に影響します。この例では、すべてのマシンに影響する週次スケジュールは、それぞれに指定された期間に応じて、経理部門のマシンの日次スケジュールよりも早く再起動を開始する可能性があります。

再起動スケジュールについて詳しく知るには、「再起動スケジュールの内部」を参照してください。

再起動スケジュールの表示

1. 左ペインで を選択します。
2. グループを選択し、アクションバーで をクリックします。
3. ページを選択します。

ページには、構成されている各スケジュールについて次の情報が含まれています。

- スケジュール名
- 使用されているタグ制限（ある場合）
- マシンの再起動が実行される頻度
- マシンユーザーが通知を受け取るかどうか
- スケジュールが有効になっているかどうか

タグを追加 (適用) する

タグ制限を使用する再起動スケジュールを構成する場合は、スケジュールが影響するマシンにタグが追加されていることを確認してください。上記の例では、経理チームが使用する各マシンにタグが適用されています。詳細については、「タグ」を参照してください。

1台のマシンに複数のタグを適用できますが、再起動スケジュールで指定できるタグは1つだけです。

1. 左側のペインで**デリバリーグループ**を選択します。
2. スケジュールによって制御されるマシンを含むグループを選択します。
3. をクリックし、タグを追加するマシンを選択します。
4. アクションバーの をクリックします。
5. タグが存在する場合は、タグ名の横にあるチェックボックスをオンにします。タグが存在しない場合は、 をクリックし、タグの名前を指定します。タグが作成されたら、新しく作成されたタグ名の横にあるチェックボックスをオンにします。
6. ダイアログで をクリックします。

再起動スケジュールを作成する

> **注:**
>
> 再起動スケジュールは、電源管理されているすべてのマルチセッションマシンと、電源管理されていないマルチセッションマシンに適用できます。

1. 左ペインで を選択します。
2. グループを選択し、アクションバーの をクリックします。
3. ページで をクリックします。
4. 「**再起動スケジュールの追加**」ページで:

- スケジュールを有効にするには、 を選択します。スケジュールを無効にするには、 を選択します。
- スケジュール名と説明を入力します。
- については、タグの制限を適用します。
- については、メンテナンスモードのマシンをこのスケジュールに含めるかどうかを選択します。代わりにPowerShellを使用するには、「メンテナンスモードのマシンのスケジュールされた再起動」を参照してください。
- については、再起動の発生頻度（毎日、毎週、毎月、または1回）を選択します。 または を選択した場合は、1つまたは複数の特定の日を指定できます。
- については、スケジュールを実行する頻度を指定します。
- については、スケジュールの最初の発生の開始日を指定します。
- については、24時間形式で再起動を開始する時刻を指定します。
- について:
  - 自然な再起動を使用しない場合は、 または を選択します。
  - 自然な再起動を使用する場合は、 を選択します。

    自然な再起動を使用するように構成された再起動スケジュールを開始すると:

    - デリバリーグループに属するすべてのアイドル状態のマシンはすぐに再起動されます
    - 1つ以上の有効なセッションを持つデリバリーグループに属する各マシンは、すべてのセッションがログオフされたときに再起動されます。

    注記:

    通常の再起動スケジュールは、電源管理されたマシンのみ再起動できます。

- で、再起動が開始される前に該当するマシンに通知メッセージを表示するかどうかを選択します。デフォルトでは、メッセージは表示されません。
- 再起動が開始される15分前にメッセージを表示することを選択した場合、(で) 最初のメッセージの後に5分ごとにメッセージを繰り返すように選択できます。デフォルトでは、メッセージは繰り返されません。
- 通知のタイトルとテキストを入力します。デフォルトのテキストはありません。

メッセージに再起動までのカウントダウンを含める場合は、変数 **%m%** を含めます。すべてのマシンを同時に再起動することを選択しなかった場合、メッセージは、再起動の前に適切なタイミングで各マシンに表示されます。

5. をクリックして変更を適用し、 ウィンドウを閉じます。
6. をクリックして行った変更を適用し、ウィンドウを開いたままにします。または、 をクリックして変更を適用してウィンドウを閉じます。

ドレイン後の再起動

PowerShellを使用してマシンの再起動スケジュールを作成または更新する場合 (`New-BrokerRebootSchedulev2` または `Set-BrokerRebootSchedulev2`)、別の再起動期間値が利用可能です。

`-UseNaturalReboot <Boolean>` パラメーターを使用してドレイン後の再起動機能を有効にすると、すべてのセッションがドレインされた後、すべてのマシンが再起動されます。再起動時刻になると、マシンはドレイン状態になり、すべてのセッションがログオフされると再起動されます。

この機能は、シングルセッションまたはマルチセッションのマシンを含むデリバリーグループでサポートされています。このオプションは、電源管理されているマシンと、電源管理されていないマシンの両方で使用できます。

オンプレミス環境では、この機能は PowerShell を使用する場合にのみサポートされます。この機能は Web Studio では利用できません。

再起動スケジュールの編集、削除、有効化、または無効化

1. 左側のペインで を選択します。
2. グループを選択し、アクションバーで**編集**をクリックします。
3. **再起動スケジュール**ページで、スケジュールのチェックボックスをオンにします。
   - スケジュールを編集するには、**編集**をクリックします。再起動スケジュールの作成のガイダンスを使用して、スケジュール構成を更新します。
   - スケジュールを有効または無効にするには、**編集**をクリックします。**再起動スケジュールを有効にする**チェックボックスをオンまたはオフにします。
   - スケジュールを削除するには、 をクリックします。削除を確認します。スケジュールを削除しても、影響を受けるマシンに適用されているタグには影響しません。

データベース停止によるスケジュールされた再起動の遅延

> **注：**

> この機能はPowerShellでのみ利用可能です。

> デリバリーグループ内のマシン（VDA）のスケジュールされた再起動が開始される前にサイトデータベースの停止が発生した場合、停止が終了したときに再起動が開始されます。これは予期しない結果を招く可能性があります。

たとえば、デリバリーグループの再起動を非稼働時間中（03:00開始）に発生するようにスケジュールしたとします。スケジュールされた再起動が開始される1時間前（02:00）にサイトデータベースの停止が発生しました。停止は6時間（08:00まで）続きます。再起動スケジュールは、Delivery Controllerとサイトデータベース間の接続が復元されたときに開始されます。VDAの再起動は元のスケジュールから5時間後に開始され、稼働時間中にVDAが再起動することになります。

この状況を回避するために、`New-BrokerRebootScheduleV2`および`Set-BrokerRebootScheduleV2`コマンドレットで`MaxOvertimeStartMins`パラメーターを使用できます。この値は、再起動スケジュールが開始できる、スケジュールされた開始時刻を超える最大分数を示します。

- その時間内（スケジュールされた時刻 + `MaxOvertimeStartMins`）にデータベース接続が復元された場合、VDAの再起動が開始されます。
- その時間内にデータベース接続が復元されない場合、VDAの再起動は開始されません。
- このパラメーターが省略されているか、値がゼロの場合、停止期間に関係なく、データベースへの接続が復元されたときにスケジュールされた再起動が開始されます。

詳細については、コマンドレットのヘルプを参照してください。この機能は PowerShell でのみ利用できます。Web Studio で再起動スケジュールを構成する際には、この値を設定できません。

メンテナンスモードのマシンのスケジュールされた再起動

> **注:**

> この機能はPowerShellでのみ利用可能です。オプション`IgnoreMaintenanceMode`は、Citrix Virtual Apps and Desktops 7 2006以降でサポートされています。

> 再起動スケジュールがメンテナンスモードのマシンに影響するかどうかを示すには、`BrokerRebootScheduleV2` コマンドレットで `IgnoreMaintenanceMode` オプションを使用します。

たとえば、次のコマンドレットは、メンテナンスモードのマシン (メンテナンスモードではないマシンに加えて) を再起動するスケジュールを作成します。

```
New-Brokerrebootschedulev2 rebootSchedule1 -DesktopGroupName <myDesktopGroup>
-IgnoreMaintenanceMode $true
```

次のコマンドレットは、既存の再起動スケジュールを変更します。

```
Set-Brokerrebootschedulev2 rebootSchedule1 -IgnoreMaintenanceMode $true
```

詳細については、コマンドレットのヘルプを参照してください。この機能はPowerShellでのみ利用可能です。

1回限りの再起動スケジュールを有効にする

PowerShellを使用して1回限りの再起動スケジュールを有効にする場合は、以下の `BrokerCatalogRebootSchedule` PowerShellコマンドを使用して、再起動スケジュールを作成、変更、削除します。

- Get-BrokerCatalogRebootSchedule
- New-BrokerCatalogRebootSchedule
- Set-BrokerCatalogRebootSchedule
- ブローカーカタログの再起動スケジュールを削除
- ブローカーカタログの再起動スケジュール名を変更

制限事項:

- タイムゾーンが構成されていないカタログに関連付けられたカタログ再起動スケジュールは作成されますが、開始されません。
- カタログ再起動スケジュールが作成されると、その再起動スケジュールはデリバリーグループに属するカタログVMでのみ実行されます。

例、,

- **BankTellers** という名前のカタログ内のVMの再起動スケジュールを、Feb 3, 2022 の午前2時から午前4時の間に開始するように作成します。

```
C:\PS> New-BrokerCatalogRebootSchedule -Name BankTellers -CatalogName
BankTellers  -StartDate "2022-02-03" -StartTime "02:00" -Enabled $true
-RebootDuration 120
```

- UID 17のカタログ内のVMの再起動スケジュールを、Feb 3, 2022の午前1時から午前5時の間に開始するように作成します。再起動の10分前に、各VMは、すべてのユーザーセッションで、タイトルが「**WARNING: Reboot pending**」、メッセージが「**Save your work**」のメッセージボックスを表示するように設定されます。

```
C:\PS> New-BrokerCatalogRebootSchedule -Name 'Update reboot'
-CatalogUid 17 -StartDate "2022-02-03" -StartTime "01:00" -Enabled
$true -RebootDuration 240 -WarningTitle "WARNING: Reboot pending"
-WarningMessage "Save your work" -WarningDuration 10
```

- **Old Name** という名前のカタログ再起動スケジュールを **New Name** に変更します。

```
C:\PS> Rename-BrokerCatalogRebootSchedule -Name "Old Name" -NewName
"New Name"
```

- UID 1 を持つすべてのカタログ再起動スケジュールを表示し、その後、UID 1 を持つカタログ再起動スケジュールを **New Name** に変更します。

```
C:\PS> Get-BrokerCatalogRebootSchedule -Uid 1 | Rename-
BrokerCatalogRebootSchedule -NewName "New Name" -PassThru
```

- **Accounting** という名前のカタログ再起動スケジュールを、各VMの再起動の10分前に、タイトルが「**WARNING: Reboot pending**」、メッセージが「**Save your work**」のメッセージを表示するように設定します。このメッセージは、そのVM上のすべてのユーザーセッションに表示されます。

```
C:\PS> Set-BrokerCatalogRebootSchedule -Name Accounting -WarningMessage
"Save your work" -WarningDuration 10 -WarningTitle "WARNING: Reboot
pending"
```

- 無効になっているすべての再起動スケジュールを表示し、その後、無効になっているすべての再起動スケジュールを有効にします。

```
C:\PS> Get-BrokerCatalogRebootSchedule -Enabled $false | Set-
BrokerCatalogRebootSchedule -Enabled $true
```

- UID 17のカタログ再起動スケジュールを、各VMの再起動の15分前、10分前、5分前に「**Rebooting in %m% minutes**」というメッセージを表示するように設定します。

```
C:\PS> Set-BrokerCatalogRebootSchedule 17 -WarningMessage "Rebooting in
%m% minutes." -WarningDuration 15 -WarningRepeatInterval 5
```

- 「**MyCatalog**」という名前のカタログのタイムゾーンを構成します。

```
C:\PS> Set-BrokerCatalog -Name "MyCatalog" -TimeZone &lt;TimeZone>
```

デリバリーグループ内の電源管理対象マシン

電源管理できるのは仮想シングルセッションOSマシンのみで、物理マシン（リモートPCアクセスを含む）はできません。GPU機能を備えたシングルセッションOSマシンは一時停止できないため、電源オフ操作は失敗します。マルチセッションOSマシンでは、再起動スケジュールを作成できます。

プールされたマシンを含むデリバリーグループでは、仮想シングルセッションOSマシンは次のいずれかの状態になります。

- ランダムに割り当てられ、使用中
- 割り当てられておらず、未接続

静的マシンを含むデリバリーグループでは、仮想シングルセッションOSマシンは次のようになります。

- 永続的に割り当てられ、使用中
- 永続的に割り当てられ、未接続（ただし準備完了）
- 割り当てられておらず、未接続

通常の使用時、静的デリバリーグループには通常、永続的に割り当てられたマシンと割り当てられていないマシンの両方が含まれます。最初は、デリバリーグループが作成されたときに手動で割り当てられたマシンを除き、すべてのマシンは割り当てられていません。ユーザーが接続すると、マシンは永続的に割り当てられます。これらのデリバリーグループ内の割り当てられていないマシ

ンは完全に電源管理できますが、永続的に割り当てられたマシンは部分的にしか管理できません。

- **プールとバッファー:** プールされたデリバリーグループおよび割り当てられていないマシンを持つ静的デリバリーグループの場合、プール（この場合）とは、電源オン状態に保たれ、ユーザーが接続する準備ができている、割り当てられていない、または一時的に割り当てられたマシンのセットです。ユーザーはログオン後すぐにマシンを取得します。プールサイズ（電源オン状態に保たれるマシンの数）は、時間帯によって構成可能です。静的デリバリーグループの場合、SDKを使用してプールを構成します。

  バッファーとは、プールのマシンの数がしきい値を下回ったときに電源がオンになる、割り当てられていないマシンの追加のスタンバイセットです。しきい値はデリバリーグループサイズのパーセンテージです。大規模なデリバリーグループの場合、しきい値を超えるとかなりの数のマシンがオンになる可能性があります。したがって、デリバリーグループのサイズを慎重に計画するか、SDKを使用してデフォルトのバッファーサイズを調整してください。
- **電源状態タイマー:** 電源状態タイマーを使用して、ユーザーが指定された時間切断された後にマシンを一時停止できます。たとえば、ユーザーが少なくとも10分間切断されている場合、勤務時間外にマシンは自動的に一時停止します。

  タイマーは、平日と週末、およびピーク時と非ピーク時の間隔で構成できます。
- **永続的に割り当てられたマシンの部分的な電源管理:** 永続的に割り当てられたマシンでは、電源状態タイマーを設定できますが、プールやバッファーは設定できません。マシンは各ピーク期間の開始時にオンになり、各非ピーク期間の開始時にオフになります。消費されたマシンを補うために利用可能になるマシンの数について、割り当てられていないマシンで得られるようなきめ細かな制御はできません。

仮想シングルセッションOSマシンの電源管理

1. 左ペインで**Delivery Groups**を選択します。
2. グループを選択し、アクションバーで**デリバリーグループの編集**をクリックします。
3. **電源管理**ページで、**マシンの電源管理**から**平日**を選択します。デフォルトでは、平日は月曜日から金曜日です。
4. ランダムなデリバリーグループの場合、**電源をオンにするマシン**で**編集**をクリックし、平日のプールサイズを指定します。次に、電源をオンにするマシンの数を選択します。
5. **ピーク時間**で、各日のピーク時間とオフピーク時間を設定します。
6. 平日のピーク時間と非ピーク時間の電源状態タイマーを設定します:**ピーク時間中 > 切断時**で、デリバリーグループ内の切断されたマシンを一時停止するまでの遅延（分単位）を指定し、**一時停止**を選択します。**オフピーク時間中 > 切断時**で、デリバリーグループ内のログオフ

されたマシンをシャットダウンするまでの遅延を指定し、**シャットダウン**を選択します。このタイマーは、ランダムなマシンを含むデリバリーグループでは使用できません。

7. **マシンの電源管理**で**週末**を選択し、週末のピーク時間と電源状態タイマーを設定します。
8. 加えた変更を適用してウィンドウを開いたままにするには、**適用**をクリックします。または、変更を適用してウィンドウを閉じるには、**保存**をクリックします。

SDKを使用して、次の操作を行います。

- 電源状態タイマーに応じてマシンを一時停止ではなくシャットダウンするか、タイマーを接続解除ではなくログオフに基づいて設定します。
- デフォルトの平日と週末の定義を変更します。
- 電源管理を無効にします。CTX217289を参照してください。

切断されたセッションを持つVDIマシンが異なる時間帯に移行する際の電源管理

> **重要:**
>
> この機能強化は、切断されたセッションを持つVDIマシンにのみ適用されます。ログオフされたセッションを持つVDIマシンには適用されません。
>
> 以前のリリースでは、アクション（切断アクション="**一時停止**"または"**シャットダウン**"）が必要な時間帯に移行するVDIマシンは、電源がオンのままでした。このシナリオは、マシンがアクション（切断アクション="**何もしない**"）が不要な時間帯（ピーク時またはオフピーク時）に切断された場合に発生しました。

Citrix Virtual Apps and Desktops 7 1909以降、指定された切断時間が経過すると、宛先期間に構成されている切断アクションに応じて、マシンは中断または電源オフされます。

たとえば、VDIデリバリーグループに対して次の電源ポリシーを構成します。

- `PeakDisconnectAction`を「Nothing」に設定します
- `OffPeakDisconnectAction`を「Shutdown」に設定します
- `OffPeakDisconnectTimeout`を「10」に設定します

電源ポリシーの切断アクションに関する詳細については、https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/about_Broker_PowerManagement/#power-policyお

よびhttps://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/Get-BrokerDesktopGroup/を参照してください。

以前のリリースでは、ピーク時にセッションが切断されたVDIマシンは、ピークからオフピークに移行しても電源がオンのままでした。Citrix Virtual Apps and Desktops 7 1909以降、期間の移行時に`OffPeakDisconnectAction`と`OffPeakDisconnectTimeout`のポリシーアクションがVDIマシンに適用されます。その結果、マシンはオフピークに移行してから10分後に電源がオフになります。

以前の動作（つまり、ピークからオフピーク、またはオフピークからピークに切断されたセッションで移行するマシンに対してアクションを実行しない）に戻したい場合は、次のいずれかを実行します。

- `LegacyPeakTransitionDisconnectedBehaviour`レジストリ値を`1`に設定します。これは、以前の動作を有効にする*true*に相当します。デフォルトでは、値は`0`、つまり*false*であり、期間の移行時に切断電源ポリシーアクションをトリガーします。
  - パス: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\DesktopServer`
  - 名前: `LegacyPeakTransitionDisconnectedBehaviour`
  - 種類: `REG_DWORD`
  - データ: `0x00000001 (1)`
- `Set-BrokerServiceConfigurationData` PowerShellコマンドを使用して設定を構成します。例：
  - `PS C:\> Set-BrokerServiceConfigurationData HostingManagement.LegacyPeakTransitionDisconnectedBehaviour -SettingValue $true`

マシンは、期間移行時に電源ポリシーアクションが適用される前に、次の基準を満たす必要があります。

- 切断されたセッションがあること。
- 保留中の電源アクションがないこと。
- 異なる時間帯に移行するVDI（シングルセッション）デリバリーグループに属していること。
- 特定の時間帯（ピーク時またはオフピーク時）に切断され、電源アクションが割り当てられている期間に移行するセッションがあること。

カタログの電源オン状態のVDAの割合を変更する

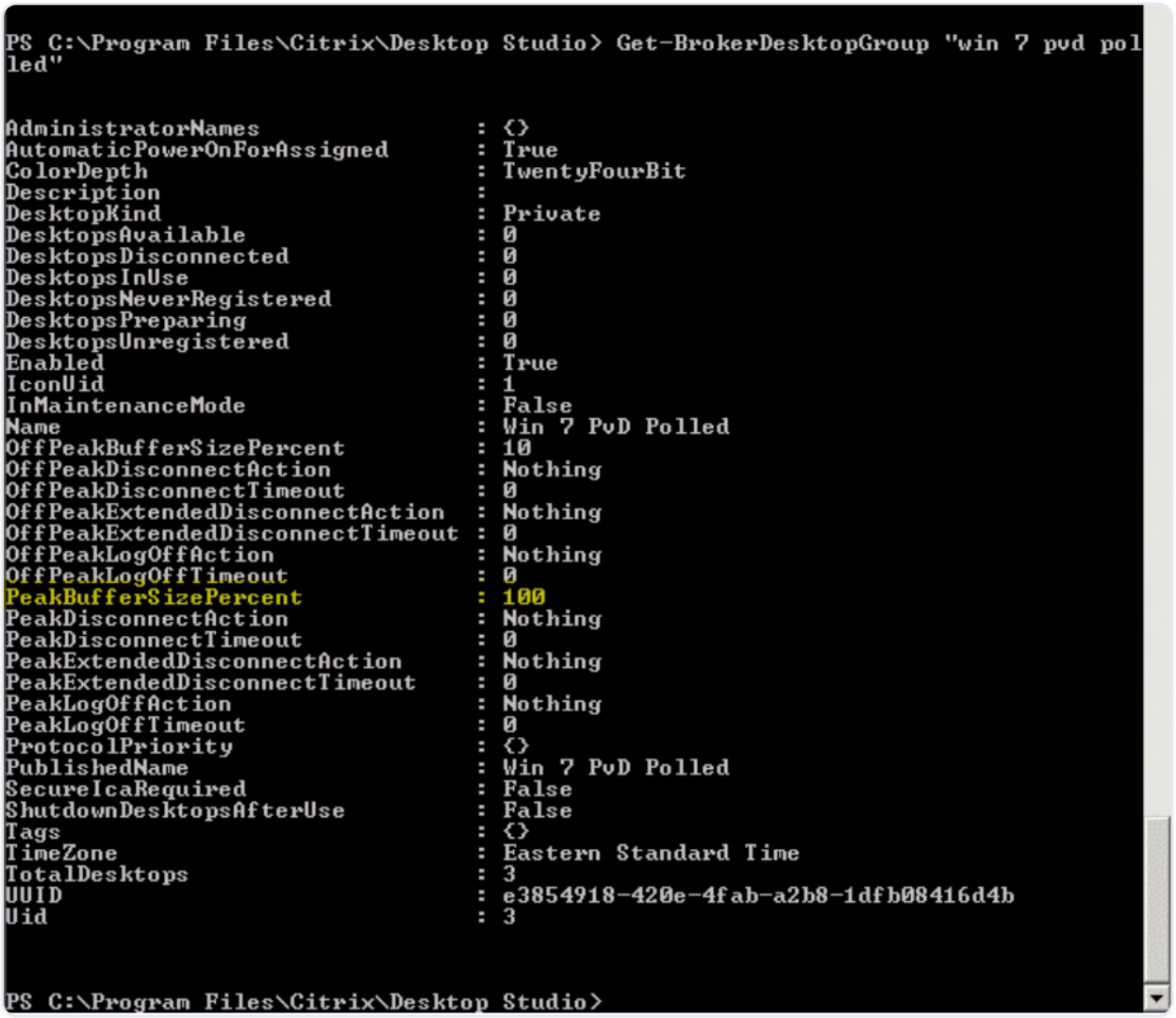
1. デリバリーグループの**電源管理**セクションから、デリバリーグループのピーク時間を調整します。
2. デスクトップグループ名をメモします。
3. 管理者権限でPowerShellを起動し、次のコマンドを実行します。「Desktop Group Name」を、実行中のVDAの割合が変更されたデスクトップグループの名前に置き換えます。

   ```
   asnp Citrix*
   ```

   ```
   # Set-BrokerDesktopGroup "Desktop Group Name" -PeakBufferSizePercent 100
   ```

   値が100の場合、VDAの100%が準備完了状態であることを意味します。
4. 次のコマンドを実行してソリューションを確認します。

   ```
   #Get-BrokerDesktopGroup "Desktop Group Name"
   ```



変更が有効になるまで最大1時間かかる場合があります。

ユーザーがログオフした後にVDAをシャットダウンするには、次のように入力します。

```
# Set-BrokerDesktopGroup "Desktop Group Name" -ShutDownDesktopsAfterUse $True
```

ピーク時にVDAを再起動して、ユーザーがログオフした後にすぐに使用できるようにするには、次のように入力します。

```
# Set-BrokerDesktopGroup "Desktop Group Name"
-AutomaticPowerOnForAssignedDuringPeak $True
```

セッション

- セッションのログオフまたは切断、またはユーザーへのメッセージ送信
- セッションのプレ起動とセッションの維持を構成する
- メンテナンスモードのマシンから切断された場合のセッション再接続を制御する
- セッションローミングを構成する

セッションのログオフまたは切断

1. 左ペインで****を選択します。
2. デリバリーグループを選択し、アクションバーで****を選択します。
3. 中央ペインでマシンを選択し、アクションバーで****を選択してから、セッションを選択します。
    - または、中央ペインで****タブを選択し、セッションを選択します。
4. セッションからログオフするには、アクションバーで**ログオフ**を選択します。セッションが閉じられ、ユーザーはログアウトされます。特定のユーザーに割り当てられていない限り、マシンは他のユーザーが利用できるようになります。
5. セッションを切断するには、アクションバーで**切断**を選択します。アプリケーションはセッション内で実行を継続し、マシンはそのユーザーに割り当てられたままになります。ユーザーは同じマシンに再接続できます。

シングルセッションOSマシンでは、未使用のセッションを自動的に処理するように電源状態タイマーを構成できます。詳細については、「電源管理されたマシン」を参照してください。

デリバリーグループにメッセージを送信する

1. 左ペインで**Delivery Groups**を選択します。
2. デリバリーグループを選択し、アクションバーで**View Machines**を選択します。

3. 中央ペインで、メッセージを送信するマシンを選択します。
4. アクションバーで**View Sessions**を選択します。
5. 中央ペインで、すべてのセッションを選択し、アクションバーで**メッセージの送信**を選択します。
6. メッセージを入力し、**OK**をクリックします。必要に応じて、重大度レベルを指定できます。オプションには、**重大**、**質問**、**警告**、**情報**があります。

または、Citrix Directorを使用してメッセージを送信することもできます。詳しくは、「ユーザーへのメッセージの送信」を参照してください。

デリバリーグループでセッションの事前起動とセッションの維持を構成する

これらの機能は、マルチセッションOSマシンでのみサポートされています。

セッションの事前起動とセッションの維持機能は、要求される前にセッションを開始すること（セッションの事前起動）と、ユーザーがすべてのアプリケーションを閉じた後もアプリケーションセッションをアクティブに保つこと（セッションの維持）により、指定されたユーザーがアプリケーションにすばやくアクセスできるようにします。

デフォルトでは、セッションの事前起動とセッションの維持は使用されません。セッションは、ユーザーがアプリケーションを起動したときに開始（起動）され、セッション内の最後に開いたアプリケーションが閉じるまでアクティブなままになります。

留意事項：

- デリバリーグループはアプリケーションをサポートしている必要があり、マシンはマルチセッションOS用のVDA（バージョン7.6以降）を実行している必要があります。
- これらの機能は、Windows向けCitrix Workspaceアプリを使用している場合にのみサポートされ、追加のCitrix Workspaceアプリ構成も必要です。手順については、お使いのWindows向けCitrix Workspaceアプリのバージョンの製品ドキュメントで「セッションの事前起動」を検索してください。
- HTML5向けCitrix Workspaceアプリはサポートされていません。
- セッションの事前起動を使用している場合、ユーザーのマシンがサスペンドモードまたは休止状態になった場合、事前起動は機能しません（セッションの事前起動設定に関係なく）。ユーザーは自分のマシン/セッションをロックできます。ただし、ユーザーがCitrix Workspaceアプリからログオフすると、セッションは終了し、事前起動は適用されなくなります。
- セッションの事前起動を使用している場合、物理クライアントマシンはサスペンドまたは休止状態の電源管理機能を使用できません。クライアントマシンのユーザーはセッションをロックできますが、ログオフしてはいけません。

- 事前起動セッションと残存セッションは、接続されている場合にのみ同時接続ライセンスを消費します。ユーザー/デバイスライセンスを使用している場合、ライセンスは90日間有効です。未使用の事前起動セッションと残存セッションは、デフォルトで15分後に切断されます。この値はPowerShell（`New/Set-BrokerSessionPreLaunch` コマンドレット）で構成できます。
- これらの機能が互いに補完し合うように調整するには、ユーザーのアクティビティパターンを慎重に計画し、監視することが不可欠です。最適な構成は、ユーザーがより早くアプリケーションを利用できるというメリットと、ライセンスの使用とリソースの割り当てにかかるコストとのバランスを取ります。
- Citrix Workspaceアプリで、スケジュールされた時刻にセッションの事前起動を構成することもできます。

未使用の事前起動セッションと残存セッションがアクティブなままになる期間

ユーザーがアプリケーションを起動しない場合に、未使用のセッションがアクティブなままになる期間を指定する方法はいくつかあります。構成されたタイムアウトとサーバー負荷のしきい値です。これらすべてを構成できます。最初に発生したイベントにより、未使用のセッションが終了します。

- **タイムアウト：** 構成されたタイムアウトは、未使用の事前起動セッションまたは残存セッションがアクティブなままになる分数、時間、または日数を指定します。タイムアウトを短く設定しすぎると、事前起動セッションは、ユーザーにアプリケーションへのより迅速なアクセスというメリットを提供する前に終了してしまいます。タイムアウトを長く設定しすぎると、サーバーに十分なリソースがないため、受信ユーザー接続が拒否される可能性があります。

  このタイムアウトは、管理コンソールからではなく、SDKからのみ（`New/Set-BrokerSessionPreLaunch` コマンドレット）有効にできます。タイムアウトを無効にすると、そのデリバリーグループのコンソール表示や**デリバリーグループの編集**ページには表示されません。
- **しきい値：** サーバー負荷に基づいて事前起動セッションと残存セッションを自動的に終了することで、サーバーリソースが利用可能である限り、セッションが可能な限り長く開いたままになるようにします。未使用の事前起動セッションと残存セッションは、新しいユーザーセッションにリソースが必要なときに自動的に終了するため、接続拒否の原因にはなりません。

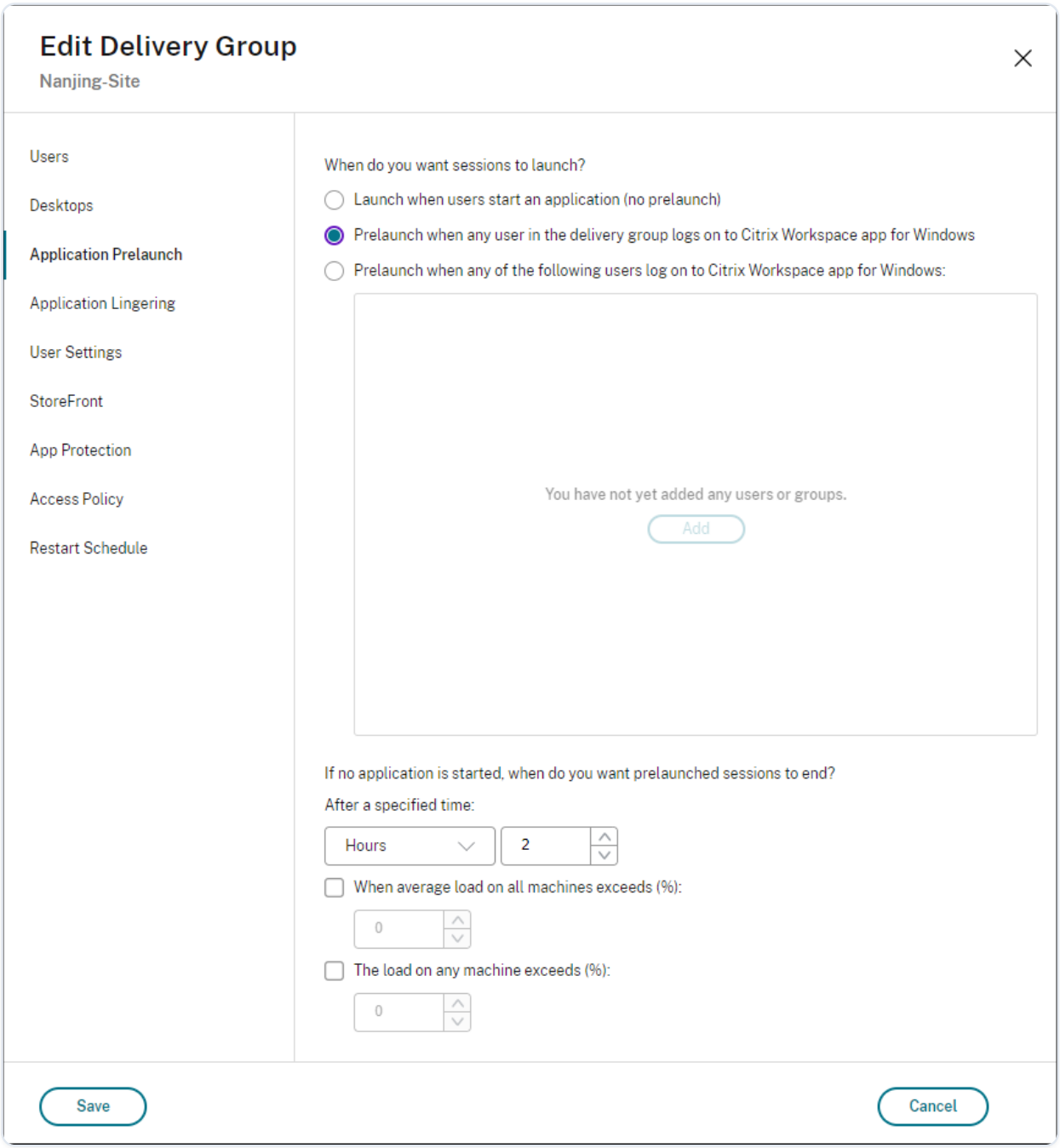
  2つのしきい値を構成できます。デリバリーグループ内のすべてのサーバーの平均負荷率と、グループ内の単一サーバーの最大負荷率です。しきい値を超えると、事前起動または残存状態にあった時間が最も長いセッションが終了します。負荷がしきい値を下回るまで、セッションは1分間隔で1つずつ終了します。しきい値を超えている間は、新しい事前起動セッションは開始されません。

コントローラーに登録されていないVDAを持つサーバー、およびメンテナンスモードのサーバーは、完全にロードされていると見なされます。計画外の停止が発生すると、容量を解放するために、プレランチセッションとリンガーセッションは自動的に終了します。

セッションのプレランチを有効にするには

1. グループを選択し、アクションバーで**デリバリーグループの編集**をクリックします。
2. **アプリケーションのプレランチ**ページで、セッションを起動するタイミングを選択して、セッションのプレランチを有効にします。

    - ユーザーがアプリケーションを起動したとき。これはデフォルト設定です。セッションのプレランチは無効になっています。
    - デリバリーグループ内のいずれかのユーザーがCitrix Workspaceアプリ for Windowsにログオンしたとき。
    - ユーザーおよびユーザーグループのリスト内のいずれかのユーザーがCitrix Workspaceアプリ for Windowsにログオンしたとき。このオプションを選択する場合は、ユーザーまたはユーザーグループも指定してください。



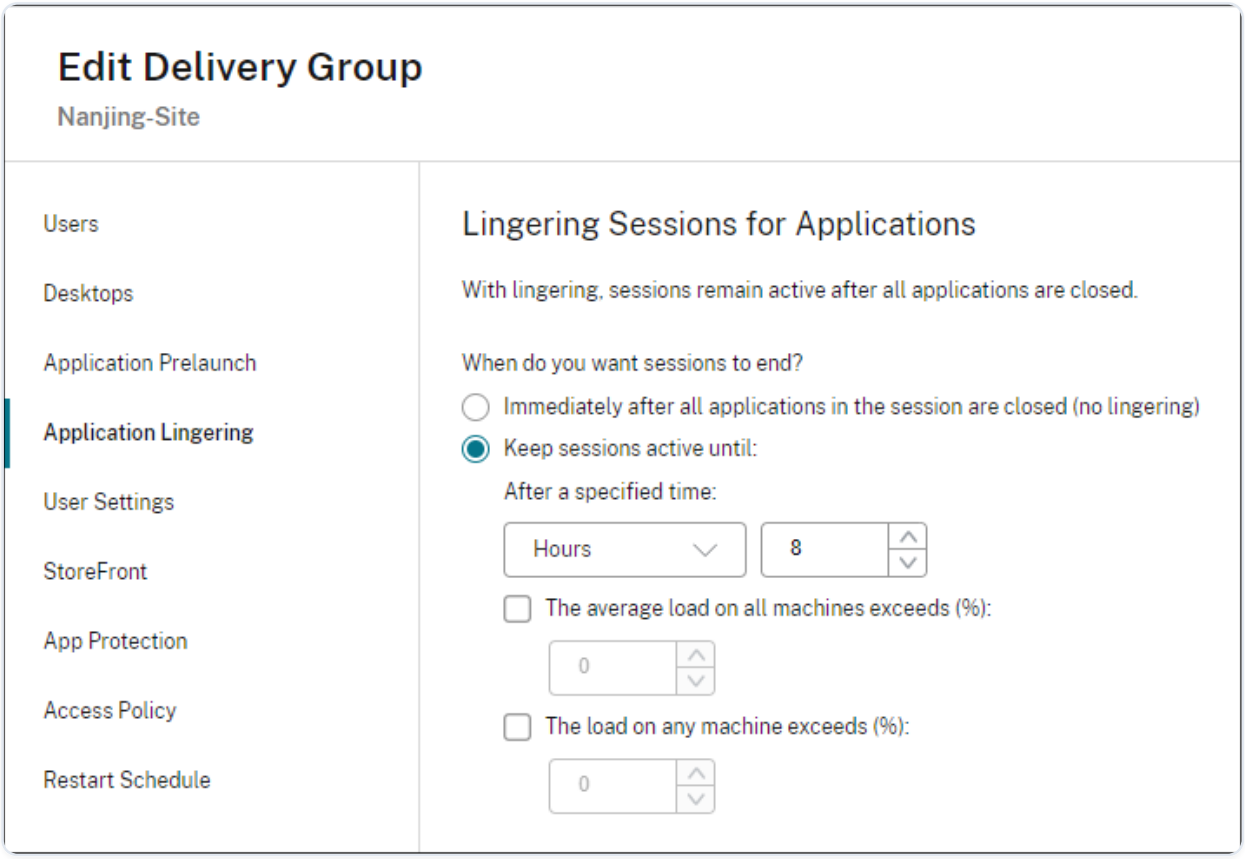
3. ユーザーがアプリケーションを起動すると、プレランチセッションは通常のセッションに置き換えられます。ユーザーがアプリケーションを起動しない場合（プレランチセッションが使用されない場合）、次の設定がそのセッションがアクティブなままになる期間に影響します。

   - 指定された時間間隔が経過したとき。時間間隔は変更できます（1〜99日、1〜2376時間、または1〜142,560分）。
   - デリバリーグループ内のすべてのマシンの平均負荷が指定された割合（1〜99%）を超えたとき。
   - デリバリーグループ内のいずれかのマシンの負荷が指定された割合（1〜99%）を超えたとき。

まとめ: プレランチセッションは、ユーザーがアプリケーションを起動する、指定された時間が経過する、または指定された負荷しきい値を超過する、のいずれかのイベントが発生するまでアクティブなままになります。

セッションのリンガーを有効にするには

1. 左側のペインで**デリバリーグループ**を選択します。
2. グループを選択し、アクションバーで**デリバリーグループの編集**をクリックします。
3. **アプリケーションの残存**ページで、**セッションをアクティブに維持する期間**を選択してセッションの残存を有効にします。



4. ユーザーが別のアプリケーションを起動しない場合、残存セッションがアクティブなままになる期間は、いくつかの設定によって影響を受けます。

   - 指定された時間間隔が経過した場合。時間間隔は、1～99日、1～2376時間、または1～142,560分に変更できます。
   - デリバリーグループ内のすべてのマシンの平均負荷が指定された割合（1～99%）を超えた場合。
   - デリバリーグループ内のいずれかのマシンの負荷が指定された割合（1～99%）を超えた場合。

まとめ: 残存セッションは、ユーザーがアプリケーションを起動する、指定された時間が経過する、または指定された負荷しきい値を超える、のいずれかのイベントが発生するまでアクティブなままです。

メンテナンスモードのマシンから切断された場合のセッション再接続を制御する

> **注：**
>
> この機能はPowerShellでのみ利用可能です。

> メンテナンスモードのマシンで切断されたセッションが、デリバリーグループ内のマシンに再接続することを許可するかどうかを制御できます。

バージョン2106より前は、メンテナンスモードのマシンから切断されたシングルセッションのプールされたデスクトップセッションの再接続は許可されていませんでした。バージョン2106以降では、メンテナンスモードのマシンから切断された後の再接続（セッションの種類に関係なく）を許可または禁止するようにデリバリーグループを構成できます。

デリバリーグループを作成または編集する際（`New-BrokerDesktopGroup`、`Set-BrokerDesktopGroup`）、`-AllowReconnectInMaintenanceMode <boolean>`パラメーターを使用して、メンテナンスモードのマシンから切断されたマシンへの再接続を許可または禁止します。

- trueに設定すると、セッションはグループ内のマシンに再接続できます。
- 「false」に設定されている場合、セッションはグループ内のマシンに再接続できません。

デフォルト値:

- シングルセッション: 無効
- マルチセッション: 有効

セッションローミングの構成

デフォルトでは、デリバリーグループでセッションローミングが有効になっています。セッションは、ユーザーとともにクライアントデバイス間をローミングします。ユーザーがセッションを起動し、別のデバイスに移動すると、同じセッションが使用され、アプリケーションは両方のデバイスで同時に利用可能になります。複数のデバイスでアプリケーションを表示できます。アプリケーションは、デバイスや現在のセッションの有無にかかわらず追従します。多くの場合、アプリケーションに割り当てられたプリンターやその他のリソースも追従します。または、PowerShellを使用することもできます。詳細については、「セッションローミング」を参照してください。

アプリケーションのセッションローミングの構成

アプリケーションのセッションローミングを構成するには、次の手順に従います。

1. コンソールで、左側のペインで を選択します。
2. グループを選択し、アクションバーで を選択します。
3. ページで、 チェックボックスをオンにして、セッションローミングを有効にします。
   - 有効にすると、ユーザーがアプリケーションセッションを起動し、別のデバイスに移動した場合、同じセッションが使用され、両方のデバイスで利用可能になります。無効にすると、セッションはデバイス間をローミングしなくなります。
4. **「OK」**を選択して変更を適用し、ウィンドウを閉じます。

デスクトップのセッションローミングを構成する

デスクトップのセッションローミングを構成するには、次の手順に従います。

1. コンソールで、左側のペインの**デリバリーグループ**を選択します。
2. グループを選択し、アクションバーで**編集**を選択します。
3. **デスクトップ**ページで、デスクトップを選択し、**編集**を選択します。
4. **セッションローミング**チェックボックスをオンにして、セッションローミングを有効にします。

- 有効にすると、ユーザーがデスクトップを起動してから別のデバイスに移動した場合、同じセッションが使用され、アプリケーションは両方のデバイスで利用可能になります。無効にすると、セッションはデバイス間をローミングしなくなります。

OKを選択して変更を適用し、ウィンドウを閉じます。

アプリケーション

デリバリーグループのアプリケーションを表示および追加します。

1. コンソールで、左ペインの**デリバリーグループ**を選択します。
2. グループを選択します。このグループにアプリケーションが含まれている場合、アクションバーに**アプリケーションの表示**が表示されます。
3. **アプリケーションの表示**を選択します。このグループで利用可能なすべてのアプリケーションが表示される**アプリケーション**ノードに移動します。
4. このグループにアプリケーションを追加するには、**デリバリーグループ**ノードに移動し、グループを選択して、アクションバーで**アプリケーションの追加**を選択します。

VDA上のCitrix Secure Access Clientからのシームレスなログオン

VDAに存在するCitrix Secure Access (CSA) クライアントからCitrix Secure Private Accessへ、シングルサインオン (SSO) を使用してCitrix Workspaceにシームレスにログオンできます。この機能は、シングルセッションVDAとマルチセッションVDAの両方に適用されます。

これを実現する手順は次のとおりです。

1. 既存のデリバリーグループを編集して、SPA SSOを有効にします。例：

   ```
   Set-BrokerDesktopGroup -Name &lt;String> -SpaSsoEnabled 1
   ```

2. Get -BrokerDesktopGroup PowerShellコマンドを使用して、デリバリーグループのSPA SSOのステータスを確認します。例：

   ```
   Get-BrokerDesktopGroup -Name &lt;String> -property 'SpaSsoEnabled'
   ```

3. SPAで、アプリケーションとポリシーを作成します。TCP/UDPアプリの構成およびアプリケーションのアクセスポリシーの構成を参照してください。
4. シングルセッションまたはマルチセッションVDAにRDP接続し、最新のCSAエージェントをインストールします。
5. Citrix Workspaceを開き、シングルセッションまたはマルチセッションVDAにログオンします。

トラブルシューティング

- Delivery Controllerに登録されていないVDAは、ブローカーセッションの起動時に考慮されません。これにより、利用可能なはずのリソースが十分に活用されないことになります。VDAが登録されない理由はさまざまであり、その多くは管理者がトラブルシューティングできます。詳細表示には、カタログ作成ウィザードと、デリバリーグループにカタログを追加した後のトラブルシューティング情報が表示されます。

  デリバリーグループを作成すると、デリバリーグループの詳細ペインに、登録可能だが登録されていないマシンの数が表示されます。たとえば、1台以上のマシンが電源オンでメンテナンスモードではないが、現在Controllerに登録されていない場合などです。「登録されていないが、登録されるべき」マシンを表示するときは、詳細ペインの**トラブルシューティング**タブで、考えられる原因と推奨される是正措置を確認してください。

  機能レベルに関するメッセージについては、「VDAのバージョンと機能レベル」を参照してください。

VDA登録のトラブルシューティングについては、「CTX136668」を参照してください。

- デリバリーグループの表示では、詳細ペインの**インストール済みVDAバージョン**が、マシンに実際にインストールされているバージョンと異なる場合があります。マシンのWindowsのプログラムと機能の表示には、実際のVDAバージョンが表示されます。
- **電源状態不明**ステータスのマシンについては、ガイダンスとして「CTX131267」を参照してください。

アプリケーショングループの作成

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

はじめに

アプリケーショングループを使用すると、アプリケーションのコレクションを管理できます。異なるデリバリーグループ間で共有されるアプリケーション、またはデリバリーグループ内のユーザーのサブセットによって使用されるアプリケーションのために、アプリケーショングループを作成します。アプリケーショングループはオプションです。複数のデリバリーグループに同じアプリケーションを追加する代わりに利用できます。デリバリーグループを複数のアプリケーショングループに関連付けたり、アプリケーショングループを複数のデリバリーグループに関連付けたりできます。

アプリケーショングループを使用すると、より多くのデリバリーグループを使用するよりも、アプリケーション管理とリソース制御の利点が得られます。

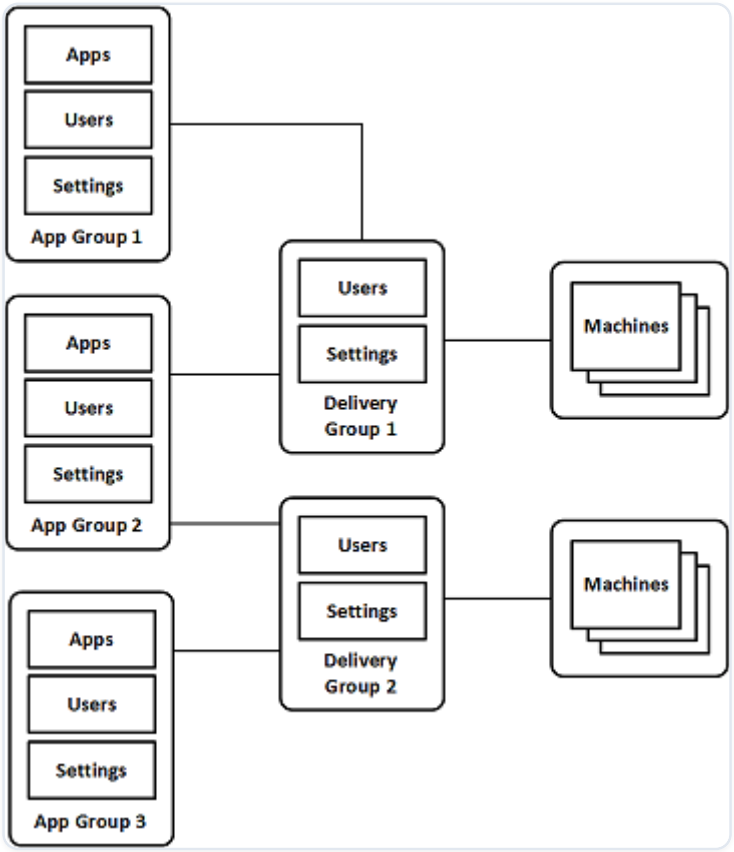
- アプリケーションとその設定を論理的にグループ化することで、それらのアプリケーションを単一の単位として管理できます。たとえば、同じアプリケーションを個々のデリバリーグループに一度に1つずつ追加（公開）する必要はありません。
- アプリケーショングループ間のセッション共有により、リソース消費を節約できます。その他のケースでは、アプリケーショングループ間のセッション共有を無効にすることが有益な場合があります。

- タグ制限機能を使用すると、選択したデリバリーグループ内のマシンのサブセットのみを考慮して、アプリケーショングループからアプリケーションを公開できます。タグ制限を使用すると、既存のマシンを複数の公開タスクに使用できるため、追加のマシンを展開および管理するコストを節約できます。タグ制限は、デリバリーグループ内のマシンを細分化（またはパーティション分割）するものと考えることができます。タグ制限のあるアプリケーショングループまたはデスクトップを使用すると、デリバリーグループ内のマシンのサブセットを分離してトラブルシューティングする際に役立ちます。

構成例

例 1:

次の図は、アプリケーショングループを含むCitrix Virtual Apps and Desktops展開を示しています。



この構成では、アプリケーションはデリバリーグループではなく、アプリケーショングループに追加されます。デリバリーグループは、使用されるマシンを指定します。（図には示されていませんが、マシンはマシンカタログにあります。）

アプリケーショングループ1はデリバリーグループ1に関連付けられています。アプリケーショングループ1で指定されたユーザーは、アプリケーショングループ1のアプリケーションにアクセスします。これらのグループは、デリバリーグループ1のユーザーリストにも含まれている場合にのみ表示されます。この構成は、アプリケーショングループのユーザーリストが、関連付けられたデリ

バリーグループのユーザーリストのサブセット（制限）であるというガイダンスに従います。アプリケーショングループ1の設定（アプリケーショングループ間のアプリケーションセッション共有、関連付けられたデリバリーグループなど）は、そのグループ内のアプリケーションとユーザーに適用されます。デリバリーグループ1の設定は、アプリケーショングループ1と2のユーザーに適用されます。これは、これらのアプリケーショングループがそのデリバリーグループに関連付けられているためです。

アプリケーショングループ2は、2つのデリバリーグループ（1と2）に関連付けられています。これらのデリバリーグループのそれぞれには、アプリケーションが起動されるときにデリバリーグループがチェックされる順序を示す優先度がアプリケーショングループ2で割り当てられています。優先度が同じデリバリーグループは負荷分散されます。アプリケーショングループ2で指定されたユーザーは、アプリケーショングループ2内のアプリケーションにアクセスします。ただし、それらのユーザーはデリバリーグループ1およびデリバリーグループ2のユーザーリストにも含まれている必要があります。

例 2:

このシンプルなレイアウトでは、タグ制限を使用して、特定のデスクトップおよびアプリケーションの起動に考慮されるマシンを制限します。このサイトには、1つの共有デリバリーグループ、1つの公開デスクトップ、および2つのアプリケーションで構成された1つのアプリケーショングループがあります。

タグの例(/en-us/citrix-virtual-apps-desktops/2503/media/tags-example.png)

3台のマシン（VDA 101～103）のそれぞれにタグが追加されています。

アプリケーショングループは、「Orange」タグ制限で作成されました。その各アプリケーションは、そのデリバリーグループ内で「Orange」タグを持つマシン（VDA 102および103）でのみ起動されます。

アプリケーショングループ（およびデスクトップ）でタグ制限を使用するためのより包括的な例とガイダンスについては、タグを参照してください。

ガイダンスと考慮事項

Citrixでは、アプリケーションをアプリケーショングループまたはデリバリーグループのいずれかに追加することをお勧めします。両方に追加することはお勧めしません。そうしないと、2種類のグループにアプリケーションが存在することによる複雑さが増し、管理がより困難になる可能性があります。

デフォルトでは、アプリケーショングループは有効になっています。アプリケーショングループを作成した後、グループを編集してこの設定を変更できます。アプリケーショングループの管理を参照してください。

デフォルトでは、アプリケーショングループ間のアプリケーションセッション共有は有効になっています。アプリケーショングループ間のセッション共有を参照してください。

Citrixでは、デリバリーグループを現在のバージョンにアップグレードすることをお勧めします。このプロセスには、次のものが必要です。

1. デリバリーグループで使用されているマシン上のVDAをアップグレードする。
2. それらのマシンを含むマシンカタログをアップグレードする。
3. デリバリーグループをアップグレードする。

詳細については、「デリバリーグループの管理」を参照してください。

アプリケーショングループを使用するには、コアコンポーネントが最小バージョン7.9である必要があります。

アプリケーショングループを作成するには、デリバリーグループ管理者組み込みロールの委任管理権限が必要です。詳細については、委任管理を参照してください。

この記事では、アプリケーションを複数のアプリケーショングループに「関連付ける」ことについて言及しています。これは、利用可能なソースからそのアプリケーションのインスタンスを追加する操作とは区別されます。同様に、デリバリーグループはアプリケーショングループに関連付けられており、互いに追加されたり、コンポーネントになったりするものではありません。

アプリケーショングループとのセッション共有

アプリケーションセッション共有が有効になっている場合、すべてのアプリケーションは同じアプリケーションセッションで起動します。これにより、より多くのアプリケーションセッションを起動するのにかかるコストが削減され、コピー＆ペースト操作など、クリップボードを使用するアプリケーション機能を利用できるようになります。ただし、状況によってはセッション共有を解除できます。

アプリケーショングループを使用する場合、デリバリーグループのみを使用しているときに利用できる標準のセッション共有動作を拡張する、次の3つの方法でアプリケーションセッション共有を構成できます。

- アプリケーショングループ間でセッション共有が有効。
- 同じアプリケーショングループ内のアプリケーション間でのみセッション共有が有効。

- セッション共有が無効。

アプリケーショングループ間のセッション共有

アプリケーショングループ間でアプリケーションセッション共有を有効にすることも、または、同じアプリケーショングループ内のアプリケーションにのみアプリケーションセッション共有を制限するために無効にすることもできます。

- **アプリケーショングループ間のセッション共有を有効にすることが役立つ例：**

  アプリケーショングループ1にはWordやExcelなどのMicrosoft Officeアプリケーションが含まれています。アプリケーショングループ2にはメモ帳や電卓などの他のアプリケーションが含まれており、両方のアプリケーショングループは同じデリバリーグループに接続されています。両方のアプリケーショングループにアクセスできるユーザーが、Wordを起動してアプリケーションセッションを開始し、次にメモ帳を起動します。コントローラーが、ユーザーの既存のWord実行セッションがメモ帳の実行に適していると判断した場合、メモ帳は既存のセッション内で起動されます。メモ帳が既存のセッションから実行できない場合（たとえば、タグ制限によりセッションが実行されているマシンが除外される場合など）、セッション共有を使用するのではなく、適切なマシン上に新しいセッションが作成されます。

- **アプリケーショングループ間のセッション共有を無効にすることが役立つ例：**

  同じマシンにインストールされている他のアプリケーションと相互運用性が低いアプリケーションのセットを含む構成。たとえば、同じソフトウェアスイートの2つの異なるバージョンや、同じWebブラウザの2つの異なるバージョンなどです。ユーザーが同じセッションで両方のバージョンを起動することを許可しない方がよいでしょう。

  ソフトウェアスイートのバージョンごとにアプリケーショングループを作成し、各バージョンのソフトウェアスイートのアプリケーションを対応するアプリケーショングループに追加します。これらのアプリケーショングループのそれぞれでグループ間のセッション共有が無効になっている場合、それらのグループで指定されたユーザーは、同じバージョンのアプリケーションを同じセッションで実行できます。ユーザーは同時に他のアプリケーションを実行できますが、同じセッションでは実行できません。異なるバージョンのアプリケーション、またはアプリケーショングループに含まれていないアプリケーションを起動すると、そのアプリケーションは新しいセッションで起動されます。

このアプリケーショングループ間のセッション共有機能は、セキュリティサンドボックス機能ではありません。これは完璧ではなく、ユーザーが他の手段（たとえば、Windowsエクスプローラーを介して）でアプリケーションをセッションに起動するのを防ぐことはできません。

マシンが容量に達している場合、新しいセッションは開始されません。必要に応じて、セッション共有を使用して、マシン上の既存のセッションで新しいアプリケーションが開始されます。

アプリケーションセッション共有が許可されているアプリケーショングループに対してのみ、プレ起動セッションを利用可能にできます。（セッションリンガー機能を使用するセッションは、すべてのアプリケーショングループで利用可能です。）これらの機能は、アプリケーショングループに関連付けられている各デリバリーグループで有効にして構成する必要があります。アプリケーショングループでは構成できません。

デフォルトでは、アプリケーショングループを作成すると、アプリケーショングループ間のアプリケーションセッション共有が有効になります。グループの作成時にこれを変更することはできません。アプリケーショングループを作成した後、グループを編集してこの設定を変更できます。(/ja-jp/citrix-virtual-apps-desktops/2503/install-configure/application-groups-manage.html)を参照してください。

アプリケーショングループ内のセッション共有を無効にする

同じアプリケーショングループ内のアプリケーション間でアプリケーションセッション共有を防ぐことができます。

- **アプリケーショングループ内のセッション共有を無効にすることが役立つ例:**

  ユーザーに、別々のモニターでアプリケーションの複数の同時フルスクリーンセッションにアクセスさせたい場合。

  アプリケーショングループを作成し、そこにアプリケーションを追加します。

デフォルトでは、アプリケーショングループを作成すると、アプリケーションセッション共有が有効になります。グループの作成時にこの設定を変更することはできません。アプリケーショングループを作成した後、グループを編集してこの設定を変更できます。(/ja-jp/citrix-virtual-apps-desktops/2503/install-configure/application-groups-manage.html)を参照してください。

アプリケーショングループを作成する

アプリケーショングループを作成するには：

1. Web Studioにサインインします。
2. 左ペインで**アプリケーション**を選択し、**アプリケーショングループ**タブを選択します。
3. フォルダーを使用してアプリケーショングループを整理するには、**アプリケーショングループ**ルートフォルダーの下にフォルダーを作成します。詳細については、「フォルダーを使用したアプリケーショングループの整理」を参照してください。
4. グループを作成するフォルダーを選択し、**アプリケーショングループの作成**をクリックします。グループ作成ウィザードが**はじめに**ページから起動します。このページは、今後のウィザード起動時に表示しないように設定できます。

5. ウィザードに従って、以下に説明するページで設定を構成します。各ページでの作業が完了したら、**概要**ページに到達するまで**次へ**を選択します。

手順1. デリバリーグループ

デリバリーグループページには、すべてのデリバリーグループと、各グループに含まれるマシンの数が一覧表示されます。

- **互換性のあるデリバリーグループ**リストには、選択可能なデリバリーグループが含まれています。互換性のあるデリバリーグループには、ランダム（永続的または静的に割り当てられていない）なマルチセッションまたはシングルセッションOSマシンが含まれています。
- **互換性のないデリバリーグループ**リストには、選択できないデリバリーグループが含まれています。各エントリには、静的に割り当てられたマシンが含まれているなど、互換性がない理由が説明されています。

アプリケーショングループは、アプリケーションを配信できる共有（プライベートではない）マシンを含むデリバリーグループに関連付けることができます。

以下の両方の条件が満たされている場合、デスクトップのみを配信する共有マシンを含むデリバリーグループを選択することもできます。

- デリバリーグループに共有マシンが含まれており、XenDesktopバージョン7.9より前のバージョンで作成されている。
- デリバリーグループの編集権限がある。

アプリケーショングループ作成ウィザードがコミットされると、デリバリーグループの種類は自動的に「デスクトップとアプリケーション」に変換されます。

関連付けられたデリバリーグループがないアプリケーショングループを作成できますが（アプリケーションを整理するため、または現在使用されていないアプリケーションのストレージとして機能させるためなど）、少なくとも1つのデリバリーグループを指定するまで、そのアプリケーショングループをアプリケーションの配信に使用することはできません。また、デリバリーグループが指定されていない場合、**スタート**メニューソースからアプリケーショングループにアプリケーションを追加することはできません。

選択したデリバリーグループは、アプリケーションの配信に使用されるマシンを指定します。アプリケーショングループに関連付けるデリバリーグループの横にあるチェックボックスをオンにします。

タグ制限を追加するには、**タグを持つマシンへの起動を制限する**を選択し、ドロップダウンリストからタグを選択します。

ステップ2. ユーザー

アプリケーショングループでアプリケーションユーザーを指定します。前のページで選択したデリバリーグループ内のすべてのユーザーとユーザーグループを許可するか、それらのデリバリーグループから特定のユーザーとユーザーグループを選択します。指定されたユーザーに利用を制限する場合、デリバリーグループで指定されたユーザー、アプリケーショングループのみがこのグループ内のアプリケーションにアクセスできます。基本的に、アプリケーショングループ内のユーザーリストは、デリバリーグループ内のユーザーリストに対するフィルターとして機能します。

認証されていないユーザーによるアプリケーションの使用の有効化または無効化は、アプリケーショングループではなく、デリバリーグループでのみ利用できます。

展開でユーザーリストがどこに指定されているかについては、ユーザーリストが指定されている場所を参照してください。

ステップ3. アプリケーション

知っておくと良いこと:

- デフォルトでは、追加する新しいアプリケーションは**アプリケーション**という名前のフォルダーに配置されます。別のフォルダーを指定することもできます。アプリケーションを追加しようとして、同じ名前のアプリケーションがそのフォルダーに存在する場合、追加しようとしているアプリケーションの名前を変更するよう求められます。提案された一意の名前に同意すると、その新しい名前でアプリケーションが追加されます。そうでない場合は、追加する前に自分で名前を変更する必要があります。詳細については、アプリケーションフォルダーの管理を参照してください。
- アプリケーションのプロパティ（設定）は、追加時または後で変更できます。アプリケーションプロパティの変更を参照してください。同じ名前の2つのアプリケーションを同じユーザーに公開する場合、Web Studioで**アプリケーション名（ユーザー向け）**プロパティを変更してください。そうしないと、ユーザーはCitrix Workspaceアプリで重複した名前を目にすることになります。
- アプリケーションを複数のアプリケーショングループに追加する場合、それらのすべてのグループでアプリケーションを表示する十分な権限がないと、表示の問題が発生する可能性があります。そのような場合は、より高い権限を持つ管理者に相談するか、アプリケーションが追加されたすべてのグループを含むようにスコープを拡張してください。

ドロップダウンメニューから**追加**をクリックして、アプリケーションソースを表示します。

- **スタートメニューから:** 選択したデリバリーグループ内のマシンで検出されたアプリケーション。このソースを選択すると、検出されたアプリケーションのリストを含む新しいページが起動します。追加するアプリケーションのチェックボックスを選択し、**OK**をクリックします。

以下のいずれかを選択した場合、このソースは選択できません。

- 関連付けられたデリバリーグループがないアプリケーショングループ。
- 関連付けられたデリバリーグループにマシンが含まれていないアプリケーショングループ。
- マシンが含まれていないデリバリーグループ。

- **手動で定義:** サイト内またはネットワーク上の他の場所にあるアプリケーション。このソースを選択すると、実行可能ファイルへのパス、作業ディレクトリ、オプションのコマンドライン引数、管理者およびユーザーの表示名を入力する新しいページが起動します。この情報を入力したら、**OK** をクリックします。
- **既存:** 以前にサイトに追加されたアプリケーション。このソースを選択すると、検出されたアプリケーションのリストが表示された新しいページが起動します。追加するアプリケーションのチェックボックスをオンにして、**OK** をクリックします。サイトにアプリケーションがない場合、このソースは選択できません。
- **App-V:** App-Vパッケージ内のアプリケーション。このソースを選択すると、**App-Vサーバー** または **アプリケーションライブラリ** を選択する新しいページが起動します。表示された画面から、追加するアプリケーションのチェックボックスをオンにして、**OK** をクリックします。詳しくは、「App-Vアプリケーションの展開と配信」を参照してください。サイトでApp-Vが構成されていない場合、このソースは選択できません（または表示されない場合があります）。

記載されているように、**追加** ドロップダウンメニューの一部のエントリは、その種類の有効なソースがない場合、選択できません。互換性のないソースはまったく表示されません（たとえば、アプリケーショングループにアプリケーショングループを追加することはできないため、アプリケーショングループを作成するときにそのソースは表示されません）。

手順 4. スコープ

このページは、以前にカスタムスコープを作成した場合にのみ表示されます。デフォルトでは、**すべて** のスコープが選択されています。詳しくは、「委任管理」を参照してください。

手順 5. 概要

アプリケーショングループの名前を入力します。説明を（オプションで）入力することもできます。

概要情報を確認し、**完了** をクリックします。

アプリケーショングループの管理

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

はじめに

この記事では、作成したアプリケーショングループを管理する方法について説明します。

アプリケーショングループまたはデリバリーグループ内のアプリケーションの管理方法（以下を含む）については、アプリケーションを参照してください。

- アプリケーショングループ内のアプリケーションの追加または削除。
- アプリケーショングループの関連付けの変更。

アプリケーショングループの管理には、Delivery Group Administrator組み込みロールの委任管理権限が必要です。詳細については、委任管理を参照してください。

アプリケーショングループの有効化または無効化

アプリケーショングループが有効になっている場合、そのグループに追加されたアプリケーションを配信できます。アプリケーショングループを無効にすると、そのグループ内の各アプリケーションが無効になります。ただし、それらのアプリケーションが他の有効なアプリケーショングループにも関連付けられている場合、それらの他のグループから配信できます。アプリケーションがアプリケーショングループに関連付けられたデリバリーグループに明示的に追加された場合、アプリケーショングループを無効にしても、それらのデリバリーグループ内のアプリケーションには影響しません。

アプリケーショングループは、作成時に有効になります。グループ作成時にこの構成を変更することはできません。

1. 左ペインで を選択し、 タブを選択します。
2. アプリケーショングループを選択し、アクションバーで を選択します。
3. ページで、 チェックボックスをオンまたはオフにします。

4. ウィンドウを開いたままにするには**適用**をクリックし、変更を適用してウィンドウを閉じるには**保存**をクリックします。

アプリケーショングループ間のアプリケーションセッション共有を有効または無効にする

アプリケーショングループ間のセッション共有は、アプリケーショングループの作成時に有効になります。グループの作成時にこの構成を変更することはできません。詳細については、「アプリケーショングループとのセッション共有」を参照してください。

1. 左ペインで**アプリケーション**を選択し、**アプリケーショングループ**タブを選択します。
2. アプリケーショングループを選択し、アクションバーで**アプリケーショングループの編集**を選択します。
3. **設定**ページで、**アプリケーショングループ間のアプリケーションセッション共有を有効にする**チェックボックスをオンまたはオフにします。
4. ウィンドウを開いたままにするには**適用**をクリックし、変更を適用してウィンドウを閉じるには**保存**をクリックします。

アプリケーショングループ内でのアプリケーションセッション共有を無効にする

同じアプリケーショングループ内のアプリケーション間のセッション共有は、アプリケーショングループの作成時にデフォルトで有効になります。アプリケーショングループ間のアプリケーションセッション共有を無効にしても、同じアプリケーショングループ内のアプリケーション間のセッション共有は有効のままです。

PowerShell SDKを使用して、含まれるアプリケーション間でアプリケーションセッション共有が無効になっているアプリケーショングループを構成できます。状況によっては、このオプションが望ましい場合があります。たとえば、ユーザーにシームレスではないアプリケーションを、個別のモニター上の全画面表示のアプリケーションウィンドウで起動させたい場合があります。

アプリケーショングループ内でアプリケーションセッション共有を無効にすると、そのグループ内の各アプリケーションは新しいアプリケーションセッションで起動します。同じアプリケーションを実行している適切な切断されたセッションが利用可能な場合、そのセッションは再接続されます。たとえば、メモ帳を実行している切断されたセッションでメモ帳を起動すると、新しいセッションを作成する代わりにそのセッションが再接続されます。複数の適切な切断されたセッションが利用可能な場合、ランダムではあるが決定論的な方法で、いずれかのセッションが再接続のために選択されます。同じ状況でこの状況が再発生した場合、同じセッションが選択されますが、それ以外の場合、セッションは必ずしも予測可能ではありません。

PowerShell SDKを使用して、既存のアプリケーショングループ内のすべてのアプリケーションのアプリケーションセッション共有を無効にするか、アプリケーションセッション共有を無効にしたグループを作成します。

PowerShellコマンドレットの例

セッション共有を無効にするには、Broker PowerShellコマンドレット`New-BrokerApplicationGroup`または`Set-BrokerApplicationGroup`を使用し、パラメーター`SessionSharingEnabled`を`False`に、パラメーター`SingleAppPerSession`を`True`に設定します。

- たとえば、グループ内のすべてのアプリケーションでアプリケーションセッション共有を無効にしたアプリケーショングループを作成するには、次のようにします。

  ```
  New-BrokerApplicationGroup AppGr1 -SessionSharingEnabled $False
  -SingleAppPerSession $True
  ```

- 例えば、既存のアプリケーショングループ内のすべてのアプリケーション間でアプリケーションセッション共有を無効にするには:

  ```
  Set-BrokerApplicationGroup AppGR1 -SessionSharingEnabled $False
  -SingleAppPerSession $True
  ```

考慮事項

- `SingleAppPerSession`プロパティを有効にするには、`SessionSharingEnabled`プロパティをFalseに設定する必要があります。2つのプロパティを同時に有効にすることはできません。`SessionSharingEnabled`パラメーターは、アプリケーショングループ間のセッション共有を指します。
- アプリケーションセッション共有は、アプリケーショングループに関連付けられているがデリバリーグループには関連付けられていないアプリケーションに対してのみ機能します。デリバリーグループに直接関連付けられているすべてのアプリケーションは、デフォルトでセッションを共有します。
- アプリケーションが複数のアプリケーショングループに割り当てられている場合、グループに競合する設定がないことを確認してください。例えば、オプションが`True`に設定されているグループと、オプションが`False`に設定されている別のグループがある場合、予測できない動作になります。

アプリケーショングループの名前を変更する

1. 左ペインで**アプリケーション**を選択し、次に**アプリケーショングループ**タブを選択します。

2. アプリケーショングループを選択し、次にアクションバーで**アプリケーショングループの名前を変更**を選択します。
3. 新しい一意の名前を指定し、次に**OK**をクリックします。

アプリケーショングループとのデリバリーグループの関連付けを追加、削除、または優先順位を変更する

アプリケーショングループは、アプリケーションを配信できる共有（プライベートではない）マシンを含むデリバリーグループに関連付けることができます。

以下の両方の条件が満たされている場合、デスクトップのみを配信する共有マシンを含むデリバリーグループを選択することもできます:

- デリバリーグループに共有マシンが含まれており、7.9より前のバージョンで作成されていること。
- 「デリバリーグループの編集」権限を持っている必要があります。

アプリケーショングループの編集ダイアログがコミットされると、デリバリーグループの種類は自動的に「デスクトップとアプリケーション」に変換されます。

1. 左側のペインで**アプリケーション**を選択し、**アプリケーショングループ**タブを選択します。
2. アプリケーショングループを選択し、アクションバーで**アプリケーショングループの編集**を選択します。
3. **デリバリーグループ**ページを選択します。
4. デリバリーグループを追加するには、**追加**をクリックします。利用可能なデリバリーグループのチェックボックスをオンにします。（互換性のないデリバリーグループは選択できません。）選択が完了したら、**OK**をクリックします。
5. デリバリーグループを削除するには、削除するグループのチェックボックスをオンにして、**削除**をクリックします。プロンプトが表示されたら削除を確定します。
6. デリバリーグループの優先度を変更するには、デリバリーグループのチェックボックスをオンにして、**優先度の編集**をクリックします。優先度（0 = 最高）を入力し、**OK**をクリックします。
7. 変更を適用してウィンドウを開いたままにするには**適用**をクリックし、変更を適用してウィンドウを閉じるには**保存**をクリックします。

アプリケーショングループのタグ制限を追加、変更、または削除する

タグ制限の追加、変更、削除は、アプリケーション起動の対象となるマシンに予期せぬ影響を与える可能性があります。(/ja-jp/citrix-virtual-apps-desktops/2503/manage-deployment/tags.html)の考慮事項と注意事項を確認してください。

1. 左ペインで**アプリケーション**を選択し、**アプリケーショングループ**タブを選択します。
2. アプリケーショングループを選択し、アクションバーで**アプリケーショングループの編集**を選択します。
3. **デリバリーグループ**ページを選択します。
4. タグ制限を追加するには、**タグを持つマシンへの起動を制限する**を選択し、ドロップダウンリストからタグを選択します。
5. タグ制限を変更または削除するには、別のタグを選択するか、「**Restrict launches to machines with this tag**」のチェックを外してタグ制限を完全に削除します。
6. 加えた変更を適用してウィンドウを開いたままにするには、**適用**をクリックします。または、変更を適用してウィンドウを閉じるには、**保存**をクリックします。

アプリケーショングループでのユーザーの追加または削除

ユーザーの詳細については、「アプリケーショングループの作成」(/ja-jp/citrix-virtual-apps-desktops/2503/install-configure/application-groups-create.html#step-2-users)を参照してください。

1. 左ペインで**アプリケーション**を選択し、**アプリケーショングループ**タブを選択します。
2. アプリケーショングループを選択し、アクションバーで**アプリケーショングループの編集**を選択します。
3. **ユーザー**ページを選択します。関連付けられたデリバリーグループ内のすべてのユーザーにアプリケーショングループ内のアプリケーションの使用を許可するか、特定のユーザーとグループのみに許可するかを指定します。ユーザーを追加するには、**追加**をクリックし、追加するユーザーを指定します。ユーザーを削除するには、1人以上のユーザーを選択し、**削除**をクリックします。
4. 加えた変更を適用してウィンドウを開いたままにするには、**適用**をクリックします。または、変更を適用してウィンドウを閉じるには、**保存**をクリックします。

アプリケーショングループでのアプリケーションアイコンの追加、変更、または削除

アプリケーションアイコンを追加、変更、または削除するには、次の手順を実行します。

1. 左ペインで **Applications** を選択します。
2. **Applications** タブで、アプリケーションを選択し、**Properties** を選択します。

   アプリケーショングループレベルで変更を行うには、**Application Groups** タブに移動し、グループ内のアプリケーションを選択して、**Properties** を選択します。
3. **デリバリー**ページを選択し、**変更**を選択します。**アイコンの選択**ウィンドウが表示されます。
4. **アイコンの選択**ウィンドウで、次のいずれかを実行します。

   - アイコンを追加するには、**Add** を選択し、アイコンを参照します。
   - アイコンを削除するには、アイコンを選択し、**Remove** を選択します。
   - アイコンを変更するには、アプリケーションのアイコンを選択します。

   > **重要:**
   >
   > - サイズが200 KBを超えるアイコンは追加できません。
   > - .iconファイルのみ追加できます。
   > - 組み込みアイコンは削除できません。
   > - 使用中のアプリケーションのアイコンは削除できません。

5. **Save** を選択して変更を適用し、ウィンドウを閉じます。

アプリケーショングループのスコープを変更する

スコープは、作成した場合にのみ変更できます（「すべてのスコープ」は編集できません）。詳しくは、「委任管理」を参照してください。

1. 左側のペインで**アプリケーション**を選択し、**アプリケーショングループ**タブを選択します。
2. アプリケーショングループを選択し、アクションバーで**アプリケーショングループの編集**を選択します。
3. **スコープ**ページを選択します。スコープの横にあるチェックボックスをオンまたはオフにします。
4. 行った変更を適用してウィンドウを開いたままにするには**適用**をクリックし、変更を適用してウィンドウを閉じるには**保存**をクリックします。

アプリケーション グループのスコープを変更する

スコープを変更できるのは、スコープを作成した場合のみです (「すべてのスコープ」は編集できません)。詳細については、「委任管理」を参照してください。

1. 左側のペインで を選択し、 タブを選択します。
2. アプリケーション グループを選択し、アクション バーで を選択します。
3. ページを選択します。変更するスコープの横にあるチェック ボックスをオンまたはオフにします。
4. 変更を適用してウィンドウを開いたままにするには を選択し、変更を適用してウィンドウを閉じるには を選択します。

アプリケーション グループを削除する

アプリケーションは、少なくとも1つのデリバリー グループまたはアプリケーション グループに関連付けられている必要があります。アプリケーション グループを削除した結果、1つ以上のアプリケーションがどのグループにも属さなくなった場合、そのグループを削除するとそれらのアプリケーションも削除されるという警告が表示されます。その後、削除を確定またはキャンセルできます。

アプリケーションを削除しても、元のソースから削除されるわけではありません。ただし、再度利用可能にする場合は、もう一度追加する必要があります。

1. 左側のペインで を選択し、 タブを選択します。
2. アプリケーション グループを選択し、アクション バーで を選択します。
3. プロンプトが表示されたら削除を確定します。

フォルダーを使用してアプリケーション グループを整理する

フォルダーを作成してアプリケーション グループを整理し、簡単にアクセスできるようにすることができます。

必要な役割

デフォルトでは、以下の組み込みロールのいずれかを持っている場合、アプリケーショングループのフォルダーを作成および管理できます。

- クラウド管理者
- フル管理者
- アプリケーション グループ管理者

カスタム ロールを作成することで、管理アクションを他のユーザーに委任できます。次の表に、各アクションに必要な権限を示します。

アクション	必要な権限
アプリケーショングループフォルダーの作成	アプリケーショングループフォルダーの作成
アプリケーショングループフォルダーの削除	アプリケーショングループフォルダーの削除
アプリケーショングループフォルダーの移動	アプリケーショングループフォルダーの移動
アプリケーショングループフォルダーの名前変更	アプリケーショングループフォルダーの編集
アプリケーショングループをフォルダーに移動する	アプリケーショングループフォルダーの編集、アプリケーショングループプロパティの編集

詳しくは、「役割の作成と管理」を参照してください。

フォルダーの作成と管理

アクションバーまたは右クリックメニューを使用して、アプリケーショングループフォルダーを作成および管理できます。さらに、アプリケーショングループまたはフォルダーをフォルダーツリー内の目的の場所にドラッグすることもできます。

知っておくと便利な情報:

- フォルダーは最大5レベルまでネストできます（デフォルトのルートフォルダーを除く）。
- フォルダーにはアプリケーショングループとサブフォルダーを含めることができます。フォルダーとそのサブフォルダーにアプリケーショングループが含まれていない場合にのみ、フォルダーを削除できます。
- Web Studioのすべてのノード（**マシンカタログ**、**デリバリーグループ**、**アプリケーション**、**アプリケーショングループ**など）は、バックエンドで同じフォルダーツリーを共有します。フォルダーの名前変更または移動時の名前の競合を避けるため、異なるノード間で最上位フォルダーに一意の名前を使用してください。

  `New-BrokerAdminFolder` SDKコマンドレットを使用してフォルダーを作成し、それを**アプリケーショングループ**ノードの下に表示したい場合は、`Set-BrokerAdminFolderMetadata` コマンドレットを使用して `ContainsApplicationGroups` メタデータを追加する必要があります。

例:

```
Set-BrokerAdminFolderMetadata -AdminFolderId {adminFolderUid} -Name
ContainsApplicationGroups -Value true
```

リモートPCアクセス

注：

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

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

Remote PC Accessは、仮想デスクトップとアプリケーションを提供するCitrix Virtual Apps and Desktopsと同じコンポーネントを使用します。その結果、Remote PC Accessの展開と構成の要件およびプロセスは、仮想リソースを提供するためのCitrix Virtual Apps and Desktopsの展開に必要なものと同じです。この一貫性により、一貫した統一された管理エクスペリエンスが提供されます。ユーザーは、Citrix HDX™を使用してオフィスPCセッションを配信することで、最高のユーザーエクスペリエンスを得られます。

この機能は、**Remote PC Access**タイプのマシンカタログで構成されており、以下の機能を提供します。

- OUを指定してマシンを追加する機能。この機能により、PCの一括追加が容易になります。
- オフィスWindows PCにログオンするユーザーに基づいた自動ユーザー割り当て。シングルユーザーおよび複数ユーザーの割り当てをサポートしています。デフォルトでは、複数のユーザーを次の未割り当てマシンに自動的に割り当てます。自動割り当てを単一ユーザーに制限す

るには、Web Studioにサインインし、**設定**に移動して、**Remote PC Accessの複数ユーザーの自動割り当てを有効にする**設定をオフにします。

Citrix Virtual Apps and Desktopsは、他の種類のマシンカタログを使用することで、物理PCのより多くのユースケースに対応できます。これらのユースケースには以下が含まれます。

- 物理Linux PC
- プールされた物理PC（つまり、ランダムに割り当てられ、専用ではないもの）

> **注:**
>
> サポートされているOSバージョンの詳細については、シングルセッションOSおよびLinux VDAのVDAのシステム要件を参照してください。

> オンプレミス展開の場合、Remote PC AccessはCitrix Virtual Apps and Desktops AdvancedまたはPremiumライセンスでのみ有効です。セッションは、他のCitrix Virtual Desktops™ セッションと同じ方法でライセンスを消費します。Citrix Cloudの場合、Remote PC AccessはCitrix DaaS（旧Citrix Virtual Apps and Desktopsサービス）およびWorkspace Premium Plusで有効です。

考慮事項

Citrix Virtual Apps and Desktopsに一般的に適用されるすべての技術要件と考慮事項はRemote PC Accessにも適用されますが、物理PCのユースケースにより関連性が高かったり、排他的であったりするものもあります。

> **重要:**
>
> Windows 11物理システム（および一部のWindows 10を実行しているシステム）には、仮想化ベースのセキュリティ機能が含まれており、その結果、VDAソフトウェアがそれらを仮想マシンとして誤って検出します。この問題を軽減するには、以下のオプションがあります。

> - VDAコマンドラインインストールの一部として、「/remotepc」オプションとともに「/physicalmachine」オプションを使用する

- 前述のオプションを使用しなかった場合、VDAのインストール後に次のレジストリ値を追加します `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`
  - 名前: ForceEnableRemotePC
  - 種類: DWORD
  - データ: 1

展開に関する考慮事項

Remote PC Accessの展開を計画する際には、いくつかの一般的な決定を行う必要があります。

- 既存のCitrix Virtual Apps and Desktops展開にRemote PC Accessを追加できます。このオプションを選択する前に、次の点を考慮してください。
  - 現在のDelivery ControllerまたはCloud Connectorは、Remote PC Access VDAに関連する追加の負荷をサポートするのに適切なサイズですか？
  - オンプレミスのサイトデータベースとデータベースサーバーは、Remote PC Access VDAに関連する追加の負荷をサポートするのに適切なサイズですか？
  - 既存のVDAと新しいRemote PC Access VDAの数が、サイトごとにサポートされる最大VDA数を超えることはありませんか？
- VDAは、自動化されたプロセスを通じてオフィスPCに展開する必要があります。利用可能なオプションは次のとおりです。
  - SCCMなどの電子ソフトウェア配布 (ESD) ツール: SCCMを使用してVDAをインストールする。
  - 展開スクリプト: スクリプトを使用してVDAをインストールする。
- Remote PC Accessのセキュリティに関する考慮事項を確認してください。

注:

Remote PC Access を設計する際は、リモート PC の GPU に接続され、現在構成/動作している物理モニターの数を考慮する必要があります。モニターが Citrix セッションで使用されていなくても、GPU によって検出された場合、そのモニターの存在は GPU がサポートする最大モニター数制限にカウントされます。

マシンカタログに関する考慮事項

必要なマシンカタログの種類は、ユースケースによって異なります。

- Remote PC Accessマシンカタログ
  - Windows専用PC
  - Windows専用マルチユーザーPC。このユースケースは、複数のユーザーが異なるシフトでリモートからアクセスできる物理的なオフィスPCに適用されます。
  - プールされたWindows PC。このユースケースは、コンピューターラボのように、複数の不特定多数のユーザーがアクセスできる物理PCに適用されます。
- シングルセッションOSマシンカタログ
  - 静的 - 専用Linux PC
  - ランダム - プールされたLinux PC

マシンカタログの種類を特定したら、次の点を考慮してください。

- マシンは一度に1つのマシンカタログにのみ割り当てることができます。
- 委任管理を容易にするために、地理的な場所、部署、または各カタログの管理を適切な管理者に委任しやすくするその他のグループに基づいてマシンカタログを作成することを検討してください。
- マシンアカウントが存在するOUを選択する際は、より詳細な粒度を得るために下位レベルのOUを選択してください。そのような粒度が必要ない場合は、上位レベルのOUを選択できます。たとえば、Bank/Officers/Tellers の場合、より詳細な粒度を得るには **Tellers** を選択します。それ以外の場合は、要件に基づいて **Officers** または **Bank** を選択できます。
- Remote PC Access マシンカタログに割り当てられた後にOUを移動または削除すると、VDAの関連付けに影響を与え、将来の割り当てで問題が発生します。したがって、マシンカタログのOU割り当て更新がActive Directoryの変更計画に考慮されるように、適切に計画してください。
- OU構造のためにマシンカタログにマシンを追加するOUを選択するのが容易でない場合、OUを選択する必要はありません。後でPowerShellを使用してカタログにマシンを追加できます。デスクトップ割り当てがデリバリーグループで正しく構成されていれば、ユーザーの自動割り当ては引き続き機能します。ユーザー割り当てとともにマシンカタログにマシンを追加するサンプルスクリプトは、GitHubで入手できます。
- 統合されたWake on LANは、**Remote PC Access**タイプのマシンカタログでのみ利用可能です。

Linux VDAに関する考慮事項

これらの考慮事項は、Linux VDAに固有のものです。

- 物理マシンでは、Linux VDAを非3Dモードでのみ使用してください。NVIDIAドライバーの制限により、HDX 3Dモードが有効になっている場合、PCのローカル画面をブラックアウトできず、セッションのアクティビティが表示されます。この画面を表示することはセキュリティリスクです。
- 物理Linuxマシンには、シングルセッションOSタイプのマシンカタログを使用します。
- 自動ユーザー割り当てはLinuxマシンでは利用できません。
- ユーザーがすでにPCにローカルでログオンしている場合、StoreFront™からPCを起動しようとすると失敗します。
- 省電力オプションはLinuxマシンでは利用できません。

技術要件と考慮事項

このセクションには、物理PCの技術要件と考慮事項が含まれています。

- 以下はサポートされていません。
  - KVMスイッチ、またはセッションを切断できるその他のコンポーネント。
  - オールインワンPC、NVIDIA Optimusラップトップ、PCなどのハイブリッドPC。
  - デュアルブートマシン。
- キーボードとマウスはPCに直接接続してください。モニターや、電源を切ったり切断したりできるその他のコンポーネントに接続すると、これらの周辺機器が利用できなくなる可能性があります。入力デバイスをモニターなどのコンポーネントに接続する必要がある場合は、それらのコンポーネントの電源を切らないでください。
- PCはActive Directory Domain Servicesドメインに参加している必要があります。
- Secure BootはWindows 10およびWindows 11でのみサポートされています。
- PCにはアクティブなネットワーク接続が必要です。信頼性と帯域幅を向上させるため、有線接続が推奨されます。
- Wi-Fiを使用する場合は、次の操作を行います。

  a. 電源設定でワイヤレスアダプターをオンのままにするように設定します。

  b. ユーザーがログオンする前にワイヤレスネットワークに自動接続できるように、ワイヤレスアダプターとネットワークプロファイルを構成します。そうしないと、ユーザーがログ

オンするまでVDAは登録されません。ユーザーがログオンするまで、PCはリモートアクセスに利用できません。

c. Delivery ControllersまたはCloud ConnectorsがWi-Fiネットワークから到達可能であることを確認します。

- ラップトップコンピューターでRemote PC Accessを使用できます。ラップトップがバッテリーで動作するのではなく、電源に接続されていることを確認してください。ラップトップの電源オプションをデスクトップPCのオプションと一致するように構成します。例:

  a. 休止状態機能を無効にします。

  b. スリープ機能を無効にします。

  c. 蓋を閉じたときの動作を**何もしない**に設定します。

  d. 「電源ボタンを押したときの動作」を**シャットダウン**に設定します。

  e. ビデオカードとNICの省電力機能を無効にします。

- Remote PC Accessは、Windows 10を搭載したSurface Proデバイスでサポートされています。以前に述べたラップトップと同じガイドラインに従ってください。
- ドッキングステーションを使用している場合、ラップトップのドッキング解除と再ドッキングが可能です。ラップトップをドッキング解除すると、VDAはWi-Fi経由でDelivery ControllerまたはCloud Connectorに再登録されます。ただし、ラップトップを再ドッキングしても、ワイヤレスアダプターを切断しない限り、VDAは有線接続に切り替わりません。一部のデバイスには、有線接続が確立されたときにワイヤレスアダプターを切断する組み込み機能が提供されています。その他のデバイスでは、ワイヤレスアダプターを切断するためにカスタムソリューションまたはサードパーティ製ユーティリティが必要です。以前に述べたWi-Fiに関する考慮事項を確認してください。

  Remote PC Accessデバイスのドッキングとドッキング解除を有効にするには、次の操作を行います。

  a. **スタート**メニューで、**設定 > システム > 電源とスリープ**を選択し、**スリープ**を**なし**に設定します。

  b. **デバイスマネージャー > ネットワークアダプター > イーサネットアダプター**で、**電源の管理**に移動し、**電力の節約のために、コンピューターでこのデバイスの電源をオフにできるようにする**のチェックを外します。**このデバイスで、コンピューターのスタンバイ状態を解除できるようにする**がチェックされていることを確認します。

- 同じオフィスPCにアクセスする複数のユーザーは、Citrix Workspaceで同じアイコンを見ます。ユーザーがCitrix Workspaceにログオンすると、そのリソースがすでに別のユーザーによって使用されている場合、利用不可として表示されます。
- オフィスPCにアクセスする各クライアントデバイス（例：自宅のPC）にCitrix Workspaceアプリをインストールします。

構成シーケンス

このセクションでは、**Remote PC Access**タイプのマシンカタログを使用する場合にRemote PC Accessを構成する方法の概要を説明します。その他の種類のマシンカタログの作成方法については、マシンカタログの作成を参照してください。

1. オンプレミスサイトのみ - 統合されたWake on LAN機能を使用するには、「Wake on LAN」に概説されている前提条件を構成します。
2. Remote PC Access用に新しいCitrix Virtual Apps and Desktopsサイトが作成された場合：

   a. **Remote PC Access**サイトタイプを選択します。

   b. 「**電源管理**」ページで、デフォルトのRemote PC Accessマシンカタログの電源管理を有効または無効にするかを選択します。この設定は、後でマシンカタログのプロパティを編集して変更できます。Wake on LANの構成の詳細については、「Wake on LAN」を参照してください。

   c. 「**ユーザー**」および「**マシンアカウント**」ページで情報を入力します。

   これらの手順を完了すると、**Remote PC Access Machines**という名前のマシンカタログと、**Remote PC Access Desktops**という名前のデリバリーグループが作成されます。
3. 既存のCitrix Virtual Apps and Desktopsサイトに追加する場合：

   a. 種類が**Remote PC Access**のマシンカタログを作成します（ウィザードのオペレーティングシステムページ）。マシンカタログの作成方法について詳しくは、「マシンカタログの作成」を参照してください。ターゲットPCがRemote PC Accessで使用できるように、正しいOUを割り当ててください。

   b. マシンカタログ内のPCへのユーザーアクセスを提供するデリバリーグループを作成します。デリバリーグループの作成方法について詳しくは、「デリバリーグループの作成」を参照してください。デリバリーグループを、PCへのアクセスを必要とするユーザーを含むActive Directoryグループに割り当ててください。
4. オフィスPCにVDAを展開します。

- シングルセッションOSコアVDAインストーラー（VDAWorkstationCoreSetup.exe）を使用することをお勧めします。
- シングルセッションのフルVDAインストーラー（VDAWorkstationSetup.exe）を`/remotepc/physicalmachine`オプションとともに使用することもできます。これは、コアVDAインストーラーを使用した場合と同じ結果になります。

> **注：**
>
> RemotePCのインストールでは、特定のユーザーシナリオでVDAが期待どおりに動作するように、`/physicalmachine`引数を`/remotepc`とともに使用します。

- ヘルプデスクチームがCitrix Directorを介してリモートサポートを提供できるように、Windowsリモートアシスタンスを有効にすることを検討してください。そのためには、`/enable_remote_assistance`オプションを使用します。詳細については、「コマンドラインを使用したインストール」を参照してください。
- Directorでログオン期間情報を表示するには、シングルセッションのフルVDAインストーラーを使用し、**Citrix User Profile Management WMI Plugin**コンポーネントを含める必要があります。このコンポーネントは、`/includeadditional`オプションを使用して含めます。詳細については、「コマンドラインを使用したインストール」を参照してください。
- SCCMを使用してVDAを展開する方法については、「SCCMを使用したVDAのインストール」を参照してください。
- 展開スクリプトを使用してVDAを展開する方法については、「スクリプトを使用したVDAのインストール」を参照してください。

手順2～4を正常に完了すると、ユーザーがPCにローカルでログオンしたときに、自分のマシンに自動的に割り当てられます。

5. ユーザーには、オフィスPCにリモートでアクセスするために使用する各クライアントデバイスにCitrix Workspaceアプリをダウンロードしてインストールするよう指示してください。Citrix Workspaceアプリは、`https://www.citrix.com/downloads/`またはサポートされているモバイルデバイスのアプリケーションストアから入手できます。

レジストリを介して管理される機能

> **注意:**

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

複数ユーザーの自動割り当てを無効にする

各Delivery Controller™で、次のレジストリ設定を追加します。

`HKEY_LOCAL_MACHINE\Software\Citrix\DesktopServer`

- 名前: AllowMultipleRemotePCAssignments
- 種類: DWORD
- データ: 0

スリープモード (最小バージョン 7.16)

Remote PC Accessマシンをスリープ状態にするには、VDAにこのレジストリ設定を追加し、マシンを再起動します。再起動後、オペレーティングシステムの省電力設定が尊重されます。事前設定されたアイドルタイマーが経過すると、マシンはスリープモードに入ります。マシンがウェイクアップすると、Delivery Controllerに再登録されます。

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`

- 名前: DisableRemotePCSleepPreventer
- 種類: DWORD
- データ: 1

セッション管理

既定では、ローカルユーザーがそのマシンでセッションを開始すると (CTRL+ALT+DELを押すことで)、リモートユーザーのセッションは自動的に切断されます。この自動的な動作を防ぐには、オフィスPCに以下のレジストリエントリを追加し、その後、マシンを再起動します。

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA\RemotePC`

- 名前: SasNotification
- 種類: DWORD
- データ: 1

既定では、タイムアウト期間内に接続メッセージが確認されない場合、リモートユーザーがローカルユーザーよりも優先されます。この動作を設定するには、次の設定を使用します。

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA\RemotePC`

- 名前: RpcaMode
- 種類: DWORD
- データ:
  - 1 - 指定されたタイムアウト期間内にメッセージングUIに応答しない場合、リモートユーザーが常に優先されます。この設定が構成されていない場合、この動作がデフォルトです。
  - 2 - ローカルユーザーが優先されます。

Remote PC Access モードを適用するためのタイムアウトは、デフォルトで30秒です。このタイムアウトは構成できますが、30秒より短く設定しないでください。タイムアウトを構成するには、次のレジストリ設定を使用します。

`HKLM\SOFTWARE\Citrix\PortICA\RemotePC`

- 名前: RpcaTimeout
- 種類: DWORD
- データ: タイムアウトの秒数（10進値）

ユーザーが強制的にコンソールアクセスを取得したい場合: ローカルユーザーは、10秒の間にCtrl+Alt+Delを2回押すことで、リモートセッションのローカル制御を取得し、切断イベントを強制できます。

レジストリ変更とマシンの再起動後、リモートユーザーが使用中のPCにローカルユーザーがCtrl+Alt+Delを押してログオンしようとすると、リモートユーザーにプロンプトが表示されます。このプロンプトは、ローカルユーザーの接続を許可するか拒否するかを尋ねます。接続を許可すると、リモートユーザーのセッションは切断されます。

セッション管理のログ記録

Remote PC Access には、アクティブな ICA® セッションを持つPCに誰かがアクセスしようとしたときにログを記録するログ機能が追加されました。これにより、不要なアクティビティや予期せぬアクティビティがないか環境を監視し、インシデントを調査する必要がある場合にそのようなイベントを監査できます。

イベントはWindowsイベントビューアーを使用してログに記録され、**アプリケーションとサービス > Citrix > HostCore > ICA Service > Admin** にあります。

Remote PC Access の使用時にログに記録されるイベントは3種類あります。

Ctrl+Alt+Delイベント

このイベントは、アクティブなリモートセッション中にローカルユーザーがコンソールキーボードでCtrl+Alt+Delを押したときに表示されます。

イベントの詳細

- ログ名: アプリケーションとサービス
- イベントID: 43, 44, 45
- ソース: ICA サービス

イベント ID 43

このイベント ID は、SasNotification レジストリ値が存在しない場合、または SasNotification レジストリ値が 0 の場合に表示されます。

- メッセージ:

```
Ctrl+Alt+Del has been pressed on the endpoint.

The session management behavior is set to automatically disconnect the
remote session.
```

イベント ID 44

このイベントIDは、SasNotificationレジストリ値が1で、RpcaModeレジストリ値が1であるか、またはRpcaModeレジストリ値が存在しない場合に表示されます。

- メッセージ:

```
Ctrl+Alt+Del has been pressed on the endpoint.

The session management behavior is set to notify the remote user. The
user preference is set to remote user.
```

イベント ID 45

このイベント ID は、SasNotification レジストリ値が 1 で、RpcaMode レジストリ値が 2 の場合に表示されます。

- メッセージ:

```
Ctrl+Alt+Del has been pressed on the endpoint.

The session management behavior is set to notify the remote user.

The user preference is set to local user.
```

リモートセッション切断イベント

このイベントは、リモートセッションがさまざまな理由で切断された場合に表示されます。

イベントの詳細

- ログ名: アプリケーションとサービス
- イベントID: 46, 47, 48
- ソース: ICA Service

イベントID 46

このイベントIDは、リモートセッションが切断され、SasNotification レジストリ値が存在しないか、SasNotification レジストリ値が0である場合に表示されます。

- メッセージ:

```
The remote session for &lt;remoteUserName> has been disconnected.
```

イベントID 47

このイベントIDは、リモートユーザーがセッションの切断に同意し、SasNotification レジストリ値が1であり、RpcaMode レジストリ値が1であるか、RpcaMode レジストリ値が2であるか、または RpcaMode レジストリ値が存在しない場合に表示されます。

- メッセージ:

```
The remote session for &lt;remoteUserName> has been disconnected
because the user accepted the request to disconnect the session.
```

イベントID 48

このイベントIDは、リモートユーザーが指定されたタイムアウト期間内に切断要求を拒否せず、SasNotification レジストリ値が1であり、RpcaMode レジストリ値が2である場合に表示されます。

- メッセージ:

```
The remote session for &lt;remoteUserName> has been disconnected
because the user did not decline the disconnection request within the
configured timeout period (&lt;timeout period>).
```

Ctrl+Alt+Del 2回押しイベント

このイベントは、10秒以内にCtrl+Alt+Delが2回押された場合に表示されます。

イベントの詳細

- ログ名: アプリケーションとサービス
- イベントID: 49
- ソース: ICA Service

イベントID 49

このイベントIDは、Ctrl+Alt+Delが10秒以内に2回押されたときに表示されます。

- メッセージ:

```
The remote session for &lt;remoteUserName> has been forcibly
disconnected.
```

Wake on LAN (LAN 経由での起動)

Remote PC AccessはWake on LANをサポートしており、これにより、ユーザーは物理PCをリモートで起動できます。この機能により、ユーザーは使用していないときにオフィスPCの電源を切っておくことで、エネルギーコストを節約できます。また、誤ってマシンの電源がオフになった場合でも、リモートアクセスを可能にします。

Wake on LAN機能を使用すると、デリバリーコントローラーからの指示があった場合、PC上で実行されているVDAから、そのPCが存在するサブネットにマジックパケットが直接送信されます。これにより、追加のインフラストラクチャコンポーネントやマジックパケット配信のためのサードパーティソリューションに依存することなく、この機能が動作します。

Wake on LAN機能は、レガシーなSCCMベースのWake on LAN機能とは異なります。SCCMベースのWake on LANの詳細については、「Wake on LAN – SCCM統合」を参照してください。

制限事項

Wake on LAN機能を使用するRemote PC Accessは、ピーク時の自動電源オンをサポートしていません。

システム要件

Wake on LAN機能を使用するためのシステム要件は次のとおりです。

- コントロールプレーン:
  - シトリックス DaaS™
  - Citrix Virtual Apps and Desktops の 2009 以降のバージョン
- 物理PC:
  - VDA バージョン 2009 以降
  - Windows 10 または Windows 11。サポートの詳細については、VDA のシステム要件を参照してください。
  - BIOS/UEFI で Wake on LAN が有効になっていること
  - Windows の構成内で、ネットワークアダプターのプロパティで Wake on LAN が有効になっていること

Wake on LAN の構成

Studio を使用した Wake on LAN の構成

Wake on LAN 接続を作成するには:

1. 左側のペインで、**「ホスティング」**ノードを選択します。
2. **「接続とリソースの追加」**を選択します。
3. ウィザードの**「接続」**ページで、以下を指定します。
   a. 接続の種類: Remote PC Wake on LAN
   b. ゾーン名: Remote PC Access カタログが存在するゾーンを選択します
   c. 接続名: Wake on LAN 接続の名前を入力します
4. 「接続とリソースの追加」ウィザードの残りの手順を完了します。

Wake on LAN接続をRemote PC Accessマシンカタログに追加するには：

1. 新しいRemote PC Accessマシンカタログを作成している場合は、マシンカタログセットアップウィザードの**マシンタイプ**ページで、ドロップダウンリストを使用して接続を追加できます。
2. 既存のマシンカタログにWake on LAN接続を追加したい場合：
    a. 左側の**マシンカタログ**ノードに移動します。
    b. 適切なRemote PC Accessマシンカタログを選択します。
    c. マシンカタログを右クリックするか、上部の**その他**メニューを選択します。
    d. **マシンカタログの編集**を選択します。
    e. **電源管理**ページで、**はい**を選択します。
    f. ドロップダウンリストから適切な接続を選択します。
    g. **保存**を選択します。

> **注:**
>
> Studioを介したWake on LANの設定は、現時点ではCitrix DaaSでのみ利用可能です。

PowerShell を使用して Wake on LAN を構成する

PowerShell を使用して Wake on LAN を構成するには：

1. 既に存在しない場合は、Remote PC Access マシンカタログを作成します。
2. 既に存在しない場合は、Wake on LAN ホスト接続を作成します。
3. Wake on LAN ホスト接続の一意の識別子を取得します。
4. Wake on LAN ホスト接続をマシンカタログに関連付けます。

Wake on LAN ホスト接続を作成するには：

```
# Load Citrix SnapIns

Add-PSSnapIn -Name "*citrix*"



# Provide the name of the Wake on LAN host connection
```

```
[string]$connectionName = "Remote PC Access Wake on LAN"



# Create the hypervisor connection

$hypHc = New-Item -Path xdhyp:\Connections `

                -Name $connectionName `

                -HypervisorAddress "N/A" `

                -UserName "woluser" `

                -Password "wolpwd" `

                -ConnectionType Custom `

                -PluginId VdaWOLMachineManagerFactory `

                -CustomProperties "<CustomProperties></CustomProperties>"
`

                -Persist



$bhc = New-BrokerHypervisorConnection -HypHypervisorConnectionUid
$hypHc.HypervisorConnectionUid



# Wait for the connection to be ready before trying to use it

while (-not $bhc.IsReady)

{

    Start-Sleep -s 5

    $bhc = Get-BrokerHypervisorConnection -HypHypervisorConnectionUid
$hypHc.HypervisorConnectionUid
```

```
}
```

ホスト接続の準備ができたら、次のコマンドを実行してホスト接続の一意の識別子を取得します。

```
$bhc = Get-BrokerHypervisorConnection -Name "<WoL Connection Name>"

$hypUid = $bhc.Uid
```

接続の一意の識別子を取得したら、次のコマンドを実行して、その接続を Remote PC Access マシンカタログに関連付けます。

```
Get-BrokerCatalog -Name "<Catalog Name>" | Set-BrokerCatalog
-RemotePCHypervisorConnectionUid $hypUid
```

設計上の考慮事項

Remote PC Access で Wake on LAN を使用する予定がある場合は、次の点を考慮してください。

- 複数のマシンカタログで同じ Wake on LAN ホスト接続を使用できます。
- あるPCが別のPCを起動するには、両方のPCが同じサブネットにあり、同じWake on LANホスト接続を使用している必要があります。PCが同じマシンカタログにあるか、異なるマシンカタログにあるかは関係ありません。
- ホスト接続は特定のゾーンに割り当てられます。展開に複数のゾーンが含まれている場合は、各ゾーンに Wake on LAN ホスト接続が必要です。これはマシンカタログにも当てはまります。
- マジックパケットは、グローバルブロードキャストアドレス 255.255.255.255 を使用してブロードキャストされます。このアドレスがブロックされていないことを確認してください。
- そのサブネット内のマシンを起動できるようにするには、Wake on LAN 接続ごとに、サブネット内で少なくとも1台のPCがオンになっている必要があります。

運用上の考慮事項

Wake on LAN機能を使用する際の考慮事項は次のとおりです。

- 統合されたWake on LAN機能を使用してPCを起動するには、VDAが少なくとも1回登録されている必要があります。

- Wake on LANはPCの起動にのみ使用できます。再起動やシャットダウンなどの他の電源操作はサポートしていません。
- Wake on LAN接続が作成されると、Web Studioに表示されます。ただし、オンプレミスのCitrix Virtual Apps and Desktopsを使用している場合、Web Studio内でそのプロパティを編集することはサポートされていません。
- マジックパケットは次の2つの方法のいずれかで送信されます。

  a. ユーザーがPCへのセッションを起動しようとし、VDAが未登録の場合

  b. 管理者がWeb StudioまたはPowerShellから手動で電源オンコマンドを送信した場合

- デリバリーコントローラーはPCの電源状態を認識しないため、Web Studioでは電源状態の下に**サポートされていません**と表示されます。デリバリーコントローラーはVDAの登録状態を使用して、PCがオンかオフかを判断します。

Wake on LAN – SCCM統合

SCCM統合Wake on LANは、Remote PC Accessの代替Wake on LANオプションであり、オンプレミスのCitrix Virtual Apps and Desktopsでのみ利用可能です。

システム要件

SCCM統合Wake on LAN機能を使用するためのシステム要件は次のとおりです。

- シトリックス バーチャル アプリケーションズ アンド デスクトップ 1912 以降
- 物理PC:
  - VDAバージョン1912以降
  - Windows 10。サポートの詳細については、VDAシステム要件を参照してください。
  - ウェイク・オン・LANがBIOS/UEFIで有効になっていること
  - Wake on LANがWindows構成内のネットワークアダプターのプロパティで有効になっていること
- システムセンターコンフィギュレーションマネージャー (SCCM) 2012 R2 以降

SCCM 統合型 Wake on LAN の構成

以下の前提条件を完了してください。

1. 組織内でSCCM 2012 R2、2016、または2019を構成します。次に、すべてのRemote PC AccessマシンにSCCMクライアントを展開し、スケジュールされたSCCMインベントリサイクルが実行されるのを待つか、必要に応じて手動で強制実行します。

2. Wake Proxyのサポートについては、SCCMでオプションを有効にします。Remote PC Access Wake on LAN機能を使用するPCを含む組織内の各サブネットについて、3台以上のマシンがセンチネルマシンとして機能できることを確認してください。
3. マジックパケットのサポートについては、サブネット指向ブロードキャストまたはユニキャストのいずれかを使用してマジックパケットを送信できるように、ネットワークルーターとファイアウォールを構成します。
4. 各PCのBIOS/UEFI設定でWake on LANを構成します。
5. まだVDAを展開していない場合は、物理PCに展開します。

前提条件に対処した後、Delivery ControllerがSCCMと通信できるように、以下の手順を完了してください。

1. SCCMのホスト接続を作成します。詳細については、接続とリソースを参照してください。
    - 接続の種類として**Microsoft Configuration Manager Wake on LAN**を選択します。
    - 入力された資格情報には、スコープ内のコレクションへのアクセス権があり、**Remote Tools Operator**ロールが必要です。
2. Web Studioで接続を選択し、**接続の編集**を選択して、**詳細設定**をクリックします。
3. Wake on LANの処理に適したオプションを選択します。
    - Wake-upプロキシを使用している場合は、最初のオプションである**Microsoft System Center Configuration Manager Wake-upプロキシ**を選択します。
    - マジックパケットを使用している場合は、2番目のオプションである**Delivery Controllerによって送信されるWake on LANパケット**を選択します。
        - 適切な送信方法（**サブネット指向ブロードキャスト**または**ユニキャスト**）を選択します。

ホスト接続を作成したら、その接続をRemote PC Accessカタログに関連付けます。

- 新しいRemote PC Accessカタログを作成する場合は、カタログ作成ウィザードの**オペレーティングシステム**ページで、カタログの種類として**Remote PC Access**を選択し、ドロップダウンリストから適切な接続を選択します。
- 既存のRemote PC AccessカタログにWake on LANを追加するには：
    a. Web Studioの**マシンカタログ**ノードに移動し、マシンカタログを選択して、**マシンカタログの編集**を選択します。
    b. **電源管理**タブを選択し、マシンカタログの電源管理を有効にするには**はい**を選択します。

c. ドロップダウンリストから適切な接続を選択し、**OK**をクリックします。

トラブルシューティング

モニターのブランキングが機能しない

アクティブなHDXセッション中にWindows PCのローカルモニターがブランクにならない場合（ローカルモニターにセッションの内容が表示される場合）、GPUベンダーのドライバーに問題がある可能性があります。この問題を解決するには、次のレジストリ値を設定して、Citrix Indirect Displayドライバー（IDD）にグラフィックカードのベンダードライバーよりも高い優先順位を与えます。

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics\AdapterMerits`

- 名前: CitrixIDD
- 種類: DWORD
- データ: 3

ディスプレイアダプターの優先順位とモニターの作成の詳細については、Knowledge Centerの記事CTX237608を参照してください。

セッション管理通知が有効になっているマシンでCtrl+Alt+Delを選択すると、セッションが切断されます

SasNotificationレジストリ値によって制御されるセッション管理通知は、VDAでRemote PC Accessモードが有効になっている場合にのみ機能します。物理PCでHyper-Vの役割または仮想化ベースのセキュリティ機能が有効になっている場合、そのPCは仮想マシンとして報告されます。VDAが仮想マシン上で実行されていることを検出すると、Remote PC Accessモードを自動的に無効にします。Remote PC Accessモードを有効にするには、次のレジストリ値を追加します。

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`

- 名前: ForceEnableRemotePC
- 種類: DWORD
- データ: 1

設定を有効にするには、PCを再起動します。

診断情報

Remote PC Accessに関する診断情報は、Windowsアプリケーションイベントログに書き込まれます。情報メッセージはスロットリングされません。エラーメッセージは、重複するメッセージを破棄することでスロットリングされます。

- 3300 (情報): マシンがカタログに追加されました
- 3301 (情報): マシンがデリバリーグループに追加されました
- 3302 (情報): ユーザーに割り当てられたマシン
- 3303 (エラー): 例外

電源管理

Remote PC Access の電源管理が有効になっている場合、サブネット指向ブロードキャストでは、Controller とは異なるサブネットにあるマシンを起動できないことがあります。サブネット指向ブロードキャストを使用してサブネット間で電源管理が必要で、AMT サポートが利用できない場合は、Wake-up プロキシまたはユニキャスト方式を試してください。これらの設定が電源管理接続の高度なプロパティで有効になっていることを確認してください。

アクティブなリモートセッションはローカルのタッチスクリーン入力を記録する

VDA が Remote PC Access モードを有効にすると、マシンはアクティブなセッション中にローカルのタッチスクリーン入力を無視します。物理 PC で Hyper-V ロールまたは仮想化ベースのセキュリティ機能が有効になっている場合、PC は仮想マシンとして報告されます。VDA が仮想マシン上で実行されていることを検出すると、Remote PC Access モードは自動的に無効になります。Remote PC Access モードを有効にするには、次のレジストリ設定を追加します。

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`

- 名前: ForceEnableRemotePC
- 種類: DWORD
- データ: 1

設定を有効にするには、PC を再起動します。

その他のリソース

以下は Remote PC Access に関するその他のリソースです。

- ソリューション設計ガイダンス: Remote PC Access の設計上の決定事項。

- Remote PC Access アーキテクチャの例: Citrix Remote PC Access ソリューションのリファレンスアーキテクチャ。

コンテンツの公開

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

> Microsoft WordドキュメントやWebリンクなどのリソースへのURLまたはUNCパスであるアプリケーションを公開できます。この機能は公開コンテンツとして知られています。コンテンツを公開する機能により、ユーザーへのコンテンツ配信方法に柔軟性が加わります。既存のアクセス制御とアプリケーション管理の恩恵を受けることができます。また、コンテンツを開くためにローカルアプリケーションを使用するか、公開アプリケーションを使用するかを指定することもできます。

公開されたコンテンツは、StoreFront™およびCitrix Workspace™アプリの他のアプリケーションと同様に表示されます。ユーザーはアプリケーションにアクセスするのと同じ方法でアクセスします。クライアントでは、リソースは通常どおり開きます。

- ローカルにインストールされたアプリケーションが適切である場合、それが起動されてリソースが開かれます。
- ファイルの種類関連付けが定義されている場合、公開アプリケーションが起動されてリソースが開かれます。

コンテンツはPowerShell SDKを使用して公開します。Web Studioを使用してコンテンツを公開することはできません。ただし、公開後にWeb Studioを使用してアプリケーションのプロパティを編集することはできます。

構成の概要と準備

コンテンツの公開には、次の主要なプロパティを持つ`New-BrokerApplication`コマンドレットを使用します。（すべてのコマンドレットプロパティの説明については、コマンドレットのヘルプを参照してください。）

```
New-BrokerApplication –ApplicationType PublishedContent
-CommandLineExecutable location -Name app-name -DesktopGroup delivery-
group-name
```

`ApplicationType`プロパティは`PublishedContent`である必要があります。

`CommandLineExecutable`プロパティは、公開コンテンツの場所を指定します。以下の形式がサポートされており、255文字の制限があります。

- HTML Webサイトアドレス（例：`<http://www.citrix.com>`）
- Webサーバー上のドキュメントファイル（例：`https://www.citrix.com/press/pressrelease.doc`）
- FTPサーバー上のディレクトリ（例：`ftp://ftp.citrix.com/code`）
- FTPサーバー上のドキュメントファイル（例：`ftp://ftp.citrix.com/code/Readme.txt`>）
- UNCディレクトリパス（例：`file://myServer/myShare or \\\\myServer\\myShare`）
- UNCファイルパス（例：`file://myServer/myShare/myFile.asf` または `\\myServer\myShare\myFile.asf`）

正しいSDKがあることを確認してください。

- Citrix DaaS（旧Citrix Virtual Apps and Desktopsサービス）の展開の場合、Citrix Virtual Apps and Desktops Remote PowerShell SDKをダウンロードしてインストールします。
- オンプレミスのCitrix Virtual Apps and Desktops展開の場合、Delivery ControllerとともにインストールされるpowerShell SDKを使用します。公開コンテンツアプリケーションを追加するには、最低バージョン7.11のDelivery Controllerが必要です。

以下の手順では例を使用します。例では、次のようになります:

- マシンカタログが作成されています。
- `PublishedContentApps`という名前のデリバリーグループが作成されています。このグループは、カタログからマルチセッションOSマシンを使用します。WordPadアプリケーションがグループに追加されています。
- デリバリーグループ名、`CommandLineExecutable`の場所、およびアプリケーション名が割り当てられます。

はじめに

PowerShell SDKを含むマシンで、PowerShellを開きます。

次のコマンドレットは、適切なPowerShell SDKスナップインを追加し、返されたデリバリーグループレコードを割り当てます。

`Add-PsSnapin Citrix* $dg = Get-BrokerDesktopGroup –Name PublishedContentApps`

Citrix DaaSを使用している場合は、Citrix Cloud™の資格情報を入力して認証します。複数の顧客がいる場合は、1つを選択します。

URLを公開する

場所とアプリケーション名を割り当てた後、次のコマンドレットは、Citrixのホームページをアプリケーションとして公開します。

```
$citrixUrl = "https://www.citrix.com/"

$appName = "Citrix Home Page"



New-BrokerApplication –ApplicationType PublishedContent –
CommandLineExecutable $citrixURL –Name $appName –DesktopGroup $dg.Uid
```

成功を確認します。

- StoreFrontを開き、PublishedContentAppsデリバリーグループ内のアプリケーションにアクセスできるユーザーとしてログオンします。デフォルトのアイコンを持つ新しく作成されたアプリケーションが表示されます。アイコンのカスタマイズについては、`<https://www.citrix.com/blogs/2013/08/21/xd-tipster-changing-delivery-group-icons-revisited-xd7/>`を参照してください。
- **Citrix Home Page**アプリケーションをクリックします。URLは、ローカルで実行されているデフォルトブラウザの新しいタブで起動します。

UNCパスにあるリソースを公開する

この例では、管理者は`PublishedResources`という名前の共有をすでに作成しています。場所とアプリケーション名を割り当てた後、以下のコマンドレットはその共有内のRTFファイルとDOCXファイルをリソースとして公開します。

```
$rtfUNC = "\\GMSXJ-EDGE0.xd.local\\PublishedResources\\PublishedRTF.rtf"

$rtfAppName = "PublishedRTF"



New-BrokerApplication –ApplicationType PublishedContent

–CommandLineExecutable $rtfUNC -Name $rtfAppName

-DesktopGroup $dg.Uid



$docxUNC = "\\GMSXJ-EDGE0.xd.local\PublishedResources\PublishedDOCX.docx"

$docxAppName = "PublishedDOCX"



New-BrokerApplication –ApplicationType PublishedContent

–CommandLineExecutable $docxUNC -Name $docxAppName

-DesktopGroup $dg.Uid
```

成功を確認します。

- StoreFrontウィンドウを更新して、新しく公開されたドキュメントを表示します。
- **PublishedRTF**および**PublishedDOCX**アプリケーションをクリックします。各ドキュメントは、ローカルで実行されているWordPadで開きます。

PublishedContentアプリケーションの表示と編集

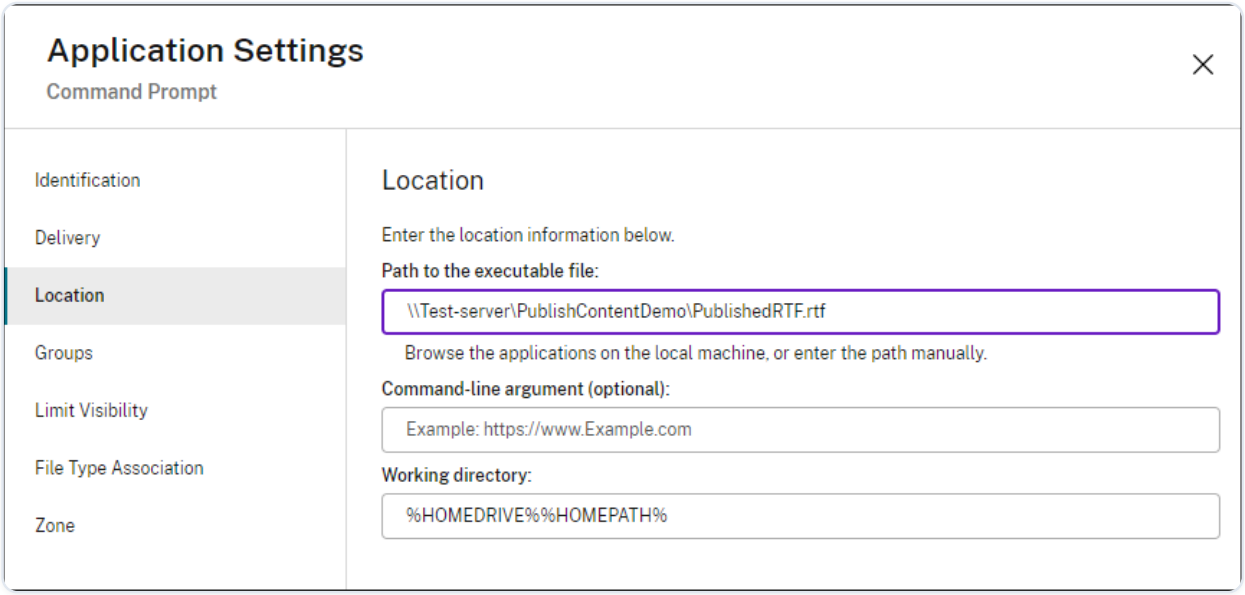
公開されたコンテンツは、他のアプリケーションタイプと同じ方法で管理します。

`PublishedContent`アプリケーションを表示および編集するには、次の手順に従います。

1. Web Studioにサインインし、左ペインで**アプリケーション**を選択します。
2. **アプリケーション**タブで、PublishedContentアプリケーションを選択し、**プロパティ**を選択します。

アプリケーションプロパティ（ユーザーの可視性、グループ関連付け、ショートカットなど）は、公開されたコンテンツに適用されます。ただし、「**場所**」ページでは、コマンドライン引数または作業ディレクトリのプロパティを変更できません。

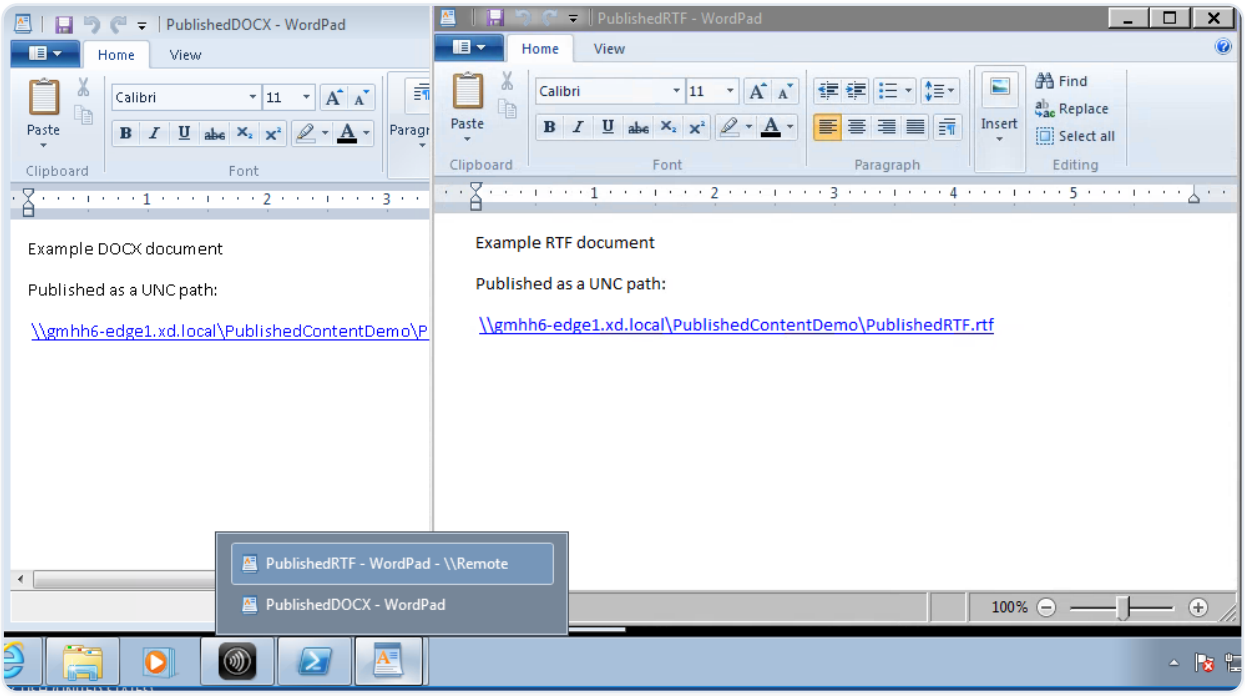
3. リソースを変更するには、そのページの「**実行可能ファイルへのパス**」フィールドを変更します。



4. 公開されたアプリケーションを使用して`PublishedContent`アプリケーションを開く（ローカルアプリケーションではなく）には、次の手順に従います。

   この例では、公開されたWordPadアプリケーションが編集され、.rtfファイル用のファイルタイプ関連付けが作成されます。

   a. デリバリーグループのメンテナンスモードをオンにします。
   b. **ファイルタイプ関連付け**プロパティを編集します。
   c. 完了したら、メンテナンスモードをオフにします。
   d. ファイルタイプ関連付けの変更を読み込むためにStoreFrontを更新し、**PublishedRTF**および**PublishedDOCX**アプリケーションをクリックします。違いに注目してください。**PublishedDOCX**は引き続きローカルのWordPadで開きます。しかし、**PublishedRTF**はファイルタイプ関連付けにより、公開されたWordPadで開くようになりました。



詳細情報

- マシンカタログを作成する
- デリバリーグループを作成する
- アプリケーションプロパティを変更する

サーバー VDI

Server VDI (Virtual Desktop Infrastructure) 機能を使用して、単一ユーザー向けにサーバーオペレーティングシステムからデスクトップを配信します。

- エンタープライズ管理者は、サーバーオペレーティングシステムをVDIデスクトップとして配信できます。これは、エンジニアやデザイナーなどのユーザーにとって価値があります。
- サービスプロバイダーは、クラウドからデスクトップを提供できます。これらのデスクトップは、Microsoft Services Provider License Agreement (SPLA) に準拠しています。

サポート:

- Citrix Virtual Apps and Desktops™ および Citrix DaaS (旧 Citrix Virtual Apps and Desktops service) の展開では、Server VDI は Windows Server 2022、Windows Server 2019、および Windows Server 2025 でサポートされています。
- すべてのServer VDI展開は、ユーザーパーソナライゼーションレイヤーテクノロジーをサポートしています。

- Server VDIがスキャナーなどのTWAINデバイスで動作するには、Windows Serverデスクトップエクスペリエンス機能がインストールされている必要があります。
- 以下の機能はServer VDIでは使用できません:
  - ホスト型アプリケーション
  - ローカルアプリアクセス
  - 直接（ブローカーなし）デスクトップ接続
  - リモートPCアクセス

Server VDIのインストールと構成

1. Windowsサーバーをインストール用に準備します。
   - Windows Server Manager を使用して、リモートデスクトップサービスロールサービスがインストールされていないことを確認します。以前にインストールされていた場合は、削除します。これらのロールサービスがインストールされていると、VDA のインストールは失敗します。
   - **各ユーザーを単一セッションに制限する** プロパティが有効になっていることを確認します。Windows サーバーで、ターミナルサーバー設定のレジストリを編集します。

     `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server`

     `DWORD fSingleSessionPerUser = 1`
2. Citrix Virtual Apps and Desktops インストーラーのコマンドラインインターフェイスを使用して、サポートされているサーバーまたはサーバーマスターイメージに VDA をインストールし、`/servervdi` オプションを指定します。（デフォルトでは、インストーラーのグラフィカルインターフェイスは、サーバーオペレーティングシステムへの Windows シングルセッション OS VDA のインストールをブロックします。コマンドラインを使用すると、この動作が上書きされます。）次のいずれかのコマンドを使用します。
   - Citrix Virtual Apps and Desktops 展開の場合：
     - `XenDesktopVdaSetup.exe /servervdi`
     - `VDAWorkstationSetup.exe /servervdi`
   - Citrix DaaS™ 展開の場合：
     - `VDAWorkstationSetup.exe /servervdi`

   その他のオプション：

- Delivery Controller または Cloud Connector を指定するには、`/controllers` を使用します。
- ファイアウォールを手動で構成する場合を除き、ファイアウォールでポートを開くには `/enable_hdx_ports` を使用します。
- イメージに VDA をインストールし、そのイメージから MCS を使用してサーバー VM を作成する場合は、`/mastermcsimage`（または `/masterimage`）を使用します。
- すべてのオプションの詳細については、「コマンドラインを使用したインストール」を参照してください。

3. Server VDI用のマシンカタログを作成します。カタログ作成ウィザードで:
   - **オペレーティングシステム**ページで、**シングルセッションOS**を選択します。
   - **概要**ページで、管理者向けに、Server VDI であることを明確に示すマシンカタログ名と説明を指定します。これは、カタログがServer VDIをサポートしていることをStudioで示す唯一のインジケーターです。

   Studioで検索を使用すると、VDAがマルチセッションマシンにインストールされている場合でも、Server VDIカタログは**シングルセッションOSマシン**タブに表示されます。
4. デリバリーグループを作成し、作成したServer VDIカタログを選択します。

VDAのインストール中にデリバリーコントローラーまたはCloud Connectorを指定しなかった場合は、後でそれらを指定することを忘れないでください。詳細については、「VDA登録」を参照してください。

ユーザーパーソナライゼーションレイヤー

> **注：**

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

> Citrix Virtual Apps and Desktopsのユーザーパーソナライゼーションレイヤー機能は、非永続的なマシンカタログの機能を拡張し、セッション間でユーザーのデータとローカルにインストールされたアプリケーションを保持します。基盤となるCitrix App Layeringテクノロジーを

> 搭載したユーザーパーソナライゼーションレイヤー機能は、非永続的なマシンカタログでCitrix ProvisioningおよびMachine Creation Services™ (MCS)をサポートします。

マスターイメージ内でVirtual Delivery Agentとともにユーザーパーソナライゼーションレイヤーコンポーネントをインストールします。VHDファイルは、ユーザーがローカルにインストールしたアプリケーションを保存します。イメージにマウントされたVHDは、ユーザー自身の仮想ハードドライブとして機能します。

> **重要：**

> ユーザーパーソナライゼーションレイヤーは、Citrix Virtual Apps and Desktopsに展開するか、イメージテンプレートで有効になっているApp Layeringユーザーレイヤーに展開できますが、両方にはできません。App Layering内のレイヤーにユーザーパーソナライゼーションレイヤー機能をインストールしないでください。

> この機能はPersonal vDisk (PvD)に代わるものであり、非永続的（プールされた）デスクトップ環境でユーザーに永続的なワークスペースエクスペリエンスも提供します。

ユーザーパーソナライゼーションレイヤー機能を展開するには、記事に詳述されている手順を使用してインストールおよび構成します。

アプリケーションのサポート

以下の例外を除き、ユーザーがデスクトップにローカルにインストールするすべてのアプリケーションは、ユーザーパーソナライゼーションレイヤーでサポートされます。

例外

以下のアプリケーションは例外であり、ユーザーパーソナライゼーションレイヤーではサポートされません。

- MS OfficeやVisual Studioなどのエンタープライズアプリケーション。
- ネットワークスタックまたはハードウェアを変更するアプリケーション。例: VPNクライアント。
- ブートレベルドライバーを持つアプリケーション。例：ウイルススキャナー。
- ドライバーストアを使用するドライバーを持つアプリケーション。例：プリンタードライバー。

> **注:**
>
> Windowsグループポリシーオブジェクト (GPO) を使用してプリンターを利用可能にできます。

サポートされていないアプリケーションをローカルにインストールすることをユーザーに許可しないでください。代わりに、これらのアプリケーションはマスターイメージに直接インストールしてください。

ローカルユーザーまたは管理者アカウントを必要とするアプリケーション

ユーザーがアプリケーションをローカルにインストールすると、そのアプリはユーザーレイヤーに格納されます。その後、ユーザーがローカルユーザーまたはグループを追加または編集しても、その変更はセッションを超えて保持されません。

> **重要:**
>
> 必要なローカルユーザーまたはグループは、マスターイメージに追加してください。

要件

ユーザーパーソナライゼーションレイヤー機能には、以下のコンポーネントが必要です。

- シトリックス バーチャル アプリケーションズ アンド デスクトップス 7 1909 以降
- Virtual Delivery Agent (VDA)、バージョン1912以降
- Citrix Provisioning™、バージョン1909以降
- Windowsファイル共有 (SMB)、またはオンプレミスAD認証が有効なAzure Files

OSがシングルセッションとして展開されている場合、以下のWindowsバージョンでユーザーパーソナライゼーションレイヤー機能を展開できます。サポートは、シングルセッション上の単一ユーザーに限定されます。

- ウィンドウズ 11 エンタープライズ x64
- Windows 10 Enterprise x64、バージョン1607以降
- Windows Server 2019 (Azure Files がサポートされています)
- Windows Server 2022 (Azure Files がサポートされています)

Citrix Virtual Apps and Desktops 7の場合、User personalization layersでのAzure Filesの使用は、Windows Server 2022、Windows Server 2019、およびWindows 10クライアントでサポートされています。

> **注:**
>
> サーバーOSを使用している場合、Server VDIのみがサポートされます。展開の詳細については、Server VDIの記事を参照してください。

> ユーザーパーソナライゼーションレイヤーは、マシンごとに一度に1人のユーザーのみをサポートし、その後、ディスクをリセットするためにマシンを再起動する必要があります。マルチセッションサーバーオペレーティングシステムではユーザーパーソナライゼーションレイヤーを使用できません。シングルセッションサーバーシステムでのみ使用できます。ユーザーパーソナライゼーションレイヤーは、非永続デスクトップでのみサポートされます。

> ユーザーパーソナライゼーションレイヤー機能がインストールされている場合は、アンインストールします。最新リリースをインストールする前に、マスターイメージを再起動します。

ファイル共有を設定する

ユーザーパーソナライゼーションレイヤー機能には、Windows Server Message Block (SMB) ストレージが必要です。Windowsファイル共有を作成するには、使用しているWindowsオペレーティングシステムの通常の手順に従ってください。

Azureベースのカタログでは Azure Filesを使用する方法の詳細については、ユーザーパーソナライゼーションレイヤーのAzure Filesストレージを設定するを参照してください。

推奨事項

ユーザーパーソナライゼーションレイヤーの展開を成功させるには、このセクションの推奨事項に従ってください。

マイクロソフト システムセンター コンフィグレーションマネージャー (SCCM)

SCCMとユーザーパーソナライゼーションレイヤー機能を使用している場合は、VDI環境でイメージを準備するためのMicrosoftのガイドラインに従ってください。詳細については、このMicrosoft TechNet記事を参照してください。

ユーザーレイヤーのサイズ

ユーザーレイヤーは、ディスク上のスペースが使用されるにつれて拡張するシンプロビジョニングディスクです。ユーザーレイヤーに許可されるデフォルトのサイズは10 GBで、これは推奨される最小値です。

> **注:**
>
> インストール中に値がゼロ (0) に設定されている場合、デフォルトのユーザーレイヤーサイズは10 GBに設定されます。

> ユーザーレイヤーのサイズを変更したい場合は、**User Layer Size**ポリシーに別の値を入力できます。「**Optional: Click Select next to User Layer Size in GB.**」の下にある「**Step 5: Create delivery group custom policies**」を参照してください。

ユーザーレイヤーサイズを上書きするためのツール (オプション)

Windowsツールを使用してユーザーレイヤーファイル共有にクォータを定義することで、ユーザーレイヤーサイズを上書きできます。

以下のMicrosoftクォータツールのいずれかを使用して、**Users**という名前のユーザーレイヤーディレクトリにハードクォータを設定します。

- ファイルサーバーリソースマネージャー (FSRM)
- クォータマネージャー

> **注:**
>
> クォータを増やすと、新しいユーザーレイヤーに影響し、既存のユーザーレイヤーを拡張します。クォータを減らすと、新しいユーザーレイヤーにのみ影響します。既存のユーザーレイヤーのサイズが小さくなることはありません。

ユーザーパーソナライゼーションレイヤーを展開する

ユーザーパーソナライゼーション機能を展開する際は、Web Studio内でポリシーを定義します。その後、その機能が展開されるマシンカタログにバインドされているデリバリーグループにポリシーを割り当てます。

マスターイメージにユーザーパーソナライゼーションレイヤーの設定がない場合、サービスはアイドル状態のままであり、オーサリングアクティビティを妨げません。

マスターイメージでポリシーを設定すると、サービスはマスターイメージ内でユーザーレイヤーを実行およびマウントしようとします。マスターイメージは予期しない動作や不安定性を示します。

ユーザーパーソナライゼーションレイヤー機能を展開するには、以下の手順をこの順序で完了します。

- ステップ1：Citrix Virtual Apps and Desktops環境の可用性を確認します。
- ステップ2：マスターイメージを準備します。
- ステップ3：マシンカタログを作成します。
- ステップ4：デリバリーグループを作成します。
- ステップ5：デリバリーグループのカスタムポリシーを作成します。

> **注:**
>
> イメージ上のWindows 10をアップグレードした後、初めてログインするのに通常よりも時間がかかります。ユーザーレイヤーは新しいバージョンのWindows 10用に更新する必要があり、その結果、ログオン時間が増加します。

ステップ 1: Citrix Virtual Apps and Desktops 環境が利用可能であることを確認する

この新機能で使用できるように、Citrix Virtual Apps and Desktops環境が利用可能であることを確認してください。セットアップの詳細については、「Citrix Virtual Apps and Desktopsのインストールと構成」を参照してください。

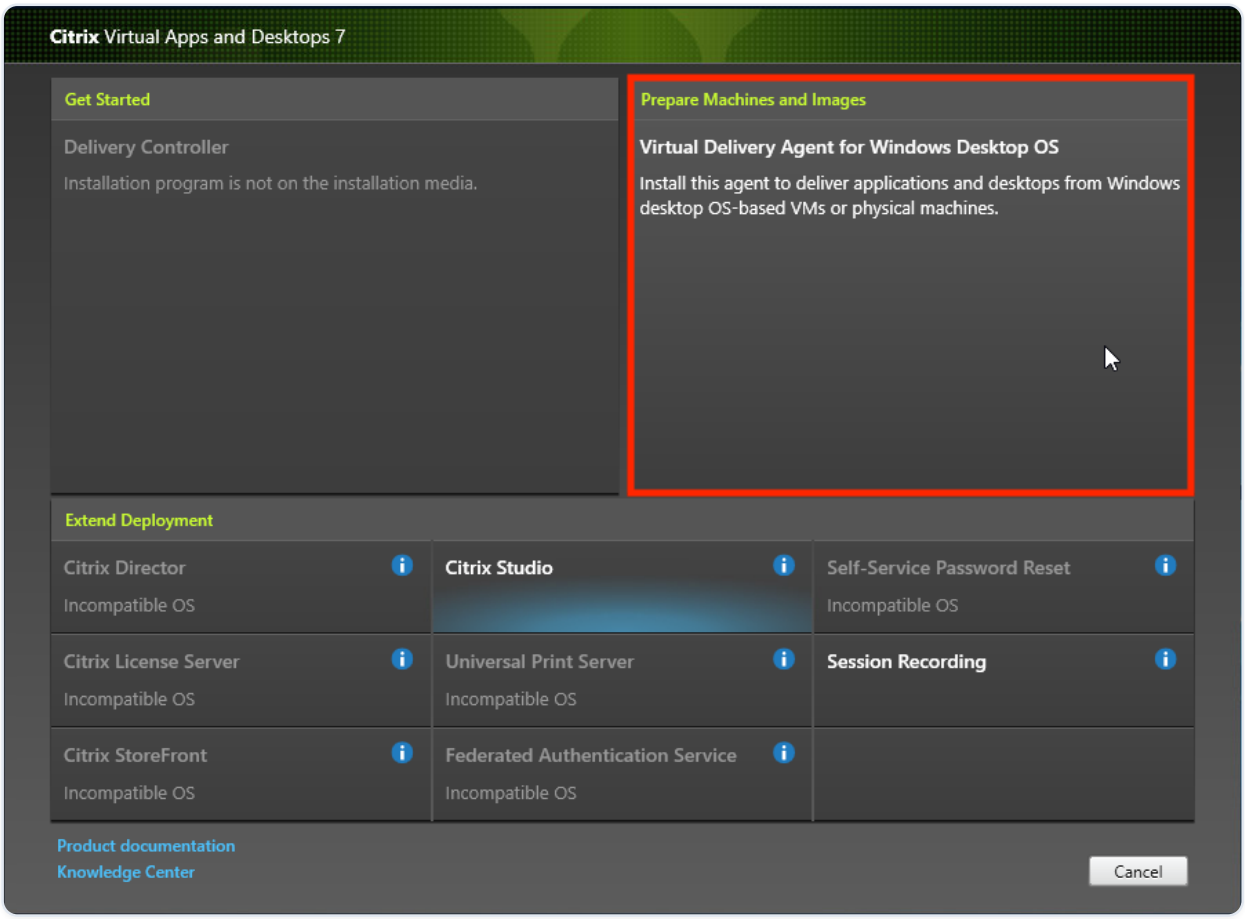
ステップ 2: マスターイメージを準備する

マスターイメージを準備するには:

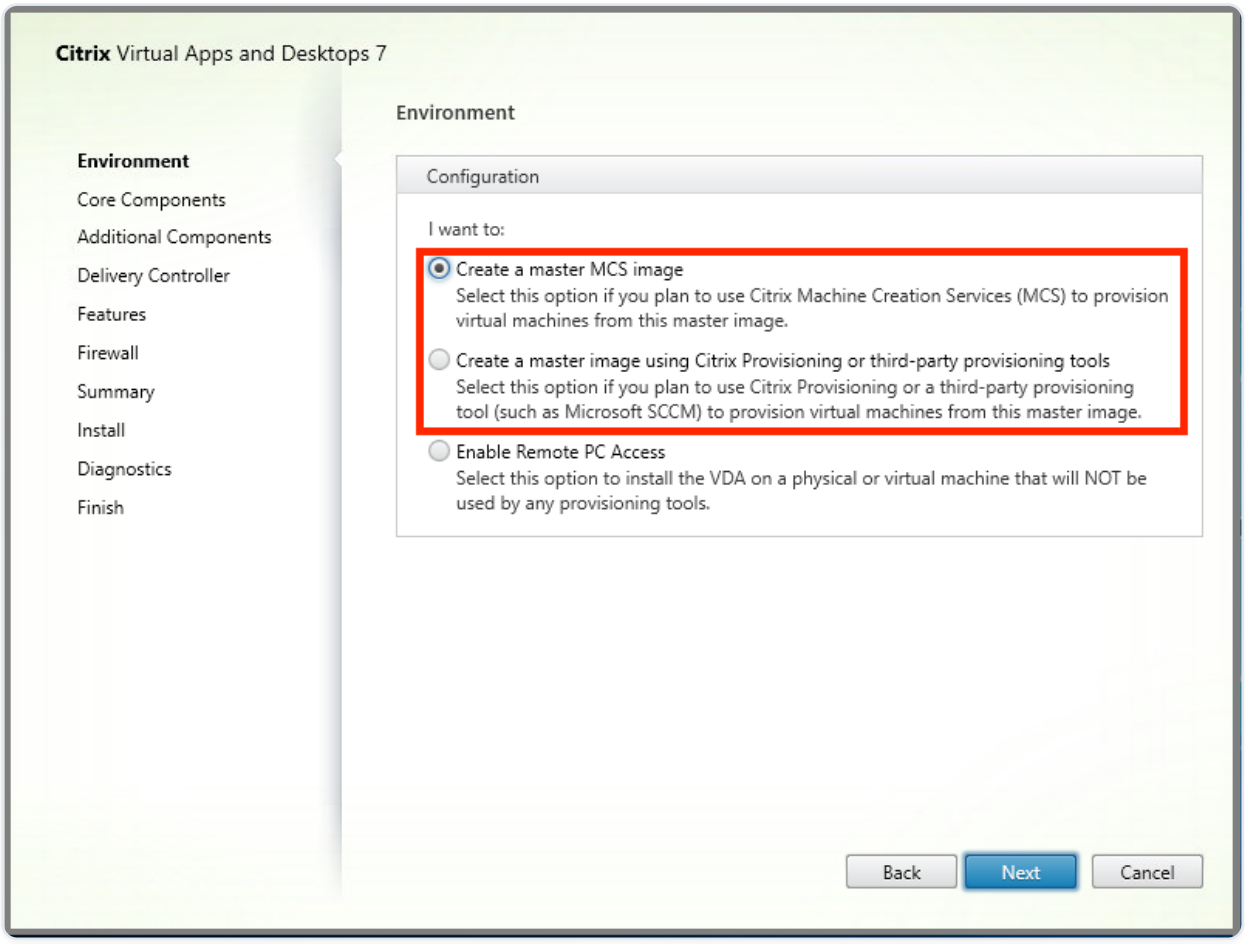
1. マスターイメージを見つけます。組織のエンタープライズアプリケーションと、ユーザーが一般的に役立つその他のアプリをインストールします。
2. Server VDI を展開する場合は、Server VDI の記事の手順に従ってください。オプションコンポーネントである **User personalization layer** を必ず含めてください。詳細については、VDA のインストール用コマンドラインオプション を参照してください。

3. Windows 10 を使用している場合は、Virtual Delivery Agent (VDA) 1912 以降をインストールします。古いバージョンの VDA がすでにインストールされている場合は、まず古いバージョンをアンインストールします。新しいバージョンをインストールするときは、オプションコンポーネントである **Citrix User Personalization Layer** を次のように選択してインストールしてください。

   a. **Virtual Delivery Agent for Windows Desktop OS** タイルをクリックします。

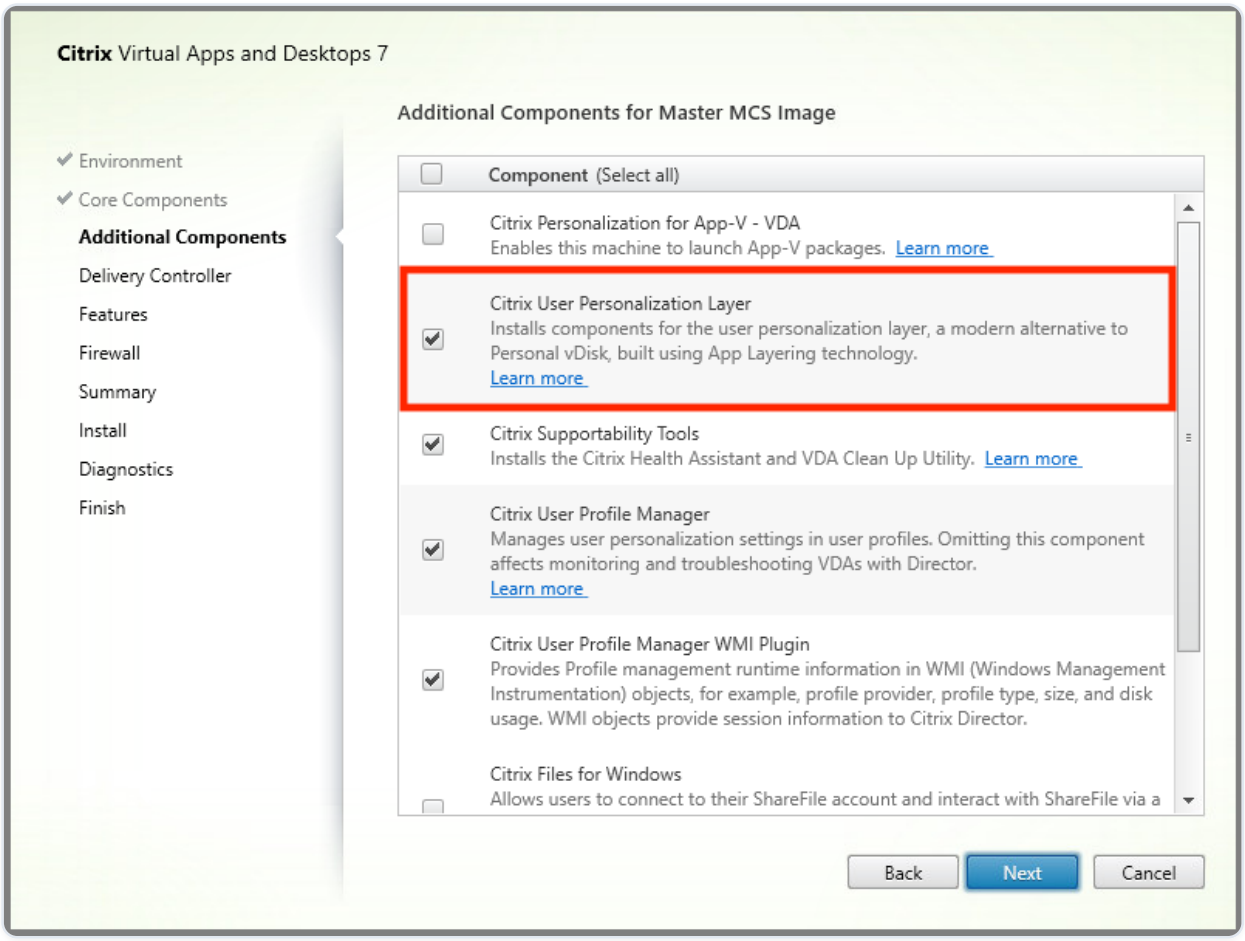


   a. **環境: マスター MCS イメージを作成** または **Citrix Provisioning またはサードパーティのプロビジョニングツールを使用してマスターイメージを作成** のいずれかを選択します。



a. **コアコンポーネント: 次へ** をクリックします。

b. **追加コンポーネント: Citrix User Personalization Layer** をオンにします。



a. 残りのインストール画面をクリックして進み、必要に応じて VDA を構成し、**インストール**をクリックします。インストール中にイメージが 1 回以上再起動します。

4. **Windows Update** は無効のままにします。ユーザーパーソナライゼーションレイヤーのインストーラーは、イメージ上の Windows Update を無効にします。更新は無効のままにしてください。

イメージを Web Studio にアップロードする準備ができました。

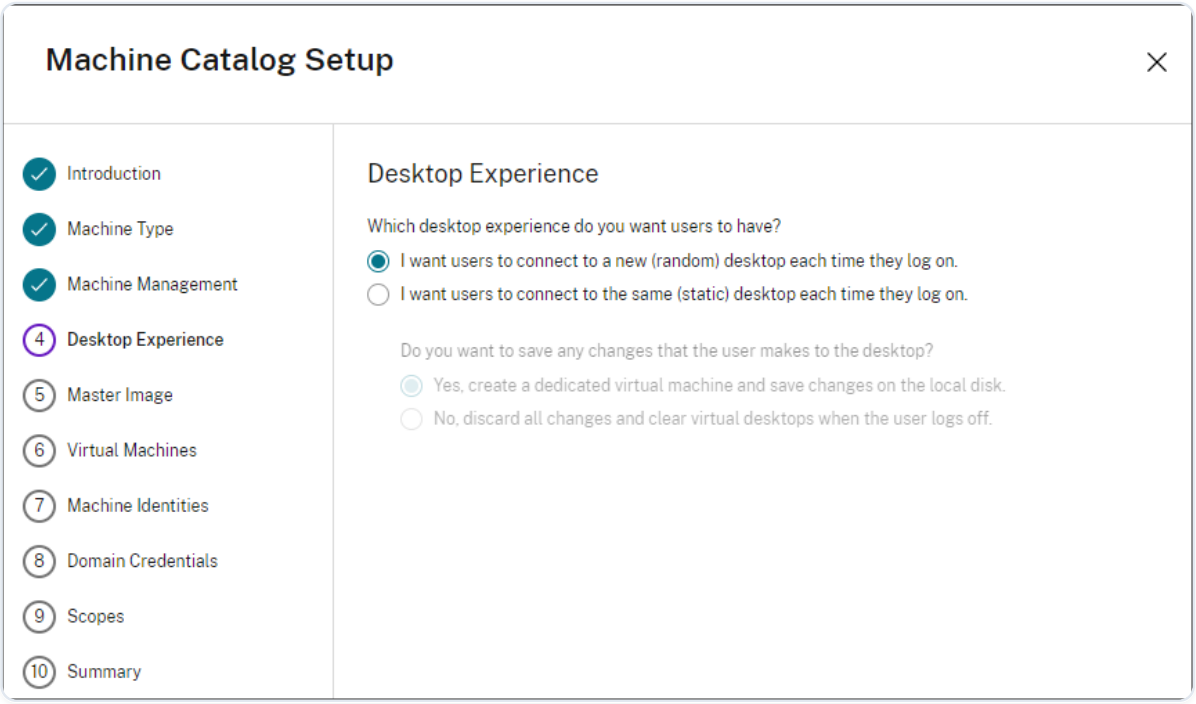
> **注:**
>
> ユーザーパーソナライゼーションレイヤー (UPL) を単にアップグレードしたい場合は、新しいバージョンの UPL とスタンドアロンパッケージを使用してアップグレードできます。VDA をアップグレードする必要はありません。

ステップ3：マシンカタログを作成する

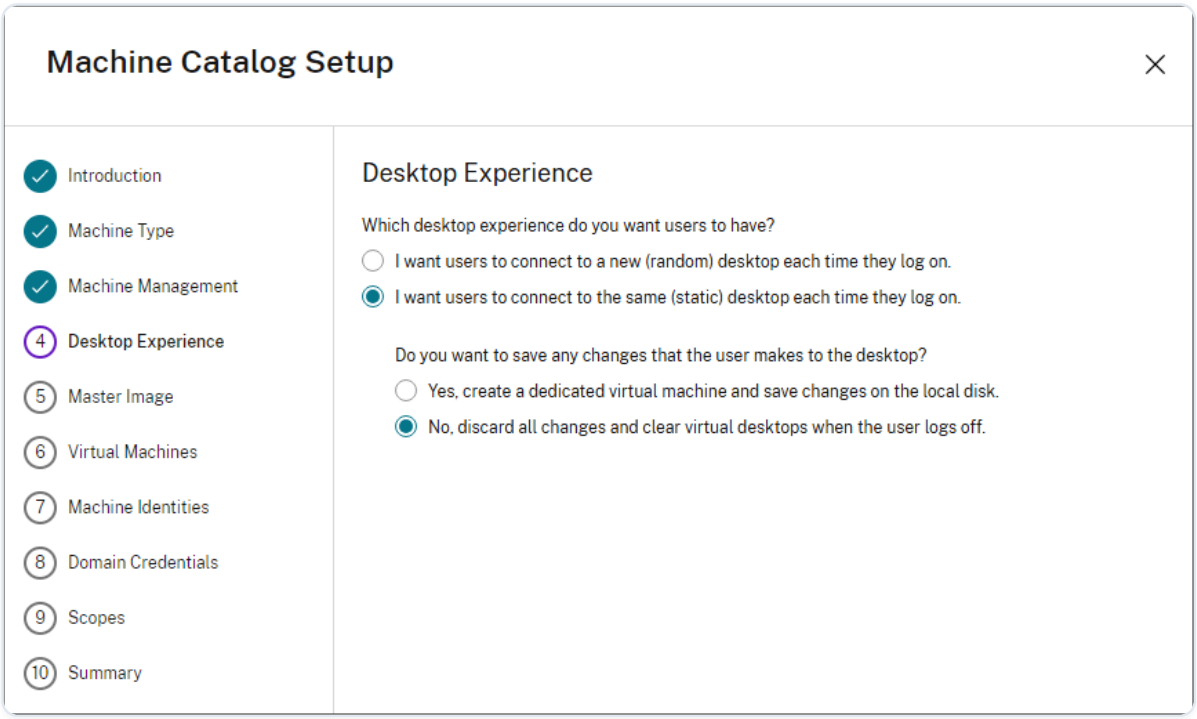
Web Studioで、マシンカタログを作成する手順に従います。カタログ作成時には、以下のオプションを使用します。

1. **オペレーティングシステム**を選択し、**シングルセッションOS**に設定します。
2. **マシン管理**を選択し、**電源管理されているマシン**に設定します。たとえば、仮想マシンやブレードPCなどです。
3. **デスクトップエクスペリエンス**を選択し、以下の例のように、**プールされたランダム**または**プールされた静的**カタログタイプに設定します。

   - **プールされたランダム:**



   - **プールされた静的:** プールされた静的を選択した場合、次のスクリーンショットに示すように、ユーザーがログオフしたときにすべての変更を破棄し、仮想デスクトップをクリアするようにデスクトップを構成します。



注:

ユーザーパーソナライゼーションレイヤーは、Citrix Personal vDiskを使用するように構成されている、または専用仮想マシンとして割り当てられているプールされた静的カタログをサポートしていません。

4. MCSを使用している場合は、**イメージ**と、前のセクションで作成したイメージのスナップショットを選択します。
5. 環境の必要に応じて、残りのカタログプロパティを構成します。

ステップ 4: デリバリーグループを作成する

作成したマシンカタログのマシンを含め、**デリバリーグループ**を作成して構成します。詳細については、デリバリーグループの作成を参照してください。

ステップ 5: デリバリーグループのカスタムポリシーを作成する

Virtual Delivery Agent 内でユーザーレイヤーのマウントを有効にするには、構成パラメーターを使用して以下を指定します。

- ネットワーク上のどこでユーザーレイヤーにアクセスするか。
- ユーザーレイヤーディスクの最大許容サイズ。

Web Studioでパラメーターをカスタムポリシーとして定義し、デリバリーグループに割り当てます。

1. Web Studio にサインインし、左ペインで を選択します。

   Studioでポリシーを選択する(/en-us/citrix-virtual-apps-desktops/2503/media/upl-studio-select-policies.png)

2. アクションバーで を選択します。 ウィンドウが表示されます。
3. 検索フィールドに `user layer` と入力します。利用可能なポリシーのリストに、次の3つのポリシーが表示されます。

   - ユーザーレイヤーの除外
   - ユーザーレイヤーリポジトリパス
   - ユーザーレイヤーサイズ (GB)

   > **注:**
   >
   > サイズを増やすと、新しいユーザーレイヤーに影響し、既存のユーザーレイヤーが拡張されます。サイズを減らすと、新しいユーザーレイヤーにのみ影響します。既存のユーザーレイヤーのサイズが小さくなることはありません。

   ユーザーレイヤーポリシーを選択する(/en-us/citrix-virtual-apps-desktops/2503/media/user-layer-policies.png)

4. 「**User Layer Repository Path**」の横にあるチェックボックスをオンにして、「**Edit**」をクリックします。「**Edit Setting**」ウィンドウが表示されます。
5. 「**Value**」フィールドにパスを入力し、「**Save**」をクリックします。

   - **パス形式:** `\\server-name-or-address\share-name\folder`
   - **パスの例:** `\\Server\Share\UPLUsers`
   - **結果のパスの例: CoolCompanyDomain** の **Alex** という名前のユーザーの場合、パスは次のようになります: `\\Server\Share\UPLUsers\Users\CoolCompanyDomain_Alex\A_OK`

   リポジトリパス (/en-us/citrix-virtual-apps-desktops/2503/media/upl-user-layer-repo-enter-path-no-variables.png)

`%USERNAME%` および `%USERDOMAIN%` 変数、マシン環境変数、および Active Directory (AD) 属性を使用してパスをカスタマイズできます。これらの変数を展開すると、明示的なパスになります。

環境変数の例:

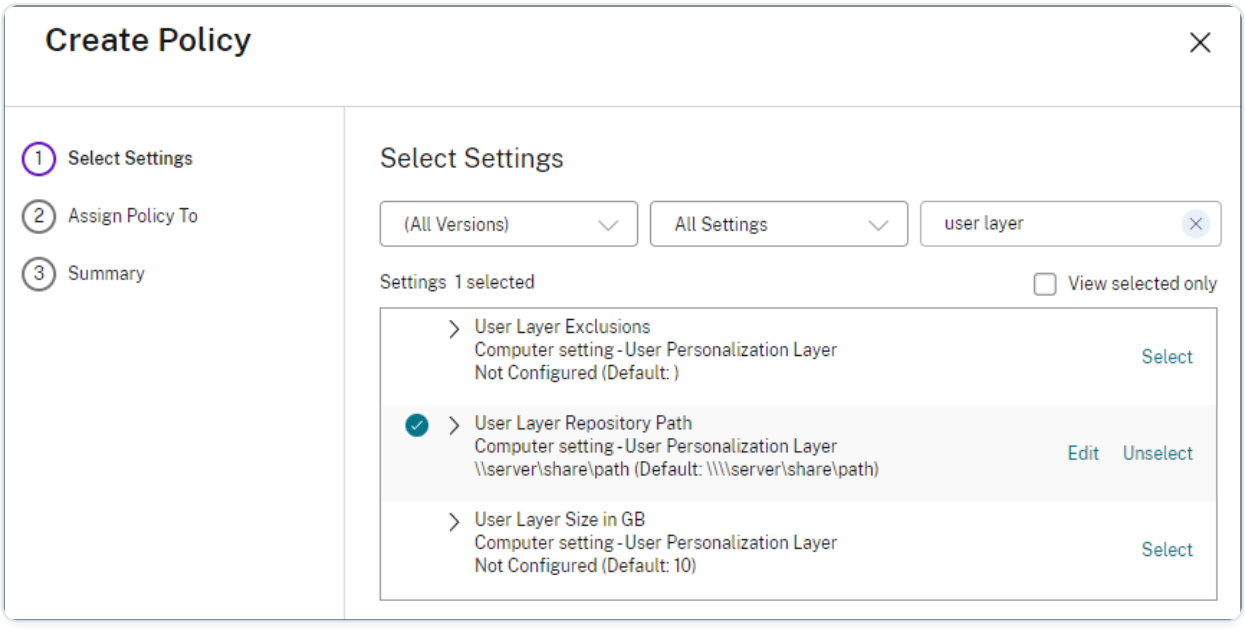
- **パス形式:** `\\Server-name-or-address\share-name\folder-with-environment-variables`
- **パスの例:** `\\Server\Share\UPLUserLayers\%USERNAME%\%USERDOMAIN%`
- **結果のパスの例: CoolCompanyDomain** の **Alex** という名前のユーザーの場合、パスは次のようになります: `\\Server\Share\UPLUserLayers\Alex\CoolCompanyDomain\A_OK`

環境変数を含むリポジトリパス (/en-us/citrix-virtual-apps-desktops/2503/media/upl-user-layer-repo-enter-path-variables.png)

カスタム AD 属性の例:

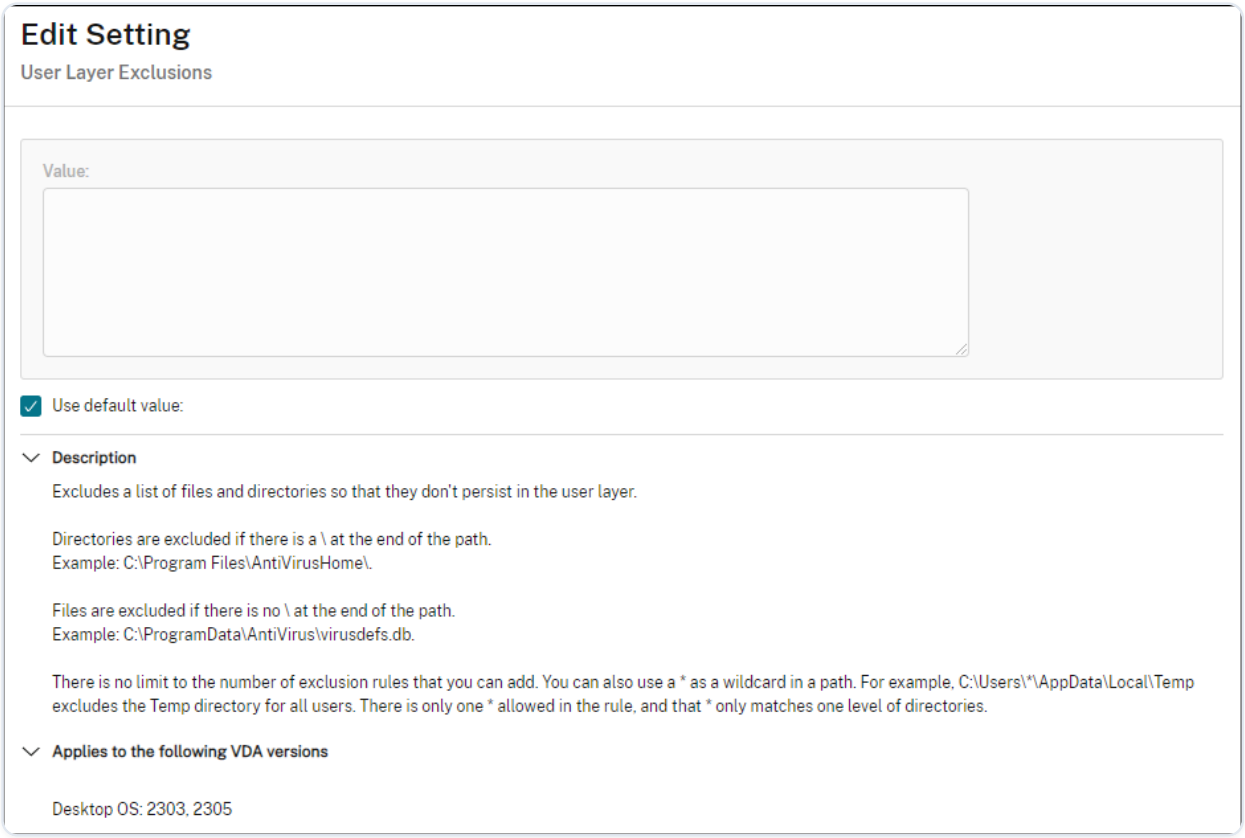
- パス形式: `\\Server-name-or-address\share-name\AD-attribute`
- パスの例: `\\Server\share#sAMAccountName#`
- 結果のパスの例: `\\Server\share\JohnSmith` (現在のユーザーに対して #sAMAccountName# が JohnSmith に解決される場合)

6. オプション: **ユーザーレイヤーサイズ (GB)** の横にあるチェックボックスをオンにして、**編集**をクリックします。

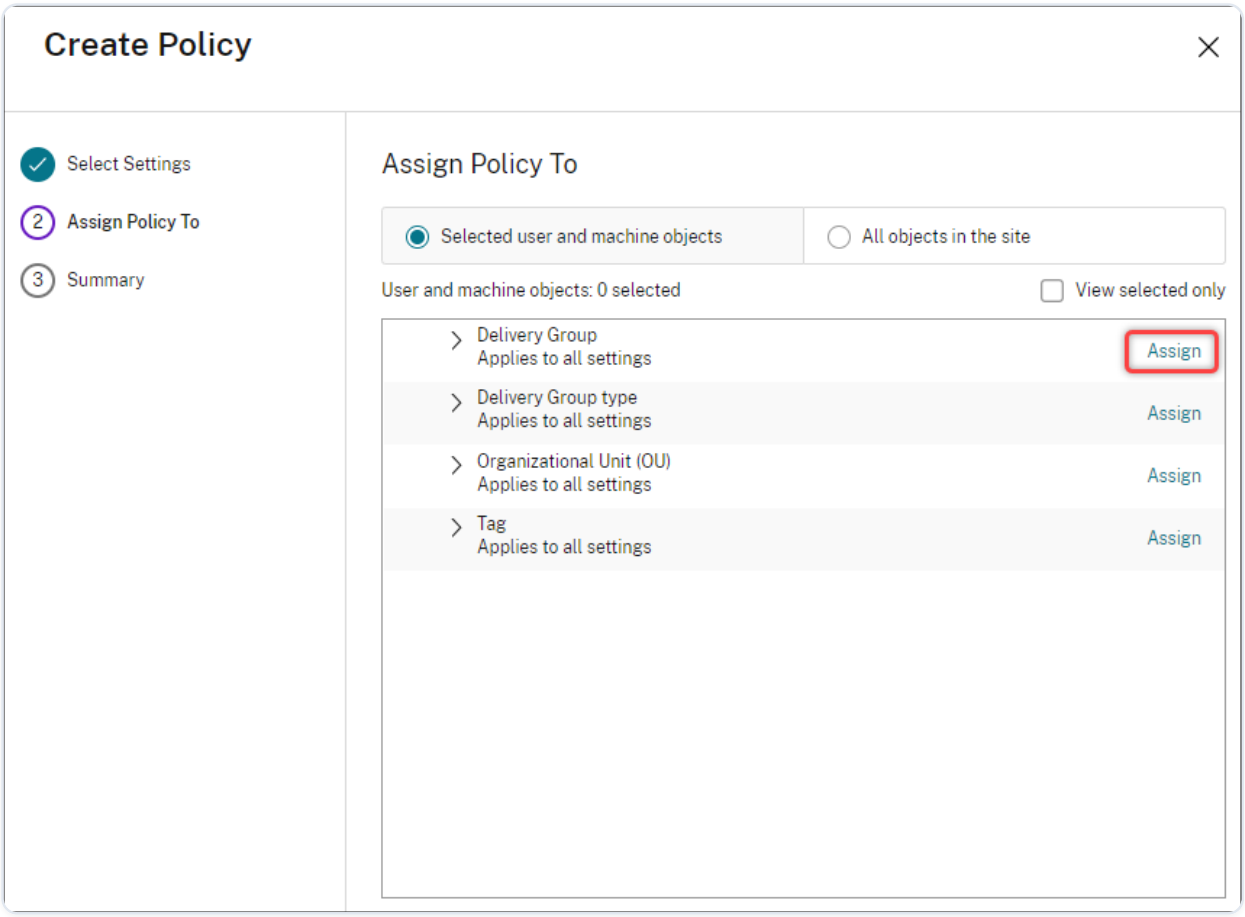


設定の編集ウィンドウが表示されます。

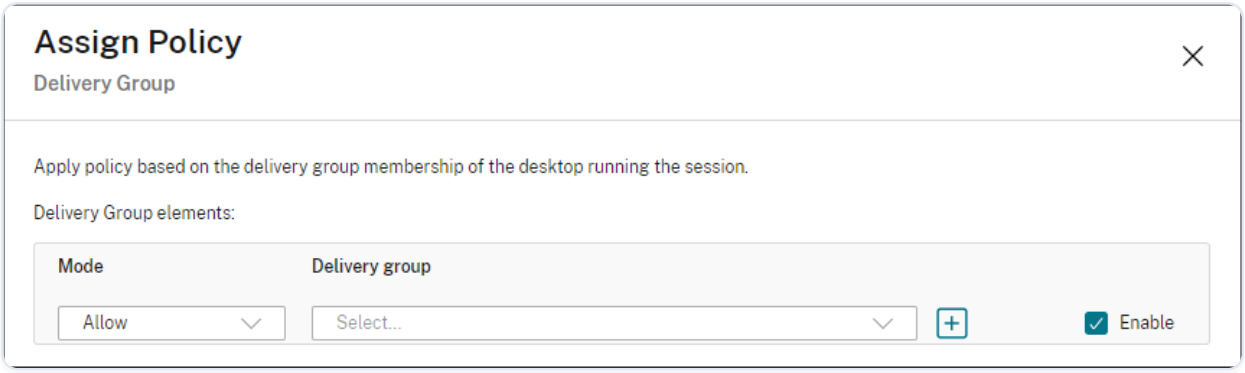
7. オプション: デフォルト値の **10 GB** を、各ユーザーレイヤーが拡張できる最大サイズに変更します。**保存**をクリックします。
8. オプション: **ユーザーレイヤーの除外**の横にあるチェックボックスをオンにして、**編集**をクリックします。



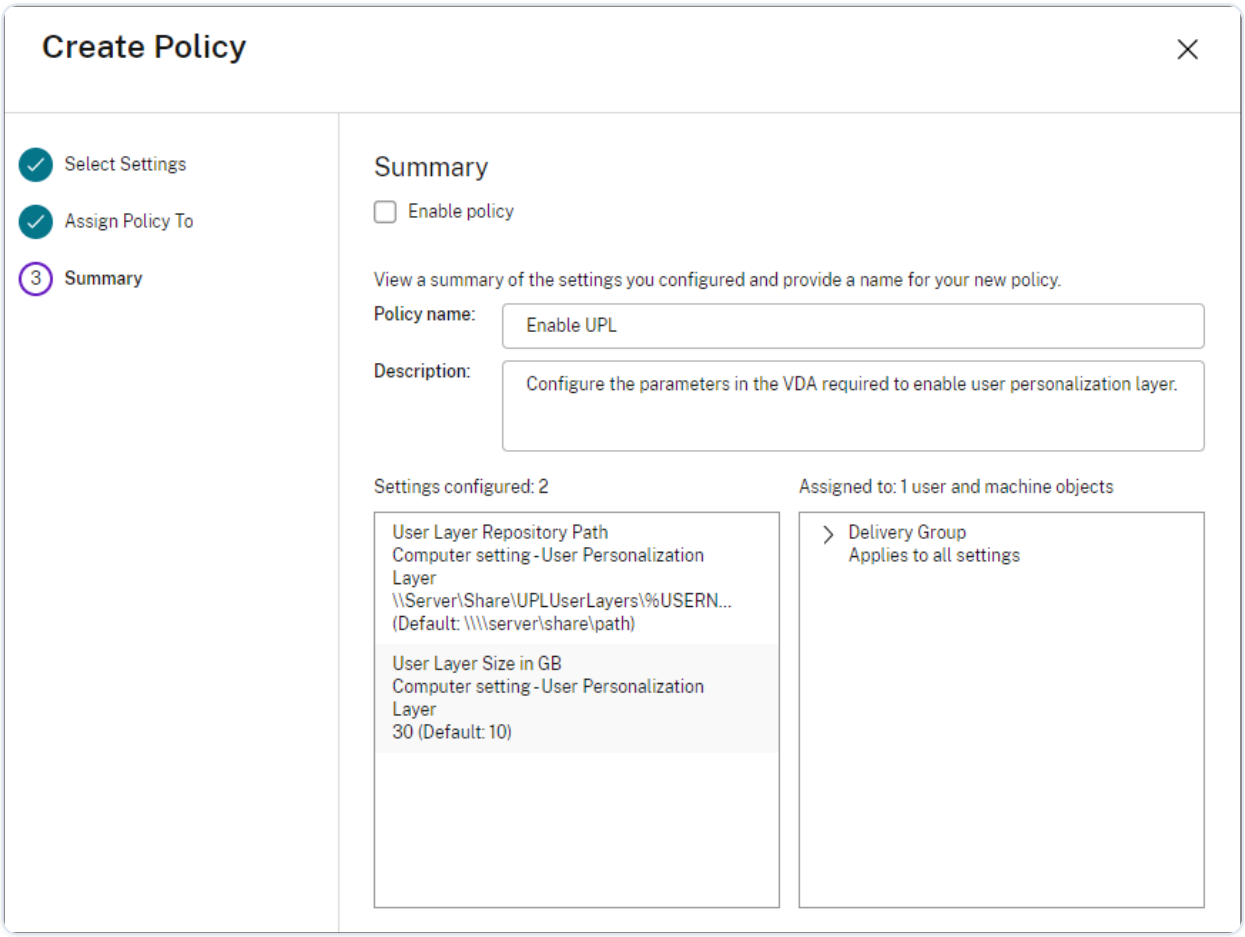
9. オプション: 除外するファイルとフォルダーを指定し、**保存**をクリックします。詳細については、Citrix App Layering のドキュメントを参照してください。
10. **次へ**をクリックして、割り当てるユーザーとマシンを設定します。この画像で強調表示されている**デリバリーグループの割り当て**リンクをクリックします。



11. **デリバリーグループ**メニューで、前のセクションで作成したデリバリーグループを選択します。**OK**をクリックします。



12. ポリシーの名前を入力します。チェックボックスをオンにしてポリシーを有効にし、**完了**をクリックします。



ユーザーレイヤーフォルダーのセキュリティ設定を構成する

ドメイン管理者として、ユーザーレイヤーのストレージ場所を複数指定できます。各ストレージ場所（デフォルトの場所を含む）に`\Users`サブフォルダーを作成します。次の設定を使用して、各場所を保護します。

設定名	値	適用先	
作成者/所有者	変更	サブフォルダーとファイルのみ	
所有者の権利	変更	サブフォルダーとファイルのみ	
ユーザーまたはグループ	フォルダーの作成/データの追加; フォルダーの横断/ファイルの実行; フォルダーの一覧表示/データの読み取り; 属性の読み取り	選択したフォルダーのみ	

設定名	値	適用先	
システム	フルコントロール	選択したフォルダー、サブフォルダー、およびファイル	
ドメイン管理者、および選択された管理者グループ	フルコントロール	選択したフォルダー、サブフォルダー、およびファイル	

ユーザーレイヤーメッセージ

ユーザーがユーザーレイヤーにアクセスできない場合、次のいずれかの通知メッセージが表示されます。

- **ユーザーレイヤーが使用中です**

  `We were unable to attach your user layer because it is in use. Any changes you make to application settings or data will not be saved. Be sure to save any work to a shared network location.`.

- **ユーザーレイヤーが利用できません**

  `We were unable to attach your user layer. Any changes you make to application settings or data will not be saved. Be sure to save any work to a shared network location.`.

- **ユーザーサインアウト後にシステムがリセットされませんでした**

  `This system was not shut down properly. Please log off immediately and contact your system administrator.`.

トラブルシューティング時に使用するログファイル

ログファイル ulayersvc.log には、変更がログに記録されるユーザーパーソナライゼーションレイヤーソフトウェアの出力が含まれています。

```
C:\ProgramData\Unidesk\Logs\ulayersvc.log
```

ユーザーレイヤー/UPL領域の再利用

ユーザーレイヤー/UPL領域の再利用を使用すると、ユーザーがログオフするたびにVHDXファイルを自動的に圧縮できます。 詳細については、ユーザーレイヤー/UPL領域の再利用を参照してください。

制限事項

ユーザーパーソナライゼーションレイヤー機能をインストールして使用する際は、以下の制限事項に注意してください。

- App Layering内のレイヤーにユーザーパーソナライゼーションレイヤーソフトウェアを展開しようと*しないでください*。Citrix Virtual Apps and Desktopsでユーザーパーソナライゼーションレイヤーを展開するか、App Layeringイメージテンプレートでユーザーレイヤーを有効にするかのいずれかであり、両方ではありません。どちらのプロセスでも、必要なユーザーレイヤーが生成されます。
- 永続的なマシンカタログでユーザーパーソナライゼーションレイヤー機能を構成*しないでください*。
- セッションホストを*使用しないでください*。
- 新しいOSインストールを実行しているイメージ (Windows 10の同じバージョンであっても) でマシンカタログを更新*しないでください*。ベストプラクティスは、マシンカタログ作成時に使用した同じマスターイメージ内でOSの更新を適用することです。
- 起動時ドライバーやその他の早期起動パーソナライゼーションを*使用しないでください*。
- PvDデータをユーザーパーソナライゼーションレイヤー機能に移行*しないでください*。
- 既存のユーザーレイヤーを完全なApp Layering製品からユーザーパーソナライゼーションレイヤー機能に移行*しないでください*。
- 異なるマスターOSイメージを使用して作成されたユーザーレイヤーにアクセスするために、ユーザーレイヤーのSMBパスを変更*しないでください*。
- ユーザーがセッションからログアウトし、再度ログインすると、新しいセッションはプール内の別のマシンで実行されます。VDI環境では、Microsoft Software Centerは最初のマシンでアプリケーションを**インストール済み**と表示しますが、2番目のマシンでは**利用不可**と表示します。

  アプリケーションの実際のステータスを確認するには、ユーザーにSoftware Centerでアプリケーションを選択し、**インストール**をクリックするように指示します。その後、SCCMはステータスを実際の値に更新します。

- ユーザーパーソナライゼーションレイヤー機能が有効になっているVDA内で、Software Centerが起動直後に停止することがあります。この問題を回避するには、XenDesktop VDI環境でのSCCMの実装に関するMicrosoftの推奨事項に従ってください。また、Software Centerを起動する前に、`ccmexec`サービスが実行されていることを確認してください。
- グループポリシー（コンピューターの構成）では、ユーザーレイヤーの設定がマスターイメージに適用された設定を上書きします。したがって、GPOを使用してコンピューターの構成で行った変更は、次回のセッションログイン時にユーザーに常に適用されるとは限りません。

  この問題を回避するには、次のコマンドを発行するユーザーログオンスクリプトを作成します。

  ```
  gpupdate /force
  ```

  たとえば、あるお客様は、ユーザーがログインするたびに次のコマンドを実行するように設定しました。

  ```
  gpudate /Target:Computer /force
  ```

  最良の結果を得るには、ユーザーがログインした後、ユーザーレイヤーで直接コンピューター設定に変更を適用します。
- ドメインユーザーアカウントは、マスターイメージに最後にログインしたユーザーであってはなりません。そうしないと、そのイメージからプロビジョニングされたマシンに問題が発生する可能性があります。
- 純粋なAzure AD環境でUPLが有効になっている場合、Azure上で実行されているWindowsの根本的な問題により、カスタム証明書は永続化されません。Microsoftが将来の機能強化でこの問題を修正した場合、この記事を更新します。

コンポーネントの削除

コンポーネントを削除するには、Citrix®はWindowsのプログラムの削除または変更機能を使用することを推奨します。または、コマンドライン、あるいはインストールメディア上のスクリプトを使用してコンポーネントを削除することもできます。

コンポーネントを削除しても、前提条件は削除されず、ファイアウォール設定も変更されません。たとえば、デリバリーコントローラー™を削除しても、SQL Serverソフトウェアとデータベースは削除されません。

Web Interfaceを含む以前の展開からControllerをアップグレードした場合は、Web Interfaceコンポーネントを個別に削除する必要があります。インストーラーを使用してWeb Interfaceを削除することはできません。

以下に記載されていない機能の削除については、その機能のドキュメントを参照してください。

準備

Controllerを削除する前に、サイトから削除してください。詳しくは、「Controllerの削除」を参照してください。

StudioとDirectorを閉じてから削除してください。

Windowsのプログラムの削除または変更機能を使用してコンポーネントを削除する

Windowsのプログラムの削除または変更機能から:

- Controller、Studio、Director、License Server、またはStoreFrontを削除するには、**Citrix Virtual Apps *version*** または **Citrix Virtual Apps and Desktops™ *version*** を右クリックし、**アンインストール**を選択します。インストーラーが起動し、削除するコンポーネントを選択できます。

  または、StoreFront™を削除するには、**Citrix StoreFront**を右クリックし、**アンインストール**を選択します。
- VDAを削除するには、**Citrix Virtual Delivery Agent *version*** を右クリックし、**アンインストール**を選択します。インストーラーが起動し、削除するコンポーネントを選択できます。削除後、デフォルトでマシンは自動的に再起動します。
- Universal Print Serverを削除するには、**Citrix Universal™ Print Server**を右クリックし、**アンインストール**を選択します。

コマンドラインを使用してコアコンポーネントを削除する

`\x64\XenDesktop Setup` ディレクトリから、`XenDesktopServerSetup.exe` コマンドを実行します。

- 1つまたは複数のコンポーネントを削除するには、`/remove` および `/components` オプションを指定します。
- すべてのコンポーネントを削除するには、`/removeall` オプションを指定します。

コマンドとパラメーターの詳細については、「コマンドラインを使用したインストール」を参照してください。

例えば、次のコマンドはWeb Studioを削除します。

```
\x64\XenDesktop Setup\XenDesktopServerSetup.exe /remove /components webstudio
```

アップグレード中に、`\x64\Licensing\CitrixLicensing.exe /quiet` または `\x64\Licensing\CitrixLicensing.exe /quiet /l install.log` コマンドを使用して最初にライセンスサーバーをインストールし、その後コアコンポーネントをインストールした場合は、アンインストールも同じ順序で行ってください。

1. コマンドラインを使用してライセンスサーバーをアンインストールする：

   ```
   CitrixLicensing.exe /quiet /uninstall /l uninstall.log
   ```

2. GUIまたはコマンドラインを使用してコンポーネントをアンインストールします。詳細については、「コンポーネントの削除」を参照してください。

コマンドライン `XenDesktopServerSetup.exe` または `removeall` を使用してライセンスサーバーとコンポーネントをアンインストールした場合は、レジストリエントリと残りのファイルをクリーンアップしてください。

レジストリエントリをクリーンアップするには:

1. レジストリキー `Citrix Licensing` を検索し、そのエントリを削除します。ほとんどの場合、エントリは次の場所にあります。

   ```
   "Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\Cur
   rentVersion\Uninstall\
   ```

2. レジストリキーの **Uninstall String** が指すフォルダーを削除します。

コマンドラインを使用してVDAを削除する

`\x64\XenDesktop Setup` ディレクトリから、`XenDesktopVdaSetup.exe` コマンドを実行します。

- 1つ以上のコンポーネントを削除するには、`/remove` と `/components` オプションを使用します。たとえば、VDA と Citrix Workspace アプリを削除するには、`/remove /components vda,plugin` を使用します。
- `/removeall` オプションは VDA のみを削除します。Citrix Workspace アプリは削除しません。

コマンドとパラメーターの詳細については、コマンドラインを使用したインストール を参照してください。

デフォルトでは、削除後にマシンは自動的に再起動します。

Active Directory でスクリプトを使用して VDA を削除するには、スクリプトを使用した VDA のインストールまたは削除 を参照してください。

アップグレードと移行

はじめに

アップグレードすると、新しいマシンやサイトをセットアップすることなく、展開がCitrix Virtual Apps and Desktops™ 7 **Current Release (CR)**に変更されます。これはインプレースアップグレードとして知られています。

アップグレードすると、利用資格のある最新の機能とテクノロジーにアクセスできるようになります。アップグレードには、以前のバージョンからの修正、明確化、および機能強化も含まれる場合があります。

アップグレードの概要

1. アップグレードを開始する前に、展開のアップグレードの記事を確認してください。これは、アップグレードの準備方法と実装方法を学ぶための主要な情報源です。
2. 現在のカスタマーサクセスサービスの日付が有効であり、期限切れになっていないことを確認してください。詳細については、Customer Success Services renewal licensesの記事を参照してください。
3. 準備ガイダンスを完了します。
4. インストーラーを実行してコアコンポーネントをアップグレードします。
5. システムデータベースとサイトをアップグレードします。
6. イメージ上のVDA（またはマシンに直接）をアップグレードします。
7. その他のコンポーネントをアップグレードします。

各準備およびアップグレードの手順については、展開のアップグレードで詳しく説明しています。

アップグレード可能なバージョン

次のバージョンからCitrix Virtual Apps and Desktops 2407にアップグレードできます。

- Virtual Apps and Desktops 2203 LTSR（CUの有無にかかわらず、CU5までを含む）
- Virtual Apps and Desktops 1912 LTSR（CUの有無にかかわらず、CU9までを含む）
- Citrix Virtual Apps and Desktopsの現在サポートされているCRバージョン

アップグレード可能なCitrix Virtual Apps and Desktops（およびXenApp and XenDesktop）のバージョンの一覧については、https://docs.citrix.com/jp/ja/upgrade.htmlも参照してください。

注:

- アップグレードプロセスを開始する前に、Citrix®は、お客様が管理された環境でアップグレードをテストし、特定の要件を満たしていることを確認することをお勧めします。さらに、スムーズな移行を確実にするために、非推奨リストや既知の問題を含むすべての関連製品ドキュメントを確認することをお勧めします。このアプローチは、本番システムへの潜在的な中断を軽減し、全体的なアップグレードエクスペリエンスを向上させるのに役立ちます。
- Citrix Virtual Apps and Desktops 1912 LTSRは、まもなくサポート終了フェーズに達します。 サポートされているバージョンの一覧については、「製品マトリックス」を参照してください。

よくある質問

このセクションでは、Citrix Virtual Apps and Desktopsのアップグレードに関するよくある質問に回答します。

- **Virtual Apps and Desktops環境をアップグレードする正しい順序は何ですか？**

  推奨されるアップグレードシーケンスの図と説明については、「アップグレードシーケンス」および「アップグレード手順」を参照してください。

- **私のサイトには複数のDelivery Controller（異なるゾーン）があります。一部のControllerのみをアップグレードした場合、どうなりますか？同じメンテナンス期間中にサイト内のすべてのControllerをアップグレードする必要がありますか？**

  各Controller上のさまざまなサービスが相互に通信するため、すべてのDelivery Controllerを同じメンテナンス期間中にアップグレードすることがベストプラクティスです。異なるバージョンを維持すると問題が発生する可能性があります。メンテナンス期間中には、Controllerの半分をアップグレードし、サイトをアップグレードしてから、残りのControllerをアップグレードすることをお勧めします。詳細については、「アップグレード手順」を参照してください。

- **最新バージョンに直接アップグレードできますか、それとも段階的なアップグレードを行う必要がありますか？**

アップグレード先のバージョンの**新機能**の記事で明示的に記載されていない限り、ほとんどの場合、最新バージョンにアップグレードし、中間リリースをスキップできます。

- **お客様はLong Term Service Release (LTSR) 環境からCurrent Releaseにアップグレードできますか？**

  はい。お客様はLong Term Service Releaseに長期間とどまる必要はありません。ビジネス要件と機能に基づいて、LTSR環境をCurrent Releaseに移行できます。

- **コンポーネントの混在バージョンは許可されていますか？**

  各サイト内で、Citrixはすべてのコンポーネントを同じバージョンにアップグレードすることを推奨します。一部のコンポーネントで以前のバージョンを使用することは可能ですが、最新バージョンのすべての機能が利用できない場合があります。詳細については、混在環境に関する考慮事項を参照してください。

- **Current Releaseはどのくらいの頻度でアップグレードする必要がありますか？**

  Current Release は、リリース日から 6 か月後に End of Maintenance (EOM) に達します。Citrix は、お客様が最新の Current Release を採用することを推奨しています。Current Release は、リリース日から 18 か月後に End of Life (EOL) に達します。

- **推奨されるのは、LTSRへのアップグレードですか、それともCRへのアップグレードですか？**

  Current Release (CR) は、最新かつ最も革新的なアプリ、デスクトップ、およびサーバー仮想化の機能を提供します。これにより、最先端のテクノロジーを維持し、競合他社の一歩先を行くことができます。

  Long Term Service Release (LTSR) は、長期間にわたって同じベースバージョンを維持することを好む大規模なエンタープライズ本番環境に最適です。

```
For details, see [Servicing Options]( https://www.citrix.com/support/
citrix-customer-success-services/citrix-virtual-apps-and-desktops-
servicing-options.md).
```

- **ライセンスをアップグレードする必要がありますか？**

  現在のライセンスの有効期限が切れておらず、アップグレード先のリリースで有効であることを確認してください。CTX111618を参照してください。更新の詳細については、Customer Success Servicesの更新ライセンスを参照してください。

- **アップグレードにはどのくらい時間がかかりますか？**

展開のアップグレードに必要な時間は、インフラストラクチャとネットワークによって異なります。そのため、正確な時間を提供することはできません。

- **ベストプラクティスは何ですか？**

  準備ガイダンスを理解し、それに従ってください。

- **サポートされているオペレーティングシステムは何ですか？**

  アップグレード先のバージョンのシステム要件の記事に、サポートされているOSが記載されています。

  現在の展開でサポートされなくなったオペレーティングシステムを使用している場合は、以前のオペレーティングシステムを参照してください。

- **サポートされているVMware vSphere (vCenter + ESXi) のバージョンは何ですか？**

  CTX131239には、サポートされているホストとバージョン、および既知の問題へのリンクが記載されています。

- **私のバージョンはいつEOLになりますか？**

  製品マトリックスを確認してください。

- **最新リリースにおける既知の問題は何ですか？**

  - シトリックス バーチャル アプリケーションズ アンド デスクトップス
  - StoreFront
  - シトリックス プロビジョニング
  - シトリックス ライセンス サーバー
  - Windows 用 シトリックス ワークスペース アプリ

詳細情報

Long Term Service Release (LTSR) の展開更新には、累積更新プログラム (CU) が使用されます。CUはLTSRのベースラインコンポーネントを更新し、各CUには独自のメタインストーラーが含まれています。

各CUには専用のドキュメントがあります。たとえば、2203 LTSRの場合、最新のCUについては、そのLTSRの**新機能**ページにあるリンクを確認してください。各CUページには、サポートされているバージョン情報、手順、およびCUダウンロードパッケージへのリンクが含まれています。

移行

クラウドへの移行

Citrix Virtual Apps and Desktopsの自動構成ツールを使用して、オンプレミス展開をクラウドに移行できます。詳細については、「Migrate to Cloud」を参照してください。

レガシー移行

移行とは、以前の展開から新しいバージョンにデータを移動することです。このプロセスには、新しいコンポーネントのインストールと新しいサイトの作成、古いファームからのデータのエクスポート、そして新しいサイトへのデータのインポートが含まれます。

XenAppおよびXenDesktopのバージョン、または以前のCitrix Virtual Apps and Desktopsのバージョンを移行するためのサポートされているツールやスクリプトはありません。この製品ドキュメントで説明されているCitrix Virtual Apps and Desktopsのバージョンについては、*アップグレード*がサポートされています。

以前のXenApp 6.xの移行コンテンツについては、以下を参照してください。スクリプトも記事もサポートまたは保守されていません。

- XenApp 6.xバージョンのオープンソース移行スクリプトは`<https://github.com/citrix/xa65migrationtool>`で入手できます。Citrixはこれらの移行スクリプトをサポートまたは保守していません
- 7.xでの変更点
- XenApp 6.5ワーカーを新しいVDAにアップグレードする
- XenApp 6.xを移行する

展開のアップグレード

> **注:**
>
> この記事では、Web Studio を含む展開のアップグレードについて説明します。Citrix Studio を含むアップグレードについては、Citrix Virtual Apps and Desktops™ 7 2212 以前の同等の記事を参照してください。

はじめに

新しいマシンやサイトを最初にセットアップすることなく、特定の展開を新しいバージョンにアップグレードできます。これはインプレースアップグレードと呼ばれます。

アップグレードできる Citrix Virtual Apps and Desktops のバージョンについては、「アップグレードできるバージョン」を参照してください。

Citrix Virtual Apps and Desktops のリリースにアップグレードする前に、現在の Customer Success Services の日付が有効であり、期限切れになっていないことを確認してください。詳しくは、「Customer Success Services の更新ライセンス」の記事を参照してください。

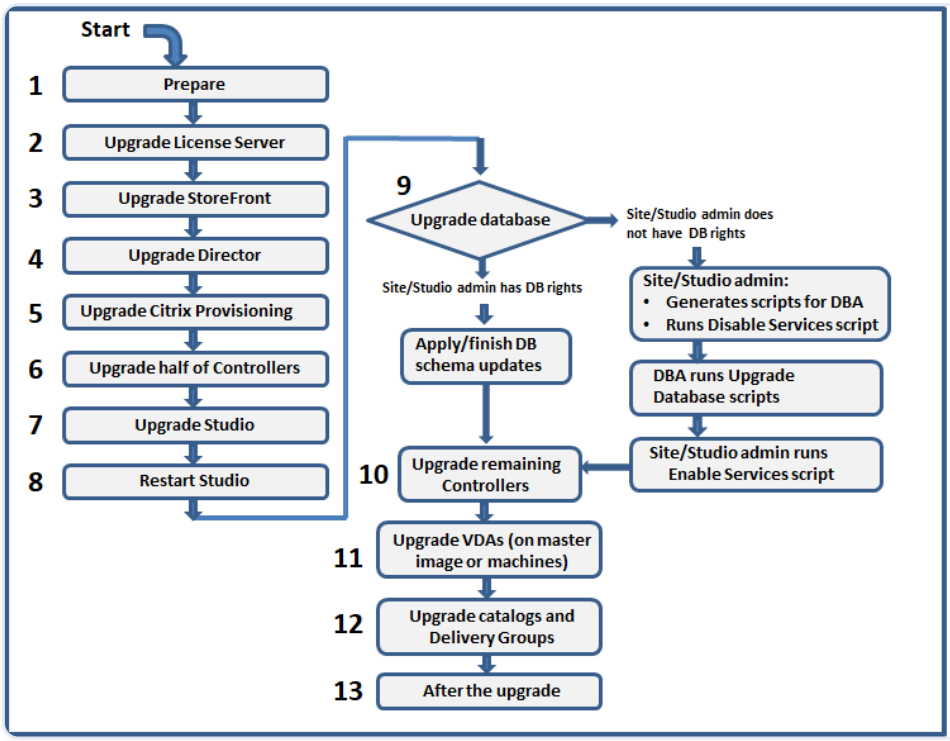
アップグレードを開始するには、新しいバージョンのインストーラーを実行して、以前にインストールされたコアコンポーネント、VDA、およびその他の特定のコンポーネントをアップグレードします。次に、データベースとサイトをアップグレードします。

新しいバージョンが提供されている場合、フルプロダクトインストーラー（およびスタンドアロン VDA インストーラー）でインストールできるコンポーネントはすべてアップグレードできます。フルプロダクトインストーラーでインストールされないその他のコンポーネント（Citrix Provisioning™ や Profile Management など）については、そのコンポーネントのドキュメントを参照してください。ホストのアップグレードについては、該当するドキュメントを参照してください。

アップグレードを開始する前に、この記事のすべての情報を確認してください。

アップグレードシーケンス

次の図は、アップグレードシーケンスの手順を示しています。「アップグレード手順」には、図の各手順の詳細が含まれています。



注:

障害を回避するため、新しいマシンカタログの作成、マシンカタログの削除、デリバリーグループ内のマシンの更新など、プロビジョニングおよびデリバリーグループ関連のタスクを実行する前に、すべてのDelivery Controllerとデータベースをアップグレードする必要があります。

ハイブリッド権限ライセンス

ハイブリッド権限ライセンスは、お客様が永続ライセンスからクラウドサービスサブスクリプションに移行またはアップグレードする際に、クラウドサービスサブスクリプションに加えて提供される期間ベースのサブスクリプションライセンスです。DaaSサブスクリプションと合わせてハイブリッド権限アドオンを購入することもできます。

SaaS属性を持つハイブリッドライツライセンスをお持ちの場合、Citrix Virtual Apps and Desktops LTSR 2203以降にアップグレードすると、Citrix Virtual Apps and Desktops LTSR 1912では利用できなかった機能にアクセスできるようになります。これらの機能には、Microsoft Azure、AWS EC2、Google Cloudなどのパブリッククラウドでのワークロードのプロビジョニングとホスティングが含まれます。新しいライセンスファイルを展開する前に、ライセンスサーバーを最新バージョンに更新してください。

SaaS属性のないハイブリッド権限ライセンスにアクセスできる場合は、以下の手順に従ってSaaS属性を持つ新しいハイブリッド権限ライセンスにアクセスしてください。

注:

- 新しいライセンスコードが記載されたメールが届きます。詳しくは、「ライセンスアクセスコードの使用」を参照してください。
- 既存のライセンスは取り消されます。取り消されたライセンスはライセンスサーバーから削除し、その後新しいライセンスをインストールする必要があります。詳しくは、「ライセンスファイルの削除」を参照してください。

1. citrix.comのライセンス管理ポータルにアクセスし、クラウドプロビジョニング権限が有効になっている（SaaS属性を持つ）新しいハイブリッド権限ライセンスファイルをダウンロードします。詳しくは、「ライセンスのダウンロード」を参照してください。次の画像は、IncrementsセクションにSaaS属性を持つハイブリッド権限ライセンスファイルを示しています。

```
INCREMENT XDT_PLT_CCS CITRIX 2022.1201 01-dec-2022 5 \
    VENDOR_STRING=;LT=RetailS;GP=720;PSL=10;CL=VDS,VDA,VDE,VDP,SaaS:SA=0;ODP=0;NUDURMIN=2880;NUDURMAX=525600;AP=ADMIN/INT/14
    OVERDRAFT=1 DUP_GROUP=V ISSUED=18-dec-2005 NOTICE="Citrix \
    Systems Inc." SN=RetailSSaaS SIGN="..."
```

2. ライセンスサーバーにハイブリッド権限ライセンスファイルをインストールします。詳しくは、「ライセンスのインストール」を参照してください。
3. ライセンスのエディションまたはモデルに変更がある場合は、brokerコマンドを実行してエディションとモデルを設定してから、インプレースアップグレードを開始してください。Brokerコマンドの詳細については、「Broker PowerShell SDK」セクションを参照してください。

Citrix Virtual Apps and DesktopsのCurrent ReleasesおよびLong Term Service Releasesでのパブリッククラウドサポートの詳細については、CTX270373を参照してください。

アップグレード手順

主要な製品コンポーネントのほとんどは、コンポーネントを含むマシンで製品インストーラーを実行することでアップグレードできます。

1台のマシンに複数のコンポーネント（Studioやライセンスサーバーなど）が含まれている場合、製品メディアにそれらのソフトウェアの新しいバージョンが含まれていれば、そのマシン上のすべてのコンポーネントがアップグレードされます。

インストーラーを使用するには：

- フル製品インストーラーのグラフィカルインターフェイスを実行するには、マシンにログオンし、メディアを挿入するか、新しいリリースのISOドライブをマウントします。「**AutoSelect**」をダブルクリックします。
- コマンドラインインターフェイスを使用するには、適切なコマンドを発行します。「コマンドラインを使用したインストール」を参照してください。

手順1：準備

アップグレードを開始する前に、準備が整っていることを確認してください。必要なタスクを読み、完了してください：

- PVD、AppDisks™、およびサポートされていないホストの削除
- PvDまたはAppDiskコンポーネントを持つVDA
- 制限事項
- 混在環境に関する考慮事項
- 以前のオペレーティングシステム
- 準備
- サイトの事前テスト
- SQL Serverのバージョンチェック

手順2：ライセンスサーバーのアップグレード

インストールに新しいバージョンのCitrix License Serverソフトウェアが含まれている場合は、他のコンポーネントよりも先にこのコンポーネントをアップグレードしてください。

まだ新しいバージョンと互換性があるかどうかを判断していない場合は、他のコアコンポーネントをアップグレードする前に、ライセンスサーバーでインストーラーを実行することが不可欠です。

ステップ3：StoreFront™のアップグレード

インストールメディアに新しいバージョンのStoreFrontソフトウェアが含まれている場合は、StoreFrontサーバーを含むマシンでインストーラーを実行します。

- グラフィカルインターフェイスで、**Extend deployment**セクションから**Citrix StoreFront**を選択します。
- コマンドラインから、Citrix Virtual Apps and Desktopsインストールメディアの`x64`フォルダーにある`CitrixStoreFront-x64.exe`を実行します。

ステップ4：Directorのアップグレード

インストールメディアに新しいバージョンのDirectorソフトウェアが含まれている場合は、Directorを含むマシンでインストーラーを実行します。

ステップ5：Citrix Provisioningのアップグレード

Citrix Provisioningのインストールメディアは、Citrix Virtual Apps and Desktopsのインストールメディアとは別に提供されています。Citrix Provisioningサーバーおよびターゲットデバイスソフトウェアのインストールとアップグレードの方法については、Citrix Provisioning製品ドキュメントを参照してください。

ステップ6：Delivery Controllerの半分をアップグレードする

たとえば、サイトに4つのControllerがある場合、そのうちの2つでインストーラーを実行します。

Controllerの半分をアクティブなままにしておくことで、ユーザーはサイトにアクセスできます。VDAは残りのControllerに登録できます。Controllerの数が少ないため、サイトの容量が低下する場合があります。アップグレードは、最終的なデータベースアップグレードステップ中に新しいクライアント接続を確立する際に、一時的な中断のみを引き起こします。アップグレードされたControllerは、サイト全体がアップグレードされるまで要求を処理できません。

サイトにControllerが1つしかない場合、アップグレード中は動作しません。

実際のアップグレードが開始される前に、最初のControllerでサイトの事前テストが実行されます。詳細については、「サイトの事前テスト」を参照してください。

ステップ7：Studioのアップグレード

Web Studio をまだアップグレードしていない場合（別のコンポーネントと同じマシンにあったため）、Studio が含まれているマシンでインストーラーを実行します。

> **注:**
>
> Web Studioをアップグレードした後、バージョン情報がすぐに更新されない場合があります。Web Studioがすでに最新の状態であっても、アップグレードを促されることがありま

す。この問題に対処するには、Web Studioサーバーに移動し、Internet Information Services (IIS) マネージャーを開き、 > > に移動して、 ペインで を選択します。

ステップ8：Studioの再起動

アップグレードされた Web Studio を再起動します。アップグレードプロセスが自動的に再開されます。

ステップ9：データベースとサイトのアップグレード

注:

障害を避けるため、新しいマシンカタログの作成、マシンカタログの削除、デリバリーグループ内のマシンの更新など、プロビジョニングおよびデリバリーグループ関連のタスクを実行する前に、すべてのDelivery Controllerとデータベースをアップグレードする必要があります。

SQL Serverデータベースのスキーマを更新するために必要な権限については、準備を確認してください。

- SQL Serverデータベーススキーマを更新する十分な権限がある場合は、自動データベースアップグレードを開始できます。データベースとサイトを自動的にアップグレードするに進んでください。
- データベースの十分な権限がない場合は、スクリプトを使用する手動アップグレードを開始し、データベース管理者（必要な権限を持つ人）の助けを借りて進めることができます。手動アップグレードの場合、Studioユーザーがスクリプトを生成し、サービスを有効/無効にするスクリプトを実行します。データベース管理者は、SQLCMDユーティリティまたはSQLCMDモードのSQL Server Management Studioを使用して、データベーススキーマを更新する他のスクリプトを実行します。データベースとサイトを手動でアップグレードするに進んでください。
- マルチゾーン展開でデータベースとサイトを自動的にアップグレードする場合、Citrixは、dbschemaのアップグレードを、サイトのSQL Serverデータベースをホストするのと同じゾーンで実行することを推奨します。そうしないと、データベースとサイトの自動アップグレードが失敗する可能性があります。

Citrixは、アップグレード前にデータベースをバックアップすることを強く推奨します。CTX135207を参照してください。データベースのアップグレード中は、製品サービスが無効にな

ります。その間、Controllerはサイトの新しい接続を仲介できないため、慎重に計画してください。

データベースとサイトを自動的にアップグレードする

1. 新しくアップグレードされたStudioを起動します。
2. サイトのアップグレードを自動的に開始することを示し、準備ができたことを確認します。

データベースとサイトのアップグレードが進行します。

データベースとサイトを手動でアップグレードする

1. 新しくアップグレードされたStudioを起動します。
2. サイトを手動でアップグレードすることを示します。ウィザードはライセンスサーバーの互換性を確認し、確認を求めます。
3. データベースをバックアップしたことを確認します。

   ウィザードは、スクリプトとアップグレード手順のチェックリストを生成して表示します。アップグレード対象の製品バージョン以降、データベースのスキーマが変更されていない場合、そのスクリプトは生成されません。たとえば、ログデータベースのスキーマが変更されない場合、`UpgradeLoggingDatabase.sql`スクリプトは生成されません。
4. 以下のスクリプトを記載されている順序で実行します。

   - `DisableServices.ps1`: Studioユーザーは、製品サービスを無効にするために、このPowerShellスクリプトをControllerで実行します。
   - `UpgradeSiteDatabase.sql`: データベース管理者は、サイトデータベースを含むサーバーでこのSQLスクリプトを実行します。
   - `UpgradeMonitorDatabase.sql`: データベース管理者は、モニターデータベースを含むサーバーでこのSQLスクリプトを実行します。
   - `UpgradeLoggingDatabase.sql`: データベース管理者は、構成ログデータベースを含むサーバーでこのSQLスクリプトを実行します。このスクリプトは、このデータベースが変更された場合（たとえば、ホットフィックスを適用した後など）にのみ実行します。
   - `EnableServices.ps1`: Studioユーザーは、製品サービスを有効にするために、このPowerShellスクリプトをControllerで実行します。

   データベースのアップグレードが完了し、製品サービスが有効になると、Studioは環境と構成を自動的にテストし、HTMLレポートを生成します。問題が特定された場合は、データベースのバックアップを復元できます。問題を解決した後、データベースを再度アップグレードできます。

5. チェックリストのタスクを完了したら、**Finish upgrade**をクリックします。

ステップ 10: 残りのDelivery Controllerをアップグレードする

新しくアップグレードされたStudioから、ナビゲーションペインで**Citrix Studio** *サイト名*を選択します。**共通タスク**タブで、**残りのDelivery Controllerをアップグレード**を選択します。

> **注：**
>
> **残りのDelivery Controllerをアップグレード**を利用可能にするには、サイト用に少なくとも1つのマシンカタログと1つのデリバリーグループを作成します。

> アップグレードが完了し、完了を確認したら、Studioを閉じてから再度開きます。Studioは、Controllerのサービスをサイトに登録するため、またはゾーンIDが存在しない場合にゾーンIDを作成するために、追加のサイトアップグレードを促すことがあります。

ステップ 11: VDAをアップグレードする

> **重要：**
>
> VDAをバージョン1912以降にアップグレードする場合は、「VDAを1912以降にアップグレードする」を参照してください。

> VDAを含むマシンで製品インストーラーを実行します。

Machine Creation Services™とマスターイメージを使用してマシンを作成した場合、ホストに移動し、マスターイメージ上のVDAをアップグレードします。利用可能なVDAインストーラーのいずれかを使用できます。

- グラフィックインターフェイスのガイダンスについては、「VDAのインストール」を参照してください。
- コマンドラインのガイダンスについては、「コマンドラインを使用したインストール」を参照してください。

Citrix Provisioningを使用してマシンを作成した場合は、アップグレードに関するガイダンスについて「Citrix Provisioning製品ドキュメント」を参照してください。

ステップ 12: マシンカタログとデリバリーグループを更新する

- アップグレードされたVDAを使用するマシンでカタログを更新する。
- VDAがアップグレードされたマシンを使用するカタログをアップグレードする(/ja-jp/citrix-virtual-apps-desktops/2503/install-configure/machine-catalogs-manage.html#upgrade-a-catalog-or-revert-an-upgrade)。
- VDAがアップグレードされたマシンを使用するデリバリーグループをアップグレードする(/ja-jp/citrix-virtual-apps-desktops/2503/install-configure/delivery-groups-manage.html#upgrade-a-delivery-group-or-revert-an-upgrade)。

ステップ13：アップグレード後

展開環境の他のコンポーネントをアップグレードします。ガイダンスについては、以下の製品ドキュメントを参照してください。

- StoreFront(/ja-jp/storefront/current-release/install-standard.html#upgrade-storefront)
- AppDNA(/ja-jp/dna/current-release/upgrade.html)
- シトリックス アプリケーション レイヤリング
- HDX リアルタイム最適化パック
- プロファイル管理
- シトリックス プロビジョニング
- セッション録画
- ワークスペース環境管理

Microsoft SQL Server Express LocalDBソフトウェアを以降のバージョンに交換する必要がある場合は、「SQL Server Express LocalDBの交換」を参照してください(#replace-sql-server-express-localdb)。

データベーススキーマのアップグレード

展開環境を更新すると、複数のデータベーススキーマをアップグレードできます。次の表に、そのプロセスでアップグレードされるデータベーススキーマを示します。

From\To	1912 CU1	1912 CU2	1912 CU3	1912 CU4	1912 CU5	2203
7.15 RTM or 7.15 CU releases	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config; Logging
1912 RTM	Config	Site, Config	Site, Config	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config; Logging
1912 CU1		Site	Site, Config	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config; Logging
1912 CU2			Site, Config	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config; Logging
1912 CU3				Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config; Logging
1912 CU4					Site, Config	Site; Monitor; Config; Logging
1912 CU5						Site; Monitor; Config; Logging
2112						Site; Monitor; Config

用語の定義:

- サイト: サイトデータストア。Dbschemaの更新はサイトデータストアに対して行われます。
- モニター: モニターデータストア。Dbschemaの更新はモニターデータストアに対して行われます。
- 構成: 構成テーブル。構成テーブルでは、Desktop Studioのバージョン、ライセンス情報、またはその両方が更新されます。
- ロギング: ロギングデータストア。Dbschemaの更新はロギングデータストアに対して行われます。

VDAを2203以降にアップグレードする

Personal vDisk (PvD) コンポーネントがVDAにインストールされていた場合、そのVDAはバージョン2203以降にアップグレードできません。新しいVDAを使用するには、現在のVDAをアンインストールしてから、新しいVDAをインストールする必要があります。

この指示は、PvDを一度も使用したことがない場合でも適用されます。

以前のバージョンでPvDコンポーネントがインストールされた可能性のある方法は次のとおりです。

- VDA インストーラーのグラフィカルインターフェイスでは、PvD は **追加コンポーネント** ページでオプションでした。
- コマンドラインでは、`/baseimage` オプションで PvD がインストールされました。このオプションを指定した場合、またはこのオプションを含むスクリプトを使用した場合は、PvD がインストールされました。

VDAにPvDがインストールされているかどうかわからない場合は、マシンまたはイメージで新しいVDA（2203以降）のインストーラーを実行してください。

- PvD がインストールされている場合、互換性のないコンポーネントがあることを示すメッセージが表示されます。
  - グラフィカルインターフェイスから、メッセージを含むページで **キャンセル** をクリックし、インストーラーを閉じたいことを確認します。
  - CLIから、コマンドは表示されたメッセージとともに失敗します。
- PvDがインストールされていない場合、アップグレードは続行されます。

実行手順

VDAにPvDがインストールされていない場合は、通常のアップグレード手順に従ってください。

VDAにPvDがインストールされている場合：

1. 現在のVDAをアンインストールします。
2. 新しいVDAをインストールします。

Windows 10 (1607以前、更新なし) マシンでPvDの使用を継続したい場合は、VDA 7.15 LTSRがサポートされる最新バージョンです。

> **注:**
>
> *XenAppおよびXenDesktop 7.15 LTSRで、Windows 7デスクトップとPersonal vDiskを使用できますか？*
>
> Citrixは、2016年1月に発表されたXenAppおよびXenDesktop 7.6 LTSRからPersonal vDisk (PvD) を除外しました。さらに、CitrixはPvDテクノロジーの非推奨を発表し、今後Citrix App Layeringの使用を開始することを顧客に推奨しています。Citrix App Layering (バージョン4.4以降) は、XenAppおよびXenDesktop 7.15 LTSRの互換性のあるコンポーネントです。ただし、Windows 7で既存のPvD展開を使用している顧客がCitrix App Layeringテクノロジーに移行するのを支援するため、Citrixは、XenAppおよびXenDesktop 7.15 LTSR Cumulative Updates (CUs) を通じて、Windows 7デスクトップ向けPvD展開の期間限定サポートをJan 14, 2020まで提供することを決定しました。PvDコンポーネントは、LTSR CUsから削除され、Jan 14, 2020以降はサポートされなくなります。また、Jan 14, 2020以降にWindows 7でPvDを使用すると、LTSRサイトは非準拠になります。また、Windows 10向けPvDは7.15 LTSRから引き続き除外されます。したがって、顧客は7.15 LTSRサイトでこれを使用しないでください。

PvD、AppDisks、およびサポートされていないホストを削除する

以下のテクノロジーとホストタイプは、Citrix Virtual Apps and Desktops 7 Current Releaseの展開ではサポートされていません。

- カタログ内のユーザーのVMの隣にデータを保存するための**Personal vDisks (PvD)**。ユーザーパーソナライゼーションレイヤー機能がユーザーの永続性を処理するようになりました。
- デリバリーグループで使用されるアプリケーションを管理するための**AppDisks**。
- **ホストタイプ:** Azure Classic、CloudPlatform (元のCitrix製品)。
    - このリリースでサポートされているホストタイプについては、システム要件を参照してください。

- ARMおよびAWSを継続して使用できる代替方法については、CTX270373を参照してください。

現在の展開でPvDまたはAppDiskを使用している場合、あるいはサポートされていないホストの種類（Microsoft Azure Classicなど）への接続がある場合は、それらのテクノロジを使用する項目を削除した後にのみ、バージョン2006（またはそれ以降のサポートされているバージョン）にアップグレードできます。現在の展開でパブリッククラウドホスト接続（AWSなど）を使用している場合は、アップグレードする前にハイブリッド権限ライセンスがあることを確認してください。インストーラーがサポートされていないテクノロジまたはハイブリッド権限ライセンスのないホスト接続を1つ以上検出すると、アップグレードは一時停止または停止し、説明メッセージが表示されます。インストーラーログには詳細が含まれています。

アップグレードを確実に成功させるには、サポートされていない項目を削除するための該当するガイダンスを確認し、それに従ってください。

- PvDの削除
- AppDiskの削除
- サポートされていないホスト項目の削除

展開でPvDまたはAppDiskを使用していなかった場合でも、関連するMSIが以前のVDAインストールまたはアップグレードに含まれていた可能性があります。VDAをバージョン2006（またはそれ以降のサポートされているバージョン）にアップグレードする前に、たとえ一度も使用していなくても、そのソフトウェアを削除する必要があります。グラフィカルインターフェイスを使用する場合、その削除は自動的に行われるか、CLIを使用する際に削除オプションを含めることができます。詳細については、PvDまたはAppDiskコンポーネントを持つVDAのアップグレードを参照してください。

PvDの削除

PvDを使用するように構成されているすべてのマシンを削除するまで、展開のアップグレードは成功しません。これはカタログとデリバリーグループに影響します。

グループとカタログからPvDを削除するには：

1. Studioで、デリバリーグループにPvDを使用するカタログのマシンが含まれている場合、「それらのマシンをグループから削除」(/ja-jp/citrix-virtual-apps-desktops/2503/install-configure/delivery-groups-manage.html#remove-a-machine-from-a-delivery-group)します。
2. Studioで、PvDを使用するマシンを含む「すべてのカタログを削除」(/ja-jp/citrix-virtual-apps-desktops/2503/install-configure/machine-catalogs-manage.html#delete-a-catalog)します。

VDAのアップグレード： 展開のアップグレードでは、VDAにAppDiskまたはPvDコンポーネントがインストールされているかどうかは検出されません。ただし、VDAインストーラーは検出します。詳細については、「PvDまたはAppDiskコンポーネントを持つVDA」(#vdas-that-have-pvd-or-appdisks-components)を参照してください。

PvDの代わりにApp Layeringを使用する予定がある場合は、データの移行に関する情報についてPvDからApp Layeringへの移行を参照してください。

AppDiskを削除する

AppDiskを使用するすべてのデリバリーグループからAppDiskを削除し、その後AppDisk自体を削除するまで、展開のアップグレードは続行できません。

1. Studioナビゲーションペインで**デリバリーグループ**を選択します。
2. グループを選択し、アクションペインで**AppDiskの管理**をクリックします。
3. グループからAppDiskを削除するアクションをクリックします。
4. AppDiskを使用する各デリバリーグループに対して、手順2と3を繰り返します。
5. Studioナビゲーションペインで**AppDisk**を選択します。
6. AppDiskを選択し、AppDiskを削除するアクションをクリックします。
7. 各AppDiskについて、手順5と6を繰り返します。

VDAのアップグレード: 展開のアップグレードでは、VDAにAppDiskまたはPvDコンポーネントがインストールされているかどうかは検出されません。ただし、VDAインストーラーは検出します。詳細については、PvDまたはAppDiskコンポーネントを持つVDAを参照してください。

サポートされていないホストアイテムを削除する

サイトがサポートされていないホストタイプ（Citrix CloudPlatformやMicrosoft Azure Classicなど）への接続を持っている場合、バージョン2006（またはそれ以降のサポートされているバージョン）への展開のアップグレードは続行できません。アップグレードを試みる前に、以下のタスクを完了してください。

Studioから：

- サポートされていないホストへのすべての接続を削除。
- サポートされていないホストのマスターイメージで作成されたカタログのマシンがデリバリーグループに含まれている場合、それらのマシンをグループから削除します。
- サポートされていないホストのマスターイメージを使用して作成されたすべてのカタログを削除します。

PvDまたはAppDisksコンポーネントがインストールされているVDA

PvDおよびAppDisksテクノロジを有効にするコンポーネントがVDAにインストールされている場合、それらのコンポーネントが削除されるまで、そのVDAをアップグレードすることはできません。

> **注:**
>
> バージョン1912にアップグレードする場合、現在のVDAをアンインストールしてから新しいVDAをインストールする必要がありました。このバージョンでは、Citrixがコンポーネントを削除してアップグレードを続行するかどうかを尋ねられます。

> AppDiskおよびPvDコンポーネントは、それらのテクノロジを一度も使用したことがない場合でも、以前のVDAバージョンでインストールされていた可能性があります。

- グラフィカルインターフェイス：VDAインストーラーの**追加コンポーネント**ページには、**Citrix AppDisk / Personal vDisk**オプションが含まれていました。7.15 LTSRおよびそれ以前の7.xリリースでは、このオプションがデフォルトで有効になっていました。したがって、デフォルトを受け入れた場合（または、このオプションが提供されたリリースで明示的に有効にした場合）、そのコンポーネントがインストールされました。
- CLI: `/baseimage`オプションを指定すると、コンポーネントがインストールされました。

対処法

VDAインストーラーが現在インストールされているVDAでAppDisksまたはPvDコンポーネントを検出しない場合、アップグレードは通常どおり続行されます。

インストーラーが現在インストールされているVDAでAppDisksまたはPvDコンポーネントを検出した場合：

- グラフィカルインターフェイス：アップグレードが一時停止します。サポートされていないコンポーネントを自動的に削除するかどうかを尋ねるメッセージが表示されます。**OK**をクリックすると、コンポーネントが自動的に削除され、アップグレードが続行されます。
- CLI：コマンドの失敗を避けるため、コマンドに次のオプションを含めます。
  - `/remove_appdisk_ack`
  - `/remove_pvd_ack`

制限事項

アップグレードには、次の制限事項が適用されます。

- **選択的なコンポーネントのインストール：** 新しいバージョンにコンポーネントをインストールまたはアップグレードしても、アップグレードが必要な他のコンポーネント（別のマシン上）をアップグレードしない場合、Studioから通知されます。たとえば、アップグレードにControllerとStudioの新しいバージョンが含まれているとします。Controllerをアップグレードしても、Studioがインストールされているマシンでインストーラーを実行しない場合、Studioをアップグレードするまで、Studioはサイトの管理を続行できません。

  VDAをアップグレードする必要はありませんが、Citrixでは、利用可能なすべての機能を使用できるように、すべてのVDAをアップグレードすることをお勧めします。
- **早期リリースまたはテクノロジープレビューバージョン：** 早期リリース、テクノロジープレビュー、またはプレビューバージョンからアップグレードすることはできません。
- **以前のオペレーティングシステム上のコンポーネント：** MicrosoftまたはCitrixによってサポートされなくなったオペレーティングシステムに、現在のVDAをインストールすることはできません。詳しくは、「以前のオペレーティングシステム」を参照してください。
- **混在環境/サイト：** 以前のバージョンのサイトと現在のバージョンのサイトを継続して実行する必要がある場合は、「混在環境に関する考慮事項」を参照してください。
- **製品の選択：** 以前のバージョンからアップグレードする場合、インストール時に設定された製品（Citrix Virtual AppsまたはCitrix Virtual Apps and Desktops）を選択または指定することはありません。

混在環境に関する考慮事項

アップグレード時には、エディションとバージョンに含まれるすべての新規機能および拡張機能にアクセスできるように、すべてのコンポーネントとVDAをアップグレードすることをお勧めします。

たとえば、以前のControllerバージョンを含む展開で現在のVDAを使用することはできますが、現在のリリースに含まれる新機能は利用できない場合があります。また、最新ではないバージョンを使用している場合、VDA登録の問題が発生する可能性があります。

環境によっては、すべてのVDAを最新バージョンにアップグレードできない場合があります。その場合、マシンカタログを作成するときに、マシンにインストールされているVDAバージョンを指定できます。（これは機能レベルと呼ばれます。）デフォルトでは、この設定は推奨される最小VDAバージョンを指定します。ほとんどの展開では、デフォルト値で十分です。カタログにデフォ

ルトよりも古いVDAが含まれている場合にのみ、設定を以前のバージョンに変更することを検討してください。マシンカタログでVDAバージョンを混在させることは推奨されません。

カタログがデフォルトの最小VDAバージョン設定で作成され、1つ以上のマシンがデフォルトバージョンよりも古いVDAを持っている場合、それらのマシンはControllerに登録できず、機能しません。

詳しくは、「VDAバージョンと機能レベル」を参照してください。

異なるバージョンを持つ複数のサイト

環境に異なる製品バージョンのサイト（例：XenDesktop 7.18サイトとCitrix Virtual Apps and Desktops 1909サイト）が含まれる場合、CitrixはStoreFrontを使用して異なる製品バージョンからのアプリケーションとデスクトップを集約することを推奨します。詳細については、StoreFrontのドキュメントを参照してください。

混在環境では、各リリースに対応するStudioおよびDirectorのバージョンを引き続き使用しますが、異なるバージョンは別々のマシンにインストールされていることを確認してください。

以前のオペレーティングシステム

サポートされているオペレーティングシステム（OS）バージョンを実行しているマシンに、コンポーネントの以前のバージョンをインストールしたとします。現在、より新しいコンポーネントバージョンを使用したいと考えていますが、そのOSはコンポーネントの現在のバージョンではサポートされていません。

たとえば、Windows Server 2016マシンにサーバーVDAをインストールしたとします。現在、そのVDAを現在のリリースにアップグレードしたいと考えていますが、アップグレード先の現在のリリースではWindows Server 2016はサポートされていません。

許可されていないオペレーティングシステムにコンポーネントをインストールまたはアップグレードしようとすると、「このオペレーティングシステムにはインストールできません」などのエラーメッセージが表示されます。

これらの考慮事項は、Current ReleaseおよびLong Term Service Releaseバージョンのアップグレードに適用されます。（LTSRバージョンにCUを適用することには影響しません。）

サポートされているOSについては、以下のリンクを参照してください。

- Citrix Virtual Apps and Desktops (最新リリース):
  - デリバリーコントローラー、Studio、Director、VDA、ユニバーサルプリントサーバー
  - フェデレーション認証サービス

  - StoreFront、Self-Service Password Reset、およびSession Recordingについては、現在のリリースのシステム要件の記事を参照してください。

- LTSRについては、お使いのLTSRバージョンとCUのコンポーネントリストを参照してください。（メインのCitrix Virtual Apps and Desktops製品ドキュメントページからLTSRバージョンを選択してください。）

無効なオペレーティングシステム

以下の表は、現在のリリースでコンポーネントのインストール/アップグレードに無効な以前のオペレーティングシステムを一覧表示しています。各OSでサポートされている最新の有効なコンポーネントバージョンと、インストールおよびアップグレードが無効になったコンポーネントバージョンを示しています。

表中のオペレーティングシステムにはサービスパックと更新プログラムが含まれます。

オペレーティングシステム	コンポーネント/機能	最新の有効なバージョン	インストール/アップグレードが不可能になったバージョン
Windows 7および Windows 8	VDA	7.15 LTSR	7.16
Windows 7および Windows 8	その他のインストーラーコンポーネント	7.17	7.18
Windows 10 バージョン 1607 より前のもの	VDA	7.15 LTSR	7.16
Windows 10 x86 バージョン	VDA	1906.2.0	1909
Windows サーバー 2008 R2	VDA	7.15 LTSR	7.16
Windows サーバー 2008 R2	その他のインストーラーコンポーネント	7.17	7.18
Windows サーバー 2012	VDA	7.15 LTSR	7.16

オペレーティングシステム	コンポーネント/機能	最新の有効なバージョン	インストール/アップグレードが不可能になったバージョン
Windows サーバー 2012	その他のインストーラーコンポーネント	7.17	7.18
ウィンドウズ サーバー 2012 R2	その他のインストーラーコンポーネント *	1912 LTSR	2003
ウィンドウズ サーバー 2012 R2	サーバーVDI	7.15 LTSR	7.16
Windows サーバー 2016	サーバーVDI	7.15 LTSR	7.16

Windows XP および Windows Vista は、7.x のコンポーネントまたはテクノロジーでは無効です。

※ Delivery Controller、Studio、Director、およびVDAに適用されます。

実行できること

選択肢があります。次のことができます。

- 現在のOSを継続して使用する](#continue-with-the-current-os)
- マシンを再イメージ化またはアップグレードする](#reimage-or-upgrade-the-machine)
- 新しいマシンを追加し、古いマシンを削除する](#add-new-machines-and-then-remove-old-machines)

現在のOSを継続して使用する

これらの方法はVDAで実行可能です。以前のOSを搭載したマシンの使用を継続する場合は、次のいずれかを選択できます。

- インストールされているコンポーネントバージョンを継続して使用する。
- 最新の有効なコンポーネントバージョンをダウンロードし、そのバージョンにコンポーネントをアップグレードする。（これは、最新の有効なコンポーネントバージョンがまだインストールされていないことを前提としています。）

例えば、Windows 7 SP1マシンに7.14 VDAがインストールされているとします。Windows 7 OSマシンで有効な最新のVDAバージョンは、XenApp and XenDesktop 7.15 LTSRです。7.14を使い続けるか、7.15 LTSR VDAをダウンロードしてVDAをそのバージョンにアップグレードすることが

できます。これらの以前のVDAバージョンは、より新しいバージョンのDelivery Controllerを含む展開環境で動作します。例えば、7.15 LTSR VDAはCitrix Virtual Apps and Desktops 7 1808 Controllerに接続できます。

マシンの再イメージ化またはアップグレード

これらの方法は、VDAや、Delivery Controllerなどのコアコンポーネントがインストールされていない他のマシンに適用できます。次のいずれかを選択してください。

- マシンをサービスから外し（メンテナンスモードをオンにしてすべてのセッションを閉じさせてから）、サポートされているWindows OSバージョンに再イメージ化し、コンポーネントの最新バージョンをインストールできます。
- 再イメージ化せずにVDAマシンでOSをアップグレードするには、まずアップグレード先のOSでサポートされているVDAバージョンをインストールするか、OSのアップグレード後にVDAをアップグレードする必要があります。そうしないと、Citrixソフトウェアはサポートされません。VDAをアンインストールせずにインプレースアップグレードを実行する場合、以下の最小OSバージョンにアップグレードできます。
  - 2023-07 Cumulative Update for Windows 11 (KB5028185) 以降がインストールされている Windows 11 (ビルド 22621.1992 以降)。
  - 2023-07 Dynamic Update for Windows 10 (KB5028311) がインストールされている Windows 10。
- アップグレードを計画しているWindowsバージョンが上記のガイドラインに合致しない場合、OSをアップグレードする前にVDAをアンインストールし、OSのアップグレードが完了した後にサポートされているVDAバージョンをインストールする必要があります。

新しいマシンを追加し、古いマシンを削除する

この方法は、Delivery Controller™ またはその他のコアコンポーネントを含むマシンでOSをアップグレードする必要がある場合に実行可能です。

Citrixは、サイト内のすべてのControllerが同じOSを持つことを推奨します。以下のアップグレードシーケンスは、異なるControllerが異なるOSを持つ期間を最小限に抑えます。

1. サイト内のすべてのDelivery Controllerのスナップショットを取得し、サイトデータベースをバックアップします。
2. サポートされているオペレーティングシステムを搭載したクリーンなサーバーに新しいDelivery Controllerをインストールします。
3. 新しいControllerをサイトに追加します。

4. 現在のリリースで無効なオペレーティングシステムで実行されているControllerを削除します。Controllerの削除に関する推奨事項については、「Delivery Controllers」を参照してください。

準備

アップグレードを開始する前に、以下の情報を確認し、必要なタスクを完了してください。

> **注:**
>
> VDAのアップグレードはアップグレードシーケンスの後に行われますが、アップグレードを開始する前にインストーラーを選択し、手順を確認しておくことをお勧めします。これにより、何が予想されるかを知ることができます。

インストーラーとインターフェイスを選択する

コンポーネントをアップグレードするには、製品ISOからフルプロダクトインストーラーを使用します。VDAは、フルプロダクトインストーラーまたはスタンドアロンVDAインストーラーのいずれかを使用してアップグレードできます。すべてのインストーラーは、グラフィカルインターフェイスとコマンドラインインターフェイスを提供します。

詳細については、「インストーラー」を参照してください。

インストールの詳細： 準備作業を完了し、インストーラーを開始する準備ができたら、インストール記事には、表示される内容（グラフィカルインターフェイスを使用している場合）または入力する内容（コマンドラインインターフェイスを使用している場合）が示されています。

- グラフィカルインターフェイスを使用してコアコンポーネントをインストール/アップグレードする
- コマンドラインを使用してコアコンポーネントをインストール/アップグレードする
- グラフィカルインターフェイスを使用してVDAをインストール/アップグレードする
- コマンドラインを使用してVDAをインストール/アップグレードする

`VDAWorkstationCoreSetup.exe`インストーラーでシングルセッションVDAを最初にインストールした場合、Citrixはそのインストーラーを使用してアップグレードすることを推奨します。フルプロダクトVDAインストーラーまたは`VDAWorkstationSetup.exe`インストーラーを使用してVDAをアップグレードすると、アップグレードから明示的に除外しない限り、元々除外されていたコンポーネントがインストールされる可能性があります。

VDAを現在のリリースにアップグレードする際、アップグレードプロセス中にマシンの再起動が発生します（この要件は7.17リリースから始まりました）。これは回避できません。再起動後、アップグレードは自動的に再開されます（コマンドラインで`/noresume`を指定しない限り）。

データベース操作

サイト、監視、および構成ログデータベースをバックアップします。CTX135207の手順に従ってください。アップグレード後に問題が発見された場合、バックアップを復元できます。

サポートされなくなったSQL Serverバージョンのアップグレードについては、SQL Server version checkを参照してください。（これは、サイト、監視、および構成ログデータベースに使用されるSQL Serverを指します。）

Microsoft SQL Server Express LocalDBは、ローカルホストキャッシュで使用するために自動的にインストールされます。以前のバージョンを置き換える必要がある場合、新しいバージョンはSQL Server Express LocalDB 2019である必要があります。コンポーネントとサイトをアップグレードした後にSQL Server Express LocalDBを新しいバージョンに置き換える方法の詳細については、Replace SQL Server Express LocalDBを参照してください。

Citrixライセンスが最新であることを確認する

Citrixライセンスの管理に関する包括的な情報については、Activate, upgrade, and manage Citrix licensesを参照してください。

フル製品インストーラーを使用してライセンスサーバーをアップグレードできます。または、ライセンスコンポーネントを個別にダウンロードしてアップグレードすることもできます。Upgradeを参照してください。

アップグレードする前に、Customer Success Services / Software Maintenance / Subscription Advantageの有効期限が新しい製品バージョンに対応していることを確認してください。日付は2021年11月15日以降である必要があります。

Citrixライセンスサーバーの互換性を確認する

Citrixライセンスサーバーが新しいバージョンと互換性があることを確認してください。これには2つの方法があります。

- 他のCitrixコンポーネントをアップグレードする前に、Delivery Controllerを含むマシンでISOレイアウトから`XenDesktopServerSetup.exe`インストーラーを実行します。互換性の問題がある場合、インストーラーは推奨される解決手順とともにそれを報告します。
- インストールメディアの`XenDesktop Setup`ディレクトリから、コマンド`.\LicServVerify.exe -h <license-server-fqdn> -p 27000 -v`を実行します。表示によ

り、ライセンスサーバーが互換性があるかどうかが示されます。ライセンスサーバーに互換性がない場合は、ライセンスサーバーをアップグレードしてください。

StoreFrontの変更をバックアップする

アップグレードを開始する前に、*default.ica*や*usernamepassword.tfrm*など、`C:\inetpub\wwwroot\Citrix\<StoreName>\App_Data`内のファイルを変更した場合は、各ストアのファイルをバックアップしてください。アップグレード後、それらを復元して変更を元に戻すことができます。

アプリケーションとコンソールを閉じる

アップグレードを開始する前に、管理コンソールやPowerShellセッションなど、ファイルロックを引き起こす可能性のあるすべてのプログラムを閉じます。

マシンを再起動すると、すべてのファイルロックが解除され、保留中のWindowsアップデートがないことが保証されます。

アップグレードを開始する前に、サードパーティの監視エージェントサービスをすべて停止して無効にします。

適切な権限があることを確認する

ドメインユーザーであることに加えて、製品コンポーネントをアップグレードするマシンではローカル管理者である必要があります。

サイトデータベースとサイトは、自動または手動でアップグレードできます。データベースを自動でアップグレードする場合、Studioユーザーの権限には、SQL Serverデータベーススキーマを更新する機能（たとえば、`db_securityadmin`または`db_owner`データベースロール）が含まれている必要があります。詳しくは、データベースを参照してください。

Studioユーザーがこれらの権限を持っていない場合、手動データベースアップグレードを開始すると、スクリプトが生成されます。Studioユーザーは、Studioから一部のスクリプトを実行します。データベース管理者は、SQL Server Management Studioなどのツールを使用して、他のスクリプトを実行します。

その他の準備タスク

- 必要に応じて、テンプレートをバックアップし、ハイパーバイザーをアップグレードする
- 事業継続計画で定められたその他の準備タスクを完了する。

サイトの事前テスト

Delivery Controllerとサイトをアップグレードする場合、実際のアップグレードが開始される前にサイトの事前テストが実行されます。これらのテストでは、以下を確認します。

- サイトデータベースに到達可能であり、バックアップされていること
- 重要なCitrixサービスへの接続が正しく機能していること
- Citrixライセンスサーバーのアドレスが利用可能であること
- 構成ログデータベースに到達できること
- パブリッククラウドホスト接続（例：AWS）を追加する場合は、Hybrid Rights Licenseがあることを確認してください。そうでない場合、予備サイトテストは一時停止または停止し、説明メッセージが表示されます。

テストの実行後、結果のレポートを表示できます。検出された問題を修正し、テストを再度実行できます。予備サイトテストを実行せず、問題を解決しないと、サイトの動作に影響を与える可能性があります。

テスト結果を含むレポートは、インストールログと同じディレクトリにあるHTMLファイル（`PreliminarySiteTestResult.html`）です。このファイルは、存在しない場合に作成されます。ファイルが存在する場合、その内容は上書きされます。

テストを実行する

- インストーラーのグラフィカルインターフェイスを使用してアップグレードする場合、ウィザードにはテストを開始してレポートを表示できるページが含まれています。テストが実行され、レポートを確認し、見つかった問題を解決した後、テストを再実行できます。テストが正常に完了したら、 をクリックしてウィザードを続行します。
- コマンドラインインターフェイスを使用してアップグレードする場合、テストは自動的に実行されます。デフォルトでは、テストが失敗した場合、アップグレードは実行されません。レポートを確認し、問題を解決した後、コマンドを再実行してください。

Citrixは、Controllerとサイトのアップグレードを続行する前に、常に予備サイトテストを実行し、問題を解決することを推奨しています。テストを実行するのにかかるわずかな時間で得られる潜在的なメリットは十分にあります。ただし、この推奨されるアクションを上書きすることもできます。

- グラフィカルインターフェイスでアップグレードする場合、テストをスキップしてアップグレードを続行することを選択できます。
- コマンドラインからアップグレードする場合、テストをスキップすることはできません。デフォルトでは、サイトテストが失敗すると、アップグレードを実行せずにインストーラーが失

敗します。通常、`/ignore_site_test_failure` オプションを含めると、テストの失敗は無視され、アップグレードが続行されます。（例外については、SQL Serverのバージョンチェック を参照してください。）

複数のControllerをアップグレードする場合

1つのControllerでアップグレードを開始し、同じサイト内の別のControllerでアップグレードを開始する場合（最初のアップグレードが完了する前）：

- 最初のControllerで予備サイトテストが完了している場合、他のControllerのウィザードには予備サイトテストページは表示されません。
- 他のControllerでアップグレードを開始したときに最初のControllerでのテストが進行中の場合、他のControllerのウィザードにサイトテストページが表示されます。ただし、最初のControllerでのテストが完了すると、最初のControllerからのテスト結果のみが保持されます。

サイトの健全性に関連しないテストの失敗

- 予備サイトテストがメモリ不足で失敗した場合は、より多くのメモリを確保してからテストを再実行してください。
- アップグレードの権限はあるがサイトテストを実行する権限がない場合、予備サイトテストは失敗します。これを解決するには、テストを実行する権限を持つユーザーアカウントでインストーラーを再実行してください。

SQL Serverバージョンの確認

Citrix Virtual Apps and Desktopsの展開を成功させるには、サイト、モニター、および構成ログデータベースにサポートされているバージョンのMicrosoft SQL Serverが必要です。サポートされなくなったSQL ServerバージョンでCitrix展開をアップグレードすると、機能上の問題が発生し、サイトはサポート対象外となります。

アップグレード先のCitrixリリースでサポートされているSQL Serverのバージョンについては、そのリリースのシステム要件の記事を参照してください。

Controllerをアップグレードする際、Citrixインストーラーは、サイト、モニター、および構成ログデータベースに使用されている現在インストールされているSQL Serverのバージョンをチェックします。

- チェックの結果、現在インストールされているSQL Serverのバージョンが、アップグレード先のCitrixリリースでサポートされているバージョンではないと判断された場合：

  - グラフィカルインターフェイス：アップグレードはメッセージとともに停止します。「**I understand**」をクリックし、次に「**Cancel**」をクリックしてCitrixインストーラーを閉じます。（アップグレードを続行することはできません。）
  - コマンドラインインターフェイス：コマンドは失敗します（コマンドに`/ignore_db_check_failure`オプションを含めた場合でも）。

  SQL Serverのバージョンをアップグレードしてから、Citrixのアップグレードを再度開始してください。
- チェックで現在インストールされているSQL Serverのバージョンを特定できない場合は、現在インストールされているバージョンがアップグレード先のバージョンでサポートされているか（システム要件）を確認してください。
  - グラフィカルインターフェイス: アップグレードがメッセージとともに停止します。
    - 現在インストールされているSQL Serverのバージョンがサポートされている場合は、「**I understand**」をクリックしてメッセージを閉じ、次に「**Next**」をクリックしてCitrixのアップグレードを続行します。
    - 現在インストールされているSQL Serverのバージョンがサポートされていない場合は、「**I understand**」をクリックしてメッセージを閉じ、次に「**Cancel**」をクリックしてCitrixのアップグレードを終了します。SQL Serverをサポートされているバージョンにアップグレードしてから、Citrixのアップグレードを再度開始してください。
  - コマンドラインインターフェイス: コマンドがメッセージとともに失敗します。メッセージを閉じた後:
    - 現在インストールされているSQL Serverのバージョンがサポートされている場合は、`/ignore_db_check_failure`オプションを指定してコマンドを再度実行します。
    - 現在インストールされているSQL Serverのバージョンがサポートされていない場合は、SQL Serverをサポートされているバージョンにアップグレードします。コマンドを再度実行してCitrixのアップグレードを開始します。

SQL Serverのアップグレード

新しいSQL Serverサーバーを立ち上げてサイトデータベースを移行する場合、接続文字列を更新する必要があります。

サイトが現在、サイトデータベースにSQL Server Expressを使用している場合 (Citrixがサイト作成時に自動的にインストールしたもの):

1. 最新のSQL Server Expressバージョンをインストールします。

2. データベースをデタッチします。
3. データベースを新しいSQL Server Expressにアタッチします。
4. 接続文字列を移行します。

詳細については、接続文字列の構成およびMicrosoft SQL Serverの製品ドキュメントを参照してください。

SQL Server Express LocalDBの置き換え

Microsoft SQL Server Express LocalDB は、Local Host Cache がスタンドアロンで使用する SQL Server Express の機能です。Local Host Cache は、SQL Server Express LocalDB 以外の SQL Server Express のコンポーネントを必要としません。

Citrix は SQL Server Express LocalDB を自動的に更新しません。SQL Server Express LocalDB のバージョンを更新するには、このセクションのガイダンスに従ってください。

- Delivery Controller を Citrix Virtual Apps and Desktops バージョン 2203 LTSR 以降のバージョンにアップグレードする場合、サポートされるバージョンは SQL Server Express LocalDB 2019 または SQL Server Express LocalDB 2022 です。

必要なもの:

- Citrix Virtual Apps and Desktops インストールメディア。
- Windows Sysinternals ツールボックスのPsExecツール。

手順:

1. Citrix Virtual Apps and Desktopsのコンポーネント、データベース、およびサイトのアップグレードを完了します。(これらのデータベースアップグレードは、サイト、監視、および構成ログデータベースに影響します。SQL Server Express LocalDBを使用するローカルホストキャッシュデータベースには影響しません。)
2. SQL Server Express LocalDBを更新するDelivery Controllerにログオンします。
3. MicrosoftからPsExecをダウンロードし、そのDelivery Controller上のアクセスしやすい場所 (例: C:\Temp) に配置します。
4. Windowsシステムサービスから、Delivery Controller上のCitrix High Availability Serviceを停止します。
5. Delivery Controllerでコマンドプロンプトを開き、PsExecがある場所 (例: `C:\Temp`) に移動し、次のコマンドを実行してNetwork Serviceアカウントでコマンドプロンプトを昇格させます。

```
psexec -i -u "NT AUTHORITY\NETWORKSERVICE" cmd
```

6. `whoami`を実行して、コマンドプロンプトがNetwork Serviceアカウントとして実行されていることを確認します。次の出力が表示されるはずです: `nt authority\networkservice`。
7. コマンドプロンプトを使用してSQL LocalDBインスタンスに移動します。
   - SQL LocalDB 2014からアップグレードする場合:

     ```
     cd "C:\Program Files\Microsoft SQL Server\120\Tools\Binn"
     ```

   - SQL LocalDB 2017からアップグレードする場合:

     ```
     cd "C:\Program Files\Microsoft SQL Server\140\Tools\Binn"
     ```

   - SQL LocalDB 2019からアップグレードする場合:

     ```
     cd "C:\Program Files\Microsoft SQL Server\150\Tools\Binn"
     ```

8. SQL LocalDBインスタンスを停止して削除します: `CitrixHA`。

```
SqlLocalDB stop CitrixHA



SqlLocalDB delete CitrixHA
```

9. Delivery Controllerから次のファイルを削除します。

```
C:\Windows\ServiceProfiles\NetworkService\HADatabaseName.*

C:\Windows\ServiceProfiles\NetworkService\HADatabaseName_log.*

C:\Windows\ServiceProfiles\NetworkService\HAImportDatabaseName.* (if
exists)

C:\Windows\ServiceProfiles\NetworkService\HAImportDatabaseName_log.*
(if exists)
```

10. 既存のSQL LocalDB SQL Server Expressを、プログラムを削除するためのWindowsネイティブ機能を使用して、Delivery Controllerからアンインストールします。
11. アンインストールが完了したら、Delivery Controllerを再起動します。
12. Windowsシステムサービスから、Delivery Controller上のCitrix High Availability Serviceを停止します。
13. Citrix Virtual Apps and Desktopsのインストールメディアを Delivery Controllerにマウントします。
14. Delivery ControllerにSQL Server Express LocalDB 2022を管理者としてインストールします。

    a. Citrix Virtual Apps and Desktopsインストールメディアの `Support > SQLLocalDB` フォルダーにある `sqllocaldb.msi` ファイルを使用します。たとえば、インストールメディアが `E drive` ドライブにマウントされている場合、ファイルは `E:\Support\SQLLocalDB\sqllocaldb.msi` にあります。インストールを完了するには再起動が必要です。

    b. 新しいSQL LocalDBは `C:\Program Files\Microsoft SQL Server\160\Tools\Binn` にある必要があります。

15. Windowsシステムサービスから、Delivery Controller上のCitrix High Availability Serviceを開始します。
16. Delivery Controllerのコマンドプロンプトで、 `C:\Program Files\Microsoft SQL Server\160\Tools\Binn` に移動し、 `SqlLocalDB i` を実行してCitrixHAインスタンスが作成されたことを確認します。返されたインスタンスのリストに `CitrixHA` が含まれている必要があります。

    > **注:**
    >
    > Citrix High Availability Serviceの開始後、CitrixHAデータベースが作成されるまでに最大15分かかる場合があります。

17. 必要に応じてHigh Availability Service（セカンダリブローカー）が引き継ぐことができることを確認するために、ローカルホストキャッシュデータベースファイルが作成されていることを確認します。

    a. Delivery Controllerで、 `C:\Windows\ServiceProfiles\NetworkService` を参照します。

    b. `HaDatabaseName.mdf` と `HaDatabaseName_log.ldf` が作成されていることを確認します。

18. 残りのDelivery Controllerで手順を繰り返します。

セキュリティ

FIDO2 および WebAuthn 認証

FIDO2 および WebAuthn を使用したローカル認証と仮想認証

ユーザーは、FIDO2 セキュリティキーと、TPM 2.0 および Windows Hello を搭載した統合生体認証デバイスを使用して、仮想セッションで FIDO2 または WebAuthn を利用するアプリケーションに認証できます。

FIDO2 の詳細については、「FIDO2: WebAuthn & CTAP」を参照してください。

この機能の使用方法については、「FIDO2 リダイレクト」を参照してください。

> **注**
>
> この機能は、WebAuthnまたはFIDO2を使用した仮想セッションへのログオンをサポートしていません。この機能は、仮想セッション内のアプリケーションでこれらの認証方法を使用することのみを許可します。

サポートマトリックス

セッションホストオペレーティングシステム	WEB アプリケーション認証	UWP アプリケーション認証
ウィンドウズ サーバー 2016	USB リダイレクト経由でサポート	サポートされていません
ウィンドウズ サーバー 2019	対応	未対応
ウィンドウズ サーバー 2022	対応	対応
ウィンドウズ 10	対応	対応
ウィンドウズ 11	対応	対応

詳細については、以下の要件を確認してください。

Webアプリケーション認証

要件

WebアプリケーションでFIDO2およびWebAuthn認証を使用するための要件は次のとおりです。

Citrix® コントロールプレーン

- シトリックス バーチャル アプリケーションズ アンド デスクトップ™ 2009以降

セッションホスト

- オペレーティングシステム
  - Windows 10 1809 以降
  - Windows Server 2019 以降のバージョン
- VDA
  - Windows: バージョン2009以降

クライアントデバイス

- オペレーティングシステム
  - Windows 10 1809 以降
  - Linux: Workspace app for Linux の システム要件 を参照してください
- ワークスペース アプリ
  - Windows: バージョン 2009.1 以降
  - Linux: 2303 以降

Webブラウザーの要件

- 32ビットおよび64ビットブラウザ

サポートされる認証方法

- FIDO2セキュリティキー
- ウィンドウズ ハロー
  - TPM 2.0
  - 統合生体認証

    - 顔認証
    - 指紋スキャナー
  - WebAuthn

UWPアプリケーション認証

Citrix Virtual Apps and Desktops 2112のリリースにより、CitrixはUWPアプリケーションでのWebAuthnおよびFIDO2認証をサポートします。

Microsoft Teams、Microsoft Outlook for Office 365、OneDriveなどのアプリケーションは、Azure Active Directoryへのリンクとして UWPアプリケーションを認証に使用します。Citrixは、これらのアプリケーションを認証するためにFIDO2を使用することをサポートするようになりました。

要件

UWPアプリケーションでFIDO2およびWebAuthn認証を使用するための要件は次のとおりです。

Citrixコントロールプレーン

- Citrix Virtual Apps and Desktops のバージョン 2112 以降

セッションホスト

- オペレーティングシステム
  - Windows 10 1809以降
  - Windows 11 オペレーティングシステム
  - ウィンドウズサーバー 2022 以降
- VDA
  - Windows: バージョン2112以降

クライアントデバイス

- オペレーティングシステム
  - Windows 10 1809 以降
  - ウィンドウズ 11
  - Linux: Workspace app for Linuxのシステム要件を参照してください。
- Workspaceアプリ
  - Windows: バージョン2009.1以降

- Linux: 2303以降

UWPアプリケーションの要件

- 32 ビットおよび 64 ビットアプリケーション

サポートされる認証方法

- FIDO2セキュリティキー
- ウィンドウズ ハロー
  - TPM 2.0
  - 統合生体認証
    - 顔認識
    - 指紋スキャナー
  - WebAuthn

> **注:**
>
> 上記の認証方法のサポートは、基盤となるオペレーティングシステムの機能によって異なります。

> クライアント、VDA、またはオペレーティングシステムがこの機能をサポートしていないため、FIDO2リダイレクトが利用できないシナリオでは、USBベースのFIDO2キーをUSBリダイレクトを使用してリダイレクトできます。 FIDO2リダイレクトが利用可能なシナリオでも、USBリダイレクトを使用してUSBベースのFIDO2キーをリダイレクトすることが可能です。この場合、FIDO2リダイレクトを無効にし、適切なUSBリダイレクトルールを設定する必要があります。 USBリダイレクトルールを使用してFIDO2キーを設定する方法の詳細については、USBリダイレクトデバイスルールのドキュメントを参照してください。

msedgewebview2.exeベースのアプリケーションの詳細設定

> **注：**
>
> レジストリを誤って編集すると、オペレーティングシステムの再インストールが必要になるような深刻な問題が発生する可能性があります。Citrixは、レジストリエディターの誤った使

> 用によって生じる問題が解決されることを保証できません。 レジストリエディターは自己責任で使用してください。編集する前に必ずレジストリをバックアップしてください。

> msedgewebview2.exeベースのWebアプリケーションを使用する企業の場合、HDXセッション内でFIDO2リダイレクトが機能するように、VDAに追加のレジストリ値を追加する必要があります。

AllowProcessesレジストリ値にmsedgewebview2.exeのフルパスを追加します。

- キー: HKLM\SOFTWARE\Citrix\WebAuthnAllowedProcesses
- 値の名前: AllowProcesses
- 値の型: REG_MULTISZ
- 値のデータ: `<add full path of the msedgewebview2.exe here >`

64ビットアプリケーションの場合、以下の値を設定する必要があります。

- キー: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxHook\AppInit_DLLs\CtxWebAuthnHook\msedgewebview2
- キー: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxHook\AppInit_DLLs\CtxWebAuthnHook
- 値の名前: FilePathName
- 値の型: REG_SZ
- 値のデータ: C:\Program Files\Citrix\HDX\bin\CtxWebAuthnHook.dll
- キー: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxHook\AppInit_DLLs\CtxWebAuthnHook
- 値の名前: Flag
- 値の型: DWORD
- 値のデータ: 00000002

32ビットアプリケーションの場合、次の値を設定する必要があります:

- キー: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\CtxHook\AppInit_DLLs\CtxWebAuthnHook\m
- キー: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\CtxHook\AppInit_DLLs\CtxWebAuthnHook
- 値の名前: FilePathName
- 値の型: REG_SZ
- 値のデータ: C:\Program Files\Citrix\HDX\bin\CtxWebAuthnHook.dll

- キー: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\CtxHook\AppInit_DLLs\CtxWebAuthnHook
- 値の名前: Flag
- 値の型: DWORD
- 値のデータ: 00000002

msedgewebview2.exeベースのアプリケーションでFIDO2リダイレクトを有効にするには、レジストリ値を設定した後、VDAを再起動してください。

シトリックス バーチャル アプリケーションズ アンド デスクトップス™ を シトリックス ゲートウェイ と統合する

StoreFront™ サーバーは、公開されたリソースとデータへのアクセスを管理するために展開および構成されます。リモートアクセスの場合、StoreFront の前に Citrix Gateway を追加することをお勧めします。

> **注:**
>
> Citrix Virtual Apps and Desktops を Citrix Gateway と統合する方法の詳細な構成手順については、StoreFront ドキュメントを参照してください。

> 次の図は、Citrix Gateway を含む簡素化された Citrix 展開の例を示しています。Citrix Gateway は StoreFront と通信し、Citrix Virtual Apps and Desktops によって提供されるアプリとデータを保護します。ユーザーデバイスは Citrix Workspace™ アプリを実行して、安全な接続を作成し、アプリ、デスクトップ、ファイルにアクセスします。

Citrix Gateway を含む簡素化された Citrix 展開(/en-us/citrix-virtual-apps-desktops/2503/media/sample-deployment-overview.png)

ユーザーは Citrix Gateway を使用してログオンし、認証します。Citrix Gateway は DMZ に展開され、保護されています。二要素認証が構成されています。ユーザー資格情報に基づいて、ユーザーには関連するリソースとアプリケーションが提供されます。アプリケーションとデータは適切なサーバー上にあります（図には示されていません）。セキュリティ上重要なアプリケーションとデータには、個別のサーバーが使用されます。

セキュリティに関する考慮事項とベストプラクティス

注:

組織は、規制要件を満たすために特定のセキュリティ標準に準拠する必要がある場合があります。このようなセキュリティ標準は時間とともに変化するため、このドキュメントではこの主題については扱いません。セキュリティ標準とCitrix製品に関する最新情報については、Citrix Trust Centerを参照してください。

ファイアウォール

環境内のすべてのマシンを、必要に応じてエンクレーブ境界を含め、境界ファイアウォールで保護します。

環境内のすべてのマシンは、パーソナルファイアウォールによって保護されている必要があります。コアコンポーネントとVDAをインストールする際、Windowsファイアウォールサービスが検出された場合（ファイアウォールが有効になっていない場合でも）、コンポーネントと機能の通信に必要なポートを自動的に開くように選択できます。これらのファイアウォールポートを手動で構成することもできます。別のファイアウォールを使用する場合は、手動で構成する必要があります。必要なポートの詳細については、Tech Paper: Citrixテクノロジーで使用される通信ポートを参照してください。

従来の環境をこのリリースに移行する場合、既存の境界ファイアウォールの再配置や新しい境界ファイアウォールの追加が必要になる場合があります。たとえば、データセンター内の従来のクライアントとデータベースサーバーの間に境界ファイアウォールがあるとします。このリリースを使用する場合、その境界ファイアウォールは、仮想デスクトップとユーザーデバイスが一方にあり、データセンター内のデータベースサーバーとDelivery Controllerがもう一方にあるように配置する必要があります。したがって、データベースサーバーとControllerを格納するために、データセンター内にエンクレーブを作成することを検討してください。また、ユーザーデバイスと仮想デスクトップの間に保護を設けることも検討してください。

注:

TCPポート1494と2598はICAとCGPに使用されるため、データセンター外のユーザーがアクセスできるようにファイアウォールで開かれている可能性が高いです。Citrixは、管理インターフェースが意図せず攻撃にさらされる可能性を避けるため、これらのポートを他の目的で使用しないことを推奨します。ポート1494と2598は、Internet Assigned Number Authority (http://www.iana.org/) に正式に登録されています。

Delivery Controller™とのセキュアな通信

HTTPSを使用した通信の暗号化

StoreFrontとNetScaler Gatewayは、HTTPまたはHTTPSを介してDelivery Controllerで実行されているXMLサービスと通信します。構成によっては、VDAはWebSocketを使用してDelivery Controllerと通信する場合があります。Directorは、HTTPまたはHTTPSを介してODataを使用して監視データと通信します。HTTPSを有効にし、HTTPを無効にすることをお勧めします。これには、Delivery ControllerでTLSを有効にする必要があります。

- StoreFrontをHTTPSを使用して接続するように構成するには、Citrix Virtual Apps and Desktopsのリソースフィードを追加するおよびCitrix Gatewayアプライアンスを追加するを参照してください。
- NetScaler GatewayをHTTPSを使用してDelivery Controllerに接続するように構成するには、NetScaler GatewayでSecure Ticket Authorityを構成するを参照してください。

セキュリティキー

Security Keysを使用すると、承認されたStoreFrontおよびNetScalerサーバーのみがクラウドコネクタ経由でDaaSに接続できるようになります。XML信頼を有効にしている場合は、これが特に重要です。

XML信頼

デフォルトでは、StoreFrontが列挙や起動などのアクションのためにデリバリーコントローラーに接続する場合、DaaSがユーザーを認証し、ユーザーのグループメンバーシップを確認できるように、StoreFrontはユーザーのActive Directory資格情報を渡す必要があります。ただし、ドメインパススルー、スマートカード、SAMLなどの他の認証方法を使用する場合、StoreFrontはActive Directoryパスワードを持っていません。この場合、「XML信頼」を有効にする必要があります。XML信頼が有効になっている場合、Citrix Virtual Apps and Desktopsは、ユーザーのパスワードを検証することなく、アプリケーションの列挙や起動など、ユーザーに代わってStoreFrontがアクションを実行することを許可します。XML信頼を有効にする前に、Security KeysまたはファイアウォールやIPsecなどの別のメカニズムを使用して、信頼できるStoreFrontサーバーのみがデリバリーコントローラーに接続できるようにしてください。

XML信頼設定を確認、有効化、または無効化するには、Citrix Virtual Apps and Desktops PowerShell SDKを使用します。

- XML信頼設定の現在の値を確認するには、`Get-BrokerSite`を実行し、`TrustRequestsSentToTheXMLServicePort`の値を調べます。

- XML信頼を有効または無効にするには、`Set-BrokerSite`をパラメーター`TrustRequestsSentToTheXmlServicePort`とともに実行します。

VDAとDelivery Controller間の通信

VDAがコントローラーと通信するためのメカニズムは2つあります。

- ウィンドウズ コミュニケーション ファンデーション

  Windows Communication Foundation (WCF) のメッセージレベル保護は、デリバリーコントローラーとVDA間の通信を保護します。これにより、TLSを使用した追加のトランスポートレベル保護の必要がなくなります。VDAとデリバリーコントローラー間の通信に使用されるデフォルトポートは80です。ただし、ポートをカスタマイズできます。詳細については、VDAのカスタマイズを参照してください。

  WCFにおけるメッセージセキュリティの詳細については、MicrosoftドキュメントのWCFにおけるメッセージセキュリティを参照してください。

  WCF構成は、コントローラーとVDA間の相互認証にKerberosを使用します。暗号化には256ビットキーのCBCモードAESを使用します。メッセージの整合性にはSHA-1を使用します。

  Microsoftによると、WCFで使用されるセキュリティプロトコルは、WS-SecurityPolicy 1.2を含むOASIS（Organization for the Advancement of Structured Information Standards）の標準に準拠しています。また、Microsoftは、WCFがSecurity Policy 1.2に記載されているすべてのアルゴリズムスイートをサポートしていると述べています。

  コントローラーとVDA間の通信には、basic256アルゴリズムスイートが使用され、そのアルゴリズムは前述のとおりです。

  WCF構成は、メッセージレベルのセキュリティ暗号化とともに、SOAP over HTTPプロトコルを使用します。

- WebSockets

  これはWCFの最新の代替手段です。VDAからDelivery Controllerへの通信にTLSポート443のみを使用するという利点があります。現在、MCSでプロビジョニングされたマシンでのみ利用可能です。詳細については、「VDAとDelivery Controller間のWebSocket通信」(/ja-jp/citrix-virtual-apps-desktops/2503/secure/websocket-vda-support)を参照してください。

Delivery ControllerとLicense Server間のセキュアな通信

Delivery ControllerはHTTPS経由でLicense Serverと通信します。デフォルトでは自己署名証明書を使用しますが、これをエンタープライズまたはパブリック証明機関によって発行された証明書に

置き換えることをお勧めします。詳細については、Citrix Licensing ManagerおよびWeb Services for Licensingで使用される証明書の手動インストールを参照してください。

WebブラウザーとWeb StudioおよびDirector間の安全な通信

Web StudioとDirectorは、Delivery Controllerと同じマシン、または別のマシンにインストールできます。ユーザーはWebブラウザーを使用してWeb StudioとDirectorに接続します。デフォルトでは、Web Studioは自己署名証明書を使用してHTTPSを有効にしますが、スタンドアロンでインストールされたDirectorはHTTPSを構成しません。適切な証明書を使用して、「Web StudioおよびDirectorでTLSを有効にする」(/ja-jp/citrix-virtual-apps-desktops/2503/secure/tls-studio)ことをお勧めします。

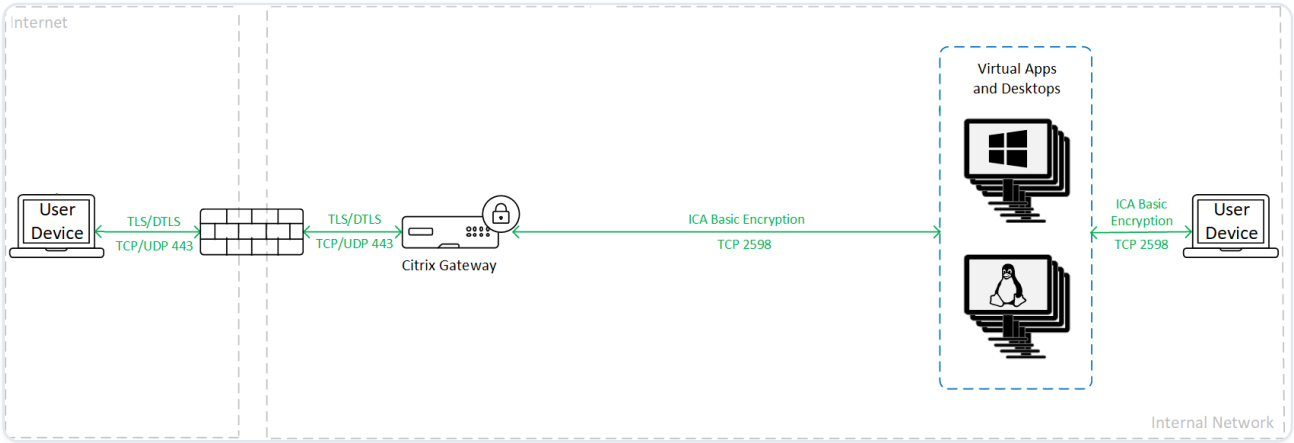
ICA®通信の保護

Citrix Virtual Apps and Desktops™は、クライアントとVDA間のICAトラフィックを保護するためのいくつかのオプションを提供します。利用可能なオプションは次のとおりです。

- **基本暗号化:** デフォルト設定です。
- **SecureICA:** RC5 (128ビット) 暗号化を使用してセッションデータを暗号化できます。
- **VDA TLS/DTLS:** TLS/DTLSを使用したネットワークレベルの暗号化を可能にします。

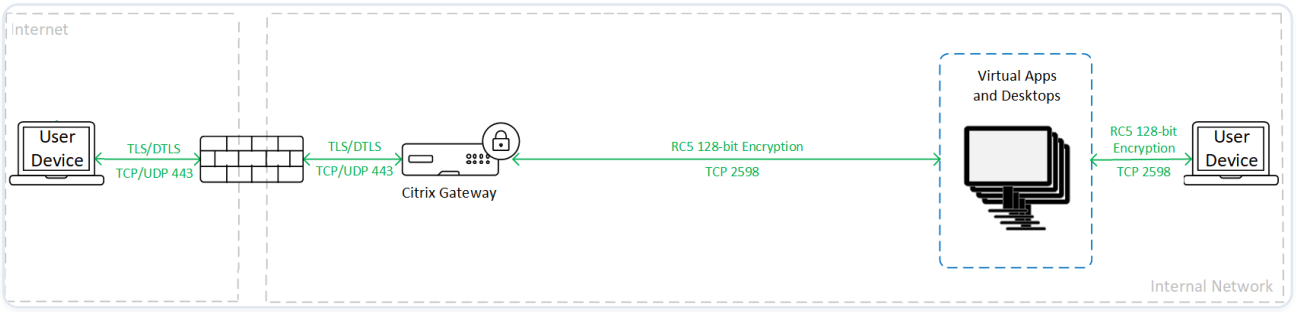
基本暗号化

基本暗号化を使用する場合、トラフィックは次の図に示すように暗号化されます。



SecureICA

SecureICAを使用すると、トラフィックは次の図に示すように暗号化されます。



詳細については、セキュリティポリシー設定を参照してください。

> **注1：**
>
> SecureICAは、Workspace app for HTML5ではサポートされていません。

> **注2：**
>
> Citrix SecureICAはICA/HDXプロトコルの一部ですが、Transport Layer Security (TLS) のような標準準拠のネットワークセキュリティプロトコルではありません。

VDA TLS/DTLS

VDA TLS/DTLS暗号化を使用すると、トラフィックは次の図に示すように暗号化されます。

TLS/DTLS使用時のトラフィック暗号化(/en-us/citrix-virtual-apps-desktops/2503/media/vda-tls.png)

VDA TLS/DTLSを構成するには、「VDA上のTLS設定」を参照してください。

仮想チャネル

環境で許可されるCitrix以外の仮想チャネルを制御するには、「仮想チャネル許可リスト」を使用します。

印刷サーバーとの安全な通信

Virtual Delivery Agent (VDA) と Universal Print Server 間の TCP ベースの接続で TLS を有効にできます。詳細については、Universal Print ServerでのTransport Layer Security (TLS) を参照してください。

サイトデータベースとの安全な通信

サイトデータベースへのTLSを有効にする方法については、「CTX137556」を参照してください。

VDAマシンのセキュリティ

一般的な推奨事項

VDAが最新のオペレーティングセキュリティアップデートとウイルス対策で常に最新の状態に保たれていることを確認してください。

アプリケーションセキュリティ

管理者以外のユーザーが悪意のある操作を実行するのを防ぐため、Citrix®は、VDAホスト上のインストーラー、アプリケーション、実行可能ファイル、およびスクリプトに対してWindows AppLockerルールを構成することを推奨します。

8.3形式のファイル名

VDAで8.3形式のファイル名を無効にできます。「Microsoft fsutil documentation」を参照してください。

データストレージに関する考慮事項

デスクトップ環境は、プールされたデスクトップや専用デスクトップなど、さまざまな種類のデスクトップで構成されている場合があります。ユーザーは、プールされたデスクトップなど、ユーザー間で共有されるデスクトップにデータを保存してはなりません。ユーザーが専用デスクトップにデータを保存する場合、そのデスクトップが後で他のユーザーに利用可能になった場合は、そのデータを削除する必要があります。

ユーザーアカウント管理

アカウント管理にはWindowsのベストプラクティスを適用してください。Machine Creation ServicesまたはProvisioning Servicesによって複製される前に、テンプレートまたはイメージ上にアカウントを作成しないでください。保存された特権ドメインアカウントを使用してタスクをスケジュールしないでください。共有Active Directoryマシンアカウントを手動で作成しないでください。これらの慣行は、マシン攻撃がローカルの永続的なアカウントパスワードを取得し、それらを使用して他のユーザーに属するMCS/PVS共有イメージにログオンするのを防ぐのに役立ちます。

ユーザーには、必要な機能のみを付与してください。Microsoft Windowsの特権は、通常の方法でデスクトップに引き続き適用されます。つまり、ユーザー権利の割り当てを通じて特権を構成し、

グループポリシーを通じてグループメンバーシップを構成します。このリリースの利点の1つは、デスクトップが保存されているコンピューターに対する物理的な制御を付与することなく、ユーザーにデスクトップへの管理権限を付与できることです。

デスクトップの特権を計画する際は、以下に注意してください。

- 既定では、非特権ユーザーがデスクトップに接続すると、自分のユーザーデバイスのタイムゾーンではなく、デスクトップを実行しているシステムのタイムゾーンが表示されます。ユーザーがデスクトップを使用する際にローカル時刻を表示できるようにする方法については、「Delivery Groupの管理」の記事を参照してください。
- デスクトップの管理者であるユーザーは、そのデスクトップを完全に制御できます。デスクトップが専用デスクトップではなくプールされたデスクトップである場合、そのユーザーは、将来のユーザーを含むそのデスクトップの他のすべてのユーザーに関して信頼されている必要があります。デスクトップのすべてのユーザーは、この状況によってデータセキュリティに永続的なリスクが生じる可能性があることを認識する必要があります。この考慮事項は、単一ユーザーのみが使用する専用デスクトップには適用されません。そのユーザーは、他のどのデスクトップの管理者であってもなりません。
- デスクトップの管理者であるユーザーは、一般的にそのデスクトップにソフトウェア（悪意のあるソフトウェアを含む）をインストールできます。また、デスクトップに接続されているネットワーク上のトラフィックを監視または制御できる可能性もあります。

ログオン権限の管理

ログオン権限は、ユーザーアカウントとコンピューターアカウントの両方に必要です。Microsoft Windowsの特権と同様に、ログオン権限は通常の方法でデスクトップに適用され続けます。ユーザー権利の割り当てを通じてログオン権限を構成し、グループポリシーを通じてグループメンバーシップを構成します。

Windowsのログオン権限は、ローカルログオン、リモートデスクトップサービス経由のログオン、ネットワーク経由のログオン（ネットワークからこのコンピューターにアクセス）、バッチジョブとしてのログオン、サービスとしてのログオンです。

コンピューターアカウントの場合、コンピューターに必要なログオン権限のみを付与します。「ネットワークからこのコンピューターにアクセス」というログオン権限は、Delivery Controllerのコンピューターアカウントに必要です。

ユーザーアカウントの場合、ユーザーに必要なログオン権限のみを付与します。

Microsoftによると、既定では、Remote Desktop Usersグループには「リモートデスクトップサービスを介したログオンを許可する」というログオン権限が付与されています（ドメインコントローラーを除く）。

組織のセキュリティポリシーによっては、このグループをそのログオン権限から削除するよう明示的に規定している場合があります。次のアプローチを検討してください。

- Multi-session OS用Virtual Delivery Agent（VDA）は、Microsoft Remote Desktop Servicesを使用します。Remote Desktop Usersグループを制限付きグループとして構成し、Active Directoryグループポリシーを介してグループのメンバーシップを制御できます。詳細については、Microsoftのドキュメントを参照してください。
- Single-session OS用VDAを含むCitrix Virtual Apps and Desktopsのその他のコンポーネントでは、Remote Desktop Usersグループは不要です。したがって、これらのコンポーネントでは、Remote Desktop Usersグループに「リモートデスクトップサービスを介したログオンを許可する」というログオン権限は必要ありません。削除できます。さらに、次の点に注意してください。
    - リモートデスクトップサービスを介してそれらのコンピューターを管理する場合は、そのようなすべての管理者がすでにAdministratorsグループのメンバーであることを確認してください。
    - リモートデスクトップサービスを介してそれらのコンピューターを管理しない場合は、それらのコンピューターでリモートデスクトップサービス自体を無効にすることを検討してください。

「リモートデスクトップサービスを介したログオンを拒否する」というログオン権限にユーザーとグループを追加することは可能ですが、ログオン拒否権限の使用は一般的に推奨されません。詳細については、Microsoftのドキュメントを参照してください。

Delivery Controllerのセキュリティ

Delivery Controller上のWindowsサービス

Delivery Controllerのインストールにより、以下のWindowsサービスが作成されます。

- Citrix AD Identity Service (NT SERVICE\CitrixADIdentityService): VMのMicrosoft Active Directoryコンピューターアカウントを管理します。
- Citrix Analytics (NT SERVICE\CitrixAnalytics): サイト管理者がこの収集を承認した場合、Citrixが使用するためにサイト構成の使用状況情報を収集します。その後、この情報をCitrixに送信し、製品の改善に役立てます。

- Citrix App Library (NT SERVICE\CitrixAppLibrary): AppDiskの管理とプロビジョニング、AppDNA統合、およびApp-Vの管理をサポートします。
- Citrix Broker Service (NT SERVICE\CitrixBrokerService): ユーザーが利用できる仮想デスクトップまたはアプリケーションを選択します。
- Citrix Configuration Logging Service (NT SERVICE\CitrixConfigurationLogging): 管理者がサイトに対して行ったすべての構成変更およびその他の状態変更を記録します。
- Citrix Configuration Service (NT SERVICE\CitrixConfigurationService): 共有構成用のサイト全体のレポジトリ。
- Citrix Delegated Administration Service (NT SERVICE\CitrixDelegatedAdmin): 管理者に付与された権限を管理します。
- Citrix Environment Test Service (NT SERVICE\CitrixEnvTest): 他のデリバリーコントローラーサービスの自己テストを管理します。
- Citrix Host Service (NT SERVICE\CitrixHostService): Citrix Virtual AppsまたはCitrix Virtual Desktopsの展開で使用されるハイパーバイザーインフラストラクチャに関する情報を保存し、コンソールがハイパーバイザープール内のリソースを列挙するために使用する機能も提供します。
- Citrix Machine Creation Services (NT SERVICE\CitrixMachineCreationService): デスクトップVMの作成をオーケストレーションします。
- Citrix Monitor Service (NT SERVICE\CitrixMonitor): Citrix Virtual AppsまたはCitrix Virtual Desktopsのメトリックを収集し、履歴情報を保存し、トラブルシューティングおよびレポートツール用のクエリインターフェイスを提供します。
- Citrix StoreFront Service (NT SERVICE\ CitrixStorefront): StoreFrontの管理をサポートします。(StoreFrontコンポーネント自体の一部ではありません。)
- Citrix StoreFront Privileged Administration Service (NT SERVICE\CitrixPrivilegedService): StoreFrontの特権管理操作をサポートします。(StoreFrontコンポーネント自体の一部ではありません。)
- Citrix Config Synchronizer Service (NT SERVICE\CitrixConfigSyncService): メインサイトデータベースからローカルホストキャッシュに構成データを伝播します。
- Citrix High Availability Service (NT SERVICE\CitrixHighAvailabilityService): メインサイトデータベースが利用できない場合に、ユーザーが利用できる仮想デスクトップまたはアプリケーションを選択します。

Delivery Controllerのインストールでは、以下のWindowsサービスも作成されます。これらは、他のCitrixコンポーネントと一緒にインストールされる際にも作成されます。

- Citrix Diagnostic Facility COM Server (NT SERVICE\CdfSvc): Citrixサポートが使用するための診断情報の収集をサポートします。
- Citrix Telemetry Service (NT SERVICE\CitrixTelemetryService): Citrixによる分析のために診断情報を収集し、管理者が分析結果と推奨事項を表示して、サイトの問題の診断に役立てることができます。

Delivery Controllerのインストールでは、以下のWindowsサービスも作成されます。これは現在使用されていません。有効になっている場合は、無効にしてください。

- シトリックス リモート ブローカー プロバイダー (NT SERVICE\XaXdCloudProxy)

Delivery Controllerのインストールでは、以下のWindowsサービスも作成されます。これらは現在使用されていませんが、有効にする必要があります。無効にしないでください。

- シトリックス オーケストレーション サービス (NT SERVICE\CitrixOrchestration)
- シトリックス トラスト サービス (NT SERVICE\CitrixTrust)

Except for the Citrix StoreFront™ Privileged Administration Service, these services are granted the logon right Log on as a service and the privileges Adjust memory quotas for a process, Generate security audits, and Replace a process level token. You do not need to change these user rights. These privileges are not used by the Delivery Controller and are automatically disabled.

Citrix StoreFront Privileged AdministrationサービスとCitrix Telemetry Serviceを除き、前述のDelivery Controller WindowsサービスはNETWORK SERVICE IDとしてログオンするように構成されています。これらのサービス設定を変更しないでください。

Citrix Config Synchronizer Serviceは、NETWORK SERVICEアカウントがDelivery Controller上のローカル管理者グループに属している必要があります。これにより、ローカルホストキャッシュが正しく機能します。

Citrix StoreFront Privileged Administration サービスは、ローカルシステム (NT AUTHORITY\SYSTEM) としてログオンするように構成されています。これは、通常サービスでは利用できない Delivery Controller StoreFront の操作 (Microsoft IIS サイトの作成を含む) に必要です。サービス設定を変更しないでください。

Citrix Telemetry Service は、独自のサービス固有のIDとしてログオンするように構成されています。

Citrix Telemetry Service は無効にできます。このサービスと、すでに無効になっているサービスを除き、これらの Delivery Controller Windows サービスを他に無効にしないでください。

ログオン権限の管理

VDA のコンピューターアカウントには、「ネットワークからこのコンピューターにアクセス」のログオン権限が必要です。詳細については、「Active Directory OU ベースの Controller 検出」を参照してください。

クライアントアクセス

クライアントアクセスは通常、Citrix StoreFront を展開することで提供されます。StoreFront のセキュリティ保護の詳細については、「StoreFront のドキュメント」を参照してください。

リモートユーザーが StoreFront および VDA に安全に接続できるようにするには、NetScaler® Gateway を展開します。

Citrix は、クライアントが Citrix Workspace アプリを使用して StoreFront に接続することを推奨しています。詳細については、各オペレーティングシステム用の Citrix Workspace アプリの(/ja-jp/citrix-workspace-app.html)ドキュメントのセキュリティセクションを参照してください。または、ユーザーは Web ブラウザーを使用して StoreFront にアクセスすることもできます。

ユーザーが Citrix Workspace™ アプリ以外のアプリケーションを実行する能力が限られているシンクライアントをユーザーに提供することを検討してください。デバイスが組織によって管理されている場合は、オペレーティングシステムのセキュリティ更新プログラムとウイルス対策ソフトウェアの展開を確実にするためのポリシーを導入する必要があります。ただし、多くの場合、ユーザーは組織の管理外にある管理されていないデバイスから接続できる必要があります。次の機能の使用を検討してください。

- Endpoint Analysis は、オペレーティングシステムやウイルス対策などのセキュリティ情報をエンドポイントでスキャンし、セキュリティ要件を満たさないクライアントへのアクセスを拒否します。
- App Protection は、キーロガーと画面キャプチャをブロックします。

混在バージョン環境

たとえば、VDA のバージョンが Delivery Controller と異なる混在バージョン環境は、一部のアップグレード中に避けられません。ベストプラクティスに従い、異なるバージョンの Citrix コンポーネントが共存する時間を最小限に抑えてください。混在バージョン環境では、たとえばセキュリティポリシーが均一に適用されない場合があります。

> **注:**

これは他のソフトウェア製品にも共通しています。以前のバージョンの Active Directory を使用すると、後のバージョンの Windows ではグループポリシーが部分的にしか適用されません。

以下のシナリオでは、特定の混在バージョンCitrix環境で発生する可能性のあるセキュリティ問題について説明します。Citrix Receiver 1.7を使用して、XenApp and XenDesktop 7.6 Feature Pack 2のVDAを実行している仮想デスクトップに接続すると、ポリシー設定の**デスクトップとクライアント間のファイル転送を許可する**がサイトで有効になりますが、XenApp and XenDesktop 7.1を実行しているDelivery Controllerでは無効にできません。これは、製品の後のバージョンでリリースされたポリシー設定を認識しないためです。このポリシー設定により、ユーザーはファイルを仮想デスクトップにアップロードおよびダウンロードできるようになり、これがセキュリティ問題となります。この問題を回避するには、Delivery Controller（またはStudioのスタンドアロンインスタンス）をバージョン7.6 Feature Pack 2にアップグレードし、グループポリシーを使用してポリシー設定を無効にします。または、影響を受けるすべての仮想デスクトップでローカルポリシーを使用します。

Remote PC Accessのセキュリティに関する考慮事項

Remote PC Accessは、次のセキュリティ機能を実装しています。

- スマートカードの使用がサポートされています。
- リモートセッションが接続されると、オフィスPCのモニターは空白で表示されます。
- Remote PC Accessは、CTRL+ALT+DEL、USB対応スマートカード、生体認証デバイスを除くすべてのキーボードおよびマウス入力をリモートセッションにリダイレクトします。
- SmoothRoamingは単一ユーザーのみがサポートされます。
- ユーザーがオフィスPCにリモートセッションを接続している場合、そのユーザーのみがオフィスPCのローカルアクセスを再開できます。ローカルアクセスを再開するには、ユーザーはローカルPCでCtrl-Alt-Delを押し、リモートセッションで使用したのと同じ資格情報でログオンします。システムに適切なサードパーティの資格情報プロバイダー統合がある場合、ユーザーはスマートカードを挿入するか、生体認証を利用してローカルアクセスを再開することもできます。このデフォルトの動作は、グループポリシーオブジェクト（GPO）を介して高速ユーザー切り替えを有効にするか、レジストリを編集することで上書きできます。

注:

> Citrixでは、VDA管理者権限を一般セッションユーザーに割り当てないことを推奨しています。

自動割り当て

デフォルトでは、Remote PC Accessは複数のユーザーのVDAへの自動割り当てをサポートしています。XenDesktop 5.6 Feature Pack 1では、管理者はRemotePCAccess.ps1 PowerShellスクリプトを使用してこの動作を上書きできます。このリリースでは、複数の自動リモートPC割り当てを許可または禁止するためにレジストリエントリを使用します。この設定はサイト全体に適用されます。

> **注意:**

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

> 自動割り当てを単一ユーザーに制限するには：

サイト内の各Controllerで、次のレジストリエントリを設定します。

```
HKEY_LOCAL_MACHINE\Software\Citrix|DesktopServer

Name: AllowMultipleRemotePCAssignments

Type: REG_DWORD

Data: 0 = Disable multiple user assignment, 1 = (Default) Enable multiple
user assignment.
```

既存のユーザー割り当てがある場合は、SDKコマンドを使用してそれらを削除し、VDAが後で単一の自動割り当ての対象となるようにします。

- VDAから割り当て済みのすべてのユーザーを削除します: `$machine.AssociatedUserNames | %{ Remove-BrokerUser-Name $_ -Machine $machine`

- Delivery GroupからVDAを削除します: `$machine | Remove-BrokerMachine -DesktopGroup $desktopGroup`

物理的なオフィスPCを再起動します。

証明書を管理する

TLSは、2者間の信頼を確立するために証明書を使用します。サービスを提供する各サーバーに適切な証明書をインストールし、そのサーバーに接続するマシンがその証明書を信頼することを確認する必要があります。証明書の署名には、次のオプションがあります。

- 自己署名証明書。これらは推奨されません。これらの証明書は、信頼する必要がある他のマシンに手動でコピーする必要があるため、管理が困難です。
- エンタープライズ認証局。既存のPKIが導入されている場合、これは通常、内部デバイス間で使用する証明書に署名する最も簡単なオプションです。
- 公開認証局。これには、ドメインの所有権を認証局に証明する必要があります。管理されていないクライアントデバイスは、主要な公開認証局からの証明書を信頼するように通常事前に構成されているという利点があります。

新しい証明書を作成する

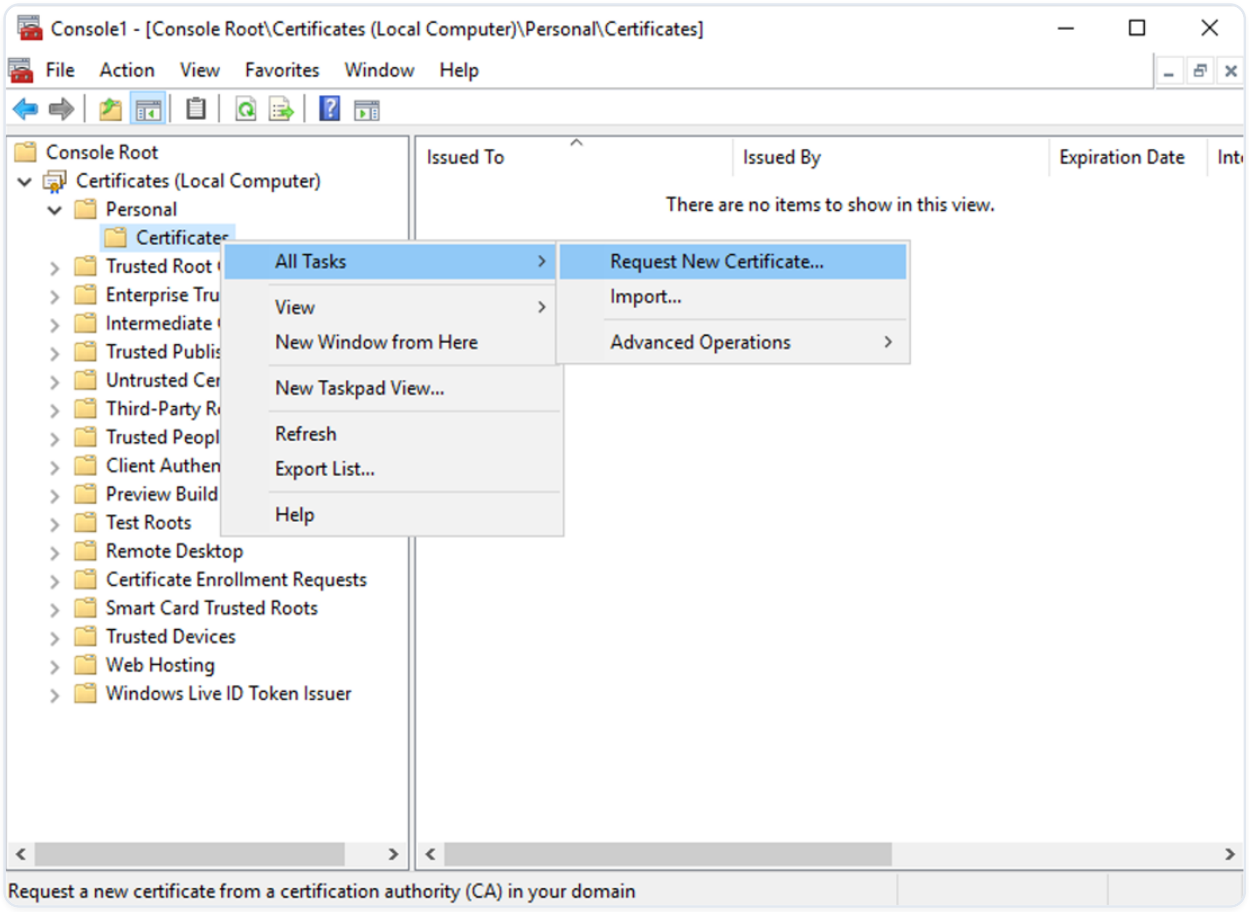
証明書の作成については、組織のポリシーと手順に従ってください。

Microsoft 証明機関を使用して証明書を作成する

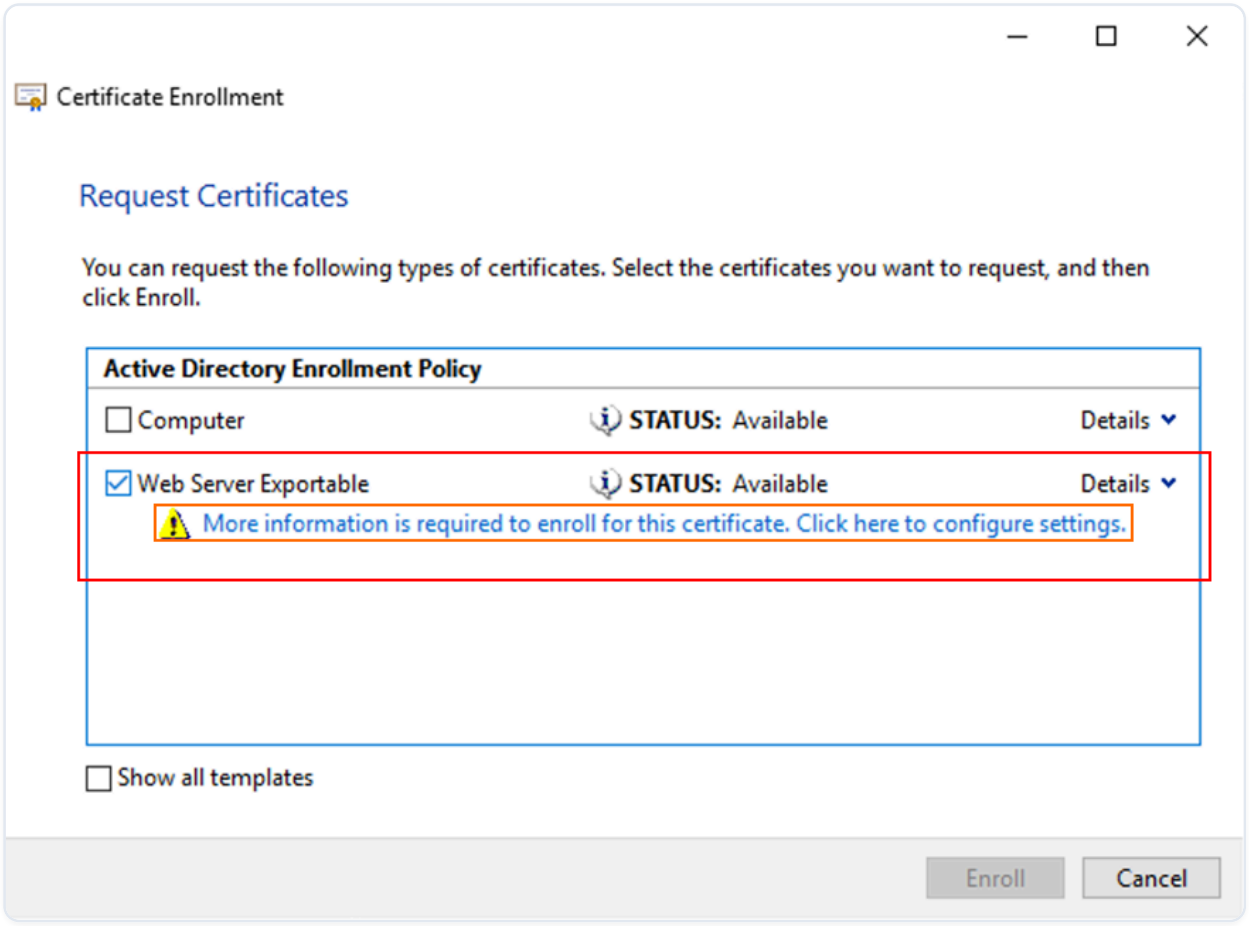
Microsoft 証明機関が Active Directory ドメインまたは Delivery Controller が参加している信頼されたフォレストに統合されている場合、証明書 MMC スナップインの証明書登録ウィザードから証明書を取得できます。Microsoft 証明機関は、Web サーバーでの使用に適した証明書テンプレートを公開している必要があります。

ルート証明書は、グループポリシーを使用してドメイン上の他のマシンに自動的に展開されます。したがって、ドメイン上の他のすべてのマシンは、Microsoft証明機関を使用して作成された証明書を信頼します。ドメイン上にないマシンがある場合は、ルート証明機関証明書をエクスポートして、それらのマシンにインポートする必要があります。

1. サーバーで、MMCコンソールを開き、証明書スナップインを追加します。プロンプトが表示されたら、コンピューターアカウントを選択します。
2. **個人 > 証明書**を展開し、**すべてのタスク > 新しい証明書の要求**コンテキストメニューコマンドを使用します。



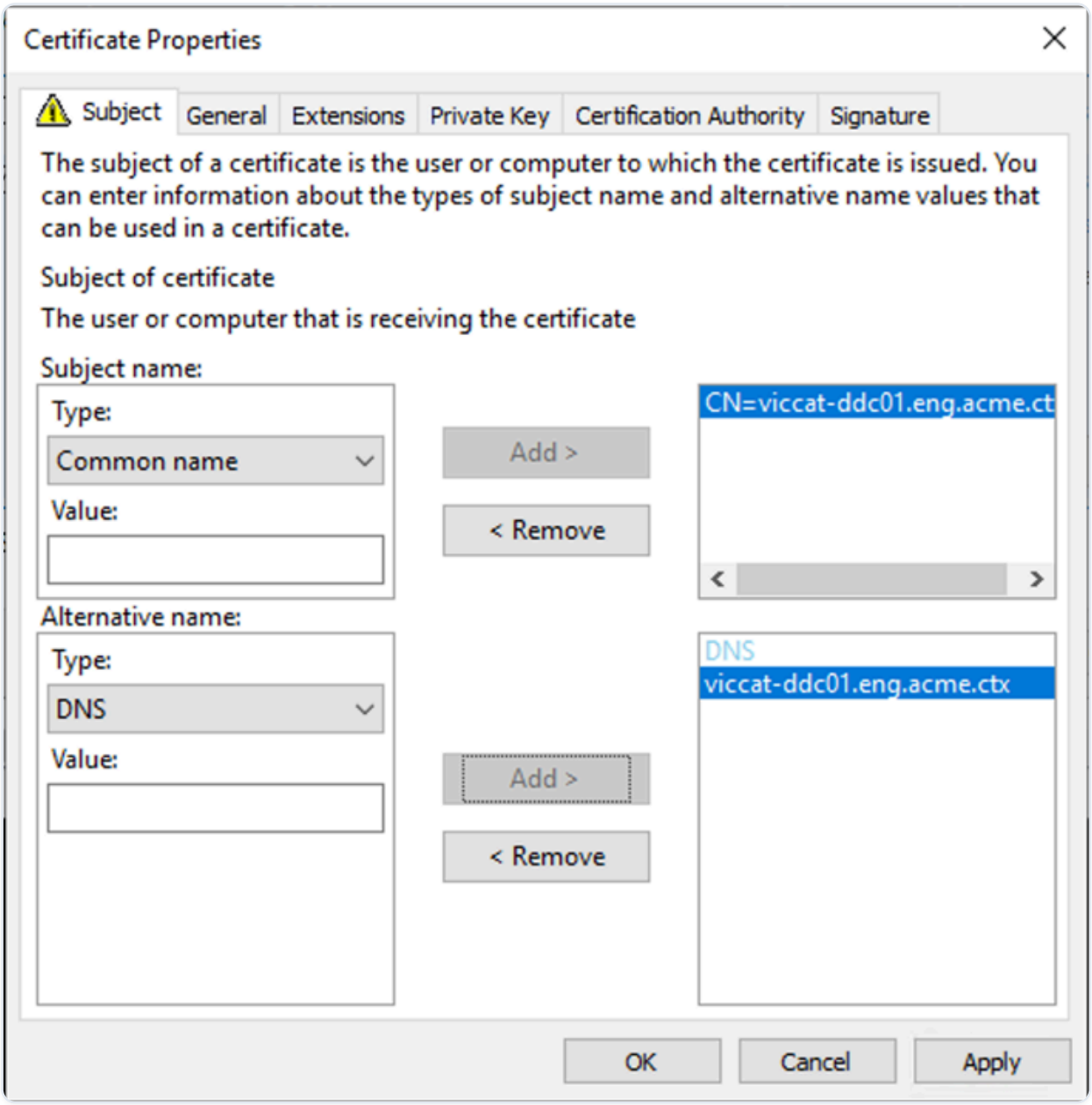
3. **次へ**をクリックして開始し、**次へ**をクリックしてActive Directory登録から証明書を取得することを確認します。
4. **Webサーバーエクスポート可能**などの適切なテンプレートを選択します。テンプレートが件名の値を自動的に提供するように設定されている場合は、詳細を指定せずに**登録**をクリックできます。それ以外の場合は、**この証明書を登録するには詳細情報が必要です。設定を構成するにはここをクリックしてください。**をクリックします。



5. 証明書テンプレートの詳細を指定するには、**詳細**矢印ボタンをクリックし、次の項目を設定します。

   サブジェクト名: 共通名を選択し、サーバーのFQDNを追加します。

   代替名: を選択し、サーバーの FQDN を追加します。



6. **OK**を押します。
7. **Enroll** を押して証明書を作成します。証明書の一覧に表示されます。

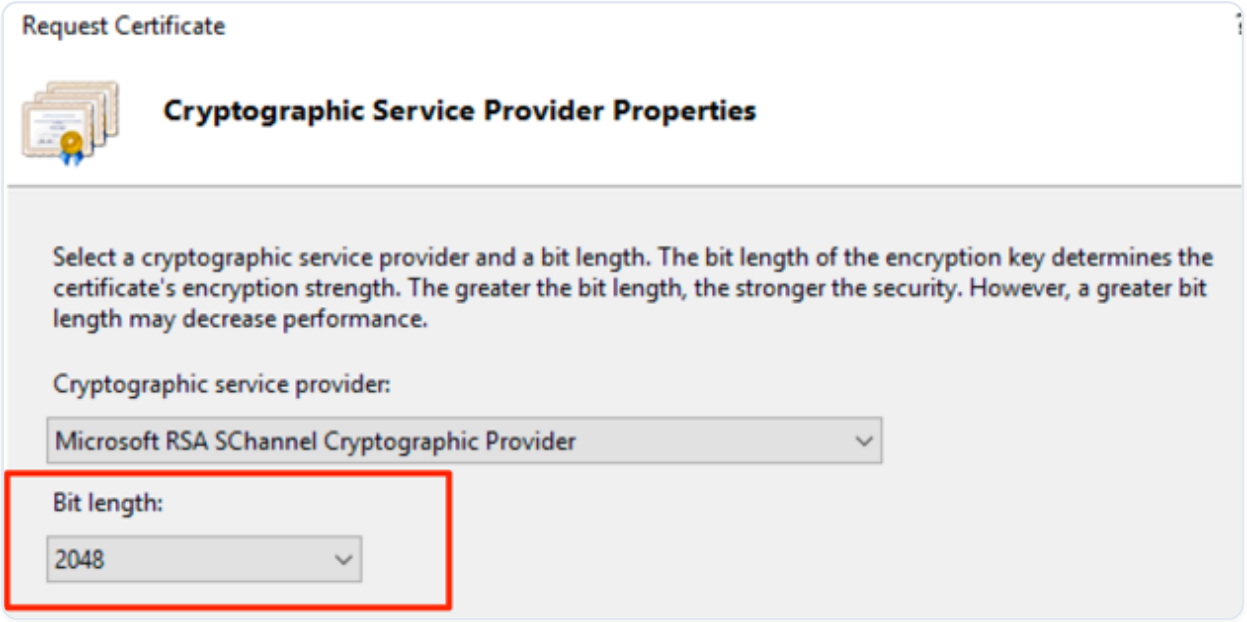
   個人証明書のスクリーンショット(/en-us/citrix-virtual-apps-desktops/2503/media/personal-certificates.png)

IIS を使用して証明書要求を作成する

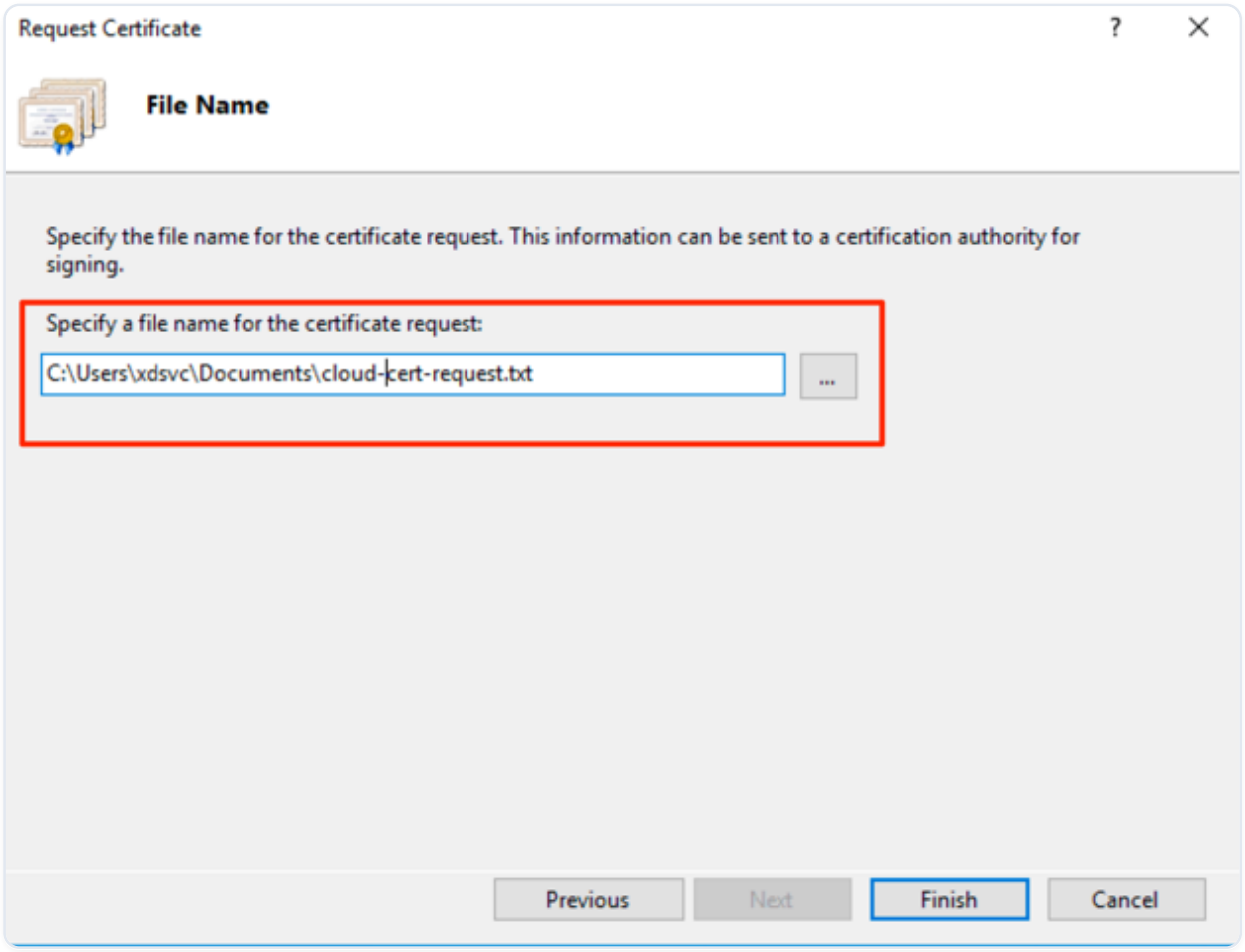
IIS がサーバーにインストールされている場合は、次の手順を実行します。

1. **インターネット インフォメーション サービス (IIS) マネージャー**を開きます。
2. 接続リストでサーバーノードを選択します。
3. **サーバー証明書**を開きます。 (/en-us/citrix-virtual-apps-desktops/2503/media/iis-server-certificates.png)

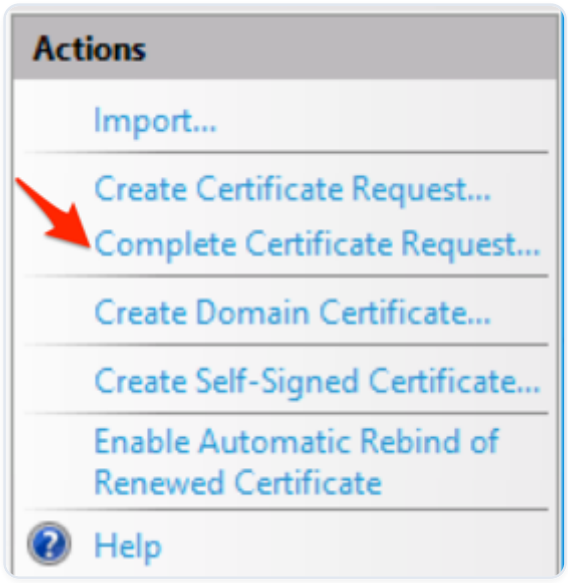
4. **操作**ペインから、**証明書要求の作成...**を選択します。 (/en-us/citrix-virtual-apps-desktops/2503/media/iis-create-certificate-request.png)
5. **識別名プロパティ**を入力します。 (/en-us/citrix-virtual-apps-desktops/2503/media/iis-request-certificate-properties.png)
6. 「**暗号化サービスプロバイダーのプロパティ**」画面で、「**暗号化サービスプロバイダー**」はデフォルトのままにします。キーサイズは「**2048**」以上に設定します。



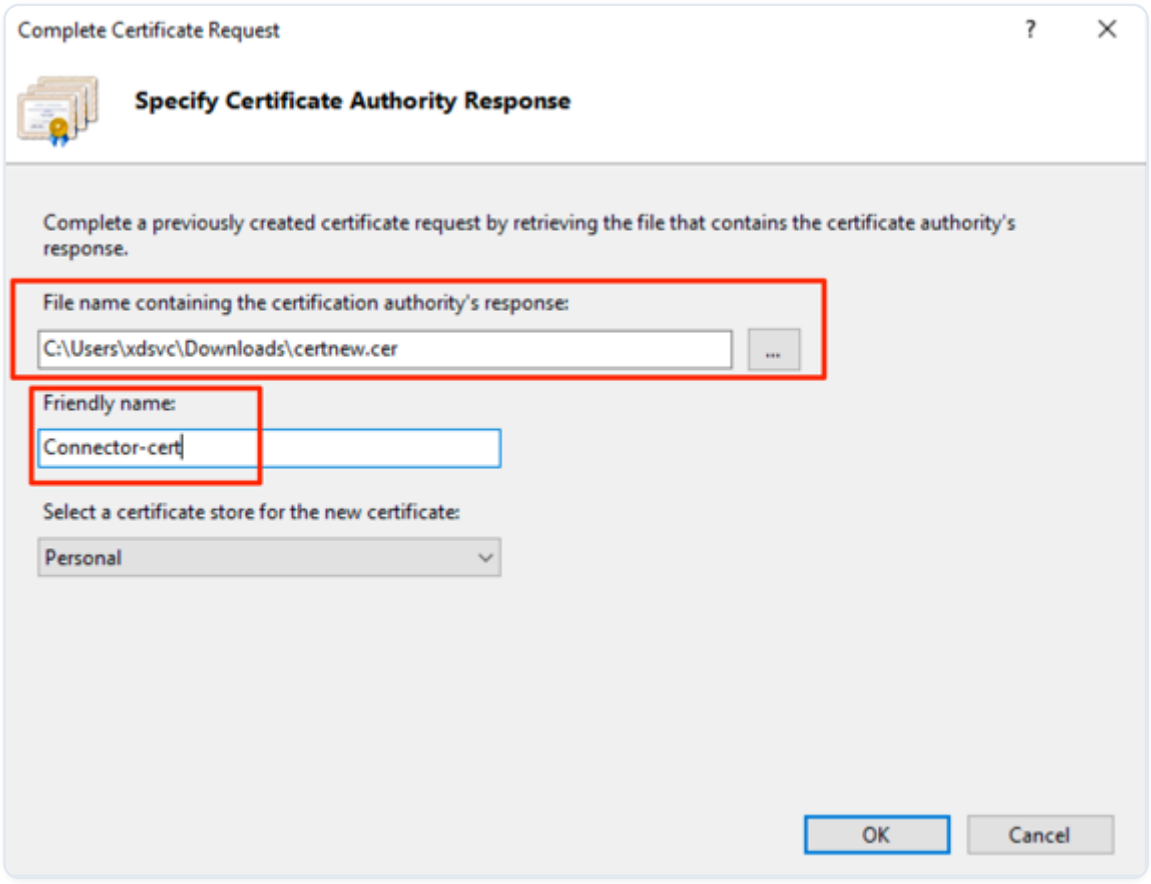
7. ファイル名を選択し、「**完了**」を押します。



8. CSRを証明機関にアップロードします。
9. 証明書を受け取ったら、「**操作**」ペインから「**証明書の要求を完了する...**」を選択します。



10. 証明書を選択し、「**フレンドリ名**」を入力して「**OK**」を押します。



サブジェクトの別名を設定する方法はありません。そのため、証明書は共通名を使用して指定されたサーバーに限定されます。

証明書スナップインから証明書署名要求を作成する

証明書MMCスナップイン内から、証明書署名要求を作成できます。これにより、証明書を提供する証明機関に送信できるファイルが生成されます。その後、ローカルの秘密鍵と結合するために証明書をインポートする必要があります。

1. サーバーで、MMCコンソールを開き、証明書スナップインを追加します。プロンプトが表示されたら、を選択します。
2. 「**個人**」>「**証明書**」を展開します。
3. 「**すべてのタスク**」>「**高度な操作**」>「**カスタム要求の作成**」を選択します。
4. 「**開始する前に**」で、「**次へ**」を選択します。
5. 「**証明書の登録ポリシーの選択**」画面で、適切な既存のポリシーを選択するか、「**登録ポリシーなしで続行**」を選択します。
6. 「**カスタム要求**」画面で、登録ポリシーを使用している場合は、利用可能な場合は、たとえば「**Webサーバーのエクスポート可能**」など、適切なテンプレートを選択します。
7. 「**証明書情報**」画面で、「**詳細**」を展開し、「**プロパティ**」を選択します。

8. **証明書のプロパティ**ウィンドウの**全般**タブで、適切なフレンドリ名を入力します。
9. **サブジェクト**タブで、次のようにします。
    a. **サブジェクト名**で、**共通名**を選択し、サーバーのFQDNを入力します。ワイルドカードを入力できます。**追加**を選択します。
    b. **サブジェクト名**で、組織、組織単位、地域、都道府県、国に適切な値を追加します。
    c. **代替名**で、**DNS**を選択します。サーバーのFQDNを追加します。複数のサーバーFQDNまたはワイルドカードFQDNを追加できます。
10. **拡張機能**タブで、次のようにします。
    - **キー使用法**で、**デジタル署名**と**キーの暗号化**を追加します。
    - **拡張キー使用法（アプリケーションポリシー）で、サーバー認証とクライアント認証**を追加します。
11. **秘密キー**タブで、次のようにします。
    - **暗号化サービスプロバイダー（CSP）の選択**で、適切なプロバイダーを選択します。
    - **キーオプション**で、適切なキーサイズを選択します。RSAプロバイダーの場合、最小で2048のキーサイズを使用します。セキュリティを強化するために4096を選択することもできますが、パフォーマンスにわずかな影響があります。
    - **キーオプション**で、**秘密キーをエクスポート可能にする**を選択します。
12. **OK**を選択します。
13. **次へ**を選択します。
14. **参照**を選択し、要求を保存します。
15. 「**完了**」を選択します。
16. CSR を証明機関にアップロードします。
17. 証明書を受け取ったら、秘密キーにリンクされるように、同じサーバーにインポートします。

新しい自己署名証明書を作成する

自己署名証明書は、デリバリーコントローラー™とWeb Studioのインストール中に作成されます。新しい自己署名証明書を生成し、既存の証明書を置き換えるために使用できます。

IIS マネージャーの使用

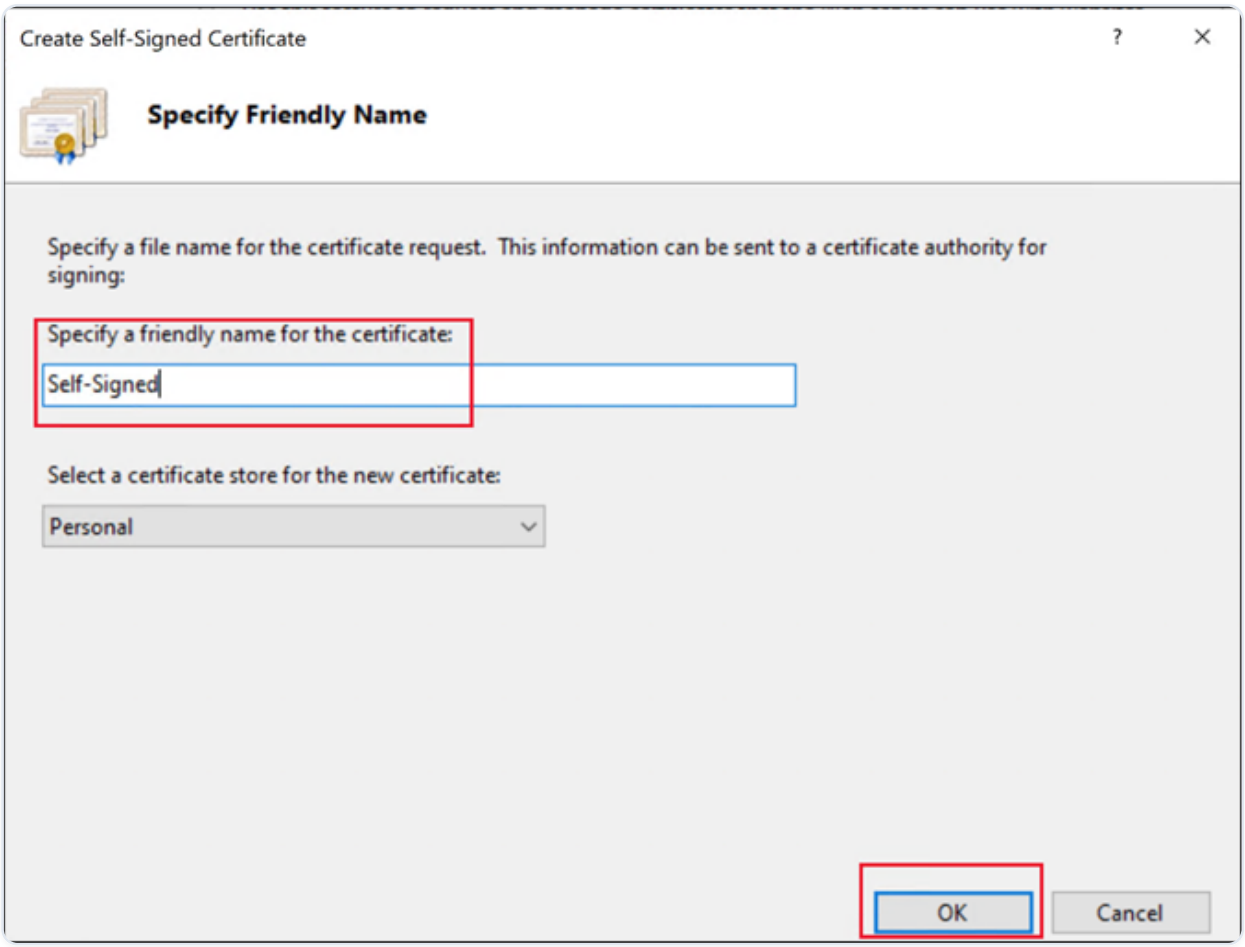
サーバーにIISがインストールされている場合は、次の手順を実行できます。

1. 管理者としてサーバーにログオンします。

2. IIS マネージャーを開きます
3. **サーバー証明書**を開きます
4. **操作**ペインで、**自己署名証明書の作成**を選択します。

   サーバー証明書(/en-us/citrix-virtual-apps-desktops/2503/media/server-certificates.png)

5. **自己署名証明書の作成**で、証明書の名前を入力し、**OK**をクリックします。自己署名証明書が作成されます。



PowerShell の使用

PowerShellを使用して自己署名証明書を作成できます。

```
$certSubject = "CN=myddc.example.com" # The FQDN of the server.

$friendlyName = "Self-Signed-3"

$expireYears = 5
```

```
## Create new self-signed certificate under LocalMachine\My

$certificate = New-SelfSignedCertificate -Subject $certSubject
-CertStoreLocation "Cert:\LocalMachine\My\" -KeyExportPolicy Exportable
-KeySpec Signature -KeyLength 2048 -KeyAlgorithm RSA -HashAlgorithm SHA256
-FriendlyName $friendlyName -NotAfter $
([System.DateTime]::Now.AddYears($expireYears))



# Add to trusted root certificates

$rootCertStore = Get-Item "Cert:\LocalMachine\Root\"

$rootCertStore.Open([System.Security.Cryptography.X509Certificates.OpenFla
gs]::ReadWrite)

$rootCertStore.Add($certificate)
```

既存の証明書をインポートする

以下のいずれかの方法を使用して、既存の証明書をサーバーにインポートできます。

証明書のインポートウィザード

1. PFXファイルをダブルクリックするか、ファイルを右クリックして「**PFXのインストール**」を選択します。これにより、「**証明書のインポートウィザード**」が開きます。
2. 「**ストアの場所**」で、「**ローカルコンピューター**」を選択します。

   証明書のインポートウィザードのスクリーンショット(/en-us/citrix-virtual-apps-desktops/2503/media/certificate-import-wizard.png)
3. 必要に応じてパスワードを入力します。

   証明書のインポートウィザード、秘密キーの保護手順のスクリーンショット(/en-us/citrix-virtual-apps-desktops/2503/media/key-protection.png)
4. **証明書ストア** を選択します。サーバー証明書の場合は、**個人** を選択します。これがこのマシンから信頼したいルート証明書または自己署名証明書である場合は、**信頼されたルート証明機関** を選択します。

   証明書のインポートウィザード、証明書ストアの手順のスクリーンショット(/en-us/citrix-virtual-apps-desktops/2503/media/certificate-store.png)

コンピューター証明書の管理コンソールを使用する

1. コンピューター証明書の管理コンソールを開き、適切な証明書ストアに移動します。サーバー証明書の場合、通常は「**個人**」 > 「**証明書**」です。ルート証明書または自己署名証明書を信頼するには、「**信頼されたルート証明機関**」 > 「**証明書**」を選択します。
2. 証明書を右クリックし、「**すべてのタスク**」>「**インポート...**」を選択します。

   コンピューター証明書の管理コンソール(/en-us/citrix-virtual-apps-desktops/2503/media/manage-computer-certificates-console.png)
3. 「**参照...**」を選択し、ファイルを選択します。
4. 必要に応じてパスワードを入力します。

PowerShell を使用する

証明書をインポートするには、PowerShell コマンドレット Import-PfxCertificate を使用します。たとえば、パスワード `123456` を使用して証明書 `certificate.pfx` を個人証明書ストアにインポートするには、次のコマンドを実行します。

```
Import-PfxCertificate -Password $(ConvertTo-SecureString -String "123456"
-AsPlainText -Force) -CertStoreLocation Cert:\LocalMachine\My\ -FilePath .
\Desktop\certificate.pfx
```

信頼されたルート証明書をインポートするには、`CertStoreLocation` を `Cert:\LocalMachine\Root\` に設定します。

秘密キーなしで証明書をエクスポートする

証明書を他のデバイスにインポートして信頼できるようにエクスポートするには、秘密キーを除外する必要があります。

1. コンピューター証明書の管理を開きます。「**個人**」>「**証明書**」に移動し、エクスポートする証明書を選択します。
2. 「**操作**」メニューから「**すべてのタスク**」を選択し、次に「**エクスポート**」を選択します。

   エクスポートメニューのある証明書管理のスクリーンショット(/en-us/citrix-virtual-apps-desktops/2503/media/certificate-export.png)
3. 「**いいえ、秘密キーをエクスポートしません**」を選択し、「**次へ**」を押します。

   証明書のエクスポート(/en-us/citrix-virtual-apps-desktops/2503/media/certificate-export-no-private-key.png)

4. 形式「**DER encoded binary X.509 (.CER)**」（デフォルト）を選択し、「**次へ**」を押します。
5. ファイル名を入力し、「**次へ**」を押します。

   「証明書のエクスポートウィザード、ファイル名」のスクリーンショット(/en-us/citrix-virtual-apps-desktops/2503/media/certificate-export-file.png)
6. 「**完了**」を選択します。

   「証明書のエクスポートウィザード、エクスポート成功」のスクリーンショット(/en-us/citrix-virtual-apps-desktops/2503/media/certificate-export-complete.png)

秘密キーを含む証明書のエクスポート

証明書を他のサーバーで使用できるようにエクスポートするには、秘密キーを含める必要があります。

1. コンピューター証明書の管理を開きます。「**個人**」>「**証明書**」に移動し、エクスポートする証明書を選択します。
2. 「**操作**」メニューから「**すべてのタスク**」を選択し、次に「**エクスポート**」を選択します。

   「エクスポート」メニューを含む証明書管理のスクリーンショット(/en-us/citrix-virtual-apps-desktops/2503/media/certificate-export.png)
3. 「**はい、秘密キーをエクスポートします**」を選択し、次に「**次へ**」を選択します。

   「証明書のエクスポート」(/en-us/citrix-virtual-apps-desktops/2503/media/certificate-export-private-key.png)
4. 「**セキュリティ**」タブでパスワードを入力し、「**次へ**」を選択します。

   「証明書のエクスポートウィザード、セキュリティ手順」のスクリーンショット(/en-us/citrix-virtual-apps-desktops/2503/media/certificate-export-password.png)
5. ファイル名を入力し、「**次へ**」を選択します。

   「証明書のエクスポートウィザード、ファイル名」のスクリーンショット(/en-us/citrix-virtual-apps-desktops/2503/media/certificate-export-file.png)
6. 「**完了**」を選択します。

   証明書のエクスポートウィザード、エクスポート成功のスクリーンショット](/en-us/citrix-virtual-apps-desktops/2503/media/certificate-export-complete.png)

証明書をPEM形式に変換する

デフォルトでは、Windowsは秘密鍵を含む.pfxファイルとして、PKCS#12形式で証明書をエクスポートします。NetScaler® Gatewayまたはライセンスサーバーで証明書を使用するには、証明書と秘密鍵をPEM形式の別々のファイルに抽出する必要があります。これはopensslを使用して実行できます。

証明書をPEM形式でエクスポートするには、以下を実行します。

```
openssl pkcs12 -in name.pfx -clcerts -nokeys -out name.cer
```

既存のパスワードと新しいパスフレーズの入力を求められます

キーをPEM形式でエクスポートするには、以下を実行します。

```
openssl pkcs12 -in name.pfx -nocerts -out name.key
```

証明書の信頼

- パブリック認証局からの証明書を使用する場合、デバイスには通常、ルート証明書が事前に構成されています。
- エンタープライズ認証局を使用する場合、その証明書を信頼する必要があるすべてのデバイスにルート証明書を展開する必要があります。Active Directory証明書サービスを使用している場合、ルート証明書はグループポリシーを使用してドメイン上のすべてのマシンにも展開されます。NetScaler Gatewayや他のドメイン上のマシンなど、ドメインに参加していないマシンには、ルート証明書を手動でインポートする必要があります。
- 自己署名証明書を使用している場合は、その証明書を信頼する必要があるすべてのマシンに手動でインストールする必要があります。

Windowsから自己署名証明書または信頼されたルート証明書をエクスポートするには、秘密鍵なしで証明書をエクスポートするを参照してください。

Windowsが証明書を信頼するようにするには、**信頼されたルート証明機関**ストアに証明書をインポートする必要があります。PowerShellを使用する場合は、ストア**Cert:\\LocalMachine\Root**を入力します。

NetScalerが証明書を信頼するようにするには、まず証明書をPEM形式に変換する、次にルート証明書をインストールする必要があります。

スマートカード

スマートカードおよび同等のテクノロジーは、この記事で説明されているガイドライン内でサポートされています。Citrix Virtual AppsまたはCitrix Virtual Desktops™でスマートカードを使用するには、次の手順を実行します。

- スマートカードの使用に関する組織のセキュリティポリシーを理解します。これらのポリシーには、たとえば、スマートカードの発行方法やユーザーがスマートカードを保護する方法が記載されている場合があります。これらのポリシーの一部は、Citrix Virtual Apps™またはCitrix Virtual Desktops環境で再評価する必要がある場合があります。
- スマートカードで使用するユーザーデバイスの種類、オペレーティングシステム、および公開アプリケーションを決定します。
- スマートカードテクノロジーと、選択したスマートカードベンダーのハードウェアおよびソフトウェアについて理解します。
- 分散環境でデジタル証明書を展開する方法を把握します。

> **注:**

> (/ja-jp/citrix-virtual-apps-desktops/2503/secure/smart-cards.html#fast-smart-card)ではスマートカードの登録はサポートされていません。スマートカードの登録は、高速スマートカードが無効になっている場合に機能する可能性がありますが、スマートカードとミドルウェアの種類によって異なります。Citrix Virtual Apps and Desktopsとの統合および仮想セッションを介したスマートカード登録のサポートについては、スマートカードおよびミドルウェアベンダーにお問い合わせください。

スマートカードの種類

エンタープライズスマートカードとコンシューマースマートカードは、同じ寸法、電気コネクタを持ち、同じスマートカードリーダーに適合します。

エンタープライズ用途のスマートカードには、デジタル証明書が含まれています。これらのスマートカードはWindowsログオンをサポートし、ドキュメントや電子メールのデジタル署名および暗号化用のアプリケーションでも使用できます。Citrix Virtual Apps and Desktops™はこれらの用途をサポートしています。

コンシューマー用途のスマートカードにはデジタル証明書は含まれていません。共有シークレットが含まれています。これらのスマートカードは、支払い（チップアンドシグネチャーまたはチップアンドPINクレジットカードなど）をサポートできます。Windowsログオンや一般的なWindows

アプリケーションはサポートしていません。これらのスマートカードで使用するには、特殊なWindowsアプリケーションと適切なソフトウェアインフラストラクチャ（たとえば、支払いカードネットワークへの接続を含む）が必要です。Citrix Virtual AppsまたはCitrix Virtual Desktopsでこれらの特殊なアプリケーションをサポートする方法については、Citrix担当者にお問い合わせください。

企業向けスマートカードには、同様の方法で使用できる互換性のある同等品があります。

- スマートカードと同等のUSBトークンは、USBポートに直接接続します。これらのUSBトークンは通常、USBフラッシュドライブと同じくらいのサイズですが、携帯電話で使用されるSIMカードと同じくらい小さい場合もあります。これらは、スマートカードとUSBスマートカードリーダーの組み合わせとして表示されます。
- Windows Trusted Platform Module (TPM)を使用する仮想スマートカードは、スマートカードとして表示されます。これらの仮想スマートカードは、Citrix Workspace app（最小バージョンCitrix Receiver 4.3）を使用するWindows 8およびWindows 10でサポートされています。
    - Citrix Virtual Apps and Desktops (旧 XenApp および XenDesktop) の XenApp および XenDesktop 7.6 FP3 以前のバージョンは、仮想スマートカードをサポートしていません。
    - 仮想スマートカードの詳細については、「仮想スマートカードの概要」を参照してください。

    注：「仮想スマートカード」という用語は、ユーザーコンピューターに保存されているデジタル証明書を指す場合もあります。これらのデジタル証明書は、厳密にはスマートカードと同等ではありません。

Citrix Virtual Apps and Desktops のスマートカードサポートは、Microsoft Personal Computer/Smart Card (PC/SC) 標準仕様に基づいています。最低要件として、スマートカードおよびスマートカードデバイスは、基盤となる Windows オペレーティングシステムでサポートされており、対象となる Windows オペレーティングシステムを実行しているコンピューターで使用するために、Microsoft Windows Hardware Quality Labs (WHQL) によって承認されている必要があります。ハードウェアの PC/SC 準拠に関する追加情報については、Microsoft のドキュメントを参照してください。他の種類のユーザーデバイスも PS/SC 標準に準拠している場合があります。詳細については、「Citrix Ready プログラム」を参照してください。

通常、各ベンダーのスマートカードまたは同等のものには、個別のデバイスドライバーが必要です。ただし、スマートカードが NIST Personal Identity Verification (PIV) 標準などの標準に準拠している場合、さまざまなスマートカードに単一のデバイスドライバーを使用できる可能性があります。デバイスドライバーは、ユーザーデバイスと Virtual Delivery Agent (VDA) の両方にインストールする必要があります。デバイスドライバーは、Citrix パートナーから入手できるスマートカードミドルウェアパッケージの一部として提供されることがよくあります。スマートカードミド

ルウェアパッケージは、高度な機能を提供します。デバイスドライバーは、Cryptographic Service Provider (CSP)、Key Storage Provider (KSP)、またはミニドライバーとも呼ばれます。

Windows システム向けの以下のスマートカードとミドルウェアの組み合わせは、その種類の代表的な例として Citrix によってテストされています。ただし、他のスマートカードとミドルウェアも使用できます。Citrix 互換のスマートカードとミドルウェアの詳細については、`<http://www.citrix.com/ready>` を参照してください。

ミドルウェア	対応カード
Gemalto .NET カード用ミニドライバー	ジェムアルト .NET v2+

他の種類のデバイスでのスマートカードの使用については、そのデバイスの Citrix Workspace™ アプリのドキュメントを参照してください。

リモートPCアクセス

スマートカードは、Windows 10、Windows 8、または Windows 7 を実行している物理的なオフィス PC へのリモートアクセスでのみサポートされます。

Remote PC Access でテストされたスマートカードは次のとおりです。

ミドルウェア	対応カード
Gemalto .NET ミニドライバー	ジェムアルト .NET v2+

高速スマートカード

高速スマートカードは、既存のHDX PC/SCベースのスマートカードリダイレクトに対する改善です。スマートカードが高遅延のWAN環境で使用される場合のパフォーマンスを向上させます。遅延が大きい場合、パフォーマンスの向上は著しいものになります（例: Windows高速スマートカードログオンでは15秒、PC/SCベースのスマートカードリダイレクトでは1分以上）。

高速スマートカードは、現在サポートされているWindows VDAを搭載したホストマシンでデフォルトで有効になっています。ホスト側で高速スマートカードを無効にするには（診断目的など）、レジストリ設定「Disable Cryptographic Redirection」をゼロ以外の値に設定します。

```
HKLM\SOFTWARE\Citrix\SmartCard

CryptographicRedirectionDisable (DWORD)
```

クライアント側で高速スマートカードを有効にするには、関連付けられたStoreFrontサイトの *default.ica* ファイルにSmartCardCryptographicRedirection ICAパラメーターを含めます。

```
[WFClient]

SmartCardCryptographicRedirection=On
```

さらに、クライアント側では、以下のレジストリ設定により、高速スマートカードを強制的に有効または無効にすることができます（診断目的など）。

- HKLM\SOFTWARE\Citrix\ICA Client\SmartCard\ForceEnableCryptographicRedirection（ゼロ以外のDWORDとして）

または

- HKLM\SOFTWARE\Citrix\ICA Client\SmartCard\ForceDisableCryptographicRedirection（ゼロ以外のDWORDとして）

クライアントマシンが64ビットの場合、32ビットレジストリハイブを(`WOW6432Node`を使用して)指定する必要があります。

制限事項:

- Citrix Workspaceアプリ for Windowsのみが高速スマートカードをサポートします。default.icaファイルで高速スマートカードを構成した場合でも、Windows用ではないCitrix Workspaceアプリは、既存のPC/SCリダイレクトを依然として使用します。
- 高速スマートカードがサポートする唯一のダブルホップシナリオは、両方のホップで高速スマートカードが有効になっているICA® > ICAです。高速スマートカードはICA > RDPのダブルホップシナリオをサポートしないため、これらのシナリオは機能しません。
- 高速スマートカードは次世代暗号化をサポートしていません。そのため、楕円曲線暗号 (ECC) スマートカードもサポートしていません。
- 高速スマートカードは、読み取り専用キーコンテナ操作のみをサポートしています。
- 高速スマートカードは、スマートカードPINの変更をサポートしていません。

VDAバージョン2203およびWindows向けCitrix Workspaceアプリバージョン2202以降では、高速スマートカードは次世代暗号化 (CNG) と互換性があります。さらに、楕円曲線暗号 (ECC) スマートカードは、ECDSAとECDHの両方で、P-256、P-384、P-521ビットの以下の曲線でサポートされています。

VDAバージョン2203以降、高速スマートカードは、同じユーザーのログオンセッション内のアプリケーション間でスマートカードPINをキャッシュする機能を追加します。たとえば、**セッションPINキャッシュ**が有効になっていて、エンドユーザーが以前にOutlookにスマートカードPINを提供している場合、その後Wordを使用してドキュメントに署名すると、Wordはすでにキャッシュされているスマートカードpin (Outlookに送信されたもの) を使用します。**セッションPINキャッシュ**は、ユーザーがスマートカードPINを入力する回数を減らすことで、ユーザーエクスペリエンスを向上させます。さらに、スマートカードがVDAへのログオンに使用される場合、Windowsスマートカードログオンpinは、オプションで**セッションPINキャッシュ**に保存できます。これにより、ユーザーエクスペリエンスがさらに向上します。

セッションPINキャッシュはデフォルトで無効になっています。VDA上の以下のレジストリ設定で有効化および制御できます。

HKLM\SOFTWARE\Citrix\SmartCard内:

- `EnablePinSessionCache` をDWORDとして (有効にするにはゼロ以外)
- `EnableLogonPinSessionCache` をDWORDとして (有効にするにはゼロ以外)
- `PinSessionCacheEntryStaleTimeout` をDWORDとして (エントリが古くなるまでの秒数、デフォルトは1時間)

スマートカードリーダーの種類

スマートカードリーダーは、ユーザーデバイスに内蔵されている場合や、ユーザーデバイスに別途接続されている場合があります (通常はUSBまたはBluetooth経由)。USBチップ/スマートカードインターフェースデバイス (CCID) 仕様に準拠する接触型カードリーダーがサポートされています。これらには、ユーザーがスマートカードを挿入するスロットまたはスワイプがあります。ドイツ信用経済 (DK) 規格は、接触型カードリーダーの4つのクラスを定義しています。

- クラス1スマートカードリーダーは最も一般的で、通常はスロットを備えています。クラス1スマートカードリーダーはサポートされており、通常、オペレーティングシステムに付属の標準CCIDデバイスドライバーで使用できます。
- クラス2スマートカードリーダーには、ユーザーデバイスからアクセスできないセキュアキーパッドも含まれています。クラス2スマートカードリーダーは、セキュアキーパッドが統合されたキーボードに組み込まれている場合があります。クラス2スマートカードリーダーについては、Citrix担当者にお問い合わせください。セキュアキーパッド機能を有効にするには、リーダー固有のデバイスドライバーが必要になる場合があります。
- クラス3スマートカードリーダーには、セキュアディスプレイも含まれています。クラス3スマートカードリーダーはサポートされていません。

- クラス4スマートカードリーダーはセキュアトランザクションモジュールも搭載しています。クラス4スマートカードリーダーはサポートされていません。

> **注:**
>
> スマートカードリーダーのクラスは、USBデバイスクラスとは関係ありません。

> スマートカードリーダーは、対応するデバイスドライバーをインストールしてユーザーデバイスにインストールする必要があります。

サポートされているスマートカードリーダーについては、使用しているCitrix Workspaceアプリのドキュメントを参照してください。Citrix Workspaceアプリのドキュメントでは、サポートされているバージョンはスマートカードに関する記事またはシステム要件に関する記事に記載されています。

ユーザーエクスペリエンス

スマートカードのサポートはCitrix Virtual Apps and Desktopsに統合されており、デフォルトで有効になっている特定のICA/HDXスマートカード仮想チャネルを使用します。

重要: スマートカードリーダーに汎用USBリダイレクトを使用しないでください。これはスマートカードリーダーではデフォルトで無効になっており、有効にしてもサポートされません。

複数のスマートカードと複数のリーダーを同じユーザーデバイスで使用できますが、パススルー認証を使用している場合は、ユーザーが仮想デスクトップまたはアプリケーションを起動するときに、スマートカードは1枚のみ挿入されている必要があります。アプリケーション内でスマートカードを使用する場合（デジタル署名や暗号化機能など）、スマートカードの挿入やPINの入力を求めるプロンプトが他に表示されることがあります。これは、複数のスマートカードが同時に挿入されている場合に発生する可能性があります。

- スマートカードがすでにリーダーに挿入されているにもかかわらず、スマートカードの挿入を求めるプロンプトが表示された場合、ユーザーは［キャンセル］を選択する必要があります。
- PINの入力を求められた場合、ユーザーはPINを再度入力する必要があります。

PINは、カード管理システムまたはベンダーユーティリティを使用してリセットできます。

> **重要:**

> Citrix Virtual AppsまたはCitrix Virtual Desktopsセッション内で、Microsoftリモートデスクトップ接続アプリケーションでスマートカードを使用することはサポートされていません。これは「ダブルホップ」の使用と呼ばれることがあります。

スマートカードを展開する前に

- スマートカードリーダー用のデバイスドライバーを入手し、ユーザーデバイスにインストールします。多くのスマートカードリーダーは、Microsoftが提供するCCIDデバイスドライバーを使用できます。
- スマートカードベンダーからデバイスドライバーと暗号化サービスプロバイダー（CSP）ソフトウェアを入手し、ユーザーデバイスと仮想デスクトップの両方にインストールします。ドライバーとCSPソフトウェアは、Citrix Virtual Apps and Desktopsと互換性がある必要があります。互換性については、ベンダーのドキュメントを確認してください。ミニドライバーモデルをサポートおよび使用するスマートカードを使用する仮想デスクトップの場合、スマートカードミニドライバーは自動的にダウンロードされますが、http://catalog.update.microsoft.comまたはベンダーから入手することもできます。また、PKCS#11ミドルウェアが必要な場合は、カードベンダーから入手してください。
- 重要：Citrixは、Citrixソフトウェアをインストールする前に、物理コンピューターにドライバーとCSPソフトウェアをインストールしてテストすることを推奨します。
- Windows 10でInternet Explorerを使用してスマートカードを使用するユーザーのために、Citrix Receiver™ for WebのURLを信頼済みサイトリストに追加します。Windows 10では、信頼済みサイトの場合、Internet Explorerはデフォルトで保護モードで実行されません。
- 公開鍵インフラストラクチャ（PKI）が適切に構成されていることを確認します。これには、Active Directory環境で証明書からアカウントへのマッピングが正しく構成されており、ユーザー証明書の検証が正常に実行できることを確認することが含まれます。
- 展開が、Citrix WorkspaceアプリやStoreFrontなど、スマートカードで使用される他のCitrixコンポーネントのシステム要件を満たしていることを確認します。
- サイト内の以下のサーバーへのアクセスを確保します。
    - スマートカード上のログオン証明書に関連付けられているユーザーアカウントのActive Directoryドメインコントローラー
    - デリバリーコントローラー™
    - Citrix ストアフロント
    - Citrix ゲートウェイ/Citrix アクセス ゲートウェイ 10.x
    - VDA

- （Remote PC Accessの場合、オプション）：Microsoft Exchange Server

スマートカードの使用を有効にする

ステップ 1. カード発行ポリシーに従って、ユーザーにスマートカードを発行します。

ステップ2. (オプション) リモートPCアクセスでユーザーを有効にするためにスマートカードを設定します。

ステップ3. Delivery ControllerとStoreFrontをインストールして構成します（まだインストールされていない場合）。これはスマートカードのリモート処理用です。

ステップ4. スマートカードの使用のためにStoreFrontを有効にします。詳細については、StoreFrontのドキュメントの「スマートカード認証の構成」を参照してください。

ステップ5. スマートカードの使用のためにCitrix Gateway/Access Gatewayを有効にします。詳細については、NetScalerのドキュメントの「認証と承認の構成」および「Web Interfaceを使用したスマートカードアクセスの構成」を参照してください。

ステップ6. スマートカードの使用のためにVDAを有効にします。

- VDAに必要なアプリケーションと更新プログラムがあることを確認します。
- ミドルウェアをインストールします。
- スマートカードのリモート処理を設定し、ユーザーデバイス上のCitrix Workspaceアプリと仮想デスクトップセッションの間でスマートカードデータの通信を有効にします。

ステップ7. スマートカードの使用のためにユーザーデバイス（ドメイン参加済みまたは非ドメイン参加済みマシンを含む）を有効にします。詳細については、StoreFrontのドキュメントの「スマートカード認証の構成」を参照してください。

- 証明機関のルート証明書と発行証明機関の証明書をデバイスのキーストアにインポートします。
- ベンダーのスマートカードミドルウェアをインストールします。
- Windows用Citrix Workspaceアプリをインストールして構成し、Group Policy Management Consoleを使用してicaclient.admをインポートし、スマートカード認証を有効にしてください。

ステップ8. 展開をテストします。テストユーザーのスマートカードで仮想デスクトップを起動し、展開が正しく構成されていることを確認します。可能なすべてのアクセスメカニズム（たとえば、Internet ExplorerおよびCitrix Workspaceアプリを介したデスクトップへのアクセス）をテストします。

スマートカードリーダーの挿入回数を追跡する

スマートカードのリモート処理では、SCardGetStatusChange関数を使用して、スマートカードがリーダーに挿入または取り外された回数を追跡できます。この関数は、監視するリーダーごとに1つずつ、SCARD_READERSTATEデータ構造の配列を更新します。各SCARD_READERSTATEのdwEventStateフィールドの上位ワード（16ビット）には、リーダーカウントが含まれます。詳細については、Microsoftの記事「SCardGetStatusChangeA function」および「SCARD_READERSTATEA structure」を参照してください。

「**リーダー挿入回数レポート**」設定はデフォルトで無効になっています。追跡を有効にするには、次のレジストリキーを追加します。

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartCard

名前: EnableReaderInsertCountReporting

種類: DWORD

値: ゼロ以外の任意の値

セッションが切断されると、カウントはゼロにリセットされます。

「**リーダー挿入回数レポート**」は、サードパーティのスマートカードミドルウェアと互換性があります。

スマートカードの展開

この製品バージョンおよびこのバージョンを含む混在環境では、以下の種類のスマートカード展開がサポートされています。その他の構成は機能する可能性がありますが、サポートされていません。

タイプ	STOREFRONT™ 接続
ローカルのドメイン参加済みコンピューター	直接接続
ドメイン参加済みコンピューターからのリモートアクセス	Citrix Gateway経由で接続
ドメインに参加していないコンピューター	直接接続
ドメインに参加していないコンピューターからのリモートアクセス	Citrix Gateway経由で接続

タイプ	STOREFRONT™ 接続
ドメインに参加していないコンピューターおよびDesktop Applianceサイトにアクセスするシンクライアント	Desktop Applianceサイト経由で接続
ドメイン参加済みコンピューターおよびXenApp® Services URL経由でStoreFrontにアクセスするシンクライアント	XenApp Services URL を介して接続

展開タイプは、スマートカードリーダーが接続されているユーザーデバイスの特性によって定義されます。

- デバイスがドメイン参加済みか、非ドメイン参加済みか。
- デバイスがStoreFrontにどのように接続されているか。
- 仮想デスクトップとアプリケーションを表示するためにどのソフトウェアが使用されているか。

さらに、Microsoft WordやMicrosoft Excelなどのスマートカード対応アプリケーションをこれらの展開で使用できます。これらのアプリケーションを使用すると、ユーザーはドキュメントにデジタル署名したり、暗号化したりできます。

バイモーダル認証

これらの展開のそれぞれで可能な場合、Receiverは、スマートカードの使用とユーザー名およびパスワードの入力のいずれかを選択できるようにすることで、バイモーダル認証をサポートします。これは、スマートカードが使用できない場合（たとえば、ユーザーが自宅に忘れた場合やログオン証明書の有効期限が切れた場合など）に役立ちます。

ドメインに参加していないデバイスのユーザーはReceiver for Windowsに直接ログオンするため、ユーザーが明示的な認証にフォールバックできるようにすることができます。バイモーダル認証を構成すると、ユーザーは最初にスマートカードとPINを使用してログオンするように求められますが、スマートカードに問題が発生した場合は明示的な認証を選択するオプションがあります。

Citrix Gatewayを展開する場合、ユーザーは自分のデバイスにログオンし、Receiver for WindowsによってCitrix Gatewayへの認証を求められます。これは、ドメイン参加済みデバイスと非ドメイン参加済みデバイスの両方に適用されます。ユーザーは、スマートカードとPIN、または明示的な資格情報のいずれかを使用してCitrix Gatewayにログオンできます。これにより、Citrix Gatewayログオンに対してバイモーダル認証をユーザーに提供できます。Citrix GatewayからStoreFrontへの

パススルー認証を構成し、スマートカードユーザーの資格情報検証をCitrix Gatewayに委任することで、ユーザーはStoreFrontにサイレント認証されます。

複数のActive Directoryフォレストに関する考慮事項

Citrix環境では、スマートカードは単一のフォレスト内でサポートされます。フォレストをまたがるスマートカードログオンには、すべてのユーザーアカウントへの直接的な双方向フォレスト信頼が必要です。スマートカードを含むより複雑なマルチフォレスト展開（つまり、信頼が一方通行であるか、異なるタイプである場合）はサポートされていません。

リモートデスクトップを含むCitrix環境でスマートカードを使用できます。この機能は、ローカル（スマートカードが接続されているユーザーデバイス上）またはリモート（ユーザーデバイスが接続するリモートデスクトップ上）にインストールできます。

スマートカード取り外しポリシー

製品に設定されているスマートカード取り外しポリシーは、セッション中にリーダーからスマートカードを取り外した場合に何が起こるかを決定します。スマートカード取り外しポリシーは、Windowsオペレーティングシステムを介して構成および処理されます。

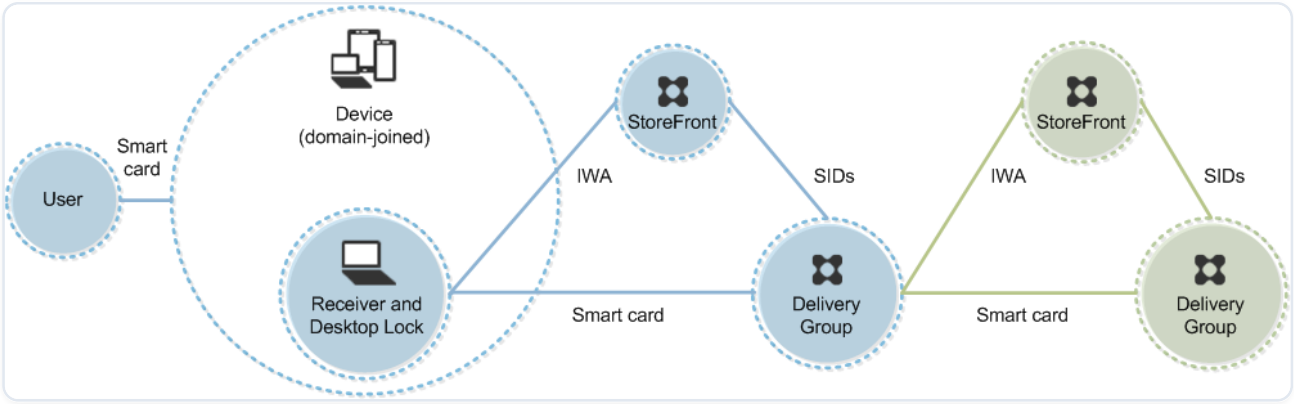
ポリシー設定	デスクトップの動作
アクションなし	アクションなし。
ワークステーションをロック	デスクトップセッションは切断され、仮想デスクトップはロックされます。
強制ログオフ	ユーザーは強制的にログオフされます。ネットワーク接続が失われ、この設定が有効になっている場合、セッションがログオフされ、ユーザーはデータを失う可能性があります。
リモートターミナルサービスセッションの場合に切断	セッションは切断され、仮想デスクトップはロックされます。

証明書失効チェック

証明書失効チェックが有効になっていて、ユーザーが無効な証明書を含むスマートカードをカードリーダーに挿入した場合、ユーザーは証明書に関連するデスクトップまたはアプリケーションを認証したりアクセスしたりできません。たとえば、無効な証明書がメールの復号化に使用された場合、メールは暗号化されたままになります。認証に使用されるものなど、カード上の他の証明書がまだ有効な場合、それらの機能はアクティブなままです。

展開例：ドメイン参加済みコンピューター

この展開では、Desktop Viewerを実行し、StoreFrontに直接接続するドメイン参加済みユーザーデバイスが使用されます。



ユーザーはスマートカードとPINを使用してデバイスにログオンします。Receiverは、統合Windows認証 (IWA) を使用してユーザーをStoreFrontサーバーに認証します。StoreFrontは、ユーザーセキュリティ識別子 (SID) をCitrix Virtual AppsまたはCitrix Virtual Desktopsに渡します。ユーザーが仮想デスクトップまたはアプリケーションを起動すると、シングルサインオン機能がReceiverで構成されているため、PINの再入力を求められることはありません。

この展開は、2番目のStoreFrontサーバーとアプリケーションをホストするサーバーを追加することで、ダブルホップに拡張できます。仮想デスクトップからのReceiverは、2番目のStoreFrontサーバーに認証します。この2番目の接続には、任意の認証方法を使用できます。最初のホップに示されている構成は、2番目のホップで再利用することも、2番目のホップでのみ使用することもできます。

展開例: ドメイン参加済みコンピューターからのリモートアクセス

この展開には、Desktop Viewerを実行し、Citrix Gateway/Access Gatewayを介してStoreFrontに接続するドメイン参加済みユーザーデバイスが含まれます。

展開例：ドメイン参加済みコンピューターからのリモートアクセス(/en-us/citrix-virtual-apps-desktops/2503/media/smartcard2_1.png)

ユーザーはスマートカードとPINを使用してデバイスにログオンし、その後Citrix Gateway/Access Gatewayに再度ログオンします。この展開ではReceiverがバイモーダル認証を許可しているため、この2回目のログオンはスマートカードとPIN、またはユーザー名とパスワードのいずれかで行うことができます。

ユーザーはStoreFrontに自動的にログオンし、StoreFrontはユーザーセキュリティ識別子 (SID) をCitrix Virtual Apps™またはCitrix Virtual Desktopsに渡します。ユーザーが仮想デスクトップまたは

アプリケーションを起動すると、シングルサインオン機能がReceiverで構成されているため、PINの再入力を求められることはありません。

この展開は、2番目のStoreFrontサーバーとアプリケーションをホストするサーバーを追加することで、ダブルホップに拡張できます。仮想デスクトップからのReceiverは、2番目のStoreFrontサーバーに認証します。この2番目の接続には、任意の認証方法を使用できます。最初のホップに示されている構成は、2番目のホップで再利用することも、2番目のホップでのみ使用することもできます。

展開例：ドメイン非参加コンピューター

この展開には、Desktop Viewerを実行し、StoreFrontに直接接続するドメイン非参加ユーザーデバイスが含まれます。

展開例：ドメイン非参加コンピューター(/en-us/citrix-virtual-apps-desktops/2503/media/smartcard3_1.png)

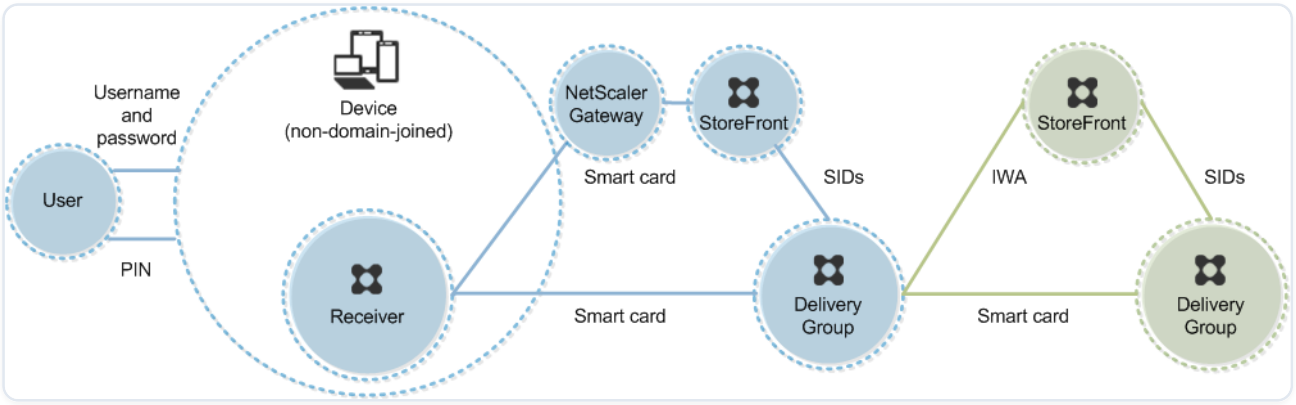
ユーザーはデバイスにログオンします。通常、ユーザーはユーザー名とパスワードを入力しますが、デバイスがドメインに参加していないため、このログオンの資格情報はオプションです。この展開ではバイモーダル認証が可能であるため、Receiverはユーザーにスマートカードと PIN、またはユーザー名とパスワードのいずれかを要求します。その後、ReceiverはStoreFrontに認証します。

StoreFrontは、ユーザーセキュリティ識別子 (SID) をCitrix Virtual AppsまたはCitrix Virtual Desktopsに渡します。ユーザーが仮想デスクトップまたはアプリケーションを起動すると、この展開ではシングルサインオン機能が利用できないため、PINの再入力を求められます。

この展開は、2番目のStoreFrontサーバーとアプリケーションをホストするサーバーを追加することで、ダブルホップに拡張できます。仮想デスクトップからのReceiverは、2番目のStoreFrontサーバーに認証します。この2番目の接続には、任意の認証方法を使用できます。最初のホップに示されている構成は、2番目のホップで再利用することも、2番目のホップでのみ使用することもできます。

展開例：ドメイン非参加コンピューターからのリモートアクセス

この展開では、Desktop Viewer を実行し、StoreFront に直接接続するドメインに参加していないユーザーデバイスが使用されます。



ユーザーはデバイスにログオンします。通常、ユーザーはユーザー名とパスワードを入力しますが、デバイスがドメインに参加していないため、このログオンの資格情報はオプションです。この展開ではバイモーダル認証が可能なため、Receiver はスマートカードとPIN、またはユーザー名とパスワードのいずれかをユーザーに要求します。その後、Receiver は StoreFront に対して認証を行います。

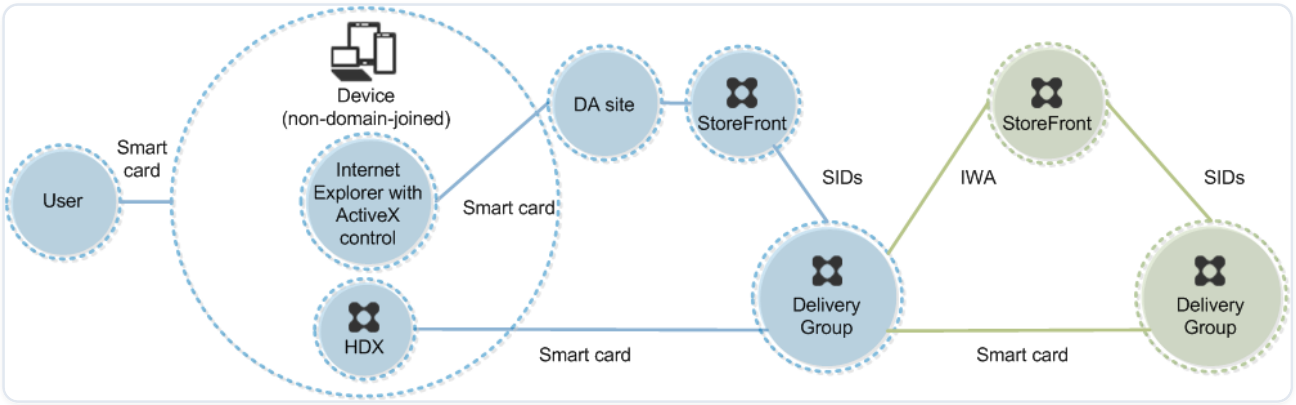
StoreFront はユーザーセキュリティ識別子 (SID) を Citrix Virtual Apps または Citrix Virtual Desktops に渡します。ユーザーが仮想デスクトップまたはアプリケーションを起動すると、この展開ではシングルサインオン機能が利用できないため、ユーザーは再度PINの入力を求められます。

この展開は、2番目のStoreFrontサーバーとアプリケーションをホストするサーバーを追加することで、ダブルホップに拡張できます。仮想デスクトップからのReceiverは、2番目のStoreFrontサーバーに対して認証を行います。この2番目の接続には、任意の認証方法を使用できます。最初のホップで示された構成は、2番目のホップで再利用することも、2番目のホップでのみ使用することもできます。

展開例: ドメインに参加していないコンピューターとシンクライアントがDesktop Applianceサイトにアクセスする

この展開では、Desktop Lock を実行し、Desktop Appliance サイトを介して StoreFront に接続する可能性のあるドメインに参加していないユーザーデバイスが使用されます。

Desktop Lock は、Citrix Virtual Apps、Citrix Virtual Desktops、および VDI-in-a-Box とともにリリースされる個別のコンポーネントです。これは Desktop Viewer の代替であり、主に再利用されたWindowsコンピューターとWindowsシンクライアント向けに設計されています。Desktop Lock は、これらのユーザーデバイスのWindowsシェルとタスクマネージャーを置き換え、ユーザーが基盤となるデバイスにアクセスできないようにします。Desktop Lock を使用すると、ユーザーは Windows Server MachineデスクトップとWindows Desktop Machineデスクトップにアクセスできます。Desktop Lock のインストールはオプションです。



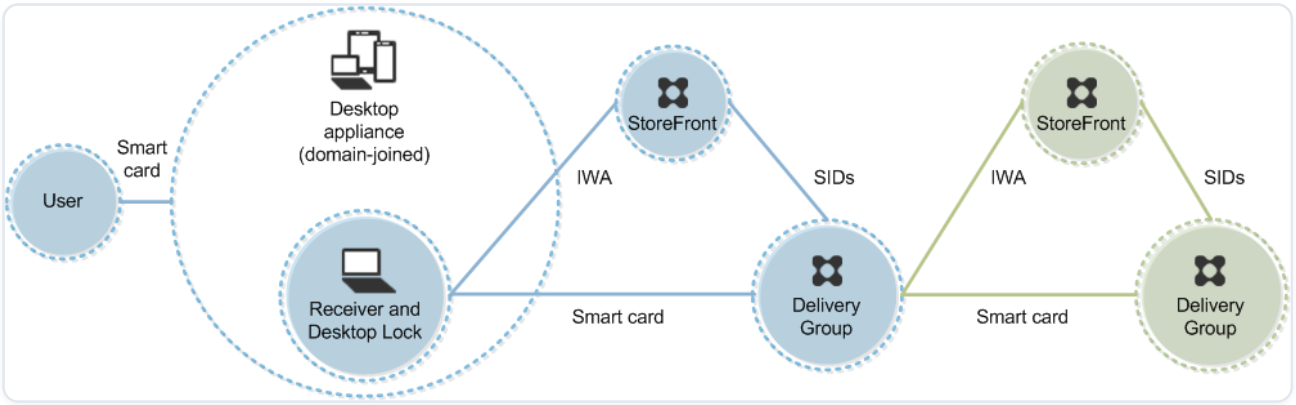
ユーザーはスマートカードを使用してデバイスにログオンします。デバイスでDesktop Lockが実行されている場合、デバイスはキオスクモードで実行されているInternet Explorerを介してDesktop Applianceサイトを起動するように構成されます。サイト上のActiveXコントロールがユーザーにPINを要求し、それをStoreFrontに送信します。StoreFrontはユーザーセキュリティ識別子 (SID) をCitrix Virtual AppsまたはCitrix Virtual Desktopsに渡します。割り当てられたデスクトップグループのアルファベット順リストで最初に利用可能なデスクトップが起動します。

この展開は、2番目のStoreFrontサーバーとアプリケーションをホストするサーバーを追加することで、ダブルホップに拡張できます。仮想デスクトップからのReceiverは、2番目のStoreFrontサーバーに対して認証を行います。この2番目の接続には、任意の認証方法を使用できます。最初のホップで示された構成は、2番目のホップで再利用することも、2番目のホップでのみ使用することもできます。

展開例: ドメインに参加しているコンピューターとシンクライアントがXenApp Services URLを介してStoreFrontにアクセスする

この展開では、Desktop Lock を実行し、XenApp Services URL を介して StoreFront に接続するドメインに参加しているユーザーデバイスが使用されます。

Desktop Lock は、Citrix Virtual Apps、Citrix Virtual Desktops、および VDI-in-a-Box とともにリリースされる個別のコンポーネントです。これは Desktop Viewer の代替であり、主に再利用されたWindowsコンピューターとWindowsシンクライアント向けに設計されています。Desktop Lockは、これらのユーザーデバイスのWindowsシェルとタスクマネージャーを置き換え、ユーザーが基盤となるデバイスにアクセスできないようにします。Desktop Lock を使用すると、ユーザーはWindows Server MachineデスクトップとWindows Desktop Machineデスクトップにアクセスできます。Desktop Lock のインストールはオプションです。



ユーザーはスマートカードとPINを使用してデバイスにログオンします。デバイスでDesktop Lockが実行されている場合、統合Windows認証 (IWA) を使用してStoreFrontサーバーにユーザーを認証します。StoreFrontは、ユーザーセキュリティ識別子 (SID) をCitrix Virtual AppsまたはCitrix Virtual Desktopsに渡します。ユーザーが仮想デスクトップを起動すると、Receiverでシングルサインオン機能が構成されているため、PINの再入力を求められることはありません。

この展開は、2番目のStoreFrontサーバーとアプリケーションをホストするサーバーを追加することで、ダブルホップに拡張できます。仮想デスクトップからのReceiverは、2番目のStoreFrontサーバーに対して認証を行います。この2番目の接続には、任意の認証方法を使用できます。最初のホップに示されている構成は、2番目のホップで再利用することも、2番目のホップでのみ使用することもできます。

スマートカードによるパススルー認証とシングルサインオン

パススルー認証

スマートカードを使用した仮想デスクトップへのパススルー認証は、Windows 10、Windows 8、Windows 7 SP1 Enterprise および Professional Edition を実行しているユーザーデバイスでサポートされています。

スマートカードを使用したホスト型アプリケーションへのパススルー認証は、Windows Server 2012 および Windows Server 2008 R2 SP1 を実行しているサーバーでサポートされています。

スマートカードを使用したホスト型アプリケーションでパススルー認証を使用するには、サイトの認証方法としてスマートカードによるパススルーを構成する際に、Kerberos の使用を有効にしてください。

注：スマートカードによるパススルー認証の利用可否は、以下を含む（ただしこれらに限定されない）多くの要因に依存します。

- パススルー認証に関する組織のセキュリティポリシー。
- ミドルウェアの種類と構成。

- スマートカードリーダーの種類。
- ミドルウェアのPINキャッシュポリシー。

スマートカードによるパススルー認証は、Citrix StoreFront で構成されます。詳細については、StoreFront のドキュメントを参照してください。

シングルサインオン

シングルサインオンは、仮想デスクトップおよびアプリケーションの起動時にパススルー認証を実装する Citrix の機能です。この機能は、ドメイン参加済みでStoreFrontに直接接続するスマートカード展開、およびドメイン参加済みでNetScaler経由でStoreFrontに接続するスマートカード展開で使用でき、ユーザーがPINを入力する回数を減らすことができます。これらの展開タイプでシングルサインオンを使用するには、StoreFrontサーバーにある default.ica ファイルで以下のパラメーターを編集します。

- ドメイン参加済みでStoreFrontに直接接続するスマートカード展開 — DisableCtrlAltDel を Off に設定
- ドメイン参加済みでNetScaler経由でStoreFrontに接続するスマートカード展開 — UseLocalUserAndPassword を On に設定

これらのパラメーターの設定に関する詳細な手順については、StoreFrontまたはCitrix Gatewayのドキュメントを参照してください。

シングルサインオン機能の可用性は、以下を含む（ただしこれらに限定されない）多くの要因に依存します。

- シングルサインオンに関する組織のセキュリティポリシー。
- ミドルウェアの種類と構成。
- スマートカードリーダーの種類。
- ミドルウェアのPINキャッシュポリシー。

> **注:**
>
> ユーザーがスマートカードリーダーが接続されたマシン上のVirtual Delivery Agent (VDA) にログオンすると、スマートカードやパスワードなど、以前に成功した認証モードを表すWindowsタイルが表示されることがあります。その結果、シングルサインオンが有効になっている場合、シングルサインオンタイルが表示されることがあります。ログオンするには、シングルサインオンタイルは機能しないため、ユーザーは別のタイルを選択するために**ユーザーの切り替え**を選択する必要があります。

Delivery ControllerでTLSを有効にする

デフォルトでは、HTTPとHTTPSの両方が有効になっています。HTTPSは、サーバーのFQDNを共通名として使用する自己署名証明書を使用しますが、これはStoreFront™やWebブラウザによって信頼されません。

delivery controller™でTLSを有効にするには、次の操作を行う必要があります。

- すべてのDelivery Controllerでサーバー証明書を取得、インストール、登録します。詳細については、「証明書の要求とインストール」を参照してください。
- TLS証明書を使用してポートを構成します。詳細については、「証明書のインストール」を参照してください。
- 監視サービスでHTTPSを有効にする。
- HTTPを無効にしてHTTPSトラフィックを強制します。詳細については、「HTTPSトラフィックのみを強制する」を参照してください。
- オプションで、ControllerがHTTPおよびHTTPSトラフィックをリッスンするために使用するポートを変更できます。詳細については、「HTTPまたはHTTPSポートの変更」を参照してください。

証明書の要求とインストール

TLSを使用するには、共通名またはサブジェクトの別名がサーバーのFQDNと一致する証明書をインストールする必要があります。delivery controllerの前にロードバランサーを使用している場合は、サーバーとロードバランサーの両方のFQDNをサブジェクトの別名として含めます。詳細については、「証明書」を参照してください。StoreFrontがdelivery controllerに接続するには、RSAデジタル署名アルゴリズムを使用する必要があります。StoreFrontはECDSAアルゴリズムを使用する証明書をサポートしていません。

SSL/TLSリスナーポートの構成

Web StudioおよびDirectorの一部としてインストールされるIIS Windowsコンポーネントが同じサーバーにインストールされている場合は、IISを使用してTLSを構成できます。詳細については、「Web StudioおよびDirectorでTLSを有効にする」を参照してください。それ以外の場合は、PowerShellを使用して証明書を構成するには、次の手順を実行します。

1. 既存の証明書がバインドされているかどうかを確認するには、コマンドプロンプトを開き、`netsh http show sslcert`を実行します。

```
netsh http show sslcert
```

2. 既存のバインドがある場合は、それを削除します。

```
netsh http delete sslcert ipport=0.0.0.0:443
```

既存のバインドで指定されていた場合は、`0.0.0.0:443`を特定のIPアドレスとポートに置き換えます。

3. 以前にインストールした証明書のサムプリントを見つけます。サムプリントを表示するには、**コンピューター証明書の管理**を開き、証明書を参照して開き、**詳細**タブに移動します。

サムプリントを示す証明書のプロパティのスクリーンショット(/en-us/citrix-virtual-apps-desktops/2503/media/certificate-thumbprint.png)

または、PowerShellを使用することもできます。たとえば、次のスクリプトは、共通名がサーバーのホスト名と一致する証明書を検索し、サムプリントを出力します。

```
$HostName =
([System.Net.Dns]::GetHostByName(($env:computerName))).Hostname

$Thumbprint = (Get-ChildItem -Path Cert:\LocalMachine\My | Where-Object
{$_.Subject -match ("CN=" + $HostName)}).Thumbprint -join ';'

Write-Host -Object "Certificate Thumbprint for $($HostName): $
($Thumbprint)" -Foreground Yellow
```

証明書の共通名がホスト名と一致しない場合、これは失敗します。ホスト名に対して複数の証明書がある場合、これは連結された複数のサムプリントを返し、適切なサムプリントを選択する必要があります。

次の例では、フレンドリ名で証明書を検索します。

```
$friendlyName = "My certificate name"

$Thumbprint = (Get-ChildItem -Path Cert:\LocalMachine\My | Where-Object
{$_.FriendlyName -eq $friendlyNam}).Thumbprint -join ';'
```

```
Write-Host -Object "Certificate Thumbprint for $friendlyName: $
($Thumbprint)" -Foreground Yellow
```

指定されたフレンドリ名を持つ証明書が複数ある場合、これは連結された複数のサムプリントを返し、適切なサムプリントを選択する必要があります。

4. 証明書をポートにバインドするには、`netsh http add sslcert`コマンドを使用します。

```
netsh http add sslcert ipport=[IP address]:443 certhash=[certificate
hash] appid=[application GUID] disablelegacytls=enable
```

- `ipport`: IPアドレスとポート。0.0.0.0:443を使用すると、すべてのIPアドレスに適用されます。代わりに、特定のIPアドレスを指定することもできます。
- `certhash`: 前の手順で特定した証明書のサムプリント。
- `appid`: シトリックス ブローカー サービスのグイッド。

> **注:**
>
> 証明書を更新または再バインドする際は、任意のGUIDではなく、Broker Serviceに関連付けられた特定の`appid`を使用してください。
>
> Citrix Broker Serviceの正しい`appid`を見つけるには：

a. 管理者としてPowerShellコマンドウィンドウを開き、次のコマンドを実行します。

```
Get-WmiObject -Class Win32_Product | Select-String -Pattern
"broker"
```

b. 出力でCitrix Broker ServiceのIdentifyingNumber (GUID) を見つけます（例：`{D333C884-187F-447C-8C67-463F33989C8F}`）。このGUIDを`appid`パラメーターに使用します。

- `disablelegacytls=enable`: レガシーバージョンのTLSを無効にします。このパラメーターはWindows 2022以降で利用可能です。Windows 2022ではTLS 1.0と1.1を無効にします。Windows 2025では、TLS 1.0と1.1がデフォルトで無効になっているため、これは不要です。

たとえば、すべてのIPアドレスでサムプリント `bc96f958848639fd101a793b87915d5f2829b0b6` の証明書をポート `443` にバインドするには、次のコマンドを実行します。

```
netsh http add sslcert ipport=0.0.0.0:443
certhash=bc96f958848639fd101a793b87915d5f2829b0b6 appid={91fe7386-
e0c2-471b-a252-1e0a805febac} disablelegacytls=enable
```

HTTPSが有効になったら、StoreFront展開とNetScaler Gatewayを構成して、デリバリーコントローラーへの接続にHTTPではなくHTTPSを使用するようにします。

HTTPS 用のモニターサービス OData API を構成する

モニターサービスは、Citrix®およびサードパーティアプリケーションがデータを照会できるように、OData v3およびv4 APIを提供します。DirectorはOData API V3を使用して監視サービスに接続します。HTTPS用にモニターOData APIを構成するには、次の手順を完了します。

1. 次のPowerShellを実行します。

```
$serviceGroup = Get-ConfigRegisteredServiceInstance -ServiceType
Monitor | Select -First 1 ServiceGroupUid

Remove-ConfigServiceGroup -ServiceGroupUid
$serviceGroup.ServiceGroupUid

& 'C:\Program Files\Citrix\Monitor\Service\citrix.monitor.exe'
-ConfigureFirewall -RequireODataTls –ODataPort 443 -RequireODataSdkTls
–ODataSdkPort 443

get-MonitorServiceInstance | register-ConfigServiceInstance

Get-ConfigRegisteredServiceInstance -ServiceType Config | Reset-
MonitorServiceGroupMembership
```

2. テキストエディターでファイル `C:\Program Files\Citrix\Monitor\Service\Citrix.Monitor.exe.Config` を開きます。要素 `<add key="owin:baseAddress" value="http://localhost/citrix/monitor/odata/v4" />` を見つけて、 `<add key="owin:baseAddress" value="https://localhost/citrix/monitor/odata/v4" />` に変更します。

暗号スイートを構成する

暗号スイートの順序リストには、`TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384`または`TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256`の暗号スイート（またはその両方）を含める必要があります。また、これらの暗号スイートは、`TLS_DHE_`の暗号スイートよりも前に配置する必要があります。

1. Microsoftグループポリシーエディターを使用して、**コンピューターの構成 > 管理用テンプレート > ネットワーク > SSL構成設定**に移動します。
2. 「SSL暗号スイートの順序」ポリシーを編集します。デフォルトでは、このポリシーは「未構成」に設定されています。このポリシーを「有効」に設定します。
3. スイートを正しい順序に並べ替えます。使用したくない暗号スイートはすべて削除します。

`TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384`または`TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256`のいずれかが、`TLS_DHE_`の暗号スイートよりも前に配置されていることを確認してください。

Microsoft Learnで、TLS暗号スイートの順序の構成も参照してください。

HTTPS トラフィックのみを強制する

XML Service が HTTP トラフィックを無視するように構成することをお勧めします。

1. `regedit` を実行します。
2. `HKLM\Software\Citrix\DesktopServer\`を開く
3. `XmlServicesEnableNonSsl`という名前の新しいDWORD値を作成し、0に設定します。
4. Broker Serviceを再起動します。

HTTPSトラフィックを無視するために作成できる対応するレジストリDWORD値`XmlServicesEnableSsl`があります。これが0に設定されていないことを確認してください。

HTTPまたはHTTPSポートを変更する

デフォルトでは、Controller上のXMLサービスは、HTTPトラフィックにはポート80を、HTTPSトラフィックにはポート443をリッスンします。デフォルト以外のポートを使用することもできますが、Controllerを信頼できないネットワークに公開することによるセキュリティリスクに注意してください。デフォルトを変更するよりも、スタンドアロンのStoreFrontサーバーを展開する方が望ましいです。

Controllerで使用されるデフォルトのHTTPまたはHTTPSポートを変更するには、Studioから次のコマンドを実行します。

```
BrokerService.exe -StoreFrontPort <http-port> -StoreFrontTlsPort <https-port>
```

ここで：

- `<http-port>`はHTTPトラフィックのポート番号です
- `<https-port>`はHTTPSトラフィックのポート番号です。

注:

ポートを変更した後、Studioはライセンスの互換性とアップグレードに関するメッセージを表示する場合があります。この問題を解決するには、次のPowerShellコマンドレットシーケンスを使用してサービスインスタンスを再登録します。

```
Get-ConfigRegisteredServiceInstance -ServiceType Broker -Binding XML_HTTPS |

Unregister-ConfigRegisteredServiceInstance

Get-BrokerServiceInstance | where Binding -eq "XML_HTTPS" |

Register-ConfigServiceInstance
```

Web StudioとDirectorでTLSを有効にする

HTTPSを有効にすることで、Web StudioおよびDirectorへの接続を保護するために、常にTLSを使用することをお勧めします。この記事では、Web StudioおよびDirectorが信頼された証明書を使用し、HTTPS経由で安全なアクセスを確保するように構成する方法について説明します。

デフォルトの動作

Web Studioをインストールすると、インストーラーは自己署名証明書を作成し、現在のサーバーのポート443にバインドします。ローカルサーバーでは、WebブラウザーからHTTPS経由でWeb StudioおよびDirectorにアクセスできます。

ただし、別のマシンからHTTPS経由でWeb StudioまたはDirectorにアクセスしようとすると、ブラウザーは証明書を信頼しないため、セキュリティエラーを表示します。

注:

Web StudioなしでDirectorをインストールした場合、インストーラーは自己署名証明書を作成しません。

HTTPS経由で安全なアクセスを有効にする

Web Studioサーバーⅰ以外のマシンからHTTPS経由でWeb StudioまたはDirectorへのアクセスを許可するには、次の手順に従います。

1. 信頼された証明書を作成またはインポートする(#create-or-import-a-trusted-certificate)。
2. IISで証明書をポート443にバインドする(#bind-the-certificate-to-port-443)。
3. （オプション）HTTP Strict Transport Security（HSTS）を有効にする(#optional-enable-http-strict-transport-security-hsts)。
4. Web Studioがプロキシとして構成されていない場合（クライアントマシンがWeb StudioとDelivery Controllerの両方に接続する場合）、Delivery ControllerでTLSを有効にする(/ja-jp/citrix-virtual-apps-desktops/2503/secure/tls-ddc)。

注:

自己署名証明書の使用は、各マシンでの手動構成が必要となるため、推奨されません。詳細については、「自己署名証明書を使用する(#use-the-self-signed-certificate)」を参照してください。

信頼された証明書を作成またはインポートする

サーバーに接続するマシンによって信頼されている、エンタープライズまたはパブリック認証局からの証明書を使用することをお勧めします。

詳細については、「新しい証明書の作成」および「既存の証明書のインポート」を参照してください。証明書の共通名またはサブジェクトの別名は、ユーザーがWeb StudioまたはDirectorに接続するために使用するFQDNと一致している必要があります。サーバーの前にロードバランサーが展開されている場合は、ロードバランサーのFQDNを使用します。

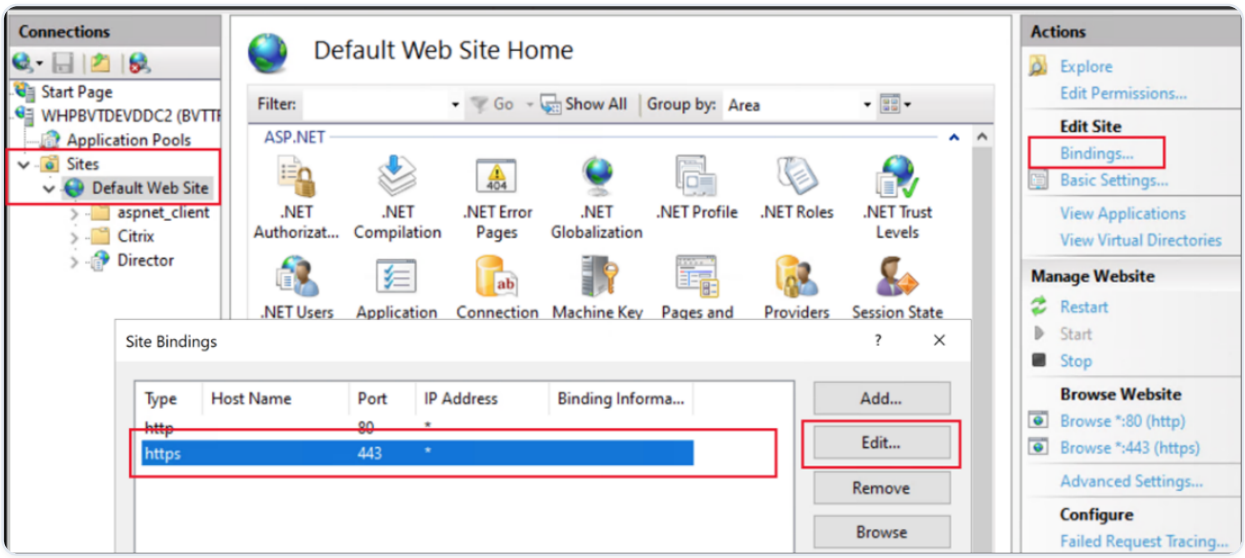
証明書をポート443にバインドする

信頼された証明書を作成またはインポートした後、IISでポート `443` にバインドします。これはインストール前でもインストール後でも実行できます。ポート `443` の証明書バインドがすでに構成されている場合、インストーラーは変更を行いません。

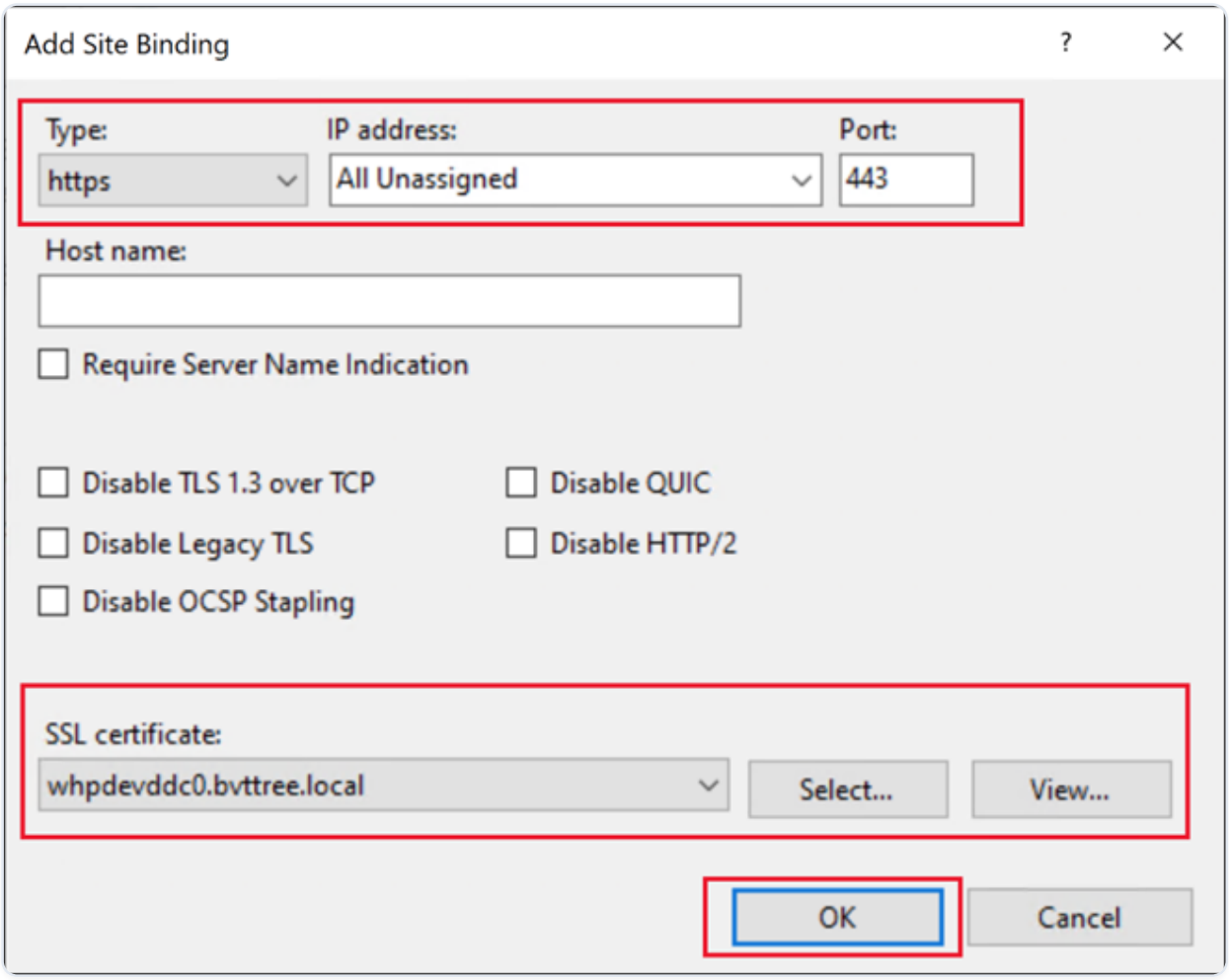
> **注:**
>
> デフォルトでは、Web StudioとDirectorはセキュアなHTTPSアクセスにポート443を使用します。必要に応じてポート番号を変更できます。詳細については、デフォルトのポート番号の変更 を参照してください。

証明書をポート `443` にバインドするには、次の手順に従います。

1. 管理者としてサーバーにログオンします。
2. IISマネージャーを開き、**サイト > 既定のWebサイト > バインド** に移動します。
3. 種類が **https** の既存のバインドがある場合は、それを選択して **編集...** をクリックします。**https** バインドがない場合は、**追加** をクリックします。



4. サイトバインドを作成または編集します。
   a. 新しいバインドの場合、種類を **https** に、ポートを `443` に設定します。
   b. 適切なSSL証明書を選択します。
   c. Windows Server 2022以降では、オプションで **レガシーTLSを無効にする** を選択して、ユーザーが最新のTLSバージョンのみを使用して接続できるようにします。
   d. **OK**をクリックします。



または、PowerShellを使用して証明書を変更することもできます。たとえば、次のスクリプトは、指定された共通名を持つ証明書を検索し、それをすべてのIPアドレス、ポート443にバインドし、レガシーTLSバージョンを無効にします。

```
$certSName = 'CN=whpdevddc0.bvttree.local'  # The subject name of the
certificate

$certificate = Get-ChildItem -Path Cert:\LocalMachine\My\ | ? {$_.Subject
-eq $certSName}

netsh http add sslcert ipport=0.0.0.0:443 certhash=$
($certificate.Thumbprint) certstorename=My appid="{91fe7386-e0c2-471b-
a252-1e0a805febac}" disablelegacytls=enable
```

なお、`appid` は、どのアプリケーションが証明書を追加したかを識別するために使用できる任意の GUID です。

自己署名証明書を使用する

既存の自己署名証明書を使用できますが、サーバーにアクセスする各マシンを手動で構成する必要があるため、推奨されません。

Web Studio に接続する必要があるマシンに自己署名証明書をインストールするには、次の手順を実行します。

1. Web StudioおよびDelivery Controllerサーバーから既存の自己署名証明書をエクスポートします。
2. サーバーにアクセスする必要があるマシンの**信頼されたルート証明書**ストアに証明書をインポートします。

(オプション) HTTP Strict Transport Security (HSTS) を有効にする

HTTP Strict Transport Security (HSTS)は、サイトにアクセスする際にHTTPSのみを使用するようWebブラウザに指示します。ユーザーがHTTPを使用してURLにアクセスしようとすると、ブラウザは自動的にHTTPSに切り替わります。この設定により、クライアント側とサーバー側の両方で安全な接続検証が保証されます。ブラウザは、設定された期間この検証を維持します。

Windows Server 2019 以降では、IIS で HSTS を構成できます。

1. **インターネットインフォメーションサービス (IIS) マネージャー**を開きます。
2. **既定のWebサイト** (または適切なWebサイト) を選択します。
3. 右側の**操作**ペインで、**HSTS...** を選択します。
4. **有効にする**を選択し、最大有効期間を入力します（例: 1年の場合は31536000）。
5. **HTTP を HTTPS にリダイレクト**を選択します。

> **注:**
>
> Web Studio は、Studio Web サイトへのアクセス時に HTTP を HTTPS にリダイレクトする **URL 書き換え**ルールを自動的に構成します。ただし、このオプションは Director および IIS サイト上の他のすべてのアプリケーションにも適用されます。

6. **OK** をクリックします。

HSTS 設定のスクリーンショット(/en-us/citrix-virtual-apps-desktops/2503/media/iis-hsts.png)

(オプション) デフォルトのポート番号を変更する

デフォルトでは、Web Studio と Director はセキュアな HTTPS アクセスにポート 443 を使用します。このポート番号を変更するには、`Default Web Site` で目的のポートのサイトバインディングを作成するために、次の手順に従います。

手順:

1. Web Studio をホストしているサーバーで、**インターネット インフォメーション サービス (IIS) マネージャー**を開きます。
2. **接続**ペインで、サーバーノードを展開し、**サイト**の下にある**既定の Web サイト**を選択します。
3. 右側の**操作**ペインで、**バインド**をクリックします。

   新しいポートを設定(/en-us/citrix-virtual-apps-desktops/2503/media/web-studio-new-port.png)
4. **サイトバインド**ウィンドウで、**追加**をクリックします。
5. 「サイトバインドの追加」ウィンドウで、新しいバインドに対して以下を設定します。

   a. **種類**: **https** を選択します。

   b. **IPアドレス**: 適切なIPアドレスを選択するか、該当する場合は「未割り当てのすべて」のままにします。

   c. **ポート**: 目的のポート番号（例: 444）を入力します。

   d. **SSL証明書**: セキュアな通信のために適切なSSL証明書を選択します。

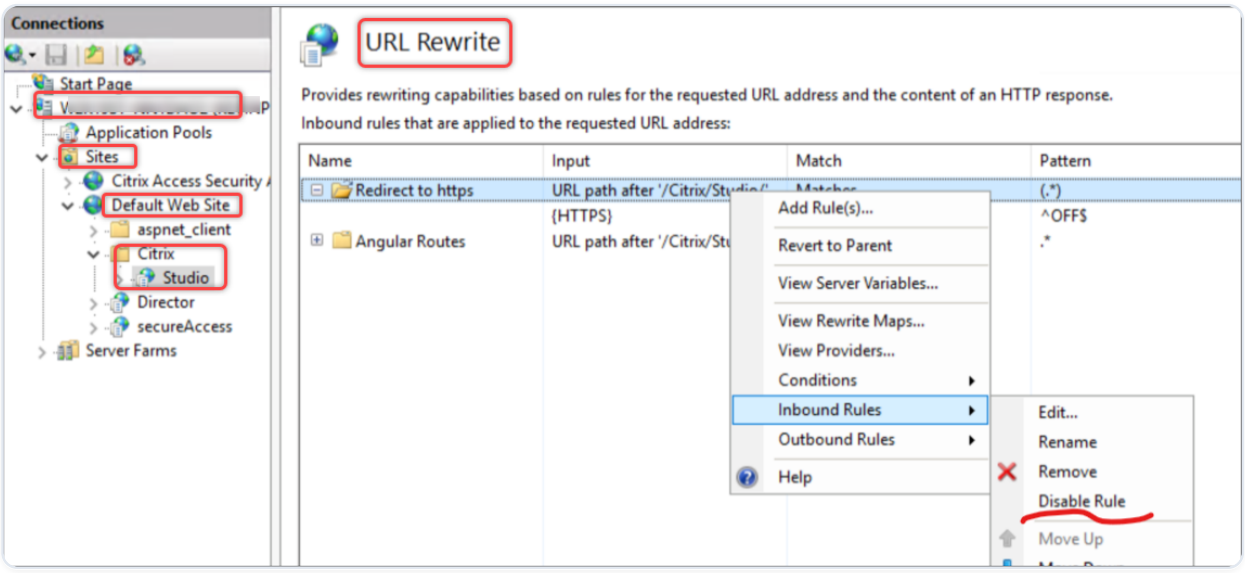
   > **注:**
   >
   > Delivery Controller™ と Web Studio が別々のマシンにインストールされており、サーバーに他のサービスやWebサイトが展開されていない場合は、ポート443を削除できます。それ以外の場合は、オーケストレーションサービスや他のFMAサービスとの通信問題を避けるために、このポートを維持してください。

6. **OK** をクリックしてバインドを保存し、**サイトバインド** ウィンドウを閉じます。
7. **IISマネージャー** で、サーバーノードをクリックし、**操作** ペインで **再起動** をクリックして新しいバインドを適用します。

（オプション）HTTPS リダイレクトを無効にする

Web Studio をインストールすると、デフォルトで、すべてのHTTPアクセスはHTTPSに自動的にリダイレクトされます。このリダイレクトを無効にしてHTTPアクセスを許可することも可能です。この方法は、HTTPアクセスをブロックするための他の対策を講じている場合にのみ推奨されます。Web Studio の前にTLS終端ロードバランサーがある場合でも、ロードバランサーとWeb Studio の間でHTTPSを使用することをお勧めします。

1. Web Studio サーバーにログオンします。
2. **インターネットインフォメーションサービス (IIS) マネージャー** を開き、*Server_name* > **サイト > 既定のWebサイト > URL書き換え** に移動します。
3. 次のスクリーンショットに示すように、**httpsへのリダイレクト** の **受信規則** を無効にします。



IIS で HSTS を有効にしている場合は、**Redirect Http to Https** もクリアする必要があります。

VDAでTLS / DTLSを有効にする

以下のタスクを完了して、Citrix Workspace™ アプリと Virtual Delivery Agent (VDA) 間の TLS 接続を有効にします。

- VDA に証明書をインストールします。詳細については、「証明書のリクエストとインストール」を参照してください。
- VDA がインストールされているマシンで TLS を構成します。(便宜上、VDA がインストールされているマシンは、以降「VDA」と表記します。) TLS/DTLS の構成には、Citrix が提供する PowerShell スクリプトを使用することを強くお勧めします。詳細については、「PowerShell スクリプトを使用した VDA での TLS の構成」を参照してください。ただし、TLS/DTLS を手動で構成する場合は、「VDA での TLS の手動構成」を参照してください。

- Studio で一連の PowerShell コマンドレットを実行して、VDA を含むデリバリーグループで TLS を構成します。詳細については、「デリバリーグループでの TLS の構成」を参照してください。

要件と考慮事項:

- コンポーネントのインストール、サイトの作成、マシンカタログの作成、およびデリバリーグループの作成後に、デリバリーグループと VDA で TLS を構成します。
- デリバリーグループで TLS を構成するには、Controller アクセスルールを変更する権限が必要です。この権限は、フル管理者 (Full Administrator) が持っています。
- VDA で TLS を構成するには、VDA がインストールされているマシンで Windows 管理者である必要があります。
- Machine Creation Services™ または Provisioning Services によってプロビジョニングされたプールされた VDA では、再起動時に VDA マシンイメージがリセットされ、以前の TLS 設定が失われます。VDA が再起動されるたびに PowerShell スクリプトを実行して、TLS 設定を再構成してください。

デリバリーグループには、TLS が構成されている VDA と TLS が構成されていない VDA が混在することはできません。デリバリーグループの TLS を構成する前に、そのデリバリーグループ内のすべての VDA に対して TLS がすでに構成されていることを確認してください。

VDA で TLS を構成すると、インストールされている TLS 証明書のアクセス許可が変更され、ICA® Service に証明書の秘密キーへの読み取りアクセス権が付与され、ICA Service に次の情報が通知されます。

- TLS に使用する証明書ストア内の証明書。
- TLS 接続に使用する TCP ポート番号。

  Windows ファイアウォール (有効な場合) は、この TCP ポートでの受信接続を許可するように構成する必要があります。この構成は、PowerShell スクリプトを使用すると自動的に行われます。
- 許可するTLSプロトコルのバージョン。

> **重要:**
>
> Citrixでは、TLS 1.2以降を使用することをお勧めします。SSLおよび古いバージョンのTLSは非推奨です。

> サポートされているTLSプロトコルバージョンには階層があります（低い方から高い方へ）：SSL 3.0、TLS 1.0、TLS 1.1、TLS 1.2、TLS 1.3。許可される最小バージョンを指定します。そのバージョンまたはそれより高いバージョンを使用するすべてのプロトコル接続が許可されます。

たとえば、最小バージョンとしてTLS 1.1を指定した場合、TLS 1.1、TLS 1.2、およびTLS 1.3プロトコル接続が許可されます。最小バージョンとしてSSL 3.0を指定した場合、サポートされているすべてのバージョンの接続が許可されます。最小バージョンとしてTLS 1.3を指定した場合、TLS 1.3接続のみが許可されます。

- 許可するTLS暗号スイート。

暗号スイートは、接続に使用される暗号化を選択します。クライアントとVDAは、異なる暗号スイートのセットをサポートできます。クライアント（Citrix Workspaceアプリ）が接続し、サポートされているTLS暗号スイートのリストを送信すると、VDAはクライアントの暗号スイートの1つを、自身の構成済み暗号スイートのリストにある暗号スイートの1つと照合し、接続を受け入れます。一致する暗号スイートがない場合、VDAは接続を拒否します。

VDAは、3つの暗号スイートセット（コンプライアンスモードとも呼ばれます）をサポートしています：GOV（政府）、COM（商用）、およびALL。許容される暗号スイートは、Windows FIPSモードにも依存します。Windows FIPSモードの詳細については、`<http://support.microsoft.com/kb/811833>`を参照してください。次の表に、各セットの暗号スイートを示します。

暗号スイート	すべて	COM	GOV	すべて	COM	GOV
FIPSモード	オフ	オフ	オフ	オン	オン	オン
TLS_AES_256_GCM_SHA384	X		X	X		X
TLS_AES_128_GCM_SHA256	X			X		X
TLS_ECDHE_RS	X		X	X		X

暗号スイート	すべて	COM	GOV	すべて	COM	GOV
A_WITH_AES_256_GCM_SHA384						
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	X		X	X		X
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	X	X		X	X	

注記：

VDAはDHE暗号スイート（例：TLS_DHE_RSA_WITH_AES_256_GCM_SHA384、TLS_DHE_RSA_WITH_AES_256_CBC_SHA、TLS_DHE_RSA_WITH_AES_128_GCM_SHA256、TLS_DHE_RSA_WITH_AES_128_CBC_SHA）をサポートしていません。Windowsによって選択された場合、接続は失敗します。

NetScaler Gatewayを使用している場合は、バックエンド通信の暗号スイートサポートに関する情報について、NetScalerのドキュメントを参照してください。TLS暗号スイートのサポートについては、「Citrix ADCアプライアンスで利用可能な暗号」を参照してください。DTLS暗号スイートのサポートについては、「DTLS暗号のサポート」を参照してください。

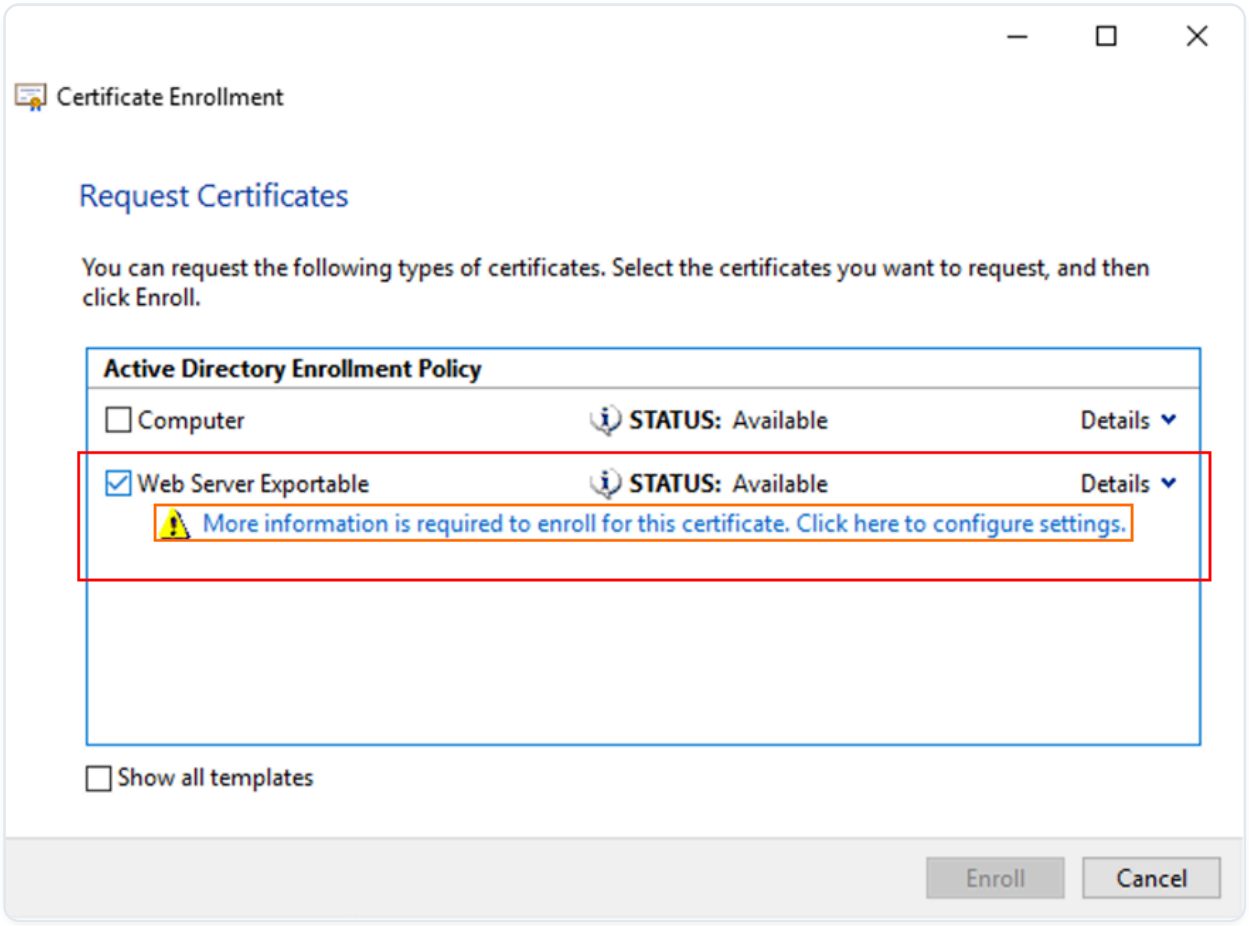
証明書の要求とインストール

TLSを使用するには、代替名にVDAのFQDNが含まれる証明書をインストールする必要があります。この証明書は、VDAに直接接続する（Citrix Gatewayを介さない）すべてのクライアントによって信頼されている必要があります。証明書を簡単に展開できない管理対象外のデバイスがVDAに接続できるようにするには、NetScaler® Gatewayの展開を検討してください。

Microsoft証明機関を使用して証明書を作成する

クライアントとVDAが信頼されたフォレストにあり、Microsoft証明機関がある場合、証明書MMCスナップインの証明書登録ウィザードから証明書を取得できます。

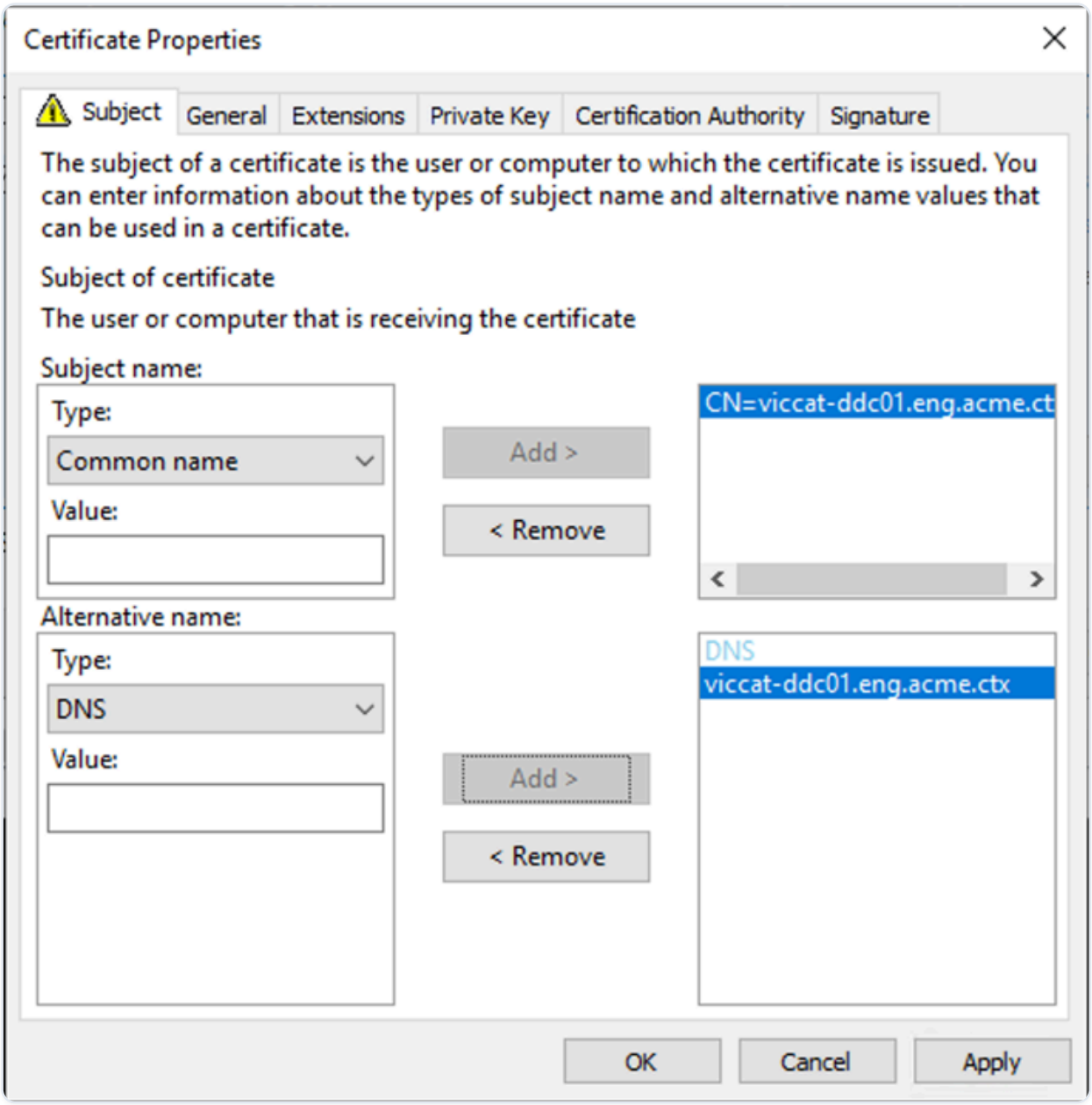
1. VDAで、MMCコンソールを開き、証明書スナップインを追加します。プロンプトが表示されたら、「コンピューターアカウント」を選択します。
2. **個人 > 証明書**を展開し、コンテキストメニューコマンドの**すべてのタスク > 新しい証明書の要求**を使用します。
3. 開始するには**次へ**をクリックし、Active Directory登録から証明書を取得することを確認するために**次へ**をクリックします。
4. サーバー認証証明書のテンプレートを選択します。デフォルトのWindows **コンピューター**または**Webサーバー（エクスポート可能）**のいずれも使用できます。**テンプレートが件名の値を自動的に提供するように設定されている場合は、詳細を指定せずに登録**をクリックできます。



5. 証明書テンプレートのさらに詳細な情報を提供するには、**詳細**をクリックして、以下を構成します。

   サブジェクト名 — タイプ **共通名** を選択し、VDA の FQDN を追加します。

   代替名 — タイプ **DNS** を選択し、VDA の FQDN を追加します。



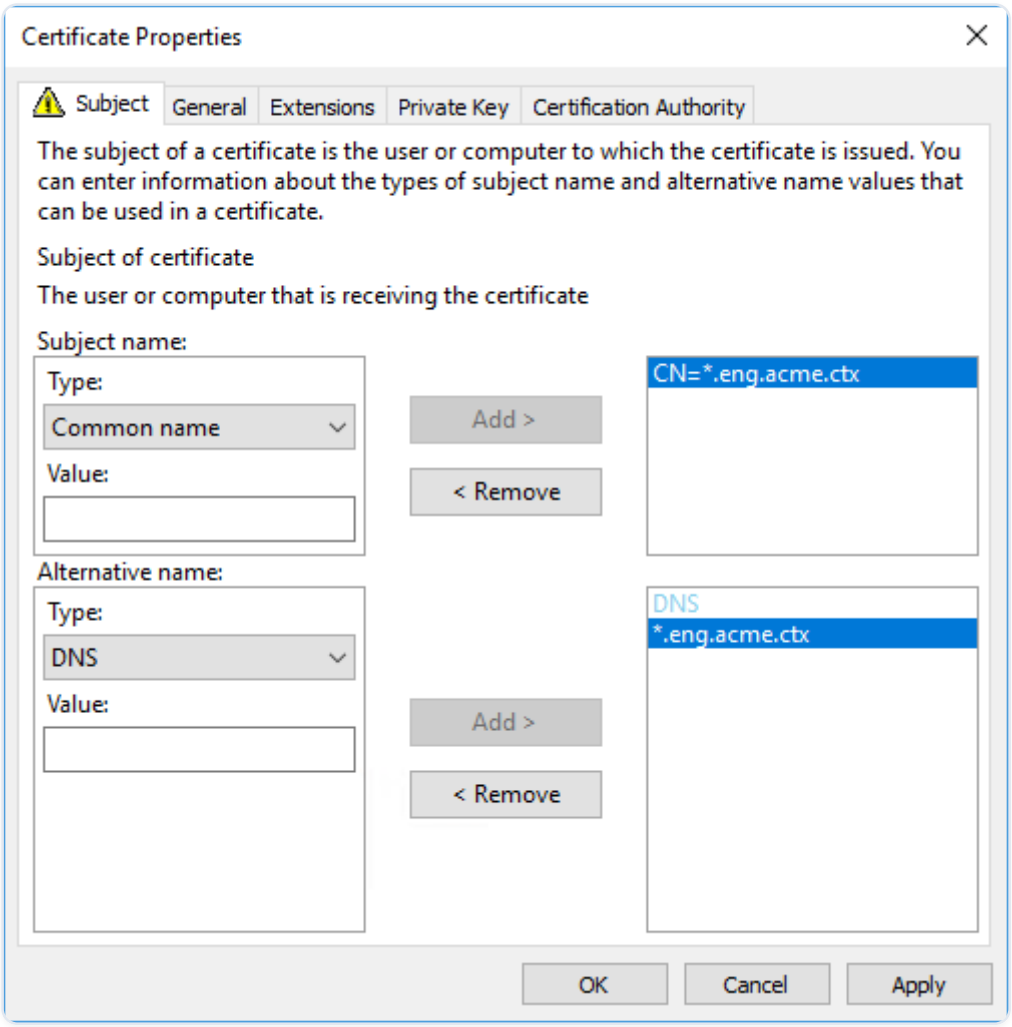
注:

Active Directory証明書サービス証明書自動登録を使用して、VDAへの証明書の発行と展開を自動化します。これは証明書の自動登録を有効にする)で説明されています。

ワイルドカード証明書を使用して、1つの証明書で複数のVDAを保護できます。

サブジェクト名 — タイプ **共通名** を選択し、VDA の *.primary.domain を入力します。

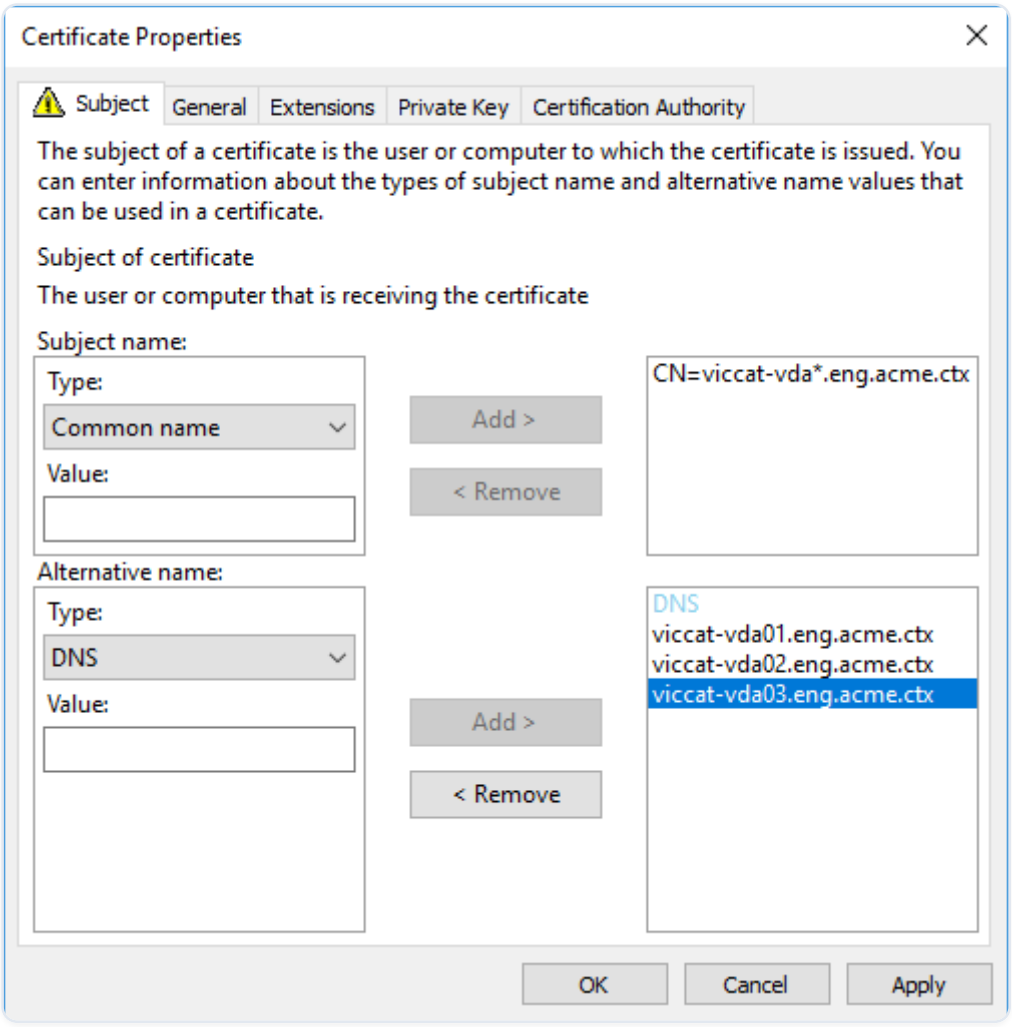
代替名 — タイプ **DNS** を選択し、VDA の *.primary.domain を追加します。



SAN証明書を使用して、1つの証明書で複数の特定のVDAを保護できます。

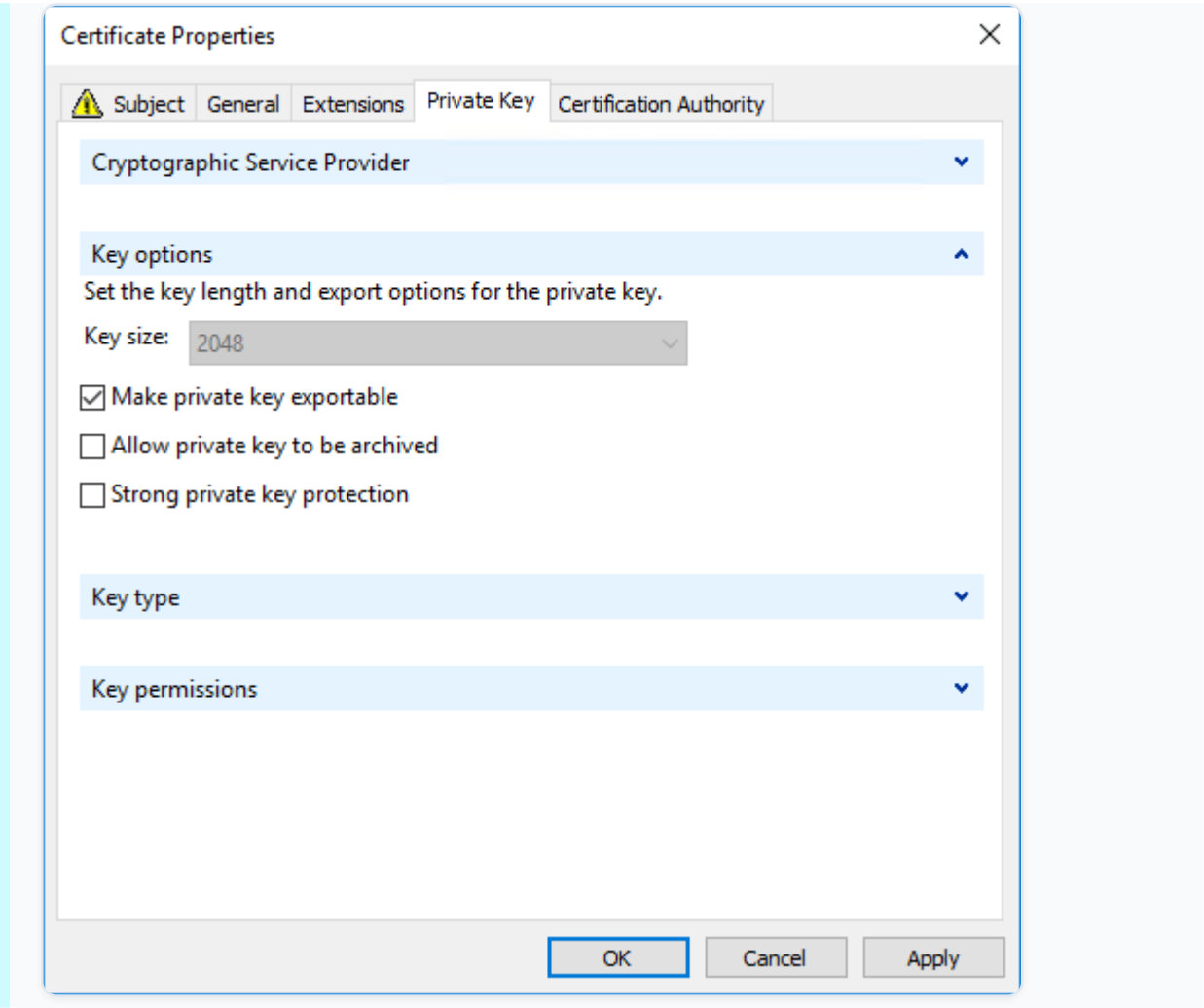
サブジェクト名 — タイプ **共通名** を選択し、証明書の使用状況を識別するのに役立つ文字列を入力します。

代替名 — タイプ **DNS** を選択し、各 VDA の FQDN のエントリを追加します。最適な TLS ネゴシエーションを確保するために、代替名の数を最小限に抑えてください。



注:

ワイルドカード証明書とSAN証明書の両方で、タブの**秘密キーをエクスポート可能にする**が選択されている必要があります。



PowerShellスクリプトを使用してVDAでTLSを構成する

証明書ストアのローカルコンピューター > 個人 > 証明書領域にTLS証明書をインストールします。その場所に複数の証明書がある場合は、PowerShellスクリプトに証明書のサムプリントを指定します。

注:

XenAppおよびXenDesktop 7.15 LTSR以降、PowerShellスクリプトはVDAのFQDNに基づいて正しい証明書を検索します。VDAのFQDNに対して単一の証明書のみが存在する場合、サムプリントを指定する必要はありません。

Enable-VdaSSL.ps1スクリプトは、VDAでTLSリスナーを有効または無効にします。このスクリプトは、インストールメディアの*Support* > *Tools* > *SslSupport*フォルダーにあります。

TLSを有効にすると、DHE暗号スイートは無効になります。ECDHE暗号スイートは影響を受けません。

TLSを有効にすると、スクリプトは指定されたTCPポートの既存のWindowsファイアウォール規則をすべて無効にします。次に、ICAサービスがTLS TCPポートとUDPポートでのみ受信接続を受け入れることを許可する新しい規則を追加します。また、次のWindowsファイアウォール規則も無効にします。

- Citrix ICA（デフォルト：1494）
- Citrix CGP（デフォルト：2598）
- Citrix WebSocket（デフォルト：8008）

その結果、ユーザーはTLSまたはDTLSを使用してのみ接続できます。TLSまたはDTLSなしでは、ICA/HDX、セッションの信頼性を備えたICA/HDX、またはWebSocket経由のHDXを使用できません。

> **注:**
>
> DTLSは、UDPリアルタイムトランスポート経由のICA/HDXオーディオ、またはICA/HDX Framehawkではサポートされていません。
>
> 「ネットワークポート」を参照してください。(/ja-jp/tech-zone/build/tech-papers/citrix-communication-ports.html#citrix-virtual-apps-and-desktops).

このスクリプトには、以下の構文の説明と追加の例が含まれています。この情報はNotepad++などのツールを使用して確認できます。

> **重要:**
>
> EnableまたはDisableパラメーター、およびCertificateThumbPrintパラメーターのいずれかを指定します。その他のパラメーターはオプションです。

構文

```
Enable-VdaSSL {-Enable | -Disable} -CertificateThumbPrint "<thumbprint>" [-SSLPort <port>] [-SSLMinVersion "<min-ssl-version>"] [-SSLCipherSuite"\<suite>"]
```

パラメーター	説明
有効化	VDAにTLSリスナーをインストールして有効にします。このパラメーターまたはDisableパラメーターのいずれかが必要です。
無効化	VDA上のTLSリスナーを無効にします。このパラメーターまたはEnableパラメーターのいずれかが必要です。このパラメーターを指定した場合、他のパラメーターは無効になります。
証明書のサムプリント "<thumbprint>"	引用符で囲まれた、証明書ストア内のTLS証明書のサムプリント。スクリプトは指定されたサムプリントを使用して、使用する証明書を選択します。このパラメーターが省略された場合、誤った証明書が選択されます。
SSLポート <port>	TLSポート。デフォルト: 443
SSL最小バージョン "<version>"	引用符で囲まれた最小TLSプロトコルバージョン。有効な値: `SSL_3.0`、`TLS_1.0` (デフォルト)、`TLS_1.1`、`TLS_1.2`、および `TLS_1.3`。`TLS_1.3`は、Windows 11またはWindows Server 2022以降が必要です。
SSLCipherSuite "<スイート>"	引用符で囲まれたTLS暗号スイート。有効な値: 「GOV」、「COM」、および「ALL」（デフォルト）。

例

次のスクリプトは、TLSプロトコルバージョン値をインストールして有効にします。サムプリント (この例では「12345678987654321」と表記) は、使用する証明書を選択するために使用されます。

```
Enable-VdaSSL -Enable -CertificateThumbPrint "12345678987654321"
```

次のスクリプトは、TLSリスナーをインストールして有効にし、TLSポート400、GOV暗号スイート、および最小TLS 1.2プロトコル値を指定します。サムプリント (この例では「12345678987654321」と表記) は、使用する証明書を選択するために使用されます。

```
Enable-VdaSSL -Enable

-CertificateThumbPrint "12345678987654321"

-SSLPort 400 -SSLMinVersion "TLS_1.2"

-SSLCipherSuite "All"
```

次のスクリプトは、VDA上のTLSリスナーを無効にします。

```
Enable-VdaSSL -Disable
```

VDAでTLSを手動で構成する

VDAでTLSを手動で構成する場合、各VDA上の適切なサービスに対して、TLS証明書の秘密キーへの一般的な読み取りアクセス権を付与します。WindowsシングルセッションOS用VDAの場合はNT SERVICE\PorticaService、WindowsマルチセッションOS用VDAの場合はNT SERVICE\TermService。VDAがインストールされているマシンで:

手順1。Microsoft管理コンソール（MMC）を起動します: スタート > ファイル名を指定して実行 > mmc.exe。

手順2。MMCに証明書スナップインを追加します:

1. > を選択します。
2. を選択し、 をクリックします。
3. 「このスナップインは常に次の証明書を管理します:」というプロンプトが表示されたら、「コンピューターアカウント」を選択し、 をクリックします。
4. 「このスナップインで管理するコンピューターを選択してください」というプロンプトが表示されたら、「ローカルコンピューター」を選択し、 をクリックします。

手順 3. 「証明書 (ローカルコンピューター) > 個人 > 証明書」で、証明書を右クリックし、「すべてのタスク」>「秘密キーの管理」を選択します。

手順 4. アクセス制御リストエディターに「(FriendlyName) の秘密キーのアクセス許可」が表示されます。ここで (FriendlyName) は TLS 証明書の名前です。次のいずれかのサービスを追加し、読み取りアクセス権を付与します。

- Windows シングルセッション OS 用の VDA の場合、「PORTICASERVICE」

- Windows マルチセッション OS 用の VDA の場合、「TERMSERVICE」

手順 5. インストールされている TLS 証明書をダブルクリックします。証明書のダイアログで、「詳細」タブを選択し、一番下までスクロールします。「拇印」をクリックします。

手順 6. regedit を実行し、HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd に移動します。

1. SSL Thumbprint キーを編集し、TLS 証明書の拇印の値をこのバイナリ値にコピーします。「バイナリ値の編集」ダイアログボックスの不明な項目（「0000」や特殊文字など）は無視しても問題ありません。
2. SSLEnabled キーを編集し、DWORD 値を 1 に変更します。(後で SSL を無効にするには、DWORD 値を 0 に変更します。)
3. デフォルト設定を変更する場合（オプション）は、同じレジストリパスで以下を使用します。

   SSLPort DWORD – SSL ポート番号。デフォルト: 443。

   SSLMinVersion DWORD – 1 = SSL 3.0、2 = TLS 1.0、3 = TLS 1.1、4 = TLS 1.2、5 = TLS 1.3。デフォルト: 2 (TLS 1.0)。

   SSLCipherSuite DWORD – 1 = GOV、2 = COM、3 = ALL。デフォルト: 3 (ALL)。

手順 7. TLS の TCP および UDP ポートがデフォルトの 443 ではない場合、Windows ファイアウォールで開いていることを確認します。(Windows ファイアウォールで受信規則を作成する際は、そのプロパティで「接続を許可する」と「有効」が選択されていることを確認してください。)

手順 8. 他のアプリケーションやサービス（IISなど）が TLS TCP ポートを使用していないことを確認します。

手順 9. マルチセッション VDA の場合、変更を有効にするにはマシンを再起動します。(シングルセッション VDA マシンを再起動する必要はありません。)

ステップ10. 接続の問題を回避するために、VDAでサポートされている暗号スイートが最も高い優先順位を持つように、Windowsの暗号スイート設定を変更します。

> **重要:**
>
> 以下に概説するグループポリシーの変更は、システムを再起動した後にのみ有効になります。

MCSまたはPVSでプロビジョニングされた非永続セッションホストを使用している場合は、これらの設定をマスターイメージに適用する必要があります。

オプション1:

グループポリシーエディターを使用して、 > > > > > に移動します。以下の暗号スイートがリストの最上位にあることを確認してください。

```
TLS_AES_256_GCM_SHA384_P384

TLS_AES_256_GCM_SHA384_P256

TLS_AES_128_GCM_SHA256_P384

TLS_AES_128_GCM_SHA256_P256

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384_P384

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384_P256

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P384

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P256

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P384

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P256
```

注:

TLS_AES_256_GCM_SHA384およびTLS_AES_128_GCM_SHA256は、Windows 11およびWindows Server 2022以降にのみ適用されます。古いオペレーティングシステムを使用している場合は、これらの暗号スイートをリストに含めないでください。

リストされている暗号スイートは、楕円曲線P384またはP256も指定しており、「curve25519」が選択されないようにしています。FIPSモードは「curve25519」の使用を妨げません。

リストから暗号スイートを削除する必要はありません。これらの設定はシステム全体に適用されるため、暗号スイートを削除する場合は、セッションホストで実行されているアプリケーションやサービスによってそれらが必要とされていないことを確認する必要があります。

オプション2:

グループポリシーエディターを使用して、 > > > > > に移動します。以下の暗号スイートがリストの最上位にあることを確認してください。

```
TLS_AES_256_GCM_SHA384

TLS_AES_128_GCM_SHA256

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
```

注:

TLS_AES_256_GCM_SHA384およびTLS_AES_128_GCM_SHA256は、Windows 11およびWindows Server 2022以降にのみ適用されます。古いオペレーティングシステムを使用している場合は、これらの暗号スイートをリストに含めないでください。

リストから暗号スイートを削除する必要はありません。これらの設定はシステム全体に適用されるため、暗号スイートを削除する場合は、セッションホストで実行されているアプリケーションやサービスによってそれらが必要とされていないことを確認する必要があります。

グループポリシーエディターを使用して、 > > > > > に移動します。設定を有効にし、以下の曲線をリストに含めます。

```
NistP384

NistP256
```

注:

これにより、「curve25519」が選択されないようにします。FIPSモードは「curve25519」の使用を妨げません。

VDAは、グループポリシーリストと、選択されたコンプライアンスモード（COM、GOV、またはALL）のリストの両方に表示される場合にのみ、暗号スイートを選択します。暗号スイートは、クライアント（Citrix Workspaceアプリ）から送信されたリストにも表示されている必要があります。

デリバリーグループでTLSを構成する

TLS接続用に構成したVDAを含む各デリバリーグループに対して、この手順を完了してください。

1. Studioから、PowerShellコンソールを開きます。
2. **Get-BrokerAccessPolicyRule -DesktopGroupName '\<*delivery-group-name*>' \| Set-BrokerAccessPolicyRule -HdxSslEnabled $true**を実行します。
3. **Set-BrokerSite -DnsResolutionEnabled $true**を実行します。

自動登録を使用したプールされたVDAのSSL有効化

プールされたVDAを使用する場合、マスターイメージに証明書を追加すると、すべてのVDAが同じイメージを共有します。ワイルドカード証明書を使用できますが、欠点は、いずれかのVDAが侵害された場合、この強力な証明書により、すべてのVDAに属するHDX™接続が危険にさらされる可能性があることです。

代わりに、より安全な代替策として、Microsoft Active Directory証明書サービスを活用して、グループポリシーを使用して証明書を自動的にプロビジョニングする方法があります。VDA上でスタートアップスクリプトを使用して、新しい証明書を動的にプロビジョニングし、VDAへのSSLを有効にすることができます。

このアプローチは、シングルセッションのデスクトップVDAでのみ機能することに注意してください。マルチセッションVDAの場合、ICAリスナーは起動プロセス中に早すぎる段階で起動され、証明書が自動的にプロビジョニングされる前になります。

Active Directory証明書サービスは内部のエンタープライズ証明機関を使用するため、すべてのWindowsインストールによって自動的に信頼されるわけではありません。クライアントが企業によって管理され、ドメインフォレストの一部である場合、信頼されたCA証明書はグループポリシーを使用して自動的に配布できます。BYODやその他のドメインに参加していないデバイスの場合、信頼されたCA証明書を別のメカニズム（ダウンロードリンクの提供など）でユーザーに配布するか、NetScaler Gatewayを使用する必要があります。

証明書の自動登録を有効にする

まず、VDAドメインフォレスト内のサーバーにActive Directory証明書サービスロールがインストールされており、エンタープライズCAが提供されていることを確認してください。そうでない場合、自動登録は不可能です。

VDAは起動ごとに証明書要求を送信するため、これによりエンタープライズCAに通常よりもかなり高い負荷がかかる可能性があることに注意してください。負荷に対処するために、CAサーバーに十分なCPUとメモリを割り当て、これまでと同様に、本番環境に移行する前にラボ環境で展開のスケーラビリティをテストしてください。

グループポリシー管理エディターで、SSLが有効なプールされたVDAを含む組織単位に適用される新しいポリシーを次のように作成します。

1. コンピューターの構成 -> ポリシー -> Windows の設定 -> セキュリティの設定 -> 公開キーのポリシー を展開します。
2. 「証明書サービス クライアント – 自動登録ポリシー」オブジェクトのプロパティを編集します。
3. 下のスクリーンショットに示すように構成します。
4. 自動証明書要求コンテナーを右クリックし、新規 -> 自動証明書要求... を選択します。
5. 自動証明書要求セットアップウィザードで、「次へ」をクリックします。
6. コンピューター証明書テンプレートが選択されていることを確認し、「次へ」をクリックします。
7. 「完了」をクリックします。

登録ポリシーのスクリーンショット (/en-us/citrix-virtual-apps-desktops/2503/media/ssltask-autoenrollment-policy.png)

Windowsマスターイメージの準備

`Support\Tools\SslSupport` フォルダーにある製品インストールメディアから Enable-VdaSsl.ps1 スクリプトをVDAマスターイメージにコピーします。マスターイメージには、HDX

SSL接続に使用する証明書を含めないでください。証明書は、MCSまたはPVSマシンカタログが作成されるときにプロビジョニングされます。次に、次のように新しいスケジュールされたタスクを作成します（スケジュールされたタスクは今すぐ実行しないでください）。

1. タスクスケジューラを開きます。
2. **操作**ペインで、「**タスクの作成...**」を押します。
3. 「全般」タブで:

   - 「**名前**」を入力します。例: `Enable VDA SSL`
   - 「**ユーザーまたはグループの変更...**」をクリックし、「ユーザーまたはグループの選択」ダイアログボックスで `SYSTEM` を入力し、「**OK**」をクリックします。

   タスク作成の「操作」タブのスクリーンショット (/en-us/citrix-virtual-apps-desktops/2503/media/ssltask-general.png)
4. 「トリガー」タブを選択します。
5. 「**新規...**」をクリックします。「**新しいトリガー**」ダイアログで:

   a. 「**タスクの開始**」を「**イベント時**」に設定します。

   b. 「**ログ**」を「**Microsoft-Windows-CertificateServicesClient-Lifecycle-System/Operational**」に設定します。

   c. 「**ソース**」を「**Microsoft-Windows-CertificateServicesClient-Lifecycle-System**」に設定します。

   d. 「**イベント ID**」を `1006` に設定します。

   e. 「**OK**」をクリックしてトリガーを保存します。

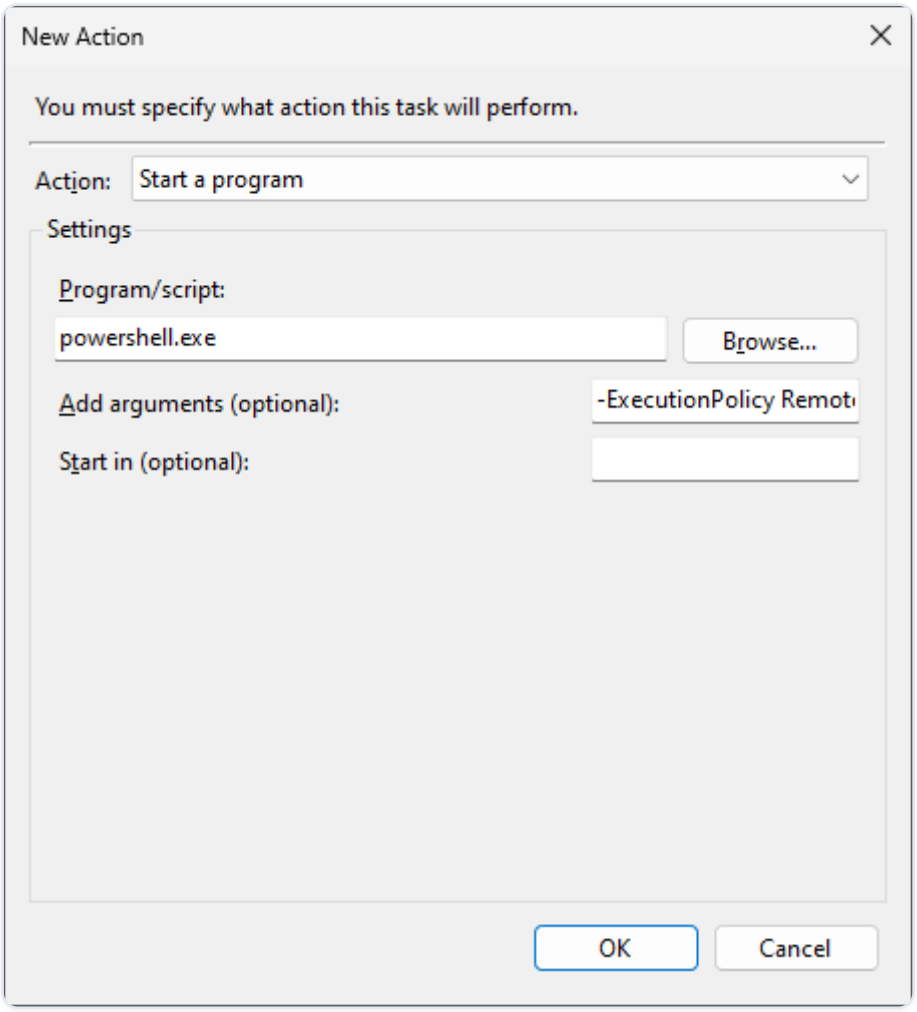
   「新しいトリガー」ウィンドウのスクリーンショット (/en-us/citrix-virtual-apps-desktops/2503/media/ssltask-trigger.png)
6. 「**操作**」タブを選択します。
7. 「**新規...**」をクリックします。
8. 「**新しい操作**」ダイアログで:

   a. 「**操作**」を「**プログラムの開始**」に設定します。

   b. 「プログラム/スクリプト」フィールドに `powershell.exe` と入力します。

   c. 「引数の追加」フィールドに、PowerShellスクリプトへのパスを含めて `-ExecutionPolicy RemoteSigned Enable-VdaSsl.ps1 -Enable -Confirm:$False` を入力します。

d. アクションを保存するには、**OK**を押します。



9. タスクを保存するには、**OK**を押します。

トラブルシューティング

接続エラーが発生した場合は、VDAのシステムイベントログを確認してください。

Windows向けCitrix Workspaceアプリを使用しているときに、TLSエラーを示す接続エラーが表示された場合は、Desktop Viewerを無効にしてから、もう一度接続を試してください。接続が失敗しても、基になるTLSの問題の説明が提供される場合があります。たとえば、証明機関に証明書を要求するときに、誤ったテンプレートを指定したなどです。

HDX Adaptive Transportを使用するほとんどの構成は、Citrix Workspaceアプリ、Citrix Gateway、およびVDAの最新バージョンを使用しているものを含め、DTLSで正常に動作します。Citrix WorkspaceアプリとCitrix Gatewayの間でDTLSを使用し、Citrix GatewayとVDAの間でDTLSを使用する一部の構成では、追加のアクションが必要です。

次の場合、追加の操作が必要です。

- Citrix ReceiverのバージョンがHDX Adaptive TransportとDTLSをサポートしている場合: Receiver for Windows (4.7、4.8、4.9)、Receiver for Mac (12.5、12.6、12.7)、Receiver for iOS (7.2、7.3.x)、またはReceiver for Linux (13.7)

かつ、以下のいずれかが当てはまる場合:

- Citrix GatewayのバージョンはVDAへのDTLSをサポートしているが、VDAのバージョンはDTLSをサポートしていない（バージョン7.15以前）。
- VDAのバージョンはDTLSをサポートしている（バージョン7.16以降）が、Citrix GatewayのバージョンはVDAへのDTLSをサポートしていない。

Citrix Receiver™ からの接続が失敗するのを避けるには、次のいずれかを実行します。

- Citrix Receiverを、Receiver for Windowsバージョン4.10以降、Receiver for Mac 12.8以降、またはReceiver for iOSバージョン7.5以降に更新する。
- Citrix Gatewayを、VDAへのDTLSをサポートするバージョンに更新する。
- VDAをバージョン7.16以降に更新する。
- VDAでDTLSを無効にする。
- HDX Adaptive Transportを無効にする。

> **注:**
>
> Receiver for Linuxの適切なアップデートはまだ利用できません。Receiver for Android（バージョン3.12.3）は、Citrix Gateway経由のHDX Adaptive TransportおよびDTLSをサポートしていないため、影響を受けません。

> VDAでDTLSを無効にするには、VDAファイアウォール構成を変更してUDPポート443を無効にします。ネットワークポートを参照してください。

TLS と HTML5 ビデオリダイレクト、およびブラウザコンテンツリダイレクト

HTML5ビデオリダイレクトとブラウザコンテンツリダイレクトを使用して、HTTPS Webサイトをリダイレクトできます。これらのWebサイトに挿入されるJavaScriptは、VDAで実行されているCitrix HDX HTML5ビデオリダイレクトサービスへのTLS接続を確立する必要があります。これを

実現するために、HTML5ビデオリダイレクトサービスは、VDA上の証明書ストアに2つのカスタム証明書を生成します。サービスを停止すると、証明書は削除されます。

HTML5 ビデオリダイレクトポリシーは、デフォルトで無効になっています。

ブラウザコンテンツリダイレクトは、デフォルトで有効になっています。

HTML5ビデオリダイレクトの詳細については、マルチメディアポリシー設定を参照してください。

Universal Print Server で TLS を有効にする

Virtual Delivery Agent (VDA) とユニバーサルプリントサーバー間のTCPベースの接続には、トランスポート層セキュリティ (TLS) プロトコルがサポートされています。

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

VDA と Universal Print Server 間の印刷接続の種類

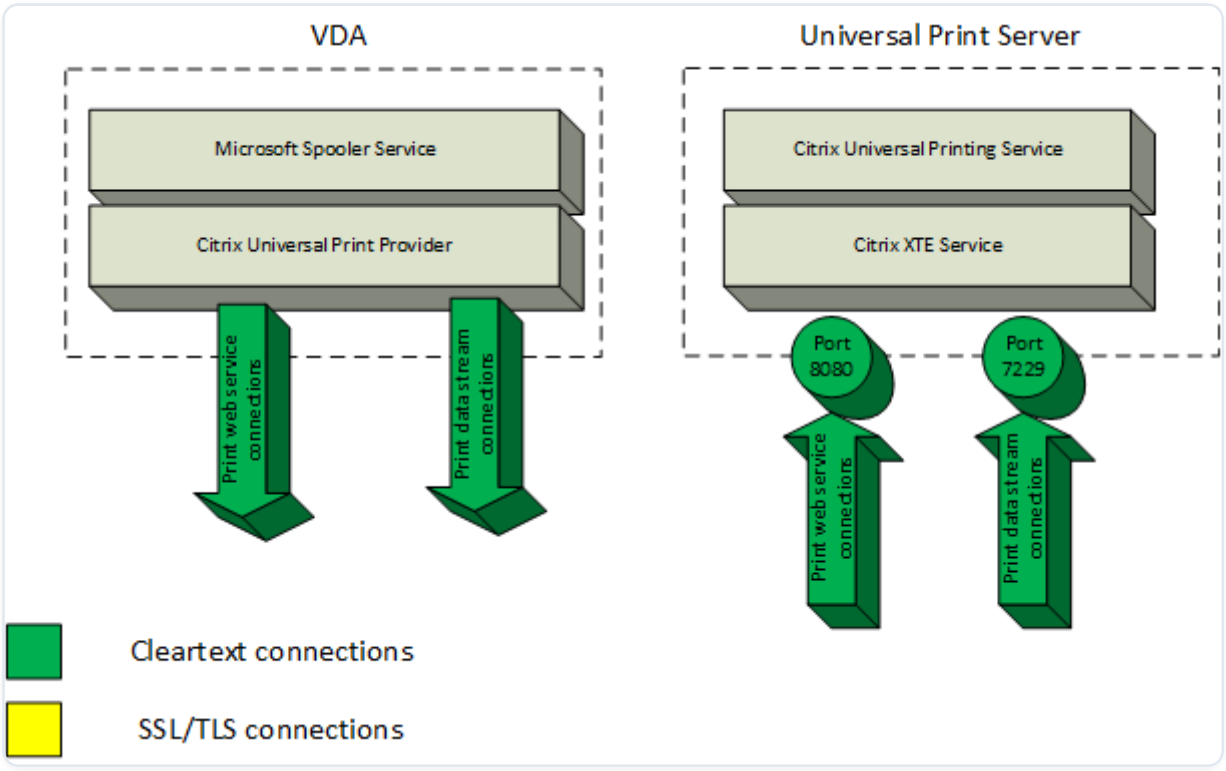
クリアテキスト接続

印刷に関連する以下の接続は、VDAから発信され、ユニバーサルプリントサーバー上のポートに接続します。これらの接続は、**SSL enabled** ポリシー設定が **Disabled** (デフォルト) に設定されている場合にのみ行われます。

- クリアテキスト印刷Webサービス接続 (TCPポート8080)
- クリアテキスト印刷データストリーム (CGP) 接続 (TCPポート7229)

Microsoft のサポート記事 Service overview and network port requirements for Windows には、Microsoft Windows Print Spooler サービスが使用するポートが記載されています。このドキュメントの SSL/TLS 設定は、Windows Print Spooler サービスによって行われる NetBIOS および RPC 接続には適用されません。**Universal Print Server enable** ポリシー設定が **Enabled with fallback**

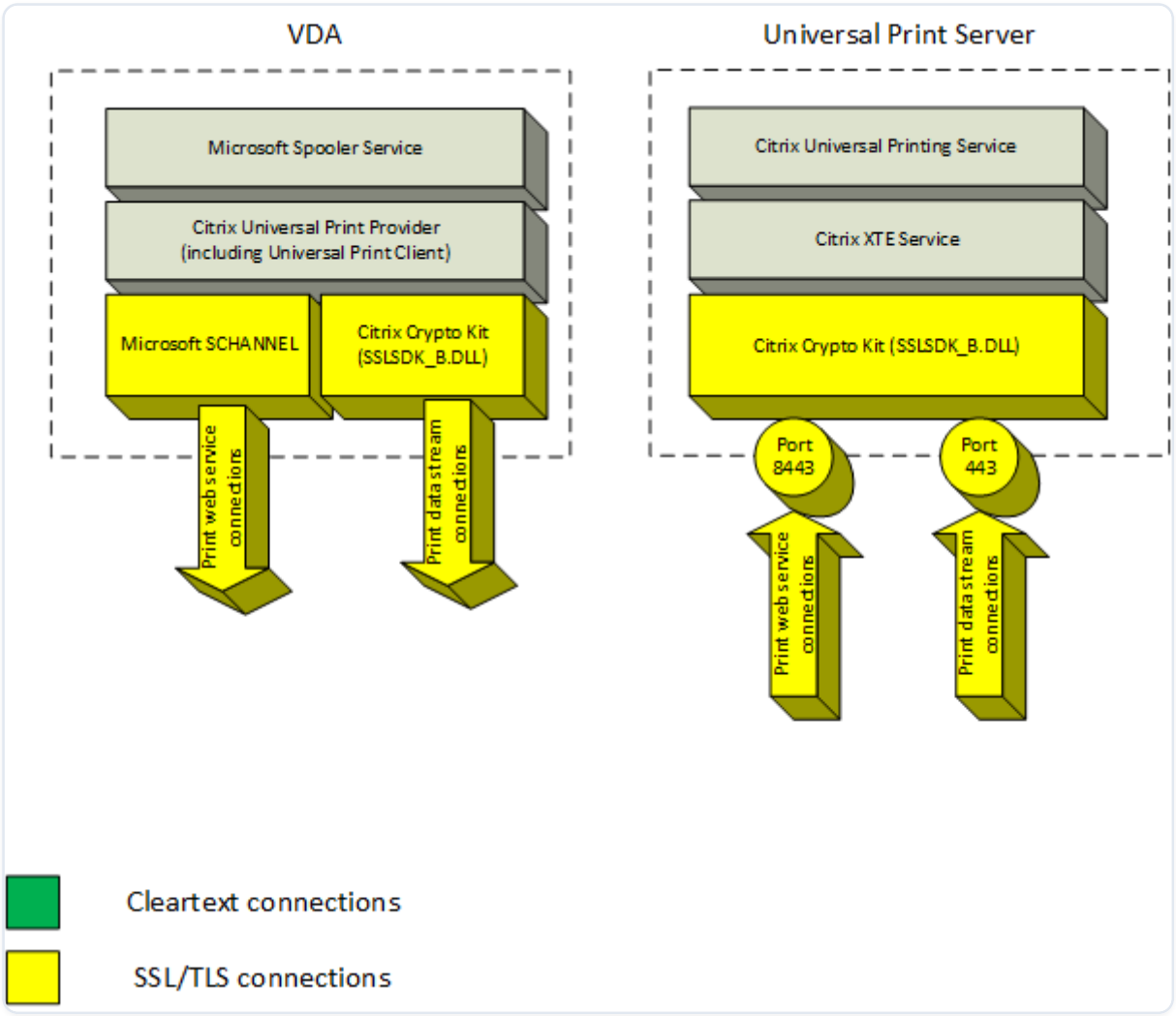
to Windows' native remote printing に設定されている場合、VDA は Windows Network Print Provider (win32spl.dll) をフォールバックとして使用します。



暗号化された接続

印刷に関連するこれらのSSL/TLS接続は、VDAから発信され、ユニバーサルプリントサーバー上のポートに接続します。これらの接続は、**SSL enabled** ポリシー設定が **Enabled** に設定されている場合にのみ行われます。

- 暗号化された印刷Webサービス接続 (TCPポート8443)
- 暗号化された印刷データストリーム (CGP) 接続 (TCPポート443)



SSL/TLS クライアント構成

VDA は SSL/TLS クライアントとして機能します。

暗号化された印刷Webサービス接続（TCPポート8443）用にMicrosoft SCHANNEL SSPを構成するには、Microsoftグループポリシーとレジストリを使用します。Microsoftサポート記事のTLS Registry Settingsに、Microsoft SCHANNEL SSPのレジストリ設定が記載されています。

VDAでグループポリシーエディターを使用して、**［コンピューターの構成］>［管理用テンプレート］>［ネットワーク］>［SSL構成設定］>［SSL暗号スイートの順序］**の順に移動します。TLS 1.3が設定されている場合は、次の順序を選択します。

TLS_AES_256_GCM_SHA384 TLS_AES_128_GCM_SHA256

TLS 1.2 が設定されている場合は、次の順序を選択します。

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384_P384
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384_P256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P384

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P384
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P256

> **注:**
>
> このグループポリシー設定が構成されている場合、VDA は、暗号化された印刷 Web サービス接続 (デフォルトポート: 8443) の暗号スイートを、接続が両方の SSL 暗号スイートリストに表示されている場合にのみ選択します。

- グループポリシーSSL暗号スイート順序リスト
- 選択したSSL暗号スイートポリシー設定（COM、GOV、またはALL）に対応するリスト

> このグループポリシー構成は、VDA 上の他の TLS アプリケーションおよびサービスにも影響します。アプリケーションが特定の暗号スイートを必要とする場合は、このグループポリシー暗号スイート順序リストに追加する必要がある場合があります。

> **重要:**
>
> TLS 構成のグループポリシーの変更は、オペレーティングシステムの再起動後にのみ有効になります。

> Citrix ポリシーを使用して、暗号化された印刷データストリーム (CGP) 接続 (TCP ポート 443) の SSL/TLS 設定を構成します。

SSL/TLS サーバー構成

ユニバーサルプリントサーバーはSSL/TLSサーバーとして機能します。

SSL/TLS設定を構成するには、`Enable-UpsSsl.ps1` PowerShellスクリプトを使用します。

Universal Print ServerにTLS証明書をインストールする

HTTPSの場合、VDAsによって信頼されているSSLサーバー証明書をUniversal Print Serverにインストールする必要があります。Microsoft Active Directory証明書サービスまたは別の認証局を使用して、Universal Print Serverの証明書を要求します。

マイクロソフト アクティブ ディレクトリ証明書サービスを使用して証明書を登録/要求する際は、次の考慮事項に留意してください。

1. 証明書をローカルコンピューターの**個人**証明書ストアに配置します。
2. 証明書のサブジェクト識別名 (Subject DN) の**共通名**属性を、Universal Print Serverの完全修飾ドメイン名 (FQDN) に設定します。これは証明書テンプレートで指定します。
3. 証明書要求と秘密鍵の生成に使用される暗号化サービスプロバイダー (CSP) を**Microsoft Enhanced RSA and AES Cryptographic Provider (Encryption)**に設定します。これは証明書テンプレートで指定します。
4. キーサイズを2048ビット以上に設定します。これは証明書テンプレートで指定します。

証明書の作成とインストールについて詳しくは、「証明書の管理」を参照してください。

Universal Print ServerでのSSLの構成

Universal Print Server上のXTEサービスは、受信接続をリッスンします。SSLが有効になっている場合、SSLサーバーとして機能します。受信接続には、印刷コマンドを含む印刷Webサービス接続と、印刷ジョブを含む印刷データストリーム接続の2種類があります。これらの接続でSSLを有効にできます。SSLはこれらの接続の機密性と整合性を保護します。デフォルトでは、SSLは無効になっています。

SSLの構成に使用されるPowerShellスクリプトは、インストールメディアにあり、ファイル名は次のとおりです: `\Support\Tools\SslSupport\Enable-UpsSsl.ps1.`.

Universal Print Serverでのリスニングポート番号の構成

XTEサービスのデフォルトポートは次のとおりです。

- クリアテキスト印刷Webサービス（HTTP）TCPポート: 8080
- クリアテキスト印刷データストリーム (CGP) TCPポート: 7229
- 暗号化された印刷Webサービス (HTTPS) TCPポート: 8443
- 暗号化された印刷データストリーム (CGP) TCPポート: 443

Universal Print Server の XTE サービスで使用されるポートを変更するには、管理者として PowerShell で次のコマンドを実行します (Enable-UpsSsl.ps1 PowerShell スクリプトの使用に関する注意点については、後のセクションを参照してください):

1. `Stop-Service CitrixXTEServer, UpSvc`
2. `Enable-UpsSsl.ps1 -Enable -HTTPSPort <port> -CGPSSLPort <port>` or `Enable-UpsSsl.ps1 -Disable -HTTPPort <port> -CGPPort <port>`

3. `Start-Service CitrixXTEServer`

Universal Print Server での TLS 設定

負荷分散構成で複数の Universal Print Server を使用している場合は、すべての Universal Print Server で **TLS** 設定が一貫して構成されていることを確認してください。

Universal Print Server で TLS を構成すると、インストールされている TLS 証明書のアクセス許可が変更され、Universal Printing Service に証明書の秘密キーへの読み取りアクセス権が付与されます。また、Universal Printing Service に次の情報が通知されます。

- TLS に使用する証明書ストア内の証明書。
- TLS 接続に使用する TCP ポート番号。

Windows ファイアウォール (有効な場合) は、これらの TCP ポートでの受信接続を許可するように構成する必要があります。この構成は、Enable-UpsSsl.ps1 PowerShell スクリプトを使用すると自動的に行われます。

- 許可する TLS プロトコルのバージョン。

Universal Print Server は TLS プロトコルバージョン 1.3 および 1.2 をサポートしています。許可される最小バージョンを指定します。

デフォルトの TLS プロトコルバージョンは 1.2 です。

> **注:**
>
> TLS 1.1 および 1.0 は、Citrix Virtual Apps and Desktops バージョン 2311 以降ではサポートされなくなりました。

- 許可する TLS 暗号スイート。

暗号スイートは、接続に使用される暗号アルゴリズムを選択します。VDA と Universal Print Server は、異なる暗号スイートのセットをサポートできます。VDA が接続し、サポートされている TLS 暗号スイートのリストを送信すると、Universal Print Server はクライアントの暗号スイートのいずれかを、自身の構成済み暗号スイートのリストにある暗号スイートのいずれかと照合し、接続を受け入れます。一致する暗号スイートがない場合、Universal Print Server は接続を拒否します。

Universal Print Server は、OPEN、FIPS、および SP800-52 ネイティブ Crypto Kit モードに対して、GOV(ernment)、COM(mercial)、および ALL という名前の以下の暗号スイートセットをサポートしています。許容される暗号スイートは、**SSL FIPS Mode** ポリシー設定と Windows FIPS Mode にも依存します。Windows FIPS モードの詳細については、このMicrosoft サポート記事を参照してください。

暗号スイート（優先順位の降順）	OPEN ALL	OPEN COM	OPEN GOV	FIPS ALL	FIPS COM	FIPS GOV	SP800-52 ALL	SP800-52 COM	SP800-52 GOV
TLS_ECDHE_RSA_AES256_GCM_SHA384	X		X	X		X	X		X
TLS_ECDHE_RSA_AES256_CBC_SHA384	X		X	X		X	X		X
TLS_ECDHE_RSA_	X	X		X	X		X	X	

暗号スイート（優先順位の降順）	OPEN ALL	OPEN COM	OPEN GOV	FIPS ALL	FIPS COM	FIPS GOV	SP800-52 ALL	SP800-52 COM	SP800-52 GOV
AES256_CBC_SHA									

PowerShellスクリプトを使用してUniversal Print ServerでTLSを構成する

証明書ストアの**ローカルコンピューター > 個人 > 証明書**領域にTLS証明書をインストールします。その場所に複数の証明書がある場合は、証明書のサムプリントを`Enable-UpsSsl.ps1` PowerShellスクリプトに指定します。

> **注:**
>
> PowerShellスクリプトは、Universal Print ServerのFQDNに基づいて正しい証明書を検索します。Universal Print ServerのFQDNに対して証明書が1つしかない場合は、証明書のサムプリントを指定する必要はありません。

> `Enable-UpsSsl.ps1`スクリプトは、VDAからUniversal Print ServerへのTLS接続を有効または無効にします。このスクリプトは、インストールメディアの**Support > Tools > SslSupport**フォルダーにあります。

TLSを有効にすると、スクリプトはUniversal Print ServerのTCPポートに対する既存のWindowsファイアウォール規則をすべて無効にします。その後、XTEサービスがTLS TCPおよびUDPポートでのみ着信接続を受け入れることを許可する新しい規則を追加します。また、以下のWindowsファイアウォール規則も無効にします。

- クリアテキスト印刷Webサービス接続（デフォルト：8080）
- クリアテキスト印刷データストリーム（CGP）接続（デフォルト：7229）

その結果、VDAはTLSを使用している場合にのみこれらの接続を行うことができます。

注:

TLSを有効にしても、VDAからUniversal Print ServerへのWindows Print Spooler RPC/SMB接続には影響しません。

重要:

最初のパラメーターとして**Enable**または**Disable**のいずれかを指定します。ローカルコンピューターの個人証明書ストアにUniversal Print ServerのFQDNを持つ証明書が1つしかない場合、CertificateThumbprintパラメーターはオプションです。その他のパラメーターもオプションです。

構文

```
Enable-UpsSSL.ps1 -Enable [-HTTPPort &lt;port&gt;] [-CGPPort &lt;port&gt;] [-HTTPSPort &lt;port&gt;] [-CGPSSLPort &lt;port&gt;] [-SSLMinVersion &lt;version&gt;] [-SSLCipherSuite &lt;name&gt;] [-CertificateThumbprint &lt;thumbprint&gt;] [-FIPSMode &lt;Boolean&gt;] [-ComplianceMode &lt;mode&gt;]

Enable-UpsSSL.ps1 -Disable [-HTTPPort &lt;portnum&gt;] [-CGPPort &lt;portnum&gt;]
```

パラメーター	説明
有効にする	XTEサーバーでSSL/TLSを有効にします。このパラメーターまたはDisableパラメーターのいずれかが必要です。
無効にする	XTEサーバーでSSL/TLSを無効にします。このパラメーターまたはEnableパラメーターのいずれかが必要です。
CertificateThumbprint `"<thumbprint>"`	ローカルコンピューターの個人証明書ストアにあるTLS証明書のサムプリント。引用符で囲まれています。スクリプトは、指定されたサムプリントを使用して、使用する証明書を選択します。

パラメーター	説明
HTTPポート `<port>`	クリアテキスト印刷Webサービス (HTTP/SOAP) ポート。デフォルト: 8080
CGPポート `<port>`	クリアテキスト印刷データストリーム (CGP) ポート。デフォルト: 7229
HTTPSポート `<port>`	暗号化された印刷Webサービス (HTTPS/SOAP) ポート。デフォルト: 8443
CGPSSLポート `<port>`	暗号化された印刷データストリーム (CGP) ポート。デフォルト: 443
SSLMinVersion `"<version>"`	最小TLSプロトコルバージョン。引用符で囲まれています。有効な値: 「TLS_1.2」および「TLS_1.3」。デフォルト: TLS_1.2。
SSLCipherSuite `"<name>"`	TLS暗号スイートパッケージの名前。引用符で囲まれています。有効な値: 「GOV」、「COM」、および「ALL」(デフォルト)。
FIPSモード `<Boolean>`	XTEサーバーでFIPS 140モードを有効または無効にします。有効な値: FIPS 140モードを有効にする場合は$true、FIPS 140モードを無効にする場合は$false。

例

次のスクリプトはTLSを有効にします。サムプリント（この例では「12345678987654321」として表されています）は、使用する証明書を選択するために使用されます。

```
Enable-UpsSsl.ps1 –Enable -CertificateThumbprint "12345678987654321"
```

次のスクリプトはTLSを無効にします。

```
Enable-UpsSsl.ps1 –Disable
```

FIPSモードの構成

米国連邦情報処理標準（FIPS）モードを有効にすると、Universal Print Serverの暗号化された接続にはFIPS 140準拠の暗号化のみが使用されるようになります。

クライアントでFIPSモードを構成する前に、サーバーでFIPSモードを構成してください。

Windows FIPSモードの有効化または無効化の方法については、Microsoft社の公式資料をご確認ください。

クライアントでのFIPSモードの有効化

Delivery Controller™でWeb Studioを実行し、**UPS FIPS Mode** Citrixポリシー設定を**Enabled**に設定します。Citrixポリシーを有効にします。

各VDAで以下を実行します。

1. Windows FIPSモードを有効にします。
2. VDAを再起動します。

サーバーでのFIPSモードの有効化

各Universal Print Serverで以下を実行します。

1. Windows FIPSモードを有効にします。
2. 管理者として次のPowerShellコマンドを実行します: `stop-service CitrixXTEServer, UpSvc`
3. `-Enable -FIPSMode $true` パラメーターを指定して、`Enable-UpsSsl.ps1` スクリプトを実行します。
4. Universal Print Serverを再起動します。

クライアントでのFIPSモードの無効化

Web Studioで、Citrixポリシー設定の**UPS FIPS Mode**を**Disabled**に設定します。Citrixポリシーを有効にします。**UPS FIPS Mode** Citrixポリシー設定を削除することもできます。

各VDAで次の操作を行います:

1. Windows FIPSモードを無効にします。
2. VDAを再起動します。

サーバーでのFIPSモードの無効化

各Universal Print Serverで次の操作を行います:

1. Windows FIPSモードを無効にします。
2. 管理者として次のPowerShellコマンドを実行します: `stop-service CitrixXTEServer, UpSvc`

3. `-Enable -FIPSMode $false`パラメーターを指定して、`Enable-UpsSsl.ps1`スクリプトを実行します。
4. Universal Print Serverを再起動します。

> **注：**
>
> SSLプロトコルバージョンがTLS 1.3に設定されている場合、FIPSモードはサポートされません。

SSL/TLSプロトコルバージョンの構成

デフォルトのSSL/TLSプロトコルバージョンはTLS 1.2です。TLS 1.2とTLS 1.3は、運用環境での使用が推奨されるSSL/TLSプロトコルバージョンです。トラブルシューティングのために、非運用環境で一時的にSSL/TLSプロトコルバージョンを変更する必要がある場合があります。

Universal Print Serverでは、SSL 2.0およびSSL 3.0はサポートされていません。

サーバーでのSSL/TLSプロトコルバージョンの設定

各Universal Print Serverで、次の手順を実行します。

1. 管理者としてこのPowerShellコマンドを実行します: `stop-service CitrixXTEServer, UpSvc`
2. `-Enable -SSLMinVersion`バージョンパラメーターを指定して、`Enable-UpsSsl.ps1`スクリプトを実行します。テストが完了したら、これをTLS 1.2またはTLS 1.3に戻すことを忘れないでください。
3. Universal Print Serverを再起動します。

クライアントでのSSL/TLSプロトコルバージョンの設定

Studioで、**SSLプロトコルバージョン**ポリシー設定を目的のプロトコルバージョンに設定し、ポリシーを有効にします。

VDAのオペレーティングシステムが選択されたTLSバージョンをサポートしていることを確認してください。Windowsでサポートされ ているTLSバージョンについては、Microsoft Learn - TLS protocol version supportを参照してください。デフォルトを上書きするようにレジストリを構成するには、Microsoft Learn - TLS, DTLS, and SSL protocol version settingsを参照してください。

トラブルシューティング

接続エラーが発生した場合は、Universal Print Server上のC:\Program Files (x86)\Citrix\XTE\logs\error.logファイルを確認してください。

SSL/TLSハンドシェイクが失敗した場合、このログファイルにエラーメッセージ「**SSL handshake from client failed**」が表示されます。このような失敗は、VDAとUniversal Print Server上のSSL/TLSプロトコルバージョンが一致しない場合に発生する可能性があります。

Universal Print Serverのホスト名を含む以下のポリシー設定で、Universal Print ServerのFQDNを使用してください。

- セッションプリンター
- プリンターの割り当て
- 負荷分散のためのUniversal Print Server

Universal Print ServerとVDAでシステムクロック（日付、時刻、タイムゾーン）が正しいことを確認してください。

仮想チャネル許可リスト

仮想チャネル許可リストは、環境内で許可されるCitrix以外の仮想チャネルを制御できる機能です。デフォルトでは、仮想チャネル許可リスト機能は有効になっています。その結果、Citrix Virtual Apps and Desktops™セッションで開くことが許可されるのはCitrix仮想チャネルのみです。自社製かサードパーティ製かにかかわらず、カスタム仮想チャネルを使用する必要がある場合は、これらを許可リストに明示的に追加する必要があります。

構成

仮想チャネル許可リストは、デフォルトで有効になっています。この機能は、Citrixポリシーの次の設定を使用して構成できます。

- **仮想チャネル許可リスト**: 機能を有効または無効にし、仮想チャネルをリストに追加します。
- **仮想チャネル許可リストのログスロットリング**: 仮想チャネル許可リストのイベントログのスロットリング期間を設定します。
- **仮想チャネル許可リストのログ記録**: 仮想チャネル許可リストのログレベルを設定します。

許可リストへの仮想チャネルの追加

仮想チャネルを許可リストに追加するには、以下の情報が必要です。

1. コードで定義されている仮想チャネル名。最大7文字です。例: `CTXCVC1`。
2. VDAマシン上で仮想チャネルを開くプロセスへのパス。例: `C:\Program Files\Application\run.exe`。

必要な情報が揃ったら、仮想チャネル許可リストポリシー設定を使用して仮想チャネルを許可リストに追加する必要があります。仮想チャネルをリストに追加するには、仮想チャネル名を入力し、その後にコンマ、そして仮想チャネルにアクセスするプロセスへのパスを入力します。複数のプロセスがある場合は、各プロセスをコンマで区切って追加できます。

単一のプロセスの場合

前の例を使用して、以下のエントリをリストに追加します。

```
CTXCVC1,C:\Program Files\Application\run.exe
```

複数のプロセスの場合

複数のプロセスがある場合は、次のエントリをリストに追加します。

```
CTXCVC1,C:\Program Files\Application\run.exe,C:\Program Files\Application\run2.exe
```

ワイルドカードの使用

ワイルドカード（*）の使用がサポートされています。アプリケーションのバージョンによってディレクトリ名や実行可能ファイル名が変わる場合、またはサードパーティコンポーネントがユーザープロファイルにインストールされている場合に、ワイルドカードを使用できます。

次のシナリオでワイルドカードを使用できます。

- ディレクトリ名を完全に置き換える場合。 例: `C:\Program Files\Application*\run1.exe`
- ディレクトリ名の一部を置き換える場合。 例: `C:\Program Files\Application\v*\run1.exe`
- 実行可能ファイル名を置き換える場合。 例: `C:\Program Files\Application\v1.2*.exe`
- 実行可能ファイル名の一部を置き換える場合。 例: `C:\Program Files\Application\v1.2\run*.exe`

次の制限が適用されます。

- ワイルドカードは、単一のディレクトリを置き換えるためにのみ使用できます。たとえば、実行可能ファイルが `C:\Program Files\Application\v1.2\run1.exe` にある場合
  - 許可: `C:\Program Files\Application*\run1.exe`
  - 不許可: `C:\Program Files*\run1.exe`
- エントリにはファイル名拡張子を含める必要があります。
  - 許可済み: `C:\Program Files\Application\v1.2*.exe`
  - 許可されていません: `C:\Program Files\Application\v1.2*`
- すべてのパスはローカルである必要があります。

注:

- ネットワークパスは許可されていません。
- ワイルドカードのサポートは、Citrix Virtual Apps and Desktops 2206 から利用可能です。
- ワイルドカードのサポートは、Citrix Virtual Apps and Desktops 2203 LTSR の CU2 から利用可能です。

システム環境変数の使用

許可リスト内の信頼されたプロセスの定義を簡素化するために、システム環境変数を使用できます。`%programfiles%`、`%programfiles(x86)%`、`%systemdrive%`、`%systemroot%` などの既成の変数を使用できます。

システムレベルで定義されている限り、カスタム環境変数も使用できます。

以下の例は、既成の環境変数を示しています。

- `%programfiles%\Application\v1.2\run.exe`
- `%programfiles%\Application*\run.exe`
- `%programfiles(x86)%\Application\v1.*\run.exe`

以下の例は、カスタムシステム環境変数を示しています。

- カスタム変数名: `app`
- カスタム変数値: `%programfiles%\Application\`

- 許可リストエントリ: `CTXCVC1,%app%\run.exe`

> **注:**
>
> ユーザー環境変数はサポートされていません。

> 環境変数のサポートは、Citrix Virtual Apps and Desktopsバージョン2209以降で利用可能です。

仮想チャネル名とプロセスを取得する

VDAマシン上で仮想チャネル名とそれを開くプロセスを取得する最も簡単な方法は、仮想チャネルを提供した開発者またはサードパーティベンダーから情報を入手することです。

または、機能のログを適用し、以下の手順に従って情報を取得することもできます。

1. カスタム仮想チャネルのクライアントコンポーネントとサーバーコンポーネントが配置されたら、仮想アプリケーションまたは仮想デスクトップを起動します。
2. VDAマシンのシステムイベントログで、カスタム仮想チャネル名とそれを開こうとしたプロセスを探します。利用可能なイベントの詳細については、「イベントログ」を参照してください。
3. セッションからログアウトします。
4. 識別された仮想チャネルとプロセスについて、仮想チャネル許可リストポリシー設定にエントリを追加します。
5. マシンを再起動します。
6. VDAが登録されたら、仮想アプリケーションまたは仮想デスクトップを実行して、カスタム仮想チャネルが正常に開くことを検証します。

Citrix仮想チャネルに関する考慮事項

すべての組み込みCitrix仮想チャネルは信頼されており、追加設定なしで開くことができます。ただし、以下の2つの機能は外部依存関係があるため、許可リストに明示的なエントリが必要です。

- マルチメディアリダイレクト
- スカイプ フォー ビジネス向け HDXリアルタイム最適化パック

マルチメディアリダイレクト

Windows Media Player以外のメディアプレーヤーをシステムメディアプレーヤーとして使用する場合、それを信頼されたプロセスとして許可リストに追加する必要があります。許可リストのエントリには、以下の情報が必要です。

- 仮想チャネル名: `CTXMM`
- プロセス: VDAマシンで使用されるメディアプレーヤーへのパス。例: `C:\Program Files (x86)\Windows Media Player\wmplayer.exe`。
- 許可リストエントリ: `CTXMM,C:\Program Files (x86)\Windows Media Player\wmplayer.exe`

スカイプ フォー ビジネス向け HDXリアルタイム最適化パック

許可リストのエントリには、以下の情報が必要です。

- 仮想チャネル名: `CTXRMEP`
- プロセス: VDAマシン内のSkype for Business実行可能ファイルへのパス。これはSkype for Businessのバージョンやカスタムインストールパスの使用によって異なる場合があります。例: `C:\Program Files\Microsoft Office\root\Office16\lync.exe.`.
- 許可リストエントリ: `CTXRMEP,C:\Program Files\Microsoft Office\root\Office16\lync.exe`

VDAとデリバリーコントローラー™間のウェブソケット通信

この記事では、WCF通信の代替として、VDAとDelivery Controller間の通信にWebSocket接続を設定する方法について説明します。これにより、VDAからDelivery Controllerへの通信にTLSポート443のみを使用するという利点が得られます。

動作の仕組み

以下のセクションでは、Delivery ControllerとVDA間のWebSocket接続のワークフローについて説明します。

通常のブローカー処理操作中

1. Citrix Virtual Apps and Desktops™管理者は、Machine Creation Service (MCS)を使用してVDAをプロビジョニングすることでプロセスを開始します。

2. MCSプロビジョニングプロセス中に、MCSは各VDAの公開鍵と秘密鍵のペアを生成し、Delivery Controller上のFMAトラストサービスに公開鍵を登録します。MCSは、公開鍵と秘密鍵のペアをVDAのIDディスク下のファイルとして保存します。
3. VDAマシンが起動すると、VDAマシンにインストールされているMCSエージェントはIDディスクからキーペアを読み取り、この情報をVDAレジストリの場所に書き込みます。
4. VDAにインストールされているブローカーエージェントは、レジストリからキーペアを読み取り、秘密鍵で署名されたサービスキーを含むSSL対応のWebSocketリクエストをDelivery Controllerに生成します。
5. Delivery Controllerは、FMAトラストサービスからの公開鍵を使用して、署名されたサービスキー認証ヘッダーを検証します。
6. 検証が完了すると、システムはVDAとDelivery Controller間のWebSocket接続を確立します。

LHCモードがアクティブになった場合

LHCのWebSocketサポートを有効にすると、LHCモード中にVDAがHigh Availability ServiceとのWebSocket接続を確立しようとした際、High Availability Serviceはローカルデータベースからの公開鍵を使用して署名されたサービスキー認証ヘッダーを検証します。これによりWebSocket接続が認証され、LHCモードでもVDAとDelivery Controller間のWebSocket接続が成功します。

WebSocketのサポート

始める前に

1. サイトを構成します。詳細については、「サイトの作成」を参照してください。
2. Delivery Controller に TLS 証明書をインストールします。詳細については、「Controller への TLS サーバー証明書のインストール」を参照してください。
3. Delivery Controller を信頼するように、VDA にルート CA および中間 CA をインストールします。

手順

WebSocket 接続を設定するには、次の手順に従います。

1. Delivery ControllerでWebSocket接続を有効にします。サイト上の各Delivery Controllerで次のコマンドを実行します。

   ```
   New-ItemProperty "HKLM:\SOFTWARE\Citrix\DesktopServer\WorkerProxy" -Name "WebSocket_Enabled" -PropertyType "DWord" -Value 1 -Force
   ```

2. WebSocket を有効にした後、Broker Service を再起動します。

3. LHC モードの WebSocket サポートを有効にします。サイトに存在する各 Delivery Controller で次のコマンドを実行します。

```
New-ItemProperty "HKLM:\SOFTWARE\Citrix\DesktopServer\LHC" -Name
"WebSocketEnabledLhc" -PropertyType "DWord" -Value 1 -Force
```

4. MCS プロビジョニングを使用して、AD 参加済み VDA のマシンカタログを作成します。詳細については、「マシンカタログの作成」を参照してください。
5. デリバリーグループを作成し、VDA を追加します。詳細については、「デリバリーグループの作成」を参照してください。
6. VDA で WebSocket 接続を有効にします。VDA で次の PowerShell コマンドを実行します。

```
New-ItemProperty
"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CitrixBrokerAgent
\WebSocket" -Name "Enabled" -PropertyType "DWord" -Value 1 -Force
```

- WebSocket が有効になっているか確認するには、次のレジストリキーの値をチェックします。`Enabled` の値は 1 である必要があります。

  キー:

  ```
  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CitrixBrokerAge
  nt\WebSocket
  ```

  名前: Enabled

  種類: REG_DWORD

  値: 1

HDX™ 接続性

Citrix HDXは、あらゆるデバイスおよびあらゆるネットワーク上で、集中型アプリケーションおよびデスクトップのユーザーに高精細なエクスペリエンスを提供する幅広いテクノロジーのセットを表しています。

HDXは、次の3つの技術原則に基づいて設計されています。

- インテリジェントなリダイレクト
- 適応型圧縮
- データ重複排除

これらをさまざまな組み合わせで適用すると、ITエクスペリエンスとユーザーエクスペリエンスが最適化され、帯域幅の消費が削減され、ホスティングサーバーあたりのユーザー密度が向上します。

HDXの機能では、独自のプロプライエタリなトランスポートプロトコルを介して接続し、セッション確立時に最大伝送ユニットを利用し、Citrix SD-WANで接続を最適化できます。

アダプティブトランスポート

アダプティブトランスポートは、Citrix Virtual Apps and Desktops™のメカニズムであり、優先トランスポートプロトコルを使用してHDXセッションの接続を確立し、優先プロトコルでの接続が利用できない場合はTCPへのフォールバックを提供します。

次のトランスポートプロトコルがサポートされています。

- エンライトンド データ トランスポート (EDT)
- 伝送制御プロトコル (TCP)

構成

アダプティブトランスポートはデフォルトで有効になっています。アダプティブトランスポートは、以下のモードで動作するように構成できます。

- **優先**: (デフォルト) クライアントは優先プロトコルで接続を試行し、優先プロトコルでの接続が利用できない場合はTCPにフォールバックします。

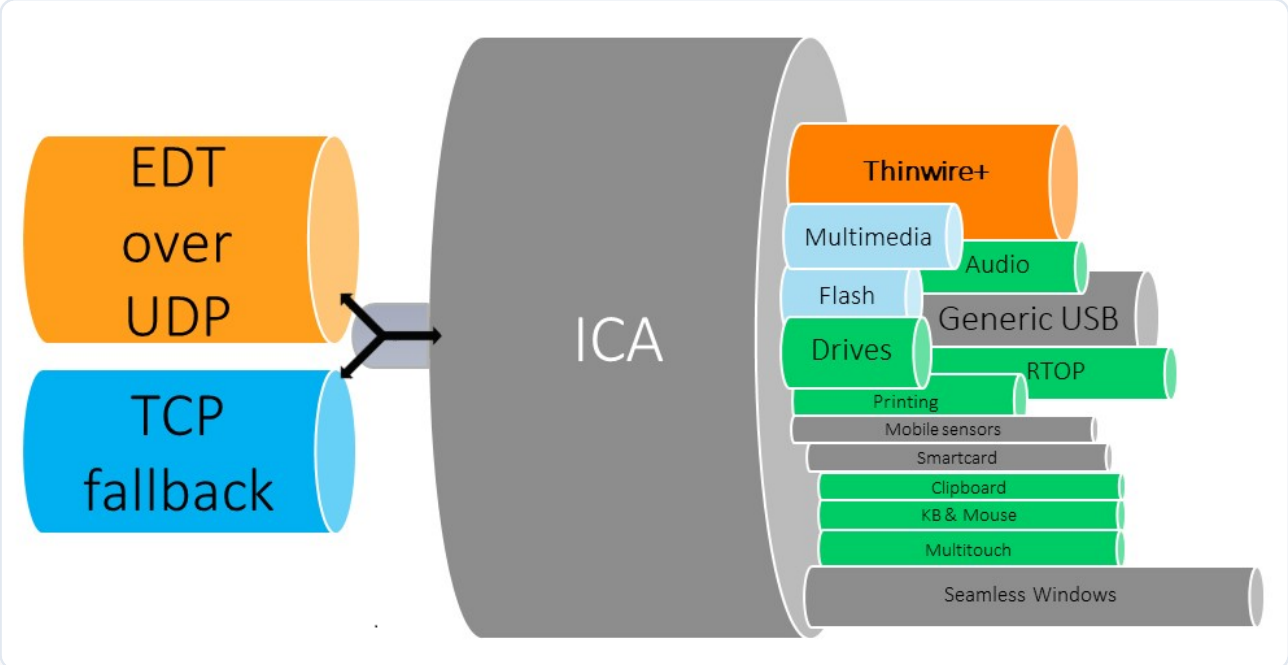
- **診断モード**: クライアントは優先プロトコルのみを使用して接続を試行します。TCPへのフォールバックは無効になります。
- **オフ**: クライアントはTCPのみを使用して接続を試行します。

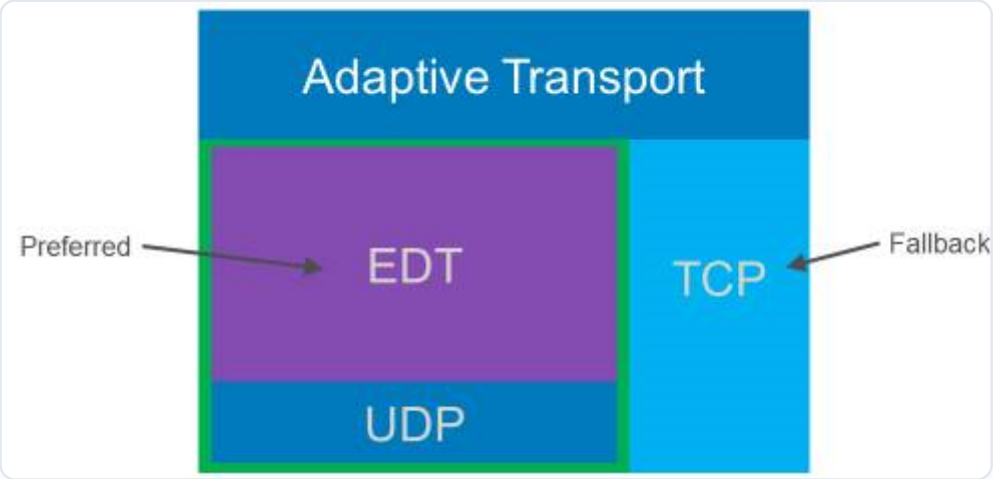
動作の仕組み

アダプティブトランスポートが`Preferred`に設定されている場合、クライアントは優先プロトコルとTCPの両方でセッションへの接続を並行して試行します。これにより、優先プロトコルで接続できない場合や、クライアントがTCPの使用にフォールバックする必要がある場合に、接続時間を最適化できます。TCPを使用して接続が確立された場合、クライアントは5分ごとにバックグラウンドで優先プロトコルでの接続を試行します。

アダプティブトランスポートが`Diagnostic mode`に設定されている場合、クライアントは優先プロトコルのみでセッションに接続します。クライアントが優先プロトコルを使用して接続を確立できない場合、TCPへのフォールバックは行われず、接続は失敗します。

アダプティブトランスポートが`Off`に設定されている場合、**アダプティブトランスポート**は無効になり、クライアントはTCPのみを使用してセッションに接続します。





システム要件

アダプティブトランスポートとEDTを使用するための要件は次のとおりです。

- コントロールプレーン
  - シトリックス DaaS（旧称 シトリックス バーチャル アプリケーションズ アンド デスクトップス サービス）
  - Citrix Virtual Apps and Desktops：現在サポートされているバージョン
- バーチャル デリバリー エージェント
  - Windows：現在サポートされているバージョン（2402以降を推奨）
  - Linux：現在サポートされているバージョン（2402以降を推奨）
- Citrix Workspace™ アプリ
  - Windows：現在サポートされているバージョン（2402以降を推奨）
  - Linux：現在サポートされているバージョン（2402以降を推奨）
  - Mac：現在サポートされているバージョン（2402以降を推奨）
  - iOS：Apple App Storeで入手可能な最新バージョン
  - Android：Google Playで入手可能な最新バージョン
- シトリックス ネットスケーラー® ゲートウェイ
  - 14.1.12.30 以降 (推奨)
  - 13.1.17.42 以降 (13.1-52.19 以降を推奨)

> **注:**

Linux VDAの詳細については、Linux Virtual Delivery Agentのドキュメントを参照してください。

ネットワーク要件

EDTをアダプティブトランスポートで使用するためのネットワーク要件を以下に示します。

セッションホスト

セッションホストにWindows Defender ファイアウォールなどのファイアウォールがある場合は、内部接続に対して以下の受信トラフィックを許可する必要があります。

説明	ソース	プロトコル	ポート
内部接続 - セッションの信頼性が有効	クライアント	UDP	2598
内部接続 - セッションの信頼性が無効			1494
内部接続 - HDX™ Direct または VDA SSL			443

注:

VDAインストーラーは、Windows Defender ファイアウォールに適切な受信規則を追加します。別のファイアウォールを使用する場合は、上記の規則を追加する必要があります。

内部ネットワーク

次の表に、ネットワークでEDTを使用するために必要なファイアウォール規則を示します。

説明	プロトコル	送信元	宛先	宛先ポート
直接内部接続 - セッションの信頼性が有効	UDP	クライアントネットワーク	VDAネットワーク	2598

説明	プロトコル	送信元	宛先	宛先ポート
直接内部接続 - セッションの信頼性が無効				1494
直接内部接続 - HDX DirectまたはVDA SSL				443
ネットスケーラー ゲートウェイ		NetScaler SNIP		2598
ネットスケーラー ゲートウェイ - VDA SSL				443

注:

Citrix Gateway Service を使用している場合、EDT をトランスポートプロトコルとして使用するには、**Rendezvous** を有効にする必要があります。システムおよびネットワーク要件については、Rendezvous ドキュメントを参照してください。

クライアントネットワーク

以下の表は、クライアントデバイスの接続要件を示しています。

説明	プロトコル	ソース	宛先	宛先ポート
内部接続 - セッションの信頼性が有効	UDP	クライアントIP	VDAネットワーク	2598
内部接続 - セッションの信頼性が無効				1494

説明	プロトコル	ソース	宛先	宛先ポート
内部接続 - HDX Direct または SSL VDA				443
外部接続 - NetScaler Gateway			NetScaler Gateway パブリック IP アドレス	443
外部接続 - Citrix Gateway Service			Citrix Gateway サービス	443

注:

Citrix Gateway Serviceを使用している場合、クライアントは`<https://*.*.nssvc.net>`に到達できる必要があります。`<https://*.*.nssvc.net>`を使用してすべてのサブドメインを許可できない場合は、代わりに`<https://*.c.nssvc.net>`と`<https://*.g.nssvc.net>`を使用できます。詳細については、Knowledge Centerの記事CTX270584を参照してください。

エンライトンド データ トランスポート

Enlightened Data Transport (EDT) は、ユーザーデータグラムプロトコル (UDP) 上に構築されたCitrix 独自のトランスポートプロトコルです。これにより、困難な長距離接続でも優れたユーザーエクスペリエンスを提供し、サーバーのスケーラビリティを維持します。EDT は、信頼性の低いネットワーク上のすべての ICA® 仮想チャネルのデータスループットを向上させ、より良く、より一貫したユーザーエクスペリエンスを提供します。

Adaptive Transport が有効になっている場合、EDT が推奨プロトコルです。

知っておくべきこと

- NetScaler® Gateway および Citrix Gateway Service で **MTU Discovery** と EDT を使用するには、**Session Reliability** を有効にする必要があります。
- パケットの断片化は、パフォーマンスの低下や、場合によってはセッションを開けない原因となることがあります。これを防ぐには、EDT MTU をネットワークに適した値に調整する必要

があります。EDT MTU Discovery を使用するか、非標準 MTU のネットワークで EDT を使用する場合の MSS の構成方法 に記載されている手動の回避策を使用できます。

- NetScaler Gateway で EDT の使用を有効にする方法の詳細については、Enlightened Data Transport をサポートするように NetScaler Gateway を構成する を参照してください。

EDT MTU検出

MTU Discovery を使用すると、EDT はセッションを確立する際に最大転送単位 (MTU) を自動的に決定できます。これにより、パフォーマンスの低下やセッションの確立の失敗につながる可能性のある EDT パケットの断片化を防ぎます。

MTU Discovery はデフォルトで有効になっています。無効にする必要がある場合は、詳細についてレジストリで管理される HDX 機能 を参照してください。

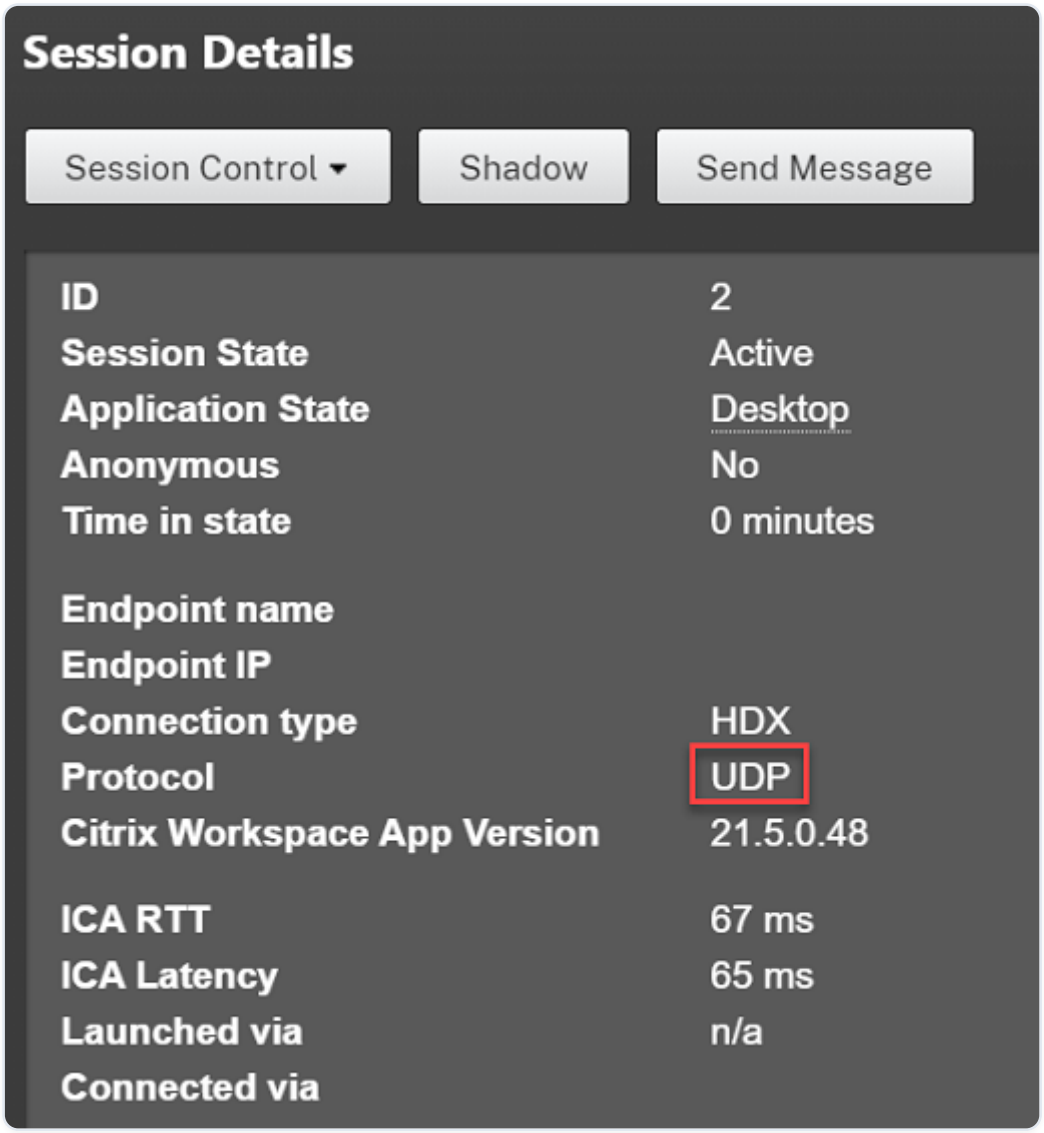
非対称パスを介した動的ルーティングによりセッションの MTU が変更される可能性があるシナリオでは、MTU Discovery はセッションの MTU を検出してそれに応じて調整することもできます。再検出はデフォルトで無効になっています。有効にするには、レジストリで管理される HDX 機能 を参照してください。

> **注:**
>
> - MTU Discovery が機能するには、**Session Reliability** を有効にする必要があります。
> - Multi-Stream ICA を使用した MTU Discovery は、VDA バージョン 2209 以降で利用可能です。

トラブルシューティング

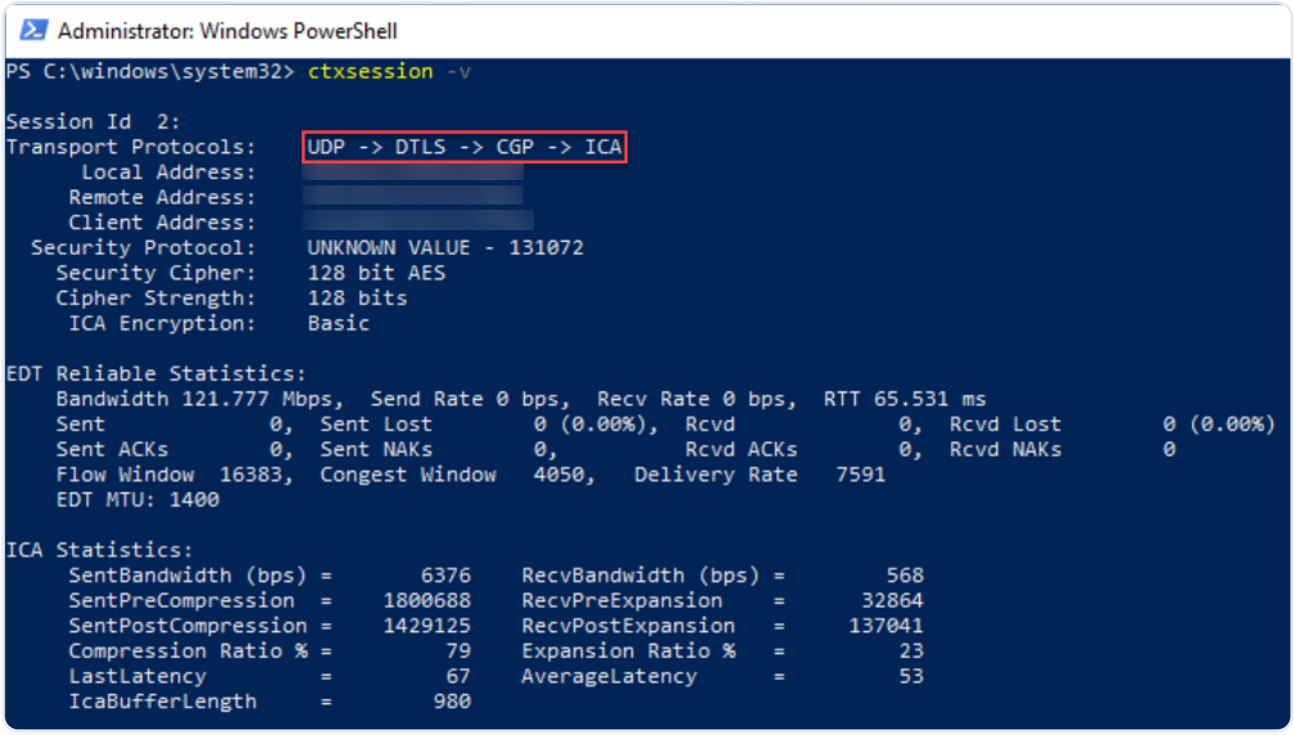
セッションのトランスポートプロトコルとしてEDTが使用されていることを確認するには、DirectorまたはVDA上の`CtxSession.exe`コマンドラインユーティリティを使用できます。

Directorでセッションを検索し、**詳細**を選択します。**接続の種類**が`HDX`で、**プロトコル**が`UDP`の場合、EDTがセッションのトランスポートプロトコルとして使用されています。



CtxSession.exeユーティリティを使用するには、セッション内でコマンドプロンプトまたはPowerShellを起動し、`ctxsession.exe`を実行します。詳細な統計情報を表示するには、`ctxsession.exe -v`を実行します。EDTが使用されている場合、トランスポートプロトコルは次のいずれかを表示します。

- **UDP > ICA®** (セッションの信頼性が無効)
- **UDP > CGP > ICA** (セッションの信頼性が有効)
- **UDP > DTLS > CGP > ICA** (ICAはDTLSでエンドツーエンド暗号化されています)



EDTでセッションが接続に失敗する場合

アダプティブトランスポートと**EDT**のトラブルシューティングには、以下をお勧めします。

1. システム要件、ネットワーク要件、既知の問題、および留意事項を確認し、すべての項目が対処されていることを確認してください。
2. StudioまたはGPOに、目的の**HDXアダプティブトランスポート**設定を上書きするCitrix®ポリシーがないか確認します。
3. クライアントに、目的のHDXアダプティブトランスポート設定を上書きする設定がないか確認します。これは、GPO設定、オプションのWorkspaceアプリ管理テンプレートを使用して構成された設定、またはレジストリやクライアントの構成ファイルでの**HDXoverUDP**設定の手動構成である可能性があります。
4. マルチセッションVDAマシンで、UDPリスナーがアクティブであることを確認します。VDAマシンでコマンドプロンプトを開き、`netstat -a -p udp`を実行します。詳細については、「HDX Enlightened Data Transportプロトコルを確認する方法」を参照してください。
5. ネットワークファイアウォールとVDAマシンで実行されているファイアウォールの両方で、適切なファイアウォールルールが構成されているか確認します。
6. NetScaler® GatewayまたはCitrix Gateway Serviceをバイパスして内部で直接セッションを起動し、使用中のプロトコルを確認します。セッションがEDTを使用している場合、VDAはNetScaler GatewayまたはCitrix Gateway Serviceを介した外部接続にEDTを使用する準備ができています。

7. EDTが直接内部接続では機能するが、NetScaler GatewayまたはCitrix Gateway Serviceを介するセッションでは機能しない場合：
   - **セッションの信頼性**が有効になっていることを確認します。
   - NetScaler Gatewayを使用している場合は、Enlightened Data TransportおよびHDX Insightをサポートするように NetScaler Gatewayを構成するに記載されている必要な構成に準拠していることを確認してください。
8. Citrix Gateway Serviceを使用している場合は、Rendezvousが有効になっていて機能していることを確認してください。
9. ユーザーの接続に非標準のMTUが必要かどうかを確認します。実効MTUが1500バイト未満の接続ではEDTパケットの断片化が発生し、パフォーマンスに影響を与えたり、セッション起動の失敗を引き起こしたりする可能性があります。この問題は、VPN、一部のWi-Fiアクセスポイント、4Gや5Gなどのモバイルネットワークを使用している場合に一般的です。MTU Discoveryが有効になっているか、非標準MTUのネットワークでEDTを使用する際のMSSの構成方法に記載されているようにカスタムMTUを設定していることを確認してください。

既知の問題

- 非対称ネットワークパスは、NetScaler GatewayまたはCitrix Gateway Serviceを介さない接続でMTU Discoveryの失敗を引き起こす可能性があります。この問題に対処するには、VDAバージョン2103以降にアップグレードしてください。
- NetScaler Gatewayを使用している場合、非対称ネットワークパスはMTU Discoveryの失敗を引き起こす可能性があります。これは、Gatewayの問題により、EDTパケットヘッダーのDon't Fragment（DF）ビットが伝播されないためです。この問題の修正は、ファームウェアリリース13.1ビルド17.42以降で利用可能です。修正を有効にする方法の詳細については、NetScaler Gatewayのドキュメントを参照してください。
- DS-Liteネットワークを介して接続するユーザーの場合、MTU Discoveryが失敗することがあります。一部のモデムでは、パケット処理が有効になっている場合にDFビットが尊重されず、MTU Discoveryが断片化を検出できないことがあります。この状況では、以下のオプションが利用可能です。
  - ユーザーのモデムでパケット処理を無効にします。
  - **MTU Discovery**を無効にし、非標準MTUのネットワークでEDTを使用する際のMSSの構成方法に記載されているようにハードコードされたMTUを使用します。
  - セッションにTCPの使用を強制するために**Adaptive Transport**を無効にします。ユーザーの一部のみが影響を受ける場合は、他のユーザーがEDTを引き続き使用できるように、クライアント側で無効にすることを検討してください。

HDX™ ダイレクト

Citrixが提供するリソースにアクセスする際、直接通信が可能な場合、HDX Directは内部および外部のクライアントデバイスがセッションホストとの安全な直接接続を確立することを可能にします。

システム要件

HDX Directを使用するためのシステム要件は以下のとおりです。

- コントロールプレーン
  - シトリックス DaaS™
  - シトリックス Virtual Apps and Desktops™ 2503 以降
- バーチャル デリバリー エージェント (VDA)
  - Windows: バージョン 2503 以降
- ワークスペース アプリ
  - Windows: バージョン 2503 以降
  - Linux: バージョン 2411 以降
  - Mac: バージョン 2411 以降
- アクセスティア
  - シトリックス ワークスペース™
  - シトリックス ストアフロント™ 2503 以降
  - シトリックス ゲートウェイ サービス
  - シトリックス ネットスケーラー® ゲートウェイ

ネットワーク要件

以下は、HDX Direct を使用するためのネットワーク要件です。

セッションホスト

セッションホストに Windows Defender ファイアウォールなどのファイアウォールがある場合は、内部接続のために以下の受信トラフィックを許可する必要があります。

説明	ソース	プロトコル	ポート
直接内部接続	クライアント	TCP	443
直接内部接続	クライアント	UDP	443

注:

VDAインストーラーは、Windows Defender ファイアウォールに適切な受信ルールを追加します。別のファイアウォールを使用している場合は、上記のルールを追加する必要があります。

クライアントネットワーク

以下の表は、内部および外部ユーザー向けのクライアントネットワークについて説明しています。

内部ユーザー

説明	プロトコル	送信元	送信元ポート	宛先	宛先ポート
直接内部接続	TCP	クライアントネットワーク	1024–65535	VDAネットワーク	443
直接内部接続	UDP	クライアントネットワーク	1024–65535	VDAネットワーク	443

外部ユーザー

説明	プロトコル	ソース	ソースポート	宛先	宛先ポート
STUN (外部ユーザーのみ)	UDP	クライアントネットワーク	1024〜65535	インターネット (下記の注記を参照)	3478, 19302
外部ユーザー接続	UDP	クライアントネットワーク	1024〜65535	データセンターのパブリックIPアドレス	1024–65535

データセンターネットワーク

次の表は、内部ユーザーと外部ユーザー向けのデータセンターネットワークについて説明しています。

内部ユーザー

説明	プロトコル	送信元	ソースポート	宛先	宛先ポート
直接内部接続	TCP	クライアントネットワーク	1024–65535	VDAネットワーク	443
直接内部接続	UDP	クライアントネットワーク	1024–65535	VDAネットワーク	443

外部ユーザー

説明	プロトコル	送信元	ソースポート	宛先	宛先ポート
STUN（外部ユーザーのみ）	UDP	VDAネットワーク	1024–65535	インターネット (下記の注記を参照)	3478, 19302
外部ユーザー接続	UDP	DMZ / 内部ネットワーク	1024–65535	VDAネットワーク	55000–55250
外部ユーザー接続	UDP	VDAネットワーク	55000–55250	クライアントのパブリックIP	1024〜65535

注：

VDAとWorkspaceアプリの両方が、以下のサーバーに同じ順序でSTUNリクエストを送信しようとします。

- stun.cloud.com:3478

- stun.cloudflare.com:3478
- stun.l.google.com:19302

HDX Directポート範囲ポリシー設定を使用して外部ユーザー接続のデフォルトポート範囲を変更した場合、対応するファイアウォールルールはカスタムポート範囲と一致する必要があります。

構成

HDX Directはデフォルトで無効になっています。この機能は、Citrixポリシーの**HDX Direct**設定を使用して構成できます。

- **HDX Direct**: 機能を有効または無効にする場合。
- **HDX Directモード**: **HDX Direct**が内部クライアントのみで利用可能か、内部クライアントと外部クライアントの両方で利用可能かを決定します。
- **HDX Directポート範囲**: VDAが外部クライアントからの接続に使用するポート範囲を定義します。

必要に応じて、HDX Directで使用されるSTUNサーバーのリストは、以下のレジストリ値を編集することで変更できます。

- キー：HKLM\SOFTWARE\Citrix\HDX-Direct
- 値の型: REG_MULTI_SZ
- 値の名前：STUNServers
- データ：stun.cloud.com:3478 stun.cloudflare.com:3478 stun.l.google.com:19302

注：

外部ユーザー向けのHDX Directは、転送プロトコルとしてEDT (UDP) を使用する場合にのみ利用可能です。そのため、Adaptive Transportを有効にする必要があります。

考慮事項

HDX Directを使用する際の考慮事項は次のとおりです。

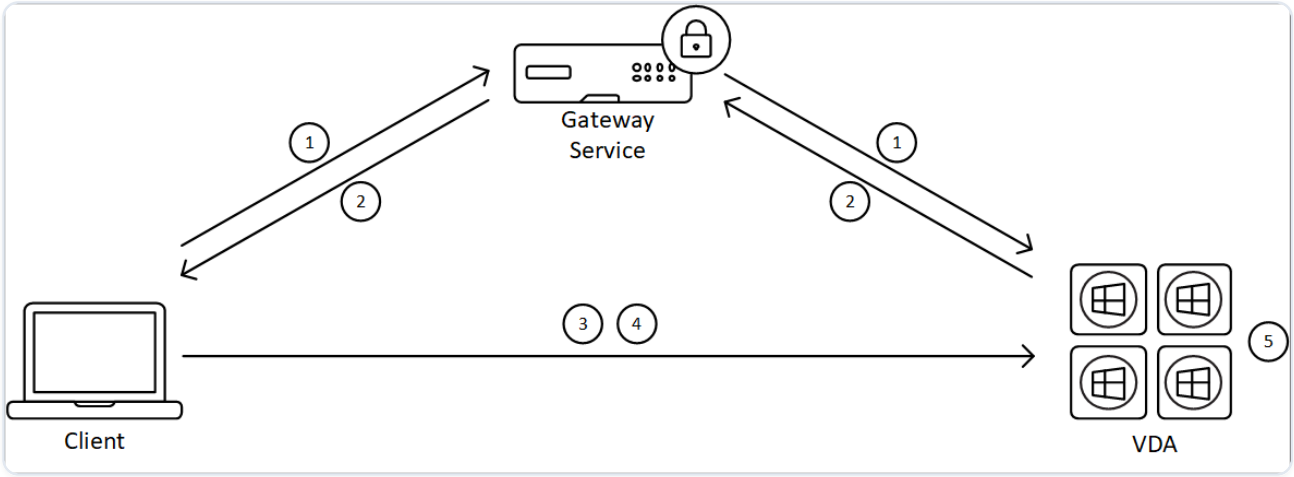
- 外部ユーザー向けのHDX Directは、転送プロトコルとしてEDT (UDP) を使用する場合にのみ利用可能です。そのため、**Adaptive Transport**を有効にする必要があります。
- **HDX Insight**を使用している場合、**HDX Direct**を使用すると、セッションがNetScaler Gatewayを介してプロキシされなくなるため、HDX Insightのデータ収集が妨げられることに注意してください。

動作の仕組み

HDX Directを使用すると、直接通信が可能な場合、クライアントはセッションホストへの直接接続を確立できます。HDX Directを使用して直接接続が行われる場合、ネットワークレベルの暗号化 (TLS/DTLS) で直接接続を保護するために自己署名証明書が使用されます。

内部ユーザー

次の図は、内部ユーザーのHDX Direct接続プロセスの概要を示しています。



1. クライアントはGateway Serviceを介してHDXセッションを確立します。
2. 接続が成功すると、VDAはHDX接続を介して、VDAマシンのFQDN、そのIPアドレスのリスト、およびVDAマシンの証明書をクライアントに送信します。
3. クライアントは、VDAに直接到達できるかどうかを確認するためにIPアドレスをプローブします。
4. クライアントが共有されたいずれかのIPアドレスでVDAに直接到達できる場合、クライアントはVDAとの直接接続を確立します。この接続は、ステップ(2)で交換された証明書と一致する証明書を使用して(D)TLSで保護されます。
5. 直接接続が正常に確立されると、セッションは新しい接続に転送され、Gateway Serviceへの接続は終了します。

> **注:**

> 上記のステップ2で接続を確立した後、セッションはアクティブになります。その後の手順は、ユーザーが仮想アプリケーションまたはデスクトップを使用する能力を遅らせたり、妨げたりすることはありません。その後の手順のいずれかが失敗した場合でも、Gatewayを介した接続はユーザーのセッションを中断することなく維持されます。

従来の直接接続

Storefront、Direct Workload Connectionを備えたWorkspace、または内部接続専用に構成されたWorkspaceを使用する場合、クライアントとセッションホストの間で直接接続が確立され、最初にGatewayを介してルーティングする必要はありません。

これらの場合、接続は本質的に直接的であるため、HDX Directはトリガーされません。ただし、HDX Directが有効になっている場合、これらの接続はHDX Direct証明書を利用してセッションを保護します。

外部ユーザー

次の図は、外部ユーザー向けのHDX Direct接続プロセスの概要を示しています。

HDX Direct接続プロセス(/en-us/citrix-virtual-apps-desktops/2503/media/hdx-direct-connection-process.png)

1. クライアントはGateway Serviceを介してHDXセッションを確立します。
2. 接続が成功すると、クライアントとVDAの両方がSTUNリクエストを送信して、それぞれのパブリックIPアドレスとポートを検出します。
3. STUNサーバーは、クライアントとVDAにそれぞれのパブリックIPアドレスとポートで応答します。
4. HDX接続を介して、クライアントとVDAはそれぞれのパブリックIPアドレスとUDPポートを交換し、VDAはクライアントに証明書を送信します。
5. VDAは、クライアントのパブリックIPアドレスとUDPポートにUDPパケットを送信します。クライアントは、VDAのパブリックIPアドレスとUDPポートにUDPパケットを送信します。
6. VDAからのメッセージを受信すると、クライアントはセキュアな接続要求で応答します。
7. DTLSハンドシェイク中に、クライアントは証明書がステップ(4)で交換された証明書と一致することを確認します。検証後、クライアントは認証トークンを送信します。これでセキュアな直接接続が確立されます。
8. 直接接続が正常に確立されると、セッションは新しい接続に転送され、Gateway Serviceへの接続は終了します。

> **注:**
>
> 上記のステップ2で接続が確立された後、セッションはアクティブになります。その後のステップは、ユーザーが仮想アプリケーションまたはデスクトップを使用する能力を遅らせたり、妨げたりすることはありません。その後のステップのいずれかが失敗した場合でも、Gatewayを介した接続はユーザーのセッションを中断することなく維持されます。

証明書管理

概要

HDX™ Direct接続は、ネットワークレベルの暗号化によって保護されています。これを容易にするため、各セッションホストには一意の自己署名ルートCA証明書と、その自己署名ルートCA証明書によって署名された対応するサーバー証明書があります。

このソリューションには、次の利点があります。

- **セキュリティの合理化:** HDX Direct接続は、環境内で証明書を管理する管理上のオーバーヘッドなしに保護されます。
- **攻撃対象領域の削減:** 各ホストは一意のキーと証明書のセットを持つため、攻撃対象領域は単一のホストに限定されます。
- **非永続環境のセキュリティ強化:** 非永続セッションホストを持つ環境では、再起動時に新しいキーと証明書が生成されるため、セキュリティがさらに強化されます。

セッションホスト

Citrix ClxMtp Service と **Citrix Certificate Manager Service** は、各セッションホストで証明書を管理する2つのサービスです。ClxMtp Serviceはキーの生成とローテーションを処理し、Certificate Manager Serviceは証明書を生成および管理します。

自己署名ルートCAとサーバー証明書の2つの証明書が作成されます。どちらも2年間の有効期間で発行されますが、キーがローテーションされると置き換えられます。さらに、非永続マシンが再起動するたびに新しい証明書が生成されます。

各証明書の詳細は次のとおりです。

- **自己署名ルートCA**
  - 発行先は CA-Citrix-Certificate-Manager です
  - 発行元はCA-Citrix-Certificate-Managerです。

    - 発行者の詳細: 組織はCitrix Systems, Inc.です。

- **サーバー証明書**

    - 発行先: \<ホストFQDN\> (例: FTLW11-001.ctxlab.net)
    - 発行元: CA-Citrix-Certificate-Manager
    - 発行元詳細: 組織はCitrix Systems, Inc.

> **注：**
>
> Citrix Certificate Managerサービスは、2048ビットのキーを利用するRSA証明書を生成します。

> Citrix Certificate Managerサービスによって作成された既存のマシン証明書があり、そのサブジェクト名がマシンのFQDNと一致しない場合、新しい証明書が生成されます。

キーのローテーション

Citrix ClxMtp Serviceは、6か月ごとにキーを自動的にローテーションします。ただし、セッションホストのレジストリでローテーションカウンターを増やすことで、手動でキーのローテーションをトリガーできます。

キーをローテーションするには、次の値を更新します。

- キー: SOFTWARE\Citrix\ClxMtpConnectorSvcRotateKeyPairs
- 値の型: DWORD
- 値の名前: ClxMtpRotateRequestCounter
- データ: 整数 (10進数)

> **注：**
>
> 初めてキーをローテーションする場合:

1. ClxMtpConnectorSvcRotateKeyPairsキーを作成します。
2. ClxMtpRotateRequestCounter値を1に作成して設定します。

その後のキーのローテーションでは、ClxMtpRotateRequestCounter値を1増やします。

値が更新されると、**Citrix ClxMtp Service** は再起動を必要とせずにキーを自動的にローテーションします。その後、**Citrix Certificate Manager Service** は新しいキーを検出すると、新しい証明書を自動的に生成します。

クライアントデバイス

ルートCA証明書は、WorkspaceまたはStorefront™によって、すでに確立されている安全で信頼された接続パスを介してクライアントに送信されます。これにより、CA証明書をクライアントデバイスの証明書ストアに配布する必要がなくなり、クライアントがHDX Direct接続のセキュリティ保護に使用される証明書を信頼するようになります。

カスタム証明書の使用

HDX Directは、独自のPKIによって発行および管理される証明書の使用をサポートしています。以下の手順では、証明書のインストール方法、必要な権限の構成方法、セッションマネージャーサービスへのバインド方法、および必要なTLSリスナーの有効化方法について説明します。

1. マシンでHDX Directが無効になっている場合は、ステップ2に進みます。HDX Directが有効になっている場合は、以下の手順に従ってください。
    a. レジストリエディター (regedit.exe) を開き、**HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd** に移動します。
    b. **SSLEnabled** の値を **0** に設定します。
    c. **HKLM\Software\Citrix\HDX-Direct** に移動します。
    d. **HdxDirectCaInTls** の値を **0** に設定します。
2. PKIによって発行された適切な証明書を、マシンの証明書ストアにインストールします。
3. セッションマネージャーサービスに証明書の秘密キーへの読み取りアクセス権を付与します。
    a. Microsoft 管理コンソール (**MMC**) を起動します: > > mmc.exe。
    b. **ファイル > スナップインの追加と削除**に移動します。
    c. **証明書**を選択し、**追加**をクリックします。
    d. **コンピューターアカウント**を選択し、**次へ**をクリックします。
    e. **ローカルコンピューター**を選択し、**完了**をクリックします。
    f. **証明書 (ローカルコンピューター) > 個人 > 証明書**に移動します。
    g. 適切な証明書を右クリックし、**すべてのタスク > 秘密キーの管理**を選択します。

h. 次のいずれかのサービスを追加し、読み取りアクセス権を付与します。

- **シングルセッションVDA**の場合: `NT SERVICE\PorticaService`
- **マルチセッションVDA**の場合: `NT SERVICE\TermService`

i. **適用**をクリックし、次に**OK**をクリックします。

4. 証明書をセッションマネージャーサービスにバインドします。

a. 証明書のサムプリントを取得します (証明書をダブルクリック > **詳細** > **サムプリント**)。

b. レジストリエディター (regedit.exe) を開き、**HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd**に移動します。

c. 「**SSLThumbprint**」の値を編集し、証明書のサムプリントを貼り付けます。

5. Citrix TLSリスナーを有効にします。

a. 同じレジストリの場所で、「**SSLEnabled**」の値を「**1**」に設定します。

6. HDX Directを有効にします（Citrixポリシー内）。

Citrix Virtual Apps and Desktopsのインストールメディアには、これらのタスクのいくつかを自動化するPowerShellスクリプト（Enable-VdaSSL.ps1）が含まれています。

- 証明書のキーのアクセス許可を設定する
- 証明書をセッションマネージャーサービスにバインドする
- Citrix TLSリスナーを有効にする

このスクリプトは、Support > Tools > SslSupportディレクトリにあります。詳細については、「PowerShellスクリプトを使用してVDAでTLSを構成する」を参照してください。

> **注：**
>
> 独自の証明書を使用している場合、セッションホストに接続するデバイスには、正しいルートCA証明書と中間CA証明書がインストールされている必要があります。

NAT互換性

外部ユーザーデバイスとセッションホスト間の直接接続を確立するために、HDX™ DirectはNATトラバーサルのためにホールパンチングを利用し、クライアントデバイスとセッションホストの

パブリックIPアドレスとポートマッピングの交換を容易にするためにSTUNを利用します。これは、VoIP、ユニファイドコミュニケーション、P2Pソリューションの仕組みと似ています。

ファイアウォールやその他のネットワークコンポーネントがSTUNリクエストとHDXセッションのUDPトラフィックを許可するように構成されている限り、外部ユーザー向けのHDX Directは動作すると予想されます。ただし、ユーザーとセッションホストのネットワークのNATタイプが互換性のない組み合わせとなり、HDX Directが失敗する特定のシナリオがあります。

検証

クライアントおよびセッションホスト上のNATタイプとフィルタリングは、STUNTMANのSTUNクライアントユーティリティを使用して検証できます。

1. stunprotocol.orgからターゲットプラットフォームに適したパッケージをダウンロードし、その内容を抽出します。
2. ターミナルプロンプトを開き、内容が抽出されたディレクトリに移動します。
3. NATバインディングおよび動作テストを実行するには、次のコマンドを実行します。
   `stunclient.exe stunserver2025.stunprotocol.org --mode behavior`
4. バインディングおよび動作テストが成功した場合、**binding test**と**behavior test**の両方が成功を報告し、NATの動作が指定されます。

   テストが失敗した場合、**binding test**および/または**behavior test**が失敗を報告します。

5. NATバインディングおよびフィルタリングテストを実行するには、次のコマンドを実行します。 `stunclient.exe stunserver2025.stunprotocol.org --mode filtering`
6. バインディングおよびフィルタリングテストが成功した場合、**binding test**と**filtering test**の両方が成功を報告し、NATのフィルタリングタイプが指定されます。

   テストが失敗した場合、**binding test**および/または**filtering test**が失敗を報告します。

上記のテストを実行した後、NATの動作とフィルタリングの組み合わせに基づいて、外部ユーザー向けのHDX Directが動作すると予想されるかどうかを判断するために、次の表を確認してください。

クライアントNAT動作	クライアントNATフィルタリング	セッションホストNAT動作	セッションホストNATフィルタリング	動作が期待されるか？
エンドポイント独立マッピング	任意	エンドポイント独立マッピング	任意	はい
エンドポイント独立マッピング	エンドポイント独立フィルタリング	アドレス依存マッピング	任意	はい
エンドポイント独立マッピング	アドレス依存フィルタリング	アドレス依存マッピング	任意	いいえ
エンドポイント独立マッピング	アドレスおよびポート依存フィルタリング	アドレス依存マッピング	任意	いいえ
エンドポイント独立マッピング	エンドポイント独立フィルタリング	アドレスおよびポート依存マッピング	エンドポイント独立フィルタリング	はい
エンドポイント独立マッピング	アドレス依存フィルタリング	アドレス依存マッピング	任意	いいえ
エンドポイント独立マッピング	アドレスおよびポート依存フィルタリング	アドレス依存マッピング	任意	いいえ
アドレス依存マッピング	任意	エンドポイント独立マッピング	エンドポイント独立フィルタリング	はい
アドレス依存マッピング	任意	エンドポイント独立マッピング	アドレス依存フィルタリング	いいえ
アドレス依存マッピング	任意	エンドポイント独立マッピング	アドレスおよびポート依存フィルタリング	いいえ

クライアントNAT動作	クライアントNATフィルタリング	セッションホストNAT動作	セッションホストNATフィルタリング	動作が期待されるか？
アドレス依存マッピング	任意	アドレス依存マッピング	任意	いいえ
アドレス依存マッピング	任意	アドレスおよびポート依存マッピング	任意	いいえ
アドレスおよびポート依存マッピング	任意	エンドポイント独立マッピング	エンドポイント独立フィルタリング	はい
アドレスおよびポート依存マッピング	任意	エンドポイント独立マッピング	アドレス依存フィルタリング	いいえ
アドレスおよびポート依存マッピング	任意	エンドポイント独立マッピング	アドレスおよびポート依存フィルタリング	いいえ
アドレスおよびポート依存マッピング	任意	アドレス依存マッピング	任意	いいえ
アドレスおよびポート依存マッピング	任意	アドレスおよびポート依存マッピング	任意	いいえ
失敗	任意	任意	任意	いいえ
任意	任意	失敗	任意	いいえ
失敗	任意	失敗	任意	なし

トラブルシューティング

HDX Direct が直接接続を正常に確立したことを確認するには、VDA マシンで `CtxSession.exe` ユーティリティを使用できます。

`CtxSession.exe` ユーティリティを使用するには、セッション内でコマンドプロンプトまたは PowerShell を起動し、`ctxsession.exe -v` を実行します。**HDX Direct** 接続が正常に確立されている場合、**HDX Direct Status** は `Connected` です。

HDX Direct のトラブルシューティング(/en-us/citrix-virtual-apps-desktops/2503/media/hdx-direct-troubleshooting.png)

セッションホストのイベントログで、HDX™ Direct 接続が正常に確立されたか、または失敗したかに関する情報を確認することもできます。詳細については、「**イベントログ**」セクションを参照してください。

> 注:
>
> 環境およびセッションホストで利用可能な IP アドレスの数によっては、HDX Direct 接続が確立されるまでに最大 5 分かかる場合があります。

HDX Direct が直接接続を確立できない場合

HDX Direct が直接接続を確立できない場合は、次の手順を確認してください。

1. 使用している VDA バージョンと Workspace アプリバージョンが、システム要件に従ってこの機能をサポートしていることを確認します。
2. HDX Direct を有効にするポリシーが VDA に適用されており、この機能を無効にする優先度の高い他のポリシーがないことを確認します。
3. 目的の HDX Direct モードを設定するポリシーが VDA に適用されており、この構成を上書きする優先度の高い他のポリシーがないことを確認します。
4. Citrix ClxMtp Service がセッションホストで実行されていることを確認します。
5. Citrix Certificate Manager Service がセッションホストで実行されていることを確認します。実行されていない場合は、手動で開始してみてください。HDX Direct が無効になっている場合、このサービスは自動的に停止します。
6. セッションホストに自己署名ルート CA 証明書があるかどうかを確認します。
    a. 発行先: `CA-Citrix-Certificate-Manager`
    b. 発行元: `CA-Citrix-Certificate-Manager`
    c. 発行者の詳細: 組織はCitrix Systems, Inc.です。
7. セッションホストに自己署名サーバー証明書があるか確認します。

a. 発行先: `<host FQDN>` (例: FTLW11-001.ctxlab.net)

b. 発行元: `CA-Citrix-Certificate-Manager`

c. 発行者の詳細: 組織はCitrix Systems, Inc.です。

8. 証明書が見つからない場合は、Citrixテクニカルサポートにお問い合わせください。
9. 証明書が存在する場合:

a. セッションホストでCitrix Certificate Managerサービスを停止します。

b. 自己署名ルートCA証明書と自己署名サーバー証明書の両方を削除します。

c. セッションホストでCitrix Certificate Managerサービスを開始します。サービスは開始されると新しい証明書を作成します。

10. 内部ユーザーの場合:

a. セッションホストのファイアウォールが、HDX over EDTの場合はUDP 443、HDX over TCPの場合はTCP 443の受信トラフィックをブロックしていないことを確認してください。

b. クライアントネットワークとセッションホストネットワーク間のUDP 443およびTCP 443のトラフィックをネットワークファイアウォールがブロックしていないことを確認してください。

11. 外部ユーザーの場合：

a. セッションホストにSTUNサーバーのリストが含まれていることを確認します。

- キー：HKLM\SOFTWARE\Citrix\HDX-Direct
- 値の型：REG_MULTI_SZ
- 値の名前：STUNServers
- データ：stun.cloud.com:3478 stun.cloudflare.com:3478 stun.l.google.com:19302

b. クライアントとセッションホストのNATタイプを確認し、その組み合わせが機能すると予想されることを確認します。詳細については、「NAT互換性」セクションを参照してください。

c. クライアントまたはセッションホストのいずれかでNATテストが失敗した場合：

i. システムでファイアウォールが実行されている場合は、UDP 3478での送信トラフィックをブロックしていないことを確認します。

ii. ネットワークファイアウォールがUDP 3478での送信トラフィックをブロックしていないことを確認します。

iii. ファイアウォールがSTUNサーバーの応答をブロックしていないことを確認します。

d. ネットワークファイアウォールに、必要なすべてのトラフィックを許可するように適切なルールが構成されていることを確認します。詳細については、「ネットワーク要件」セクションを参照してください。

e. HDX Directポート範囲ポリシー設定を使用してデフォルトのポート範囲を変更する場合は、ファイアウォールルールがカスタムポート範囲に設定されていることを確認します。

イベントログ

以下のイベントがVDAマシンのイベントログに記録されます:

ログ	ID	送信元	レベル	説明
アプリケーションとサービスログ > Citrix-HostCore-HDX Direct/操作	1	HDX ダイレクト	情報	内部ユーザー `<username>` のHDX Direct接続が確立されました。
アプリケーションとサービスログ > Citrix-HostCore-HDX Direct/操作	2	HDX ダイレクト	情報	外部ユーザー `<username>` のHDX Direct接続が確立されました。
アプリケーションとサービスログ > Citrix-HostCore-HDX Direct/操作	3	HDX ダイレクト	情報	ユーザー `<username>` のHDX Direct接続に失敗しました。

既知の問題

- Rendezvousが無効になっている場合、Gateway Service を使用するWorkspace環境では、外部ユーザー向けのHDX Directが失敗する可能性があります。この問題を解決するには、Rendezvous が有効になっていることを確認してください。
- 既に **HDX Direct** が有効になっているマシンで VDA のインプレースアップグレードを実行した後、HDX Direct が動作しなくなる可能性があります。この問題を解決するには、次の手順を実行します。

  a. セッションホスト上でCitrix Certificate Managerサービスを停止します。

b. 自己署名ルートCA証明書と自己署名サーバー証明書を削除します。
c. レジストリを開きます。
d. `HKLM\Software\Citrix\HDX-Direct` キーを削除します。
e. `HKLM\SYSTEM\CurrentControlSet\Control\TerminalServer\Wds\icawd` にアクセスします。
f. **SSLEnabled** の値を `0` に設定します。
g. **SSLThumbprint** の値の内容を削除します。
h. **Citrix Certificate Managerサービス**を開始します。

セキュア HDX™

セキュア HDX は、トラフィックパス内のネットワーク要素が HDX トラフィックを検査できないようにするアプリケーションレベル暗号化 (ALE) ソリューションです。これは、Citrix Workspace™ アプリ (クライアント) と VDA (セッションホスト) の間で、AES-256-GCM 暗号化を使用して、アプリケーションレベルで真のエンドツーエンド暗号化 (E2EE) を提供することで実現されます。

システム要件

以下の一覧は、セキュア HDX を使用するためのシステム要件を示しています。

- コントロールプレーン
  - シトリックス DaaS™
  - シトリックス Virtual Apps and Desktops™ 2503 以降
- セッションホスト
  - オペレーティングシステム
    - Windows 10 バージョン 22H2
    - Windows 11 22H2 以降
    - Windows Server 2019 またはそれ以降
  - バーチャル デリバリー エージェント (VDA)
    - Windows: バージョン 2503 以降
    - Linux: バージョン 2407 以降

- Workspaceアプリ
  - Windows: バージョン2503以降
  - Linux: バージョン2408以降
  - Mac: バージョン2409以降
  - Chrome OS: バージョン2409以降
  - HTML5: バージョン2408以降
  - Android: バージョン2503以降
  - iOS: バージョン2503以降
- アクセスティア
  - シトリックス ワークスペース
  - Citrix StoreFront™ 2402以降

> **注：**
>
> Linux VDA で Secure HDX を構成する方法の詳細については、Linux VDA のドキュメントを参照してください。

構成

Secure HDX はデフォルトで無効になっています。この機能は、Citrix ポリシーの Secure HDX 設定を使用して構成できます。

Secure HDX: この機能を有効にするか無効にするかを定義します。

> **重要:**
>
> Secure HDX を有効にするデリバリーグループで Secure ICA® が有効になっている場合は、まず Secure ICA を無効にする必要があります (デリバリーグループの編集 > ユーザー設定)。

HDX インサイトとスマートコントロール

Secure HDX が有効になっている場合に、NetScaler Gateway で HDX Insight と SmartControl を使用するための要件は次のとおりです。

- NetScaler 14.1 Build 47.46 以降。
- Citrix ポリシーで **ネットワーク テレメトリ** を有効にする必要があります。
- **セッションの信頼性** を有効にする必要があります。この設定はデフォルトで有効になっているため、無効にするポリシーがないことを確認してください。

> **注:**
>
> Secure HDX を使用した HDX Insight と SmartControl は、次のシナリオでのみ利用できます。
>
> - トランスポートプロトコルとしてTCPを使用する接続
> - IPv4 を使用する接続
> - 次の Workspace アプリバージョンを使用するクライアント:
>   - Windows: 2503 以降
>   - Mac: 2505 以降
>   - Linux: 2508 以降

考慮事項

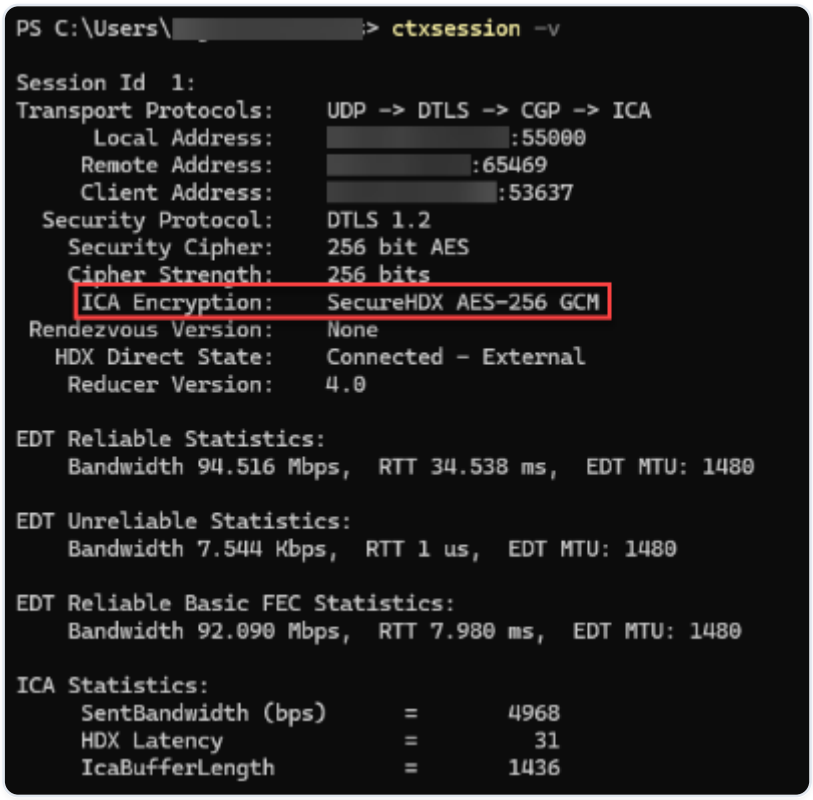
Secure HDX を使用する際の考慮事項は次のとおりです。

- ユーザーが Secure HDX が有効になっているセッションホストに、この機能をサポートしていないクライアントを使用して接続しようとすると、接続は拒否されます。
- Secure HDX でサポートされているのは、コネクタレスワークロードのサービス継続性 のみです。標準バージョンのサービス継続性を使用している場合、クラウドサービスの停止が発生すると、Secure HDX が有効になっているセッションホストには接続できません。
- Secure HDX が有効になっている場合、マルチストリーム ICA はサポートされません。
- HDX トラフィックが暗号化されるため、HDX トラフィックの検査に依存するサードパーティソリューションを使用している場合、Secure HDX を有効にするとそれらは機能しなくなります。

トラブルシューティング

Secure HDX がアクティブであることを確認するには、VDA マシンで `ctxsession.exe` ユーティリティを使用します。

`CtxSession.exe` ユーティリティを使用するには、セッション内でコマンドプロンプトまたは PowerShell を開き、`ctxsession.exe -v` を実行します。Secure HDX が使用されている場合、ICA Encryption に `SecureHDX AES-256 GCM` と表示されます。



セッションで Secure HDX が有効にならない場合

- 使用している VDA バージョンが、システム要件に従ってこの機能をサポートしていることを確認してください。
- Secure HDX を有効にするポリシーが VDA に適用されており、この機能を無効にする優先度の高い他のポリシーがないことを確認してください。
- Secure HDX を構成したときにセッションホストがすでに実行されていた場合は、変更を有効にするためにマシンを再起動してください。

仮想チャネル許可リスト

仮想チャネル許可リストは、Citrix以外の仮想チャネルのうち、どのチャネルを環境で許可するかを制御できる機能です。デフォルトでは、仮想チャネル許可リスト機能は有効になっています。その結果、Citrix Virtual Apps and Desktops™セッションでは、Citrix仮想チャネルのみが開くことが

許可されます。自社開発またはサードパーティ製のカスタム仮想チャネルを使用する必要がある場合は、それらを明示的に許可リストに追加する必要があります。

構成

仮想チャネル許可リストはデフォルトで有効になっています。この機能は、Citrixポリシーの以下の設定を使用して構成できます。

- **仮想チャネル許可リスト**: この機能を有効または無効にし、仮想チャネルをリストに追加します。
- **仮想チャネル許可リストログスロットリング**: 仮想チャネル許可リストのイベントログのスロットリング期間を設定します。
- **仮想チャネル許可リストログ記録**: 仮想チャネル許可リストのログレベルを設定します。

仮想チャネルを許可リストに追加する

仮想チャネルを許可リストに追加するには、以下の情報が必要です。

1. コードで定義されている仮想チャネル名。最大7文字です。例: `CTXCVC1`。
2. VDAマシンで仮想チャネルを開くプロセスのパス。例: `C:\Program Files\Application\run.exe`。

必要な情報が揃ったら、仮想チャネル許可リストポリシー設定を使用して、仮想チャネルを許可リストに追加する必要があります。リストに仮想チャネルを追加するには、仮想チャネル名の後にコンマ、そして仮想チャネルにアクセスするプロセスのパスを入力します。複数のプロセスがある場合は、各プロセスをコンマで区切って追加できます。

単一のプロセスの場合

前の例を使用して、次のエントリをリストに追加します。

```
CTXCVC1,C:\Program Files\Application\run.exe
```

複数のプロセスの場合

複数のプロセスがある場合は、次のエントリをリストに追加します。

```
CTXCVC1,C:\Program Files\Application\run.exe,C:\Program Files\Application\run2.exe
```

ワイルドカードの使用

ワイルドカード (*) の使用がサポートされています。アプリケーションのバージョンに基づいてディレクトリ名または実行可能ファイル名が変更される場合、またはサードパーティコンポーネントがユーザープロファイルにインストールされている場合に、ワイルドカードを使用できます。

次のシナリオでワイルドカードを使用できます。

- 完全なディレクトリ名を置き換える場合。 例: `C:\Program Files\Application*\run1.exe`
- ディレクトリ名の一部を置き換える場合。 例: `C:\Program Files\Application\v*\run1.exe`
- 実行可能ファイル名を置き換える場合。 例: `C:\Program Files\Application\v1.2*.exe`
- 実行可能ファイル名の一部を置き換える場合。 例: `C:\Program Files\Application\v1.2\run*.exe`

次の制限が適用されます。

- ワイルドカードは、単一のディレクトリを置き換えるためにのみ使用できます。たとえば、実行可能ファイルが `C:\Program Files\Application\v1.2\run1.exe` にある場合
  - 許可: `C:\Program Files\Application*\run1.exe`
  - 不許可: `C:\Program Files*\run1.exe`
- エントリにはファイル名拡張子を含める必要があります。
  - 許可: `C:\Program Files\Application\v1.2*.exe`
  - 不許可: `C:\Program Files\Application\v1.2*`
- すべてのパスはローカルである必要があります。

> **注:**
>
> - ネットワークパスは許可されていません。
> - ワイルドカードのサポートは、Citrix Virtual Apps and Desktops 2206から利用可能です。

- ワイルドカードのサポートは、Citrix Virtual Apps and Desktops 2203 LTSRのCU2から利用可能です。

システム環境変数の使用

システム環境変数を使用して、許可リスト内の信頼されたプロセスの定義を簡素化できます。`%programfiles%`、`%programfiles(x86)%`、`%systemdrive%`、および`%systemroot%`などの標準変数を使用できます。

システムレベルで定義されている限り、カスタム環境変数も使用できます。

以下の例は、標準の環境変数を示しています:

- `%programfiles%\Application\v1.2\run.exe`
- `%programfiles%\Application*\run.exe`
- `%programfiles(x86)%\Application\v1.*\run.exe`

以下の例は、カスタムシステム環境変数を示しています:

- カスタム変数名: `app`
- カスタム変数値: `%programfiles%\Application\`
- 許可リストエントリ: `CTXCVC1,%app%\run.exe`

注:

ユーザー環境変数はサポートされていません。

環境変数のサポートは、Citrix Virtual Apps and Desktops バージョン 2209 以降で利用可能です。

仮想チャネル名とプロセスを取得する

VDAマシン上で仮想チャネル名とそれを開くプロセスを取得する最も簡単な方法は、その仮想チャネルを提供した開発者またはサードパーティベンダーから情報を入手することです。

または、機能のログを適用し、以下の手順に従って情報を取得することもできます。

1. カスタム仮想チャネルのクライアントコンポーネントとサーバーコンポーネントが配置されたら、仮想アプリケーションまたは仮想デスクトップを起動します。
2. VDAマシンのシステムイベントログで、カスタム仮想チャネル名とそれを開こうとしたプロセスを探します。利用可能なイベントの詳細については、イベントログを参照してください。
3. セッションからログアウトします。
4. 特定された仮想チャネルとプロセスに対して、仮想チャネル許可リストポリシー設定にエントリを追加します。
5. マシンを再起動します。
6. VDAが登録されたら、仮想アプリケーションまたは仮想デスクトップを実行して、カスタム仮想チャネルが正常に開くことを検証します。

Citrix仮想チャネルに関する考慮事項

すべての組み込みCitrix仮想チャネルは信頼されており、追加設定なしで開くことができます。ただし、以下の2つの機能は外部依存関係があるため、許可リストに明示的なエントリが必要です。

- マルチメディアリダイレクト
- スカイプ フォー ビジネス向け HDX リアルタイム最適化パック

マルチメディアリダイレクト

Windows Media Player以外のメディアプレーヤーをシステムメディアプレーヤーとして使用する場合、それを信頼されたプロセスとして許可リストに追加する必要があります。許可リストのエントリには、以下の情報が必要です。

- 仮想チャネル名: `CTXMM`
- プロセス: VDAマシンで使用されるメディアプレーヤーへのパス。例: `C:\Program Files (x86)\Windows Media Player\wmplayer.exe`。
- 許可リストエントリ: `CTXMM,C:\Program Files (x86)\Windows Media Player\wmplayer.exe`

スカイプ フォー ビジネス向け HDX リアルタイム最適化パック

許可リストのエントリには、以下の情報が必要です。

- 仮想チャネル名: `CTXRMEP`
- プロセス: VDAマシン内のSkype for Business実行可能ファイルへのパス。これはSkype for Businessのバージョンやカスタムインストールパスの使用によって異なる場合があります。例: `C:\Program Files\Microsoft Office\root\Office16\lync.exe.`.

- 許可リストエントリ: `CTXRMEP,C:\Program Files\Microsoft Office\root\Office16\lync.exe`

トラブルシューティング

カスタム仮想チャネルが開かない場合は、次の手順を確認してください。

1. 正しいVDAバージョンを使用していることを確認してください。
2. 仮想チャネル許可リストにカスタム仮想チャネルを含むポリシーがVDAに適用されており、この構成を上書きする優先度の高い他のポリシーがないことを確認してください。
3. VDAのイベントログを確認し、報告されている仮想チャネル名が許可リストで定義されているものと一致することを確認してください。

    a. 複数のプロセスがある場合は、仮想チャネルを許可リストに追加するで説明されているように、これらが適切に定義されていることを確認してください。

    b. 定義されたプロセスパスでワイルドカードを使用している場合は、ワイルドカードの使用のガイドラインに従っていることを確認してください。

    c. 定義されたプロセスパスで環境変数を使用している場合は、システム環境変数の使用のガイドラインに従っていることを確認してください。

イベントログ

次のイベントがVDAマシンのイベントログに記録されます。

シングルセッションVDA

次のイベントがシングルセッションVDAマシンのイベントログに記録されます。

ログ名	ID	送信元	レベル	説明
システム	2001	`Picadd`	情報	カスタム仮想チャネル `<vcName>` はプロセス `<processName>` によって開かれました
システム	2002	`Picadd`	警告	カスタム仮想チャネル `<vcName>` はプロセス

ログ名	ID	送信元	レベル	説明
				`<processName>` によって開くことができません
システム	2003	`Picadd`	情報	`<username>` がカスタム仮想チャネル `<vcName>` を開きました
システム	2004	`Picadd`	警告	`<username>` がカスタム仮想チャネル `<vcName>` を開こうとしました
システム	2005	`Picadd`	エラー	ポリシー `<pathInPolicy>` で指定されたパスをプロセスパスに解決できません
システム	2007	`Picadd`	情報	ロードされたプロセスパスは `<processPath>` です
システム	2008	`Picadd`	エラー	VCポリシーパス内の環境変数 `<varName>` が見つかりません

マルチセッションVDA

以下のイベントがマルチセッションVDAマシンのイベントログに記録されます。

ログ名	ID	送信元	レベル	説明
システム	13	`Rpm`	情報	カスタム仮想チャネル `<vcName>` がプロセス `<processName>` によって開かれました
システム	14	`Rpm`	警告	カスタム仮想チャネル `<vcName>` はプロセス `<processName>` によって開くことができません
システム	15	`Rpm`	情報	`<username>` がカスタム仮想チャネル `<vcName>` を開きました
システム	16	`Rpm`	警告	`<username>` がカスタム仮想チャネル `<vcName>` を開こうとしました
システム	17	`Rpm`	エラー	ポリシー `<pathInPolicy>` で指定されたパスをプロセスパスに解決できません
システム	18	`Rpm`	情報	読み込まれたプロセスパスは

ログ名	ID	送信元	レベル	説明
				`<processPath>` です
システム	19	`Rpm`	エラー	VCポリシーパス内の環境変数 `<varName>` が見つかりません

既知のサードパーティ仮想チャネル

以下は、カスタムCitrix®仮想チャネルを使用する既知のサードパーティソリューションです。このリストには、カスタムCitrix仮想チャネルを使用するすべてのソリューションが含まれているわけではありません。

- カーナー
- ControlUp
- シスコ ウェブエックス チームズ
- Cisco WebEx Meetings 仮想デスクトップソフトウェア
- deviceTrust
- エピック ワープドライブ
- エピック スリングショット
- インプリバタ ワンサイン
- Midmark IQPath クライアント拡張機能
- Nuance PowerMic クライアント拡張機能
- ニュアンス ドラゴン メディカル ネットワーク エディション 360 vSync
- VDI 用 ズームミーティング
- アルティマ IA-コネクト

関連する仮想チャネルを許可リストに追加するための詳細については、ソリューションのベンダーにお問い合わせください。または、仮想チャネル名とプロセスの取得セクションに記載されている手順に従ってください。

DVC用仮想チャネル許可リスト

DVC用仮想チャネル許可リストを使用して、環境内で許可されるカスタム動的仮想チャネルを制御できます。デフォルトでは、動的仮想チャネルは許可されていません。動的仮想チャネルが必要な場合は、明示的に許可リストに追加する必要があります。

構成

DVC用仮想チャネル許可リストは、デフォルトで有効になっています。この機能は、Citrix®ポリシーの以下の設定を使用して構成できます。

- DVC用仮想チャネル許可リスト: この機能を有効または無効にし、動的仮想チャネルをリストに追加します。
- 仮想チャネル許可リストログスロットリング: 仮想チャネル許可リストのイベントログのスロットリング期間を設定します。
- 仮想チャネル許可リストログ記録: 仮想チャネル許可リストのログレベルを設定します。

許可リストへの動的仮想チャネルの追加

動的仮想チャネルを許可リストに追加するには、以下の情報が必要です。

1. クライアント上のDVCプラグインの名前。例: `DvcPlugin1.dll`。
2. DVCリスナーの名前。例: `ListenerName1`。
3. VDAマシン上で動的仮想チャネルにアクセスするプロセスのパス。例: `C:\Program Files\Application\run.exe`。

必要な情報が揃ったら、DVC用仮想チャネル許可リストポリシー設定を使用して、動的仮想チャネルを許可リストに追加する必要があります。動的仮想チャネルをリストに追加するには、セッションホストでDVCにアクセスするプロセスのパスを入力し、その後にコンマ、クライアント側プラグイン名、コンマ、およびプラグインが使用するリスナーの名前を入力します。複数のリスナー名はコンマで区切って追加できます。

単一リスナーの場合

前の例を使用して、次のエントリをリストに追加します。 `C:\Program Files\App\run1.exe,DvcPlugin1,ListenerName1`

複数リスナーの場合

複数のリスナーがある場合は、リストに次のエントリを追加します。 `C:\Program Files\App\run1.exe,DvcPlugin1,ListenerName1,ListenerName2`

ワイルドカードの使用

ワイルドカード (*) の使用がサポートされています。アプリケーションのバージョンに基づいてディレクトリ名または実行可能ファイル名が変更される場合、またはサードパーティコンポーネントがユーザープロファイルにインストールされている場合に、ワイルドカードを使用できます。

次のシナリオでワイルドカードを使用できます。

- 完全なディレクトリ名を置き換える場合。例: `C:\Program Files\App*\run1.exe`
- ディレクトリ名の一部を置き換える場合。例: `C:\Program Files\App\v*\run1.exe`
- 実行可能ファイル名を置き換える場合。例: `C:\Program Files\App\v1.2*.exe`
- 実行可能ファイル名の一部を置き換える場合。例: `C:\Program Files\App\v1.2\run*.exe`

次の制限が適用されます。

- ワイルドカードは、単一のディレクトリを置き換えるためにのみ使用できます。たとえば、実行可能ファイルが `C:\Program Files\App\v1.2\run1.exe` にある場合
  - 許可される例: `C:\Program Files\App*\run1.exe`
  - 許可されない例: `C:\Program Files*\run1.exe`
- エントリにはファイル名拡張子を含める必要があります。
  - 許可される例: `C:\Program Files\App\v1.2*.exe`
  - 許可されていません: `C:\Program Files\App\v1.2*`
- すべてのパスはローカルである必要があります。

デバイス

HDX™は、あらゆるデバイスで、あらゆる場所で高精細なユーザーエクスペリエンスを提供します。「デバイス」セクションの記事では、以下のデバイスについて説明します。

- スキャン
- 汎用USBデバイス
- クライアントドライブマッピング
- モバイルおよびタッチスクリーンデバイス
- シリアルデバイス
- 特殊キーボード
- Webカメラ

最適化されたUSBデバイスと汎用USBデバイス

最適化されたUSBデバイスとは、Citrix Workspace™アプリが特定のサポートを提供するデバイスです。たとえば、HDX Multimedia仮想チャネルを使用してWebカメラをリダイレクトする機能などです。汎用デバイスとは、Citrix Workspaceアプリで特定のサポートがないUSBデバイスです。

デフォルトでは、汎用USBリダイレクトは、汎用モードに設定しない限り、最適化された仮想チャネルサポートを持つUSBデバイスをリダイレクトできません。

一般的に、USBデバイスは汎用モードよりも最適化モードの方がパフォーマンスが向上します。ただし、最適化モードではUSBデバイスが完全な機能を持たない場合があります。その機能に完全にアクセスするには、汎用モードに切り替える必要があるかもしれません。

USB大容量記憶装置では、Citrix®ポリシーによって制御されるクライアントドライブマッピングまたは汎用USBリダイレクト、あるいはその両方を使用できます。主な違いは次のとおりです。

汎用USBリダイレクトとクライアントドライブマッピングポリシーの両方が有効になっており、セッション開始前または開始後に大容量記憶装置が挿入されると、クライアントドライブマッピングを使用してリダイレクトされます。

これらの条件が満たされると、マスストレージデバイスは汎用USBリダイレクトを使用してリダイレクトされます。

- 汎用USBリダイレクトとクライアントドライブマッピングポリシーの両方が有効になっています。
- デバイスが自動リダイレクト用に構成されています。
- マスストレージデバイスがセッション開始前または開始後に挿入されます。

詳細については、`<http://support.citrix.com/article/CTX123015>`を参照してください。

機能	クライアントドライブマッピング	汎用USBリダイレクト
デフォルトで有効	はい	いいえ
読み取り専用アクセスを構成可能	はい	いいえ
暗号化されたデバイスアクセス	はい、仮想セッションでデバイスにアクセスする前に暗号化が解除されている場合。	シトリックス バーチャル デスクトップ™ のみ

スキャン

スキャナーは、画像、印刷されたテキスト、手書き、または物体を光学的にスキャンし、デジタル画像に変換するデバイスです。

スキャナーを使用しており、お使いのコンピューターがWindowsを実行している場合、WIAスキャナードライバーを使用している可能性が高いです。このドライバーは、コンピューターとスキャナー間の通信を担当します。

- **Windows Image Acquisition** (WIA) は、ソフトウェアがスキャナーなどのイメージングハードウェアと通信できるようにする、Microsoftのドライバーモデルおよびアプリケーションプログラミングインターフェース (API) です。
- **TWAIN** (WindowsおよびMac) は、標準インターフェースを提供することでスキャナーとアプリケーションを接続する、別のスキャンプロトコルです。TWAINを使用すると、アプリケーションはTWAIN準拠デバイス (スキャナー、デジタルカメラなど) から画像を取得できます。
- **SANE:** スキャンプロトコルは、ソフトウェアアプリケーションがイメージスキャナーと通信し、制御できるようにするための一連の標準とガイドラインです。SANEは **S**canner **A**ccess **N**ow **E**asy の略で、そのプロトコルは、異なるコンピューターシステムで実行されているソフトウェアによってスキャナーハードウェアがどのようにアクセス、管理、制御されるかを定義します。

TWAIN リダイレクト

はじめに

ユーザーは、Citrix HDX™セッション内のアプリケーションから、クライアントエンドポイントに接続されたTWAIN準拠のスキャナーを使用してドキュメントをスキャンできます。Citrixスキャンモジュールは、スキャン要求をクライアントエンドポイントにリダイレクトして処理します。完了すると、スキャンされた情報はVDAホストに送り返されます。

要件

Citrix コントロールプレーン

- シトリックス バーチャル アプリ アンド デスクトップ™ 1912 以降
- シトリックス DaaS™

セッションホスト

- オペレーティングシステム
  - Windows 10 1809以降
  - ウィンドウズ 11
  - ウィンドウズ サーバー 2022 以降
- VDA
  - バージョン1912以降
- アプリケーション
  - 32ビットアプリケーション
  - 64ビットアプリケーション

> **注:**

> - セッションホスト上の64ビットアプリケーションでスキャン機能を有効にするには、64ビットTWAINデータソースマネージャー (twaindsm.dll) が必要です。このコンポーネントはオペレーティングシステムによってプリインストールされていません。
> - 64ビットスキャンアプリケーションにこのファイルが含まれていない場合は、アプリケーションベンダーに連絡して64ビットtwaindsm.dllを入手してください。

- 入手後、管理者はファイルをセッションホストの**System32**フォルダーに手動でコピーし、マシンを再起動する必要があります。

クライアントデバイス

- オペレーティングシステム
  - Windows 10 1809 以降
  - ウィンドウズ 11
- Workspaceアプリ
  - Windows: バージョン1912以降
- スキャナー
  - TWAIN準拠スキャナー
  - クライアントエンドポイントにTWAINドライバーをインストールする

構成

TWAINリダイレクトはデフォルトで有効になっています。TWAINリダイレクトを構成し、スキャンエクスペリエンスを最適化するために、以下のポリシー設定が利用可能です。

- **クライアントTWAINデバイスリダイレクト:** TWAINリダイレクトを有効または無効にするには。
- **TWAIN圧縮レベル:** クライアントからVDAに転送される画像の圧縮レベルを設定します。

詳細については、TWAINデバイスポリシー設定を参照してください。

トラブルシューティング

TWAINリダイレクト機能は、公開されているテストアプリTwackerでテストできます。このアプリは、このURLからダウンロードできます。

HDXセッション内でTWAIN機能を検証するには、以下の手順に従ってください。

1. VDAホストに**Twacker**をインストールします。
2. **Twacker**（32ビットまたは64ビット版）を起動します。
3. **ファイル > ソースの選択**をクリックし、リストからスキャナーを選択します。
4. **ファイル > 取得**をクリックします。

5. **スキャンボタン**をクリックして、スキャナーをテストします。

Twacker が正常にスキャンできる場合、**Citrix Virtual Apps and Desktops** のセットアップは次の状態であることが確認できます。

- TWAINリダイレクトを使用するように正しく構成されている
- すべてのローカルクライアントデバイス要件を満たしていること

特定のアプリケーション内でスキャンに関する問題が引き続き発生する場合は、ソフトウェアの問題である可能性が高いです。

WIAデバイス

デジタルカメラやスキャナーなどの WIA デバイスは、WIA フレームワークを使用して、サーバーでホストされている画像処理アプリケーションと通信します。

前提条件

- スキャナーは WIA 準拠である必要があります。
- WIA ドライバーをローカルデバイスにインストールします。サーバーには必要ありません。
- スキャナーをローカルに接続します (たとえば、USB 経由で)。
- スキャナーが TWAIN ドライバーではなく、ローカルの Windows イメージ取得サービスを使用していることを確認してください。
- テストに使用されるユーザーアカウントに、ICA® セッション内の帯域幅を制限するポリシーが適用されていないことを確認してください。たとえば、クライアント USB リダイレクト帯域幅制限などです。

構成

WIA リダイレクトはデフォルトで無効になっています。Citrix® ポリシーで次の設定を有効にできます。

- WIA リダイレクト: この設定は、ユーザーがユーザーデバイス上の WIA デバイスにアクセスすることを許可または禁止します。

> **注:**
>
> レジストリを誤って編集すると、オペレーティングシステムの再インストールが必要になるような深刻な問題が発生する可能性があります。Citrix は、レジストリエディターの誤った使用によって発生した問題が解決されることを保証できません。 レジストリエディターの使

> 用は、お客様ご自身の責任で行ってください。編集する前に、必ずレジストリをバックアップしてください。

> 許可リストを使用すると、VDA 上のどのアプリケーションが Windows イメージ取得スキャナーリダイレクトにアクセスできるかを制御できます。レジストリエディターは、Windows イメージ取得を含む各 VDA の許可リスト設定からの入力を使用します。デフォルトでは、どのアプリケーションも Windows イメージ取得にアクセスできません。

64 ビットアプリケーションの場合、次の値を設定する必要があります。

スキャンアプリケーションのフルパスをAllowProcessesレジストリ値に追加します。

- キー: HKLM\SOFTWARE\Citrix\WIAAllowedProcesses
- 値の名前: AllowProcesses
- 値の型: REG_MULTISZ
- 値のデータ: `<add full path of the scanning application >`
- キー: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxHook\AppInit_DLLs\WIAHook\<App_Name>

32ビットアプリケーションの場合、以下の値を設定する必要があります。

スキャンアプリケーションのフルパスをAllowProcessesレジストリ値に追加します。

- キー: HKLM\SOFTWARE\Citrix\WOW6432Node\WIAAllowedProcesses
- 値の名前: AllowProcesses
- 値の型: REG_MULTISZ
- 値のデータ: `<add full path of the scanning application >`
- キー: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\CtxHook\AppInit_DLLs\WIAHook\<App_N

WIAベースのアプリケーションでWIAリダイレクトを有効にするレジストリ値を設定した後、VDA を再起動します。

ポリシー設定の詳細については、「WIAデバイスのポリシー設定」を参照してください。

SANE リダイレクト

はじめに

ユーザーは、ChromeOSエンドポイントからCitrix®セッション内のTWAINアプリケーションからドキュメントをスキャンできます。ユーザーがアプリケーションからドキュメントをスキャンしようとすると、Citrixスキャンモジュールはリクエストをクライアントエンドポイントにリダイレクトし、スキャナーからのスキャンを実現します。スキャンが完了すると、ファイルはVDAに送信されます。

要件

シトリックス コントロールプレーン

- Citrix Virtual Apps and Desktops™ のバージョン 2411 以降
- シトリックス DaaS™

セッションホスト

- オペレーティングシステム
  - Windows 10 1809 以降
  - ウィンドウズ 11
  - Windows Server のバージョン 2019 以降
- VDA
  - バージョン2411以降

クライアントデバイス

- オペレーティングシステム
  - ChromeOS v129以降
- Workspaceアプリ
  - ChromeOS: バージョン2409以降
- スキャナー
  - スキャナーは Chrome OS でサポートされている必要があります
  - サポートされているデバイス: Fujitsu FI-7160、FI-8170

> **注:**
>
> 上記以外のスキャナーは、Chrome OSでサポートされている場合、ネイティブのTwain UIを使用して使用できます。

- USB経由でクライアントエンドポイントにローカルに接続されている必要があります。

構成

この機能を有効にするための追加の構成は不要です。この機能はデフォルトで有効になっています。

> **注:**
>
> この機能を無効にするには、Web Studio/DaaSコンソールを開きます。SANEスキャナーリダイレクトポリシー設定を「禁止」に設定します。

トラブルシューティング

イベントログ

管理者は、スキャン関連のさまざまなイベントメッセージを表示できます。

以下に、VDAホストのイベントビューアーに記録される、さまざまなスキャン関連操作のイベントメッセージを示します。これらは、Windowsログのアプリケーションセクションで、イベントソースとしてHDX™ Scannerを使用して表示できます。

イベントID	イベントテキスト	説明
2	AllowScannerSANERedirectionポリシーが無効になっています。スキャナーはリダイレクトされません。	SaneRedirectionポリシーが無効になっていることを示します。
3	スキャン詳細: ページ数 - '[pages]', アプリケーション - '[application]', スキャナー - '[scanner]', ユーザー - '[user]', 1ページあたりの平均時間 - '[time]'ミリ秒。	スキャンが完了したときに生成されます。

イベントID	イベントテキスト	説明
101	スキャンするページが見つかりません。	ドキュメントが検出されなかったときに生成されます。
102	スキャン失敗 - デバイスのドキュメントフィーダーが詰まっています。	スキャナーのドキュメントフィーダーでの紙詰まりによりスキャンが失敗した場合に生成されます。
103	スキャン失敗 - '[failure]'。スキャナーアプリケーションを閉じて再起動してください。	サポートされていない操作、ファイル終端エラー、アクセス拒否エラーなどのエラーによりスキャンが失敗した場合に生成されます。
104	アプリケーションでメモリ障害が発生しました。アプリケーションを再起動してください。	メモリ不足によりスキャンが失敗した場合に生成されます。
201	ユーザーによってスキャン操作がキャンセルされました。	ユーザーによってスキャン操作がキャンセルされた場合に生成されます。
202	スキャン中にセッションが切断されました。	スキャン中にHDXセッションが切断された場合に生成されます。
203	TWAINとSANE間の変換は「[capability]」に対してサポートされていません。スキャナー/アプリケーションがサポートされているか確認してください。	指定された機能に対するTWAINとSANE間の変換がサポートされていないことを示します。
205	スキャナー「[scanner]」をアクティブに設定できませんでした。スキャナーの電源が入っていて接続されているか確認してください。	スキャナーへの接続が開けなかった場合に生成されます。

イベントID	イベントテキスト	説明
206	スキャナーが見つかりません。スキャナーの電源が入っていて接続されているか確認してください。	クライアントエンドポイントでスキャナーが検出されない場合に生成されます。

既知の制限事項

1. ネットワーク認証スキャナーはサポートされていません。
2. VDA上のFujitsu Paperstreamアプリなど、一部のプロプライエタリなスキャンアプリケーションでは、リダイレクトされたスキャナーがサポート対象として表示されない場合があります。
3. ネイティブUIを使用する場合、サードパーティAPIの制限により、ページ幅、ページ高さ、用紙サイズ、明るさ、コントラストなどのスキャナー設定の一部が尊重されない場合があります。

USBデバイス

はじめに

汎用USBリダイレクト機能により、クライアントマシンからHDX™セッションへのUSBデバイスのリダイレクトが可能になり、エンドユーザーはHDXセッションで幅広い汎用USBデバイスを操作できます。これは、最適化されたサポートがない、または不適切な特殊デバイスをユーザーが使用する必要があるシナリオで役立ちます。

> **注:**
>
> 仮想チャネルサポート用に最適化されていないUSBデバイスは、生のUSBリダイレクトを使用して汎用USB仮想チャネルにフォールバックします。

仕組み?

汎用USBリダイレクトは低レベルで機能し、クライアントマシンとXenDesktop®仮想デスクトップ間でUSB要求および応答メッセージをリダイレクトします。

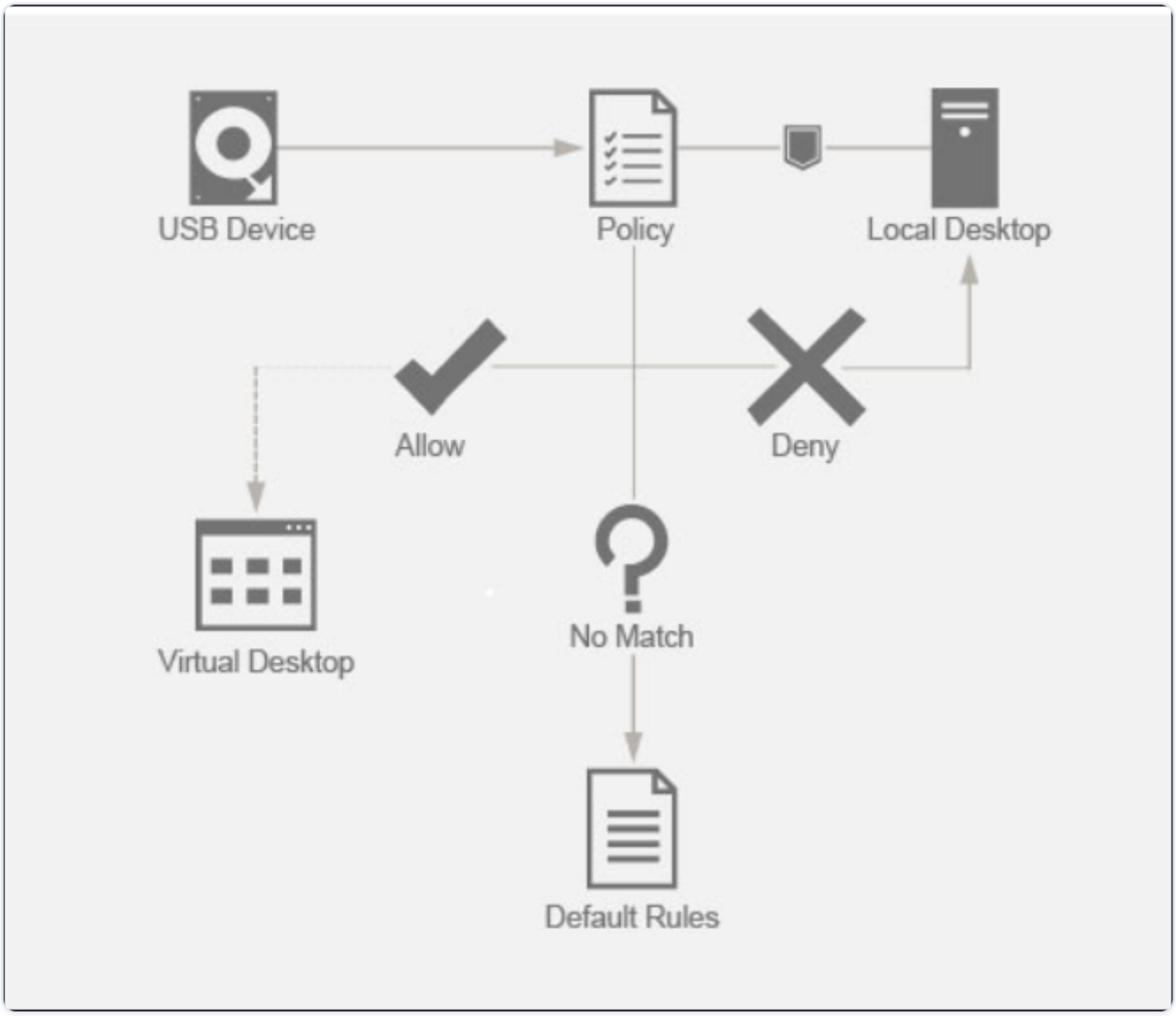
これにより、クライアントマシンに互換性のあるデバイスドライバーが不要になり、ドライバーは仮想デスクトップでのみサポートされることが期待されます。USBリダイレクトポリシー規則は、DDCポリシー規則が評価および適用された後、クライアント側ポリシーとデフォルト規則が

尊重されるように、特定の優先順位に従います。これにより、Citrix管理者は、不正なデバイスや偽装されたデバイスがセッション内にリダイレクトされるのを防ぐことができます。

さらに、リモートセッションへのアクセスを試みる不正なデバイスのイベントログを監査およびフラグ付けすることができ、管理者はデータ漏洩を防ぐために追加の措置を講じることができます。

ユーザーがUSBデバイスを接続すると、セッションホストは一致が見つかるまで各ポリシー規則に対してそれを連続的にチェックします。任意のデバイスに対する最初の一致が最終的なものと見なされます。

- 最初の一致が許可規則である場合、デバイスは仮想デスクトップにリダイレクトされます。
- 最初の一致が拒否規則である場合、デバイスはセッションにリダイレクトされず、ローカルユーザーデバイスでのみ使用できます。一致が見つからない場合は、デフォルト規則が使用されます。



汎用USBリダイレクトとの互換性

以下のCitrix Workspace™アプリは、汎用USBリダイレクトをサポートしています:

- Citrix Workspace app for Windows については、Citrix Workspace app for Windows を参照してください。
- Citrix Workspace app for Mac については、Citrix Workspace app for Mac を参照してください。
- Citrix Workspace app for Linux については、Citrix Workspace app for Linux を参照してください。
- Citrix Workspace app for Chrome OS については、Citrix Workspace app for Chrome を参照してください。

Citrix Workspaceアプリのバージョンについては、Citrix Workspace app feature matrix を参照してください。

設定

USBリダイレクトはデフォルトで無効になっています。Citrix®ポリシーで以下の設定を使用して、汎用USBリダイレクトを構成できます。

- **クライアントUSBデバイスリダイレクト**: USBリダイレクトを有効または無効にする
- **クライアントUSBデバイスリダイレクト規則**: 特定のデバイスアクション、つまり特定のデバイスへのアクセスを許可または拒否するように指定する
- **クライアントUSBデバイスリダイレクト規則 (バージョン2)**: USBデバイスのフィルタリング、分割、自動接続の規則を指定する
- **クライアントUSBデバイス最適化規則**: 最適化を無効にするか、最適化モードを変更する
- **既存のUSBデバイスの自動接続を許可する**: HDX™セッションの開始時にクライアントエンドポイントに接続されている既存のUSBデバイスの自動接続を許可または防止する
- **新しく接続されたUSBデバイスの自動検出を許可する**: HDXセッション中にクライアントエンドポイントに接続されるUSBデバイスの自動接続を許可または防止する

詳細については、「USBポリシー設定」を参照してください。

USBリダイレクトの構成方法

デフォルトでは、USBリダイレクト構成は無効になっています。これを使用するには、USBリダイレクトポリシーと特定のリダイレクト規則をDDCで有効にして構成する必要があります。

> **注:**
>
> バージョン2212より前のコンポーネントを使用している場合、またはLinux/Mac版Workspaceアプリを使用している場合は、USBリダイレクトの構成方法の詳細について「レガシーUSBリダイレクト構成」を参照してください。

汎用USBリダイレクトの有効化

1. **Citrix Web Studio™ポリシー**を開き、**［ポリシー］**タブをクリックします。
2. **［ポリシーの作成］をクリックし、［ICA®］>［USBデバイスポリシー］**を展開します。
3. **クライアントUSBデバイスリダイレクトポリシー**を編集します。
4. 「**許可**」を選択し、「**保存**」をクリックします。

USBリダイレクトポリシー規則の作成

ユーザーがUSBデバイスをVirtual Desktopにリダイレクトしようとすると、一致が見つかるまで各USBポリシー規則に対して順にチェックされます。いずれかのデバイスに対する最初の一致が最終と見なされます。最初の一致が**許可**規則である場合、一致したデバイスは仮想デスクトップにリダイレクトされることが許可されます。最初の一致が**拒否**規則である場合、一致したデバイスはローカルデスクトップでのみ利用可能です。一致が見つからない場合は、デフォルトの規則が使用されます。

デバイス規則

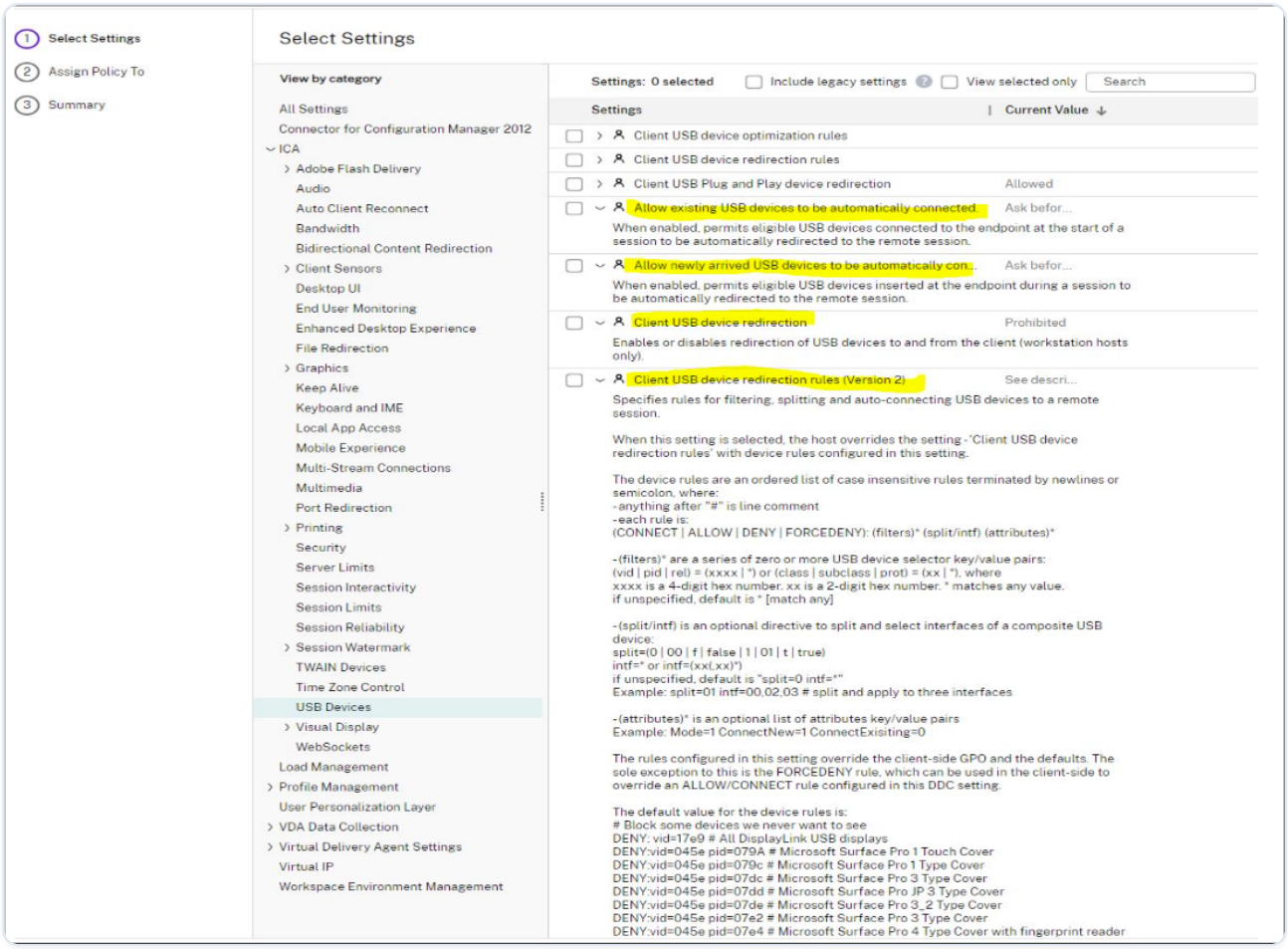
通常のUSBデバイスと同様に、エンドポイントのポリシーまたはクライアントCitrix Workspace™アプリ構成で設定されたデバイス規則は、転送するデバイスを選択します。Citrix Workspaceアプリはこれらの規則を使用して、どのUSBデバイスをリモートセッションへの転送を許可または禁止するかを決定します。

各規則は、アクションキーワード（**Allow、Connect、またはDeny**）、コロン（:）、およびエンドポイントのUSBサブシステムにある実際のデバイスと一致する0個以上のフィルターパラメーターで構成されます。これらのフィルターパラメーターは、すべてのUSBデバイスが自身を識別するために使用するUSBデバイス記述子メタデータに対応しています。

デバイスルールはクリアテキストであり、各ルールは1行に記述され、#文字の後にオプションのコメントが続きます。ルールは上から下へ（優先順位の降順で）照合されます。デバイスまたは子インターフェイスに一致する最初のルールが適用されます。同じデバイスまたはインターフェイスを選択する後続のルールは無視されます。

例: 許可: VID=1050 PID=0421 #デバイス1 **例:** 接続: VID=xxxx PID=yyyy Class=03 #デバイス2

キーワード	説明
CONNECT	このキーワードを使用して、USB仮想チャネル経由でのデバイスのリダイレクトを許可し、セッション起動時および挿入時に自動リダイレクトを有効にします。
ALLOW	このキーワードを使用して、USB仮想チャネル経由でデバイスのリダイレクトを許可します
拒否	このキーワードを使用して、USB仮想チャネル経由でデバイスのリダイレクトを拒否します



DDCでポリシーを設定する：

1. **Citrix Web Studio ポリシー**」を開き、「**ポリシー**」タブをクリックします。
2. **ポリシーの作成**」をクリックし、「**ICA > USB デバイス ポリシー**」を展開します。
3. **クライアントUSBデバイスリダイレクトルール（バージョン2）**を編集します。

4. リダイレクトする必要がある各USBデバイスについて、説明に記載されている例に基づいて値を設定し、をクリックします。

   例：許可：VID=056A PID=00A4 #STU-430 拒否：Class=08 subclass=05 # マスストレージ

   > **注：**
   >
   > Citrix管理者が**デフォルト値を使用**をチェックして**保存**をクリックすると、デフォルトのルールはVDAの次のレジストリにあります。
   >
   > **注意!**
   >
   > レジストリエディターを使用する前に、この記事の最後にある免責事項を参照してください。
   >
   > `HKLM\SOFTWARE\Wow6432Node\Citrix\PortICA\GenericUSB\DeviceRules`

> **注:**
>
> グループポリシーデバイスルールを使用してクライアントデバイスでポリシーを設定できますが、CVADおよびCWAの新しいバージョンではもはや必要ありません。
>
> USB デバイスのレガシー構成については、「レガシー USB リダイレクト構成」を参照してください。

USBデバイスの自動リダイレクトを構成する (オプション)

USBサポートが有効になっている場合、USBデバイスは自動的にリダイレクトされます。また、USBユーザー設定はUSBデバイスを自動的に接続するように設定されています。すべてのUSBデバイスをリダイレクトすることが常に最適とは限りません。ユーザーは、自動的にリダイレクトされないUSBデバイスリストからデバイスを明示的にリダイレクトできます。USBデバイスが一覧表示されたりリダイレクトされたりするのを防ぐには、クライアントエンドポイントまたはDDCポリシーのいずれかでDeviceRulesを使用します。 このポリシーは、DDC、GPOを使用したクライアント、Citrix Workspace Preferences、またはCDViewerのタブのいずれかで設定できます。これらのすべての方法は以下に説明されています。

DDCでのポリシーの設定:

USB デバイスの自動リダイレクトを許可するように設定できる DDC 上のポリシーは 2 つあります。

- 既存のUSBデバイスを自動的に接続することを許可する
- 新しく接続されたUSBデバイスを自動的に接続することを許可する

a. 「**Citrix Web Studioポリシー**」を開き、「**ポリシー**」タブをクリックします。

b. 「**ポリシーの作成**」をクリックし、「**ICA > USBデバイスポリシー**」を展開します。

c. **既存のUSBデバイスを自動的に接続することを許可する**設定を編集します。

d. **デフォルト値を使用**チェックボックスをオフにし、ドロップダウンメニューから**利用可能なUSBデバイスを自動的にリダイレクト**を選択して、**保存**をクリックします。

e. **新しく接続されたUSBデバイスを自動的に接続することを許可する**設定を編集します。

f. **デフォルト値を使用**チェックボックスをオフにし、ドロップダウンメニューから**利用可能なUSBデバイスを自動的にリダイレクト**を選択して、**保存**をクリックします。

USBデバイスリダイレクトルールの理解

Citrix Client USBリダイレクトを使用する場合、さまざまなルールがどのように優先順位付けされ、適用されるかを理解することが重要です。これは一連の指示のようなものだと考えてください。システムは特定の順序でルールをチェックし、特定のデバイスに対して最初に見つかったルールが適用されます。その**同じデバイス**に対してリストのさらに下に見つかった他のルールは無視されます。

デバイスルールが評価される順序は次のとおりです。

- **クライアントUSBデバイスリダイレクトルール (バージョン2)**: このポリシー設定で構成されたデバイスルールには、最高の優先順位が与えられます。特定のデバイスに対するルールがここで見つかった場合、そのルールが適用され、その特定のデバイスに対する他のルールは考慮されません。
- **クライアントUSBデバイスリダイレクトルール**: 次に、Citrix Studio内のこのレガシー設定で定義されたルールが続きます。バージョン2ポリシーでデバイスのルールが見つからなかった場合、システムはこのポリシー設定で定義されたルールをチェックします。ここでも、デバイスのルールが見つかった場合、それが適用され、システムはその特定のデバイスのルールを探すのを停止します。

> **注:**

> 上記のポリシー設定は、Studioで**クライアントUSBデバイスリダイレクトルール (バージョン2)が設定されていない場合、またはCitrix Workspace App for Windows**のバージョンが2212より古い場合にのみ適用されます。

- **クライアント側グループポリシーオブジェクト (GPO)**: 両方のStudioポリシー設定を確認した後もデバイスに適用されるルールがない場合、システムはクライアント側グループポリシーオブジェクトを介して構成されたルールに従います。
- **クライアント側レジストリ設定**: 最後に、クライアント側レジストリ設定が最も低い優先順位で適用されます。

この階層により、特定のデバイスに対してより具体的または新しい構成が優先され、USBデバイスリダイレクトを管理するための明確で予測可能な方法が提供されます。階層が評価の順序を決定する一方で、上位レベルでデバイスに対して見つかったルールは、その**同じデバイス**に対する下位レベルでのルールの適用を妨げることを覚えておくことが重要です。 ただし、下位レベルで設定されたルールが完全に無視されるわけではありません。まだルールが適用されていないデバイスについては、引き続き評価されます。

この階層化されたアプローチは、**下位互換性**も保証します。Citrix Virtual Apps and Desktops™ または Citrix Workspace app の古いバージョンからアップグレードする場合、既存のクライアント側構成は保持されます。これにより、エンタープライズ管理者は、Studioのより高度な**バージョン2デバイスルール**ポリシー設定への移行パスを、即座の中断なしに計画する時間を確保できます。

例:

例えば、ベンダーID (VID) `xxxx` および製品ID (PID) `yyyy` を持つ特定のUSBデバイスがあるとします。

- Citrix Studioの**クライアントUSBデバイスリダイレクトルール (バージョン2)**ポリシー設定で、`CONNECT VID=xxxx PID=yyyy` のルールセットがあります。
- 別に、クライアント側の**グループポリシーオブジェクト (GPO)**で、同じデバイスに対して `DENY` のルール `DENY: VID=xxxx PID=yyyy` があります。

このデバイスがクライアントエンドポイントに接続されると、システムはまずバージョン2のStudioポリシーのルールを評価します。システムは`CONNECT`ルール`VID=xxxx PID=yyyy`を見つけます。このルールは最も高い優先順位レベルにあるため、すぐに適用されます。その後、システムはこの特定のデバイスに対するそれ以上のルールを無視します。したがって、クライアント側のGPOに`DENY`ルールが存在しても、それは無視され、デバイスは正常にリダイレクトされます。

複合デバイスとデバイス分割

複合USBデバイスは、コンピューターに接続された複数の独立したUSBデバイスのように機能する単一のデバイスです。単一のUSBコネクターを持ちますが、それぞれ独自の機能セットを持つ複数のインターフェイスをコンピューターに公開できます。ユーザーが複合USBデバイスを接続すると、ホストデバイスはすべての機能（インターフェイス）を各ポリシー規則と照合して確認します。いずれかの機能（インターフェイス）に対する最初の照合が拒否規則である場合、その規則は複合デバイスに対して最終的なものと見なされ、デバイスは拒否されます。機能（インターフェイス）に対する最初の照合が許可規則である場合、ホストデバイスは次の機能（インターフェイス）に対して規則の照合を続行します。ポリシー規則によって機能（インターフェイス）が拒否されない場合、複合デバイスは許可されます。複合デバイスに対する最終的な照合が拒否規則である場合、デバイスはローカルデスクトップでのみ利用可能になり、それ以外の場合は仮想デスクトップにリモート接続されます。照合が見つからない場合は、デフォルト規則が使用されます。

デバイス分割(/en-us/citrix-virtual-apps-desktops/2503/media/device-splitting.png)

複合デバイスの特定の機能のみを許可するために、デバイスリダイレクト規則（バージョン2）ポリシーで適切な規則を使用して複合デバイスを分割できます。たとえば、FIDO2キーのHID機能のみを使用し、スマートカード機能は使用したくない場合があります。その場合、規則は次のように設定します。

1. Connect: VID=1050 PID=0407 class=03 split=01 intf=00,01 #Yubikey Series 5のFIDO2 HID機能が許可されました。
2. Deny: VID=1050 PID=0407 split=01 intf=02 #Yubikey Series 5のスマートカード機能がブロックされました。

> **ヒント:**
>
> 新しいポリシー規則を作成する際は、USB Webサイトで入手できるUSBクラスコードを参照してください。

署名パッドの構成

1. VDAホストに適切なデバイスドライバーをインストールします。
2. **Citrix Web Studio™**で**クライアントUSBデバイスリダイレクト**ポリシー設定を有効にします。
3. **クライアントUSBデバイスリダイレクト規則（バージョン2）**ポリシー設定を編集します。

a. リダイレクトする必要がある署名パッドの**VID**と**PID**情報を設定し、**保存**をクリックします。例：**Connect**: VID=06A8 PID=0057 class=03 #Topaz HSB

4. **クライアントUSBデバイス最適化規則**ポリシー設定を編集します。

   a. モードとその他のデバイス情報を設定します。例：Mode=00000004 VID=06A8 PID=0057 class=03 #キャプチャモードで動作する入力デバイス

5. ポリシー設定「**既存のUSBデバイスの自動接続を許可**」を編集します。
6. 「**デフォルト値を使用**」チェックボックスをオフにし、ドロップダウンメニューから「**利用可能なUSBデバイスを自動的にリダイレクト**」を選択して、「**保存**」をクリックします。
7. ポリシー設定「**新しく接続されたUSBデバイスの自動接続を許可**」を編集します。
8. 「**デフォルト値を使用**」チェックボックスをオフにし、ドロップダウンメニューから「**利用可能なUSBデバイスを自動的にリダイレクト**」を選択して、「**保存**」をクリックします。

これらの設定が構成されると、以降のセッション起動ではデバイスが自動的にリダイレクトされ、追加のエンドユーザー操作は不要になります。

> **注:**
>
> リダイレクトするデバイスの実際のVIDとPIDに置き換えます。

USBリダイレクトを使用したBloombergキーボードの構成

1. **Citrix Web Studio**でポリシー設定「**クライアントUSBデバイスリダイレクト**」を有効にします。
2. Bloomberg 5キーボードは、ポリシー設定「**クライアントUSBデバイスリダイレクト規則(バージョン2)**」でデフォルトで設定されており、追加の管理者操作は不要です。
3. ポリシー設定「**既存のUSBデバイスの自動接続を許可**」を編集します。
4. 「**デフォルト値を使用**」チェックボックスをオフにし、ドロップダウンメニューから「**利用可能なUSBデバイスを自動的にリダイレクト**」を選択して、「**保存**」をクリックします。
5. ポリシー設定「**新しく接続されたUSBデバイスの自動接続を許可**」を編集します。
6. 「**デフォルト値を使用**」チェックボックスをオフにし、ドロップダウンメニューから「**利用可能なUSBデバイスを自動的にリダイレクト**」を選択して、「**保存**」をクリックします。

これらの設定が構成されると、以降のHDX™セッションではBloombergキーが自動的に表示され、追加のエンドユーザー操作は不要になります。

USBリダイレクトを使用したFIDO2キーの構成

Citrixでは、HDXセッションでFIDO2キーを使用するためにFIDO2リダイレクトを使用することを推奨しています。ただし、代わりにUSBリダイレクトを使用してFIDO2キーをリダイレクトする必要がある状況もあります。これには、クライアント、VDA、またはオペレーティングシステム（例：Windows Server 2016）で機能がサポートされていないため、FIDO2リダイレクトが利用できないシナリオが含まれます。

また、キーに複数のモードが有効になっているが、HDXセッションではその一部のみを許可したいという状況もあります。たとえば、FIDO2とOTPは許可したいが、スマートカードはブロックしたい場合などです。

次の手順は、USBリダイレクトを使用してFIDO2キー（Yubikey vid=1050, pid=0407）を構成する方法を示しています。

1. **Citrix Web Studio**で、**クライアントUSBデバイスリダイレクト**ポリシー設定を有効にします。
2. **クライアントUSBデバイスリダイレクト規則（バージョン2）**ポリシー設定を編集します。
    a. セッションでリダイレクトするFIDO2キーの**VID**と**PID**情報、および分割デバイス構成を設定し、**保存**をクリックします。
    b. **接続**: VID=1050 PID=0407 class=03 split=01 intf=00,01 #Yubikeyシリーズ5で許可されるFIDO2 HID機能。
    c. **拒否**: VID=1050 PID=0407 split=01 intf=02 # Yubikeyシリーズ5スマートカード機能はブロックされました。
3. ポリシー設定**既存のUSBデバイスの自動接続を許可する**を編集します。
4. **デフォルト値を使用**チェックボックスをオフにし、ドロップダウンメニューから**利用可能なUSBデバイスを自動的にリダイレクトする**を選択して、**保存**をクリックします。
5. ポリシー設定**新しく接続されたUSBデバイスの自動接続を許可する**を編集します。
6. **デフォルト値を使用**チェックボックスをオフにし、ドロップダウンメニューから**利用可能なUSBデバイスを自動的にリダイレクトする**を選択して、**保存**をクリックします。

これらの設定が構成されると、FIDO2キーボードは以降のHDXセッションで自動的に提示され、追加のエンドユーザー操作は不要になります。

USBリダイレクトを使用した3Dマウスの構成

現在、3dConnexion SpaceMouseドライバーはワークステーションOS（Windows 10およびWindows 11）でのみサポートされています。サーバーOSでは動作しません。以下は、ワークステーションOSでSpaceMouse Enterprise（vid=046D, pid=C016）を構成する手順です。

1. VDAホストに最新のWindowsドライバーをインストールします。
2. 「**Citrix Web Studio**」で「**クライアントUSBデバイスリダイレクト**」ポリシー設定を有効にします。
3. 「**クライアントUSBデバイスリダイレクト規則**」（**バージョン2**）ポリシー設定を編集します。
    a. リダイレクトする必要がある署名パッドの**VID**および**PID**情報を追加し、**保存**をクリックします。例：**Connect**: VID=046D PID=C016 #SpaceMouse Enterprise
4. 「**クライアントUSBデバイス最適化規則**」ポリシー設定を編集します。
    a. 他のデバイス情報とともにモードを設定します。例：Mode=00000004 VID=046D PID=C016 class=03 #Input device operating in capture mode
5. 「**既存のUSBデバイスの自動接続を許可する**」ポリシー設定を編集します。
6. **デフォルト値を使用**チェックボックスをオフにし、ドロップダウンメニューから**利用可能なUSBデバイスを自動的にリダイレクト**を選択して、**保存**をクリックします。
7. 「**新しく接続されたUSBデバイスの自動接続を許可する**」ポリシー設定を編集します。
8. **デフォルト値を使用**チェックボックスをオフにし、ドロップダウンメニューから**利用可能なUSBデバイスを自動的にリダイレクト**を選択して、**保存**をクリックします。

USBリダイレクトと異なるデバイス規則を使用して2つ以上のデバイスを構成する

複数のデバイスを、異なるデバイス規則を使用してHDXセッション内でリダイレクトできます。管理者は、一方のデバイスを自動的にリダイレクトし、もう一方のデバイスをエンドユーザーがリダイレクトするオプションを提供したい場合があります。以下に、異なる規則で2つのデバイスを構成する手順を示します。

1. 「**Citrix Web Studio**」で「**クライアントUSBデバイスリダイレクト**」ポリシー設定を有効にします。
2. 「**クライアントUSBデバイスリダイレクト規則**」（**バージョン2**）ポリシー設定を編集します。
    a. セッションで適切なデバイスルールを使用してリダイレクトする2つのデバイスの**VID**および**PID**情報を追加し、**保存**をクリックします。

b. **許可**: VID=0911 PID=0c1c #フィリップス スピーチマイク.

c. **接続**: VID=06A8 PID=0043 class=03 # トパーズ HSB シグネチャパッド

3. ポリシー設定「**既存のUSBデバイスの自動接続を許可する**」を編集します。
4. **デフォルト値を使用**チェックボックスをオフにし、ドロップダウンメニューから「**利用可能なUSBデバイスを自動的にリダイレクトする**」を選択して、**保存**をクリックします。
5. ポリシー設定「**新しく接続されたUSBデバイスの自動接続を許可する**」を編集します。
6. **デフォルト値を使用**チェックボックスをオフにし、ドロップダウンメニューから「**利用可能なUSBデバイスを自動的にリダイレクトする**」を選択して、**保存**をクリックします。

これらの設定が構成されると、Topaz HSB署名パッドは以降のHDXセッションで自動的に表示され、エンドユーザーによる追加のアクションは不要になります。一方、Phillips speech micは、エンドユーザーがConnection CenterまたはCDViewerのタブでリダイレクトを有効にする必要があります。

トラブルシューティング

USBリダイレクト関連の問題を特定するには、以下の手順に従う必要があります。

1. USBリダイレクトのシステム要件が満たされていることを確認します。これには、正しいCVADおよびCWAバージョン、サポートされているデバイス、および検討中のOSプラットフォーム上のデバイスドライバーが含まれます。
2. 環境で使用されているコンポーネントのバージョンとプラットフォームに基づいて、構成が適切であることを確認します。(/ja-jp/citrix-virtual-apps-desktops/2503/devices/usb-devices/legacy-usb-redirection-configuration.html)を必要とするコンポーネントの詳細については、「レガシーUSBリダイレクト構成」の注記を参照してください。
3. クライアントが列挙したデバイスの下に、デバイスがリストされていることを確認します。

   a. Workspace設定ツールバー: Workspaceアプリの設定ツールバーの「デバイス」タブに列挙されているデバイスを確認します (**CWAアイコン > 接続センター > 設定** を右クリック… **デバイス** タブをクリック)。

   b. `CtxUsbDiagnostics.exe` (推奨): このツールをコマンドプロンプトウィンドウで実行します。出力には、特定のセッションに関するデバイス固有の情報が表示されます。デバイスがリダイレクトされているかどうかを示します。また、デバイスルールセットが原因でデバイスがリダイレクトされていないかどうかも示します。詳細については、診断ツールを参照してください。

c. USBViewまたはその他のサードパーティツール: エンドポイント/クライアントマシンでUSBViewのようなサードパーティツールを実行し、デバイスがエンドポイントで検出されていることを確認します。

4. デバイスが列挙されている場合:

   a. 特定のデバイスについてCtxUsbDiagnosticsツールの出力に拒否ルールが表示される場合は、Studioで構成されているポリシーを確認し、バージョン2ポリシーでルールが正しく設定されていることを確認します。拒否ルールがStudioポリシーに表示されない場合は、クライアント側ポリシー、そして最後にクライアント側デフォルトの順に確認して、一致する拒否ルールを見つけます。

   b. CtxUsbDiagnosticsの出力に拒否ルールがない場合、CWAは、設定ウィンドウのデバイスタブ（デバイス > デバイスの管理）で適切なボタンをチェック/クリックすることで、デバイスのリダイレクトを許可します。一度リダイレクトされたデバイスはセッションで利用可能になります。これは、HDXセッションでデバイスマネージャー/USBViewまたは同様のアプリケーションを確認することで検証できます。

5. セッション内にデバイスが表示されない場合:

   a. VDAホストに正しいデバイスドライバーが正しくインストールされていない可能性があります。VDAホストに最新バージョンのデバイスドライバーが正しくインストールされていることを確認します。一部のデバイスドライバーはターミナルサーバーマシンでサポートされていないため、リダイレクトしようとしているデバイスがこれに該当しないことを確認してください。

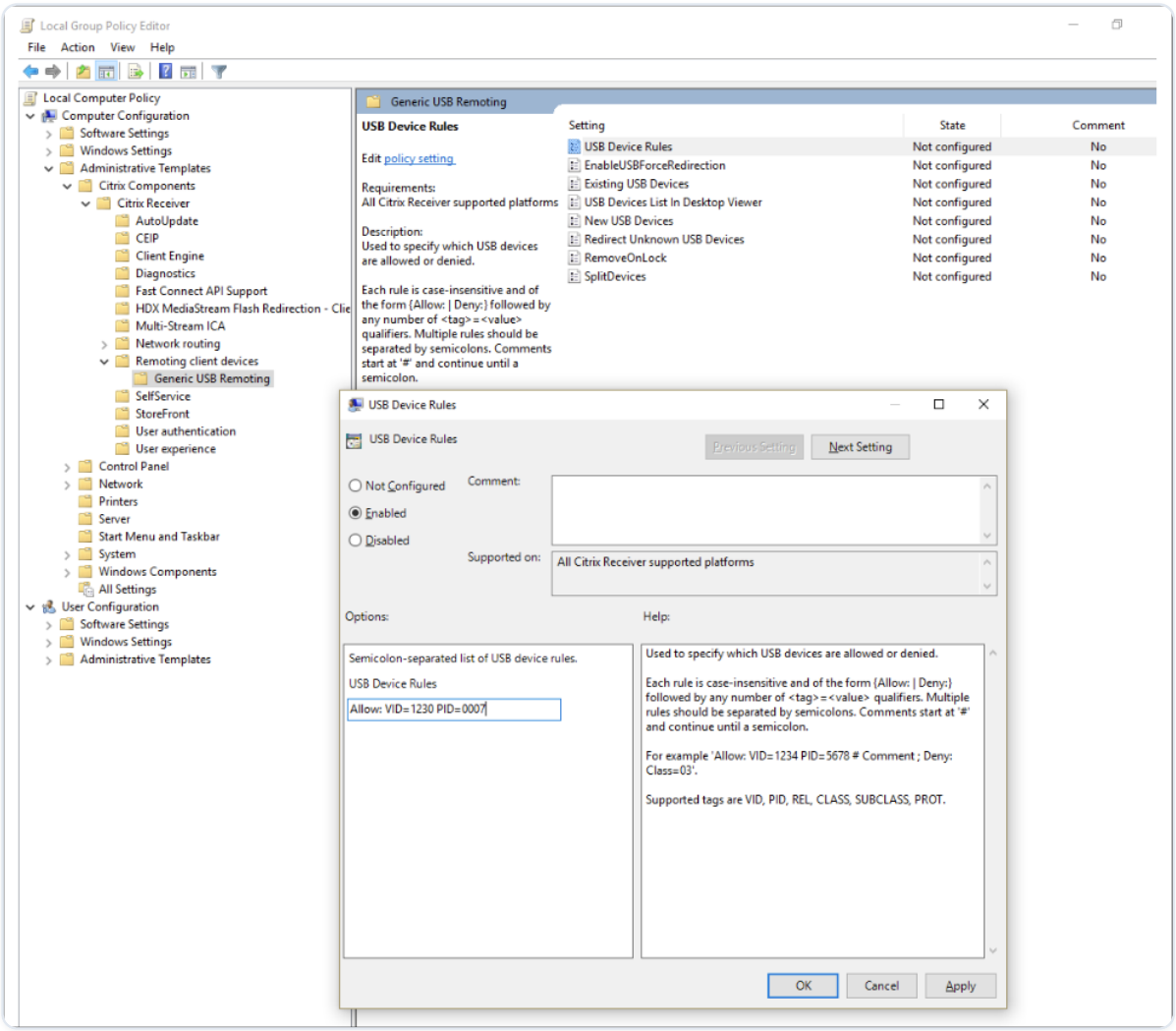
   b. クライアントエンドポイントでデバイスが使用されていないことを確認します。一部のデバイスはクライアントエンドポイントにもドライバーのインストールが必要であり、これによりセッションでのリダイレクトが妨げられる可能性があります。

6. クライアントエンドポイントでUSB関連のルールが正しく設定されていることを確認します。

   a. **ウィンドウズ用 CWA** :

      i. クライアント上のグループポリシー（これに関する詳細とSSを追加）が適切に設定されており、Studioで設定されたルールと競合しないことを検証します。

      ii. クライアントのレジストリ内のデフォルトルールを検証します。



`(HKLM\SOFTWARE\Wow6432Node\Citrix\PortICA\GenericUSB\DeviceRules) are appropriately set and not in conflict with the rules set in Studio and client group policy.`.

b. CWA for Linux - CWA for Linux の問題のトリアージについては、CWA for Linux の USB ドキュメントを参照してください。

c. CWA for Mac - CWA for Mac の問題のトリアージについては、CWA for Mac を参照してください。

注:

- TSVDA では、オーディオデバイスはデフォルトで USB リダイレクトの使用がブロックされています。これらのデバイスを使用する推奨される方法は、最適化されたオーディオVCを使用することです。

- デバイスを分割するための正しいデバイスリダイレクトルールが設定されていても、USB複合デバイスが自動的に分割されない場合があります。この問題は、デバイスが低電力モードになっているために発生します。このような場合、低電力モードに入った子デバイスがデバイスリストに表示されないことがあります。この問題を解決するには、次の回避策を使用できます。
  - セッションを切断し、USBデバイスを挿入してから、セッションに再接続します。
  - USBデバイスを抜き差しします。この操作により、デバイスは低電力モードから復帰します。
- 場合によっては、バッテリー寿命を最適化するためにUSBバッテリーセーバー設定が有効になっていることがあります。クライアントエンドポイントがスリープ状態になると、USBデバイスが切断される可能性があります。このようなシナリオでは、セッションでデバイスを再度表示するために、デバイスを切断して再接続する必要がある場合があります。

イベントログ

管理者は、ユーザーがリダイレクトしようとする可能性のある不正なデバイスを監視し、適切な措置を講じることができます。以下に、リダイレクトが許可されているデバイスと許可されていないデバイスについて、VDAホストのイベントビューアーに記録されるイベントメッセージの一部を示します。

Id	1000
Name	UsbEventAcceptDevice
Severity	Informational
Facility	System
Text	The Citrix USB Service allows the USB Device with Product ID: %2, Vendor ID: %3, and Device ID: %4 to be remoted.
Comment	This message logs the device info of a device redirected in an HDX session

Id	1001
Name	UsbEventPolicyRejectsDeviceV1
Severity	Warning
Facility	System
Text	The USB device with Product ID: 0x%2, Vendor ID: 0x%3, and Device ID: 0x%4 is not being redirected because the Citrix USB policy, "DENY: ...%5..." is in effect. If you wish to redirect the device, please set an allow rule that matches the device in the "Client USB device redirection rules" policy in Citrix Studio.
Comment	This message displays a message of the device not getting redirected if a DENY rule is being enforced by the legacy “Client USB device redirection rules” policy rule.
Arguments	

Id	1002
Name	UsbEventPolicyRejectsDeviceV2
Severity	Warning
Facility	System
Text	The USB device with Product ID: 0x%2, Vendor ID: 0x%3, and Device ID: 0x%4 is not being redirected because the Citrix USB policy, "DENY: ...%5..." is in effect. If you wish to redirect the device, please set an allow rule that matches the device in the "Client USB device redirection rules (Version 2)" policy in Citrix Studio.
Comment	This message displays a message of the device not getting redirected if a DENY rule is being enforced by the "Client USB device redirection rules (Version 2)" policy rule. For instance, if the studio policy rule allows an approved set of devices and denies all other devices and an end user tries to create a new rule on the client endpoint via group policy, this event will get logged. This message would be indicative of an unauthorized device redirection attempt.
Arguments	

USB診断ツール

`CtxUsbDiagnostics.exe`は、VDA上のコマンドラインツールであり、Citrix管理者がクライアントで発生するUSBデバイスのリダイレクトに関する問題を迅速に診断し、解決するのに役立ちます。このユーティリティツールは、HDXセッション内でリダイレクトに失敗しているクライアントに接続されたUSBデバイスに関連する構成の問題をトリアージするために必要な重要な情報を収集します。

> **注：**
>
> - システムレベルの操作を実行するためにツールが必要な権限を持っていることを確認するには、コマンドプロンプトまたはPowerShellを管理者として実行する必要があります。

- `CtxUsbDiagnostics.exe` は `C:\Program Files\Citrix\HDX\bin\CtxUsbDiagnostics.exe` にあります。 そして、すでに環境変数の一部です。このパスに移動する必要はなく、昇格された権限でコマンドプロンプトからこのツールを直接実行できます。

要件

セッションホスト

- オペレーティングシステム
  - Windows 10 1809 以降
  - Windows 11 21H2 以降
  - ウィンドウズ サーバー 2016 以降
- VDA
  - Windows: Citrix Virtual Apps and Desktops™ のバージョン 2311 以降

クライアントデバイス

- オペレーティングシステム
  - Windows 10 1809 以降
- Workspace アプリ
  - Windows: バージョン 2311 以降

ツールの機能?

このツールは現在、以下を提供します。

- SessionID
- VDA デバイスポリシー (Studio で設定されたデバイスルール)
- クライアントデバイスとクライアントデバイスポリシー (デバイスルール)
- デバイスのリスト、そのリダイレクト状態、および許可または拒否された理由



注記：

> 管理者は、すべてのアクティブなセッションのデバイス情報を表示できます。

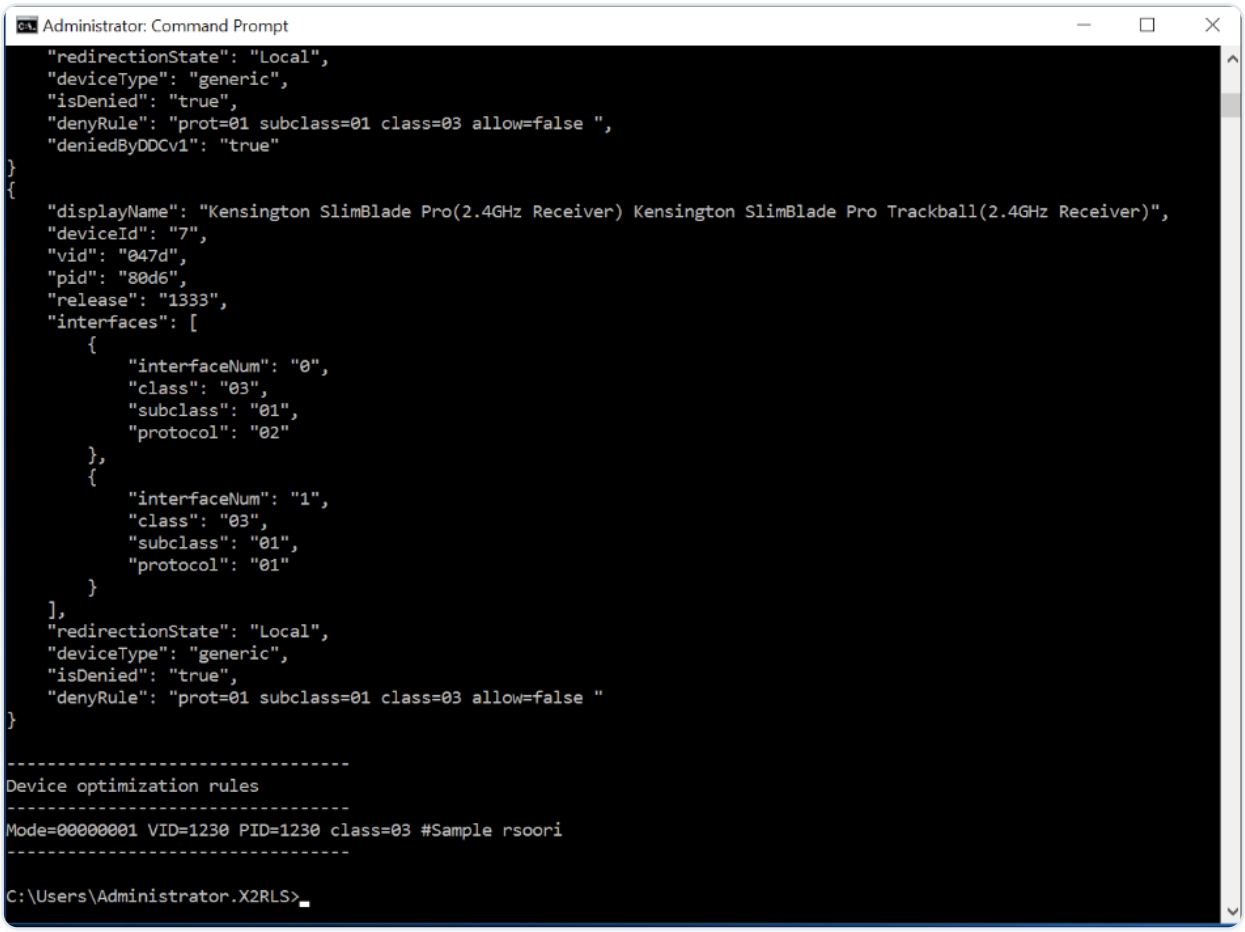
表示される情報

- **Citrix Studio ルール - バージョン 1/2**
  - DDC ルールは、Studio でレガシーな「**クライアント USB デバイスリダイレクトルール**」または「**クライアント USB デバイスリダイレクトルール (バージョン 2)**」ポリシーが使用されていることを示します。このセクションに記載されている情報は、Citrix® 管理者によって構成されたすべてのルールを一覧表示します。



- **クライアントのデフォルトデバイスルール**
  - このセクションでは、クライアントのレジストリに設定されている規則を一覧表示します。

- **デバイス最適化ルール**
  - このセクションでは、「クライアントUSBデバイス最適化規則」で設定されているデバイス最適化規則を一覧表示します。



デバイスリスト

このセクションでは、クライアントエンドポイントに接続されている各デバイスに関する貴重な情報、ハードウェア情報、リダイレクトされているかどうか、正しいデバイスリダイレクト規則が設定されているかどうかなどを一覧表示します。

タグ名	説明
displayName	デバイスの一般名を一覧表示します。
ベンダーID	ベンダーID
製品ID	製品ID
インターフェイス	このサブセクションでは、複合デバイスが複数の子デバイスに分割されている場合に、すべてのインターフェイスを一覧表示します。
InterfaceNum	インターフェイス記述子のインデックスを示します
クラス	クラスコード

タグ名	説明
サブクラス	サブクラスコード
プロトコル	プロトコル
redirectionState	**Local** は、デバイスがICA®セッションでリダイレクトされていないことを示します。**ThisSession** は、デバイスがICAセッションでリダイレクトされていることを示します。**OtherSession** は、デバイスが別のICAセッションでリダイレクトされていることを示します。
deviceType	**汎用**は、デバイスに最適化された仮想チャネルがなく、トラフィックがUSB仮想チャネルを介して流れていることを示します。**最適化済み**は、デバイスに関連付けられたデータ転送が専用の仮想チャネルを介して行われていることを意味します。
isDenied	**true**は、管理者が設定したポリシー規則によりデバイスがリダイレクトされないことを示します。`false`は、適用されたポリシーによりデバイスがリダイレクトされることを示します。
denyRule	このフィールドは、**isDenied**が`true`に設定されている場合に役立ちます。これは、デバイスがリダイレクトされない原因となっているポリシー内の特定の規則を管理者に伝えます。

レガシーUSBリダイレクト設定

バージョン2212より前のコンポーネントを使用している場合、またはLinux版CWAを使用している場合は、環境でのUSBリダイレクトを構成するためにこのガイドに従ってください。

汎用USBリダイレクトの有効化

1. **Citrix Web Studio™ポリシー**を開き、**ポリシー**タブをクリックします。
2. **ポリシーの作成**をクリックし、**ICA® > USBデバイスポリシー**を展開します。
3. **クライアントUSBデバイスリダイレクト**ポリシー設定を編集します。

4. **許可**を選択し、**保存**をクリックします。

USBリダイレクトポリシー規則の作成

ユーザーがUSBデバイスを仮想デスクトップにリダイレクトしようとすると、一致が見つかるまで、各USBポリシー規則に対して順にチェックされます。いずれかのデバイスに対する最初の一致が最終と見なされます。最初の一致が許可規則である場合、一致したデバイスは仮想デスクトップにリダイレクトが許可されます。最初の一致が拒否規則である場合、一致したデバイスはローカルデスクトップでのみ利用可能です。一致が見つからない場合、デフォルト規則が使用されます。

Studioコンソールで適切なデバイス規則を設定する:

1. **Citrix Web Studioポリシー**を開き、**ポリシー**タブをクリックします。
2. **ポリシーの作成**をクリックし、**ICA > USBデバイスポリシー**を展開します。
3. **クライアントUSBデバイスリダイレクト規則**ポリシー設定を編集します。
4. リダイレクトする必要がある各USBデバイスについて、説明に記載されている例に基づいて値を設定し、をクリックします。 例： Allow: VID=056A PID=00A4 #STU-430 Deny: Class=08 subclass=05 # Mass Storage

> **注:**
>
> Citrix®管理者が「既定値を使用」をチェックして「保存」をクリックすると、既定のルールはVDAの次のレジストリで見つけることができます。
>
> **注意:**
>
> レジストリエディターを使用する前に、この記事の最後にある「免責事項」を参照してください。
> `HKLM\SOFTWARE\Wow6432Node\Citrix\PortICA\GenericUSB\DeviceRules`

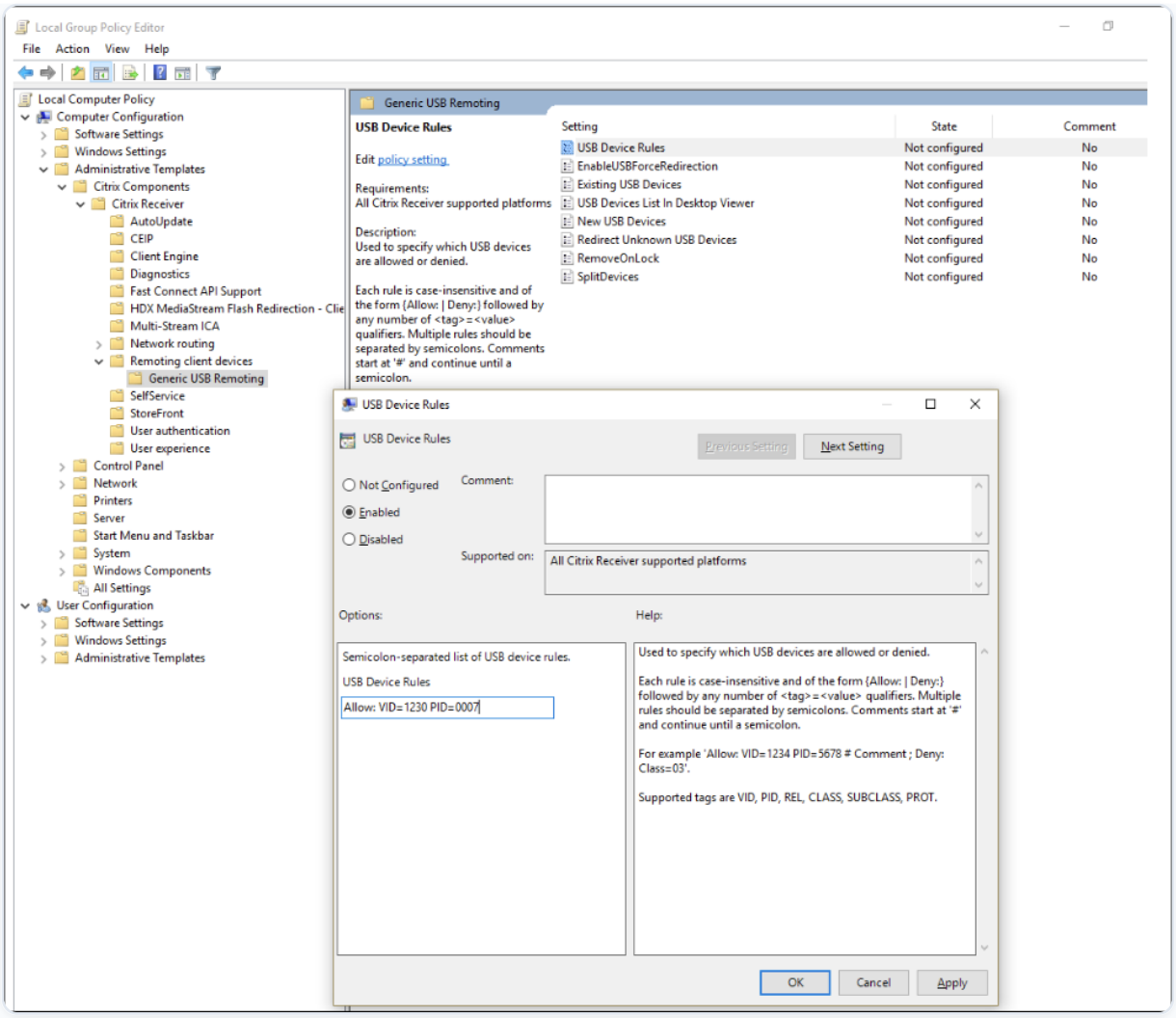
クライアントで適切なGPOを設定する:

1. **ローカルグループポリシーエディター**を開き、**管理用テンプレート > Citrixコンポーネント > Citrix Receiver™ > クライアントデバイスのリモート処理 > 汎用USBリモート処理**に移動します。

2. **USBデバイスルール**設定を開き、**有効**に設定します。次の例のようにUSBデバイスルールを追加します。 Allow: VID=1230 PID=0007ルールは、ベンダーID 1230および製品ID 0007のデバイスを許可します。

注:

特定のデバイスをデバイスルールリストの最上位に配置する必要がある場合は、Allow: VID=xxxx PID=xxxxルールを使用します。



注:

USBViewやConnectionツールバーなどのツールを使用して、VIDやPIDなどのデバイスの詳細を特定できます。

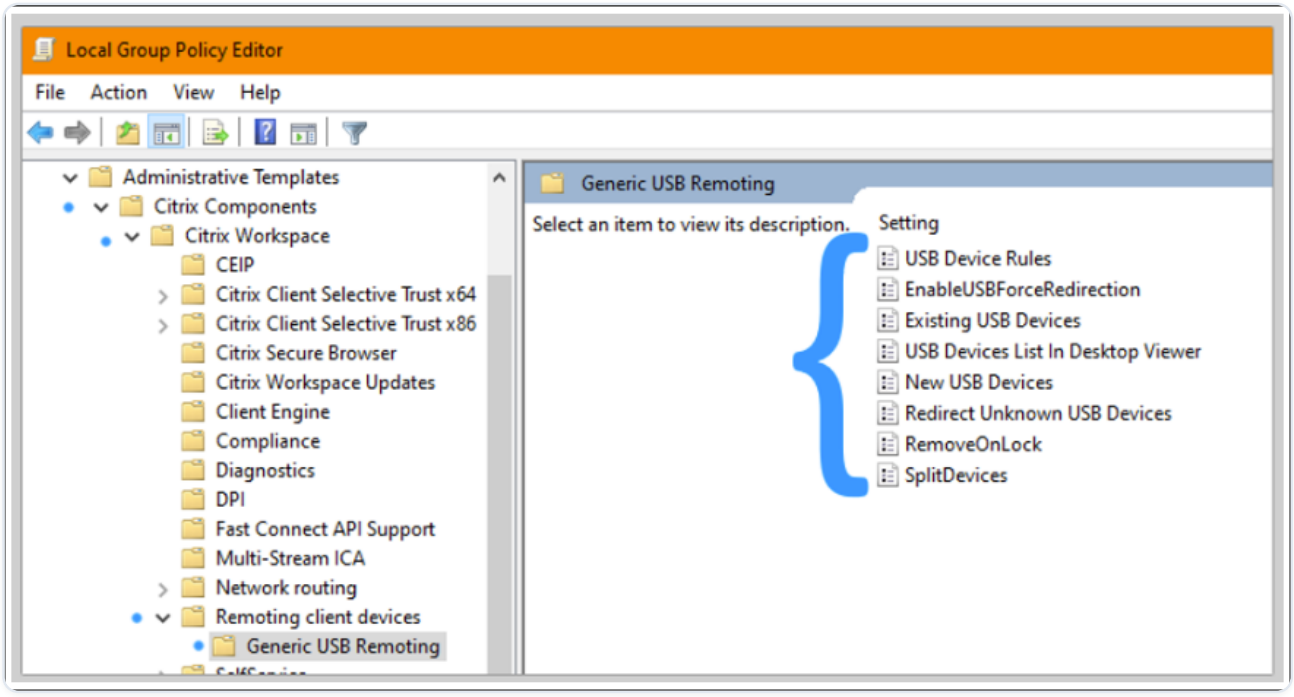
USBデバイスの自動リダイレクトを構成する

USBサポートが有効になっている場合、USBデバイスは自動的にリダイレクトされます。また、USBユーザー設定はUSBデバイスを自動的に接続するように設定されています。すべてのUSBデバイスをリダイレクトすることが常に最適とは限りません。ユーザーは、自動的にリダイレクトされないUSBデバイスをUSBデバイスリストから明示的にリダイレクトできます。USBデバイスが一覧表示されたりリダイレクトされたりするのを防ぐには、クライアントエンドポイントでDeviceRulesポリシー設定を使用します。

このポリシーは、GPO、クライアント側レジストリ、Citrix Workspace™設定、またはCDViewerの「接続」タブを使用してクライアントで設定できます。これらの方法はすべて以下で説明します。

クライアントでGPOを使用する:

1. 「**ローカル グループ ポリシー エディター**」を開き、「**管理用テンプレート > Citrix コンポーネント > Citrix Receiver > クライアントデバイスのリモート処理 > 汎用USBリモート処理**」に移動します。
2. 「**新しいUSBデバイス**」を開き、「**有効**」を選択して「**OK**」をクリックします。
3. 「**既存のUSBデバイス**」を開き、「**有効**」を選択して「**OK**」をクリックします。



Citrix Connection Centerを使用する:

1. 「**Citrix Workspaceの基本設定 > 接続**」に移動します。
2. 以下のオプションが選択されていることを確認します。

a. セッションの開始時に、デバイスを自動的に接続する

b. セッションの実行中に新しいデバイスが接続された場合、デバイスを自動的に接続する。

3. 「**OK**」をクリックします。

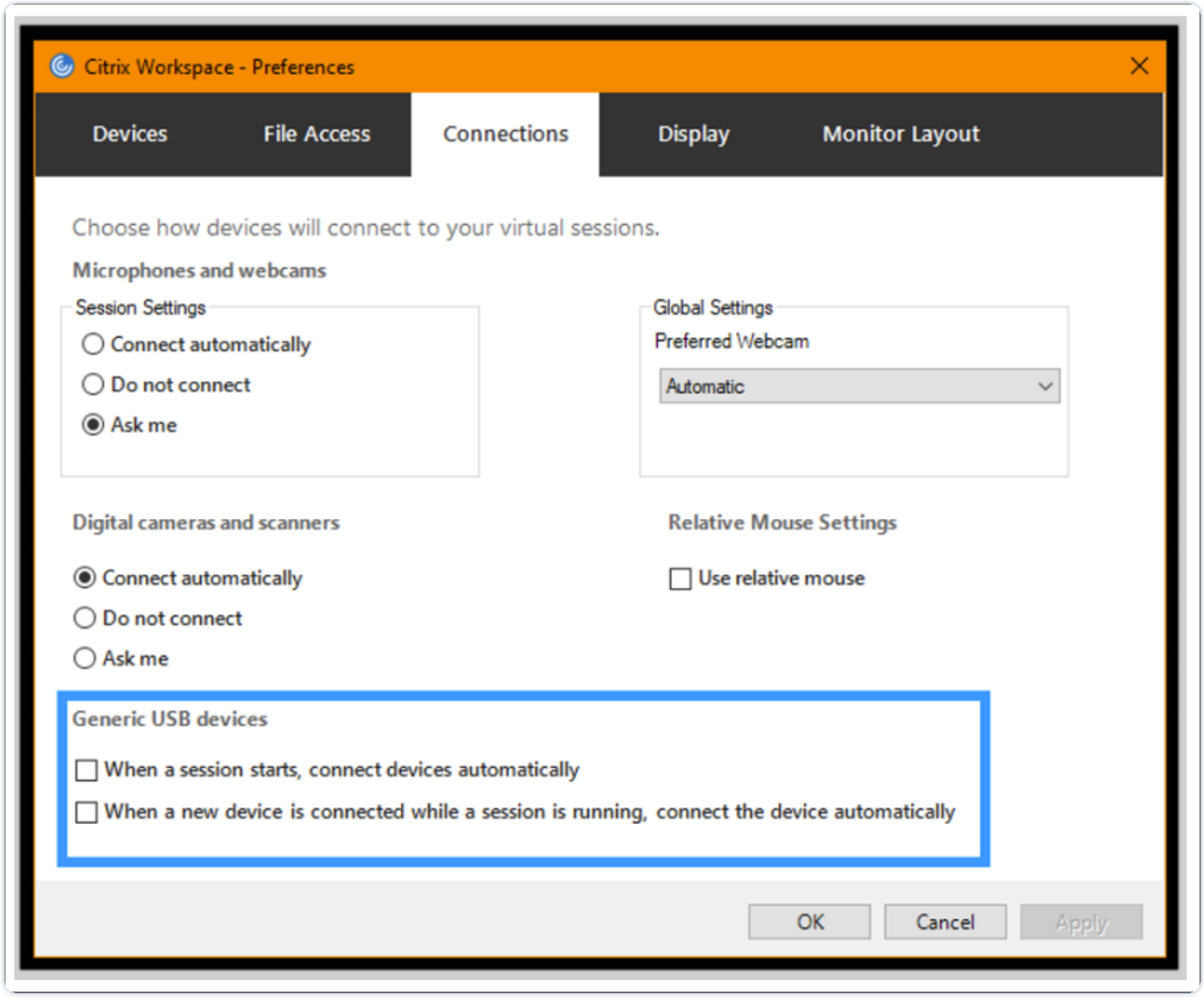
CDViewer接続ツールバーを使用する:

1. セッションの開始後、**CDViewer**ドロップダウンをクリックし、**Citrix Workspaceの基本設定 > 接続**タブを選択します。
2. 以下のオプションが選択されていることを確認します。

a. セッションの開始時に、デバイスを自動的に接続する

b. セッションの実行中に新しいデバイスが接続された場合、デバイスを自動的に接続する。

3. 「**適用**」と「**OK**」をクリックしてポリシーを保存します。



クライアントベースの構成の場合、レジストリキーは次の場所にあるクライアントデバイスに設定されます。

注意:

レジストリエディターを使用する前に、この記事の最後にある免責事項を参照してください。 `HKLM\SOFTWARE\Wow6432Node\Citrix\ICA Client\GenericUSB`

異なるデバイスルールを持つUSBリダイレクトを使用して2つ以上のデバイスを構成する

複数のデバイスを異なるデバイスルールでHDX™セッション内にリダイレクトできます。管理者は、一方のデバイスを自動的にリダイレクトし、もう一方のデバイスをエンドユーザーがリダイレクトするオプションを提供したい場合があります。以下に、異なるルールで2つのデバイスを構成する手順を示します。

1. **クライアントUSBデバイスリダイレクト**ポリシー設定を**Citrix Web Studio**で有効にします。
2. クライアント側のGPOで**USBデバイスルール**設定を編集します。
    a. **ローカルグループポリシーエディター**を開き、**管理用テンプレート > Citrixコンポーネント > Citrix Receiver > クライアントデバイスのリモート処理 > Generic USB Remoting**に移動します。
    b. **USBデバイスルール設定**を開き、設定を有効にします。この例のようにUSBデバイスルールを追加します。**Allow: VID=0911 PID=0c1c**ルールは、**ベンダーID 0911**および**製品ID 0c1c**を持つデバイスを許可しますが、自動的にはリダイレクトされません。**Connect: VID=06A8 PID=0043**ルールは、ステップ3で述べられている自動リダイレクトポリシーが設定されている場合、**ベンダーID 06A8**および**製品ID 0043**を持つデバイスを自動的にリダイレクトします。
    c. **Allow**: VID=0911 PID=0c1c #Phillips スピーチマイク。
    d. **Connect**: VID=06A8 PID=0043 class=03 # Topaz HSB シグネチャパッド
3. **ローカルグループポリシーエディター**を開き、**管理用テンプレート > Citrixコンポーネント > Citrix Receiver > クライアントデバイスのリモート処理 > Generic USB Remoting**に移動します。
4. **新しいUSBデバイス**を開き、**有効**を選択して「**OK**」をクリックします。
5. **既存のUSBデバイス**を開き、**有効**を選択して**OK**をクリックします。

これらの設定が構成されると、Topaz署名パッドはHDXセッション内に自動的にリダイレクトされ、セッション内でPhillipsスピーチマイクをリダイレクトするには追加のエンドユーザー操作が

必要になります（接続センターまたはCD Viewerのデバイスタブでリダイレクトオプションを選択）。

> **注：**

> 上記の手順2と3の設定は、GenericUSBキー（HKLM\SOFTWARE\Wow6432Citrix\ICA Client\GenericUSB）の下にあるクライアント側のレジストリ値「**DeviceRules**」に直接適用できますが、これは推奨される方法ではありません。

汎用USBリダイレクトとクライアントドライブに関する考慮事項

HDX™テクノロジーは、ほとんどの一般的なUSBデバイスに対して**最適化されたサポート**を提供します。最適化されたサポートは、WAN経由でより優れたパフォーマンスと帯域幅効率を提供し、ユーザーエクスペリエンスを向上させます。最適化されたサポートは、特に高遅延またはセキュリティに敏感な環境において、通常は最良の選択肢です。

HDXテクノロジーは、最適化されたサポートがない、または不適切な特殊なデバイスに対して**汎用USBリダイレクト**を提供します。例：

- USBデバイスに、マウスやWebカメラのボタンの増加など、最適化されたサポートに含まれない高度な機能がある場合。
- ユーザーが最適化されたサポートに含まれない機能を必要とする場合。
- USBデバイスが、試験・測定機器や産業用コントローラーなどの特殊なデバイスである場合。
- アプリケーションが、USBデバイスとしてデバイスへの直接アクセスを必要とする場合。
- USBデバイスにWindowsドライバーしか利用できない場合。たとえば、スマートカードリーダーには、Android版Citrix Workspace™アプリ用のドライバーがない場合があります。
- Citrix Workspaceアプリのバージョンが、このタイプのUSBデバイスに対して最適化されたサポートを提供していない場合。

汎用USBリダイレクトでは、次のようになります。

- ユーザーはユーザーデバイスにデバイスドライバーをインストールする必要がありません。
- USBクライアントドライバーはVDAマシンにインストールされます。

> **重要:**

- 汎用USBリダイレクトは、最適化されたサポートと組み合わせて使用できます。汎用USBリダイレクトを有効にする場合は、汎用USBリダイレクトと最適化されたサポートの両方について、CitrixのUSBデバイスポリシー設定を構成してください。
- クライアントUSBデバイス最適化ルールにあるCitrixポリシー設定は、特定のUSBデバイスに対する汎用USBリダイレクトの特定のポリシー設定です。ここで説明されている最適化されたサポートには適用されません。

USBデバイスのパフォーマンスに関する考慮事項

ネットワークの遅延と帯域幅は、一部の種類のUSBデバイスで汎用USBリダイレクトを使用する場合、ユーザーエクスペリエンスとUSBデバイスの動作に影響を与える可能性があります。たとえば、タイミングに敏感なデバイスは、高遅延で低帯域幅のリンクでは正しく動作しない場合があります。可能な場合は、代わりに最適化されたサポートを使用してください。

一部のUSBデバイスは、使用可能にするために高い帯域幅を必要とします。たとえば、3Dマウス（通常、高い帯域幅を必要とする3Dアプリで使用されます）などです。帯域幅を増やすことができない場合でも、帯域幅ポリシー設定を使用して他のコンポーネントの帯域幅使用量を調整することで、問題を軽減できる場合があります。詳細については、クライアントUSBデバイスリダイレクトの帯域幅ポリシー設定と、マルチストリーム接続ポリシー設定を参照してください。

USBデバイスのセキュリティに関する考慮事項

一部のUSBデバイスは、スマートカードリーダー、指紋リーダー、署名パッドなど、本質的にセキュリティに敏感です。USBストレージデバイスなどの他のUSBデバイスは、機密データである可能性のあるデータを送信するために使用できます。

USBデバイスはマルウェアを配布するためによく使用されます。Citrix WorkspaceアプリとCitrix Virtual Apps and Desktops™の設定により、これらのUSBデバイスからのリスクを軽減できますが、排除することはできません。この状況は、汎用USBリダイレクトが使用されているか、最適化されたサポートが使用されているかに関わらず適用されます。

重要:

セキュリティに敏感なデバイスとデータについては、常にHDX接続を保護してください。クライアントとVDA間の通信を参照してください。

必要なUSBデバイスのサポートのみを有効にしてください。このニーズを満たすように、汎用USBリダイレクトと最適化されたサポートの両方を構成してください。

USBデバイスを安全に使用するためのガイダンスをユーザーに提供してください。

- 信頼できるソースから入手したUSBデバイスのみを使用してください。
- インターネットカフェのフラッシュドライブなど、開かれた環境でUSBデバイスを放置しないでください。
- 複数のコンピューターでUSBデバイスを使用するリスクを説明してください。

USBマスストレージデバイスのセキュリティ制御

USBマスストレージデバイスには、最適化されたサポートが提供されます。このサポートは、Citrix Virtual Apps and Desktopsのクライアントドライブマッピングの一部です。ユーザーがログオンすると、ユーザーデバイス上のドライブが仮想デスクトップ上のドライブ文字に自動的にマッピングされます。ドライブは、マッピングされたドライブ文字を持つ共有フォルダーとして表示されます。クライアントドライブマッピングを構成するには、**クライアントリムーバブルドライブ**設定を使用します。この設定は、ICAポリシー設定のファイルリダイレクトポリシー設定セクションにあります。

USB大容量ストレージデバイスでは、クライアントドライブマッピング、汎用USBリダイレクト、またはその両方を使用できます。これらはCitrix®ポリシーを使用して制御します。主な違いは次のとおりです。

機能	クライアントドライブマッピング	汎用USBリダイレクト
デフォルトで有効	はい	いいえ
読み取り専用アクセスを構成可能	はい	いいえ

注：

USBリダイレクトは、50 Kbpsなどの低帯域幅接続でもサポートされています。ただし、大きなファイルのコピーは機能しません。

クライアントドライブマッピング

クライアントドライブマッピングを使用すると、クライアントエンドポイント上のストレージドライブがCitrix HDX™セッション内で利用可能になり、ファイルやフォルダーをクライアントからセッションホストへ、またはその逆に転送できます。この機能は、読み取りおよび書き込み権限の両方でデフォルトで有効になっています。ユーザーがマップされたクライアントデバイス上のファイルやフォルダーを追加または変更できないようにするには、**読み取り専用クライアントドライブアクセス**ポリシー設定を有効にします。この設定をポリシーに追加するときは、**クライアントドライブリダイレクト**設定が**許可**に設定されており、ポリシーにも追加されていることを確認してください。

セキュリティ上の予防措置として、エンドポイントドライブはデフォルトで実行権限なしでマップされます。ユーザーがマップされたクライアントドライブから直接実行可能ファイルを実行できるようにするには、セッションホストで**ExecuteFromMappedDrive**レジストリ値を編集します。詳細については、**レジストリで管理されるHDX機能**セクションのマップされたクライアントドライブを参照してください。

要件

CDMを使用するための要件は次のとおりです。

Citrixコントロールプレーン

- シトリックス Virtual Apps and Desktops™ 1912以降
- シトリックス DaaS™

セッションホスト

- オペレーティングシステム
  - Windows 10 1809以降
  - Windows Server 2016、またはそれ以降のバージョン
  - Linux: Linux VDAのシステム要件を参照してください。
- VDA
  - Windows: Citrix Virtual Apps and Desktops 1912、またはそれ以降のバージョン
  - Linux: Linux VDA のドキュメントを参照してください。

クライアントデバイス

- オペレーティングシステム

- Windows 10 1809 以降
- Linux: Workspace app for Linuxのシステム要件を参照してください。

関連ポリシー

CDM設定については、ポリシー設定リファレンスセクションを参照してください。

ダブルホップシナリオ

CDMはダブルホップシナリオでサポートされています。デフォルトでは、クライアントエンドポイントのドライブはセカンドホップセッションにマップされ、ファーストホップのドライブは利用できません。ただし、クライアントエンドポイントのドライブの代わりに、ファーストホップのドライブがセカンドホップセッションにマップされるように設定することも可能です。

この機能を構成するには、次のレジストリ値を編集します。

- キー: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ClientDrive\
- 値の名前: NativeDriveMapping
- 値の型: REG_SZ
- 値のデータ:
  - True - セカンドホップセッションでファーストホップセッションのドライブをマップします
  - False - 2番目のホップセッションでクライアントエンドポイントのドライブをマップします

注:

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

モバイルデバイスとタッチスクリーンデバイス

Citrix Virtual Apps and Desktops™ を使用すると、ユーザーは公開されたアプリケーションやデスクトップにモバイルおよびタッチスクリーンクライアントデバイスからアクセスできます。

要件

Citrix® コントロールプレーン

- シトリックス バーチャルアプリとデスクトップ 1912 以降
- シトリックス DaaS™

セッションホスト

- オペレーティングシステム
  - Windows 10 1903 以降
  - Windows 11 21H2 以降
- VDA
  - Windows: シトリックス バーチャルアプリ アンド デスクトップ バージョン 7.15 以降

クライアントデバイス

- オペレーティングシステム
  - Windows 10 1809 以降
  - Windows 11 21H2 以降
- Windows 用 Citrix Workspace™ アプリ バージョン 1808 以降

Windows Continuum を使用するタッチスクリーンデバイスのタブレットモード

Continuum は、クライアントデバイスの使用方法に適応する Windows 10 の機能です。VDA は、タッチ対応クライアントでキーボードまたはマウスの存在を検出すると、クライアントをデスクトップモードにします。キーボードまたはマウスが存在しない場合、VDA はクライアントをタブレット/モバイルモードにします。この検出は、セッションの接続時および再接続時、ならびにセッション中にキーボードまたはマウスが接続または切断されたときに発生します。

この機能はデフォルトで有効になっています。この機能を無効にするには、ポリシー設定 タブレットモード切り替えポリシー設定 を構成します。

上記のタッチスクリーンデバイスの要件に加えて、Windows Continuumには以下が必要です。

ゼノサーバー (旧 シトリックス ハイパーバイザー™)

- シトリックス ハイパーバイザー 8.2 以降

- ラップトップ/タブレットの切り替えを許可するには、XenServer CLIコマンドを実行します。
  xe vm-param-set uuid=\<VM_UUID\> platform:acpi_laptop_slate=1

重要:

メタデータ設定を変更した後、既存のマシンカタログのベースイメージを更新しても、以前にプロビジョニングされたVMには影響しません。XenServer VMベースイメージを変更した後、カタログを作成し、ベースイメージを選択して、新しいMachine Creation Services™ (MCS) マシンをプロビジョニングします。

セッションホスト

- オペレーティングシステム
  - Windows 10 1903 以降
  - Windows 11 21H2 以降
- VDA
  - Windows: バージョン 7.16 以降
  - **オペレーティングシステム構成の現在の制限により、ユーザーは最初のICA®セッションを開始してVDAを再起動した後、ドロップダウンメニューから次のオプションを設定する必要があります。**
    - **設定 > システム > タブレットモード**
      - ハードウェアに適したモードを使用する
      - 常に切り替える（確認しない）

タブレットモードは、タッチスクリーンにより適したユーザーインターフェイスを提供します。

- わずかに大きいボタン。
- スタート画面と起動するすべてのアプリが全画面で開きます。
- タスクバーに「戻る」ボタンが含まれています。
- タスクバーからアイコンが削除されます。

ファイルエクスプローラーにアクセスできます。

Windows 10 は、この更新された BIOS に基づいて、ターゲット仮想マシンに GPIO ドライバーをロードします。これは、仮想マシン内でタブレットモードとデスクトップモードを切り替えるために使用されます。

Citrix Workspace app for HTML5 は Windows Continuum 機能に対応していません。

デスクトップモードは、PCとキーボード、マウスを使用するのと同じ方法で操作できる、従来のユーザーインターフェイスを提供します。

マイクロソフト サーフェス プロ および サーフェス ブック のペン

Windows Ink ベースのアプリケーションで標準のペン機能をサポートしています。サポートには、ポインティング、消去、筆圧、Bluetooth 信号、およびオペレーティングシステムのファームウェアとペンモデルに応じたその他の機能が含まれます。たとえば、筆圧は最大 4096 レベルです。この機能はデフォルトで有効になっています。

ペン機能のサポート要件は次のとおりです。

Citrix コントロールプレーン

- Citrix Virtual Apps and Desktops 1903 以降
- Citrix DaaS

セッションホスト

- オペレーティングシステム
  - Windows 10 1809 以降
  - Windows 11 21H2 以降
- VDA
  - ウィンドウズ: Citrix Virtual Apps and Desktops 1903 以降

クライアントデバイス

- オペレーティングシステム
  - Windows 10 1809 以降
  - Windows 11 21H2 以降
- Windows向けCitrix Workspaceアプリ バージョン1902以降

Windows Inkとペン機能のデモンストレーションについては、このグラフィックをクリックしてください:



この機能を無効または有効にするには、レジストリを介して管理される機能のリストにあるMicrosoft Surface ProおよびSurface Bookペンを参照してください。

既知の問題

ペンサポートに関する既知の問題は次のとおりです:

- ウィンドウズサーバー 2k22 のOSの制限により、2k22サーバーアプリケーションまたはデスクトップに接続している場合、ユーザーはコントロールパネルでペンのショートカットを設定したり、ペン/インクの設定を調整したりすることはできません。
- OSの制限により、ペン対応のWindows 11クライアントからのペンのショートカットは認識されません。

シリアルポート

ほとんどの新しいPCには、シリアル（COM）ポートが内蔵されていません。USBコンバーターを使用すると、ポートを簡単に追加できます。シリアルポートに適したアプリケーションには、センサー、コントローラー、古いチェックリーダー、パッドなどがよく含まれます。一部のUSB仮想COMポートデバイスは、Windows提供のドライバー（usbser.sys）の代わりにベンダー固有のドライバーを使用します。これらのドライバーを使用すると、USBデバイスの仮想COMポートを強制的に設定できるため、異なるUSBソケットに接続しても変更されません。これは、**デバイスマネージャー > ポート (COM と LPT) > プロパティ**から、またはデバイスを制御するアプリケーションから行うことができます。

クライアントCOMポートマッピングにより、ユーザーのエンドポイントのCOMポートに接続されたデバイスを仮想セッション中に使用できます。これらのマッピングは、他のネットワークマッピングと同様に使用できます。

各COMポートについて、オペレーティングシステムのドライバーはCOM1やCOM2などのシンボリックリンク名を割り当てます。アプリケーションは、そのリンクを使用してポートにアクセスします。

> **重要:**

デバイスがUSBを直接使用してエンドポイントに接続できるからといって、汎用USBリダイレクトを使用してリダイレクトできるわけではありません。一部のUSBデバイスは仮想COMポートとして機能し、アプリケーションは物理シリアルポートと同じ方法でアクセスできます。オペレーティングシステムはCOMポートを抽象化し、ファイル共有のように扱うことができます。仮想COMの2つの一般的なプロトコルは、CDC ACMまたはMCTです。RS-485ポートを介して接続した場合、アプリケーションがまったく機能しない場合があります。RS-485をCOMポートとして使用するには、RS-485-to-RS232コンバーターを入手してください。 **重要:**

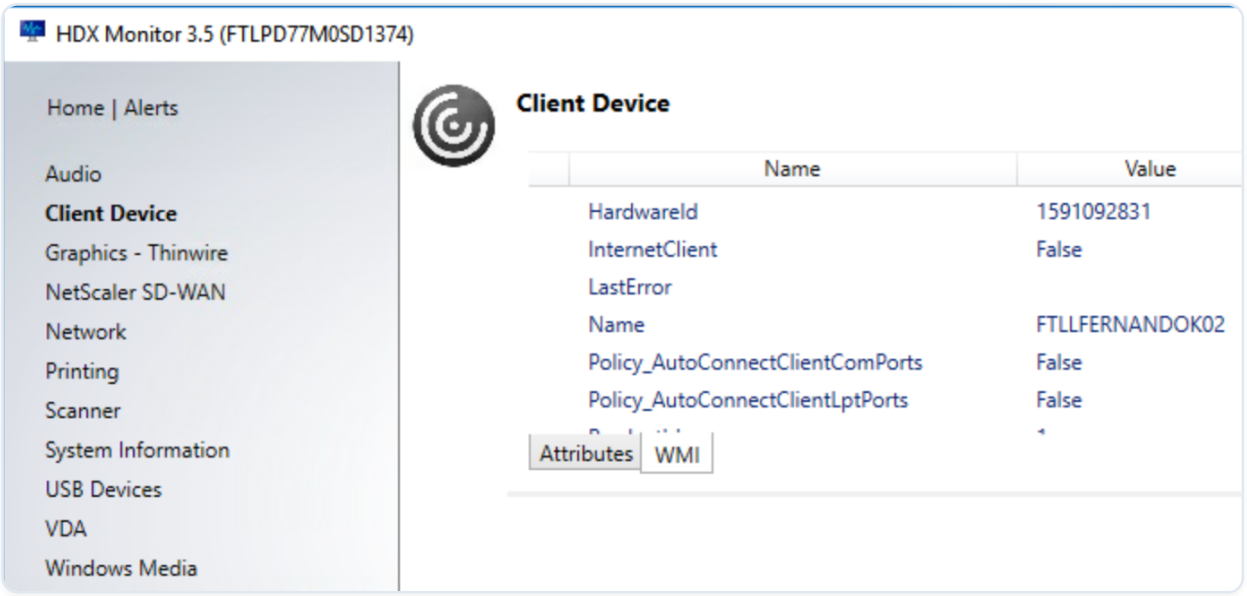
一部のアプリケーションは、クライアントワークステーションのCOM1またはCOM2に接続されている場合にのみ、デバイス（たとえば、署名パッド）を一貫して認識します。

クライアントCOMポートをサーバーCOMポートにマッピングする

クライアントCOMポートをCitrix®セッションにマッピングするには、3つの方法があります。

- Studioポリシー。ポリシーの詳細については、「ポートリダイレクトポリシー設定」を参照してください。
- VDAコマンドプロンプト。
- リモートデスクトップ（ターミナルサービス）構成ツール。

1. **クライアントCOMポートリダイレクト**ポリシーと**クライアントCOMポートの自動接続Studio**ポリシーを有効にします。適用後、一部の情報はHDX™ Monitorで利用できます。



2. **クライアントCOMポートの自動接続**がポートのマッピングに失敗した場合は、ポートを手動でマッピングするか、ログオンスクリプトを使用できます。VDAにログオンし、コマンドプロンプトウィンドウで次のように入力します。

   NET USE COMX: `\CLIENT\COMZ`:

   または

   NET USE COMX: `\CLIENT\CLIENTPORT:COMZ`:

   X はVDA上のCOMポートの番号です（ポート1～9がマッピングに利用可能です）。**Z** はマッピングしたいクライアントCOMポートの番号です。

   操作が成功したことを確認するには、VDAのコマンドプロンプトで「**NET USE**」と入力します。表示されるリストには、マップされたドライブ、LPTポート、およびマップされたCOMポートが含まれています。



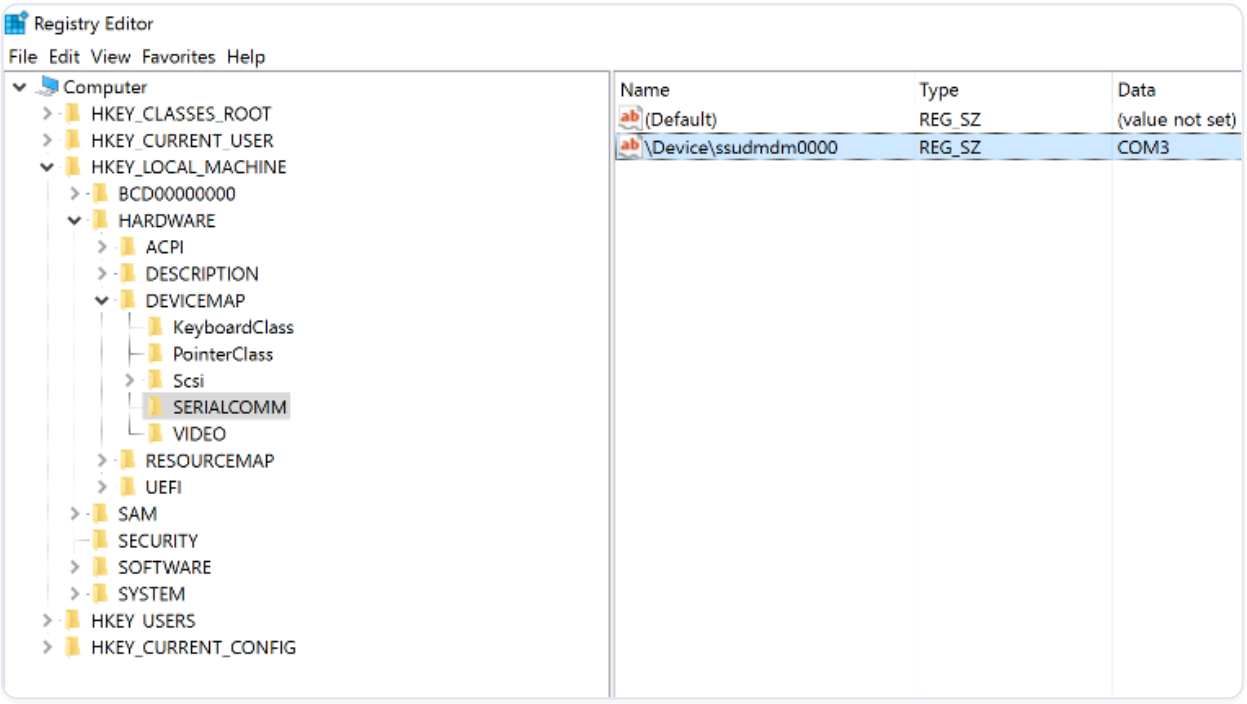
3. このCOMポートを仮想デスクトップまたはアプリケーションで使用するには、ユーザーデバイスアプリケーションをインストールし、マップされたCOMポート名を指定します。たとえば、クライアント上のCOM1をサーバー上のCOM3にマップする場合、VDAにCOMポートデバイスアプリケーションをインストールし、セッション中にCOM3を指定します。このマップされたCOMポートは、ユーザーデバイス上のCOMポートと同様に使用します。

重要:

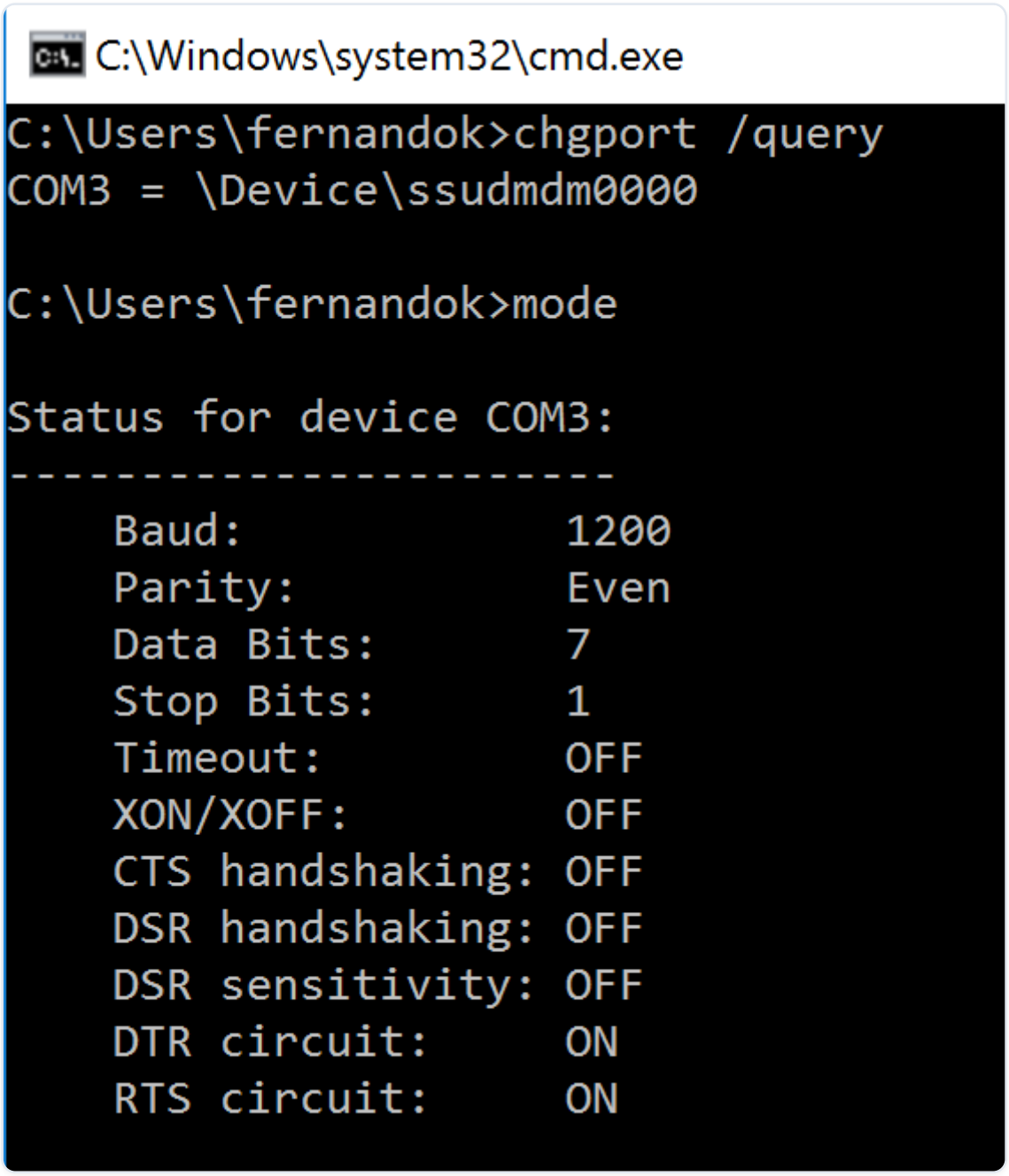
COMポートマッピングはTAPI互換ではありません。Windows Telephony Application Programming Interface (TAPI) デバイスをクライアントCOMポートにマップすることはできません。TAPIは、データ、FAX、音声通話の電話機能をアプリケーションが制御するための標準的な方法を定義します。TAPIは、ダイヤル、応答、通話終了などのシグナリングを管理します。また、保留、転送、会議通話などの付加サービスも管理します。

トラブルシューティング

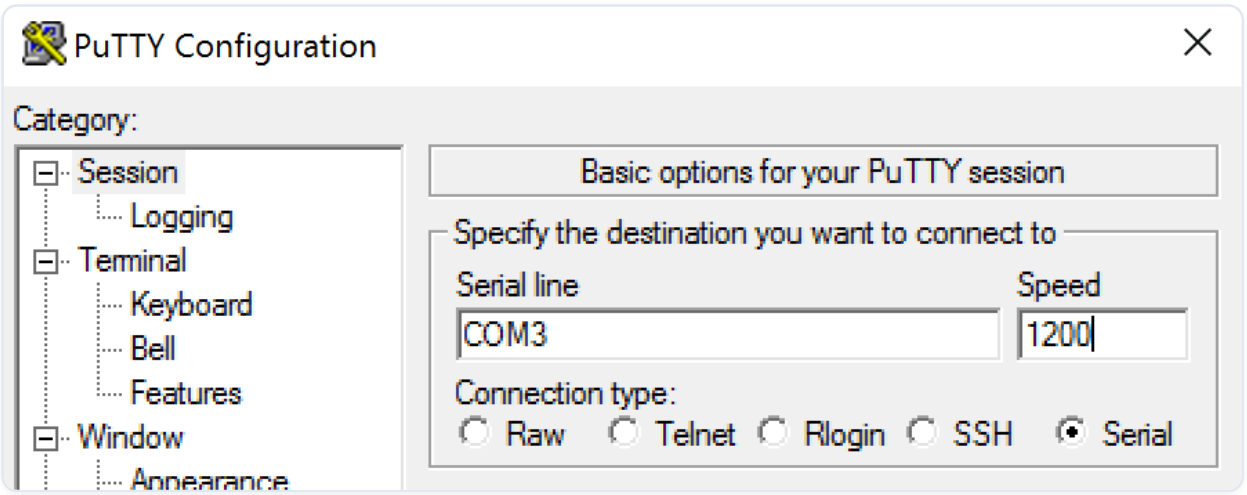
1. Citrixをバイパスして、エンドポイントからデバイスに直接アクセスできることを確認してください。ポートがVDAにマップされていない間は、Citrixセッションに接続されていません。デバイスに付属のトラブルシューティング手順に従い、まずローカルで動作することを確認してください。 シリアルCOMポートにデバイスが接続されている場合、ここに示されているハイブにレジストリキーが作成されます。



この情報は、コマンドプロンプトで「**chgport /query**」を実行することでも確認できます。



デバイスのトラブルシューティング手順が利用できない場合は、PuTTYセッションを開いてみてください。「**Session**」を選択し、「**Serial line**」でCOMポートを指定します。



ローカルコマンドウィンドウで **MODE** を実行できます。出力には、使用中のCOMポートと、PuTTYセッションで必要となるBaud/Parity/Data Bits/Stop Bitsが表示される場合があります。PuTTY接続が成功した場合は、**Enter** を押してデバイスからのフィードバックを確認します。入力した文字が画面に繰り返されたり、応答されたりする場合があります。この手順が失敗した場合、仮想セッションからデバイスにアクセスすることはできません。

2. ローカルのCOMポートをVDAにマッピングし（ポリシーまたは **NET USE COMX: \\\CLIENT\COMZ:** を使用）、前の手順と同じPuTTY手順を繰り返しますが、今回はVDA PuTTYから実行します。PuTTYが「**Unable to open connection to COM1. Unable to open serial port**」というエラーを表示して失敗する場合、別のデバイスがCOM1を使用している可能性があります。
3. **chgport /query** を実行します。VDA上の組み込みWindowsシリアルドライバーが \Device\Serial0をVDAのCOM1ポートに自動割り当てしている場合は、次の操作を行います。
   A. VDAでCMDを開き、**NET USE.** と入力します。

   B. VDA上の既存のマッピング（例：COM1）を削除します。

   NET USE COM1 /DELETE

   C. デバイスをVDAにマッピングします。

   NET USE COM1: `\CLIENT\COM3` :

   D. VDA上のアプリケーションをCOM3にポイントします。

   最後に、ローカルのCOMポート（例：COM3）をVDA上の別のCOMポート（COM1以外、例：COM3）にマッピングしてみてください。アプリケーションがそれを指していることを確認してください。 **NET USE COM3: \\\CLIENT\COM3**
4. ポートがマッピングされていることが確認でき、PuTTYは動作しているもののデータが通過しない場合、それは競合状態である可能性があります。アプリケーションがマッピングされる前にポートに接続して開いてしまい、マッピングをロックしている可能性があります。次のいずれかを試してください。

   - 同じサーバーで公開されている2番目のアプリケーションを開きます。ポートがマッピングされるまで数秒待ってから、ポートを使用しようとする実際のアプリケーションを開きます。
   - Studioではなく、Active DirectoryのグループポリシーエディターからCOMポートリダイレクトポリシーを有効にします。これらのポリシーは、**Client COM port redirection** と **Auto connect client COM ports** です。このように適用されたポリシーは、Studioポリシーよりも前に処理され、COMポートが確実にマッピングされることを保証する場合があ

ります。CitrixポリシーはVDAにプッシュされ、次の場所に保存されます。`HKLN\SOFTWARE\Policies\Citrix \<user session ID\>`

- ユーザーにこのログオンスクリプトを使用するか、アプリケーションを公開する代わりに、まずVDA上のマッピングを削除し、仮想COMポートを再マッピングしてからアプリケーションを起動する.batスクリプトを公開します。

@echo off NET USE COM1 /delete NET USE COM2 /delete NET USE COM1: `\CLIENT\COM1`: NET USE COM2: `\CLIENT\COM2`: MODE COM1: BAUD=1200 (または必要な値) MODE COM2: BAUD=9600 PARITY=N Data=8 Stop=1 (または必要な値) START `C:\Program Files\<Your Software Path>\<your_software.exe>`

5. SysinternalsのProcess Monitorは、最後の手段となるツールです。VDAでこのツールを実行する際、COM3、picaser.sys、CdmRedirector、特に\<your_app\>.exeのようなオブジェクトを見つけてフィルターします。エラーは「Access Denied」または類似の形で表示される場合があります。

特殊キーボード

Bloombergキーボード

警告:

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

Citrix Virtual Apps and Desktops™は、Bloombergモデル5、モデル4 Starboardキーボード（およびそれ以前のモデル3）をサポートしています。このキーボードにより、金融業界のお客様は、キーボードの特殊機能を使用して金融市場データにアクセスし、迅速な取引を実行できます。

重要:

> Bloombergキーボードは1つのセッションでのみ使用することをお勧めします。複数の同時セッション（1つのクライアントから複数のセッションへ）でキーボードを使用することはお勧めしません。

> Bloombergキーボードは、1つの物理シェルに複数のUSBデバイスを搭載したUSB複合デバイスです。

- キーボード。
- 指紋リーダー。
- 音量を上げ下げするキー、およびスピーカーとマイクをミュートするキーを備えたオーディオデバイス。このデバイスには、オンボードスピーカー、マイク、およびマイクとヘッドセット用のジャックが含まれています。
- これらすべてのデバイスをシステムに接続するためのUSBハブ。

要件:

- Citrix Workspace™ app for Windows が接続するセッションは、USB デバイスをサポートしている必要があります。
- Bloomberg キーボードモデル 5 をサポートするには、Citrix Workspace app 2207 for Linux 以降が必要です。
- Bloombergキーボードモデル5をサポートするには、Windows版Citrix Workspaceアプリ2109以降が必要です。
- Bloombergキーボードモデル3および4をサポートするには、Windows版Citrix Workspaceアプリ1808以降、またはWindows版Citrix Receiver 4.8以降が必要です。
- モデル4でKVMモード（KVM経由でルーティングされた1本のUSBケーブルを含む2本のUSBケーブル）を使用するには、Windows版Citrix Workspaceアプリ1808以降、またはWindows版Citrix Receiver 4.12以降が必要です。

Windows版Citrix WorkspaceアプリでのBloombergキーボードの構成については、Bloombergキーボードの構成を参照してください。

Bloombergキーボードのサポートを有効にするには、レジストリで管理される機能の一覧にあるBloombergキーボードを参照してください。

サポートを確認する:

Citrix WorkspaceアプリでBloombergキーボードのサポートが有効になっているかどうかを確認するには、Desktop ViewerがBloombergキーボードのデバイスを正しく報告しているかを確認します。

デスクトップシナリオ:

Desktop Viewerを開きます。Bloombergキーボードのサポートが有効になっている場合、Desktop ViewerにはUSBアイコンの下に3つのデバイスが表示されます。

Bloomberg 5キーボードの場合:

- ブルームバーグ LP ブルームバーグ バイオメトリック モジュール
- Bloomberg LP Keyboard（2つのインターフェイスを持つ複合デバイス）
- Bloomberg LP Keyboard Audio（3つのインターフェイスを持つ複合デバイス）

Bloomberg 3および4キーボードの場合:

- ブルームバーグ 指紋スキャナー
- Bloombergキーボード機能
- Bloomberg LPキーボード 2013

シームレスアプリケーションのみのシナリオ:

Citrix Workspaceアプリの通知領域アイコンから「**接続センター**」メニューを開きます。Bloombergキーボードのサポートが有効になっている場合、3つのデバイスが「**デバイス**」メニューに表示されます。

これらの各デバイスのチェックマークは、それらがセッションにリモート接続されていることを示します。

Windows - キーボードおよびIMEサポートツール

これは、キーボードと入力メソッドエディターに関連する問題を診断できるセルフサービスコマンドラインツールです。

さまざまなユーザー要件を満たし、プラットフォームの汎用性を提供し、ユーザーにパーソナライズされたニーズを提供するために、キーボードと入力方式エディター (IME) の機能は、VDA と Citrix Workspace™ アプリのさまざまな構成と機能に依存しています。

VDA またはクライアント側の設定が正しくない場合、予期しない入力動作が発生する可能性があります。

ただし、Citrix® はいくつかの一般的な使用シナリオに対して推奨設定を提供しており、これらの推奨事項は診断結果にも含まれています。

このツールを使用すると、以下のカテゴリの問題を特定できます。

- **キーボードタイプの不整合:** VDA キーボードタイプとクライアントキーボードタイプをチェックし、不整合がないか確認します。たとえば、VDA が 101 英語キーボードを使用しているのに、クライアントが日本語 106 キーボードを使用している場合などです。この診断は、JP 106/109 キーボードおよび KO 103/106 キーボードの使用事例を対象としています。
- **キーボードレイアウト同期モードの不整合:** キーボードレイアウト同期設定、レジストリ設定、グループポリシーをチェックし、特定の環境における同期モード構成の問題を解決します。
- **クライアントキーボードレイアウトとVDAキーボードレイアウトの不整合:** クライアントキーボードレイアウトがVDAキーボードレイアウトと同じであるかを確認します。
- **アプリケーションセッションでリモート言語バーが表示されない:** エンドユーザーがアプリケーションセッションを起動し、複数のキーボードレイアウトを使用している場合に、リモート言語バーが表示されているかどうかを確認します。

このコマンドラインツールはWindows VDA - `CtxKbImeDiagnostics.exe` にホストされています。 コマンドラインインターフェースは以下のとおりです。

インターフェース	説明	注
`CtxKbimeDiagnostics`	現在のICA®セッションのみの診断結果を表示	ユーザーが管理者権限を持っている場合、すべてのアクティブなICAセッションの診断を表示します。ユーザーが管理者権限を持っていない場合、現在のユーザーのICAセッションの診断を表示します
`CtxKbimeDiagnostics [-v]`	現在のセッションの設定情報と診断結果を表示	ユーザーが管理者権限を持っている場合、すべてのアクティブなICAセッションの診断を表示します
`CtxKbimeDiagnostics [-v] [-s Session_Id]`	このセッションの設定情報と診断結果を表示	

インターフェース	説明	注
`CtxKbimeDiagnostics [-s Session_Id]`	セッションを指定し、そのセッションの診断結果を表示します	管理者権限は他のICAセッションを照会できます/通常ユーザーは自身のICAセッションのみを照会できます
`CtxKbimeDiagnostics [-s Session_Id] [-v]`	セッションを指定し、そのセッションのすべての設定情報と診断結果を表示します	管理者権限は他のICAセッションを照会できます。通常ユーザーは自身のICAセッションのみを照会できます
`CtxKbimeDiagnostics [-h]`	サポートされている引数/パラメーターと例を表示	「ヘルプ」インターフェース
`CtxKbimeDiagnostics [-V]`	現在のツールのバージョンを表示	

注:

このバージョンでは、クライアントとしてCWA Windowsのみがサポートされています。

Webカメラ

高精細ウェブカメラストリーミング

仮想セッション内で実行されているビデオ会議アプリケーションでウェブカメラを使用できます。サーバー上のアプリケーションは、サポートされているフォーマットタイプに基づいてウェブカメラのフォーマットと解像度を選択します。セッションが開始されると、クライアントはウェブカメラ情報をサーバーに送信します。ビデオ会議アプリケーションからウェブカメラを選択します。ウェブカメラとアプリケーションの両方が高精細レンダリングをサポートしている場合、アプリケーションは高精細解像度を使用します。ウェブカメラの解像度は最大1920x1080までサポートしています。

この機能には、Citrix Receiver for Windows バージョン4.10以降が必要です。HDXウェブカメラリダイレクトをサポートするCitrix Workspaceアプリプラットフォームのリストについては、「Citrix Workspace app feature matrix」を参照してください。

高精細ウェブカメラストリーミングの詳細については、「HDX video conferencing and webcam video compression」を参照してください。

レジストリキーを使用してこの機能を無効または有効にし、特定の解像度を構成できます。詳細については、レジストリで管理される機能のリストにある「High-definition webcam streaming and High-definition webcam resolution」を参照してください。

グラフィック

HDX™ 3D プロ

HDX 3D Pro（現在はHDX Graphicsとして知られています）は、要求の厳しいグラフィックワークロードに対して高性能なユーザーエクスペリエンスを提供します。デフォルトでは、GPUを活用してDirectXおよびOpenGLアプリケーションの両方にハードウェアアクセラレーションを提供します。以前はHDX 3D Proに関連付けられていたこの機能は、追加のポリシーや構成を必要とせずに、すべてのユーザーが標準で利用できるようになりました。

ハードウェアアクセラレーションを使用すると、設計、エンジニアリング、マルチメディア制作などの分野で使用されるものを含め、最もグラフィック負荷の高いアプリケーションでも、ユーザーにシームレスで応答性の高いエクスペリエンスを提供できます。

Citrix Virtual Apps and Desktops™のHDX 3D Pro機能により、ハードウェアアクセラレーションのためにグラフィックス処理ユニット（GPU）を使用すると最高のパフォーマンスを発揮するデスクトップとアプリケーションを提供できます。これらのアプリケーションには、OpenGLおよびDirectXベースの3Dプロフェッショナルグラフィックアプリケーションが含まれます。標準VDAはDirectXのGPUアクセラレーションのみをサポートします。

HDX 3D Proポリシー設定については、3Dグラフィックワークロードの最適化を参照してください。

サポートされているすべてのCitrix Workspaceアプリは、3Dグラフィックで使用できます。複雑な3Dワークロード、高解像度モニター、マルチモニター構成、高フレームレートアプリケーションで最高のパフォーマンスを得るには、Citrix Workspace app for WindowsおよびCitrix Workspace app for Linuxの最新バージョンをお勧めします。Citrix Workspaceアプリのサポートされているバージョンに関する詳細については、Citrix Workspaceアプリのライフサイクルマイルストーンを参照してください。

3Dプロフェッショナルアプリケーションの例は次のとおりです。

- コンピューター支援設計、製造、エンジニアリング (CAD/CAM/CAE) アプリケーション
- 地理情報システム (GIS) ソフトウェア
- 医用画像処理通信システム (PACS)

- 最新のOpenGL、DirectX、NVIDIA CUDA、OpenCL、およびWebGLバージョンを使用するアプリケーション
- 並列コンピューティングにNVIDIA Compute Unified Device Architecture (CUDA) GPUを使用する計算集約型の非グラフィックアプリケーション

HDX 3D Proは、あらゆる帯域幅で最高のユーザーエクスペリエンスを提供します。

- WAN接続の場合：1.5 Mbpsという低い帯域幅のWAN接続でも、インタラクティブなユーザーエクスペリエンスを提供します。
- LAN接続の場合：LAN接続でローカルデスクトップと同等のユーザーエクスペリエンスを提供します。

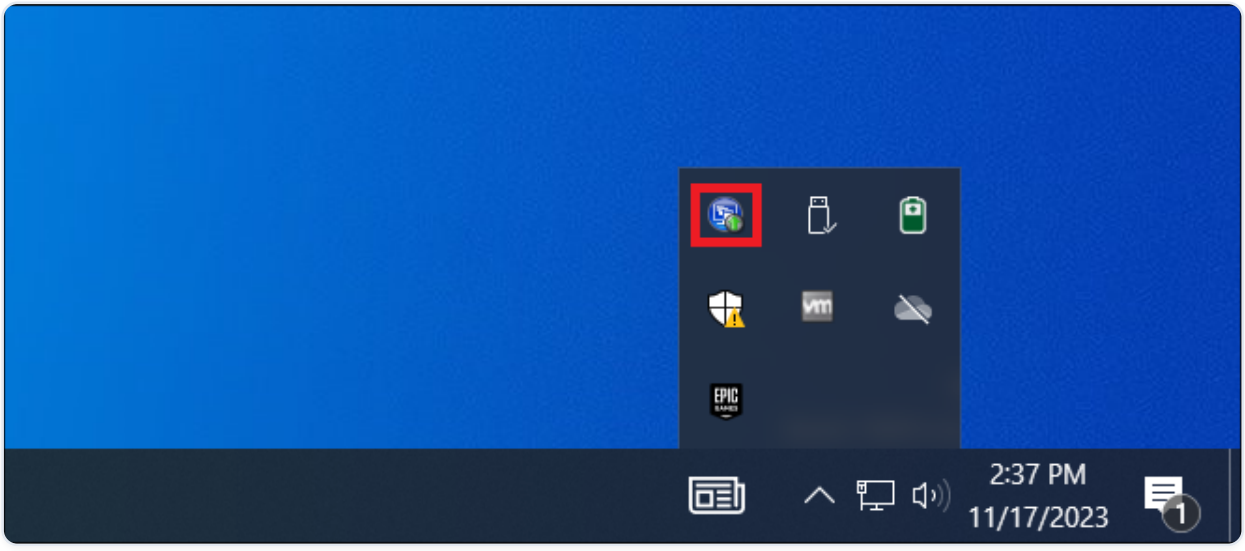
  複雑で高価なワークステーションを、グラフィック処理をデータセンターに移動して一元管理することで、よりシンプルなユーザーデバイスに置き換えることができます。

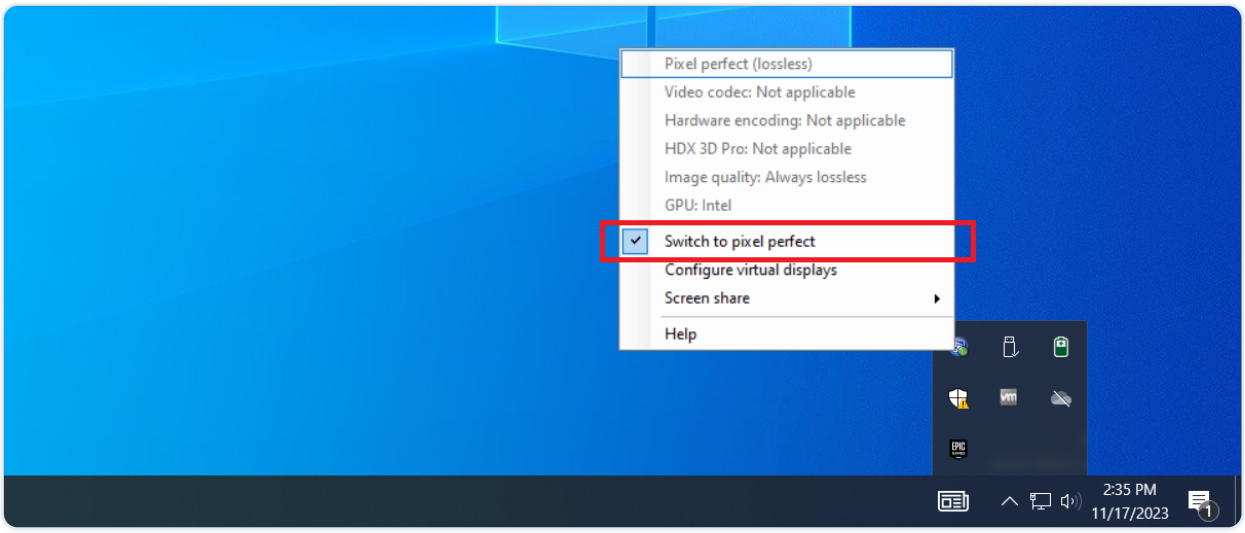
特殊なユースケース向けのロスレス圧縮オプション

HDX 3D Proは、医用画像処理など、ピクセルパーフェクトなグラフィックが必要なアプリケーションをサポートするために、CPUベースのロスレスコーデックも提供します。真のロスレス圧縮は、より多くのネットワークおよび処理リソースを消費するため、特殊なユースケースでのみ推奨されます。

ロスレス圧縮を使用する場合：

- 通知領域アイコンであるグラフィックステータスインジケーターのロスレスインジケーターは、表示されている画面がロッシーフレームかロスレスフレームかをユーザーに通知します。このアイコンは、**視覚品質**ポリシー設定で**ロスレスにビルド**が指定されている場合に役立ちます。送信されるフレームがロスレスの場合、ロスレスインジケーターは緑色に変わります。





- ロスレススイッチを使用すると、ユーザーはセッション中にいつでも**Always Lossless**モードに変更できます。セッション内で**Lossless**を選択または解除するには、アイコンを右クリックして**Switch to pixel perfect**をクリックするか、ショートカットALT+SHIFT+1を使用します。
    - ロスレス圧縮の場合：HDX 3D Proは、ポリシーで選択されたコーデックに関係なく、ロスレスコーデックを圧縮に使用します。
    - ロッシー圧縮の場合：HDX 3D Proは、デフォルトまたはポリシーによって選択された元のコーデックを使用します。 ロススレススイッチの設定は、以降のセッションでは保持されません。すべての接続でロスレスコーデックを使用するには、**視覚品質ポリシー**設定で**常にロスレス**を選択します。

セッション内でロスレスを選択または解除するためのデフォルトのショートカットALT+SHIFT+1を上書きできます。`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HDX3D\LLIndicator`で新しいレジストリ設定を構成します。

- 名前: HKEY_LOCAL_MACHINE_HotKey, 種類: String
- ショートカットの組み合わせを設定する形式は、C=0|1, A=0|1, S=0|1, W=0|1, K=val です。キーはコンマ「,」で区切る必要があります。キーの順序は関係ありません。
- A、C、S、W、Kはキーであり、C=Control、A=ALT、S=SHIFT、W=Win、K=有効なキーです。Kに許可される値は、0〜9、a〜z、および任意の仮想キーコードです。
- 例： F10の場合、K=0x79を設定 Ctrl + F10の場合、C=1, K=0x79を設定 Alt + Aの場合、A=1, K=a または A=1, K=A または K=A, A=1を設定 Ctrl + Alt + 5の場合、C=1, A=1, K=5 または A=1, K=5, C=1を設定 Ctrl + Shift + F5の場合、A=1, S=1, K=0x74を設定

HDX 3D Proのユーザーエクスペリエンスを最適化する

複数のユーザーが帯域幅が制限された接続（たとえば、支社など）を共有している場合、各ユーザーが利用できる帯域幅を制限するために、Overall session bandwidth limitポリシー設定を使用す

ることをお勧めします。この設定を使用すると、ユーザーがログオンおよびログオフする際に、利用可能な帯域幅が大幅に変動することがなくなります。HDX 3D Proは利用可能なすべての帯域幅を使用するように自動的に調整されるため、ユーザーセッション全体で利用可能な帯域幅が大きく変動すると、パフォーマンスに悪影響を及ぼす可能性があります。 たとえば、20人のユーザーが60 Mbpsの接続を共有している場合、各ユーザーが利用できる帯域幅は、同時ユーザー数に応じて3 Mbpsから60 Mbpsの間で変動する可能性があります。このシナリオでユーザーエクスペリエンスを最適化するには、ピーク時にユーザーごとに必要な帯域幅を決定し、常にその量にユーザーを制限してください。 3Dマウスのユーザーの場合、Generic USB Redirection仮想チャネルの優先度を0に引き上げることをお勧めします。仮想チャネルの優先度を変更する方法については、Knowledge Center記事CTX128190を参照してください。 HDX Monitorツールを使用して、HDX視覚化テクノロジーの動作と構成を検証し、HDXの問題を診断およびトラブルシューティングします。このツールは、Citrix Virtual Apps and Desktopsインストールメディアの「**Support**」フォルダーにあります。

GPU アクセラレーション

HDX™ Graphicsは、Virtual Delivery Agent (VDA) とエンドポイントデバイスの両方でGPUハードウェアをシームレスに活用します。

以前はHDX 3D Proとして知られていたこの標準のハードウェアアクセラレーションは、デフォルトで有効になっており、シングルセッションおよびマルチセッションオペレーティングシステムの両方で、グラフィックを多用するDirectXおよびOpenGLアプリケーションのパフォーマンスを大幅に向上させます。

Citrix Virtual Apps and Desktops™ は、Windows マルチセッション OS セッションで実行されるグラフィックを多用するアプリケーションを、サーバーのグラフィック処理ユニット (GPU) でレンダリングすることをサポートします。OpenGL、DirectX、Direct3D、および Windows Presentation Foundation (WPF) のレンダリングをサーバーの GPU に移動することで、サーバーの CPU をより効率的に使用できます。

Windows Serverはマルチユーザーオペレーティングシステムであるため、複数のユーザーがGPU仮想化 (vGPU) の必要なしに、Citrix Virtual Apps™によってアクセスされるGPUを共有できます。

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

GPU 共有

GPU共有により、リモートデスクトップセッションでOpenGLおよびDirectXアプリケーションのGPUハードウェアレンダリングが可能になります。これには次の特性があります。

- アプリケーションのスケーラビリティとパフォーマンスを向上させるために、ベアメタルまたは仮想マシンで使用できます。
- 複数の同時セッションがGPUリソースを共有できるようにします (ほとんどのユーザーは専用GPUのレンダリングパフォーマンスを必要としません)。
- 特別な設定は不要です。

GPUは、ハイパーバイザーおよびGPUベンダーの要件に従って、フルパススルーモードまたは仮想GPU (vGPU) モードのいずれかでWindows Server仮想マシンに割り当てることができます。物理Windows Serverマシンへのベアメタル展開もサポートされています。

GPU共有は特定のグラフィックカードに依存しません。

- 仮想マシンでは、使用中のハイパーバイザーと互換性のあるグラフィックカードを選択してください。XenServerのハードウェア互換性リストについては、Hypervisor Hardware Compatibility Listを参照してください。
- ベアメタルで実行する場合、オペレーティングシステムによって有効化された単一のディスプレイアダプターを使用することをお勧めします。ハードウェアに複数のGPUがインストールされている場合は、デバイスマネージャーを使用して、1つを除くすべてを無効にしてください。

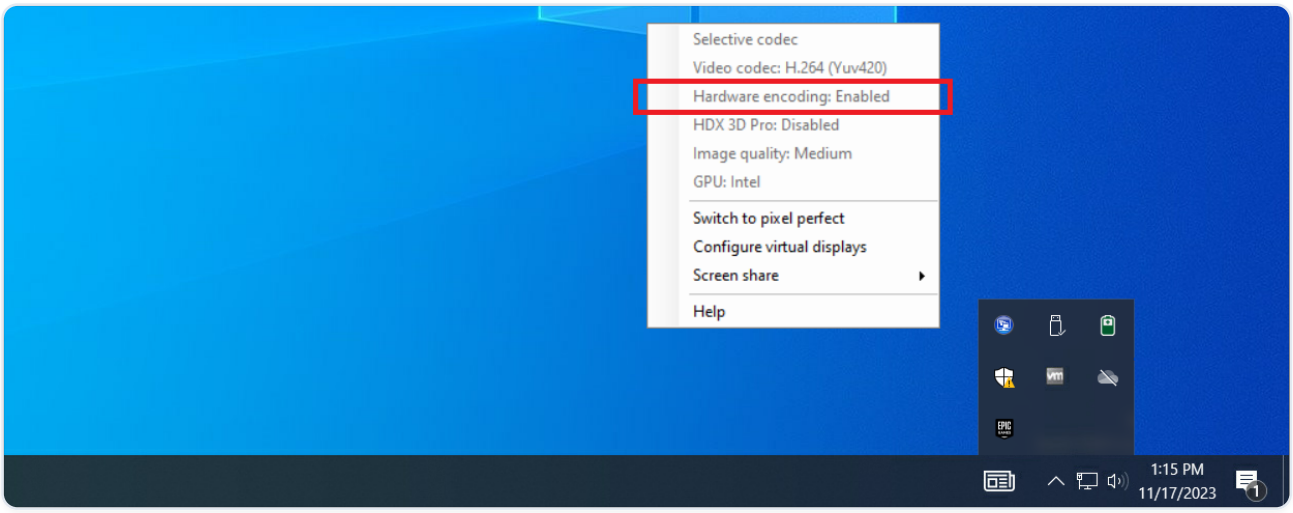
GPU Sharing を使用したスケーラビリティは、いくつかの要因によって異なります。

- 実行されているアプリケーション
- 消費するビデオ RAM の量
- グラフィックカードの処理能力

一部のアプリケーションは、他のアプリケーションよりもビデオ RAM の不足をうまく処理します。ハードウェアが過負荷になると、グラフィックカードドライバーの不安定化やクラッシュが発生する可能性があります。このような問題を回避するには、同時ユーザー数を制限してください。

- NVIDIA GPUおよびIntel Iris Proグラフィックプロセッサ用の高性能ビデオエンコーダーへのアクセス。ポリシー設定（デフォルトで有効）がこの機能を制御し、H.264エンコーディング（利用可能な場合）にハードウェアエンコーディングの使用を許可します。そのようなハードウェアが利用できない場合、VDAはソフトウェアビデオコーデックを使用したCPUベースのエンコーディングにフォールバックします。詳細については、「グラフィックポリシー設定」を参照してください。

GPU アクセラレーションが機能していることを確認するには、グラフィックステータスインジケーターを使用できます。



DirectX、Direct3D、および WPF レンダリング

DirectX、Direct3D、および WPF レンダリングは、ディスプレイドライバーインターフェイス（DDI）バージョン 9ex、10、または 11 をサポートする GPU を搭載したサーバーでのみ利用できます。

- Windows Server 2016以降では、RDセッションホストサーバー上のリモートデスクトップサービス（RDS）セッションは、Microsoft Basic Render Driverをデフォルトのアダプターとして使用します。Windows Server 2016以降のRDSセッションでGPUを使用するには、グループポリシーの**ローカルコンピューターポリシー** \> **コンピューターの構成** \> **管理用テンプレート** \> **Windowsコンポーネント** \> **リモートデスクトップサービス** \> **リモートデスクトップセッションホスト** \> **リモートセッション環境**で、**すべてのリモートデスクトップサービスセッションにハードウェアの既定のグラフィックアダプターを使用する**設定を有効にします。
- WPFアプリケーションがサーバーのGPUを使用してレンダリングできるようにするには、WindowsマルチセッションOSセッションを実行しているサーバーのレジストリに設定を作成します。レジストリ設定の詳細については、レジストリを介して管理される機能のリストにある「Windows Presentation Foundation (WPF) レンダリング」を参照してください。

CUDAまたはOpenCLアプリケーションのGPUアクセラレーション

ユーザーセッションで実行されているCUDAおよびOpenCLアプリケーションのGPUアクセラレーションは、デフォルトで無効になっています。

CUDAアクセラレーション機能を使用するには、レジストリ設定を有効にします。詳細については、レジストリを介して管理される機能のリストにある「CUDAまたはOpenCLアプリケーションのGPUアクセラレーション」を参照してください。

10ビット ハイダイナミックレンジ (HDR)

10ビットハイダイナミックレンジ (HDR) 仮想デスクトップセッションを使用すると、拡張された色域、より高いコントラストと明るさで高品質の画像やビデオをレンダリングするための、強化されたエンコードおよびデコード機能を利用できます。

システム要件

エンドポイント:

- NVIDIA GPU 用の Citrix Workspace™ アプリ for Windows 2209 以降
- エンドポイントで10ビットHEVC (H.265) 444デコードをサポートするNVIDIA GPU
- 10ビットHDR対応モニター。ディスプレイ設定を使用して、すべてのモニターで10ビットHDRを有効にする必要があります。

サーバー:

- NVIDIA GPU 用の Windows シングルセッションOS VDA 2209 以降、および Intel GPU 用の VDA 2308 以降
- VDAで10ビットHEVC 444エンコードをサポートするNVIDIA GPU

必須ポリシー

エンドポイント:

- グラフィックのH.265デコードを有効にする

サーバー:

- 3Dグラフィックワークロード向けに最適化
- グラフィックステータスインジケーター (オプション)

サーバー構成

10ビットHDR対応のエンドポイントモニターでCitrix®セッションを起動すると、HDRセッションがデフォルトで有効になります。マルチモニターHDRセッションでは、すべてのエンドポイントモニターで10ビットHDRが有効になっている必要があります。HDRセッションは、ウィンドウモードと全画面モードの両方でサポートされます。

参照白色レベル

この設定は、ニット値によって白色輝度レベルを定義します。セッション内の相対的なHDR画面の明るさを制御します。デフォルト値は80ニットです。異なるニット値を定義するには、次のレジストリキーを設定します。

- HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics
- 種類: REG_DWORD
- 名前: RefWhiteLevel

設定を有効にするには、セッションのサイズを変更するか、セッションを切断して再起動する必要があります。

EDIDのオーバーライド

VDAをHDRセッションでエンドポイントモニターのEDIDを使用するように構成できます。これにより、色域と輝度範囲を一致させることで、モニターの表示機能を最大限に活用できます。デフォルトでは、HDRセッションはHDR1000対応のディスプレイを想定しています。 エンドポイントモニターのEDIDは、NVIDIAまたはその他のツールを使用してエクスポートできます。次のレジストリキーを使用してVDAに適用します。

- HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics
- 種類: REG_BINARY
- 項目名: EDIDOverride

EDIDをレジストリに保存する際、コンマ、スペース、または特殊文字を含めてはなりません。
オーバーライドEDIDを有効にするには、サインアウトして新しいセッションを起動します。

視覚的にロスレスなエクスペリエンス

視覚的にロスレスなエクスペリエンスを実現するには、次のポリシーを有効にします。

- 視覚的にロスレスな圧縮を許可する
- 視覚品質: 常にロスレスまたはロスレスに構築

ポリシーが設定された後、グラフィックステータスインジケーターを使用して、イメージ品質スライダーを使用するか、ピクセルパーフェクトモードに切り替えることで、HDRセッションの品質を制御できます。

Windowsの画面ロックを許可する

このポリシーを使用すると、画面ロックを含むすべてのWindowsディスプレイタイムアウトを、ワークステーションOS上のCitrix Virtual Desktopセッションに適用できます。この設定は、Citrix StudioのCitrixグループポリシーオブジェクトを使用して設定できます。

デフォルトでは、この設定が有効になっていない場合、アクティブなセッション中にCitrix Virtual Desktopはセッションロック、スクリーンセーバー、またはディスプレイオフのタイムアウトに応答しません。

ワークステーションVDAでパスワード保護されたスクリーンセーバーが構成されている場合、スクリーンセーバーのタイムアウトに達したときにCitrix Virtual Desktopセッションが自動的にロックされるようにするには、この設定を有効にする必要があります。

VDAでディスプレイオフタイムアウトが構成されているときにこの設定を有効にすると、そのタイムアウトの期限切れにより、ユーザーがセッションとの対話を再開するまで更新されないセッションになります。たとえば、表示されている時間は更新されず、新しい通知も表示されません。

その他の考慮事項

- 仮想GPU上で最大4台のモニターで10ビットHDRセッションを起動できます。
- 次の場合、Citrixセッションは8ビットの非HDRモードに戻ります。
    - いずれかのエンドポイントモニターで10ビットHDRが有効になっていない場合
    - 画面共有を有効にする。
    - VDA上で仮想ディスプレイレイアウトを設定する。
    - **視覚的にロスレスな圧縮を許可**ポリシーを設定せずに、ピクセルパーフェクトモードに切り替える。

HDX™ 画面共有

HDX画面共有は、Citrix独自の高性能かつ低遅延の画面共有テクノロジーです。画面共有により、ユーザーはCitrix Virtual Desktopセッションを、画面コンテンツ、キーボード、マウスコントロールを含めて他のユーザーと共有できます。

システム要件

- Windows: シングルセッションまたはマルチセッションOS VDA
- Linux: Linuxセッションの共有に関する詳細については、Linux VDAドキュメントを参照してください。

- 共有できるのはデスクトップセッションのみです。
- セッションをホストするVDAと、共有セッションに接続するマシンとの間にネットワーク接続が必要です。ネットワークポート要件は、使用中のICAポート（TCP/UDP 1494または2598）と画面共有ポリシーの構成（デフォルトでTCP 52525～52625）に基づいています。

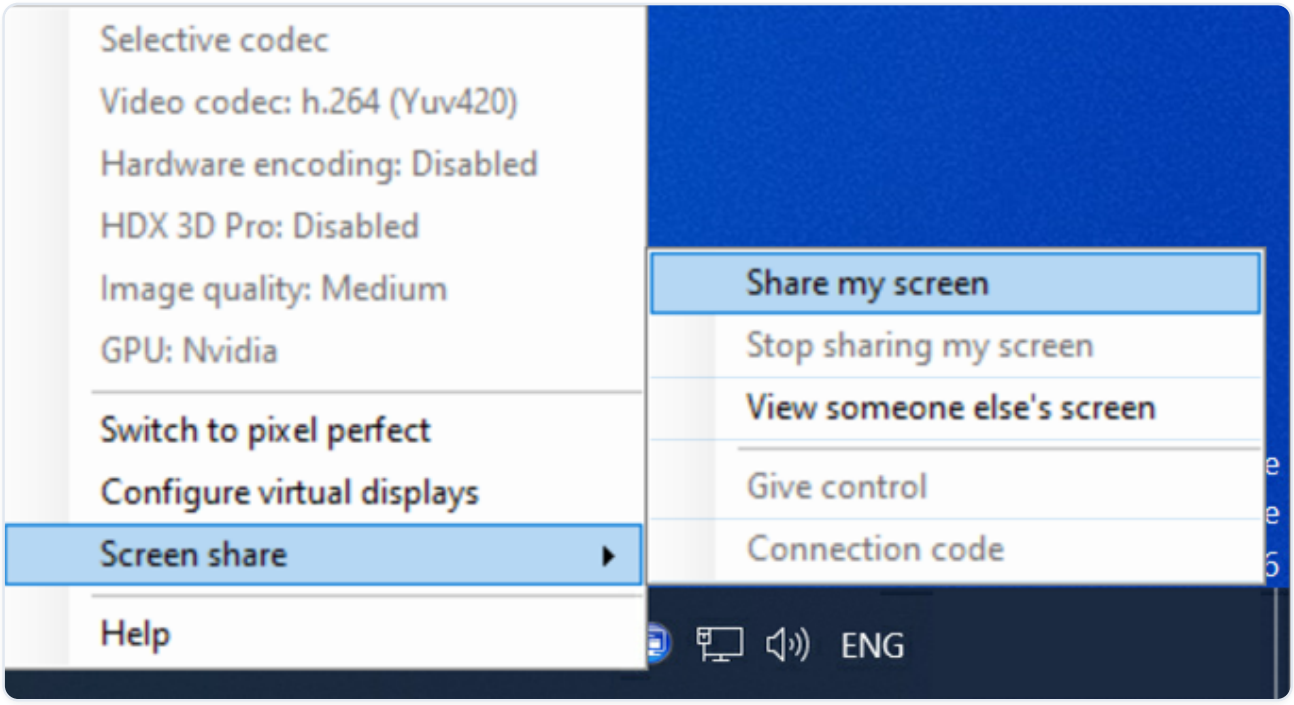
構成

画面共有はCitrixポリシーを使用して有効にする必要があります。画面共有はデフォルトで無効になっています。画面共有ポリシーを構成して、機能を有効または無効にし、使用可能なネットワークポート範囲を割り当てます。

セッションの共有と接続のコントロールを含むユーザーインターフェイスを表示するには、グラフィックステータスインジケーターポリシーを有効にします。

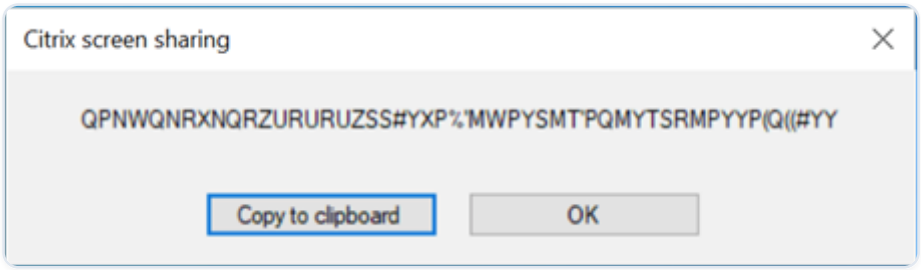
セッションの共有

セッションを共有するには、Windows通知領域にあるHDXグラフィックステータスインジケーターアイコンを探します。それを右クリックしてメニューを表示し、**画面共有 > 画面を共有**を選択します。



クリップボードにコピーをクリックするか、ダイアログボックスに表示されている文字列全体を手動で選択してコピーします。この文字列は、電子メールやIMクライアントなどの任意のアプリケーションに貼り付けて、他のユーザーに配布できます。

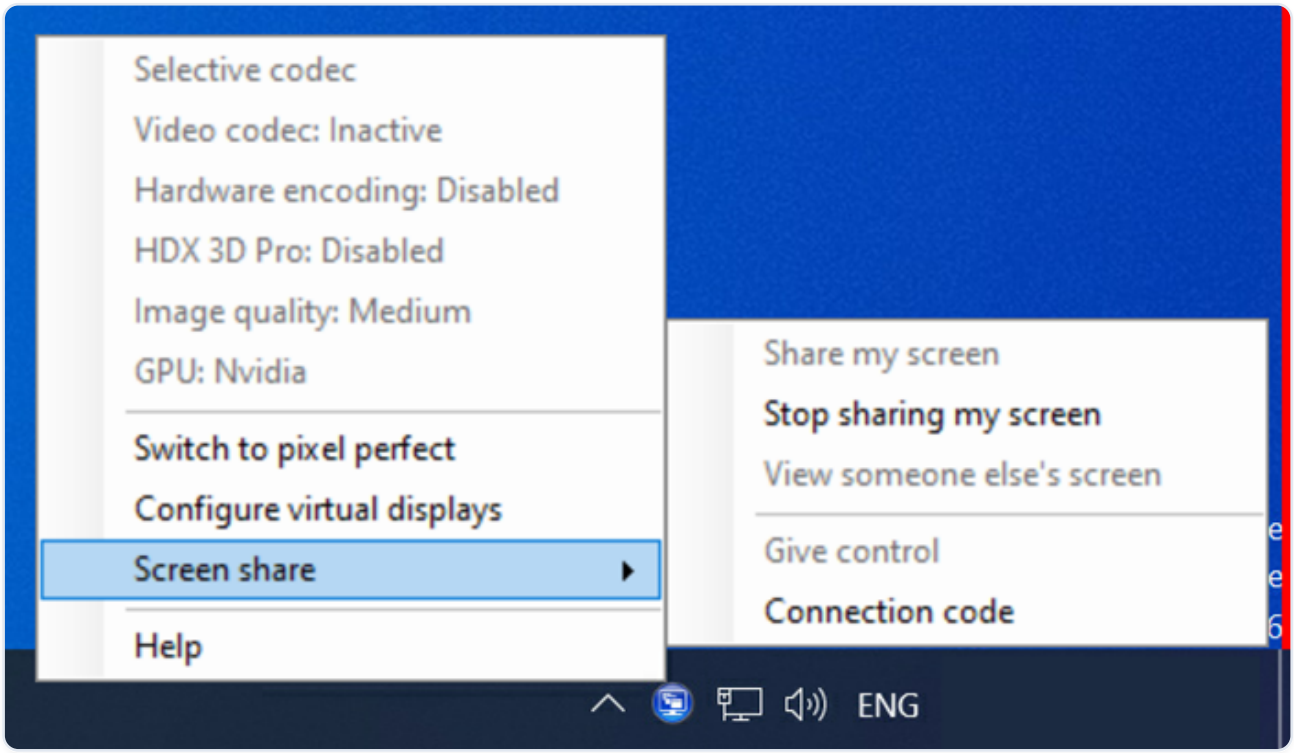
OKまたは**x**をクリックしてダイアログボックスを閉じます。セッションが共有されている間はいつでも、**画面共有 > 接続コード**メニューオプションから接続コードを取得できます。



画面の周囲に赤い枠が表示され、セッションが共有されており、他のユーザーから見えていることを示します。

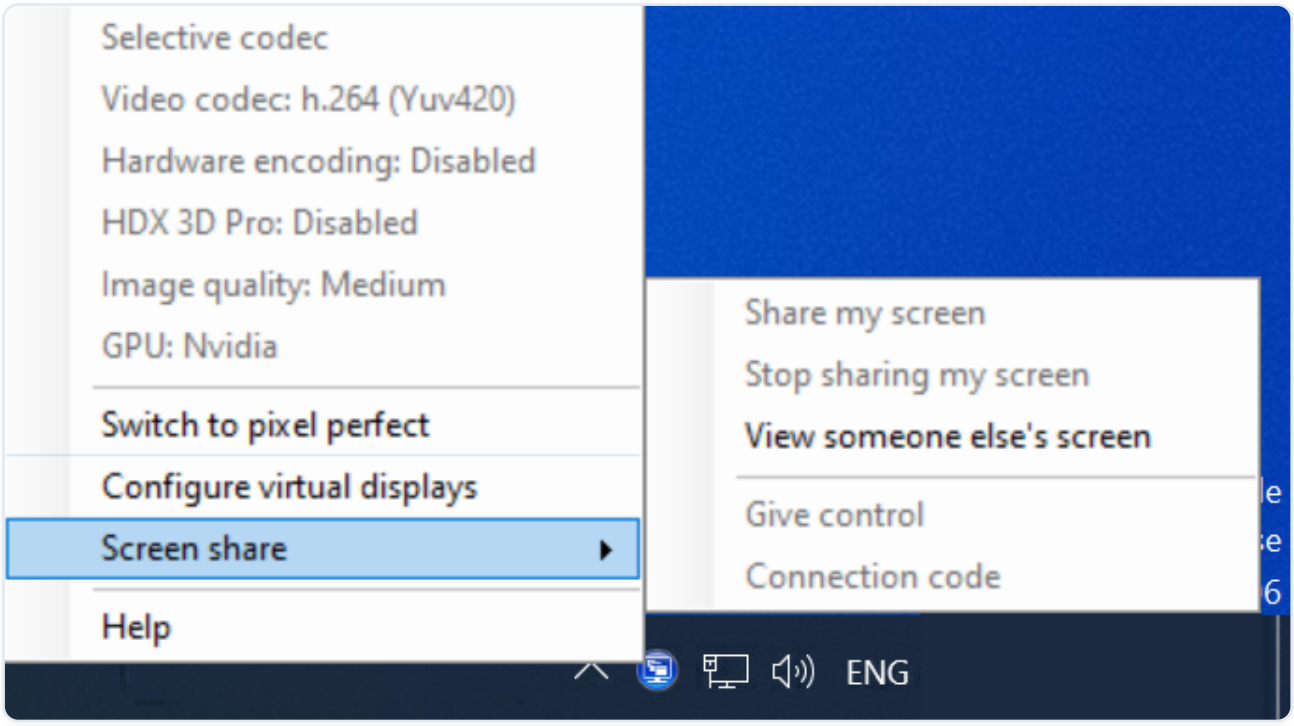
キーボードとマウスのコントロールも、**［画面共有］>［コントロールを付与］**メニューオプションを使用して他のユーザーと共有できます。

［画面共有］>［画面共有を停止］メニューオプションを使用して、セッションの共有を停止し、すべてのユーザーを切断します。

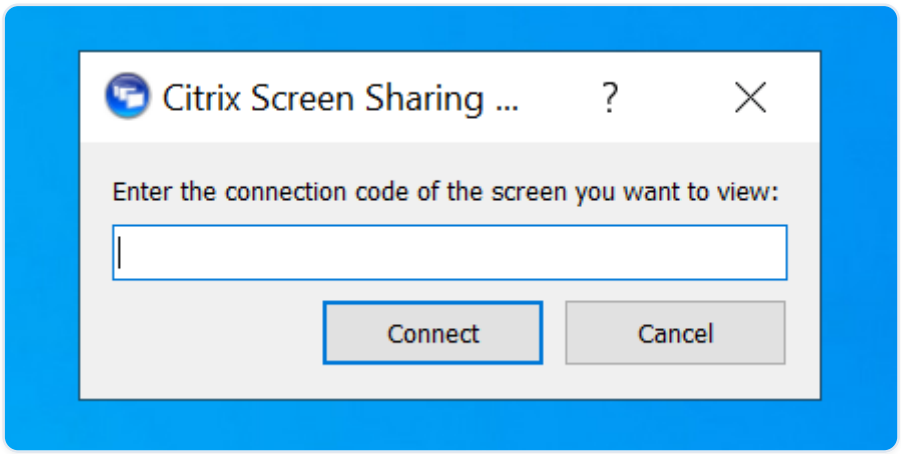


共有セッションへの接続

他のユーザーのセッションに接続するには、Windows の通知領域にある HDX グラフィックステータスインジケーターアイコンを探します。それを右クリックしてメニューを表示し、**画面共有 > 他のユーザーの画面を表示**を選択します。

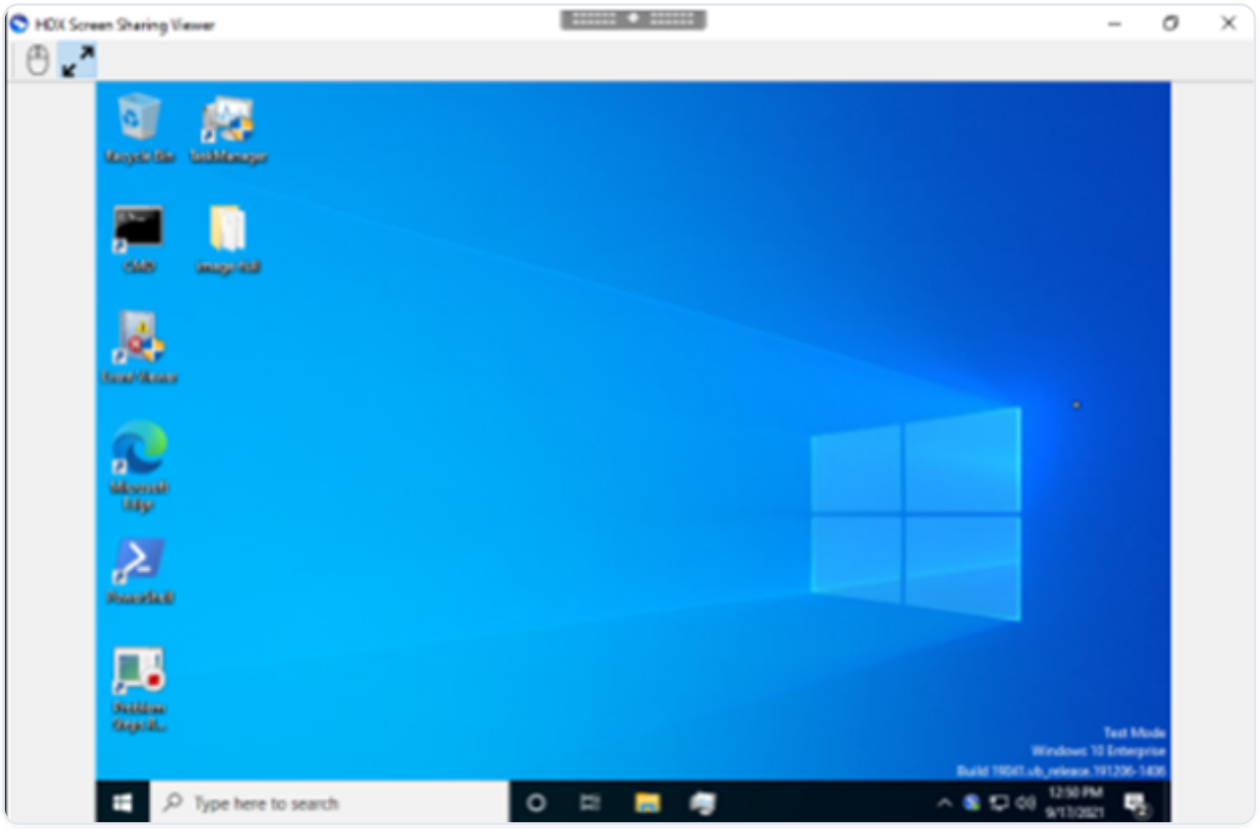


セッションを共有しているユーザーから提供された接続文字列をテキストボックスに入力または貼り付けます。**接続**をクリックして接続を確立します。



HDX 画面共有ビューアウィンドウの左上隅にあるマウスアイコンをクリックすると、キーボードとマウスの制御を要求できます。

共有セッションからいつでも切断するには、**HDX 画面共有ビューア**ウィンドウを閉じます。



その他の考慮事項

- 画面共有ビューアアプリケーションは、VDA に *C:\Program Files\Citrix\HDX\bin\TwPlayer.exe* として含まれており、Virtual Apps Server を使用して公開アプリケーションとして展開される場合があります。この代替展開モデルにより、仮想デスクトップにアクセスできないユーザーとのコラボレーションが可能になります。
- 共有セッションに接続できるユーザー数は、画面共有ポリシーのネットワークポート範囲を使用して制限できます。ユーザーごとに1つのポートが必要です。デフォルトの範囲では、最大100人のユーザーが許可されます。
- セッションに接続されているすべてのモニターが共有されます。個々のモニターを選択することはできません。
- H.265 ビデオコーデックはサポートされていません。

セッションベースのウォーターマーク

テキストベースのセッションウォーターマークは、データ盗難を抑止し、追跡を可能にするのに役立ちます。この追跡可能な情報は、写真やスクリーンショットを使用してデータを盗む者への抑止力として、セッションデスクトップに表示されます。テキストのレイヤーであるウォーターマークを指定できます。

ウォーターマークは、元のドキュメントの内容を変更することなく、セッション画面全体に表示できます。テキストベースのセッションウォーターマークには、VDAのサポートが必要です。

> **重要:**
>
> テキストベースのセッションウォーターマークは、セキュリティ機能ではありません。このソリューションはデータ盗難を完全に防ぐものではありませんが、ある程度の抑止力と追跡可能性を提供します。この機能を使用した場合の完全な情報追跡可能性は保証しませんが、必要に応じて他のセキュリティソリューションと組み合わせて使用することをお勧めします。

> セッションウォーターマークはテキストであり、ユーザーに配信されるセッションに適用されます。セッションウォーターマークには、データ盗難を追跡するための情報が含まれています。最も重要なデータは、スクリーンイメージが取得された現在のセッションのログオンユーザーのIDです。データ漏洩をより効果的に追跡するために、サーバーまたはクライアントのインターネットプロトコルアドレスや接続時間などの他の情報を含めることをお勧めします。

ユーザーエクスペリエンスを調整するには、セッションウォーターマークポリシー設定 を使用して、画面上の配置とウォーターマークの外観を構成します。

要件:

仮想配信エージェント:

マルチセッションOS 7.17 シングルセッションOS 7.17

制限事項:

- ローカルアプリアクセス、Windowsメディアリダイレクト、MediaStream、ブラウザコンテンツリダイレクト、およびHTML5ビデオのリダイレクトが使用されているセッションでは、セッションウォーターマークはサポートされていません。セッションウォーターマークを使用するには、これらの機能が無効になっていることを確認してください。
- セッションが全画面ハードウェアアクセラレーションモード（全画面H.264またはH.265エンコーディング）で実行されている場合、セッションウォーターマークはサポートされず、表示されません。
- これらのHDX™ポリシーを設定すると、ウォーターマーク設定は有効にならず、セッションディスプレイにウォーターマークは表示されません。

ビデオコーデックにハードウェアエンコーディングを使用 を **有効 圧縮にビデオコーデックを使用** に、**画面全体** に

- これらのHDXポリシーを設定した場合、動作は未定義であり、ウォーターマークが表示されない可能性があります。

  ビデオコーデックにハードウェアエンコードを使用する を **有効 圧縮にビデオコーデックを使用する** に、**優先される場合にビデオコーデックを使用する** に設定します。

  ウォーターマークが表示されるようにするには、**ビデオコーデックにハードウェアエンコードを使用する** を **無効** に設定するか、**圧縮にビデオコーデックを使用する** を **アクティブに変化する領域の場合** または **ビデオコーデックを使用しない** に設定します。
- セッションウォーターマークは、Thinwireグラフィックモードのみをサポートします。
- セッションレコーディングを使用している場合、記録されたセッションにはウォーターマークは含まれません。
- Windowsリモートアシスタンスを使用している場合、ウォーターマークは表示されません。
- ユーザーが画面をキャプチャするために **Print Screen** キーを押した場合、VDA側でキャプチャされた画面にはウォーターマークは含まれません。キャプチャされた画像がコピーされるのを防ぐための対策を講じることをお勧めします。

Thinwire

Thinwire の構成

Thinwire は、その構成に応じてさまざまなグラフィックエンコードモードで動作できます。Thinwire の主な構成ポリシーは、「圧縮にビデオコーデックを使用する」ポリシーです。

- 優先する場合に使用する（デフォルト）
- 頻繁に変化する領域の場合
- 画面全体の場合
- ビデオコーデックを使用しない

以下のセクションでは、各モードについて詳しく説明します。

圧縮設定にビデオコーデックを使用する	テキスト	画像	動画像とビデオ	ユースケース
優先する場合に使用する（GPU）	ロスレス	JPEG	インテリジェントビルドからロスレス / ビデオコーデック*	グラフィックを多用するアプリケーションを含む、ほとんどのワークロードのデフォルト
推奨される場合に使用（GPUなし）	ロスレス	JPEG	ビデオコーデック	ほとんどのワークロードのデフォルト
頻繁に変化する領域向け	ロスレス	JPEG	ビデオコーデック	
画面全体向け	ビデオコーデック	ビデオコーデック	ビデオコーデック	ビルドトゥロスレスが推奨されない、ゲームなどのグラフィックを多用するアプリケーション
ビデオコーデックを使用しない	ロスレス	JPEG	アダプティブJPEG	セッションの対話性よりも画質が優先される場合。GPU使用率が最小限に抑えられるため、最高の拡張性。

*特定の条件が満たされた場合にのみ、インテリジェントビルドトゥロスレスが使用されます。

ほとんどのユースケースでは、Thinwire の設定をデフォルトのままにしておくことで、最高のパフォーマンスと表示品質が得られます。

さまざまなユースケースの詳細については、Techzone ドキュメントの HDX Graphics の設計上の決定事項 を参照してください。

Thinwire フルスクリーンエンコーダー

概要

Citrix Virtual Apps and Desktops™ 2503 以降のリリースに伴い、「3Dグラフィックワークロード向けに最適化」ポリシーは非推奨となり、削除されました。

このポリシーはフルスクリーンエンコーダーに置き換えられ、特定のグラフィック負荷の高いワークロード向けに機能が強化され、ユーザーエクスペリエンスが向上しました。

フルスクリーンエンコーダーは、「圧縮にビデオコーデックを使用」ポリシーを「画面全体」に設定することで構成できます。

フルスクリーンエンコーダーは構成を簡素化し、グラフィック負荷の高いワークロードに対して堅牢なパフォーマンスを提供します。画面分析や帯域幅の最適化を一切行わず、画面全体がビデオコーデックを使用してエンコードされることを保証し、フレームレートとインタラクティブ性を最大化します。

このモードは、一貫したグラフィック忠実度が最重要である3Dアプリケーションやワークロードに特に適しています。

フルスクリーンエンコーダーの主な利点は、YUV444カラースペースを活用できることです。さらに、フルスクリーンエンコーディングは、セレクティブエンコーダーと比較して、最大120フレーム/秒 (FPS) の可能な限り最高のフレームレートを提供できますが、その結果、より多くの帯域幅とリソースを使用します。

フルスクリーンエンコーダーを使用する場合

グラフィックを多用するアプリケーションの場合、フルスクリーンエンコーダーを試す前にロスレスビルドを検討する必要があります。ロスレスビルドは、視覚的品質ポリシーを「ロスレスビルド」に設定し、「圧縮にビデオコーデックを使用」ポリシーをデフォルト設定の「優先する場合に使用」のままにしておくことで設定できます。

The Full Screen Encoder is only recommended if higher moving image quality is required as it supports the YUV444 color space (see “Allow Visually Lossless” policy). Video Editing is a good example of where this extra fidelity might be required, however, this will come at a considerably higher bandwidth cost.

構成

フルスクリーンエンコーダーを有効にするには:

1. Citrix Studioでグラフィックポリシー設定に移動します。

2. 「圧縮にビデオコーデックを使用する」ポリシーを見つけます。
3. ポリシーを「画面全体」に設定します。
4. ポリシーの変更を適用し、デリバリーグループに伝播します。

コーデックの動作と構成に関する追加の詳細については、自動ビデオコーデック構成ドキュメントを参照してください。

グラフィックエンコーダー(/en-us/citrix-virtual-apps-desktops/2503/media/policy-for-the-entire-screen.png)

監視

フルスクリーンエンコーダーを監視するには、セッション内でグラフィックスステータスインジケーターを使用できます。現在、グラフィックスステータスインジケーターはデフォルトでは有効になっていません。

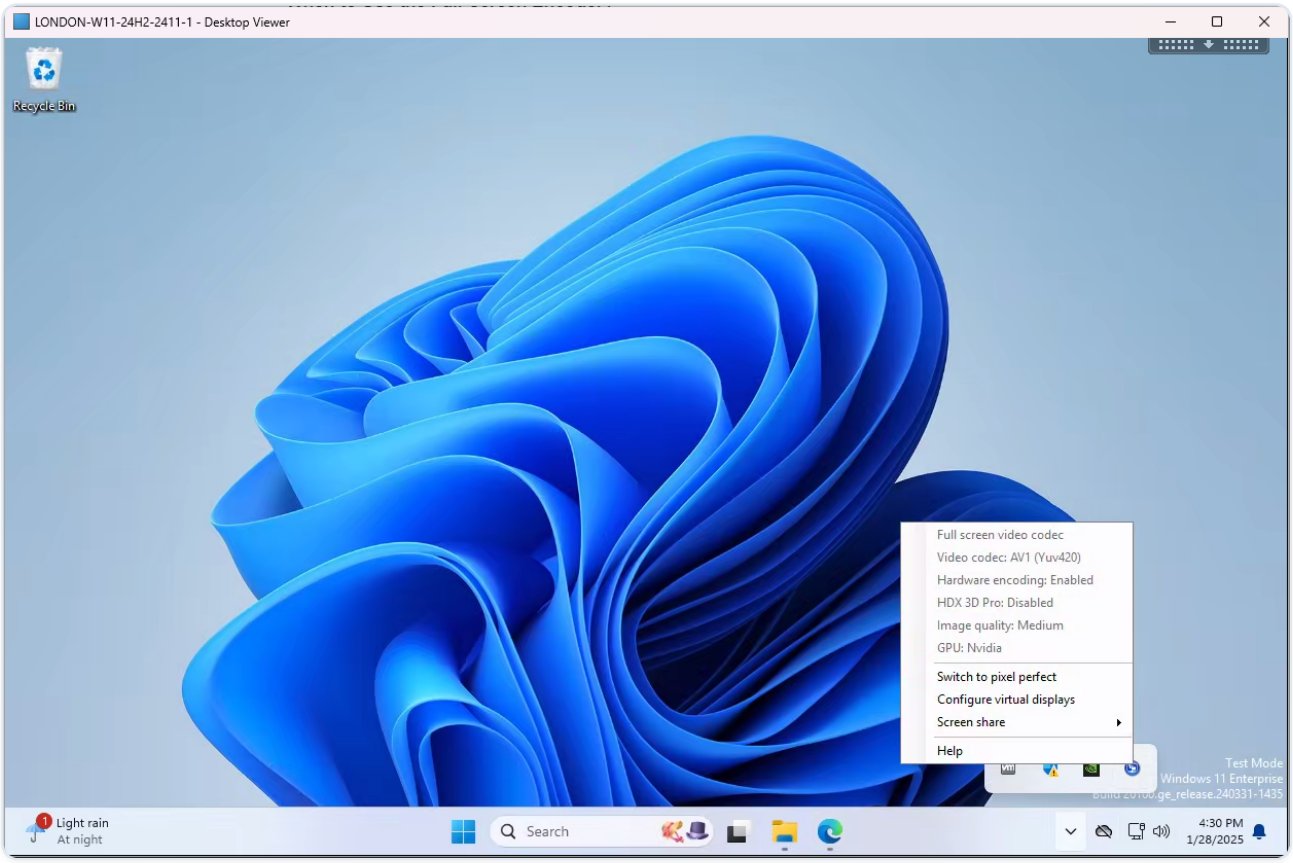
グラフィックスステータスインジケーターを有効にするには：

1. Citrix Studioでグラフィックポリシー設定に移動します。
2. 「グラフィックスステータスインジケーター」ポリシーを見つけます。
3. ポリシーを「有効」に設定します。
4. ポリシーの変更を適用し、デリバリーグループに伝播します。

グラフィックスエンコーダー(/en-us/citrix-virtual-apps-desktops/2503/media/policy-enable-gsi.png)

グラフィックスステータスインジケーターは、リモートセッションのタスクトレイで利用可能になります。

フルスクリーンエンコーダーを使用している場合、グラフィックスステータスインジケーターには以下が表示されます。



非推奨のポリシー - 3Dグラフィックワークロードの最適化

以前は、「3Dグラフィックワークロード向けに最適化」ポリシーは、フルスクリーンエンコーダーと同様の機能を提供していました。しかし、このポリシーには高度な機能がありませんでした。

このポリシーを削除することで、構成が簡素化され、さまざまなワークロードと環境においてパフォーマンスの一貫性が確保されます。

Thinwire 選択的エンコーダー

選択的エンコーディングは、Thinwireのデフォルトの動作モードです。このモードでは、Thinwireは画面コンテンツをリアルタイムで分析し、最適な視覚品質、セッション忠実度、および帯域幅使用量のために、画面の各部分をエンコードする最良の方法を選択します。

選択的エンコーディングでは、以下が使用されます。

- テキスト: ロスレスエンコーディング
- シンプルな画像と単色: ロスレスエンコーディング
- 複雑な/写真のような画像: JPEGエンコーディング
- 一時的なコンテンツと動画: ビデオコーデック、YUV 4:2:0カラーモードのH.264 / H.265 / AV1。

選択的エンコーディングには、以下の特徴があります。

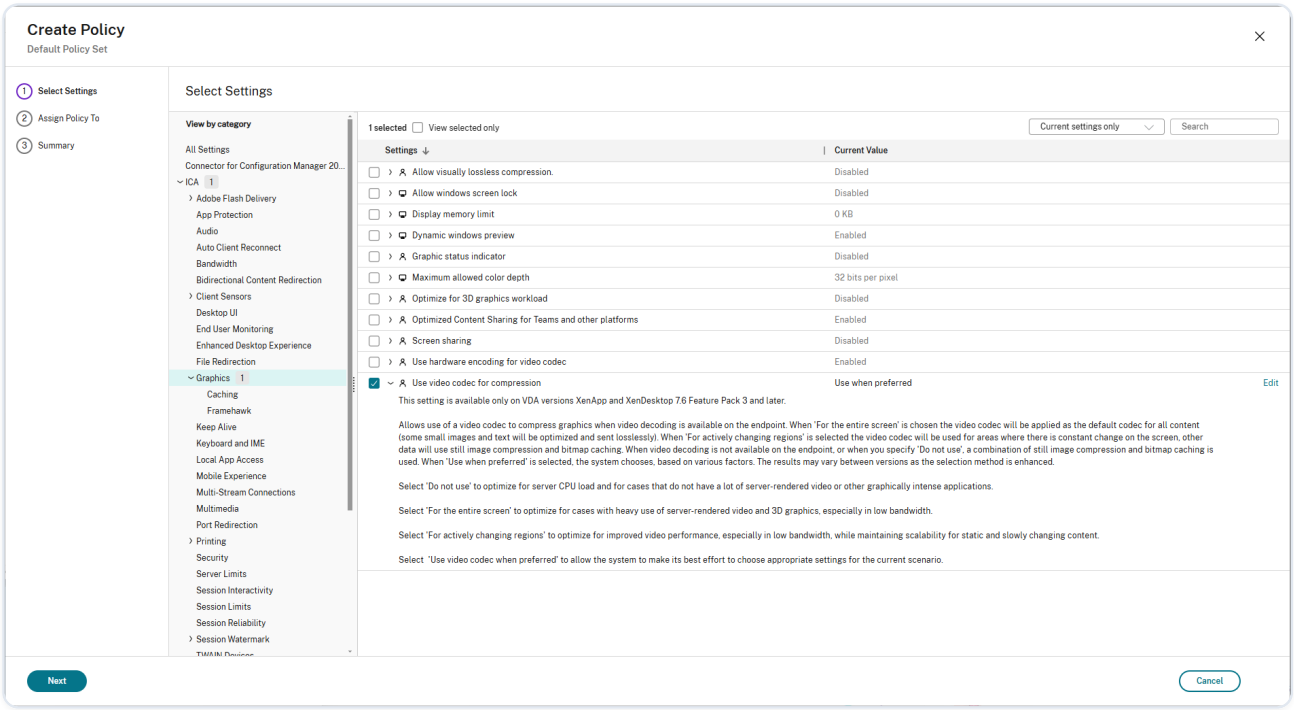
- アダプティブディスプレイ: Thinwireのアダプティブディスプレイテクノロジーは、動画（ビデオ、移動中の3D）を識別し、画像が移動している画面の部分でビデオコーデックを使用します。
- インテリジェントビルドトゥロスレス: GPUが存在する場合、インテリジェントビルドトゥロスレスを使用して、動きが検出されたときに最高のセッションインタラクティビティを提供し、動きが停止した後はピクセルパーフェクトな画像を保証できます。Thinwireは、応答時間監視や画面アクティビティなど、いくつかの要因に基づいて、モニターごとにインテリジェントビルドトゥロスレスを自動的に有効にします。
- ハードウェアアクセラレーション: Virtual Delivery Agent (VDA) にGPUが存在する場合、フルスクリーンエンコーダーはGPUを活用してハードウェアアクセラレーションによるエンコーディングを行い、CPU使用率を削減し、パフォーマンスを向上させます。
- 自動ビデオコーデック選択: 使用されるビデオコーデックは、VDAとクライアントの機能に基づいて動的に選択されます。サポートされるコーデックは次のとおりです。
  - AV1: その効率性と高品質な圧縮により推奨されます。
  - H.265 (HEVC): AV1をサポートしないシステムの場合のフォールバックとして使用されます。
  - H.264 (AVC): レガシーまたは低機能のシナリオ、またはVDAにGPUが存在しない場合に使用されます。

構成

選択的エンコードはデフォルトの動作モードであるため、追加の構成は不要です。デフォルトでは、サーバー側GPUが利用可能な場合、選択的エンコードはIntelligent Build to Losslessを使用します。

選択的エンコーディングを明示的に設定するには：

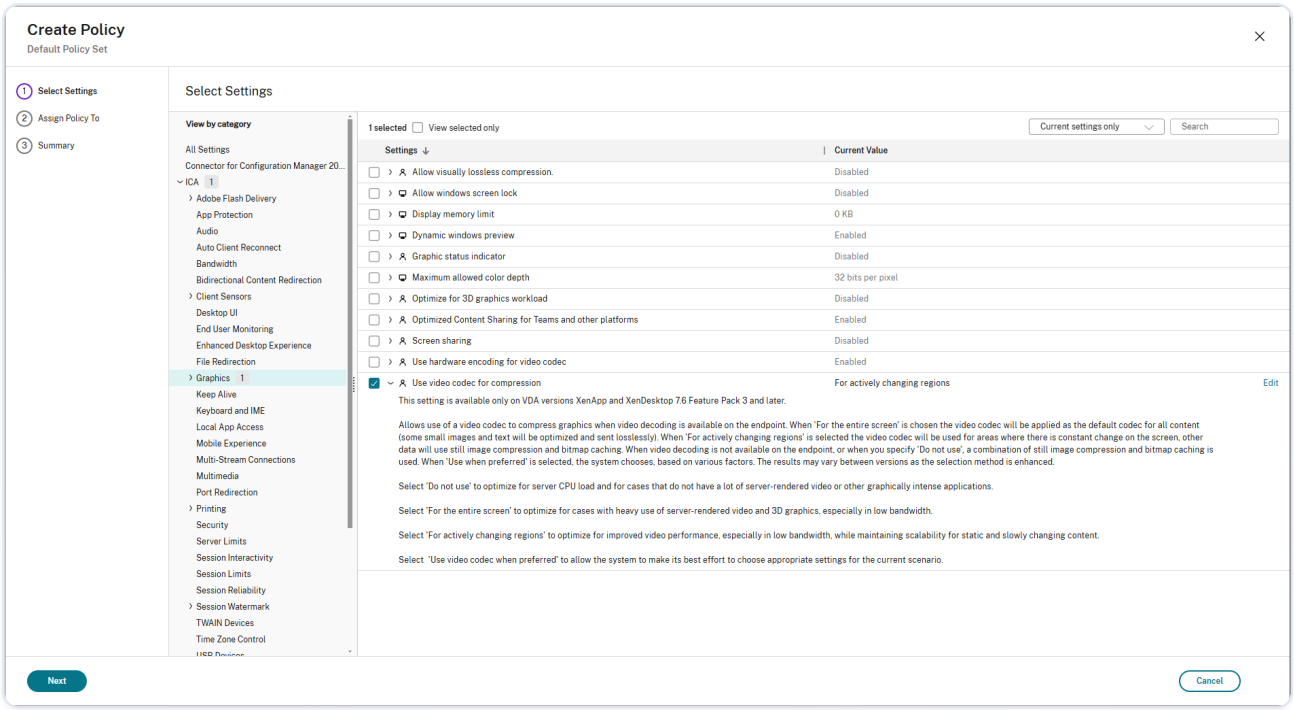
1. Citrix Studioでグラフィックポリシー設定に移動します。
2. 「ビデオコーデックを圧縮に使用する」ポリシーを見つけます。
3. ポリシーを「優先時に使用」に設定します。
4. ポリシーの変更を適用し、デリバリーグループに伝播します。



Intelligent Build to Losslessは、Citrix Virtual Apps and Desktops™バージョン2503で導入されました。2503より前のCVADバージョンでは、選択的エンコードはIntelligent Build to Losslessなしで機能します。

GPUを搭載したVDAでIntelligent Build to Losslessなしで選択的エンコードを使用するには（2503より前のバージョンのレガシー動作を設定するため）：

1. Citrix Studioでグラフィックポリシー設定に移動します。
2. 「ビデオコーデックを圧縮に使用する」ポリシーを見つけます。
3. ポリシーを「アクティブに変更される領域の場合」に設定します。
4. ポリシーの変更を適用し、デリバリーグループに伝播します。



2503より前のバージョンでは、「use when preferred」と「for actively changing regions」は同じでした。2503では、「use when preferred」のデフォルト設定に、GPUが利用可能な場合の「Intelligent Build to lossless」が含まれます。GPUがない場合、「use when preferred」は「for actively changing regions」と同じです。

インテリジェントビルドツーロスレス

インテリジェントビルドトゥロスレスの監視

インテリジェントビルドトゥロスレスは、Citrix®セッション内からグラフィックステータスインジケーターで監視できます。現在、グラフィックステータスインジケーターはデフォルトでは有効になっていません。

グラフィックステータスインジケーターを有効にするには：

1. Citrix Studioでグラフィックポリシー設定に移動します。
2. 「グラフィックステータスインジケーター」ポリシーを見つけます。
3. ポリシーを「有効」に設定します。
4. ポリシーの変更を適用し、デリバリーグループに伝播します。

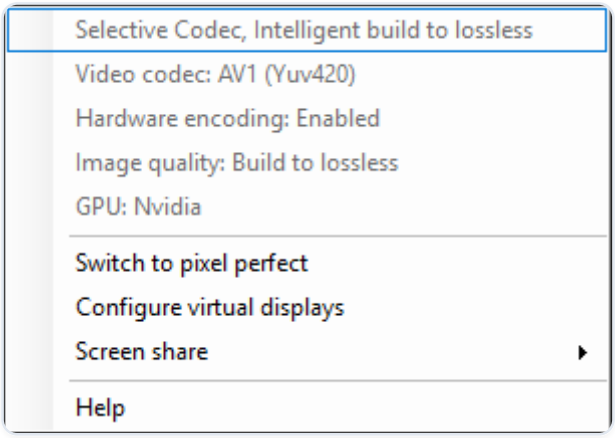
グラフィックステータスインジケーターは、リモートセッションのタスクトレイで利用できます。

インテリジェントビルドトゥロスレスが利用可能な場合、グラフィックステータスインジケーターの最初の行に「Selective Codec, Intelligent Build To Lossless」と表示されます。~~~~

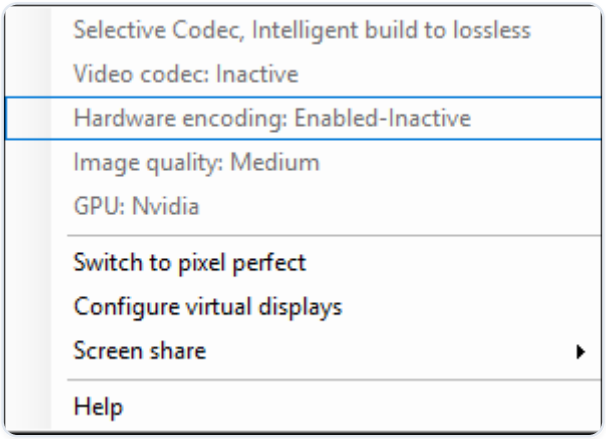
注:

「圧縮にビデオコーデックを使用する」がデフォルトのままか、明示的に「優先する場合に使用する」に設定されており、かつGPUでGPUが利用可能な場合、インテリジェントビルドトゥロスレスは自動的に利用可能になります。

インテリジェントビルドトゥロスレスが利用可能であっても、まだアクティブでない場合、セッションは通常の選択モードを使用し、グラフィックステータスインジケーターは画質を「中」（または視覚品質ポリシーで設定された低、高）と表示します。



Thinwireが現在の画面アクティビティに基づいて1つ以上のモニターでインテリジェントビルドトゥロスレスを有効にするのに好ましい条件を検出すると、グラフィックステータスインジケーターも画質（4行目）がインテリジェントビルドトゥロスレスに変更されることを示します。



Intelligent Build to Losslessのより詳細なテストと監視のために、どのモニターがBuild to Losslessモードであるかを示すモニターごとの視覚的インジケーターを有効にすることもできます。

この設定は、テストとトラブルシューティングのみを目的としており、本番環境では使用しないでください。Intelligent Build to Lossless visual indicator を有効にするには、以下のKB記事を参照してください。

ビデオコーデックは使用しないでください

リモートセッションのエンコードにビデオコーデックを使用することには、いくつかの利点があります。高速で比較的軽量です。ビデオコーデックは、リモートセッションでよくあるように、動画の処理に優れており、そのために設計されています。

しかし、画質や色精度が最優先される場合など、ビデオコーデックの使用が最適なソリューションではないシナリオもあります。当社の選択的エンコーダーは、ほとんどの場合、画面のどの部分がビデオコーデックによるエンコードの恩恵を受けるかを判断するのに非常に優れた仕事をしますが、Thinwireに画面圧縮のためにビデオコーデックを一切使用しないように強制することもできます。

Thinwireがビデオコーデックを使用しないように設定されている場合、Thinwireは圧縮にJPEGとロスレスRLEのみを使用し、可能な限り最高の画質を維持します。Thinwireは、選択的エンコードまたは全画面エンコードを使用する場合よりも、かなり多くの帯域幅を使用します。

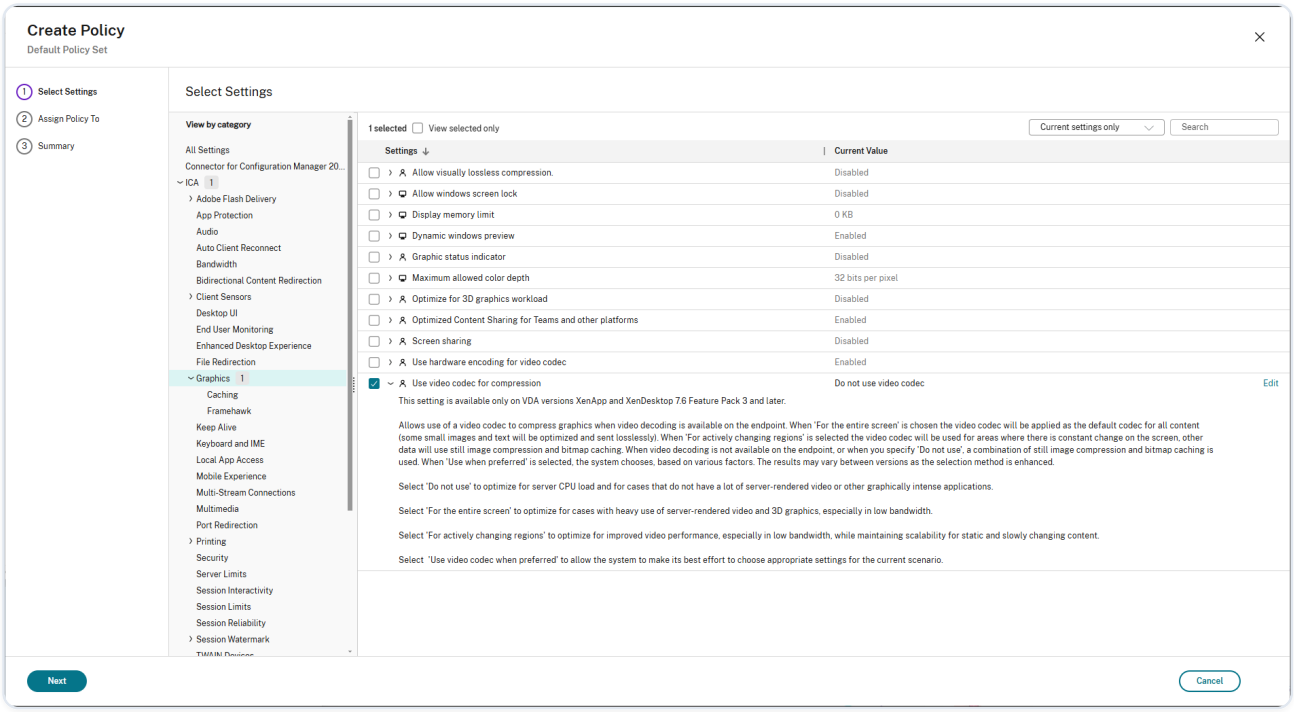
ビデオコーデックを使用しない場合の利用方法

画質とVDAのスケーラビリティが最も重要な要素となるシナリオでは、当社のThinwireフルスクリーンエンコーダーモードの使用を検討できます。ビデオコーデックを使用しないことで、一般的に圧縮にビデオコーデックを使用する場合よりもCPUオーバーヘッドが低いため、VDAのスケーラビリティを最大化できます。

しかし、これらのほとんどのケースでは、当社の選択的エンコーダーは、特にBuild to losslessまたはintelligent build to losslessと組み合わせた場合、ビデオコーデック圧縮を使用しない場合よりも、同じ品質、より優れたパフォーマンス、およびより低い帯域幅を提供します。

構成

Thinwireポリシー「圧縮にビデオコーデックを使用する」を「ビデオコーデックを使用しない」に設定します。



常にロスレスモード

常にロスレスモードを使用すると、イメージの非可逆データがクライアントに送信されることがなくなります。つまり、すべてのフレームは非可逆コーデックでのみエンコードされ、品質はピクセルパーフェクトになります。

常にロスレスの圧縮率は、他のモードを使用する場合ほど良くなく、常にロスレスモードを設定すると、かなりの帯域幅が使用されます。これにより、十分な帯域幅がない場合にインタラクティブ性に大きな影響を与える可能性があります。

Citrix®は、医用画像処理のユースケースなど、ロスレスの画質が必要な特定のユースケースでのみ、この設定の使用を推奨しています。

常にロスレス(/en-us/citrix-virtual-apps-desktops/2503/media/policy-visualquality-alwayslossless.png)

Always Losslessモードを明示的に設定するだけでなく、エンドユーザーは、グラフィックスステータスインジケーターが利用可能な場合、セッション内でロスレスモードを切り替えることもできます。

現在、グラフィックスステータスインジケーターはデフォルトでは有効になっていません。

グラフィックステータスインジケーターを有効にするには：

1. Citrix Studioでグラフィックポリシー設定に移動します。
2. 「グラフィックスステータスインジケーター」ポリシーを見つけます。

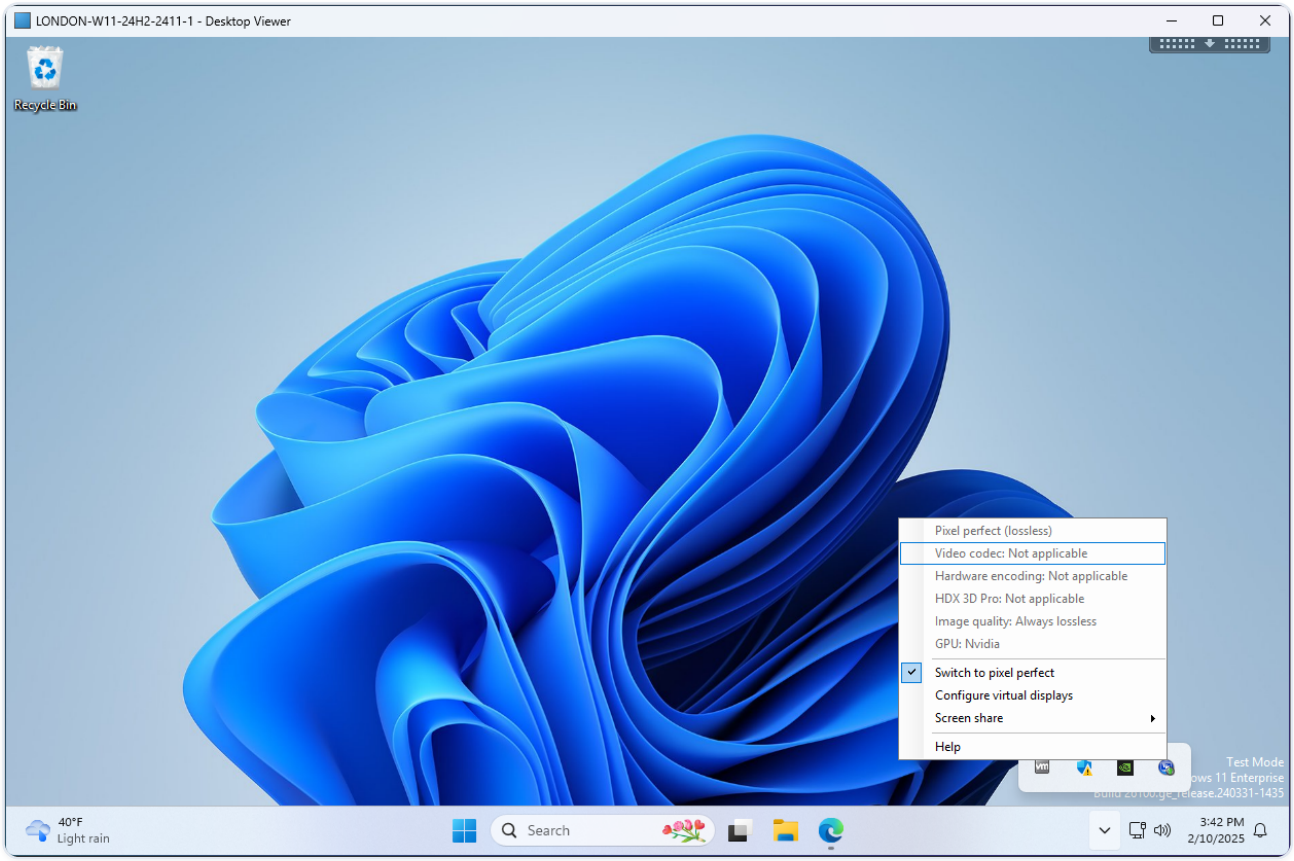
3. ポリシーを「有効」に設定します。
4. ポリシーの変更を適用し、デリバリーグループに伝播します。

GSIを有効にする(/en-us/citrix-virtual-apps-desktops/2503/media/policy-enable-gsi.png)

エンドユーザーとしてAlways Losslessモードを切り替えるには：

1. タスクトレイにあるグラフィックスステータスインジケーターを見つけます。
2. VDAのタスクトレイにあるグラフィックスステータス 1. 1. インジケーターを右クリックします。
3. 「Switch to Pixel Perfect」を選択します。

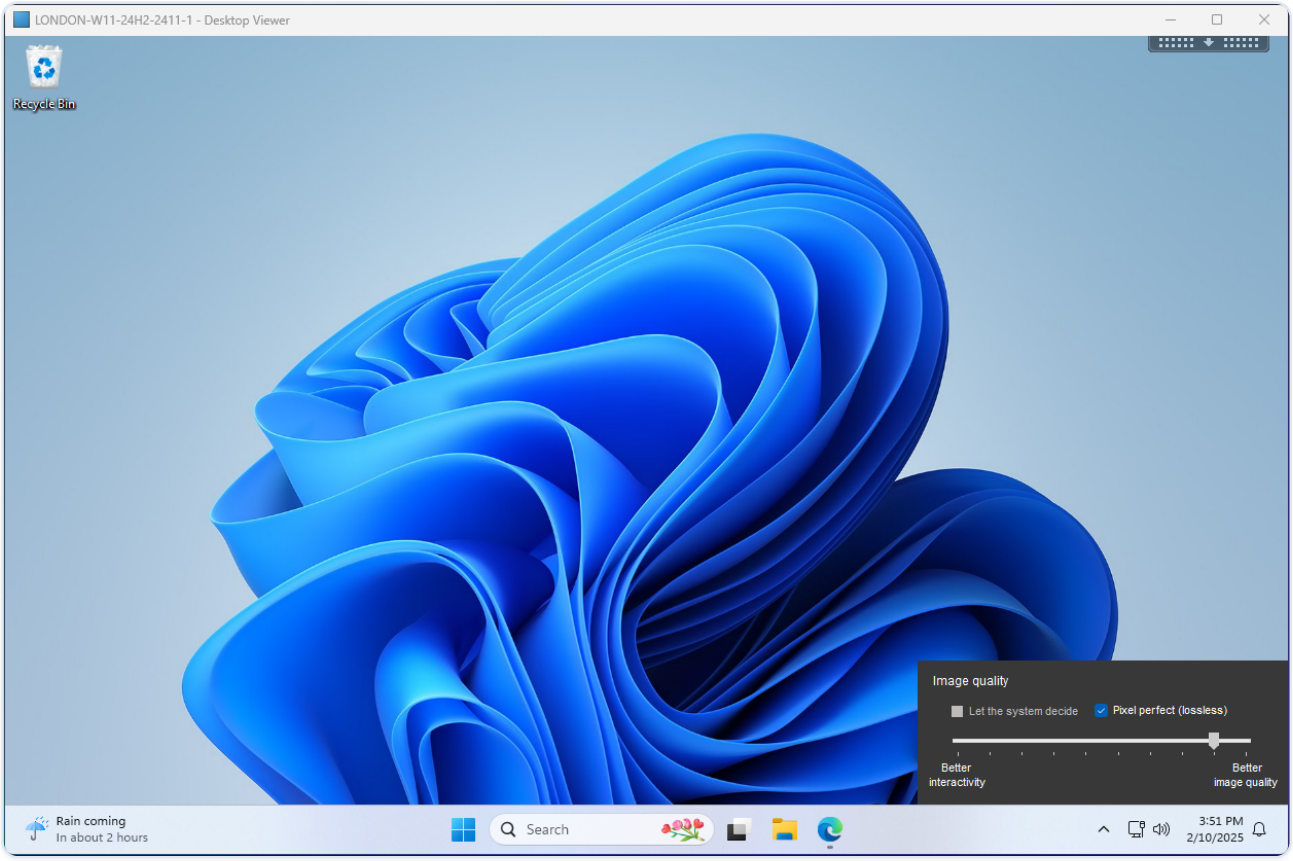
グラフィックスステータスインジケーターのアイコンが緑色になり、ロスレスモードが有効になっていることを示します。



または、：

1. タスクトレイでグラフィックスステータスインジケーターを見つけます。
2. VDAのタスクトレイにあるグラフィックスステータスインジケーターをクリックします。
3. 「システムに決定させる」の選択を解除します。
4. 「ピクセルパーフェクト (ロスレス)」を選択します。

グラフィックスステータスインジケーターのアイコンが緑色になり、ロスレスモードが有効になっていることを示します。



カラースペース

これは、YUV 4:2:0およびYUV 4:4:4のカラースペースと色圧縮設定について説明する新しいセクションです。

概要

選択されたカラースペースによって、HDX™ Graphicsがどの色圧縮モード（クロマサブサンプリングとも呼ばれる）を使用するか、または使用しないかが決まります。デフォルトでは、HDX GraphicsはYUV 4:2:0クロマサブサンプリングを使用します。

クロマサブサンプリングは、VDAからクライアントにビデオデータを送信するために必要な帯域幅を削減するために使用される技術です。人間の目は色の変化（色度）よりも明るさ（輝度）の変化に敏感であるため、送信される色情報の量を減らすことで機能します。

4:2:0、4:2:2、4:4:4 のような比率で示される、さまざまなクロマサブサンプリング方式が存在します。これらの比率は、輝度情報に対してサンプリングされる色度情報の量を表します。

4:4:4 - クロマサブサンプリングなし。すべての色情報が保持されます。これにより、最高の画質と色精度が得られますが、最も多くの帯域幅を必要とします。

4:2:0 - 色度情報は、水平方向と垂直方向の両方で2分の1にサブサンプリングされます。これにより、最大の帯域幅削減が実現されますが、目立つ色のにじみが発生する可能性があります。



Citrix HDX グラフィックは、仮想デスクトップ環境での帯域幅の使用を最適化するためにクロマサブサンプリングを利用します。デフォルトでは、HDX は画面コンテンツのエンコードに YUV 4:2:0 を使用します。これにより、一般的なオフィス生産性アプリケーション/ほとんどのユースケースにおいて、画質と帯域幅効率の良好なバランスが提供されます。

画面全体がビデオコーデック（フルスクリーンエンコーダーを使用）でエンコードされると、色圧縮により、テキストなどの高コントラストの詳細が劣化し、ぼやけて読みにくくなる可能性があります。

医療画像処理、ビデオ編集、CAD/CAMアプリケーションなど、色精度が最重要となるシナリオでは、HDXはYUV 4:4:4もサポートしています。

これにより、エンコード中に色情報が失われないことが保証され、可能な限り最高の画像忠実度と色精度が提供されます。YUV 4:4:4 は YUV 4:2:0 よりも大幅に多くの帯域幅を使用することに注意してください。

帯域幅の輻輳に関連する問題を回避するために、本番環境でYUV 4:4:4を有効にする前に、テストシナリオで帯域幅の使用状況を検証してください。

マルチメディア

HDX™ テクノロジースタックは、2つの補完的なアプローチを通じてマルチメディアアプリケーションの配信をサポートします。

- サーバー側レンダリングによるマルチメディア配信
- クライアント側レンダリングによるマルチメディアリダイレクト

この戦略により、優れたユーザーエクスペリエンスで幅広いマルチメディア形式を配信し、サーバーのスケーラビリティを最大化してユーザーあたりのコストを削減できます。

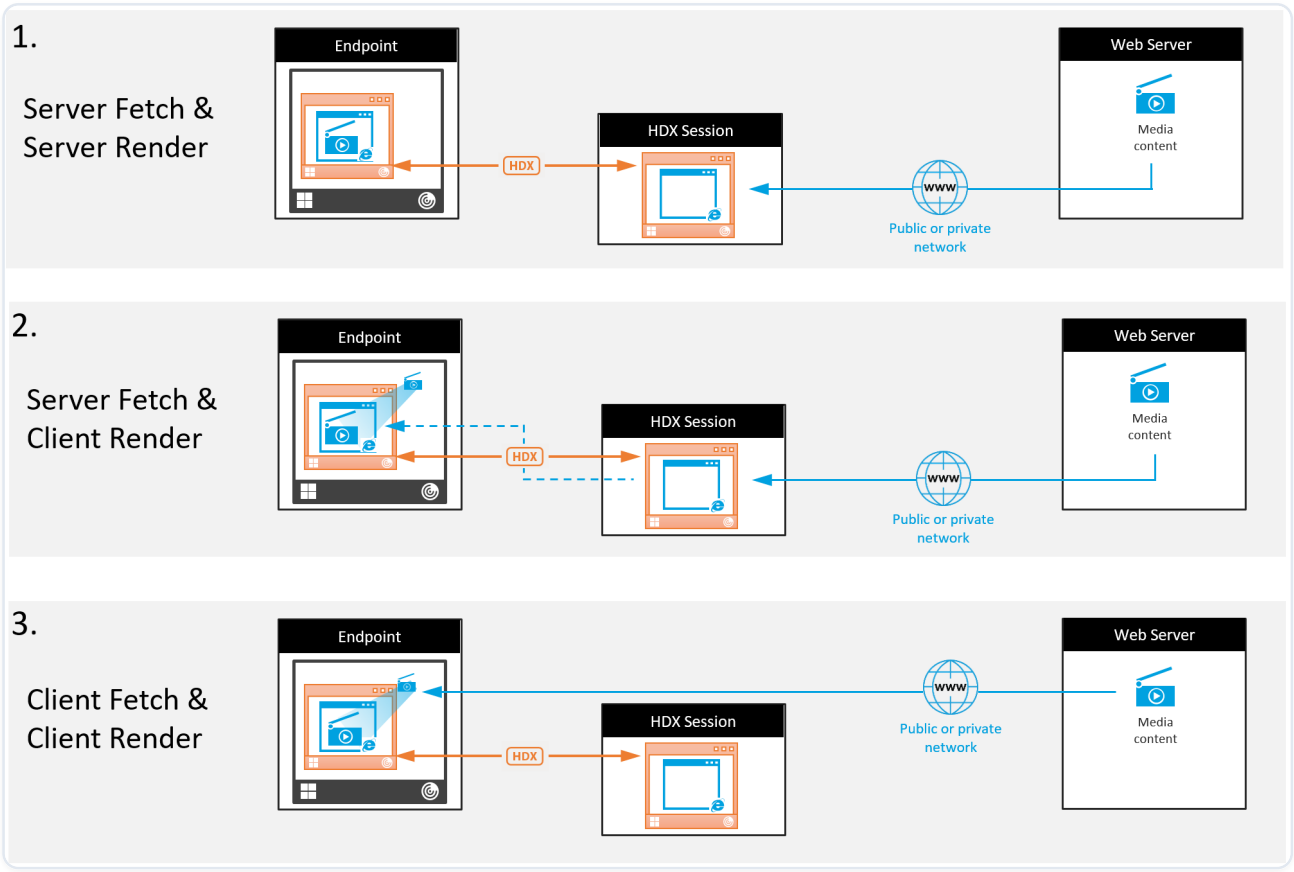
サーバーレンダリングによるマルチメディア配信では、オーディオおよびビデオコンテンツは、アプリケーションによってCitrix Virtual Apps and Desktopsサーバー上でデコードおよびレンダリングされます。その後、コンテンツは圧縮され、ICAプロトコルを使用してユーザーデバイス上のCitrix Workspaceアプリに配信されます。この方法は、さまざまなアプリケーションやメディア形式との互換性が最も高くなります。ビデオ処理は計算負荷が高いため、サーバーレンダリングによるマルチメディア配信は、オンボードのハードウェアアクセラレーションから大きな恩恵を受けます。たとえば、DirectX Video Acceleration (DXVA) のサポートにより、H.264デコードを個別のハードウェアで実行することでCPUの負荷が軽減されます。Intel Quick Sync、AMD RapidFire、NVIDIA NVENCテクノロジーは、ハードウェアアクセラレーションによるH.264エンコードを提供します。

ほとんどのサーバーはビデオ圧縮用のハードウェアアクセラレーションを提供しないため、すべてのビデオ処理がサーバーCPUで行われると、サーバーのスケーラビリティに悪影響が及びます。多くのマルチメディア形式をユーザーデバイスにリダイレクトしてローカルでレンダリングすることで、高いサーバーのスケーラビリティを維持できます。

- Windows Mediaリダイレクトは、通常Windows Media Playerに関連付けられているさまざまなメディア形式について、サーバーの負荷を軽減します。
- HTML5ビデオは普及しており、Citrix®はこの種のコンテンツ向けのリダイレクトテクノロジーを導入しました。HTML5、HLS、DASH、またはWebRTCを使用するWebサイトには、ブラウザーコンテンツリダイレクトをお勧めします。
- 一般的なコンテンツリダイレクトテクノロジーであるHost-to-client redirectionおよびLocal App Accessをマルチメディアコンテンツに適用できます。

これらのテクノロジーを組み合わせると、リダイレクトを設定しない場合、HDXはサーバー側レンダリングを実行します。 リダイレクトを設定すると、HDXはサーバーフェッチとクライアントレンダリング、またはクライアントフェッチとクライアントレンダリングのいずれかを使用します。これらの方法が失敗した場合、HDXは必要に応じてサーバー側レンダリングにフォールバックし、フォールバック防止ポリシーの対象となります。

シナリオ例



シナリオ1。（サーバーフェッチとサーバーレンダリング）：

1. サーバーはソースからメディアファイルを取得し、デコードしてから、オーディオデバイスまたはディスプレイデバイスにコンテンツを提示します。
2. サーバーは、表示デバイスまたはオーディオデバイスから、それぞれ提示された画像またはサウンドを抽出します。
3. サーバーは必要に応じてそれを圧縮し、クライアントに送信します。

このアプローチでは、高いCPUコスト、高い帯域幅コスト（抽出された画像/サウンドが効率的に圧縮されていない場合）、および低いサーバーのスケーラビリティが発生します。

Thinwireおよびオーディオ仮想チャネルがこのアプローチを処理します。このアプローチの利点は、クライアントのハードウェアおよびソフトウェア要件を削減することです。このアプローチを

使用すると、デコードはサーバー上で行われ、より幅広い種類のデバイスとフォーマットで動作します。

シナリオ2。（サーバーフェッチとクライアントレンダリング）：

このアプローチは、メディアコンテンツがデコードされ、オーディオまたは表示デバイスに提示される前に傍受できることに依存します。圧縮されたオーディオ/ビデオコンテンツは、代わりにクライアントに送信され、そこでローカルにデコードおよび提示されます。このアプローチの利点は、それらがクライアントデバイスにオフロードされ、サーバーのCPUサイクルを節約できることです。

しかし、これはクライアントに追加のハードウェアおよびソフトウェア要件ももたらします。クライアントは、受信する可能性のある各フォーマットをデコードできる必要があります。

シナリオ3。（クライアントフェッチとクライアントレンダリング）：

このアプローチは、メディアコンテンツのURLがソースからフェッチされる前に傍受できることに依存します。URLはクライアントに送信され、そこでメディアコンテンツがフェッチ、デコード、およびローカルに提示されます。このアプローチは概念的にシンプルです。その利点は、サーバーが制御コマンドのみを送信するため、サーバーのCPUサイクルと帯域幅の両方を節約できることです。ただし、メディアコンテンツが常にクライアントからアクセスできるとは限りません。

フレームワークとプラットフォーム：

シングルセッションオペレーティングシステム（Windows、Mac OS X、Linux）は、マルチメディアアプリケーションのより迅速な開発を可能にするマルチメディアフレームワークを提供します。この表は、より一般的なマルチメディアフレームワークの一部を示しています。各フレームワークは、メディア処理をいくつかの段階に分割し、パイプラインベースのアーキテクチャを使用します。

フレームワーク	プラットフォーム
DirectShow	Windows (98以降)
メディア ファンデーション	ウィンドウズ (Vista以降)
Gストリーマー	リナックス
クイックタイム	マック オーエス テン

メディアリダイレクトテクノロジーでのダブルホップサポート

オーディオリダイレクト	いいえ
ブラウザコンテンツリダイレクト	いいえ
HDX Webカメラリダイレクト	はい
HTML5ビデオのリダイレクト	はい
Windows Mediaリダイレクト	はい

オーディオ機能

HDXオーディオ機能を最適化するポリシーに、以下のCitrixポリシー設定を構成して追加できます。使用方法の詳細、および他のポリシー設定との関係と依存関係については、「オーディオポリシー設定」、「帯域幅ポリシー設定」、および「マルチストリーム接続ポリシー設定」を参照してください。

アダプティブオーディオ

アダプティブオーディオを使用すると、VDAでオーディオ品質ポリシーを手動で構成する必要がありません。アダプティブオーディオは、環境に合わせて設定を最適化し、古いオーディオ圧縮形式を置き換えて、優れたユーザーエクスペリエンスを提供します。

アダプティブオーディオはデフォルトで有効になっています。アダプティブオーディオを無効にするには、「オーディオポリシー設定」を参照してください。

重要：

リアルタイムオーディオアプリケーションが必要な場合、Citrix®はTCPではなくUser Datagram Protocol (UDP) を使用してオーディオを配信することを推奨します。UDP経由で利用できるオーディオトランスポートオプションは次のとおりです。

- UDP経由のオーディオ
- HDX™アダプティブトランスポート (Enlightened Data Transport)

> DTLSを使用したUDPオーディオ暗号化は、Citrix GatewayとCitrix Workspace™アプリの間でのみ利用可能です。そのため、TCPトランスポートを使用する方が望ましい場合があります。TCPは、VDAからCitrix Workspaceアプリへのエンドツーエンドの TLS暗号化をサポートします。

> アダプティブオーディオとUDPオーディオの詳細については、「UDPリアルタイムトランスポート経由のオーディオとオーディオUDPポート範囲」を参照してください。

オーディオのロストレラントモード

バージョン2308以降、損失許容モードはオーディオをサポートします。この機能は、リアルタイムストリーミングのユーザーエクスペリエンスを向上させ、ユーザーが遅延やパケット損失のあるネットワーク経由で接続している場合に、EDT経由のオーディオ品質を改善します。

損失許容モードとEDTの詳細については、Citrix Virtual Apps and Desktopsドキュメントの「追加情報」を参照してください。

オーディオの損失許容モードはデフォルトで有効になっています。無効になっている場合、または再度有効にする場合は、次の手順を実行します。

1. HDXアダプティブトランスポート（EDT）を有効にします。
2. オーディオの損失許容モードを有効にします。

クライアントの要件と設定

以下は、損失許容モードをサポートするCitrix Workspaceアプリの最小バージョンです。

- Windows向けCitrix Workspaceアプリ 2309
- Linux向けCitrix Workspaceアプリ 2311
- Mac向けCitrix Workspaceアプリ 2311

さらに、以下にご注意ください。

- (オプション) Citrix WorkspaceアプリとVDA間の直接接続の場合、VDAでのDTLSの有効化が必要です。
- (オプション) リモート接続の場合、損失許容モードはCitrix Gateway ServiceまたはNetScaler Gatewayでもサポートされている必要があります。

オーディオ品質

一般的に、音質が高いほど、より多くのオーディオデータをユーザーデバイスに送信するため、帯域幅とサーバーCPU使用率を多く消費します。サウンド圧縮を使用すると、音質とセッション全体のパフォーマンスのバランスを取ることができます。Citrixポリシー設定を使用して、サウンドファイルに適用する圧縮レベルを構成します。

デフォルトでは、TCPトランスポートが使用されている場合、**オーディオ品質ポリシー**設定は「高 - 高精細オーディオ」に設定されています。UDPトランスポート（推奨）が使用されている場合、ポリシーは「中 - 音声に最適化」に設定されます。**高精細オーディオ**設定は、高忠実度のステレオオーディオを提供しますが、他の品質設定よりも多くの帯域幅を消費します。最適化されていない音声チャットまたはビデオチャットアプリケーション（ソフトフォンなど）には、このオーディオ品質を使用しないでください。その理由は、リアルタイム通信に適さない遅延をオーディオパスに導入する可能性があるためです。選択したトランスポートプロトコルに関係なく、リアルタイムオーディオには「音声に最適化」ポリシー設定を推奨します。

帯域幅が制限されている場合（たとえば、衛星接続やダイヤルアップ接続など）、オーディオ品質を**低**に下げると、可能な限り少ない帯域幅を消費します。この状況では、低帯域幅接続のユーザー向けに個別のポリシーを作成し、高帯域幅接続のユーザーが悪影響を受けないようにします。

設定の詳細については、「オーディオポリシー設定」を参照してください。ユーザーデバイスでClient audio settingsを有効にすることを忘れないでください。

オーディオ再生および録音の帯域幅ガイドライン:

- アダプティブオーディオ（デフォルト）
  - ビットレート: 可変アダプティブ
  - チャンネル数: 再生用2（ステレオ）、マイクキャプチャ用1（モノラル）
  - 周波数: 48000 Hz
  - ビット深度: 16ビット
- 高音質
  - ビットレート：再生で約100 kbps（最小75、最大175 kbps）/マイクキャプチャで約70 kbps
  - チャンネル数：再生で2（ステレオ）、マイクキャプチャで1（モノラル）
  - 周波数：44100 Hz
  - ビット深度: 16ビット

- 中品質 (VoIPに推奨)
  - ビットレート: 再生時 ~16 kbps (最小20 kbps、最大40 kbps)、マイクキャプチャ時 ~16 kbps
  - チャンネル数: 再生とキャプチャの両方で1 (モノラル)
  - 周波数: 16000 Hz (広帯域)
  - ビット深度: 16ビット
- 低品質
  - ビットレート: 再生時約11 kbps (最小10; 最大25 kbps)、マイクキャプチャ時約11 kbps
  - チャンネル数: 再生時およびキャプチャ時ともに1 (モノラル)
  - 周波数: 8000 Hz (ナローバンド)
  - ビット深度: 16-bit

クライアントオーディオリダイレクト

ユーザーデバイス上のスピーカーまたはその他のサウンドデバイスを介して、サーバー上のアプリケーションからオーディオを受信できるようにするには、**クライアントオーディオリダイレクト**設定を**許可**のままにします。これはデフォルトです。

クライアントオーディオマッピングは、サーバーとネットワークに余分な負荷をかけます。ただし、クライアントオーディオリダイレクトを禁止すると、すべてのHDXオーディオ機能が無効になります。

設定の詳細については、「オーディオポリシー設定」を参照してください。ユーザーデバイスでクライアントオーディオ設定を有効にすることを忘れないでください。

クライアントマイクのリダイレクト

ユーザーデバイス上のマイクなどの入力デバイスを使用してユーザーがオーディオを録音できるようにするには、**クライアントマイクのリダイレクト**設定をデフォルト（許可）のままにします。

セキュリティのため、ユーザーデバイスは、信頼できないサーバーがマイクへのアクセスを試みた場合に、ユーザーに警告します。ユーザーはマイクを使用する前に、アクセスを許可するか拒否するかを選択できます。ユーザーはCitrix Workspaceアプリでこの警告を無効にできます。

設定の詳細については、「オーディオポリシー設定」を参照してください。ユーザーデバイスでクライアントオーディオ設定を有効にすることを忘れないでください。

オーディオプラグアンドプレイ

Audio Plug N Playポリシー設定は、複数のオーディオデバイスを使用してサウンドを録音および再生することを許可または禁止します。この設定はデフォルトで**有効**です。Audio Plug N Playにより、オーディオデバイスが認識されるようになります。ユーザーセッションが開始された後で接続されていなくても、デバイスは認識されます。

この設定は、WindowsマルチセッションOSマシンにのみ適用されます。

設定の詳細については、「オーディオポリシー設定」を参照してください。

オーディオリダイレクト帯域幅制限とオーディオリダイレクト帯域幅制限（パーセント）

オーディオリダイレクト帯域幅制限ポリシー設定は、セッションでのオーディオの再生および録音における最大帯域幅（キロビット/秒）を指定します。

オーディオリダイレクト帯域幅制限（パーセント）設定は、オーディオリダイレクトの最大帯域幅を、利用可能な総帯域幅のパーセンテージとして指定します。

デフォルトでは、両方の設定でゼロ（最大なし）が指定されています。両方の設定が構成されている場合、帯域幅制限が最も低い方が使用されます。

設定の詳細については、「帯域幅ポリシー設定」を参照してください。ユーザーデバイスでクライアントオーディオ設定を有効にすることを忘れないでください。

UDPリアルタイムトランスポート経由のオーディオとオーディオUDPポート範囲

デフォルトでは、ユーザーデータグラムプロトコル（UDP）リアルタイムトランスポート経由のオーディオは許可されています（インストール時に選択した場合）。これにより、UDPリアルタイムトランスポート経由のオーディオを使用する接続のために、サーバー上にUDPポートが開かれます。ネットワークの混雑やパケット損失がある場合は、可能な限り最高のユーザーエクスペリエンスを確保するために、オーディオにUDP/RTPを構成することをお勧めします。ソフトフォンアプリケーションなどのリアルタイムオーディオの場合、UDPオーディオはEDTよりも推奨されます。UDPは再送信なしでパケット損失を許容するため、パケット損失が多い接続で遅延が追加されることはありません。

> **重要:**

Citrix Gatewayがパスにない場合、UDPで送信されるオーディオデータは暗号化されません。Citrix GatewayがCitrix Virtual Apps and Desktops™リソースにアクセスするように構成されている場合、エンドポイントデバイスとCitrix Gateway間のオーディオトラフィックはDTLSプロトコルを使用して保護されます。

オーディオUDPポート範囲は、Windows VDAがユーザーデバイスとオーディオパケットデータを交換するために使用するポート番号の範囲を指定します。

デフォルトでは、範囲は16500から16509です。

注:

アダプティブオーディオにAudio over UDP Real-time Transportが不要な場合、Citrixではポリシー設定を無効にすることをお勧めします。これにより、Citrix Workspaceアプリクライアントが UDP接続のオープンを要求したり、不要なCitrix Workspaceアプリクライアントのファイアウォール構成ダイアログウィンドウが表示されたりするのを防ぐことができます。

Audio over UDP Real-time Transportの設定の詳細については、「オーディオポリシー設定」を参照してください。オーディオUDPポート範囲の詳細については、「マルチストリーム接続ポリシー設定」を参照してください。ユーザーデバイスでクライアントオーディオ設定を有効にすることを忘れないでください。

Audio over UDPにはWindows VDAが必要です。Linux VDAでサポートされているポリシーについては、「ポリシーサポートリスト」を参照してください。

ユーザーデバイスのオーディオ設定ポリシー

1. グループポリシーオブジェクト管理用テンプレートの構成に従って、グループポリシテンプレートをロードします。
2. グループポリシーエディターで、**［管理用テンプレート］>［Citrix Components］>［Citrix Workspace］>［ユーザーエクスペリエンス］**の順に展開します。
3. **［クライアントオーディオ設定］で、［未構成］、［有効］**、または**［無効］**を選択します。

   - **［未構成］**。デフォルトでは、オーディオリダイレクトは高品質オーディオまたは以前に構成されたカスタムオーディオ設定を使用して有効になります。
   - **［有効］**。選択したオプションを使用してオーディオリダイレクトを有効にします。

- **［無効］**。オーディオリダイレクトを無効にします。

4. **［有効］を選択した場合は、音質を選択します。UDPオーディオの場合は、［中］**（デフォルト）を使用します。
5. UDPオーディオの場合のみ、**［リアルタイムトランスポートを有効にする］**を選択し、ローカルのWindowsファイアウォールで開く受信ポートの範囲を設定します。
6. Citrix GatewayでUDPオーディオを使用するには、**［ゲートウェイ経由のリアルタイムトランスポートを許可する］**を選択します。Citrix GatewayをDTLSで構成します。詳しくは、こちらの記事を参照してください。

管理者として、これらの変更を行うためのエンドポイントデバイスを制御できない場合は、StoreFront の default.ica 属性を使用して UDP Audio を有効にします。たとえば、BYOD (個人所有デバイス) や自宅のコンピューターの場合などです。

1. StoreFront マシンで、メモ帳などのエディターを使用して C:\inetpub\wwwroot\Citrix\\\<Store Name>\App_Data\default.ica を開きます。
2. セクションに以下のエントリを作成します。

   ; このテキストはリアルタイムトランスポートを有効にします

   RTPオーディオを有効にする=true

   ; このテキストはゲートウェイ経由のリアルタイムトランスポートを許可します

   ゲートウェイ経由のUDPを有効にする=true

   ; このテキストはオーディオ品質を「中」に設定します

   AudioBandwidthLimit=1

   ; UDP ポート範囲

   RtpAudioLowestPort=16500

   RtpAudioHighestPort=16509

default.ica を編集してユーザーデータグラムプロトコル (UDP) オーディオを有効にすると、そのストアを使用しているすべてのユーザーに対して UDP オーディオが有効になります。

マルチメディア会議中のエコーを回避する

オーディオまたはビデオ会議のユーザーはエコーを聞くことがあります。エコーは通常、スピーカーとマイクが互いに近すぎるときに発生します。そのため、オーディオおよびビデオ会議にはヘッドセットの使用をお勧めします。

HDXは、エコーを最小限に抑えるエコーキャンセレーションオプション（デフォルトで有効）を提供します。エコーキャンセレーションの有効性は、スピーカーとマイクの間の距離に影響されます。デバイスが互いに近すぎたり遠すぎたりしないようにしてください。

レジストリ設定を変更して、エコーキャンセルを無効にできます。詳細については、レジストリで管理される機能のリストにあるマルチメディア会議中のエコーを回避するを参照してください。

ソフトフォン

ソフトフォンとは、電話インターフェースとして機能するソフトウェアです。コンピューターやその他のスマートデバイスからインターネット経由で通話するためにソフトフォンを使用します。ソフトフォンを使用すると、画面を使って電話番号をダイヤルしたり、その他の電話関連機能を実行したりできます。

Citrix Virtual Apps and Desktopsは、ソフトフォンを配信するためのいくつかの代替手段をサポートしています。

- **制御モード**。ホストされているソフトフォンが物理的な電話機を制御します。このモードでは、Citrix Virtual Apps and Desktopsサーバーを介してオーディオトラフィックは流れません。
- **HDX RealTime最適化ソフトフォンサポート（推奨）**。メディアエンジンはユーザーデバイス上で実行され、Voice over Internet Protocolトラフィックはピアツーピアで流れます。例については、以下を参照してください。
    - Microsoft Teams向けHDX最適化
    - HDX RealTime Optimization Pack、Microsoft Skype for Businessの配信を最適化します
    - Cisco Jabber ソフトフォン VDI用（旧称VXME）
    - シスコ Webex Meetings VDI用(https://www.cisco.com/c/en/us/td/docs/collaboration/meeting_center/wvdi/wvdi-b-admin-guide/wvdi-b-admin-guide_chapter_010.html)
    - Avaya VDI Equinox（旧称VDIコミュニケーター）
    - Zoom VDI プラグイン
    - ジェネシス ピュアエンゲージ クラウド
    - Nuance Dragon PowerMic 音声入力デバイス

- **ローカルアプリアクセス**。Citrix Virtual Apps and Desktopsの機能で、ソフトフォンなどのアプリケーションをWindowsユーザーデバイス上でローカルに実行しながら、仮想/公開デスクトップとシームレスに統合されているように見せることができます。この機能は、すべてのオーディオ処理をユーザーデバイスにオフロードします。詳細については、ローカルアプリアクセスとURLリダイレクトを参照してください。
- **HDX RealTime汎用ソフトフォンサポート**。ICA経由のVoice over Internet Protocol。

汎用ソフトフォンサポート

汎用ソフトフォンサポートにより、データセンターのXenAppまたはXenDesktop上で、変更されていないソフトフォンをホストできます。オーディオトラフィックは、Citrix ICAプロトコル（UDP/RTPの使用が望ましい）を介して、Citrix Workspaceアプリを実行しているユーザーデバイスに送信されます。

汎用ソフトフォンサポートは、HDX RealTimeの機能です。このソフトフォン配信のアプローチは、特に次の場合に役立ちます。

- ソフトフォンを配信するための最適化されたソリューションが利用できず、ユーザーがLocal App Accessを使用できるWindowsデバイスを使用していない場合。
- ソフトフォンの最適化された配信に必要なメディアエンジンがユーザーデバイスにインストールされていないか、ユーザーデバイスで実行されているオペレーティングシステムのバージョンで利用できない場合。このシナリオでは、汎用HDX RealTimeが貴重なフォールバックソリューションを提供します。

Citrix Virtual Apps and Desktopsを使用したソフトフォン配信には、次の2つの考慮事項があります。

- ソフトフォンアプリケーションが仮想/公開デスクトップにどのように配信されるか。
- オーディオがユーザーのヘッドセット、マイク、スピーカー、またはUSB電話機との間でどのように配信されるか。

Citrix Virtual Apps and Desktopsには、汎用ソフトフォン配信をサポートするための多数のテクノロジーが含まれています。

- リアルタイムオーディオの高速エンコードと帯域幅効率のための、音声に最適化されたコーデック。
- 低遅延オーディオスタック。
- ネットワーク遅延が変動するときにオーディオをスムーズにするための、サーバー側ジッターバッファ。

- サービス品質 (QoS) のためのパケットタグ付け (DSCPおよびWMM)。
  - RTPパケット (レイヤー3) 用のDSCPタグ付け
  - Wi-Fi用のWMMタグ付け

Citrix Workspace appのWindows、Linux、Chrome、Mac版もVoice over Internet Protocolに対応しています。Citrix Workspace app for Windowsは、以下の機能を提供します。

- クライアント側のジッターバッファ - ネットワーク遅延が変動してもスムーズなオーディオを保証します。
- エコーキャンセレーション - ヘッドセットを使用しない作業者向けに、マイクとスピーカー間の距離の許容範囲を広げます。
- オーディオプラグアンドプレイ - オーディオデバイスはセッション開始前に接続する必要はありません。いつでも接続できます。
- オーディオデバイスルーティング - ユーザーは着信音をスピーカーに、音声パスをヘッドセットに振り向けることができます。
- マルチストリームICA - ネットワーク経由での柔軟なQuality of Serviceベースのルーティングを可能にします。
- ICAは4つのTCPストリームと2つのUDPストリームをサポートします。UDPストリームの1つは、RTP経由のリアルタイムオーディオをサポートします。

Citrix Workspace appの機能の概要については、Citrix Receiver Feature Matrixを参照してください。

システム構成の推奨事項

クライアントハードウェアとソフトウェア: 最適なオーディオ品質を得るには、最新バージョンのCitrix Workspace appと、音響エコーキャンセレーション (AEC) 機能を備えた高品質のヘッドセットをお勧めします。Citrix Workspace appのWindows、Linux、Mac版はVoice over Internet Protocolをサポートしています。また、Dell WyseはThinOS (WTOS) 向けにVoice over Internet Protocolサポートを提供しています。

CPUに関する考慮事項: VDAのCPU使用率を監視し、各仮想マシンに2つの仮想CPUを割り当てる必要があるかどうかを判断してください。リアルタイムの音声とビデオはデータ集約型です。2つの仮想CPUを構成すると、スレッド切り替えの遅延が減少します。したがって、Citrix Virtual Desktops™ VDI環境では2つのvCPUを構成することをお勧めします。

2つの仮想CPUを持つことは、物理CPUの数を2倍にすることを必ずしも意味しません。物理CPUはセッション間で共有できるためです。

セッション信頼性機能に使用されるCitrix Gateway Protocol (CGP) もCPU消費を増加させます。高品質のネットワーク接続では、VDAでのCPU消費を削減するためにこの機能を無効にすることができます。強力なサーバーでは、上記のいずれのステップも不要な場合があります。

UDPオーディオ: UDP経由のオーディオは、ネットワークの輻輳とパケット損失に対して優れた耐性を提供します。利用可能な場合は、TCPの代わりにUDPをお勧めします。

LAN/WAN構成: 良好なリアルタイムオーディオ品質のためには、ネットワークの適切な構成が不可欠です。通常、過剰なブロードキャストパケットがジッターを引き起こす可能性があるため、仮想LAN (VLAN) を構成する必要があります。IPv6対応デバイスは多くのブロードキャストパケットを生成する可能性があります。IPv6サポートが不要な場合は、それらのデバイスでIPv6を無効にすることができます。Quality of Serviceをサポートするように構成してください。

WAN接続の使用設定: LANおよびWAN接続でボイスチャットを使用できます。WAN接続では、オーディオ品質は接続の遅延、パケット損失、ジッターに依存します。WAN接続のユーザーにソフトフォンを提供する場合は、データセンターとリモートオフィス間でNetScaler® SD-WANを使用することをお勧めします。これにより、高いサービス品質が維持されます。NetScaler SD-WANは、UDPを含むMulti-Stream ICAをサポートしています。また、単一のTCPストリームの場合でも、さまざまなICA仮想チャネルの優先順位を区別して、優先度の高いリアルタイムオーディオデータが優先的に処理されるようにすることが可能です。

DirectorまたはHDX Monitorを使用して、HDX構成を検証します。

リモートユーザー接続: Citrix Gatewayは、UDP/RTPトラフィックをネイティブに（TCPでのカプセル化なしで）配信するためにDTLSをサポートしています。 ポート443経由のUDPトラフィックに対して、ファイアウォールを双方向に開きます。

コーデックの選択と帯域幅の消費: ユーザーデバイスとデータセンター内のVDA間では、**Optimized-for-Speech**コーデック設定（中品質オーディオとも呼ばれます）を使用することをお勧めします。VDAプラットフォームとIP-PBX間では、ソフトフォンは構成またはネゴシエートされたコーデックを使用します。例：

- G711は良好な音声品質を提供しますが、1通話あたり80キロビット/秒から100キロビット/秒の帯域幅を必要とします（ネットワークレイヤー2のオーバーヘッドによって異なります）。
- G729は良好な音声品質を提供し、1通話あたり30キロビット/秒から40キロビット/秒という低い帯域幅を必要とします（ネットワークレイヤー2のオーバーヘッドによって異なります）。

仮想デスクトップへのソフトフォンアプリケーションの配信

XenDesktop®仮想デスクトップにソフトフォンを配信するには、2つの方法があります。

- アプリケーションは仮想デスクトップイメージにインストールできます。
- アプリケーションはMicrosoft App-Vを使用して仮想デスクトップにストリーミングできます。このアプローチには、仮想デスクトップイメージが整理された状態に保たれるため、管理上の利点があります。仮想デスクトップにストリーミングされた後、アプリケーションは通常の方法でインストールされたかのようにその環境で実行されます。すべてのアプリケーションがApp-Vと互換性があるわけではありません。

ユーザーデバイスとの間でオーディオを配信する

汎用HDX RealTimeは、ユーザーデバイスとの間でオーディオを配信する2つの方法をサポートしています。

- 「**Citrix Audio Virtual Channel**」。Citrix Audio Virtual Channelはオーディオ転送専用に設計されているため、一般的に推奨されます。
- 「**汎用USBリダイレクト**」。ユーザーデバイスがCitrix Virtual Apps and Desktopsサーバーへのまたは LANに類似した接続上にある場合、ボタンまたはディスプレイ（あるいはその両方）を持つオーディオデバイス、ヒューマンインターフェースデバイス（HID）をサポートします。

Citrix オーディオ仮想チャネル

双方向のCitrixオーディオ仮想チャネル（CTXCAM）により、オーディオをネットワーク経由で効率的に配信できます。汎用HDX RealTimeは、ユーザーのヘッドセットまたはマイクからオーディオを取得して圧縮します。次に、それをICA経由で仮想デスクトップ上のソフトフォンアプリケーションに送信します。同様に、ソフトフォンのオーディオ出力は圧縮され、反対方向にユーザーのヘッドセットまたはスピーカーに送信されます。この圧縮は、ソフトフォン自体が使用する圧縮（G.729やG.711など）とは独立しています。これは、Optimized-for-Speechコーデック（中品質）を使用して行われます。その特性は、Voice over Internet Protocolに最適です。エンコード時間が短く、ネットワーク帯域幅はピーク時で約56キロビット/秒（各方向28 Kbps）しか消費しません。このコーデックはデフォルトのオーディオコーデックではないため、Studioコンソールで明示的に選択する必要があります。デフォルトはHDオーディオコーデック（高品質）です。このコーデックは高忠実度のステレオサウンドトラックに優れていますが、Optimized-for-Speechコーデックと比較してエンコードが遅くなります。

汎用 USB リダイレクト

Citrix汎用USBリダイレクトテクノロジー（CTXGUSB仮想チャネル）は、複合デバイス（オーディオとHID）やアイソクロナスUSBデバイスを含むUSBデバイスをリモートで利用するための汎用的な手段を提供します。このアプローチは、LAN接続ユーザーに限定されます。その理由は、USBプロトコルがネットワーク遅延に敏感であり、かなりのネットワーク帯域幅を必要とする傾

向があるためです。アイソクロナスUSBリダイレクトは、一部のソフトフォンを使用する場合にうまく機能します。このリダイレクトは、優れた音声品質と低遅延を提供します。ただし、Citrixオーディオ仮想チャネルはオーディオトラフィックに最適化されているため、こちらが推奨されます。主な例外は、ボタン付きのオーディオデバイスを使用する場合です。たとえば、データセンターにLAN接続されたユーザーデバイスに接続されているUSB電話などです。この場合、汎用USBリダイレクトは、電話機またはヘッドセットのボタンがソフトフォンに信号を送信して機能を制御することをサポートします。デバイス上でローカルに機能するボタンには問題ありません。

オーディオ診断コマンドラインツール

VDA上のオーディオ診断コマンドラインツールを使用して、オーディオポリシー、構成、データ転送に関連するセッションデータを照会できます。

使用方法

コマンドプロンプトを開き、`C:\Program Files\Citrix\HDX\bin`フォルダーから`CtxAudio.exe`を実行します。

- 管理者としてツールを実行すると、すべてのアクティブなICAセッションのオーディオ情報が表示されます。
- 非管理者としてツールを実行すると、現在ユーザーのICAセッションオーディオ情報が表示されます。

出力

このツールは、セッション内のオーディオ関連の問題の診断に役立つさまざまな構成設定を出力します。

セクション	説明
ポリシー情報	現在のセッションに適用されるオーディオポリシー。
設定情報	レジストリに保存されているオーディオ関連の構成設定。
状態情報	現在のセッションに適用されているオーディオの状態、バージョン、コーデック、およびトランスポート。

セクション	説明
デバイス情報	セッションで使用されているデバイス名、その役割、およびステータス。

注:

出力は、マルチセッション (TS) VDA またはシングルセッション VDA (WSVDA) のどちらでツールを実行するかによって異なります。

制限事項

クライアントにオーディオデバイスをインストールし、オーディオリダイレクトを有効にして、RDSセッションを開始します。オーディオファイルが再生に失敗し、エラーメッセージが表示されることがあります。

回避策として、RDSマシンにレジストリキーを追加し、マシンを再起動します。詳細については、レジストリで管理される機能のリストにあるオーディオの制限を参照してください。

ブラウザコンテンツリダイレクト

はじめに

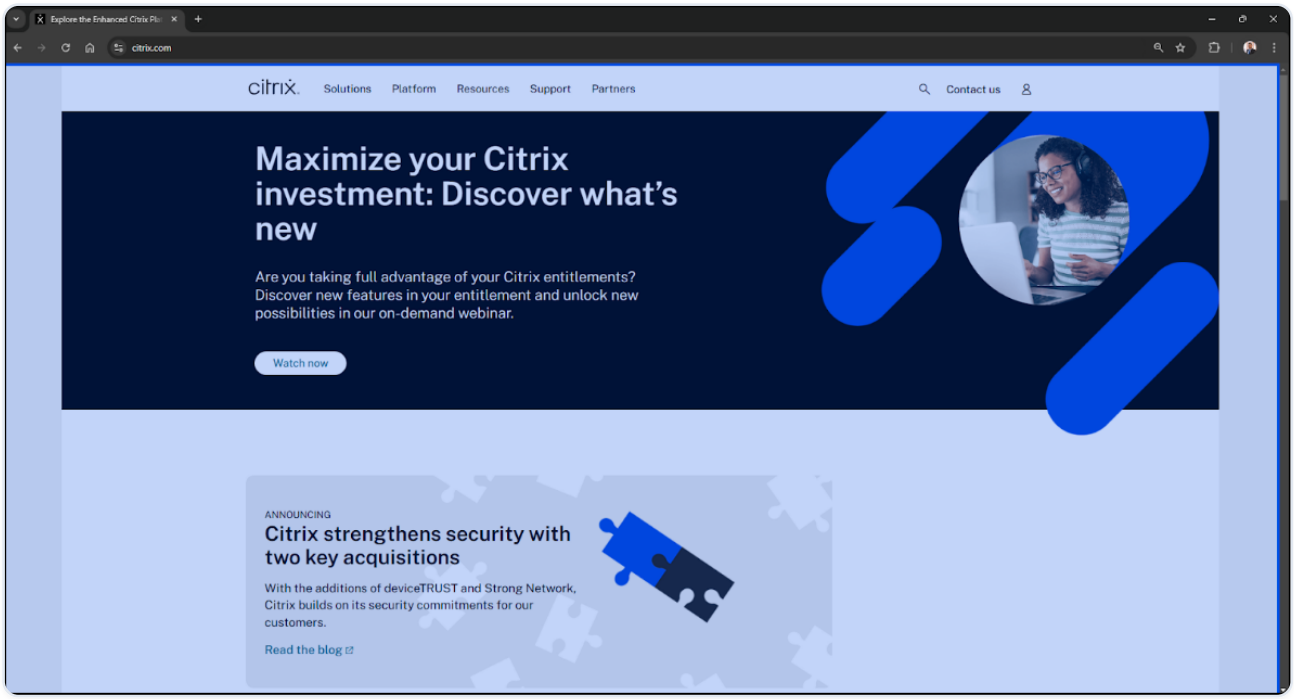
ブラウザコンテンツリダイレクト (BCR) は、Citrix Virtual Apps and Desktops™環境でのWebブラウジングのユーザーエクスペリエンスを向上させます。Webページのレンダリングをユーザーのローカルマシンにオフロードすることで、BCRはサーバーの負荷を軽減し、特に複雑なWebサイトやリソースを大量に消費するWebサイトのパフォーマンスを向上させます。

動作の仕組み

BCRは、Citrix Workspace™アプリを利用して、ユーザーデバイス上に安全なブラウジング環境を作成します。ユーザーが許可されたWebページにアクセスすると、ブラウザウィンドウのビューポートがクライアントにリダイレクトされます。クライアント側のブラウザエンジンは、ローカルマシンのリソースを活用してページをレンダリングし、読み込み時間の短縮とスムーズな操作を実現します。

ブラウザのビューポートのみがリダイレクトされることに注意してください。ビューポートとは、ブラウザ内でコンテンツが表示される長方形の領域です。ビューポートには、アドレス

バー、お気に入りツールバー、ステータスバーなどは含まれません。これらの項目はユーザーインターフェイスにあり、VDA内のブラウザで引き続き実行されます。



新機能

ブラウザコンテンツリダイレクトにおけるブラウザプロファイル共有 (テクニカルプレビュー)

BCRは、新しいプロファイル共有機能により、VDA側での認証とCookie共有を可能にし、合理化されたユーザーエクスペリエンスを提供します。この機能強化により、冗長なログインが不要になり、BCRウィンドウが閉じられた後でもBCRセッション全体で認証とCookieの永続性を維持することで、生産性が向上します。このシームレスなエクスペリエンスは、認証がクライアントではなくVDAから行われることを保証することで、セキュリティをさらに強化します。

例:

- **以前のエクスペリエンス:** 以前は、BCR内で認証されたページを開くたびに、ユーザーは資格情報を再入力する必要があり、SSOの永続性が失われていました。SSOは、BCRウィンドウが開いている間のみ維持されました。ウィンドウを閉じたり再度開いたりすると、ユーザーはログインプロセスを繰り返す必要がありました。
- **新しいエクスペリエンス:** プロファイル共有により、ユーザーは資格情報の入力を求められることがなくなりました。SSOはVDAブラウザからシームレスに保持され、大幅に改善された中断のないエクスペリエンスを提供します。

注:

この機能は特定のプロバイダーに限定されません。したがって、他のプロバイダー (Microsoft認証、PingIDなど) でも機能します。ただし、現在の検証は上記のプロバイダーに対して行われています。

テクニカルプレビューの要件

- シトリックス バーチャルアプリおよびデスクトップ 2503
- シトリックス ワークスペースアプリ 2503
- ブラウザリダイレクト拡張機能 25.3.4 以降
  - Microsoft Edge 拡張機能
  - Google Chrome 拡張機能

フィードバックフォーム

構成

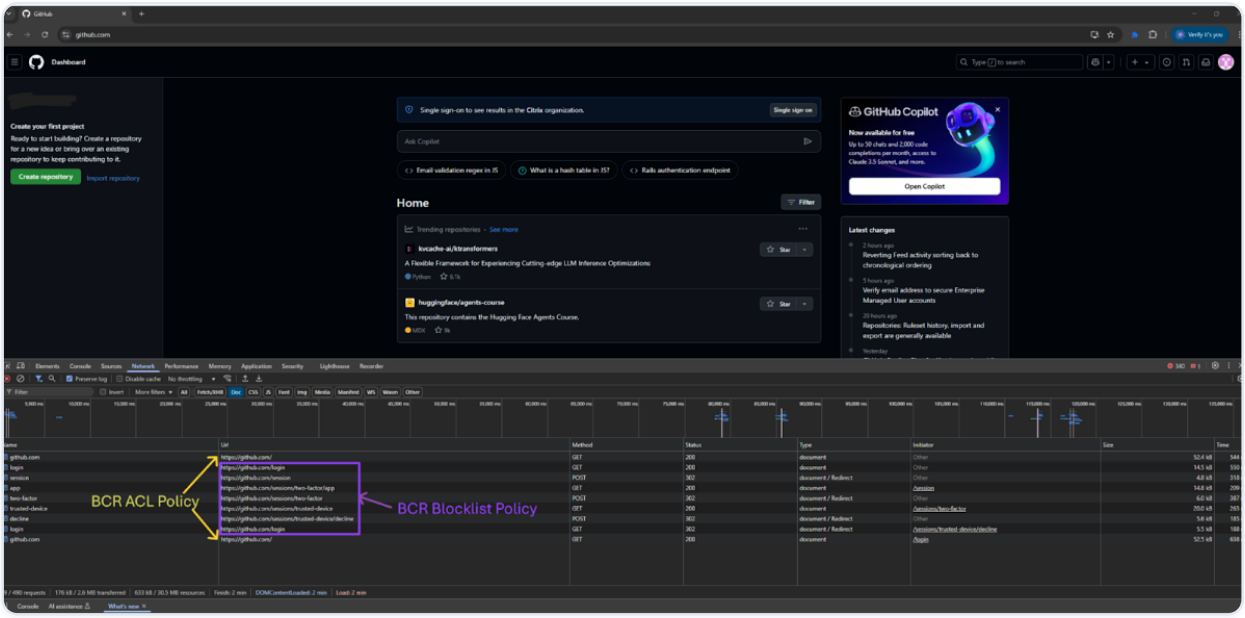
この機能が導入される前は、ウェブサイトによる認証に使用されるURLを指定するために、ブラウザコンテンツリダイレクト認証サイトポリシーが使用されていました。認証サイトを設定することで、管理者は認証（または）中間ログインページをクライアントにリダイレクトすることを許可していました。プロファイル共有の導入により、BCRはVDA側のブラウザの認証Cookieを活用するため、認証サイトポリシーのURLは、代わりにブラウザコンテンツリダイレクトブロックリストポリシーで構成する必要があります。これにより、認証がVDAを介して行われるようになります。

- VDAでこの機能を有効にするには、HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HDXMediaStreamキーに、以下のレジストリ値（Dword BrowserProfileSharing value 1）を作成します。
- リダイレクトするウェブサイトでブラウザコンテンツリダイレクトACL構成ポリシーを設定します。この点に関する構成の変更はありません。
- 認証サイトポリシーにすでにURLが構成されている場合は、それらをブラウザコンテンツリダイレクトブロックリストポリシーにコピーし、認証サイトポリシーを無効にします。
- 以前に認証/中間サイトを設定していない場合は、ブロックリストで設定する必要がある中間URLを特定するために以下のプロセスに従ってください。BCR拡張機能がインストールされていないChromeまたはEdgeブラウザで開発者ツールを使用して、中間ログインページを特定します。

例 1:

github.com の例を次に示します。この方法は、BCR でリダイレクトしたいすべてのウェブサイトに使用でき、適切な構成がされていることを確認できます。

- Chromeを開き、CTRL+SHIFT+Iを押して開発者ツールを起動します。
- 「Network」タブをクリックします。
- 「Preserve log」設定をチェックします。
- ネットワークログを簡素化するために、「Doc」フィルターをクリックします。
- 「Name」の横を右クリックし、「URL」列を追加します。
- 開発者ツールを開いたまま、github.comにアクセスします。
- github.comにサインインします。
- github.comの初期ページから、ログオン後の最終的な宛先までのすべての中間ホップをメモします。
- これらの中間URLは、ブラウザコンテンツリダイレクトのブロックリストポリシーに入力されます。
- その他の非ログインページは、ブラウザコンテンツリダイレクトのACLポリシーに入力されます。



例 2:

meet.google.com と Okta の例を次に示します。この場合、以前の例に従ってURLを特定し、ワイルドカードを使用して冗長な構成を排除しました。

- ブラウザコンテンツリダイレクトACLポリシー

  - `<https://meet.google.com/>`*
  - `<https://workspace.google.com/products/meet/>`*

- ブラウザコンテンツリダイレクトブロックリスト
  - `<https://accounts.google.com/>`*
  - `<https://sso.xyzcompany.com/>`* - SSOページの構成方法に基づいて、このURLはお客様の環境に固有のものとなります
  - `<https://www.google.com/a/xyzcompany.com/>`* - SSOページの構成方法に基づいて、このURLはお客様の環境に固有のものとなります

主な利点

ブラウザコンテンツリダイレクトは、Webトラフィックをインテリジェントに管理し、インフラストラクチャへの負担を軽減しながら、ユーザーに優れたエクスペリエンスを提供します。

組織にとっての利点は次のとおりです。

- **コスト削減:** リソースを大量に消費するWebページをユーザーデバイスにオフロードすることで、貴重なサーバーリソースを解放し、帯域幅の消費を削減します。これにより、ハードウェアとネットワークのコストが削減されます。
- **ユーザーエクスペリエンスの向上:** グラフィックを多用するWebサイトでも、よりスムーズで応答性の高いブラウジングエクスペリエンスをユーザーに提供します。ネイティブのようなパフォーマンスを提供し、遅延をなくし、生産性を向上させます。
- **セキュリティの向上:** 内部および外部リソースへのアクセスを許可しながら、セキュアな環境を維持します。
- **柔軟性の向上:** 基本的なWebブラウジングから、プロキシトラバーサルやSSO認証を必要とする複雑なWebアプリケーションまで、幅広いユースケースをサポートします。Citrix Web Studio™のきめ細かなポリシーコントロールでリダイレクト設定を簡単に管理できます。

システム要件

サーバー側コンポーネント

シトリックス バーチャル アプリ アンド デスクトップ

- 長期サービスリリース
  - 最小要件 - サポート終了していないLTSR版のCitrix Virtual Apps and Desktopsリリース
  - 推奨されるバージョンは、Citrix Virtual Apps and Desktops 2402以降です。

- 現在のリリース
  - 最小要件 - サポート終了していないCR版のCitrix Virtual Apps and Desktopsリリース
  - 推奨 - 最新のCitrix Virtual Apps and Desktopsリリース

ブラウザコンポーネント

- ブラウザ
  - マイクロソフト エッジ
  - グーグル クローム
- ブラウザリダイレクト拡張機能
  - グーグル クローム ストア
  - マイクロソフト エッジ ストア
- 最高のパフォーマンスを得るには、最新バージョンのブラウザーを使用することをお勧めします

> **注:**
>
> Browser Content RedirectionまたはBi-directional Content Redirectionを有効にするには、Microsoft Edgeアドオンストアからブラウザリダイレクト拡張機能を使用する場合、Virtual Delivery Agent (VDA) バージョン2503がインストールされていることを確認してください。古いVDAバージョンでは、Microsoft Edgeブラウザ内でChromeウェブストアから拡張機能をインストールすることで、同じ機能を実現できます。
>
> 上記の拡張機能リンクは一般提供 (GA) されており、本番レベルの展開に関連しています。GA拡張機能に加えて、Citrixはベータ版 (GA + 1) 拡張機能も特にGoogle Chrome Storeで公開しています。
>
> Citrixは、今後のアップデートがテストされ、問題が早期に報告されるように、お客様がベータ版のテストユーザーを持つことを推奨しています。これにより、GA拡張機能が正式に展開される際にスムーズなプロセスが保証されます。
>
> 拡張機能のリリースは通常、Citrix Workspaceアプリのリリースと一致します。

クライアント側コンポーネント

ウィンドウズ

- Windows 10または11
- Citrix Workspaceアプリ
  - 最小要件 - サポート終了していないCitrix Workspaceアプリ
  - 推奨
    - 長期サービスリリース - Citrix Workspaceアプリ 2402 最新CU
    - 現在のリリース - Citrix Workspaceアプリ 2405 以降

> **注記：**
>
> - Browser content redirectionは、Citrix Workspaceアプリ Windows LTSRリリース1912および2203.1ではサポートされていません。
> - Browser content redirectionに必要なクライアント側ブラウザエンジンは、Citrix WorkspaceアプリのCurrent Releasesにデフォルトでインストールされます。
> - ブラウザコンテンツリダイレクトに必要なクライアント側ブラウザエンジンは、Citrix Workspace App 2402 LTSRリリースではデフォルトでインストールされません。管理者は、ADDLOCALスイッチを利用して、Citrix Workspace AppにBCRブラウザコンポーネントをインストールできます。
> - Windows向けCitrix Workspaceアプリ2507以降、ブラウザコンテンツリダイレクト (BCR) はモジュールコンポーネントとして管理されますが、引き続きCitrix Workspaceアプリに同梱されています。BCRコンポーネントは、CRとLTSRの間の一貫性を確保するため、LTSRバージョンでもデフォルトでインストールされるようになりました。さらに、通常のCitrix Workspaceアプリのリリースサイクル外で独立した更新や暫定パッチが必要な状況のために、スタンドアロンのBCRパッケージが公開されます。詳細については、Citrix Workspace App Windowsのドキュメントを参照してください。

リナックス

- Citrix Workspaceアプリ
  - 最小要件 - サポート終了していないCitrix Workspaceアプリ

- 推奨 - Citrix Workspaceアプリ2408以降 詳細については、Citrix Workspace App Linuxのドキュメントを参照してください。

注:

Linux向けCitrix Workspaceアプリ2601以降、ブラウザコンテンツリダイレクト (BCR) はモジュールコンポーネントとして管理されます。BCRコンポーネントは、一貫したユーザーエクスペリエンスを確保するため、引き続きLinux向けCitrix Workspaceアプリに同梱され、デフォルトでインストールされます。さらに、通常のCitrix Workspaceアプリのリリースサイクル外で独立した更新や暫定パッチが必要な状況のために、スタンドアロンのBCRパッケージが公開されます。詳細については、Citrix Workspace App Linuxのドキュメントを参照してください。

ChromeOS

- Citrix Workspace アプリ
  - Chromeウェブストアの最新バージョン

MacOS

- macOS 11 ビッグサー
- macOS 12 モントレー
- macOS 13 ベンチュラ
- macOS 14 Sonoma (14.2.1まで)
- Citrix Workspace アプリ
  - 最小要件 - Citrix Workspace app 2411以降

注:

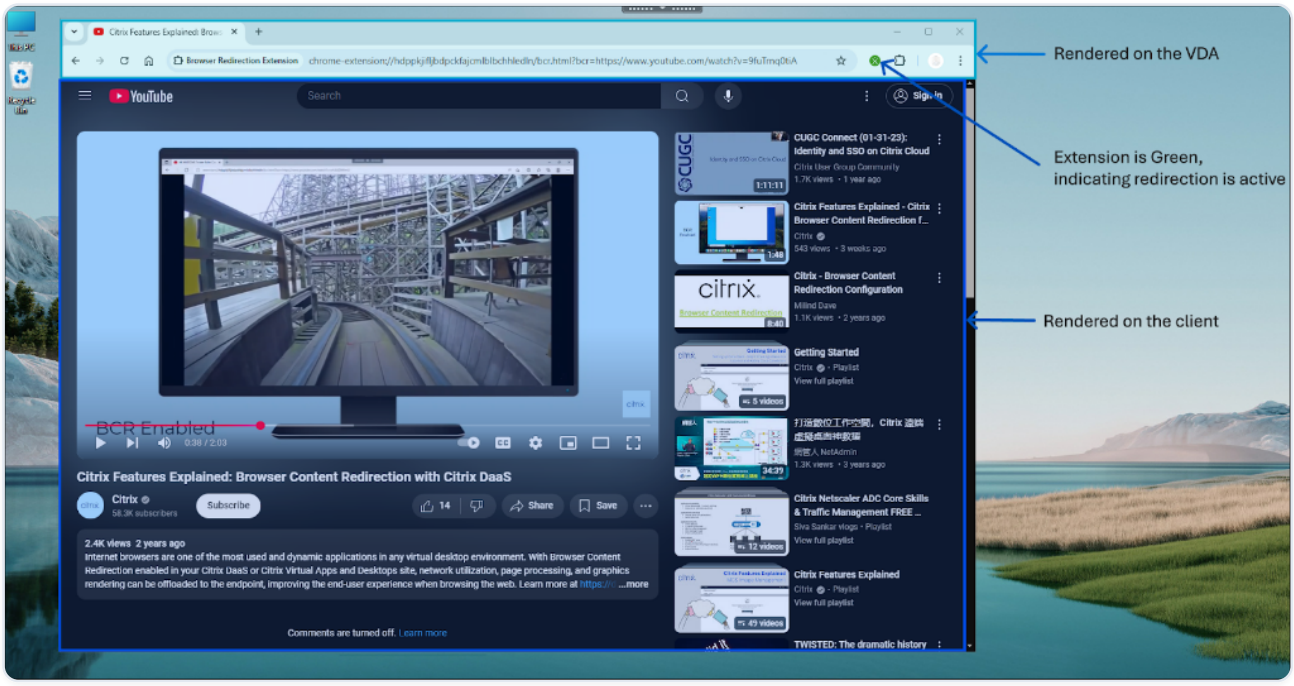
- MacOSの場合、ブラウザコンテンツリダイレクトパッケージはCitrix Workspace Appとは独立しており、常に最新バージョンです。そのため、このパッケージは指定された最小バージョンより上の複数のCWAバージョンと互換性があります。
- Citrix Workspace App Macへの依存性がないため、ブラウザコンテンツリダイレクトのバージョン番号はCitrix Workspace App Macのバージョンと一致しません。

- クライアント側ブラウザエンジンはCitrix Workspace App Macにはパッケージ化されていません。Citrix DownloadsからMac用のクライアント側をダウンロードしてインストールしてください。
- IntelおよびARMパッケージは別々です。そのため、MacOSエンドポイントに適したバージョンをインストールする必要があります。
- Mac版Citrix Workspace app 2511.1以降、モジュラーBCRコンポーネントはデフォルトでインストールされますが、Citrix Workspace Appにはパッケージ化されていません。これにより、Citrix Downloadsからコンポーネントを手動でダウンロードしてインストールする必要がなくなります。スタンドアロンのBCRパッケージは、通常のCitrix Workspace appリリースサイクル外で独立した更新や暫定的なパッチが必要な状況向けに公開されます。詳細については、Citrix Workspace App Mac documentationを参照してください。

設定手順

1. システム要件に従って、クライアント側およびサーバー側コンポーネントをインストールします。
    - 拡張機能の展開の詳細については、「拡張機能の展開」セクションを参照してください。
2. スタジオポリシーを構成します。
    - Web Studioポリシーは、さまざまなユースケースに合わせてブラウザコンテンツリダイレクトを構成するためのきめ細かな方法を提供します。
    - 基本ポリシーにより、管理者はブラウザコンテンツリダイレクトで許可/不許可にする必要があるURLを構成できます。
    - URLはワイルドカードで構成できます。
3. サポートされているWebブラウザを開き、許可されたURLに移動します。
    - 許可リストで一致が見つかった場合、Webサイトはクライアントにリダイレクトされます。
    - Citrix Workspaceアプリは、シームレスなエクスペリエンスのために、ビューポートをVDA側のブラウザにブレンドします。
4. 拡張機能のロゴの色は、コンテンツリダイレクトのステータスを示します。
    - 緑: アクティブで接続済み
    - 灰色: 現在のタブで非アクティブ/アイドル状態

- 赤: 破損/動作していません



注:

- HTML5ビデオリダイレクトとブラウザコンテンツリダイレクトは独立した機能です。この機能が動作するためにHTML5ビデオリダイレクトポリシーは必要ありません。ただし、Citrix HDX™ HTML5ビデオリダイレクトサービスはブラウザコンテンツリダイレクトに使用されます。
- すべての設定は、レジストリキーではなくWeb Studioを介して行うことをお勧めします。

構成オプション

ブラウザコンテンツリダイレクトは、さまざまな顧客環境のユースケースに合わせて構成するためのさまざまな方法を提供します。ポリシー設定の詳細については、ブラウザコンテンツリダイレクトポリシー設定を参照してください。

リダイレクトメカニズム

クライアントフェッチ クライアントレンダー

既定では、ブラウザコンテンツリダイレクトはこのモードで動作します。つまり、クライアント側のブラウザエンジンがWebページに直接アクセスします。これには、クライアントネットワークからWebページへの必要なアクセスが必要です。クライアントフェッチクライアントレンダーのシナ

リオでは、Citrix VDAからクライアントへネットワーク、CPU、RAMの使用量をすべてオフロードするため、ブラウザコンテンツリダイレクトを設定する最も最適な方法です。

ポリシー構成オプション

- ブラウザコンテンツリダイレクト：許可
- ブラウザコンテンツリダイレクトACL構成
    - リダイレクトする必要があるURLを指定します。デフォルトでは、YouTubeのみがリダイレクト用に構成されているWebサイトです。
- ブラウザコンテンツリダイレクトブロックリスト構成
    - 特定のURLまたはサブURLのリダイレクトをブロックするためのオプションの構成オプションです。最大限のカスタマイズを行うには、上記のオプションと組み合わせてこのオプションを活用してください。

サーバーフェッチ クライアントレンダー

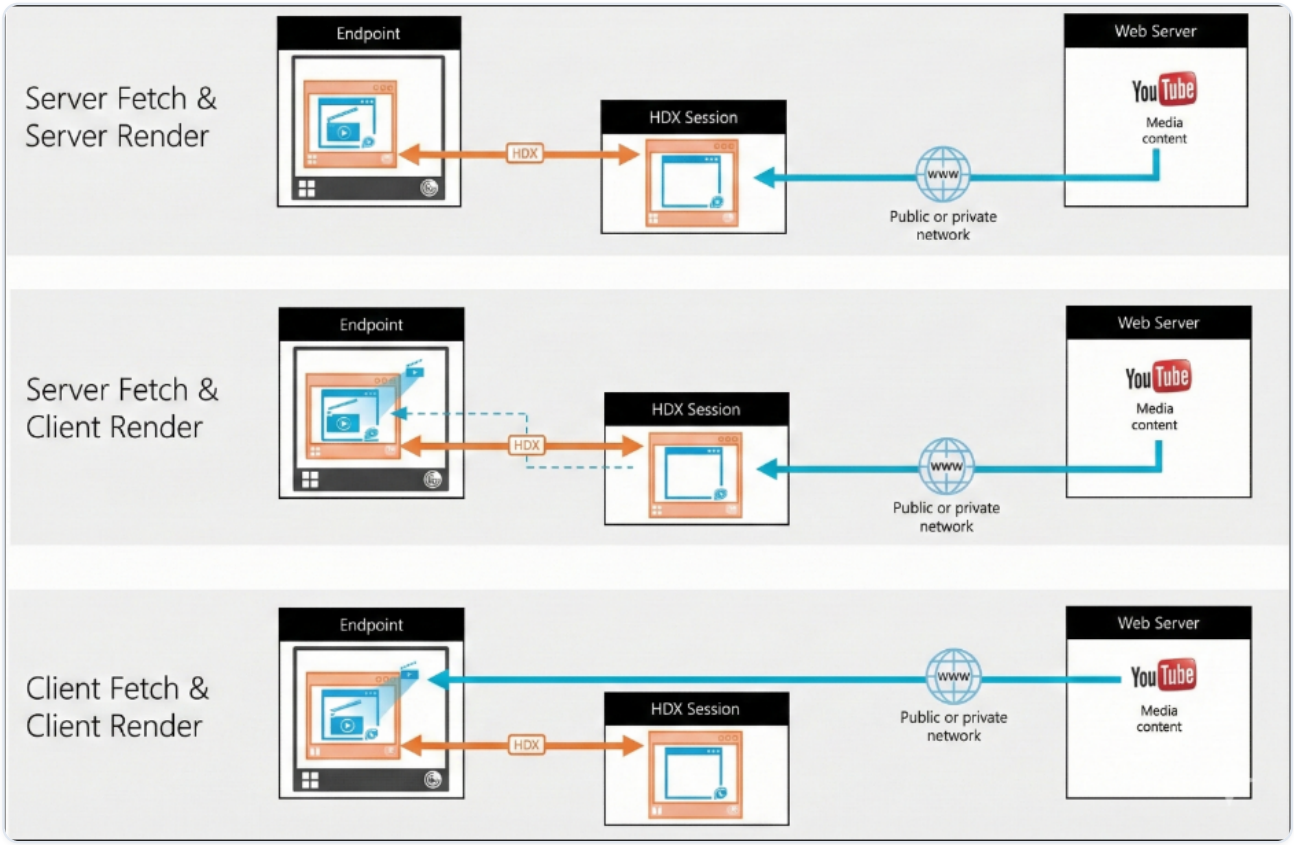
この場合、クライアント側のブラウザエンジンは仮想チャネルを使用してVDA経由でWebサーバーに接続し、コンテンツを取得します。このオプションは、クライアントがインターネットアクセスを持たない場合（シンクライアントなど）に役立ちます。VDAでのCPUとRAMの消費は少ないですが、ICA®仮想チャネルで帯域幅が消費されます。

このシナリオには3つの動作モードがあります。「プロキシ」という用語は、VDAがインターネットアクセスを取得するためにアクセスするプロキシデバイスを指します。

ポリシー構成オプション

- クライアントフェッチ クライアントレンダーのセクションで指定されたポリシーに加えて、以下を構成します
- ブラウザコンテンツリダイレクトプロキシ構成
    - **直接または透過:** サーバーフェッチクライアントレンダーを活用したい場合、およびVDAからWebページへの直接アクセスまたは透過プロキシアクセスがある場合に、これを構成します。ポリシーにはキーワード「DIRECT」を構成する必要があります。
    - **明示的プロキシ:** サーバーフェッチクライアントレンダリングを活用したい場合、およびVDAからウェブページへの明示的なプロキシアクセスがある場合に、これを構成します
    - **PACファイル:** PACファイルに依存している場合、VDA内のブラウザが指定されたURLの取得に適切なプロキシサーバーを自動的に選択できるように、これを構成します。

フォールバックモード



クライアントリダイレクトが失敗する場合があります。たとえば、クライアントマシンがインターネットに直接アクセスできない場合、エラー応答がVDAに戻されることがあります。そのような場合、VDA上のブラウザはページを再読み込みし、サーバー上でレンダリングできます。

認証の処理

認証サイト

Browser Content Redirectionの現在の実装では、リダイレクトメカニズムに関係なく、Browser Content Redirectionがウェブサイトへのログインを処理できるように、認証サイトを構成する必要があります。

例:

1. ブラウザコンテンツリダイレクトのACL構成で`<https://www.youtube.com/>`*のみが構成されており、認証サイトが構成されていない場合、BCRはウェブサイトにサインインする際にサーバー側レンダリングにフォールバックし、そこで処理を続行します。
2. この場合、BCRが認証サイトを処理できるように、必要に応じて`<https://www.accounts.google.com/>`*やIdPウェブサイトなどの他の認証サイトを構成します。各ウェブサイトのサインインは異なる動作をするため、リストに記載されていることを確認してください

3. 構成されている場合、BCRは認証を処理します。たとえば、クライアントフェッチクライアントレンダリングの場合、認証もクライアント側のブラウザエンジンから行われ、シームレスなサインインエクスペリエンスが提供されます。

ポリシー構成オプション

リダイレクトメカニズムのセクションで言及されているポリシーに加えて、Browser Content Redirection認証サイトポリシーを構成します。

> **注:**
>
> - BCRクライアント側ブラウザは、リダイレクトされたウィンドウが閉じられた後、クッキー（認証を含む）を永続化しません。これは、BCRウィンドウが完全に閉じられて再度開かれたときに、ウェブサイトに再ログインする必要があるという形で現れます。
> - BCRクライアント側ブラウザは、VDA側ブラウザからCookieを読み取りません。したがって、ユーザーのパーソナライゼーションと設定はVDAブラウザと同期しません。

統合Windows認証

ブラウザコンテンツリダイレクトは、VDAと同じドメイン内で統合Windows認証 (IWA) を使用して構成されている場合、ウェブサイトへのシームレスな認証方法を提供できます。

ポリシー構成オプション

- Browser Content Redirection統合Windows認証サポートポリシーを構成します。

シングルサインオンを有効にする前に、以下を完了してください。

- ホスト名から構築されたサービスプリンシパル名 (SPN) のチケットを発行するようにKerberosインフラストラクチャを構成します。例: HTTP/serverhostname.com。
- サーバーフェッチクライアントレンダリングの場合: サーバーフェッチモードでブラウザコンテンツリダイレクトを使用する場合、VDAでDNSが適切に構成されていることを確認してください。
- クライアントフェッチクライアントレンダリングの場合: クライアントフェッチモードでブラウザコンテンツリダイレクトを使用する場合、クライアントデバイスでDNSが適切に構成されており、オーバーレイからWebサーバーのIPアドレスへのTCP接続を許可していることを確認してください。

プロキシ認証

ブラウザコンテンツリダイレクトは、サーバーからコンテンツをフェッチする際に、Webプロキシへのシームレスな認証方法を提供できます。有効にすると、ブラウザコンテンツリダイレクトはKerberosサービスチケットを自動的に取得して使用し、プロキシで認証します。

ポリシー構成オプション

- ブラウザコンテンツリダイレクトのサーバーフェッチプロキシ認証ポリシーを構成します。

サーバーフェッチプロキシ認証ポリシーを有効にする前に、以下を完了してください。

- PACファイルを構成して、ダウンストリームWebプロキシ経由でトラフィックをルーティングし、プロキシがKerberos認証を使用するように設定する必要があります。

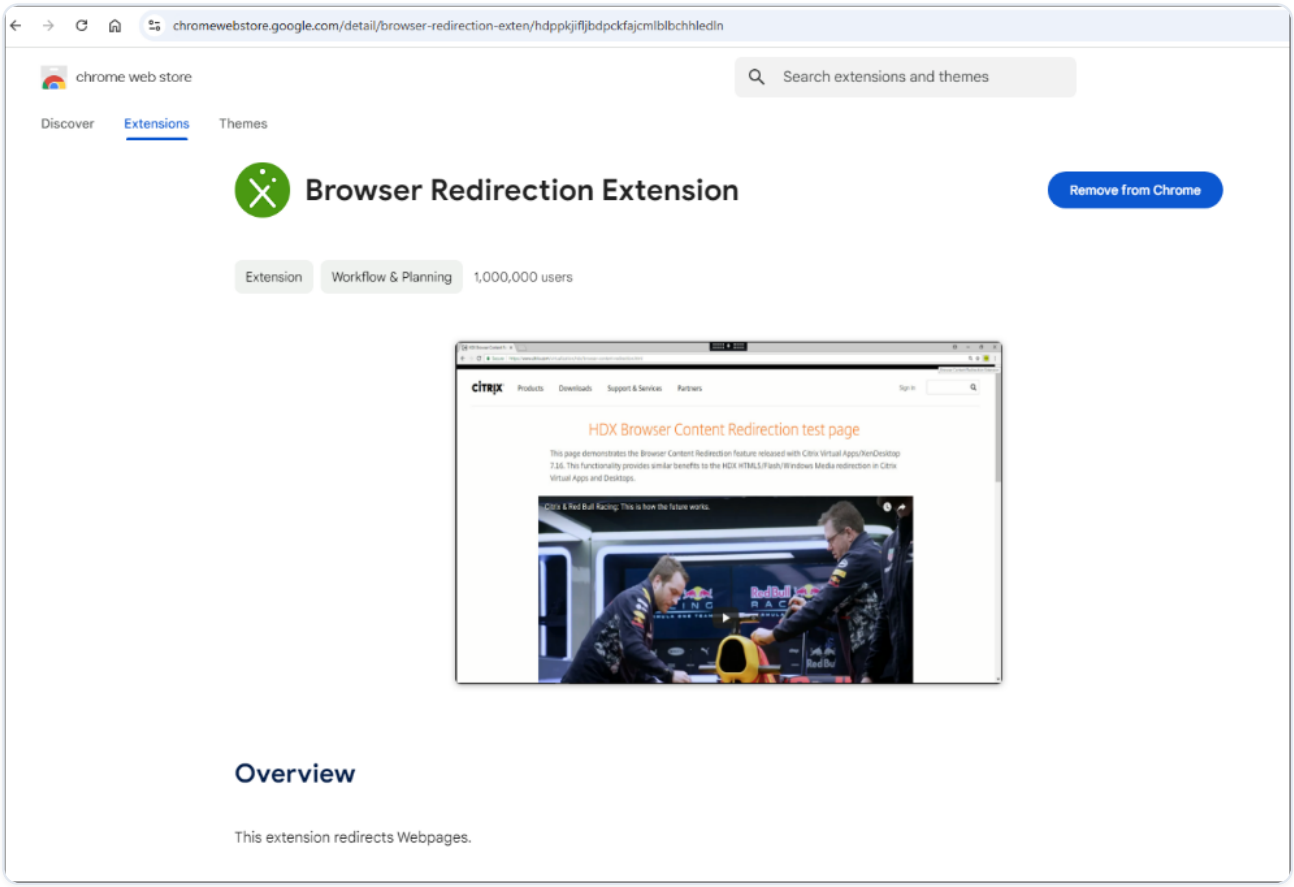
ユースケース

ブラウザコンテンツリダイレクト（BCR）は、特にリソースを大量に消費し、企業が頻繁にアクセスする幅広いWebサイトで利用できます。これには、YouTubeのようなビデオストリーミングプラットフォームが含まれ、レンダリングをエンドポイントデバイスにオフロードすることで、サーバー負荷を軽減し、コストを節約できるという大きなメリットがあります。さらに、BCRは、ビデオ会議やコラボレーションツール（Google Meet、Teams Web、Zoom Web）などのユニファイドコミュニケーションアプリケーションや、コンタクトセンターアプリケーション（Genesys Cloud）に最適であり、スムーズなパフォーマンスと強化されたユーザーエクスペリエンスを保証します。BCRを活用することで、企業はリソースを最適化し、さまざまなWebベースのアプリケーションで効率を向上させることができます。特定のWebサイトの構成方法については、CTX238236を参照してください。

拡張機能の展開

手動で展開

ブラウザリダイレクト拡張機能は、ChromeおよびEdgeのウェブストアで公開されています。この拡張機能は、VDA上のブラウザでのみ必要であり、クライアント側では必要ありません。拡張機能をインストールするには、Chrome / Edgeウェブストアに移動し、「Browser redirection extension」を検索して、それぞれのブラウザに追加します。この方法は個々のユーザー向けです。多数のユーザーに拡張機能を展開するには、グループポリシーを使用して拡張機能を展開します。



グループポリシーを使用した展開

前提条件

- **アクセス:** グループポリシーを構成するマシンまたはActive Directory環境で、管理者権限が必要です。
- **ADMXファイル:** お使いのChromeのバージョンに対応するGoogle Chrome ADMXファイル（管理用テンプレート）をダウンロードしてください。これらはGoogle Chrome Enterprise Helpページで入手できます。
- **Edgeテンプレート:** Microsoft Edge Enterprise landingページからMicrosoft Edgeの管理用テンプレート（ADMXファイル）をダウンロードしてください。
- **拡張機能IDと更新URL:** Citrix Browser Content Redirection拡張機能の拡張機能IDと更新URL。

GOOGLE CHROMEの手順

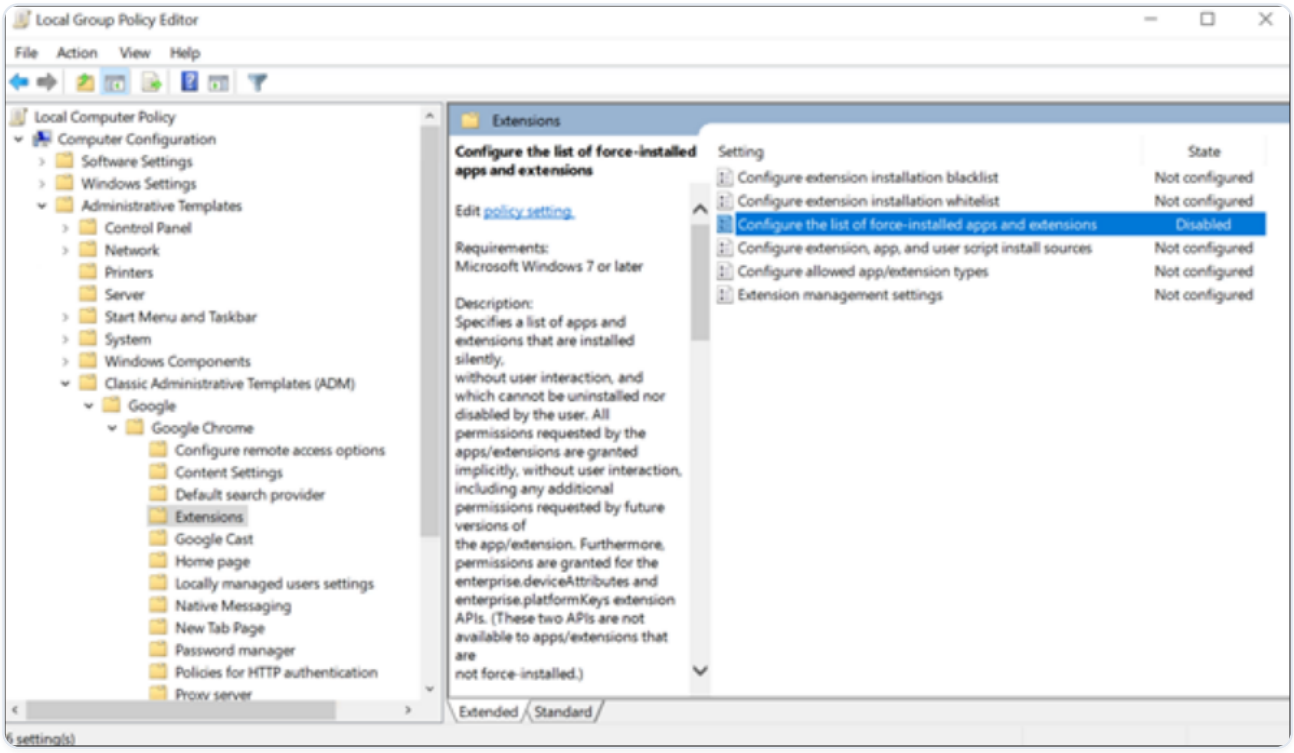
1. ADMXファイルのインポート:
    - Chrome ADMX ファイルを管理用テンプレートの中央ストアにコピーします。これは通常、ドメインコントローラー上の %SystemRoot%\PolicyDefinitions です。
2. グループポリシー管理を開く:
    - グループポリシー管理コンソール (gpmc.msc) を起動します。

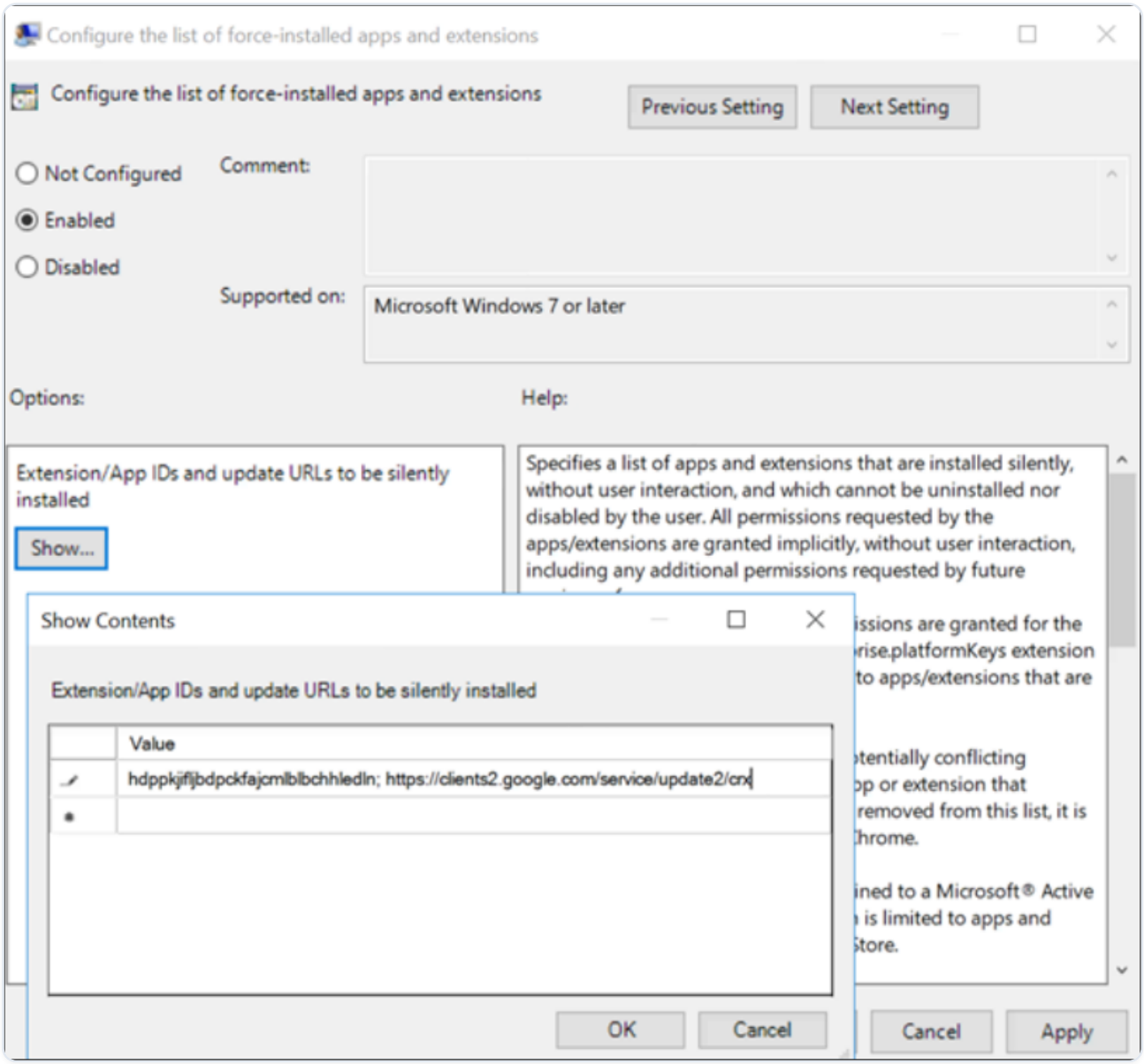
3. GPOを作成または編集します。
    - 新しいグループポリシーオブジェクト (GPO) を作成するか、拡張機能を展開するユーザーまたはコンピューターに適用される既存のGPOを編集します。
4. 拡張機能の設定に移動します。
    - GPOエディターで、以下に移動します。
        - ユーザーの構成 > 管理用テンプレート > 従来の管理用テンプレート (ADM) > Google > Google Chrome > 拡張機能
5. 「強制インストールするアプリと拡張機能のリストを構成する」を有効にします。
    - このポリシー設定をダブルクリックし、「有効」を選択します。
    - 「強制インストールするアプリと拡張機能のリストを構成する」設定が無効に設定されている場合、拡張機能はすべてのユーザーのChromeから自動的に削除されます。
6. 拡張機能IDと更新URLを追加します。
    - 「表示」ボタンをクリックします。
    - 拡張機能IDと更新URLを次の形式で入力します: <extension_id>;<update_url>
    - 値: hdppkjifljbdpckfajcmlblbchhledln; https://clients2.google.com/service/update2/crx (更新用URL)
7. GPOを適用する:
    - Active Directory構造内の適切な組織単位 (OU) にGPOをリンクします。
8. グループポリシーを更新する:
    - ターゲットマシンで、gpupdate /force を実行してポリシーをすぐに適用するか、ポリシーが自動的に更新されるのを待ちます。

MICROSOFT EDGE の手順

1. ADMXファイルをインポートする:
    - Edge ADMXファイルを、管理用テンプレートの中央ストア (%SystemRoot%\PolicyDefinitions) にコピーします。
2. グループポリシー管理を開く:
    - グループポリシー管理コンソール (gpmc.msc) を起動します。

3. GPOを作成または編集する:
    - 新しいGPOを作成するか、既存のGPOを編集します。
4. 拡張機能の設定に移動する:
    - GPOエディターで、以下に移動します:
        - コンピューターの構成 > ポリシー > 管理用テンプレート > Microsoft Edge > 拡張機能
5. 「サイレントインストールされる拡張機能を制御する」を有効にする:
    - このポリシー設定をダブルクリックし、「有効」を選択します。
6. 拡張機能IDと更新URLを追加します。
    - 「表示」ボタンをクリックします。
    - 拡張機能IDと更新URLを次の形式で入力します: <extension_id>;<update_url>
    - 値: hdppkjifljbdpckfajcmlblbchhledln; `<https://clients2.google.com/service/update2/crx>` (更新プログラムのダウンロード元URL)
7. GPOを適用します。
    - Active Directory構造内の適切な組織単位 (OU) にGPOをリンクします。
8. グループポリシーを更新:
    - ターゲットマシンで、gpupdate /forceを実行するか、自動更新を待ちます。


Local Group Policy Editor
File Action View Help
Local Computer Policy
Computer Configuration
Software Settings
Windows Settings
Administrative Templates
Control Panel
Network
Printers
Server
Start Menu and Taskbar
System
Windows Components
Classic Administrative Templates (ADM)
Google
Google Chrome
Configure remote access options
Content Settings
Default search provider
Extensions
Google Cast
Home page
Locally managed users settings
Native Messaging
New Tab Page
Password manager
Policies for HTTP authentication
Proxy server
Extensions
Configure the list of force-installed apps and extensions
Edit policy setting.
Requirements:
Microsoft Windows 7 or later
Description:
Specifies a list of apps and extensions that are installed silently,
without user interaction, and which cannot be uninstalled nor disabled by the user. All permissions requested by the apps/extensions are granted implicitly, without user interaction, including any additional permissions requested by future versions of
the app/extension. Furthermore, permissions are granted for the enterprise.deviceAttributes and enterprise.platformKeys extension APIs. (These two APIs are not available to apps/extensions that are
not force-installed.)
Setting
State
Configure extension installation blacklist
Not configured
Configure extension installation whitelist
Not configured
Configure the list of force-installed apps and extensions
Disabled
Configure extension, app, and user script install sources
Not configured
Configure allowed app/extension types
Not configured
Extension management settings
Not configured
Extended
Standard
6 setting(s)



トラブルシューティング

トラブルシューティング情報については、ナレッジセンターの記事「ブラウザコンテンツリダイレクトのトラブルシューティング方法」を参照してください。

ブラウザコンテンツリダイレクトの制限事項

サーバー側の制限事項 (VDA)

ブラウザコンテンツリダイレクトは、次のユースケースをサポートできません。記載されているシナリオまたは新しいシナリオで機能強化が必要な場合は、Citrix製品チームにお問い合わせください。

- ポップアップウィンドウは、ブラウザコンテンツリダイレクトではサポートされていません。
- セッションクッキーの永続性はサポートされていません。

- ブラウザコンテンツリダイレクトが使用されている場合、HTML5ビデオリダイレクトポリシーは無効にする必要があります。
- セッションの切断/再接続のシナリオでは、BCRが再度機能するためにVDAブラウザウィンドウを更新する必要があります。
- BCR化されたウィンドウからの印刷とファイルのダウンロードはサポートされていません。
- シークレットモードまたはプライベートブラウジングモードは、ブラウザコンテンツリダイレクトではサポートされていません。

クライアント側の制限 (CWA)

- ブラウザコンテンツリダイレクトは、ARMhfフレームワークではサポートされていません。
- BCRは、1つのブラウザで最大25個のリダイレクトされたタブ、2つのブラウザで合計30個のリダイレクトされたタブをサポートします。

HDX™ビデオ会議とWebカメラビデオ圧縮

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

> Webカメラは、HDX Webカメラビデオ圧縮またはHDXプラグアンドプレイ汎用USBリダイレクトを使用して、仮想セッション内で実行されているアプリケーションで使用できます。モードを切り替えるには、**Citrix Workspace™アプリ > 環境設定 > デバイス**を使用します。Citrixは、可能な限り常にHDX Webカメラビデオ圧縮を使用することをお勧めします。HDX汎用USBリダイレクトは、HDXビデオ圧縮とのアプリケーション互換性の問題がある場合、またはWebカメラの高度なネイティブ機能が必要な場合にのみ推奨されます。パフォーマンスを向上させるには、CitrixはVirtual Delivery Agentに少なくとも2つの仮想CPUを搭載することをお勧めします。

ユーザーがHDX Webカメラビデオ圧縮から切り替えるのを防ぐには、**ICA®ポリシー設定 > USBデバイスポリシー**設定の下にあるポリシー設定を使用して、USBデバイスリダイレクトを無効にします。Citrix Workspaceアプリのユーザーは、Desktop Viewerの［マイクとWebカメラ］設定で

［マイクまたはWebカメラを使用しない］を選択することにより、デフォルトの動作を上書きできます。

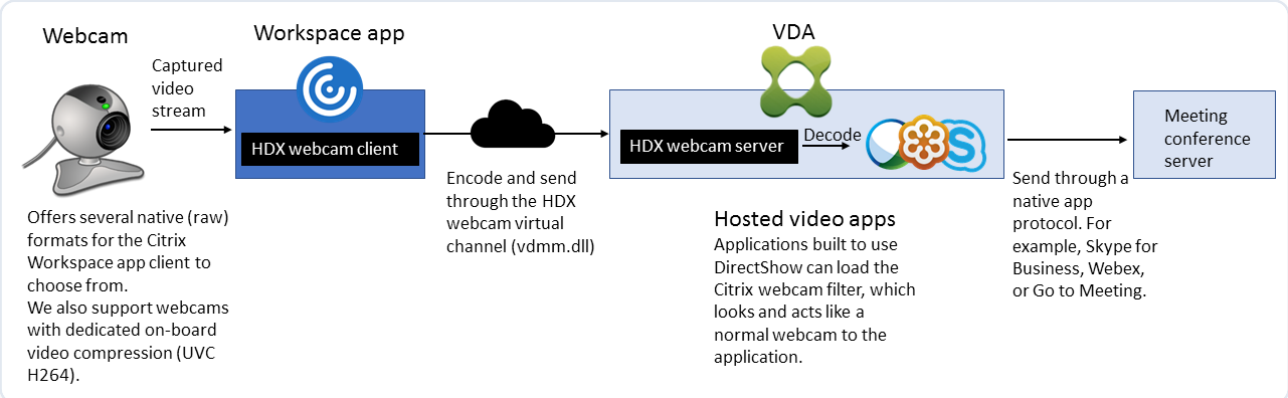
HDX Webカメラビデオ圧縮

HDX Webカメラビデオ圧縮は、**最適化された**Webカメラモードとも呼ばれます。この種類のWebカメラビデオ圧縮は、H.264ビデオを仮想セッションで実行されているビデオ会議アプリケーションに直接送信します。VDAリソースを最適化するために、HDX Webカメラ圧縮はWebカメラビデオのエンコード、トランスコード、デコードを行いません。この機能はデフォルトで有効になっています。

サーバーからビデオ会議アプリへの直接ビデオストリーミングを無効にするには、VDAでレジストリキーを0に設定します。詳しくは、レジストリで管理される機能の一覧にあるWebカメラビデオ圧縮を参照してください。

ビデオストリーミングリソースのデフォルト機能を無効にすると、HDX Webカメラビデオ圧縮は、クライアントオペレーティングシステムの一部であるマルチメディアフレームワークテクノロジーを使用して、キャプチャデバイスからのビデオをインターセプトし、トランスコードして圧縮します。キャプチャデバイスの製造元は、OSカーネルストリーミングアーキテクチャに接続するドライバーを提供します。

クライアントはWebカメラとの通信を処理します。その後、クライアントはビデオを適切に表示できるサーバーにのみ送信します。サーバーはWebカメラを直接処理しませんが、その統合により、デスクトップで同じエクスペリエンスが得られます。Workspaceアプリは、帯域幅を節約し、WANシナリオでの回復性を向上させるためにビデオを圧縮します。



HDX Webカメラビデオ圧縮には、**マルチメディア会議**ポリシーを有効にする必要があります。このポリシーはデフォルトで有効になっています。

Webカメラがハードウェアエンコードをサポートしている場合、HDXビデオ圧縮はデフォルトでハードウェアエンコードを使用します。ハードウェアエンコードは、ソフトウェアエンコードよりも多くの帯域幅を消費する可能性があります。ソフトウェア圧縮を強制するには、クライアン

トでレジストリキーを編集します。詳しくは、レジストリで管理される機能の一覧にあるWebカメラソフトウェア圧縮を参照してください。

HDX Webカメラビデオ圧縮の要件

HDX Webカメラビデオ圧縮は、Citrix Workspaceアプリの次のバージョンをサポートしています。

プラットフォーム	プロセッサ
Windows 用 Citrix Workspace アプリ	Citrix Workspaceアプリ for Windowsは、XenAppおよびXenDesktop 7.17以降で32ビットおよび64ビットアプリのWebカメラビデオ圧縮をサポートします。以前のバージョンでは、Citrix Workspaceアプリ for Windowsは32ビットアプリのみをサポートします。
Mac 用 Citrix Workspace アプリ	Citrix Workspaceアプリ for Mac 2006以降は、XenAppおよびXenDesktop 7.17以降で64ビットアプリのWebカメラビデオ圧縮をサポートします。以前のバージョンでは、Citrix Workspaceアプリ for Macは32ビットアプリのみをサポートします。
Linux 用 Citrix Workspace アプリ	Citrix Workspaceアプリ for Linuxは、仮想デスクトップ上で32ビットおよび64ビットの両方のアプリをサポートします。
Chrome 用 Citrix Workspace アプリ	一部のARM ChromebookはH.264エンコードをサポートしていないため、最適化されたHDX Webカメラビデオ圧縮を使用できるのは32ビットアプリのみです。

Media Foundationベースのビデオアプリケーションは、Windows 10以降およびWindows Server 2019以降でHDX Webカメラビデオ圧縮をサポートしています。詳しくは、Knowledge Centerの記事CTX132764を参照してください。

その他のユーザーデバイス要件:

- サウンドを生成するための適切なハードウェア。
- DirectShow互換のWebカメラ（Webカメラのデフォルト設定を使用）。ハードウェアエンコード対応のWebカメラは、クライアント側のCPU使用率を削減します。

- HDX Webカメラビデオ圧縮の場合、可能であればカメラメーカーから入手したWebカメラドライバーをクライアントにインストールします。デバイスドライバーのインストールはサーバー上では不要です。

Webカメラによってフレームレート、明るさ、コントラストのレベルが異なります。Webカメラのコントラストを調整すると、アップストリームトラフィックを大幅に削減できます。Citrixは、初期機能検証のために以下のWebカメラを使用しています:

- Microsoft LifeCam VXモデル（2000、3000、5000、7000）
- クリエイティブ ライブ！カム オプティア プロ
- ロジクール クイックカム メッセンジャー
- ロジクール C600、C920
- HP デラックス ウェブカメラ

優先ビデオフレームレートを調整するには、クライアントでレジストリキーを編集します。詳細については、レジストリで管理される機能のリストにあるWebcam video compression frame rateを参照してください。

高解像度Webカメラストリーミング

サーバー上のビデオ会議アプリケーションは、サポートされているフォーマットタイプに基づいてWebカメラのフォーマットと解像度を選択します。セッションが開始されると、クライアントはWebカメラ情報をサーバーに送信します。アプリケーションからWebカメラを選択します。Webカメラとビデオ会議アプリケーションが高解像度レンダリングをサポートしている場合、アプリケーションは高解像度を使用します。すべてのWebカメラ解像度をサポートしています。

この機能には、Citrix Workspaceアプリ for Windows バージョン1808以降、またはCitrix Receiver for Windows バージョン4.10以降が必要です。

レジストリキーを使用して、この機能を無効または有効にできます。詳細については、レジストリで管理される機能のリストにあるHigh-definition webcam streamingを参照してください。

メディアタイプネゴシエーションが失敗した場合、HDXはデフォルトのVGA解像度 (640 x 480ピクセル) にフォールバックします。クライアントのレジストリキーを使用して、デフォルトの解像度を構成できます。カメラが指定された解像度をサポートしていることを確認してください。詳細については、レジストリで管理される機能のリストにある高解像度Webカメラ解像度を参照してください。

HDX Webカメラビデオ圧縮は、プラグアンドプレイの汎用USBリダイレクトと比較して帯域幅を大幅に削減し、WAN接続でも良好に機能します。帯域幅を調整するには、クライアントでレジス

トリキーを設定します。詳細については、レジストリで管理される機能のリストにあるHigh-definition webcam bandwidthを参照してください。

ビット/秒単位で値を入力します。帯域幅を指定しない場合、ビデオ会議アプリケーションはデフォルトで350000 bpsを使用します。

HDXプラグアンドプレイ汎用USBリダイレクト

HDXプラグアンドプレイ汎用USBリダイレクト（アイソクロナス）は、**汎用**ウェブカメラモードとも呼ばれます。HDXプラグアンドプレイ汎用USBリダイレクトの利点は、シンクライアント/エンドポイントにドライバーをインストールする必要がないことです。USBスタックは仮想化されており、ローカルクライアントに接続するものはすべてリモートVMに送信されます。リモートデスクトップは、まるでネイティブに接続したかのように動作します。Windowsデスクトップは、ハードウェアとのすべてのやり取りを処理し、プラグアンドプレイロジックを実行して正しいドライバーを見つけます。ほとんどのウェブカメラは、ドライバーがサーバーに存在し、ICA経由で動作できる場合に機能します。汎用ウェブカメラモードは、ネットワーク経由でUSBプロトコルを使用して非圧縮ビデオを送信するため、はるかに多くの帯域幅（毎秒数メガビット）を使用します。

HTML5マルチメディアリダイレクト

HTML5マルチメディアリダイレクトは、HDX™ MediaStreamのマルチメディアリダイレクト機能を拡張し、HTML5オーディオおよびビデオに対応します。特にモバイルデバイスへのマルチメディアコンテンツのオンライン配信の増加により、ブラウザ業界は、オーディオとビデオを提示するためのより効率的な方法を開発してきました。

Flashは標準でしたが、プラグインが必要で、すべてのデバイスで動作せず、モバイルデバイスではバッテリー消費量が多くなります。YouTube、Netflix、およびMozilla、Google、Microsoftの新しいブラウザバージョンなどの企業は、HTML5に移行しており、これが新しい標準となっています。

HTML5ベースのマルチメディアには、独自のプラグインに比べて多くの利点があります。以下に例を挙げます。

- 企業に依存しない標準 (W3C)
- 簡素化されたデジタル著作権管理 (DRM) ワークフロー
- プラグインによって引き起こされるセキュリティ問題なしに、より優れたパフォーマンス

HTTPプログレッシブダウンロード

HTTPプログレッシブダウンロードは、HTML5をサポートするHTTPベースの擬似ストリーミング方式です。プログレッシブダウンロードでは、ブラウザはHTTP Webサーバーからダウンロード中に、単一のファイル（単一の品質でエンコードされたもの）を再生します。ビデオは受信時にドライブに保存され、ドライブから再生されます。ビデオを再視聴する場合、ブラウザはキャッシュからビデオを読み込むことができます。

プログレッシブダウンロードの例については、HTML5ビデオのリダイレクトテストページを参照してください。Webページ内のビデオ要素を検査し、HTML5ビデオタグ内のソース（mp4コンテナ形式）を見つけるには、ブラウザの開発者ツールを使用します。

HTML5とFlashの比較

機能	HTML5	フラッシュ
独自のプレーヤーが必要	いいえ	はい
モバイルデバイスで動作	はい	一部
異なるプラットフォームでの実行速度	高い	遅い
iOSでサポート	はい	いいえ
リソース使用量	少ない	多い
ロードが速い	はい	いいえ

要件

mp4形式のプログレッシブダウンロードのリダイレクトのみをサポートしています。WebMおよびDASH/HLSのようなアダプティブビットレートストリーミング技術はサポートしていません。

以下をサポートしており、ポリシーを使用してこれらを制御します。詳細については、「マルチメディアポリシー設定」を参照してください。

- サーバー側レンダリング
- サーバーフェッチクライアントレンダリング
- クライアント側フェッチとレンダリング

Citrix Workspace™アプリおよびCitrix Receiver™の最小バージョン:

- Windows用Citrix Workspaceアプリ 1808
- Windows用シトリックス レシーバー 4.5
- Linux用Citrix Workspaceアプリ 1808
- Linux用シトリックス レシーバー 13.5

最小VDAブラウザバージョン	WINDOWS オペレーティングシステム バージョン/ビルド/サービスパック
インターネットエクスプローラー 11.0	ウィンドウズ 10 x86 (1607 RS1) および x64 (1607 RS1); ウィンドウズ 7 x86 および x64; ウィンドウズ サーバー 2016 RTM 14393 (1607); ウィンドウズ サーバー 2012 R2
Firefox 47 証明書をFirefoxの証明書ストアに手動で追加するか、Windowsの信頼された証明書ストアから証明書を検索するようにFirefoxを設定します。詳細については、`https://wiki.mozilla.org/CA:AddRootToFirefox`を参照してください。	ウィンドウズ 10 x86 (1607 RS1) および x64 (1607 RS1); ウィンドウズ 7 x86 および x64; ウィンドウズ サーバー 2016 RTM 14393 (1607); ウィンドウズ サーバー 2012 R2
クローム 51	Windows 10 の x86 (1607 RS1) および x64 (1607 RS1) 版、Windows 7 の x86 および x64 版、Windows Server 2016 RTM 14393 (1607)、Windows Server 2012 R2

HTML5ビデオリダイレクトソリューションのコンポーネント

- **HdxVideo.js** - Webサイト上のビデオコマンドをインターセプトするJavaScriptフック。HdxVideo.jsは、セキュアWebSocket (SSL/TLS) を使用してWebSocketServiceと通信します。
- **WebSocket SSL証明書**
  - CA (ルート) の場合：**Citrix XenApp/XenDesktop HDX In-Product CA** (C = US; S = Florida; L = Fort Lauderdale; O = Citrix Systems, Inc.; OU = XenApp and XenDesktop Engineering; CN = Citrix XenApp and XenDesktop HDX In-Product CA) 場所: **証明書 (ローカルコンピューター) > 信頼されたルート証明機関 > 証明書**。
  - エンドエンティティ (リーフ) の場合：**Citrix XenApp/XenDesktop HDX Service** (C = US; S = Florida; L = Fort Lauderdale; O = Citrix Systems, Inc.; OU = XenApp and XenDesktop Engineering; CN = Citrix XenApp and XenDesktop HDX Service) 場所: **証明書 (ローカルコンピューター) > 個人 > 証明書**。

- **WebSocketService.exe** - ローカルシステムで実行され、SSL終端とユーザーセッションマッピングを実行します。127.0.0.1ポート9001でTLS Secure WebSocketがリッスンしています。
- **WebSocketAgent.exe** - ユーザーセッションで実行され、WebSocketServiceコマンドの指示に従ってビデオをレンダリングします。

HTML5ビデオのリダイレクトを有効にするにはどうすればよいですか?

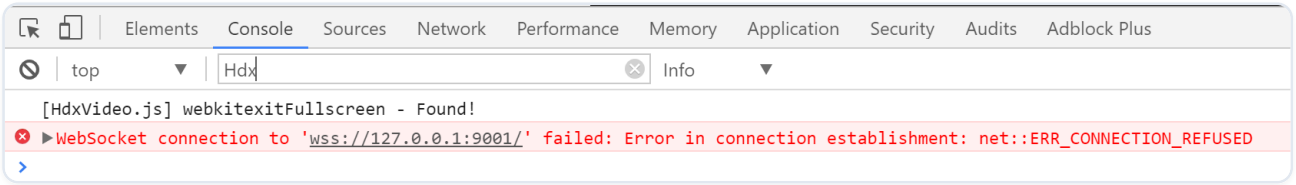
このリリースでは、この機能は管理されたWebページでのみ利用可能です。HTML5マルチメディアコンテンツが利用可能なWebページに、HdxVideo.js JavaScript (Citrix Virtual Apps and Desktopsインストールメディアに含まれています) を追加する必要があります。たとえば、社内トレーニングサイトのビデオなどです。

youtube.comのような、アダプティブビットレート技術（例：HTTPライブストリーミング（HLS）やHTTP経由のダイナミックアダプティブストリーミング（DASH））に基づいたウェブサイトはサポートされていません。

詳細については、「*マルチメディアポリシー設定*」を参照してください。

トラブルシューティングのヒント

ウェブページがHdxVideo.jsを実行しようとすると、エラーが発生する可能性があります。JavaScriptの読み込みに失敗すると、HTML5リダイレクトメカニズムも失敗します。ブラウザの開発者ツールウィンドウでコンソールを検査し、HdxVideo.jsに関連するエラーがないことを確認してください。例：



Microsoft Teams の最適化 (新規)

Citrix® は、VDI 環境で Microsoft Teams のオーディオとビデオを最適化する2つの方法をサポートしています。Citrix HDX™ Optimization と Microsoft の Teams 向け新規 VDI ソリューションです。Classic Teams はサポート終了 (EOL) となったため、このページで説明されている最適化アプローチは現在の Microsoft Teams クライアントに適用されます。

> **注記:**

Microsoft は、Windows エンドポイントにおける Microsoft Teams 向け WebRTC ベースの Citrix HDX Optimization の非推奨化を発表しました。2つのマイルストーンが適用されます。

- October 1, 2026 - サポート終了: Microsoft または Citrix による公式サポートは終了します。
- April 1, 2027 - 提供終了: WebRTC ベースの最適化は機能しなくなります。レガシー最適化のための Citrix Studio ポリシーは適用されなくなります。

お客様は、Teams 向け新規 VDI ソリューションへの移行をお勧めします。この変更は Windows エンドポイントのみに影響します。macOS、Linux、ChromeOS、および HTML5 エンドポイントは影響を受けません。詳細については、Microsoft Blog を参照してください。

最適化アプローチ

- **Citrix HDX Optimization (MTOP)**: Citrix と Microsoft の組み合わせソリューションで、Citrix が所有する仮想チャネル (CTXMTOP) を使用します。メディアオフロードは、Citrix Workspace™ アプリの `HdxRtcEngine` によって処理されます。このソリューションは、従来 MTOP と呼ばれています。
- **Teams 用の新しい VDI ソリューション**: Microsoft が所有および管理する新しい最適化で、Microsoft が所有する仮想チャネル (MSTEAMS、MSTEAM1、MSTEAM2) を使用します。Windows および Mac エンドポイントで利用できます。詳細については、Microsoft ドキュメントの Teams 用の新しい VDI ソリューション を参照してください。

主な違い

CITRIX HDX 最適化	TEAMS 向け新規 VDI ソリューション
最適化は Citrix と Microsoft の組み合わせソリューションであり、Citrix が所有する仮想チャネル (CTXMTOP) を使用します。	最適化ソリューションは Microsoft が所有および管理しており、Microsoft が所有する仮想チャネル (MSTEAMS、MSTEAM1、MSTEAM2) を使用します。
メディアオフロードは、Citrix Workspaceアプリに存在する`HdxRtcEngine`によって処理されます。	メディアオフロードは、WindowsおよびMacエンドポイント上のSlimCoreメディアエンジンによって処理されます。

CITRIX HDX 最適化	TEAMS 向け新規 VDI ソリューション
エンドポイントには、Citrix Workspaceアプリのインストール以外に追加コンポーネントは必要ありません。	追加コンポーネントである**Teams VDI Plugin**は、さまざまな方法でエンドポイントに展開する必要があります。このプラグインは、SlimCoreメディアエンジンのダウンロードと更新を管理します。
エンドポイントプラットフォーム（Windows、macOS、Linux、ChromeOS）で利用可能です。	エンドポイントプラットフォーム（WindowsおよびMac）で利用可能です。
新機能は、CitrixとMicrosoftが連携して管理します。	新機能はMicrosoftによって管理されます。ユーザーは、Citrix HDX最適化では利用できない一部の新機能にアクセスできます。
関連するコンポーネントに応じて、CitrixとMicrosoftの両方でサポートされます。お客様はCitrixまたはMicrosoftのいずれかにケースをオープンでき、必要に応じて適切なチームにリダイレクトされます。	Microsoftが所有およびサポートしています。Citrixは、Citrix Workspaceアプリ、仮想チャネル許可リスト、プラグイン展開メカニズムなど、関連するCitrixコンポーネントをサポートします。

相互運用性とローミング

Citrix HDX最適化とTeams向けの新VDIソリューションは並行して存在できますが、Teamsクライアントは一度にいずれか一方のみを使用します。

- 最適化は、Teamsアプリの起動時に次の順序で選択されます。Teams向けの新VDIソリューション、次にCitrix HDX最適化（WebRTC）、次に標準のオーディオ/ビデオリダイレクト。
- Teams向けの新VDIソリューションが失敗した場合、TeamsはWebRTCではなく、標準のオーディオ/ビデオリダイレクトに直接フォールバックします。選択を再実行し、適切な最適化を選択するには、Teamsアプリの再起動が必要です。
- エンドポイント間のローミングはシームレスであり、Teamsアプリの再起動は必要ありません。これには、ユーザーがTeams向けの新VDIソリューションをサポートするエンドポイントとサポートしないエンドポイントの間をローミングする場合も含まれます。

Citrix HDX™ 最適化

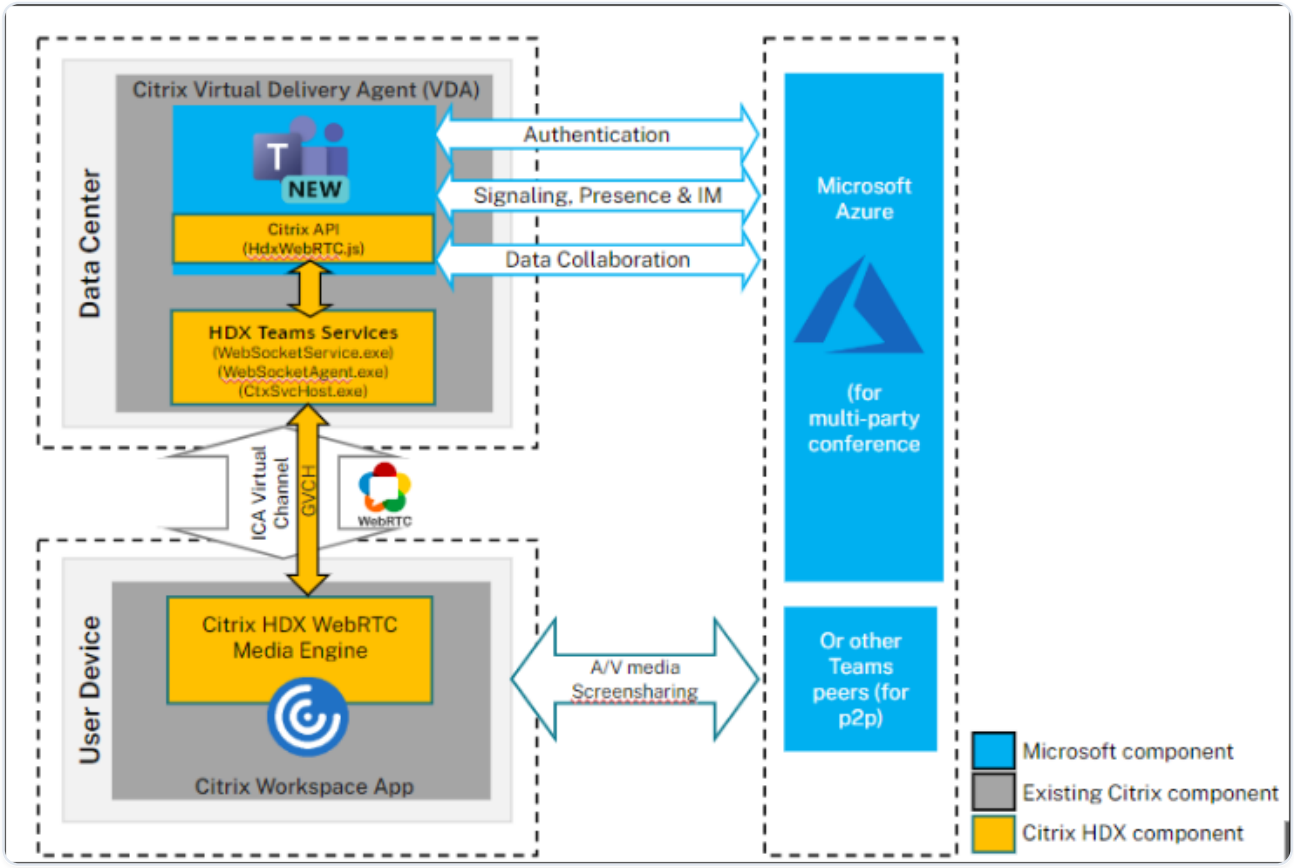
> **注:**

Microsoft は、Windows エンドポイントにおける Microsoft Teams 向け WebRTC ベースの HDX 最適化の非推奨化を発表しました。2つのマイルストーンが適用されます。

- October 1, 2026 - サポート終了: Microsoft または Citrix による公式サポートは終了します
- April 1, 2027 - 提供終了: Microsoft は、Windows エンドポイント向け HDX WebRTC 最適化の非推奨を発表しました。WebRTC ベースの最適化は機能しなくなります。レガシー最適化のための Citrix Studio ポリシーは適用されなくなります。

お客様は、Microsoft Teams 向けに新しい VDI ソリューション (SlimCore) への移行が推奨されます。この変更は Windows エンドポイントのみに影響し、macOS、Linux、ChromeOS、および HTML5 エンドポイントは影響を受けません。詳細については、Microsoft Blog を参照してください。

Citrix HDX (WebRTC 最適化) では、オフロードされたメディアの処理を担当するエンドポイント上のメディアエンジン (HdxRtcEngine) は Citrix Workspace™ アプリに組み込まれており、Citrix Workspace アプリをインストールすると、エンジンも自動的にインストールされます。



システム要件

このセクションでは、新しい Teams クライアントをサポートするために必要な最小バージョンと推奨バージョンを示します。最小バージョンでは、一部の重要なバグ修正や最新機能が利用できない場合があることに注意してください。最新の修正と機能で最高の体験を得るには、推奨バージョンを展開してください。

VDI オペレーティングシステム

詳細については、Microsoft ドキュメントに記載されている推奨事項を参照してください。

注:

- Windows Server 2016 はサポートされていません。Citrix は、それに応じてアップグレードを計画することをお勧めします。
- バージョンは頻繁に更新されるため、ここに記載されているバージョンはサポート終了となる可能性があります。したがって、異なるコンポーネントのサポートされているバージョンを使用していることを確認するために、Citrix Workspace app および Citrix Virtual Apps and Desktops の製品ライフサイクルページを参照してください。
- Citrix Virtual Apps and Desktops™ 1912 LTSR を使用している場合、2024 年 12 月にサポート終了となるため、Citrix はアップグレードを計画することをお勧めします。

仮想配信エージェント (VDA)

最小バージョン	推奨バージョン
1912 LTSR CU8+; 2203 LTSR (任意のCU); 2212 CR	2203 LTSR CU5+ (または) 2402 LTSR およびそれ以降のCRバージョン

Citrix Workspace アプリ

最小バージョン	推奨バージョン
Windows 2203 LTSR (最新の累積更新プログラム); Windows 2302 CR; Linux 2207; Mac 2302; Chrome/HTML5 2301	ウィンドウズ 2402 LTSR; ウィンドウズ 2405 CR; リナックス 2405; マック 2405; クローム OS/HTML5 2405

展開

1. VDI に新しい Teams クライアントをインストールします。詳細については、「VDI 用の新しい Teams を展開する」を参照してください。
2. 新しい Teams を最適化するために、VDA で次のレジストリキーを構成します。

   - **場所**: `HKLM\SOFTWARE\WOW6432Node\Citrix\WebSocketService`
   - **キー (REG_Multi_SZ)**: `ProcessWhitelist`
   - **値**: `msedgewebview2.exe`

   > **注:**
   >
   > Citrix Virtual Apps and Desktops 2402 LTSR (または) Citrix Virtual Apps and Desktops 2203 LTSR CU5+ 以降では、`msedgewebview2.exe` レジストリエントリはデフォルトで許可リストに含まれているため、手動で構成する必要はありません。

3. Microsoft Teamsリダイレクト ポリシーが有効になっていることを確認してください。このポリシーはデフォルトで有効になっています。
4. クライアント側で追加の構成は必要ありません。ウィザードの指示に従ってCitrix Workspace アプリをインストールしてください。

App レイヤリング

新しいMicrosoft Teamsはインストール方法が変更され、C:\Program Files\WindowsApps にインストールされるようになりました。この変更をサポートするには、App Layeringバージョン2403.2 以降を実行する必要があります。この修正を含むアップグレードディスクは、App Layeringダウンロード ページからダウンロードできます。

詳細については、App Layering ドキュメントを参照してください。

Citrix プロファイル管理

New Microsoft Teams のローミングを有効にする方法については、Citrix Profile Management のドキュメントを参照してください。Citrix Profile Management の現在の最小バージョンガイダンスは 2402 LTSR (または) 2203 LTSR CU5+ です。

ネットワークに関する考慮事項

New Teams のネットワーク要件は Classic Teams と変わりません。したがって、Classic Teams ドキュメントのネットワーク要件セクションを参照してください。

機能マトリックスとバージョンサポート

バージョンは頻繁に更新されるため、ここに記載されている一部の古いバージョンはサポート終了となる可能性があります。したがって、異なるコンポーネントのサポートされているバージョンを使用していることを確認するために、Citrix Workspace App および Citrix Virtual Apps and Desktops の製品ライフサイクルページを参照してください。

注:

- ここで言及されているバージョンは、特定の機能がサポートされる最小バージョン、または新しいTeamsがサポートされる最小バージョンのうち、いずれか高い方です。
- 最小バージョンセクションに記載されているCitrix Virtual Apps and Desktops 1912 LTSR CU8+は、2024年12月にサポート終了となるため、下記の表には記載されていません。ただし、それまでは引き続きサポート対象バージョンです。
- 最小Citrix Virtual Apps and Desktopsバージョンが `N/A` である機能は、VDA側からの変更を伴わなかったことを意味します。

機能	VDA (最小バージョン)	WINDOWS 用 CITRIX WORKSPACE アプリ (最小バージョン)	MAC 向け CITRIX WORKSPACE アプリ (最小バージョン)	LINUX 向け CITRIX WORKSPACE アプリ (最小バージョン)	CHROMEOS 用 CITRIX WORKSPACE アプリ (最小バージョン)
オーディオ/ビデオ (P2Pおよび会議)	2203 LTSR (任意の CU), 2212 CR	2203 LTSR 最新のCU, 2302 CR	2302	2207	2301
画面共有	2203 LTSR (任意の CU), 2212 CR	2203 LTSR 最新のCU, 2302 CR	2302	2207	2301
i. 画面インジケーターの赤い枠線	2203 LTSR (任意の	2203 LTSR 最新のCU, 2302 CR	2302	2207	いいえ

機能	VDA (最小バージョン)	WINDOWS 用 CITRIX WORKSPACE アプリ (最小バージョン)	MAC 向け CITRIX WORKSPACE アプリ (最小バージョン)	LINUX 向け CITRIX WORKSPACE アプリ (最小バージョン)	CHROMEOS 用 CITRIX WORKSPACE アプリ (最小バージョン)
	CU), 2212 CR				
ii. キャプチャを Desktop Viewerに制限	2203 LTSR (任意の CU), 2212 CR	2203 LTSR 最新CU、2302 CR	2302	2207	なし
iii. マルチモニター	2203 LTSR (任意の CU)、2212 CR	2203 LTSR 最新CU、2302 CR	2302	2207	なし
DTMF	N/A	2203 LTSR 最新CU、2302 CR	2302	2207	2301
プロキシサーバーのサポート	該当なし	2203 LTSR 最新CU、2302 CR	2302	2207	2305
アプリ共有	2203 LTSR (任意の CU)、2212 CR	2203 LTSR 最新CU、2302 CR	2302	2209	いいえ
ライブキャプション	該当なし	2203 LTSR 最新CU、2302 CR	2302	2207	2303
動的e911	該当なし	2203 LTSR 最新CU、2302 CR	2302	2207	2301

機能	VDA (最小バージョン)	WINDOWS 用 CITRIX WORKSPACE アプリ (最小バージョン)	MAC 向け CITRIX WORKSPACE アプリ (最小バージョン)	LINUX 向け CITRIX WORKSPACE アプリ (最小バージョン)	CHROMEOS 用 CITRIX WORKSPACE アプリ (最小バージョン)
コントロールを付与	該当なし	2203 LTSR 最新CU、2302 CR	2302	2207	いいえ
制御のリクエスト	N/A	2203 LTSR 最新 CU、2302 CR	2302	2207	2303
マルチウィンドウ	2203 LTSR (任意の CU)、2212 CR	2203 LTSR 最新 CU、2302 CR	2302	2207	2303
会議の文字起こし	2203 LTSR (任意の CU)、2212 CR	2203 LTSR 最新CU、2302 CR	2302	2207	2303
背景のぼかし	2203 LTSR (任意の CU)、2212 CR	2203 LTSR 最新CU、2302 CR	2302	2212	2303
画面共有 (アプリ保護機能付き)	2203 LTSR (任意の CU)、2212 CR	2402 LTSR, 2309.1 CR	2308	2311	いいえ
サイマルキャスト	2203 LTSR (任意の CU), 2212 CR	2402 LTSR, 2305 CR	2305	2305	2312

機能	VDA (最小バージョン)	WINDOWS 用 CITRIX WORKSPACE アプリ (最小バージョン)	MAC 向け CITRIX WORKSPACE アプリ (最小バージョン)	LINUX 向け CITRIX WORKSPACE アプリ (最小バージョン)	CHROMEOS 用 CITRIX WORKSPACE アプリ (最小バージョン)
セカンダリリンガー	2203 LTSR (任意の CU), 2212 CR	2402 LTSR, 2307.1 CR	2308	2308	2312
システムオーディオの共有	2203 LTSR (任意の CU), 2212 CR	2402 LTSR, 2403 CR	2405	2402	いいえ

トラブルシューティングとその他の考慮事項

新しいTeamsについては、CTX253754、Microsoft Teamsのトラブルシューティングを参照してください。新しいTeamsに関連する最新情報については、CTX585013を参照してください。

既知の制限事項

Citrix Workspaceアプリの制限事項

- HIDサポート - 通話の応答と終了はサポートされていません。音量の上げ下げはサポートされています。
- VDAでSnipping Toolを使用している間は、Microsoft Teamsのコンテンツのスクリーンショットを撮ることはできません。ただし、クライアント側でSnipping Toolを使用すると、コンテンツをキャプチャできます。
- システムオーディオ共有の制限事項
  - RAVEおよびBCRでリダイレクトされたアプリまたはタブで画面を共有している場合、この機能を使用してオーディオを共有することはできません。
  - この機能は公開デスクトップでのみサポートされています

VDAに関する制限事項

- 公開（シームレス）アプリケーションとしての新しいTeamsはサポートされていません

    - CVAD 2402 LTSR、2203 LTSR CU5以降で修正済み

- Citrix WorkspaceアプリのHigh DPI設定を「はい」に構成すると、リダイレクトされたビデオウィンドウがずれて表示されます。この制限は、モニターのDPIスケーリング係数が100%を超えて設定されている場合に発生します。
- Microsoft Teams 2.1は、一度に1つのWebカメラのリダイレクトのみをサポートします。ただし、シングルセッションVDAでは、複数のWebカメラのリダイレクトやプラグアンドプレイ（PnP）Webカメラのリダイレクトはサポートしていません。

Citrix WorkspaceアプリとVDAに関する制限

- 最適化された通話の音量は、クライアントマシンの音量バーを使用してのみ制御でき、VDA上では制御できません。

Microsoftからの制限の詳細については、VDIでサポートされていない機能を参照してください。

Teams向け新しいVDIソリューション

> **注:**
>
> Teams向け新しいVDIソリューションは現在、Citrix®上のWindowsおよびMacエンドポイントで一般提供されています。このソリューションには、最小限のMicrosoft Teamsバージョンが必要です。「システム要件」(#system-requirements)を参照してください。

> Teams向け新しいVDIソリューションでは、MicrosoftはCitrix Virtual Channel SDKを使用してカスタム仮想チャネルを構築します。エンドポイントでは、メディアは`HdxRtcEngine`ではなく、Microsoftメディアエンジン (SlimCore) にオフロードされます。カスタム仮想チャネルは、VDA上のTeamsとエンドポイント上のメディアエンジン間の通信を伝送します。

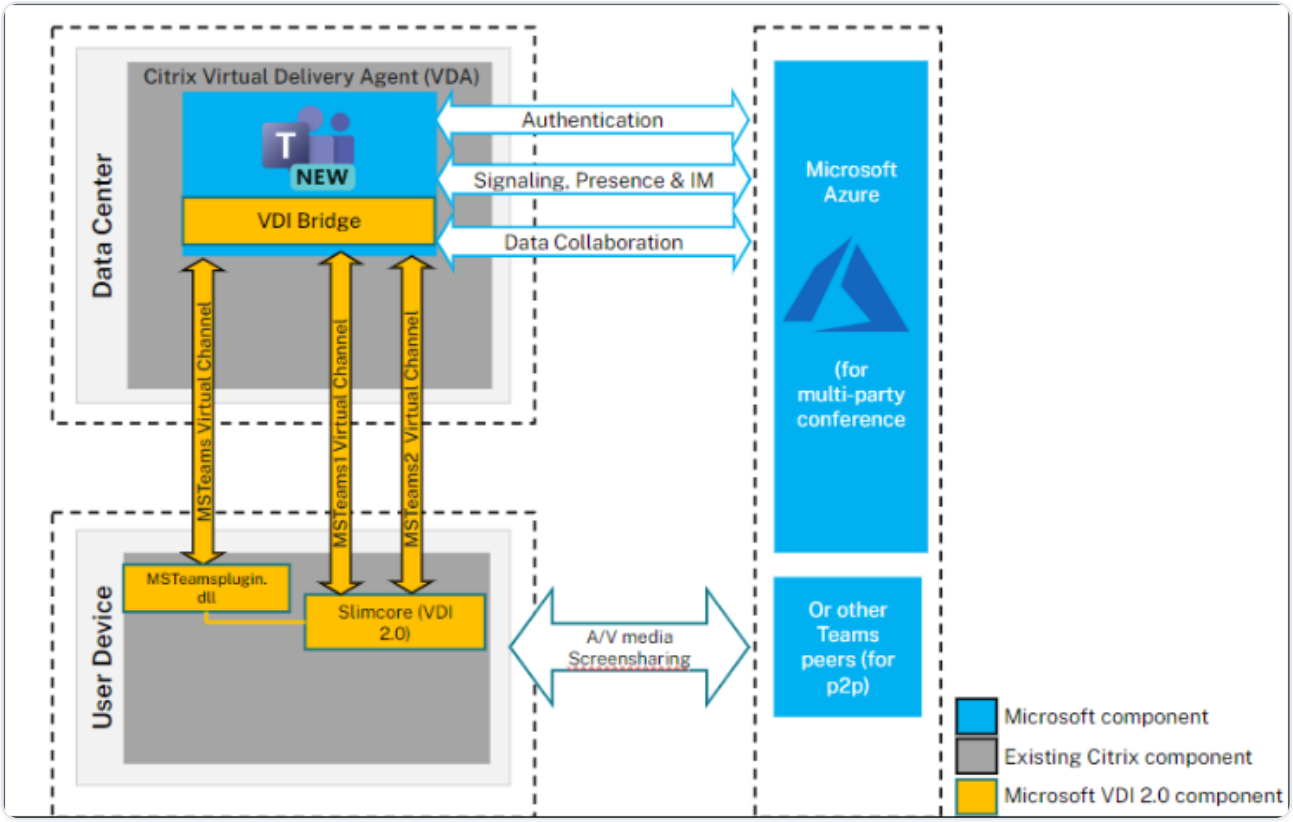
> **注:**
>
> Microsoftは、WindowsエンドポイントにおけるWebRTCベースのCitrix HDX™ Optimization for Microsoft Teamsの廃止を発表しました。2つのマイルストーンが適用されます。

> - October 1, 2026 - サポート終了: MicrosoftまたはCitrixによって公式にサポートされなくなります。

- April 1, 2027 - 提供終了: WebRTCベースの最適化は機能しなくなります。レガシー最適化用のCitrix Studioポリシーは適用されなくなります。

お客様は、Teams向け新しいVDIソリューションへの移行をお勧めします。この変更はWindowsエンドポイントのみに影響します。macOS、Linux、ChromeOS、およびHTML5エンドポイントは影響を受けません。詳細については、Microsoft Blogを参照してください。

このソリューションはMicrosoftが所有および管理しています。Citrixは、関連するCitrixコンポーネント（Citrix Workspace™アプリ、仮想チャネル許可リスト、およびこのページで説明されているプラグイン展開メカニズム）をサポートします。Microsoftが所有するアーキテクチャと詳細については、MicrosoftドキュメントのTeams向け新しいVDIソリューションを参照してください。



システム要件

このセクションでは、Teams向け新しいVDIソリューションをサポートするために必要な最小バージョンと推奨バージョンを一覧表示します。最小バージョンでは、一部の重要なバグ修正や最新機能が利用できない場合があります。最良のエクスペリエンスを得るには、推奨バージョンを展開してください。

バーチャル デリバリー エージェント (VDA)

注:

2203 LTSR CU2以前、または2303 CR以前のバージョンを使用している場合は、それらのバージョンの制限を理解し、アップグレードを計画するためにCTX682593を参照してください。

最小バージョン	推奨バージョン
2203 LTSR CU3; 2305 CR	2203 LTSR CU5以降; 2402 LTSRおよびそれ以降のCR

Windows版 Citrix Workspaceアプリ

最小バージョン	推奨バージョン
2203 LTSR (最新のCU); 2302 CR	2402 LTSR; 2405 CR以降

Mac向けCitrix Workspaceアプリ

最小バージョン	推奨バージョン
2508.10	2607 またはそれ以降

MacエンドポイントにはmacOS 14、15、または26が必要です。macOS 26には、Citrix Workspaceアプリ2511以降が必要です。Citrix Workspaceアプリ for Mac 2508.10では、プラグインを手動でインストールする必要があります。Citrix Workspaceアプリ、クライアントアプリ管理、または仮想チャネルプラグインマネージャーを介してプラグインをインストールするオプションは、Citrix Workspaceアプリ for Mac 2603から利用できます。

Microsoft Teamsの最小バージョン、エンドポイントOS要件、およびハードウェア要件については、Microsoftのドキュメントを参照してください。

コンポーネント

- 新しいTeams `vdiBridge`: Teamsにバンドルされているサーバー側仮想チャネルモジュール。

- カスタム仮想チャネル（VC）: Microsoft Teamsが所有するカスタムVC。
- プラグイン: クライアント側VC DLL。メディアエンジンのダウンロードとクリーンアップを担当します。
- メディアエンジン（SlimCore）: MicrosoftによってMSIXパッケージとして提供される、オペレーティングシステム固有のメディアエンジン。

展開

1. 前提条件に記載されているMicrosoft Teamsのバージョンがあることを確認してください。
2. Microsoft Teamsの仮想チャネルを許可するように、**仮想チャネル許可リスト**ポリシーを構成します。これらのチャネルにより、Teamsクライアントはクライアント側プラグインに接続できます。詳細については、「仮想チャネルのセキュリティ」を参照してください。

   このソリューションには、3つのカスタム仮想チャネルが必要です。`ms-teams.exe`実行可能ファイルとカスタム仮想チャネルを許可するには、ワイルドカードを使用します。

   ```
   MSTEAMS,C:\Program Files\WindowsApps\MSTeams*8wekyb3d8bbwe\ms-teams.exe

   MSTEAM1,C:\Program Files\WindowsApps\MSTeams*8wekyb3d8bbwe\ms-teams.exe

   MSTEAM2,C:\Program Files\WindowsApps\MSTeams*8wekyb3d8bbwe\ms-teams.exe
   ```

   注:

   - VDA 2603以降では、これら3つの仮想チャネルがデフォルトで許可されます。これらのバージョンでは、Studioポリシーの構成は不要です。
   - 仮想チャネル許可リストポリシーのワイルドカードは、CVAD 2203 LTSR CU2以降、またはCitrix Virtual Apps and Desktops™ 2206 CR以降で利用できます。
   - ポリシーを有効にするには、VDAマシンを再起動する必要があります。
   - MSTeamsのインストールパスはMSIXアプリケーションであるため変更されるため、ワイルドカードが必要です。上記に示されている正確な行を許可してください。

3. このソリューションは、Citrixポリシーではなく、Microsoft Teams側のポリシーによって制御されます。デフォルトで有効になっています。特定のユーザーグループに対して有効または無効にするには、Microsoftドキュメントを参照してください。

4. エンドポイントにTeamsプラグインを展開します。Teamsプラグインをインストールするオプションを参照してください。
5. メディアエンジンのステージングと登録、およびMSIXのインストールをブロックする可能性のあるグループポリシーについては、Microsoftのドキュメントを参照してください。

Teamsプラグインをインストールするオプション

インストール方法に関係なく、プラグインはエンドポイントのCitrix Workspaceアプリの場所に配置されます。

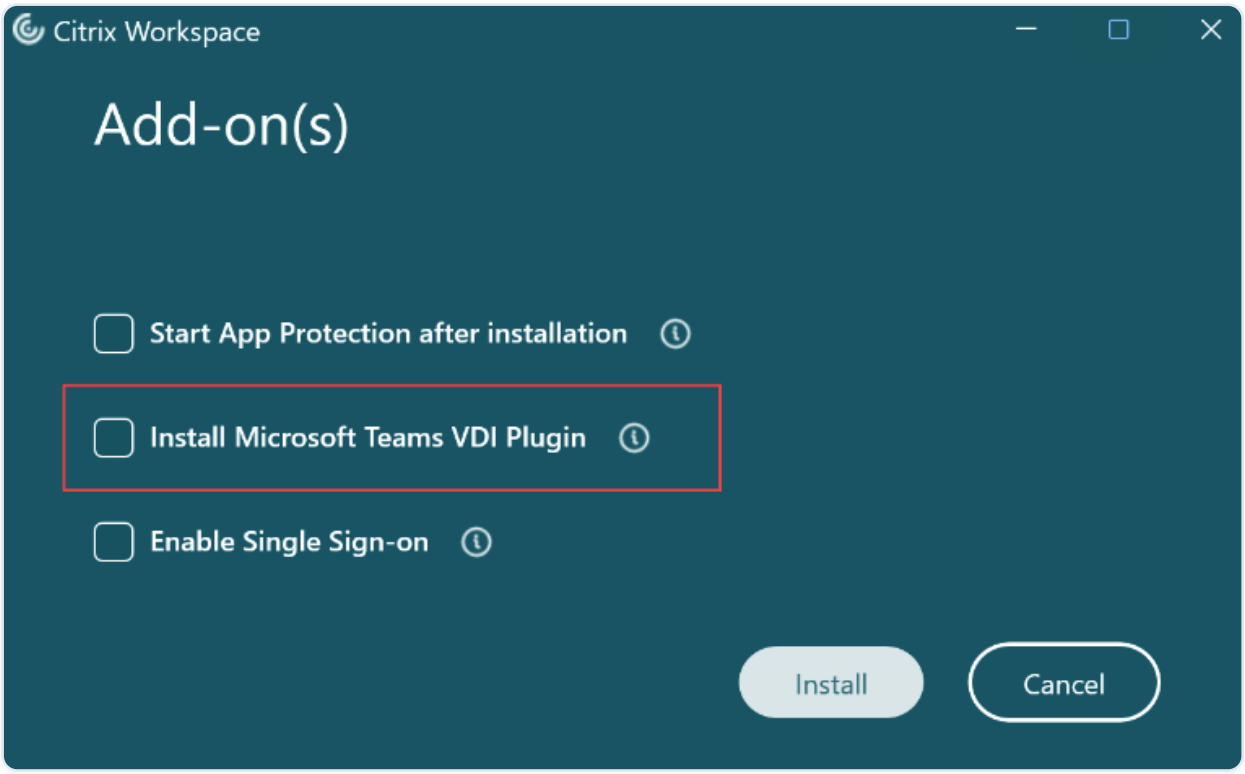
- Windows (`MsTeamsPluginCitrix.dll`): 64ビット `C:\Program Files (x86)\Citrix\ICA Client`; 32ビット `C:\Program Files\Citrix\ICA Client`
- Mac: `/Applications/Utilities/MsTeamsVdi.Plugin.app`

注:

- Windowsでは、仮想チャネルが正しく開くように、Citrix Workspaceアプリを管理者モードでインストールしてください。Citrix Workspaceアプリのユーザーごとのインストールはサポートされていません。
- Citrix WorkspaceアプリがMicrosoft Storeからインストールされている場合、Microsoft Teams VDIプラグインはサポートされません。
- エンドポイントにCitrix Workspaceアプリが見つからない場合、プラグインのインストールは停止します。
- Windowsでは、プラグインとCitrix Workspaceアプリは同じアーキテクチャである必要があります。32ビットのCitrix Workspaceアプリは64ビットのプラグインをロードできません。
- プラグインはアップグレードまたは修復できますが、ダウングレードはできません。また、アクティブなセッションがない場合にのみ可能です。

オプション1：Citrix Workspaceアプリのインストール経由

- **Windows:** 新規インストールまたは手動アップグレード中に、**アドオン**ページで**Microsoft Teams VDIプラグインのインストール**を選択します。Citrix Workspaceアプリ for Windows 2508以降では、このオプションはデフォルトで選択されています。インストールをスキップするには、このチェックを外してください。アップグレード時には、以前の選択が記憶されます。



コマンドラインから`/InstallMSTeamsPlugin`スイッチを使用してインストールすることもできます。たとえば、`CitrixWorkspaceApp.exe /InstallMSTeamsPlugin=Y`はプラグインをインストールし、`/InstallMSTeamsPlugin=N`はインストールを防止します。

新規インストールの場合は、Citrix Workspaceアプリ for Windows 2402 LTSRが最小要件です。インプレースアップグレードの場合は、Citrix Workspaceアプリ for Windows 2405 CRが最小要件です。詳細については、「サードパーティ製プラグインのインストール」を参照してください。

- **Mac:** Citrix Workspaceアプリのインストール中にプラグインをインストールするオプションは、Citrix Workspaceアプリ for Mac 2603以降で利用可能であり、ユーザーによる操作が必要です。Citrix Workspaceアプリ for Mac 2607では、プラグインがデフォルトで自動的にインストールされます。Citrix Workspaceアプリ for Mac 2508.10では、プラグインを手動でインストールしてください。オプション2: プラグインを直接ダウンロードするを参照してください。

オプション2: プラグインを直接ダウンロードする

- **Windows:** MSIをダウンロードし、SCCMやIntuneなどのツールを使用して、サポートされている任意のCitrix Workspaceアプリのバージョンに展開します。
  - 32ビット版Citrix Workspaceアプリ：aka.ms/plugin
  - 64ビット版Citrix Workspaceアプリ：aka.ms/plugin_x64
  - ArmベースのCitrix Workspaceアプリ：aka.ms/plugin_arm64

- **Mac:** aka.ms/macpluginからプラグインをダウンロードし、JAMFなどのツールを使用して展開します。

オプション3：クライアントアプリ管理（旧Global App Configuration service）

Client App Management（旧Global App Configuration service、またはGACS）は、管理対象および非管理対象のエンドポイントのアプリ設定を管理し、エンドポイント全体にTeamsプラグインを展開できます。Macでは、Citrix Workspaceアプリ for Mac 2603以降が必要です。「Microsoft Teams VDIプラグインの管理」を参照してください。

オプション4: 仮想チャネルプラグインマネージャー

仮想チャネルプラグインマネージャーは、New VDI solution for Teamsを含む、エンドポイントコンポーネントを必要とするアプリケーションのために、クライアントエンドポイント全体にプラグインを展開します。VDAで実行されているアプリケーションを検出し、ユーザーにエンドポイントへのプラグインのインストールを促します。管理者はBYODシナリオでこれを使用できます。Macでは、Citrix Workspaceアプリ for Mac 2603以降が必要です。「仮想チャネルプラグインマネージャー」を参照してください。

プラグインの更新シナリオ

プラグインがオプション1、3、または4を通じてインストールされている場合、CitrixはTeamsプラグインの更新をシームレスに処理します。プラグインが手動でインストールされている場合 (オプション2)、Citrixは更新を処理しません。

- プラグインの自動更新のために、Citrix Workspaceアプリの自動更新がオンになっていることを確認してください。
- 少なくともCitrix Workspaceアプリ for Windows 2405以降であることを確認してください。Citrix Workspaceアプリ for Windows 2508以降では、Citrix Workspaceアプリが自動更新されると、プラグインが自動的にインストールされます。
- Citrixはプラグインのアンインストールを処理しません。必要に応じて、プラグインを個別にアンインストールしてください。

> **注:**
>
> CitrixはTeamsプラグインの更新を処理しますが、メディアエンジンは処理しません。Microsoftがメディアエンジンを提供し、更新します。

Citrix公開アプリとしてのTeams

Citrix Virtual Appsアプリケーションとして公開されたTeamsは、必要なすべてのコンポーネントが最小バージョンを満たしている場合、このソリューションで最適化できます。必要なバージョンと既知の制限については、Microsoftドキュメントを参照してください。

相互運用性とローミング

Teams向けNew VDIソリューションとCitrix HDX最適化がどのように相互運用され、ローミングがどのように動作するかについては、Microsoft Teamsの最適化を参照してください。

ネットワークに関する考慮事項

Microsoftドキュメントのネットワークに関する考慮事項を参照してください。

機能サポート

機能セットと実装はMicrosoftが所有しています。Microsoftドキュメントの機能リストを参照してください。

トラブルシューティング

Microsoft Teamsクライアントは最適化ステータスを報告し、最適化に失敗した場合はエラーコードを報告します。これらのステータスインジケーターとエラーコードはMicrosoftによって定義されています。完全なリストとエンドツーエンドのトラブルシューティングについては、Microsoftドキュメントの Troubleshooting the New VDI solution for Teamsを参照してください。

Citrix Monitorは、このソリューションの最適化状態を可視化します。セッションの詳細では、セッショントポロジビューに、アプリケーションが最適化されているかどうか、およびプラグインマネージャー、プラグインとそのバージョン、仮想チャネルの状態、仮想チャネル許可リストのステータスなど、不足しているコンポーネントが示されます。詳細については、リアルタイム通信最適化の可視性を参照してください。

一部のMicrosoftエラーコードは、Citrix側の構成を示しています。一般的なCitrixの確認事項：

- Teamsクライアントがカスタム仮想チャネルがブロックされていると報告した場合（Microsoftエラー2003）、仮想チャネル許可リストにMSTEAMS、MSTEAM1、およびMSTEAM2が含まれていることを確認してください。
- Teamsクライアントがプラグインが検出されないと報告した場合（Microsoftエラー2000）、プラグインがインストールされ、ロードされていることを確認してください。Process Explorerで `wfica32.exe` を選択し、下部ペインを表示して、DLLタブで `MsTeamsPluginCitrix.dll` を確認します。

- Teamsクライアントがサポートされていないバージョンを報告した場合（Microsoftエラー2004）、サポートされているバージョンにアップグレードしてください。System requirementsを参照してください。

既知の制限事項

機能と実装はMicrosoftが所有しています。Microsoftのドキュメントで既知の問題を参照してください。

Microsoft Teamsの最適化 (クラシック)

Microsoft Teamsの監視、トラブルシューティング、サポート

Teamsの監視

このセクションでは、HDX を使用した Microsoft Teams の最適化を監視するためのガイドラインを提供します。 最適化モードで実行しており、`HdxRtcEngine.exe` がクライアントマシンで実行されている場合、VDA 上で `WebSocketAgent.exe` と呼ばれるプロセスがセッションで実行されています。Director の **アクティビティマネージャー** を使用してアプリケーションを確認します。

アクティビティマネージャーでTeamsを監視](/en-us/citrix-virtual-apps-desktops/2503/media/teams-activity-manager.png)

Microsoft Teams の最適化ステータスは、Director > **ユーザーの詳細**ページ > **セッションの詳細**パネル > **MS Teams の最適化**フィールドで確認できます。Microsoft Teams が最適化されていることは、クリアなオーディオとビデオなど、より良いユーザーエクスペリエンスのために不可欠です。この機能は、VDA バージョン 2311 以降で利用可能です。サポートされている Citrix Workspace™ アプリのバージョンは、「Microsoft Teams の最適化」に記載されています。Director は、Microsoft Teams が公開アプリケーションとして、または公開デスクトップ内で実行されている場合にのみ、Microsoft Teams の最適化ステータスを表示します。 詳細については、「Microsoft Teams の最適化ステータス」(/ja-jp/citrix-virtual-apps-desktops/2503/director/troubleshoot-deployments/user-issues#microsoft-teams-optimization-status) を参照してください。

VDA バージョン 1912 以降では、Citrix HDX Monitor (バージョン 3.11 以降) を使用してアクティブな Teams 通話を監視できます。Citrix Virtual Apps and Desktops 製品 ISO には、フォルダー `layout\image-full\Support\HDX Monitor` に最新の `hdxmonitor.msi` が含まれています。VDA バージョン 1912 以降では、Citrix HDX Monitor (バージョン 3.11 以降) を使用してアクティブな Microsoft Teams 通話を監視できます。Citrix Virtual Apps and Desktops 製品 ISO には、フォルダー `layout\image-full\Support\HDX Monitor` に最新の `hdxmonitor.msi` が含まれています。

詳細については、Knowledge Center の記事 CTX253754 の「*監視*」を参照してください。

トラブルシューティング

このセクションでは、Microsoft Teams の最適化を使用する際に発生する可能性のある問題に対するトラブルシューティングのヒントを提供します。詳細については、CTX253754 を参照してください。

バーチャル デリバリー エージェント上

BCR_x64.msi によって 4 つのサービスがインストールされます。そのうち 2 つのみが、VDA での Microsoft Teams リダイレクトを担当します。

ブラウザコンテンツリダイレクトによってインストールされる4つのサービス (/en-us/citrix-virtual-apps-desktops/2503/media/team-services.png)

- **Citrix HDX Teams リダイレクトサービス** は、Microsoft Teams で使用される仮想チャネルを確立します。このサービスは CtxSvcHost.exe に依存しています。
- **Citrix HDX HTML5 ビデオリダイレクトサービス** は、127.0.0.1:9002 TCP でリッスンする WebSocketService.exe として実行されます。WebSocketService.exe は主に 2 つの機能を実行します。

  i. **セキュアな WebSocket の TLS 終端** は、Microsoft Teams アプリ内のコンポーネントである vdiCitrixPeerConnection.js からセキュアな WebSocket 接続を受信します。Process Monitor で追跡できます。証明書の詳細については、セクション (TLS および HTML5 ビデオリダイレクト、ブラウザコンテンツリダイレクト) を参照してください。

  一部のアンチウイルスおよびデスクトップセキュリティソフトウェアは、`WebSocketService.exe`とその証明書の適切な機能に干渉します。Citrix HDX HTML5ビデオリダイレクトサービスが`services.msc`コンソールで実行されている場合でも、netstatで確認すると、localhost `127.0.0.1:9002` TCPソケットはリスニングモードになっていません。サービスを再起動しようとすると、ハングアップします（「停止中…」）。`WebSocketService.exe`プロセスに適切な除外を適用してください。

  「プロセスモニター」(/en-us/citrix-virtual-apps-desktops/2503/media/team-process-monitor.png)

  ii. **ユーザーセッションマッピング。** Microsoft Teamsアプリケーションが起動すると、WebSocketService.exeはVDAのユーザーセッションでWebSocketAgent.exeプロセスを開始します。WebSocketService.exeは、LocalSystemアカウントとしてセッション0で実行されます。

「WebSocketAgent.exeサービス」(/en-us/citrix-virtual-apps-desktops/2503/media/websocketservice-websocketagent.png)

VDAでWebSocketService.exeサービスがアクティブなリッスン状態にあるかどうかを確認するには、`netstat`を使用できます。

昇格されたコマンドプロンプトウィンドウから`netstat -anob -p tcp`を実行します。

```
 TCP    127.0.0.1:9001         0.0.0.0:0              LISTENING       11740
[WebSocketService.exe]
 TCP    127.0.0.1:9002         0.0.0.0:0              LISTENING       11740
[WebSocketService.exe]
```

接続が成功すると、状態はESTABLISHEDに変わります。

```
 TCP    127.0.0.1:9002         127.0.0.1:58069        ESTABLISHED     8096
[WebSocketService.exe]
 TCP    127.0.0.1:58069        127.0.0.1:9002         ESTABLISHED     748
[Teams.exe]
```

重要：

WebSocketService.exeは、127.0.0.1:9001と127.0.0.1:9002の2つのTCPソケットでリッスンします。ポート9001は、ブラウザコンテンツリダイレクトとHTML5ビデオリダイレクトに使用されます。ポート9002は、Microsoft Teamsリダイレクトに使用されます。Teams.exeとWebSocketService.exe間の直接通信を妨げる可能性のあるプロキシ構成がVDAのWindows OSにないことを確認してください。Internet Explorer 11で明示的なプロキシ（**インターネットオプション > 接続 > LAN の設定 > プロキシサーバー**）を構成すると、接続が割り当てられたプロキシサーバーを経由する場合があります。手動および明示的なプロキシ設定を使用する場合は、**ローカルアドレスにはプロキシサーバーを使用しない**がチェックされていることを確認してください。

サービスの位置と説明

サービス	WINDOWS SERVER OSでの実行可能ファイルへのパス	ログオンユーザー	説明
Citrix HTML5ビデオリダイレクトサービス	"C:\Program Files (x86)\Citrix\System32\WebSocketService.exe" /service	ローカルシステムアカウント	仮想デスクトップとエンドポイントデバイス間でメディアリダイレクトを実行するために必要な初期

サービス	WINDOWS SERVER OSでの実行可能ファイルへのパス	ログオンユーザー	説明
			フレームワークを、複数のHDXマルチメディアサービスに提供します。
Citrix HDXブラウザリダイレクトサービス	"C:\Program Files (x86)\Citrix\System32\CtxSvcHost.exe" -g BrowserRedirSvcs	このアカウント (ローカルサービス)	エンドポイントデバイスと仮想デスクトップ間でブラウザコンテンツリダイレクトを提供します。
Citrixポート転送サービス	"C:\Program Files (x86)\Citrix\System32\CtxSvcHost.exe" -g PortFwdSvcs	このアカウント (ローカルサービス)	ブラウザコンテンツリダイレクトのために、エンドポイントデバイスと仮想デスクトップ間でポート転送を提供します。
Citrix HDX Teamsリダイレクトサービス	"C:\Program Files (x86)\Citrix\System32\CtxSvcHost.exe" -g TeamsSvcs	ローカルシステムアカウント	エンドポイントデバイスと仮想デスクトップ間のMicrosoft Teamsリダイレクトを提供します。

シトリックス ワークスペース アプリ

ユーザーのエンドポイントでは、Windows版Citrix WorkspaceアプリがHdxTeams.exeまたはHdxRtcEngine.exeという新しいサービスをインスタンス化します。これは、VDAでMicrosoft Teamsが起動し、ユーザーがセルフプレビューで周辺機器を呼び出したりアクセスしようとしたときに実行されます。このサービスが表示されない場合は、以下を確認してください。

1. Windows版Workspaceアプリバージョン1905以降がインストールされていることを確認してください。WorkspaceアプリのインストールパスにHdxTeams.exeまたはHdxRtcEngine.exeとwebrpc.dllバイナリが表示されますか？
2. ステップ1を検証した場合は、HdxTeams.exeまたはHdxRtcEngine.exeが起動しているかどうかを確認するために、以下を実行してください。

    a. VDAでMicrosoft Teamsを終了します。

b. VDAでservices.mscを開始します。
c. Citrix HDX Teams Redirection Serviceを停止します。
d. ICA®セッションを切断します。
e. ICAセッションを接続します。
f. Citrix HDX Teams Redirection Serviceを開始します。
g. Citrix HDX HTML5 Video Redirection Serviceを再起動します。
h. VDAでMicrosoft Teamsを起動します。

3. クライアントエンドポイントでHdxTeams.exeまたはHdxRtcEngine.exeがまだ起動していない場合は、以下を実行してください。

a. VDA を再起動します。
b. クライアントエンドポイントを再起動します。

サポート

Citrix と Microsoft は、Microsoft Teams の最適化を使用して、Citrix Virtual Apps and Desktops™ からの Microsoft Teams の配信を共同でサポートしています。この共同サポートは、両社の緊密な連携の結果です。有効なサポート契約があり、このソリューションで問題が発生した場合は、問題の原因となっていると思われるコードのベンダーにサポートチケットをオープンしてください。つまり、Teams の場合は Microsoft、最適化コンポーネントの場合は Citrix です。 Citrix または Microsoft がチケットを受け取り、問題をトリアージし、必要に応じてエスカレートします。各社のサポートチームに連絡する必要はありません。

問題が発生した場合は、Teams UI で **>** をクリックすることをお勧めします。技術的な問題をより迅速に解決するために、VDA 側のログは Citrix と Microsoft の間で自動的に共有されます。

ログの収集

HDX メディアエンジンログは、ユーザーのマシン上（VDA 上ではない）で見つけることができます。問題が発生した場合は、必ずサポートケースにログを添付してください。

Windowsログ：

Windowsログは、**HDXTeams**フォルダー内の%TEMP%にあります（AppData/Local/Temp/HDXTeamsまたはAppData/Local/Temp/HdxRtcEngine）。webrpc_Day_Month_timestamp_Year.txtという名前の.txtファイルを探してください。Citrix Workspaceアプリの新しいバージョン（Citrix Workspaceアプリ2009.5以降など）を使用している場合は、ログをAppData\Local\Temp\HdxRtcEngineに保存します。

各セッションはログ用の個別のフォルダーを作成します。

Macログ：

1. VDWEBRTCログ - 仮想チャネルの実行を記録します。

   場所：`/Users/<User Name>/Library/Logs/Citrix Workspace/CitrixViewer_<Y_M_D_H_M_S>.txt`

2. HdxRtcEngineログ - HdxRtcEngine上のプロセスの実行を記録します。

   場所: `$TMPDIR/hdxrtcengine/<W_M_D_H_M_S_Y>/hdxrtcengine.log`

   HdxRtcEngineログはデフォルトで有効になっています。

3. Webrpcログ - webrtcライブラリのラップアップの実行を記録する最も重要なログです。

   場所: `/Users/<USERNAME>/Library/Logs/HdxRtcEngine/<W_M_D_H_M_S_Y>/webrpc.log`

Linuxログ：

Linuxログは`/tmp/webrpc/<current date>/ and /tmp/hdxrtcengine/<current date>/`フォルダーにあります。 Webrtcログ：`/tmp/webrpc/<current date>/webrtc.log` カーネルログ：`/var/log/syslog`

ICE/STUN/TURN/ログ：

通話確立時には、以下の4つのICEフェーズが必要です。

- 候補収集
- 候補交換
- 接続チェック (STUNバインド要求)
- 候補昇格

HdxRtcEngine.exe ログには、関連するInteractive Connectivity Establishment (ICE) エントリが含まれています。これらのエントリは、通話設定が成功するために必要です。収集段階のサンプルスニペットを以下に示します。

```
RPCStubs Info: -> device id = \\?
\display#int3470#4&1835d135&0&uid13424#{65e8773d-8f56-11d0-
a3b9-00a0c9223196}\{bf89b5a5-61f7-4127-a279-e187013d7caf} label =
Microsoft Camera Front groupId =
```

```
webrtcapi.RTCPeerConnection Info: createOffer. audio = 1 video = 1

webrtcapi.RTCPeerConnection Info: setLocalDescription.

>>> begin:sdp

[…]



webrtcapi.RTCPeerConnection Info: OnSignalingChange. signaling state =
HaveLocalOffer



webrtcapi.RTCPeerConnection Info: OnIceGatheringChange. state = Gathering



[…]

>>> begin:sdp

candidate:840548147 1 udp 2122194687 10.108.124.215 56927 typ host
generation 0 ufrag oVk6 network-id 1

<<< end:sdp

[…]

>>> begin:sdp

candidate:1938109490 1 udp 24911871 52.114.xxx.xxx 52786 typ relay raddr
73.205.xxx.x rport 25651 generation 0 ufrag dDML network-id 1 network-cost
10

<<< end:sdp

[…]

>>> begin:sdp

candidate:4271145120 1 udp 1685987071 66.xxx.xxx.xxx 55839 typ srflx raddr
```

```
10.108.124.215 rport 55839 generation 0 ufrag uAVH network-id 1

<<< end:sdp

[…]



webrtcapi.RTCPeerConnection Info: OnIceGatheringChange. state = Complete
webrtcapi.RTCPeerConnection Info: setRemoteDescription.

>>> begin:sdp

[…]



webrtcapi.RTCPeerConnection Info: OnSignalingChange. signaling state =
HaveRemotelOffer
```

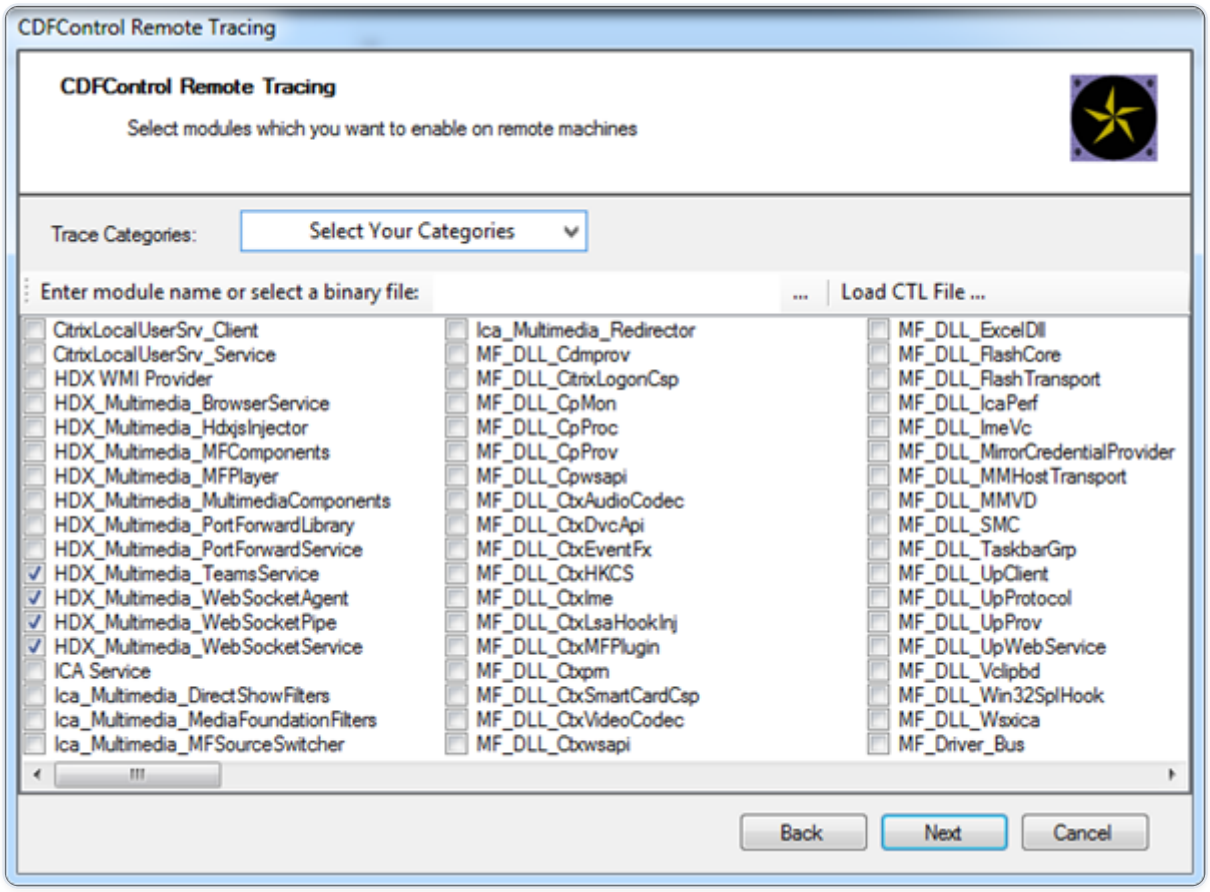
複数のICE候補がある場合、優先順位は次のとおりです。

1. ホスト
2. ピア反射型
3. サーバー反射型
4. トランスポートリレー

問題が発生し、それを一貫して再現できる場合は、Microsoft Teamsで**ヘルプ > 問題の報告**をクリックすることをお勧めします。Microsoftにケースをオープンした場合、技術的な問題を解決するためにログがCitrixとMicrosoftの間で共有されます。 Citrixサポートに連絡する前にCDFトレースをキャプチャすることも有益です。詳細については、Knowledge Centerの記事CDFcontrolを参照してください。

CDFトレースの収集に関する推奨事項については、Knowledge Centerの記事Recommendations for Collecting the CDF Tracesを参照してください。

VDA側のCDFトレース - 次のCDFトレースプロバイダーを有効にします:



Workspaceアプリ側のCDFトレース - 次のCDFトレースプロバイダーを有効にします:

Workspace App 側の CDF トレース(/en-us/citrix-virtual-apps-desktops/2503/media/team-cwa-cdf-traces.png)

- IcaClient_DriversVd_TeamsRedir (オプション)
- IcaClient_Multimedia_HdxTeams (Citrix Workspaceアプリ2012以降が必要)

Windows Media リダイレクト

Windows Media リダイレクトは、サーバーがストリーミングオーディオとビデオをユーザーに配信する方法を制御し、最適化します。サーバーではなくクライアントデバイスでメディアランタイムファイルを再生することで、Windows Media リダイレクトはマルチメディアファイルの再生に必要な帯域幅を削減します。Windows Media リダイレクトは、仮想Windowsデスクトップで実行されているWindows Media Playerおよび互換性のあるプレーヤーのパフォーマンスを向上させます。

Windows Media クライアント側コンテンツフェッチの要件が満たされない場合、メディア配信は自動的にサーバー側フェッチを使用します。この方法はユーザーには透過的です。Citrix Scoutを使用して、HostMMTransport.dllからCitrix Diagnosis Facility (CDF) トレースを実行し、使用されている方法を特定できます。詳細については、Citrix Scoutを参照してください。

Windows Media リダイレクトは、ホストサーバーでメディアパイプラインをインターセプトし、メディアデータをネイティブの圧縮形式でキャプチャし、コンテンツをクライアントデバイスにリダイレクトします。クライアントデバイスは、ホストサーバーから受信したメディアデータを解凍およびレンダリングするためにメディアパイプラインを再構築します。Windows Media リダイレクトは、Windowsオペレーティングシステムを実行しているクライアントデバイスでうまく機能します。これらのデバイスには、ホストサーバーに存在していたメディアパイプラインを再構築するために必要なマルチメディアフレームワークがあります。Linuxクライアントは、同様のオープンソースメディアフレームワークを使用してメディアパイプラインを再構築します。

ポリシー設定の**Windows Media Redirection**は、この機能を制御し、デフォルトで**Allowed**になっています。通常、この設定は、サーバーからレンダリングされるオーディオおよびビデオの品質を、クライアントデバイスでローカルに再生されるコンテンツに匹敵するレベルまで向上させます。まれに、Windows Media リダイレクトを使用して再生されるメディアが、基本的なICA®圧縮と通常のオーディオを使用してレンダリングされるメディアよりも悪く見えることがあります。この機能を無効にするには、ポリシーに**Windows Media Redirection**設定を追加し、その値を**Prohibited**に設定します。

ポリシー設定について詳しくは、「マルチメディアポリシー設定」(/ja-jp/citrix-virtual-apps-desktops/2503/policies/reference/ica-policy-settings/multimedia-policy-settings.html)を参照してください。

制限事項:

セッション内でWindows Media PlayerとRemote Audio & Video Extensions (RAVE) が有効になっている場合、黒い画面が表示されることがあります。この黒い画面は、ビデオコンテンツを右クリックして**常に手前に表示**を選択した場合に表示されることがあります。

仮想チャネルプラグインマネージャー

仮想チャネルプラグインマネージャーの概要

機能の理解

Citrix®は、お客様の環境が複雑になる可能性があり、管理対象および非管理対象のエンドポイント全体にプラグインを展開するにはかなりの労力が必要であることを理解しています。この機能は、そのプロセスを簡素化するように設計されています。

この機能には2つのコンポーネントが含まれています。1つはVDA側（検出プロセス）、もう1つはCitrix Workspace™ App側（インストーラープロセス）です。管理者が、ポリシーの有効化、レジ

ストリエントリの作成、監視するアプリケーションの指定など、上記の前提条件を満たすと、次のようになります。

- VDA側の検出プロセスは、エンドユーザーが仮想デスクトップにログオンすると、アプリケーションの起動を監視します
- 検出プロセスはCitrix Workspace App側に通知し、指定されたアプリケーションを最適化するために必要なプラグインをインストールするようユーザーに促します
- ユーザーの画面にプラグインに関する簡単な詳細を示すポップアップが表示されます。ユーザーは、プラグインをインストールするか、スキップするか、またはインストールしないかを選択できます
    - ユーザーがインストールプロセスをスキップした場合、そのセッションではポップアップが再度表示されることはありません。インストールプロンプトは、セッションの再接続時に表示されます。
    - ユーザーがプラグインをインストールしないことを選択した場合、その選択はユーザープロファイルに記録され、管理者が確認できるようになります。
- ユーザーがプラグインをインストールすることを選択した場合、Citrix Workspace App側がエンドポイントにプラグインをダウンロードしてインストールします。
    - インストールが成功すると、プラグインを有効にするためにセッションを再接続するようユーザーにメッセージが表示されます。ユーザーはすぐに再接続するか、成功メッセージを閉じて後で再接続するかを選択できます。
    - インストールが失敗した場合、ユーザーにはエラーメッセージが表示され、失敗は管理者が確認できるように記録されます。

仮想チャネルプラグインマネージャーの構成

展開

1. Microsoft Teamsリダイレクトポリシーが有効になっているか確認します。詳細については、Microsoft Teamsリダイレクトポリシーを参照してください。

   監視対象のアプリケーションに関わらず、このポリシーを有効にする必要があります。今後、より多くのアプリケーションがサポートされ、Microsoft Teamsの代わりにそれらのアプリケーションを監視したい場合でも、このポリシーは有効にしておく必要があります。このポリシーはデフォルトで有効になっています。

2. 仮想チャネルプラグインマネージャーポリシーを有効にする必要があります。ポリシーを有効にする方法の詳細については、仮想チャネルプラグインマネージャーポリシー設定を参照してください。

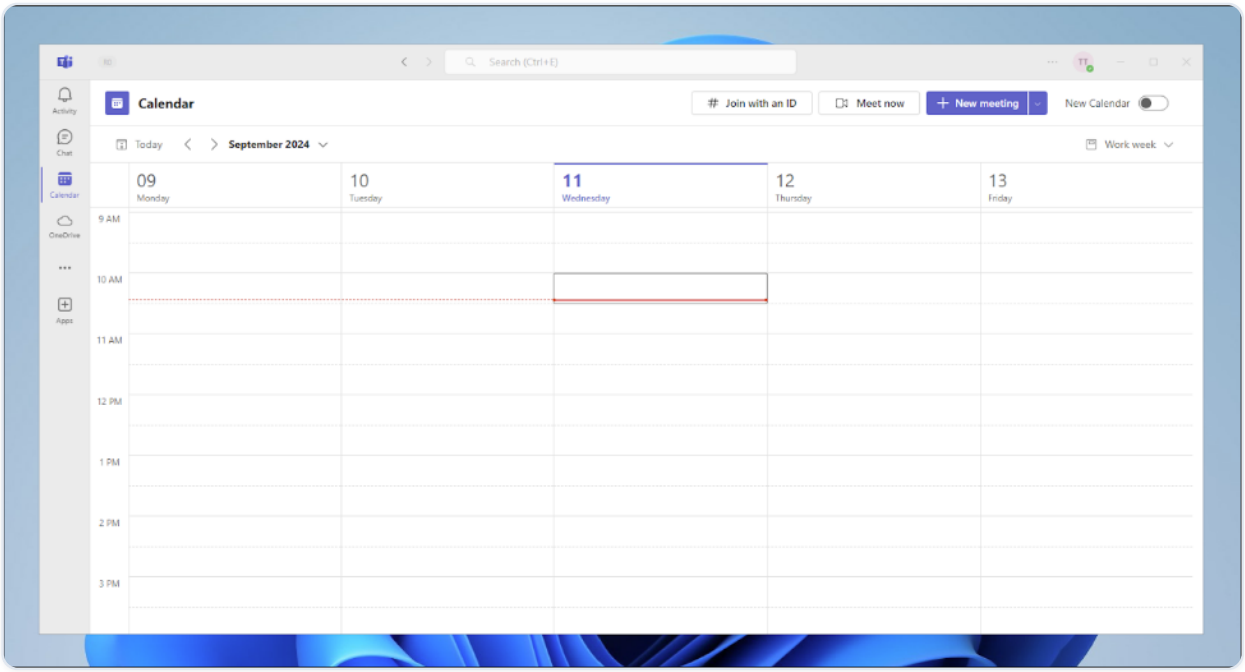
   このポリシーは、Citrix Studioのマルチメディアポリシー設定で利用できます。このポリシーを有効にすると、監視するアプリケーション名（例: 「Microsoft Teams」）を指定できます。このポリシーはデフォルトで無効になっています。

3. Citrix Workspace™アプリはシステムワイドモードでインストールする必要があります。

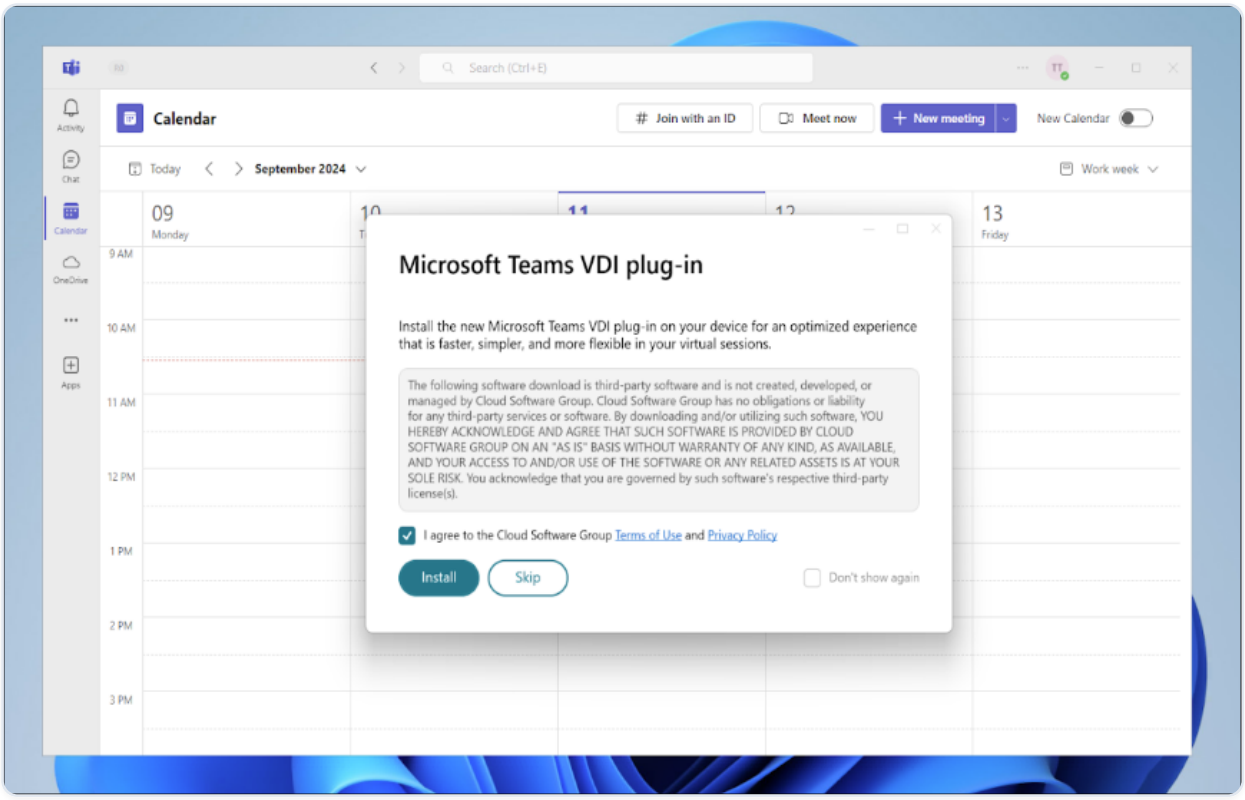
> **注:**
>
> プラグインは、サードパーティのCDNからエンドポイントにダウンロードされます。たとえば、Microsoft Teamsを選択した場合、プラグインはMicrosoft CDNからダウンロードされます。したがって、エンドポイントはサードパーティのCDNにアクセスできる必要があります。そうでない場合、プラグインのインストールは失敗します。

手順

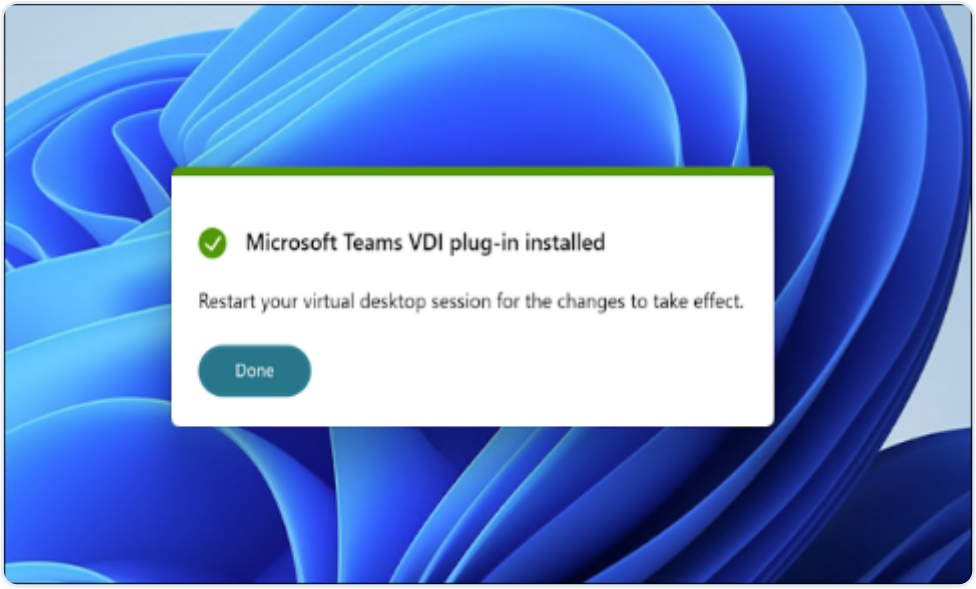
1. ユーザーはCitrixセッションでアプリケーションを起動します。例: Microsoft Teams。



2. ユーザーは、より良いエクスペリエンスのためにエンドポイントにTeams VDIプラグインをインストールするためのポップアップを受け取ります。プラグインはエンドポイントにインストールされるため、ポップアップはセッション内ではなくセッションの上に表示されます。



3. ユーザーがインストールボタンをクリックすると、プラグインがインストールされます。変更を有効にするには、仮想デスクトップセッションを再起動する必要があります。



既知の問題と制限事項

- 2407 VDAでは、機能を有効にするために、ポリシーに加えてVDA上で以下のレジストリ設定を1に設定する必要があります。このレジストリ設定は、2411 VDA以降では自動的に許可され、構成する必要はありません。

  `HKLM\SOFTWARE\Citrix\HDXMediaStream

Name: EnableAppDetector Type: DWORD`

- さらなる制限事項が追加される予定です。

Unified Communications SDK の最適化

はじめに

Citrix Virtual Apps and Desktops を使用すると、様々なエンドポイントデバイス上のユーザーにアプリケーションを配信できます。これらのアプリケーションの多くには、音声会議やビデオ会議などのリアルタイム通信 (RTC) 機能が含まれています。しかし、仮想化環境でこれらのアプリケーションを配信する際には、課題が生じることがあります。従来の配信方法では、メディアストリーム (オーディオ/ビデオ) をクライアントデバイスからデータセンター内の VDI サーバーにルーティングし、その後エンドポイントに送り返します。この「ヘアピン」方式は、特に帯域幅を大量に消費するオーディオおよびビデオ通話の場合、サーバーに不要なトラフィックと処理オーバーヘッドを発生させます。

Citrix Unified Communications SDK (UCSDK) は、テクノロジーベンダーがCitrix環境で使用するためにこれらのRTCアプリケーションを最適化できるようにするテクノロジーです。アプリケーションが最適化されると、ローカルデスクトップで実行されているアプリケーションと同等か、それ以上のユーザーエクスペリエンスを提供できます。今日の社会では、生産性とコラボレーションのために、シームレスなリアルタイム通信が不可欠です。仮想環境でアプリケーションを使用する場合、音声通話やビデオ通話、画面共有、その他の通信機能がローカルデスクトップと同じくらいスムーズに機能することが重要です。最適化されたアプリケーションは、このエクスペリエンスを提供します。

この製品ドキュメントでは、Citrixのお客様がUCSDK最適化アプリケーションを学習し、展開するために必要なすべての詳細を説明します。

動作の仕組み

Citrixは、VDI内のリアルタイム通信アプリケーション向けに最適化された配信方法を提供しています。このアプローチでは、Unified Communications SDK (UCSDK) を活用して、仮想化されたアプリケーションを2つの部分に分割します。

- **ユーザーインターフェイス (UI):** ユーザーインターフェイスは仮想ホスト内に残り、仮想デスクトップまたはアプリケーションウィンドウ内にシームレスに表示されます。
- **メディアエンジン:** メディア処理タスク (オーディオとビデオのエンコード/デコード) は、ユーザーのローカルデバイスにオフロードされます。これにより、サーバーの負荷が最小限に抑えられ、ネットワーク使用量が最適化されます。

通常、Citrixはリアルタイム通信分野のテクノロジーベンダーにUCSDKを提供し、それらのアプリケーションにUCSDKを統合するために協力しています。一度統合されると、UCSDK最適化アプリケーションを使用するCitrixのお客様は、強化されたエクスペリエンスを得ることができます。Citrix UCSDKは、カスタムの社内アプリケーションが構築される場合にも、Citrixのお客様が利用できます。ただし、ほとんどの場合、お客様はUCSDKを利用して開発する必要はなく、最適化されたエクスペリエンスを実現するためにCitrix環境とアプリケーションを構成するだけで済みます。

> **注:**
>
> Citrix WebRTC SDKまたはHDX™最適化アプリケーションへの言及は、Citrix UCSDKとの統合を示しており、互換的に使用できます。

主な利点

Citrix UCSDKで最適化されたアプリケーションを使用すると、次のことが期待できます。

- プロセッサ負荷の高いメディアエンコード/デコードをCitrix Virtual Delivery Agent (VDA) からクライアントエンドポイントにオフロードすることで、メディア処理パフォーマンスが向上し、エンドユーザーの全体的な応答性が高まります。
- Citrix VDAでのCPUと帯域幅の使用量を削減し、IT部門がホストあたりより多くの同時実行ユーザーをサポートできるようにし、企業がCitrix仮想デスクトップの展開を費用対効果の高い方法で拡張できるようにします。
- 最適化されたエンドポイントがレガシー仮想デスクトップの寿命を延ばし、ホストインフラストラクチャの必要性を減らすことで、企業の総所有コストを削減し、時間の経過とともに設備投資と運用コストを削減します。
- Windows、Mac、Linux、ChromeOS、およびHTML5エンドポイントプラットフォームのサポート。

ユースケース

UCSDKは、WebRTC標準に準拠するリアルタイム通信アプリケーションを最適化するために特別に構築されています。ここでは、主要なシナリオと、UCSDKを使用できる/すでに使用しているWebRTCベースのアプリケーションの種類を示します。

- **サービスとしてのコンタクトセンター (CCaaS) / クラウドコンタクトセンタープラットフォーム:** 主に複数のチャネルにわたる顧客とのやり取りを管理し、エージェントのワークフローを最適化します。

    - 例: アマゾン コネクト、トゥイリオ、アバイア エクスペリエンス プラットフォーム、トークデスク、コンテンツ グル

- **サービスとしてのユニファイドコミュニケーション (UCaaS) / クラウドビジネスコミュニケーション:** 音声、ビデオ、チームメッセージング、プレゼンスを統合し、包括的なビジネスコミュニケーションを実現します。
    - 例: リング セントラル、エイトバイエイト、インターメディア、アルカテル・ルーセント レインボー
- **サービスとしてのコミュニケーションプラットフォーム (CPaaS):** リアルタイム通信機能をカスタムアプリケーションに直接組み込むためのAPIを提供します。
    - 例: トゥイリオ、リボン コミュニケーションズ
- **エンタープライズビデオ会議とコラボレーション:** 高品質のビデオ会議、カンファレンス、高度なコラボレーション機能のための専用プラットフォーム。
    - 例: Pexip
- **金融取引通信:** 金融市場の独自の、高性能でコンプライアンスに準拠した通信ニーズのために設計されています。
    - 例: IPC Unigy
- **仮想学習およびトレーニングプラットフォーム:** インタラクティブで高品質な仮想教室およびトレーニング体験のために設計されています。
    - 例: ヴィテロ

Citrix UCSDKの基盤となるWebRTCは、その最適化機能がWebRTCベースのあらゆる通信アプリケーションに拡張できることを意味します。これにより、現在UCSDKで最適化されているとリストされていない場合でも、リアルタイムインタラクションにWebRTCを利用する幅広いアプリケーションの最適化が可能になります。最適化を希望するユースケースやアプリケーションについては、Citrixまでお問い合わせください。

UCSDK アーキテクチャ

UCSDK アーキテクチャ (/en-us/citrix-virtual-apps-desktops/2503/media/ucsdk-architecture.png)

- ベンダーアプリケーション: これは、UCSDK を統合した、デスクトップベースまたはブラウザベースのサードパーティ製リアルタイム通信アプリケーションです。

- UCSDK JS: UCSDK JS は、ベンダーアプリケーションがオーディオ/ビデオをエンドポイントにオフロードするために利用する API を提供します。
- HdxRtcEngine: これは、Citrix Workspace Appに組み込まれたWebRTCメディアエンジンで、オフロードされたオーディオ/ビデオ通話を処理および管理します。

SDKがロードされて使用されると、リダイレクトが成功した場合、クライアントエンドポイントで`HdxRtcEngine.exe`プロセスが起動されます。`HdxRtcEngine.exe`がクライアントエンドポイントで起動されると、すべてのシグナリングおよびペイロードデータはCitrix VDAからクライアントエンドポイントに流れ、クラウドに到達し、クライアントエンドポイントに戻ってからVDAに転送されます。たとえば、フローの完全な往復は次のようになります。

```
Vendor App -> CitrxWebrtc.js SDK -> Citrix VDA components -> Citrix Client Endpoint components -> Cloud -> Citrix Client Endpoint components -> Citrix VDA components -> CitrxWebrtc.js SDK -> Vendor App
```

システム要件

システム要件は、最新バージョンのUCSDK - 5.0.0で必要となるCitrixコンポーネントのさまざまなバージョンを示しています。SDKの以前のバージョンおよび特定の機能要件に関する互換性の詳細については、以下のバージョンと機能マトリックス表を参照してください。

> **注:**
>
> お客様が UCSDK に追加された機能を使用するには、ベンダーアプリケーションが適切な UCSDK バージョンを統合し、その機能を有効にしていること、および環境で適切な VDA および CWA バージョンを使用していることを確認してください。

完全互換バージョン

完全互換バージョンとは、これらのバージョンのCitrixコンポーネントを最新バージョンのUCSDKと組み合わせて使用することで、利用可能なすべての機能を利用できることを示します。UCSDKの現在の最新バージョンである5.0.0の場合、Citrixコンポーネントの完全互換バージョンは以下のとおりです。

- **シトリックス バーチャル アプリ™ アンド デスクトップ**：2603
- **シトリックス ワークスペース アプリ Windows**：2603
- **Citrix Workspace App Mac:** リリース予定
- **Citrix Workspace アプリ リナックス:** 2603

- **Citrix Workspace App ChromeOS/HTML5:** リリース予定

> **注記:**
>
> UCSDK最適化は、Windows、Mac、Linux、ChromeOS、HTML5のすべてのエンドポイントプラットフォームでサポートされています。上記のリストで特定のエンドポイントプラットフォームに**リリース予定**と表示されている場合、それは最新のUCSDK機能と完全に互換性のあるバージョンがまだリリースされていないことを意味します。したがって、お客様は、新しいUCSDKを使用しても、Citrix Workspaceアプリの古いバージョンを使用して既存の機能を継続して使用できます。

構成

UCSDKの機能は、ベンダーが統合したUCSDKのバージョンとベンダーが有効にした機能、Citrix Virtual Apps and Desktops、および使用中のCitrix Workspaceアプリのバージョンの3つの要因に依存します。

Citrix側では、最適化されたアプリケーションが最適化されるように、以下が構成されていることを確認してください。

1. Microsoft Teamsリダイレクトポリシーがオンになっていることを確認します。詳細については、(/ja-jp/citrix-virtual-apps-desktops/2503/policies/reference/ica-policy-settings/multimedia-policy-settings#microsoft-teams-redirection)を参照してください。このポリシーはデフォルトでONになっています。
2. `CitrixWebrtc.js` SDKを利用するサードパーティのElectronまたはブラウザベースのアプリケーションは、デフォルトではサポートされていません。`CtxHdxWebSocketService` (`WebSocketService.exe`) は、許可リストにないアプリケーションからの接続を許可しません。目的のアプリケーションバイナリ実行可能ファイル名をホワイトリストレジストリキーに追加する必要があります。

VDA上

- キーパスを作成します: `HKLM\Software\WOW6432Node\Citrix\WebSocketService`
- キー名: `ProcessWhitelist`
- 種類: `MULTISZ`
- キー値: `Mytestapp.exe`

複数のアプリケーションがある場合は、各アプリケーションを新しい行に入力します。テキストファイルからコピー＆ペーストしたり、コンマを挿入したりしないでください。指定された名前がアプリケーションの実行可能ファイル名と一致していることを確認してください。このレジストリ値は大文字と小文字を区別しません。

アプリケーションが本格的なデスクトップアプリケーションではなくブラウザ経由でアクセスされる場合、レジストリ値で例えば `chrome.exe` を許可する必要があります。

上記のレジストリが正常に構成されたら、VDA を再起動するか、`CtxHdxWebSocketService` を再起動してホワイトリストの設定を完了します。

クライアント上

設定は不要です。Citrix Workspace アプリをインストールするだけです。

各ベンダーは非常に特定のアプリケーション名を持っている場合があります。したがって、WebSocketService で許可する必要があるアプリケーション名を決定するには、現在のベンダーサポート セクションにリンクされているベンダーのドキュメントを参照してください。

バージョンと機能マトリックス

バージョンアップは頻繁に行われるため、特定のバージョンがサポートされていることを確認するには、Citrix Virtual Apps and Desktops および Citrix Workspace app の製品ライフサイクルページを参照してください。多くの古い機能については、表に記載されているバージョンは、このドキュメントの作成時点での最終サポート対象のCurrent Release (CR) バージョンです。

機能	UCSDK バージョン	VDA	CWA ウィンドウズ	CWA MAC	CWA リナックス	CWA CHROME OS/ HTML5
オーディオ/ビデオ (p2p & 会議)	3.1.0	2203 LTSR 最新 CU / 2311 CR	2402 LTSR 最新 CU / 2311 CR	2311	2311	2312
画面共有	3.1.0	2203 LTSR 最新 CU / 2311 CR	2402 LTSR 最新 CU / 2311 CR	2311	2311	2312
DTMF	3.1.0	2203 LTSR 最	2402 LTSR 最	2311	2311	2312

機能	UCSDK バージョン	VDA	CWA ウィンドウズ	CWA MAC	CWA リナックス	CWA CHROME OS/ HTML5
		新 CU / 2311 CR	新 CU / 2311 CR			
プロキシサーバーのサポート	3.1.0	2203 LTSR 最新 CU / 2311 CR	2402 LTSR 最新 CU / 2311 CR	2311	2311	2312
アプリ共有	3.1.0	2203 LTSR 最新のCU / 2311 CR	2402 LTSR 最新のCU / 2311 CR	2311	2311	N/A
動的e911	3.1.0	2203 LTSR 最新のCU / 2311 CR	2402 LTSR 最新のCU / 2311 CR	2311	2311	2312
マルチウィンドウ	3.1.0	2203 LTSR 最新 CU / 2311 CR	2402 LTSR 最新 CU / 2311 CR	2311	2311	2312
SDP Unified Plan サポート	3.1.0	2203 LTSR 最新 CU / 2311 CR	2402 LTSR 最新 CU / 2311 CR	2311	2311	2312
ストリーム解像度 / Simulcast	3.1.0	2203 LTSR 最新のCU / 2311 CR	2402 LTSR 最新のCU / 2311 CR	2311	2311	2312
リモートオーディオ (ループ付き)	3.1.0	2203 LTSR 最新のCU / 2311 CR	2402 LTSR 最新のCU / 2311 CR	2311	2311	2405

機能	UCSDK バージョン	VDA	CWA ウィンドウズ	CWA MAC	CWA リナックス	CWA CHROME OS/ HTML5
ブラウザベースの UCSDK (ブートストラップサポート)	4.0.2	2407 CR	2402 LTSR 最新CU / 2311 CR	2311	2311	2312
Web HID API	4.0.2	2203 LTSR 最新CU / 2311 CR	2409.10	2411	2411	2505
ウェブオーディオAPI	4.0.2	2203 LTSR 最新CU / 2311 CR	2405	2405	2405	N/A
ICEを再起動	4.1.0	2203 LTSR 最新 CU / 2311 CR	2503.2	2503	2503	2502.10
画面録画 (プレビュー)[1]	4.1.0	2503	2503.2	N/A	N/A	N/A
SmartSync	5.0.0	2203 LTSR 最新 CU / 2311 CR	2603	N/A	2604	N/A

注:

画面録画用の新しいポリシーを導入しました。そのため、CVAD 2503 に付属する Delivery Controller™ のバージョン 2503 が必要です。

現在のベンダーサポート

いくつかのサードパーティベンダーが、Unified Communications SDK を自社製品に統合しています。ベンダーとそのサポートドキュメントの現在のリストを以下に示します。

ベンダー	ドキュメント
アマゾン コネクト	Citrixクラウドデスクトップ向けAmazon Connectオーディオの最適化
RingCentral	Citrix VDI環境でのRingCentralの使用
ファイブナイン	Citrix環境でのFive9 WebRTC
トゥイリオ	シトリックス VDIでのトゥイリオ フレックス
アバイア	Citrix向けAvaya Experience Platform Public Cloud VDIソリューション
8x8	デスクトップおよびWeb向け8x8 WorkとのCitrix VDI統合
コンテンツ グル	コンテンツ グル シトリックス統合
リボンコミュニケーションズ	リボンコミュニケーションズ Citrix WebRTC SDK
インターメディア	「Citrix Virtual Apps and Desktops へのIntermedia Unite のインストール」(https://support.intermedia.com/app/articles/detail/a_id/24355)
アルカテル・ルーセント レインボー	レインボー デスクトップ アプリケーション 用 Citrix 最適化
トークデスク	トークデスク Agent Workspace VDI Connect
IPC	IPC ユニジー ソフト クライアント Citrix VDI
ヴィテロ	Citrix VDI 用 ヴィテロ インスパイア
ペクシプ	「Citrix Pexip Infinity Docs での Connect デスクトップアプリの展開」(https://docs.pexip.com/clients/using_citrix_client.htm)

ベンダー	ドキュメント
Zoom Web アプリ	Zoom Web App の WebRTC リダイレクトを構成する](https://support.zoom.com/hc/en/article?id=zm_kb&sysparm_article=KB0083142)

トラブルシューティング

トラブルシューティング情報については、Citrix Unified Communications SDK で最適化されたアプリのトラブルシューティング ガイダンス を参照してください。

既知の問題と制限事項

このセクションでは、現在認識されている既知の問題と制限事項について説明します。

一般的なコンテンツリダイレクト

クライアントフォルダーリダイレクト

クライアントフォルダーリダイレクトは、クライアント側のファイルがホスト側のセッションでアクセス可能になる方法を変更します。サーバーでクライアントドライブマッピングのみを有効にすると、クライアント側の完全なボリュームは、ユニバーサルネーミングコンベンション (UNC) リンクとしてセッションに自動的にマップされます。サーバーでクライアントフォルダーリダイレクトを有効にし、ユーザーがユーザーデバイスでそれを構成すると、ユーザーが指定したローカルボリュームの一部がリダイレクトされます。

ユーザーが指定したフォルダーのみが、セッション内でUNCリンクとして表示されます。つまり、ユーザーデバイス上の完全なファイルシステムではなく、指定されたフォルダーのみが表示されます。レジストリを介してUNCリンクを無効にすると、クライアントフォルダーはセッション内でマップされたドライブとして表示されます。

クライアントフォルダーリダイレクトは、WindowsシングルセッションOSマシンでのみサポートされています。

外部USBドライブのクライアントフォルダーリダイレクトは、デバイスの取り外しと再接続時には保存されません。

サーバーでクライアントフォルダーリダイレクトを有効にします。次に、クライアントデバイスで、リダイレクトするフォルダーを指定します。クライアントフォルダーオプションを指定するために使用するアプリケーション (CtxCFRUI.exe) は、このリリースで提供されるCitrix Workspaceアプリに含まれています。

要件:

サーバーの場合:

- ウィンドウズ サーバー 2022
- ウィンドウズ サーバー 2019、スタンダードおよびデータセンター エディション

クライアントの場合:

- ウィンドウズ 10

- ウィンドウズ 11

サーバーでクライアントフォルダーリダイレクトを有効にするには、レジストリで管理される機能のリストにあるクライアントフォルダーリダイレクトを参照してください。

ユーザーデバイスで、リダイレクトするフォルダーを指定します:

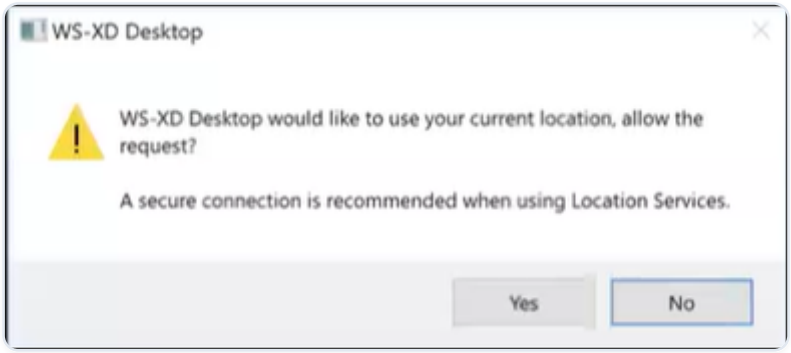
1. Citrix Workspace™アプリの最新バージョンがインストールされていることを確認してください。
2. Citrix Workspaceアプリのインストールディレクトリから、CtxCFRUI.exe **(..\Citrix\ICA Client\CtxCFRUI.exe)** を起動します。
3. **Custom** ラジオボタンを選択し、フォルダーを追加、編集、または削除します。
4. 設定を有効にするには、セッションを切断して再接続します。

クライアント位置情報リダイレクト

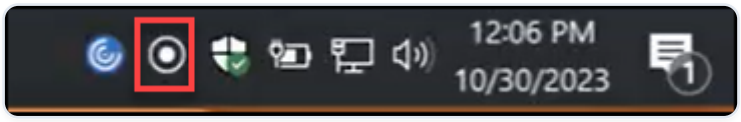
クライアント位置情報リダイレクトを有効にすると、VDAでホストされているアプリとデスクトップセッションが、クライアントの現在の位置情報にシームレスにアクセスできるようになります。マルチセッションオペレーティングシステム（TS VDAまたはマルチセッションWS VDA）では、各セッションは接続されたクライアントによって提供される独自の場所を持ちます。この機能を使用すると、位置情報に依存するVDA上のアプリケーションは、クライアントの正確な位置情報を取得できます。

詳細については、Microsoftドキュメントを参照してください。

クライアント位置情報リダイレクトが有効になり、サーバー側とクライアント側の両方で位置情報へのアクセスが許可されると、位置情報にアクセスするアプリケーションまたはデスクトップを起動したときに、クライアントは次のダイアログボックスで現在の位置情報を共有するように求めます。



クライアント位置情報リダイレクトを有効にすると、VDAでホストされているアプリまたはデスクトップが現在の位置情報を照会したときに、クライアントのタスクバーに次のアイコンが表示されます。



システム要件

サーバーの場合：

- シングルセッション (Win10/11) またはマルチセッション (Win 11 22H2 および Server 2022 23H2 以降) OS VDA
- Citrix Workspace™アプリ for Windows、iOS、またはAndroid

構成

この機能が動作するには、Citrix®ポリシーを使用してクライアント位置情報リダイレクトを有効にする必要があります。クライアント位置情報リダイレクトはデフォルトで無効になっています。

クライアント位置情報リダイレクトを有効にするには、次の手順を実行します。

Windows VDAおよびクライアント側で：

1. **設定 > プライバシー > 位置情報**で、次のオプションを有効にします。
    - **このデバイスでの位置情報へのアクセスを許可する**
    - **アプリがあなたの位置情報にアクセスすることを許可する**
    - **デスクトップアプリがあなたの位置情報にアクセスすることを許可する**
2. マルチセッションOSの場合、**位置情報の上書き**設定を有効にします。

Controller/DDC側で:

Studio > ポリシー > 位置情報 > 設定 > アプリケーションがクライアントデバイスの物理的な位置情報を使用することを許可するポリシーを有効にします。 詳細については、「クライアントセンサーポリシー設定」を参照してください。

双方向コンテンツリダイレクト

双方向コンテンツリダイレクトにより、Webブラウザ内、またはアプリケーションに埋め込まれたHTTPまたはHTTPS URLを、Citrix VDAセッションとクライアントエンドポイント間で双方向に転送できます。Citrixセッションで実行されているブラウザに入力されたURLは、クライアントのデフォルトブラウザを使用して開くことができます。逆に、クライアントで実行されているブラウザに入力されたURLは、公開アプリケーションまたはデスクトップのいずれかを使用して、Citrix

セッションで開くことができます。双方向コンテンツリダイレクトの一般的なユースケースには、次のようなものがあります。

- 開始ブラウザがソースへのネットワークアクセスを持たない場合のWeb URLのリダイレクト。
- ブラウザの互換性およびセキュリティ上の理由によるWeb URLのリダイレクト。
- Citrixセッションまたはクライアントでwebブラウザを実行したくない場合に、アプリケーションに埋め込まれたWeb URLのリダイレクト。

システム要件

- シングルセッションまたはマルチセッションOS VDA
- Citrix Workspace™アプリ for Windows 2311以降
- Citrix Workspace™アプリ for Linux 2503以降
- Citrix Workspace™アプリ for Mac 2607以降

ブラウザー：

- シトリックス ブラウザ リダイレクション拡張機能を搭載したグーグル クローム
  - Google Chrome拡張機能
- シトリックス ブラウザ リダイレクション拡張機能を搭載したマイクロソフト エッジ
  - Microsoft Edge拡張機能

構成

Citrix Virtual Apps and Desktops™バージョン2311以降、双方向コンテンツリダイレクトはCitrix Studioのみで構成されます。以前のリリースでは、クライアントエンドポイントとStudioの両方でポリシー設定が構成されていました。双方向コンテンツリダイレクトはデフォルトで無効になっています。

VDA の構成については、**ICA ポリシー**設定の 双方向コンテンツリダイレクト を参照してください。

ブラウザリダイレクトを機能させるには、表示されているコマンドを使用して、元のブラウザ（URLがリダイレクトされる元）にブラウザ拡張機能を登録する必要があります。使用しているブラウザに基づいて、必要に応じてVDAとクライアントでコマンドを実行します。

ブラウザ	VDA	クライアント
グーグル クローム	"%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe" /regChrome	"%ProgramFiles(x86)%\Citrix\ICA Client\redirector.exe" /regChrome
マイクロソフト エッジ	"%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe" /regEdge	"%ProgramFiles(x86)%\Citrix\ICA Client\redirector.exe" /regEdge
すべての利用可能なブラウザ	"%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe" /regall	"%ProgramFiles(x86)%\シトリックス\ICA クライアント\redirector.exe" /regall

ブラウザ拡張機能を登録解除するには:

ブラウザ	VDA	クライアント
グーグル クローム	"%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe" /unregChrome	"%ProgramFiles(x86)%\Citrix\ICA Client\redirector.exe" /unregChrome
マイクロソフト エッジ	"%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe" /unregEdge	"%ProgramFiles(x86)%\Citrix\ICA Client\redirector.exe" /unregEdge
すべての利用可能なブラウザ	"%ProgramFiles(x86)%\シトリックス\HDX\bin\vdaredirector.exe" /unregall	"%ProgramFiles(x86)%\シトリックス\ICA クライアント\redirector.exe" /unregall

注:

- 管理者権限を持つコマンドプロンプト (CMD) ウィンドウでこれらのコマンドを実行します。

- 登録コマンドを実行すると、Chrome および Edge ブラウザは、初回起動時にCitrix Browser Redirection Extension を有効にするようユーザーに促します。
- 登録コマンドは、Browser Redirection Extension をネイティブメッセージングホストにリンクし、これにより拡張機能がネイティブコードと通信できるようになります。これがないと、ブラウザは通信をブロックします。
- ブラウザ拡張機能は、Google Chrome Web Store から手動でインストールすることもできます。Microsoft Edge アドオンストアからBrowser Redirection Extension を使用するには、Virtual Delivery Agent (VDA) バージョン2503以降が必要です。古いVDAバージョンでは、Microsoft Edgeブラウザ内でGoogle Chrome Web Storeから拡張機能をインストールしてください（「Chrome Web StoreからMicrosoft Edgeに拡張機能を追加する」を参照）。
- システム要件に記載されているCitrix Workspaceアプリのバージョンは、双方向コンテンツリダイレクトとOAuthリダイレクトの両方をサポートするために必要な最小バージョンです。
- Macの場合：公証済みアプリケーションに対するmacOSのセキュリティ要件により、カスタムOAuthコールバックURLスキームはCitrixに事前登録する必要があり、インストール後に動的に変更することはできません。デフォルトでは `citrix-oauth-redir` のみがサポートされています。URLスキームを登録するには、Citrix製品チームにお問い合わせください。

Citrix VDAからクライアントへのワイルドカードリダイレクト

双方向コンテンツリダイレクトは、リダイレクトするURLを定義する際にワイルドカードの使用をサポートします。双方向コンテンツリダイレクトを構成するには、構成手順を参照してください。

VDAからクライアントへのカスタムプロトコルリダイレクト

双方向コンテンツリダイレクトは、Citrix VDAからクライアントへのカスタムプロトコルのリダイレクトをサポートします。HTTPまたはHTTPS以外のプロトコルがサポートされています。双方向コンテンツリダイレクトを構成するには、構成手順を参照してください。

Web Studioで、**双方向コンテンツリダイレクト**のカスタムプロトコルを設定します。

注:

- これらのコマンドを実行するには、管理者権限が必要です。
- クライアントは、プロトコルを処理するために登録されたアプリケーションを持っている必要があります。そうでない場合、URLはクライアントにリダイレクトされますが、起動に失敗します。
- ChromeおよびEdgeブラウザで入力または起動するカスタムプロトコルURLはサポートされておらず、リダイレクトされません。
- 以下のプロトコルはサポートされていません: `rtsp://, rtspu://, pnm://, mms://`。

その他の考慮事項

- ブラウザの要件と構成は、リダイレクトを開始するブラウザにのみ適用されます。リダイレクトが成功した後にURLが開かれる宛先ブラウザは、サポートの対象とはなりません。VDAからクライアントにURLをリダイレクトする場合、サポートされるブラウザ構成はVDA上でのみ必要です。逆に、クライアントからVDAにURLをリダイレクトする場合、サポートされるブラウザ構成はクライアント上でのみ必要です。リダイレクトされたURLは、方向に応じて、クライアントまたはVDAのいずれかの宛先マシンで構成されたデフォルトのブラウザに引き渡されます。VDAとクライアントで同じブラウザタイプを使用する必要はありません。
- リダイレクトルールがループ構成にならないことを確認してください。たとえば、VDAポリシーが`https://www.citrix.com`をリダイレクトするように設定され、クライアントポリシーが同じURLをリダイレクトするように設定されている場合、無限ループが発生します。
- URL短縮サービスはサポートされていません。
- クライアントからVDAへのリダイレクトには、管理者権限でWindowsクライアントがインストールされている必要があります。
- 宛先ブラウザがすでに開いている場合、リダイレクトされたURLは新しいタブで開きます。そうでない場合、URLは新しいブラウザウィンドウで開きます。
- ローカルアプリアクセス (LAA) が有効になっている場合、双方向コンテンツリダイレクトは機能しません。

ホストからクライアントへのリダイレクト

ホストからクライアントへのリダイレクトにより、Citrix®セッションで実行されているアプリケーションにハイパーリンクとして埋め込まれたURLを、ユーザーのエンドポイントデバイス上

の対応するアプリケーションを使用して開くことができます。ホストからクライアントへのリダイレクトの一般的なユースケースには、次のようなものがあります。

- Citrixサーバーがソースへのインターネットまたはネットワークアクセスを持たない場合のWebサイトのリダイレクト。
- セキュリティ、パフォーマンス、互換性、またはスケーラビリティの理由から、Citrixセッション内でWebブラウザを実行することが望ましくない場合のWebサイトのリダイレクト。
- URLを開くために必要なアプリケーションがCitrixサーバーにインストールされていない場合の特定のURLタイプのリダイレクト。

ホストからクライアントへのリダイレクトは、Webページでアクセスしたり、Citrixセッションで実行されているWebブラウザのアドレスバーに入力したりするURLを対象としていません。Webブラウザでのリダイレクトについては、「双方向URLリダイレクト」または「ブラウザコンテンツリダイレクト」を参照してください。

システム要件

- マルチセッションOS VDA
- サポートされているクライアント:
  - Windows向けCitrix Workspace™アプリ
  - Mac向けCitrix Workspaceアプリ
  - Linux向けCitrix Workspaceアプリ
  - HTML5向けCitrix Workspaceアプリ
  - Chrome向けCitrix Workspaceアプリ

クライアントデバイスには、URLタイプのリダイレクトを処理するためのアプリケーションがインストールされ、構成されている必要があります。

構成

この機能を有効にするには、ホストからクライアントへのリダイレクト Citrixポリシーを使用します。**ホストからクライアントへのリダイレクト**は、デフォルトで無効になっています。ホストからクライアントへのリダイレクトポリシーを有効にすると、Citrix Launcherアプリケーションが Windowsサーバーに登録され、URLをインターセプトしてクライアントデバイスに送信できるようになります。

次に、必要なURLタイプのデフォルトアプリケーションとしてCitrix Launcherを使用するようにWindowsグループポリシーを構成する必要があります。CitrixサーバーVDAで、ServerFTAdefaultPolicy.xmlファイルを作成し、次のXMLコードを挿入します。

```
<?xml version="1.0" encoding="UTF-8"?>



<DefaultAssociations>



<Association Identifier="http" ProgId="ServerFTAHTML"
ApplicationName="ServerFTA" />



<Association Identifier="https" ProgId="ServerFTAHTML"
ApplicationName="ServerFTA" />



</DefaultAssociations>
```

グループポリシー管理コンソールから、**コンピューターの構成 > 管理用テンプレート > Windowsコンポーネント > エクスプローラー > 既定の関連付け構成ファイルの設定** に移動し、ServerFTAdefaultPolicy.xmlファイルを保存します。

注:

Citrixサーバーにグループポリシー設定がない場合、Windowsは、URLを開くためのアプリケーションを選択するようユーザーに求めます。

デフォルトでは、次のURLタイプのリダイレクトをサポートしています。

- HTTP
- HTTPS
- RTSP

- RTSPU
- PNM
- MMS

リダイレクトのリストに、追加の標準またはカスタムURLタイプを含めるには、前述のServerFTAdefaultPolicy.xmlファイルに新しい**関連付け識別子**の行を作成します。例：

```
<Association Identifier="ftp" ProgId="ServerFTAHTML"
ApplicationName="ServerFTA" />
```

```
<Association Identifier="mailto" ProgId="ServerFTAHTML"
ApplicationName="ServerFTA" />
```

```
<Association Identifier="customtype1" ProgId="ServerFTAHTML"
ApplicationName="ServerFTA" />
```

```
<Association Identifier="customtype2" ProgId="ServerFTAHTML"
ApplicationName="ServerFTA" />
```

URLタイプをリストに追加するには、クライアント構成も必要です。Windowsクライアントで次のレジストリキーと値を作成します。

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

- キー：HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Policies\Citrix\ICA Client\SFTA
- 値の名前：ExtraURLProtocols
- 値の型：REG_SZ
- 値のデータ：必要なURLタイプをセミコロンで区切って指定します。URLのオーソリティ部分より前のすべてを含めます。例：`ftp://;mailto:;customtype1://;custometype2://`

URLの種類はWindowsクライアントにのみ追加できます。上記のレジストリ設定がないクライアントは、Citrixセッションへのリダイレクトを拒否します。クライアントには、指定されたURLの種類を処理するようにインストールおよび構成されたアプリケーションが必要です。

デフォルトのリダイレクトリストからURLタイプを削除するには、サーバーVDAで次のレジストリキーと値を作成します。

- キー：HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\SFTA
- 値の名前：DisableServerFTA
- 値の型：DWORD
- 値のデータ: 1
- 値の名前: NoRedirectClasses
- 値の型: REG_MULTI_SZ
- 値のデータ: 次の値の任意の組み合わせを指定します: `http`、`https`、`rtsp`、`rtspu`、`pnm`、または`mms`。複数の値を別々の行に入力します。例:

`http`

`https`

`rtsp`

特定のWebサイトのセットに対してホストからクライアントへのリダイレクトを有効にするには、サーバーVDAでレジストリキーと値を作成します。

- キー: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\SFTA
- 値の名前: ValidSites
- 値の型: REG_MULTI_SZ
- 値のデータ: 任意の完全修飾ドメイン名 (FQDN) の組み合わせを指定します。複数のFQDNを別々の行に入力します。プロトコル (`http://` または `https://`) を含めず、FQDNのみを含めます。FQDNには、アスタリスク (`*`) をワイルドカード文字として左端の位置にのみ含めることができます。このワイルドカードは、RFC 6125 のルールと一致する単一レベルのドメインに一致します。例:

`www.exmaple.com`

`*.example.com`

> **注:**
>
> **ValidSites**キーは、**DisableServerFTA**キーおよび**NoRedirectClasses**キーと併用することはできません。

サーバーVDAのデフォルトブラウザ構成

このセクションで参照されているホストからクライアントへのリダイレクトを有効にすると、サーバーVDA上の以前のデフォルトブラウザー構成はすべて上書きされます。Web URLがリダイレクトされない場合、Citrix Launcherは、`command_backup`レジストリキーで構成されているブラウザーにURLを渡します。このキーはデフォルトでInternet Explorerを指していますが、別のブラウザーへのパスを含むように変更できます。詳しくは、レジストリで管理される機能の一覧にあるサーバーVDAのデフォルトブラウザー構成を参照してください。

ローカルアプリアクセスとURLリダイレクト

はじめに

ローカルアプリアクセスは、ローカルにインストールされたWindowsアプリケーションを、デスクトップを切り替えることなくホストされたデスクトップ環境にシームレスに統合します。ローカルアプリアクセスを使用すると、次のことが可能になります。

- 物理的なラップトップ、PC、またはその他のデバイスにローカルにインストールされているアプリケーションに、仮想デスクトップから直接アクセスできます。
- 柔軟なアプリケーション配信ソリューションを提供します。仮想化できない、またはIT部門が保守していないローカルアプリケーションをユーザーが持っている場合でも、それらのアプリケーションは仮想デスクトップにインストールされているかのように動作します。
- アプリケーションが仮想デスクトップとは別にホストされている場合のダブルホップ遅延を排除します。これを行うには、公開されたアプリケーションへのショートカットをユーザーのWindowsデバイスに配置します。
- 次のようなアプリケーションを使用できます。
  - GoToMeetingなどのビデオ会議ソフトウェア。
  - まだ仮想化されていない特殊なアプリケーションまたはニッチなアプリケーション。
  - ユーザーデバイスからサーバーへ、そしてサーバーからユーザーデバイスへ大量のデータを転送する可能性のあるアプリケーションおよび周辺機器。たとえば、DVDバーナーやTVチューナーなどです。

Citrix Virtual Apps and Desktops™では、ホストされたデスクトップセッションはURLリダイレクトを使用してローカルアプリアクセスアプリケーションを起動します。URLリダイレクトにより、アプリケーションは複数のURLアドレスで利用可能になります。デスクトップセッション内のブラウザーで埋め込みリンクを選択すると、ローカルブラウザー（ブラウザーのURLブロックリストに基づく）が起動します。ブロックリストにないURLに移動した場合、そのURLはデスクトップセッションで再度開かれます。

URLリダイレクトはデスクトップセッションでのみ機能し、アプリケーションセッションでは機能しません。アプリケーションセッションで使用できる唯一のリダイレクト機能は、ホストからクライアントへのコンテンツリダイレクトです。これは、サーバーFTA（ファイルタイプ関連付け）リダイレクトの一種です。このFTAは、HTTP、HTTPS、RTSP、MMSなどの特定のプロトコルをクライアントにリダイレクトします。たとえば、HTTPで埋め込みリンクのみを開く場合、リンクはクライアントアプリケーションで直接開かれます。URLブロックリストまたは許可リストのサポートはありません。

ローカルアプリアクセスが有効になっている場合、ローカルで実行されているアプリケーション、ユーザーがホストするアプリケーションからのリンクとして、またはデスクトップ上のショートカットとしてユーザーに表示されるURLは、次のいずれかの方法でリダイレクトされます。

- ユーザーのコンピューターからホストされたデスクトップへ
- Citrix Virtual Apps and Desktopsサーバーからユーザーのコンピューターへ
- 起動された環境でレンダリングされます（リダイレクトされません）

特定のWebサイトからのコンテンツのリダイレクトパスを指定するには、Virtual Delivery AgentでURL許可リストとURLブロックリストを構成します。これらのリストには、URLリダイレクトポリシー設定を指定する複数文字列のレジストリキーが含まれています。詳細については、「ローカルアプリアクセス ポリシー設定」を参照してください。

URLは、以下の例外を除き、VDAでレンダリングできます。

- 地域/ロケール情報 — msn.comやnews.google.comなど、ロケール情報を必要とするWebサイト（地域に基づいて国固有のページを開く）。たとえば、VDAが英国のデータセンターからプロビジョニングされ、クライアントがインドから接続している場合、ユーザーはin.msn.comが表示されることを期待しますが、実際にはuk.msn.comが表示されます。
- マルチメディアコンテンツ — リッチメディアコンテンツを含むWebサイトは、クライアントデバイスでレンダリングされると、エンドユーザーにネイティブなエクスペリエンスを提供し、高遅延ネットワークでも帯域幅を節約します。この機能は、Silverlightなどの他のメディアタイプを含むサイトをリダイレクトします。このプロセスは安全な環境で行われます。つま

り、管理者が承認したURLはクライアントで実行され、残りのURLはVDAにリダイレクトされます。

URLリダイレクトに加えて、FTAリダイレクトを使用できます。FTAは、セッション内でファイルが検出されたときにローカルアプリケーションを起動します。ローカルアプリが起動された場合、ローカルアプリはそのファイルを開くためにファイルへのアクセス権を持っている必要があります。したがって、ローカルアプリケーションを使用して、ネットワーク共有上またはクライアントドライブ上（クライアントドライブマッピングを使用）にあるファイルのみを開くことができます。たとえば、PDFファイルを開く際に、PDFリーダーがローカルアプリである場合、そのPDFリーダーを使用してファイルが開かれます。ローカルアプリはファイルに直接アクセスできるため、ファイルを開くためのICA®を介したファイルのネットワーク転送は発生しません。

要件、考慮事項、および制限事項

WindowsマルチセッションOS用VDAおよびWindowsシングルセッションOS用VDAの有効なオペレーティングシステムで、ローカルアプリアクセスをサポートしています。ローカルアプリアクセスには、Citrix Workspaceアプリ for Windowsバージョン4.1（最小）が必要です。以下のブラウザーがサポートされています。

- Edge、最新バージョン
- Firefox、最新バージョンおよび延長サポートリリース
- Chrome、最新バージョン

ローカルアプリアクセスとURLリダイレクトを使用する際の以下の考慮事項と制限事項を確認してください。

- ローカルアプリアクセスは、すべてのモニターにまたがる全画面表示の仮想デスクトップ向けに設計されています。
    - ウィンドウモードで実行される仮想デスクトップや、すべてのモニターをカバーしない仮想デスクトップでローカルアプリアクセスを使用すると、ユーザーエクスペリエンスが混乱する可能性があります。
    - 複数モニター — 1つのモニターが最大化されると、そのセッションで起動されたすべてのアプリケーションのデフォルトデスクトップになります。このデフォルトは、後続のアプリケーションが通常別のモニターで起動される場合でも発生します。
    - この機能は1つのVDAをサポートします。複数の同時VDAとの統合はありません。
- 一部のアプリケーションは予期しない動作をし、ユーザーに影響を与える可能性があります。

- ドライブ文字がユーザーを混乱させる可能性があります。たとえば、仮想デスクトップのC:ドライブではなく、ローカルのC:ドライブなどです。
- 仮想デスクトップで利用可能なプリンターは、ローカルアプリケーションでは利用できません。
- 昇格された権限を必要とするアプリケーションは、クライアントホスト型アプリケーションとして起動できません。
- シングルインスタンスアプリケーション（Windows Media Playerなど）に対する特別な処理はありません。
- ローカルアプリケーションは、ローカルマシンのWindowsテーマで表示されます。
- 全画面表示アプリケーションはサポートされていません。これらのアプリケーションには、PowerPointのスライドショーやデスクトップ全体を覆うフォトビューアなど、全画面で開くアプリケーションが含まれます。
- Local App Accessは、ローカルアプリケーションのプロパティ（クライアントのデスクトップやスタートメニューのショートカットなど）をVDAにコピーします。ただし、ショートカットキーや読み取り専用属性などの他のプロパティはコピーしません。
- 重なり合うウィンドウの順序の処理方法をカスタマイズするアプリケーションは、予測できない結果になる可能性があります。たとえば、一部のウィンドウが非表示になることがあります。
- ショートカットはサポートされていません。これには、マイコンピュータ、ごみ箱、コントロールパネル、ネットワークドライブのショートカット、フォルダーのショートカットが含まれます。
- 次のファイルの種類とファイルはサポートされていません。カスタムファイルの種類、関連付けられたプログラムのないファイル、zipファイル、隠しファイル。
- 32ビットと64ビットが混在するクライアントホスト型またはVDAアプリケーションでは、タスクバーのグループ化はサポートされていません。つまり、32ビットのローカルアプリケーションと64ビットのVDAアプリケーションをグループ化することです。
- COMを使用してアプリケーションを起動することはできません。たとえば、Officeアプリケーション内から埋め込みOfficeドキュメントをクリックしても、プロセスの起動が検出されず、ローカルアプリケーションの統合が失敗します。

- ダブルホップシナリオ（ユーザーが別の仮想デスクトップセッション内から仮想デスクトップを起動するケース）はサポートされていません。
- URLリダイレクトは、明示的なURL（つまり、ブラウザのアドレスバーに表示されるURL、またはブラウザに応じてブラウザ内ナビゲーションを使用して見つかるURL）のみをサポートします。

- URLリダイレクトは、アプリケーションセッションではなく、デスクトップセッションでのみ機能します。
- VDAセッションのローカルデスクトップフォルダーでは、ユーザーはファイルを作成できません。
- ローカルで実行されているアプリケーションの複数のインスタンスは、仮想デスクトップ用に設定されたタスクバー設定に従って動作します。ただし、ローカルで実行されているアプリケーションへのショートカットは、それらのアプリケーションの実行中のインスタンスとはグループ化されません。また、ホストされているアプリケーションの実行中のインスタンスや、ホストされているアプリケーションへのピン留めされたショートカットともグループ化されません。ユーザーは、タスクバーからローカルで実行されているアプリケーションのウィンドウのみを閉じることができます。ユーザーはローカルアプリケーションウィンドウをデスクトップのタスクバーとスタートメニューにピン留めできますが、これらのショートカットを使用するとアプリケーションが常に起動するとは限りません。
- **Allow Local App Access**ポリシー設定を**Enabled**に設定すると、ブラウザコンテンツリダイレクトはサポートされません。デフォルトでは、ローカルアプリアクセスは禁止されています。

Windowsとの連携

ローカルアプリアクセスとWindowsとの連携には、次の動作が含まれます。

- Windows 8およびWindows Server 2012のショートカット動作
  - クライアントにインストールされているWindowsストアアプリケーションは、ローカルアプリアクセスのショートカットの一部として列挙されません。
  - 画像ファイルとビデオファイルは、デフォルトでWindowsストアアプリケーションを使用して開かれます。ただし、ローカルアプリアクセスはWindowsストアアプリケーションを列挙し、デスクトップアプリケーションでショートカットを開きます。
- ローカルプログラム
  - Windows 7の場合、フォルダーはスタートメニューにあります。
  - Windows 8の場合、ローカルプログラムは、ユーザーがスタート画面からカテゴリとして**すべてのアプリ**を選択した場合にのみ利用できます。すべてのサブフォルダーがローカルプログラムに表示されるわけではありません。
- アプリケーション用のWindows 8グラフィック機能

  - デスクトップアプリケーションはデスクトップ領域に制限されており、スタート画面とWindows 8スタイルのアプリケーションによって覆われます。
  - ローカルアプリアクセスアプリケーションは、マルチモニターモードではデスクトップアプリケーションのように動作しません。マルチモニターモードでは、スタート画面とデスクトップが異なるモニターに表示されます。

- Windows 8およびローカルアプリアクセスURLリダイレクト
  - Windows 8のInternet Explorerではアドオンが有効になっていないため、URLリダイレクトを有効にするにはデスクトップ版Internet Explorerを使用してください。
  - Windows Server 2012では、Internet Explorerはデフォルトでアドオンを無効にします。URLリダイレクトを実装するには、Internet Explorerの拡張構成を無効にします。その後、Internet Explorerのオプションをリセットして再起動し、標準ユーザー向けにアドオンが有効になっていることを確認してください。

ローカルアプリアクセスとURLリダイレクトを構成する

Citrix Workspace™アプリでローカルアプリアクセスとURLリダイレクトを使用するには：

- ローカルクライアントマシンにCitrix Workspaceアプリをインストールします。Citrix Workspaceアプリのインストール中に両方の機能を有効にすることも、グループポリシーエディターを使用してローカルアプリアクセステンプレートを有効にすることもできます。
- **Allow Local App Access**ポリシー設定を**Enabled**に設定します。URLリダイレクトのURL許可リストおよびブロックリストポリシー設定も構成できます。詳しくは、「ローカルアプリアクセス ポリシー設定」を参照してください。

ローカルアプリアクセスとURLリダイレクトを有効にする

すべてのローカルアプリケーションでローカルアプリアクセスを有効にするには、次の手順に従います。

1. Web Studioにサインインし、左側のペインで**ポリシー**をクリックします。
2. アクションバーで、**ポリシーの作成**をクリックします。
3. ポリシーの作成ウィンドウで、検索ボックスに「Allow Local App Access」と入力し、**選択**をクリックします。
4. 設定の編集ウィンドウで、**許可**を選択します。デフォルトでは、**ローカルアプリアクセスを許可**ポリシーは禁止されています。この設定が許可されている場合、VDAは公開アプリケーションとローカルアプリアクセスのショートカットをセッションで有効にするかどうかをエンドユーザーが決定できるようにします。（この設定が禁止されている場合、公開アプリケーショ

ンとローカルアプリアクセスのショートカットはどちらもVDAでは機能しません。）このポリシー設定は、マシン全体とURLリダイレクトポリシーに適用されます。

5. ポリシーの作成ウィンドウで、検索ボックスに「URL redirection allow list」と入力し、**選択**をクリックします。URLリダイレクト許可リストは、リモートセッションのデフォルトブラウザーで開くURLを指定します。
6. 「設定の編集」ウィンドウで、**追加**をクリックしてURLを追加し、**OK**をクリックします。
7. 「ポリシーの作成」ウィンドウで、検索ボックスに「URL redirection block list」と入力し、**選択**をクリックします。URLリダイレクトブロックリストは、エンドポイントで実行されているデフォルトのブラウザにリダイレクトされるURLを指定します。
8. 「設定の編集」ウィンドウで、**追加**をクリックしてURLを追加し、**OK**をクリックします。
9. 「設定」ページで、**次へ**をクリックします。
10. 「ユーザーとマシン」ページで、該当するデリバリーグループにポリシーを割り当て、**次へ**をクリックします。
11. 「概要」ページで、設定を確認し、**完了**をクリックします。

Citrix Workspaceアプリのインストール中にすべてのローカルアプリケーションでURLリダイレクトを有効にするには、次の手順に従います。

1. マシン上のすべてのユーザーに対してCitrix Workspaceアプリをインストールするときに、URLリダイレクトを有効にします。これにより、URLリダイレクトに必要なブラウザアドオンも登録されます。
2. コマンドプロンプトから、次のいずれかのオプションを使用してCitrix Workspaceアプリをインストールするための適切なコマンドを実行します。

   - CitrixReceiver.exe の場合は、`/ALLOW_CLIENTHOSTEDAPPSURL=1` を使用します。
   - CitrixReceiverWeb.exe の場合は、`/ALLOW_CLIENTHOSTEDAPPSURL=1` を使用します。

グループポリシーエディターを使用してローカルアプリアクセステンプレートを有効にする

> **注:**
>
> - グループポリシーエディターを使用してローカルアプリアクセステンプレートを有効にする前に、receiver.admx/admlテンプレートファイルをローカルGPOに追加します。

- Windows用Citrix Workspaceアプリのテンプレートファイルは、CitrixBase.admx/CitrixBase.admlを%systemroot%\policyDefinitionsフォルダーに追加した場合にのみ、ローカルGPOの**管理用テンプレート > Citrixコンポーネント > Citrix Workspace**フォルダーで利用できます。

グループポリシーエディターを使用してローカルアプリアクセステンプレートを有効にするには、次の手順に従います。

1. **gpedit.msc**を実行します。
2. **コンピューターの構成 > 管理用テンプレート > クラシック管理用テンプレート (ADM) > Citrix Components > Citrix Workspace > ユーザーエクスペリエンス**に移動します。
3. **ローカルアプリアクセス設定**をクリックします。
4. **有効**を選択し、次に**URLリダイレクトを許可**を選択します。URLリダイレクトの場合、この記事の後半にある「*ブラウザアドオンの登録*」セクションで説明されているコマンドラインを使用して、ブラウザアドオンを登録します。

公開アプリケーションのみにアクセスを許可する

レジストリエディターまたはPowerShell SDKを使用して、公開アプリケーションへのアクセスを提供できます。

レジストリエディターについては、レジストリを介して管理される機能のリストにある「公開アプリケーションのローカルアプリアクセス」を参照してください。

PowerShell SDKを使用するには：

1. Delivery Controller™が実行されているマシンでPowerShellを開きます。
2. 次のコマンドを入力します：`set-configsitemetadata -name "studio_clientHostedAppsEnabled" -value "true"`。

クラウドサービス展開で**ローカルアプリアクセスアプリケーションの追加**にアクセスするには、Citrix DaaS Remote PowerShell SDKを使用します。詳しくは、「Citrix DaaS Remote PowerShell SDK」を参照してください。

1. インストーラーをダウンロードします：

   `<https://download.apps.cloud.com/CitrixPoshSdk.exe>`

2. 次のコマンドを実行します：

a. `asnp citrix.*`.

b. `Get-XdAuthentication`

3. 次のコマンドを入力します: `set-configsitemetadata -name "studio_clientHostedAppsEnabled" -value "true"`。

該当する前の手順を完了したら、以下の手順に従って続行します。

1. Web Studioにサインインし、左側のペインで**アプリケーション**を選択します。
2. 上部中央のペインで、空白領域を右クリックし、コンテキストメニューから**ローカルアプリアクセスアプリケーションの追加**を選択します。アクションバーで**ローカルアプリアクセスアプリケーションの追加**をクリックすることもできます。アクションバーにローカルアプリアクセスアプリケーションの追加オプションを表示するには、**更新**をクリックします。
3. ローカルアプリアクセスアプリケーションを公開します。

   - ローカルアプリケーションアクセスウィザードが起動し、はじめにページが表示されます。このページは、今後のウィザード起動時に表示しないように設定できます。
   - ウィザードは、以下に説明するグループ、場所、識別、配信、概要の各ページを案内します。各ページの作業が完了したら、概要ページに到達するまで**次へ**をクリックします。
   - グループページで、新しいアプリケーションを追加するデリバリーグループを1つ以上選択し、**次へ**をクリックします。
   - 場所ページで、ユーザーのローカルマシン上のアプリケーションの完全な実行可能パスと、アプリケーションが配置されているフォルダーへのパスを入力します。Citrixでは、システム環境変数パスを使用することをお勧めします。例: %ProgramFiles(x86)%\Internet Explorer\iexplore.exe。
   - 識別ページで、デフォルト値を受け入れるか、必要な情報を入力してから**次へ**をクリックします。
   - 配信ページで、このアプリケーションをユーザーに配信する方法を設定し、**次へ**をクリックします。選択したアプリケーションのアイコンを指定できます。また、仮想デスクトップ上のローカルアプリケーションへのショートカットを、スタートメニュー、デスクトップ、またはその両方に表示するかどうかを指定することもできます。
   - 概要ページで設定を確認し、**完了**をクリックしてローカルアプリケーションアクセスウィザードを終了します。

ブラウザアドオンの登録

> **注:**

> URLリダイレクトに必要なブラウザアドオンは、コマンドラインからCitrix Workspaceアプリを/ALLOW_CLIENTHOSTEDAPPSURL=1オプションを使用してインストールすると、自動的に登録されます。

> 1つまたはすべてのアドオンを登録および登録解除するには、次のコマンドを使用します。

- クライアントデバイスでアドオンを登録するには: \<*client-installation-folder*>\redirector.exe /reg\<*browser*>
- クライアントデバイスでアドオンの登録を解除するには: \<*client-installation-folder*>\redirector.exe /unreg\<*browser*>
- VDAでアドオンを登録するには: \<*VDAinstallation-folder*>\VDARedirector.exe /reg\<*browser*>
- VDAでアドオンの登録を解除するには: \<*VDAinstallation-folder*>\VDARedirector.exe /unreg\<*browser*>

ここで、\<*browser*>はInternet Explorer、Firefox、Chrome、またはAllです。

たとえば、次のコマンドは、Citrix Workspaceアプリを実行しているデバイスにInternet Explorerアドオンを登録します。

C:\Program Files\Citrix\ICA Client\redirector.exe/regIE

次のコマンドは、WindowsマルチセッションOS VDA上のすべてのアドオンを登録します。

C:\Program Files (x86)\Citrix\HDX\bin\VDARedirector.exe /regAll

ブラウザ間のURLインターセプト

- デフォルトでは、Internet Explorerは指定されたURLをリダイレクトします。URLがブロックリストにない場合でも、ブラウザまたはWebサイトが別のURLにリダイレクトすると、最終的なURLはリダイレクトされません。ブロックリストにある場合でもリダイレクトされません。

URLリダイレクトが正しく機能するには、ブラウザからプロンプトが表示されたときにアドオンを有効にしてください。インターネットオプションを使用しているアドオン、またはプロンプト内のアドオンが無効になっている場合、URLリダイレクトは正しく機能しません。

- Firefoxのアドオンは常にURLをリダイレクトします。

アドオンがインストールされると、Firefoxは新しいタブページにアドオンのインストールを許可するか、または防止するかを尋ねます。機能が動作するようにアドオンを許可してください。

- Chromeのアドオンは、入力されたURLではなく、常にナビゲートされた最終URLをリダイレクトします。

拡張機能は外部からインストールされています。拡張機能を無効にすると、ChromeでURLリダイレクト機能が動作しません。シークレットモードでURLリダイレクトが必要な場合は、ブラウザ設定でそのモードでの拡張機能の実行を許可してください。

ログオフ時および切断時のローカルアプリケーションの動作を構成する

> **注:**
>
> これらの手順に従って設定を構成しない場合、デフォルトでは、ユーザーが仮想デスクトップからログオフまたは切断しても、ローカルアプリケーションは引き続き実行されます。再接続後、ローカルアプリケーションが仮想デスクトップで利用可能な場合、それらは再統合されます。

ログオフ時および切断時のローカルアプリケーションの動作を構成するには、レジストリを介して管理される機能のリストにあるログオフ時および切断時のローカルアプリケーションの動作を参照してください。

印刷

環境内のプリンターの管理は、多段階のプロセスです。

1. まだ印刷の概念に慣れていない場合は、慣れてください。
2. 印刷アーキテクチャを計画します。これには、ビジネスニーズ、既存の印刷インフラストラクチャ、ユーザーとアプリケーションが現在印刷とどのようにやり取りしているか、およびどの印刷管理モデルが環境に最適かを分析することが含まれます。
3. プリンターのプロビジョニング方法を選択し、印刷設計を展開するためのポリシーを作成して、印刷環境を構成します。新しい従業員やサーバーが追加されたときにポリシーを更新します。
4. ユーザーに展開する前に、パイロット印刷構成をテストします。
5. プリンタードライバーを管理し、印刷パフォーマンスを最適化することで、Citrix® 印刷環境を維持します。
6. 発生する可能性のある問題をトラブルシューティングします。

印刷の概念

展開の計画を開始する前に、印刷に関する以下の主要な概念を理解していることを確認してください。

- 利用可能なプリンタープロビジョニングの種類
- 印刷ジョブがどのようにルーティングされるか
- プリンタードライバー管理の基本

印刷の概念は、Windows の印刷の概念に基づいています。環境内で印刷を構成し、正常に管理するには、Windows のネットワーク印刷とクライアント印刷がどのように機能するか、およびそれがこの環境での印刷動作にどのように変換されるかを理解する必要があります。

印刷プロセス

この環境では、すべての印刷はアプリケーションをホストするマシン上で（ユーザーによって）開始されます。印刷ジョブは、ネットワークプリントサーバーまたはユーザーデバイスを介して印刷デバイスにリダイレクトされます。

仮想デスクトップおよびアプリケーションのユーザーには、永続的なワークスペースはありません。セッションが終了すると、ユーザーのワークスペースは削除されるため、すべての設定は各セッションの開始時に再構築される必要があります。その結果、ユーザーが新しいセッションを開始するたびに、システムはユーザーのワークスペースを再構築する必要があります。

ユーザーが印刷する場合：

- ユーザーに提供するプリンターを決定します。これはプリンタープロビジョニングとして知られています。
- ユーザーの印刷設定を復元します。
- セッションのデフォルトプリンターを決定します。

プリンタープロビジョニング、印刷ジョブのルーティング、プリンタープロパティの保持、およびドライバー管理のオプションを構成することで、これらのタスクの実行方法をカスタマイズできます。さまざまなオプション設定が、環境での印刷パフォーマンスとユーザーエクスペリエンスにどのように影響するかを評価するようにしてください。

プリンタープロビジョニング

セッションでプリンターを利用可能にするプロセスは、プロビジョニングとして知られています。プリンタープロビジョニングは通常、動的に処理されます。つまり、セッションに表示されるプリンターは事前に決定されて保存されるわけではありません。代わりに、ログオン時および再接続時にセッションが構築される際に、ポリシーに基づいてプリンターが組み立てられます。その結果、ポリシーに反映されていれば、プリンターはポリシー、ユーザーの場所、およびネットワークの変更に応じて変更される可能性があります。したがって、異なる場所に移動するユーザーは、ワークスペースの変更を確認する場合があります。

システムはまた、クライアント側のプリンターを監視し、クライアント側のプリンターへの追加、削除、変更に基づいて、セッション内で自動作成されたプリンターを動的に調整します。この動的なプリンター検出は、モバイルユーザーがさまざまなデバイスから接続する際に役立ちます。

プリンタープロビジョニングの最も一般的な方法は次のとおりです。

- **Universal Print Server** - Citrix Universal Print Server は、ネットワークプリンターのユニバーサル印刷サポートを提供します。Universal Print Server は、ユニバーサル印刷ドライバーを使用します。このソリューションにより、マルチセッションOSマシンで単一のドライバーを使用して、任意のデバイスからネットワーク印刷を行うことができます。

Citrix は、リモートプリントサーバーのシナリオで Citrix Universal™ Print Server を推奨しています。Universal Print Server は、最適化され圧縮された形式で印刷ジョブをネットワーク経由で転送するため、ネットワーク使用量を最小限に抑え、ユーザーエクスペリエンスを向上させます。

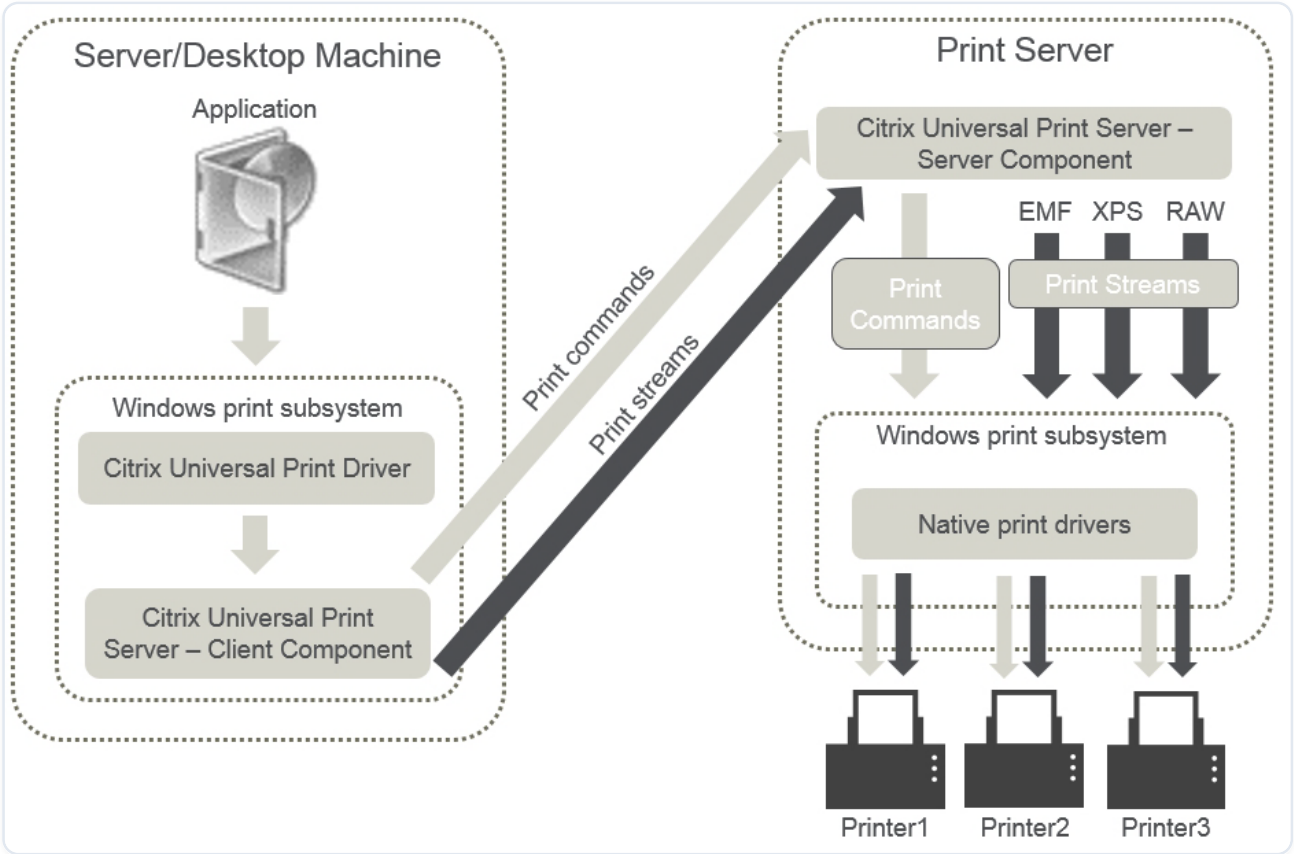
Universal Print Server の機能は次のとおりです。

クライアントコンポーネント、**UPClient** - セッションネットワークプリンターをプロビジョニングし、ユニバーサル印刷ドライバーを使用する各マルチセッションOSマシンでUPClientを有効にします。

サーバーコンポーネントである **UPServer** - セッションネットワークプリンターをプロビジョニングし、セッションプリンターにユニバーサルプリントドライバーを使用する（セッションプリンターが集中管理されているかどうかにかかわらず）各プリントサーバーにUPServerをインストールします。

Universal Print Serverの要件とセットアップの詳細については、システム要件とインストールの記事を参照してください。

次の図は、Universal Print Serverを使用する環境におけるネットワークベースのプリンターの一般的なワークフローを示しています。



Citrix Universal Print Serverを有効にすると、接続されているすべてのネットワークプリンターが自動検出によって自動的にそれを利用します。

- **自動作成** - *自動作成*とは、各セッションの開始時に自動的に作成されるプリンターを指します。リモートネットワークプリンターとローカルに接続されたクライアントプリンターの両方を自動作成できます。ユーザーあたりのプリンター数が多い環境では、デフォルトのクライアントプリンターのみを自動作成することを検討してください。自動作成するプリンターの数を減らすと、マルチセッションOSマシンでのオーバーヘッド（メモリとCPU）が少なくなります。自動作成されるプリンターを最小限に抑えることで、ユーザーのログオン時間を短縮することもできます。

  自動作成されたプリンターは、以下に基づいています。

  - ユーザーデバイスにインストールされているプリンター。
  - セッションに適用されるポリシー。

    自動作成ポリシー設定により、自動作成されるプリンターの数または種類を制限できます。デフォルトでは、ローカルに接続されたプリンターとネットワークプリンターを含む、ユーザーデバイス上のすべてのプリンターを自動的に構成すると、プリンターはセッションで利用可能になります。

  ユーザーがセッションを終了すると、そのセッションのプリンターは削除されます。

  クライアントおよびネットワークプリンターの自動作成には、関連するメンテナンスが必要です。たとえば、プリンターを追加するには、次の操作が必要です。

  - セッションプリンターポリシー設定を更新します。
  - プリンタードライバーマッピングおよび互換性ポリシー設定を使用して、すべてのマルチセッションOSマシンにドライバーを追加します。

印刷ジョブのルーティング

印刷経路という用語は、印刷ジョブがルーティングされる経路と、印刷ジョブがスプールされる場所の両方を包含します。この概念の両方の側面が重要です。ルーティングはネットワークトラフィックに影響します。スプールは、ジョブを処理するデバイスのローカルリソースの利用に影響します。

この環境では、印刷ジョブは印刷デバイスへ2つの経路を取ることができます。クライアント経由、またはネットワーク印刷サーバー経由です。これらの経路は、クライアント印刷経路およびネットワーク印刷経路と呼ばれます。どちらの経路がデフォルトで選択されるかは、使用されるプリンターの種類によって異なります。

ローカル接続プリンター

システムは、マルチセッションOSマシンからクライアントを介して、ローカルに接続されたプリンターにジョブをルーティングし、その後印刷デバイスに送信します。ICA®プロトコルは、印刷ジョブのトラフィックを最適化し、圧縮します。印刷デバイスがユーザーデバイスにローカルに接続されている場合、印刷ジョブはICA仮想チャネルを介してルーティングされます。

ローカル接続プリンターへの印刷ジョブのルーティング図(/en-us/citrix-virtual-apps-desktops/2503/media/cds-print-local-attached.png)

ネットワークベースのプリンター

デフォルトでは、ネットワークプリンター宛てのすべての印刷ジョブは、マルチセッションOSマシンからネットワーク経由で直接印刷サーバーにルーティングされます。ただし、以下の状況では、印刷ジョブはICA接続経由で自動的にルーティングされます。

- 仮想デスクトップまたはアプリケーションが印刷サーバーに接続できない場合。
- マルチセッションOSマシンでネイティブプリンタードライバーが利用できない場合。

Universal Print Serverが有効になっていない場合、ネットワーク印刷用にクライアント印刷経路を構成することは、ICA接続経由でジョブを送信することによって得られる最適化とトラフィック圧縮の恩恵を受けることができる、広域ネットワークなどの低帯域幅接続に役立ちます。

クライアント印刷経路を使用すると、印刷ジョブに割り当てられるトラフィックを制限したり、帯域幅を制限したりすることもできます。印刷機能のないシンクライアントなどの場合で、ユーザーデバイス経由でジョブをルーティングできない場合は、ICA/HDXトラフィックを優先し、良好なセッション内ユーザーエクスペリエンスを確保するために、Quality of Serviceを構成する必要があります。

ネットワーク接続プリンターへの印刷ジョブのルーティング図(/en-us/citrix-virtual-apps-desktops/2503/media/cds-print-network-attached.png)

印刷ドライバー管理

Citrix Universal Printer Driver (UPD) は、ほとんどのプリンターと互換性のある、デバイスに依存しない印刷ドライバーです。Citrix UPDは2つのコンポーネントで構成されています。

サーバーコンポーネント。Citrix UPD は、Citrix Virtual Apps and Desktops™ VDA のインストールの一部としてインストールされます。VDA は、Citrix UPD とともに以下のドライバーをインストールします：「Citrix Universal Printer」（EMF ドライバー）と「Citrix XPS Universal Printer」（XPS ドライバー）。

Name	Processor	Type
Citrix Universal Printer	x64	Type 3 - User Mode
Citrix XPS Universal Printer	x64	Type 3 - User Mode

VDAインストーラーでは、Universal Print Server PDFプリンタードライバーのインストールを制御するオプションが提供されなくなりました。PDFプリンタードライバーは常に自動的にインストールされるようになりました。7.17 VDA（またはそれ以降のサポート対象バージョン）にアップグレードすると、以前にインストールされていたCitrix PDFプリンタードライバーは自動的に削除され、最新バージョンに置き換えられます。

印刷ジョブが開始されると、ドライバーはアプリケーションの出力を記録し、変更を加えることなくエンドポイントデバイスに送信します。

クライアントコンポーネント。Citrix UPDは、Citrix Workspace™アプリのインストールの一部としてインストールされます。Citrix Virtual Apps and Desktopsセッションの受信印刷ストリームを取得します。その後、印刷ストリームをローカル印刷サブシステムに転送し、そこでデバイス固有のプリンタードライバーを使用して印刷ジョブがレンダリングされます。

Citrix UPDは、以下の印刷形式をサポートしています。

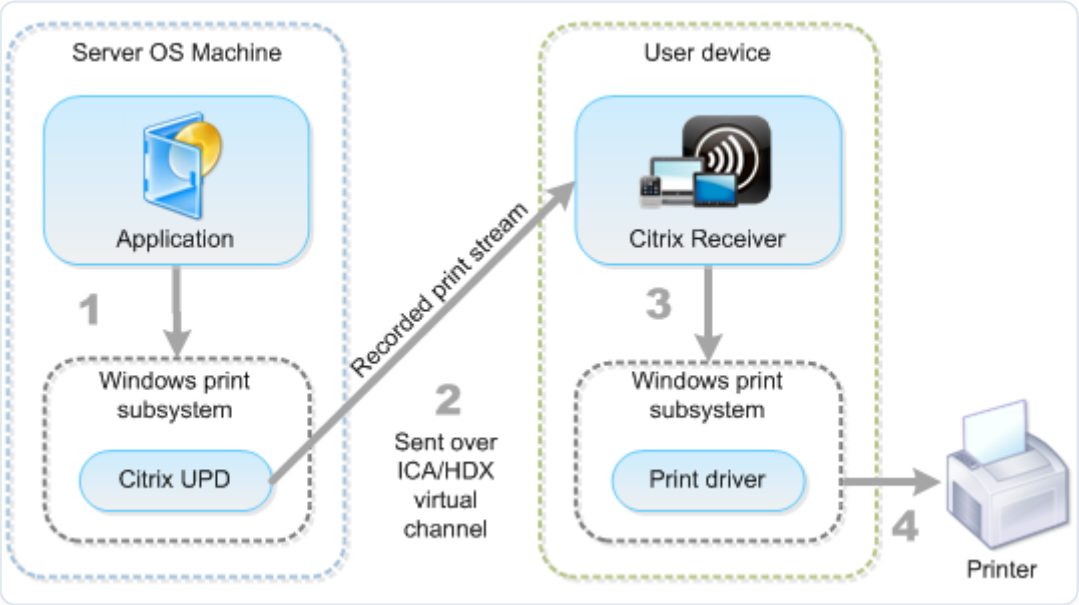
- 拡張メタファイル形式（**EMF**）、デフォルト。EMFは、Windowsメタファイル（WMF）形式の32ビットバージョンです。EMFドライバーは、Windowsベースのクライアントのみが使用できます。
- XML Paper Specification（**XPS**）。XPSドライバーはXMLを使用して、Adobe PDF形式に似たプラットフォームに依存しない「電子ペーパー」を作成します。
- Printer Command Language（**PCL5c**および**PCL4**）。PCLは、もともとHewlett-Packardがインクジェットプリンター向けに開発した印刷プロトコルです。基本的なテキストとグラフィックの印刷に使用され、HP LaserJetおよび多機能周辺機器で広くサポートされています。
- PostScript（**PS**）。PostScriptは、テキストやベクターグラフィックの印刷に使用できるコンピューター言語です。このドライバーは、低コストのプリンターや多機能周辺機器で広く使用されています。

PCLおよびPSドライバーは、MacやUNIXクライアントなどのWindows以外のデバイスを使用する場合に最適です。Citrix UPDがドライバーを使用しようとする順序は、Universal driver preferenceポリシー設定を使用して変更できます。

Citrix UPD（EMFおよびXPSドライバー）は、ステープルや用紙トレイ選択などの高度な印刷機能をサポートしています。これらの機能は、ネイティブドライバーがMicrosoft Print Capabilityテクノロジーを使用して利用可能にしている場合に利用できます。ネイティブドライバーは、Print Capabilities XMLで標準化されたPrint Schema Keywordsを使用する必要があります。非標準の

キーワードが使用されている場合、Citrix Universal Print Driverでは高度な印刷機能は利用できません。

次の図は、Universal Print Driverのコンポーネントと、デバイスにローカルに接続されたプリンターの一般的なワークフローを示しています。



ドライバー管理戦略を計画する際には、Universal Print Driver、デバイス固有のドライバー、またはその両方をサポートするかどうかを決定します。標準ドライバーをサポートする場合は、以下を決定する必要があります。

プリンターの自動作成中に、システムがユーザーデバイスに接続された新しいローカルプリンターを検出すると、Multi-session OSマシンで必要なプリンタードライバーをチェックします。デフォルトでは、Windowsネイティブドライバーが利用できない場合、システムはUniversal Print Driverを使用します。

印刷を成功させるには、Multi-session OSマシン上のプリンタードライバーとユーザーデバイス上のドライバーが一致している必要があります。次の図は、クライアント印刷でプリンタードライバーが2か所でどのように使用されるかを示しています。

クライアントがローカルプリンターに印刷する図(/en-us/citrix-virtual-apps-desktops/2503/media/cds-print-client-routing.png)

- サポートするドライバーの種類。
- Multi-session OS マシンにプリンタードライバーがない場合に、自動的にインストールするかどうか。
- ドライバー互換性リストを作成するかどうか。

関連コンテンツ

- 印刷構成の例(/ja-jp/citrix-virtual-apps-desktops/2503/printing/printing-configuration-example.html)
- ベストプラクティス、セキュリティに関する考慮事項、およびデフォルトの操作(/ja-jp/citrix-virtual-apps-desktops/2503/printing/printing-best-practices.html)
- 印刷ポリシーと設定(/ja-jp/citrix-virtual-apps-desktops/2503/printing/printing-policies-preferences.html)
- プリンターのプロビジョニング(/ja-jp/citrix-virtual-apps-desktops/2503/printing/printing-provision-printers.html)
- 印刷環境の維持(/ja-jp/citrix-virtual-apps-desktops/2503/printing/printing-maintain-environment.html)

印刷構成の例

ニーズと環境に最も適した印刷構成オプションを選択することで、管理を簡素化できます。デフォルトの印刷構成はほとんどの環境でユーザーが印刷できるようにしますが、デフォルトでは期待されるユーザーエクスペリエンスや、環境にとって最適なネットワーク使用量と管理オーバーヘッドを提供できない場合があります。

印刷構成は以下に依存します。

- ビジネスニーズと既存の印刷インフラストラクチャ。

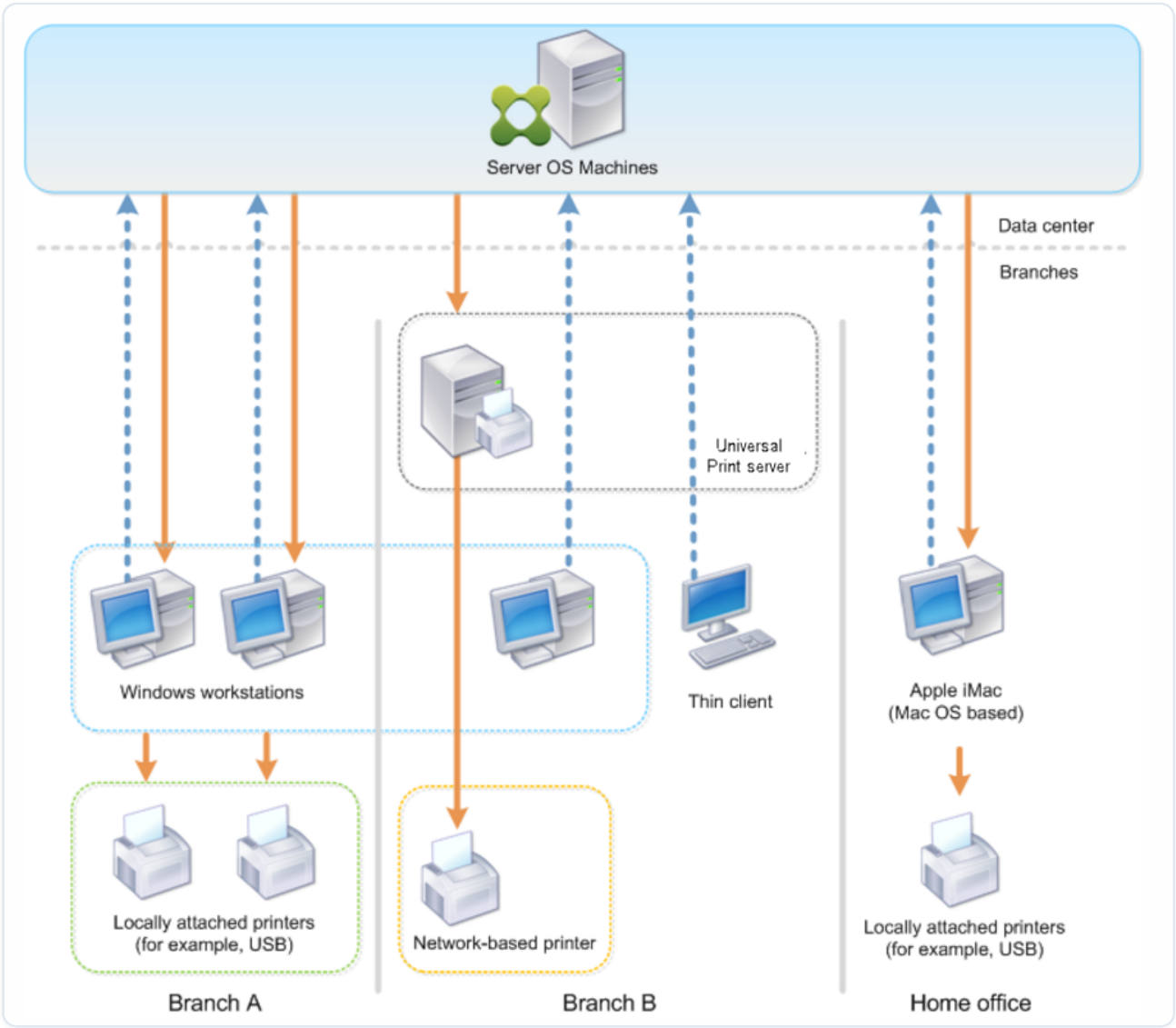
  組織のニーズに合わせて印刷構成を設計してください。既存の印刷実装（ユーザーがプリンターを追加できるか、どのユーザーがどのプリンターにアクセスできるかなど）は、印刷構成を定義する際に役立つガイドとなる場合があります。
- 組織に特定のユーザー（例えば、人事部や給与計算用のプリンター）のためにプリンターを予約するセキュリティポリシーがあるかどうか。
- ユーザーが主要な作業場所から離れているときに印刷する必要があるかどうか（ワークステーション間を移動する作業者や出張中の作業者など）。

印刷構成を設計する際は、ユーザーがローカルユーザーデバイスから印刷する場合と同じエクスペリエンスをセッション内で得られるように努めてください。

印刷展開の例

次の図は、これらのユースケースの印刷展開を示しています。

- **支社A** - 少数のWindowsワークステーションを持つ小規模な海外支社。各ユーザーワークステーションには、ローカルに接続されたプライベートプリンターがあります。
- **支社B** - シンクライアントとWindowsベースのワークステーションを持つ大規模な支社。効率向上のため、この支社のユーザーはネットワークベースのプリンター（フロアごとに1台）を共有しています。支社内にあるWindowsベースのプリントサーバーが印刷キューを管理します。
- **ホームオフィス** - 会社のCitrix®インフラストラクチャにアクセスするMac OSベースのユーザーデバイスを持つホームオフィス。ユーザーデバイスにはローカルに接続されたプリンターがあります。



以下のセクションでは、環境の複雑さを最小限に抑え、その管理を簡素化する構成について説明します。

自動作成されたクライアントプリンターとCitrix Universal™ プリンタードライバー

支店Aでは、すべてのユーザーがWindowsベースのワークステーションで作業しているため、自動作成されたクライアントプリンターとユニバーサルプリンタードライバーが使用されます。これらのテクノロジーには、次の利点があります。

- パフォーマンス - 印刷ジョブはICA®印刷チャネルを介して配信されるため、印刷データを圧縮して帯域幅を節約できます。

  大容量のドキュメントを印刷する単一のユーザーが他のユーザーのセッションパフォーマンスを低下させないようにするため、最大印刷帯域幅を指定するようにCitrixポリシーが構成されています。

  代替ソリューションとして、印刷トラフィックが個別の低優先度TCP接続内で転送されるマルチストリームICA接続を活用する方法があります。マルチストリームICAは、WAN接続でQuality of Service (QoS) が実装されていない場合のオプションです。
- 柔軟性 - Citrix Universalプリンタードライバーを使用すると、データセンターに新しいプリンタードライバーを統合することなく、クライアントに接続されているすべてのプリンターを仮想デスクトップまたはアプリケーションセッションから使用できます。

Citrix ユニバーサルプリントサーバー

支店Bでは、すべてのプリンターがネットワークベースであり、そのキューはWindowsプリントサーバーで管理されているため、Citrix Universal Print Serverが最も効率的な構成です。

必要なすべてのプリンタードライバーは、ローカル管理者によってプリントサーバーにインストールおよび管理されます。プリンターを仮想デスクトップまたはアプリケーションセッションにマッピングする方法は次のとおりです。

- Windowsベースのワークステーションの場合 - ローカルITチームは、ユーザーが適切なネットワークベースのプリンターをWindowsワークステーションに接続するのを支援します。これにより、ユーザーはローカルにインストールされたアプリケーションから印刷できます。

  仮想デスクトップまたはアプリケーションセッション中に、ローカルで構成されたプリンターは自動作成によって列挙されます。その後、仮想デスクトップまたはアプリケーションは、可能であれば直接ネットワーク接続としてプリントサーバーに接続します。

  Citrix Universal Print Serverコンポーネントがインストールされ、有効になっているため、ネイティブプリンタードライバーは必要ありません。ドライバーが更新されたり、プリンターキューが変更されたりしても、データセンターで追加の構成は必要ありません。

- シンクライアントの場合 - シンクライアントユーザーの場合、プリンターは仮想デスクトップまたはアプリケーションセッション内で接続する必要があります。ユーザーに最もシンプルな印刷エクスペリエンスを提供するために、管理者は、フロアごとに単一のCitrixセッションプリンターポリシーを構成して、フロアのプリンターをデフォルトプリンターとして接続します。

  ユーザーがフロア間を移動しても正しいプリンターが接続されるようにするため、ポリシーはサブネットまたはシンクライアントの名前に基づいてフィルタリングされます。この構成は近接印刷と呼ばれ、ローカルプリンタードライバーのメンテナンスを可能にします（委任された管理モデルに従って）。

  プリンターキューを変更または追加する必要がある場合、Citrix管理者は、環境内でそれぞれのセッションプリンターポリシーを変更する必要があります。

ネットワーク印刷トラフィックはICA仮想チャネル外に送信されるため、QoSが実装されます。ICA/HDXトラフィックで使用されるポートのインバウンドおよびアウトバウンドネットワークトラフィックは、他のすべてのネットワークトラフィックよりも優先されます。この構成により、ユーザーセッションが大規模な印刷ジョブの影響を受けないことが保証されます。

自動作成されたクライアントプリンターとCitrixユニバーサルプリンタードライバー

ユーザーが標準外のワークステーションで作業し、管理されていない印刷デバイスを使用するホームオフィスの場合、最も簡単なアプローチは、自動作成されたクライアントプリンターとユニバーサルプリンタードライバーを使用することです。

展開の概要

まとめると、サンプルの展開は次のように構成されています。

- マルチセッションOSマシンにはプリンタードライバーはインストールされません。Citrixユニバーサルプリンタードライバーのみが使用されます。ネイティブ印刷へのフォールバックとプリンタードライバーの自動インストールは無効になっています。
- すべてのユーザーに対してすべてのクライアントプリンターを自動作成するようにポリシーが構成されています。マルチセッションOSマシンは、デフォルトで印刷サーバーに直接接続します。必要な構成は、ユニバーサルプリントサーバーコンポーネントを有効にすることだけです。
- 支店Bの各フロアにセッションプリンターポリシーが構成され、各フロアのすべてのシンクライアントに適用されます。
- 優れたユーザーエクスペリエンスを保証するために、支店BにはQoSが実装されています。

ベストプラクティス、セキュリティに関する考慮事項、およびデフォルトの操作

ベストプラクティス

特定の環境に最適な印刷ソリューションを決定する要因は多数あります。これらのベストプラクティスの一部は、お客様のサイトには適用されない場合があります。

- Citrix Universal™ Print Serverを使用します。
- UniversalプリンタードライバーまたはWindowsネイティブドライバーを使用します。
- マルチセッションOSマシンにインストールされているプリンタードライバーの数を最小限に抑えます。
- ネイティブドライバーへのドライバーマッピングを使用します。
- 未テストのプリンタードライバーを本番環境にインストールしないでください。
- ドライバーの更新は避けてください。常にドライバーをアンインストールし、プリントサーバーを再起動してから、交換用ドライバーをインストールするようにしてください。
- 未使用のドライバーをアンインストールするか、プリンタードライバーマッピングと互換性ポリシーを使用して、そのドライバーでプリンターが作成されないようにします。
- バージョン2のカーネルモードドライバーの使用は避けてください。
- プリンターモデルがサポートされているかどうかを確認するには、製造元に問い合わせるか、www.citrix.com/readyにあるCitrix Ready製品ガイドを参照してください。

  一般的に、Microsoftが提供するすべてのプリンタードライバーはTerminal Servicesでテストされており、Citrixで動作することが保証されています。ただし、サードパーティのプリンタードライバーを使用する前に、Windows Hardware Quality Labs (WHQL) プログラムによってTerminal Services向けにドライバーが認定されていることをプリンタードライバーベンダーに確認してください。Citrixはプリンタードライバーを認定しません。

セキュリティに関する考慮事項

Citrixの印刷ソリューションは、設計上安全です。

- Citrix Print Manager Service は、ログオンとログオフ、切断、再接続、セッション終了などのセッションイベントを常に監視し、対応します。実際のセッションユーザーを偽装してサービス要求を処理します。
- Citrix の印刷機能は、各プリンターにセッション内で一意の名前空間を割り当てます。

- Citrix の印刷機能は、自動作成されたプリンターのデフォルトのセキュリティ記述子を設定し、あるセッションで自動作成されたクライアントプリンターが他のセッションで実行されているユーザーからアクセスできないようにします。デフォルトでは、管理ユーザーは、任意のクライアントプリンターの権限を表示および手動で調整できる場合でも、誤って別のセッションのクライアントプリンターに印刷することはできません。

デフォルトの印刷操作

デフォルトでは、ポリシー規則を何も構成しない場合、印刷動作は次のとおりです。

- ユニバーサルプリントサーバーは無効になります。
- ユーザーデバイスで構成されているすべてのプリンターは、各セッションの開始時に自動的に作成されます。

  この動作は、Citrixポリシー設定「クライアントプリンターの自動作成」を「すべてのクライアントプリンターを自動作成」オプションで構成することに相当します。
- システムは、ユーザーデバイスにローカルに接続されたプリンターにキューイングされたすべての印刷ジョブを、クライアント印刷ジョブとして（つまり、ICA®チャネル経由でユーザーデバイスを介して）ルーティングします。
- システムは、ネットワークプリンターにキューイングされたすべての印刷ジョブを、Multi-session OS マシンから直接ルーティングします。システムがネットワーク経由でジョブをルーティングできない場合、ユーザーデバイスを介してリダイレクトされたクライアント印刷ジョブとしてルーティングします。

  この動作は、Citrixポリシー設定「プリントサーバーへの直接接続」を無効にすることに相当します。
- システムは、ユーザーの印刷設定と印刷デバイス固有の設定を組み合わせた印刷プロパティを、ユーザーデバイスに保存しようとします。クライアントがこの操作をサポートしない場合、システムは印刷プロパティを Multi-session OS マシンのユーザープロファイルに保存します。

  この動作は、Citrixポリシー設定「プリンタープロパティの保持」を「クライアントに保存されていない場合のみプロファイルに保持」オプションで構成することに相当します。
- VDAバージョン7.16以降では、V3インボックスプリンタードライバーがオペレーティングシステムに含まれていないため、Citrixポリシー設定「インボックスプリンタードライバーの自動インストール」はWindows 8以降のWindowsオペレーティングシステムバージョンには影響しません。

- 7.16より前のVDAでは、Multi-session OSマシンで利用可能な場合、システムはプリンタードライバーのWindowsバージョンを使用します。プリンタードライバーが利用できない場合、システムはWindowsオペレーティングシステムからドライバーをインストールしようとします。ドライバーがWindowsで利用できない場合、Citrixユニバーサルプリントドライバーを使用します。

  この動作は、Citrixポリシー設定「インボックスプリンタードライバーの自動インストール」を有効にし、ユニバーサル印刷設定を「要求されたドライバーが利用できない場合のみユニバーサル印刷を使用」で構成することに相当します。

  「インボックスプリンタードライバーの自動インストール」を有効にすると、多数のネイティブプリンタードライバーがインストールされる可能性があります。

> **注:**
>
> 印刷の出荷時デフォルト設定が不明な場合は、新しいポリシーを作成し、すべての印刷ポリシー規則を「有効」に設定して表示します。表示されるオプションがデフォルトです。

常時オンのログ記録

VDA上のプリントサーバーおよび印刷サブシステムで、常時オンのログ記録機能が利用可能です。

ログをZIP形式でまとめてメール送信する場合、またはCitrix Insight Servicesにログを自動的にアップロードする場合は、**Start-TelemetryUpload** PowerShellコマンドレットを使用します。

印刷ポリシーと設定

ユーザーが公開アプリケーションからプリンターにアクセスする際、Citrix®ポリシーを設定して以下を指定できます。

- プリンターがどのようにプロビジョニングされるか（またはセッションに追加されるか）
- 印刷ジョブがどのようにルーティングされるか
- プリンタードライバーがどのように管理されるか

異なるユーザーデバイス、ユーザー、またはポリシーがフィルターされるその他のオブジェクトに対して、異なる印刷構成を設定できます。

ほとんどの印刷機能は、Citrixの印刷ポリシー設定を通じて構成されます。印刷設定は標準のCitrixポリシー動作に従います。

ユーザーのネットワークアカウントに十分な権限がある場合、システムはセッションの終了時にプリンター設定をプリンターオブジェクトまたはクライアント印刷デバイスに書き込むことができます。デフォルトでは、Citrix Workspace™アプリは、設定や環境設定を他の場所で探す前に、セッション内のプリンターオブジェクトに保存されている設定を使用します。

デフォルトでは、システムはプリンタープロパティをユーザーデバイス上（デバイスがサポートしている場合）またはMulti-session OSマシンのユーザープロファイルに保存または保持します。ユーザーがセッション中にプリンタープロパティを変更すると、それらの変更はマシンのユーザープロファイルに更新されます。ユーザーが次回ログオンまたは再接続すると、ユーザーデバイスは保持された設定を継承します。つまり、ユーザーデバイスでのプリンタープロパティの変更は、ユーザーがログオフして再度ログオンするまで、現在のセッションには影響しません。

印刷設定の保存場所

Windowsの印刷環境では、印刷設定への変更はローカルコンピューターまたはドキュメントに保存できます。この環境では、ユーザーが印刷設定を変更すると、設定は次の場所に保存されます。

- **ユーザーデバイス自体** - Windowsユーザーは、コントロールパネルでプリンターを右クリックし、を選択することで、ユーザーデバイスのデバイス設定を変更できます。たとえば、ページ方向として「横」が選択されている場合、「横」はそのプリンターのデフォルトのページ方向設定として保存されます。
- **ドキュメント内** - ワープロプログラムやデスクトップパブリッシングプログラムでは、ページ方向などのドキュメント設定は、多くの場合ドキュメント内に保存されます。たとえば、ドキュメントを印刷キューに入れると、Microsoft Wordは通常、指定した印刷設定（ページ方向やプリンター名など）をドキュメント内に保存します。これらの設定は、次回そのドキュメントを印刷するときにデフォルトで表示されます。
- **ユーザーがセッション中に行った変更から** - システムは、自動作成されたプリンターの印刷設定への変更がセッション内のコントロールパネル（つまり、Multi-session OSマシン上）で行われた場合にのみ、その変更を保持します。
- **Multi-session OSマシン上** - これらは、マシン上の特定のプリンタードライバーに関連付けられたデフォルト設定です。

Windowsベースの環境で保持される設定は、ユーザーが変更を行った場所によって異なります。これは、スプレッドシートプログラムなどのある場所で表示される印刷設定が、ドキュメントなどの他の場所での設定と異なる場合があることも意味します。結果として、特定のプリンターに適用される印刷設定は、セッション中に変更される可能性があります。

ユーザーの印刷設定の階層

印刷設定は複数の場所に保存できるため、システムは特定の優先順位に従ってそれらを処理します。また、デバイス設定はドキュメント設定とは明確に区別され、通常はドキュメント設定よりも優先されることに注意することが重要です。

デフォルトでは、システムは他の設定を考慮する前に、ユーザーがセッション中に変更した印刷設定（つまり、保持された設定）を常に適用します。ユーザーが印刷すると、システムはMulti-session OSマシンに保存されているデフォルトのプリンター設定と、保持されているクライアントプリンター設定を結合して適用します。

ユーザーの印刷設定の保存

Citrixでは、プリンタープロパティの保存場所を変更しないことをお勧めします。プリンタープロパティをユーザーデバイスに保存するデフォルト設定は、一貫した印刷プロパティを確保するための最も簡単な方法です。システムがユーザーデバイスにプロパティを保存できない場合、Multi-session OSマシンのユーザープロファイルに自動的にフォールバックします。

次のシナリオに該当する場合は、プリンタープロパティ保持ポリシー設定を確認してください。

- ユーザーがユーザーデバイスにプリンタープロパティを保存できないレガシープラグインを使用している場合。
- Windowsネットワークで強制プロファイルを使用しており、ユーザーのプリンタープロパティを保持したい場合。

プリンターのプロビジョニング

Citrix Universal™ プリントサーバー

環境に最適な印刷ソリューションを決定する際には、次の点を考慮してください。

- Universal Print Serverは、Windows Print Providerでは利用できない機能（イメージとフォントのキャッシュ、高度な圧縮、最適化、QoSサポートなど）を提供します。
- ユニバーサル印刷ドライバーは、Microsoftによって定義された公開デバイス非依存設定をサポートします。ユーザーが印刷ドライバーメーカー固有のデバイス設定にアクセスする必要がある場合、Universal Print ServerとWindowsネイティブドライバーの組み合わせが最適なソリューションとなる可能性があります。この構成により、Universal Print Serverの利点を維持しつつ、ユーザーに特殊なプリンター機能へのアクセスを提供できます。考慮すべきトレードオフとして、Windowsネイティブドライバーにはメンテナンスが必要です。

- Citrix Universal Print Serverは、ネットワークプリンターのユニバーサル印刷をサポートします。Universal Print Serverは、マルチセッションOSマシン上の単一ドライバーであるユニバーサル印刷ドライバーを使用し、シンクライアントやタブレットを含むあらゆるデバイスからのローカルまたはネットワーク印刷を可能にします。

Universal Print ServerをWindowsネイティブドライバーとともに使用するには、Universal Print Serverを有効にします。デフォルトでは、Windowsネイティブドライバーが利用可能な場合はそれが使用されます。そうでない場合は、ユニバーサル印刷ドライバーが使用されます。Windowsネイティブドライバーのみを使用する、またはユニバーサル印刷ドライバーのみを使用するなど、この動作に変更を加えるには、ユニバーサル印刷ドライバーの使用ポリシー設定を更新します。

Universal Print Serverのインストール

Universal Print Serverを使用するには、インストールドキュメントに記載されているとおり、プリントサーバーにUpsServerコンポーネントをインストールして構成します。詳しくは、(/ja-jp/citrix-virtual-apps-desktops/2503/install-configure/install-core.html)および(/ja-jp/citrix-virtual-apps-desktops/2503/install-configure/install-command.html)を参照してください。

XenApp 6.5など、UPClientコンポーネントを個別に展開したい環境の場合：

1. WindowsシングルセッションOSまたはWindowsマルチセッションOS用のCitrix Virtual Apps and Desktops™ Virtual Delivery Agent (VDA) スタンドアロンパッケージをダウンロードします。
2. (/ja-jp/citrix-virtual-apps-desktops/2503/install-configure/install-command.html)に記載されているコマンドライン手順を使用してVDAを抽出します。
3. \\Image-Full\\Support\\VcRedist_2013_RTMから前提条件をインストールします。
    - Vcredist_x64 / vcredist_x86
        - 32ビット展開の場合はx86を、64ビット展開の場合は両方を実行します。
4. 「\\Image-Full\\x64\\Virtual Desktop Components」または「\\Image-Full\\x86\\Virtual Desktop Components」からcdfの前提条件をインストールします。
    - Cdf_x64 / Cdf_x86
        - x86は32ビット用、x64は64ビット用
5. 「\\Image-Full\\x64\\Virtual Desktop Components」または「\\Image-Full\\x86\\Virtual Desktop Components」でUPClientコンポーネントを見つけます。
6. UPClientコンポーネントを抽出し、そのMSIを起動してインストールします。

7. UPClientコンポーネントのインストール後、再起動が必要です。

Universal Print ServerのCEIPをオプトアウトする

Universal Print Serverをインストールすると、Citrix Customer Experience Improvement Program (CEIP) に自動的に登録されます。最初のデータアップロードは、インストール日時から7日後に実行されます。

CEIPをオプトアウトするには、レジストリキー `HKLM\Software\Citrix\Universal Print Server\CEIPEnabled` を編集し、**DWORD**値を**0**に設定します。

再度オプトインするには、DWORD値を1に設定します。

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

詳細については、Citrix Insight Servicesを参照してください。

ユニバーサルプリントサーバーの構成

Universal Print Serverを構成するには、以下のCitrixポリシー設定を使用します。詳細については、画面上のポリシー設定ヘルプを参照してください。

- **Universal Print Serverを有効にする**。Universal Print Serverはデフォルトで無効になっています。Universal Print Serverを有効にすると、Universal Print Serverが利用できない場合にWindows Print Providerを使用するかどうかを選択できます。Universal Print Serverを有効にすると、ユーザーはWindows Print ProviderおよびCitrix Providerインターフェイスを介してネットワークプリンターを追加および列挙できます。
- **Universal Print Server印刷データストリーム (CGP) ポート**。Universal Print Server印刷データストリームCGP (Common Gateway Protocol) リスナーが使用するTCPポート番号を指定します。デフォルトは**7229**です。
- **ユニバーサルプリントサーバー Webサービス (HTTP/SOAP) ポート**。ユニバーサルプリントサーバー リスナーが受信HTTP/SOAP要求に使用するTCPポート番号を指定します。デフォルトは**8080**です。

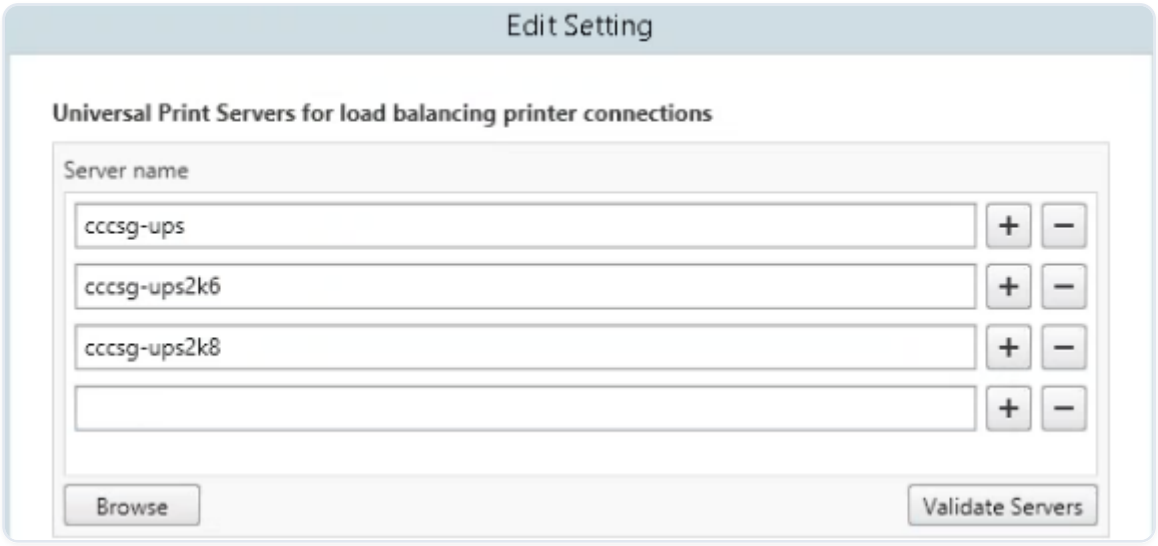
Citrix Virtual Apps and Desktops VDAへのUniversal Print Server通信のデフォルトポートであるHTTP 8080を変更するには、Universal Print Serverコンピューターで以下のレジストリを作成し、ポート番号の値を変更する必要があります。

`HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\PrintingPolicies`

"UpsHttpPort"=DWORD:\<portnumber\>

このポート番号は、StudioのHDXポリシー、Universal Print Server Webサービス (HTTP/SOAP) ポートと一致している必要があります。

- **Universal Print Server印刷ストリーム入力帯域幅制限 (kbps)**。CGPを使用して各印刷ジョブからUniversal Print Serverに配信される印刷データの転送速度の上限 (キロビット/秒) を指定します。デフォルトは0 (無制限) です。
- **負荷分散用のUniversal Print Server**。この設定では、他のCitrix印刷ポリシー設定を評価した後、セッション起動時に確立されたプリンター接続の負荷分散に使用するUniversal Print Serverを一覧表示します。プリンター作成時間を最適化するために、Citrixはすべての印刷サーバーが同じ共有プリンターのセットを持つことを推奨します。



- **Universal Print Serverサービス停止しきい値**。負荷分散装置が、利用できない印刷サーバーが回復するのを待つ時間を指定します。この時間を過ぎると、サーバーが永続的にオフラインであると判断され、その負荷が他の利用可能な印刷サーバーに再分散されます。デフォルトは180 (秒) です。

Delivery Controller™で印刷ポリシーが変更されると、ポリシー変更がVDAに適用されるまでに数分かかる場合があります。

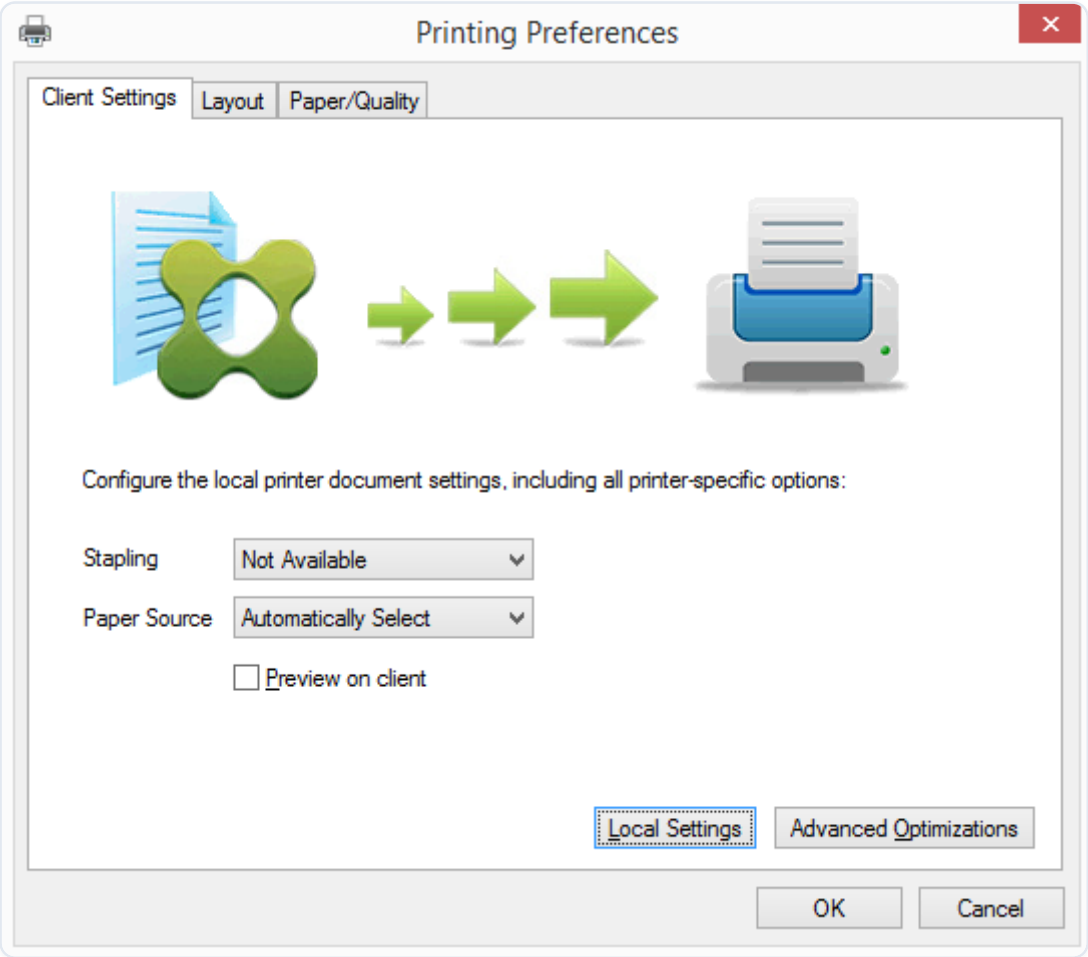
他のポリシー設定との相互作用 - Universal Print Serverは、他のCitrix印刷ポリシー設定を尊重し、以下の表に示すようにそれらと相互作用します。提供される情報は、Universal Print Serverポリシー設定が有効になっており、Universal Print Serverコンポーネントがインストールされ、ポリシー設定が適用されていることを前提としています。

ポリシー設定	**相互作用**
クライアントプリンターリダイレクト、クライアントプリンターの自動作成	Universal Print Serverが有効になると、クライアントネットワークプリンターは、ネイティブドライバーではなくUniversal Print Driverを使用して作成されます。ユーザーには以前と同じプリンター名が表示されます。
セッションプリンター	Citrix Universal Print Serverソリューションを使用する場合、ユニバーサルプリントドライバーのポリシー設定が適用されます。
プリントサーバーへの直接接続	Universal Print Serverが有効で、ユニバーサルプリントドライバーの使用ポリシー設定がユニバーサル印刷のみを使用するように構成されている場合、ユニバーサルプリントドライバーを使用して、プリントサーバーへの直接ネットワークプリンター接続を作成できます。
UPDの優先設定	EMFおよびXPSドライバーをサポートします。

ユーザーインターフェイスへの影響 - Universal Print Serverで使用されるCitrix Universal Print Driverは、以下のユーザーインターフェイスコントロールを無効にします。

- プリンターのプロパティダイアログボックスの「ローカルプリンター設定」ボタン
- ドキュメントのプロパティダイアログボックスの「ローカルプリンター設定」ボタンと「クライアントでプレビュー」ボタン

Citrix Universal Print Driver（EMFおよびXPSドライバー）は、ステープルや給紙元などの高度な印刷機能をサポートしています。セッション内のUPDにマップされているクライアントプリンターまたはネットワークプリンターがこれらの機能をサポートしている場合、ユーザーはカスタムUPD印刷ダイアログからステープルまたは給紙元のオプションを選択できます。



ステープルやセキュアPINなどの非標準のプリンター設定を行うには、Citrix UPD EMFまたはXPSドライバーを使用するクライアントマッププリンターのカスタムUPD印刷ダイアログで、**ローカル設定**を選択します。マップされたプリンターの**印刷設定**ダイアログがセッション外のクライアントに表示され、ユーザーは任意のプリンターオプションを変更できます。変更されたプリンター設定は、そのドキュメントを印刷する際にアクティブなセッションで使用されます。

これらの機能は、ネイティブドライバーがMicrosoft Print Capabilityテクノロジーを使用して利用可能にしている場合に利用できます。ネイティブドライバーは、Print Capabilities XMLで標準化されたPrint Schema Keywordsを使用する必要があります。非標準のキーワードが使用されている場合、Citrix Universal Print Driverを使用しても高度な印刷機能は利用できません。

Universal Print Serverを使用する場合、Citrix Print Providerのプリンターの追加ウィザードは、Windows Print Providerのプリンターの追加ウィザードと同じですが、以下の例外があります。

- 名前またはアドレスでプリンターを追加する場合、プリントサーバーのHTTP/SOAPポート番号を指定できます。そのポート番号はプリンター名の一部となり、表示されます。
- Citrix Universal Print Driverの使用ポリシー設定でユニバーサル印刷を使用する必要があると指定されている場合、プリンターを選択するとUniversal Print Driver名が表示されます。Windows Print ProviderはUniversal Print Driverを使用できません。

Citrix Print Providerは、クライアント側レンダリングをサポートしていません。

Universal Print Serverの詳細については、CTX200328を参照してください。

自動作成されたクライアントプリンター

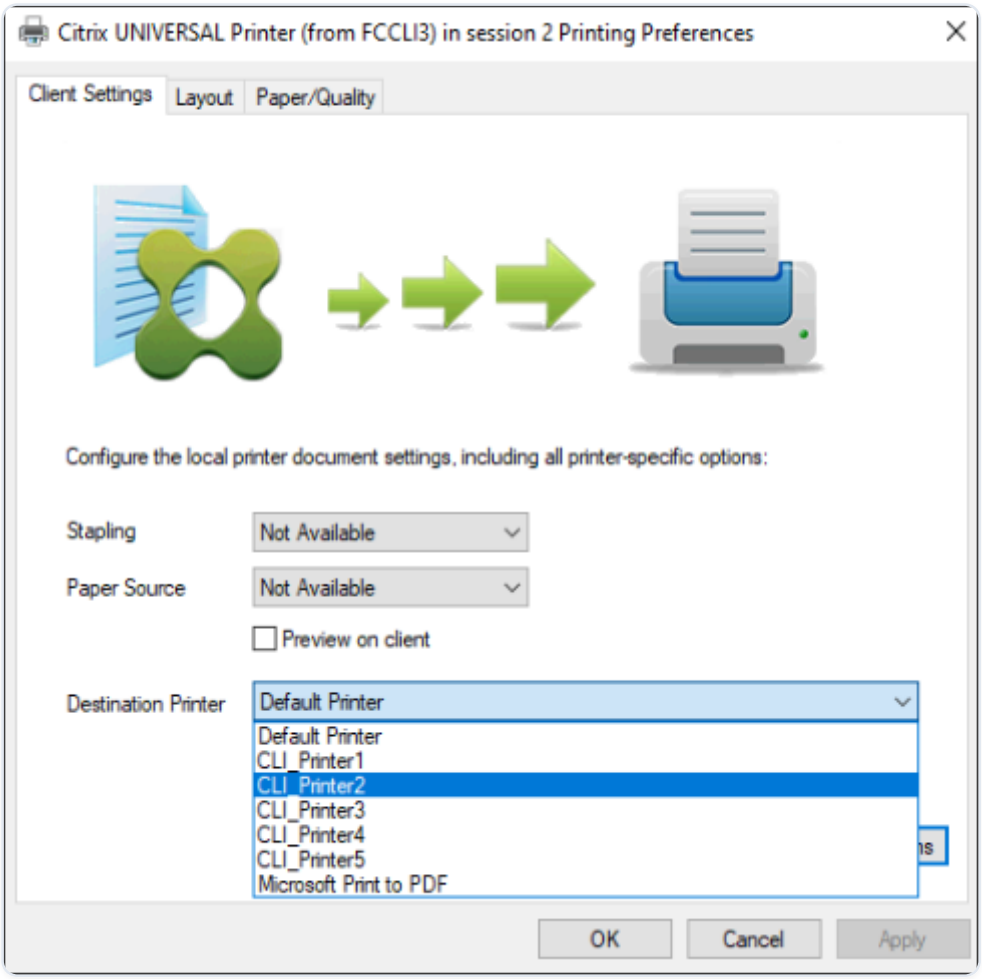
クライアントプリンター向けに、以下のユニバーサル印刷ソリューションが提供されています。

- **Citrix Universal Printer** - セッション開始時に作成される、印刷デバイスに紐付けられていない汎用プリンターです。Citrix Universal Printerのみを自動作成して使用すると、リソース使用量とユーザーサインイン時間の削減が期待できます。Universal Printerは、あらゆるクライアント側印刷デバイスに印刷できます。

  Citrix Universal Printerは、環境内のすべてのユーザーデバイスまたはCitrix Workspace™アプリで動作しない場合があります。Citrix Universal PrinterにはWindows環境が必要であり、Citrix Offline Plug-inやクライアントにストリーミングされるアプリケーションはサポートしていません。そのような環境では、自動作成されたクライアントプリンターとユニバーサルプリントドライバーの使用を検討してください。

  非Windows版Citrix Workspaceアプリでユニバーサル印刷ソリューションを使用するには、PostscriptまたはPCLベースの他のユニバーサルプリントドライバーのいずれかを使用してください。

  Citrix Universal Printerを使用すると、クライアントのデフォルトプリンターまたは特定のクライアントプリンターを印刷先として選択できます。印刷ジョブに特定のプリンターを選択するには、**印刷設定**ダイアログボックスを開きます。**宛先プリンター**ドロップダウンを選択します。**デフォルトプリンター**オプションは、印刷ジョブをクライアントのデフォルトプリンターに送信します。セッションを実行しているエンドポイントに接続されているクライアントリダイレクトプリンターも一覧表示されます。選択したプリンターは、今後の印刷ジョブの宛先プリンターとして保存されます。



- **Citrix Universal Print Driver** - デバイスに依存しないプリンタードライバーです。Citrix Universal Print Driverを構成すると、システムはデフォルトでEMFベースのUniversal Print Driverを使用します。

  Citrix Universal Print Driverは、古いまたは高度でないプリンタードライバーよりも小さい印刷ジョブを作成する可能性があります。ただし、特殊なプリンターの印刷ジョブを最適化するには、デバイス固有のドライバーが必要になる場合があります。

ユニバーサル印刷の構成 - ユニバーサル印刷を構成するには、以下のCitrixポリシー設定を使用します。詳細については、画面上のポリシー設定ヘルプを参照してください。

- ユニバーサルプリントドライバーの使用。ユニバーサル印刷を使用するタイミングを指定します。
- 汎用ユニバーサルプリンターの自動作成。ユニバーサル印刷に対応したユーザーデバイスが使用されている場合に、セッション用の汎用Citrix Universal Printerオブジェクトの自動作成を有効または無効にします。デフォルトでは、汎用Universal Printerオブジェクトは自動作成されません。

- ユニバーサルドライバーの優先順位。システムがユニバーサルプリントドライバーを使用しようとする順序を、リストの最初のエントリから指定します。ドライバーの追加、編集、削除、およびリスト内のドライバーの順序変更が可能です。
- ユニバーサル印刷プレビューの優先順位。自動作成されたプリンターまたは汎用ユニバーサルプリンターに対して、印刷プレビュー機能を使用するかどうかを指定します。
- ユニバーサル印刷EMF処理モード。Windowsユーザーデバイス上のEMFスプールファイルの処理方法を制御します。デフォルトでは、EMFレコードはプリンターに直接スプールされます。プリンターに直接スプールすることで、スプーラーはレコードをより速く処理し、CPUリソースの使用量を削減できます。

その他のポリシーについては、印刷パフォーマンスの最適化を参照してください。用紙サイズ、印刷品質、色、両面印刷、部数などの設定のデフォルトを変更するには、CTX113148を参照してください。

ユーザーデバイスからプリンターを自動作成 - セッションの開始時に、システムはデフォルトでユーザーデバイス上のすべてのプリンターを自動作成します。ユーザーにプロビジョニングされるプリンターの種類を制御したり、自動作成を防止したりできます。

Citrixポリシー設定 「クライアントプリンターの自動作成」を使用して、自動作成を制御します。以下を指定できます。

- ネットワークプリンターおよびローカルに接続されたプリンターを含む、ユーザーデバイスに表示されるすべてのプリンターが、各セッションの開始時に自動的に作成される（デフォルト）
- ユーザーデバイスに物理的に接続されているすべてのローカルプリンターが自動的に作成される
- ユーザーデバイスのデフォルトプリンターのみが自動的に作成される
- すべてのクライアントプリンターで自動作成が無効になる

「クライアントプリンターの自動作成」設定を使用するには、「クライアントプリンターのリダイレクト」設定が「許可」（デフォルト）になっている必要があります。

ユーザーにネットワークプリンターを割り当てる

デフォルトでは、ユーザーデバイス上のネットワークプリンターはセッションの開始時に自動的に作成されます。システムでは、各セッション内で作成するネットワークプリンターを指定することで、列挙およびマップされるネットワークプリンターの数を減らすことができます。このようなプリンターはセッションプリンターと呼ばれます。

IPアドレスでセッションプリンターポリシーをフィルタリングして、近接印刷を提供できます。近接印刷により、指定されたIPアドレス範囲内のユーザーは、同じ範囲内に存在するネットワーク印刷デバイスに自動的にアクセスできます。近接印刷はCitrix Universal Print Serverによって提供され、このセクションで説明されている構成は必要ありません。

近接印刷には、次のシナリオが含まれる場合があります。

- 社内ネットワークは、ユーザーにIPアドレスを自動的に割り当てるDHCPサーバーで運用されています。
- 社内のすべての部門には、一意に指定されたIPアドレス範囲があります。
- ネットワークプリンターは、各部署のIPアドレス範囲内に存在します。

近接印刷が構成されており、従業員がある部署から別の部署に移動した場合でも、追加の印刷デバイス構成は必要ありません。ユーザーデバイスが新しい部署のIPアドレス範囲内で認識されると、その範囲内のすべてのネットワークプリンターにアクセスできるようになります。

セッションでリダイレクトする特定のプリンターを構成する - 管理者によって割り当てられたプリンターを作成するには、Citrixポリシー設定の「セッションプリンター」を構成します。次のいずれかの方法を使用して、そのポリシーにネットワークプリンターを追加します。

- `\\servername\printername`の形式を使用して、プリンターのUNCパスを入力します。
- ネットワーク上のプリンターの場所を参照します。
- 特定のサーバー上のプリンターを参照します。`\\servername`の形式を使用してサーバー名を入力し、「参照」をクリックします。

重要: サーバーは、適用されているすべてのポリシーの有効なセッションプリンター設定を、最も高い優先度から最も低い優先度までマージします。プリンターが複数のポリシーオブジェクトで構成されている場合、カスタムのデフォルト設定は、そのプリンターが構成されている最も優先度の高いポリシーオブジェクトからのみ取得されます。

セッションプリンター設定で作成されたネットワークプリンターは、サブネットなどのオブジェクトでフィルタリングすることにより、セッションが開始された場所に応じて異なる場合があります。

セッションのデフォルトネットワークプリンターを指定する - デフォルトでは、ユーザーのメインプリンターがセッションのデフォルトプリンターとして使用されます。Citrixポリシー設定の「デフォルトプリンター」を使用して、セッションでユーザーデバイスのデフォルトプリンターがどのように確立されるかを変更します。

1. 「デフォルトプリンター設定」ページで、「クライアントのデフォルトプリンターを選択」の設定を選択します。

    - ネットワークプリンター名。「セッションプリンター」ポリシー設定で追加されたプリンターがこのメニューに表示されます。このポリシーのデフォルトとして使用するネットワークプリンターを選択します。
    - ユーザーのデフォルトプリンターを調整しない。デフォルトプリンターには、現在のターミナルサービスまたはWindowsユーザープロファイル設定を使用します。詳細については、画面上のポリシー設定ヘルプを参照してください。

2. 影響を与えたいユーザーグループ（またはその他のフィルターされたオブジェクト）にポリシーを適用します。

近接印刷を構成する - 近接印刷はCitrix Universal Print Serverによっても提供されており、ここに記載されている構成は必要ありません。

1. 各サブネットに対して個別のポリシーを作成します（またはプリンターの場所に合わせます）。
2. 各ポリシーで、そのサブネットの地理的な場所にあるプリンターをセッションプリンター設定に追加します。
3. デフォルトプリンター設定を「ユーザーのデフォルトプリンターを調整しない」に設定します。
4. クライアントIPアドレスでポリシーをフィルターします。DHCP IPアドレス範囲の変更を反映するように、これらのポリシーを必ず更新してください。

印刷環境の維持

印刷環境の維持には、次のものが含まれます。

- プリンタードライバーの管理
- 印刷パフォーマンスの最適化
- プリンターの表示と印刷キューの管理

プリンタードライバーの管理

管理オーバーヘッドとプリンタードライバーの問題の可能性を最小限に抑えるため、Citrix Universal™プリンタードライバーの使用をお勧めします。

自動作成が失敗した場合、デフォルトでは、Windowsに付属のWindowsネイティブプリンタードライバーがシステムにインストールされます。ドライバーが利用できない場合、システムはUniversal Print Driverにフォールバックします。プリンタードライバーのデフォルトについて詳しくは、「ベストプラクティス、セキュリティに関する考慮事項、およびデフォルトの操作」を参照してください。

Citrix Universal Print Driverがすべてのシナリオでオプションではない場合、Multi-session OSマシンにインストールされるドライバーの数を最小限に抑えるためにプリンタードライバーをマップします。さらに、プリンタードライバーをマップすると、次のことが可能になります。

- 指定されたプリンターがCitrix Universal Print Driverのみを使用できるようにする
- 指定されたドライバーでプリンターを作成することを許可または禁止する
- 古いドライバーまたは破損したドライバーを適切なプリンタードライバーに置き換える
- クライアントドライバー名に対して、Windowsサーバーで利用可能なドライバーを置き換える

プリンタードライバーの自動インストールを防止する - Multi-session OSマシン全体で一貫性を確保するために、プリンタードライバーの自動インストールを無効にする必要があります。これは、Citrix®ポリシー、Microsoftポリシー、またはその両方を通じて実現できます。Windowsネイティブプリンタードライバーの自動インストールを防止するには、Citrixポリシー設定の「インボックスプリンタードライバーの自動インストール」を無効にします。

クライアントプリンタードライバーをマッピングする - 各クライアントは、ログオン時にクライアント側のプリンターに関する情報（プリンタードライバー名を含む）を提供します。クライアントプリンターの自動作成中に、クライアントから提供されたプリンターモデル名に対応するWindowsサーバープリンタードライバー名が選択されます。その後、自動作成プロセスは、識別された利用可能なプリンタードライバーを使用して、リダイレクトされたクライアント印刷キューを構築します。

ドライバー置換ルールを定義し、マップされたクライアントプリンタードライバーの印刷設定を編集する一般的なプロセスは次のとおりです。

1. 自動作成されたクライアントプリンターのドライバー置換ルールを指定するには、Citrixポリシー設定の「Printer driver mapping and compatibility」を構成します。これには、クライアントプリンタードライバー名を追加し、「Find printer driver」メニューからクライアントプリンタードライバーの代わりに置換するサーバードライバーを選択します。この設定ではワイルドカードを使用できます。たとえば、すべてのHPプリンターに特定のドライバーを使用させるには、ポリシー設定で「HP*」と指定します。
2. プリンタードライバーを禁止するには、ドライバー名を選択し、「Do not create」設定を選択します。

3. 必要に応じて、既存のマッピングを編集したり、マッピングを削除したり、リスト内のドライバーエントリの順序を変更したりします。
4. マップされたクライアントプリンタードライバーの印刷設定を編集するには、プリンタードライバーを選択し、「Settings」をクリックして、印刷品質、向き、色などの設定を指定します。プリンタードライバーがサポートしない印刷オプションを指定した場合、そのオプションは無効になります。この設定は、ユーザーが以前のセッションで設定した保持されているプリンター設定を上書きします。
5. 特定のドライバーでのみ利用可能なプリンター機能もあるため、ドライバーをマッピングした後は、プリンターの動作を詳細にテストすることをCitrixは推奨します。

ユーザーがログオンすると、システムはクライアントプリンターを設定する前に、クライアントプリンタードライバーの互換性リストをチェックします。

印刷パフォーマンスの最適化

印刷パフォーマンスを最適化するには、Universal Print ServerとUniversal Print Driverを使用します。以下のポリシーは、印刷の最適化と圧縮を制御します。

- ユニバーサル印刷の最適化のデフォルト。セッション用にユニバーサルプリンターが作成される際のデフォルト設定を指定します。
    - 希望する画質は、ユニバーサル印刷に適用されるデフォルトの画像圧縮制限を指定します。デフォルトでは、「Standard Quality」が有効になっており、ユーザーは標準または低品質の圧縮を使用してのみ画像を印刷できることを意味します。
    - ヘビーウェイト圧縮を有効にするは、画質を損なうことなく、「希望する画質」で設定された圧縮レベルを超えて帯域幅を削減することを有効または無効にします。デフォルトでは、ヘビーウェイト圧縮は無効になっています。
    - 画像とフォントのキャッシュ設定は、印刷ストリームに複数回出現する画像とフォントをキャッシュするかどうかを指定し、各固有の画像またはフォントがプリンターに一度だけ送信されるようにします。デフォルトでは、埋め込み画像とフォントはキャッシュされます。
    - 非管理者によるこれらの設定の変更を許可するは、ユーザーがセッション内でデフォルトの印刷最適化設定を変更できるかどうかを指定します。デフォルトでは、ユーザーはデフォルトの印刷最適化設定を変更できません。
- ユニバーサル印刷の画像圧縮制限。Universal Print Driverで印刷される画像の最大品質と最小圧縮レベルを定義します。デフォルトでは、画像圧縮制限は「Best Quality (lossless compression)」に設定されています。

- ユニバーサル印刷の印刷品質制限。セッションで印刷出力を生成するために利用できる最大ドット/インチ (dpi) を指定します。デフォルトでは、制限は指定されていません。

デフォルトでは、ネットワークプリンター宛てのすべての印刷ジョブは、マルチセッションOSマシンからネットワーク経由で直接プリントサーバーにルーティングされます。ネットワークにかなりの遅延や帯域幅の制限がある場合は、ICA®接続経由で印刷ジョブをルーティングすることを検討してください。そのためには、Citrixポリシー設定の「プリントサーバーへの直接接続」を無効にします。ICA接続経由で送信されるデータは圧縮されるため、WANを介してデータが転送される際の帯域幅の消費が少なくなります。

印刷帯域幅を制限してセッションパフォーマンスを向上させる - マルチセッションOSマシンからユーザープリンターにファイルを印刷している間、特にユーザーが低速ネットワーク経由でサーバーにアクセスしている場合、帯域幅の競合により、他の仮想チャネル（ビデオなど）のパフォーマンスが低下する可能性があります。このような劣化を防ぐために、ユーザー印刷で使用される帯域幅を制限できます。印刷のデータ転送速度を制限することで、ビデオ、キーストローク、マウスデータの転送のためにHDX™データストリームでより多くの帯域幅を利用できるようになります。

> **重要:**
>
> プリンターの帯域幅制限は、他のチャネルが使用されていない場合でも常に適用されます。
>
> 以下のCitrixポリシーの帯域幅プリンター設定を使用して、印刷帯域幅のセッション制限を構成します。サイトの制限を設定するには、Studioを使用してこのタスクを実行します。個々のサーバーの制限を設定するには、各マルチセッションOSマシンでローカルにWindowsのグループポリシー管理コンソールを使用してこのタスクを実行します。

- プリンターリダイレクト帯域幅制限設定は、印刷に利用できる帯域幅をキロビット/秒 (kbps) で指定します。
- 「Printer redirection bandwidth limit percent」設定は、印刷に利用できる帯域幅を、利用可能な全体の帯域幅の割合に制限します。

  注：プリンターリダイレクト帯域幅制限パーセント設定を使用して帯域幅をパーセンテージで指定するには、全体セッション帯域幅制限も有効にする必要があります。

  両方の設定に値を入力した場合、最も制限の厳しい設定（低い方の値）が適用されます。

印刷帯域幅に関するリアルタイム情報を取得するには、Citrix Directorを使用します。

ユニバーサルプリントサーバーの負荷分散

ユニバーサルプリントサーバーソリューションは、負荷分散ソリューションにさらにプリントサーバーを追加することで拡張できます。各VDAには、印刷負荷をすべてのプリントサーバーに分散するための独自のロードバランサーがあるため、単一障害点はありません。

ポリシー設定のUniversal Print Servers for load balancingとUniversal Print Servers out-of-service thresholdを使用して、負荷分散ソリューション内のすべてのプリントサーバーに印刷負荷を分散します。

プリントサーバーで予期せぬ障害が発生した場合、各VDAのロードバランサーのフェイルオーバーメカニズムは、障害が発生したプリントサーバーに割り当てられていたプリンター接続を他の利用可能なプリントサーバーに自動的に再分散します。これにより、既存および新規のすべてのセッションは、ユーザーエクスペリエンスに影響を与えることなく、また管理者の即時介入を必要とせずに正常に機能します。

管理者は、一連のパフォーマンスカウンターを使用して、VDA上でロードバランスされたプリントサーバーのアクティビティを監視し、以下を追跡できます。

- VDA上のロードバランスされたプリントサーバーのリストとその状態（利用可能、利用不可）
- 各プリントサーバーによって受け入れられたプリンター接続数
- 各プリントサーバーで失敗したプリンター接続数
- 各プリントサーバー上のアクティブなプリンター接続数
- 各プリントサーバー上の保留中のプリンター接続数

印刷キューの表示と管理

次の表は、環境内でプリンターを表示し、印刷キューを管理できる場所をまとめたものです。

	印刷経路	場所
クライアントプリンター（ユーザーデバイスに接続されたプリンター）	クライアント印刷経路	UACが有効な場合：Microsoft管理コンソールにある印刷の管理スナップイン。UACが無効な場合：Windows 8より前：コントロールパネル、Windows 8：印刷の管理スナップイン

	印刷経路	場所
ネットワークプリンター（ネットワークプリントサーバー上のプリンター）	ネットワーク印刷経路	UAC有効時: 印刷サーバー \> Microsoft Management Consoleにある印刷の管理スナップイン; UAC無効時: 印刷サーバー \> コントロールパネル
ネットワークプリンター (ネットワーク印刷サーバー上のプリンター)	クライアント印刷経路	UAC有効時: 印刷サーバー \> Microsoft Management Consoleにある印刷の管理スナップイン; UAC無効時: Windows 8より前: コントロールパネル、Windows 8: 印刷の管理スナップイン
ローカルネットワークサーバープリンター (マルチセッションOSマシンに追加されたネットワーク印刷サーバーからのプリンター)	ネットワーク印刷経路	UAC有効時: 印刷サーバー \> コントロールパネル; UAC無効時: 印刷サーバー \> コントロールパネル

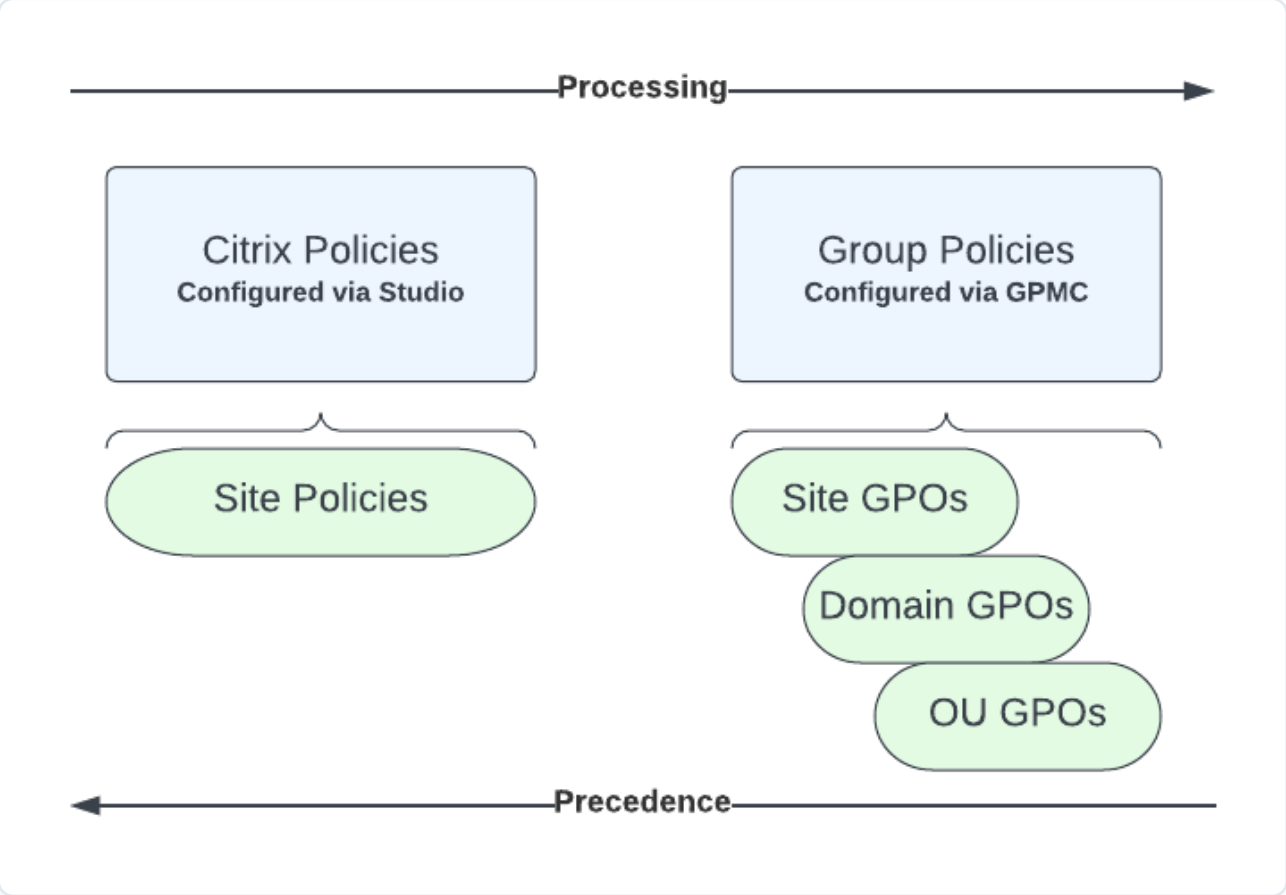
注:

ネットワーク印刷パスを使用するネットワークプリンターの印刷キューはプライベートであり、システムを通じて管理できません。

ポリシー

ポリシーとは、ユーザー、デバイス、または接続タイプのグループに対して、セッション、帯域幅、およびセキュリティがどのように管理されるかを定義する設定の集合です。

ポリシー設定は、物理マシンおよび仮想マシン、またはユーザーに適用できます。設定は、ローカルレベルの個々のユーザー、またはActive Directoryのセキュリティグループに適用できます。構成は特定の基準とルールを定義します。ポリシーを明示的に割り当てない場合、設定はすべての接続に適用されます。



ポリシーはネットワークのさまざまなレベルに適用できます。組織単位GPOレベルに配置されたポリシー設定は、ネットワーク上で最も高い優先順位を持ちます。ドメインGPOレベルのポリシーは、サイトグループポリシーオブジェクトレベルのポリシーを上書きします。サイトグループポリシーオブジェクトレベルは、MicrosoftおよびCitrixローカルポリシーレベルの両方における競合するポリシーを上書きします。

すべてのCitrixローカルポリシーは、Web Studioコンソールで作成および管理され、サイトデータベースに保存されます。グループポリシーは、Microsoftグループポリシー管理コンソール（GPMC）を使用して作成および管理され、Active Directoryに保存されます。Microsoftローカルポリシーは、Windowsオペレーティングシステムで作成され、レジストリに保存されます。

Studioはモデリングウィザードを使用して、管理者がテンプレートとポリシー内の構成設定を比較し、競合する設定や冗長な設定を排除するのに役立ちます。管理者はGPMCを使用してGPOを設定し、設定を構成できます。また、それらをネットワークのさまざまなレベルのターゲットユーザーセットに適用することもできます。

これらのGPOはActive Directoryに保存されます。これらの設定の管理へのアクセスは、セキュリティ上の理由からほとんどのIT担当者に対して制限されています。

設定は優先順位とその条件に従ってマージされます。無効な設定は、下位の有効な設定を上書きします。未構成のポリシー設定は無視され、下位の設定を上書きしません。

ローカルポリシーは、Active Directoryのグループポリシーと競合することもあり、状況によっては互いに上書きし合う可能性があります。

すべてのポリシーは次の順序で処理されます。

1. エンドユーザーはドメイン資格情報を使用してマシンにログオンします。
2. 資格情報はドメインコントローラーに送信されます。
3. Active Directoryはすべてのポリシー（エンドユーザー、エンドポイント、組織単位、ドメイン）を適用します。
4. エンドユーザーはCitrix Workspace™アプリにログオンし、アプリケーションまたはデスクトップにアクセスします。
5. CitrixおよびMicrosoftのポリシーは、エンドユーザーおよびリソースをホストするマシンに対して処理されます。
6. Active Directoryは、ポリシー設定の優先順位を決定します。その後、それらをエンドポイントデバイスのレジストリと、リソースをホストするマシンに適用します。
7. エンドユーザーがリソースからログオフします。エンドユーザーおよびエンドポイントデバイスに対するCitrixポリシーは、アクティブではなくなります。
8. エンドユーザーがユーザーデバイスからログオフすると、GPOユーザーポリシーが解放されます。
9. エンドユーザーがデバイスの電源を切ると、GPOマシンポリシーが解放されます。

ユーザー、デバイス、およびマシンのグループに対してポリシーを作成する場合、一部のメンバーは異なる要件を持つ可能性があり、一部のポリシー設定に例外が必要になる場合があります。例外は、ポリシーが誰または何に影響するかを決定するStudioおよびGPMCのフィルターによって作成されます。

> **注:**
>
> 同じGPO内でWindowsポリシーとCitrixポリシーを混在させることはサポートしていません。

ポリシーの操作

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

ユーザーアクセスとセッション環境を制御するためにCitrixポリシーを構成します。Citrixポリシーは、接続、セキュリティ、帯域幅の設定を制御する最も効率的な方法です。特定のユーザーグループ、デバイス、または接続タイプに対してポリシーを作成できます。各ポリシーには複数の設定を含めることができます。

Citrixポリシーを操作するためのツール

Citrixポリシーでは、以下のツールを使用できます。

- **Web Studio。** グループポリシーを管理する権限がないCitrix管理者の場合は、Web Studioを使用してサイトのポリシーを作成します。Web Studioを使用して作成されたポリシーはサイトデータベースに保存され、VDAがブローカーに登録されたとき、またはユーザーがそのVDAに接続したときに、更新がVDAにプッシュされます。
- **ローカルグループポリシーエディター**（Microsoft管理コンソールスナップイン）。ネットワーク環境でActive Directoryを使用しており、グループポリシーを管理する権限がある場合は、ローカルグループポリシーエディターを使用してサイトのポリシーを作成できます。構成した

設定は、グループポリシー管理コンソールで指定したグループポリシーオブジェクト（GPO）に影響します。

重要:

一部のポリシー設定を構成するには、ローカルグループポリシーエディターを使用することをお勧めします。例としては、VDAをコントローラーに登録するための設定や、Microsoft App-Vサーバーに関連する設定などがあります。 追加のポリシー検証が追加されます。その結果、無効なポリシー設定が存在する場合、インプレースアップグレードを行うとポリシーデータが失われる可能性があります。Web Studio以外の方法でポリシーを作成または編集する場合は、最新バージョンのSDKとスナップインを使用することをCitrixは推奨します。

ポリシーの処理順序と優先順位

グループポリシー設定は、次の順序で処理されます。

1. ローカルGPO
2. Virtual Apps and DesktopsサイトGPO（サイトデータベースに保存）
3. サイトレベルGPO
4. ドメインレベルのGPO
5. 組織単位

ただし、競合が発生した場合、最後に処理されたポリシー設定が以前に処理された設定を上書きします。ポリシー設定の優先順位は次のとおりです。

1. 組織単位
2. ドメインレベルのGPO
3. サイトレベルのGPO
4. Virtual Apps and DesktopsサイトGPO（サイトデータベースに保存）
5. ローカルGPO

例えば、Citrix管理者がWeb Studioを使用して、会社の営業担当者向けにクライアントファイルリダイレクトを有効にするポリシー（ポリシーA）を作成します。一方、別の管理者がグループポリシーエディターを使用して、営業担当者向けにクライアントファイルリダイレクトを無効にするポリシー（ポリシーB）を作成します。営業担当者が仮想デスクトップにログオンすると、ポリシー

Bが適用され、ポリシーAは無視されます。その理由は、ポリシーBがドメインレベルで処理され、ポリシーAがVirtual Apps and DesktopsサイトGPOレベルで処理されたためです。

ただし、ユーザーがICA®またはリモートデスクトッププロトコル（RDP）セッションを起動すると、Citrixセッション設定は、Active Directoryポリシーで構成された設定、またはリモートデスクトップセッションホスト構成を使用して構成された設定を上書きします。この設定には、一般的なRDPクライアント接続設定に関連する設定が含まれます。RDPクライアント接続設定の例としては、デスクトップの壁紙、メニューアニメーション、ドラッグ中のウィンドウコンテンツの表示などがあります。

複数のポリシーを使用する場合、競合する設定を含むポリシーに優先順位を付けることができます。詳細については、「ポリシーの比較、優先順位付け、モデル化、トラブルシューティング」を参照してください。

Citrixポリシーのワークフロー

ポリシーを構成するプロセスは次のとおりです。

1. ポリシーを作成します。
2. ポリシー設定を構成します。
3. ポリシーをマシンオブジェクトとユーザーオブジェクトに割り当てます。
4. ポリシーの優先順位を設定します。
5. Citrix Group Policy Modelingウィザードを実行して、有効なポリシーを確認します。

> **注:**
>
> Citrix Group Policy Modelingウィザードを開くには、**［ポリシー］>［モデリング］タブに移動し、アクションバーで［モデリングウィザードの起動］をクリックします。**［モデリング］**タブは、お客様のご要望に応じてWeb Studioで利用できます。

Citrixポリシーと設定をナビゲートする

ローカルグループポリシーエディターでは、ポリシーと設定は「コンピューターの構成」と「ユーザーの構成」の2つのカテゴリに表示されます。各カテゴリにはCitrixポリシーノードがあります。このスナップインのナビゲートと使用の詳細については、Microsoftのドキュメントを参照してください。

Web Studioでは、ポリシー設定は、影響を与える機能または特徴に基づいてカテゴリに分類されます。たとえば、 セクションには、プロファイル管理のポリシー設定が含まれています。

- コンピューター設定（マシンに適用されるポリシー設定）は、仮想デスクトップの動作を定義し、仮想デスクトップの起動時に適用されます。これらの設定は、仮想デスクトップでアクティブなユーザーセッションがない場合でも適用されます。
- ユーザー設定は、ICAを使用して接続する際のユーザーエクスペリエンスを定義します。ユーザーポリシーは、ユーザーがICAを使用して接続または再接続するときに適用されます。ユーザーがRDPを使用して接続したり、コンソールに直接ログオンしたりした場合は、ユーザーポリシーは適用されません。

  ポリシー、設定、またはテンプレートにアクセスするには、Web Studioの左ペインで**ポリシー**を選択します。

  - **［ポリシー］**タブにはすべてのポリシーが一覧表示されます。ポリシーを選択すると、下部に次のタブが表示されます。
    - 概要 - 名前、優先度、有効/無効の状態、および説明を一覧表示
    - 設定 - 構成されているすべての設定を一覧表示
    - 割り当て先 - ポリシーが割り当てられているユーザーオブジェクトとマシンオブジェクトを一覧表示します。 詳しくは、「ポリシーの作成」を参照してください。
  - 「**テンプレート**」タブには、Citrix が提供するテンプレートと、作成したカスタムテンプレートが一覧表示されます。テンプレートを選択すると、下部に次のタブが表示されます。
    - 説明（テンプレートを使用する理由）
    - 設定（構成済みの設定のリスト）。詳細については、「ポリシーテンプレート」を参照してください。
  - 「**比較**」タブでは、ポリシーまたはテンプレートの設定を、他のポリシーまたはテンプレートの設定と比較できます。たとえば、ベストプラクティスへの準拠を確実にするために、設定値を検証したい場合があります。詳細については、「ポリシーの比較、優先順位付け、モデル化、トラブルシューティング」を参照してください。

  ポリシーまたはテンプレートで設定を検索するには：

  a. ポリシーまたはテンプレートを選択します。
  b. アクションバーで**ポリシーの編集**または**テンプレートの編集**を選択します。
  c. **設定**ページで、**検索**フィールドに設定の名前を入力します。

検索を絞り込むには、以下を選択します。

- 特定の製品バージョン
- カテゴリ（例：帯域幅）
- 設定名に含まれるキーワード
- **View selected only** チェックボックス
- 選択したポリシーに追加された設定のみを検索する場合。

フィルタリングされていない検索の場合は、**All Settings** を選択します。

- ポリシー内で設定を検索するには：

a. ポリシーを選択します。

b. **Settings** タブを選択し、設定の名前を入力します。

特定の製品バージョンを選択するか、カテゴリを選択することで、検索を絞り込むことができます。フィルタリングされていない検索の場合は、**All Settings** を選択します。

ポリシーは、一度作成されると、使用されたテンプレートとは独立します。新しいポリシーの**Description**フィールドを使用して、使用されたソーステンプレートを追跡できます。

グループポリシーエディターでは、コンピューター設定とユーザー設定は、両方の種類の設定を含むテンプレートから作成された場合でも、個別に適用する必要があります。この例では、コンピューターの構成で「非常に高精細なユーザーエクスペリエンス」を使用することを選択しています。

- レガシーグラフィックモードは、このテンプレートから作成されたポリシーで使用されるコンピューター設定です。
- グレー表示されているユーザー設定は、このテンプレートから作成されたポリシーでは使用されません。

ローカルグループポリシーエディターの図](/en-us/citrix-virtual-apps-desktops/2503/media/group-policy-editor-template-example.png)

ポリシーテンプレート

> **注:**

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

> テンプレートは、特定の成果を達成するためのポリシー作成に使用することが推奨される設定の集合です。たとえば、エンドユーザーに高精細なユーザーエクスペリエンスを提供するためのポリシーを作成する場合、「非常に高精細なユーザーエクスペリエンス」テンプレートで定義されている設定を、そのようなポリシーを作成するための参照および開始点として使用できます。

テンプレートはポリシーではありません。テンプレートはCitrixポリシー設定の補足ドキュメントです。これらは、特定のユーザー関連設定の集合的な機能を示します。

テンプレートの使用は任意です。管理者はテンプレートを使用せずにポリシーを作成できます。テンプレートは、サイトをどのように構成すべきかについて大まかなアイデアを持っているものの、目的の構成を実現するためにどの設定を使用すべきか確信が持てない管理者にとって役立ちます。

管理者は、既存のテンプレートまたは既存のポリシーを使用して、あるいはゼロからテンプレートを作成できます。

ADMX/ADML

ここで説明するCitrixグループポリシーテンプレートは、Windowsポリシーテンプレートとは関係ありません。ここで説明するテンプレートとWindowsポリシーテンプレートは、2つの異なる概念です。CitrixグループポリシーテンプレートはADMXファイルではありません。

組み込みのCitrixテンプレート

次のポリシーテンプレートが利用可能です。

- **非常に高精細なユーザーエクスペリエンス**。このテンプレートは、ユーザーエクスペリエンスを最大化するデフォルト設定を適用します。複数のポリシーが優先順位に従って処理されるシナリオで、このテンプレートを使用します。
- **高サーバー拡張性**。サーバーリソースを節約するために、このテンプレートを適用します。このテンプレートは、ユーザーエクスペリエンスとサーバーの拡張性のバランスを取ります。単一サーバーでホストできるユーザー数を増やしながら、良好なユーザーエクスペリエンスを提供します。このテンプレートは、グラフィックの圧縮にビデオコーデックを使用せず、サーバー側のマルチメディアレンダリングを防止します。

- **高サーバー拡張性 - レガシーOS**。この高サーバー拡張性テンプレートは、Windows Server 2008 R2またはWindows 7以前を実行しているVDAにのみ適用されます。このテンプレートは、これらのオペレーティングシステムにより効率的なレガシーグラフィックモードに依存しています。
- **NetScaler SD-WAN向けに最適化**。Citrix Virtual Desktopsの配信を最適化するために、NetScaler SD-WANを使用している支社から作業するユーザーにこのテンプレートを適用します。(NetScaler SD-WANはCloudBridgeの新しい名称です)。
- **WAN向けに最適化**。このテンプレートは、共有WAN接続を使用する支社のタスクワーカーや、グラフィックがシンプルなユーザーインターフェイスとマルチメディアコンテンツが少ないアプリケーションにアクセスする低帯域幅接続のリモート拠点向けです。このテンプレートは、ビデオ再生エクスペリエンスと一部のサーバー拡張性を犠牲にして、帯域幅効率を最適化します。
- **WAN向けに最適化 - レガシーOS**。この*WAN向けに最適化*テンプレートは、Windows Server 2008 R2またはWindows 7以前を実行しているVDAにのみ適用されます。このテンプレートは、これらのオペレーティングシステムにとってより効率的なレガシーグラフィックモードに依存しています。
- **セキュリティと制御**。このテンプレートは、リスク許容度が低い環境で使用し、Citrix Virtual Apps and Desktopsでデフォルトで有効になっている機能を最小限に抑えます。このテンプレートには、ユーザーデバイスでの印刷、クリップボード、周辺機器、ドライブマッピング、ポートリダイレクト、およびFlashアクセラレーションへのアクセスを無効にする設定が含まれています。このテンプレートを適用すると、より多くの帯域幅を使用し、サーバーあたりのユーザー密度を低下させる可能性があります。

組み込みのCitrixテンプレートをデフォルト設定で使用することをお勧めしますが、特定の推奨値がない設定もあります。たとえば、WAN向けに最適化されたテンプレートに含まれる**セッション全体の帯域幅制限**などです。この場合、テンプレートはその設定を公開し、管理者がこの設定がシナリオに適用される可能性が高いことを理解できるようにします。

テンプレートのデフォルト設定画像(/en-us/citrix-virtual-apps-desktops/2503/media/template-default-settings.png)

XenAppおよびXenDesktop 7.6 FP3より前の展開（ポリシー管理とVDA）を使用しており、高いサーバー拡張性とWAN向けに最適化されたテンプレートが必要な場合は、該当する場合にこれらのテンプレートのレガシーOSバージョンを使用してください。

> **注:**

> Citrixは組み込みテンプレートを作成および更新します。これらのテンプレートを変更または削除することはできません。

Web Studioを使用したテンプレートの作成と管理

テンプレートに基づいてテンプレートを作成するには：

1. Web Studioにサインインし、左ペインで**ポリシー**を選択します。
2. **テンプレート**タブを選択し、テンプレートを作成する元のテンプレートを選択します。
3. **テンプレートの作成**タブを選択します。**設定の選択**画面が表示されます。
4. テンプレートに含めるポリシー設定を選択して構成します。
5. 「**次へ**」をクリックします。「**概要**」画面が表示されます。
6. テンプレートの名前を入力します。
7. **Finish** をクリックします。新しいテンプレートが **Templates** タブに表示されます。

ポリシーに基づいてテンプレートを作成するには：

1. Web Studio にサインインし、左ペインで **Policies** を選択します。
2. **Policies** タブを選択し、テンプレートの作成元となるポリシーを選択します。
3. **More** タブをクリックします。
4. **Save as Template** を選択します。**Select Settings** 画面が表示されます。
5. テンプレートに含める新しいポリシー設定を選択して構成します。
6. **Next** をクリックします。**Summary** 画面が表示されます。
7. テンプレートの名前と説明を入力し、**Finish** をクリックします。

テンプレートと委任管理

Web Studio のテンプレートはサイトデータベースに保存されます。これに対し、Citrix Studio のテンプレートは、現在の管理者のユーザープロファイルフォルダーに `.gpt` 拡張子のファイルとして保存されます。ある管理者が作成した Citrix Studio テンプレートは、他の管理者や、別のマシン上の同じ管理者には表示されません。Web Studio のテンプレートは、権限と委任管理の対象となるすべての管理者に表示されます。

ポリシーの作成

> **注:**

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

> ポリシーを作成する前に、それが影響を与える可能性のあるユーザーまたはデバイスのグループを決定します。ユーザーの職務、接続の種類、ユーザーデバイス、または地理的な場所に基づいてポリシーを作成することができます。Windows Active Directoryグループポリシーで使用するのと同じ基準を使用することもできます。

すでにグループに適用されるポリシーを作成している場合は、別のポリシーを作成するのではなく、そのポリシーを編集することを検討してください。ポリシーを編集した後、適切な設定を構成します。特定の機能を有効にするためだけ、または特定のユーザーにポリシーが適用されないようにするためだけにポリシーを作成することは避けてください。

ポリシーを作成する際、ポリシーテンプレートの設定に基づいて作成し、必要に応じて設定をカスタマイズできます。テンプレートを使用せずに、必要なすべての設定を追加して作成することもできます。

Web Studioでは、**Enable policy**チェックボックスが明示的にオンにされていない限り、新しく作成されたポリシーは無効に設定されます。

ポリシー作成時および設定構成時に、システムは設定タイプを表示するオプションを提供します。次の設定タイプを表示できます。

- すべての設定 - すべてのVDAバージョンに適用されるすべてを表示
- 現在の設定のみ - 現在のVDAバージョンに固有の設定を表示
- レガシー設定のみ - 非推奨のVDAバージョンにのみ適用される設定を表示

設定を構成しながら設定を表示するには：

1. Web Studioにサインインし、左ペインで**Policies**を選択します。
2. **Policies**タブで、**Create Policy**をクリックします。
3. **Select Settings**テーブルで、**Settings**の横にあるドロップダウンをクリックします。
4. ドロップダウンから次のいずれかのオプションを選択します。

- すべての設定 - すべてのVDAバージョンのすべての設定を表示
- 現在の設定のみ - 現在のVDAバージョンのみの設定を表示します

- レガシー設定のみ - 非推奨のVDAバージョンのみの設定を表示します

1. 「**設定**」テーブルには、前の手順に基づいて利用可能な設定が一覧表示されます。

ポリシー設定

ポリシー設定は、有効、無効、または未構成にできます。デフォルトでは、ポリシー設定は構成されていません。つまり、ポリシーに追加されていません。設定は、ポリシーに追加された場合にのみ適用されます。

ポリシー設定は、依存するポリシー間の明確さを提供するために強化されています。この機能により、子ポリシー設定が有効になるように、親ポリシーが最初に構成されることが保証されます。

ポリシー設定を構成するには：

1. **ポリシーの作成**ページで、**設定の選択**の下にある「overall」を検索します。 **セッション全体の帯域幅制限**に関連するすべてのポリシー（親と子）が一覧表示されます。
2. 子ポリシーにカーソルを合わせると、ツールヒントが表示され、**セッション全体の帯域幅制限**親ポリシーが構成されるまで子ポリシーを構成できないことが示されます。
3. 親ポリシー設定を構成し、次に子ポリシー設定を構成して、**保存**をクリックします。
4. **設定**列と**現在の値**列には、**ポリシーの作成/編集**テーブルで構成された値が表示されます。このテーブルには、構成された設定を変更するための**編集**オプションが表示されます。

依存ポリシー設定(/en-us/citrix-daas/media/dependent-policy-settings.png)

> **注:**
>
> - 親ポリシーが構成されるまで、子ポリシーは選択できません。
> - 親ポリシーのチェックが外れると、関連付けられている子ポリシーもチェックが外れるか、選択解除されることを示すポップアップメッセージが表示されます。

次の表に、親ポリシーとそれに対応する依存ポリシーまたは子ポリシーのリストを示します。

親ポリシー	依存子ポリシー
セッション全体の帯域幅制限	オーディオリダイレクトの帯域幅制限（パーセント）

親ポリシー	依存子ポリシー
	クリップボードリダイレクトの帯域幅制限（パーセント）
	COMポートリダイレクトの帯域幅制限（パーセント）
	ファイルリダイレクトの帯域幅制限（パーセント）
	HDX™ MediaStreamマルチメディアアクセラレーションの帯域幅制限（パーセント）
	LPTポートリダイレクト帯域幅制限の割合
	プリンターリダイレクト帯域幅制限の割合
	クライアントUSBデバイスリダイレクト帯域幅制限の割合
	TWAINデバイスリダイレクト帯域幅制限の割合
双方向コンテンツリダイレクトを許可する	クライアントにリダイレクトされる許可されたURL
	VDAにリダイレクトされる許可されたURL
CPU使用率	CPU使用率から除外されるプロセスの優先度
レガシーグラフィックモード	プログレッシブ圧縮レベル
セッションウォーターマークを有効にする	ウォーターマークのカスタムテキスト
	セッションウォーターマークのスタイル
	ウォーターマークの透明度
HDXアダプティブトランスポート	オーディオの損失許容モード

一部のポリシー設定は、次のいずれかの状態になります。

- 許可または禁止は、設定によって制御されるアクションを許可または防止します。ユーザーがセッションで設定のアクションを管理することを許可または防止される場合があります。たとえば、メニューアニメーション設定が「許可」に設定されている場合、ユーザーはクライアント環境でメニューアニメーションを制御できます。
- 有効または無効は、設定をオンまたはオフにします。設定を無効にすると、下位のポリシーでは有効になりません。

さらに、一部の設定は、依存する設定の有効性を制御します。たとえば、クライアントドライブのリダイレクトは、ユーザーがデバイス上のドライブにアクセスできるかどうかを制御します。ユーザーがネットワークドライブにアクセスできるようにするには、この設定と**クライアントネットワークドライブ**設定の両方をポリシーに追加する必要があります。**クライアントドライブのリダイレクト**設定が無効になっている場合、**クライアントネットワークドライブ**設定が有効になっていても、ユーザーはネットワークドライブにアクセスできません。

一般に、マシンに影響を与えるポリシー設定の変更は、仮想デスクトップの再起動時またはユーザーのログオン時に有効になります。ユーザーに影響を与えるポリシー設定の変更は、ユーザーが次回ログオンしたときに有効になります。Active Directoryを使用している場合、ポリシー設定はActive Directoryが90分間隔でポリシーを再評価するときに更新されます。そして、ポリシー設定は、仮想デスクトップの再起動時またはユーザーのログオン時に適用されます。

一部のポリシー設定では、設定をポリシーに追加するときに値を入力または選択できます。「デフォルト値を使用」を選択することで、設定の構成を制限できます。この選択により、設定の構成が無効になり、ポリシーが適用されるときに設定のデフォルト値のみが使用されるようになります。この選択は、「デフォルト値を使用」を選択する前に入力された値に関係なく適用されます。

セキュアデフォルト設定が有効になっている場合、VDAインストール中に、ポリシー設定の優先順位は次のように影響を受けます。

- カスタマイズされた設定が最も高い優先順位を持ちます
- セキュアなデフォルト設定が2番目の優先順位を持ちます
- デフォルト設定が最も低い優先順位を持ちます

ポリシーのセキュアデフォルト設定を表示するには：

1. Web Studioにログオンします。
2. 左側のナビゲーションで、「**ポリシー**」をクリックします。
3. 「**ポリシー**」タブで、「**ポリシーの作成**」をクリックします。
4. 「**設定の選択**」テーブルで、現在の値が「**許可済み ?**」である設定にマウスカーソルを合わせると、「**セキュリティ保護されたデフォルト値: 禁止**」が表示されます。

ベストプラクティスとして：

- 個々のユーザーではなく、グループにポリシーを割り当てます。グループにポリシーを割り当てると、グループへのユーザーの追加または削除時に割り当てが自動的に更新されます。
- リモートデスクトップセッションホスト構成で、競合する設定や重複する設定を有効にしないでください。リモートデスクトップセッションホスト構成は、Citrixポリシー設定と同様の機能を提供することがあります。トラブルシューティングを容易にするため、可能な限りすべての設定を一貫して（有効または無効に）保ってください。
- 未使用のポリシーは無効にします。設定が追加されていないポリシーは、不要な処理を発生させます。

ポリシーの割り当て

ポリシーを作成するときは、特定のユーザーおよびマシンオブジェクトに割り当てます。そのポリシーは、特定の基準またはルールに従って接続に適用されます。一般に、基準の組み合わせに基づいて、ポリシーに好きなだけ割り当てを追加できます。

割り当てを指定しない場合、または割り当てを指定しても無効にした場合、ポリシーは**すべて**の接続に適用されます。

> **注:**
>
> ポリシーの割り当ては、ポリシーフィルターとも呼ばれます。詳細については、以下のトピックを参照してください。
>
> - ポリシーのフィルターを作成、変更、または削除する
> - フィルターはどのように適用されますか？
>
> 次の表に、利用可能な割り当てを示します。

割り当て名	ポリシーの適用基準
アクセス制御	クライアントが接続しているアクセス制御条件。*接続の種類* - NetScaler® Gatewayを使用しているかどうかにかかわらず、接続にポリシーを適用

割り当て名	ポリシーの適用基準
	するかどうか。*NetScaler Gatewayファーム名* - NetScaler Gateway仮想サーバーの名前。*アクセス条件* - 使用するエンドポイント分析ポリシーまたはセッションポリシーの名前。
NetScaler SD-WAN	ユーザーセッションがNetScaler SD-WANを介して起動されるかどうか。**注：**ポリシーにはNetScaler SD-WAN割り当てを1つだけ追加できます。
クライアントIPアドレス	クライアントが接続しているIPアドレス。これは、クライアントがセッションに接続する方法によって異なります。 • 直接内部ネットワーク接続: IPアドレスはクライアントのプライベートIPアドレスになります。 • NetScaler Gateway接続: IPアドレスはNetScalerのサブネットIPアドレスになります。
	ゲートウェイサービス接続。 • Rendezvousが無効の場合、IPアドレスはCloud Connectorのいずれかの IPアドレスになります。

割り当て名	ポリシーの適用基準	
	• Rendezvousが有効の場合、IPアドレスはGateway Serviceのパブリックアドレスになります。 IPv4の例: 12.0.0.0, 12.0.0.*, 12.0.0.1-12.0.0.70, 12.0.0.1/24; IPv6の例: 2001:0db8:3c4d:0015:0:0:abcd:ef12, 2001:0db8:3c4d:0015::/54	
クライアント名	ユーザーデバイスの名前。完全一致: ClientABCName。ワイルドカードの使用: Client*Name。	
クライアントプラットフォーム	セッションの接続に使用されるユーザーデバイスのOSタイプ（Windows、Linux、iOS、Android、HTML5など）。必要なVDAバージョン: 2503以降	
デリバリーグループ	デリバリーグループのメンバーシップ。	
デリバリーグループの種類	デスクトップまたはアプリケーションの種類: プライベートデスクトップ、共有デスクトップ、プライベートアプリケーション、または共有アプリケーション。**注:** プライベートデスクトップおよび共有デスクトップのフィルターオプションは、Citrix Virtual Apps and Desktops	

割り当て名	ポリシーの適用基準
	7.xでのみ利用可能です。詳細については、CTX219153を参照してください。
組織単位 (OU)	組織単位。
タグ	タグ。**注:** このポリシーは、タグ付けされたすべてのマシンに適用されます。アプリケーションタグは含まれません。
ユーザーまたはグループ	ユーザーまたはグループ名。

ユーザーがログオンすると、接続の割り当てに一致するすべてのポリシーが特定されます。これらのポリシーは優先順位順に並べ替えられ、設定の複数のインスタンスが比較されます。各設定は、ポリシーの優先順位に従って適用されます。無効になっているポリシー設定は、有効になっている下位ランクの設定よりも優先されます。構成されていないポリシー設定は無視されます。

重要:

Group Policy Management Console を使用して Active Directory ポリシーと Citrix ポリシーの両方を構成する場合、割り当てと設定が期待どおりに適用されないことがあります。詳細については、CTX127461を参照してください。

クライアントIPポリシーフィルターが常にクライアントのプライベートIPアドレスを使用するように設定するには、セッションホストで次のレジストリ設定を構成します。

- キー: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Ica\GroupPolicy`
- 値の型: `DWORD`
- 値の名前: `UseClientDeviceIpForPolicyFilter`
- 値のデータ: `1`

「Unfiltered」という名前のポリシーがデフォルトで提供されます。

- Web Studio を使用して Citrix ポリシーを管理する場合、Unfiltered ポリシーに追加した設定は、サイト内のすべてのサーバー、デスクトップ、および接続に適用されます。
- ローカルグループポリシーエディターを使用して Citrix ポリシーを管理する場合、Unfiltered ポリシーに追加した設定は、すべてのサイトと接続に適用されます。サイトと接続は、ポリシーを含むグループポリシーオブジェクト (GPO) のスコープ内にある必要があります。たとえば、Sales OU には、米国の営業チームのすべてのメンバーを含む Sales-US という GPO が含まれています。Sales-US GPO は、いくつかのユーザーポリシー設定を含む Unfiltered ポリシーで構成されています。米国の営業マネージャーがサイトにログオンすると、Unfiltered ポリシーの設定がセッションに自動的に適用されます。この構成は、ユーザーが Sales-US GPO のメンバーであるためです。

割り当てのモードは、ポリシーがすべての割り当て条件に一致する接続にのみ適用されるかどうかを決定します。モードが「許可」（デフォルト）に設定されている場合、ポリシーは割り当て条件に一致する接続にのみ適用されます。モードが「拒否」に設定されている場合、接続が割り当て条件に一致しない場合にポリシーが適用されます。以下の例は、複数の割り当てが存在する場合に、割り当てモードがCitrixポリシーにどのように影響するかを示しています。

- **例: 異なるモードを持つ同種の割り当て** - 同じタイプの2つの割り当てを持つポリシーで、一方が「許可」に設定され、もう一方が「拒否」に設定されている場合、接続が両方の割り当てを満たしていれば、「拒否」に設定された割り当てが優先されます。例:

  ポリシー 1 には次の割り当てが含まれます。

  - 割り当てAは営業グループを指定します。モードは「許可」に設定されています。
  - 割り当てBは営業マネージャーのアカウントを指定します。モードは「拒否」に設定されています。

  割り当てBのモードが「拒否」に設定されているため、営業マネージャーがサイトにログオンしても、ユーザーが営業グループのメンバーであっても、ポリシーは適用されません。
- **例: 同様のモードを持つ異なるタイプの割り当て** - 異なるタイプの2つ以上の割り当てが「許可」に設定されているポリシーでは、ポリシーが適用されるためには、接続が各タイプの少なくとも1つの割り当てを満たす必要があります。例:

  ポリシー 2 には次の割り当てが含まれます。

  - 割り当てCは、営業グループを指定するユーザー割り当てです。モードは「許可」に設定されています。
  - 割り当てDは、10.8.169.*（企業ネットワーク）を指定するクライアントIPアドレス割り当てです。モードは「許可」に設定されています。

営業マネージャーがオフィスからサイトにログオンすると、接続が両方の割り当てを満たすため、ポリシーが適用されます。

ポリシー3には、次の割り当てが含まれます。

- 割り当てEは、営業グループを指定するユーザー割り当てです。モードは「許可」に設定されています。
- 割り当てFは、NetScaler Gatewayの接続条件を指定するアクセスコントロール割り当てです。モードは「許可」に設定されています。

営業マネージャーがオフィスからサイトにログオンしても、接続が割り当てFを満たさないため、ポリシーは適用されません。

Web Studioを使用して、テンプレートに基づいてポリシーを作成する

1. Web Studioにサインインし、左側のペインで**［ポリシー］**を選択します。
2. **［テンプレート］**タブを選択し、テンプレートを選択します。
3. アクションバーで**［テンプレートからポリシーを作成］**を選択します。
4. デフォルトでは、新しいポリシーはテンプレートのすべてのデフォルト設定を使用します。この場合、**［テンプレートのデフォルト設定（推奨）］**が選択されています。設定を変更する場合は、［デフォルト設定を変更して追加］**を選択し、設定を追加または削除します。
5. 次のいずれかを選択して、ポリシーの適用方法を指定します。

   - **選択したユーザーおよびマシンオブジェクト**。ポリシーを選択したユーザーおよびマシンオブジェクトに適用するには、**［割り当て］**をクリックして、ポリシーを適用するユーザーおよびマシンオブジェクトを選択します。
   - **サイト内のすべてのオブジェクト**。ポリシーをサイト内のすべてのユーザーおよびマシンオブジェクトに適用します。

6. ポリシーの名前を入力します。ポリシーが影響する対象（例：経理部、リモートユーザーなど）に基づいてポリシーに名前を付けることを検討してください。必要に応じて、説明を追加します。

   ポリシーはデフォルトで無効になっています。有効にできます。ポリシーを有効にすると、ログオンするユーザーにすぐに適用できるようになります。無効にすると、ポリシーが適用されなくなります。ポリシーの優先順位を付けたり、後で設定を追加したりする必要がある場合は、適用する準備ができるまでポリシーを無効にしておくことを検討してください。

Web Studio を使用してポリシーを作成する

1. Web Studio にサインインし、左側のペインで を選択します。
2. タブを選択します。
3. アクションバーで を選択します。
4. ポリシー設定を追加および構成します。
5. 次のいずれかを選択して、ポリシーの適用方法を指定します。
   - 選択したユーザーおよびマシンオブジェクトに割り当て、ポリシーを適用する必要があるユーザーおよびマシンオブジェクトを選択します。
   - サイト内のすべてのオブジェクトに割り当てて、サイト内のすべてのユーザーおよびマシンオブジェクトにポリシーを適用します。
6. ポリシーの名前を入力するか、デフォルトを受け入れます。ポリシーが影響する対象（例: 経理部、リモートユーザー）に基づいてポリシーに名前を付けることを検討してください。必要に応じて、説明を追加します。

   ポリシーはデフォルトで有効になっています。無効にできます。ポリシーを有効にすると、ログオンするユーザーにすぐに適用できるようになります。無効にすると、ポリシーが適用されなくなります。ポリシーの優先順位を付けたり、後で設定を追加したりする必要がある場合は、適用する準備ができるまでポリシーを無効にしておくことを検討してください。

グループポリシーエディターを使用してポリシーを作成および管理する

グループポリシーエディターから、**コンピューターの構成またはユーザーの構成**を展開します。**ポリシー**ノードを展開し、次に、**Citrixポリシー**を選択します。適切なアクションを選択してください。

タスク	手順
ポリシーを作成する	**ポリシー**タブで、**新規**をクリックします。
既存のポリシーを編集する	**ポリシー**タブで、ポリシーを選択し、**編集**をクリックします。
既存のポリシーの優先度を変更する	**ポリシー**タブでポリシーを選択し、**上位**または**下位**をクリックします。
ポリシーの概要情報を表示する	**ポリシー**タブでポリシーを選択し、**概要**タブをクリックします。

タスク	手順
ポリシー設定を表示および修正する	**ポリシー**タブでポリシーを選択し、**設定**タブをクリックします。
ポリシーフィルターを表示および修正する	**ポリシー**タブでポリシーを選択し、**フィルター**タブをクリックします。ポリシーに複数のフィルターを追加する場合、ポリシーが適用されるには、すべてのフィルター条件が満たされている必要があります。
ポリシーを有効または無効にする	**ポリシー**タブでポリシーを選択し、**アクション > 有効**または**アクション > 無効**を選択します。
既存のテンプレートからポリシーを作成する	**テンプレート**タブでテンプレートを選択し、**新しいポリシー**をクリックします。

ポリシーセット

ポリシーセットは、Citrix Virtual Apps and Desktops™ のオブジェクトであり、ポリシーを集約して、簡素化されたロールベースのアクセスと容易な管理を可能にします。管理者チームや会社の論理的な区分を反映するようにポリシーセットを作成できます。例えば、地理的地域、事業部門、または特定のユースケースごとにポリシーセットを作成できます。作成後、スコープとデリバリーグループがポリシーセットに割り当てられ、承認された管理者のみが関連するユーザーとマシンに適用されるポリシーを管理できるようになります。

注:

ポリシーセットを有効にする前に、Citrix® は以下の点に注意することを推奨します。

- 追加のポリシー検証が追加されます。その結果、無効なポリシー設定が存在する場合、インプレースアップグレードを行うとポリシーデータが失われる可能性があります。
- 無効なデータを検出するには、GPOスキャナーツール を使用し、アップグレード前に必要な編集を行ってください。詳細については、CTX676686 を参照してください。
- 今後のすべてのアップグレードでは、最新のSDKを使用することをCitrixは推奨します。ポリシーの更新に古いSDKを使用すると、無効なデータがポリシー設定に追加される可能性があり、ポリシーデータが失われるリスクにつながる可能性があります。

利点

- 分散型管理者チーム向けのロールベースのアクセス制御
- 合併、買収、統合の簡素化
- 制限された障害ドメイン
- ポリシーのマルチテナントサポート

ポリシーセットを有効にする

Virtual Apps and Desktops の タブから、 に移動し、 設定をオンにします。

ポリシーセットを有効にする(/en-us/citrix-virtual-apps-desktops/2503/media/enable-policy-set.png)

> **注：**
>
> ポリシーセットを作成する前に、ポリシーセットを有効にする必要があります。

機能の比較

ポリシーセットを適用する前	ポリシーセットを適用した後
サイト全体のポリシー、設定、フィルター、およびポリシーの優先順位は、Citrix Studio内で一箇所で構成されます。	ポリシー、設定、フィルター、およびポリシーの優先順位は、各ポリシーセットに対して個別に構成されます。
1つのポリシーを管理する場合、すべてのポリシーを管理する必要があります。	フル管理者は、特定のポリシーセットを個別に管理する機能を下位レベルの管理者に委任できます。
大規模で分散された環境では、ポリシーが複雑になり、管理が困難になります。	大規模で分散された環境では、ポリシーを簡単に分割して管理できます。

ポリシーセットの仕組み?

概要

- ポリシーセットはデリバリーグループに割り当てられます
- ポリシーセットには1つまたは複数のスコープがあります

- ポリシーセットが割り当てられていないデリバリーグループは、デフォルトのポリシーセットを受け取ります
- デリバリーグループには、1つのポリシーセットのみを割り当てることができます
- 複数のデリバリーグループで同じポリシーセットを使用できます
- ポリシーセットがデリバリーグループに割り当てられていても、ポリシーはフィルターを維持します

詳細については、「フィルターはどのように適用されますか？」を参照してください。ポリシーセットのポリシー割り当てまたはポリシーフィルターの動作方法に変更はありません。つまり、ポリシーの場合と同じように機能します。

デフォルトのポリシーセット

- ポリシーセット設定がオンになると、既存のすべてのポリシーはデフォルトのポリシーセット内にグループ化されます。
- 管理者チームがポリシーセットを作成してデリバリーグループに割り当てない限り、すべてのデリバリーグループはデフォルトのポリシーセットを受け取ります。
- デリバリーグループに別のポリシーセットが割り当てられると、デフォルトのポリシーセットからポリシーを受け取らなくなります。

ポリシーセットの作成

ポリシーセットは、次の2つの方法で作成できます。

- ポリシーセットの作成 - このアクションにより、空のポリシーセットが作成されます。
- ポリシーセットのクローン - このアクションにより、既存のポリシーセットに基づいてポリシーセットが作成されます。

ポリシーセットの作成

1. Web Studioにサインインし、左ペインで**ポリシー**を選択します。

ポリシーセットを作成(/en-us/citrix-virtual-apps-desktops/2503/media/create-policy-set.png)

1. **ポリシーセットの作成**を選択します。**はじめに**タブが表示されます。
2. **次へ**をクリックするか、**名前と説明**タブをクリックします。
3. ポリシーセットの名前と説明を入力します。
4. **次へ**をクリックするか、**割り当て**タブをクリックします。
5. ポリシーセットを割り当てる1つ以上のデリバリーグループを選択します。

6. **次へ**をクリックするか、**スコープ**タブをクリックします。
7. ポリシーセットのスコープを選択します。
8. **作成**をクリックします。定義された割り当てとスコープでポリシーセットが作成されます。

ポリシーセットのクローンを作成する

1. Web Studioにサインインし、左ペインで「**ポリシー**」を選択します。
2. 「**ポリシーセットのクローンを作成**」を選択します。
3. ポリシーセットの名前を変更します。
4. ポリシーセットの割り当てを変更または作成し、**次へ**をクリックします。
5. クローンされたポリシーセットに含めるポリシーを選択または選択解除します。
6. ポリシーのスコープを変更します。
7. **作成**をクリックします。ポリシーセットが作成されます。

ポリシーセットの編集

1. Web Studioにサインインし、左ペインで**ポリシー**を選択します。
2. **ポリシーセットの編集**を選択します。
3. ポリシーセットの名前を変更し、**次へ**をクリックします。
4. ポリシーセットの割り当てを変更または作成し、**次へ**をクリックします。
5. ポリシーのスコープを変更します。
6. **Create** をクリックします。

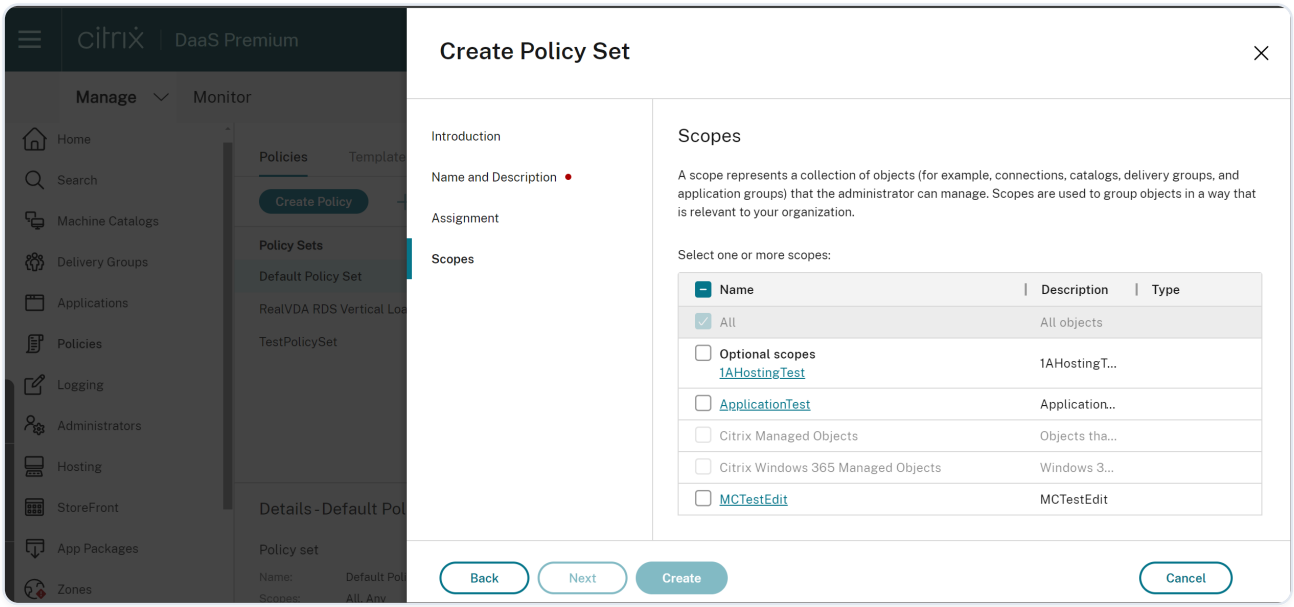
ポリシーセットの割り当て

ポリシーセットはデリバリーグループに割り当てられます。ポリシーセットの作成時または編集時に割り当てを構成できます。デリバリーグループの作成時または編集時にも割り当てを構成できます。

ポリシーセットのスコープ

管理者はポリシーセットのスコープを定義して、承認された管理者のみが表示または編集できるようにすることができます。ポリシーセットの作成時または編集時にスコープを構成できます。

ポリシーセットの導入により、API を使用して Citrix ポリシーを作成および管理することもできます。詳細については、「Citrix DaaS でポリシーセットを作成する方法」を参照してください。



ポリシーの比較、優先順位付け、モデル化、トラブルシューティング

注:

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

複数のポリシーを使用して、ユーザーの職務、地理的な場所、または接続の種類に基づいて、ユーザーのニーズを満たすように環境をカスタマイズできます。たとえば、セキュリティを強化するために、機密データを定期的に扱うユーザーグループに制限を設けることができます。

また、ユーザーが機密ファイルをローカルクライアントドライブに保存できないようにするポリシーを作成することもできます。ただし、ユーザーグループ内の一部のユーザーがローカルドライブへのアクセスを必要とする場合は、それらのユーザー専用の別のポリシーを作成できます。その後、どちらが優先されるかを制御するために、2つのポリシーのランク付けまたは優先順位付けを行います。複数のポリシーを使用する場合、次のことを決定する必要があります。

- ポリシーの優先順位付け方法
- 例外の作成方法

- ポリシーが競合する場合に有効なポリシーを表示する方法。

一般に、ポリシーは、サイト全体、特定のDelivery Controller、またはユーザーデバイス用に構成された同様の設定を上書きします。この原則の例外はセキュリティです。環境内で最も高い暗号化設定は、常に他の設定やポリシーを上書きします。最も高い暗号化設定には、オペレーティングシステムと最も制限の厳しいシャドウイング設定が含まれます。

Citrixポリシーは、オペレーティングシステムで設定したポリシーと相互作用します。Citrix環境では、Citrix設定は、Active Directoryポリシーまたはリモートデスクトップセッションホスト構成を使用して構成された同じ設定を上書きします。この設定には、一般的なリモートデスクトッププロトコル（RDP）クライアント接続設定に関連する設定が含まれます。一般的なRDP設定には、デスクトップの壁紙、メニューアニメーション、ドラッグ中のウィンドウコンテンツの表示などの設定が含まれます。

Secure ICA®などの一部のポリシー設定は、オペレーティングシステムの設定と一致している必要があります。より高い優先度の暗号化レベルが他の場所で設定されている場合、ポリシーで指定した、またはアプリケーションとデスクトクトップを配信するときに指定した**Secure ICAポリシー**設定が上書きされる可能性があります。

たとえば、デリバリーグループを作成するときに指定する暗号化設定は、環境全体で指定した暗号化設定と同じレベルである必要があります。

> **注:**
>
> ダブルホップシナリオの2番目のホップでは、シングルセッションOS VDAがマルチセッションOS VDAに接続することを考慮してください。この場合、Citrixポリシーは、シングルセッションOS VDAをユーザーデバイスであるかのように扱います。たとえば、ユーザーデバイスに画像をキャッシュするようにポリシーが設定されているとします。この例では、ダブルホップシナリオの2番目のホップ用にキャッシュされた画像は、シングルセッションOS VDAマシンにキャッシュされます。

ポリシーモデリングウィザードの使用

ポリシーモデリングは、計画およびテスト目的で、フィルター付きの有効なポリシーをシミュレートするのに役立ちます。フィルター付きの有効なポリシーのみがモデル化されます。無効なポリシーは適用されず、フィルターなしの有効なポリシーは常に適用されます。

ポリシーモデリングウィザードを開くには、次の手順を実行します。

1. 左側のナビゲーションから を選択します。
2. タブを選択します。
3. アクションバーで を選択します。
4. ページを読み、 をクリックします。
5. ユーザーまたはコンピューターを選択します。コンテナー、特定のユーザー、またはコンピューターを参照できます。 をクリックします。
6. フィルターの証拠を選択します。必要に応じて、、、 などの追加の詳細を入力して、シミュレーションをより詳細にすることができます。 をクリックします。
7. 選択内容の概要を確認し、 をクリックします。

をクリックすると、ウィザードはモデリング結果のレポートを生成します。このレポートを表示している間、次のことができます。

- ドロップダウンメニューで、、、または のいずれを表示するかを選択します。
- 検索バーを使用して、特定の設定を検索します。
- 特定の設定をクリックして、その設定の詳細を表示します。たとえば、特定のポリシーにすべてのユーザー設定が適用されなかった場合、 ペインに設定が適用されなかった理由が表示されます。
- をクリックして、モデリング結果をJSON形式、HTML形式、またはその両方でエクスポートします。

ポリシーモデリングを実行すると、さらに多くのオプションが利用可能になります。次のことができます。

- **モデリングレポートの表示**: 上記と同じモデリングレポートが開き、再度表示したりエクスポートしたりできます。
- **ポリシーモデリングの再実行**: これにより、以前に選択したのと同じ基準セットでポリシーモデリングを再実行し、新しいモデリング結果を生成できます。これは、一部のポリシーが変更され、それらの変更が現在のモデルにどのように影響するかを確認したい場合に役立ちます。
- **モデリングレポートの削除**: 現在のモデリングレポートを削除します。

ポリシーとテンプレートの比較

ポリシーまたはテンプレートの設定を、他のポリシーまたはテンプレートの設定と比較できます。たとえば、ベストプラクティスへの準拠を維持するために、設定値を検証する必要がある場合

があります。また、ポリシーまたはテンプレートの設定を、Citrixが提供するデフォルト設定と比較することもできます。

1. Web Studioにサインインし、左ペインで**［ポリシー］**を選択します。
2. **［比較］タブをクリックし、［選択］**をクリックします。
3. 比較するポリシーまたはテンプレートを選択します。比較にデフォルト値を含めるには、**［デフォルト設定と比較］**チェックボックスをオンにします。
4. **［比較］**をクリックすると、構成された設定が列に表示されます。
5. すべての設定を表示するには、**［すべての設定を表示］を選択します。デフォルトビューに戻るには、［共通設定を表示］**を選択します。

ポリシーの優先順位付け

ポリシーに競合する設定が含まれている場合、ポリシーの優先順位を付けることで、その優先順位を定義できます。ユーザーがログオンすると、接続の割り当てに一致するすべてのポリシーが特定されます。これらのポリシーは優先順位順に並べ替えられ、設定の複数のインスタンスが比較されます。各設定は、ポリシーの優先順位に従って適用されます。

ポリシーに異なる優先順位番号を付けることで、ポリシーの優先順位を付けます。デフォルトでは、新しいポリシーには最も低い優先順位が与えられます。ポリシー設定が競合する場合、優先順位が高いポリシー（優先順位番号1が最も高い）は、優先順位が低いポリシーを上書きします。設定は、優先順位と設定の条件（たとえば、設定が無効か有効か）に従ってマージされます。無効な設定は、有効な下位ランクの設定を上書きします。構成されていないポリシー設定は無視され、下位ランクの設定を上書きしません。

1. 左ペインで**［ポリシー］を選択します。［ポリシー］**タブが選択されていることを確認してください。
2. **［ポリシー］タブで、アクションバーの［ポリシーの優先順位の変更］を選択します。［ポリシーの優先順位の変更］**ページが表示されます。
3. 優先順位リストで、ポリシーの優先順位を変更するには、次のいずれかの方法を使用します。
   - ポリシーを目的の位置にドラッグします。
   - 1つ上または下に移動するには、それぞれ上矢印または下矢印アイコンをクリックします。
   - リストの先頭または末尾に移動するには、それぞれ先頭または末尾の矢印アイコンをクリックします。
   - 優先順位番号を変更するには、 アイコンをクリックし、必要に応じて番号を入力し、 をクリックします。

4. 「**保存**」をクリックします。

例外

ユーザー、ユーザーデバイス、またはマシンのグループに対してポリシーを作成する場合、グループの一部のメンバーが特定のポリシー設定の例外を必要とすることがあります。例外を作成するには、次の方法があります。

- 例外を必要とするグループメンバーのみのポリシーを作成し、そのポリシーをグループ全体のポリシーよりも上位にランク付けする
- ポリシーに追加された割り当てに拒否モードを使用する

モードが拒否に設定された割り当ては、割り当て条件に一致しない接続にのみポリシーを適用します。たとえば、ポリシーには次の割り当てが含まれます。

- 割り当てAは、範囲208.77.88.*を指定するクライアントIPアドレスの割り当てです。モードは許可に設定されています
- 割り当てBは、特定のユーザーアカウントを指定するユーザー割り当てです。モードは拒否に設定されています。

ポリシーは、割り当てAで指定された範囲のIPアドレスを使用してサイトにログオンするすべてのユーザーに適用されます。ただし、割り当てBで指定されたユーザーアカウントを使用してサイトにログオンするユーザーにはポリシーは適用されません。

接続に適用されるポリシーを決定する

複数のポリシーが適用されるため、接続が期待どおりに応答しない場合があります。優先度の高いポリシーが接続に適用される場合、元のポリシーで構成した設定が上書きされることがあります。ポリシーの結果セットを計算し、接続に対して最終的なポリシー設定がどのように結合されるかを判断できます。

ポリシーの結果セットは、次の方法で計算できます。

- **Citrixグループポリシーモデリング**ウィザードを使用して接続シナリオをシミュレートし、Citrixポリシーがどのように適用されるかを識別します。接続シナリオの条件を次のように指定できます。
    - ドメインコントローラー
    - ユーザー
    - Citrixポリシー割り当ての証拠値

    - 低速ネットワーク接続などのシミュレートされた環境設定 ウィザードが生成するレポートには、そのシナリオで有効になるCitrixポリシーが一覧表示されます。ドメインユーザーとしてコントローラーにログオンするため、ウィザードはサイトポリシー設定とActive Directoryグループポリシーオブジェクト（GPO）の両方を使用して結果を計算します。

- **グループポリシーの結果**を使用して、特定のユーザーとコントローラーに適用されているCitrixポリシーを記述したレポートを生成します。グループポリシーの結果ツールは、環境内のGPOの現在の状態を評価し、レポートを生成するのに役立ちます。生成されたレポートには、Citrixポリシーを含むこれらのオブジェクトが、特定のユーザーとコントローラーに現在どのように適用されているかが記述されています。

Web StudioでCitrixグループポリシーモデリングウィザードを起動できます。または、Windowsのグループポリシー管理コンソールからグループポリシーの結果ツールを起動することもできます。

Web Studioを使用して作成されたサイトポリシー設定は、次の場合、ポリシーの結果セットに含まれません。

- グループポリシー管理コンソールからCitrixグループポリシーモデリングウィザードを実行する場合
- グループポリシー管理コンソールからグループポリシーの結果ツールを実行する場合

最も包括的なポリシーの結果セットを取得することを確認するには、グループポリシー管理コンソールのみを使用してポリシーを作成する場合を除き、CitrixはWeb StudioからCitrixグループポリシーモデリングウィザードを起動することを推奨します。

ポリシーのトラブルシューティング

ユーザー、IPアドレス、およびその他の割り当てられたオブジェクトには、同時に適用される複数のポリシーが存在する場合があります。このシナリオでは、ポリシーが期待どおりに動作しない競合が発生する可能性があります。Citrixグループポリシーモデリングウィザードまたはグループポリシーの結果ツールを実行すると、ユーザー接続にポリシーが適用されていないことがわかる場合があります。このようなシナリオでは、ポリシー評価基準に一致する条件下でアプリケーションやデスクトップに接続するユーザーには、ポリシー設定が適用されません。この状況は次の場合に発生します。

- ポリシー評価基準に一致する割り当てを持つポリシーがありません。
- 割り当てに一致するポリシーに設定が構成されていません。
- 割り当てに一致するポリシーが無効になっています。

指定された基準を満たす接続にポリシー設定を適用する場合は、以下を確認してください。

- それらの接続に適用するポリシーが有効になっていること。
- 適用するポリシーに適切な設定が構成されていること。

デフォルトのポリシー設定

以下の表に、ポリシー設定、そのデフォルト値、およびそれらが適用されるVirtual Delivery Agent (VDA) のバージョンを示します。

ICA®

名前	デフォルト設定	VDA
アダプティブトランスポート	オフ。推奨される場合に使用	VDA 7.13～7.15; VDA 7.16以降
クライアントクリップボードリダイレクト	許可	すべてのVDAバージョン
クライアントクリップボード書き込み許可形式	形式は指定されていません	VDA 7.6 以降
デスクトップの起動	禁止	マルチセッションOS用VDA 7以降
ICAリスナーポート番号	1494	すべてのVDAバージョン
クライアント接続中の非公開プログラムの起動	禁止	マルチセッションOS用VDA 7以降
クリップボードのクライアントからセッションへの転送サイズを制限	無効	VDA 2009
クリップボードのセッションからクライアントへの転送サイズを制限	無効	VDA 2009
損失許容モード	許可	VDA 2003。注：損失許容モードはまだ利用できません。このバージョンのVDAは、利用可能になった際にそれをサポートします。

名前	デフォルト設定	VDA
損失許容しきい値	損失許容モードが利用可能な場合：パケット損失：5%、遅延：300ミリ秒（RTT）	VDA 2003から現在まで
ランデブープロトコル	無効	Citrix Cloudを介して確立されたHDXセッションにのみ適用されます。
クライアントクリップボードへの書き込みを制限	禁止	VDA 7.6から現在まで
セッションクリップボードへの書き込みを制限	禁止	VDA 7.6から現在まで
セッションクリップボード書き込み許可形式	形式は指定されていません	VDA 7.6以降
タブレットモードの切り替え	有効	VDA 7.16以降。VDA 7.14および7.15 LTSRの場合、この設定はレジストリを使用して構成します。
仮想チャネル許可リスト	有効	VDA 2109以降
セッションメトリック収集	許可	7.42以降

ICA/Adobe Flash 配信/Flash リダイレクト

名前	デフォルト設定	VDA
Flashビデオのフォールバック防止	未構成	VDA 7.6 FP3から現在まで
Flashビデオのフォールバック防止エラー *.swf	VDA 7.6 FP3から現在まで	

ICA/オーディオ

名前	デフォルト設定	VDA
アダプティブオーディオ	有効	Citrix Virtual Apps and Desktops™ 2109以降を使用するVDAの、シングルセッションOSおよびマルチセッションOSの両方のセッションに適用されます。
UDPリアルタイムトランスポート経由のオーディオ	許可	すべてのVDAバージョン
オーディオプラグアンドプレイ	許可	マルチセッションOS用VDA 7 から現在まで
オーディオ品質	高 - 高精細オーディオ	すべてのVDAバージョン
クライアントオーディオリダイレクト	許可	すべてのVDAバージョン
クライアントマイクのリダイレクト	許可	すべてのVDAバージョン
オーディオのロストレラントモード	禁止	VDAバージョン2411以前

ICA/自動クライアント再接続

名前	デフォルト設定	VDA
自動クライアント再接続	許可	すべてのVDAバージョン
自動クライアント再接続認証	認証を要求しない	すべてのVDAバージョン
自動クライアント再接続ログ	自動再接続イベントをログに記録しない	すべてのVDAバージョン
自動クライアント再接続タイムアウト	120秒	VDA 7.13 から現在まで
再接続UIの透過レベル	80%	VDA 7.13 から現在まで

ICA/帯域幅

名前	デフォルト設定	VDA
オーディオリダイレクト帯域幅制限	0 キロビット/秒	すべてのVDAバージョン
オーディオリダイレクト帯域幅制限の割合	0	すべてのVDAバージョン
クライアントUSBデバイスリダイレクト帯域幅制限	0 キロビット/秒	VDA 5.5、5.6 FP1、マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
クライアントUSBデバイスリダイレクト帯域幅制限（パーセント）	0	VDA 5.5、5.6 FP1、マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
クリップボードリダイレクト帯域幅制限	0 キロビット/秒	すべてのVDAバージョン
クリップボードリダイレクト帯域幅制限（パーセント）	0	すべてのVDAバージョン
COMポートリダイレクト帯域幅制限	0 キロビット/秒	すべてのVDAバージョン。VDA 7.0〜7.8の場合、この設定はレジストリを使用して構成します。
COMポートリダイレクト帯域幅制限の割合	0	すべてのVDAバージョン。VDA 7.0から7.8の場合、この設定はレジストリを使用して構成します
ファイルリダイレクト帯域幅制限	0 キロビット/秒	すべてのVDAバージョン
ファイルリダイレクト帯域幅制限の割合	0	すべてのVDAバージョン

名前	デフォルト設定	VDA
HDX MediaStreamマルチメディアアクセラレーション帯域幅制限	0 キロビット/秒	VDA 5.5、5.6 FP1、マルチセッションOS用VDA 7およびシングルセッションOS用VDA 7から現在のマルチセッションOS用VDAおよびシングルセッションOS用VDAまで
HDX MediaStreamマルチメディアアクセラレーション帯域幅制限の割合	0	VDA 5.5、5.6 FP1、マルチセッションOS用VDA 7から現在まで、シングルセッションOS用VDA 7から現在まで
LPTポートリダイレクト帯域幅制限	0 キロビット/秒	すべてのVDAバージョン。VDA 7.0から7.8までは、レジストリを使用してこの設定を構成します。
LPTポートリダイレクト帯域幅制限（パーセント）	0	すべてのVDAバージョン。VDA 7.0から7.8までは、レジストリを使用してこの設定を構成します。
セッション全体の帯域幅制限	0 キロビット/秒	すべてのVDAバージョン
プリンターリダイレクト帯域幅制限	0 キロビット/秒	すべてのVDAバージョン
プリンターリダイレクト帯域幅制限（パーセント）	0	すべてのVDAバージョン
TWAINデバイスリダイレクト帯域幅制限	0 キロビット/秒	VDA 5.5、5.6 FP1、マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
TWAINデバイスリダイレクト帯域幅制限率	0	VDA 5.5、5.6 FP1、マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降

ICA/双方向コンテンツリダイレクト

名前	デフォルト設定	VDA
双方向コンテンツリダイレクトを許可する	禁止	VDA 7.13以降
クライアントにリダイレクトされる許可されたURL	空	VDA 7.13 以降
VDA にリダイレクトされる許可された URL	空	VDA 7.13 以降
双方向コンテンツリダイレクト構成	無効	VDA 2311 以降

ICA/ブラウザコンテンツリダイレクト

名前	デフォルト設定	VDA
ブラウザコンテンツリダイレクト	許可	VDA 7.16 以降
ブラウザコンテンツリダイレクト ACL 構成	`https://www.youtube.com/*`	VDA 7.16 から現在まで
ブラウザーコンテンツリダイレクトの統合Windows認証サポート	禁止	VDA 2106 から現在まで
ブラウザーコンテンツリダイレクトのプロキシ構成	空	VDA 7.16 から現在まで
ブラウザーコンテンツリダイレクトのサーバーフェッチWebプロキシ認証	禁止	VDA 2012 から現在まで

ICA/クライアントセンサー

名前	デフォルト設定	VDA
アプリケーションによるクライアントデバイスの物理的な場所の使用を許可する	禁止	VDA 5.6 FP1、マルチセッションOS用VDA 7から現在まで、シングルセッションOS用VDA 7から現在まで

ICA/デスクトップUI

名前	デフォルト設定	VDA
デスクトップコンポジションリダイレクト	無効 (7.6 FP3から現在まで); 有効 (5.6から7.6 FP2まで)	VDA 5.6、シングルセッションOS用VDA 7から7.15まで
デスクトップコンポジションリダイレクトのグラフィック品質	中	VDA 5.6、シングルセッションOS用VDA 7から7.15まで
デスクトップの壁紙	許可	すべてのVDAバージョン
メニューアニメーション	許可	すべてのVDAバージョン
ドラッグ中にウィンドウの内容を表示	許可	すべてのVDAバージョン

ICA/エンドユーザー監視

名前	デフォルト設定	VDA
ICAラウンドトリップ計算	有効	すべてのVDAバージョン
ICAラウンドトリップ計算間隔	15秒	すべてのVDAバージョン
アイドル接続のICAラウンドトリップ計算	無効	すべてのVDAバージョン

ICA/強化されたデスクトップエクスペリエンス

名前	デフォルト設定	VDA
強化されたデスクトップエクスペリエンス	許可	マルチセッションOS 7以降のVDA

ICA/ファイルリダイレクト

名前	デフォルト設定	VDA
クライアントドライブの自動接続	許可	すべてのVDAバージョン
クライアントドライブのリダイレクト	許可	すべてのVDAバージョン
クライアント固定ドライブ	許可	すべてのVDAバージョン
クライアントフロッピードライブ	許可	すべてのVDAバージョン
クライアントネットワークドライブ	許可	すべてのVDAバージョン
クライアントの光学ドライブ	許可	すべてのVDAバージョン
クライアントのリムーバブルドライブ	許可	すべてのVDAバージョン
ホストからクライアントへのリダイレクト	無効	マルチセッションOS用VDA 7以降
クライアントドライブ文字の保持	無効	VDA 5、5.5、5.6 FP1、シングルセッションOS用VDA 7以降
クライアントドライブへの読み取り専用アクセス	無効	VDA 5.5、5.6 FP1、マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降

名前	デフォルト設定	VDA
特殊フォルダーのリダイレクト	許可	Web Interface展開のみ。マルチセッションOS用VDA 7以降
非同期書き込みの使用	無効	すべてのVDAバージョン

ICA/グラフィック

名前	デフォルト設定	VDA
視覚的にロスレスな圧縮を許可	無効	VDA 7.6以降
表示メモリ制限	65,536 Kb	VDA 5、5.5、5.6 FP1、シングルセッションOS用VDA 7以降
表示モードの劣化の優先順位	最初に色深度を低下させる	すべてのVDAバージョン
動的ウィンドウプレビュー	有効	VDA 5.5、5.6 FP1、マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
グラフィックステータスインジケーター	無効	VDA 7.16以降
画像キャッシュ	有効	VDA 5.5、5.6 FP1、マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
レガシーグラフィックモード	無効	マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
許可される最大色深度	32ビット/ピクセル	すべてのVDAバージョン
ディスプレイモードが劣化した場合にユーザーに通知する	無効	マルチセッションOS用VDA 7以降

名前	デフォルト設定	VDA
3Dグラフィックワークロード向けに最適化	無効	VDA 7.17から現在まで
キューイングとトッシング	有効	すべてのVDAバージョン
画面共有	無効	VDA 2112
圧縮にビデオコーデックを使用	優先される場合にビデオコーデックを使用	VDA 7.6 FP3 から現在まで
ビデオコーデックにハードウェアエンコーディングを使用	有効	VDA 7.11 から現在まで

ICA/グラフィック/キャッシュ

名前	デフォルト設定	VDA
永続キャッシュしきい値	3,000,000 ビット/秒	マルチセッションOS用VDA 7 から現在まで

ICA/グラフィック/Framehawk

名前	デフォルト設定	VDA
Framehawk 表示チャネル	無効	VDA 7.6 FP2 から現在まで
Framehawk 表示チャネルポート範囲	3224,3324	VDA 7.6 FP2 から現在まで

ICA/キープアライブ

名前	デフォルト設定	VDA
ICAキープアライブタイムアウト	60秒	すべてのVDAバージョン
ICAキープアライブ	ICAキープアライブメッセージを送信しない	すべてのVDAバージョン

ICA/キーボードおよびIME

名前	デフォルト設定	VDA
クライアントキーボードレイアウト同期およびIMEの改善	無効	1912 LTSR CU2以降にのみ適用されます。
Unicodeキーボードレイアウトマッピングを有効にする	許可 (2407以降); 禁止 (以前のバージョン)	1912 LTSR CU2以降にのみ適用されます。
キーボードレイアウト切り替えポップアップメッセージボックスを非表示にする	禁止	1912 LTSR CU2以降にのみ適用されます。

ICA/ローカルアプリアクセス

名前	デフォルト設定	VDA
ローカルアプリアクセスを許可	禁止	マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
URLリダイレクトブロックリスト	サイトは指定されていません	マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
URLリダイレクト許可リスト	サイトは指定されていません	マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降

ICA/モバイルエクスペリエンス

名前	デフォルト設定	VDA
自動キーボード表示	禁止	VDA 5.6 FP1、マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
タッチ最適化デスクトップの起動	許可	VDA 5.6 FP1、マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降。この設定は無効に

名前	デフォルト設定	VDA
		なっており、Windows 10およびWindows Server 2016マシンでは利用できません。
コンボボックスのリモート処理	禁止	VDA 5.6 FP1、マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降

ICA/マルチメディア

名前	デフォルト設定	VDA
HTML5ビデオリダイレクト	禁止	VDA 7.12から現在まで
ビデオ品質の制限	未構成	マルチセッションOS用VDA 7から現在まで、シングルセッションOS用VDA 7から現在まで
Microsoft Teamsリダイレクト	許可	マルチセッションOS用VDA 1906から現在まで、シングルセッションOS用VDA 1906から現在まで。
マルチメディア会議	許可	すべてのVDAバージョン
WAN経由のWindows Media マルチメディアリダイレクトの最適化	許可	マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
WAN経由のWindows Media マルチメディアリダイレクトの最適化にGPUを使用	禁止	マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
Windows Mediaフォールバックの防止	未構成	VDA 7.6 FP3以降
Windows Mediaクライアント側コンテンツフェッチ	許可	マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降

名前	デフォルト設定	VDA
Windows Mediaリダイレクト	許可	すべてのVDAバージョン
Windows Media リダイレクトバッファーサイズ	5秒	VDA 5、5.5、5.6 FP1から現在まで
Windows Media リダイレクトバッファーサイズの使用	無効	VDA 5、5.5、5.6 FP1から現在まで

ICA/マルチストリーム接続

名前	デフォルト設定	VDA
UDP経由のオーディオ	許可	マルチセッションOS用VDA 7から現在まで
オーディオUDPポート範囲	16500、16509	VDA 5.5、5.6 FP1、マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
マルチポートポリシー	プライマリポート (2598) が高優先度	VDA 5.5、5.6 FP1、マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
マルチストリームコンピューター設定	無効	VDA 5.5、5.6 FP1、マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
マルチストリームユーザー設定	無効	VDA 5.5、5.6 FP1、マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
マルチストリーム仮想チャネルストリーム割り当て設定	デフォルトのストリーム割り当てについては、マルチストリーム仮想チャネル割り当て設定を参照してください	VDA 2003

ICA/ポートリダイレクト

名前	デフォルト設定	VDA
クライアントCOMポートの自動接続	無効	すべてのVDAバージョン。VDA 7.0～7.8の場合、この設定はレジストリを使用して構成します
クライアントLPTポートの自動接続	無効	すべてのVDAバージョン。VDA 7.0～7.8の場合、この設定はレジストリを使用して構成します
クライアントCOMポートのリダイレクト	禁止	すべてのVDAバージョン。VDA 7.0～7.8の場合、この設定はレジストリを使用して構成します
クライアントLPTポートのリダイレクト	禁止	すべてのVDAバージョン。VDA 7.0～7.8の場合、この設定はレジストリを使用して構成します

ICA/印刷

名前	デフォルト設定	VDA
クライアントプリンターリダイレクト	許可	すべてのVDAバージョン
デフォルトプリンター	デフォルトプリンターをクライアントのメインプリンターに設定する	すべてのVDAバージョン
プリンターの割り当て	ユーザーの現在のプリンターがセッションのデフォルトプリンターとして使用されます	すべてのVDAバージョン
プリンター自動作成イベントログの優先設定	エラーと警告をログに記録	すべてのVDAバージョン

名前	デフォルト設定	VDA
セッションプリンター	プリンターは指定されていません	すべてのVDAバージョン
プリンターが作成されるまで待機 (デスクトップ)	無効	すべてのVDAバージョン

ICA/印刷/クライアントプリンター

名前	デフォルト設定	VDA
クライアントプリンターを自動作成	すべてのクライアントプリンターを自動作成	すべてのVDAバージョン
汎用ユニバーサルプリンターを自動作成	無効	すべてのVDAバージョン
クライアントプリンター名	標準プリンター名	VDA 5.6
印刷サーバーへの直接接続	有効	すべてのVDAバージョン
プリンタードライバーのマッピングと互換性	ルールは指定されていません	すべてのVDAバージョン
プリンタープロパティの保持	クライアントに保存されていない場合にのみプロファイルに保持	すべてのVDAバージョン
保持および復元されたクライアントプリンター	許可	VDA 5、5,5、5.6 FP1

ICA/Printing/Drivers

名前	デフォルト設定	VDA
インボックスプリンタードライバーの自動インストール	有効	すべてのVDAバージョン
ユニバーサルドライバーの優先順位	イーエムエフ; エックスピーエス; ピーシーエルファイブ	すべてのVDAバージョン

名前	デフォルト設定	VDA
	シー; ピーシーエルフォー; ピーエス	
ユニバーサルプリントドライバーの使用	要求されたドライバーが利用できない場合にのみユニバーサル印刷を使用する	すべてのVDAバージョン

ICA/印刷/ユニバーサルプリントサーバー

名前	デフォルト設定	VDA
Universal Print Serverの有効化	無効	すべてのVDAバージョン
Universal Print Server印刷データストリーム (CGP) ポート	7229	すべてのVDAバージョン
Universal Print Server印刷ストリーム入力帯域幅制限 (kbps)	0	すべてのVDAバージョン
Universal Print Server Web サービス (HTTP/SOAP) ポート	8080	すべてのVDAバージョン
ロードバランシング用のユニバーサルプリントサーバー	VDAバージョン7.9から現在まで	
ユニバーサルプリントサーバーのサービス停止しきい値	180 (秒)	VDAバージョン7.9から現在まで

ICA/印刷/ユニバーサル印刷

名前	デフォルト設定	VDA
ユニバーサル印刷EMF処理モード	プリンターに直接スプール	すべてのVDAバージョン
ユニバーサル印刷画像圧縮制限	最高品質（ロスレス圧縮）	すべてのVDAバージョン

名前	デフォルト設定	VDA
ユニバーサル印刷の最適化の既定値	画像圧縮: 希望する画質 = 標準品質、ヘビーウェイト圧縮を有効にする = False; 画像とフォントのキャッシュ: 埋め込み画像のキャッシュを許可する = True; 管理者以外のユーザーがこれらの設定を変更することを許可する = False;	すべてのVDAバージョン
ユニバーサル印刷プレビューの優先設定	自動作成されたプリンターまたは汎用ユニバーサルプリンターには印刷プレビューを使用しない	すべてのVDAバージョン
ユニバーサル印刷の印刷品質制限	制限なし	すべてのVDAバージョン

ICA/セキュリティ

名前	既定の設定	VDA
SecureICAの最小暗号化レベル	基本	VDA for マルチセッションOS 7から現在まで

ICA/サーバー制限

名前	デフォルト設定	VDA
サーバーアイドルタイマー間隔	0ミリ秒	VDA for マルチセッションOS 7から現在まで

ICA/セッション制限

名前	デフォルト設定	VDA
切断されたセッションタイマー	無効	VDA 5, 5.5, 5.6 FP1, VDA for シングルセッションOS 7から現在まで

名前	デフォルト設定	VDA
リモートPCアクセス切断セッションタイマー	無効	シングルセッションOS用VDA 7以降
切断セッションタイマー間隔	1,440分	VDA 5、5.5、5.6 FP1、シングルセッションOS用VDA 7以降
セッション接続タイマー	無効	VDA 5、5.5、5.6 FP1、シングルセッションOS用VDA 7以降
セッション接続タイマー間隔	1,440分	VDA 5、5.5、5.6 FP1、シングルセッションOS用VDA 7以降
セッションアイドルタイマー	有効	VDA 5、5.5、5.6 FP1、シングルセッションOS用VDA 7以降
セッションアイドルタイマー間隔	1,440分	VDA 5、5.5、5.6 FP1、シングルセッションOS用VDA 7以降

ICA/セッションの信頼性

名前	デフォルト設定	VDA
セッションの信頼性接続	許可	すべてのVDAバージョン
セッションの信頼性ポート番号	2598	すべてのVDAバージョン
セッションの信頼性タイムアウト	180秒	すべてのVDAバージョン

ICA/タイムゾーン制御

名前	デフォルト設定	VDA
レガシークライアントのローカル時間を推定する	有効	マルチセッションOS 7以降のVDA
セッション切断またはログオフ時にシングルセッションOSのタイムゾーンを復元する	有効	現在のVDAバージョン
クライアントのローカル時間を使用する	サーバーのタイムゾーンを使用する	すべてのVDAバージョン

ICA/TWAINデバイス

名前	デフォルト設定	VDA
クライアントTWAINデバイスリダイレクト	許可	VDA 5.5、5.6 FP1、マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
TWAIN圧縮レベル	中	VDA 5.5、5.6 FP1、マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降

ICA/USBデバイス

名前	デフォルト設定	VDA
クライアントUSBデバイス最適化規則	有効 (VDA 7.6 FP3以降); 無効 (VDA 7.11以降); デフォルトでは、規則は指定されていません	VDA 7.6 FP3 以降
クライアントUSBデバイスリダイレクト	禁止	すべてのVDAバージョン

名前	デフォルト設定	VDA
クライアントUSBデバイスリダイレクト規則	規則は指定されていません	すべてのVDAバージョン
クライアントUSBプラグアンドプレイデバイスリダイレクト	許可	マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降

ICA/視覚表示

名前	デフォルト設定	VDA
単純なグラフィックの優先色深度	24ビット/ピクセル	VDA 7.6 FP3 以降
ターゲットフレームレート	30 フレーム/秒	すべてのVDAバージョン
画質	中	マルチセッションOS 用 VDA 7 以降、シングルセッションOS 用 VDA 7 以降

ICA/ビジュアルディスプレイ/動画

名前	デフォルト設定	VDA
最小画像品質	標準	VDA 5.5、5.6 FP1、マルチセッションOS用VDA 7から現在まで、シングルセッションOS用VDA 7から現在まで
動画圧縮	有効	VDA 5.5、5.6 FP1、マルチセッションOS向けVDA 7 以降、シングルセッションOS向けVDA 7 以降
プログレッシブ圧縮レベル	なし	VDA 5.5、5.6 FP1、マルチセッションOS向けVDA 7 以降、シングルセッションOS向けVDA 7 以降

名前	デフォルト設定	VDA
プログレッシブ圧縮しきい値	2,147,483,647 キロビット/秒	VDA 5.5、5.6 FP1、マルチセッションOS用VDA 7 以降、シングルセッションOS用VDA 7 以降
ターゲット最小フレームレート	10 フレーム/秒	VDA 5.5、5.6 FP1、マルチセッションOS用VDA 7 以降、シングルセッションOS用VDA 7 以降

注:

ターゲット最小フレームレートポリシーは非推奨になりました。

ICA/視覚表示/静止画像

名前	デフォルト設定	VDA
追加のカラー圧縮	無効	すべてのVDAバージョン
追加のカラー圧縮しきい値	8,192 キロビット毎秒	すべてのVDAバージョン
高負荷圧縮	無効	すべてのVDAバージョン
非可逆圧縮レベル	中	すべてのVDAバージョン
非可逆圧縮しきい値	2,147,483,647 ケービーピーエス	すべてのVDAバージョン

ICA/WebSockets

名前	デフォルト設定	VDA
WebSockets接続	禁止	マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降

名前	デフォルト設定	VDA
WebSocketsポート番号	8008	マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
WebSockets信頼済みオリジンサーバーリスト	ワイルドカード「*」は、すべてのReceiver for Web URLを信頼するために使用されます	マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降

負荷管理

名前	デフォルト設定	VDA
同時ログオン許容数	2	マルチセッションOS用VDA 7以降
CPU使用率	無効	マルチセッションOS用VDA 7以降
CPU使用率から除外されるプロセスの優先度	標準以下または低	マルチセッションOS用VDA 7以降
ディスク使用率	無効	マルチセッションOS用VDA 7以降
セッションの最大数	250	マルチセッションOS用VDA 7以降
メモリ使用量	無効	マルチセッションOS用VDA 7以降
メモリ使用量のベースロード	ゼロロード: 768 MB	マルチセッションOS用VDA 7以降

プロファイル管理/詳細設定

名前	デフォルト設定	VDA
自動構成を無効にする	無効	すべてのVDAバージョン

名前	デフォルト設定	VDA
問題が発生した場合にユーザーをログオフする	無効	すべてのVDAバージョン
ロックされたファイルへのアクセス時の再試行回数	5	すべてのVDAバージョン
ログオフ時にインターネットCookieファイルを処理する	無効	すべてのVDAバージョン

プロファイル管理/基本設定

名前	デフォルト設定	VDA
アクティブライトバック	無効	すべてのVDAバージョン
Profile Management を有効にする	無効	すべてのVDAバージョン
除外されるグループ	無効。すべてのユーザーグループのメンバーが処理されます。	すべてのVDAバージョン
オフラインプロファイルのサポート	無効	すべてのVDAバージョン
ユーザーストアへのパス	ウィンドウズ	すべてのVDAバージョン
ローカル管理者によるログオンの処理	無効	すべてのVDAバージョン
処理されるグループ	無効。すべてのユーザーグループのメンバーが処理されます。	すべてのVDAバージョン

プロファイル管理/クロスプラットフォーム設定

名前	デフォルト設定	VDA
クロスプラットフォーム設定ユーザーグループ	無効。処理済みグループで指定されたすべてのユーザーグループが処理されます	すべてのVDAバージョン
クロスプラットフォーム設定を有効にする	無効	すべてのVDAバージョン
クロスプラットフォーム定義へのパス	無効。パスは指定されていません。	すべてのVDAバージョン
クロスプラットフォーム設定ストアへのパス	無効。Windows\PM_CMが使用されます。	すべてのVDAバージョン
クロスプラットフォーム設定の作成元	無効	すべてのVDAバージョン

プロファイル管理/ファイルシステム/除外

名前	デフォルト設定	VDA
除外リスト - ディレクトリ	無効。ユーザープロファイル内のすべてのフォルダーが同期されます。	すべてのVDAバージョン
除外リスト - ファイル	無効。ユーザープロファイル内のすべてのファイルが同期されます。	すべてのVDAバージョン

プロファイル管理/ファイルシステム/同期

名前	デフォルト設定	VDA
同期するディレクトリ	無効。除外されていないフォルダーのみが同期されます。	すべてのVDAバージョン
同期するファイル	無効。除外されていないファイルのみが同期されます。	すべてのVDAバージョン

名前	デフォルト設定	VDA
ミラーリングするフォルダー	無効。フォルダーはミラーリングされません。	すべてのVDAバージョン

プロファイル管理/フォルダーリダイレクト

名前	デフォルト設定	VDA
管理者アクセスを許可する	無効	すべてのVDAバージョン
ドメイン名を含める	無効	すべてのVDAバージョン

プロファイル管理/フォルダーリダイレクト/AppData(Roaming)

名前	デフォルト設定	VDA
AppData(Roaming)パス	無効。場所は指定されていません。	すべてのVDAバージョン
AppData(Roaming)のリダイレクト設定	コンテンツは、AppData(Roaming)パスのポリシー設定で指定されたUNCパスにリダイレクトされます	すべてのVDAバージョン

プロファイル管理/フォルダーリダイレクト/連絡先

名前	デフォルト設定	VDA
連絡先パス	無効。場所は指定されていません。	すべてのVDAバージョン
連絡先のリダイレクト設定	コンテンツは、**連絡先パスポリシー**設定で指定されたUNCパスにリダイレクトされます。	すべてのVDAバージョン

プロファイル管理/フォルダーリダイレクト/デスクトップ

名前	デフォルト設定	VDA
デスクトップパス	無効。場所は指定されていません。	すべてのVDAバージョン
デスクトップのリダイレクト設定	コンテンツは、**デスクトップパスポリシー**設定で指定されたUNCパスにリダイレクトされます。	すべてのVDAバージョン

プロファイル管理/フォルダーリダイレクト/ドキュメント

名前	デフォルト設定	VDA
ドキュメントパス	無効。場所は指定されていません。	すべてのVDAバージョン
ドキュメントのリダイレクト設定	コンテンツは、**ドキュメントパスポリシー**設定で指定されたUNCパスにリダイレクトされます	すべてのVDAバージョン

プロファイル管理/フォルダーリダイレクト/ダウンロード

名前	デフォルト設定	VDA
ダウンロードパス	無効。場所は指定されていません。	すべてのVDAバージョン
ダウンロードのリダイレクト設定	コンテンツは、**ダウンロードパスポリシー**設定で指定されたUNCパスにリダイレクトされます	すべてのVDAバージョン

プロファイル管理/フォルダーリダイレクト/お気に入り

名前	デフォルト設定	VDA
お気に入りパス	無効。場所は指定されていません。	すべてのVDAバージョン

名前	デフォルト設定	VDA
お気に入りのリダイレクト設定	コンテンツは、**お気に入りパスポリシー**設定で指定されたUNCパスにリダイレクトされます	すべてのVDAバージョン

プロファイル管理/フォルダーリダイレクト/リンク

名前	デフォルト設定	VDA
リンクパス	無効。場所は指定されていません。	すべてのVDAバージョン
リンクのリダイレクト設定	コンテンツは、**リンクパスポリシー**設定で指定されたUNCパスにリダイレクトされます	すべてのVDAバージョン

プロファイル管理/フォルダーリダイレクト/ミュージック

名前	デフォルト設定	VDA
ミュージックパス	無効。場所は指定されていません。	すべてのVDAバージョン
ミュージックのリダイレクト設定	コンテンツは、「**ミュージックパスポリシー**」設定で指定されたUNCパスにリダイレクトされます	すべてのVDAバージョン

プロファイル管理/フォルダーリダイレクト/ピクチャ

名前	デフォルト設定	VDA
ピクチャパス	無効。場所は指定されていません。	すべてのVDAバージョン
ピクチャのリダイレクト設定	コンテンツは、「**ピクチャパスポリシー**」設定で指定されたUNCパスにリダイレクトされます	すべてのVDAバージョン

プロファイル管理/フォルダーリダイレクト/保存されたゲーム

名前	デフォルト設定	VDA
保存されたゲームのパス	無効。場所は指定されていません。	すべてのVDAバージョン
保存されたゲームのリダイレクト設定	コンテンツは、**保存されたゲームのパス ポリシー**設定で指定されたUNCパスにリダイレクトされます	すべてのVDAバージョン

プロファイル管理/フォルダーリダイレクト/検索

名前	デフォルト設定	VDA
検索パス	無効。場所は指定されていません。	すべてのVDAバージョン
検索のリダイレクト設定	コンテンツは、**検索パスポリシー**設定で指定されたUNCパスにリダイレクトされます。	すべてのVDAバージョン

プロファイル管理/フォルダーリダイレクト/スタートメニュー

名前	デフォルト設定	VDA
スタートメニューパス	無効。場所は指定されていません。	すべてのVDAバージョン
スタートメニューのリダイレクト設定	コンテンツは、スタートメニューパスポリシー設定で指定されたUNCパスにリダイレクトされます。	すべてのVDAバージョン

プロファイル管理/フォルダーリダイレクト/ビデオ

名前	デフォルト設定	VDA
ビデオパス	無効。場所は指定されていません。	すべてのVDAバージョン

名前	デフォルト設定	VDA
ビデオのリダイレクト設定	コンテンツは、**ビデオパスポリシー**設定で指定されたUNCパスにリダイレクトされます。	すべてのVDAバージョン

プロファイル管理/ログ設定

名前	デフォルト設定	VDA
Active Directory のアクション	無効	すべてのVDAバージョン
一般情報	無効	すべてのVDAバージョン
一般的な警告	無効	すべてのVDAバージョン
ログの有効化	無効	すべてのVDAバージョン
ファイルシステムのアクション	無効	すべてのVDAバージョン
ファイルシステム通知	無効	すべてのVDAバージョン
ログオフ	無効	すべてのVDAバージョン
ログオン	無効	すべてのVDAバージョン
ログファイルの最大サイズ	1048576	すべてのVDAバージョン
ログファイルへのパス	無効。ログファイルはデフォルトの場所 (%SystemRoot%\System32\Logfiles\UserProfileManager) に保存されます。	すべてのVDAバージョン
パーソナライズされたユーザー情報	無効	すべてのVDAバージョン
ログオン時とログオフ時のポリシー値	無効	すべてのVDAバージョン
レジストリアクション	無効	すべてのVDAバージョン

名前	デフォルト設定	VDA
ログオフ時のレジストリの相違点	無効	すべてのVDAバージョン

プロファイル管理/プロファイルの処理

名前	デフォルト設定	VDA
キャッシュされたプロファイルを削除するまでの遅延	0	すべてのVDAバージョン
ログオフ時にローカルにキャッシュされたプロファイルを削除する	無効	すべてのVDAバージョン
ローカルプロファイルの競合処理	ローカルプロファイルを使用する	すべてのVDAバージョン
既存プロファイルの移行	ローカルとローミング	すべてのVDAバージョン
テンプレートプロファイルへのパス	無効。新しいユーザープロファイルは、ユーザーが最初にログオンしたデバイスのデフォルトユーザープロファイルから作成されます。	すべてのVDAバージョン
テンプレートプロファイルがローカルプロファイルを上書きする	無効	すべてのVDAバージョン
テンプレートプロファイルが移動プロファイルを上書きする	無効	すべてのVDAバージョン
すべてのログオンでCitrix®必須プロファイルとして使用されるテンプレートプロファイル	無効	すべてのVDAバージョン

プロファイル管理/レジストリ

名前	デフォルト設定	VDA
除外リスト	無効。ユーザーがログオフすると、HKCUハイブ内のすべてのレジストリキーが処理されます。	すべてのVDAバージョン
包含リスト	無効。ユーザーがログオフすると、HKCUハイブ内のすべてのレジストリキーが処理されます。	すべてのVDAバージョン

プロファイル管理/ストリーム配信ユーザープロファイル

名前	デフォルト設定	VDA
常にキャッシュ	無効	すべてのVDAバージョン
常にキャッシュサイズ	0 MB	すべてのVDAバージョン
プロファイルストリーミング	無効	すべてのVDAバージョン
ストリーミングされたユーザープロファイルグループ	無効。OU内のすべてのユーザープロファイルは通常どおり処理されます。	すべてのVDAバージョン
保留中のエリアロックファイルのタイムアウト (日数)	1日	すべてのVDAバージョン

レシーバー

名前	デフォルト設定	VDA
StoreFront™アカウントリスト	ストアは指定されていません	マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降

ユーザーパーソナライゼーションレイヤー

名前	デフォルト設定	VDA
ユーザーレイヤーリポジトリパス	無効。パスは指定されていません。	VDA 19.12以降のバージョン
ユーザーレイヤーサイズ（GB）	10 GB。ユーザーレイヤーは、設定されたサイズまで拡張するシンプロビジョニングディスクです。ユーザーレイヤーのサイズが小さくなることはありません。	VDA 19.12以降のバージョン

バーチャル デリバリー エージェント

名前	デフォルト設定	VDA
コントローラー登録IPv6ネットマスク	ネットマスクは指定されていません	マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
コントローラー登録ポート	80	すべてのVDAバージョン
コントローラーSID	SIDは指定されていません	すべてのVDAバージョン
コントローラー	コントローラーは指定されていません	すべてのVDAバージョン
コントローラーの自動更新を有効にする	有効	マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
IPv6コントローラー登録のみを使用する	無効	マルチセッションOS用VDA 7以降、シングルセッションOS用VDA 7以降
サイトGUID	GUIDは指定されていません	すべてのVDAバージョン

仮想配信エージェント/HDX 3D Pro

名前	デフォルト設定	VDA
ロスレスを有効にする	有効	VDA 5.5、5.6 FP1
HDX 3D Pro品質設定	VDA 5.5、5.6 FP1	

仮想配信エージェント/監視

名前	デフォルト設定	VDA
プロセス監視を有効にする	無効	VDA 7.11以降
リソース監視を有効にする	有効	VDA 7.11以降

仮想IP

名前	デフォルト設定	VDA
仮想IPループバックサポート	無効	VDA 7.6から現在まで
Virtual IP仮想ループバックプログラム一覧	なし	VDA 7.6から現在まで

ポリシー設定リファレンス

ポリシーには、ポリシーが適用されるときに適用される設定が含まれます。このセクションの説明では、機能を有効にするためにより多くの設定が必要かどうか、または設定に類似しているかどうかも示されています。

クイックリファレンス

以下の表は、ポリシー内で構成できる設定を一覧表示しています。左側の列で完了したいタスクを見つけ、右側の列で対応する設定を見つけてください。

すべてのポリシー設定の完全なリストは、.CHM (コンパイル済みHTML) 形式および .CSV 形式で利用できます。これらのファイルは、ブローカー (デリバリーコントローラー) がインストールされているサーバーの `\program files\citrix\grouppolicy` フォルダーにあります。ポリシー設定の最新バージョンは、こちら をクリックしてダウンロードすることもできます。

オーディオ

このタスクの場合	使用するポリシー設定
複数のオーディオデバイスの使用を許可するかどうかを制御します	オーディオプラグアンドプレイ
ユーザーデバイスのマイクからのオーディオ入力を許可するかどうかを制御します	クライアントマイクのリダイレクト
ユーザーデバイスのオーディオ品質を制御します	オーディオ品質
ユーザーデバイスのスピーカーへのオーディオマッピングを制御します	クライアントオーディオリダイレクト

ユーザーデバイスの帯域幅

使用される帯域幅を制限するには	このポリシー設定を使用します
クライアントオーディオマッピング	オーディオリダイレクト帯域幅制限またはオーディオリダイレクト帯域幅制限パーセント
ローカルクリップボードを使用した切り取りと貼り付け	クリップボードリダイレクト帯域幅制限またはクリップボードリダイレクト帯域幅制限パーセント
セッションでのローカルクライアントドライブへのアクセス	ファイルリダイレクト帯域幅制限またはファイルリダイレクト帯域幅制限パーセント
HDX™ MediaStream マルチメディアアクセラレーション	HDX MediaStream マルチメディアアクセラレーション帯域幅制限またはHDX MediaStream マルチメディアアクセラレーション帯域幅制限パーセント
クライアントセッション	セッション全体の帯域幅制限
印刷	プリンターリダイレクト帯域幅制限またはプリンターリダイレクト帯域幅制限率
TWAINデバイス（カメラやスキャナーなど）	TWAINデバイスリダイレクト帯域幅制限またはTWAINデバイスリダイレクト帯域幅制限率

使用される帯域幅を制限するには	このポリシー設定を使用します
USBデバイス	クライアントUSBデバイスリダイレクト帯域幅制限またはクライアントUSBデバイスリダイレクト帯域幅制限率

クライアントドライブとユーザーデバイスのリダイレクト

このタスクの場合	このポリシー設定を使用します
ユーザーがサーバーにログオンするときに、ユーザーデバイス上のドライブが接続されるかどうかを制御します	クライアントドライブの自動接続
サーバーとローカルクリップボード間の切り取りと貼り付けによるデータ転送を制御します	クライアントクリップボードリダイレクト
ユーザーデバイスからドライブがどのようにマップされるかを制御します	クライアントドライブリダイレクト
ユーザーのローカルハードドライブがセッション内で利用可能かどうかを制御します	クライアント固定ドライブとクライアントドライブのリダイレクト
ユーザーのローカルフロッピードライブがセッションで利用可能かどうかを制御します	クライアントフロッピードライブとクライアントドライブのリダイレクト
ユーザーのネットワークドライブがセッションで利用可能かどうかを制御します	クライアントネットワークドライブとクライアントドライブのリダイレクト
ユーザーのローカルCD、DVD、またはBlu-rayドライブがセッションで利用可能かどうかを制御します	クライアント光学ドライブとクライアントドライブのリダイレクト
ユーザーのローカルリムーバブルドライブがセッションで利用可能かどうかを制御します	クライアントリムーバブルドライブとクライアントドライブのリダイレクト
ユーザーのTWAINデバイス（スキャナーやカメラなど）がセッションで利用可能かどうかを制御し、画像データ転送の圧縮を制御します	クライアントTWAINデバイスのリダイレクト。TWAIN圧縮のリダイレクト

このタスクの場合	このポリシー設定を使用します
USBデバイスがセッションで利用可能かどうかを制御します	クライアントUSBデバイスのリダイレクトとクライアントUSBデバイスのリダイレクト規則
WAN経由でクライアントディスクへのファイルの書き込みとコピーの速度を向上させます	非同期書き込みを使用する

コンテンツリダイレクト

このタスクの場合	このポリシー設定を使用する
サーバーからユーザーデバイスへのコンテンツリダイレクトを使用するかどうかを制御します	ホストからクライアントへのリダイレクト

デスクトップUI

このタスクの場合	このポリシー設定を使用する
ユーザーセッションでデスクトップの壁紙を使用するかどうかを制御します	デスクトップの壁紙
ウィンドウのドラッグ中にウィンドウの内容を表示する	ドラッグ中のウィンドウの内容を表示する

グラフィックとマルチメディア

重要:

Flashポリシーは、古いVDAを使用している顧客が新しいコントローラー（たとえば、バージョン1912コントローラー）を使用し、引き続きFlashを使用できるようにするためにのみ残されています。このVDAバージョンはFlashをサポートしていません。

このタスクの場合	このポリシー設定を使用します
仮想デスクトップからユーザーデバイスに送信される1秒あたりの最大フレーム数を制御します	ターゲットフレームレート
ユーザーデバイスに表示される画像の視覚品質を制御します	視覚品質
セッションでアクセスされたときにWebサイトがFlashコンテンツを表示できるかどうかを制御します	Flashサーバー側コンテンツ取得URLリスト。Flash URL互換性リスト。Flashビデオフォールバック防止ポリシー設定。Flashビデオフォールバック防止エラー*.swf
サーバーレンダリングされたビデオの圧縮を制御します	圧縮にビデオコーデックを使用。ビデオコーデックにハードウェアエンコードを使用
ユーザーへのHTML5マルチメディアWebコンテンツの配信を制御します	HTML5ビデオリダイレクト

マルチストリームネットワークトラフィックの優先順位付け

このタスクの場合	このポリシー設定を使用
複数の接続にわたるICA®トラフィックのポートを指定し、ネットワークの優先順位を確立します	マルチポートポリシー
サーバーとユーザーデバイス間のマルチストリーム接続のサポートを有効にします	マルチストリーム（コンピューターおよびユーザー設定）

印刷

このタスクの場合	このポリシー設定を使用
ユーザーデバイスでのクライアントプリンターの作成を制御します	クライアントプリンターの自動作成とクライアントプリンターのリダイレクト
プリンタープロパティの保存場所を制御します	プリンタープロパティの保持

このタスクの場合	このポリシー設定を使用
クライアントまたはサーバーのどちらが印刷要求を処理するかを制御します	印刷サーバーへの直接接続
ユーザーが自分のユーザーデバイスに接続されているプリンターにアクセスできるかどうかを制御します	クライアントプリンターのリダイレクト
クライアントおよびネットワークプリンターを自動的に作成する際のネイティブWindowsドライバーのインストールを制御する	インボックスプリンタードライバーの自動インストール
ユニバーサルプリンタードライバーを使用するタイミングを制御する	ユニバーサルプリントドライバーの使用状況
ローミングユーザーセッション情報に基づいてプリンターを選択する	デフォルトプリンター
ユニバーサルプリントサーバーの負荷分散とフェイルオーバーしきい値の設定	負荷分散のためのユニバーサルプリントサーバー。ユニバーサルプリントサーバーのサービス停止しきい値

注：

ポリシーを使用して、デスクトップまたはアプリケーションセッションでスクリーンセーバーを有効にすることはできません。スクリーンセーバーを必要とするユーザーの場合、スクリーンセーバーはユーザーデバイス上で実装できます。

ICA®ポリシー設定

注:

このページでは、ICAポリシー設定の説明とサポートされている構成値について説明します。ポリシーの操作の詳細については、「ポリシーの操作」セクションを参照してください。

アダプティブトランスポート

この設定により、EDTをプライマリ、TCPをフォールバックとしてデータ転送を許可または禁止します。

デフォルトでは、アダプティブトランスポートは有効（**優先**）になっており、可能な場合はEDTが使用され、TCPにフォールバックします。必要に応じて設定を変更できます。

- **優先**。可能な場合はEDT経由のアダプティブトランスポートが使用され、TCPにフォールバックします。
- **診断モード**。EDTが強制的に有効になり、TCPへのフォールバックは無効になります。この設定はトラブルシューティングのみに推奨されます。
- **オフ**。TCPが強制的に有効になり、EDTは無効になります。

詳細については、「アダプティブトランスポート」を参照してください。

ドラッグアンドドロップ設定

この設定により、クライアントと仮想アプリケーションまたはデスクトップの間でのファイルのドラッグを許可または禁止します。デフォルトでは、ドラッグアンドドロップポリシーは無効になっています。必要に応じてこのポリシーを有効にできます。

アプリケーション起動待機タイムアウト

この設定は、セッションが最初のアプリケーションの起動を待機するミリ秒単位の待機タイムアウト値を指定します。アプリケーションの起動がこの期間を超えると、セッションは終了します。

デフォルトの時間（10,000ミリ秒）を選択するか、ミリ秒単位で数値を指定できます。

クライアントクリップボードリダイレクト

この設定により、ユーザーデバイス上のクリップボードをサーバー上のクリップボードにマッピングすることを許可または禁止します。

デフォルトでは、クリップボードのリダイレクトは許可されています。

セッションとローカルクリップボード間のコピー＆ペーストデータ転送を禁止するには、**禁止**を選択します。ユーザーは、セッション内で実行されているアプリケーション間では引き続きデータをコピー＆ペーストできます。

この設定を許可した後、クライアント接続でクリップボードが消費できる最大帯域幅を構成します。**クリップボードリダイレクト帯域幅制限**または**クリップボードリダイレクト帯域幅制限（パーセント）**の設定を使用します。

クライアントクリップボード書き込み許可形式

クライアントクリップボード書き込みの制限設定が**有効**の場合、ホストクリップボードデータはクライアントエンドポイントと共有できません。この設定を使用すると、特定のデータ形式をクライアントエンドポイントクリップボードと共有できます。この設定を使用するには、有効にして、許可する特定の形式を追加します。

以下のクリップボード形式はシステム定義です。

- CF_TEXT
- CF_BITMAP
- CF_METAFILEPICT
- CF_SYLK
- CF_DIF
- CF_TIFF
- CF_OEMTEXT
- CF_DIB
- CF_PALETTE
- CF_PENDATA
- CF_RIFF
- CF_WAVE
- CF_UNICODETEXT
- CF_ENHMETAFILE
- CF_HDROP
- CF_LOCALE
- CF_DIBV5
- CF_OWNERDISPLAY
- CF_DSPTEXT
- CF_DSPBITMAP
- CF_DSPMETAFILEPICT
- CF_DISPENHMETAFILE
- CF_HTML

XenApp and XenDesktopおよびCitrix Virtual Apps and Desktops™には、以下のカスタム形式が事前定義されています:

- CFX_RICHTEXT
- CFX_OfficeDrawingShape
- CFX_BIFF8
- CFX_FILE

HTML形式はデフォルトで無効になっています。この機能を有効にするには:

- **クライアントクリップボードリダイレクト**が**許可**に設定されていることを確認します。
- **クライアントクリップボード書き込みの制限**が**有効**に設定されていることを確認します。
- **CF_HTML**（およびサポートしたいその他の形式）のエントリを**クライアントクリップボード書き込み許可形式**に追加します。

さらにカスタム形式を追加できます。カスタム形式名は、システムに登録される形式と一致している必要があります。形式名は大文字と小文字を区別します。

クライアントクリップボードリダイレクトポリシーが**禁止**に設定されている場合、または**クライアントクリップボード書き込みの制限**ポリシーが**無効**に設定されている場合、この設定は適用されません。

> **注:**
>
> HTML形式のクリップボードコピーサポート（CF_HTML）を有効にすると、コピーされたコンテンツのソースから宛先にスクリプトがコピーされます。コピーを進める前に、ソースを信頼していることを確認してください。スクリプトを含むコンテンツをコピーした場合、それらは宛先ファイルをHTMLファイルとして保存し、実行した場合にのみ有効になります。

クリップボードクライアントからセッションへの転送サイズを制限する

この設定は、ユーザーが単一のコピー＆ペースト操作中にクライアントエンドポイントから仮想セッションに転送できるクリップボードデータの最大サイズを指定します。

クリップボードの転送サイズを制限するには、**クリップボードのクライアントからセッションへの転送サイズを制限する**設定を有効にします。次に、**サイズ制限**フィールドにキロバイト単位の値を入力して、ローカルクリップボードとセッション間のデータ転送サイズを定義します。

既定では、この設定は無効になっており、クライアントからセッションへの転送に制限はありません。

HDX™ ダイレクト

HDX Directを使用すると、直接通信が可能な場合に、クライアントがセッションホストとの直接接続を自動的に確立できます。接続は、ネットワークレベルの暗号化を使用して安全に確立されます。

HDX Direct モード

HDX Direct は、内部クライアントと外部クライアントの両方でセッションホストとの直接接続を確立するために使用できます。この設定は、HDX Direct が内部クライアントのみに利用可能か、内部クライアントと外部クライアントの両方に利用可能かを決定します。

内部のみに設定されている場合、HDX Direct は内部ネットワーク内のクライアントに対してのみ直接接続を確立しようとします。

Internal および **external** に設定されている場合、HDX Directは内部クライアントと外部クライアントの両方に対して直接接続を確立しようとします。

既定では、HDX Direct は内部クライアントのみに設定されています。

HDX Direct ポート範囲

外部ユーザーからの接続に HDX Direct が使用するポートの範囲です。 既定では、HDX Direct はポート範囲 55000～55250 を使用します。

クリップボードのセッションからクライアントへの転送サイズを制限する

この設定は、ユーザーが単一のコピー＆ペースト操作中に仮想セッションからクライアントエンドポイントに転送できるクリップボードデータの最大サイズを指定します。

クリップボードの転送サイズを制限するには、**クリップボードのセッションからクライアントへの転送サイズを制限する**設定を有効にします。次に、**サイズ制限**フィールドにキロバイト単位の値を入力して、セッションとローカルクリップボード間のデータ転送サイズを定義します。

既定では、この設定は無効になっており、セッションからクライアントへの転送に制限はありません。

クライアントクリップボード書き込みの制限

この設定が**有効**になっている場合、ホストクリップボードデータはクライアントエンドポイントと共有できません。**クライアントクリップボード書き込み許可形式**設定を有効にすることで、特定の形式を許可できます。

デフォルトでは、この設定は**無効**です。

セッションクリップボード書き込みの制限

この設定が**有効**になっている場合、クライアントクリップボードデータはセッションアプリケーションと共有できません。**セッションクリップボード書き込み許可形式**設定を有効にすることで、特定の形式を許可できます。

デフォルトでは、この設定は**無効**です。

セッションクリップボード書き込み許可形式

セッションクリップボード書き込みの制限設定が**有効**になっている場合、クライアントクリップボードデータはセッションアプリケーションと共有できません。この設定を使用して、特定のデータ形式をセッションクリップボードと共有することを許可できます。

以下のクリップボード形式はシステム定義です。

- CF_TEXT
- CF_BITMAP
- CF_METAFILEPICT
- CF_SYLK
- CF_DIF
- CF_TIFF
- CF_OEMTEXT
- CF_DIB
- CF_PALETTE
- CF_PENDATA
- CF_RIFF
- CF_WAVE
- CF_UNICODETEXT
- CF_ENHMETAFILE
- CF_HDROP
- CF_LOCALE
- CF_DIBV5
- CF_OWNERDISPLAY

- CF_DSPTEXT
- CF_DSPBITMAP
- CF_DSPMETAFILEPICT
- CF_DISPENHMETAFILE
- CF_HTML

XenApp and XenDesktopおよびCitrix Virtual Apps and Desktopsでは、以下のカスタム形式が事前定義されています。

- CFX_RICHTEXT
- CFX_OfficeDrawingShape
- CFX_BIFF8

HTML形式はデフォルトで無効になっています。この機能を有効にするには：

- **クライアントクリップボードリダイレクト**が**許可**に設定されていることを確認します。
- **セッションクリップボード書き込みの制限**が**有効**に設定されていることを確認します。
- **セッションクリップボード書き込み許可形式**に**CF_HTML**（およびサポートしたいその他の形式）のエントリを追加します。

カスタム形式をさらに追加できます。カスタム形式名は、システムに登録される形式と一致している必要があります。形式名は大文字と小文字を区別します。

この設定は、**クライアントクリップボードリダイレクト**ポリシーが**禁止**に設定されている場合、または**セッションクリップボード書き込みの制限**ポリシーが**無効**に設定されている場合には適用されません。

> **注:**
>
> HTML形式のクリップボードコピーサポート（CF_HTML）を有効にすると、コピーされたコンテンツのソースから宛先にスクリプトがコピーされます。コピーを続行する前に、ソースを信頼できることを確認してください。スクリプトを含むコンテンツをコピーした場合、それらは宛先ファイルをHTMLファイルとして保存して実行した場合にのみ有効になります。

デスクトップの起動

この設定は、VDA Direct Access Usersグループの非管理者ユーザーによる、ICA接続を使用したVDA上のセッションへの接続を許可または禁止します。

デフォルトでは、非管理者ユーザーはこれらのセッションに接続できません。

この設定は、RDP接続を使用しているVDA Direct Access Usersグループの非管理者ユーザーには影響しません。これらのユーザーは、この設定が有効または無効になっている場合でもVDAに接続できます。この設定は、VDA Direct Access Usersグループに属していない非管理者ユーザーには影響しません。これらのユーザーは、この設定が有効または無効になっている場合でもVDAに接続できません。

FIDO2リダイレクト

この設定は、FIDO2リダイレクトを有効または無効にします。FIDO2リダイレクトにより、ユーザーは仮想マシン内のローカルエンドポイントFIDO2コンポーネントを利用できます。ユーザーは、TPM 2.0およびWindows Helloを搭載したデバイスで、FIDO2セキュリティキーまたは統合生体認証を介して仮想セッションを認証できます。

この設定が**許可**されている場合、ユーザーはローカルエンドポイント機能を使用してFIDO2認証を行うことができます。デフォルトでは、この設定は**許可**されています。

ICAリスナー接続タイムアウト

この設定は、ICAプロトコルを使用した接続が完了するまでの最大待機時間を指定します。

デフォルトでは、最大待機時間は120,000ミリ秒、つまり2分です。

ICAリスナーポート番号

この設定は、サーバー上のICAプロトコルで使用されるTCP/IPポート番号を指定します。

デフォルトでは、ポート番号は1494に設定されています。

有効なポート番号は0～65535の範囲内である必要があり、他のよく知られているポート番号と競合してはなりません。ポート番号を変更した場合は、新しい値を有効にするためにサーバーを再起動してください。サーバーのポート番号を変更した場合は、サーバーに接続するすべてのCitrix Workspace™アプリまたはプラグインでも変更する必要があります。

キーボードと入力方式エディター (IME)

この設定は、次の項目を有効または無効にします。

- 動的キーボードレイアウト同期
- 入力方式エディター (IME)
- Unicode キーボードレイアウトマッピング
- キーボードレイアウト切り替え通知ダイアログメッセージを非表示または表示します

1. Web Studio で、**キーボードとIME**を選択します。
2. VDA での動的キーボードレイアウト同期と汎用クライアント入力方式エディター (IME) 機能を制御するには、**クライアントキーボードレイアウト同期とIMEの改善**を選択します。以下を構成できます。

   無効 - 動的なキーボードレイアウト同期と汎用クライアント入力方式エディター (IME)。

   動的なクライアントキーボードレイアウト同期をサポート - 動的なキーボードレイアウト同期を有効にします。

   動的クライアントキーボードレイアウト同期とIMEの改善をサポート - 動的キーボードレイアウト同期と汎用クライアント入力方式エディター (IME) の両方を有効にします。
3. Unicode キーボードマッピングを有効または無効にするには、**Unicode キーボードレイアウトマッピングを有効にする**を選択します。
4. ユーザーがクライアントキーボードレイアウトを変更したときに、キーボードレイアウトが同期中であることを示すメッセージを表示するかどうかを制御するには、**キーボードレイアウト切り替えポップアップメッセージボックスを非表示にする**を選択します。メッセージが表示されないようにすると、ユーザーは誤った文字入力にならないように、入力する前に数秒待つ必要があります。

デフォルト設定:

- **クライアントキーボードレイアウト同期とIMEの改善**
  - Windows Server 2016 および Windows Server 2019 では無効。
  - Windows Server 2012およびWindows 2010での動的クライアントキーボードレイアウト同期とIMEの改善をサポートします。
- **Unicodeキーボードレイアウトマッピングを無効にする**
- **キーボードレイアウト切り替えポップアップメッセージボックスを表示する**

このポリシーは、ポリシー設定の**説明**セクションに記載されているレジストリ設定を置き換えます。

ログオフチェッカーの起動遅延

この設定は、ログオフチェッカーの起動を遅延させる期間を指定します。このポリシーを使用して、クライアントセッションがセッションを切断するまでに待機する時間（秒単位）を設定します。

この設定は、ユーザーがサーバーからログオフするのにかかる時間も増加させます。

ロス許容モード

> **重要:**
>
> - この機能には、Windows 用 Citrix Workspace アプリ 2002 以降が必要です。VDA のこのバージョンは、利用可能になった時点でこれをサポートします。
> - グラフィックの損失許容モードは Citrix Gateway および Citrix Gateway Service でサポートされています。このモードは、直接接続でのみ利用可能です。

この設定は、グラフィックのロス許容モードを有効または無効にします。

デフォルトでは、グラフィックのロス許容モードは**許可**されています。

許可されている場合、パケット損失と遅延がしきい値を超えると、このモードに入ります。しきい値は、ロス許容しきい値ポリシーを使用して設定できます。

ロス許容しきい値

損失許容モード が利用可能な場合、この設定は、セッションがグラフィックの損失許容モードに切り替わるネットワークメトリックのしきい値を指定します。

デフォルトのしきい値は次のとおりです。

- パケット損失: 5%
- 遅延: 300 ms (RTT)

詳細については、損失許容モード を参照してください。

オーディオのロストレラントモード

この設定は、オーディオの損失許容モードを有効または無効にします。

有効にすると、オーディオは損失許容モードで送信されます。

デフォルトでは、オーディオの損失許容モードは**禁止**されています。

ポリシーを有効にするには、オーディオポリシーの損失許容モードのレジストリを編集して**許可**に設定します。

オーディオの損失許容モードを有効にするには、EDTトランスポートが必要です。

Rendezvous プロトコル

この設定は、Citrix Gateway Serviceを使用する際のHDXセッションのプロキシ方法を変更します。有効にすると、HDXトラフィックはCitrix Cloud Connectorを経由しなくなります。代わりに、VDAはCitrix Gateway Serviceに直接アウトバウンド接続を確立します（Cloud Connectorのスケーラビリティが向上します）。

> **重要:**
>
> Citrix Cloud™の機能トグルとHDXポリシー設定がこの機能を制御します。Citrix Cloudの機能トグルはデフォルトで有効になっていますが、HDX設定はデフォルトで無効になっています。HDX設定は、Citrix Gateway Serviceを介して確立されたHDXセッションにのみ影響します。この設定は、クライアントとVDA間で直接確立されたセッションや、オンプレミスのCitrix Gatewayを介して確立されたセッションには影響しません。

> 詳細については、Rendezvousプロトコルを参照してください。

Rendezvousプロキシ構成

この設定では、Rendezvous プロトコルで使用する明示的なプロキシを構成できます。トランスペアレントプロキシを使用している場合、この設定を有効にする必要はありません。

デフォルトでは、この設定は無効になっています。

無効にすると、VDA は Gateway Service との Rendezvous 接続を確立しようとするときに、非トランスペアレントプロキシを介して送信トラフィックをルーティングしません。

有効にすると、VDAはこの設定で定義されたプロキシを介してGateway ServiceとのRendezvous接続を確立しようとします。

VDA は、Rendezvous 接続に HTTP および SOCKS5 プロキシの使用をサポートしています。Rendezvous 接続にプロキシを使用するように VDA を構成するには、この設定を有効にする必要があります。また、プロキシのアドレスまたは PAC ファイルへのパスを指定します。例:

- プロキシアドレス: `http://<URL or IP>:<port>` または `socks5://<URL or IP>:<port>`
- PACファイル: `http://<URL or IP>/<path>/<filename>.pac`

  VDAバージョン2103は、PACファイルを使用したプロキシ構成でサポートされる最小バージョンです。SOCKS5プロキシのPACファイルスキーマの詳細については、「プロキシ構成」を参照してください。

> **注:**
>
> SOCKS5プロキシのみがEDTを介したデータ転送をサポートします。HTTPプロキシの場合は、ICAのトランスポートプロトコルとしてTCPを使用してください。

> 詳細については、「Rendezvousプロトコル」を参照してください。

クライアント接続中の非公開プログラムの起動

この設定は、サーバー上の RDP を介して初期アプリケーションの起動を許可するかどうかを指定します。

デフォルトでは、サーバー上でRDPを介して初期アプリケーションの起動は許可されていません。

セッションメトリックの収集

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

オペレーティングシステム、稼働時間、コンピューターシステム情報、ビデオコントローラーの詳細、VDAバージョン、展開タイプ、ドメイン参加ステータスなどのデータがCitrixによって収集されます。さらに、製品改善の取り組みを支援するために、いくつかのセッション構成、パフォーマンスおよび信頼性データも収集できます。カスタマーエクスペリエンス向上プログラムの詳細については、以下を参照してください。

- `<https://more.citrix.com/XD-CEIP>`
- `<https://docs.citrix.com/ja-jp/linux-virtual-delivery-agent/current-release/configure/administration/linux-vda-data-collection-program>`
- `<https://docs.citrix.com/ja-jp/mac-vda/configure/session/supportability-service>`

デフォルトでは、この設定は有効になっています。

タブレットモード切り替えポリシー設定

タブレットモード切り替えは、VDA上のストアアプリ、Win32アプリ、およびWindowsシェルの外観と動作を最適化します。これは、電話やタブレットなどの小型デバイス、または任意のタッチ

対応デバイスから接続する際に、仮想デスクトップを自動的にタブレットモードに切り替えることで実現されます。

このポリシーが無効になっている場合、VDAはユーザーが設定したモードになり、クライアントの種類に関係なく、常に同じモードを維持します。

自動クライアント再接続ポリシー設定

自動クライアント再接続セクションには、セッションの自動再接続を制御するためのポリシー設定が含まれています。

自動クライアント再接続

この設定は、接続が中断された後に同じクライアントによる自動再接続を許可または禁止します。

Citrix Receiver for Windows 4.7以降およびCitrix Workspaceアプリ1808以降では、自動クライアント再接続はCitrix Studioからのポリシー設定のみを使用します。Studioでこれらのポリシーを更新すると、自動クライアント再接続がサーバーからクライアントに同期されます。以前のバージョンのCitrix Receiver for Windowsで自動クライアント再接続を構成するには、Studioポリシーを使用し、レジストリまたはdefault.icaファイルを変更します。

自動クライアント再接続を許可すると、ユーザーは接続が切断されたときに中断された場所から作業を再開できます。自動再接続は、切断された接続を検出し、ユーザーをセッションに再接続します。

セッションIDと資格情報へのキーを含むCitrix Workspace™アプリのCookieが使用されない場合、自動再接続によって新しいセッションが開始される可能性があります。つまり、既存のセッションに再接続するのではなく、新しいセッションが開始されます。Cookieは、有効期限が切れている場合は使用されません。たとえば、再接続の遅延や、資格情報の再入力が必要な場合などにCookieの有効期限が切れることがあります。ユーザーが意図的に切断した場合、自動クライアント再接続はトリガーされません。

再接続が進行中の場合、セッションウィンドウはグレー表示されます。カウントダウンタイマーは、セッションが再接続されるまでの残り時間を表示します。セッションがタイムアウトすると、切断されます。

アプリケーションセッションの場合、自動再接続が許可されていると、通知領域にカウントダウンタイマーが表示されます。このタイマーは、セッションが再接続されるまでの残り時間を指定します。Citrix Workspaceアプリは、再接続が成功するか、ユーザーが再接続の試行をキャンセルするまで、セッションへの再接続を試みます。

ユーザーセッションの場合、自動再接続が許可されていると、Citrix Workspaceアプリは、再接続が成功するか、ユーザーが再接続の試行をキャンセルしない限り、指定された期間セッションへの再接続を試みます。デフォルトでは、この期間は2分です。この期間を変更するには、ポリシーを編集します。

デフォルトでは、自動クライアント再接続は許可されています。ポリシーを**禁止**に設定することで無効にできます。

自動クライアント再接続認証

この設定は、自動クライアント再接続に認証が必要かどうかを指定します。

ユーザーが最初にログオンすると、資格情報は暗号化され、メモリに保存され、暗号化キーを含むCookieが作成されます。このCookieはCitrix Workspaceアプリに送信されます。この設定が構成されている場合、Cookieは使用されません。代わりに、Citrix Workspaceアプリが自動的に再接続を試みるときに、資格情報を要求するダイアログボックスがユーザーに表示されます。

デフォルトでは、認証は不要です。

自動クライアント再接続ログ

この設定は、イベントログへの自動クライアント再接続の記録を有効または無効にします。

ログ記録が有効な場合、サーバーのシステムログは、成功および失敗した自動再接続イベントに関する情報をキャプチャします。サイトは、すべてのサーバーの再接続イベントの統合ログを提供しません。

デフォルトでは、ログ記録は無効です。

自動クライアント再接続タイムアウト

デフォルトでは、自動クライアント再接続タイムアウトは120秒に設定されており、自動クライアント再接続タイムアウトの最大設定可能値は300秒です。このポリシーを使用してタイムアウト値を設定します。

再接続UIの透過レベル

この設定により、セッションの信頼性再接続中にXenAppまたはXenDesktop®セッションウィンドウに適用される不透明度レベルを指定できます。

デフォルトでは、再接続UIの透過性は80%に設定されています。

オーディオポリシー設定

オーディオセクションには、ユーザーデバイスがパフォーマンスを低下させることなくセッションでオーディオを送受信できるようにするポリシー設定が含まれています。

アダプティブオーディオ

この設定は、アダプティブオーディオを有効または無効にします。このポリシーを有効にすると、最高のユーザーエクスペリエンスを提供するためにオーディオ品質設定が動的に調整されます。この設定は、Citrix Virtual Apps and Desktops™ 2109以降を使用するVDAのシングルセッションOSおよびマルチセッションOSセッションの両方に適用されます。

この設定が禁止されている場合、オーディオ品質ポリシーが適用されます。詳細については、「オーディオ品質」を参照してください。

デフォルトでは、アダプティブオーディオポリシーは有効になっています。

UDPリアルタイムトランスポート経由のオーディオ

この設定は、ユーザーデータグラムプロトコル (UDP) を使用してRTP経由でVDAとユーザーデバイス間でオーディオを送受信することを許可または禁止します。この設定が無効になっている場合、オーディオはTCP経由で送受信されます。

デフォルトでは、UDP経由のオーディオは許可されています。

オーディオプラグアンドプレイ

この設定は、複数のオーディオデバイスを使用してサウンドを録音および再生することを許可または禁止します。

デフォルトでは、複数のオーディオデバイスの使用は許可されています。

この設定は、WindowsマルチセッションOSマシンにのみ適用されます。

オーディオ品質

この設定は、ユーザーセッションで受信されるサウンドの品質レベルを指定します。

デフォルトでは、サウンド品質は「高 - 高精細オーディオ」に設定されています。

サウンド品質を制御するには、次のいずれかのオプションを選択します。

- 低 - 低帯域幅接続の低速接続の場合に選択します。ユーザーデバイスに送信されるサウンドは最大16 Kbpsに圧縮されます。この圧縮により、音質が大幅に低下します。しかし、低帯域幅接続でも妥当なパフォーマンスを可能にします。
- 中 - 音声向けに最適化されており、Voice over Internet Protocolアプリケーションを提供します。この設定は、512 Kbps未満の回線、または著しい輻輳やパケット損失があるような困難なネットワーク接続でメディアアプリケーションを配信します。このコーデックはエンコード時

間が高速であるため、サーバー側のメディア処理が必要な場合に、ソフトフォンやユニファイドコミュニケーションアプリケーションでの使用に最適です。

ユーザーデバイスに送信されるオーディオは最大64 Kbpsに圧縮されます。この圧縮により、ユーザーデバイスで再生されるオーディオの品質は中程度に低下しますが、低遅延で低帯域幅を消費します。Voice over Internet Protocolの品質が不十分な場合は、Audio over UDP Real-time Transportポリシー設定が「許可」に設定されていることを確認してください。

現在、UDP経由のリアルタイムトランスポート（RTP）は、このオーディオ品質が選択されている場合にのみサポートされます。低速（512 Kbps未満）回線のような困難なネットワーク接続でメディアアプリケーションを配信する場合でも、このオーディオ品質を使用してください。また、ネットワークに輻輳やパケット損失がある場合にも使用します。

- 高 - 帯域幅が豊富で音質が重要な接続には、高精細オーディオを選択します。クライアントはネイティブレートでサウンドを再生できます。サウンドはCD品質を維持する高音質レベルで圧縮され、最大112 Kbpsの帯域幅を使用します。この量のデータを送信すると、CPU使用率の増加やネットワーク輻輳が発生する可能性があります。

帯域幅は、オーディオの録音中または再生中にのみ消費されます。両方が同時に発生すると、帯域幅の消費量は2倍になります。

最大帯域幅を指定するには、**Audio redirection bandwidth limit** または **Audio redirection bandwidth limit percent** 設定を構成します。

クライアントオーディオリダイレクト

この設定は、サーバーでホストされているアプリケーションが、ユーザーデバイスにインストールされているサウンドデバイスを介してサウンドを再生できるかどうかを指定します。この設定は、ユーザーがオーディオ入力を録音できるかどうかも指定します。

デフォルトでは、オーディオリダイレクトは許可されています。

この設定を許可した後、オーディオの再生または録音によって消費される帯域幅を制限できます。オーディオによって消費される帯域幅の量を制限すると、アプリケーションのパフォーマンスが向上する可能性がありますが、オーディオ品質が低下する可能性もあります。帯域幅は、オーディオの録音中または再生中にのみ消費されます。両方が同時に発生すると、帯域幅の消費量は2倍になります。最大帯域幅を指定するには、**Audio redirection bandwidth limit** または **Audio redirection bandwidth limit percent** 設定を構成します。

Windows Multi-session OSマシンでは、複数のオーディオデバイスをサポートするために、**Audio Plug N Play** 設定が有効になっていることを確認してください。

重要：クライアントオーディオリダイレクトを禁止すると、すべてのHDX™オーディオ機能が無効になります。

クライアントマイクのリダイレクト

この設定は、クライアントマイクのリダイレクトを有効または無効にします。有効にすると、ユーザーはセッション内でマイクを使用してオーディオ入力を録音できます。

デフォルトでは、マイクのリダイレクトは許可されています。

セキュリティのため、信頼されていないサーバーがデバイスを介してマイクにアクセスしようとすると、ユーザーに警告が表示されます。ユーザーはアクセスを許可するか、許可しないかを選択できます。ユーザーはCitrix Workspace™アプリでこの警告を無効にできます。

WindowsマルチセッションOSマシンでは、複数のオーディオデバイスをサポートするために、オーディオプラグアンドプレイ設定が「有効」になっていることを確認してください。

ユーザーデバイスで**クライアントオーディオリダイレクト**設定が無効になっている場合、このルールは無効になります。

帯域幅ポリシー設定

「**帯域幅**」セクションには、クライアントセッションの帯域幅使用に関連するパフォーマンスの問題を回避するためのポリシー設定が含まれています。

重要: これらのポリシー設定を**マルチストリームポリシー**設定と併用すると、予期しない結果が生じる可能性があります。ポリシーでマルチストリーム設定を使用する場合は、これらの帯域幅制限ポリシー設定が含まれていないことを確認してください。

オーディオリダイレクト帯域幅制限

この設定は、ユーザーセッションでオーディオを再生または録音するために許可される最大帯域幅を指定します。許可される最大帯域幅はキロビット/秒で指定されます。

デフォルトでは、最大値（ゼロ）は指定されていません。

この設定に値を入力し、**オーディオリダイレクト帯域幅制限の割合**設定に値を入力した場合、最も制限の厳しい設定（小さい方の値）が適用されます。

オーディオリダイレクトの帯域幅制限（パーセント）

この設定は、オーディオの再生または録音に許可される最大帯域幅制限を、セッションの総帯域幅に対する割合として指定します。

デフォルトでは、最大値（ゼロ）は指定されていません。

この設定に値を入力し、**オーディオリダイレクト帯域幅制限**設定に値を入力した場合、最も制限の厳しい設定（小さい方の値）が適用されます。

この設定を構成する場合、クライアントセッションで利用可能な帯域幅の総量を指定する**セッション全体の帯域幅制限**設定も構成する必要があります。

クライアントUSBデバイスリダイレクト帯域幅制限

この設定は、クライアントとの間でUSBデバイスをリダイレクトするために許可される最大帯域幅を指定します。許可される最大帯域幅はキロビット/秒で指定されます。

デフォルトでは、最大値（ゼロ）は指定されていません。

この設定と**クライアントUSBデバイスリダイレクト帯域幅制限（パーセント）**設定に値を入力した場合、最も制限の厳しい設定（低い方の値）が適用されます。

クライアントUSBデバイスリダイレクト帯域幅制限（パーセント）

この設定は、USBデバイスのクライアントとの間のリダイレクトに許可される最大帯域幅を、セッションの総帯域幅に対する割合として指定します。

デフォルトでは、最大値（ゼロ）は指定されていません。

この設定と**クライアントUSBデバイスリダイレクト帯域幅制限**設定に値を入力した場合、最も制限の厳しい設定（低い方の値）が適用されます。

この設定を構成する場合、クライアントセッションで利用可能な帯域幅の総量を指定する**セッション全体の帯域幅制限**設定も構成する必要があります。

クリップボードリダイレクト帯域幅制限

この設定は、セッションとローカルクリップボード間のデータ転送に許可される最大帯域幅を指定します。許可される最大帯域幅は、キロビット/秒で指定されます。

デフォルトでは、最大値（ゼロ）は指定されていません。

この設定と**クリップボードリダイレクト帯域幅制限（パーセント）**設定に値を入力した場合、最も制限の厳しい設定（低い方の値）が適用されます。

クリップボードリダイレクト帯域幅制限（パーセント）

この設定は、セッションとローカルクリップボード間のデータ転送に許可される最大帯域幅を、セッションの総帯域幅に対する割合として指定します。

デフォルトでは、最大値（ゼロ）は指定されていません。

この設定と**クリップボードリダイレクト帯域幅制限**設定に値を入力した場合、最も制限の厳しい設定（低い方の値）が適用されます。

この設定を構成する場合、クライアントセッションで利用可能な総帯域幅を指定する**セッション全体の帯域幅制限**設定も構成する必要があります。

COMポートリダイレクト帯域幅制限

> **注:**
>
> Virtual Delivery Agent 7.0から7.8の場合、この設定はレジストリを使用して構成します。詳細については、「レジストリを使用したCOMポートおよびLPTポートリダイレクト設定の構成」を参照してください。

この設定は、クライアント接続でCOMポートにアクセスするための最大許容帯域幅をキロビット/秒で指定します。この設定に値を入力し、**COMポートリダイレクト帯域幅制限率**設定に値を入力した場合、最も制限の厳しい設定（小さい方の値）が適用されます。

COMポートリダイレクト帯域幅制限率

注：Virtual Delivery Agent 7.0から7.8の場合、この設定はレジストリを使用して構成します。詳細については、「レジストリを使用したCOMポートおよびLPTポートリダイレクト設定の構成」を参照してください。

この設定は、クライアント接続でCOMポートにアクセスするための最大許容帯域幅を、セッション全体の帯域幅に対する割合として指定します。

デフォルトでは、最大値は指定されていません（ゼロ）。

この設定に値を入力し、**COMポートリダイレクト帯域幅制限**設定に値を入力した場合、最も制限の厳しい設定（小さい方の値）が適用されます。

この設定を構成する場合、クライアントセッションで利用可能な帯域幅の合計量を指定する**セッション全体の帯域幅制限**設定も構成する必要があります。

COMポートリダイレクトの帯域幅制限

> **注:**

> Virtual Delivery Agent 7.0から7.8の場合、この設定はレジストリを使用して構成します。詳細については、「レジストリを使用したCOMポートおよびLPTポートリダイレクト設定の構成」を参照してください。

> この設定は、クライアント接続でCOMポートにアクセスするために許可される最大帯域幅をキロビット/秒で指定します。この設定に値を入力し、**COMポートリダイレクト帯域幅制限（パーセント）**設定にも値を入力した場合、最も制限の厳しい設定（小さい方の値）が適用されます。

COMポートリダイレクトの帯域幅制限（パーセント）

注：Virtual Delivery Agent 7.0から7.8の場合、この設定はレジストリを使用して構成します。詳細については、「レジストリを使用したCOMポートおよびLPTポートリダイレクト設定の構成」を参照してください。

この設定は、クライアント接続でCOMポートにアクセスするために許可される最大帯域幅を、セッションの総帯域幅に対する割合として指定します。

デフォルトでは、最大値（ゼロ）は指定されていません。

この設定に値を入力し、**COMポートリダイレクト帯域幅制限**設定に値を入力した場合、最も制限の厳しい設定（小さい方の値）が適用されます。

この設定を構成する場合、クライアントセッションで利用可能な総帯域幅を指定する**セッション全体の帯域幅制限**設定も構成する必要があります。

ファイルリダイレクト帯域幅制限

この設定は、ユーザーセッションでクライアントドライブにアクセスするための最大許容帯域幅を指定します。最大許容帯域幅はキロビット/秒で指定されます。

デフォルトでは、最大値は指定されていません（ゼロ）。

この設定に値を入力し、**ファイルリダイレクト帯域幅制限率**設定に値を入力した場合、最も制限の厳しい設定（小さい方の値）が適用されます。

ファイルリダイレクト帯域幅制限率

この設定は、クライアントドライブへのアクセスに許可される最大帯域幅制限を、セッション全体の帯域幅に対する割合として指定します。

デフォルトでは、最大値 (ゼロ) は指定されていません。

この設定に値を入力し、**ファイルリダイレクト帯域幅制限**設定にも値を入力した場合、最も制限の厳しい設定 (小さい方の値) が適用されます。

この設定を構成する場合、クライアントセッションで利用可能な帯域幅の総量を指定する**セッション全体の帯域幅制限**設定も構成する必要があります。

HDX™ MediaStreamマルチメディアアクセラレーション帯域幅制限

この設定は、HDX MediaStreamマルチメディアアクセラレーションを使用してストリーミングオーディオおよびビデオを配信するために許可される最大帯域幅制限を指定します。許可される最大帯域幅はキロビット/秒で指定されます。

デフォルトでは、最大値 (ゼロ) は指定されていません。

この設定に値を入力し、**HDX MediaStreamマルチメディアアクセラレーション帯域幅制限の割合**設定にも値を入力した場合、最も制限の厳しい設定 (小さい方の値) が適用されます。

この設定を構成する場合、クライアントセッションで利用可能な総帯域幅を指定する**セッション全体の帯域幅制限**設定も構成する必要があります。

この設定は、HDX MediaStreamマルチメディアアクセラレーションを使用してストリーミングオーディオおよびビデオを配信するために許可される最大帯域幅を、セッション全体の帯域幅に対する割合として指定します。

デフォルトでは、最大値 (ゼロ) は指定されていません。

この設定に値を入力し、**HDX MediaStreamマルチメディアアクセラレーション帯域幅制限**設定にも値を入力した場合、最も制限の厳しい設定 (小さい方の値) が適用されます。

この設定を構成する場合、クライアントセッションで利用可能な帯域幅の総量を指定する**セッション全体の帯域幅制限**設定も構成する必要があります。

LPTポートリダイレクト帯域幅制限

注：Virtual Delivery Agent 7.0から7.8の場合、この設定はレジストリを使用して構成します。詳細については、「レジストリを使用したCOMポートおよびLPTポートリダイレクト設定の構成」を参照してください。

この設定は、単一ユーザーセッションでLPTポートを使用する印刷ジョブに許可される最大帯域幅を指定します。許可される最大帯域幅は、キロビット/秒で指定されます。

デフォルトでは、最大値（ゼロ）は指定されていません。

この設定に値を入力し、**LPTポートリダイレクト帯域幅制限パーセント**設定に値を入力した場合、最も制限の厳しい設定（小さい方の値）が適用されます。

LPTポートリダイレクト帯域幅制限パーセント

注：Virtual Delivery Agent 7.0から7.8では、レジストリを使用してこの設定を構成します。詳細については、「レジストリを使用してCOMポートおよびLPTポートリダイレクト設定を構成する」を参照してください。

この設定は、単一のクライアントセッションでLPTポートを使用する印刷ジョブの帯域幅制限を、セッション全体の帯域幅に対する割合として指定します。

デフォルトでは、最大値（ゼロ）は指定されていません。

この設定に値を入力し、**LPTポートリダイレクト帯域幅制限**設定に値を入力した場合、最も制限の厳しい設定（小さい方の値）が適用されます。

この設定を構成する場合、クライアントセッションで利用可能な帯域幅の合計量を指定する**セッション全体の帯域幅制限**設定も構成する必要があります。

セッション全体の帯域幅制限

この設定は、ユーザーセッションで利用可能な帯域幅の合計量をキロビット/秒で指定します。

適用可能な最大帯域幅の上限は20 Mbps (20,000 Kbps)です。デフォルトでは、最大値（ゼロ）は指定されていません。

クライアント接続によって消費される帯域幅の量を制限すると、クライアント接続以外の他のアプリケーションが限られた帯域幅を競合している場合に、パフォーマンスが向上する可能性があります。

プリンターリダイレクト帯域幅制限

この設定は、ユーザーセッションでクライアントプリンターにアクセスするために許可される最大帯域幅を指定します。許可される最大帯域幅は、1秒あたりのキロビット単位で指定されます。

デフォルトでは、最大値（ゼロ）は指定されていません。

この設定に値を入力し、**プリンターリダイレクト帯域幅制限の割合**設定にも値を入力した場合、最も制限の厳しい設定（低い方の値）が適用されます。

プリンターリダイレクト帯域幅制限の割合

この設定は、クライアントプリンターにアクセスするために許可される最大帯域幅を、セッションの総帯域幅に対する割合として指定します。

デフォルトでは、最大値（ゼロ）は指定されていません。

この設定に値を入力し、**プリンターリダイレクト帯域幅制限**設定にも値を入力した場合、最も制限の厳しい設定（低い方の値）が適用されます。

この設定を構成する場合、クライアントセッションで利用可能な総帯域幅を指定する**セッション全体の帯域幅制限**設定も構成する必要があります。

TWAINデバイスリダイレクト帯域幅制限

この設定は、公開アプリケーションからTWAINイメージングデバイスを制御するために許可される最大帯域幅を指定します。許可される最大帯域幅は、キロビット/秒で指定されます。

デフォルトでは、最大値（ゼロ）は指定されていません。

この設定に値を入力し、**TWAINデバイスリダイレクト帯域幅制限の割合**設定にも値を入力した場合、最も制限の厳しい設定（低い方の値）が適用されます。

TWAINデバイスリダイレクト帯域幅制限の割合

この設定は、公開アプリケーションからTWAINイメージングデバイスを制御するために許可される最大帯域幅を、セッションの総帯域幅に対する割合として指定します。

デフォルトでは、最大値（ゼロ）は指定されていません。

この設定に値を入力し、**TWAINデバイスリダイレクト帯域幅制限**設定にも値を入力した場合、最も制限の厳しい設定（低い方の値）が適用されます。

この設定を構成する場合、クライアントセッションで利用可能な帯域幅の総量を指定する**Overall session bandwidth limit** 設定も構成する必要があります。

双方向コンテンツリダイレクトポリシー設定

双方向コンテンツリダイレクトセクションには、クライアントからVDAへ、およびVDAからクライアントへのURLリダイレクトを有効または無効にするポリシー設定があります。

サーバーポリシーはWeb Studioで設定されます。Citrix Workspace™アプリバージョン2311以降、この設定はWeb Studioで非推奨となった以下の3つのレガシー設定に代わるものです。

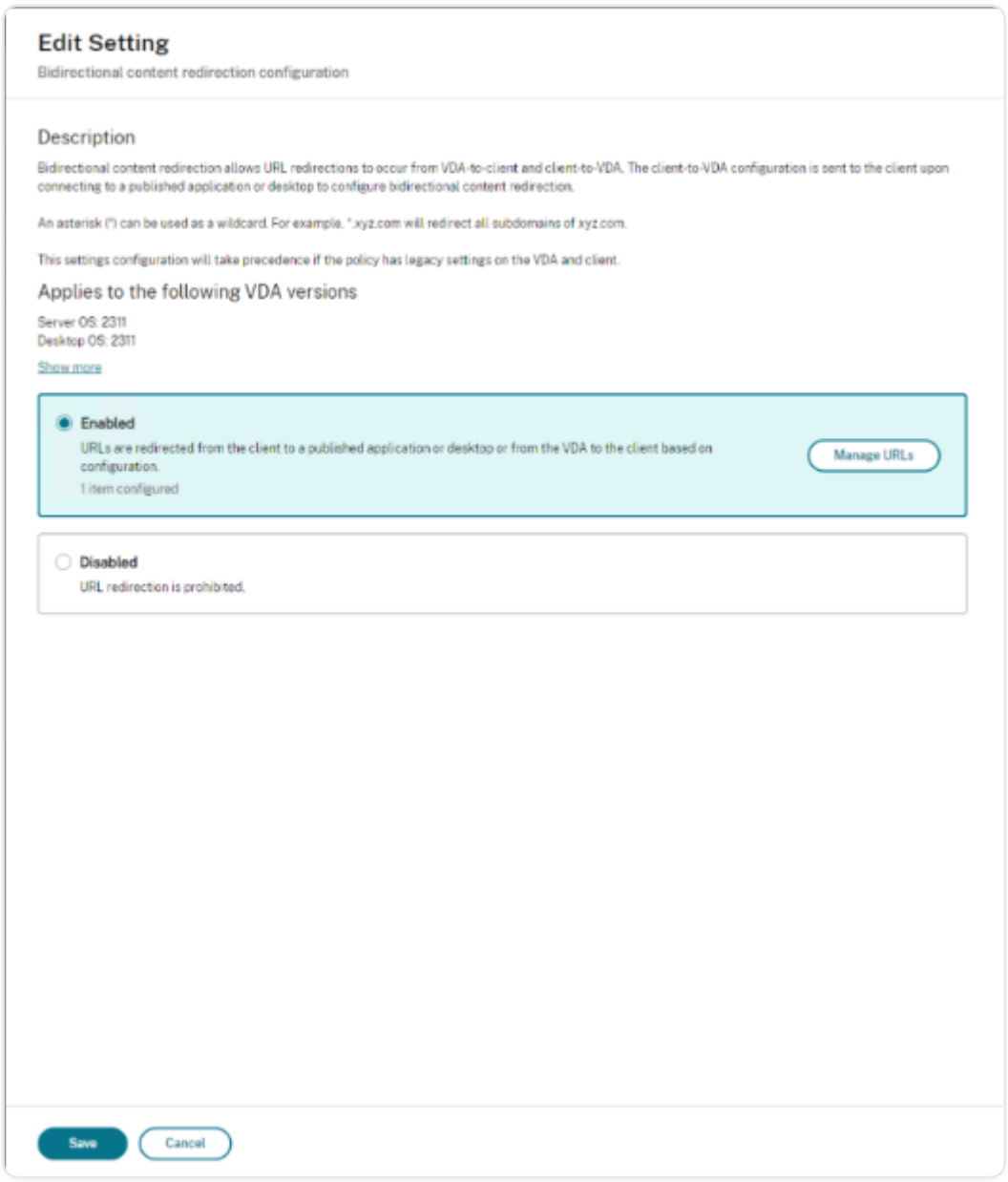
- 双方向コンテンツリダイレクトを許可する
- VDAにリダイレクトされる許可されたURL
- クライアントにリダイレクトされる許可されたURL

また、Windowsクライアント上の以下の3つのローカルグループポリシーオブジェクト（GPO）設定に代わるものです。

- 双方向コンテンツリダイレクト

- 双方向コンテンツリダイレクトのオーバーライド
- OAuthリダイレクト

この設定が有効になっている場合、公開されたアプリまたはデスクトップに接続すると、双方向コンテンツリダイレクトを構成するためのクライアントからVDAへの設定がクライアントに送信されます。



この設定が構成されている場合、Web Studioおよびクライアント上のレガシー設定よりも優先されます。Citrix®は、予期せぬ動作を避けるため、新しいポリシー設定のみを使用し、レガシー設定を削除することを推奨します。

VDAとDDCがバージョン2311以降を実行している場合、クライアントポリシーを設定してはなりません。そうでない場合、クライアントポリシーはCitrix WorkspaceアプリのGroup Policy Object管理テンプレートから設定されます。

Citrixは、クライアントからURLへのリダイレクトのためにホストからクライアントへのリダイレクトとローカルアプリアクセスを提供しています。ただし、Citrixはドメイン参加済みWindowsクライアントには双方向コンテンツリダイレクトを使用することを推奨します。

Citrixは、Desktop Studioの代わりにWeb Studioの新しいUIを使用してこの機能を構成することを推奨します。

ワイルドカードリダイレクト

双方向コンテンツリダイレクトは、リダイレクトするURLを定義する際にワイルドカードの使用をサポートしています。詳細および双方向コンテンツリダイレクトの構成については、構成の手順を参照してください。 Web Studioで、`hostToClientUrls`配列または`clientToHostUrls`配列内の`url`キーの値としてJSON文字列を編集して、ワイルドカードURLを設定します。

> **注:**
>
> - 無限ループを避けるため、`hostToClientUrls`と`clientToHostUrls`に同じURLを設定しないでください。
> - トップレベルドメインはサポートされていません。たとえば、`<https://www.citrix.*>`や`<http://www.citrix.co*>`はリダイレクトされません。

双方向コンテンツリダイレクトの構成

この機能を構成し始めるには、このポリシーを`Enabled`に設定し、**Manage URLs**をクリックします。以下の構成を設定します。

- **VDAからクライアントへのリダイレクト**
- **クライアントからVDAへのリダイレクト**

VDAからクライアントへのリダイレクト

VDAからクライアントにURLをリダイレクトするには、1行に1つのURLを入力します。ワイルドカードも使用できます。 OAuthリダイレクトを使用すると、クライアントエンドポイントのブラウザを使用して認証を実行し、トークンをVDAに送り返すことができます。

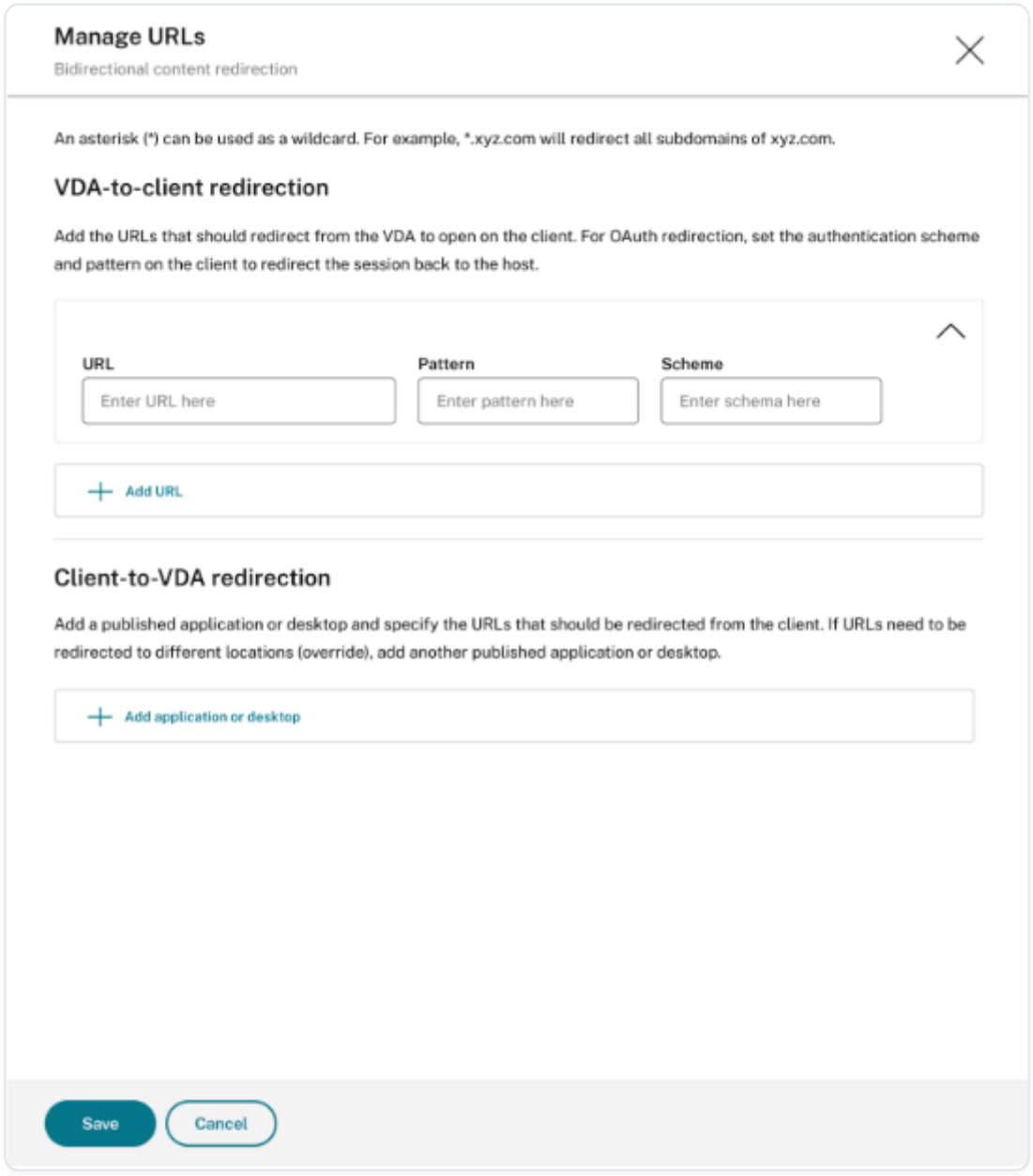
利点:

- これらの資格情報をホスト環境に保存しないようにできます。
- エンドポイントで利用可能で、VDAでは利用できない生体認証機能を使用できます。

構成：

URLのVDAからクライアントへのリダイレクトを構成するには、以下を指定します。

- **URL** (必須) VDAからクライアントで開くようにリダイレクトする必要があるURLを追加します。**OAuthリダイレクト**の場合、セッションをホストにリダイレクトするために、クライアントで認証スキームとパターンを設定します。
- **パターン**: (オプション) VDAからクライアントへのURLリダイレクトを介してクライアントにリダイレクトされると、OAuth認証フローが開始されたかのように追跡されるURL正規表現。フローが完了したとき（結果のスキームまたはリダイレクトURLパターンが開かれることによって検出される）、その結果のURLは、そのフローを開始したホストVDAにリダイレクトされます。
- **スキーム**: (オプション) **スキーム**が指定されている場合、終了URLは`<scheme>`://`<something>`の形式であると想定されます。スキームが指定されていない（空である）とします。その場合、元の結果のURLパターンは、正規表現キャプチャグループ（パターンで指定する必要がある）を介してパターンから抽出され、元のURLは`citrix-oauth-redir://`リダイレクトURLを使用するように書き換えられます。フローが完了すると、元のリダイレクトURLはホスト（VDA）にリダイレクトされます。この場合、OAuth認証サーバーは`citrix-oauth-redir://byIndex/1 (2, 3, ... N)`リダイレクトURLを許可するように構成する必要があります。



注:

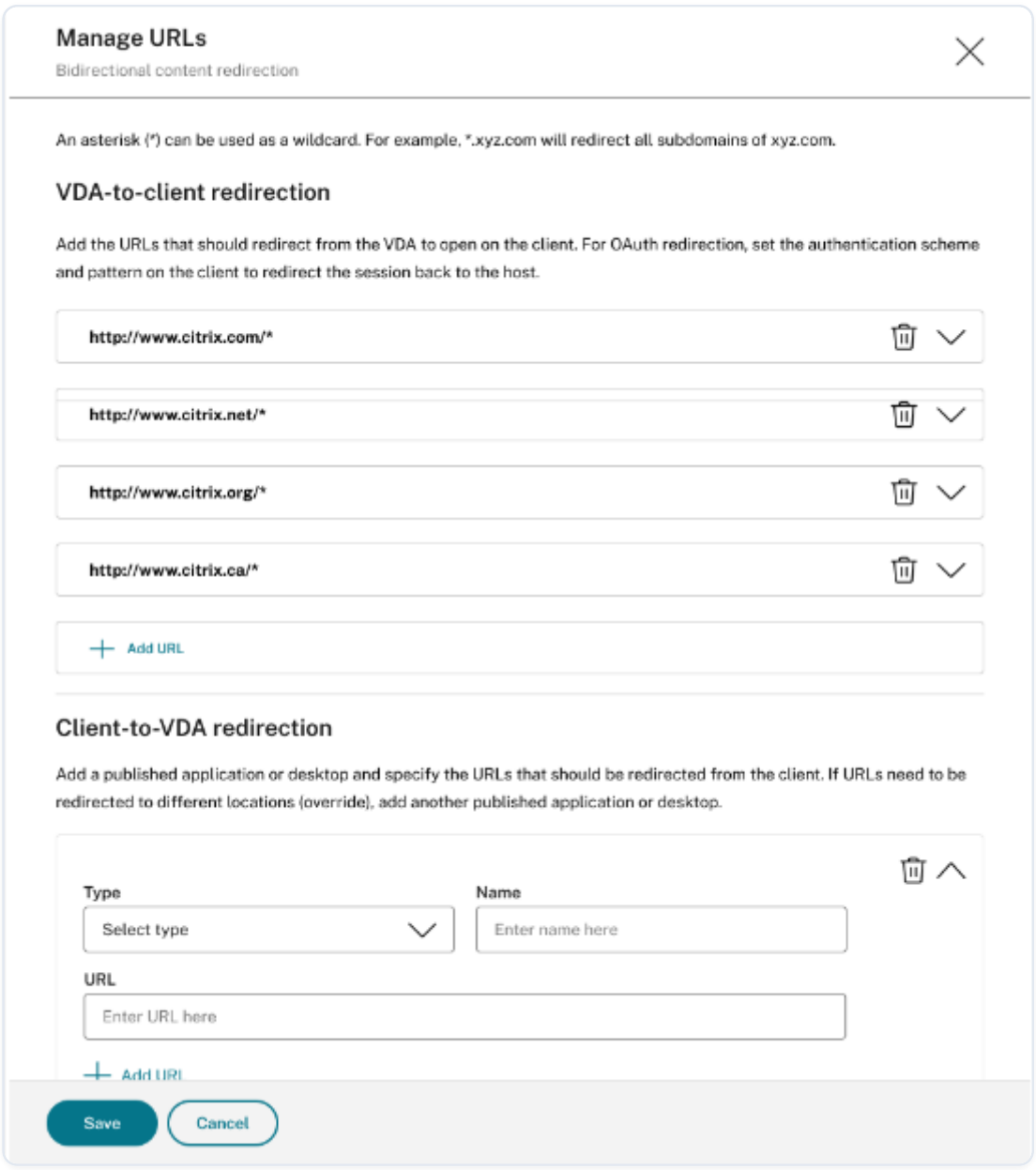
パターンと**スキーム**はどちらもオプションですが、**パターン**が指定されている場合は、**スキーム**も指定する必要があります。

クライアントからVDAへのリダイレクト

クライアントからVDAにURLをリダイレクトするには、次の手順を実行します。

1. クライアントURLの宛先を構成します。
2. 公開アプリケーションまたは公開デスクトップのいずれかを選択します。
3. そのリソースの名前を指定します。

4. そのリソースにリダイレクトする必要があるすべてのURLを追加します。 新しいアプリケーションまたはデスクトップを追加し、そのリソースにリダイレクトするURLを指定することで、このデフォルトのリソースを上書きできます。



デスクトップスタジオ

注:

Citrixは、Citrix Virtual Apps and Desktops™バージョン2402以降、この機能を構成するためにWeb Studioを使用することを推奨します。

2311の双方向コンテンツリダイレクトを構成するには、次の形式でJSON文字列を作成します。

```
{

  "version": 1,

  "hostToClientConfig": [

    {

      "hostToClientUrls": [

        {

          "url": "http://www.citrix.com/*"

        },

        {

          "url": "www.example.com"

        },

        {

          "url": "https://login.example.org/*",

          "oAuthRedirectionPattern": "https://login.example.org/
oauth2?.*",

          "oAuthScheme": "idm.desktop-authentication"

        }

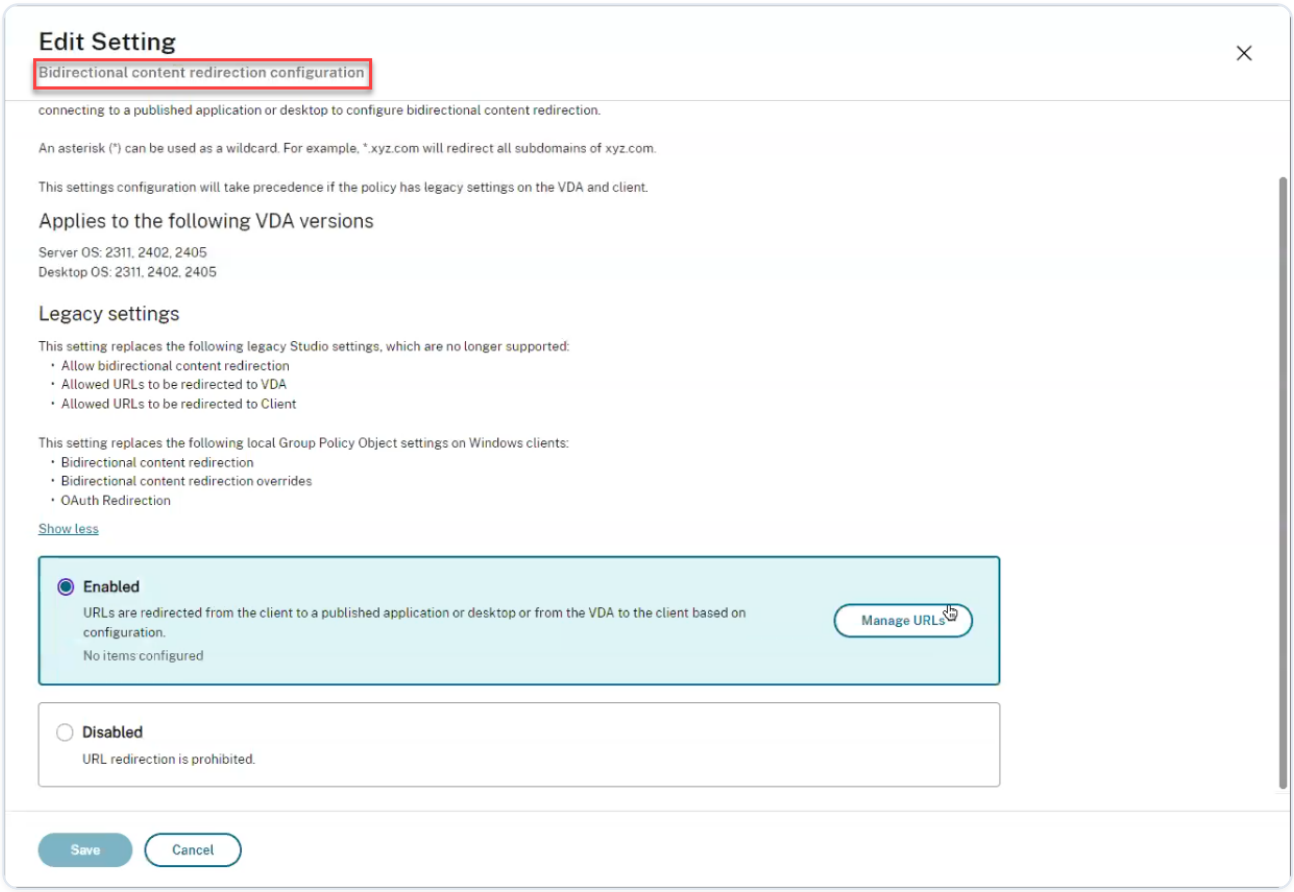
      ]

    }

  ],

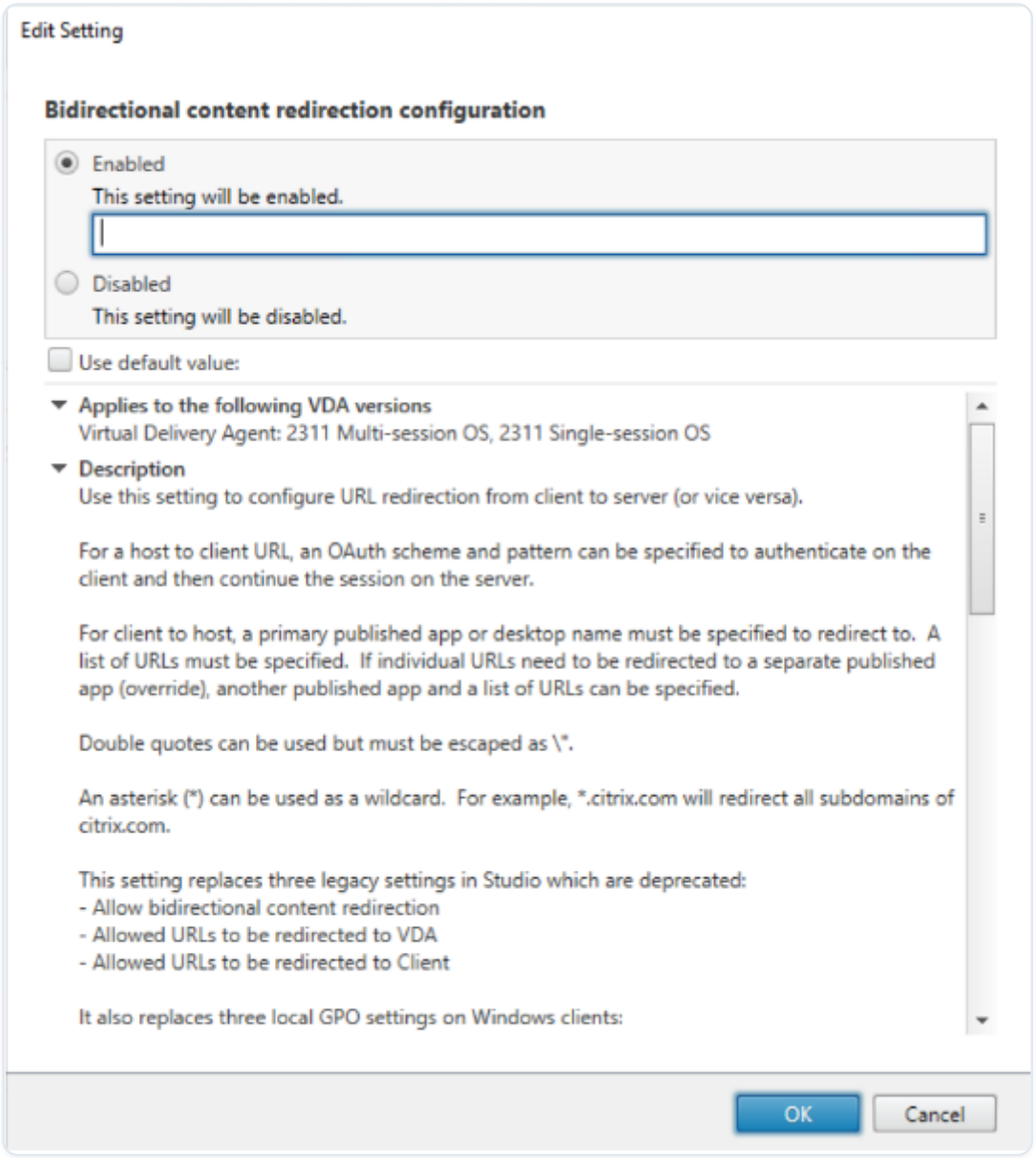
  "clientToHostConfig": [
```

```
    {
      "publishedAppOrDesktopNameType": "Desktop",
      "publishedAppOrDesktopName": "Win11Desktop",
      "clientToHostUrls": [
        "https://www.example.net",
        "https://*.citrix.example"
      ]
    },
    {
      "publishedAppOrDesktopNameType": "Application",
      "publishedAppOrDesktopName": "Chrome",
      "clientToHostUrls": [
        "https://tibco.example"
      ]
    }
  ]
}
```



次のパラメーターを設定する必要があります。

- **version**: (必須) 1に設定します。
- VDAからクライアントへのURLリダイレクトの場合、単一の`hostToClientConfig`を作成します。
- **hostToClientUrls**: (必須) ホスト（VDA）からクライアントにリダイレクトされるURLのリスト。ワイルドカードが許可されます。「*」が指定されている場合、`clientToHostConfig`は`publishedAppOrDesktopNameType`、空の`publishedAppOrDesktopName`、および空の`clientToHostUrls`とともに指定する必要があります。



OAuthリダイレクト

OAuthリダイレクトを使用すると、クライアントエンドポイントブラウザを使用して認証し、トークンをVDAに送り返すことができます。

利点:

- これらの資格情報をホストされた環境に保存することを回避できます。
- エンドポイントで利用可能で、VDAでは利用できない生体認証機能を使用できます。

URLのOAuthリダイレクトを構成するには、次のパラメーターを指定します。

- **oAuthRedirectionPattern**: (オプション) VDAからクライアントへのURLリダイレクトを介してクライアントにリダイレクトされると、OAuth認証フローが開始されたかのように追跡され、フローが完了したとき（結果のスキームまたはリダイレクトURLパターンが開かれたこと

によって検出される）、その結果のURLは、そのフローを開始したホストVDAにリダイレクトされるURL正規表現。

- **oAuthScheme**: (オプション) スキームが指定されている場合、終了URLは `<scheme>://<something>` の形式であると想定されます。スキームが指定されていない（空である）とします。その場合、元の結果URLパターンは正規表現キャプチャグループ（パターンで指定する必要がある）を介してパターンから抽出され、元のURLは `citrix-oauth-redir://` リダイレクトURLを使用するように書き換えられます。フローが完了すると、元のリダイレクトURLはホスト（VDA）にリダイレクトされます。この場合、OAuth認証サーバーは `citrix-oauth-redir://byIndex/1 (2, 3, ... N)` リダイレクトURLを許可するように構成する必要があります。

クライアントからVDAへのリダイレクトの場合、リダイレクトする各リソースに対して **clientToHostConfig** を作成します。 各リソースには、次のパラメータを含めます。

- **publishedAppOrDesktopNameType**: (必須) Web Studioで構成された公開デスクトップ（「Desktop」）または公開アプリケーション（「Application」）のいずれか。リソースが無効な場合、リダイレクトは正しく機能しません。
- **publishedAppOrDesktopName**: (必須) Web Studioで構成されたリソース名。
- **clientToHostUrls**: (必須) クライアントからホスト（VDA）にリダイレクトされるURLのリスト。ワイルドカードが許可されます。

既知の制限

PowerShellを使用してカスタムURLスキーム（HTTPまたはHTTPSではない）でブラウザを起動すると、カスタムURLはクライアントにリダイレクトされません。

ブラウザコンテンツリダイレクトポリシー設定

ブラウザコンテンツリダイレクト (BCR) は、Citrix Virtual Apps and Desktops™ 環境内でのWebブラウジングのユーザーエクスペリエンスを向上させます。Webページのレンダリングをユーザーのローカルマシンにオフロードすることで、BCRはサーバー負荷を軽減し、特に複雑なWebサイトやリソースを大量に消費するWebサイトのパフォーマンスを向上させます。 このドキュメントでは、ブラウザコンテンツリダイレクトで利用可能な各ポリシー設定オプションについて詳しく説明します。

ブラウザコンテンツリダイレクト

この設定は、ブラウザコンテンツリダイレクトの主要なオン/オフスイッチとして機能します。

- **機能:** Webページがサーバーでレンダリングされるか、ローカルデバイスでレンダリングされるかを決定します。有効にすると、Citrix Workspace™ アプリは、よりスムーズなエクスペリ

エンスのために、Webコンテンツをデバイスで取得して表示しようとします。それが失敗した場合、サーバーでのレンダリングにフォールバックします。

- **オプション:**
  - **許可:** (デフォルト) ブラウザコンテンツリダイレクトを有効にします。
  - **禁止:** ブラウザコンテンツリダイレクトを無効にします。
- **注意点:** 許可されている場合、Citrix Workspaceアプリはクライアントフェッチとクライアントレンダリングを試行します。クライアントフェッチとクライアントレンダリングが失敗した場合、ブラウザコンテンツリダイレクトはサーバー側レンダリングにフォールバックします。サーバーフェッチとクライアントレンダリングを有効にするには、「ブラウザコンテンツリダイレクトプロキシ構成」設定を有効にします。

ブラウザコンテンツリダイレクトACL構成

この設定では、ブラウザコンテンツリダイレクトの使用を許可または禁止するWebサイト（URL）のリストを作成できます。

- **機能:** ブラウザコンテンツリダイレクトで最適化されるWebサイトをきめ細かく制御できます。Webサイト全体または特定のページを指定できます。
- **動作方法:**
  - **許可されるURL:** このリストにあるWebサイトは、そのコンテンツがデバイスに表示されます。ワイルドカード（）*を使用して、複数のページまたはサブドメインを含めることができます（例：* `<https://www.example.com/>` または `<http://*.example.com/>`）。URLのプロトコル内ではワイルドカードは許可されません。
- **デフォルト:** `<https://www.youtube.com/*>`
- **例:**
  - **許可されるパターン:** <http://www.xyz.com/index.html, `<https://www.xyz.com/*>` , `<http://www.xyz.com/*videos>` *> , `<http://*.xyz.com/<>` >
  - **許可されないもの:** `<http://*.*.com/>`
  - URLでパスを指定することで、より詳細な粒度を実現できます。たとえば、`<https://www.xyz.com/sports/index.html>` を指定した場合、index.html ページのみがリダイレクトされます

ブラウザコンテンツリダイレクトのブロックリスト構成

この設定は、「ブラウザコンテンツリダイレクトACL構成」設定と連携して機能します。

- **機能:** ACL構成で許可されている場合でも、特定のWebサイトやページをブロックできるようにすることで、追加の制御レイヤーを提供します。ブロックリストが優先されます。
- **仕組み:** ACL構成によって一般的に許可されている場合でも、デバイスにリダイレクトされたくないWebサイトやページを指定します。
- **デフォルト:** URLは構成されていません
- **ワイルドカード:** ACL構成と同様に、ワイルドカード (*) を使用して複数のページやサブドメインをブロックできます。
- **例:** Webサイトのindex.htmlページのみをブロックするには、次のように入力します: `<https://www.example.com/sports/index.html>`

ブラウザコンテンツリダイレクトの認証サイト

この設定では、外部IDプロバイダー (IdP) を使用してログインするWebサイトでのブラウザコンテンツリダイレクトの動作を管理できます。

- **機能:** 認証のために別のWebサイトにリダイレクトされた場合でも (WebサイトがOktaやその他のサービスをログインに使用する場合など)、ブラウザコンテンツリダイレクトがアクティブな状態を維持するようにします。
- **仕組み:** 認証WebサイトのURLをこのリストに追加することで、ログイン中にリダイレクトプロセスが中断されないようにします。
- **デフォルト:** URL は構成されていません
- **例:** www.example.com が認証に www.example.okta.com を使用する場合、www.example.com/ をブラウザーコンテンツリダイレクト ACL 構成に追加し、認証 Web サイト www.example.okta.com をブラウザーコンテンツリダイレクト認証サイトに追加します。
- **詳細情報:** 詳細については、Citrix Knowledge Center の記事 CTX238236 および「ブラウザーコンテンツリダイレクト」の「マルチメディア」セクションを参照してください。

ブラウザコンテンツリダイレクトのプロキシ構成

この設定により、ブラウザーコンテンツリダイレクトがネットワークのプロキシサーバーをどのように使用するかをより詳細に制御できます。また、環境でクライアントフェッチクライアントレンダーが許可されていない場合に、サーバーフェッチクライアントレンダーを容易にします。

- **機能:** Citrix Workspace アプリに、Web コンテンツのフェッチにサーバーフェッチメソッドを使用するよう強制します。有効にすると、常にサーバーからコンテンツをフェッチし、デバイスに表示しようとします。
- **オプション:**

    - 明示的プロキシ: 特定のプロキシサーバーを使用します。プロキシサーバーのアドレスとポート番号を指定する必要があります (例: `<http://proxy.example.com:80>`)。
        - 許可されるパターン:
        - http://<hostname/ip address\>:\<port\> | 例: `<http://proxy.example.citrix.com:80>` `<http://10.10.10.10:8080>`
    - PAC/WPAD: PAC ファイルまたは WPAD を使用して、プロキシ設定を自動的に決定します。PAC ファイルの URL を指定する必要があります (例: `<http://wpad.myproxy.com:30/configuration/pac/Proxy.pac>`)。
        - PAC/WPAD ファイルの許可されるパターン:
        - http://<hostname/ip address\>:<port\>/<path\>/<Proxy\>.pac | 例: `<http://wpad.myproxy.com:30/configuration/pac/Proxy.pac>`
        - https://<hostname/ip address\>:<port\>/<path\>/<wpad.dat\> | 例: `<http://10.10.10.10/configuration/pac/wpad.dat>`
    - 直接/透過: プロキシサーバーを使用しないか、透過プロキシを使用します。
        - キーワード「DIRECT」を設定します
        - このキーワードでは大文字と小文字が区別されます

- **デフォルト:** 禁止 (無効)

ブラウザコンテンツリダイレクトの統合Windows認証サポート

この設定により、統合Windows認証 (IWA) を使用するWebサイトへのログインが簡素化されます。

- **動作:** ブラウザコンテンツリダイレクトが既存のWindows資格情報を使用してWebサイトに自動的にログインできるようにします。これにより、ユーザー名とパスワードを繰り返し入力する必要がなくなります。
- **オプション:**
    - **許可:** IWAを使用するWebサイトのシングルサインオン (SSO) を有効にします。
    - **禁止:** (デフォルト) SSOを無効にし、毎回資格情報を入力する必要があります。

ブラウザコンテンツリダイレクトのサーバーフェッチプロキシ認証

この設定は、サーバーからコンテンツをフェッチする際に、ブラウザコンテンツリダイレクトがWebプロキシとどのように連携するかを制御します。

- **機能:** ブラウザコンテンツリダイレクトがWindows資格情報を使用してプロキシサーバーで認証できるようにし、Webコンテンツへの安全なアクセスを確保します。
- **動作:** 有効にすると、ブラウザコンテンツリダイレクトはKerberosサービスチケットを自動的に取得して使用し、プロキシで認証します。
- **要件:** PACファイルを構成して、ダウンストリームWebプロキシを介してトラフィックをルーティングし、プロキシがKerberos認証を使用するように設定する必要があります。
- **オプション:**
  - **許可:** プロキシサーバーとのKerberos認証を有効にします。
  - **禁止:** (既定値) ブラウザコンテンツリダイレクトは、プロキシで認証するために基本認証またはその他の利用可能な資格情報を使用します。

デスクトップUIポリシー設定

デスクトップUIセクションには、デスクトップの壁紙、メニューアニメーション、ドラッグイメージなどの視覚効果を制御するポリシー設定が含まれています。これらのポリシー設定は、クライアント接続で使用される帯域幅の管理に役立ちます。帯域幅の使用量を制限することで、WANでのアプリケーションパフォーマンスを向上させることができます。

> **重要:**

> このリリースでは、レガシーグラフィックモードおよびデスクトップコンポジションリダイレクト (DCR) はサポートされていません。このポリシーは、以下を使用する場合の旧バージョンとの互換性のためのみに含まれています。

> - XenApp 7.15 LTSR
> - XenDesktop 7.15 LTSR
> - Windows 7およびWindows 2008 R2を使用している以前のVDAリリース。

デスクトップコンポジションリダイレクト

この設定は、ユーザーによりスムーズなWindowsデスクトップエクスペリエンスを提供するために、ローカルDirectXグラフィックレンダリングに以下の処理機能を使用するかどうかを指定します。

- ユーザーデバイス上のグラフィック処理ユニット（GPU）

- または、,
- ユーザーデバイス上の統合グラフィックプロセッサ（IGP）

有効にすると、**デスクトップコンポジションリダイレクト**は、サーバーの高いスケーラビリティを維持しながら、応答性の高いWindowsエクスペリエンスを提供します。

デフォルトでは、**デスクトップコンポジションリダイレクト**は無効になっています。

デスクトップコンポジションリダイレクトの選択を解除し、ユーザーセッションで必要な帯域幅を削減するには、この設定をポリシーに追加するときに、**無効**を選択します。

デスクトップコンポジションリダイレクトのグラフィック品質

この設定は、デスクトップコンポジションリダイレクトに使用されるグラフィックの品質を指定します。

デフォルトは「高」です。

「高」、「中」、「低」、または「ロスレス」の品質から選択します。

デスクトップの壁紙

この設定は、ユーザーセッションでの壁紙の表示を許可または禁止します。

デフォルトでは、ユーザーセッションで壁紙を表示できます。

デスクトップの壁紙を無効にし、ユーザーセッションで必要な帯域幅を削減するには、この設定をポリシーに追加する際に**禁止**を選択します。

メニューアニメーション

この設定は、ユーザーセッションでのメニューアニメーションを許可または禁止します。

デフォルトでは、メニューアニメーションは許可されています。

メニューアニメーションは、アクセシビリティのためのMicrosoftの個人設定です。有効にすると、短い遅延の後、スクロールまたはフェードインによってメニューが表示されます。メニューの下部に矢印アイコンが表示されます。その矢印をポイントするとメニューが表示されます。

メニューアニメーションは、このポリシー設定が**許可**に設定されており、メニューアニメーションのMicrosoft個人設定が有効になっている場合に、デスクトップで有効になります。

> **注:**

> メニューアニメーションのMicrosoft個人設定への変更はデスクトップに影響します。セッション終了時にデスクトップが変更を破棄するように設定されているとします。この場合、メニューアニメーションを有効にしているユーザーは、以降のセッションでメニューアニメーションを利用できない可能性があります。メニューアニメーションを必要とするユーザーのために、デスクトップのメインイメージでMicrosoft設定を有効にするか、デスクトップがユーザーの変更を保持するようにしてください。

ウィンドウのドラッグ中にウィンドウの内容を表示

この設定は、画面上でウィンドウをドラッグする際に、ウィンドウの内容を表示するかどうかを許可または禁止します。

デフォルトでは、ウィンドウの内容の表示は許可されています。

許可に設定すると、ウィンドウをドラッグしたときにウィンドウ全体が移動するように見えます。**禁止**に設定すると、ウィンドウをドロップするまでウィンドウのアウトラインのみが移動するように見えます。

エンドユーザー監視ポリシー設定

「**エンドユーザー監視**」セクションには、セッショントラフィックを測定するためのポリシー設定が含まれています。

ICA®ラウンドトリップ計算

この設定は、アクティブな接続に対してICAラウンドトリップ計算が実行されるかどうかを決定します。

デフォルトでは、アクティブな接続の計算は有効になっています。

デフォルトでは、各ICAラウンドトリップ測定の開始は遅延されます。この遅延は、ユーザーインタラクションを示すトラフィックが発生するまで続きます。この遅延は無期限に続く可能性があり、ICAラウンドトリップ測定がICAトラフィックの唯一の原因となるのを防ぐように設計されています。

ICAラウンドトリップ計算間隔

この設定は、ICAラウンドトリップ計算が実行される頻度を秒単位で指定します。

デフォルトでは、ICAラウンドトリップは15秒ごとに計算されます。

アイドル接続のICAラウンドトリップ計算

この設定は、アイドル接続に対してICAラウンドトリップ計算が実行されるかどうかを決定します。

デフォルトでは、アイドル接続に対して計算は実行されません。

デフォルトでは、各ICAラウンドトリップ測定の開始は遅延されます。この遅延は、ユーザーインタラクションを示すトラフィックが発生するまで続きます。この遅延は無期限に続く可能性があり、ICAラウンドトリップ測定がICAトラフィックの唯一の原因となるのを防ぐように設計されています。

ファイルリダイレクトポリシー設定

ファイルリダイレクトセクションには、クライアントドライブマッピングおよびクライアントドライブ最適化に関連するポリシー設定が含まれています。

クライアントドライブの自動接続

この設定は、ユーザーがログオンしたときにクライアントドライブの自動接続を許可または禁止します。

デフォルトでは、自動接続は許可されています。

この設定をポリシーに追加する際は、自動接続したいドライブの種類の設定を有効にしてください。たとえば、ユーザーのCD-ROMドライブの自動接続を許可するには、この設定と**クライアント光学ドライブ**設定を構成します。

関連するポリシー設定は次のとおりです。

- **クライアントドライブリダイレクト**
- **クライアントフロッピーディスクドライブ**
- **クライアント光学ドライブ**
- **クライアント固定ドライブ**
- **クライアントネットワークドライブ**
- **クライアントリムーバブルドライブ**

クライアントドライブリダイレクト

この設定は、ユーザーデバイス上のドライブとの間でファイルリダイレクトを有効または無効にします。

デフォルトでは、ファイルリダイレクトは有効になっています。

> **注:**

> クライアントドライブリダイレクトポリシー設定は、汎用USBリダイレクトを使用してセッションにマップされたドライブには適用されません。

> 有効にすると、ユーザーはすべてのクライアントドライブにファイルを保存できます。無効にすると、すべてのファイルリダイレクトが防止されます。この構成は、個々のファイルリダイレクト設定の状態に関係なく適用されます。個々のファイルリダイレクト設定には、クライアントフロッピードライブとクライアントネットワークドライブが含まれます。

関連するポリシー設定は次のとおりです。

- **クライアントフロッピードライブ**
- **クライアント光学ドライブ**
- **クライアント固定ドライブ**
- **クライアントネットワークドライブ**
- **クライアントリムーバブルドライブ**

クライアント固定ドライブ

この設定により、ユーザーはユーザーデバイス上の固定ドライブへのファイルのアクセスまたは保存を許可または禁止されます。

デフォルトでは、クライアント固定ドライブへのアクセスは許可されています。

この設定をポリシーに追加する場合は、**クライアントドライブリダイレクト**設定が存在し、許可に設定されていることを確認してください。これらの設定が無効になっている場合、クライアント固定ドライブはマップされず、**クライアント固定ドライブ**設定の状態に関係なく、ユーザーはこれらのドライブに手動でアクセスできません。

ユーザーがログオンしたときに固定ドライブが自動的に接続されるように、**クライアントドライブの自動接続**設定を構成します。

クライアントフロッピードライブ

この設定では、ユーザーがユーザーデバイス上のフロッピーディスクドライブにアクセスしたり、ファイルを保存したりすることを許可または禁止します。

デフォルトでは、クライアントフロッピードライブへのアクセスは許可されています。

この設定をポリシーに追加するときは、**クライアントドライブのリダイレクト**設定が存在し、許可に設定されていることを確認してください。これらの設定が無効になっている場合、**クライアン**

トフロッピーディスクドライブ設定の状態にかかわらず、クライアントフロッピーディスクドライブはマップされず、ユーザーはこれらのドライブに手動でアクセスできません。

ユーザーのログオン時にフロッピーディスクドライブが自動的に接続されるようにするには、**クライアントドライブの自動接続**設定を構成します。

クライアントネットワークドライブ

この設定では、ユーザーがユーザーデバイスを介してネットワーク（リモート）ドライブにアクセスしたり、ファイルを保存したりすることを許可または禁止します。

デフォルトでは、クライアントネットワークドライブへのアクセスは許可されています。

この設定をポリシーに追加するときは、**クライアントドライブのリダイレクト**設定が存在し、許可に設定されていることを確認してください。これらの設定が無効になっている場合、クライアントネットワークドライブはマップされず、ユーザーはこれらのドライブに手動でアクセスできません。この構成は、**クライアントネットワークドライブ**設定の状態にかかわらず適用されます。

ユーザーのログオン時にネットワークドライブが自動的に接続されるようにするには、**クライアントドライブの自動接続**設定を構成します。

クライアント光学ドライブ

この設定では、ユーザーが以下の場所にアクセスしたり、ファイルを保存したりすることを許可または禁止します。

- ユーザーデバイス上のCD-ROM
- ユーザーデバイス上のDVD-ROM
- ユーザーデバイス上のBD-ROMドライブ。

デフォルトでは、クライアント光学ドライブへのアクセスは許可されています。

この設定をポリシーに追加する場合は、**クライアントドライブのリダイレクト**設定が存在し、**許可**に設定されていることを確認してください。これらの設定が無効になっている場合、クライアントの光学ドライブはマップされず、ユーザーはこれらのドライブに手動でアクセスできません。この構成は、**クライアント光学ドライブ**設定の状態に関係なく適用されます。

ユーザーがログオンしたときに光学ドライブが自動的に接続されるようにするには、「**クライアントドライブの自動接続**」設定を構成します。

クライアントリムーバブルドライブ

この設定により、ユーザーはユーザーデバイス上のUSBドライブにアクセスしたり、ファイルを保存したりすることを許可または禁止されます。

デフォルトでは、クライアントリムーバブルドライブへのアクセスは許可されています。

この設定をポリシーに追加する場合は、**クライアントドライブのリダイレクト**設定が存在し、許可に設定されていることを確認してください。これらの設定が無効になっている場合、クライアントのリムーバブルドライブはマップされず、ユーザーはこれらのドライブに手動でアクセスできません。この構成は、**クライアントリムーバブルドライブ**設定の状態に関係なく適用されます。

ユーザーがログオンしたときにリムーバブルドライブが自動的に接続されるように、**クライアントドライブの自動接続**設定を構成します。

ホストからクライアントへのリダイレクト

この設定は、URLおよび一部のメディアコンテンツのファイルタイプ関連付けを有効または無効にし、ユーザーデバイスで開かれるようにします。無効にすると、コンテンツはサーバーで開かれます。

デフォルトでは、ファイルタイプ関連付けは無効になっています。

この設定を有効にすると、次のURLタイプがローカルで開かれます。

- HTTP
- HTTPS
- リアルプレイヤーおよびクイックタイム (RTSP)
- Real Player および QuickTime (RTSPU)
- レガシー Real Player (PNM)
- マイクロソフト メディア サーバー (MMS)

クライアントドライブ文字を保持する

この設定は、セッション内でクライアントドライブを同じドライブ文字にマッピングすることを有効または無効にします。

デフォルトでは、クライアントドライブ文字は保持されません。

この設定をポリシーに追加する場合は、**クライアントドライブのリダイレクト**設定が存在し、許可に設定されていることを確認してください。

読み取り専用クライアントドライブアクセス

この設定は、ユーザーとアプリケーションが以下の操作を行うことを許可または禁止します。

- マップされたクライアントドライブ上にファイルを作成する
- マップされたクライアントドライブ上のファイルを変更する

- マップされたクライアントドライブ上のフォルダーを変更する

デフォルトでは、マップされたクライアントドライブ上のファイルとフォルダーは変更できます。

有効に設定されている場合、ファイルとフォルダーは読み取り専用権限でアクセスできます。

この設定をポリシーに追加する場合は、**クライアントドライブのリダイレクト**設定が存在し、許可に設定されていることを確認してください。

特殊フォルダーリダイレクト

この設定は、Citrix Workspace™アプリおよびWeb Interfaceのユーザーが、セッションからローカルのドキュメントおよびデスクトップの特殊フォルダーを表示できるようにするか、または表示できないようにします。

デフォルトでは、特殊フォルダーリダイレクトは許可されています。

この設定は、ポリシーによってフィルター処理されたオブジェクトが、他の場所に存在する設定に関係なく、特殊フォルダーリダイレクトを持つことを防止します。この設定が禁止されている場合、StoreFront™、Web Interface、またはCitrix Workspaceアプリに指定された関連設定はすべて無視されます。

特殊フォルダーリダイレクトを許可するユーザーを定義するには、**許可**を選択し、この機能を許可するユーザーにフィルター処理されたポリシーにこの設定を含めます。この設定は、他のすべての特殊フォルダーリダイレクト設定を上書きします。

ユーザーがローカルハードドライブへのファイルアクセスまたは保存を防止するポリシー設定は、特殊フォルダーリダイレクトが機能することも防止します。この状況は、特殊フォルダーリダイレクトがユーザーデバイスと対話する必要があるために発生します。

この設定をポリシーに追加するときは、**クライアント固定ドライブ**設定が存在し、「許可」に設定されていることを確認してください。

ファイル転送ポリシー

デフォルトでは、ファイル転送は有効になっています。これらのポリシーを変更するには、Web Studioを使用し、**ユーザー設定 - ICA\ファイルリダイレクト**の下にあります。ファイル転送ポリシーを使用する際は、以下を考慮してください。

- **Chrome OS/HTML5向けCitrix Workspaceアプリのファイル転送** - ユーザーがCitrix Virtual Apps and Desktopsセッションとデバイス間でファイルを転送できるようにするか、または転送できないようにします。

- **Chrome OS/HTML5向けCitrix Workspaceアプリのファイルアップロード** - ユーザーがデバイスからCitrix Virtual Apps and Desktopsセッションにファイルをアップロードできるようにするか、またはアップロードできないようにします。
- **Chrome OS/HTML5向けCitrix Workspaceアプリのファイルダウンロード** - ユーザーがCitrix Virtual Apps and Desktopsセッションからデバイスにファイルをダウンロードできるようにするか、またはダウンロードできないようにします。

> **注:**
>
> ファイル転送ポリシーは、HTML5向けCitrix WorkspaceアプリおよびChrome OS向けCitrix Workspaceアプリにのみ適用されます。

非同期書き込みの使用

この設定は、非同期ディスク書き込みを有効または無効にします。

デフォルトでは、非同期書き込みは無効になっています。

非同期ディスク書き込みは、WAN経由でのファイル転送速度やクライアントディスクへの書き込み速度を向上させることができます。WANは通常、比較的高帯域幅で高遅延が特徴です。ただし、接続またはディスクに障害が発生した場合、書き込み中のクライアントファイルが未定義の状態になる可能性があります。この未定義の状態が発生すると、影響を受けるファイルについてポップアップウィンドウでユーザーに通知されます。ユーザーは、再接続時またはディスク障害が修正されたときに中断されたファイル転送を再開するなどの修復措置を講じることができます。

Citrix®は、リモート接続が必要で、良好なファイルアクセス速度を持ち、接続またはディスク障害が発生した場合に失われたファイルやデータを容易に回復できるユーザーに対してのみ、非同期ディスク書き込みを有効にすることを推奨します。

この設定をポリシーに追加する際は、**クライアントドライブリダイレクト**設定が存在し、「許可」に設定されていることを確認してください。この設定が無効になっている場合、非同期書き込みは行われません。

グラフィックスポリシー設定

グラフィックスセクションには、ユーザーセッションでの画像の処理方法を制御するためのポリシー設定が含まれています。

視覚的にロスレスな圧縮を許可する

この設定により、グラフィックスで真のロスレス圧縮の代わりに視覚的にロスレスな圧縮を使用できます。視覚的にロスレスな圧縮は、真のロスレス圧縮よりもパフォーマンスが向上しますが、目視では気づかない程度のわずかな損失があります。この設定は、視覚品質設定の値の使用方法を変更します。

デフォルトでは、この設定は無効になっています。

グラフィックスステータスインジケーター

この設定は、グラフィックスステータスインジケーターをユーザーセッションで実行するように構成します。このツールを使用すると、ユーザーはアクティブなグラフィックスモードに関する情報を確認できます。この情報には、ビデオコーデック、ハードウェアエンコード、画質、セッションで使用中のモニターに関する詳細が含まれます。グラフィックスステータスインジケーターを使用すると、ユーザーはピクセルパーフェクトモードを有効または無効にすることもできます。

Citrix Virtual Apps and Desktops™ 2103以降のリリースには、ユーザーが画質と対話性の適切なバランスを見つけるのに役立つ画質スライダーが含まれています。

Citrix Virtual Apps and Desktops 2109以降のリリースには、グラフィックスステータスインジケーターを使用して起動されるユーザーインターフェイスを介して仮想ディスプレイレイアウトを構成する機能が含まれています。

グラフィックスステータスインジケーターは、以前のバージョンのロスレスインジケーターツールに代わるものです。このポリシーは、Citrix Virtual Apps and Desktopsバージョン7.16から1809までででロスレスインジケーターを有効にします。

画面共有

この設定により、ユーザーは画面コンテンツ、キーボード、マウスを含むセッションを他のユーザーと共有できるようになります。

デフォルトでは、この設定は無効になっています。

VDAは、TCPポート範囲のポートを使用してデータを交換しようとします。最も低いポートから開始し、後続の接続ごとにインクリメントします。このポートは、インバウンドトラフィックとアウトバウンドトラフィックの両方を処理します。

デフォルトでは、TCPポート範囲は52525～52625に設定されています。

画面共有に使用されるポートは、ファイアウォールの例外リストに追加する必要があります。このオプションは、VDAのインストール時にチェックボックスとして表示されます。既定では、このオプションはチェックされていません。

ディスプレイメモリ制限

この設定は、セッションの最大ビデオバッファサイズをキロバイト単位で指定します。

VDAバージョン2308以前の場合、128から4,194,303までのキロバイト単位の量を指定します。指定しない場合、設定は既定で65,536キロバイトになります。

VDAバージョン2311以降の場合、任意のキロバイト単位の量を指定します。指定しない場合、または0として指定した場合、設定は既定で最大値なしになります。

> **注:**
>
> VDAバージョン2311以降の場合、Citrix®は、この設定を既定のままにすることをお勧めします。

> 接続に高解像度と複数のモニターを使用すると、より多くのメモリが必要になります。HDX™ は各セッションに必要なディスプレイメモリの量のみを割り当てるため、常に環境内の構成の上位層に基づいて必要なビデオメモリの量を計算してください。したがって、一部のユーザーのみがデフォルトよりも多くを必要とする場合でも、ディスプレイメモリ制限を増やすことによるスケーラビリティへの悪影響はありません。

必要なビデオメモリの量は、次の式を使用して計算されます。

合計ビデオメモリ = ((32 / 8) x Σ)

例1

次の例では、2 台のモニターを使用するセッションを想定します。1 台は解像度 1920x1080、もう 1 台は解像度 1280x720 です。

1. 解像度の積の合計を計算します。
   - (1080 x 1920) + (720 x 1280)
   - = 2073600 + 921600
   - = 2995200
2. 合計ビデオメモリを計算:
   - ((32 / 8) x 2995200)
   - = (4 x 2995200)
   - = 11,980,800バイトまたは11,700キロバイト

この例では、これら2つのモニター構成を持つセッションをサポートするために、11,700キロバイトのビデオメモリが必要になります。

例2

4Kモニターを4台使用する場合、上記の式を使用すると、これらのセッションには最低129,600キロバイトのビデオメモリが必要になります。

どちらの例でも、VDAバージョン2311以降を使用している場合、Citrixはディスプレイメモリ制限をデフォルトのままにすることを推奨します。

表示モードの劣化優先度

> **注：**
>
> Virtual Delivery Agent 7.xの場合、このポリシー設定は、Legacy graphics modeポリシー設定が有効になっている場合にのみ適用されます。

> セッションの表示メモリ制限に達した場合、この設定は、色深度と解像度のどちらが先に劣化するかを指定します。

デフォルトでは、色深度が先に劣化します。

セッションメモリ制限に達すると、表示される画像の品質を低下させることができます。この品質は、色深度と解像度のどちらを先に劣化させるかを選択することで低下させることができます。色深度が先に劣化する場合、表示される画像はより少ない色を使用します。解像度が先に劣化する場合、表示される画像は1インチあたりのピクセル数が少なくなります。

カラー深度または解像度が低下した場合にユーザーに通知するには、「ディスプレイモードが低下したときにユーザーに通知」設定を構成します。

動的ウィンドウプレビュー

この設定は、シームレスウィンドウの表示を次の場所で有効または無効にします。

- フリップ-
- フリップ 3D
- タスクバープレビュー
- Windows ピーク

WINDOWS AEROプレビューオプション	説明
タスクバープレビュー	ユーザーがウィンドウのタスクバーアイコンにカーソルを合わせると、そのウィンドウの画像がタスクバーの上に表示されます。
Windows ピーク	ユーザーがタスクバープレビュー画像にカーソルを合わせると、ウィンドウのフルサイズの画像が画面に表示されます。
フリップ	ユーザーがALT+TABを押すと、開いている各ウィンドウの小さなプレビューアイコンが表示されます。
フリップ 3D	ユーザーがTAB+Windowsロゴキーを押すと、開いているウィンドウの大きな画像が画面にカスケード表示されます。

デフォルトでは、この設定は有効になっています。

画像キャッシュ

> **注：**
>
> Virtual Delivery Agent 7.xの場合、このポリシー設定は、Legacy graphics modeポリシー設定が有効になっている場合にのみ適用されます。

この設定は、セッション内の画像のセクションのキャッシュと取得を有効または無効にします。画像をセクションにキャッシュし、必要に応じてこれらのセクションを取得することで、次のことが可能になります。

- ユーザーデバイスでのスクロールがよりスムーズになる
- ユーザーデバイスのネットワーク経由で送信されるデータ量を削減する
- ユーザーデバイスで必要な処理を削減する

デフォルトでは、画像キャッシュ設定は有効になっています。

> **注：**

> 画像キャッシュ設定は、画像がどのようにキャッシュされ、取得されるかを制御します。この設定は、画像がキャッシュされるかどうかを制御するものではありません。画像は、Legacy graphics mode設定が有効になっている場合にキャッシュされます。

レガシーグラフィックモード - サポートされていません。下位互換性のためのみ

> **重要：**

> このリリースでは、レガシーグラフィックモードとデスクトップコンポジションリダイレクト (DCR) はサポートされていません。このポリシーは、XenApp 7.15 LTSR、XenDesktop 7.15 LTSR、およびWindows 7とWindows 2008 R2を使用する以前のVDAリリースとの下位互換性のためだけに含められています。

> この設定は、リッチグラフィックエクスペリエンスを無効にします。この設定を使用して、レガシーグラフィックエクスペリエンスに戻し、WANまたはモバイル接続での帯域幅消費を削減します。XenAppおよびXenDesktop 7.13で導入された帯域幅削減により、このモードは廃止されました。

デフォルトでは、この設定は無効になっており、ユーザーにはリッチグラフィックエクスペリエンスが提供されます。

レガシーグラフィックモードは以下でサポートされています。

- ウィンドウズ 7
- ウィンドウズ サーバー 2008 R2 VDA.

レガシーグラフィックモードは以下ではサポートされていません。

- Windows 8.xおよび10
- Windows Server 2012、2012 R2、および2016。

XenAppおよびXenDesktop 7.6 FP3以降でのグラフィックモードとポリシーの最適化について詳しくは、CTX202687を参照してください。

許可される最大色深度

> **注：**

> Virtual Delivery Agent 7.xの場合、このポリシー設定は、レガシーグラフィックモードのポリシー設定が有効になっている場合にのみ適用されます。

> この設定は、セッションで許可される最大色深度を指定します。

デフォルトでは、許可される最大色深度は1ピクセルあたり32ビットです。

この設定は、Thinwireドライバーと接続にのみ適用されます。プライマリディスプレイドライバーとして非ThinWireドライバーを使用するVDAには適用されません。これらのVDAは、プライマリディスプレイドライバーとしてWindows Display Driver Model (WDDM) ドライバーを使用するVDAです。Windows 8などのWDDMドライバーをプライマリディスプレイドライバーとして使用するシングルセッションOS VDAの場合、この設定は効果がありません。Windows Server 2019などのWDDMドライバーを使用するWindowsマルチセッションOS VDAの場合、この設定によりユーザーがVDAに接続できなくなる可能性があります。

高い色深度を設定すると、より多くのメモリが必要になります。メモリ制限に達したときに色深度を低下させるには、**表示モードの低下設定**を構成します。色深度が低下すると、表示される画像はより少ない色を使用します。

表示モードが低下したときにユーザーに通知する

> **注:**

> Virtual Delivery Agent 7.xの場合、このポリシー設定は、レガシーグラフィックモードポリシー設定が有効になっている場合にのみ適用されます。

> この設定は、色深度または解像度が低下したときに、ユーザーに簡単な説明を表示します。

デフォルトでは、ユーザーへの通知は無効になっています。

3Dグラフィックワークロード向けに最適化する

この設定は、グラフィックを多用するワークロードに最適なデフォルト設定を構成します。グラフィックを多用するアプリケーションに重点を置くユーザーに対して、この設定を有効にします。このポリシーは、セッションでGPUが利用可能な場合にのみ適用してください。このポリシーによって設定されたデフォルト設定を明示的に上書きする他の設定は、優先されます。

デフォルトでは、3Dグラフィックワークロード向けに最適化する設定は無効になっています。

キューイングとトッシング

> **注:**
>
> Virtual Delivery Agent 7.xの場合、このポリシー設定は、レガシーグラフィックモードポリシー設定が有効になっている場合にのみ適用されます。

> この設定は、別の画像に置き換えられたキュー内の画像を破棄します。

デフォルトでは、キューイングとトッシングは有効になっています。

この設定は、グラフィックがユーザーデバイスに送信される際の応答を改善します。この設定を構成すると、フレームがドロップされるため、アニメーションが途切れることがあります。

圧縮にビデオコーデックを使用する

エンドポイントでビデオデコードが利用可能な場合に、ビデオコーデックを使用してグラフィックを圧縮できるようにします。**画面全体**が選択されている場合、ビデオコーデックはすべてのデフォルトコーデックとして適用されます。**アクティブに変化する領域**が選択されている場合、ビデオコーデックは画面上で常に変化する領域に使用され、その他のデータは静止画圧縮とビットマップキャッシュを使用します。エンドポイントでビデオデコードが利用できない場合、または**ビデオコーデックを使用しない**を指定した場合は、静止画圧縮とビットマップキャッシュの組み合わせが使用されます。**推奨される場合に使用**が選択されている場合、システムはさまざまな要因に基づいて選択します。選択方法が強化されるにつれて、バージョン間で結果が異なる場合があります。

推奨される場合に使用を選択すると、システムが現在のシナリオに最適な設定を選択するために最善を尽くすことができます。

画面全体を選択すると、特にサーバーレンダリングされたビデオや3Dグラフィックを多用する場合に、ユーザーエクスペリエンスと帯域幅の向上に最適化されます。

アクティブに変化する領域を選択すると、特に低帯域幅でのビデオパフォーマンスが向上するように最適化され、静的コンテンツやゆっくり変化するコンテンツのスケーラビリティも維持されます。この設定は、マルチモニター展開でサポートされています。

ビデオコーデックを使用しないを選択すると、サーバーのCPU負荷、および多数のサーバーレンダリングされたビデオやその他のグラフィックを多用するアプリケーションがない場合に最適化されます。

デフォルトは「**推奨時に使用**」です。

ビデオにハードウェアエンコードを使用する

この設定により、利用可能な場合にグラフィックハードウェアを使用して、ビデオコーデックで画面要素を圧縮できます。そのようなハードウェアが利用できない場合、VDAはソフトウェアビデオコーデックを使用したCPUベースのエンコードにフォールバックします。

このポリシー設定のデフォルトオプションは「**有効**」です。

複数のモニターがサポートされています。

ビデオデコードをサポートする任意のCitrix Workspace™アプリは、ハードウェアエンコードで使用できます。

NVIDIA

NVIDIA GRID GPUの場合、マルチセッションOSおよびシングルセッションOS用のVDAでハードウェアエンコードがサポートされています。

NVIDIA GPUはNVENCハードウェアエンコードをサポートしている必要があります。サポートされているGPUのリストについては、NVIDIAビデオコーデックSDKを参照してください。

NVIDIA GRIDにはドライバーバージョン3.1以降が必要です。NVIDIA Quadroにはドライバーバージョン362.56以降が必要です。CitrixはNVIDIA Release R361ブランチのドライバーを推奨しています。

ロスレステキストはNVENCハードウェアエンコードと互換性がありません。ロスレステキストを有効にした場合、ロスレステキストがNVENCハードウェアエンコードよりも優先されます。

アクティブに変化する領域に対するH.264ハードウェアコーデックの選択的な使用がサポートされています。

視覚的にロスレス（YUV 4:4:4）圧縮がサポートされています。視覚的にロスレス（グラフィックポリシー設定、視覚的にロスレス圧縮を許可）には、Citrix Workspaceアプリ1808以降またはCitrix Receiver for Windows 4.5以降が必要です。

インテル

Intel Iris Proグラフィックプロセッサの場合、ハードウェアエンコードはシングルセッションOSおよびマルチセッションOS用のVDAでサポートされています。

Intel Broadwellプロセッサファミリー以降のIntel Iris Proグラフィックプロセッサがサポートされています。Intel Remote Displays SDKバージョン1.0が必要であり、IntelのWebサイトからダウンロードできます: Remote Displays SDK。

ロスレステキストは、ビデオコーデックポリシーが画面全体に設定され、**3Dグラフィックワークロード向けに最適化**ポリシーが無効になっている場合にのみサポートされます。

視覚的にロスレス（YUV 4:4:4）はサポートされていません。

Intelエンコーダーは、最大8つのエンコードセッション（たとえば、1人のユーザーが8つのモニターを使用するか、8人のユーザーがそれぞれ1つのモニターを使用する）で良好なユーザーエクスペリエンスを提供します。8つ以上のエンコードセッションが必要な場合は、仮想マシンが接続するモニターの数を確認してください。管理者は、良好なユーザーエクスペリエンスを維持するために、このポリシー設定をユーザーごとまたはマシンごとに構成するかどうかを決定します。

AMD

AMDの場合、ハードウェアエンコードはシングルセッションOS用のVDAでサポートされています。

AMD GPUはRapidFire SDKをサポートする必要があります。例えば、AMD Radeon ProまたはFirePro GPUなどです。

エンコードを機能させるには、最新のAMDドライバーをインストールしてください。これらのドライバーは`<https://www.amd.com/en/support>`からダウンロードできます。

ロスレステキストはAMDハードウェアエンコードと互換性がありません。ロスレステキストを有効にした場合、ロスレステキストがAMDハードウェアエンコードよりも優先されます。

活発に変化する領域向けのH.264ハードウェアコーデックの選択的な使用がサポートされています。

キャッシュポリシー設定

このセクションには、クライアント接続の帯域幅が制限されている場合に、ユーザーデバイスで画像データをキャッシュできるようにするポリシー設定が含まれています。

永続キャッシュしきい値

注: Virtual Delivery Agent 7.xの場合、このポリシー設定は、**レガシーグラフィックモード**ポリシー設定が有効になっている場合にのみ適用されます。

この設定は、ユーザーデバイスのハードドライブにビットマップをキャッシュし、以前のセッションからの大きく頻繁に使用される画像を再利用できるようにします。

デフォルトでは、しきい値は1秒あたり3000000ビットです。

しきい値は、永続キャッシュ機能が有効になる下限を表します。たとえば、デフォルト値を使用すると、帯域幅が3000000 bpsを下回ったときに、ビットマップがユーザーデバイスのハードドライブにキャッシュされます。

キープアライブ ポリシー設定

キープアライブセクションには、ICA®キープアライブメッセージを管理するためのポリシー設定が含まれています。

ICA キープアライブ タイムアウト

この設定は、連続するICAキープアライブメッセージ間の秒数を指定します。

デフォルトでは、キープアライブメッセージ間の間隔は60秒です。

ICAキープアライブメッセージを送信する1～3600秒の間隔を指定します。ネットワーク監視ソフトウェアが非アクティブな接続を閉じる役割を担っている場合は、この設定を構成しないでください。

ICA キープアライブメッセージ

この設定は、定期的なICAキープアライブメッセージの送信を有効または無効にします。

デフォルトでは、キープアライブメッセージは送信されません。

この設定を有効にすると、切断された接続が切断されるのを防ぎます。サーバーがアクティビティを検出しない場合、この設定により、Remote Desktop Services (RDS) がセッションを切断するのを防ぎます。サーバーは数秒ごとにキープアライブメッセージを送信し、セッションがアクティブであるかどうかを検出します。セッションがアクティブでなくなった場合、サーバーはそのセッションを切断済みとしてマークします。

セッションの信頼性を使用している場合、ICAキープアライブは機能しません。ICAキープアライブは、セッションの信頼性を使用していない接続に対してのみ構成してください。

関連するポリシー設定: セッションの信頼性接続。

ローカルアプリアクセス ポリシー設定

「**ローカルアプリアクセス**」セクションには、ユーザーのローカルにインストールされたアプリケーションをホストされたアプリケーションと連携させるポリシー設定が含まれています。これらのポリシー設定は、ホストされたデスクトップ環境での統合を管理します。

ローカルアプリアクセスを許可

この設定は、ユーザーのローカルにインストールされたアプリケーションとホストされたアプリケーションとの統合を許可または禁止します。これらのポリシー設定は、ホストされたデスクトップ環境での統合を管理します。

ユーザーがローカルにインストールされたアプリケーションを起動すると、そのアプリケーションは実際にはローカルで実行されているにもかかわらず、仮想デスクトップ内で実行されているように見えます。

ローカルアプリアクセスを許可ポリシー設定を**有効**にすると、ブラウザコンテンツリダイレクトはサポートされず、デスクトップセッションにクライアント側の通知領域のバッテリーステータスは表示されません。

デフォルトでは、**ローカルアプリアクセスを許可**は禁止されています。

URLリダイレクトブロックリスト

この設定は、ローカルのWebブラウザにリダイレクトされて起動されるWebサイトを指定します。これらのWebサイトには、次のものが含まれる場合があります。

- msn.comやnewsgoogle.comなど、ロケール情報を必要とするWebサイト
- ユーザーデバイスでより適切にレンダリングされるリッチメディアコンテンツを含むWebサイト。

デフォルトでは、サイトは指定されていません。

URLリダイレクト許可リスト

この設定は、起動された環境でレンダリングされるWebサイトを指定します。

デフォルトでは、サイトは指定されていません。

モバイルエクスペリエンスポリシー設定

「**モバイルエクスペリエンス**」セクションには、Citrix Mobility Packを処理するためのポリシー設定が含まれています。

キーボードの自動表示

この設定は、モバイルデバイスの画面でのキーボードの自動表示を有効または無効にします。

デフォルトでは、キーボードの自動表示は無効になっています。

タッチ最適化デスクトップの起動

この設定は無効になっており、Windows 10またはWindows Server 2016マシンでは使用できません。

この設定は、Citrix Workspace™アプリの全体的なインターフェイス動作を決定します。この設定により、タブレットデバイス向けに最適化されたタッチフレンドリーなインターフェイスの使用を許可または禁止します。

デフォルトでは、タッチフレンドリーなインターフェイスが使用されます。

Windowsインターフェイスのみを使用するには、このポリシー設定を「禁止」に設定します。

コンボボックスのリモート化

この設定は、モバイルデバイスのセッションで表示できるコンボボックスの種類を決定します。デバイスネイティブのコンボボックスコントロールを表示するには、このポリシー設定を「許可」に設定します。この設定が許可されている場合、ユーザーはCitrix Workspace app for iOSセッション設定を変更して、Windowsコンボボックスを使用できます。

デフォルトでは、**コンボボックスのリモート化**機能は禁止されています。

マルチメディアポリシー設定

「**マルチメディア**」セクションには、ユーザーセッションにおけるストリーミングHTML5およびWindowsのオーディオとビデオを管理するためのポリシー設定が含まれています。

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

マルチメディアポリシー

デフォルトでは、Delivery Controller™で設定されたすべてのマルチメディアポリシーは、以下のレジストリに保存されます。

マシンポリシー:

HKEY_LOCAL_MACHINE\Software\Policies\Citrix\MultimediaPolicies

ユーザーポリシー:

HKEY_LOCAL_MACHINE\Software\Policies\Citrix{ユーザー セッション ID}\User\MultimediaPolicies

現在のユーザーセッションIDを見つけるには、Windowsコマンドラインで**qwinsta**コマンドを発行します。

HTML5ビデオリダイレクト

Citrix Virtual Apps and Desktops™サーバーがHTML5マルチメディアWebコンテンツをユーザーに配信する方法を制御し、最適化します。

デフォルトでは、この設定は無効になっています。

HTML5リダイレクトのグラフィック画像(/en-us/citrix-virtual-apps-desktops/2503/media/redirection1a.png)

このリリースでは、この機能は管理対象のWebページでのみ利用可能です。HTML5マルチメディアコンテンツ（社内トレーニングサイトのビデオなど）が利用可能なWebページにJavaScriptを追加する必要があります。

HTML5ビデオリダイレクトを構成するには:

1. VDAインストール環境の%Program Files%/Citrix/ICA Service/HTML5 Video Redirectionからファイル**HdxVideo.js**を社内Webページの場所にコピーします。
2. この行をWebページに挿入します（Webページに他のスクリプトがある場合は、それらのスクリプトの前に**HdxVideo.js**を含めます）。 `<script src="HdxVideo.js" type="text/javascript"\></script>`

注： HdxVideo.jsがWebページと同じ場所にない場合は、**src**属性を使用してそのフルパスを指定します。

JavaScriptが管理対象のWebページに追加されておらず、ユーザーがHTML5ビデオを再生する場合を想定します。この場合、Citrix Virtual Apps and Desktopsはサーバー側レンダリングにデフォルト設定されます。

HTML5ビデオのリダイレクトを機能させるには、***Windows Mediaリダイレクト***を許可します。このポリシーは、Server Fetch Client Renderには必須であり、Client Side Fetchingには必要です。Client Side Fetchingは、*Windows Mediaクライアント側コンテンツフェッチ*も許可されている必要があります。

Microsoft Edgeはこの機能をサポートしていません。

HdxVideo.jsは、ブラウザのHTML5プレーヤーコントロールを独自のコントロールに置き換えます。特定のWebサイトでHTML5ビデオリダイレクトポリシーが有効になっていることを確認するには、プレーヤーコントロールを**HTML5ビデオリダイレクト**ポリシーが禁止されているシナリオと比較します。

（ポリシーが許可されている場合のCitrixカスタムコントロール）



（ポリシーが禁止されているか、構成されていない場合のネイティブWebページコントロール）



以下のビデオコントロールがサポートされています：

- 再生
- 一時停止
- シーク
- 繰り返し
- オーディオ
- 全画面表示

HTML5ビデオリダイレクトテストページを表示できます。

TLS、HTML5ビデオリダイレクト、およびブラウザーコンテンツリダイレクト

HTML5ビデオリダイレクトを使用して、次のことができます。

- HTTPS Webサイトからのビデオのリダイレクト
- または
- Webサイト全体をリダイレクトするためのブラウザーコンテンツリダイレクト

これらのWebサイトに挿入されたJavaScriptは、VDAで実行されているCitrix HDX HTML5 Video Redirection Service (WebSocketService.exe) へのTLS接続を確立する必要があります。VDAの証明書ストアにあるCitrix HDX HTML5 Video Redirection Serviceは、次の目的で2つのカスタム証明書を生成します。

- ビデオのリダイレクトを実現する
- WebページのTLS整合性を維持する

HdxVideo.jsは、Secure WebSocketsを使用して、VDAで実行されているWebSocketService.exeと通信します。このプロセスはローカルシステムアカウントとして実行され、SSL終端とユーザーセッションマッピングを行います。

WebSocketService.exeは、127.0.0.1ポート9001でリッスンしています。

ビデオ品質の制限

この設定は、Windows Mediaにのみ適用され、HTML5には適用されません。**WAN経由のWindows Mediaマルチメディアリダイレクトの最適化**を有効にする必要があります。

この設定は、HDX™接続で許可される最大ビデオ品質レベルを指定します。設定すると、最大ビデオ品質は指定された値に制限され、環境内でマルチメディアのサービス品質 (QoS) が維持されます。

デフォルトでは、この設定は構成されていません。

許可される最大ビデオ品質レベルを制限するには、次のいずれかのオプションを選択します。

- 1080p/8.5Mbps
- 720p/4.0Mbps
- 480p/720Kbps
- 380p/400Kbps
- 240p/200Kbps

同じサーバーで複数のビデオを同時に再生すると、大量のリソースが消費され、サーバーのスケーラビリティに影響を与える可能性があります。

Microsoft Teams リダイレクト

この設定は、HDXテクノロジーに基づいてMicrosoft Teamsの最適化を有効にします。

このポリシーが有効で、サポートされているバージョンのCitrix Workspace™アプリを使用している場合、このレジストリキーはVDAで**1**に設定されます。Microsoft Teamsアプリケーションは、VDIモードでロードするためにこのキーを読み取ります。 レジストリキーを手動で設定する必要はありません。

HKEY_CURRENT_USER\Software\Citrix\HDXMediaStream

名前: MSTeamsRedirSupport

値: DWORD (1 - オン, 0 - オフ)

> **注:**

> Web Studioでポリシーが利用できない、Controllerの古いバージョン（例: バージョン7.15）でバージョン1906.2以降のVDAを使用している場合を考慮してください。この場合、HDX最適化はVDAでデフォルトで有効になっています。Workspaceアプリのバージョンが1907以降の場合、Microsoft Teamsは最適化モードで起動します。7.15 LTSR ControllerとCR VDAの混在に関する注意点については、Knowledge Centerの記事CTX205549を参照してください。

> この場合、特定のユーザーに対して機能を無効にするには、レジストリ設定を上書きできます。ユーザーの組織単位にログオンスクリプトを適用するグループポリシーを使用して、レジストリ設定を上書きします。

> デフォルトでは、Microsoft Teamsリダイレクトは有効になっています。

マルチメディア会議

この設定は、ビデオ会議アプリケーションによる最適化されたWebカメラリダイレクトテクノロジーの使用を許可または禁止します。

デフォルトでは、ビデオ会議のサポートは許可されています。

この設定をポリシーに追加する際は、**Windows Mediaリダイレクト**設定が存在し、**許可**（デフォルト）に設定されていることを確認してください。

マルチメディア会議を使用する場合は、次の条件が満たされていることを確認してください。

- マルチメディア会議に使用されるWebカメラ用のメーカー提供のドライバーがクライアントにインストールされていること。
- ビデオ会議セッションを開始する前に、Webカメラをユーザーデバイスに接続してください。サーバーは、一度に1つのインストールされたWebカメラのみを使用します。ユーザーデバイスに複数のWebカメラがインストールされている場合、サーバーは各Webカメラを順番に試行します。この試行は、ビデオ会議セッションが正常に作成されるまで続行されます。

汎用USBリダイレクトを使用してWebカメラをリダイレクトする場合、このポリシーは必要ありません。その場合は、WebカメラドライバーをVDAにインストールしてください。

WAN経由のWindows Mediaマルチメディアリダイレクトの最適化

この設定はWindows Mediaにのみ適用され、HTML5には適用されません。この設定により、以下が可能になります。

- リアルタイムマルチメディアトランスコーディング
- 劣化ネットワーク経由でのモバイルデバイスへのオーディオおよびビデオメディアストリーミングを許可
- WAN経由でWindows Mediaコンテンツが配信される方法を改善することで、ユーザーエクスペリエンスを向上させます。

デフォルトでは、WAN経由のWindows Mediaコンテンツの配信は最適化されています。

この設定をポリシーに追加する際は、**Windows Media Redirection**設定が存在し、**Allowed**に設定されていることを確認してください。

この設定が有効になっている場合、メディアストリーミングを可能にするために、必要に応じてリアルタイムのマルチメディアトランスコーディングが自動的に展開されます。また、極端なネットワーク条件下でもシームレスなユーザーエクスペリエンスを提供します。

WAN経由のWindows Mediaマルチメディアリダイレクトの最適化にGPUを使用

この設定はWindows Mediaにのみ適用され、Virtual Delivery Agent (VDA) 上のグラフィックス処理ユニット (GPU) でリアルタイムマルチメディアトランスコーディングを実行できるようにします。これにより、サーバーのスケーラビリティが向上します。GPUトランスコーディングは、VDAがハードウェアアクセラレーションに対応したGPUを搭載している場合にのみ利用可能です。それ以外の場合は、トランスコーディングはCPUにフォールバックします。

注: GPUトランスコーディングはNVIDIA GPUでのみサポートされています。

デフォルトでは、WAN経由のWindows Mediaコンテンツの配信を最適化するためにVDA上のGPUを使用することは禁止されています。

この設定をポリシーに追加する際は、以下の設定が存在し、Allowedに設定されていることを確認してください。

- **Windows Mediaリダイレクト**
- **WAN経由でのWindows Mediaマルチメディアリダイレクト設定の最適化**

Windows Mediaフォールバック防止

この設定は、ブラウザーコンテンツリダイレクト、HTML5、およびWindows Mediaに適用されます。HTML5をサポートするには、**HTML5ビデオリダイレクト**ポリシーを**許可**に設定します。

管理者は、**Windows Media フォールバック防止**ポリシー設定を使用して、ストリーミングコンテンツをユーザーに配信するために試行される方法を指定できます。

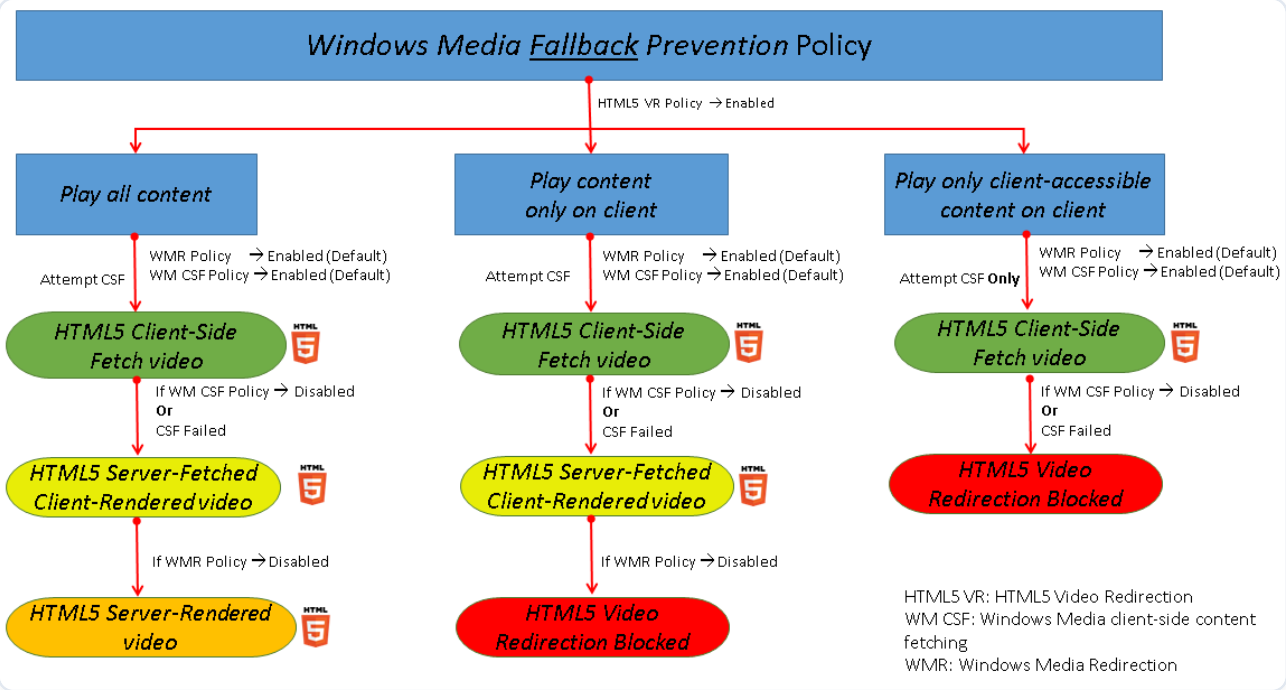
デフォルトでは、この設定は構成されていません。この設定が「未構成」に設定されている場合、動作は**すべてのコンテンツを再生**と同じになります。

この設定を構成するには、次のいずれかのオプションを選択します。

- **すべてのコンテンツを再生**。クライアント側でのコンテンツ取得を試行し、次にWindows Mediaリダイレクトを試行します。失敗した場合は、サーバーでコンテンツを再生します。
- **クライアントでのみすべてのコンテンツを再生**。クライアント側での取得を試行し、次にWindows Mediaリダイレクトを試行します。失敗した場合は、コンテンツは再生されません。
- **クライアントでクライアントがアクセス可能なコンテンツのみを再生**。クライアント側での取得のみを試行します。失敗した場合は、コンテンツは再生されません。

コンテンツが再生されない場合、プレーヤーウィンドウに次のエラーメッセージが表示されます（デフォルトの表示時間は5秒）。

「リソース不足のため、会社がビデオをブロックしました」



このエラーメッセージの表示時間は、VDA上の次のレジストリキーでカスタマイズできます。レジストリエントリが存在しない場合、表示時間はデフォルトで5秒になります。

レジストリパスは、VDAのアーキテクチャによって異なります。

`\HKLM\SOFTWARE\Wow6432Node\Citrix\HdxMediastream`

または

\HKLM\SOFTWARE\Citrix\HdxMediastream

レジストリキー：

名前: VideoLoadManagementErrDuration

種類: DWORD

範囲: 1 - DWORD制限まで（デフォルト = 5）

単位: 秒

Windows Mediaクライアント側コンテンツ取得

この設定はHTML5とWindows Mediaの両方に適用されます。この設定により、ユーザーデバイスは、XenAppまたはXenDesktop®ホストサーバーを介さずに、インターネットまたはイントラネット上のソースプロバイダーからマルチメディアファイルを直接ストリーミングできるようになります。

デフォルトでは、この設定は**許可**されています。この設定を許可すると、ネットワーク使用量とサーバーのスケーラビリティが向上します。この改善は、メディアに関する処理をホストサーバーからユーザーデバイスに移動することで実現されます。また、Microsoft DirectShowやMedia Foundationなどの高度なマルチメディアフレームワークがユーザーデバイスにインストールされているという要件もなくなります。ユーザーデバイスには、URLからファイルを再生する機能のみが必要です

この設定をポリシーに追加する場合は、**Windows Mediaリダイレクト**設定が存在し、**許可**に設定されていることを確認してください。**Windows Mediaリダイレクト**が無効になっている場合、ソースプロバイダーからユーザーデバイスへのマルチメディアファイルのストリーミングも無効になります。

Windows Mediaリダイレクト

この設定はHTML5とWindows Mediaの両方に適用され、サーバーがストリーミングオーディオとビデオをユーザーに配信する方法を制御および最適化します。

デフォルトでは、この設定は**許可**されています。HTML5の場合、ポリシー**HTML5ビデオのリダイレクト**が**禁止**されていると、この設定は有効になりません。

この設定が有効になっている場合、サーバーからレンダリングされるオーディオとビデオの品質は、ユーザーデバイスでローカルに再生されるオーディオとビデオに匹敵するレベルに向上します。サーバーはマルチメディアを元の圧縮形式でクライアントにストリーミングし、ユーザーデバイスがメディアを解凍してレンダリングできるようにします。

Windows Mediaリダイレクトは、Microsoft DirectShow、DirectX Media Objects (DMO)、およびMedia Foundationの標準に準拠するコーデックでエンコードされたマルチメディアファイルを最適化します。特定のマルチメディアファイルを再生するには、そのマルチメディアファイルのエンコード形式と互換性のあるコーデックがユーザーデバイスに存在する必要があります。

Citrix Workspaceアプリでは、デフォルトでオーディオが無効になっています。ユーザーがICA®セッションでマルチメディアアプリケーションを実行できるようにするには、オーディオをオンにするか、Citrix Workspaceアプリのインターフェイスでオーディオをオンにする権限をユーザーに付与します。

Windows Mediaリダイレクトを使用してメディアを再生したときの品質が、基本的なICA圧縮と通常のオーディオを使用してレンダリングした場合よりも悪い場合にのみ、**禁止**を選択してください。このような状況はまれですが、低帯域幅の条件下（例えば、キーフレームの頻度が低いメディアの場合）で発生する可能性があります。

Windows Mediaリダイレクトのバッファサイズ

この設定はレガシーであり、HTML5には適用されません。

この設定は、マルチメディアアクセラレーションのバッファサイズを1～10秒で指定します。

デフォルトでは、バッファサイズは5秒です。

Windows Mediaリダイレクトのバッファサイズの使用

この設定はレガシーであり、HTML5には適用されません。

この設定は、**Windows Media Redirection buffer size** 設定で指定されたバッファサイズの使用を有効または無効にします。

デフォルトでは、指定されたバッファサイズは使用されません。

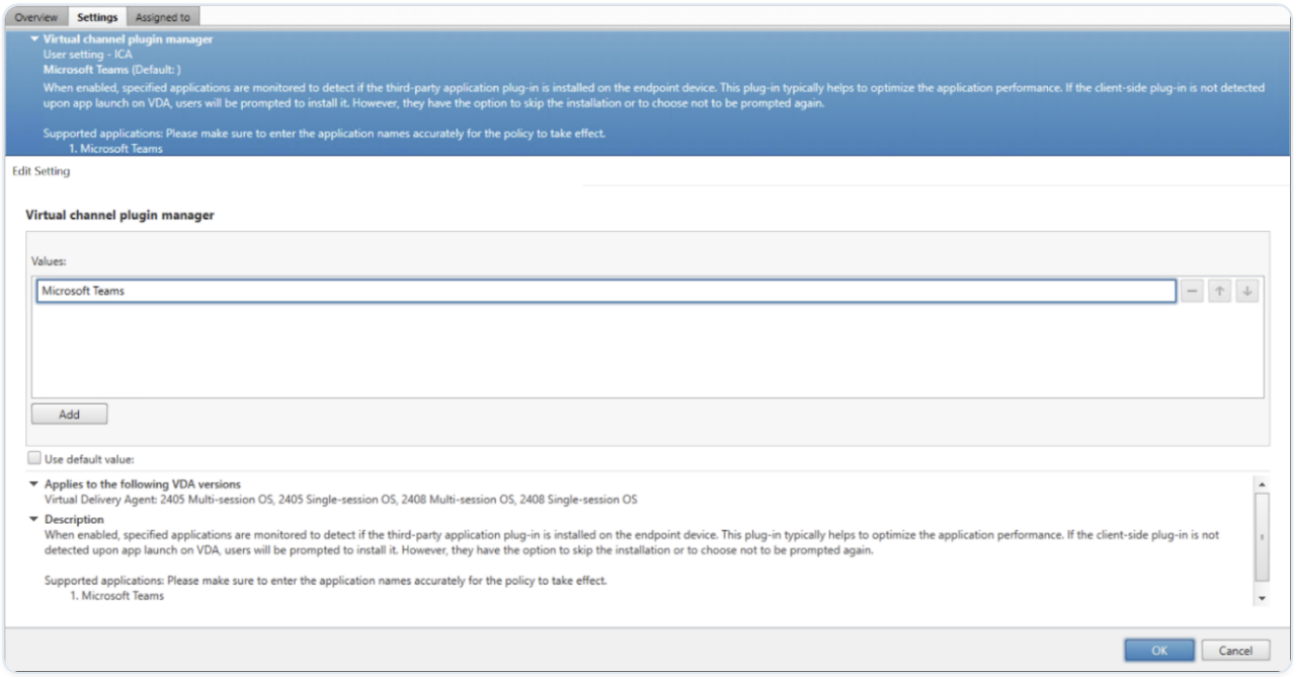
この設定が無効になっている場合、または**Windows Media Redirection buffer size** 設定が構成されていない場合、サーバーはデフォルトのバッファサイズ値（5秒）を使用します。

仮想チャネルプラグインマネージャーポリシー

仮想チャネルプラグインマネージャーセクションには、この機能を構成するためのポリシー設定が含まれています。

仮想チャネルプラグインマネージャーは、特定の指定されたアプリケーションのためにクライアントエンドポイント全体にプラグインを展開するように設計されています。プラグインマネージャーは、VDAで実行されている特定のアプリケーションを検出し、アプリケーションの実行時

に最高の体験を得るために、エンドポイントにプラグインをインストールするようユーザーに促します。



- 管理者は、ポリシーを使用して、エンドポイント全体にプラグインをインストールする必要があるアプリケーションを指定できます。
- アプリケーション名は、ポリシーの説明の「サポートされているアプリケーション」に記載されている名前と同じである必要があります。
- デフォルトでは、ポリシーは無効になっています。
- 現在サポートされているアプリケーション
    - 「マイクロソフト チームズ」
- 今後、さらに多くのアプリケーションがサポートされる予定です。

マルチストリーム接続ポリシー設定

マルチストリーム接続セクションには、セッション内の複数のICA®接続に対するQuality of Serviceの優先順位付けを管理するためのポリシー設定が含まれています。

> **注：**
>
> マルチストリーム接続ポリシーが有効になっている場合、MTU Discoveryはサポートされません。

UDP経由のオーディオ

この設定は、サーバー上でのUDP経由のオーディオを許可または禁止します。

デフォルトでは、サーバー上でのUDP経由のオーディオは許可されています。

有効にすると、この設定は、UDP経由のオーディオリアルタイムトランスポートを使用するように構成されたすべての接続をサポートするために、サーバー上でUDPポートを開きます。

オーディオUDPポート範囲

この設定は、Virtual Delivery Agent (VDA) が使用するポート番号の範囲（最小ポート番号、最大ポート番号）を指定します。この指定は、ユーザーデバイスとの間でオーディオパケットデータを交換するのに役立ちます。VDAは、ユーザーデバイスとの間でデータを交換するために、各UDPポートペアを、最小値から開始し、その後の試行ごとに2ずつ増やしながら使用しようとします。各ポートは、インバウンドトラフィックとアウトバウンドトラフィックの両方を処理します。

デフォルトでは、この範囲は16500,16509に設定されています。

マルチポートポリシー

この設定は、ICAトラフィックに使用するTCPポートを指定し、各ポートのネットワーク優先度を確立します。

デフォルトでは、プライマリポート（2598）は高優先度です。

ポートを構成する際、以下の優先度を割り当てることができます。

- **非常に高い:** ウェブカメラ会議などのリアルタイムアクティビティ向け
- **高い:** 画面、キーボード、マウスなどの対話型要素向け
- **中:** クライアントドライブマッピングなどのバルク処理向け
- **低い:** 印刷などのバックグラウンドアクティビティ向け

各ポートには一意の優先順位が必要です。たとえば、CGPポート1とCGPポート3の両方に「非常に高」の優先順位を割り当てることはできません。

ポートを優先順位付けから削除するには、ポート番号を0に設定します。プライマリポートを削除したり、その優先順位レベルを変更したりすることはできません。

この設定を構成するときは、サーバーを再起動してください。この設定は、**Multi-Stream computer** 設定ポリシー設定が有効になっている場合にのみ有効になります。

Multi-Streamコンピューター設定

この設定は、サーバー上でMulti-Streamを有効または無効にします。

デフォルトでは、Multi-Streamは無効になっています。Citrix SD-WAN™またはサードパーティ製ルーターを使用して目的のQuality of Serviceを実現する場合は、Multi-Streamコンピューターポリシー設定を構成してください。

Multi-Streamが有効になっている場合、Adaptive Transportの機能であるMTU Discoveryはサポートされません。

この設定を構成するときは、変更が有効になるようにサーバーを再起動してください。

> **重要:**
>
> このポリシー設定を、セッション全体の帯域幅制限などの帯域幅制限ポリシー設定と組み合わせて使用すると、予期しない結果が生じる可能性があります。この設定をポリシーに含める場合は、帯域幅制限設定が含まれていないことを確認してください。

Multi-Streamユーザー設定

この設定は、ユーザーデバイスでマルチストリームを有効または無効にします。

デフォルトでは、マルチストリームはすべてのユーザーに対して無効になっています。Citrix SD-WANまたはサードパーティ製ルーターを使用して目的のサービス品質を実現する場合は、マルチストリームユーザー設定を構成してください。

この設定は、**マルチストリームコンピューター**設定ポリシー設定が有効になっているホストでのみ有効になります。

> **重要:**
>
> このポリシー設定を、セッション全体の帯域幅制限などの帯域幅制限ポリシー設定と併用すると、予期しない結果が生じる可能性があります。この設定をポリシーに含める場合は、帯域幅制限設定を含めないようにしてください。

マルチストリーム仮想チャネル割り当て設定

この設定は、マルチストリームが使用されている場合に仮想チャネルが割り当てられるICAストリームを指定します。

これらの設定を構成しない場合、仮想チャネルはデフォルトのストリームに保持されます。仮想チャネルをICAストリームに割り当てるには、仮想チャネル名の横にある**ストリーム番号**リストから目的のストリーム番号（0、1、2、3）を選択します。

環境でカスタム仮想チャネルが使用されている場合は、**追加**をクリックし、**仮想チャネル**の下のテキストボックスに仮想チャネル名を指定し、その横にある**ストリーム番号**リストから目的のストリーム番号を選択します。指定する名前は、フレンドリ名ではなく、実際の仮想チャネル名である必要があります。たとえば、Citrix Browser AccelerationではなくCTXSBRです。

これらの設定は、マルチストリームコンピューター設定を有効にした場合にのみ有効になります。

デフォルトでは、仮想チャネルとそのストリーム割り当ては次のとおりです。

- AppFlow®: 2
- オーディオ: 0
- ブラウザコンテンツリダイレクト: 2
- クライアントCOMポートマッピング: 3
- クライアントドライブマッピング: 2
- クライアントプリンターマッピング: 3
- クリップボード: 2
- CTXDND: 1 (**注:** これは、Citrixセッションとローカルエンドポイント間でファイルをドラッグアンドドロップする機能をサポートします。)
- DVCプラグイン (DVCプラグインのフレンドリ名から自動生成された静的VC名、または管理者によって割り当てられたもの): 2
- エンドユーザーエクスペリエンス監視: 1
- ファイル転送 (HTML5 Receiver): 2
- 汎用データ転送: 2
- ICA制御: 1
- 入力メソッドエディター: 1
- レガシー クライアント プリンター マッピング (COM1): 1, 3
- レガシー クライアント プリンター マッピング (COM2): 2, 3
- レガシー クライアント プリンター マッピング (LPT1): 1, 3
- レガシー クライアント プリンター マッピング (LPT2): 2, 3

- ライセンス管理: 1
- Microsoft Teams/WebRTC リダイレクト: 1
- モバイルレシーバー: 1
- マルチタッチ: 1
- ポートフォワーディング: 2
- リモートオーディオおよびビデオ拡張機能 (RAVE): 2
- シームレス (透過ウィンドウ統合): 1
- センサーと位置情報: 1
- スマートカード: 1
- Thinwire グラフィックス: 1
- 透過UI統合/ログオンステータス: 2
- TWAIN リダイレクト: 2
- USB: 2
- ゼロ遅延フォントおよびキーボード: 2
- ゼロ遅延データチャネル: 2

仮想チャネルの割り当てと優先度について詳しくは、Knowledge Center の記事 CTX131001 を参照してください。

ポートリダイレクトポリシー設定

「**ポートリダイレクト**」セクションには、クライアントLPTおよびCOMポートマッピングのポリシー設定が含まれています。

Virtual Delivery Agentのバージョン**7.0より前**の場合、ポートリダイレクトを構成するには、以下のポリシー設定を使用します。VDAバージョン**7.0から7.8**の場合、これらの設定はレジストリを使用して構成します。「レジストリを使用したCOMポートおよびLPTポートリダイレクト設定の構成」を参照してください。VDAバージョン**7.9**の場合、以下のポリシー設定を使用します。

クライアントCOMポートの自動接続

この設定は、ユーザーがサイトにログオンしたときに、ユーザーデバイス上のCOMポートの自動接続を有効または無効にします。

デフォルトでは、クライアントCOMポートは自動的に接続されません。

クライアントLPTポートの自動接続

この設定は、ユーザーがサイトにログオンしたときに、ユーザーデバイス上のLPTポートの自動接続を有効または無効にします。

デフォルトでは、クライアントLPTポートは自動的に接続されません。

クライアントCOMポートリダイレクト

この設定は、ユーザーデバイス上のCOMポートへのアクセスを許可または禁止します。

デフォルトでは、COMポートリダイレクトは禁止されています。

関連するポリシー設定は次のとおりです。

- COMポートリダイレクトの帯域幅制限
- COMポートリダイレクトの帯域幅制限（パーセント）

クライアントLPTポートリダイレクト

この設定は、ユーザーデバイス上のLPTポートへのアクセスを許可または禁止します。

デフォルトでは、LPTポートリダイレクトは禁止されています。

LPTポートは、LPTポートに印刷ジョブを送信するレガシーアプリケーションでのみ使用されます。これらのポートは、ユーザーデバイス上の印刷オブジェクトに印刷ジョブを送信するレガシーアプリケーションでは使用されません。現在のほとんどのアプリケーションは、印刷ジョブをプリンターオブジェクトに送信できます。このポリシー設定は、LPTポートに印刷するレガシーアプリケーションをホストするサーバーにのみ必要です。

注: クライアントCOMポートリダイレクトは双方向ですが、LPTポートリダイレクトは出力のみであり、ICAセッション内では\\\client\LPT1および\\\client\LPT2に制限されます。

以下のポリシー設定は関連しています。

- LPTポートリダイレクト帯域幅制限
- LPTポートリダイレクト帯域幅制限パーセント

印刷ポリシー設定

印刷セクションには、クライアント印刷を管理するためのポリシー設定が含まれています。

クライアントプリンターリダイレクト

この設定は、ユーザーがセッションにログオンしたときに、クライアントプリンターがサーバーにマップされるかどうかを制御します。

デフォルトでは、クライアントプリンターのマッピングは許可されています。この設定が無効になっている場合、セッション用のPDFプリンターは自動作成されません。

関連するポリシー設定: クライアントプリンターの自動作成

デフォルトプリンター

この設定は、ユーザーデバイス上のデフォルトプリンターがセッション内でどのように確立されるかを指定します。

デフォルトでは、ユーザーの現在のプリンターがセッションのデフォルトプリンターとして使用されます。

デフォルトプリンターに現在のRemote Desktop ServicesまたはWindowsユーザープロファイル設定を使用するには、「ユーザーのデフォルトプリンターを調整しない」を選択します。このオプションを選択すると、デフォルトプリンターはプロファイルに保存されず、他のセッションまたはクライアントのプロパティに応じて変更されません。セッション内のデフォルトプリンターは、セッションで最初に自動作成されたプリンターであり、次のいずれかです。

- **コントロールパネル > デバイス**と**プリンター**でWindowsサーバーにローカルに追加された最初のプリンター。
- サーバーにローカルに追加されたプリンターがない場合、最初に自動作成されたプリンター。

このオプションを使用すると、プロファイル設定（近接印刷として知られています）を通じて、ユーザーに最も近いプリンターを提示できます。

プリンターの割り当て

この設定は、デフォルトプリンターとセッションプリンターの設定に代わるものです。個別のデフォルトプリンターとセッションプリンターの設定を使用して、サイト、大規模グループ、または組織単位の動作を構成します。**プリンターの割り当て**設定を使用して、多数のプリンターを複数のユーザーに割り当てます。

この設定は、一覧表示されたユーザーデバイス上のデフォルトプリンターがセッション内でどのように確立されるかを指定します。

デフォルトでは、ユーザーの現在のプリンターがセッションのデフォルトプリンターとして使用されます。

各ユーザーデバイスのセッションで自動作成されるネットワークプリンターも指定します。デフォルトでは、プリンターは指定されていません。

- デフォルトプリンターの値を設定する場合：

ユーザーデバイスの現在のデフォルトプリンターを使用するには、「Do not adjust」を選択します。

デフォルトプリンターに現在のRemote Desktop ServicesまたはWindowsユーザープロファイル設定を使用するには、「調整しない」を選択します。このオプションを選択した場合、デフォルトプリンターはプロファイルに保存されず、他のセッションまたはクライアントのプロパティに応じて変更されません。セッション内のデフォルトプリンターは、セッションで自動作成された最初のプリンターであり、次のいずれかです。

- **コントロールパネル > デバイスとプリンター**でWindowsサーバーにローカルに追加された最初のプリンター。
- サーバーにローカルに追加されたプリンターがない場合、最初の自動作成されたプリンター。

- **セッションプリンター値: プリンターを追加する**を設定する場合、自動作成したいプリンターのUNCパスを入力します。または、**参照**をクリックして、ネットワーク全体でプリンターを検索します。プリンターサーバーのFQDNまたはNetBIOS名を入力してプリンターを検索することもできます。詳細については、「セッションプリンター」を参照してください。プリンターを追加した後、ログオンごとに現在のセッションにカスタマイズされた設定を適用できます。

プリンター自動作成イベントログの優先設定

この設定は、プリンターの自動作成プロセス中にログに記録されるイベントを指定します。エラーや警告をログに記録しない、エラーのみをログに記録する、またはエラーと警告をログに記録するを選択できます。

デフォルトでは、エラーと警告がログに記録されます。

警告の例としては、プリンターのネイティブドライバーをインストールできず、代わりにユニバーサルプリントドライバーがインストールされるイベントがあります。このシナリオでユニバーサルプリントドライバーを使用するには、ユニバーサルプリントドライバーの使用設定を「ユニバーサル印刷のみを使用する」または「要求されたドライバーが利用できない場合のみユニバーサル印刷を使用する」に構成します。

セッションプリンター

この設定は、セッションで自動作成されるネットワークプリンターを指定します。ICA/HDXセッション内では、Citrix Print Managerサービス（CpSvc.exe）が、**セッションプリンター**ポリシー設定で指定された各ネットワークプリンターに対して、セッションログオン中にネットワークプリンター接続を作成します。セッションログオフ中にプリンターを削除します。デフォルトでは、プリンターは指定されていません。

「**Session Printer**」ポリシー設定では、ネットワークプリンターはWindows Print ServerまたはCitrix Universal™ Print Serverに配置できます。

- **Windows Print Server:** 1つ以上のネットワークプリンターを共有します。また、ネットワークプリンターを使用するために必要なネイティブプリンタードライバーも備えています。
- **Universal Print Server:** Citrix Universal Print Serverソフトウェアがインストールされている Windows Print Serverです。

Windows Print Serverを使用する場合、Citrix Print Managerサービスはネイティブプリンタードライバーを使用してネットワークプリンター接続を作成します。Citrix Virtual Apps™サーバーには、ネイティブプリンタードライバーがインストールされている必要があります。

Citrix Universal Print Serverを使用する場合、Citrix Print Managerサービスは、ネイティブプリンタードライバー、Citrix Universal Printer Driver、またはCitrix Universal XPS Printer Driverのいずれかを使用してネットワークプリンター接続を作成します。使用するドライバーは、Universal Print Driverの使用ポリシー設定によって制御されます。

すべてのWindowsプリンタードライバーは現在、v3またはv4ドライバーバージョンのいずれかに分類されます。詳細については、「Microsoft V3およびV4プリンタードライバーアーキテクチャのサポート」を参照してください。

セッションプリンターを追加し、それらがセッションに表示されることを確認するには、次の手順を実行します。

1. Web Studioにサインインし、左ペインで**Policies**を選択し、**Policies**タブをクリックします。
2. **Session printers**ポリシーを選択し、**Edit**をクリックします。
3. **Edit Setting**ページで、**Use default value**チェックボックスをオフにし、**Add**をクリックして次の手順でプリンターを追加します。

    a. プリンターのUNCパスを`\\<FQDN of the printer server>\<printer name>.`の形式で入力します。または、**Browse**をクリックしてネットワーク全体からプリンターを検索します。プリンターサーバーのFQDNまたはNetBIOS名を入力してプリンターを検索することもできます。

    > **注:**
    >
    > **Browse**を使用して特定のプリンターを検索できるようにするには、プリンターを構成する際に、**Printer Settings > Printer Properties > Sharing**の下にある**List in the directory**オプションが選択されていることを確認してください。

b. デフォルトでは、プリンターサーバーを閲覧するためにユーザー名とパスワードが使用されます。異なるドメイン資格情報が必要な場合は、**Use different domain credentials to browse**を選択し、必要なユーザー名とパスワードを入力して、**Browse**をクリックします。

c. **Done**をクリックします。

4. ポリシーが設定された後、公開されたアプリケーションにセッションプリンターが表示されない場合があります。この問題は、Citrix Virtual Appsサーバーにプリンタードライバーがないか、ポリシーが作成されているが有効になっていないために発生する可能性があります。

> **注:**
>
> セッションプリンターがネイティブプリンタードライバーを必要とし、そのネイティブプリンタードライバーがVDAにインストールされていない場合、セッションプリンターはセッション内に作成されない可能性があります。

5. 公開されたデスクトップを起動し、 **>** でセッションプリンターを手動で追加します。
6. これが失敗した場合は、Citrix Virtual Apps サーバーとプリントサーバー間の通信を調査します。RDP を使用してテストを実行することを検討してください。

プリンターが作成されるのを待つ

Delivery Controllerのポリシーを使用して、Citrix Virtual Desktopsでこの機能を有効にします。

プリンターが作成されるまで待機 (サーバーデスクトップ):

この設定により、クライアントリダイレクトされたプリンターが自動作成されるように、セッションへの接続に遅延を設けることができます。

デフォルトでは、接続遅延は発生しません。

プリンターが作成されるまで待機 (Citrix Virtual Apps):

次のPowerShellコマンドレットを実行すると、マルチセッションホストで実行されている仮想アプリへの接続に遅延を設けることができ、アプリケーションが開かれる前にクライアントリダイレクトされたプリンターが自動作成されるようになります。

```
Set-BrokerApplication -Name <VirtualAppName> -WaitForPrinterCreation $true
```

デフォルトでは、接続遅延は発生しません。

クライアントプリンターポリシー設定

クライアントプリンターセクションには、クライアントプリンターのポリシー設定が含まれます。これには、クライアントプリンターの自動作成、プリンタープロパティの保持、およびプリントサーバーへの接続に関する設定が含まれます。

クライアントプリンターの自動作成

この設定は、自動作成されるクライアントプリンターを指定します。この設定は、デフォルトのクライアントプリンター自動作成設定を上書きします。

デフォルトでは、すべてのクライアントプリンターが自動作成されます。

この設定は、**クライアントプリンターリダイレクト**設定が存在し、**許可**に設定されている場合にのみ有効になります。

この設定をポリシーに追加する際は、オプションを選択してください。

- **すべてのクライアントプリンターを自動作成**は、ユーザーデバイス上のすべてのプリンターを自動的に作成します。
- **クライアントのデフォルトプリンターのみを自動作成**は、ユーザーデバイスでデフォルトプリンターとして選択されているプリンターのみを自動的に作成します。
- **ローカル（非ネットワーク）クライアントプリンターのみを自動作成**は、LPT、COM、USB、TCP/IP、またはその他のローカルポートを介してユーザーデバイスに直接接続されているプリンターのみを自動的に作成します。
- **クライアントプリンターを自動作成しない**は、ユーザーがログオンするときにすべてのクライアントプリンターの自動作成をオフにします。このオプションを選択すると、優先度の低いポリシーで、クライアントプリンターの自動作成に関するRemote Desktop Services (RDS) の設定がこの設定を上書きします。

汎用ユニバーサルプリンターの自動作成

この設定は、セッションに対して汎用Citrix Universal™ Printerオブジェクトの自動作成を有効または無効にします。これらのセッションには、ユニバーサル印刷と互換性のあるユーザーデバイスが使用されているセッションのみが含まれます。

デフォルトでは、汎用ユニバーサルプリンターオブジェクトは自動作成されません。

次のポリシー設定が関連しています。

- ユニバーサルプリントドライバーの使用
- ユニバーサルドライバーの優先順位

PDFユニバーサルプリンターの自動作成

この設定は、以下のセッションでCitrix PDFプリンターの自動作成を有効または無効にします。

- Windows向けCitrix Workspaceアプリ（VDA 7.19以降）
- Linux向けCitrix Workspace™アプリ
- macOS向けCitrix Workspaceアプリ
- HTML5向けCitrix Workspaceアプリ
- Chrome向けCitrix Workspaceアプリ

デフォルトでは、Citrix PDFプリンターは自動作成されません。

クライアントプリンター名

この設定は、自動作成されるクライアントプリンターの命名規則を選択します。

デフォルトでは、標準のプリンター名が使用されます。

「**標準プリンター名**」を選択すると、「HPLaserJet 4 from client name in session 3」のようなプリンター名が使用されます。

「**レガシープリンター名**」を選択すると、旧式のクライアントプリンター名が使用され、製品のXenDesktopバージョンに存在したレガシープリンター名との下位互換性が維持されます。このオプションは、現在のCitrix Virtual Apps and Desktopsバージョンの製品でも使用できます。レガシープリンター名の例は「Client/clientname#/HPLaserJet 4」です。このオプションはセキュリティが低下します。

Citrix Workspaceアプリ for HTML5から起動したセッションでCitrix PDFプリンターを使用する場合は、**クライアントプリンター名**設定をデフォルトにするか、**標準プリンター名**を選択します。**レガシープリンター名**を選択した場合、Citrix Workspaceアプリ for HTML5はCitrix PDFプリンターオプションをサポートしません。

プリントサーバーへの直接接続

この設定は、仮想デスクトップまたはサーバーホスティングアプリケーションからクライアントプリンター用のプリントサーバーへの直接接続を有効または無効にします。ここで、クライアントプリンターはアクセス可能なネットワーク共有でホストされます。

デフォルトでは、直接接続が有効になっています。

ネットワークプリントサーバーが仮想デスクトップまたはサーバーホスティングアプリケーションからWANを介していない場合は、直接接続を有効にします。ネットワークプリントサーバーと

仮想デスクトップまたはサーバーホスティングアプリケーションが同じLAN上にある場合、直接通信により印刷が高速化されます。

ネットワークがWANを介している場合、または大幅な遅延や帯域幅の制限がある場合は、直接接続を無効にします。印刷ジョブはユーザーデバイスを経由してルーティングされ、そこでネットワークプリントサーバーにリダイレクトされます。ユーザーデバイスに送信されるデータは圧縮されるため、WANを介してデータが転送される際の帯域幅の消費が少なくなります。

2つのネットワークプリンターが同じ名前を持つ場合、ユーザーデバイスと同じネットワーク上のプリンターが使用されます。

プリンタードライバーのマッピングと互換性

この設定は、自動作成されたクライアントプリンターのドライバー置換ルールを指定します。

この設定は、Microsoft OneNoteおよびXPS Document Writerを自動作成されたクライアントプリンターリストから除外するように構成されています。

ドライバー置換ルールを定義すると、指定されたドライバーでプリンターが作成されることを許可または防止できます。また、作成されたプリンターがユニバーサルプリントドライバーのみを使用することを許可できます。ドライバー置換は、ユーザーデバイスが提供するプリンタードライバー名を上書きまたはマッピングし、サーバー上の同等のドライバーに置き換えます。これらのルールにより、サーバーアプリケーションは、サーバーと同じドライバーを持つがドライバー名が異なるクライアントプリンターにアクセスできるようになります。

次のことができます。

- ドライバーマッピングを追加する
- 既存のマッピングを編集する
- マッピングのカスタム設定を上書きする
- マッピングを削除
- リスト内のドライバーエントリの順序を変更

マッピングを追加する際は、クライアントプリンタードライバー名を入力し、置き換えたいサーバードライバーを選択します。

プリンタープロパティの保持

この設定は、プリンターのプロパティを保存するかどうか、およびどこに保存するかを指定します。

デフォルトでは、システムはプリンターのプロパティがユーザーデバイスに保存されるか（利用可能な場合）、またはユーザープロファイルに保存されるかを決定します。

この設定をポリシーに追加する際は、オプションを選択します。

- 「クライアントデバイスのみに保存」は、保存されない必須プロファイルまたは移動プロファイルを持つユーザーデバイス向けです。
- 「ユーザープロファイルのみに保持」は、帯域幅に制約のあるユーザーデバイス（このオプションはネットワークトラフィックを削減します）やログオン速度が重要な場合、またはレガシープラグインを使用するユーザー向けです。このオプションは、プリンタープロパティをサーバー上のユーザープロファイルに保存し、ユーザーデバイスとのプロパティ交換を防ぎます。このオプションは、リモートデスクトップサービス（RDS）の移動プロファイルが使用されている場合にのみ適用されます。
- 「クライアントに保存されていない場合のみプロファイルに保持」は、システムがプリンタープロパティの保存場所を決定できるようにします。プリンタープロパティは、利用可能な場合はユーザーデバイスに、またはユーザープロファイルに保存されます。このオプションは最も柔軟ですが、ログオン時間を遅くしたり、システムチェックのために余分な帯域幅を使用したりする可能性があります。
- 「プリンタープロパティを保持しない」は、プリンタープロパティの保存を防ぎます。

保持および復元されたクライアントプリンター

この設定は、ユーザーデバイス上のプリンターの保持と再作成を有効または無効にします。デフォルトでは、クライアントプリンターは自動的に保持および復元されます。

保持されたプリンターとは、次回のセッション開始時に再度作成される、または記憶される、ユーザーが作成したプリンターです。Citrix Virtual Apps™が保持されたプリンターを再作成する際、「**クライアントプリンターの自動作成**」設定を除くすべてのポリシー設定が考慮されます。

復元されたプリンターとは、管理者が完全にカスタマイズし、保存された状態がクライアントポートに永続的に関連付けられているプリンターです。

CITRIX PDFユニバーサルプリンタードライバー

Citrix PDFユニバーサルプリンタードライバーを使用すると、ホストされたアプリケーションまたはCitrix Virtual Apps and Desktopsによって提供される仮想デスクトップで実行されているアプリケーションで開かれたドキュメントをユーザーが印刷できるようになります。ユーザーが**Citrix PDF Printer**オプションを選択すると、ドライバーはファイルをPDFに変換し、そのPDFをローカルデバイスに転送します。その後、PDFはローカルに接続されたプリンターから表示および印刷するために開かれます。PDFは、Citrixユニバーサルプリンティングでサポートされている形式の1つです（EMFおよびXPSに加えて）。 PDFプリンターは、Citrixポリシーを使用して有効化、構成、およびデフォルトとして設定できます。**Citrix PDF Printer**オプションは、Windows、Linux、MacOS、Chrome、およびHTML5用のCitrix Workspaceアプリのユーザーが利用できます。

> **注：**
>
> WindowsエンドポイントにはPDFビューアーが必要です。クライアントには、PDFファイルを開くためにWindowsにファイルの種類関連付けが登録されているアプリケーションが必要です。

ドライバーポリシー設定

「**ドライバー**」セクションには、プリンタードライバーに関連するポリシー設定が含まれています。

インボックスプリンタードライバーの自動インストール

> **注**
>
> このポリシーは、このリリースではVDAをサポートしていません。

> この設定は、以下のプリンタードライバーの自動インストールを有効または無効にします。

- Windowsインボックスドライバーセット
- `pnputil.exe /a`を使用してホストにステージングされたドライバーパッケージ

デフォルトでは、これらのドライバーは必要に応じてインストールされます。

ユニバーサルドライバーの優先順位

この設定は、リストの最初のエントリから始まる、ユニバーサルプリンタードライバーが使用される順序を指定します。

デフォルトでは、優先順位は次のとおりです。

- EMF
- XPS
- PCL5c (ピーシーエルファイブシー)
- PCL4
- PS

ドライバーの追加、編集、削除、およびリスト内のドライバーの順序変更が可能です。

ユニバーサルプリントドライバーの使用

この設定は、ユニバーサル印刷を使用するタイミングを指定します。

既定では、要求されたドライバーが利用できない場合にのみ、ユニバーサル印刷が使用されます。

ユニバーサル印刷は、標準のモデル固有ドライバーの代わりに汎用プリンタードライバーを使用するため、ホストコンピューターでのドライバー管理の負担を軽減できる可能性があります。ユニバーサルプリンタードライバーの利用可能性は、ユーザーデバイス、ホスト、および印刷サーバーソフトウェアの機能に依存します。特定の構成では、ユニバーサル印刷が利用できない場合があります。

この設定をポリシーに追加する場合は、次の表からオプションを選択します。

オプション	説明
プリンターモデル固有のドライバーのみを使用する	クライアントプリンターが、サインイン時に自動作成される標準のモデル固有ドライバーのみを使用することを指定します。要求されたドライバーが利用できない場合、クライアントプリンターは自動作成できません。
ユニバーサル印刷のみを使用する	標準のモデル固有ドライバーは使用しないことを指定します。プリンターの作成には、ユニバーサルプリンタードライバーのみが使用されます。
要求されたドライバーが利用できない場合にのみユニバーサル印刷を使用する	利用可能な場合は、プリンター作成に標準のモデル固有ドライバーを使用します。ドライバーがサーバーで利用できない場合、クライアントプリンターは適切なユニバーサルドライバーで自動的に作成されます。
ユニバーサル印刷が利用できない場合にのみプリンターモデル固有のドライバーを使用する	利用可能な場合は、ユニバーサルプリントドライバーを使用します。ドライバーがサーバーで利用できない場合、クライアントプリンターは適切なモデル固有のプリンタードライバーで自動的に作成されます。

ユニバーサルプリントサーバーのポリシー設定

ユニバーサルプリントサーバーセクションには、ユニバーサルプリントサーバーを処理するためのポリシー設定が含まれています。

SSL暗号スイート

この設定は、暗号化された印刷データストリーム (CGP) 接続のためにUniversal Print Clientで使用されるSSL/TLS暗号スイートのセットを指定します。

暗号化された印刷Webサービス (HTTPS/SOAP) 接続のためにUniversal Print Clientで使用される暗号スイートパッケージを制御するには、を参照してください。

デフォルト値: ALL

この設定には、ALL、COM、またはGOVの次の値があります。

各値に対応する暗号スイートは次のとおりです:

ALL:

TLS_ECDHE_RSA_AES256_GCM_SHA384

TLS_ECDHE_RSA_AES256_CBC_SHA384

TLS_ECDHE_RSA_AES128_CBC_SHA

COM:

TLS_ECDHE_RSA_AES128_CBC_SHA

GOV:

TLS_ECDHE_RSA_AES256_GCM_SHA384

TLS_ECDHE_RSA_AES256_CBC_SHA384

SSL準拠モード

この設定は、Universal Print Clientが暗号化された印刷データストリーム (CGP) 接続に使用するNIST Special Publication 800-52への準拠レベルを指定します。

デフォルト値: なし。

この設定には次の値があります:

なし。

暗号化された印刷データストリーム (CGP) 接続は、デフォルトの準拠モードを使用します。

SP800-52。

暗号化された印刷データストリーム (CGP) 接続は、NIST Special Publication 800-52準拠モードを使用します。

SSL有効

この設定は、Universal Print Clientが以下の目的でSSL/TLSを使用するかどうかを指定します:

- 印刷データストリーム (CGP) 接続
- Webサービス (HTTP/SOAP) 接続

Universal Print Server enable を **Enabled with fallback to Windows' native remote printing** に設定すると、Microsoft Windows Network Print Providerによってフォールバック接続が行われます。この設定は、これらのフォールバック接続には影響しません。

既定値: 無効

この設定は次の値をとります。

有効。

Universal Print Client は、SSL/TLS を使用して Universal Print Server に接続します。

無効。

Universal Print Client は、SSL/TLS を使用して Universal Print Server に接続します。

SSL FIPS モード

この設定は、Universal Print Clientが印刷データストリーム（CGP）接続のために使用するSSL/TLS暗号化モジュールがFIPSモードで実行されるかどうかを指定します。

既定値: 無効

この設定は次の値をとります。

有効。

FIPS モードがオンです。

無効。

FIPS モードがオフです。

SSL プロトコルバージョン

この設定は、Universal Print Clientが使用するSSL/TLSプロトコルバージョンを指定します。

デフォルト値: ALL

この設定には次の値があります。

ALL。

TLSバージョン1.0、1.1、または1.2を使用します。

TLSバージョン1.

TLSバージョン1.0を使用します。

TLSv1.1。

TLSバージョン1.1を使用します。

TLSv1.2。

TLSバージョン1.2を使用します。

SSL UNIVERSAL PRINT SERVER暗号化印刷データストリーム（CGP）ポート

この設定は、Universal Print Server暗号化印刷データストリーム（CGP）ポートのTCPポート番号を指定します。このポートは、印刷ジョブのデータを受信します。

デフォルト値: 443

SSL ユニバーサルプリントサーバー暗号化WEBサービス (HTTPS/SOAP) ポート

この設定は、Universal Print Server の暗号化された Web サービス (HTTPS/SOAP) ポートの TCP ポート番号を指定します。このポートは、印刷コマンドのデータを受信します。

デフォルト値: 8443

UNIVERSAL PRINT SERVERの有効化

このポリシーは、Citrix Universal Print Server (UPS) の使用を有効または無効にします。このポリシー設定は、仮想デスクトップまたはサーバーホスティングアプリケーションを含む組織単位 (OU) に適用します。このポリシー設定には、Citrix UPSコンポーネントが要求されたプリントサーバーにインストールされていないか、利用できない場合に、ネイティブのWindowsリモート印刷サービスを使用してプリントサーバーへの接続を許可するフォールバックオプションが含まれています。このポリシーへの変更は、VDAが再起動された後にのみ適用されます。

デフォルトでは、Universal Print Serverは無効になっています。

この設定をポリシーに追加するときは、次のいずれかのオプションを選択します。

- **Windows ネイティブのリモート印刷へのフォールバックを有効にする**: 可能な場合、Universal Print Server はネットワークプリンター接続を処理します。Universal Print Server が

利用できない場合、Windows Print Provider が使用されます。Windows Print Provider は、以前に Windows Print Provider で作成されたすべてのプリンターを引き続き処理します。

- **Windows ネイティブのリモート印刷へのフォールバックなしで有効にする**: Universal Print Server は、ネットワークプリンター接続を排他的に処理します。Universal Print Server が利用できない場合、ネットワークプリンター接続は失敗します。この設定は、Windows Print Provider を介したネットワーク印刷を実質的に無効にします。この設定を含むポリシーがアクティブな間は、以前に Windows Print Provider で作成されたプリンターは作成されません。
- **無効**: Universal Print Server 機能は無効になります。UNC 名を持つネットワークプリンターに接続する際、Universal Print Server への接続は試行されません。リモートプリンターへの接続は、引き続き Windows ネイティブのリモート印刷機能を使用します。

UNIVERSAL PRINT SERVER印刷データストリーム (CGP) ポート

この設定は、Universal Print Server印刷データストリームのCommon Gateway Protocol (CGP) リスナーが使用するTCPポート番号を指定します。このポリシー設定は、プリントサーバーを含むOUにのみ適用します。

デフォルトでは、ポート番号は7229に設定されています。

有効なポート番号は1～65535の範囲である必要があります。

UNIVERSAL PRINT SERVER印刷ストリーム入力帯域幅制限 (KBPS)

この設定は、印刷データの転送速度の上限（キロビット/秒）を指定します。転送速度は、各印刷ジョブからCGPを使用してUniversal Print Serverに配信される印刷データに対して計算されます。このポリシー設定は、仮想デスクトップまたはサーバーホスティングアプリケーションを含むOUに適用します。

デフォルトでは、値は0であり、上限がないことを指定します。

UNIVERSAL PRINT SERVER WEBサービス (HTTP/SOAP) ポート

この設定は、Universal Print ServerのWebサービス (HTTP/SOAP) リスナーが使用するTCPポート番号を指定します。Universal Print Serverは、ネットワーク印刷シナリオでCitrixユニバーサル印刷ドライバーの使用を可能にするオプションコンポーネントです。

Universal Print Serverが使用される場合、印刷コマンドはCitrix Virtual Apps and Desktopsホストから SOAP over HTTPを介してUniversal Print Serverに送信されます。この設定は、Universal Print Serverが受信HTTP/SOAPリクエストをリッスンするデフォルトのTCPポートを変更します。

ホストと印刷サーバーのHTTPポートは、両方とも同じように構成する必要があります。ポートを同じように構成しない場合、ホストソフトウェアはUniversal Print Serverに接続しません。この設

定は、Citrix Virtual Apps and Desktops上のVDAを変更します。さらに、Universal Print Serverのデフォルトポートも変更する必要があります。

デフォルトでは、ポート番号は8080に設定されています。

有効なポート番号は0～65535の範囲である必要があります。

負荷分散用のUNIVERSAL PRINT SERVER

この設定は、他のCitrix®印刷ポリシー設定を評価した後、セッション起動時に確立されたプリンター接続の負荷分散に使用されるUniversal Print Serverを一覧表示します。プリンター作成時間を最適化するために、Citrixはすべての印刷サーバーが同じ共有プリンターセットを持つことを推奨します。負荷分散のために追加できる印刷サーバーの数に上限はありません。

この設定は、印刷サーバーのフェイルオーバー検出とプリンター接続の回復も実装します。印刷サーバーは定期的に可用性がチェックされます。サーバー障害が検出された場合、そのサーバーは負荷分散スキームから削除されます。また、そのサーバー上のプリンター接続は、他の利用可能な印刷サーバーに再配布されます。障害が発生した印刷サーバーが回復すると、負荷分散スキームに戻されます。

Validate Servers をクリックして、各サーバーが印刷サーバーであること、サーバーリストに重複するサーバー名が含まれていないこと、およびすべてのサーバーに同一の共有プリンターセットがインストールされていることを確認します。この操作には時間がかかる場合があります。

UNIVERSAL PRINT SERVERサービス停止しきい値

この設定は、ロードバランサーが利用できない印刷サーバーが回復するのを待つ時間を指定します。この時間を過ぎると、サーバーが永続的にオフラインであると判断され、その負荷が他の利用可能な印刷サーバーに再配布されます。

デフォルトでは、しきい値は180 (秒) に設定されています。

UNIVERSAL PRINT SERVER WEBサービス (HTTP/SOAP) 接続タイムアウト

この設定は、Universal Print Client が Universal Print Server Web サービス connect() 操作がタイムアウトするまで待機する秒数を指定します。この設定には次の値があります。これらの値はすべて数値であり、単位（時間）は秒です。

- 最小値は0です。
- 最大値は60です。
- デフォルト値は10です。

タイムアウトが1から60（両端を含む）の場合、Universal Print Client は操作が完了するまで指定された時間待機します。この操作は、TCPソケット接続操作です。ソケットは、TCP/IPネットワークを介したプロセス間通信を可能にするWindowsオペレーティングシステムの機能です。

タイムアウトが0の場合、Universal Print Client はオペレーティングシステムによって定義されたデフォルトのタイムアウトを使用します。この構成は、この変更前のUniversal Print Clientの以前のバージョンで利用可能だった構成です。

Universal Print Client は、Universal Print Server と通信する Virtual Delivery Agent (VDA) のコンポーネントです。

> **注：**
>
> このポリシー設定は、VDAバージョン7.35以降に適用されます。

UNIVERSAL PRINT SERVER WEB サービス (HTTP/SOAP) 受信タイムアウト

この設定は、Universal Print Client が Universal Print Server Web サービス recv() 操作がタイムアウトするまで待機する秒数を指定します。この設定には次の値があり、これらの値はすべて数値であり、単位（時間）は秒です。

- 最小値は0です。
- 最大値は60です。
- デフォルト値は10です。

タイムアウトが1から60（両端を含む）の場合、Universal Print Client は操作が完了するまで指定された時間待機します。この操作は、TCPソケット受信操作です。ソケットは、TCP/IPネットワークを介したプロセス間通信を可能にするWindowsオペレーティングシステムの機能です。

タイムアウトが0の場合、Universal Print Clientはオペレーティングシステムによって定義されたデフォルトのタイムアウトを使用します。この構成は、この変更前のUniversal Print Clientの以前のバージョンで利用可能だった構成です。

Universal Print Clientは、Universal Print Serverと通信するVirtual Delivery Agent (VDA) のコンポーネントです。

> **注:**
>
> このポリシー設定は、VDAバージョン7.35以降に適用されます。

UNIVERSAL PRINT SERVER WEBサービス (HTTP/SOAP) 受信タイムアウト

この設定は、Universal Print ClientがUniversal Print Server Webサービスのrecv()操作がタイムアウトするまで待機する秒数を指定します。この設定には次の値があり、これらの値はすべて数値で、単位（時間）は秒です。

- 最小値は0です。
- 最大値は60です。
- デフォルト値は10です。

タイムアウトが1から60（両端を含む）の場合、Universal Print Clientは操作が完了するまで指定された時間待機します。この操作は、TCPソケットの送信操作です。ソケットは、TCP/IPネットワークを介したプロセス間通信を可能にするWindowsオペレーティングシステムの機能です。

タイムアウトが0の場合、Universal Print Clientは、オペレーティングシステムによって定義されたデフォルトのタイムアウトを使用します。この構成は、この変更前のUniversal Print Clientの以前のバージョンで利用可能だった構成です。

Universal Print Clientは、Universal Print Serverと通信するVirtual Delivery Agent (VDA) のコンポーネントです。

注:

このポリシー設定は、VDAバージョン7.35以降で適用されます。

UNIVERSAL PRINT SERVER WEBサービス (HTTP/SOAP) 送信タイムアウト

この設定は、Universal Print Client が Universal Print Server Webサービスの send() 操作がタイムアウトするまで待機する秒数を指定します。この設定には次の値があります。これらの値はすべて数値であり、単位（時間）は秒です。

- 最小値は0です。
- 最大値は60です。
- デフォルト値は10です。

タイムアウトが1から60（両端を含む）の場合、Universal Print Client は操作が完了するまで指定された時間待機します。この操作はTCPソケット送信操作です。ソケットは、TCP/IPネットワークを介したプロセス間通信を可能にするWindowsオペレーティングシステムの機能です。

タイムアウトが0の場合、Universal Print Client はオペレーティングシステムによって定義されたデフォルトのタイムアウトを使用します。この構成は、この変更前のUniversal Print Clientの以前のバージョンで利用可能だった構成です。

Universal Print Client は、Universal Print Server と通信するVDAのコンポーネントです。

> **注:**
>
> このポリシー設定は、VDAバージョン7.35以降で適用されます。

ユニバーサル印刷ポリシー設定

ユニバーサル印刷セクションには、ユニバーサル印刷を管理するためのポリシー設定が含まれています。

ユニバーサル印刷EMF処理モード

この設定は、WindowsユーザーデバイスでのEMFスプールファイルの処理方法を制御します。

デフォルトでは、EMFレコードはプリンターに直接スプールされます。

この設定をポリシーに追加するときは、オプションを選択します。

- プリンターのEMFを再処理すると、EMFスプールファイルが強制的に再処理され、ユーザーデバイス上のGDIサブシステムを介して送信されます。この設定は、EMFの再処理を必要とするが、セッションで自動的に選択されない可能性のあるドライバーに使用できます。
- プリンターに直接スプールすると、Citrix Universal™印刷ドライバーと併用した場合、EMFレコードがスプールされ、処理のためにユーザーデバイスに配信されることが保証されます。通常、これらのEMFスプールファイルはクライアントのスプールキューに直接挿入されます。EMF形式と互換性のあるプリンターおよびドライバーの場合、これが最速の印刷方法です。

ユニバーサル印刷画像圧縮制限

この設定は以下を指定します:

- Citrix Universal印刷ドライバーで印刷される画像に利用可能な最大品質
- Citrix Universal印刷ドライバーで印刷される画像に利用可能な最小圧縮レベル

デフォルトでは、画像圧縮制限は「最高品質（ロスレス圧縮）」に設定されています。

「圧縮なし」が選択されている場合、EMF印刷のみ圧縮が無効になります。

この設定をポリシーに追加するときは、オプションを選択します。

- 圧縮なし
- 最高品質 (ロスレス圧縮)
- 高品質
- 標準品質
- 低品質 (最大圧縮)

この設定を**ユニバーサル印刷の最適化のデフォルト**設定を含むポリシーに追加する場合は、次の点に注意してください。

- **ユニバーサル印刷の画像圧縮制限**設定の圧縮レベルが、**ユニバーサル印刷の最適化のデフォルト**設定で定義されているレベルよりも低いとします。この場合、画像はユニバーサル印刷の画像圧縮制限設定で定義されているレベルで圧縮されます。
- 圧縮が無効になっている場合、ユニバーサル印刷の最適化のデフォルト設定の「希望する画質」および「ヘビーウェイト圧縮を有効にする」オプションは、ポリシーに影響しません。

ユニバーサル印刷の最適化のデフォルト

この設定は、セッション用にユニバーサル印刷ドライバーが作成されるときの印刷最適化のデフォルト値を指定します。

- 希望する画質は、ユニバーサル印刷に適用されるデフォルトの画像圧縮制限を指定します。デフォルトでは、標準品質が有効になっており、ユーザーは標準または低品質の圧縮を使用してのみ画像を印刷できます。
- ヘビーウェイト圧縮を有効にするは、画質を損なうことなく、希望する画質で設定された圧縮レベルを超えて帯域幅を削減することを有効または無効にします。デフォルトでは、ヘビーウェイト圧縮は無効になっています。
- 画像とフォントのキャッシュ設定は、印刷ストリームに複数回出現する画像とフォントをキャッシュするかどうかを指定します。この設定により、一意の画像またはフォントがプリンターに一度だけ送信されるようになります。デフォルトでは、埋め込み画像とフォントはキャッシュされます。これらの設定は、ユーザーデバイスがこの動作をサポートしている場合にのみ適用されます。
- 管理者以外のユーザーがこれらの設定を変更することを許可するは、ユーザーがセッション内でデフォルトの印刷最適化設定を変更できるかどうかを指定します。デフォルトでは、ユーザーはデフォルトの印刷最適化設定を変更できません。

注：これらのオプションはすべてEMF印刷でサポートされています。XPS印刷では、「希望する画質」オプションのみがサポートされています。

この設定を、**ユニバーサル印刷画像圧縮制限**設定を含むポリシーに追加する場合は、次の点に注意してください。

- **ユニバーサル印刷画像圧縮制限**設定の圧縮レベルが、**ユニバーサル印刷最適化のデフォルト**設定で定義されているレベルよりも低いとします。この場合、画像はユニバーサル印刷画像圧縮制限設定で定義されているレベルで圧縮されます。
- 圧縮が無効になっている場合、ユニバーサル印刷最適化のデフォルト設定の「希望する画質」および「ヘビーウェイト圧縮を有効にする」オプションは、ポリシーに影響しません。

ユニバーサル印刷プレビューの優先設定

この設定は、自動作成されたプリンターまたは汎用ユニバーサルプリンターで印刷プレビュー機能を使用するかどうかを指定します。

デフォルトでは、自動作成されたプリンターまたは汎用ユニバーサルプリンターでは印刷プレビューは使用されません。

この設定をポリシーに追加するときは、オプションを選択します。

- 自動作成されたプリンターまたは汎用ユニバーサルプリンターで印刷プレビューを使用しない
- 自動作成されたプリンターでのみ印刷プレビューを使用する
- 汎用ユニバーサルプリンターでのみ印刷プレビューを使用する
- 自動作成されたプリンターと汎用ユニバーサルプリンターの両方で印刷プレビューを使用する

ユニバーサル印刷の印刷品質制限

この設定は、セッションで印刷出力を生成するために使用できる最大ドット/インチ (dpi) を指定します。

デフォルトでは、「制限なし」が有効になっており、ユーザーは接続先のプリンターで許可されている最高の印刷品質を選択できます。

この設定が構成されている場合、出力解像度の観点から、ユーザーが利用できる最大の印刷品質が制限されます。印刷品質自体と、ユーザーが接続するプリンターの印刷品質機能の両方が、構成された設定に制限されます。

たとえば、中解像度 (600 DPI) に構成されている場合、ユーザーは最大 600 DPI の品質でしか出力を印刷できません。また、**ユニバーサルプリンター**ダイアログボックスの**詳細設定**タブにある**印刷品質**設定には、中品質 (600 DPI) までの解像度設定のみが表示されます。

この設定をポリシーに追加するときは、オプションを選択します。

- 下書き (150 DPI)

- 低解像度 (300 DPI)
- 中解像度 (600 DPI)
- 高解像度 (1200 DPI)
- 制限なし

セキュリティポリシー設定

セキュリティセクションには、セッション暗号化とログオンデータの暗号化を構成するためのポリシー設定が含まれています。

SecureICAの最小暗号化レベル

この設定は、サーバーとユーザーデバイス間で送信されるセッションデータを暗号化する最小レベルを指定します。

重要: Virtual Delivery Agent 7.xの場合、このポリシー設定は、RC5 128ビット暗号化によるログオンデータの暗号化を有効にするためにのみ使用できます。その他の設定は、Citrix Virtual Apps and Desktopsのレガシーバージョンとの下位互換性のためにのみ提供されています。

VDA 7.xの場合、セッションデータの暗号化は、VDAのデリバリーグループの基本設定を使用して設定されます。デリバリーグループでSecure ICAを有効にするが選択されている場合、セッションデータはRC5（128ビット）暗号化を使用して暗号化されます。デリバリーグループでSecure ICAを有効にするが選択されていない場合、セッションデータは基本暗号化で暗号化されます。

この設定をポリシーに追加するときは、オプションを選択します。

- Basicは、非RC5アルゴリズムを使用してクライアント接続を暗号化します。これにより、データストリームが直接読み取られるのを防ぎますが、復号化される可能性があります。デフォルトでは、サーバーはクライアントとサーバー間のトラフィックにBasic暗号化を使用します。
- RC5 (128 bit) logon onlyは、RC5 128ビット暗号化を使用してログオンデータのみを暗号化し、クライアント接続にはBasic暗号化を使用します。
- RC5 (40 bit)は、RC5 40ビット暗号化を使用してクライアント接続を暗号化します。
- RC5 (56 bit)は、RC5 56ビット暗号化を使用してクライアント接続を暗号化します。
- RC5 (128 bit)は、RC5 128ビット暗号化を使用してクライアント接続を暗号化します。

クライアントとサーバー間の暗号化に指定する設定は、環境内の他の暗号化設定やWindowsオペレーティングシステムと相互作用する可能性があります。サーバーまたはユーザーデバイスのいずれかで、より高い優先度の暗号化レベルが設定されている場合を考慮してください。この場合、公開リソースに指定した設定が上書きされる可能性があります。

特定のユーザーの通信とメッセージの整合性をさらに保護するために、暗号化レベルを上げることができます。ポリシーでより高い暗号化レベルが必要な場合、より低い暗号化レベルを使用しているCitrix Receiversは接続を拒否されます。

SecureICAは認証を実行したり、データの整合性をチェックしたりしません。サイトのエンドツーエンド暗号化を提供するには、SecureICAをTLS暗号化と組み合わせて使用します。

SecureICAはFIPS準拠アルゴリズムを使用しません。この設定が問題となる場合は、SecureICAの使用を避けるようにサーバーとCitrix Receiverを構成してください。

SecureICAは、機密性のためにRFC 2040で説明されているRC5ブロック暗号を使用します。ブロックサイズは64ビット（32ビットワード単位の倍数）です。キー長は128ビットです。ラウンド数は12です。

RC5ブロック暗号のキーは、セッションが作成されるときにネゴシエートされます。ネゴシエーションはDiffie-Hellmanアルゴリズムを使用して実行されます。このネゴシエーションでは、Diffie-Hellman公開パラメーターが使用されます。これらのパラメーターは、Virtual Delivery Agentがインストールされるときにレジストリに保存されます。公開パラメーターは秘密ではありません。Diffie-Hellmanネゴシエーションの結果は秘密キーであり、そこからRC5ブロック暗号のセッションキーが導出されます。ユーザーログオンとデータ転送には、個別のセッションキーが使用されます。また、Virtual Delivery Agentとの間のトラフィックにも個別のセッションキーが使用されます。したがって、各セッションには4つのセッションキーがあります。秘密キーとセッションキーは保存されません。RC5ブロック暗号の初期化ベクトルも秘密キーから導出されます。

サーバー制限ポリシー設定

「**サーバー制限**」セクションには、アイドル接続を制御するためのポリシー設定が含まれています。

サーバーアイドルタイマー間隔

この設定は、ユーザーからの入力がない場合に、中断されないユーザーセッションがどのくらいの期間維持されるかを決定します。データはミリ秒で計算されます。

デフォルトでは、アイドル接続は切断されません（サーバーアイドルタイマー間隔 = 0）。Citrix®は、この値を最低60000ミリ秒（60秒）に設定することを推奨しています。

ポリシーを表示するには、**Multiple Versions**を選択し、Single-session OS versionsのチェックを外し、**Server Limits**を選択します。

> **注**

> このポリシー設定が使用されている場合、セッションが指定された時間アイドル状態になると、「アイドルタイマーの期限が切れました」というダイアログボックスがユーザーに表示されることがあります。Citrixポリシー設定は、このMicrosoftダイアログボックスメッセージを制御しません。詳細については、`<http://support.citrix.com/article/CTX118618>`を参照してください。

セッション制限ポリシー設定

セッション制限セクションには、セッションが強制的にログオフされるまでに接続を維持する期間を制御するポリシー設定が含まれています。

切断されたセッションタイマー

この設定は、切断されロックされたデスクトップが、セッションがログオフされるまでにロックされたままになる期間を指定するタイマーを有効または無効にします。

このタイマーが有効になっている場合、タイマーの期限が切れると、切断されたセッションはログオフされます。

デフォルトでは、切断されたセッションはログオフされません。

Remote PC Accessの切断されたセッションタイマー

この設定は、タイマーの期限が切れた後に切断されたユーザーセッションをログオフするタイマーを有効または無効にします。この設定を有効にする場合は、**切断されたセッションタイマー間隔**設定を使用して、ユーザーセッションがログオフされるまでに切断されたデスクトップがロックされたままになる分数（期間）を指定します。

デフォルトでは、この設定は無効になっています。

切断されたセッションタイマー間隔

この設定は、切断されロックされたデスクトップが、セッションがログオフされるまでにロックされたままになる分数（期間）を指定します。

デフォルトでは、期間は1,440分（24時間）です。

切断されたセッションタイマー – マルチセッション

この設定は、切断されたRDSセッションがログオフされるまでにどのくらいの期間持続できるかを決定するタイマーを有効または無効にします。デフォルトでは、このタイマーは無効になっており、切断されたセッションはログオフされません。

切断されたセッションタイマー間隔 – マルチセッション

この設定は、切断されたRDSセッションがログオフされるまでに何分間持続できるかを決定します。デフォルトでは、期間は1440分（24時間）です。

セッション接続タイマー

この設定は、ユーザーデバイスとデスクトップ間の途切れない接続の最大期間を指定するタイマーを有効または無効にします。このタイマーが有効になっている場合、タイマーの期限が切れるとセッションは切断またはログオフされます。Microsoftの**時間制限に達したときにセッションを終了する**設定が、セッションの次の状態を決定します。

デフォルトでは、このタイマーは無効になっています。

セッション接続タイマー間隔

この設定は、ユーザーデバイスとデスクトップ間の途切れない接続の最大分数（時間）を指定します。

デフォルトでは、最大継続時間は1,440分（24時間）です。

セッション接続タイマー – マルチセッション

この設定は、ユーザーデバイスとターミナルサーバー間の途切れない接続の最大継続時間を指定するタイマーを有効または無効にします。デフォルトでは、このタイマーは無効になっています。

セッション接続タイマー間隔 – マルチセッション

この設定は、ユーザーデバイスとRDSセッション間の途切れない接続の最大分数（時間）を指定します。デフォルトでは、最大継続時間は1440分（24時間）です。

セッションアイドルタイマー

ユーザーが何も入力しない場合、この設定は以下を有効または無効にするために使用されます。

- デスクトップへの途切れないユーザーデバイス接続が維持される期間を指定するタイマー。

このタイマーの期限が切れると、セッションは切断状態になり、**切断されたセッションタイマー**が適用されます。**切断されたセッションタイマー**が無効になっている場合、セッションはログオフされません。

デフォルトでは、このタイマーは有効になっています。

セッションアイドルタイマー間隔

ユーザーからの入力がない場合、この設定は以下を指定するために使用されます。

- デスクトップへのユーザーデバイスの途切れない接続が維持される分数。

デフォルトでは、アイドル状態の接続は1,440分（24時間）維持されます。

セッションアイドルタイマー – マルチセッション

この設定は、ユーザーデバイスとターミナルサーバー間のアイドル接続の最大期間を決定するタイマーを有効または無効にします。デフォルトでは、このタイマーは無効になっています。

セッションアイドルタイマー間隔 – マルチセッション

この設定は、ユーザーデバイスとRDSセッション間のアイドル接続が何分間維持されるかを指定します。デフォルトでは、最大期間は1440分（24時間）です。

> **注:**
>
> Citrix®ポリシーを使用して構成されたマルチセッションマシンのタイマー設定は、Microsoftグループポリシーを通じて構成されたタイマー設定を上書きすることが想定されています。予期せぬ動作を避けるため、いずれか一方の方法でタイマー設定を構成することをお勧めします。

セッションの信頼性ポリシー設定

セッションの信頼性セクションには、セッションの信頼性接続を管理するためのポリシー設定が含まれています。

セッションの信頼性接続

この設定により、ネットワーク接続が失われたときにセッションを開いたままにするか、開いたままにしないかを制御できます。セッションの信頼性は、自動クライアント再接続と連携して、ネットワーク障害から回復した後、ユーザーがCitrix Workspace™アプリセッションに自動的に再接続できるようにします。デフォルトでは、セッションの信頼性は許可されています。

Web Studioの設定は、以下のクライアントに適用されます。

- Citrix Workspaceアプリ1808以降
- Citrix Receiver for Windows 4.7 およびそれ以降。

Web Studioポリシーは、クライアント上のCitrix Receiver™グループポリシーオブジェクトを上書きします。Web Studioでこれらのポリシーを更新すると、セッションの信頼性がサーバーからクライアントに同期されます。

> **注:**

- Citrix Receiver for Windows 4.7以降およびWindows用Citrix Workspaceアプリ - Web Studioでポリシーを設定します。
- Citrix Receivers for Windows 4.7より前のバージョン - Web Studioでポリシーを設定します。また、一貫した動作のために、クライアントでCitrix Receiverグループポリシーオブジェクトテンプレートを設定します。

ネットワーク接続が中断された場合でも、セッションの信頼性によりセッションはアクティブな状態を保ち、ユーザーの画面に表示され続けます。ユーザーは、ネットワーク接続が再開されるまで、使用しているアプリケーションを引き続き見ることができます。

セッションの信頼性を使用して、サーバー上でセッションをアクティブな状態に保ちます。接続が失われたことを示すために、ユーザーのディスプレイは不透明になります。ユーザーは中断中にフリーズしたセッションを見る可能性があります。ネットワーク接続が復元されると、ユーザーはアプリケーションとの対話を再開できます。セッションの信頼性により、再認証のプロンプトなしでユーザーが再接続されます。

セッションの信頼性と自動クライアント再接続の両方を使用する場合、これら2つの機能は順番に動作します。セッションの信頼性は、セッションの信頼性タイムアウト設定で指定された時間の経過後にユーザーセッションを閉じ（または切断し）ます。その後、自動クライアント再接続設定が有効になり、切断されたセッションにユーザーを再接続しようとします。

デフォルトでは、セッションの信頼性は許可されています。

注:

Citrix ADC を使用している場合、ICA 接続をプロキシするには、Citrix StoreFront の **Citrix Gateway の管理 / Secure Ticket Authority** で **セッションの信頼性を有効にする** を選択する必要があります。

セッションの信頼性のポート番号

この設定は、受信セッションの信頼性接続に使用するTCPポート番号を指定します。

デフォルトでは、ポート番号は2598に設定されています。

セッションの信頼性のタイムアウト

この設定は、時間の長さを秒単位で指定します。この時間は、セッションの信頼性プロキシがユーザーの再接続を待機し、セッションが切断されるまでの時間です。

セッションが開いている時間を延長することはできますが、この機能は利便性のためであり、ユーザーに再認証を促すものではありません。セッションが開いている時間が長くなるほど、ユーザーがデバイスを放置し、不正なユーザーがアクセスできる可能性が高まります。

デフォルトでは、タイムアウトは180秒（3分）に設定されています。

セッションウォーターマークポリシー設定

セッションウォーターマークセクションには、この機能を構成するためのポリシー設定が含まれています。 この機能を有効にすると、VDAマシンのネットワーク帯域幅とCPU使用率が大幅に増加します。利用可能なハードウェアリソースに基づいて、選択したVDAマシンにセッションウォーターマークを構成することをお勧めします。

> **重要**
>
> 他のウォーターマークポリシー設定を有効にするには、セッションウォーターマークを有効にします。より良いユーザーエクスペリエンスを実現するために、ウォーターマークテキスト項目を3つ以上有効にしないでください。

セッションウォーターマークを有効にする

この設定を有効にすると、セッションディスプレイにセッション固有の情報を表示する不透明なテキストウォーターマークが表示されます。他のウォーターマーク設定は、この設定が有効になっていることに依存します。

デフォルトでは、セッションウォーターマークは無効になっています。

クライアントIPアドレスを含める

この設定を有効にすると、セッションは現在のクライアントIPアドレスをウォーターマークとして表示します。

デフォルトでは、クライアントIPアドレスを含めるは無効になっています。

接続時間を含める

この設定を有効にすると、セッションウォーターマークに接続時間が表示されます。形式はyyyy/mm/dd hh:mmです。表示される時刻は、システムクロックとタイムゾーンに基づいています。

デフォルトでは、接続時間を含めるは無効になっています。

ログオンユーザー名を含める

この設定を有効にすると、セッションは現在のログオンユーザー名をウォーターマークとして表示します。表示形式はUSERNAME@DOMAINNAMEです。ユーザー名は最大20文字にすることをお勧めします。ユーザー名が20文字を超えると、文字フォントが過度に小さくなったり、切り捨てられたりして、ウォーターマークの効果が低下する可能性があります。

デフォルトでは、ログオンユーザー名を含めるは有効になっています。

VDAホスト名を含める

この設定を有効にすると、現在のICA®セッションのVDAホスト名がウォーターマークとしてセッションに表示されます。

デフォルトでは、VDAホスト名を含める設定が有効になっています。

VDA IPアドレスを含める

この設定を有効にすると、現在のICAセッションのVDA IPアドレスがウォーターマークとしてセッションに表示されます。

デフォルトでは、VDA IPアドレスは無効になっています。

セッションウォーターマークのスタイル

この設定は、単一のウォーターマークテキストラベルを表示するか、複数のラベルを表示するかを制御します。「**値**」ドロップダウンメニューから「**複数**」または「**単一**」を選択します。

複数は、セッションに5つのウォーターマークラベルを表示します。中央に1つ、四隅に4つです。

単一は、セッションの中央に単一のウォーターマークラベルを表示します。

デフォルトでは、セッションウォーターマークのスタイルは複数です。

ウォーターマークのカスタムテキスト

この設定を使用すると、セッションウォーターマークに表示するカスタムテキスト（例：会社名）を適用できます。空でない文字列を設定すると、ウォーターマークで有効になっている他の情報に加えて、新しい行にテキストが表示されます。ウォーターマークのカスタムテキストは25 Unicode文字に制限されています。より長い文字列を設定した場合、25文字に切り詰められます。

デフォルトのテキストはありません。

Citrix Virtual Apps and Desktops™ 7 2206以降、テキストにカスタムタグを使用してさらにカスタマイズを追加できます。その結果、カスタムテキストの最大文字数は1024に増加しました。

ウォーターマーク設定で利用可能なタグを次の表に示します。

タグ	説明	例
`<font=value>`	ウォーターマークテキストのフォントを変更できます。値はVDAで利用可能なフォントの名前です。	`<font=Courier New>`
`<fontzoom=value>`	フォントのズーム倍率をパーセンテージで設定できます。ウォーターマークテキストの200%ズームの場合、値は200です。	`<fontzoom=200>`
`<position=value>`	ウォーターマークテキストの位置を変更できます。値は `center`、`topleft`、`topright`、`bottomleft`、および `bottomright` です。このタグはシングルスタイルでのみ適用可能です。	`<position=topright>`
`<rotation=value>`	ウォーターマークのテキストを回転できます。値は度数で指定され、範囲は-360から360です。	`<rotation=45>`
`<style=value>`	表示スタイルを変更できます。このタグは、セッションウォーターマークスタイルポリシーを上書きします。	`<style=single>`

利用可能なウォーターマークスタイルは次のとおりです。

- シングルスタイル - セッションの中央に単一のウォーターマークテキストラベルが表示されます。位置タグを使用して場所を変更できます。
- xスタイルまたは複数 - セッションに5つのウォーターマークラベルが表示されます。中央に1つ、各コーナーに1つずつです。
- タイル - セッションに複数のラベルが表示されます。ウォーターマークテキストは画面全体に均等に配置されます。

ウォーターマークテキストを変更するために利用可能なタグは、次の表に記載されています。

タグ	説明
`<clientip>`	エンドポイントのIPアドレス。
`<date>`	セッションが確立された日付。
`<domain>`	ログインしているユーザーアカウントのドメイン名。
`<hostname>`	VDAのマシン名。
`<newline>`	追加の行を作成します。
`<serverip>`	VDAのIPアドレス。
`<time>`	セッションが確立された時刻。
`<username>`	ユーザー名。

注:

- **ウォーターマークカスタムテキスト**ポリシーは、**セッションウォーターマークを有効にする**ポリシーが有効になっている場合にのみ適用されます。デフォルト値は*無効*です。
- ウォーターマークテキストを変更するためのタグを使用する場合、**セッションウォーターマークを有効にする**を除く他のすべてのセッションウォーターマークポリシーは無視されます。ウォーターマークテキスト設定にタグを使用する場合、他のすべてのウォーターマークポリシーを使用できます。

透かしの透明度

ウォーターマークの不透明度を0から100まで指定できます。指定する値が大きいほど、ウォーターマークは不透明になります。

デフォルトでは、値は17です。

タイムゾーン制御ポリシー設定

タイムゾーン制御セクションには、セッションでのローカル時間の使用に関連するポリシー設定が含まれています。

レガシークライアントのローカル時間を推定する

この設定は、ユーザーデバイスのローカルタイムゾーンの推定を有効または無効にします。これらのデバイスには、サーバーに不正確なタイムゾーン情報を送信するユーザーデバイスが含まれます。

デフォルトでは、サーバーは必要に応じてローカルタイムゾーンを推定します。

この設定は、サーバーに詳細なタイムゾーン情報を送信しないレガシーなCitrix ReceiverまたはICAクライアントでの使用を目的としています。この設定が、サーバーに詳細なタイムゾーン情報を送信するCitrix Receiver（例: Windows版Citrix Receiver™のサポート対象バージョン）で使用される場合を考慮してください。この場合、この設定は効果がありません。

セッション切断またはログオフ時にデスクトップOSのタイムゾーンを復元する

ユーザーがセッションを切断またはログオフする場合を考慮してください。この場合、この設定は、シングルセッションOS VDAのタイムゾーン設定がマシンの元のタイムゾーンに復元されるかどうかを決定します。この設定を有効にすると、ユーザーが切断またはログオフしたときに、VDAはマシンのタイムゾーンを元の設定に復元します。この設定を有効にするには、**クライアントのローカル時間を使用**を**クライアントのタイムゾーンを使用**に設定します。

デフォルトでは、この設定は有効になっています。

クライアントのローカル時間を使用

この設定は、ユーザーセッションのタイムゾーン設定を決定します。選択肢は、ユーザーセッションのタイムゾーン（サーバータイムゾーン）またはユーザーデバイスのタイムゾーン（クライアントタイムゾーン）です。

デフォルトでは、ユーザーセッションのタイムゾーンが使用されます。

この設定を有効にするには、グループポリシーエディターで**タイムゾーンのリダイレクトを許可**設定を有効にします。この設定は、**ローカルコンピューターポリシー** > **コンピューターの構成** > **管理用テンプレート** > **Windowsコンポーネント** > **リモートデスクトップサービス** > **リモートデスクトップセッションホスト** > **デバイスとリソースのリダイレクト**にあります。

サーバーOSを実行しているマシンでシングルセッションVDA（旧称Workstation VDA）を使用している場合は、ローカルユーザー権限**タイムゾーンの変更**を**Everyone**に構成します。このユーザー権限は、**ローカルコンピューターポリシー** > **コンピューターの構成** > **Windowsの設定** > **セキュリティの設定** > **ローカルポリシー** > **ユーザー権利の割り当て**にあります。

> **注:**

> シングルセッションOSでは、**ユーザー**はユーザー権利の割り当て「**タイムゾーンの変更**」に含まれますが、マルチセッションOSでは含まれません。マルチセッションOSでは、タイムゾーンは以下のグループポリシーを使用して同期されます: Computer Configuration\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Device and Resource Redirection\Allow timezone redirection。このポリシーは、サーバーがマルチセッションOS VDAのリモートデスクトップセッションホストである場合（`/ServerVDI` コマンドでインストールされている場合）に適用されます。マルチセッションOSでは、デフォルトで、かつ設計上、ユーザーはタイムゾーンを変更するローカル権限を持っていません。

TWAINデバイスのポリシー設定

TWAINデバイスセクションには、以下のポリシー設定が含まれています。

- デジタルカメラやスキャナーなどのクライアントTWAINデバイスのマッピング
- サーバーからクライアントへの画像転送の最適化

> **注:**
>
> Citrix Receiver for Windows 4.5では、TWAIN 2.0がサポートされています。

クライアントTWAINデバイスのリダイレクト

TWAINデバイスは、TWAINプロトコルを使用して、サーバーでホストされている画像処理アプリケーションと通信します。

この設定により、ユーザーはユーザーデバイス上のTWAINデバイスにアクセスできるようになります。または、アクセスが禁止されます。デフォルトでは、TWAINデバイスのリダイレクトは許可されています。

関連するポリシー設定は次のとおりです。

- TWAIN圧縮レベル
- TWAINデバイスのリダイレクト帯域幅制限
- TWAINデバイスリダイレクト帯域幅制限の割合

TWAIN圧縮レベル

この設定は、クライアントからサーバーへの画像転送の圧縮レベルを指定します。最高の画質には「低」、良好な画質には「中」、低い画質には「高」を使用します。デフォルトでは、中程度の圧縮が適用されます。

USBデバイスポリシー設定

USBデバイスセクションには、USBデバイスのファイルリダイレクトを管理するためのポリシー設定が含まれています。

クライアントUSBデバイス最適化ルール

クライアントUSBデバイス最適化ルールは、最適化を無効にするか、最適化モードを変更するためにデバイスに適用できます。

ユーザーがUSB入力デバイスを接続すると、ホストは**USBポリシー**設定がそのデバイスを許可するかどうかを確認します。デバイスが許可されている場合、ホストはそのデバイスの**クライアントUSBデバイス最適化ルール**を確認します。ルールが指定されていない場合、デバイスは最適化されません。キャプチャモード (04) は、署名デバイスに推奨されるモードです。高遅延によってパフォーマンスが低下する他のデバイスの場合、管理者はインタラクティブモード (02) を有効にできます。この記事の表で利用可能なモードの説明を参照してください。

参考情報

- Wacom製署名パッドおよびタブレットを使用する場合は、スクリーンセーバーを無効にすることをお勧めします。スクリーンセーバーを無効にする手順は、このセクションの最後に記載されています。
- Wacom STU署名パッドおよびタブレットシリーズ製品の最適化のサポートは、Citrix Virtual Apps and Desktops™ポリシーのインストール時に事前設定されています。
- 署名デバイスはCitrix Virtual Apps and Desktops全体で機能し、署名デバイスとして使用するためにドライバーを必要としません。Wacomには、デバイスをさらにカスタマイズするためにインストールできる追加のソフトウェアがあります。`<http://www.wacom.com/>`を参照してください。
- 描画タブレット。特定の描画入力デバイスは、PCI/ACPIバス上でHIDデバイスとして認識される可能性があり、サポートされていません。これらのデバイスは、Citrix Virtual Desktopsセッション内でリダイレクトされるように、クライアント上のUSBホストコントローラーに接続してください。

ポリシールールは、空白で区切られたtag=value形式の式を使用します。以下のタグがサポートされています。

タグ名	説明
モード	最適化モードは、class=**03**の入力デバイスでサポートされています。サポートされているモードは次のとおりです。最適化なし - 値**01**。インタラクティブモード - 値**02**。ペンタブレットや3D Proマウスなどのデバイスに推奨されます。キャプチャモード - 値**04**。署名パッドなどのデバイスに推奨されます。
VID	デバイス記述子からのベンダーID（4桁の16進数）。
PID	デバイス記述子からの製品ID（4桁の16進数）。
REV	デバイス記述子からのリビジョンID（4桁の16進数）。
クラス	デバイス記述子またはインターフェース記述子のいずれかからのクラス。
サブクラス	デバイス記述子またはインターフェース記述子のいずれかからのサブクラス。
保護	デバイス記述子またはインターフェース記述子のいずれかからのプロトコル。

例

Mode=00000004 VID=067B PID=1230 class=03 #キャプチャモードで動作する入力デバイス

Mode=00000002 VID=067B PID=1230 class=03 #インタラクティブモードで動作する入力デバイス（デフォルト）

Mode=00000001 VID=067B PID=1230 class=03 #最適化なしで動作する入力デバイス

Mode=00000100 VID=067B PID=1230 #デバイスセットアップの最適化が無効（デフォルト）

Mode=00000200 VID=067B PID=1230 #デバイスセットアップの最適化が有効

Wacom署名パッドデバイスのスクリーンセーバーを無効にする

Wacom署名パッドおよびタブレットを使用する場合は、Citrix®は次のようにスクリーンセーバーを無効にすることをお勧めします。

1. デバイスをリダイレクトした後、**Wacom-STU-Driver**をインストールします。
2. 署名パッドコントロールパネルにアクセスするには、**Wacom-STU-Display MSI**をインストールします。
3. **コントロールパネル > Wacom STU Display > STU430**または**STU530**に移動し、お使いのモデルのタブを選択します。
4. **変更**を選択し、UACセキュリティウィンドウが表示されたら**はい**を選択します。
5. **スライドショーを無効にする**を選択し、**適用**を選択します。

1つの署名パッドモデルに対して設定が行われると、その設定はすべてのモデルに適用されます。

クライアントUSBデバイスのリダイレクト

この設定により、USBデバイスのユーザーデバイスへのリダイレクトおよびユーザーデバイスからのリダイレクトを許可または禁止します。

デフォルトでは、USBデバイスはリダイレクトされません。

クライアントUSBデバイスリダイレクト規則

この設定は、USBデバイスのリダイレクトルールを指定します。

デフォルトでは、ルールは指定されていません。

ユーザーがUSBデバイスを接続すると、ホストデバイスは一致が見つかるまで、各ポリシー規則と照合して確認します。いずれかのデバイスに対する最初の一致が決定的なものと見なされます。最初の一致が許可ルールである場合、デバイスは仮想デスクトップにリモート接続されます。最初の一致が拒否ルールである場合、デバイスはローカルデスクトップでのみ使用できます。一致が見つからない場合は、デフォルトのルールが使用されます。

ポリシー規則は{Allow:`|`Deny:}の形式をとり、その後に空白で区切られたtag=value式のセットが続きます。次のタグがサポートされています。

タグ名	説明
VID	デバイス記述子からのベンダーID
PID	デバイス記述子からの製品ID
REL	デバイス記述子からのリリースID
クラス	デバイス記述子またはインターフェイス記述子のいずれかからのクラス

タグ名	説明
サブクラス	デバイス記述子またはインターフェース記述子のいずれかからのサブクラス
プロトコル	デバイス記述子またはインターフェイス記述子のいずれかからのプロトコル

ポリシールールを作成する際は、以下を覚えておいてください。

- ルールでは大文字と小文字は区別されません。
- ルールには、# で始まるオプションのコメントを末尾に含めることができます。
- 空行および純粋なコメント行は無視されます。
- タグは一致演算子 = を使用する必要があります (例: VID=067B_。
- 各ルールは新しい行で開始するか、セミコロンで区切られたリストの一部である必要があります。
- USB Implementers Forum, Inc. のWebサイトで入手可能なUSBクラスコードを参照してください。

管理者定義の USB ポリシールールの例:

- 許可: VID=067B PID=0007 # 別の産業、別のフラッシュドライブ
- 拒否: Class=08 subclass=05 # マスストレージ
- すべての USB デバイスを拒否するルールを作成するには、他のタグなしで「DENY:」を使用します。

クライアント USB プラグアンドプレイデバイスのリダイレクト

この設定により、カメラやPOS (Point-of-Sale) デバイスなどのプラグアンドプレイデバイスをクライアントセッションで使用することが許可または禁止されます。

デフォルトでは、プラグアンドプレイデバイスのリダイレクトは許可されています。「許可」に設定すると、特定のユーザーまたはグループのすべてのプラグアンドプレイデバイスがリダイレクトされます。「禁止」に設定すると、デバイスはリダイレクトされません。

USB デバイスの自動リダイレクトを構成する

USB サポートが有効になっている場合、USB デバイスは自動的にリダイレクトされます。また、USB ユーザー設定は USB デバイスを自動的に接続するように設定されています。

注:

Receiver for Windows 4.2では、デスクトップアプライアンスモードで動作している場合も、USBデバイスは自動的にリダイレクトされます。また、接続バーは表示されません。以前のバージョンのCitrix Receiver for Windowsでは、USBデバイスは以下のモードで動作している場合も自動的にリダイレクトされます。

- デスクトップアプライアンスモード
- 仮想マシン (VM) ホスト型アプリケーション

すべてのUSBデバイスをリダイレクトすることが常に最適とは限りません。ユーザーは、自動的にリダイレクトされないUSBデバイスリストからデバイスを明示的にリダイレクトできます。USBデバイスが一覧表示されたりリダイレクトされたりするのを防ぐには、クライアントエンドポイントまたはDDCポリシーのいずれかでDeviceRulesを使用します。詳細については、管理者ガイドを参照してください。

注意:

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

USBデバイスの自動リダイレクトに関するユーザー設定

ポリシー:

1. **ローカルグループポリシーエディター**を開き、**管理用テンプレート > Citrix Components > Citrix Receiver™ > クライアントデバイスのリモート処理 > Generic USB Remoting**に移動します。
2. **新しいUSBデバイス**を開き、**有効**を選択して**OK**をクリックします。
3. 「**既存のUSBデバイス**」を開き、「**有効**」を選択して、「**OK**」をクリックします。

シトリックス レシーバー：

1. **シトリックス レシーバー 環境設定 > 接続** に移動します。
2. 次のオプションが選択されていることを確認します。
   - セッション開始時にデバイスを自動的に接続する
   - セッション実行中に新しいデバイスが接続された場合、そのデバイスを自動的に接続する。
3. 「**OK**」をクリックします。

すべてのレジストリキーとポリシーの変更は、Windowsクライアントデバイスに適用されます。

通常のUSBプリンターのリダイレクト

通常のUSBプリンターに最適なソリューションは、専用のユニバーサルプリンタードライバーと仮想チャネルを使用して印刷を実行することです。デフォルトでは、通常のUSBプリンターは自動的にリダイレクトされません。

通常のプリンターはヒューリスティックを使用して検出されます。また、例えばスキャン機能を備えた高度なプリンターは、完全に機能させるにはUSBサポートを使用してリダイレクトする必要がある場合があります。

通常のプリンターが自動的にリダイレクトされるかどうかを構成するには、このレジストリを使用します。

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB\Devices

名前: AutoRedirectPrinters

種類: DWORD

データ: 00000000

既定値は0です (自動的にリダイレクトしません)。値を0より大きい任意の数値に変更すると、USBサポートが有効になり、通常のUSBプリンターをリダイレクトできるようになります。

Active Directoryポリシーをこのレジストリキーに展開することもでき、両方が存在する場合はポリシー以外の値を上書きできます。

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB\Devices

名前: AutoRedirectPrinters

種類: DWORD

データ: 00000000

通常のオーディオデバイスのリダイレクト

通常のプリンターと同様に、通常のオーディオデバイスからオーディオデータを送信するには、ICA®の専用オーディオ仮想チャネルを使用することで最高のユーザーエクスペリエンスが実現されます。ただし、一部の特殊なデバイスはUSBサポートを使用してリダイレクトする必要がある場合があります。どのデバイスが通常のオーディオデバイスであるかを判断するためにヒューリスティックが使用されます。

クライアントエンドポイントでこのレジストリを使用して、通常のオーディオデバイスが自動的にリダイレクトされるかどうかを構成します:

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB\Devices

名前: AutoRedirectAudio

種類: DWORD

データ: 00000000

既定値は0に設定されています (自動的にリダイレクトしません)。値を0以外に変更すると、USBサポートを使用して通常のUSBオーディオデバイスがリダイレクトされます。

Active Directoryポリシーを使用して、この値をレジストリキーに展開し、両方が存在する場合は非ポリシー値を上書きできます。

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB\Devices

名前: AutoRedirectAudio

種類: DWORD

データ: 00000000

プレーンなストレージデバイス (マスストレージデバイス) のリダイレクト

プレーンなストレージデバイスの場合、最適化も行うクライアントドライブマッピングなど、専用の仮想チャネルを使用することで、最高のユーザーエクスペリエンスを実現できます。ファイルの単純な読み書きに加えて、CD/DVDの書き込みや暗号化されたファイルシステムデバイスへのアクセスなど、特定の特殊なタスクを実行するには、ジェネリックUSBサポートを使用してデバイスをリダイレクトする必要がある場合があります。

どのデバイスがプレーンなストレージデバイスであるかを判断するために、ヒューリスティックが使用されます。プレーンなストレージデバイスを自動的にリダイレクトするかどうかを設定するには、このレジストリキーを使用します。

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB\Devices

名前: AutoRedirectStorage

種類: DWORD

データ: 00000000

デフォルトは0に設定されています（自動的にリダイレクトされません）。値を0以外に変更すると、汎用USBサポートを使用してプレーンUSBストレージデバイスがリダイレクトされます。

Active Directoryポリシーを使用して、この値を以下のレジストリキーに展開し、両方が存在する場合は非ポリシー値を上書きすることもできます。

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB\Devices

名前: AutoRedirectStorage

種類: DWORD

データ: 00000000

> **注記:**
>
> 汎用USBサポートを使用している場合、プレーンストレージデバイスへの読み取り専用アクセスは構成できませんが、CDMを使用している場合は構成できます。

ハードウェア暗号化機能付きUSBフラッシュドライブのリダイレクト

ハードウェア暗号化機能付きUSBフラッシュドライブは、通常、暗号化されたストレージパーティションと、暗号化されたパーティションのロックを解除するためのユーティリティが含まれる2つ目のユーティリティパーティションで構成されています。USBフラッシュドライブデバイスの場合、最適化も実行する専用のクライアントドライブマッピング/動的サムドライブマッピングHDX仮想チャネルを使用することで、最高のユーザーエクスペリエンスを実現できます。

汎用USBリダイレクトは、次の目的で必要です。

- Windows以外のクライアント（例：Linuxクライアント）
- 顧客がクライアント上のローカル機能へのユーザーアクセスを制限（ロックダウン）しているクライアント

汎用USBリダイレクトは、ハードウェア暗号化機能のない任意のUSBストレージデバイスを、シングルセッションOSおよびマルチセッションOS VDAセッションの両方にリダイレクトできます。

Citrix Virtual Apps and Desktops 7 1808より前は、ハードウェア暗号化機能付きUSBフラッシュドライブをシングルセッションOSまたはマルチセッションOS VDAセッションに有用な方法でリダイレクトすることはできませんでした。Citrix Virtual Apps and Desktops 7 1808で導入された新機能強化により、ハードウェア暗号化機能付きUSBフラッシュドライブの汎用USBリダイレクトがシングルセッションOSおよびマルチセッションOS VDAセッションにサポートされます。 デバイスがリダイレクトされた後、そのドライブはローカルクライアントに表示されません。したがって、ドライブのロック解除が必要な場合は、セッション内で実行してください。この機能にはWindows Update KB4074590が必要です。

プレーン静止画像デバイス（スキャナーおよびデジタルカメラ）

プレーン静止画像デバイスの場合、最適化も実行する専用の仮想チャネル（TWAIN仮想チャネルなど）を使用することで、最高のユーザーエクスペリエンスを実現できます。これらのデバイスは業界標準に準拠している必要があります。デバイスが非準拠であるか、本来の意図どおりに使用されていないと見なされる場合、汎用USBリダイレクトがデバイスを使用する唯一の方法となる可能性があります。どのデバイスがプレーン静止画像デバイスであるかを判断するためにヒューリスティックが使用されます。

プレーン静止画像デバイスが自動的にリダイレクトされるかどうかを構成するには、このレジストリキーを使用します。

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB\Devices

名前: AutoRedirectImage

種類: DWORD

データ: 00000000

デフォルトは0に設定されています（自動的にリダイレクトされません）。値を0以外に変更すると、汎用USBでプレーンなUSB静止画デバイスがリダイレクトされます。

Active Directoryポリシーを使用して、この値をこのレジストリキーに展開することもでき、両方が存在する場合は非ポリシー値を上書きします。

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB\Devices

名前: AutoRedirectImage

種類: DWORD

データ: 00000000

デバイス固有の設定

Citrix最適化可能デバイスを選択するために使用されるヒューリスティックは、必ずしもお客様の希望と一致するとは限りません。Citrix最適化可能デバイスの例としては、プリンター、オーディオ、ビデオ、ストレージ、静止画デバイスなどがあります。上記にリストされていないデバイスの自動リダイレクトを制御したい場合があります。デバイス固有の基準で自動リダイレクトを制御できます。

例として、DemoTech 2,000バーコードリーダーはUSBサポートを使用してリダイレクトする必要はありません。ベンダー識別子12ABと製品識別子5678を持っています。これらの16進数はデバイスマネージャーで確認できます。

これが自動的にリダイレクトされるのを防ぐには、このデバイス固有のレジストリキーを作成します。

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB\Devices\VID12AB PID5678

名前: AutoRedirect

種類: DWORD

データ: 00000000

値が0の場合、デバイスは自動的にリダイレクトされません。0以外の値は、デバイスが自動リダイレクトの対象となることを示します（ユーザー設定による）。ベンダー識別子と製品識別子の間には単一のスペース文字があります。

この値は、Active Directoryポリシーを使用してこのレジストリキーに展開することもできます。両方が存在する場合、ポリシー以外の値を上書きします。

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB\Devices\VID12AB PID5678

名前: AutoRedirect

種類: DWORD

データ: 00000000

デバイス固有のAutoRedirect設定は、上記で説明したより一般的なAutoRedirectXXX値よりも優先されます。Citrix最適化デバイスのデフォルトのヒューリスティックは、デバイスを汎用として

誤って解釈する可能性があります。したがって、デバイス固有のAutoRedirect値を1に設定して、自動的にリダイレクトします。

既存のUSBデバイスの自動接続を許可する

この設定は、セッション開始時にエンドポイントに接続されている既存のUSBデバイスがリモートセッションに自動接続されることを許可または禁止します。

この設定をポリシーに追加するときは、次のいずれかのオプションを選択します。

- 利用可能なUSBデバイスをリダイレクトする前に確認する。
- 利用可能なUSBデバイスを自動的にリダイレクトしない。
- 利用可能なUSBデバイスを自動的にリダイレクトする。

デフォルトでは、**利用可能なUSBデバイスをリダイレクトする前に確認する**オプションが選択されています。選択されたポリシーに基づいて、クライアントの**設定** > **デバイス**セクションで選択されたオプションを上書きできます。

> **注：**
>
> 現在、**既存のUSBデバイスの自動接続を許可する**ポリシーは、Windows版Citrix Workspace™アプリにのみ適用されます。

新しく接続されたUSBデバイスの自動接続を許可する

この設定は、セッション中にエンドポイントに挿入されたUSBデバイスのリモートセッションへの自動接続を許可または防止します。

この設定をポリシーに追加するときは、次のいずれかのオプションを選択します。

- 利用可能なUSBデバイスをリダイレクトする前に確認する。
- 利用可能なUSBデバイスを自動的にリダイレクトしない。
- 利用可能なUSBデバイスを自動的にリダイレクトする。

デフォルトでは、**利用可能なUSBデバイスをリダイレクトする前に確認する**オプションが選択されています。選択されたポリシーに基づいて、クライアントの**設定** > **デバイス**セクションで選択されたオプションを上書きできます。

> **注:**

> 現在、**新しく接続されたUSBデバイスの自動接続を許可する**ポリシーは、Windows版Citrix Workspaceアプリにのみ適用されます。

クライアントUSBデバイスリダイレクト規則（バージョン2）

この設定は、USBデバイスをリモートセッションにフィルタリング、分割、および自動接続するための規則を指定します。

この設定が選択されている場合、ホストは、*クライアント USB デバイスリダイレクト規則* 設定を、この設定で構成されたデバイス規則で上書きします。

詳しくは、「複合USBデバイスリダイレクトの構成」を参照してください。

仮想チャネル許可リストポリシー設定

仮想チャネル許可リストポリシー設定は、ICA®セッションで開くことが許可されている仮想チャネルを指定する許可リストの使用を有効にします。

無効にすると、すべての仮想チャネルが許可されます。

有効にすると、Citrix®仮想チャネルのみが許可されます。

カスタムまたはサードパーティの仮想チャネルを使用するには、仮想チャネルをリストに追加します。仮想チャネルをリストに追加するには：

1. 仮想チャネル名の後にコンマを入力します。
2. 仮想チャネルにアクセスするプロセスのパスを入力します。

複数の実行可能パスをリストでき、パスはコンマで区切られます。

例:

```
CTXCVC1,C:\VC1\vchost.exe
```

```
CTXCVC2,C:\VC2\vchost.exe,C:\Program Files\Third Party\vcaccess.exe
```

Citrix Virtual Apps and Desktops 7 2109以降、仮想チャネル許可リストはデフォルトで有効になっています。許可リストに仮想チャネルを追加する方法の詳細については、「許可リストへの仮想チャネルの追加」を参照してください。

Skype for Business向けHDX RealTime Optimization Packを使用している場合は、仮想チャネルを許可リストに追加します。詳細については、HDX RealTime Optimization Packのドキュメントを参照してください。

> **重要:**
>
> 設定を有効にするには、VDAマシンを再起動する必要があります。

> 仮想チャネルの詳細については、ICA 仮想チャネルを参照してください。

仮想チャネル許可リストのログ記録

このポリシー設定を使用して、仮想チャネル許可リストのログ記録レベルを構成できます。

次のオプションが利用可能です:

オプション	説明
無効	すべてのログイベントを無効にします。
警告のみをログに記録	許可リストに含まれていない、開こうとするカスタム仮想チャネルに対してのみイベントがログに記録されます。
すべてのイベントをログに記録	すべてのイベントがログに記録されます

仮想チャネル許可リストのログスロットリング

このポリシー設定を使用して、アクティブなセッションのイベントログ記録の頻度を構成できます。

各仮想チャネルのすべてのイベントは、最初に発生したときにログに記録されます。セッションがアクティブな間、スロットリング期間中は繰り返し発生するイベントは抑制されます。セッションが切断された場合、スロットリング期間はリセットされます。

DVC 用仮想チャネル許可リスト

ICA セッションで開くことが許可されている動的仮想チャネルを指定する許可リストの使用を有効にします。

無効にすると、すべての動的仮想チャネルが許可されます。

有効にすると、動的仮想チャネルは許可されません。この機能で動的仮想チャネル (DVC) を使用するには、DVC をリストに追加する必要があります。リストに DVC を追加するには、セッションホストで DVC にアクセスするプロセスのパスを入力し、その後にコンマ、次にクライアント側

プラグイン名、その後にコンマ、そしてプラグインが使用するリスナーの名前を入力します。複数のリスナー名はコンマで区切って追加できます。

ワイルドカードを使用して、プラグインがサポートするすべてのリスナーを許可できます。

ワイルドカードを使用して、プロセスパス内の単一のディレクトリ名を置き換えたり、プロセスパス内のディレクトリ名の一部を置き換えたり、実行可能ファイル名を置き換えたり、実行可能ファイル名の一部を置き換えたりすることもできます。

この設定への変更は、セッションホストを再起動した後にのみ適用されます。

例: クライアント側プラグイン: `DvcPlugin1.dll`, `DvcPlugin2.dll`, `DvcPlugin3.dll`

許可リストエントリ: `C:\Program Files\App\run1.2.exe,DvcPlugin1,` ListenerName1 `C:\Program Files*\run*.exe,DvcPlugin2,ListenerName1,ListenerName2` `C:\Program Files\App\run1.2.exe,DvcPlugin3,*`

視覚表示ポリシー設定

視覚表示セクションには、仮想デスクトップからユーザーデバイスに送信される画像の品質を制御するためのポリシー設定が含まれています。

単純なグラフィックの優先色深度

このポリシー設定は、VDAバージョン7.6 FP3以降で利用可能です。8ビットオプションは、VDAバージョン7.12以降で利用可能です。

この設定により、ネットワーク経由で単純なグラフィックが送信される際の色深度を下げることができます。ピクセルあたり8ビットまたは16ビットに下げることで、低帯域幅接続での応答性が向上する可能性があります。ただし、この操作により画質がわずかに低下する可能性があります。圧縮にビデオコーデックを使用 ポリシー設定が**画面全体**に設定されている場合、8ビットの色深度はサポートされません。

デフォルトの優先色深度はピクセルあたり24ビットです。

8ビット設定がVDAバージョン7.11以前に適用された場合、VDAは24ビット（デフォルト）の色深度にフォールバックします。

ターゲットフレームレート

この設定は、仮想デスクトップからユーザーデバイスに送信される1秒あたりの最大フレーム数を指定します。

デフォルトでは、最大は1秒あたり30フレームです。

1秒あたりのフレーム数を高く設定する（例：30）と、ユーザーエクスペリエンスは向上しますが、より多くの帯域幅を必要とします。1秒あたりのフレーム数を減らす（例：10）と、ユーザーエクスペリエンスを犠牲にしてサーバーのスケーラビリティが最大化されます。CPUが遅いユーザーデバイスの場合は、ユーザーエクスペリエンスを向上させるために低い値を指定してください。

サポートされる1秒あたりの最大フレームレートは60です。

視覚品質

この設定は、ユーザーデバイスに表示される画像の希望する視覚品質を指定します。

デフォルトでは、この設定は中（Medium）です。

画像の品質を指定するには、次のいずれかのオプションを選択します。

- **低** - 帯域幅が制限されたネットワークで、対話性のために視覚的な品質を犠牲にできる場合に推奨されます。
- **中** - ほとんどのユースケースで最高のパフォーマンスと帯域幅効率を提供します。
- **高** - 視覚的にロスレスな画質が必要な場合に推奨されます。
- **ロスレスにビルド** - ネットワークアクティビティが高い期間は非可逆画像をユーザーデバイスに送信し、ネットワークアクティビティが低下した後は可逆画像を送信します。この設定により、帯域幅が制限されたネットワーク接続でのパフォーマンスが向上します。
- **常にロスレス** - 画像データの保持が不可欠な場合は、非可逆データがユーザーデバイスに送信されないように、**常にロスレス**を選択します。たとえば、画質の劣化が許されないX線画像を表示する場合などです。

動画ポリシー設定

「**動画**」セクションには、動的画像の圧縮を削除または変更できる設定が含まれています。

最小画像品質

注：Virtual Delivery Agent 7.xの場合、このポリシー設定は、レガシーグラフィックモードポリシー設定が有効になっている場合にのみ適用されます。

この設定は、アダプティブディスプレイの許容される最小画像品質を指定します。使用される圧縮が少ないほど、表示される画像の品質は高くなります。超高、非常に高、高、標準、低のいずれかの圧縮から選択します。

デフォルトでは、これは標準に設定されています。

動画圧縮

この設定は、アダプティブディスプレイが有効になっているかどうかを指定します。アダプティブディスプレイは、利用可能な帯域幅に基づいて、スライドショー内のビデオやトランジションスライドの画質を自動的に調整します。アダプティブディスプレイが有効になっている場合、ユーザーは品質の低下なしにスムーズに実行されるプレゼンテーションを見ることができます。

デフォルトでは、アダプティブディスプレイは有効になっています。

VDAバージョン7.0から7.6の場合、この設定はレガシーグラフィックモードが有効になっている場合にのみ適用されます。VDAバージョン7.6 FP1以降の場合、この設定はレガシーグラフィックモードが有効になっている場合、またはレガシーグラフィックモードが無効でビデオコーデックがグラフィックの圧縮に使用されていない場合に適用されます。

レガシーグラフィックモードが有効になっている場合、ポリシー変更が有効になる前にセッションを再起動する必要があります。アダプティブディスプレイはプログレッシブディスプレイと相互排他的です。アダプティブディスプレイを有効にするとプログレッシブディスプレイが無効になり、その逆も同様です。ただし、プログレッシブディスプレイとアダプティブディスプレイの両方を同時に無効にすることができます。プログレッシブディスプレイはレガシー機能であるため、XenAppまたはXenDesktopには推奨されません。プログレッシブしきい値レベルを設定すると、アダプティブディスプレイが無効になります。

プログレッシブ圧縮レベル

注：Virtual Delivery Agent 7.xの場合、このポリシー設定は、レガシーグラフィックモードポリシー設定が有効になっている場合にのみ適用されます。

この設定により、詳細度は低いものの、画像の初期表示が高速になります。

デフォルトでは、プログレッシブ圧縮は適用されません。

通常の非可逆圧縮設定で定義された、より詳細な画像は、利用可能になったときに表示されます。写真などの帯域幅を多く消費するグラフィックの表示を改善するには、非常に高い圧縮または超高圧縮を使用します。

プログレッシブ圧縮を効果的にするには、その圧縮レベルが非可逆圧縮レベル設定よりも高くする必要があります。

注: プログレッシブ圧縮に関連する圧縮レベルの増加は、クライアント接続を介した動的画像の対話性も向上させます。回転する3Dモデルなどの動的画像の品質は、画像が動きを停止するまで一時的に低下し、その時点で通常の非可逆圧縮設定が適用されます。

関連するポリシー設定は次のとおりです。

- プログレッシブ圧縮のしきい値
- プログレッシブヘビーウェイト圧縮

プログレッシブ圧縮のしきい値

注: Virtual Delivery Agent 7.x の場合、このポリシー設定は、レガシーグラフィックモードポリシー設定が有効になっている場合にのみ適用されます。

この設定は、プログレッシブ圧縮が適用される接続の最大帯域幅をキロビット/秒で表します。これは、この帯域幅以下のクライアント接続にのみ適用されます。

デフォルトでは、しきい値は1秒あたり2147483647キロビットです。

関連するポリシー設定は次のとおりです。

- プログレッシブ圧縮のしきい値
- プログレッシブヘビーウェイト圧縮

目標最小フレームレート

この設定は、低帯域幅の条件下で、動的画像に対してシステムが維持しようとする1秒あたりの最小フレームレートを指定します。

デフォルトでは、これは10fpsに設定されています。

VDAバージョン7.0から7.6の場合、この設定はレガシーグラフィックモードが有効になっている場合にのみ適用されます。VDAバージョン7.6 FP1以降の場合、この設定はレガシーグラフィックモードが無効または有効になっている場合に適用されます。

> **注:**
>
> 目標最小フレームレートポリシーは非推奨となり、10 fpsに設定されています。これは、グラフィックステータスインジケーターの品質スライダーを使用してエンドユーザーが変更できます。

静止画像ポリシー設定

静止画像セクションには、静止画像の圧縮を削除または変更できる設定が含まれています。

追加の色圧縮

この設定は、帯域幅が制限されているクライアント接続を介して配信される画像に対する追加の色圧縮の使用を有効または無効にします。これにより、表示される画像の品質を低下させることで応答性が向上します。

デフォルトでは、追加の色圧縮は無効になっています。

有効にすると、追加の色圧縮は、クライアント接続の帯域幅が「追加の色圧縮しきい値」を下回っている場合にのみ適用されます。クライアント接続の帯域幅がしきい値を超えている場合、または「無効」が選択されている場合、追加の色圧縮は適用されません。

追加の色圧縮しきい値

注：Virtual Delivery Agent 7.xの場合、このポリシー設定は、レガシーグラフィックモードポリシー設定が有効になっている場合にのみ適用されます。

この設定は、追加の色圧縮が適用される接続の最大帯域幅をキロビット/秒で表します。クライアント接続の帯域幅が設定値を下回ると、有効になっている場合、追加の色圧縮が適用されます。

デフォルトでは、しきい値は8192キロビット/秒です。

ヘビーウェイト圧縮

注：Virtual Delivery Agent 7.xの場合、このポリシー設定は、レガシーグラフィックモードポリシー設定が有効になっている場合にのみ適用されます。

この設定は、より高度でCPU負荷の高いグラフィックアルゴリズムを使用することで、画質を損なうことなくプログレッシブ圧縮を超えて帯域幅を削減することを有効または無効にします。

デフォルトでは、ヘビーウェイト圧縮は無効になっています。

有効にすると、ヘビーウェイト圧縮はすべての非可逆圧縮設定に適用されます。Citrix Workspace™アプリでサポートされていますが、他のプラグインには影響しません。

関連するポリシー設定は次のとおりです。

- プログレッシブ圧縮レベル
- プログレッシブ圧縮しきい値

非可逆圧縮レベル

注：Virtual Delivery Agent 7.xの場合、このポリシー設定は、レガシーグラフィックモードポリシー設定が有効になっている場合にのみ適用されます。

この設定は、帯域幅が制限されているクライアント接続を介して配信される画像に使用される非可逆圧縮の度合いを制御します。このような場合、圧縮なしで画像を表示すると遅くなる可能性があります。

デフォルトでは、中程度の圧縮が選択されています。

帯域幅を多く消費する画像の応答性を向上させるには、高圧縮を使用します。画質の劣化が許容されないX線画像を表示する場合など、画像データの保持が不可欠な場合は、非可逆圧縮を使用しない方がよいでしょう。

関連するポリシー設定：非可逆圧縮しきい値

非可逆圧縮しきい値

注：Virtual Delivery Agent 7.xの場合、このポリシー設定は、レガシーグラフィックモードポリシー設定が有効になっている場合にのみ適用されます。

この設定は、非可逆圧縮が適用される接続の最大帯域幅を1秒あたりのキロビット数で表します。

デフォルトでは、しきい値は1秒あたり2147483647キロビットです。

ポリシーに非可逆圧縮レベル設定を追加し、しきい値を指定しないことで、LAN経由での写真などの高精細ビットマップの表示速度を向上させることができます。

関連するポリシー設定：非可逆圧縮レベル

HDX™ レジストリで管理される機能

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

> レジストリエディターを開くには、サーバーで `regedit.exe` を実行します。次に、設定を追加または編集するレジストリキーに移動します。

デバイス

Bloombergキーボード

Citrix Virtual Apps and Desktops™は、Bloombergモデル4およびモデル3のスターボードキーボードをサポートしています。デフォルトでは、拡張Bloombergキーボードのサポートは無効になっています。

Bloombergキーボードのサポートを有効にするには、接続を開始する前にクライアントマシンで次のレジストリ値を設定します。

- **キー**: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICAClient\GenericUSB`
- **値の名前**: `EnableBloombergHID`
- **値の型**: `DWORD`
- **値のデータ**:
  - `0` - 無効
  - `1` - 有効

詳しくは、「Bloombergキーボード」を参照してください。

マップされたクライアントドライブ

セキュリティ上の予防措置として、ユーザーがCitrix Virtual Apps and Desktopsにログオンすると、デフォルトでは、サーバーはユーザーの実行権限なしでクライアントドライブをマップします。マップされたクライアントドライブにある実行可能ファイルをユーザーが実行できるようにするには、サーバーのレジストリを編集してこのデフォルト設定を上書きします。

アクセスを許可するには、次のレジストリ値を編集します（**CDMSettings**が存在しない場合は作成します）。

- **キー**: `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\CDMSettings`
- **値の名前**: `ExecuteFromMappedDrive`
- **値の型**: `DWORD`
- **値のデータ**:
  - `1` - 許可
  - `0` - マップされたドライブでのアクセス拒否

この変更は、レジストリを編集した後に接続されたセッションに適用されます。

Citrix Virtual Apps and Desktops 7 2006は、このレジストリの場所を含む最初のバージョンです。以前のバージョンのCitrix Virtual Apps and Desktopsでは、異なるレジストリの場所が使用されていました。

詳細については、「クライアントドライブマッピング」を参照してください。

マイクロソフト Surface Pro および Surface Book ペン

Citrix Virtual Apps and Desktopsは、Windows Inkベースのアプリケーションで標準のペン機能をサポートしています。デフォルトでは、この機能は有効になっています。

この機能を無効または有効にするには、次のレジストリ値を設定します。

- **キー**: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Citrix Virtual Desktop Agent\PenApi`
- **値の名前**: `DisablePen`
- **値の型**: `DWORD`
- **値のデータ**:
  - `1` - 無効
  - `0` - 有効

詳細については、「」(/ja-jp/citrix-virtual-apps-desktops/2503/devices/mobile-devices.html#microsoft-surface-pro-and-surface-book-pens)を参照してください。

Windows イメージ取得アプリケーションの許可リスト

この設定により、VDA 上のどのアプリケーションが Windows イメージ取得スキャナーリダイレクトにアクセスできるかを制御できます。

デフォルトでは、どのアプリケーションも Windows イメージ取得にアクセスできません。

VDA 上のアプリケーションに対して Windows イメージ取得を調整するには、次のレジストリ設定を作成します。

- **キー**: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix`
- **値の名前**: `WIAAllowedProcesses`

  WIAAllowedProcesses を選択して右クリックします。「**新規 > 複数行文字列値**」を選択し、新しい値を **AllowProcesses** に名前変更します。
- 値のデータ: Windows イメージ取得にアクセスできる各アプリケーションの完全なパスとプロセス名を入力します。各アプリケーションを新しい行に入力してください。

この設定への変更は、次回 VDA でセッションを起動したときに有効になります。

全般

HDX リデューサー

セッションホストで使用するHDX圧縮アルゴリズム（Reducer）のバージョンを構成できます。

シングルセッションVDAでReducer V4を有効にするには、次のレジストリ値を設定します。

キー: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\GroupPolicy\Defaults\WDSettings` **値の名前**: `ReducerOverrideMask` **値の型**: `DWORD` **値のデータ**: `23` (10進数)

マルチセッションVDAでReducer V4を有効にするには、次のレジストリ値を設定します。

- **キー**: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd`
- **値の名前**: `ReducerOverrideMask`
- **値の型**: `DWORD`
- **値のデータ**: `23` (10進数)

Rendezvousバージョンの構成

使用するRendezvousのバージョンを構成するには、次のレジストリ値を設定します:

- **キー**: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\VirtualDesktopAgent`
- **値の型**: `DWORD`
- **値の名前**: `GctRegistration`
- **値のデータ**:
  - `1` - V2 を有効にする
  - `0` - V1 を有効にする

VDA への自動ログオンを構成する

この設定により、Windows 10 シングルセッション OS およびマルチセッション OS VDA で、**常にパスワードの入力を求める** Microsoft ポリシー設定を有効または無効にできます。

常にパスワードの入力を求める が有効になっている場合、ユーザーはリモートセッションを開始する際に VDA で資格情報を入力する必要があります。この設定が無効になっている場合、ユーザーは VDA で資格情報を入力することなく、リモートセッションに自動的に接続します。

デフォルトでは、Microsoft ポリシー設定は無効になっています。**常にパスワードの入力を求める** 設定を有効または無効にするには、VDA で次のレジストリ値を設定します。

- **キー**: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Portica`
- **値の名前**: `AutoLogon`
- **値の型**: `DWORD`
- **値のデータ**:
  - `1` - Microsoft ポリシー設定を無効にし、ユーザーがリモートセッションに自動的にサインインできるようにします。

- `0` – Microsoft ポリシー設定を有効にし、ユーザーがリモートセッションを起動する際に資格情報の入力を求めます。

タイムアウト警告を無効にする

デフォルトでは、非アクティブまたはアイドル状態のセッションを持つユーザーは、セッションが自動的に切断される2分前に警告メッセージを受け取ります。

この設定は、以下のアイドルセッションタイムアウト制限に達したユーザーに対する警告メッセージを無効にし、削除します。

- ウィンドウズ サーバー 2004
- Windows 10 マルチセッション 2004 以降のマルチセッション OS

警告を削除するには、VDAで以下のレジストリ値を設定します。

- **キー**: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Winstations\ICA-CGP`
- **値の名前**: `fEnableTimeoutWarning`
- **値の型**: `DWORD`
- **値のデータ**:
  - `1` - 警告メッセージを無効にする
  - `0` - 警告メッセージを有効にする

警告メッセージを表示するには、レジストリ値を削除するか、`0`に設定します。

EDT MTU検出

MTU検出により、EDTはセッション確立時に最大転送単位（MTU）を自動的に決定できます。これにより、パフォーマンスの低下やセッション確立の失敗につながる可能性のあるEDTパケットの断片化を防ぎます。

この設定はデフォルトで有効になっています。EDT MTU検出を無効にするには、以下のレジストリ値を構成し、セッションホストを再起動します。

- **キー**: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd`
- **値の名前**: `MtuDiscovery`
- **値の型**: `DWORD`
- **値のデータ**: `0`

MTU Rediscovery を有効にするには、以下のレジストリ値を構成し、セッションホストを再起動します。

- **キー:** `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd\MtuRediscovery`
- **値の名前:** `MtuReDiscovery`
- **値の型:** `DWORD`
- **値のデータ:** `1`
- **キー:** `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd\MtuRediscovery`
- **値の名前:** `MtuReDiscoveryFrequency`
- **値の型:** `DWORD`
- **値のデータ:** `1`

これらの設定はマシン全体に適用され、サポートされているクライアントから接続するすべてのセッションに影響します。

EDTタイムアウト

VDAのEDTタイムアウトは5秒から25秒の間の任意の値に設定できます。デフォルトのEDTタイムアウト値は10秒です。

- **キー**: `HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd\Tds\udp\UDPStackParameters`
- **値の型**: `DWORD`
- **値の名前**: `edtConnectionTimeout`
- **値のデータ**: 5〜25秒（10進数）

Citrix Workspaceアプリ for Windows バージョン2409.10以前の場合も、EDTタイムアウトを設定できます。

- **キー**: `HKLM\SOFTWARE\WOW6432Node\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\EDT`
- **値の型**: `String / REG_SZ`
- **値の名前**: `edtConnectionTimeout`
- **値のデータ**: 5〜25秒（10進数）

> **注：**

> バージョン2503以降のCitrix Workspaceアプリでは、VDAからのタイムアウト設定が使用されるため、クライアントデバイスでタイムアウトを設定する必要がなくなります。

一般的なコンテンツリダイレクト

ホストからクライアントへのリダイレクト用のURLタイプを追加する

デフォルトでは、HTTP、HTTPS、RTSP、RTSPU、PNM、MMSのURLタイプのリダイレクトをサポートしています。Windowsクライアントで以下のレジストリキーと値を作成することで、URLタイプをリストに追加できます。

- **キー**: `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Policies\Citrix\ICA Client\SFTA`
- **値の名前**: `ExtraURLProtocols`
- **値の型**: `REG_SZ`
- **値のデータ**: 必要なURLタイプをセミコロンで区切って指定します。URLの権限部分より前のすべてを含めます。例: `ftp://;mailto:;customtype1://;customtype2://`

URLタイプはWindowsクライアントにのみ追加できます。このレジストリ設定がないクライアントは、Citrixセッションへのリダイレクトを拒否します。クライアントには、指定されたURLタイプを処理するようにインストールおよび構成されたアプリケーションが必要です。

詳細については、「」を参照してください(/ja-jp/citrix-virtual-apps-desktops/2503/general-content-redirection/bidirectional-content-redirection-configuration/host-to-client-redirection.html)。

クライアントフォルダーリダイレクト

クライアントフォルダーリダイレクトは、クライアント側のファイルがホスト側のセッションでアクセス可能になる方法を変更します。サーバーでクライアントフォルダーリダイレクトを有効にし、ユーザーがユーザーデバイスでそれを構成するとします。この場合、ユーザーによって指定されたローカルボリュームの一部がリダイレクトされます。

サーバーでクライアントフォルダーリダイレクトを有効にするには、次のレジストリ値を設定します。

- **キー**: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\Client Folder Redirection`
- **値の名前**: `CFROnlyModeAvailable`
- **値の型**: `DWORD`

- **値のデータ**: `1`

詳細については、「」を参照してください(/ja-jp/citrix-virtual-apps-desktops/2503/general-content-redirection/client-folder-redirection.html)。

特定のWebサイトセットに対するホストからクライアントへのリダイレクト

特定のWebサイトセットに対してホストからクライアントへのリダイレクトを有効にするには、サーバーVDAで次のレジストリ値を設定します。

- **キー**: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\SFTA`
- **値の名前**: `ValidSites`
- **値の型**: `REG_MULTI_SZ`
- **値のデータ**: 任意の組み合わせの完全修飾ドメイン名 (FQDN) を指定します。複数のFQDNは別々の行に入力します。プロトコル (`http://` または `https://`) を含めず、FQDNのみを含めます。FQDNには、ワイルドカード文字としてアスタリスク (`*`) を左端の位置にのみ含めることができます。このワイルドカードは、RFC 6125の規則に準拠して、単一レベルのドメインに一致します。例:

`www.example.com`

`*.example.com`

詳細については、「ホストからクライアントへのリダイレクト」を参照してください。

ログオフ時および切断時のローカルアプリケーションの動作

デフォルトでは、ユーザーが仮想デスクトップからログオフまたは切断しても、ローカルアプリケーションは実行を継続します。再接続後、ローカルアプリケーションが仮想デスクトップで利用可能な場合、それらは再統合されます。ログオフ時および切断時のローカルアプリケーションの動作を構成するには、ホストされたデスクトップで次のレジストリ値を設定します。

- **キー**: `HKEY_LOCAL_MACHINE\SOFTWARE\wow6432node\Citrix\Client Hosted Apps\Policies`
- **値の名前**: `Session State`
- **値の型**: `DWORD`
- **値のデータ**:
  - `1` - ユーザーが仮想デスクトップからログオフまたは切断しても、ローカルアプリケーションは引き続き実行されます。再接続すると、ローカルアプリケーションが仮想デスクトップで利用可能な場合、再統合されます。

- `3` - ユーザーが仮想デスクトップからログオフまたは切断すると、ローカルアプリケーションは閉じます。

詳細については、「ローカルアプリアクセスとURLリダイレクト」を参照してください。

ホストからクライアントへのリダイレクトのデフォルトリストからURLタイプを削除する

デフォルトのリダイレクトリストからURLタイプを削除するには、サーバーVDAで以下のレジストリキーと値を作成します。

- **キー**: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\SFTA`
- **値の名前**: `DisableServerFTA`
- **値の型**: `DWORD`
- **値のデータ**: `1`
- **値の名前**: `NoRedirectClasses`
- **値の型**: `REG_MULTI_SZ`
- **値のデータ**: 次の値を任意の組み合わせで指定します: `http`, `https`, `rtsp`, `rtspu`, `pnm`, または `mms`。複数の値を指定する場合は、それぞれを別の行に入力します。例:

`http`

`https`

`rtsp`

詳細については、「ホストからクライアントへのリダイレクト」を参照してください。

Server VDA のデフォルトブラウザ構成

Server VDA 上のデフォルトのブラウザ構成を上書きするために、ホストからクライアントへのリダイレクトを有効にできます。Web URL がリダイレクトされない場合、Citrix ランチャーは `command_backup` レジストリキーで構成されたブラウザに URL を渡します。このキーはデフォルトで Internet Explorer を指していますが、別のブラウザへのパスを含むように変更できます。

- Internet Explorer (デフォルト)
  - **キー**: `HKEY_CLASSES_ROOT\http\shell\open\command_backup`
  - **値の名前**: `Default`
  - **値の型**: `REG_SZ`
  - **値のデータ**: `"c:\program files\internet explorer\iexplore.exe" "%1"`

  - **キー**: `HKEY_CLASSES_ROOT\https\shell\open\command_backup`
  - **値の名前**: `Default`
  - **値の型**: `REG_SZ`
  - **値のデータ**: `"c:\program files\internet explorer\iexplore.exe" "%1"`

- グーグル クローム
  - **キー**: `HKEY_CLASSES_ROOT\http\shell\open\command_backup`
  - **値の名前**: `Default`
  - **値の型**: `REG_SZ`
  - **値のデータ**: `"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" "%1"`
  - **キー**: `HKEY_CLASSES_ROOT\https\shell\open\command_backup`
  - **値の名前**: `Default`
  - **値の型**: `REG_SZ`
  - **値のデータ**: `"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" "%1"`

- マイクロソフト エッジ
  - **キー**: `HKEY_CLASSES_ROOT\http\shell\open\command_backup`
  - **値の名前**: `Default`
  - **値の型**: `REG_SZ`
  - **値のデータ**: `"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" "%1"`
  - **キー**: `HKEY_CLASSES_ROOT\https\shell\open\command_backup`
  - **値の名前**: `Default`
  - **値の型**: `REG_SZ`
  - **値のデータ**: `"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" "%1"`

公開アプリケーションのローカルアプリアクセス

Local App Access は、ローカルにインストールされた Windows アプリケーションを、デスクトップを切り替えることなくホストされたデスクトップ環境にシームレスに統合します。公開アプリケーションへのアクセスを提供するには、サーバーで次のレジストリ値を設定します。

- **キー**: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\DesktopStudio`
- **値の名前**: `ClientHostedAppsEnabled`
- **値の型**: `DWORD`
- **値のデータ**:
  - `1` - 有効
  - `0` - 無効

詳細については、「Local App Access と URL リダイレクト」を参照してください。

グラフィック

CUDA または OpenCL アプリケーションの GPU アクセラレーション

ユーザーセッションで実行されている CUDA および OpenCL アプリケーションの GPU アクセラレーションは、デフォルトで無効になっています。

CUDA アクセラレーション POC 機能を使用するには、次のレジストリ設定を有効にします。

- **キー**: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\CtxHook\AppInit_Dlls\Graphics Helper`
- **値の名前**: `CUDA`
- **値の型**: `DWORD`
- **値のデータ**: `00000001`

OpenCLアクセラレーションPOC機能を使用するには、次のレジストリ設定を有効にします。

- **キー**: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\CtxHook\AppInit_Dlls\Graphics Helper`
- **値の名前**: `OpenCL`
- **値の型**: `DWORD`
- **値のデータ**: `00000001`

詳細については、WindowsマルチセッションOSのGPUアクセラレーションを参照してください。

プログレッシブモード

プログレッシブモードはデフォルトで無効になっています。次のレジストリ値でプログレッシブモードの状態を変更できます:

- **キー**: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics`
- **値の型**: `REG_DWORD`
- **値の名前**: `ProgressiveDisplay`
- **値のデータ**:
  - `0` - 常にオフ (プログレッシブモードを無効にします。この値がデフォルトです。)
  - `1` - 自動 (ネットワークの状態に基づいて切り替えます。)
  - 2 = 常にオン

詳細については、「プログレッシブモード」を参照してください。

> **注:**
>
> プログレッシブモードは非推奨になりました。Thinwireは、プログレッシブモードのほぼすべての利点を提供しながら、画像配信を最適化し、キャッシュ効率を維持する代替オプションです。

Windows Presentation Foundation (WPF) レンダリング

HDX 3D Proを使用すると、Windows Multi-session OSセッションで実行されているグラフィック負荷の高いアプリケーションを、サーバーのグラフィック処理ユニット（GPU）でレンダリングできます。Windows Presentation Foundation（WPF）レンダリングをサーバーのGPUに移行することで、グラフィックレンダリングがサーバーのCPUの速度を低下させることはありません。

サーバーのGPUを使用してWPFアプリケーションのレンダリングを有効にするには、WindowsマルチセッションOSを実行しているサーバーのレジストリに次の設定を作成します。

1. VDAでレジストリエディターを開き、次のキーに移動します。

   `HKLM\Software\Citrix\CtxHook\AppInit_DLLs\Graphics Helper`

2. 次のレジストリ値を作成または編集します。

   - AdapterHandle = 0x00000001

- DevicePath = 0x00000001
- フラグ = 0x00000412
- WPF = 0x00000001

3. WPFアプリの実行可能ファイル名でサブキーを作成します。たとえば、アプリが「mywpfapp.exe」という名前の場合、次のキーを作成します。

```
HKLM\Software\Citrix\CtxHook\AppInit_DLLs\Graphics Helper\mywpfapp.exe
```

4. 設定を有効にするには、サーバーを再起動します。

詳細については、「WindowsマルチセッションOS向けGPUアクセラレーション」および「WindowsマルチセッションOSでWPFアプリを最大限に活用する」のブログを参照してください。

マルチメディア

マルチメディア会議中のエコーを回避する

Citrix Virtual Apps and Desktopsは、エコーを最小限に抑えるエコーキャンセルオプションを提供します。この機能はデフォルトで有効になっています。エコーキャンセルを無効にするには、次のいずれかのレジストリ設定を変更できます。

- **キー**:
  - 32ビット: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ClientAudio`
  - 64ビット: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ClientAudio`
- **値の名前**: `EchoCancellation`
- **値の型**: `String/REG_SZ`
- **値のデータ**: `False`

詳細については、「オーディオ機能」を参照してください。

オーディオの制限

クライアントにオーディオデバイスをインストールし、オーディオリダイレクトを有効にしてRDSセッションを開始した後、オーディオファイルが再生されない場合があります。回避策として、RDSマシンに以下のレジストリキーを追加し、マシンを再起動してください。

- **キー**: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SCMConfig`

- **値の名前**: `EnableSvchostMitigationPolicy`
- **値の型**: `DWORD`
- **値のデータ**: `0`

詳細については、オーディオ機能を参照してください。

高解像度Webカメラの解像度

メディアタイプのネゴシエーションが失敗した場合、HDXはデフォルトのVGA解像度（640 x 480 ピクセル）にフォールバックします。クライアント上のレジストリキーを使用して、デフォルトの解像度を構成できます。以下のレジストリキーを設定する前に、カメラが指定された解像度をサポートしていることを確認してください。

- **キー**: `HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXRealTime`
- 幅
  - **値の名前**: `DefaultWidth`
  - **値の型**: `DWORD`
  - **値のデータ**: 10進数で指定する希望の幅（例：1280）
- 高さ
  - **値の名前**: `DefaultHeight`
  - **値の型**: `DWORD`
  - **値のデータ**: 10進数での希望の高さ (例: 720)

Microsoft Teamsのフォールバックモード

Microsoft Teamsが最適化されたVDIモードでロードに失敗した場合 (Teams/バージョン情報/バージョンで「Citrix HDX未接続」と表示される場合)、VDAは、ウェブカメラのリダイレクトやクライアントのオーディオおよびマイクのリダイレクトなど、従来のHDXテクノロジーにフォールバックします。Microsoft Teamsの最適化をサポートしないWorkspaceアプリのバージョン/プラットフォームOSを使用している場合、フォールバックレジストリキーは適用されません。

フォールバックメカニズムを制御するには、VDAで次のいずれかのレジストリ値を設定します。

- **キー** (いずれか1つのみ必要):
  - **コンピューター設定:** `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Teams`
  - **ユーザー設定:** `HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\Teams`

- **値の名前**: `DisableFallback`
- **値の型**: `DWORD`
- 値のデータ:
  - `1` - フォールバックモードを無効にする
  - `2` - オーディオのみを有効にする

値が存在しないか0に設定されている場合、フォールバックモードが有効になります。この機能には、Microsoft Teamsバージョン1.3.0.13565以降が必要です。詳細については、「Microsoft Teamsの最適化」を参照してください。

Citrix App Layering™を使用したMicrosoft Teamsの最適化

Citrix App Layeringを使用してVDAとMicrosoft Teamsのインストールを異なるレイヤーで管理している場合、コマンドラインから`ALLUSER=1`フラグを使用してMicrosoft Teamsをインストールする前に、Windows上に**PortICA**という名前の空のレジストリキーを作成します。デフォルトの値の名前、型、およびデータはそのままにしておきます。

- レジストリエディターの32ビット版のキー:
  `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\PortICA`
- レジストリエディターの64ビット版のキー:
  `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`

詳細については、「Microsoft Teamsの最適化」を参照してください。

Webカメラのソフトウェア圧縮

Webカメラがハードウェアエンコードをサポートしている場合、HDXビデオ圧縮はデフォルトでハードウェアエンコードを使用します。ハードウェアエンコードは、ソフトウェアエンコードよりも多くの帯域幅を消費する可能性があります。ソフトウェア圧縮を強制するには、クライアントに次の値を追加します。

- **キー**: `HKEY_CURRENT_USER\SOFTWARE\Citrix\HdxRealTime`
- **値の名前**: `DeepCompress_ForceSWEncode`
- **値の型**: `DWORD`
- **値のデータ**: `1`

詳細については、HDX webcam video compressionを参照してください。

Webカメラビデオ圧縮

HDX Webカメラビデオ圧縮は、H.264ビデオを仮想セッションで実行されているビデオ会議アプリケーションに直接送信します。VDAリソースを最適化するために、HDX Webカメラ圧縮はWebカメラビデオのエンコード、トランスコード、デコードを行いません。この機能はデフォルトで有効になっています。

サーバーからビデオ会議アプリへの直接ビデオストリーミングを無効にするには、VDAで次のレジストリ値を設定します。

- **キー**: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxRealTime`
- **値の名前**: `OfferH264ToApp`
- **値の型**: `DWORD`
- **値のデータ**: `0`

詳細については、「」(/ja-jp/citrix-virtual-apps-desktops/2503/multimedia/webcam-compression.html)を参照してください。

ウェブカメラビデオ圧縮のフレームレート

優先するビデオフレームレートを調整するには、クライアントで次のレジストリ値を編集します:

- **キー**: `HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXRealTime`
- **値の名前**: `FramesPerSecond`
- **値の型**: `DWORD`
- **値のデータ**: `15`

ウェブカメラが指定されたフレームレートをサポートしていない場合、アプリケーションはデフォルトで15 FPSを使用します。

詳細については、「」(/ja-jp/citrix-virtual-apps-desktops/2503/multimedia/webcam-compression.html)を参照してください。

負荷管理ポリシー設定

負荷管理セクションには、WindowsマルチセッションOSマシンを提供するサーバー間の負荷管理を有効化および構成するためのポリシー設定が含まれています。

負荷評価インデックスの計算については、CTX202150を参照してください。

同時ログオン許容数

この設定は、サーバーが受け入れ可能な同時ログオンの最大数を指定します。

デフォルトでは、この値は2に設定されています。

この設定が有効な場合、負荷分散は、指定された数を超えるログオンが同時にサーバーVDAでアクティブにならないように試みます。ただし、この制限は厳密には適用されません。制限を適用し（指定された数を超える同時ログオンを失敗させる）、次のレジストリキーを作成します。

> HKLM\Software\Citrix\DesktopServer\LogonToleranceIsHardLimit 種類: DWORD 値: 1

CPU使用率

この設定は、サーバーがフルロードを報告するCPU使用率のレベルをパーセンテージで指定します。有効にすると、サーバーがフルロードを報告するデフォルト値は90%です。

デフォルトでは、この設定は無効になっており、CPU使用率は負荷計算から除外されます。

CPU使用率から除外されるプロセスの優先度

> **注：**

> Workspace Environment Managementがマシンを管理するシナリオでは、この設定をCPU優先度設定と併用すると、意図しない結果が生じる可能性があります。CPU優先度設定を使用する場合は、この設定を無効にすることをお勧めします。

> この設定は、プロセスのCPU使用率がCPU使用率負荷インデックスから除外される優先度レベルを指定します。

デフォルトでは、この値は**標準以下**または**低**に設定されています。

ディスク使用量

この設定は、サーバーが75%のフルロードを報告するディスクキューの長さを指定します。有効にすると、ディスクキューのデフォルト値は8です。

デフォルトでは、この設定は無効になっており、ディスク使用率は負荷計算から除外されます。

セッションの最大数

この設定は、サーバーがホストできるセッションの最大数を指定します。有効にすると、サーバーがホストできるセッションの最大数のデフォルト設定は250になります。

デフォルトでは、この設定は有効になっています。

メモリ使用量

この設定は、サーバーがフルロードを報告するメモリ使用量のレベルをパーセンテージで指定します。有効にすると、サーバーがフルロードを報告するデフォルト値は90%になります。

デフォルトでは、この設定は無効になっており、メモリ使用量は負荷計算から除外されます。

メモリ使用量のベースロード

この設定は、ベースオペレーティングシステムのメモリ使用量の近似値を指定します。また、サーバーがゼロロードと見なされるメモリ使用量をMB単位で定義します。

デフォルトでは、この値は768 MBに設定されています。

プロファイル管理ポリシー設定

このセクションには、プロファイル管理を有効化および構成するためのポリシー設定が含まれています。

以下のようなその他の情報については、プロファイル管理ポリシーを参照してください。

- 対応する.iniファイル設定の名前
- ポリシー設定に必要なプロファイル管理のバージョン

高度なポリシー設定

ロックされたファイルへのアクセス時の再試行回数

ロックされたファイルへのアクセス時の再試行回数を設定します。

このポリシーが無効になっている場合、デフォルト値の5回の再試行が使用されます。このポリシーがここで構成されていない場合、.iniファイルの値が使用されます。このポリシーがここでも.iniファイルでも構成されていない場合、デフォルト値が使用されます。

ログオフ時にインターネットCookieファイルを処理する

一部の展開では、`Index.dat` が参照しない余分なインターネットCookieが残されます。継続的なブラウジングの後、ファイルシステムに残された余分なCookieは、プロファイルの肥大化につながる可能性があります。このポリシーを使用すると、Profile Managementを有効にして

Index.datの処理を強制し、余分なCookieを削除できます。このポリシーはログオフ時間を増加させるため、この問題が発生した場合にのみ有効にしてください。

構成の優先順位:

1. このポリシーがここで構成されていない場合、.iniファイルの値が使用されます。
2. このポリシーがここでも.iniファイルでも構成されていない場合、Index.datの処理は行われません。

自動構成を無効にする

Profile Managementは、Citrix Virtual Desktops™環境（たとえば、パーソナルvDiskの有無など）を検査し、それに応じてグループポリシーを構成します。未構成状態のProfile Managementポリシーのみが調整されるため、行ったカスタマイズはすべて保持されます。

このポリシーを使用すると、展開を高速化し、最適化を簡素化できます。このポリシーを構成する必要はありません。ただし、次のいずれかの操作を行うときに自動構成を無効にすることができます。

- 以前のバージョンからの設定を保持するためにアップグレードする
- トラブルシューティング

自動構成は、実行時に環境に応じてデフォルトのポリシー設定を自動的に構成する動的な構成チェッカーと見なすことができます。これにより、設定を手動で構成する必要がなくなります。実行時環境には以下が含まれます。

- ウィンドウズ OS
- Windows OS のバージョン
- シトリックス バーチャル デスクトップの有無
- パーソナルvDisk の有無

環境が変更された場合、自動構成によって以下のポリシーが変更される可能性があります。

- アクティブライトバック
- 常にキャッシュ
- ログオフ時にローカルにキャッシュされたプロファイルを削除
- キャッシュされたプロファイルを削除するまでの遅延
- プロファイルストリーミング

異なる OS でのポリシーのデフォルトの状態については、次の表を参照してください。

	マルチセッションOS	シングルセッションOS
アクティブライトバック	有効	Personal vDiskが使用されている場合は*無効*。それ以外の場合は有効。
常にキャッシュ	無効	Personal vDiskが使用されている場合は*無効*。それ以外の場合は有効。
ログオフ時にローカルにキャッシュされたプロファイルを削除	有効	Personal vDiskが使用されている、Citrix Virtual Desktopsが割り当てられている、またはCitrix Virtual Desktopsがインストールされていない、のいずれかの状況が発生した場合は*無効*。それ以外の場合は有効。
キャッシュされたプロファイルを削除するまでの遅延	0秒	ユーザーの変更が永続的でない場合は60秒。それ以外の場合は0秒。
プロファイルストリーミング	有効	Personal vDiskが使用されている場合は*無効*。それ以外の場合は、有効。

ただし、自動構成が無効になっている場合、上記のすべてのポリシーは既定で**無効**になります。

重要:

Personal vDiskは非推奨です。詳細については、PVD、AppDisk、およびサポートされていないホストの削除を参照してください。

Profile Management 1909以降、Windows 10（バージョン1607以降）のスタートメニューで改善されたエクスペリエンスを得ることができます。この改善は、以下のポリシーの自動構成によって実現されます。

- `Appdata\Local\Microsoft\Windows\Caches` と `Appdata\Local\Packages` を **ミラーリングするフォルダー**に追加します。

- `Appdata\Local\Microsoft\Windows\UsrClass.Dat*` を **同期するファイル**に追加します。

構成の優先順位:

1. この設定がここで構成されていない場合、.iniファイルの値が使用されます。
2. この設定がここでも.iniファイルでも構成されていない場合、自動構成が有効になります。この場合、環境が変更されると、Profile Managementの設定が変更される可能性があります。

問題が発生した場合にユーザーをログオフする

問題が発生した場合に Profile Management がユーザーをログオフさせるかどうかを指定できます。

このポリシーが無効になっているか、構成されていない場合、問題が発生すると Profile Management はユーザーに一時プロファイルを提供します。たとえば、ユーザー ストアが利用できない場合などです。

これが有効になっている場合、エラーメッセージが表示され、ユーザーはログオフされます。この設定により、問題のトラブルシューティングが簡素化されます。

構成の優先順位:

1. この設定がここで構成されていない場合、.ini ファイルの値が使用されます。
2. この設定がここでも .ini ファイルでも構成されていない場合、一時プロファイルが提供されます。

カスタマー エクスペリエンス向上プログラム

デフォルトでは、Citrix®製品の品質とパフォーマンスを向上させるために、匿名の統計情報と使用状況データを収集するカスタマーエクスペリエンス向上プログラムが有効になっています。

この設定がここで構成されていない場合、.ini ファイルの値が使用されます。

Outlook の検索インデックス ローミングを有効にする

ユーザープロファイルとともに Outlook 検索データを自動的にローミングすることで、ユーザーベースの Outlook 検索エクスペリエンスを許可します。この機能には、Outlook の検索インデックスを保存するために、ユーザー ストアに追加のスペースが必要です。

このポリシーを有効にするには、ログオフしてから再度ログオンしてください。

Outlook 検索インデックス データベース – バックアップと復元

Outlook の検索インデックス ローミングを有効にするポリシーが有効になっている場合に、ログオン中に Profile Management が何を行うかを指定できます。

このポリシーが有効になっている場合、Profile Management は、ログオン時に検索インデックス データベースが正常にマウントされるたびに、そのデータベースをバックアップします。Profile Management は、そのバックアップを検索インデックス データベースの良好なコピーとして扱います。データベースの破損により検索インデックス データベースのマウントが失敗した場合、Profile Management は検索インデックス データベースを最後に確認された良好なコピーに戻します。

> 注：
>
> 新しいバックアップが正常に保存されると、Profile Managementは以前に保存されたバックアップを削除します。バックアップは利用可能なVHDXストレージを消費します。

OUTLOOK検索データローミングの同時セッションサポートを有効にする

Profile Managementにより、同じユーザーの同時セッションでネイティブのOutlook検索エクスペリエンスが提供されます。このポリシーは、Outlookの検索インデックスローミングポリシーと併用してください。

このポリシーが有効な場合、各同時セッションは個別のOutlook OSTファイルを使用します。

デフォルトでは、Outlook OSTファイルを保存するために使用できるVHDXディスクは2つのみです（ディスクごとに1ファイル）。ユーザーがさらにセッションを開始すると、Outlook OSTファイルはローカルユーザープロファイルに保存されます。Outlook OSTファイルを保存するためのVHDXディスクの最大数を指定できます。

ONEDRIVEコンテナを有効にする

OneDriveフォルダーをユーザーと共にローミングできるようにします。

OneDriveコンテナは、VHDXベースのフォルダーローミングソリューションです。Profile Managementは、ファイル共有上にユーザーごとにVHDXファイルを作成し、ユーザーのOneDriveフォルダーをVHDXファイルに保存します。VHDXファイルは、ユーザーがログオンするときにアタッチされ、ログオフするときにデタッチされます。

UWPアプリのローミング

UWP (Universal Windows Platform) アプリをユーザーと共にローミングできるようにします。これにより、ユーザーは異なるデバイスから同じUWPアプリにアクセスできます。

このポリシーを有効にすると、Profile ManagementはUWPアプリを個別のVHDXディスクに保存することで、ユーザーと共にローミングできるようにします。これらのディスクは、ユーザーのログオン時にアタッチされ、ログオフ時にデタッチされます。

構成の優先順位:

1. ここでこの設定が構成されていない場合、.iniファイルの値が使用されます。
2. ここでも.iniファイルでもこの設定が構成されていない場合、この機能は無効になります。

UWPアプリのロード高速化を有効にする

UWPアプリの読み込み高速化を有効にします。これにより、UWPアプリの読み込みを高速化し、非永続環境での一貫性を向上させることができます。デフォルトでは、WindowsはUWPアプリの登録情報を各マシンにローカルに保存しますが、非永続環境では再起動時に失われる可能性があります。このポリシーを有効にすると、Profile Managementは各マシン用にVHDXコンテナを作成してUWPアプリの登録データを保存し、ユーザーログオンを高速化し、再起動時のデータ損失を防ぎます。

構成の優先順位:

1. GPO、Studio、またはWorkspace Experience Management (WEM) を使用してこの設定が構成されていない場合、.iniファイルの値が使用されます。
2. どこにもこの設定が構成されていない場合、この機能は無効になります。

ログオン時のユーザーグループポリシーの非同期処理を有効にする

Windowsは、ユーザーグループポリシーに同期と非同期の2つの処理モードを提供します。Windowsは、次のユーザーログオンの処理モードを決定するためにレジストリ値を使用します。レジストリ値が存在しない場合、同期モードが適用されます。レジストリ値はマシンレベルの設定であり、ユーザーと共にローミングしません。したがって、ユーザーが次の条件の場合、非同期モードは期待どおりに適用されません。

- 異なるマシンにログオンする。
- ログオフ時にローカルにキャッシュされたプロファイルを削除するポリシーが有効になっている同じマシンにログオンする。

このポリシーを有効にすると、レジストリ値はユーザーとともにローミングされます。その結果、ユーザーがログオンするたびに処理モードが適用されます。

VHDディスクの圧縮をトリガーする空き領域の比率

VHDディスクの圧縮を有効にするが有効な場合に適用されます。VHDディスクの圧縮をトリガーする空き領域比率を指定できます。ユーザーログオフ時に空き領域比率が指定された値を超えると、ディスクの圧縮がトリガーされます。

空き領域の比率 = (現在のVHDファイルサイズ – 必要な最小VHDファイルサイズ*) ÷ 現在のVHDファイルサイズ

* Microsoft Windowsオペレーティングシステムの`MSFT_Partition`クラスのGetSupportedSizeメソッドを使用して取得されます。

VHDディスクの圧縮をトリガーするログオフ回数

VHDディスクの圧縮を有効にする が有効な場合に適用されます。VHDディスクの圧縮をトリガーするユーザーログオフ回数を指定できます。

最後の圧縮以降のログオフ回数が指定された値に達すると、ディスク圧縮が再度トリガーされます。

VHDディスク圧縮のデフラグを無効にする

VHDディスクの圧縮を有効にするが有効な場合に適用されます。VHDディスク圧縮のファイルデフラグを無効にするかどうかを指定できます。

VHDディスク圧縮が有効な場合、VHDディスクファイルはまずWindows組み込みの`defrag`ツールを使用して自動的にデフラグされ、その後圧縮されます。VHDディスクのデフラグはより良い圧縮結果をもたらしますが、無効にすることでシステムリソースを節約できます。

プロファイルコンテナのマルチセッションライトバックを有効にする

マルチセッションシナリオでプロファイルコンテナへの書き戻しを有効にします。有効にすると、すべてのセッションでの変更がプロファイルコンテナに書き戻されます。そうでない場合、最初のセッションのみがプロファイルコンテナで読み取り/書き込みモードであるため、最初のセッションでの変更のみが保存されます。Citrix Profile Managementプロファイルコンテナは Citrix Profile Management 2103以降でサポートされています。FSLogix Profile ContainerはCitrix Profile Management 2003以降でサポートされています。

FSLogix Profile Container でこのポリシーを使用するには、次の前提条件が満たされていることを確認してください。

- FSLogix Profile Container 機能がインストールされ、有効になっていること。
- FSLogix でプロファイルタイプが **Try for read-write profile and fallback to read-only** に設定されていること。

ユーザーストアのレプリケート

ログオンおよびログオフごとに、リモートユーザープロファイルストアを複数のパスにレプリケートできます。これにより、Profile Management はユーザーログオンのプロファイル冗長性を提供できます。

このポリシーを有効にすると、システムI/Oが増加し、ログオフが長くなる可能性があります。

> **注:**
>
> この機能は、ファイルベースとコンテナベースの両方のプロファイルソリューションで利用できます。

ユーザーストアへの資格情報ベースのアクセスを有効にする

デフォルトでは、Citrix Profile Management は現在のユーザーを偽装してユーザーストアにアクセスします。Profile Management がユーザーストアにアクセスする際に現在のユーザーを偽装しないようにする場合は、この機能を有効にしてください。現在のユーザーがアクセス権を持たないストレージリポジトリ（例：Azure Files）にユーザーストアを配置できます。

Profile Management がユーザーストアにアクセスできるようにするには、プロファイルストレージサーバーの資格情報を Workspace Environment Management™ (WEM) または Windows 資格情報マネージャーに保存します。Profile Management が実行される各マシンで同じ資格情報を構成する必要をなくすために、Workspace Environment Management を使用することをお勧めします。Windows 資格情報マネージャーを使用する場合は、ローカルシステムアカウントを使用して資格情報を安全に保存してください。

> **注:**
>
> このポリシーは、ファイルベースとVHDXベースの両方のユーザーストアで利用できます。Profile Management のバージョン2212より前では、このポリシーはVHDXベースのユーザーストアでのみ利用できます。

> 構成の優先順位：

1. ここでこの設定が構成されていない場合、.iniファイルの値が使用されます。
2. この設定がここまたは.iniファイルで構成されていない場合、デフォルトで無効になります。

VHDXファイルのストレージパスをカスタマイズする

Profile Managementは、次のVHDXベースのポリシーを提供します: プロファイルコンテナ、Outlookの検索インデックスローミング、およびフォルダミラーリングの高速化。デフォルトでは、VHDXファイルはユーザーストアに保存されます。このポリシーを使用すると、それらを保存するための別のパスを指定できます。

VHDコンテナのデフォルト容量

VHDコンテナのデフォルトのストレージ容量（GB単位）を指定できます。

構成の優先順位:

1. ここでこの設定が構成されていない場合、.ini ファイルの値が使用されます。
2. ここで、または .ini ファイルでこの設定が構成されていない場合、デフォルトで無効になります。

VHDX ファイルのストレージ パスをカスタマイズする

Profile Management は、プロファイル コンテナー、Outlook の検索インデックス ローミング、フォルダー ミラーリングの高速化といった VHDX ベースのポリシーを提供します。デフォルトでは、VHDX ファイルはユーザー ストアに保存されます。このポリシーを使用すると、それらを保存する別のパスを指定できます。

このポリシーが有効になっている場合、Profile ManagementはVHDXベースのポリシーによって使用されているVHDXディスクを監視します。いずれかのディスクがデタッチされた場合、Profile Managementはディスクを自動的に再アタッチします。

プロファイルコンテナの自動拡張しきい値

プロファイルコンテナが自動拡張をトリガーするストレージ容量の使用率を指定できます。

構成の優先順位:

- このポリシーがここで構成されていない場合、.iniファイルの値が使用されます。
- このポリシーがここまたは.iniファイルで構成されていない場合、デフォルトはストレージ容量の90%です。

プロファイルコンテナの自動拡張増分

自動拡張がトリガーされたときに、プロファイルコンテナが自動的に拡張するストレージ容量（GB単位）を指定できます。

構成の優先順位:

- このポリシーがここで構成されていない場合、.iniファイルの値が使用されます。
- このポリシーがここまたは.iniファイルで構成されていない場合、デフォルトは10 GBです。

プロファイルコンテナの自動拡張制限

自動拡張がトリガーされたときに、プロファイルコンテナが自動的に拡張できる最大ストレージ容量（GB単位）を指定できます。

構成の優先順位:

- このポリシーがここで構成されていない場合、.iniファイルの値が使用されます。
- このポリシーがここまたは.iniファイルで構成されていない場合、デフォルトは80 GBです。

ユーザーレベルのポリシー設定を有効にする

このポリシーが有効になっている場合、マシンレベルのポリシー設定はユーザーレベルで機能し、ユーザーレベルの設定がマシンレベルの設定を上書きします。

構成の優先順位:

1. ここでこのポリシーが構成されていない場合、.iniファイルの値が使用されます。
2. ここででも.iniファイルでもこのポリシーが構成されていない場合、無効になります。

ユーザーグループの優先順位を設定する

ユーザーグループの優先順位を指定できます。この順序は、ユーザーが異なるポリシー設定を持つ複数のグループに属している場合に、どのグループが優先されるかを決定します。

ユーザーが競合するポリシー設定を持つ複数のグループに属している場合、以下を考慮してください:

- ユーザーがこのポリシーで定義されている1つ以上のグループに属している場合、最も優先順位の高いグループが優先されます。
- ユーザーがこのポリシーで定義されているどのグループにも属していない場合、アルファベット順で最も早くリストされているSIDを持つグループが優先されます。

ユーザーストアの選択方法

複数のユーザーストアが利用可能な場合に、ユーザーストアの選択方法を指定できます。オプションは次のとおりです:

- **構成順序。** Profile Managementは、最初に構成されたストアを選択します。
- **アクセスパフォーマンス。** Profile Managementは、最適なアクセスパフォーマンスを持つストアを選択します。

構成の優先順位:

1. ここでこの設定が構成されていない場合、.ini ファイルの値が使用されます。
2. ここでも .ini ファイルでもこの設定が構成されていない場合、**構成順序**が使用されます。

ユーザーストア間のセッション内プロファイルコンテナフェールオーバーを有効にする

デフォルトでは、複数のユーザーストアが展開されている場合、プロファイルコンテナのフェールオーバーはユーザーログオン時にのみ発生します。その結果、プロファイルの冗長性はユーザーログオン時にのみ利用可能です。このポリシーにより、フェールオーバーの範囲をセッション全体に拡大し、セッション全体でプロファイルの冗長性を確保できます。このポリシーが有効になっている場合、セッション中にProfile Managementがアクティブなプロファイルコンテナへの接続を失うと、自動的に別の利用可能なプロファイルコンテナに切り替わります。

構成の優先順位:

1. ここでこのポリシーが構成されていない場合、.ini ファイルの値が使用されます。
2. ここでも .ini ファイルでもこのポリシーが構成されていない場合、この設定は無効になります。

プロファイル読み込みタイムアウト

プロファイル読み込みタイムアウト機能を有効にし、タイムアウト期間を構成できます。Citrix Profile Managementは、指定されたタイムアウト時間、ユーザープロファイルの読み込みを待機し、その後一時プロファイルに切り替えます。 デフォルトでは、**プロファイル読み込みタイムアウト**設定は45秒で、有効な範囲は0～1800秒です。プロファイルの読み込みをバイパスして一時プロファイルを使用するには、タイムアウトを0秒に設定します。

構成の優先順位:

1. ここでこのポリシーが構成されていない場合、.ini ファイルの値が使用されます。
2. ここでも .ini ファイルでもこのポリシーが構成されていない場合、このポリシーはデフォルトで無効になります。

ログオフ時のプロファイル同期を制限する

ユーザー ログオフ時に同期されるユーザー ストアの数を指定できます。 デフォルトでは、Citrix Profile Management はログオフ中にすべてのユーザー ストアを同期し、すべてのストアでプロファイルが同期されるまでログオフは完了しません。 同期されるストアの数を減らすと、ログオフが高速化されます。非永続マシンでは、未同期のストアは次回のユーザー セッション中に更新され、永続マシンでは、未同期のストアはバックグラウンドで同期されます。

構成の優先順位:

1. このポリシーがここで構成されていない場合、.iniファイルの値が使用されます。
2. このポリシーがここでも.iniファイルでも構成されていない場合、ポリシーはデフォルトで無効になります。\n\n注: この設定は、ユーザー ストアのレプリケートポリシーが有効になっている場合にのみ適用されます。

プロファイルサイズがクォータを超過した場合にユーザーに通知する

ユーザープロファイルのクォータを設定し、プロファイルサイズがそれを超過した場合にユーザーに通知できます。

構成の優先順位:

1. このポリシーがここで構成されていない場合、.iniファイルの値が使用されます。
2. このポリシーがここでも.iniファイルでも構成されていない場合、この設定は無効になります。

プロファイルサイズがクォータを超過した場合の通知メッセージ

プロファイルサイズがクォータを超過した場合にユーザーに通知するポリシーが有効な場合に適用されます。ユーザーが受け取る通知メッセージを設定できます。

構成の優先順位:

1. このポリシーがここで構成されていない場合、.iniファイルの値が使用されます。
2. このポリシーがここでも.iniファイルでも構成されていない場合、この設定は無効になります。

基本的なポリシー設定

このセクションには、Profile Management の基本的な構成に関連するポリシー設定が含まれています。

Profile Management を有効にする

デフォルトでは、展開を容易にするため、Profile Management はログオンまたはログオフを処理しません。Profile Management は、他のすべてのセットアップタスクを実行し、Citrix® ユーザープロファイルが環境でどのように動作するかをテストした後にのみ有効にしてください。

このポリシーがここで構成されていない場合、.ini ファイルの値が使用されます。このポリシーがここでも .ini ファイルでも構成されていない場合、Profile Management は Windows ユーザープロファイルを一切処理しません。

処理されるグループ

コンピューターローカルグループとドメイングループ（ローカル、グローバル、ユニバーサル）の両方を使用できます。ドメイングループは、DOMAIN NAME\GROUP NAME の形式で指定する必要があります。

このポリシーがここで構成されている場合、Profile Management はこれらのユーザーグループのメンバーのみを処理します。このポリシーが無効になっている場合、Profile Management はすべてのユーザーを処理します。このポリシーがここで構成されていない場合、.ini ファイルの値が使

用されます。このポリシーがここでも .ini ファイルでも構成されていない場合、すべてのユーザーグループのメンバーが処理されます。

除外されるグループ

コンピューターローカルグループとドメイングループ（ローカル、グローバル、ユニバーサル）を使用して、特定のユーザープロファイルが処理されないようにすることができます。ドメイングループは、DOMAIN NAME\ GROUP NAME の形式で指定します。

この設定がここで構成されている場合、Profile Management はこれらのユーザーグループのメンバーを除外します。この設定が無効になっている場合、Profile Management はどのユーザーも除外しません。この設定がここで構成されていない場合、.ini ファイルの値が使用されます。この設定がここでも .ini ファイルでも構成されていない場合、どのグループのメンバーも除外されません。

ローカル管理者によるログオンの処理

BUILTIN\Administrators グループのメンバーによるログオンを処理するかどうかを指定します。Citrix Virtual Apps 環境などのマルチセッションオペレーティングシステムでは、このポリシーが無効になっているか、構成されていないと見なされます。この場合、Profile Management は、ローカル管理者ではなくドメインユーザーによるログオンを処理する必要があると想定します。シングルセッションオペレーティングシステム（Citrix Virtual Desktops 環境など）では、ローカル管理者によるログオンが処理されます。このポリシーにより、ローカル管理者権限を持つドメインユーザー（通常、割り当てられた仮想デスクトップを持つ Citrix Virtual Desktops ユーザー）は、次のことを行えます。

- 処理をバイパスする
- ログオンする
- Profile Managementで問題が発生しているデスクトップのトラブルシューティング

注：ドメインユーザーのログオンは、通常、製品ライセンスへの準拠を確実にするために、グループメンバーシップによって課される制限の対象となる場合があります。 このポリシーが無効になっている場合、Profile Managementはローカル管理者によるログオンを処理しません。このポリシーがここで構成されていない場合、.iniファイルの値が使用されます。このポリシーがここでも.iniファイルでも構成されていない場合、管理者は処理されません。

ユーザーストアへのパス

ユーザー設定（レジストリの変更と同期されたファイル）が保存されるディレクトリ（ユーザーストア）へのパスを設定します。

パスは次のいずれかです。

- 相対パス。ホームディレクトリ（通常、Active Directoryのユーザーの#homeDirectory#属性として構成されます）に対する相対パスである必要があります。
- UNCパス。通常、サーバー共有またはDFS名前空間を指定します。
- 無効または未構成。この場合、#homeDirectory#\Windowsの値が想定されます。

このポリシーでは、次の種類の変数を使用できます。

- パーセント記号で囲まれたシステム環境変数（例: %ProfVer%）。システム環境変数は通常、追加のセットアップが必要です。
- ハッシュで囲まれたActive Directoryユーザーオブジェクトの属性（例: #sAMAccountName#）。
- Profile Management変数。詳細については、Profile Management変数の製品ドキュメントを参照してください。

`%username%` と `%userdomain%` を除き、ユーザー環境変数は使用できません。場所やユーザーなどを完全に定義するために、カスタム属性を作成することもできます。属性では大文字と小文字が区別されます。

例:

- \\server\share#sAMAccountName# は、ユーザー設定をUNCパス \\server\share\JohnSmith に保存します（現在のユーザーに対して #sAMAccountName# が JohnSmith に解決される場合）。
- \\server\profiles$\%USERNAME%.%USERDOMAIN%\!CTX_OSNAME!!CTX_OSBITNESS! は \\server\profiles$\JohnSmith.DOMAINCONTROLLER1\Win8x64 に展開される場合があります。

重要: どの属性または変数を使用する場合でも、このポリシーが NTUSER.DAT を含むフォルダーの1つ上のレベルのフォルダーに展開されることを確認してください。たとえば、このファイルが \\server\profiles$\JohnSmith.Finance\Win8x64\UPM_Profile に含まれている場合、ユーザー ストアへのパスは \\server\profiles$\JohnSmith.Finance\Win8x64 (\UPM_Profile サブフォルダーではない) に設定します。

ユーザー ストアへのパスを指定する際の変数の使用に関する詳細は、以下のトピックを参照してください。

- 複数のファイルサーバーで Citrix ユーザープロファイルを共有する
- OU 内および OU 間でプロファイルを管理する
- プロファイル管理を使用した高可用性と災害復旧

「ユーザー ストアへのパス」が無効になっている場合、ユーザー設定はホームディレクトリの Windows サブディレクトリに保存されます。

このポリシーが無効になっている場合、ユーザー設定はホームディレクトリの Windows サブディレクトリに保存されます。このポリシーがここで構成されていない場合、.ini ファイルの値が使用されます。このポリシーがここでも .ini ファイルでも構成されていない場合、ホームドライブの Windows ディレクトリが使用されます。

ユーザーストアの移行

ユーザー設定（レジストリの変更と同期されたファイル）が以前に保存されていたフォルダーへのパス（以前使用していたユーザー ストアのパス）を指定します。

この設定が構成されている場合、以前のユーザー ストアに保存されているユーザー設定は、「ユーザー ストアへのパス」ポリシーで指定された現在のユーザー ストアに移行されます。

パスは絶対 UNC パスでも、ホームディレクトリに対する相対パスでも構いません。

どちらの場合も、以下の種類の変数を使用できます。

- パーセント記号で囲まれたシステム環境変数
- ハッシュ記号で囲まれた Active Directory ユーザーオブジェクトの属性

例:

- `Windows\%ProfileVer%`フォルダーは、ユーザー ストアの`Windows\W2K3`というサブフォルダーにユーザー設定を保存します (%ProfileVer%がW2K3に解決されるシステム環境変数である場合)。
- `\\server\share#SAMAccountName#`は、ユーザー設定をUNCパス`\\server\share\<JohnSmith>`に保存します (`#SAMAccountName#`が現在のユーザーに対してJohnSmithに解決される場合)。

パスでは、`%username%`と`%userdomain%`を除くユーザー環境変数を使用できます。

この設定が無効になっている場合、ユーザー設定は現在のユーザーストアに保存されます。

この設定がここで構成されていない場合、.iniファイルからの対応する設定が使用されます。

この設定がここで、または.iniファイルで構成されていない場合、ユーザー設定は現在のユーザーストアに保存されます。

アクティブライトバック

変更されたファイルとフォルダー (レジストリ エントリを除く) は、セッション中に、ログオフ前にユーザー ストアに同期できます。

このポリシーがここで構成されていない場合、.iniファイルの値が使用されます。このポリシーがここで、または.iniファイルで構成されていない場合、有効になります。

オフラインプロファイルのサポート

このポリシーにより、プロファイルは可能な限り早い機会にユーザー ストアと同期できます。これは、ローミングするラップトップまたはモバイルデバイスのユーザーを対象としています。ネットワーク接続が切断されても、再起動または休止状態の後でも、プロファイルはラップトップまたはデバイス上でそのまま維持されます。モバイルユーザーが作業すると、プロファイルはローカルで更新されます。また、ネットワーク接続が再確立されると、最終的にユーザー ストアと同期されます。

このポリシーがここで構成されていない場合、.iniファイルの値が使用されます。このポリシーがここで、または.iniファイルで構成されていない場合、オフラインプロファイルは無効になります。

アクティブライトバックレジストリ

このポリシーは「アクティブな書き戻し」と併用してください。変更されたレジストリ エントリは、セッション中にユーザー ストアに同期できます。

ここでこの設定を構成しない場合、.iniファイルの値が使用されます。

ここでも.iniファイルでもこの設定を構成しない場合、アクティブライトバックレジストリは無効になります。

セッションロックおよび切断時のアクティブライトバック

このポリシーと**アクティブなライトバック**ポリシーの両方が有効になっている場合、プロファイルファイルとフォルダーは、セッションがロックまたは切断された場合にのみ書き戻されます。

このポリシーと**アクティブなライトバック**および**アクティブなライトバックレジストリ**ポリシーの両方が有効になっている場合、レジストリエントリは、セッションがロックまたは切断された場合にのみ書き戻されます。

オフラインプロファイルのサポート

オフラインプロファイル機能を有効にします。この機能は、ネットワークから頻繁に切断されるコンピューター向けです。たとえば、サーバーやデスクトップではなく、ラップトップやモバイルデバイスなどです。

ここでこの設定が構成されていない場合、.iniファイルの値が使用されます。

ここでも.iniファイルでもこの設定が構成されていない場合、オフラインプロファイルのサポートは無効になります。

クロスプラットフォームポリシー設定

このセクションには、**Profile Management クロスプラットフォーム**設定機能を構成するためのポリシー設定が含まれています。

クロスプラットフォーム設定を有効にする

デフォルトでは、展開を容易にするために、クロスプラットフォーム設定は無効になっています。このポリシーを有効にすることで処理をオンにできますが、この機能の十分な計画とテストを行った後にのみ行ってください。

ここでこのポリシーが構成されていない場合、.iniファイルの値が使用されます。ここで、または.iniファイルでこのポリシーが構成されていない場合、クロスプラットフォーム設定は適用されません。

クロスプラットフォーム設定ユーザーグループ

1つ以上のWindowsユーザーグループを入力します。たとえば、このポリシーを使用して、テストユーザーグループのプロファイルのみを処理することができます。このポリシーが構成されている場合、Profile Managementのクロスプラットフォーム設定機能は、これらのユーザーグループのメンバーのみを処理します。このポリシーが無効になっている場合、この機能は「処理済みグループ」ポリシーで指定されたすべてのユーザーを処理します。

ここでこのポリシーが構成されていない場合、.iniファイルの値が使用されます。ここで、または.iniファイルでこのポリシーが構成されていない場合、すべてのユーザーグループが処理されます。

クロスプラットフォーム定義へのパス

ダウンロードパッケージからコピーした定義ファイルのネットワーク上の場所を識別します。このパスはUNCパスである必要があります。ユーザーはこの場所への読み取りアクセス権を持ち、管理者は書き込みアクセス権を持っている必要があります。この場所は、Server Message Block (SMB)またはCommon Internet File System (CIFS)ファイル共有である必要があります。

ここでこのポリシーが構成されていない場合、.iniファイルの値が使用されます。ここで、または.iniファイルでこのポリシーが構成されていない場合、クロスプラットフォーム設定は適用されません。

クロスプラットフォーム設定ストアへのパス

ユーザーのクロスプラットフォーム設定が保存されるフォルダーであるクロスプラットフォーム設定ストアへのパスを設定します。ユーザーはこの領域への書き込みアクセス権を持っている必要があります。パスは絶対UNCパスまたはホームディレクトリに対する相対パスにすることができます。

この領域は、複数のプラットフォームで共有されるプロファイルデータが配置されるユーザーストアの共通領域です。ユーザーはこの領域への書き込みアクセス権を持っている必要があります。パスは絶対UNCパスまたはホームディレクトリに対する相対パスにすることができます。**Path to user store** と同じ変数を使用できます。

このポリシーが無効になっている場合、パスWindows\PM_CPが使用されます。ここでこのポリシーが構成されていない場合、.iniファイルの値が使用されます。ここで、または.iniファイルでこのポリシーが構成されていない場合、デフォルト値が使用されます。

クロスプラットフォーム設定を作成するためのソース

このポリシーがそのプラットフォームのOUで有効になっている場合、プラットフォームをベースプラットフォームとして指定します。このポリシーは、ベースプラットフォームのプロファイルからクロスプラットフォーム設定ストアにデータを移行します。

各プラットフォーム独自のプロファイルセットは、別々のOUに保存されます。クロスプラットフォーム設定ストアをシードするために、どのプラットフォームのプロファイルデータを使用するかを決定する必要があります。これはベースプラットフォームと呼ばれます。クロスプラットフォーム設定ストアにデータのない定義ファイルが含まれている場合、または単一プラットフォームプロファイルのキャッシュデータがストア内の定義データよりも新しい場合を考慮してください。この場合、このポリシーを無効にしない限り、プロファイル管理は単一プラットフォームプロファイルからストアにデータを移行します。

> **重要:**
>
> このポリシーが複数のOU、または複数のユーザーオブジェクトやマシンオブジェクトで有効になっている場合、最初にユーザーがログオンするプラットフォームがベースプロファイルになります。 デフォルトでは、このポリシーは有効です。

ファイルシステム ポリシー設定

このセクションには、以下を設定するポリシーが含まれています。

- ユーザープロファイル内のどのファイルが、プロファイルがインストールされているシステムとユーザー ストアの間で同期されるか
- ユーザープロファイル内のどのディレクトリが、プロファイルがインストールされているシステムとユーザー ストアの間で同期されるか

除外ポリシー設定

このセクションでは、ユーザープロファイル内のどのファイルとディレクトリを同期プロセスから除外するかを設定するためのポリシー設定について説明します。

除外リスト - ファイル

同期中に無視されるファイルのリスト。ファイル名はユーザープロファイル (%USERPROFILE%) に対する相対パスである必要があります。ワイルドカードはファイル名とフォルダー名でサポートされていますが、ファイル名のワイルドカードのみが再帰的に適用されます。

例:

- `Desktop\Desktop.ini` は、`Desktop` フォルダー内のファイル `Desktop.ini` を無視します
- `%USERPROFILE%*.tmp` は、プロファイル全体の拡張子 `.tmp` を持つすべてのファイルを無視します
- `AppData\Roaming\MyApp*.tmp` は、プロファイルの一部にある拡張子 `.tmp` を持つすべてのファイルを無視します
- `Downloads*\a.txt` は、`Downloads` フォルダーの直下のサブフォルダーにある `a.txt` を無視します。

このポリシーが無効になっている場合、ファイルは除外されません。このポリシーがここで構成されていない場合、.ini ファイルの値が使用されます。このポリシーがここでも .ini ファイルでも構成されていない場合、ファイルは除外されません。

デフォルトの除外リストを有効にする - ディレクトリ

同期中に無視されるディレクトリのデフォルトリスト。このポリシーを使用して、GPO除外ディレクトリを手動で入力することなく指定します。

このポリシーを無効にすると、Profile Management はデフォルトでどのディレクトリも除外しません。

このポリシーをここで構成しない場合、Profile Management は .ini ファイルの値を使用します。このポリシーをここでも .ini ファイルでも構成しない場合、Profile Management はデフォルトでどのディレクトリも除外しません。

除外リスト - ディレクトリ

同期中に無視されるフォルダーのリスト。フォルダー名はユーザープロファイル (%USERPROFILE%) に対する相対パスとして指定する必要があります。フォルダー名でのワイルドカードはサポートされていますが、再帰的には適用されません。

例:

- `Desktop` は、ユーザープロファイル内の `Desktop` フォルダーを無視します。

このポリシーが無効になっている場合、フォルダーは除外されません。このポリシーがここで構成されていない場合、.iniファイルの値が使用されます。このポリシーがここで、または.iniファイルで構成されていない場合、フォルダーは除外されません。

ログオン除外チェック

この設定は、ユーザーストア内のプロファイルに除外されたファイルまたはフォルダーが含まれている場合に、Profile Managementが実行する動作を構成します。可能なポリシー設定とそれに対応するアクションを次の表に示します。

ポリシー設定	アクション
設定が無効になっているか、「ログオン時に除外されたファイルまたはフォルダーを同期する」の値がデフォルトに設定されている	ユーザーがログオンすると、Profile Managementはユーザーストアからローカルプロファイルに除外されたファイルまたはフォルダーを同期します。
設定が「ログオン時に除外されたファイルまたはフォルダーを無視する」に設定されている	ユーザーがログオンすると、Profile Managementはユーザーストア内の除外されたファイルまたはフォルダーを無視します。
設定が「ログオン時に除外されたファイルまたはフォルダーを削除する」に設定されている	ユーザーがログオンすると、Profile Managementはユーザーストア内の除外されたファイルまたはフォルダーを削除します。
設定がWeb Studioで構成されていない	.ini ファイルの値が使用されます
Web Studio または .ini ファイルで設定が構成されていません	ユーザーがログオンすると、除外されたファイルまたはフォルダーがユーザー ストアからローカル プロファイルに同期されます。

大容量ファイルの処理 - シンボリックリンクとして作成されるファイル

ログオンパフォーマンスを向上させ、サイズの大きいファイルを処理するために、Profile Management はこのリスト内のファイルをコピーする代わりにシンボリックリンクを作成します。

ファイルを参照するポリシーではワイルドカードを使用できます。例: `!ctx_localappdata!\Microsoft\Outlook*.OST`。

Microsoft Outlook のオフラインフォルダーファイル (`*.ost`) を処理するには、**Outlook** フォルダーが Profile Management の対象から除外されていないことを確認してください。

これらのファイルは、複数のセッションで同時にアクセスすることはできません。

同期ポリシー設定

同期セクションでは、プロファイルがインストールされているシステムとユーザー ストアの間で、ユーザー プロファイル内のどのファイルとフォルダーを同期するかを指定するためのポリシー設定について説明します。

同期するディレクトリ

デフォルトでは、Profile Management は、ユーザー プロファイルがインストールされているシステムとユーザー ストアの間でユーザー プロファイルを同期します。同期からフォルダーを除外した場合、このポリシーを使用すると、除外されたフォルダーのサブフォルダーを同期に含めることができます。

このリストのパスは、ユーザー プロファイルに対する相対パスである必要があります。フォルダー名でのワイルドカードはサポートされていますが、再帰的には適用されません。

このポリシーがここで構成されていない場合、.ini ファイルの値が使用されます。このポリシーがここでも .ini ファイルでも構成されていない場合、ユーザー プロファイル内の除外されていないフォルダーのみが同期されます。

同期するファイル

デフォルトでは、Profile Management は、ユーザー プロファイルがインストールされているシステムとユーザー ストアの間でユーザー プロファイルを同期します。同期からフォルダーを除外した場合、このポリシーを使用すると、除外されたフォルダー内のファイルを同期に含めることができます。

このリストのパスは、ユーザー プロファイルに対する相対パスである必要があります。ファイル名とフォルダー名でワイルドカードがサポートされていますが、ファイル名のワイルドカードのみが再帰的に適用されます。ワイルドカードをネストすることはできません。

例:

- `AppData\Local\Microsoft\Office\Access.qat` は、デフォルト構成で除外されているフォルダーの下のファイルを指定します。
- `AppData\Local\MyApp*.cfg` は、プロファイルフォルダー `AppData\Local\MyApp` およびそのサブフォルダー内の拡張子 `.cfg` を持つすべてのファイルを指定します。

このポリシーを無効にすると、有効にして空のリストを構成した場合と同じ効果があります。

このポリシーがここで構成されていない場合、.ini ファイルの値が使用されます。このポリシーがここでも .ini ファイルでも構成されていない場合、ユーザー プロファイル内の除外されていないファイルのみが同期されます。

ミラーリングするフォルダー

このポリシーを使用すると、トランザクションフォルダー（参照フォルダーとも呼ばれます）に関する問題を解決できます。そのフォルダーには相互依存ファイルが含まれており、あるファイルが別のファイルを参照しています。

フォルダーをミラーリングすることで、Profile Managementはトランザクションフォルダーとその内容を単一のエンティティとして処理し、プロファイルの肥大化を防ぐことができます。たとえば、**Internet ExplorerのCookie**フォルダーをミラーリングして、Index.datがインデックス付けするCookieと同期するようにできます。このような状況では、「最後の書き込みが優先されます」。そのため、複数のセッションで変更されたミラーリングされたフォルダー内のファイルは、最後の更新によって上書きされ、プロファイルの変更が失われることになります。

たとえば、次の表は、ユーザーがインターネットを閲覧しているときにIndex.datがCookieをどのように参照するかを示しています。

シナリオ	INDEX.DAT が COOKIE を参照する方法	
ユーザーは2つのInternet Explorerセッションを持ち、それぞれ異なるサーバー上にあり、各セッションで異なるサイトにアクセスします。	各サイトのCookieは、適切なサーバーに追加されます。	各サイトのCookieは、適切なサーバーに追加されます。
ユーザーが最初のセッションからログオフするか、セッションの途中でログオフします（アクティブなライトバッ	2番目のセッションのCookieは、最初のセッションのCookieを置き換える必要があります。	

シナリオ	INDEX.DAT が COOKIE を参照する方法	
ク機能が構成されている場合）。		
最初のセッションと2番目のセッションがマージされ、Index.dat内のCookieへの参照が古くなります。	新しいセッションでのさらなる閲覧は、繰り返しのマージと肥大化したCookieフォルダーにつながります。	

Cookieフォルダーをミラーリングすることで、この問題は解決されます。この場合、ユーザーがログオフするたびに、Cookieは最後のセッションのCookieで上書きされます。そのため、Index.datは常に最新の状態に保たれます。

ここでこのポリシーが構成されていない場合、.iniファイルの値が使用されます。ここで、または.iniファイルでこのポリシーが構成されていない場合、フォルダーはミラーリングされません。

フォルダーのミラーリングを高速化する

このポリシーと**ミラーリングするフォルダー**ポリシーの両方を有効にすると、**Profile Managementはミラーリングされた**フォルダーをVHDXベースの仮想ディスクに保存します。仮想ディスクはログオン時にアタッチされ、ログオフ時にデタッチされます。このポリシーを有効にすると、ユーザーストアとローカルプロファイル間でフォルダーをコピーする必要がなくなり、フォルダーのミラーリングが高速化されます。

フォルダーリダイレクトポリシー設定

このセクションには、プロファイルに一般的に表示されるフォルダーを共有ネットワークの場所にリダイレクトするかどうかを指定するポリシー設定が含まれています。

管理者アクセスの許可

この設定により、管理者はユーザーのリダイレクトされたフォルダーの内容にアクセスできるようになります。

> **注：**
>
> この設定は、ドメインへの完全かつ無制限のアクセス権を持つ管理者に対して権限を付与します。

> デフォルトでは、この設定は無効になっており、ユーザーにはリダイレクトされたフォルダーの内容への排他的なアクセス権が付与されます。

ドメイン名を含める

この設定により、UNC パスの一部として `%userdomain%` 環境変数を含めることができます。この UNC パスは、リダイレクトされたフォルダーに対して指定されます。

デフォルトでは、この設定は無効になっています。また、リダイレクトされたフォルダーに対して指定された UNC パスの一部として、`%userdomain%` 環境変数は含まれません。

デスクトップポリシー設定

このセクションには、`Desktop` フォルダーのコンテンツを共有ネットワークの場所にリダイレクトするためのポリシー設定が含まれています。

デスクトップパス

この設定は、**デスクトップ**フォルダーのコンテンツがリダイレクトされるネットワークの場所を指定します。

デフォルトでは、この設定は無効になっており、場所は指定されていません。

ここでこの設定が構成されていない場合、Profile Management は指定されたフォルダーをリダイレクトしません。

デスクトップのリダイレクト設定

この設定は、**デスクトップ**フォルダーのコンテンツをリダイレクトする方法を指定します。

デフォルトでは、コンテンツはUNCパスにリダイレクトされます。

ここでこの設定が構成されていない場合、Profile Management は指定されたフォルダーをリダイレクトしません。

ドキュメントポリシー設定

このセクションには、**ドキュメント**フォルダーの内容を共有ネットワークの場所にリダイレクトするためのポリシー設定が含まれています。

ドキュメントパス

この設定は、**ドキュメント**フォルダー内のファイルがリダイレクトされるネットワークの場所を指定します。

デフォルトでは、この設定は無効になっており、場所は指定されていません。

ここでこの設定が構成されていない場合、Profile Managementは指定されたフォルダーをリダイレクトしません。

ドキュメントパス設定は、**ドキュメント**フォルダーにファイルをリダイレクトするためだけでなく、**ミュージック**、**ピクチャ**、および**ビデオ**フォルダーにファイルをリダイレクトするためにも有効にする必要があります。

ドキュメントのリダイレクト設定

この設定は、**ドキュメント**フォルダーの内容をリダイレクトする方法を指定します。

デフォルトでは、コンテンツはUNCパスにリダイレクトされます。

ドキュメントフォルダーの内容をリダイレクトする方法を制御するには、次のいずれかのオプションを選択します。

- 次のUNCパスにリダイレクトします。ドキュメントパスのポリシー設定で指定されたUNCパスにコンテンツをリダイレクトします。
- ユーザーのホームディレクトリにリダイレクトします。コンテンツをユーザーのホームディレクトリにリダイレクトします。通常、Active Directoryのユーザーの#homeDirectory#属性として構成されます。

ここでこの設定が構成されていない場合、Profile Managementは指定されたフォルダーをリダイレクトしません。

ダウンロードポリシー設定

このセクションには、**ダウンロード**フォルダーのコンテンツを共有ネットワークの場所にリダイレクトするためのポリシー設定が含まれています。

ダウンロードパス

この設定は、**ダウンロード**フォルダー内のファイルがリダイレクトされるネットワークの場所を指定します。

デフォルトでは、この設定は無効になっており、場所は指定されていません。

ここでこの設定が構成されていない場合、Profile Management は指定されたフォルダーをリダイレクトしません。

ダウンロードのリダイレクト設定

この設定は、**ダウンロード**フォルダーのコンテンツをリダイレクトする方法を指定します。

デフォルトでは、コンテンツはUNCパスにリダイレクトされます。

ここでこの設定が構成されていない場合、Profile Management は指定されたフォルダーをリダイレクトしません。

お気に入りポリシー設定

このセクションには、**お気に入り**フォルダーの内容を共有ネットワークの場所にリダイレクトするためのポリシー設定が含まれています。

お気に入りパス

この設定は、**お気に入り**フォルダーの内容がリダイレクトされるネットワークの場所を指定します。

デフォルトでは、この設定は無効になっており、場所は指定されていません。

この設定がここで構成されていない場合、Profile Management は指定されたフォルダーをリダイレクトしません。

お気に入りのリダイレクト設定

この設定は、**お気に入り**フォルダーの内容をリダイレクトする方法を指定します。

デフォルトでは、内容は UNC パスにリダイレクトされます。

この設定がここで構成されていない場合、Profile Management は指定されたフォルダーをリダイレクトしません。

音楽ポリシー設定

このセクションには、**Music**フォルダーのコンテンツを共有ネットワークの場所にリダイレクトするためのポリシー設定が含まれています。

音楽パス

この設定は、**Music**フォルダーのコンテンツがリダイレクトされるネットワークの場所を指定します。

デフォルトでは、この設定は無効になっており、場所は指定されていません。

ここでこの設定が構成されていない場合、Profile Management は指定されたフォルダーをリダイレクトしません。

音楽のリダイレクト設定

この設定は、**Music**フォルダーのコンテンツをリダイレクトする方法を指定します。

デフォルトでは、コンテンツは UNC パスにリダイレクトされます。

Musicフォルダーのコンテンツをリダイレクトする方法を制御するには、次のいずれかのオプションを選択します。

- 次の UNC パスにリダイレクトします。コンテンツをミュージックパスポリシー設定で指定された UNC パスにリダイレクトします。
- ドキュメントフォルダーを基準にリダイレクトします。コンテンツをドキュメントフォルダーを基準としたフォルダーにリダイレクトします。

コンテンツを**ドキュメント**フォルダーを基準としたフォルダーにリダイレクトするには、**ドキュメントパス**設定を有効にする必要があります。

ここでこの設定が構成されていない場合、Profile Management は指定されたフォルダーをリダイレクトしません。

Searchesポリシー設定

このセクションには、**検索**フォルダーのコンテンツを共有ネットワークの場所にリダイレクトするためのポリシー設定が含まれています。

検索のリダイレクト設定

この設定は、**検索**フォルダーのコンテンツをリダイレクトする方法を指定します。

デフォルトでは、コンテンツはUNCパスにリダイレクトされます。

ここでこの設定が構成されていない場合、Profile Management は指定されたフォルダーをリダイレクトしません。

検索パス

この設定は、**検索**フォルダーのコンテンツがリダイレクトされるネットワークの場所を指定します。

デフォルトでは、この設定は無効になっており、場所は指定されていません。

ここでこの設定が構成されていない場合、Profile Management は指定されたフォルダーをリダイレクトしません。

ビデオポリシー設定

このセクションには、**ビデオ**フォルダーのコンテンツを共有ネットワークの場所にリダイレクトするためのポリシー設定が含まれています。

ビデオのリダイレクト設定

この設定は、**ビデオ**フォルダーのコンテンツをリダイレクトする方法を指定します。

デフォルトでは、コンテンツはUNCパスにリダイレクトされます。

ビデオフォルダーのコンテンツをリダイレクトする方法を制御するには、次のいずれかのオプションを選択します。

- 次のUNCパスにリダイレクトします。コンテンツを、ビデオパスポリシー設定で指定されたUNCパスにリダイレクトします。
- ドキュメントフォルダーを基準にリダイレクトします。コンテンツを、ドキュメントフォルダーを基準としたフォルダーにリダイレクトします。

コンテンツを**ドキュメント**フォルダーを基準としたフォルダーにリダイレクトするには、**ドキュメントパス**設定を有効にする必要があります。

ここでこの設定が構成されていない場合、Profile Managementは指定されたフォルダーをリダイレクトしません。

ビデオパス

この設定は、**ビデオ**フォルダーのコンテンツがリダイレクトされるネットワークの場所を指定します。

デフォルトでは、この設定は無効になっており、場所は指定されていません。

ここでこの設定が構成されていない場合、Profile Managementは指定されたフォルダーをリダイレクトしません。

ログポリシー設定

このセクションには、Profile Managementのログを構成するポリシー設定が含まれています。

Active Directoryアクション

この設定は、Active Directoryで実行されたアクションの詳細ログを有効または無効にします。

デフォルトでは、この設定は無効になっています。

この設定を有効にする場合は、**ログの有効化**設定も有効になっていることを確認してください。

この設定が Web Studio で構成されていない場合、.ini ファイルの値が使用されます。

この設定が Web Studio または .ini ファイルで構成されていない場合、以下がログに記録されます。

- エラー
- 一般情報

一般情報

この設定は、一般情報の詳細ログを有効または無効にします。

デフォルトでは、この設定は無効になっています。

この設定を有効にする場合は、**ログの有効化**設定も有効になっていることを確認してください。

この設定がここで構成されていない場合、.iniファイルの値が使用されます。

この設定がWeb Studioまたは.iniファイルで構成されていない場合、以下がログに記録されます。

- エラー
- 一般情報

一般的な警告

この設定は、一般的な警告の詳細ログを有効または無効にします。

デフォルトでは、この設定は無効になっています。

この設定を有効にする場合は、**ログの有効化**設定も有効になっていることを確認してください。

ここでこの設定が構成されていない場合、.iniファイルの値が使用されます。

Web Studioまたは.iniファイルでこの設定が構成されていない場合、以下がログに記録されます。

- エラー
- 一般情報

ログの有効化

この設定は、デバッグ（詳細ログ）モードでのProfile Managementログを有効または無効にします。デバッグモードでは、広範なステータス情報が「%SystemRoot%\System32\Logfiles\UserProfileManager」にあるログファイルに記録されます。

デフォルトでは、この設定は無効になっており、エラーのみがログに記録されます。

Citrix®は、Profile Managementのトラブルシューティングを行う場合にのみ、この設定を有効にすることをお勧めします。

この設定がここで構成されていない場合、.iniファイルの値が使用されます。

この設定がここまたは.iniファイルで構成されていない場合、エラーのみがログに記録されます。

ファイルシステムのアクション

この設定は、ファイルシステムで実行されたアクションの詳細なログ記録を有効または無効にします。

デフォルトでは、この設定は無効になっています。

この設定を有効にする際は、**ログ記録を有効にする**設定も有効になっていることを確認してください。

この設定がここで構成されていない場合、.iniファイルの値が使用されます。

この設定がWeb Studioまたは.iniファイルで構成されていない場合、以下がログに記録されます。

- エラー
- 一般情報

ログの有効化

この設定は、デバッグ（詳細ログ）モードでのProfile Managementログを有効または無効にします。デバッグモードでは、"%SystemRoot%\System32\Logfiles\UserProfileManager" にあるログファイルに詳細なステータス情報が記録されます。

デフォルトでは、この設定は無効になっており、エラーのみがログに記録されます。

Citrix®は、Profile Managementのトラブルシューティングを行う場合にのみ、この設定を有効にすることをお勧めします。

この設定がここで構成されていない場合、.iniファイルの値が使用されます。

この設定がここでも.iniファイルでも構成されていない場合、エラーのみがログに記録されます。

ファイルシステムのアクション

この設定は、ファイルシステムで実行されたアクションの詳細ログを有効または無効にします。

デフォルトでは、この設定は無効になっています。

この設定を有効にする場合は、**ログの有効化**設定も有効になっていることを確認してください。

この設定がここで構成されていない場合、.ini ファイルの値が使用されます。

この設定がWeb Studioまたは.iniファイルで構成されていない場合、以下がログに記録されます。

- エラー
- 一般情報

ファイルシステム通知

この設定は、ファイルシステム通知の詳細ログを有効または無効にします。

デフォルトでは、この設定は無効になっています。

この設定を有効にする際は、**ログ記録を有効にする**設定も有効になっていることを確認してください。

この設定がここで構成されていない場合、.ini ファイルの値が使用されます。

この設定がWeb Studioまたは.iniファイルで構成されていない場合、以下がログに記録されます。

- エラー
- 一般情報

ログオフ

この設定は、ユーザーのログオフの詳細ログを有効または無効にします。

デフォルトでは、この設定は無効になっています。

この設定を有効にする際は、**ログ記録を有効にする**設定も有効になっていることを確認してください。

この設定がここで構成されていない場合、.ini ファイルの値が使用されます。

この設定がWeb Studioまたは.iniファイルで構成されていない場合、以下がログに記録されます。

- エラー
- 一般情報

ログオン

この設定は、ユーザーのログオンの詳細ログを有効または無効にします。

デフォルトでは、この設定は無効になっています。

この設定を有効にする場合は、**ログ記録を有効にする**設定も有効になっていることを確認してください。

この設定がここで構成されていない場合、.iniファイルの値が使用されます。

この設定がWeb Studioまたは.iniファイルで構成されていない場合、以下がログに記録されます。

- エラー

- 一般情報

ログファイルの最大サイズ

この設定は、Profile Managementログファイルの最大許容サイズをバイト単位で指定します。

デフォルトでは、この値は1048576バイト（1 MB）に設定されています。

十分なディスク容量がある場合、Citrixはこのファイルのサイズを5 MB以上に増やすことを推奨します。ログファイルが最大サイズを超えて増加した場合：

- ファイルの既存のバックアップ（.bak）が削除されます
- ログファイルの名前が.bakに変更されます
- 新しいログファイルが作成されます

ログファイルは`%SystemRoot%\System32\Logfiles\UserProfileManager`に作成されます。

この設定がここで構成されていない場合、.iniファイルの値が使用されます。

この設定がここで、または.iniファイルで構成されていない場合、デフォルト値が使用されます。

ログファイルへのパス

この設定は、Profile Managementログファイルを保存するための代替パスを指定します。

デフォルトでは、この設定は無効になっており、ログファイルはデフォルトの場所である%SystemRoot%\System32\Logfiles\UserProfileManagerに保存されます。

パスはローカルドライブまたはリモートのネットワークベースドライブ（UNCパス）を指すことができます。リモートパスは大規模な分散環境で役立つ場合がありますが、ログファイルには不適切な大量のネットワークトラフィックを生成する可能性があります。永続的なハードドライブを持つプロビジョニングされた仮想マシンの場合、そのドライブへのローカルパスを設定します。この設定により、マシンの再起動時にログファイルが保持されます。永続的なハードドライブを持たない仮想マシンの場合、UNCパスを設定することでログファイルを保持できます。ただし、マシンのシステムアカウントはUNC共有への書き込みアクセス権を持っている必要があります。オフラインプロファイル機能によって管理されるラップトップには、ローカルパスを使用してください。

ログファイルにUNCパスを使用する場合、Citrixはログファイルフォルダーに適切なアクセス制御リストを適用することを推奨します。この設定により、承認されたユーザーまたはコンピューターアカウントのみが保存されたファイルにアクセスできるようになります。

ここでこの設定が構成されていない場合、.ini ファイルの値が使用されます。

ここまたは .ini ファイルでこの設定が構成されていない場合、デフォルトの場所 %SystemRoot%\System32\Logfiles\UserProfileManager が使用されます。

パーソナライズされたユーザー情報

この設定は、パーソナライズされたユーザー情報の詳細ログを有効または無効にします。

デフォルトでは、この設定は無効になっています。

この設定を有効にする場合、**ログの有効化**設定も有効になっていることを確認してください。

ここでこの設定が構成されていない場合、.ini ファイルの値が使用されます。

この設定がWeb Studioまたは.iniファイルで構成されていない場合、以下がログに記録されます。

- エラー
- 一般情報

ログオン時とログオフ時のポリシー値

この設定は、ユーザーがログオンおよびログオフするときのポリシー値の詳細ログを有効または無効にします。

デフォルトでは、この設定は無効になっています。

この設定を有効にする場合、**ログの有効化**設定も有効になっていることを確認してください。

ここでこの設定が構成されていない場合、.ini ファイルの値が使用されます。

この設定がWeb Studioまたは.iniファイルで構成されていない場合、以下がログに記録されます。

- エラー
- 一般情報

レジストリアクション

この設定は、レジストリで実行されたアクションの詳細ログを有効または無効にします。

デフォルトでは、この設定は無効になっています。

この設定を有効にする際は、**ログ記録を有効にする**設定も有効になっていることを確認してください。

この設定がここで構成されていない場合、.iniファイルの値が使用されます。

この設定がWeb Studioまたは.iniファイルで構成されていない場合、以下がログに記録されます。

- エラー
- 一般情報

ログオフ時のレジストリの差異

この設定は、ユーザーがログオフするときにレジストリの差異の詳細ログ記録を有効または無効にします。

デフォルトでは、この設定は無効になっています。

この設定を有効にする場合は、「**ログ記録を有効にする**」設定も有効になっていることを確認してください。

この設定がここで構成されていない場合、.iniファイルの値が使用されます。

この設定がWeb Studioまたは.iniファイルで構成されていない場合、以下がログに記録されます:

- エラー
- 一般情報

プロファイル処理ポリシー設定

このセクションには、Profile Management がユーザープロファイルを処理する方法を指定するポリシー設定が含まれています。

キャッシュされたプロファイルを削除するまでの遅延

この設定は、ログオフ時にProfile Managementがローカルにキャッシュされたプロファイルを削除するまでの遅延を、分単位で任意に延長する時間を指定します。

値が0の場合、ログオフプロセスの終了時にプロファイルがすぐに削除されます。Profile Managementは1分ごとにログオフをチェックします。その結果、値が60の場合、ユーザーがログオフしてから1〜2分以内にプロファイルが削除されることが保証されます。このアクションは、最後のチェックがいつ行われたかによって異なります。ログオフ中にプロセスがファイルまたはユーザーレジストリハイブを開いたままにしていることがわかっている場合、遅延を延長することは有用です。大規模なプロファイルの場合、このプロセスはログオフを高速化することもできます。

デフォルトでは、この値は0に設定されており、Profile Managementはローカルにキャッシュされたプロファイルをすぐに削除します。

この設定を有効にする場合は、「ログオフ時にローカルにキャッシュされたプロファイルを削除する」も有効になっていることを確認してください。

ここでこの設定が構成されていない場合、.iniファイルの値が使用されます。

ここで、または.iniファイルでこの設定が構成されていない場合、プロファイルはすぐに削除されます。

ログオフ時にローカルにキャッシュされたプロファイルを削除する

この設定は、ユーザーがログオフした後にローカルにキャッシュされたプロファイルが削除されるかどうかを指定します。

この設定が有効になっている場合、ユーザーのローカルプロファイルキャッシュはログオフ後に削除されます。Citrix®は、ターミナルサーバーに対してこの設定を有効にすることを推奨します。

デフォルトでは、この設定は無効になっており、ユーザーのローカルプロファイルキャッシュはログオフ後も保持されます。

ここでこの設定が構成されていない場合、.iniファイルの値が使用されます。

ここまたは.iniファイルでこの設定が構成されていない場合、キャッシュされたプロファイルは削除されません。

ローカルプロファイルの競合処理

この設定は、ユーザープロファイルが以下の両方に存在する場合のProfile Managementの動作を構成します。

- ユーザーストア
- ローカルWindowsユーザープロファイル（Citrixユーザープロファイルではない）

デフォルトでは、Profile Management はローカルの Windows プロファイルを使用しますが、それを一切変更しません。

Profile Managementの動作を制御するには、以下のいずれかのオプションを選択します。

- ローカルプロファイルを使用する。Profile Managementはローカルプロファイルを使用しますが、それを一切変更しません。
- ローカルプロファイルを削除する。Profile ManagementはローカルWindowsユーザープロファイルを削除し、その後、ユーザーストアからCitrixユーザープロファイルをインポートします。
- ローカルプロファイルの名前を変更する。Profile ManagementはローカルWindowsユーザープロファイルの名前を変更し（バックアップ目的で）、その後、ユーザーストアからCitrixユーザープロファイルをインポートします。

この設定がここで構成されていない場合、.ini ファイルの値が使用されます。

この設定がここで、または .ini ファイルで構成されていない場合、既存のローカルプロファイルが使用されます。

既存プロファイルの移行

この設定は、ユーザーがユーザー ストアに現在のプロファイルを持っていない場合に、ログオン中にユーザー ストアに移行されるプロファイルの種類を指定します。

ユーザーがユーザーストアにプロファイルを持っていない場合、Profile Managementはログオン中に既存のプロファイルを「その場で」移行できます。その後、以下の両方でユーザーストアプロファイルがProfile Managementによって使用されます。

- 現在のセッション
- 同じユーザー ストアへのパスで構成されたその他のセッション

デフォルトでは、ローカルプロファイルと移動プロファイルの両方がログオン中にユーザー ストアに移行されます。

ログオン中にユーザー ストアに移行されるプロファイルの種類を指定するには、次のいずれかのオプションを選択します。

- ローカルプロファイルと移動プロファイル
- ローカル
- ローミング
- なし (無効)

なしを選択すると、Profile Managementがインストールされていない環境であるかのように、システムは既存のWindowsメカニズムを使用してプロファイルを作成します。

ここでこの設定が構成されていない場合、.iniファイルの値が使用されます。

ここまたは.iniファイルでこの設定が構成されていない場合、既存のローカルプロファイルと移動プロファイルが移行されます。

既存のアプリケーションプロファイルの自動移行

この設定は、異なるオペレーティングシステム間での既存のアプリケーションプロファイルの自動移行を有効または無効にします。アプリケーションプロファイルには、`AppData`フォルダー内のアプリケーションデータと、`HKEY_CURRENT_USER\SOFTWARE`の下のレジストリエントリの両方が含まれます。この設定は、異なるオペレーティングシステム間でアプリケーションプロファイルを移行したい場合に役立ちます。

たとえば、オペレーティングシステム (OS) をWindows 10バージョン1803からWindows 10バージョン1809にアップグレードするとします。この設定が有効になっている場合、各ユーザーが最初にログオンしたときに、Profile Managementは既存のアプリケーション設定をWindows 10バージョン1809に自動的に移行します。その結果、`AppData`フォルダー内のアプリケーションデータと、HKEY_CURRENT_USER\SOFTWAREの下のレジストリエントリが移行されます。

複数の既存のアプリケーションプロファイルがある場合、Profile Managementは次の優先順位で移行を実行します。

1. 同じOSタイプのプロファイル (シングルセッションOSからシングルセッションOS、マルチセッションOSからマルチセッションOS)。
2. 同じWindows OSファミリーのプロファイル。例: Windows 10からWindows 10、またはWindows Server 2016からWindows Server 2016。
3. OSの以前のバージョンのプロファイル。例: Windows 7からWindows 10、またはWindows Server 2012からWindows 2016。
4. 最も近いOSのプロファイル。

注： ユーザーストアパスに変数「!CTX_OSNAME!」を含めることで、OSの短い名前を指定する必要があります。これにより、Profile Managementは既存のアプリケーションプロファイルを特定できます。

ここでこの設定が構成されていない場合、.iniファイルの設定が使用されます。

ここまたは.iniファイルでこの設定が構成されていない場合、デフォルトで無効になります。

テンプレートプロファイルへのパス

この設定は、Profile Managementがユーザープロファイルを作成するためのテンプレートとして使用するプロファイルへのパスを指定します。

指定されたパスは、NTUSER.DATレジストリファイルと、テンプレートプロファイルに必要なその他のフォルダーおよびファイルを含むフォルダーへのフルパスである必要があります。

注: パスにNTUSER.DATを含めないでください。たとえば、ファイル`\\myservername\myprofiles\template\ntuser.dat`の場合、場所を`\\myservername\myprofiles\template`として設定します。

絶対パスを使用してください。絶対パスはUNCパスまたはローカルマシン上のパスのいずれかです。後者は、たとえばCitrix Provisioning™ Servicesイメージ上にテンプレートプロファイルを永続的に指定する場合に使用します。相対パスはサポートされていません。

注: この設定は、Active Directory属性、システム環境変数、または`%USERNAME%`および`%USERDOMAIN%`変数の展開をサポートしていません。

デフォルトでは、この設定は無効になっており、新しいユーザープロファイルは、ユーザーが最初にログオンするデバイスのデフォルトユーザープロファイルから作成されます。

ここでこの設定が構成されていない場合、.iniファイルの値が使用されます。

ここまたは.iniファイルでこの設定が構成されていない場合、テンプレートは使用されません。

テンプレートプロファイルがローカルプロファイルを上書きする

この設定により、ユーザープロファイルを作成する際に、テンプレートプロファイルがローカルプロファイルを上書きできるようになります。

ユーザーがCitrixユーザープロファイルを持たず、ローカルのWindowsユーザープロファイルを持っているとします。この場合、この値が有効になっていると、デフォルトでローカルプロファイルが使用され、ユーザーストアに移行されます。このポリシー設定を有効にすると、ユーザープロファイルを作成する際に使用されるローカルプロファイルをテンプレートプロファイルが上書きできるようになります。

この設定がここで構成されていない場合、.iniファイルの値が使用されます。

この設定がここでも.iniファイルでも構成されていない場合、テンプレートは使用されません。

テンプレートプロファイルが移動プロファイルを上書きする

この設定により、ユーザープロファイルを作成する際に、テンプレートプロファイルが移動プロファイルを上書きできるようになります。

ユーザーがCitrixユーザープロファイルを持たず、移動Windowsユーザープロファイルを持っているとします。この場合、この値が有効になっていると、デフォルトで移動プロファイルが使用され、ユーザーストアに移行されます。このポリシー設定を有効にすると、ユーザープロファイルを作成する際に使用される移動プロファイルをテンプレートプロファイルが上書きできるようになります。

この設定がここで構成されていない場合、.iniファイルの値が使用されます。

この設定がここでも.iniファイルでも構成されていない場合、テンプレートは使用されません。

すべてのログオンでCitrix必須プロファイルとして使用されるテンプレートプロファイル

この設定により、Profile Managementはテンプレートプロファイルをすべてのユーザープロファイルを作成するためのデフォルトプロファイルとして使用できるようになります。

デフォルトでは、この設定は無効になっており、新しいユーザープロファイルは、ユーザーが最初にログオンしたデバイスのデフォルトユーザープロファイルから作成されます。

この設定がここで構成されていない場合、.iniファイルの値が使用されます。

この設定がここでも.iniファイルでも構成されていない場合、テンプレートは使用されません。

レジストリポリシー設定

このセクションには、Profile Management の処理に含める、または除外するレジストリキーを指定するポリシー設定が含まれています。

除外リスト

ログオフ時に無視されるHKCUハイブ内のレジストリキーのリスト。

例: Software\Policies

このポリシーが無効になっている場合、レジストリキーは除外されません。ここでこのポリシーが構成されていない場合、.iniファイルの値が使用されます。ここで、または.iniファイルでこのポリシーが構成されていない場合、レジストリキーは除外されません。

包含リスト

ログオフ時に処理されるHKCUハイブ内のレジストリキーのリスト。

例: Software\Adobe。

このポリシーが有効になっている場合、このリストにあるキーのみが処理されます。このポリシーが無効になっている場合、HKCUハイブ全体が処理されます。ここでこのポリシーが構成されていない場合、.iniファイルの値が使用されます。ここで、または.iniファイルでこのポリシーが構成されていない場合、HKCUのすべてが処理されます。

デフォルトの除外リストを有効にする - Profile Management 5.5

ユーザープロファイルに同期されないHKCUハイブ内のレジストリキーのデフォルトリスト。このポリシーを使用して、GPO除外ファイルを手動で入力することなく指定できます。

このポリシーを無効にすると、Profile Management はデフォルトでレジストリキーを除外しません。このポリシーをここで構成しない場合、Profile Management は .ini ファイルの値を使用します。このポリシーをここでも .ini ファイルでも構成しない場合、Profile Management はデフォルトでレジストリキーを除外しません。

NTUSER.DAT のバックアップ

NTUSER.DAT の最後に正常だったコピーのバックアップと、破損があった場合のロールバックを有効にします。

ここでこのポリシーを構成しない場合、プロファイル管理は.iniファイルの値を使用します。ここで、または.iniファイルでこのポリシーを構成しない場合、プロファイル管理はNTUSER.DATをバックアップしません。

ストリーム配信ユーザープロファイルポリシー設定

このセクションには、Profile Management がストリーム配信ユーザープロファイルを処理する方法を指定するポリシー設定が含まれています。

常にキャッシュ

この設定は、ユーザーのログオン後、Profile Management がストリーム配信ファイルをできるだけ早くキャッシュするかどうかを指定します。ユーザーのログオン後にファイルをキャッシュすると、ネットワーク帯域幅が節約され、ユーザーエクスペリエンスが向上します。

この設定は、**プロファイルストリーミング**設定と組み合わせて使用します。

デフォルトでは、この設定は無効になっており、ユーザーがログオンした直後にストリーミングファイルはキャッシュされません。

ここでこの設定が構成されていない場合、.iniファイルの値が使用されます。

この設定がここでも.iniファイルでも構成されていない場合、無効になります。

常にキャッシュするサイズ

この設定は、ストリーミングされるファイルのサイズの下限をMB単位で指定します。Profile Managementは、ユーザーがログオンした直後に、このサイズ以上のファイルをキャッシュします。

デフォルトでは、値は0（ゼロ）に設定されており、プロファイル全体をキャッシュする機能が使用されます。プロファイル全体をキャッシュする機能が有効になっている場合、Profile Managementは、ユーザーがログオンした後、ユーザーストア内のすべてのプロファイルコンテンツをバックグラウンドタスクとしてフェッチします。

ここでこの設定が構成されていない場合、.iniファイルの値が使用されます。

この設定がここでも.iniファイルでも構成されていない場合、無効になります。

プロファイルストリーミング

この設定は、Citrix®ストリーミングユーザープロファイル機能を有効または無効にします。有効にすると、プロファイルファイルとフォルダーは、ユーザーがログオン後にアクセスした場合にのみ、ユーザーストアからローカルコンピューターにフェッチされます。レジストリエントリと保留領域のファイルはすぐにフェッチされます。

デフォルトでは、プロファイルストリーミングは無効になっています。

この設定がここで構成されていない場合、.iniファイルの値が使用されます。

この設定がここでも .ini ファイルでも構成されていない場合、無効になります。

常にキャッシュするサイズ

この設定は、Windowsユーザーグループに基づいて、OU内のどのユーザープロファイルをストリーミングするかを指定します。

有効にすると、指定されたユーザーグループ内のユーザープロファイルのみがストリーミングされます。その他のすべてのユーザープロファイルは通常どおり処理されます。

デフォルトでは、この設定は無効になっており、OU内のすべてのユーザープロファイルは通常どおり処理されます。

この設定がここで構成されていない場合、.iniファイルの値が使用されます。

この設定がここでも.iniファイルでも構成されていない場合、すべてのユーザープロファイルが処理されます。

プロファイルストリーミング除外を有効にする

プロファイルストリーミング除外が有効な場合：

- Profile Managementは、除外リスト内のフォルダーをストリーミングしません
- ユーザーがログオンすると、すべてのフォルダーがユーザーストアからローカルコンピューターに即座にフェッチされます

詳しくは、「ユーザープロファイルのストリーミング」を参照してください。

ペンディングエリアロックファイルのタイムアウト

この設定は、ストレージサーバーが応答しなくなったときにユーザー ストアがロックされたままの場合に、保留領域からユーザー ストアにユーザーのファイルが書き戻されるまでの日数を指定します。この動作により、保留領域の肥大化が防止され、ユーザー ストアに常に最新のファイルが含まれるようになります。

デフォルトでは、この設定は1日（1）に設定されています。

この設定がここで構成されていない場合、.iniファイルの値が使用されます。

この設定がここでも.iniファイルでも構成されていない場合、デフォルト値が使用されます。

ペンディングエリアのプロファイルストリーミングを有効にする

保留領域内のファイルとフォルダーのプロファイルストリーミング機能を有効にできます。

保留領域は、プロファイルストリーミングが有効になっている間のプロファイルの一貫性を確保するために使用されます。同時セッションで変更されたプロファイルファイルとフォルダーを一時的に保存します。

デフォルトでは、このポリシーは無効になっており、保留領域内のすべてのファイルとフォルダーはログオン時にローカルプロファイルにフェッチされます。このポリシーを有効にすると、保留領域内のファイルは要求されたときにのみローカルプロファイルにフェッチされます。同時セッションのシナリオで最適なログオンエクスペリエンスを確保するには、このポリシーをプロファイルストリーミングポリシーと組み合わせて使用します。

このポリシーは、フォルダーのプロファイルストリーミングを有効にするポリシーが有効になっている場合に、保留領域内のフォルダーに適用されます。

ユーザーパーソナライゼーションポリシー設定

Virtual Delivery Agent内でユーザーレイヤーのマウントを有効にするには、構成パラメータを使用して以下を指定します。

- ネットワーク上のどこでユーザーレイヤーにアクセスするか。
- 新しいユーザーレイヤーディスクがどのくらい大きくなるか。

そのため、利用可能なポリシーのリストには、次の2つのポリシーが表示されます。

- ユーザーレイヤーリポジトリパス - 値フィールドに「\\サーバー名またはアドレス\フォルダー名」の形式でパスを入力します。
- ユーザーレイヤーサイズGB - デフォルトのユーザーレイヤーサイズである10 GBは、Citrix®が推奨する最小値です。ユーザーレイヤーは、使用されるスペースに応じて設定されたサイズに拡張されるシンプロビジョニングディスクです。ユーザーレイヤーのサイズが縮小することはありません。

> **注:**

> ユーザーレイヤーサイズを増やすと、新しいユーザーレイヤーに影響を与え、既存のユーザーレイヤーを拡張します。レイヤーサイズを減らすと、新しいユーザーレイヤーにのみ影響します。既存のユーザーレイヤーのサイズが縮小することはありません。

> 詳細については、「ユーザーパーソナライゼーションレイヤー」を参照してください。

Virtual Delivery Agent ポリシー設定

Virtual Delivery Agent (VDA)セクションには、サイトのVDAとコントローラー間の通信を制御するポリシー設定が含まれています。

重要: 自動更新機能を使用していない場合、VDAはDelivery Controller™に登録するために、これらの設定によって提供される情報を必要とします。この情報は登録に必要であるため、VDAのインストール中にこの情報を提供しない限り、グループポリシーエディターを使用して以下の設定を構成する必要があります。

- コントローラー登録 IPv6 ネットマスク
- コントローラー登録ポート
- コントローラー SID
- コントローラー
- IPv6 コントローラー登録のみを使用
- サイト GUID

コントローラー登録 IPv6 ネットマスク

このポリシー設定により、管理者はVDAを優先サブネットのみに制限できます (グローバルIPが登録されている場合でも、そちらではなく)。この設定は、VDAが登録するIPv6アドレスとネットワークを指定します。VDAは、指定されたネットマスクに一致する最初のアドレスにのみ登録します。この設定は、「IPv6コントローラー登録のみを使用」ポリシー設定が有効になっている場合にのみ有効です。

デフォルトでは、この設定は空白です。

コントローラー登録ポート

この設定は、**コントローラーの自動更新を有効にする** 設定が無効になっている場合にのみ使用してください。

この設定は、レジストリベースの登録を使用する際に、VDA がコントローラーに登録するために使用する TCP/IP ポート番号を指定します。

デフォルトでは、ポート番号は80に設定されています。

コントローラーSID

この設定は、**コントローラーの自動更新を有効にする**設定が無効になっている場合にのみ使用してください。

この設定は、VDAがレジストリベースの登録を使用する際にコントローラーに登録するために使用する、コントローラーのセキュリティ識別子 (SID) のスペース区切りリストを指定します。この設定はオプションであり、登録に使用されるコントローラーのリストを制限するために、**コントローラー**設定と組み合わせて使用される場合があります。

デフォルトでは、この設定は空白です。

コントローラー

この設定は、**コントローラーの自動更新を有効にする**設定が無効になっている場合にのみ使用してください。

この設定は、VDAがレジストリベースの登録を使用する際にコントローラーに登録するために使用する、コントローラーの完全修飾ドメイン名 (FQDN) のスペース区切りリストを指定します。この設定はオプションであり、**コントローラーSID**設定と組み合わせて使用される場合があります。

デフォルトでは、この設定は空白です。

コントローラーの自動更新を有効にする

この設定により、VDAはインストール後にコントローラーに自動的に登録できるようになります。

VDAが登録されると、登録先のコントローラーは現在のコントローラーFQDNとSIDのリストをVDAに送信します。VDAはこのリストを永続ストレージに書き込みます。各コントローラーは、90分ごとにサイトデータベースでコントローラー情報を確認します。以下のいずれかの状況が発生した場合、コントローラーは登録済みのVDAに更新されたリストを送信します。

- 前回の確認以降にコントローラーが追加または削除された
- ポリシーの変更が発生した

VDAは、受信した最新のリストにあるすべてのコントローラーからの接続を受け入れます。

デフォルトでは、この設定は有効になっています。

IPv6コントローラー登録のみを使用

この設定は、VDAがControllerに登録するために使用するアドレス形式を制御します。

- 有効にすると、VDAはマシンのIPv6アドレスを使用してControllerに登録します。VDAがControllerと通信する場合、次のアドレス順序を使用します: グローバルIPアドレス、ユニークローカルアドレス (ULA)、リンクローカルアドレス (他のIPv6アドレスが利用できない場合)。
- 無効にすると、VDAはマシンのIPv4アドレスを使用してControllerに登録し、通信します。

デフォルトでは、この設定は無効になっています。

サイトGUID

この設定は、**コントローラーの自動更新を有効にする**設定が無効になっている場合にのみ使用してください。

この設定は、Active Directoryベースの登録を使用する際に、VDAがControllerに登録するために使用するサイトのグローバル一意識別子 (GUID) を指定します。

デフォルトでは、この設定は空白です。

HDX™ 3D Pro ポリシー設定

HDX 3D Proセクションには、ユーザー向けの画質構成ツールを有効化および構成するためのポリシー設定が含まれています。このツールを使用すると、ユーザーは利用可能な帯域幅の使用を最適化できます。この最適化のために、画質と応答性のバランスがリアルタイムで調整されます。

ロスレスを有効にする

この設定は、ユーザーが画質構成ツールを使用してロスレス圧縮を有効または無効にできるかどうかを指定します。デフォルトでは、ユーザーにロスレス圧縮を有効にするオプションは提供されません。

ユーザーがロスレス圧縮を有効にしたとします。この場合、画質は画質構成ツールで利用可能な最大値に自動的に設定されます。デフォルトでは、ユーザーデバイスとホストコンピューターの機能に応じて、GPUベースまたはCPUベースの圧縮のいずれかを使用できます。

HDX 3D Pro 品質設定

この設定は、画質構成ツールでユーザーが利用できる最小値と最大値を指定します。これらの値を使用すると、画質構成ツールで画質調整の範囲を定義できます。

画質値を0から100の範囲（両端を含む）で指定します。最大値は最小値以上である必要があります。

監視ポリシー設定

「**監視**」セクションには、プロセス、リソース監視、およびアプリケーション障害監視のポリシー設定が含まれています。

これらのポリシーのスコープは、以下に基づいて定義できます。

- サイト
- デリバリーグループ
- デリバリーグループの種類
- 組織単位
- タグ

プロセスおよびリソース監視のポリシー

CPU、メモリ、プロセスの各データポイントはVDAから収集され、監視データベースに保存されます。VDAからデータポイントを送信するとネットワーク帯域幅を消費し、それらを保存すると監視データベースの相当なスペースを消費します。特定のスコープ（たとえば、特定のデリバリーグループや組織単位）に対して、リソースデータ、プロセスデータ、またはその両方を監視したくない場合を考慮してください。この場合、ポリシーを無効にすることをお勧めします。

プロセス監視を有効にする

この設定を有効にすると、VDAがインストールされたマシンで実行されているプロセスの監視が可能になります。CPU使用率やメモリ使用量などの統計情報は、監視サービスに送信されます。これらの統計情報は、Directorでのリアルタイム通知および履歴レポートに使用されます。

この設定のデフォルトは無効です。

リソース監視を有効にする

この設定を有効にすると、VDAがインストールされたマシンで重要なパフォーマンスカウンターの監視が可能になります。統計情報（CPU使用率、メモリ使用量、IOPS、ディスク遅延データなど）は監視サービスに送信されます。これらの統計情報は、Directorでのリアルタイム通知および履歴レポートに使用されます。

この設定のデフォルトは有効です。

スケーラビリティ

CPUおよびメモリデータは、各VDAから5分間隔でデータベースにプッシュされます。プロセスデータ（有効な場合）は10分間隔でデータベースにプッシュされます。IOPSおよびディスク待機時間データは1時間間隔でデータベースにプッシュされます。

CPUとメモリデータ

CPUとメモリデータは、デフォルトで**有効**です。データ保持期間の値は次のとおりです (Platinum ライセンス):

データ粒度	日数
5分間データ	1日
10分間データ	7日間
1時間データ	30日間
1日データ	90日間

IOPSとディスク待機時間データ

IOPSとディスク遅延データは、デフォルトで**有効**です。データ保持値は次のとおりです (Platinum ライセンス):

データ粒度	日数
時間データ	3日間
日次データ	90日間

データ保持設定により、1つのVDAについて1年間、以下の情報を保存するために約276 KBのディスク容量が必要になります。

- CPU
- メモリ
- IOPS
- ディスク遅延データ

マシンの数	必要なストレージ容量（概算）
1	276 KB
1K	270 MB
40K	10.6 GB

プロセスデータ

プロセスデータはデフォルトで**無効**です。必要に応じて、一部のマシンでプロセスデータを有効にすることをお勧めします。プロセスデータのデフォルトのデータ保持設定は次のとおりです。

データ粒度	日数
10分間データ	1日
時間データ	7日間

プロセスデータがデフォルトの保持設定で有効になっている場合、プロセスデータは1年間でVDAあたり約1.5 MB、ターミナルサービスVDA (TS VDA) あたり3 MBを消費します。

マシン数	必要なストレージの目安 VDA	必要なストレージの目安 TS VDA
1	1.5 MB	3 MB
1K	1.5 GB	3 GB

注:

以前に提示された数値には、インデックス領域は含まれていません。また、すべての計算は概算であり、展開によって異なります。

オプションの構成

必要に応じて、デフォルトの保持設定を変更できます。ただし、この構成は追加のストレージを消費します。以下の設定を有効にすることで、プロセス使用率データの精度を高めることができます。有効にできる構成は次のとおりです。

ENABLEMINUTELEVELGRANULARITYPROCESSUTILIZATION

ENABLEDAYLEVELGRANULARITYPROCESSUTILIZATION

これらの構成は、監視PowerShellコマンドレット: Set-MonitorConfigurationから有効にできます。

アプリケーション障害監視のポリシー

デフォルトでは、**アプリケーション障害**タブにはマルチセッションOS VDAからのアプリケーション障害のみが表示されます。アプリケーション障害監視の設定は、以下の監視ポリシーで変更できます。

アプリケーション障害の監視を有効にする

この設定を使用して、アプリケーション障害監視を構成し、アプリケーションエラーまたは障害（クラッシュおよび未処理の例外）、あるいはその両方を監視します。 **値**を**None**に設定すると、アプリケーション障害監視が無効になります。 この設定のデフォルトは「アプリケーション障害のみ」です。

シングルセッションOS VDAでのアプリケーション障害の監視を有効にする

デフォルトでは、マルチセッションOS VDAでホストされているアプリケーションからの障害のみが監視されます。シングルセッションOS VDAを監視するには、ポリシーを**Allowed**に設定します。 この設定のデフォルトは**Prohibited**です。

障害監視から除外されるアプリケーションのリスト

障害監視の対象としないアプリケーションのリストを指定します。 デフォルトでは、このリストは空です。

Analytics 用データ収集のポリシー

ANALYTICS 用 VDA データ収集

このポリシーを使用して、パフォーマンスおよびセキュリティ分析のために、VDAのパフォーマンスおよびセキュリティ関連メトリックをMonitorサービスが収集することを有効または無効にします。デフォルトでは、ポリシーは**許可**されています。VDAからのデータ収集を停止するには、ポリシーを**禁止**に設定します。

セキュリティ監視のためのクリップボード場所メタデータ収集

このポリシーを使用して、セキュリティ監視、監査、およびコンプライアンスのために、Brokerサービスによるクリップボード場所メタデータ収集を有効または無効にします。デフォルトでは、このポリシーは**有効**です。VDA からのデータ収集を停止するには、ポリシーを**無効**に設定します。

パフォーマンス監視のための診断データ収集

このポリシーを使用して、セッション情報、UPM/EUEMサービスの状態、Microsoft Teamsの最適化、接続プロトコルなどの診断データを収集するために監視サービスを有効にします。デフォルトでは、ポリシーは**有効**です。VDAsからのデータ収集を停止するには、ポリシーを**無効**に設定します。

ストレージ計画のヒント

グループポリシー。リソースデータまたはプロセスデータの監視に関心がない場合は、グループポリシーを使用してその両方またはどちらか一方をオフにできます。詳細については、ポリシーの作成の「**グループポリシー**」セクションを参照してください。

データグルーミング。デフォルトのデータ保持設定を変更して、データを早期にグルーミングし、ストレージスペースを解放できます。グルーミング設定の詳細については、APIを使用したデータアクセスの「データの粒度と保持」を参照してください。

仮想IPポリシー設定

> **重要:**
>
> - Windows 10 Enterprise multi-session は Remote Desktop IP Virtualization (Virtual IP) をサポートしていません。また、Windows 10 Enterprise multi-session では Remote Desktop IP Virtualization または仮想ループバックをサポートしていません。
> - リモートデスクトップIP仮想化 (仮想IP) は、クラウドホスト型マシンではサポートされていません。詳細については、Microsoftドキュメントを参照してください。

仮想IPセクションには、セッションが独自の仮想ループバックアドレスを持つかどうかを制御するポリシー設定が含まれています。

仮想IPループバックのサポート

この設定が有効な場合、各セッションは独自の仮想ループバックアドレスを持ちます。無効な場合、セッションは個別のループバックアドレスを持ちません。

デフォルトでは、この設定は無効になっています。

仮想IP仮想ループバックプログラムリスト

この設定は、仮想ループバックアドレスを使用できるアプリケーション実行可能ファイルを指定します。プログラムをリストに追加する際は、実行可能ファイル名のみを指定してください。完全なパスを指定する必要はありません。

デフォルトでは、実行可能ファイルは指定されていません。

仮想IPループバックポートの除外

アプリケーションがこの設定で指定されたポート上のループバックアドレスを呼び出す場合、仮想ループバックは呼び出しをセッション固有のループバックアドレスに変更しません。

レジストリを使用してCOMポートとLPTポートのリダイレクト設定を構成する

VDAバージョン7.0から7.8では、**COMポートとLPTポート**の設定はレジストリを使用してのみ構成できます。VDAバージョン7.0より前、およびVDAバージョン7.9以降では、これらの設定はWeb Studioで構成できます。詳細については、ポートリダイレクトポリシー設定および帯域幅ポリシー設定を参照してください。

COMポートおよびLPTポートリダイレクトのポリシー設定は、VDAイメージまたはマシン上のHKLM\Software\Citrix\GroupPolicy\Defaults\Deprecatedにあります。

COMポートとLPTポートのリダイレクトを有効にするには、次のようにREG_DWORD型の新しいレジストリキーを追加します。

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

レジストリキー	説明	許可される値
AllowComPortRedirection	COMポートリダイレクトを許可または禁止する	1（許可）または0（禁止）
LimitComBw	COMポートリダイレクトチャネルの帯域幅制限	数値
LimitComBWPercent	COMポートリダイレクトチャネルの帯域幅制限（セッションの総帯域幅に対する割合）	0から100までの数値
AutoConnectClientComPorts	ユーザーデバイスからCOMポートを自動的に接続する	1 (許可) または 0 (禁止)
AllowLptPortRedirection	LPTポートリダイレクトを許可または禁止する	1 (許可) または 0 (禁止)
LimitLptBw	LPTポートリダイレクトチャネルの帯域幅制限	数値
LimitLptBwPercent	LPTポートリダイレクトチャネルの帯域幅制限（セッショ	0から100までの数値

レジストリキー	説明	許可される値
	ン全体の帯域幅に対する割合)	
AutoConnectClientLptPorts	ユーザーデバイスからLPTポートを自動的に接続する	1 (許可) または 0 (禁止)

これらの設定を構成した後、マシンカタログを新しいマスターイメージまたは更新された物理マシンを使用するように変更します。ユーザーが次回ログオフしたときに、デスクトップは新しい設定で更新されます。

Configuration Manager 2012用コネクタのポリシー設定

Configuration Manager 2012用コネクタのセクションには、Citrix Connector 7.5エージェントを構成するためのポリシー設定が含まれています。

> **重要：**

> 警告、ログオフ、および再起動メッセージのポリシーは、手動またはProvisioning Servicesによって管理されるマルチセッションOSマシンカタログへの展開にのみ適用されます。これらのマシンカタログの場合、Connectorサービスは、保留中のアプリケーションのインストールまたはソフトウェア更新がある場合にユーザーに警告します。

> MCSによって管理されるカタログの場合、Web Studioを使用してユーザーに通知します。手動で管理されるシングルセッションOSカタログの場合、Configuration Managerを使用してユーザーに通知します。Provisioning Servicesによって管理されるシングルセッションOSカタログの場合、Provisioning Servicesを使用してユーザーに通知します。

警告頻度間隔

この設定は、ユーザーへの警告メッセージが表示される間隔を定義します。

間隔は、ddd.hh:mm:ssの形式で設定されます。ここで、:

- dddは日数で、オプションのパラメーターであり、0～999の範囲です。
- hhは時間で、0～23の範囲です。
- mmは分で、0～59の範囲です。
- ssは秒で、0～59の範囲です。

デフォルトでは、間隔設定は1時間（01:00:00）です。

警告メッセージボックスの本文

この設定には、今後のソフトウェア更新またはログオフが必要なメンテナンスについてユーザーに通知するメッセージの編集可能なテキストが含まれています。

デフォルトでは、メッセージは次のとおりです: {TIMESTAMP} 作業を保存してください。サーバーは {TIMELEFT} 後にメンテナンスのためオフラインになります。

警告メッセージボックスのタイトル

この設定には、ユーザーへの警告メッセージのタイトルバーの編集可能なテキストが含まれています。

デフォルトでは、タイトルは「今後のメンテナンス」です。

警告期間

この設定は、メンテナンスのどれくらい前に警告メッセージが最初に表示されるかを定義します。

時刻は ddd.hh:mm:ss の形式で設定されます。ここで、:

- ddd は日数で、オプションのパラメーターであり、範囲は 0〜999 です。
- hh は時間で、範囲は 0〜23 です。
- mm は分で、範囲は 0〜59 です。
- ss は秒で、範囲は 0〜59 です。

デフォルトでは、設定は 16 時間 (16:00:00) であり、最初の警告メッセージがメンテナンスの約 16 時間前に表示されることを示します。

最終強制ログオフメッセージボックスの本文

この設定には、強制ログオフが開始されたことをユーザーに警告するメッセージの編集可能なテキストが含まれています。

デフォルトでは、メッセージは次のとおりです: サーバーは現在、メンテナンスのためオフラインになります

最終強制ログオフメッセージボックスのタイトル

この設定には、最終的な強制ログオフメッセージのタイトルバーの編集可能なテキストが含まれます。

デフォルトでは、タイトルは「ITスタッフからの通知」です。

強制ログオフの猶予期間

この設定は、ユーザーにログオフを通知してから、保留中のメンテナンスを処理するために強制ログオフが実行されるまでの期間を定義します。

時間はddd.hh:mm:ssの形式で設定されます。ここで、:

- dddは日数で、オプションのパラメーターであり、範囲は0〜999です。
- hhは時間で、範囲は0〜23です。
- mmは分で、範囲は0〜59です。
- ssは秒で、範囲は0〜59です。

デフォルトでは、強制ログオフの猶予期間設定は5分 (00:05:00) です。

強制ログオフメッセージボックスの本文

この設定には、強制ログオフを開始する前に作業を保存してログオフするようユーザーに伝えるメッセージの編集可能なテキストが含まれます。

デフォルトでは、メッセージには次の内容が含まれます: {TIMESTAMP} 作業を保存してログオフしてください。サーバーは{TIMELEFT}後にメンテナンスのためオフラインになります。

強制ログオフメッセージボックスのタイトル

この設定には、強制ログオフメッセージのタイトルバーの編集可能なテキストが含まれます。

デフォルトでは、タイトルは「ITスタッフからの通知」です。

イメージ管理モード

Connectorエージェントは、Provisioning ServicesまたはMCSによって管理されているマシンのクローン上で実行されているかどうかを自動的に検出します。エージェントは、イメージ管理されたクローンでのConfiguration Managerの更新をブロックし、カタログのマスターイメージに更新を自動的にインストールします。

マスターイメージが更新された後、Web Studioを使用してMCSカタログクローンの再起動をオーケストレーションします。Connector Agentは、Configuration Managerのメンテナンスウィンドウ中にPVSカタログクローンの再起動を自動的にオーケストレーションします。Configuration Managerによってカタログクローンにソフトウェアがインストールされるようにこの動作を上書きするには、「イメージ管理モード」を「無効」に変更します。

再起動メッセージボックスの本文

この設定には、サーバーが再起動されるときにユーザーに通知するメッセージの編集可能なテキストが含まれています。

デフォルトでは、メッセージは「サーバーは現在、メンテナンスのためにオフラインになります。」です。

エージェントタスクが実行される通常の時間間隔

この設定は、Citrix Connector™エージェントタスクが実行される頻度を決定します。

時刻はddd.hh:mm:ssの形式で設定され、ここで:

- dddは日数で、オプションのパラメーターであり、0～999の範囲です。
- hhは時間で、0～23の範囲です。
- mmは分で、0～59の範囲です。
- ssは秒で、0～59の範囲です。

デフォルトでは、通常の時間間隔設定は5分（00:05:00）です。

ポリシーの変更

次の表に、Citrix Virtual Apps and Desktops™ 7 2503 のポリシー更新（追加、削除、名前の変更、デフォルト状態の変更を含む）を示します。

ポリシー設定	変更点
プロファイル管理 > 詳細設定 > ログオフ時のプロファイル同期を制限	ユーザーログオフ時に同期されるユーザーストアの数を設定するための新しいポリシーです。詳細はこちら。
プロファイル管理 > 詳細設定 > プロファイル読み込みタイムアウト	プロファイル読み込みタイムアウトを設定するための新しいポリシーです。詳細はこちら。
クライアントプリンターポリシー設定 > 保持および復元されたクライアントプリンター	2402 以降非推奨

> **注:**

アップグレードする前に、すべての非推奨設定を削除してください。非推奨設定が使用されたままになっている場合、アップグレードはエラーで失敗する可能性があります。

管理

Citrix Virtual Apps and Desktops™ サイトの管理には、さまざまな項目とタスクが含まれます。

ライセンス

サイトを作成する際には、Citrix License Serverへの有効な接続が必要です。後で、Studioからライセンスの追加、ライセンスの種類やモデルの変更、ライセンス管理者の管理など、いくつかのライセンス関連タスクを完了できます。StudioからLicense Administration Consoleにアクセスすることもできます。

アプリケーション

デリバリーグループ、およびオプションでアプリケーショングループ内のアプリケーションを管理します。

ゾーン

地理的に分散した展開では、ゾーンを使用してアプリケーションとデスクトップをエンドユーザーに近づけることで、パフォーマンスを向上させることができます。サイトをインストールして構成すると、すべてのコントローラー、マシンカタログ、およびホスト接続は1つのプライマリゾーンに配置されます。後で、Studioを使用してこれらの項目を含むサテライトゾーンを作成できます。サイトに複数のゾーンがある場合、新しく作成されたマシンカタログ、ホスト接続、または追加されたコントローラーをどのゾーンに配置するかを指定できます。ゾーン間で項目を移動することもできます。

接続とリソース

アプリケーションやデスクトップをユーザーに提供するマシンをホストするためにハイパーバイザーまたはその他のサービスを使用している場合、サイトを作成する際に、そのハイパーバイザーまたはその他のサービスへの最初の接続を作成します。その接続のストレージとネットワークの詳細がそのリソースを構成します。後で、その接続とそのリソースを変更したり、さらに多くの接続を作成したりできます。構成された接続を使用するマシンを管理することもできます。

ローカルホストキャッシュ

ローカルホストキャッシュにより、Delivery Controller™とサイトデータベース間の接続が失敗した場合でも、サイト内の接続仲介操作を続行できます。

仮想IPと仮想ループバック

Microsoft の仮想IPアドレス機能は、公開アプリケーションにセッションごとに一意の動的に割り当てられたIPアドレスを提供します。Citrix の仮想ループバック機能を使用すると、localhost との通信に依存するアプリケーションを、localhost 範囲内の一意の仮想ループバックアドレスを使用するように構成できます。

デリバリーコントローラー

この記事では、サイトからのControllerの追加と削除に関する考慮事項と手順について説明します。また、Controllerを別のゾーンまたはサイトに移動する方法、およびVDAを別のサイトに移動する方法についても説明します。

ControllerへのVDA登録

VDAがアプリケーションとデスクトップの配信を支援する前に、Controllerに登録（通信を確立）する必要があります。Controllerのアドレスは、この記事で説明されているいくつかの方法で指定できます。サイトでControllerが追加、移動、削除される際に、VDAが最新の情報を持っていることが重要です。

セッション

セッションアクティビティを維持することは、最高のユーザーエクスペリエンスを提供するために不可欠です。いくつかの機能により、セッションの信頼性を最適化し、不便さ、ダウンタイム、生産性の損失を軽減できます。

- セッションの信頼性
- クライアントの自動再接続
- ICA®キープアライブ
- ワークスペースコントロール
- セッションローミング

Studioでの検索の使用

Studioでマシン、セッション、マシンカタログ、アプリケーション、またはデリバリーグループに関する情報を表示したい場合は、柔軟な検索機能を使用します。

タグ

タグを使用して、マシン、アプリケーション、グループ、ポリシーなどのアイテムを識別します。その後、特定のタグを持つアイテムに適用されるように特定の操作を調整できます。

IPv4/IPv6

Citrix Virtual Apps and Desktops は、純粋な IPv4、純粋な IPv6、および IPv4 と IPv6 の重複するネットワークを使用するデュアルスタック展開をサポートしています。この記事では、これらの展開について説明し、図解します。また、IPv4 または IPv6 の使用を制御する Citrix ポリシー設定についても説明します。

ユーザープロファイル

デフォルトでは、VDA をインストールすると Citrix Profile Management が自動的にインストールされます。このプロファイルソリューションを使用する場合は、一般的な情報についてこの記事を確認してください。詳細については、Profile Management ドキュメントを参照してください。

Citrix Diagnostic Facility (CDF) トレースの収集

CDFControl ユーティリティは、さまざまな Citrix トレースプロバイダーから表示される Citrix Diagnostic Facility (CDF) トレースメッセージをキャプチャするためのイベントトレースコントローラーまたはコンシューマーです。これは、複雑な Citrix 関連の問題のトラブルシューティング、フィルターサポートの解析、およびパフォーマンスデータの収集のために作成されています。

シトリックス インサイト サービス

Citrix Insight Services (CIS) は、計測、テレメトリ、およびビジネスインサイト生成のための Citrix プラットフォームです。

シトリックス スカウト

Citrix Scout は診断情報を収集し、ヘルスチェックを実行します。結果は、Citrix Virtual Apps and Desktops 展開におけるプロアクティブなメンテナンスに利用できます。Citrix は、Citrix Insight Services を通じて診断コレクションの包括的で自動化された分析を提供します。また、Scout を使用して、単独で、または Citrix サポートのガイダンスを受けて問題をトラブルシューティングすることもできます。

アプリケーション

> **注:**
>
> Citrix Virtual Apps and Desktops™展開は、Web Studio（Webベース）とCitrix Studio（Windowsベース）の2つの管理コンソールを使用して管理できます。この記事ではWeb

> Studioのみを扱います。Citrix Studioについては、Citrix Virtual Apps and Desktops 7 2212以前の同等の記事を参照してください。

はじめに

展開でデリバリーグループのみを使用している場合（アプリケーショングループを使用していない場合）、アプリケーションをデリバリーグループに追加します。アプリケーショングループも使用している場合は、通常、代わりにアプリケーショングループにアプリケーションを追加します。このガイダンスにより、管理が容易になります。アプリケーションは常に、少なくとも1つのデリバリーグループまたはアプリケーショングループに属している必要があります。

アプリケーションの追加ウィザードでは、1つ以上のデリバリーグループ、または1つ以上のアプリケーショングループを選択できますが、両方を同時に選択することはできません。後でアプリケーションのグループ関連付けを変更することはできますが（たとえば、アプリケーションをアプリケーショングループからデリバリーグループに移動するなど）、ベストプラクティスではその複雑さを追加することは推奨されません。アプリケーションは1種類のグループに保持してください。

アプリケーションを複数のグループに関連付ける場合、それらのすべてのグループでアプリケーションを表示するのに十分な権限がないと、表示の問題が発生する可能性があります。そのような場合は、より高い権限を持つ管理者に相談するか、アプリケーションが関連付けられているすべてのグループを含むようにスコープを拡張してください。

同じ名前のアプリケーションを2つ（異なるグループからでも）同じユーザーに公開する場合は、Web Studioで`Application name (for user)`プロパティを変更してください。そうしないと、ユーザーはCitrix Workspace™アプリで重複した名前を目にすることになります。

アプリケーションのプロパティ（設定）は、追加時または後で変更できます。アプリケーションが配置されているアプリケーションフォルダーも、アプリケーションの追加時または後で変更できます。

詳細については、以下を参照してください。

- デリバリーグループの作成
- アプリケーショングループの作成
- タグ

アプリケーションの追加

アプリケーションは、デリバリーグループまたはアプリケーショングループの作成時に追加できます。これらの手順は、デリバリーグループの作成およびアプリケーショングループの作成に詳述されています。次の手順では、グループ作成後にアプリケーションを追加する方法について説明します。

知っておくと良いこと：

- Remote PC Accessデリバリーグループにはアプリケーションを追加できません。
- アプリケーションの追加ウィザードを使用して、デリバリーグループまたはアプリケーショングループからアプリケーションを削除することはできません。これは別の操作です。

1つ以上のアプリケーションを追加するには：

1. 左ペインで**アプリケーション**を選択し、アクションバーで**アプリケーションの追加**を選択します。
2. アプリケーションの追加ウィザードが**はじめに**ページとともに起動します。このページは、今後のウィザード起動時に表示しないように設定できます。
3. ウィザードは、**グループ**、**アプリケーション**、**概要**の各ページを案内します。各ページの作業が完了したら、**次へ**をクリックして**概要**ページに進みます。

単一のデリバリーグループまたはアプリケーショングループにアプリケーションを追加する場合の、手順1の代替案：

- **1つのデリバリーグループにのみアプリケーションを追加する場合：** 手順1で、Web Studioの左ペインで**デリバリーグループ**を選択し、中央ペインでデリバリーグループを選択してから、アクションバーで**アプリケーションの追加**を選択します。ウィザードには**グループ**ページは表示されません。
- **1つのアプリケーショングループにのみアプリケーションを追加する場合：** 手順1で、Web Studioの左ペインで**アプリケーション**を選択し、中央ペインでアプリケーショングループを選択してから、アクションバーのアプリケーショングループ名の下にある**アプリケーションの追加**エントリを選択します。ウィザードには**グループ**ページは表示されません。

グループページ

このページには、サイト内のすべてのデリバリーグループが一覧表示されます。アプリケーショングループも作成している場合は、アプリケーショングループとデリバリーグループが一覧表示されます。どちらかのグループを選択できますが、両方のグループを同時に選択することはできません。つまり、アプリケーショングループとデリバリーグループに同時にアプリケーションを追加す

ることはできません。通常、アプリケーショングループを使用している場合は、デリバリーグループではなくアプリケーショングループにアプリケーションを追加します。

アプリケーションを追加するときは、少なくとも1つのデリバリーグループ（または、利用可能な場合はアプリケーショングループ）の横にあるチェックボックスをオンにします。すべてのアプリケーションは、常に少なくとも1つのグループに関連付けられている必要があります。

アプリケーションページ

アプリケーションソースを表示するには、**追加**をクリックします。

- **メニューから:** 選択したデリバリーグループ内のマシンで検出されたアプリケーション。このソースを選択すると、検出されたアプリケーションのリストを含む新しいページが起動します。追加するアプリケーションのチェックボックスをオンにして、 をクリックします。

  このソースは、(1) 関連付けられたデリバリーグループがないアプリケーショングループを選択した場合、(2) マシンが含まれていない関連付けられたデリバリーグループがあるアプリケーショングループを選択した場合、または (3) マシンが含まれていないデリバリーグループを選択した場合は、選択できません。

- **手動:** デリバリーグループ内のVDA上、またはネットワーク内の別の場所にあるアプリケーション。このソースを選択すると、アプリケーションを次の方法で追加する新しいページが開きます。

  - 実行可能ファイルへのパス、作業ディレクトリ、オプションのコマンドライン引数、および管理者とユーザーの表示名を入力します。
  - デリバリーグループ内のVDAからアプリケーションを選択します。これを行うには、 をクリックし、VDAにアクセスするための資格情報を入力し、VDAへの接続を待ってから、VDAからアプリケーションを選択します。選択したアプリケーションのプロパティが、ページ上のフィールドに自動的に入力されます。

- **既存:** 以前にサイトに追加されたアプリケーション。このソースを選択すると、検出されたアプリケーションのリストを含む新しいページが起動します。追加するアプリケーションのチェックボックスをオンにして、 をクリックします。

  サイトにアプリケーションがない場合、このソースは選択できません。

- **アプリケーションパッケージ:** App-V、MSIX、MSIX app attach、またはFlexAppアプリケーションパッケージ内のアプリケーション。このソースを選択すると、 ページが起動します。アプリケーションパッケージソースを選択し、表示された結果から追加するアプリケーションを選択して、 を選択します。詳しくは、「Appパッケージの展開と配信」を参照してください。

- **アプリケーショングループ:** アプリケーショングループ。このソースを選択すると、アプリケーショングループのリストを含む新しいページが起動します。（表示には各グループ内のアプリケーションもリストされますが、個々のアプリケーションではなくグループのみを選択できます。）選択したグループ内の現在および将来のすべてのアプリケーションが追加されます。追加するアプリケーショングループのチェックボックスをオンにして、 をクリックします。

  このソースは、(1) アプリケーショングループがない場合、または (2) 選択したデリバリーグループがアプリケーショングループをサポートしていない場合（たとえば、静的に割り当てられたマシンを持つデリバリーグループ）は選択できません。

表に示されているように、 リストの一部のソースは、その種類の有効なソースがない場合は選択できません。互換性のないソース（たとえば、アプリケーショングループにアプリケーショングループを追加できないなど）はリストに含まれません。選択したグループに既に追加されているアプリケーションは選択できません。

このページまたは後で、アプリケーションのプロパティ（設定）を変更できます。

デフォルトでは、追加されたアプリケーションは`Applications`という名前のアプリケーションフォルダーに配置されます。このページまたは後でアプリケーションを変更できます。アプリケーションを追加しようとして、同じ名前のアプリケーションが同じフォルダーに存在する場合、追加するアプリケーションの名前を変更するように求められます。提示された新しい名前を受け入れるか、拒否してアプリケーションの名前を変更するか、別のフォルダーを選択できます。たとえば、 フォルダーに`app`が既に存在し、そのフォルダーに`app`という名前の別のアプリケーションを追加しようとすると、新しい名前`app_1`が提示されます。

概要ページ

10個以下のアプリケーションを追加する場合、その名前は**** にリストされます。10個を超えるアプリケーションを追加する場合、合計数が指定されます。

概要情報を確認し、**「完了」**をクリックします。

アプリケーションのグループ関連付けを変更する

アプリケーションを追加した後、そのアプリケーションが関連付けられているデリバリーグループとアプリケーショングループを変更できます。

アプリケーションを別のグループにドラッグできます。これは、アクションバーのコマンドを使用する代替手段です。

アプリケーションがアプリケーショングループを使用するか直接的かにかかわらず、複数のデリバリーグループに関連付けられている場合、グループの優先順位を使用して、複数のグループが評価される順序を指定できます。グループは、アクセスポリシー、ユーザーリスト、スマートアクセスタグなどの要因に基づいて考慮対象から除外でき、グループから選択される特定のマシンは、ゾーンの優先順位、起動準備状況、タグ制限などの要因によって影響を受ける可能性があります。デフォルトでは、すべてのグループの優先順位は0（最高）です。デリバリーグループの優先順位が同じ場合、アプリケーションの起動には最も負荷の低いデリバリーグループが選択されます。この場合、垂直ロードバランシングは考慮されません。

アプリケーションは、アプリケーションを配信できる共有（プライベートではない）マシンを含むデリバリーグループに関連付けることができます。また、(1) デリバリーグループに共有マシンが含まれており、XenDesktop 7.xのバージョン7.9より前に作成されたもので、(2) `Edit delivery group` 権限がある場合、デスクトップのみを配信する共有マシンを含むデリバリーグループを選択することもできます。プロパティダイアログがコミットされると、デリバリーグループの種類は自動的に `desktops and applications` に変換されます。

1. Web Studioにサインインし、左ペインで を選択し、アプリケーションを選択します。
2. アクションバーで を選択します。
3. ページを選択します。

    - グループを追加するには、 をクリックし、 または を選択します。（アプリケーショングループを作成していない場合、唯一の項目は です。）次に、1つ以上の利用可能なグループを選択します。アプリケーションと互換性のないグループ、またはすでにアプリケーションに関連付けられているグループは選択できません。
    - グループを削除するには、1つ以上のグループを選択し、 をクリックします。グループの関連付けを削除した結果、アプリケーションがどのグループにも関連付けられなくなる場合、アプリケーションが削除されることを警告されます。
    - グループの優先順位を変更するには、グループを選択し、 をクリックします。優先順位の値を選択し、 をクリックします。

4. 完了したら、 をクリックして変更を適用し、ウィンドウを開いたままにするか、 をクリックして変更を適用し、ウィンドウを閉じます。

アプリケーションの複製、有効化または無効化、名前の変更、または削除

次のアクションが利用可能です。

- **複製：** 異なるパラメーターまたはプロパティを持つ別のバージョンを作成するために、アプリケーションを複製したい場合があります。アプリケーションを複製すると、一意のサフィックスで自動的に名前が変更され、元のアプリケーションの隣に配置されます。また、アプリケーションを複製してから、別のグループに追加したい場合もあります。（複製後、アプリケーションを移動する最も簡単な方法はドラッグすることです。）
- **有効化または無効化：** アプリケーションの有効化と無効化は、デリバリーグループまたはアプリケーショングループの有効化と無効化とは異なるアクションです。
- **名前の変更：** 一度に1つのアプリケーションのみ名前を変更できます。アプリケーションの名前を変更しようとして、同じ名前のアプリケーションが同じフォルダーまたはグループに存在する場合、別の名前を指定するように求められます。
- **削除：** アプリケーションを削除すると、関連付けられていたデリバリーグループおよびアプリケーショングループから削除されますが、元々アプリケーションを追加するために使用されたソースからは削除されません。アプリケーションの削除は、デリバリーグループまたはアプリケーショングループから削除するのとは異なるアクションです。

アプリケーションを複製、有効化、無効化、名前変更、または削除するには：

1. 左側のペインで を選択します。
2. 中央のペインで1つ以上のアプリケーションを選択し、アクションバーで適切なタスクを選択します。
3. プロンプトが表示されたら、アクションを確認します。

デリバリーグループからアプリケーションを削除する

アプリケーションは、少なくとも1つのデリバリーグループまたはアプリケーショングループに関連付けられている（属している）必要があります。アプリケーションをデリバリーグループから削除しようとして、そのアプリケーションがどのデリバリーグループまたはアプリケーショングループとも関連付けがなくなる場合、続行するとアプリケーションが削除されることが通知されます。その場合、そのアプリケーションを配信したい場合は、有効なソースから再度追加する必要があります。

1. 左側のペインで を選択します。
2. デリバリーグループを選択します。中央下部のペインで、 タブの削除するアプリケーションを選択します。
3. アクションバーから を選択します。
4. 削除を確認します。

アプリケーショングループからアプリケーションを削除する

アプリケーションは、少なくとも1つのデリバリーグループまたはアプリケーショングループに属している必要があります。アプリケーションをアプリケーショングループから削除しようとして、その結果、そのアプリケーションがどのグループにも属さなくなる場合、続行するとアプリケーションが削除されるという通知が表示されます。その場合、そのアプリケーションを配信したい場合は、有効なソースから再度追加する必要があります。

1. 左ペインで**アプリケーション**を選択します。
2. 中央ペインでアプリケーショングループを選択し、1つ以上のアプリケーションを選択します。
3. アクションバーで**アプリケーショングループから削除**を選択します。
4. 削除を確認します。

アプリケーションプロパティを変更する

アプリケーションのプロパティは、一度に1つしか変更できません。

アプリケーションのプロパティを変更するには：

1. 左ペインで**アプリケーション**を選択します。
2. アプリケーションを選択し、アクションバーで**アプリケーションプロパティの編集**を選択します。
3. 変更したいプロパティを含むページを選択します。
4. 完了したら、**適用**をクリックして変更を適用し、ウィンドウを開いたままにするか、**OK**をクリックして変更を適用し、ウィンドウを閉じます。

次のリストでは、ページが括弧内に表示されます。

プロパティ	ページ
Citrix Workspaceアプリでアプリケーションが表示されるカテゴリまたはフォルダー	配信
コマンドライン引数。(#pass-parameters-to-published-applications)を参照	場所
アプリケーションが利用可能なデリバリーグループおよびアプリケーショングループ	グループ
説明	識別

プロパティ	ページ
ファイル名拡張子とファイルの種類関連付け: アプリケーションが自動的に開く拡張子	ファイルの種類関連付け
アイコン	配信
StoreFront™用キーワード	識別
制限。(#configure-application-limits)を参照	配信
名前: ユーザーおよび管理者が参照する名前	識別
実行可能ファイルへのパス。「公開アプリケーションへのパラメーターの受け渡し」を参照してください。(#pass-parameters-to-published-applications)	場所
ユーザーのデスクトップ上のショートカット: 有効または無効	配信
可視性: Citrix Workspaceアプリでアプリケーションを表示できるユーザーを制限します。非表示のアプリケーションでも起動できます。利用不可かつ非表示にするには、別のグループに追加します。	可視性の制限
作業ディレクトリ	場所

アプリケーションの変更は、現在のアプリケーションユーザーがセッションからログオフするまで有効にならない場合があります。

アプリケーション制限を構成する

アプリケーションの使用状況を管理するために、アプリケーション制限を構成します。たとえば、アプリケーション制限を使用して、アプリケーションに同時にアクセスするユーザーの数を管理できます。同様に、アプリケーション制限を使用して、リソースを大量に消費するアプリケーションの同時インスタンス数を管理できます。この制限は、サーバーのパフォーマンスを維持し、サービスの劣化を防ぐのに役立ちます。

この機能は、Controllerによって仲介されるアプリケーション起動の数（Citrix WorkspaceアプリやStoreFrontなどから）を制限するものであり、他の方法で起動できる実行中のアプリケーションの

数を制限するものではありません。これは、アプリケーション制限が同時使用の管理において管理者を支援するものの、すべてのシナリオで強制力を持つわけではないことを意味します。たとえば、Controllerが停止モードの場合、アプリケーション制限は適用できません。

デフォルトでは、同時に実行できるアプリケーションインスタンスの数に制限はありません。アプリケーション制限の設定はいくつかあります。それらのいずれか、またはすべてを構成できます。

- デリバリーグループ内のすべてのユーザーによるアプリケーションの同時インスタンスの最大数。
- デリバリーグループ内のユーザーごとに1つのアプリケーションインスタンス。
- マシンごとのアプリケーションの同時インスタンスの最大数（PowerShellのみ）。

制限が構成されている場合、ユーザーが構成された制限を超えるアプリケーションのインスタンスを起動しようとすると、エラーメッセージが生成されます。複数の制限が構成されている場合、最初の制限に達したときにエラーが報告されます。

アプリケーション制限の使用例：

- **同時インスタンスの最大数制限：** デリバリーグループで、アプリケーション `Alpha` の同時インスタンスの最大数を15に構成します。その後、そのデリバリーグループのユーザーは、そのアプリケーションの15個のインスタンスを同時に実行しています。そのデリバリーグループのいずれかのユーザーが `Alpha` を起動しようとすると、エラーメッセージが生成されます。構成された同時アプリケーションインスタンス制限（15）を超えるため、`Alpha` は起動されません。
- **ユーザーごとのインスタンス数制限：** 別のデリバリーグループで、アプリケーション `Beta` のユーザーごとのインスタンス数オプションを有効にします。ユーザーのTonyはアプリケーション `Beta` を正常に起動します。その日の後半、そのアプリケーションがTonyのセッションでまだ実行されている間に、彼は `Beta` の別のインスタンスを起動しようとします。エラーメッセージが生成され、ユーザーごとのインスタンス数制限を超えるため、`Beta` は起動されません。
- **同時インスタンスの最大数とユーザーごとのインスタンス数制限：** 別のデリバリーグループで、同時インスタンスの最大数を10に構成し、アプリケーション `Delta` のユーザーごとのインスタンス数オプションを有効にします。その後、そのデリバリーグループの10人のユーザーがそれぞれ `Delta` のインスタンスを実行している場合、そのデリバリーグループの他のユーザーが `Delta` を起動しようとすると、エラーメッセージが表示されます。`Delta` は起動されません。現在の10人の `Delta` ユーザーのいずれかがそのアプリケーションの2番目のイン

スタンスを起動しようとすると、エラーメッセージが表示され、2番目のインスタンスは起動されません。

- **マシンごとの同時インスタンスの最大数とタグ制限の使用：** アプリケーション `Charlie` には、特定のサーバーで同時に実行できるインスタンスの数を規定するライセンスとパフォーマンス要件があります。これらの要件は、サイト内のすべてのサーバーで同時に実行できるインスタンスの数も規定します。

  アプリケーションのインスタンスごとのマシン制限は、サイト内のすべてのサーバーに影響します（特定のデリバリーグループ内のマシンだけでなく）。サイトに3台のサーバーがあるとします。アプリケーション `Charlie` の場合、マシンごとのアプリインスタンス制限を2に構成します。したがって、サイト全体でアプリケーション `Charlie` のインスタンスは6つまでしか起動できません。（これは、3台のサーバーそれぞれでCharlieのインスタンスが2つという制限です。）

  デリバリーグループ内の特定のコンピューターにのみアプリケーションの使用を制限するには（サイト全体のすべてのコンピューターでのインスタンスを制限することに加えて）：

  - それらのマシンにタグ付け機能を使用します。
  - そのアプリケーションのマシンごとの最大インスタンス数を構成します。

アプリケーションがControllerのブローカー以外の方法で起動され（たとえば、Controllerが停止モードの場合など）、構成された制限を超過した場合、ユーザーは制限を超過しないように十分なインスタンスを閉じるまで、それ以上のインスタンスを起動できません。制限を超過したインスタンスは強制的にシャットダウンされません。ユーザーが閉じるまで継続して実行が許可されます。

セッションローミングを無効にする場合は、ユーザーごとのアプリケーションインスタンス数制限を無効にします。ユーザーごとのアプリケーションインスタンス数制限を有効にする場合は、新しいデバイスで新しいセッションを許可する2つの値のいずれも構成しないでください。ローミングについて詳しくは、「セッション」を参照してください。

デリバリーグループごとの最大インスタンス数制限と、ユーザーごとのインスタンス数制限を構成するには：

1. 左ペインで**アプリケーション**を選択し、アプリケーションを選択します。
2. アクションバーで**アプリケーションプロパティの編集**を選択します。
3. **デリバリー**ページで、次のいずれかのオプションを選択します。
   - **アプリケーションの無制限の使用を許可する**。同時に実行されるインスタンス数に制限はありません。これがデフォルトです。

- **アプリケーションの制限を設定する**。2種類の制限があります。いずれかまたは両方を指定します。
  - マシンごとに同時に実行できるインスタンスの最大数を指定します
  - ユーザーごとにアプリケーションのインスタンスを1つに制限する

4. **OK**をクリックして変更を適用しダイアログボックスを閉じるか、**適用**をクリックして変更を適用しダイアログボックスを開いたままにします。

マシンごとの最大インスタンス数制限を構成するには（PowerShellのみ）：

- PowerShellで（Citrix Cloud™展開の場合はRemote PowerShell SDKを、オンプレミス展開の場合はPowerShell SDKを使用して）、適切な`BrokerApplication`コマンドレットを`MaxPerMachineInstances`パラメーターとともに実行します。
- ガイダンスについては、`Get-Help`コマンドレットを使用します。例：

  ```
  Get-Help Set-BrokerApplication –Parameter MaxPerMachineInstances
  ```

公開アプリケーションにパラメーターを渡す

アプリケーションのプロパティの**場所**ページを使用して、コマンドラインを入力し、公開アプリケーションにパラメーターを渡します。

公開アプリケーションをファイルの種類に関連付けると、記号`"%*"`（二重引用符で囲まれたパーセント記号とアスタリスク記号）がアプリケーションのコマンドラインの末尾に追加されます。これらの記号は、ユーザーデバイスに渡されるパラメーターのプレースホルダーとして機能します。

公開アプリケーションが期待どおりに起動しない場合は、そのコマンドラインに正しい記号が含まれていることを確認してください。デフォルトでは、記号`"%*"`が追加されると、ユーザーデバイスから提供されるパラメーターが検証されます。ユーザーデバイスから提供されるカスタマイズされたパラメーターを使用する公開アプリケーションの場合、コマンドライン検証をバイパスするために、記号`"%**"`がコマンドラインに追加されます。アプリケーションのコマンドラインにこれらの記号が表示されない場合は、手動で追加してください。

実行可能ファイルへのパスにスペースを含むディレクトリ名が含まれている場合（例: `"C:\Program Files"`）、そのスペースがコマンドラインの一部であることを示すために、アプリケーションのコマンドラインを二重引用符で囲みます。これを行うには、パスの周りに二重引用符を追加し、`%*`記号の周りにもう一組の二重引用符を追加します。パスの閉じ引用符と`%*`記号の開き引用符の間にスペースを含めるようにしてください。

たとえば、公開アプリケーションであるWindows Media Playerのコマンドラインは次のとおりです。

```
"C:\Program Files\Windows Media Player\mplayer1.exe" "%*"
```

> **注:**
>
> 公開アプリケーションを起動するためのコマンドラインの最大文字数 (引数を含む) は203文字です。

公開アプリケーションでのセッションサインアウトの問題のトラブルシューティング

アプリケーションを公開する場合、公開アプリケーションのメイン実行可能ファイルのみが指定されます。ただし、一部のアプリケーションは、バックグラウンドで実行され、メインの公開アプリケーションが閉じられても対応するメイン実行可能ファイルによって閉じられない追加の（子）プロセスを生成する場合があります。追加のプロセスは、実行されるスクリプトや、`Run`や`RunOnceKey`のような特定のレジストリキーから作成されることもあります。これらのアプリケーションは、正常なサインアウトを妨げ、セッションが残存したりハングしたりする原因となり、セッションが閉じられず、ユーザーがサインアウトされない可能性があります。

この場合、Citrix Director を使用してこれらのセッションをリセットまたは終了する必要があります。

セッションが適切にサインアウトされない問題を特定し、トラブルシューティングするために、Citrixは3つのレジストリエントリを提供しています。これらの問題によりセッションが適切にログオフされない場合の特定とトラブルシューティングは、次の3つのステップからなるプロセスです。

1. どのセッションが公開アプリケーションによって正常なサインアウトを妨げているかを特定する
2. それらの公開アプリケーションが追加の（子）プロセスを生成するかどうかを特定する
3. これらのプロセスを指定されたレジストリエントリに追加して、サインアウトを妨げないようにする

ステップ2: 公開アプリケーションが追加の（子）プロセスを生成するかどうかを特定する

公開アプリケーションが正常なサインアウトを妨げていると特定されたら、次のステップは、このアプリケーションが実行時に追加のプロセスを生成するかどうかを判断することです。

公開アプリケーションが閉じられたときに、`HKCU\Software\CitrixVolatile\Seamless\Sessions\[ID]\LogoffCheckerBlockingProcess` を読んで、どのプロセスが正常なサインアウトをブロックしているかを判断できます。

以下の例では、キー `LogoffCheckerBlockingProcess` に次のエントリが含まれています。

```
PhoneExperienceHost.exe

SkypeApp.exe

SkypeBackgroundHost.exe
```

これらのプロセスが正常なサインアウトを妨げていました。

> **注:**
>
> 確認したいセッションの正しいセッションIDで を置き換えてください。

ステップ3: これらのプロセスを指定されたレジストリエントリに追加して、サインアウトを妨げないようにする

これらのプロセスを以下のレジストリキーに追加することで、今後のセッションでサインアウトが妨げられるのを防ぐことができます。

```
Add the process file name to the following registry key:

Caution! Refer to the Disclaimer at the end of this article before using
the Registry Editor.

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWI

Value Name:LogoffCheckSysModules

Type:REG_SZ

String:MyAppName.exe
```

`LogoffCheckSysModules` の詳細については、公開アプリケーションからの正常なログオフによりセッションがアクティブ状態になる を参照してください。

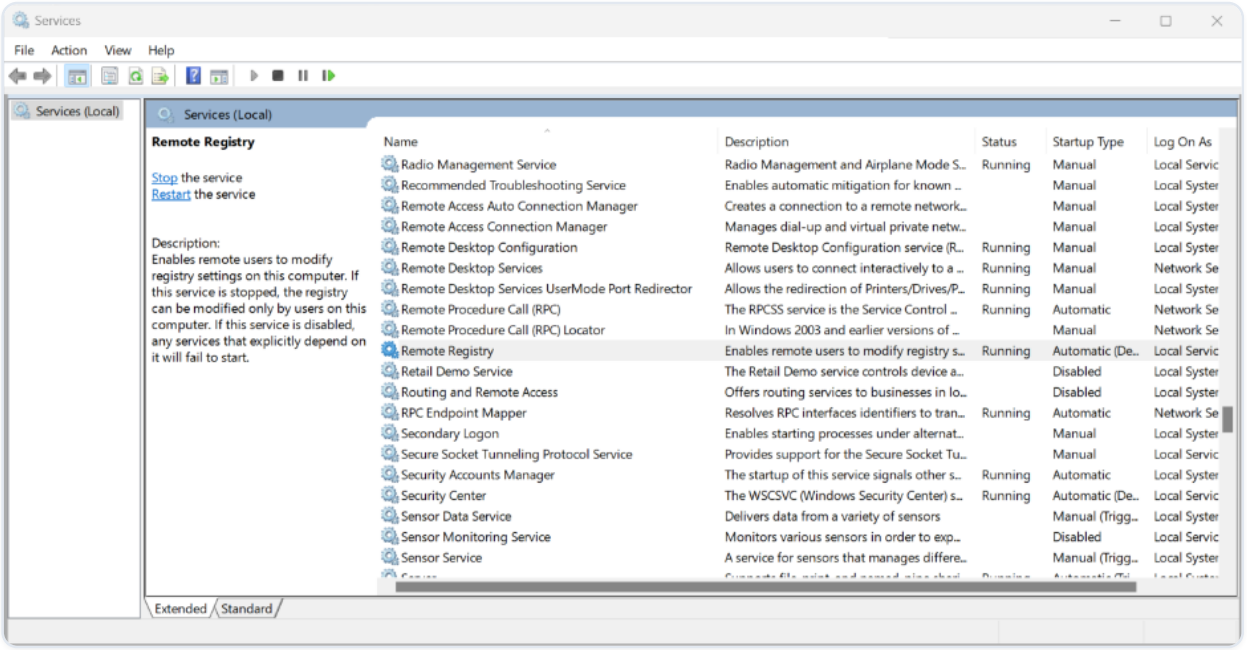
ステップバイステップのトラブルシューティングガイド

1. テスト対象のVDAでリモートレジストリサービスを開始します。

   a. コントロールパネルで、**管理ツール > サービス** を選択します。

   b. **リモートレジストリサービス** を右クリックし、**プロパティ** を選択します。

   c. **スタートアップの種類** で、ドロップダウンメニューから **自動** を選択します。



2. テスト対象のVDAでWindowsファイアウォールをオフにするか、ポート455を有効にする受信ファイアウォール規則を作成します。

   a. コントロールパネルで、**Windows Defender Firewall > Advanced Settings**を選択します。

   b. **受信の規則**を右クリックし、**新しい規則**を選択します。

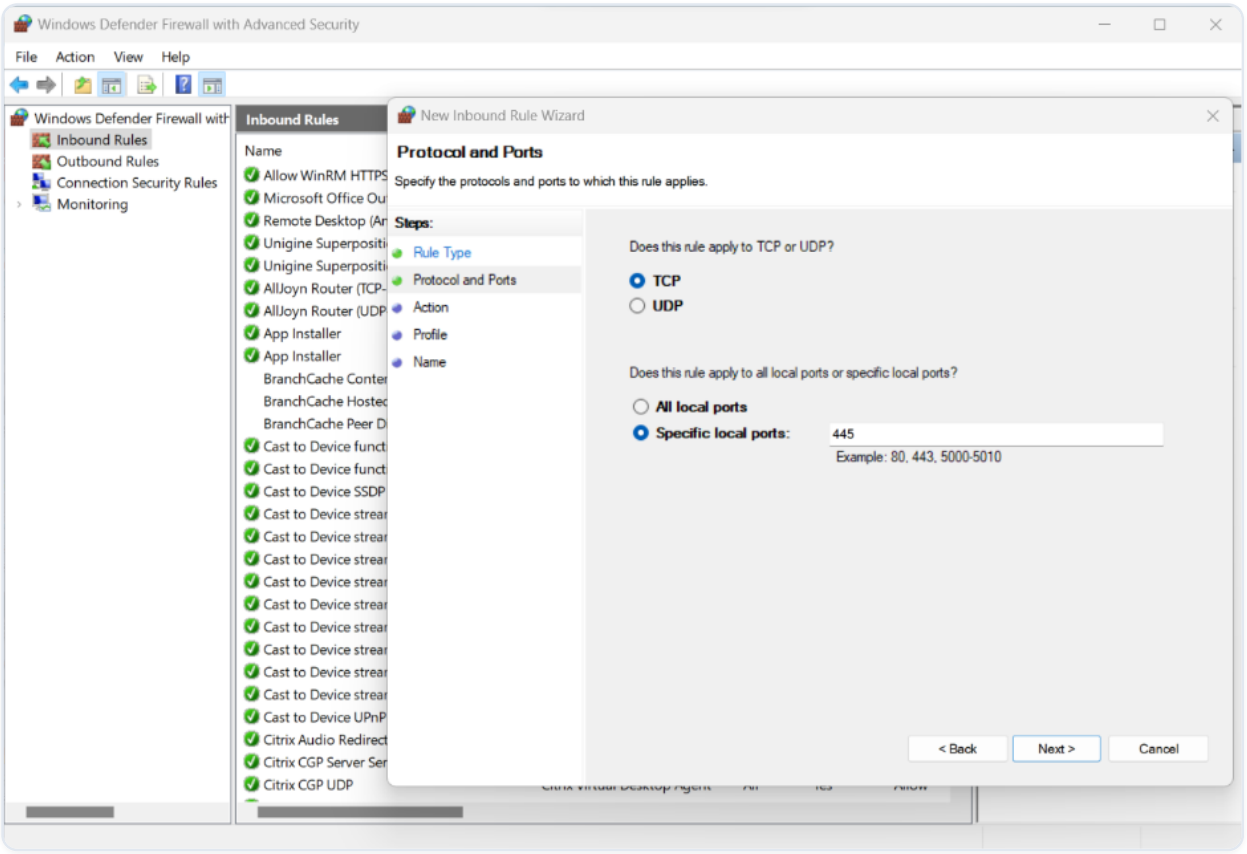
   c. **新しい受信の規則ウィザード**で、**ポート**を選択します。

   d. **プロトコルおよびポート**ページで、**TCPおよび特定のローカルポート**を選択します。ローカルポートとして `445` を入力します。

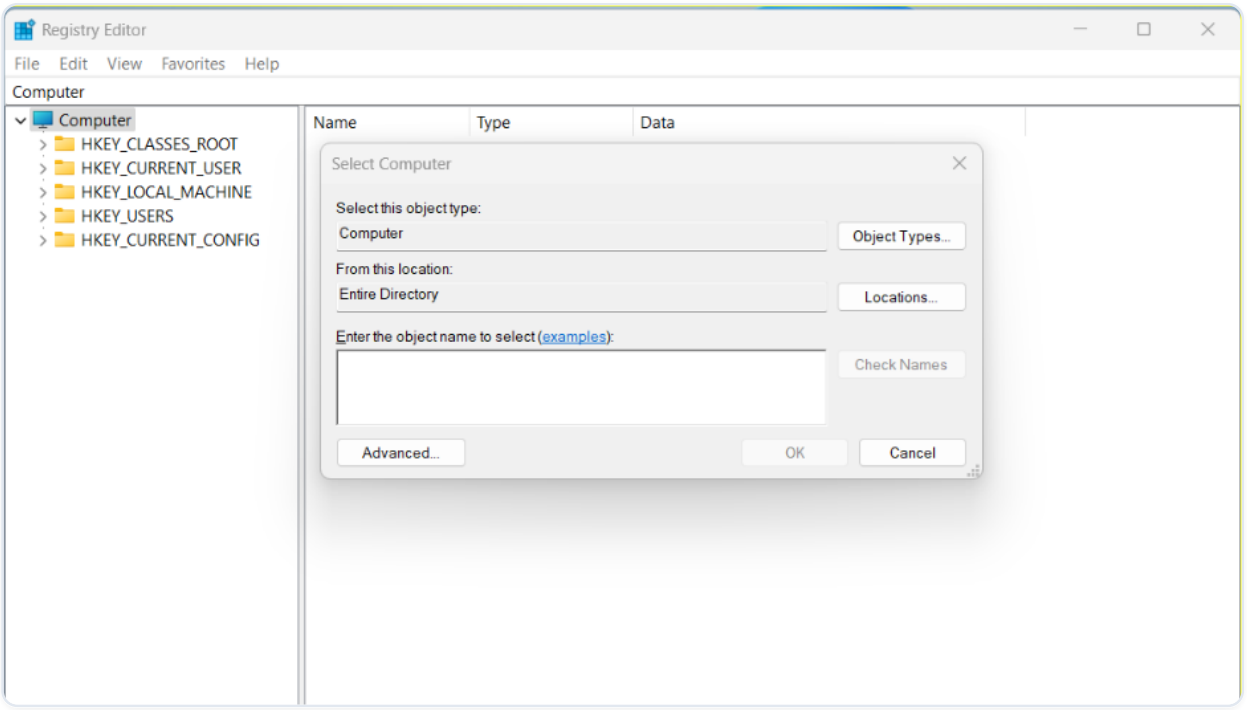
   e. **操作**ページで**接続を許可する**を選択します。

   f. 新しい受信規則を適用するファイアウォールプロファイルを選択します。

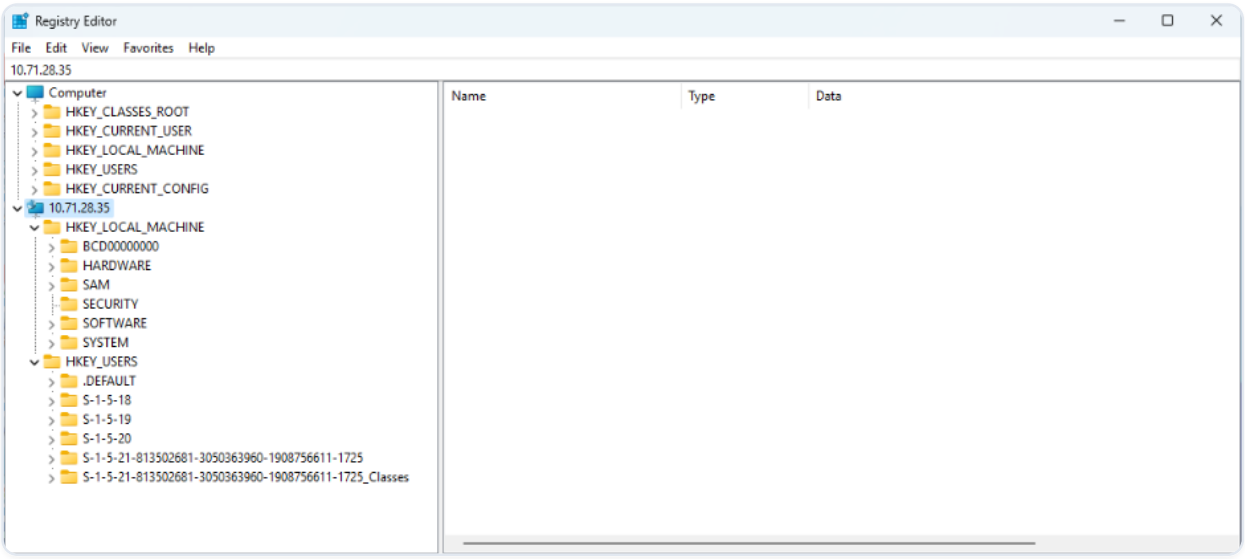
   g. ファイアウォール規則に名前を付け、**完了**を選択して**新しい受信の規則ウィザード**を終了します。



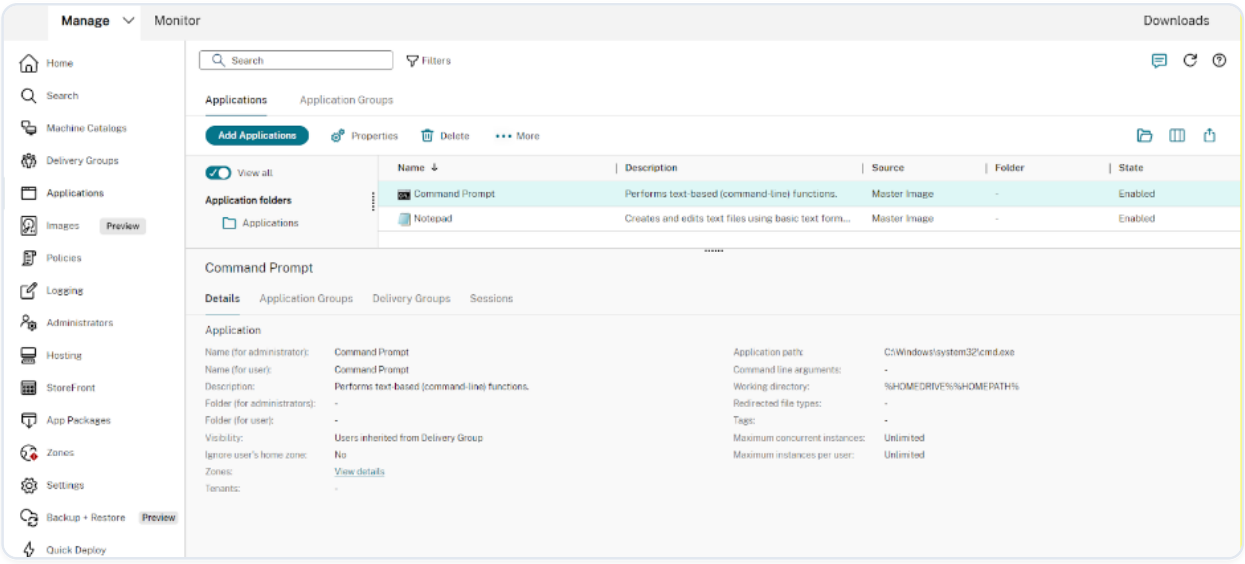
3. 同じドメイン内の別のVM（DC、DDC、または別のVDAでも可）から、`Regedit`を実行し、リモートレジストリに接続します。



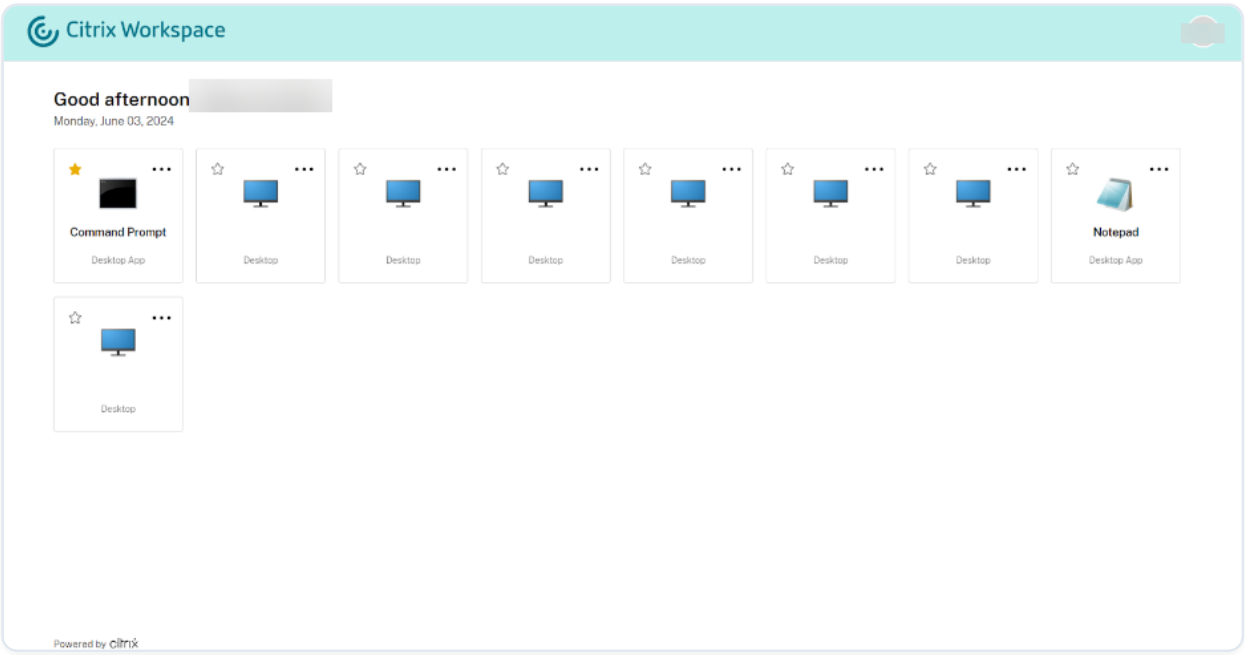
4. テスト対象のVDAのIPアドレスを入力し、**OK**をクリックします。`regedit`ツリーには、テスト対象のVDAのブランチが表示される必要があります。



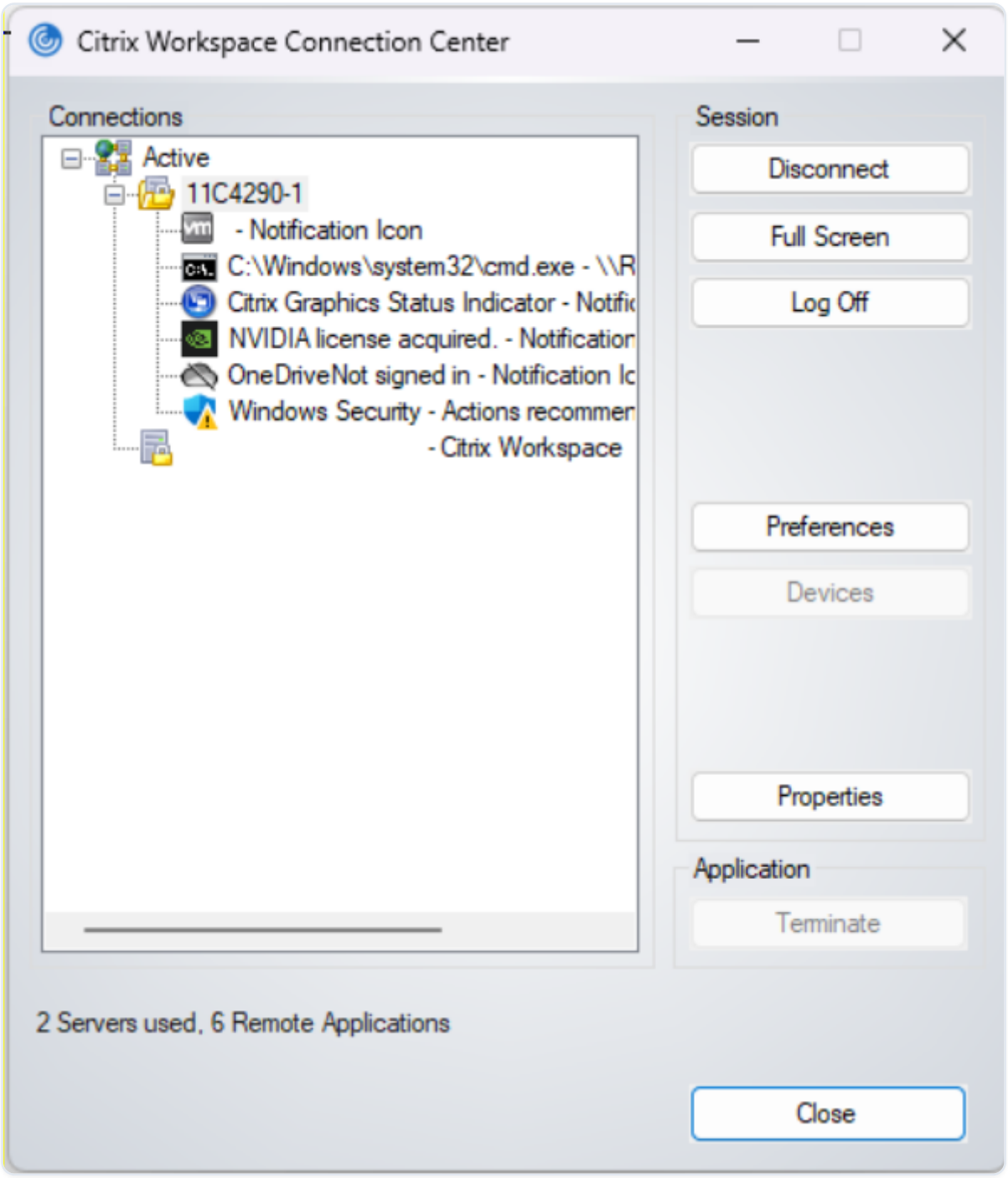
5. **コマンドプロンプト**公開アプリケーションを開きます。



Citrix Workspace に **コマンドプロンプト** アプリが表示されます。



6. クライアントで**接続センター**を開きます。これは、開いているシームレスアプリを閉じた後にセッションがサインアウトされたときに監視するために使用されます。次の画像で、リモートVDI上でコマンドプロンプトプロセス`c:\Windows\system32\cmd.exe`がアクティブであることがわかります。



7. **regedit** が実行されている VDA から、次のリモート IP の場所に移動します。
`HKEY_USERS\S-1-X-XX-XXXXXXXX-XXXXXXXXXXX-XXXXXXXXXX-XXXX\SOFTWARE\CitrixVolatile\Seamless\Sessions\X\`

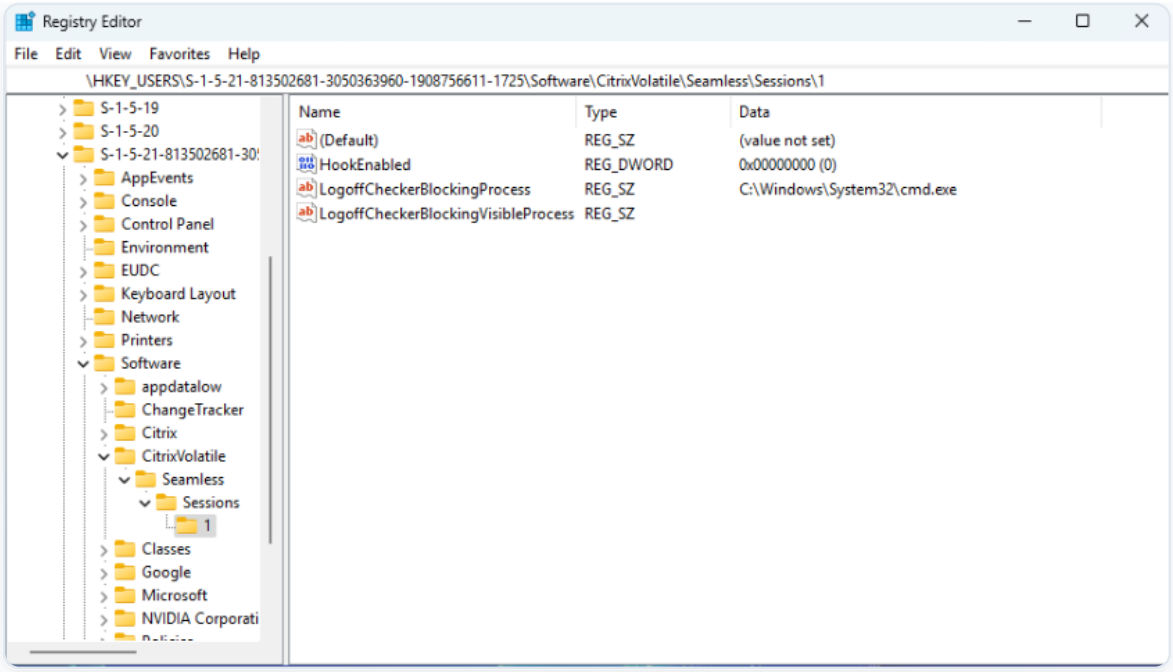
> **注:**

新しいセッションを開くたびにこのパスは変更されます。

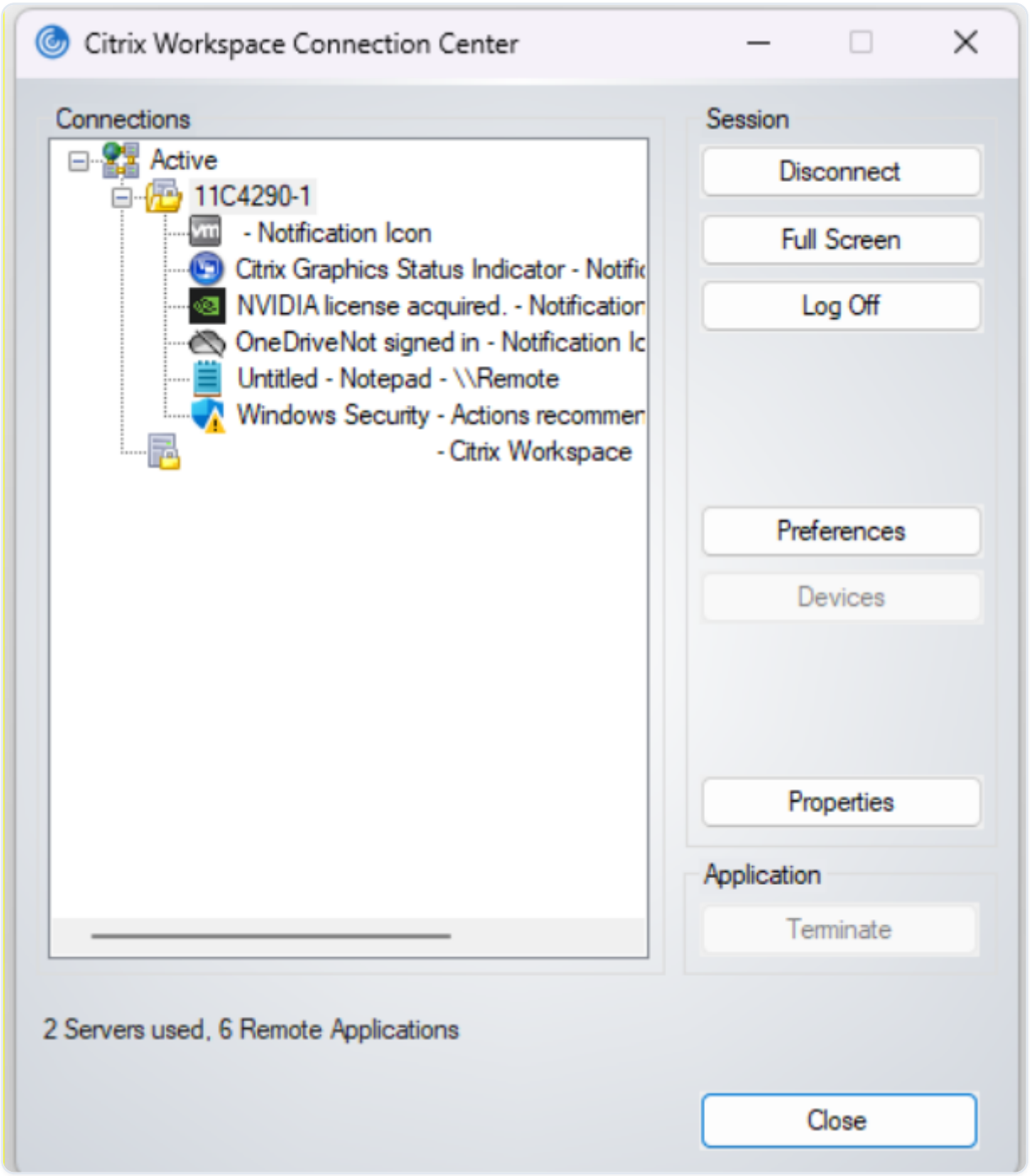
8. ここで読み取るべきキーが2つあります（ここでは変更しないでください）：**LogoffCheckBlockingProcess**と**LogoffCheckerBlockingVisibleProcess**。これらのキーは、サインアウトをブロックしているプログラムを表示します。最初のキーは、`C:\Windows\System32\cmd.exe`が開いていてまだ閉じられていないため、それを表示するはずです。

注:

LogoffCheckBlockingProcess と **LogoffCheckerBlockingVisibleProcess** は手動で編集しないでください。これらのレジストリ値を手動で編集すると、セッションが不安定になる可能性があります。

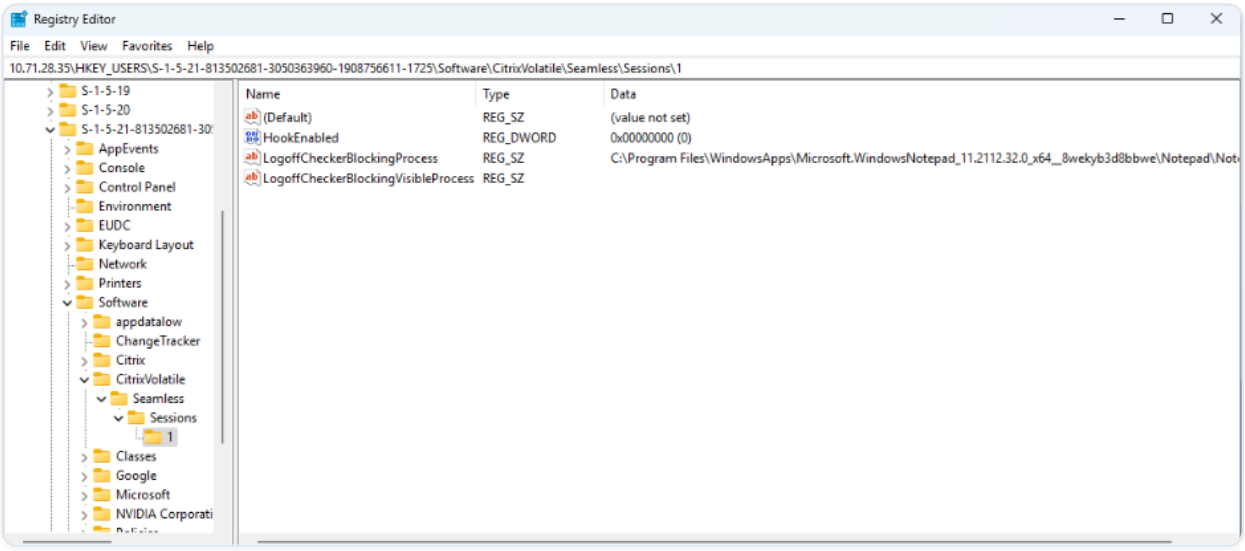


9. 右上隅の**X**をクリックして、**Seamless CMD**を終了します。
10. 接続センターでセッションが閉じるかどうかを確認します。閉じるまでに最大30秒かかる場合があります。セッションが閉じれば、正常なサインアウトを妨げるアプリケーションやプロセスはなかったことになります。



11. セッションが閉じなかった場合は、F5 キーで **regedit** の出力を更新します。
12. **LogoffCheckBlockingProcess**と**LogoffCheckerBlockingVisibleProcess**の内容を再度確認します。CMDは存在しないはずですが、別のプロセスがリストされているはずです。現在セッションのサインアウトをブロックしているプロセスがここに表示されているはずです。

    このケースでは、コマンドプロンプトが閉じられる前に、公開されたコマンドプロンプトから**Notepad.exe**が開かれており、このリモートのメモ帳プロセスが正常なサインアウトを妨げています。



13. この実行可能ファイルのパスと、それが表示されたキーをメモし、リモートツリーの下にある以下のレジストリキーに入力します。

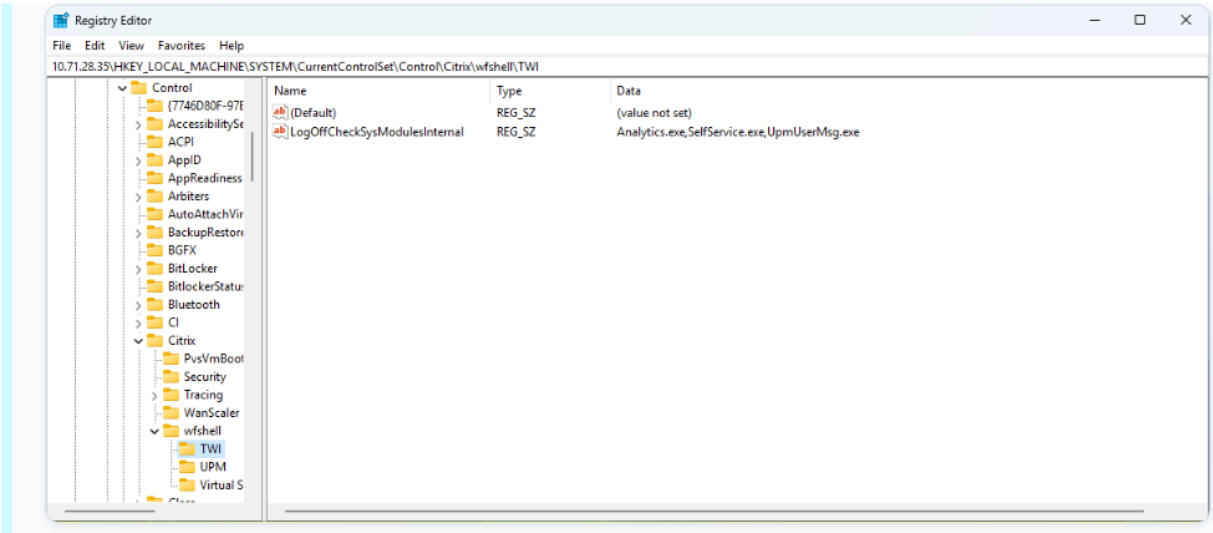
    - **LogoffCheckBlockingProcess** に表示される場合:

      `HKLM\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWILogoffCheckSysModulesInterna`

    - **LogoffCheckerBlockingVisibleProcess** に表示される場合:

      `HKLM\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWILogoffCheckVisibleSysModules`

> **注:**
>
> キーにすでに1つ以上のエントリがある場合は、末尾にコンマを追加し、そのコンマの後に新しいエントリを配置します。



14. クライアントの接続センターからセッションをサインアウトし、リモートアプリケーションを再度開きます。

15. リモートアプリケーションを閉じてから30秒以内にセッションが自動的にサインアウトされるまで、手順9〜16を繰り返します。

> **注:**
>
> トラブルシューティング後、必要に応じてリモートレジストリへのアクセスを許可するために、一時的なファイアウォールの変更を元に戻します。

公開アプリケーションを開くときにWindowsの免責事項メッセージを全画面表示で見るためにLogonUIを変更する方法

認証パススルーが発生しないシナリオ向けに、**LogonUI**ウィンドウのスケーリングが改善されました。**LogonUI**ウィンドウは、使用されているモニターの解像度とDPI設定に基づいてスケーリングされ、これにより、完全な**LogonUI**ウィンドウがクリッピングなしで表示されることが保証されます。

ウィンドウのサイズは、レジストリでピクセル単位で手動で設定することもできます。

1. **ファイル名を指定して実行**コマンドで`regedit`を使用して**レジストリエディター**を開きます。
2. `HKEY_LOCAL_MACHINE\Software\Citrix\CtxHook\AppInit_DLLS\Seamless Hook\`にアクセスします。
3. 2つの新しいDWORDキー、**LogonUIWidth** と **LogonUIHeight** を作成します。
4. キーの値を、**LogonUI** ウィンドウに必要な幅と高さ（ピクセル単位）に設定します。

   LogonUI ウィンドウのサイズを手動で設定すると、自動スケーリングは無効になります。

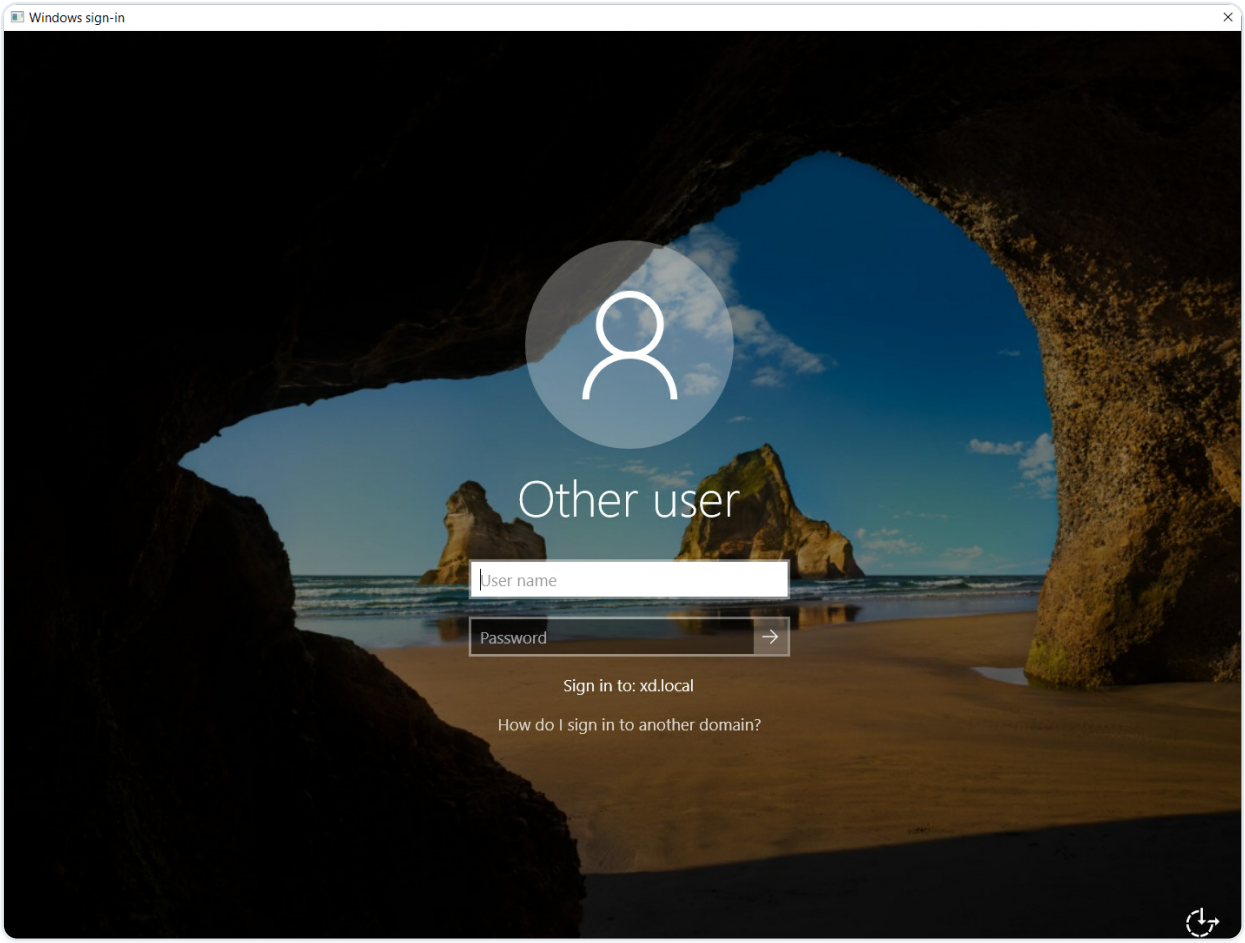
> **注:**
>
> これらのレジストリパスは、2407以降で変更されました。古いレジストリ値は無視され、非推奨です。

> デフォルトでは、**LogonUI** ウィンドウには閉じるボタン付きのタイトルバーが含まれており、必要に応じてエンドユーザーがセッションから切断できるようになっています。

タイトルバーを無効にする

次のレジストリキーを使用して、**LogonUI** ウィンドウのタイトルバーを無効にできます。

1. **ファイル名を指定して実行** コマンドで `regedit` を使用してレジストリエディターを開きます。
2. `HKEY_LOCAL_MACHINE\Software\Citrix\CtxHook\AppInit_DLLS\Seamless Hook\` にアクセスします。
3. 新しいDWORDキー **LogonUICaption** を作成し、キーの値を `0` に設定します。



アプリケーションフォルダーの管理

デフォルトでは、デリバリーグループに追加する新しいアプリケーションは、**Applications**という名前のフォルダーに配置されます。デリバリーグループの作成時、アプリケーションの追加時、または後で別のフォルダーを指定できます。

知っておくと便利な情報:

- Applicationsフォルダーの名前を変更したり削除したりすることはできませんが、その中に含まれるすべてのアプリケーションを、作成した他のフォルダーに移動することはできます。

- フォルダー名には1〜64文字を含めることができます。スペースも使用できます。
- フォルダーは最大5レベルまでネストできます。
- フォルダーにアプリケーションを含める必要はありません。空のフォルダーも許可されます。
- Web Studioでは、フォルダーを移動したり、作成時に別の場所を指定したりしない限り、フォルダーはアルファベット順に表示されます。
- 親フォルダーが異なる限り、同じ名前のフォルダーを複数持つことができます。同様に、異なるフォルダーにある限り、同じ名前のアプリケーションを複数持つことができます。
- フォルダー内のアプリケーションを表示するには`View Applications`権限が必要です。アプリケーションを含むフォルダーを削除、名前変更、または削除するには、そのフォルダー内のすべてのアプリケーションに対して`Edit Application Properties`権限が必要です。
- 以下のほとんどの手順では、Web Studioのアクションバーを使用してアクションを要求します。または、右クリックメニューを使用するか、項目をドラッグすることもできます。たとえば、意図しない場所にフォルダーを作成または移動した場合、ドラッグアンドドロップで正しい場所に移動できます。
- Web Studioのすべてのノード（**Machine Catalogs**、**Delivery Groups**、**Applications**、**Application Groups**など）は、バックエンドで同じフォルダーツリーを共有しています。フォルダーの名前変更や移動時に名前の競合を避けるため、異なるノード間で最上位フォルダーに一意の名前を使用してください。

  `New-BrokerAdminFolder` SDKコマンドレットを使用してフォルダーを作成し、それを**Applications**ノードの下に表示したい場合は、`Set-BrokerAdminFolderMetadata`コマンドレットを使用して`ContainsApplications`メタデータを追加する必要があります。

  例:

  ```
  Set-BrokerAdminFolderMetadata -AdminFolderId {adminFolderUid} -Name
  ContainsApplications -Value true
  ```

アプリケーションフォルダーを管理するには、左側のペインで**Applications**を選択します。ガイダンスとして、次の一覧を使用してください。

- **すべてのフォルダーを表示するには（ネストされたフォルダーを除く）：** フォルダーリストの上にある**Show all**をクリックします。
- **最上位レベルにフォルダーを作成するには（ネストしない）：** **Applications**フォルダーを選択します。新しいフォルダーを**Applications**以外の既存のフォルダーの下に配置するには、そ

のフォルダーを選択します。次に、アクションバーで**Create Folder**を選択します。名前を入力します。

- **フォルダーを移動するには：** フォルダーを選択し、アクションバーで**Move Folder**を選択します。フォルダーにネストされたフォルダーが含まれていない限り、一度に1つのフォルダーしか移動できません。（フォルダーを移動する最も簡単な方法は、ドラッグすることです。）
- **フォルダーの名前を変更するには：** フォルダーを選択し、アクションバーで**Rename Folder**を選択します。名前を入力します。
- **フォルダーを削除するには：** フォルダーを選択し、アクションバーで**Delete Folder**を選択します。アプリケーションや他のフォルダーを含むフォルダーを削除すると、それらのオブジェクトも削除されます。アプリケーションを削除すると、デリバリーグループからのアプリケーションの割り当てが削除されます。マシンからは削除されません。
- **アプリケーションをフォルダーに移動するには：** 1つまたは複数のアプリケーションを選択します。次に、アクションバーで**Move Application**を選択します。フォルダーを選択します。

デリバリーグループまたはアプリケーショングループを作成するときに、**Application**ページで追加するアプリケーションをフォルダーに配置することもできます。デフォルトでは、追加されたアプリケーションは**Applications**フォルダーに入ります。フォルダーを選択または作成するには、**Change**をクリックします。

公開デスクトップでのアプリケーションのローカル起動を制御する

ユーザーが公開デスクトップ内から公開アプリケーションを起動する際、そのデスクトップセッションでアプリケーションを起動するか、公開アプリケーションとして起動するかを制御できます。Citrix Workspaceアプリは、VDA上のWindowsレジストリでアプリケーションのインストールパスを検索し、存在する場合はアプリケーションのローカルインスタンスを起動します。それ以外の場合は、ホストされたアプリケーションのインスタンスが起動されます。VDAにインストールされていないアプリケーションを起動すると、ホストされたアプリケーションが起動されます。詳細については、「vPrefer起動」を参照してください。

PowerShell（Citrix Cloud展開環境ではRemote PowerShell SDK、オンプレミス展開環境ではPowerShell SDKを使用）で、このアクションを変更できます。

`New-Broker` Applicationまたは`Set-BrokerApplication` コマンドレットで、`LocalLaunchDisabled` オプションを使用します。例：

```
Set-BrokerApplication -LocalLaunchDisabled <Boolean>
```

デフォルトでは、このオプションの値はfalse（`-LocalLaunchDisabled $false`）です。公開デスクトップ内から公開アプリケーションを起動すると、そのデスクトップセッション内でアプリケーションが起動されます。

オプションの値をtrue（`-LocalLaunchDisabled $true`）に設定すると、公開アプリケーションが起動されます。これにより、公開デスクトップから（Windows用Citrix Workspaceアプリを使用して）公開アプリケーションへの個別の追加セッションが作成されます。

要件と制限：

- アプリケーションの`ApplicationType`値は`HostedOnDesktop`である必要があります。
- このオプションは、適切なPowerShell SDKを介してのみ利用可能です。現在、Web Studioのグラフィカルインターフェイスでは利用できません。
- このオプションには、最低限以下のものが必要です: StoreFront 3.14、Citrix Receiver for Windows 4.11、およびDelivery Controller 7.17。

アプリパッケージ

アプリケーションパッケージは、Citrix® が管理する事前構成されたアプリケーション展開です。これにより、アプリケーションを仮想化でき、ユーザーデバイスのオペレーティングシステムやインターフェイスから独立してアプリケーションが実行されることを意味します。

アプリケーションパッケージは、アプリケーション管理を簡素化し、ITのオーバーヘッドを削減し、アプリケーションがライフサイクル全体を通じて安全かつ機能的であることを保証します。

Citrix は、ユーザーにアプリケーションを配信するために以下のパッケージングテクノロジーをサポートしています。

- App-V アプリケーション
- MSIX および MSIX app attach アプリケーション
- FlexApp アプリケーション

この記事では、Citrix Virtual Apps and Desktops™ 環境でこれらのパッケージ化されたアプリケーションを展開および配信する方法を説明します。

> **注:**
>
> - Citrix Virtual Apps and Desktops 展開は、Web Studio (Webベース) と Citrix Studio (Windowsベース) の2つの管理コンソールを使用して管理できます。この記事ではWeb

Studioのみを扱います。Citrix Studioに関する情報については、Citrix Virtual Apps and Desktops 7 2212以前の同等の記事を参照してください。

- アプリケーションパッケージの展開と配信にWeb StudioとCitrix Studioを相互に利用することはお勧めしません。それぞれ異なるメカニズムを使用しており、App-Vサーバーの情報が一方では正しく表示されるが、もう一方では表示されないといった不一致が生じる可能性があります。また、Citrix StudioはApp-Vのみをサポートしていることにも注意してください。

App-V アプリケーション

Application Virtualization (App-V) はMicrosoftのテクノロジーであり、エンドユーザーのデバイスにインストールすることなく、アプリケーションをストリーミングしてアクセスできます。Citrix Virtual Apps and Desktops はApp-Vを使用してアプリケーションを配信でき、これにより、さまざまなクライアントマシン間でアプリケーションを管理するための集中化された効率的な方法が提供されます。

App-Vパッケージアプリケーションを配信する際に操作するコンポーネントと概念の詳細については、Microsoftのドキュメント「Application Virtualization (App-V) for Windows client overview」を参照してください。

重要な用語

- **管理サーバー**: App-V インフラストラクチャを管理するための一元化されたコンソールを提供し、App-V デスクトップクライアントとリモートデスクトップサービスクライアントの両方に仮想アプリケーションを配信します。App-V 管理サーバーは、管理者に必要なセキュリティ、測定、監視、およびデータ収集を認証、要求、提供します。このサーバーは、Active Directory とサポートツールを使用してユーザーとアプリケーションを管理します。
- **パブリッシングサーバー**: 特定のユーザー向けにアプリケーションをApp-Vクライアントに提供し、ストリーミング用の仮想アプリケーションパッケージをホストします。パッケージは管理サーバーから取得します。
- **動的構成ファイル**: App-Vパッケージは動的構成ファイルを使用してカスタマイズできます。これをパッケージに適用すると、その特性を変更できます。たとえば、追加のアプリケーションショートカットや動作を定義するために使用できます。詳細については、「動的構成ファイル」を参照してください。

動的構成ファイル

Citrix App-Vは、両方の種類の動的構成ファイルをサポートしています。ファイル設定は、アプリケーションの起動時に適用されます。

- **展開構成ファイル**は、すべてのユーザーに対してマシン全体の構成を提供します。これらのファイルは`<packageFileName>_DeploymentConfig.xml`という名前で、適用されるApp-Vパッケージと同じフォルダーにあることが想定されています。これらのファイルは、シングルおよびデュアル管理者管理でサポートされています。
- **ユーザー構成ファイル**は、パッケージに対するユーザーごとのカスタマイズをサポートするユーザー固有の構成を提供します。シングル管理者では、次の形式で名前が付けられ、適用されるApp-Vパッケージと同じフォルダーにあるユーザー構成ファイルがサポートされます: `<packageFileName>_[UserSID | Username | GroupSID |GroupName_]UserConfig.xml`.

  特定のパッケージに対して複数のユーザー構成ファイルが存在する場合、それらは次の優先順位で適用されます。

  a. ユーザーSID
  b. ユーザー名
  c. ADグループSID (最初に見つかったものが優先)
  d. ADグループ名 (最初に見つかったものが優先)
  e. デフォルト

  例:

  ```
  MyAppVPackage_S-1-5-21-000000001-0000000001-000000001-001_UserConfig.xml

  MyAppVPackage_joeblogs_UserConfig.xml

  MyAppVPackage_S-1-5-32-547_UserConfig.xml

  MyAppVPackage_Power Users_UserConfig.xml

  MyAppVPackage_UserConfig.xml
  ```

  注:

  ファイル名のユーザー固有の部分は、オプションで末尾に配置することもできます (例: `MyAppVPackage_UserConfig_joeblogs.xml`)。

> **重要:**
>
> パッケージ内のアプリケーションが起動しているユーザーセッションがある場合、動的展開構成に変更を適用することはできません。他のユーザー (ただし現在のユーザーではない) がパッケージ内のアプリケーションを起動している場合は、動的ユーザー構成ファイルに変更を適用できます。

動的構成ファイルの場所

シングル管理者管理では、Citrix App-Vコンポーネントは、App-Vパッケージと同じフォルダーにある動的構成ファイルのみを処理します。

パッケージ内のアプリケーションが起動されると、対応する動的構成ファイルへの変更が再適用されます。動的構成ファイルがパッケージとは異なる場所にある場合は、マッピングファイルを使用してパッケージを展開構成ファイルにマッピングします。

マッピングファイルを作成するには:

1. 新しいテキストファイルを開きます。
2. 各動的構成ファイルについて、`<PackageGuid> : path` の形式を使用してパッケージへのパスを指定する行を追加します。

   例:

   ```
   F1f4fd78ef044176aad9082073a0c780 : c:\widows\file\packagedeploy.xml
   ```

3. ファイルをパッケージと同じフォルダーに `ctxAppVDynamicConfigurations.cfg` として保存します。

App-Vパッケージと同じUNC共有上のディレクトリ階層全体が、パッケージ内のアプリケーションが起動されるたびに、このファイルを求めて再帰的に上位検索されます。

方法

App-Vパッケージを配信および管理するには、次の方法を使用できます:

- **デュアル管理者**: この方法では、Citrix Virtual Apps and DesktopsとApp-Vサーバーが連携してパッケージを配信および管理します。この方法では、Citrix Virtual Apps and DesktopsがApp-Vサーバーの状態のスナップショットビューを定期的に更新する必要があります。これには、ハードウェア、インフラストラクチャ、および管理のオーバーヘッドが発生します。Citrix

Virtual Apps and DesktopsとApp-Vサーバーは、特にユーザー権限に関して同期を維持する必要があります。

この方法は、密接に結合されたApp-VおよびCitrix展開で最適に機能します。この方法では、次のようになります。

- **App-V管理サーバー**は動的構成ファイルを処理します
- **App Packages Delivery Component** (VDAマシンにインストール): アプリケーションの起動に必要な適切な公開サーバーの登録を管理します。

これにより、適切なタイミングで公開サーバーがユーザーと同期されます。公開サーバーは、構成されている設定を使用して、アプリパッケージのライフサイクル（ログオン時の更新や接続グループなど）の他の側面を維持します。

- **シングル管理者**: アプリケーションパッケージはネットワーク共有に保存されます。Citrix Virtual Apps and Desktops は、パッケージを独立して配信および管理します。

  この方法では、展開にApp-Vサーバーとデータベースインフラストラクチャが不要になるため、オーバーヘッドが削減されます。

  この方法では、App-Vパッケージをネットワーク共有に保存し、その場所からメタデータを環境にアップロードします。その後、VDAマシンにインストールされているApp Packages Delivery Componentが、次のようにアプリケーションを管理および配信します。

  - アプリケーションが起動されたときに、展開構成ファイルとユーザー構成ファイルを処理します。
  - ホストマシン上のパッケージのライフサイクルのすべての側面を管理します。

注:

- 1つまたは両方の管理方法を同時に使用できます。つまり、アプリケーションをデリバリーグループに追加するときに、アプリケーションはApp-Vサーバーまたはネットワーク共有にあるApp-Vパッケージから取得できます。
- 両方の管理方法を同時に使用していて、App-Vパッケージが両方の場所に動的構成ファイルを持っている場合、App-Vサーバー内のファイル（デュアル管理）が使用されます。
- Web Studioのナビゲーションペインでを選択すると、パッケージ名とソースが表示されます。**パッケージの種類**列は、パッケージの配信に使用されるテクノロジーと、**アプリ**

ケーションライブラリで参照されている場所を示します。パッケージを選択すると、詳細ペインにパッケージ内のアプリケーションとショートカットが一覧表示されます。

MSIXおよびMSIXアプリ添付アプリケーション

MSIXはWindowsアプリパッケージ形式であり、すべてのWindowsアプリに最新のパッケージングエクスペリエンスを提供します。MSIXは、Win32、.NET、UWPアプリなど、さまざまなWindowsアプリケーションタイプに適しています。

MSIX app attachは、仮想ハードディスクに事前に展開されたMSIXパッケージを利用します。これは、パッケージコンテンツをストリーミングするのではなく、必要に応じてターゲットマシンにマウントできます。これにより、展開時間の短縮、ネットワークトラフィックの削減、ターゲットマシンでのIOPSの低減が可能です。ただし、app attachディスクの作成と維持には追加の作業が必要です。

Citrix Virtual Apps and Desktopsは、VDAマシンにインストールされている**App Packages Delivery Component**を介して、MSIXおよびMSIX app attachアプリケーションをユーザーに配信します。このコンポーネントは、ホストマシン上のパッケージのライフサイクルのあらゆる側面を管理します。

MSIXおよびMSIX app attachの詳細については、Microsoftのドキュメントを参照してください。それぞれ、MSIX documentationとApp Attach in Azure Virtual Desktopです。

注:

- 当社は、デスクトップVDAおよびサーバーVDAでネイティブMSIXパッケージをサポートしており、MSIX app attachは、デスクトップVDAでのみ、`.vhd`、`.vhdx`、および`.cim`ディスクイメージ形式でサポートしています。
- Microsoftは、Server 2019向けにAppAttachの実装を提供していません。AppAttachはServer 2022および2025に存在しますが、Microsoftはこれらのバージョンでのサポートを提供していません。したがって、当社もServer 2022および2025でのAppAttachをサポートしていません。
- Windows Server 2019でサイドローディングを有効にします。
- VDAがパッケージの署名に使用されている証明書を信頼していることを確認してください。

FlexApp アプリケーション

FlexAppは、Liquidwareが開発したアプリケーションレイヤリングソリューションです。これは、従来のアプリケーションインストールプロセスを通じて基盤となるベースイメージを変更することなく、任意のアプリケーションをWindowsセッションにアタッチします。

FlexApp One アプリケーションは、単一の共有可能なファイルにカプセル化されており、Windows セッションに追加のアプリケーションレイヤーを必要とせずに動作できます。ユーザーはコンテナファイルをクリックすることでアプリケーションを起動でき、1つまたは複数のアプリケーションを Windows ワークスペースに迅速に統合できます。

Citrixは、VDAマシンにインストールされているApp Packages Delivery ComponentとFlexApp配信エージェントを介して、FlexAppアプリケーションをユーザーに配信します。これら2つのコンポーネントは、ホストマシン上のパッケージのライフサイクルのあらゆる側面を管理します。

アプリケーションパッケージの展開と配信

前提条件

App-V、MSIX、MSIX app attach、およびFlexAppパッケージの配信をサポートするには、まずVDAマシンに**App Packages Delivery Component**をインストールする必要があります。詳細については、Install the App Packages Delivery Component on VDA machinesを参照してください。

VDAマシンへのAPP PACKAGES DELIVERY COMPONENTのインストール

App Packages Delivery Componentは、App-V、MSIX、MSIX app attach、およびFlexApp形式のアプリケーションパッケージの公開プロセスを管理します。このコンポーネントは、VDAをインストールする際にはデフォルトでインストールされません。VDAのインストール中またはインストール後にコンポーネントをインストールできます。

VDAのインストール中にコンポーネントをインストールするには、次のいずれかの方法を使用します。

- インストールウィザードで、**追加コンポーネント**ページに移動し、**App Packages Delivery Component**チェックボックスを選択します。
- コマンドラインインターフェイスで、`/includeadditional "Citrix Personalization for App-V – VDA"`オプションを使用します。

VDAのインストール後にコンポーネントをインストールするには、次の手順に従います。

1. VDAマシンで、**コントロールパネル > プログラム > プログラムと機能**に移動し、**Citrix Virtual Delivery Agent**を右クリックして、**変更**を選択します。

2. 表示されるウィザードで、**追加コンポーネント**ページに進み、**App Packages Delivery Component**チェックボックスを有効にします。

注:

- Microsoft App-V Desktop Clientは、ユーザーデバイス上でApp-Vパッケージから仮想アプリケーションを実行するコンポーネントです。Windows 10 (1607以降) およびWindows Server 2019以降には、このApp-Vクライアントソフトウェアがすでに含まれています。VDAマシンでのみ有効にする必要があります。詳細については、このMicrosoftドキュメント記事を参照してください: App-Vインボックスクライアントを有効にする。
- FlexAppアプリケーションの場合、App Packages Delivery ComponentとともにVDAにFlexApp One Agentをインストールします。

FLEXAPP ONE AGENT をインストールする

1. VDA で管理者コマンドプロンプトを起動します。
2. 任意の FlexApp One Package のネットワークパスを見つけます。
3. 次のコマンドを入力します。

```
\\path\to\any\FlexAppOnePackage.exe --install
```

4. 表示されるプロンプトはすべて受け入れます。

パッケージ化されたアプリケーションを配信する

前提条件のインストールが完了したら、ユーザーにパッケージアプリケーションを配信するために、次の手順を実行します。

1. アプリケーションパッケージをネットワーク共有に保存する。
2. アプリケーションパッケージを環境にアップロードする。
3. アプリケーションをデリバリーグループに追加する。
4. 相互依存するApp-Vパッケージの自動配信を有効にするには、分離グループを作成します。

アプリケーションパッケージをネットワーク共有に保存する

インフラストラクチャをセットアップしたら、アプリケーションパッケージを生成し、UNCまたはSMBネットワーク共有、あるいはAzureファイル共有などのネットワークロケーションに保存します。

詳細な手順は次のとおりです。

1. アプリケーションパッケージを生成します。詳細については、Microsoftのドキュメント「App-V仮想化アプリケーションの作成と管理」を参照してください。
2. アプリケーションパッケージをネットワークロケーションに保存します。
   - **App-V Single Admin**の場合：パッケージと対応する動的構成ファイル（App-V）をUNCまたはSMBネットワーク共有、あるいはAzureファイル共有に保存します。
   - **App-V Dual Admin**の場合：UNCパスからApp-V管理サーバーにパッケージを公開します。（HTTP URLからの公開はサポートされていません。）
   - **MSIXまたはMSIX app attach**の場合：パッケージをUNCまたはSMBネットワーク共有、あるいはAzureファイル共有に保存します。
   - **FlexApp** の場合: パッケージをUNCまたはSMBネットワーク共有、あるいはAzureファイル共有に保存します。
3. VDAがパッケージストレージパスに対する読み取り権限を持っていることを確認します。
   - ADドメイン内のUNCまたはSMBネットワーク共有にパッケージを保存する場合、VDAマシンにストレージパスへの読み取り権限を付与します。これを行うには、マシンのADアカウントに共有への読み取り権限を明示的に付与するか、その権限を持つADグループにアカウントを含めます。
   - Azureファイル共有にパッケージを保存する場合、まずユーザーアカウントにAzure内のストレージパスへの読み取り権限を付与します。次に、VDAマシンで実行されている `ctxAppVService` がそのユーザーアカウントを使用してパッケージストレージパスにアクセスするように構成します。詳細な手順については、ユーザーログオンアカウントの変更を参照してください。

ユーザーログオンアカウントの変更

次の2つのシナリオでユーザーログオンアカウントを変更します。

- リンクされたADアカウントを使用してAzureファイル共有上のパッケージにアクセスする場合:
  - 接続エンティティはユーザーアカウントである必要があり、マシンアカウントであってはなりません。Azure ADはファイル共有上のマシンアカウントに読み取り権限を付与しないためです。
- MSIXおよびMSIX AppAttachパッケージにサービスが含まれている場合:
  - パッケージは、非管理者ユーザーに公開される前に、ローカルマシンで管理者権限を持つユーザーアカウントを使用して公開される必要があります。これは、パッケージ化された

サービスをインストールするために必要であり、パッケージはマシンではなくユーザーにのみ公開できるため、デフォルトのLocalServiceアカウントは不適切です。

VDAは`ctxAppVService`を呼び出してパッケージストレージパスにアクセスし、管理者権限を必要とする操作を実行します。デフォルトでは、`ctxAppVService`はマシンのIDを使用してADに認証するマシンのLocalServiceアカウントのコンテキストで実行されるため、上記のシナリオには適していません。

いずれの場合も、サービスは、ローカルで管理者権限を持ち、パッケージのストレージ場所（SMB共有またはAzureファイル共有）への読み取りアクセス権が付与されているADユーザーアカウントを使用するように再構成する必要があります。手順は次のとおりです。

1. **サービス**を開始し、**ctxAppVService**を右クリックして、**プロパティ**を選択します。
2. **ログオン**タブで、**このアカウント**を選択します。
    a. ローカル管理者権限とパッケージストレージパスへの読み取り権限を持つユーザーアカウントを入力します。
    b. ユーザーのパスワードを2回入力します。
3. **OK**をクリックします。

アプリケーションパッケージを環境にアップロードする

必要に応じてアプリケーションパッケージをネットワークの場所に保存した後、配信のために環境にアップロードします。必要に応じて、以下のいずれかの方法を使用します。

- 一括アップロード
- 個別にアップロード

準備

Citrix Virtual Apps and Desktops は、パッケージ検出のためのネットワークロケーションへの接続を設定するために VDA マシンを使用します。したがって、事前にデリバリーグループを作成し、グループ内の少なくとも1つの VDA が次の要件を満たしていることを確認してください。

- VDAバージョン:
    - App-Vパッケージを検出する場合: 2203以降
    - MSIXおよびMSIXアプリ添付パッケージを検出する場合: 2209以降
    - FlexAppパッケージを検出する場合: 2311以降およびFlexApp Agentソフトウェア
- アプリケーションパッケージ配信コンポーネント: インストール済み

- パッケージの場所に対する権限: 読み取り（詳細については、ネットワーク共有にアプリケーションパッケージを保存するを参照してください。）
- 電源: オン
- 状態: 登録済み

アプリケーションパッケージを一括でアップロードする
ネットワーク上の場所にあるパッケージをお使いの環境にアップロードします。アップロードする前に、以下の項目を準備してください:

- 準備の要件を満たすデリバリーグループ
- ネットワーク上の場所のパス

パッケージを一括でアップロードするには、次の手順に従います:

1. 左側のペインで、**アプリパッケージ**を選択します。
2. **ソース**タブで、**ソースの追加**ボタンをクリックします。**ソースの追加**ページが表示されます。
3. **名前**フィールドに、パッケージソースのわかりやすい名前を入力します。
4. **デリバリーグループ**フィールドで、**デリバリーグループの選択**をクリックします。次に、準備に記載されている要件を満たすデリバリーグループを選択し、**OK**をクリックします。
5. **場所の種類**フィールドで、パッケージの保存場所に基づいて**Microsoft App-Vサーバー**または**ネットワーク共有**を選択し、その後、対応する設定を完了します:
    - **Microsoft App-Vサーバー**を選択した場合、次の情報を入力します:
        - 管理サーバーのURL。例: `http://appv-server.example.com`
        - 管理サーバー管理者のログオン資格情報。
        - 公開サーバーのURLとポート番号。例: `http://appv-server.example.com:3330`
    - **ネットワーク共有**を選択した場合は、次の情報を指定します。
        - ネットワーク共有のUNCパスを入力します。例: `\\Package-Server\apps\`
        - アップロードするパッケージの種類を選択します。オプションには、App-V、MSIX、MSIX app attach、およびFlexAppが含まれます。
        - パッケージのサブフォルダーを検索するかどうかを指定します。

        > **注:**

> `cim`イメージを含むフォルダー構造でMSIX app attachパッケージを検索する場合は、**サブフォルダーを検索**を選択していることを確認してください。そうしないと、ディスクが正しく検出されません。

6. 「**ソースの追加**」をクリックします。

「**ソースの追加**」ページが閉じ、新しく追加されたソースがソースリストに表示されます。Citrix Virtual Apps and Desktopsは、デリバリーグループ内のVDAを使用してパッケージを環境にアップロードします。アップロードが完了すると、ステータスフィールドに「*インポート成功*」と表示されます。対応するパッケージは「**パッケージ**」タブに表示されます。

> **注:**
>
> ソースの場所でパッケージの更新を確認し、それらを環境にインポートするには、ソースリストで場所を選択し、「**パッケージの更新を確認**」をクリックします。

アプリケーションパッケージを1つずつアップロードする
ネットワーク共有から環境にアプリケーションパッケージをアップロードします。アップロードする前に、次の項目が準備されていることを確認してください。

- 準備に記載されている要件を満たすデリバリーグループ
- ネットワークの場所のパス。

パッケージを環境にアップロードするには、次の手順に従います。

1. 左ペインで、**App Packages** を選択します。
2. **Packages** タブで、**Add Package** ボタンをクリックします。**Add Package** ページが表示されます。
3. **Delivery group** フィールドで、**Select a delivery group** をクリックします。次に、Preparations に記載されている要件を満たすデリバリーグループを選択し、**OK** をクリックします。
4. **Package full path** フィールドに、必要に応じてパスを入力します。
   - 複数のパッケージを一度にアップロードするには、セミコロン (`;`) で区切って完全なパスを入力します。例: `\\Package-Server\apps\office365.appv;\\Package-Server\apps\skype.msix;\\Package-Server\apps\slack.vhd`

- ネットワーク共有にあるすべてのパッケージをアップロードするには、ストレージパスを入力します。例: \\package-Server\apps\

5. **Add Package** をクリックします。

   アプリケーションパッケージが「**パッケージ**」タブに表示されます。

アプリケーションをデリバリーグループに追加する

アプリケーションパッケージが環境に完全にアップロードされたら、必要に応じて、そのアプリケーションを1つ以上のデリバリーグループに追加します。その結果、それらのデリバリーグループに関連付けられたユーザーはアプリケーションにアクセスできるようになります。

> **注:**
>
> - パッケージ化されたアプリケーションは、デリバリーグループを介してシングルセッションVDAおよびマルチセッションVDAに配信できます。
> - デフォルトでは、エンドユーザーは、*シングルセッション* (または *デスクトップ* と呼ばれる) VDAに関連付けられたデリバリーグループに割り当てられたすべてのパッケージ化されたアプリケーションにアクセスできます。*デスクトップ* VDA上のパッケージ化されたアプリケーションの可視性を特定のユーザーまたはグループに制限するには、**Applications** ノードに移動し、アプリケーションを選択してから、**Edit Application Properties > Limit Visibility** を選択して変更を加えます。アプリケーションの可視性を制限する を参照してください。

パッケージ内の1つ以上のアプリケーションを複数のデリバリーグループに追加するには、次の手順に従います。

1. 左ペインで、**App Packages** を選択します。
2. 「**パッケージ**」タブで、必要に応じてパッケージを選択します。
3. アクションバーで、**デリバリーグループの追加**をクリックします。「**アプリケーションをデリバリーグループに割り当てる**」ページが表示されます。
4. 必要に応じてパッケージ内の1つ以上のアプリケーションを選択し、**次へ**をクリックします。
5. デリバリーグループのリストで、アプリケーションを割り当てるグループを選択し、**次へ**をクリックします。

> **注:**

- MSIXまたはMSIXアプリ添付パッケージを選択した場合、VDAバージョンが2106以降のデリバリーグループのみがリストに表示されます。
- *FlexApp*パッケージを選択した場合、VDAバージョンが2402以降のデリバリーグループのみがリストに表示されます。

6. **完了**をクリックします。

さまざまなパッケージのアプリケーションを複数のデリバリーグループに追加するには、次の手順に従います。

1. 左ペインで、**アプリパッケージ**を選択します。
2. 「**アプリケーション**」タブで、**アプリケーションの追加**を選択します。
3. 「**グループ**」ページで、必要に応じて1つ以上のデリバリーグループを選択します。
4. 「**アプリケーション**」ページで、次のように1つ以上のアプリケーションパッケージを選択します。
   a. **追加**をクリックし、**アプリケーションパッケージ**を選択します。
   b. 必要なパッケージソースの種類（例：App-V Single Admin）を選択します。この種類のすべてのパッケージが表示されます。
   c. 必要に応じて1つ以上のパッケージを選択します。
   d. **OK** をクリックし、次に **次へ** をクリックします。
   e. 異なるパッケージタイプのアプリケーションを追加するには、手順 a から d を繰り返します。
5. **完了** をクリックします。

次の場合に、パッケージ化されたアプリケーションをデリバリーグループに追加することもできます。

- デリバリーグループを作成する場合。詳細については、「デリバリーグループの作成」を参照してください。
- 既存のデリバリーグループまたはアプリケーショングループを編集する場合。詳細については、「アプリケーションの追加」を参照してください。

(オプション) APP-Vパッケージの分離グループを作成する

相互依存するApp-Vパッケージを自動的に配信できるように、分離グループを作成できます。

注:

分離グループは、App-Vシングル管理者方式でサポートされています。App-Vデュアル管理者方式を使用している場合は、Microsoft App-Vインフラストラクチャで *接続グループ* を作成することで、同じ目標を達成できます。詳細については、このMicrosoftドキュメント記事「接続グループファイルについて」を参照してください。

分離グループについて

分離グループとは、仮想環境を作成するために同じWindows Sandboxで実行する必要がある、相互依存するアプリケーションパッケージの集合です。Citrix App-V分離グループは、App-V接続グループに似ていますが、同一ではありません。分離グループには、次の2種類のパッケージが含まれます。

- **明示的なアプリケーションパッケージ**：特定のライセンス要件を持つアプリケーション。これらのアプリケーションをデリバリーグループに追加することで、特定のユーザー範囲に制限できます。
- **自動アプリケーションパッケージ**：デリバリーグループに追加されているかどうかに関係なく、常にすべてのユーザーが利用できるアプリケーション。

たとえば、アプリケーション`app-a`を実行するにはJRE 1.7が必要です。app-a（*Explicit*とマーク）とJRE 1.7（*Automatic*とマーク）を含む分離グループを作成できます。次に、`app-a`のApp-Vパッケージを1つ以上のデリバリーグループに追加します。ユーザーがapp-aを起動すると、JRE 1.7が自動的に展開されます。

ユーザーが分離グループ内で*Explicit*とマークされたApp-Vアプリケーションを起動すると、Citrix Virtual Apps and Desktopsはデリバリーグループ内のアプリケーションに対するユーザーのアクセス許可を確認します。ユーザーがアプリケーションにアクセスする権限を持っている場合、同じ分離グループ内の*Automatic*アプリケーションパッケージはユーザーが利用できるようになります。

*Automatic*パッケージをどのデリバリーグループにも追加する必要はありません。分離グループ内に別の*Explicit*アプリケーションパッケージがある場合、そのパッケージは、同じデリバリーグループ内にある場合にのみユーザーが利用できるようになります。

App-V分離グループを作成する

分離グループを作成し、相互依存するアプリケーションパッケージを追加します。詳細な手順は次のとおりです。

1. **Isolation Groups**タブで、**Add Isolation Group**をクリックします。

2. 分離グループの名前と説明を入力します。環境内のすべてのApp-V Single Adminパッケージが**Available Packages**リストに表示されます。
3. **Available Packages**リストから必要に応じてアプリケーションを選択し、右矢印をクリックします。選択したアプリケーションは**Packages in Isolation Group**リストに表示されます。
4. **Deployment**フィールドで、アプリケーションに対して**Explicit**または**Automatic**を選択します。
5. 手順2〜3を繰り返して、さらにパッケージを追加します。
6. リスト内のパッケージの順序を調整するには、上矢印または下矢印をクリックします。
7. **Save**をクリックします。

> **注:**
>
> 分離グループの構成により、VDA上にApp-V接続グループが作成されます。展開シナリオは複雑になる可能性があり、App-Vクライアントは一度に1つのアクティブな接続グループにのみ存在するパッケージをサポートします。同じパッケージを、同じデリバリーグループに追加された2つの異なる分離グループに追加することは避けることをお勧めします。

ベストプラクティス

- App-Vパッケージを展開するには、PowerShellコマンド`Enable-AppV`を使用してVDAでApp-Vサブシステムを有効にします。
- MSIX（およびAppAttach）パッケージを展開するには、VDAがパッケージの署名に使用されている証明書を信頼する必要があります。
- Windows Server 2019では、MSIXパッケージを展開するためにサイドローディングを有効にします。Windows 10、11、Windows Server 2022、および2025ではサイドローディングは不要です。
- App AttachはWindows Server 2019では全く実装されておらず、Windows Server 2022または2025ではMicrosoft（およびCitrix）によって現在サポートされていません。

詳細設定

パッケージ化されたアプリケーションの公開を自動化する

PowerShellコマンドを使用して、パッケージ化されたアプリケーションの公開を自動化できます。

Delivery Controller™上で、以下のPowerShellコマンドを実行します:

1. パッケージ検出モジュールに存在するコマンドをロードするには:

```
Import-Module "D:
\Support\Tools\Scripts\Citrix.Cloud.AppLibrary.Admin.v1.psm1"
```

> **注:**
>
> パッケージ検出モジュールのバージョンは、Citrix Virtual Apps and Desktops ISOのステップ1で言及されているパスにあります。

2. パッケージ検出モジュールは、公開するパッケージタイプもサポートするCitrix Virtual Apps and DesktopsバージョンのISOから取得する必要があります。つまり、FlexAppOneアプリケーションには2311以降が必要です。利用可能な最新バージョンを使用することをお勧めします。
3. 関連するデリバリーグループIDとパッケージ化されたアプリケーションIDを取得するには:

```
Get-BrokerDesktopGroup | Format-Table Uid, Name

Get-AppLibAppVApplication | Format-Table Uid, Name
```

4. パッケージを公開し、適切なBrokerMachineConfigurationを作成するには:

```
Publish-PackagedApplication -AppLibararyApplicationUid
<AppLibararyApplication.Uid > -DesktopGroupUid <DesktopGroup.Uid>
```

5. Broker構成を同期するには（これらの構成は後でVDA上のBrokerエージェントに送信されます）：

```
Update-DesktopGroupMachineConfigurations -DesktopGroupUid
<DesktopGroup.Uid>
```

> **注：**
>
> PowerShellコマンドラインを介してデリバリーグループからパッケージ化されたアプリケーションを公開または削除した後には、PowerShellコマンド `Update-`

> `DesktopGroupMachineConfigurations` を必ず実行してください。そうしないと、公開されたアプリケーションに関する情報がVDAに正しく送信されず、起動に失敗します。

アプリケーションの可視性を制限する

Citrix Virtual Apps and Desktops環境では、パッケージからのアプリケーションがデスクトップに公開されると、システムはそれらのアプリケーションに対するActive Directory (AD) のユーザーおよびグループの可視性設定を尊重します。ただし、ユーザーがパッケージ内の1つのアプリケーションに対してのみ可視性を持っている場合でも、個々のパッケージコンポーネントはVDA上で細分化できないため、パッケージ全体を仮想デスクトップ（またはシームレスアプリ）セッションに展開する必要があります。さらに、VDAバージョン2503より前では、最初の公開後にアプリケーションの可視性を低下させる変更を行っても、その後のデスクトップ起動時に以前に公開されたパッケージがクリーンアップされることはありません。また、デスクトップとワークスペースの可視性など、他の可視性レイヤーは、これらのAD可視性割り当ての上に動作します。

パッケージ化されたアプリケーションがWorkspaceに表示されるべきか、ユーザーのVDIデスクトップセッションに展開されるべきかを制御できます。パッケージ化されたアプリケーションが公開されたら、PowerShellコマンド `Set-BrokerApplication -Name "MyApp" -PackagedApplicationVisibility "Workspace|Desktop|WorkspaceAndDesktop"` を使用して、`BrokerApplictaion` の `PackagedApplicationVisibility` プロパティを更新できます。

`PackagedApplicationVisibility` のデフォルト値は `WorkspaceAndDesktop` です。

値 `Workspace`: アプリはWorkspaceAppにのみ表示され、シームレスなAppLaunchに利用できますが、ユーザーが開始するデスクトップセッションには自動的に公開されません。

値 `Desktop`: アプリのアイコンをWorkspaceAppから非表示にし、シームレスなAppLaunchでは利用できなくなりますが、ユーザーがADグループ設定を通じてアクセス権を持っている場合は、引き続きユーザーのデスクトップセッションに展開できます。

> **注：**
>
> シングルセッション静的デスクトップに公開されたパッケージ化されたアプリケーションは、この設定で構成された値に関係なく、Workspace Appでは利用できません。

ユニバーサル Windows プラットフォームアプリ

ユニバーサル Windows プラットフォーム (UWP) アプリについては、以下の Microsoft ドキュメントを参照してください。

- ユニバーサル Windows プラットフォーム (UWP) アプリとは
- Windows パッケージマネージャー

要件と制限

Citrix Virtual Apps and Desktops™ は、以下の Windows マシン上の VDA で UWP アプリを使用することをサポートしています。

- Windows 10 以降のバージョン
- Windows Server 2016 以降のバージョン

VDA はバージョン 7.11 以降である必要があります。

UWP アプリを使用する場合、以下の Citrix Virtual Apps and Desktops の機能はサポートされていないか、制限されています。

- ファイルタイプの関連付けはサポートされていません。
- ローカルアプリアクセスはサポートされていません。
- 動的プレビュー：セッションで実行中のアプリが重なっている場合、プレビューにはデフォルトのアイコンが表示されます。動的プレビューに使用される Win32 API は、UWP アプリではサポートされていません。
- アクションセンターのリモート処理：UWP アプリは、セッション内のメッセージを表示するためにアクションセンターを使用できます。これらのメッセージは現在、ユーザーに表示するためにエンドポイントにリダイレクトされません。

同じサーバーから UWP アプリと非 UWP アプリを起動することはサポートされていません。代わりに、UWP アプリと非 UWP アプリを別々のデリバリーグループまたはアプリケーショングループに配置してください。

マシンにインストールされているすべてのUWPアプリが列挙されるため、Citrix®はWindowsストアへのユーザーアクセスを無効にすることを推奨します。これにより、あるユーザーがインストールしたUWPアプリに別のユーザーがアクセスできなくなります。

サイドローディング中、UWPアプリはマシンにインストールされ、他のユーザーが使用できるようになります。別のユーザーがアプリを起動すると、そのアプリがインストールされ、OSはその

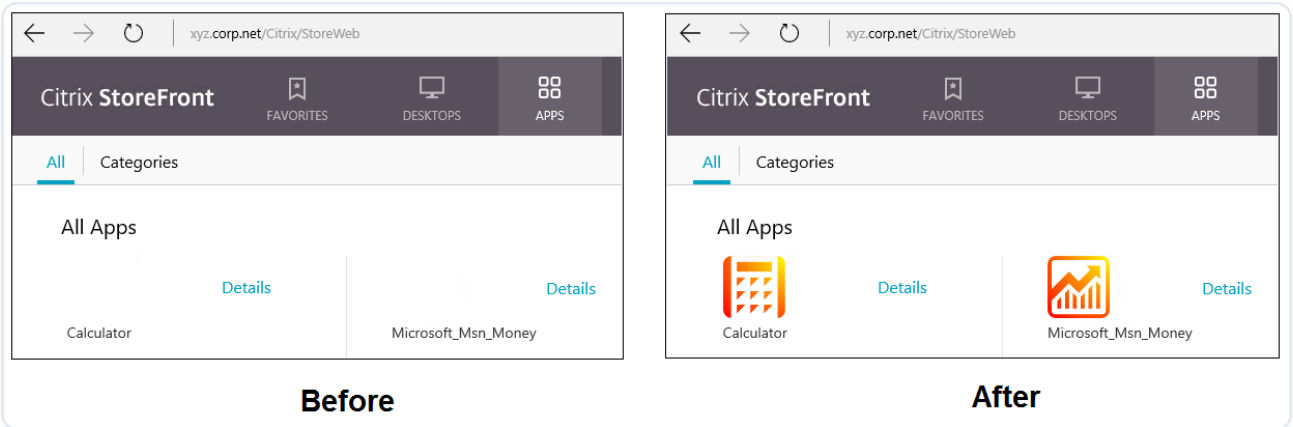
ユーザーによって「インストール済み」であることを示すようにAppXデータベースを更新します。

固定ウィンドウまたはシームレスウィンドウで起動された公開済みUWPアプリから開始された正常なログオフにより、VDAセッションが閉じられず、ユーザーが強制的にログオフされる場合があります。この場合、VDAセッションに残っているいくつかのプロセスが、セッションが適切に閉じられるのを妨げます。これを解決するには、VDAセッションが閉じられるのを妨げているプロセスを特定し、CTX891671のガイダンスに従って、「LogoffCheckSysModules」レジストリキー値に追加します。

UWPアプリのアプリケーション表示名と説明が正しくない場合があります。アプリケーションをデリバリーグループに追加する際に、これらのプロパティを編集して修正してください。

その他の問題については、既知の問題を確認してください。

現在、いくつかのUWPアプリは透明度が有効な白いアイコンを持っており、StoreFront表示の白い背景に対してアイコンが見えなくなることがあります。この問題を回避するには、背景を変更できます。たとえば、StoreFrontマシンでファイル`C:\inetpub\wwwroot\Citrix\StoreWeb\custom\style.css`を編集します。ファイルの最後に`.storeapp-icon {background-image: radial-gradient( circle at top right, yellow, red ); }`を追加します。次の図は、この例の変更前と変更後を示しています。



Windows Server 2016以降のバージョンでは、UWPアプリの起動時にサーバーマネージャーも起動する場合があります。これを防ぐには、`HKLM\Software\Microsoft\ServerManager\DoNotOpenServerManagerAtLogon`レジストリキーを使用して、ログオン時のサーバーマネージャーの自動起動を無効にできます。詳細については、`<https://blogs.technet.microsoft.com/rmilne/2014/05/30/how-to-hide-server-manager-at-logon/>`を参照してください。

UWPアプリのインストールと公開

UWPアプリのサポートはデフォルトで有効になっています。

VDA（またはマスターイメージ）に1つ以上のUWPアプリをインストールするには、次のいずれかの方法を使用します。

- Deployment Image Servicing and Management (DISM) などのツールを使用して、Windows Store for Businessからオフラインインストールを完了し、デスクトップイメージにアプリを展開します。詳細については、Windows Package Managerを参照してください。
- アプリをサイドロードします。詳細については、Windowsクライアントデバイスでの基幹業務 (LOB) アプリのサイドロードを参照してください。
- 各対象ユーザー向けに、Windows Store for Businessから直接UWPアプリをインストールします。

Citrix Virtual AppsまたはCitrix Virtual Desktops™で1つ以上のUWPアプリを追加（公開）するには：

1. マシンにUWPアプリがインストールされたら、UWPアプリをデリバリーグループまたはアプリケーショングループに追加します。これは、グループの作成時または後で行うことができます。**アプリケーション**ページで、**追加**メニューから**スタートメニューから**を選択します。
2. アプリケーションリストが表示されたら、公開するUWPアプリを選択します。
3. ウィザードを続行するか、編集ダイアログを閉じます。

VDAでユニバーサルアプリの使用を無効にするには、レジストリ設定 **EnableUWASeamlessSupport**を `HKLM\Software\Citrix\VirtualDesktopAgent\FeatureToggle` に追加し、**0**に設定します。

UWPアプリのアンインストール

`Remove-AppXPackage` のようなコマンドでUWPアプリをアンインストールすると、その項目は管理者に対してのみアンインストールされます。アプリを起動して使用した可能性のあるユーザーのマシンからアプリを削除するには、各マシンで削除コマンドを実行します。1つのコマンドですべてのユーザーのマシンからAppXパッケージをアンインストールすることはできません。

構成のバックアップまたは移行

この機能は、構成のバックアップを取るのに役立ちます。バックアップは、復元機能と合わせて、オンプレミスからクラウドへ、またはあるクラウドサイトから別のクラウドサイトへのサイト情報の移行を容易にします。また、緊急時にはサイトの即時復旧も容易にします。

バックアップを取るには、以下の方法を使用できます。

1. バックアップ + 復元

   a. Web Studioと統合されています。

2. 自動構成ツール (ACT)

   a. PowerShellベースのツール。使用するにはツールをインストールします。「Download Automated Configuration」を参照してください。

バックアップは以下の目的で使用できます。

1. 復元
2. 移行

Citrix®は、記載されているシナリオに次のツールを推奨します。

バックアップ

環境	ユースケース	推奨ツール	特別な考慮事項	リンク
DaaS とオンプレミス	オンデマンドおよびスケジュールされたバックアップ	バックアップ + 復元	Citrix がバックアップを保持し、必要に応じてユーザーがダウンロードできます	Web Studio を使用したバックアップと復元
DaaS とオンプレミス	オンデマンドおよびスケジュールされたバックアップ	ACT	ユーザーがバックアップを保持します	Automated Configuration Tool を使用したバックアップと復元

移行

環境	ユースケース	推奨ツール	特別な考慮事項	リンク
オンプレミスからクラウドへ	1つのオンプレミスサイトをDaaSに移行する	ACT		オンプレミスからクラウドへの移行
	複数のオンプレミスサイトを1	ACT	サイトのマージ	複数のオンプレミスサイトを単一のクラウドサ

環境	ユースケース	推奨ツール	特別な考慮事項	リンク
	つのDaaSサイトに統合する			イトにマージする
オンプレミスからオンプレミスへ	1つのオンプレミスサイトを別のオンプレミスサイトに移行する	ACT		POC ガイド: 自動構成ツール - オンプレミスからオンプレミスへの移行
	複数のオンプレミスサイトを別のオンプレミスサイトに統合する	ACT	サイト統合	POC ガイド: 自動構成ツール - オンプレミスからオンプレミスへの移行
				複数のオンプレミスサイトを単一のクラウドサイトにマージする
クラウドからクラウドへ	1つのDaaSサイトを別のDaaSサイトに移行する	ACT		クラウドからクラウドへの移行
複数のDaaSサイトを1つのDaaSサイトに統合する	サイト統合	ACT		クラウドからクラウドへの移行 (/ja-jp/citrix-virtual-apps-desktops/2503/manage-deployment/migrate-cloud-to-cloud.html)
				複数のオンプレミスサイトを単一のクラウドサイトに移行する (/ja-jp/citrix-virtual-apps-

環境	ユースケース	推奨ツール	特別な考慮事項	リンク
				desktops/2503/manage-deployment/multi-site-merge)

構成のバックアップと復元

この機能により、管理者はクラウド構成のバックアップを作成できます。これにより、Citrix®構成のコピーが常に利用可能になり、すぐに使用できるようになります。バックアップと復元機能は、オンプレミスからクラウドへ、またはあるクラウドサイトから別のクラウドサイトへのサイト情報の移行を容易にします。誤って変更が発生した場合は、バックアップを選択して復元を選択するだけで、数回のクリックで再び稼働できます。特定のコンポーネントをバックアップおよび復元することもできます。

この機能では、次のものをバックアップおよび復元できます。

- タグ
- 管理者ロール
- 管理スコープ
- ホスト接続

> **注：**
>
> ホスト接続をバックアップできるようになりました。シークレットは毎回入力する必要があります。インポートまたは更新されるホスト接続に対してのみシークレットを要求するために、インポート前チェックモードが実行されます。

- StoreFront™
- デリバリーグループ
- アプリケーショングループ
- アプリケーション
- AppV分離グループ
- AppLibパッケージ検出

- グループポリシー
- ユーザーゾーン設定
- 手動でプロビジョニングされた、またはPVSでプロビジョニングされたマシンカタログ
- 管理フォルダー
  - アプリケーションフォルダー
  - デリバリーグループフォルダー
  - マシンカタログフォルダー
- サイト設定

重要:

- 異なるコンポーネントを復元するには、リストの順序に従ってください。たとえば、アプリケーション、デリバリーグループ、およびグループポリシーを復元したい場合は、次の順序に従う必要があります。
  - デリバリーグループ
  - アプリケーション
  - グループポリシー
- MCS マシンカタログをバックアップまたは復元することはできません。

バックアップの種類

要件に応じてバックアップを実行するには、次のオプションを使用します。

- **オンデマンド**: サイト構成をリアルタイムでバックアップします。このアクションは、現在のCitrix Cloud™サイト構成をバックアップします。
- **スケジュール済み**: サイト構成をスケジュールされた間隔でバックアップします。これは、指定された間隔で繰り返されます。

注:

フル権限を持つ管理者とクラウド管理者のみが、オンデマンドまたはスケジュールされたバックアップと復元を実行できます。

Web Studio を使用したバックアップと復元

この記事では、コンソールの左ペインにある **バックアップと復元** ノードで実行できるアクションについて説明します。

バックアップと復元 を使用すると、管理者は Web Studio からバックアップを作成できます。

ストレージの場所を設定する

バックアップを作成する前に、バックアップを保存するストレージの場所を設定する必要があります。

1. Web Studio から、**管理** をクリックします。
2. 左側のメニューから、**バックアップ+復元** を選択します。
3. **バックアップと復元** タブ内で、**ストレージの設定** をクリックします。

   バックアップのストレージの場所を設定する (/en-us/citrix-virtual-apps-desktops/2503/media/first-time-backup-storage-1.png)
4. ドロップダウンリストから、**ストレージの種類** を選択します。ストレージの種類は、ファイルストレージまたはAzureストレージにすることができます。

   > **注:**
   >
   > - その場所は、すべてのDelivery Controllerからアクセスできる必要があります。
   > - フォルダーへのアクセスにユーザー名とパスワードが必要な場合は、企業のパスワードポリシーによってパスワードの有効期間が制限されないようにしてください。

5. 以下を選択します。
   - 最大バックアップ数
   - 最大ピン留めバックアップ数
   - 自動ピン留めバックアップの最大数
6. ストレージの場所を保存するには **Save** をクリックし、ストレージの場所を保存してバックアップを作成するには **Save and create backup** をクリックします。

ストレージの場所を設定したら、バックアップを作成できます。

オンデマンドバックアップの作成

1. Web Studio から、**Manage** をクリックします。
2. 左側のメニューから、**Backup and Restore** を選択します。
3. ストレージの場所が設定されているがバックアップが存在しない場合、バックアップを作成するよう求められます。

   初期バックアップの作成(/en-us/citrix-virtual-apps-desktops/2503/media/backup-after-storage-creation.png)

   既存のバックアップがある場合は、**Create backup** をクリックできます。
4. **Create backup** ページで、メモを入力し、**Create backup** をクリックします。

   バックアップをトリガーした管理者の名前でバックアップされるバックアップコンポーネントを示す概要アクティビティが表示されます。
5. バックアップが正常に完了すると、**Backup and Restore** タブの下に項目として表示されます。
6. 特定のバックアップを選択すると、**Details** タブでそのバックアップに関する詳細情報が表示されます。
7. バックアップを削除するには、バックアップを右クリックして **Delete backup** をクリックします。

バックアップをピン留めする

Citrix® は最新のバックアップ 30 個を保存します。30 個を超えるバックアップを作成すると、システムは作成された順序で古いバックアップを削除します。30 個のバックアップ制限に加えて新しいバックアップが作成されるたびに、システムは最初に作成されたバックアップを削除します。バックアップのピン留めは、特定のバックアップが自動的に削除されるのを防ぐために使用されます。最大 5 個のバックアップをピン留めできます。ピン留めされたバックアップがある場合、30 個のバックアップに加えて、すべてのピン留めされたバックアップを保持します。つまり、最大 35 個のバックアップ (ピン留めされていない 30 個とピン留めされた 5 個) を保持できます。

1. バックアップをピン留めするには、右クリックします。

スケジュールされたバックアップを作成する

組織の要件に合ったバックアップスケジュールを作成し、バックアップと復元プロセスを自動化します。バックアップは、選択した頻度 (毎日、毎週、毎月、またはその他の適切な頻度) でバックグラウンドで実行されます。

1. スケジュールタブに移動し、**スケジュールを作成**を選択します。
2. **スケジュールを作成**ページで、以下を入力します。
    - : このバックアップスケジュールを有効にするには、 を選択します。
    - : バックアップスケジュールの名前を入力します。
    - : 説明を入力します。
    - : 任意のタイムゾーンを選択します。
    - : バックアップを実行する頻度を選択します。
    - : スケジュールを繰り返す日数間隔を入力します。
    - : 開始日を入力します。
    - : バックアップを開始する時刻を 24 時間形式で入力します。
3. **完了**を選択します。

スケジュールされたバックアップを制限する

同一のバックアップを避けるため、スケジュールされたバックアップを1日1回に制限できます。

1. 「**バックアップと復元**」ノードの「**設定**」タブに移動します。
2. 「**スケジュールされたバックアップ**」ボックスで「**変更**」をクリックします。
3. トグルを切り替えて、スケジュールされたバックアップを1日1回に制限することを有効にします。

スケジュールされたバックアップの自動ピン留め

スケジュールされたバックアップの自動ピン留めは、選択したスケジュールによって作成されたバックアップを自動的にピン留めします。自動ピン留めには、1つのスケジュールのみを選択できます。

スケジュールされたバックアップの自動ピン留めを使用すると、最大6つのスケジュールされたバックアップを保持できます。最大制限に達すると、最も古い自動ピン留めされたバックアップが削除されます。

> 「**注：**」:

> Citrixは最大6つの自動ピン留めされたバックアップを保存します。システムは、6番目のバックアップ以降に作成された古いバックアップを、作成された順序で削除します。6つのバッ

> クアップ制限に加えて新しく作成されるバックアップごとに、システムは最初に作成されたバックアップを削除します。

1. 「**バックアップと復元**」ノードの「**設定**」タブに移動します。
2. 自動ピン留めのためにスケジュールされたバックアップを選択します。
3. トグルを切り替えて、自動ピン留めされたスケジュールを有効にします。
4. スケジュールを選択し、「**保存**」をクリックします。

バックアップストレージの編集

バックアップストレージ設定を編集して、ストレージの種類と場所、最大バックアップ数、最大ピン留めバックアップ数、および最大自動ピン留めバックアップ数を変更できます。

1. **バックアップと復元**ノードの**設定**タブに移動します。
2. **ストレージ**ボックスで**変更**をクリックします。
3. **バックアップストレージの編集**ダイアログでストレージ設定を変更します。

復元

この機能により、管理者はバックアップからサイト構成を復元できます。一度に1つのコンポーネントのみを復元できます。

> **注：**
>
> - 一度に1つのコンポーネントのみを復元することで、コンポーネント間の依存関係による復元中の競合を防ぎます。
> - ホスト接続を復元するワークフローは、ホスト接続を復元しようとするたびにシークレットを入力する必要があるため、他のコンポーネントとは異なります。**バックアップの復元**をクリックすると、シークレットを入力するダイアログが表示されます。たとえば、Azureでは、接続の作成に使用した英数字のアプリケーションシークレットを入力します。

1. Web Studioから、**管理**をクリックします。
2. 左側のメニューから、**バックアップと復元**を選択します。
3. リストから特定のバックアップをクリックします。
4. **バックアップの復元**をクリックします。

5. **バックアップの復元**ウィンドウで、以下を入力します。

   - **コンポーネント**：復元するコンポーネントを選択します。
   - **フィルター**：復元するメンバー名をコンマ区切りのリストで指定します。たとえば、*chrome*という単語でフィルターすると、chromeという名前のオブジェクトのみが復元されます。同様に、`chr`というフレーズは、`chr`で始まるオブジェクトを復元します。

     コンポーネントメンバーを表示するには、バックアップを選択し、「**詳細 > コンポーネント**」に移動します。コンポーネントを選択し、「**コンポーネントメンバーの表示**」をクリックします。
   - **チェックモード**：実際の復元操作が実行されたときに復元する必要があるものを確認するには、**はい**を選択します。このオプションは、実際の復元をトリガーすることなく、復元に必要なすべてを事前に評価します。たとえば、アプリケーションコンポーネントの復元プロセスが実行されたときに復元されるアプリケーションのリストが表示されます。

     > **注：**
     >
     > チェックモードでは、実際の復元は実行されません。このオプションでは、コンポーネント間の依存関係もチェックされません。最適な結果を得るには、一度に1つのコンポーネントでチェックモードを使用することをお勧めします。

   - **復元タイプ**：いずれかを選択します。
     - **不足のみ**：この復元タイプを使用して、コンポーネントとメンバーをサイトに追加します。このオプションは、復元されるバックアップの構成が異なっていても、既存のコンポーネントとメンバーを変更しません。
     - **不足と既存の更新**：この復元タイプを使用して、コンポーネントをサイトに追加および更新します。このオプションは、既存のコンポーネントとメンバーの構成が異なる場合、バックアップの構成で更新します。
   - **メモ**：メモを入力します。

6. **復元**を選択します。

復元アクションが完了すると、復元結果が**復元**ウィンドウに表示されます。すべての復元アクションは、**履歴**タブに一覧表示されます。

履歴

履歴タブで、すべてのバックアップおよび復元アクションを追跡できます。

アクションの下に、削除されたすべてのバックアップとバックアップ履歴が表示されます。

バックアップの詳細を表示するには：

1. **履歴**タブに移動します。
2. バックアップアクションを選択し、**詳細の表示**をクリックします。

バックアップ結果には、次の詳細が表示されます。

- 期間
- 注
- 管理者名
- バックアップされたコンポーネント

「**履歴**」ページの右上にある検索バーを使用して、特定のバックアップを検索します。たとえば、特定の管理者によって実行されたバックアップや、特定の日に実行されたバックアップを検索できます。

自動構成ツールを使用したバックアップと復元

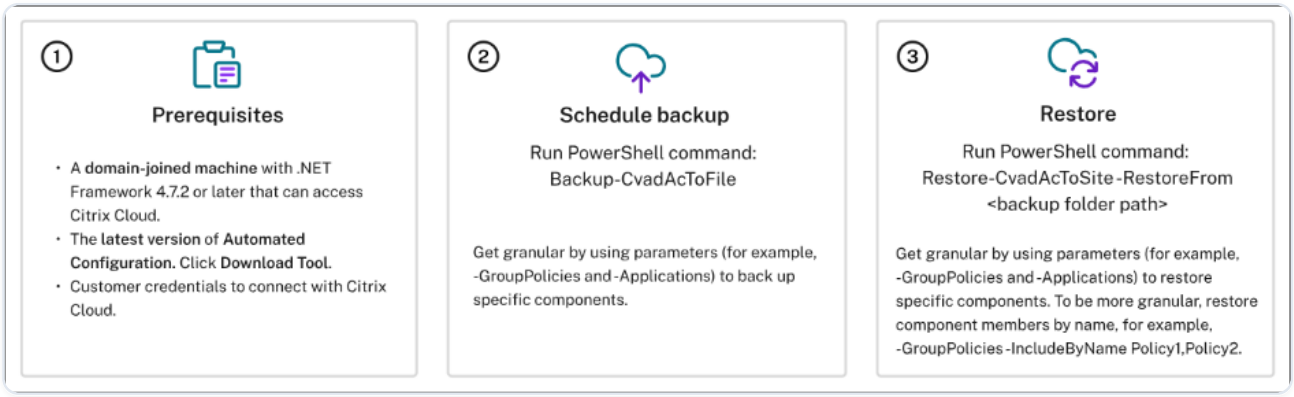
自動構成ツールを使用すると、以下の環境でオンデマンドおよびスケジュールされたバックアップを実行できます。

- シトリックス バーチャルアプリおよびデスクトップ™
- DaaS

自動構成ツールは、以下の目的で使用できます。

- バックアップと復元（オンデマンドおよびスケジュールされたバックアップ）
- 移行（オンデマンドバックアップ）

移行のための自動構成ツール



シトリックス バーチャルアプリおよびデスクトップ

構成をバックアップするための前提条件

- Citrix Virtual Apps and Desktops のすべてのバージョン。
- Auto Config を実行するマシン。このデバイスは次のいずれかです。
  - デリバリーコントローラー™
  - .NET Framework 4.7.2 以降および Citrix PowerShell SDK がインストールされたドメイン参加済みマシン。Citrix PowerShell の場合、Web Studio をインストールする必要があります。

バックアップ

1. 「Automated Configuration」をインストールします。詳細については、「Automated Configuration のダウンロード」を参照してください。
2. **Auto-Config** をダブルクリックします。
3. PowerShell ウィンドウで、すべてのコンポーネントをエクスポートするためにコマンド `Backup-CvadAcToFile` を実行します。オンプレミス構成をエクスポートしても、変更されることはありません。

コマンドを初めて実行すると、プロセスは次の場所に `.yml` 構成ファイルを含むフォルダーを作成します。 `%HOMEPATH%\Documents\Citrix\AutoConfig`。

そのフォルダーには、最近エクスポートされたバックアップファイルが含まれており、以前の各バックアップはサブフォルダーに保存されます。

復元

1. **Auto-Config** をダブルクリックします。
2. 復元を実行するには、次のコマンドを実行します。

```
Restore-CvadAcToSite -Environment OnPrem -RestoreFolder <folder path of the backup files>
```

3. コマンドを実行した後、エクスポートの状態を確認し、ログフォルダーは次の場所で利用できます: `%HOMEPATH%\Documents\Citrix\AutoConfig`。
4. エラーまたは例外がある場合は、ログファイルの **Fixups** セクションを参照してください。

DaaS

構成をバックアップするための前提条件

- アクティブなリソースの場所とコネクタがインストールされているDaaS環境。
- Citrix Cloud にアクセスするサイトへの接続。詳細については、「システムおよび接続要件」を参照してください。

> **注**
>
> Automated Configuration を使用して、クラウドから MCS をバックアップすることはできません。

バックアップ

次のファイルをバックアップします:

- 顧客 ID、クライアント ID、およびシークレットキー情報を含む `CustomerInfo.yml` ファイル。顧客 ID、クライアント ID、およびシークレットキーを取得するプロセスについて詳しくは、「顧客 ID、クライアント ID、およびシークレットキーの生成」を参照してください。この情報を `CustomerInfo.yml` ファイルに追加する方法については、「顧客情報ファイルの入力」を参照してください。
- クラウド内のリソースの場所をマッピングする情報を含む `ZoneMapping.yml` ファイル。ゾーンをマッピングする方法について詳しくは、「ゾーンマッピングファイルの入力」を参照してください。
- ホスト接続に関する情報を含む `CvadAcSecurity.yml` ファイル。

1. Automated Configuration をインストールします。詳しくは、「Automated Configuration のインストール」を参照してください。

> **注**

> DaaS のバックアップの場合、Automated Configuration は、インターネットアクセスがあり、管理者が直接アクセスできるマシンにインストールします。

1. **Auto Config** をダブルクリックします。
2. PowerShell ウィンドウで、次のコマンドを実行してバックアップを作成します: `Export-CvadAcToFile`

コマンドを初めて実行すると、プロセスによって .yml 構成ファイルを含むフォルダーが次の場所に作成されます: `%HOMEPATH%\Documents\Citrix\AutoConfig`

このフォルダーには、最近のエクスポートからのバックアップファイルが含まれており、以前の各バックアップはサブフォルダーに保存されます。

復元

1. 「**Auto Config**」をダブルクリックします。
2. PowerShellウィンドウで、復元を実行するには、次のコマンドを実行します。

```
Restore-CvadAcToSite -RestoreFolder <folder path of the backup files>
```

3. コマンドを実行したら、エクスポートの状態を確認し、ログフォルダーは`%HOMEPATH%\Documents\Citrix\AutoConfig`にあります。
4. エラーまたは例外がある場合は、ログファイルの**Fixups**セクションを参照してください。

きめ細かい移行

> **注**
>
> コンポーネントの移行順序の詳細については、コンポーネントの移行順序を参照してください。

コンポーネント全体の復元

コンポーネントを復元するには、1つ以上のパラメーターを選択する必要があります。

例として、デリバリーグループとマシンカタログコンポーネント全体を復元するには、次のコマンドを実行します。

```
Restore-CvadAcToSite -RestoreFolder %HOMEPATH%
\Documents\Citrix\AutoConfig/Backup_yyyy_mm_dd_hh_mm_ss -DeliveryGroups
-MachineCatalogs
```

コンポーネントメンバーの復元

1つ以上のコンポーネントメンバーを復元するには、`IncludeByName`機能を使用します。選択したコンポーネントとインクルージョンリストとともに、`Restorefolder`パラメーターを指定して`Restore`コマンドレットを呼び出す必要があります。

例として、バックアップから2つのグループポリシーを復元するには:

```
Restore-CvadAcToSite -RestoreFolder %HOMEPATH%
\Documents\Citrix\AutoConfig/Backup_yyyy_mm_dd_hh_mm_ss -GroupPolicies
-IncludeByName Policy1,Policy2
```

完全なクラウドサイト構成の復元

すべてのコンポーネントまたはクラウドサイト全体を復元するには、次のコマンドを実行します。

```
Restore-CvadAcToSite -RestoreFolder %HOMEPATH%
\Documents\Citrix\AutoConfig/Backup_yyyy_mm_dd_hh_mm_ss
```

バックアップと復元のためのAutomated Configurationツール

Automated Configuration ツールのコマンドは、Web Studio が使用するバックアップおよび復元 API をトリガーします。

`BckRstr` コマンドレットはコンソールにログを記録します。ログ情報を含むフォルダーは `\Documents\Citrix\AutoConfig` には作成されません。

> **注：**
>
> Citrix Virtual Apps and Desktops および Citrix DaaS™ で構成をバックアップするための前提条件は、PowerShell セッションでの自動構成ツールと同じです。

バックアップ

Delivery Controllerで新しいバックアップアクションを開始するには、PowerShellウィンドウで`New-BckRstrBackup` を実行します。

復元

既存のバックアップから単一コンポーネントのメンバーを復元するには、PowerShellウィンドウで `Restore-BckRstrBackups` を実行します。

コマンドの完全なリストについては、「バックアップと復元用の自動構成ツールコマンドレット」を参照してください。

バックアップと復元のベストプラクティス

この記事では、バックアップと復元の計画をより適切に行うのに役立ついくつかの推奨事項を提供します。

カテゴリ	ベストプラクティス
バックアップのスケジュール設定	サイト構成の変更頻度に応じて、毎日、毎週、または毎月の頻度で実行できるデフォルトのバックアップスケジュールを設定します。このデフォルトスケジュールは、アクティビティの少ない時間帯（週末や深夜など）に設定してください。スケジュールされたバックアップの詳細については、「スケジュールされたバックアップの作成」を参照してください。
	同じ日に実行される可能性のある複数のバックアップスケジュールが定義されている場合は、**バックアップと復元**ノードの**設定**タブを使用して、1日あたりのバックアップ数を1つにリセットします。
バックアップの管理	30個のバックアップ制限に達しても保持されるように、常にゴールデンコピーバックアップをピン留めしてください。選択したバックアップをピン留めするには、バックアップを右クリックします。

よくある質問

カスタム管理者はバックアップと復元を実行できますか?

いいえ。バックアップと復元機能は、フル権限を持つ管理者のみに制限されています。

特定のコンポーネントをバックアップできますか?

いいえ。現在、オンデマンドバックアップとスケジュールされたバックアップは、サイト構成全体をバックアップします。コンポーネントにはいくつかの依存関係と前提条件があります。これらの依存関係が適切に解決されるように、コンポーネント全体をバックアップできます。ただし、特定のコンポーネントを復元することはできます。

バックアップをダウンロードできますか?

現在、バックアップをダウンロードするにはACTを使用します。Automated Configuration for Virtual Apps and DesktopsからACTをダウンロードできます。

MCSカタログをバックアップおよび復元できますか?

現在、MCSカタログをバックアップおよび復元することはできません。ACTを使用してMCSカタログをバックアップし、別のサイトにインポートできます。

構成をCitrix Cloud™に移行する

Automated Configuration Tool (ACT) を使用すると、Citrix Virtual Apps and Desktops™ の構成 (ポリシー、アプリケーション、カタログ、管理者ロール、スコープなど) を、1つ以上のオンプレミスサイトからCitrix Cloudでホストされているサイトに移行できます。また、異なるクラウドリージョンまたはテナント間で情報を移行するためにも使用できます。

このツールは、1つ以上のオンプレミスサイトを構成ファイルのコレクションとして検出し、エクスポートします。これらのファイルはオプションで編集できます。これらのファイルの構成は、Citrix DaaSにインポートできます。 移行は、ツールを複数回実行することで段階的に行われ、目的の構成状態を簡単に実現できます。

ACTは一度きりの移行ツールではありません。日常的なクラウド運用を管理するために使用できます。たとえば、次のとおりです。

- テストまたはステージングのクラウドアカウントから本番クラウドアカウントへの転送を自動化する
- 構成のバックアップと復元
- 1つのクラウド環境を複数のクラウドに分割する

以下の*2分間の*ビデオでは、Automated Configurationのクイックツアーを提供します。

<iframe src="https://www.youtube.com/embed/uyQ9o2L1DXQ" width="720px" height="480px" frameborder="0" title="YouTube video player" allowfullscreen=""> </iframe>
Automated Configurationの詳細については、Tech Zoneの概念実証: Automated Configuration Toolを参照してください。

展開の移動と、オンプレミス構成を移行用に準備する方法の詳細については、Tech Zoneの展開ガイド: Citrix Virtual Apps and DesktopsをオンプレミスからCitrix Cloudに移行するを参照してください。

既知の制限事項

- Machine Creation Services™を介してプロビジョニングされたマシンカタログには、特別な考慮事項があります。MCSの詳細については、Machine Creation Servicesでプロビジョニングされたカタログの移行についてを参照してください。

構成を移行するための前提条件

Citrix Virtual Apps and Desktopsから構成を*エクスポート*するには、次のものが必要です。

- Citrix Virtual Apps and Desktops: 現行リリースとその直前のリリース、またはCitrix Virtual Apps and Desktops、XenAppおよびXenDesktop® LTSRs: 全バージョン
- .NET Framework 4.7.2以降およびCitrix PowerShell SDKがインストールされたドメイン参加済みマシン。これはDelivery Controllerに自動的にインストールされます。（オンプレミスのDelivery Controller以外のマシンで実行するには、Citrix Studioがインストールされている必要があります。Studioは正しいPowerShellスナップインをインストールするためです。Studioインストーラーは Citrix Virtual Apps and Desktopsのインストールメディアにあります。）

Citrix DaaSに構成を*インポート*するには、以下が必要です。

- Citrix Cloudにアクセスできるマシン。これはDelivery Controller™やドメイン参加済みマシンである必要はありません。
- Citrix DaaSがプロビジョニングされていること。
- Connectorがインストールされ、オンプレミス環境と同じドメインにドメイン参加しているアクティブなリソースの場所。
- Citrix Cloudにアクセスするサイトへの接続が許可され、利用可能であること。詳細については、「システムおよび接続要件」を参照してください。

> **注:**
>
> Automated ConfigurationはCloud Connectorシステムにはインストールできません。

主な手順

1. Automated Configuration Toolをダウンロードし、システム要件を確認します。「Automated Configurationのダウンロード」を参照してください。
2. Citrix Cloudポータルから生成された`CustomerName`、`CustomerID`、および`SecretKey`の値を`CustomerInfo.yml`ファイルに入力します。「顧客ID、クライアントID、およびシークレットキーの生成」および「顧客情報ファイルの入力」を参照してください。
3. オンプレミスサイトに複数のゾーンが含まれている場合は、ゾーンをCitrix DaaSリソースの場所にマッピングするように`ZoneMapping.yml`ファイルを更新します。「ゾーンマッピングファイルの入力」を参照してください。
4. サイトに複数のホスティング接続が含まれている場合は、Citrix DaaSに移行する各ホストタイプの接続情報で`CvadAcSecurity.yml`ファイルを更新します。ホスト接続が1つしかない場合は、そのホスト接続の接続情報で`CvadACSecurity.yml`ファイルを更新します。「ホスト接続のセキュリティファイルの更新」を参照してください。
5. ACTを開き、`Export-CvadAcToFile`コマンドを使用してオンプレミスサイトをエクスポートします。移行でサポートされるコンポーネントのリストについては、「サポートされる移行オブジェクト」を参照してください。エクスポートの手順については、「オンプレミス構成のエクスポート」を参照してください。
6. `Merge-CvadAcToSite`コマンドを使用して、コンポーネントを段階的にインポートします。または、サイト全体を一度に移行します。コンポーネント移行順序に記載されている順序でコンポーネントを移行してください。インポートの手順については、インポートの実行を参照してください。
7. クラウドサイトをアクティブ化します。サイトのアクティブ化を参照してください。

Automated Configuration をダウンロード

Citrix Downloadsから Automated Configuration ツールをダウンロードしてインストールします。

Automated Configuration をアップグレード

機能上のエラーを防ぐため、常に最新バージョンの ACT を使用してください。

ツールのバージョンを確認するには、次の手順を実行します。

1. **Auto Config** アイコンをダブルクリックします。PowerShell ウィンドウが表示されます。
2. バージョン番号を確認するには、次のコマンドを実行します。

```
Get-CvadAcStatus
```

3. Citrix Downloadsに記載されているバージョンと、お使いのツールのバージョンを比較してください。ツールの最新バージョンはそこにあります。
4. ツールの最新バージョンをダウンロードしてインストールします。Automated Configuration をアップグレードするために、古いバージョンをアンインストールする必要は*ありません*。

> **注:**
>
> Automated Configuration でクラウドにアクセスするためのコマンドレットを実行すると、新しいバージョンがダウンロード可能になったときにツールが通知します。コマンドレットの詳細については、Automated Configuration ツールコマンドレットを参照してください。

顧客 ID、クライアント ID、およびシークレットキーを生成する

オンプレミスサイトを Citrix DaaS に移行するには、Citrix Cloud ポータルから顧客 ID、クライアント ID、およびシークレットキーを使用して`CustomerInfo.yml`ファイルに入力します。

顧客IDを取得するには：

1. Citrix Cloudアカウントにサインインし、顧客を選択します。
2. グリッドアイコンをクリックし、**Identity and Access Management**を選択します。
3. **API access > Secure clients**に移動します。顧客IDがページに表示されます。

クライアントIDとシークレットキーを取得するには：

1. **Secure clients**ページで、ボックスに名前を入力します。この名前は、複数のクライアントIDとシークレットキーを区別するために使用されます。
2. クライアントIDとシークレットキーを作成するには、「Create Client」をクリックします。
3. クライアントIDとシークレットキーを安全な場所にコピーし、この情報を含む`.csv`ファイルをダウンロードします。`.csv`ファイルを使用して`CustomerInfo.yml`ファイルを生成します。

> **注:**
>
> - クライアントIDとシークレットキーには有効期限がありません。これらが侵害された場合は、**ゴミ箱**アイコンを使用して直ちに削除し、新しいものを作成してください。

- シークレットキーを紛失または忘れた場合、それを取得することはできません。新しいクライアントIDとシークレットキーを作成する必要があります。

顧客情報ファイルを生成する

`CustomerInfo.yml`ファイルを使用すると、コマンドレットを実行するたびに顧客情報パラメーターを指定する必要がなくなります。顧客情報のいずれかは、コマンドレットパラメーターを使用して上書きできます。

`New-CvadAcCustomerInfoFile`コマンドレットを使用して`CustomerInfo.yml`ファイルを作成します。

重要:

`CustomerInfo.yml`ファイルを手動で編集しないでください。そうすると、意図しない書式設定エラーが発生する可能性があります。

`New-CvadAcCustomerInfoFile` cmdletには次の必須パラメーターがあります。

- CustomerId: 顧客のID。
- ClientId: Citrix Cloud で作成された顧客のクライアントID。
- Secret: Citrix Cloud で作成された顧客のシークレット。

例:

```
New-CvadAcCustomerInfoFile -CustomerId markhof123 -ClientId
6813EEA6-46CC-4F8A-BC71-539F2DAC5984 -Secret TwBLaaaaaaaaaaaaaaaaw==
```

ダウンロードした`security.csv`ファイルを指す`SecurityCsvFileSpec`パラメーターを使用して、`CustomerInfo.yml`を作成することもできます。CustomerIdも指定する必要があります。

```
New-CvadAcCustomerInfoFile -SecurityCsvFileSpec C:
\Users\my_user_name\downloads/security.csv -CustomerId markhof123
```

`Set-CvadAcCustomerInfoFile` cmdletを使用して`CustomerInfo.yml`ファイルを更新します。このcmdletはクライアントIDのみを変更します。

```
Set-CvadAcCustomerInfoFile -ClientId C80487EE-7113-49F8-85DD-2CFE30CC398E
```

以下はCustomerInfo.ymlファイルのサンプルです。

```
# Created/Updated on 2020/01/29 16:46:47

CustomerId: 'markhof123'

ClientId: '6713FEA6-46CC-4F8A-BC71-539F2DDK5384'

Secret: 'TwBLaaabbbaaaaaaaaaaw=='

Environment: Production

AltRootUrl: ''

StopOnError: False

AlternateFolder: ''

Locale: 'en-us'

Editor: 'C:\Program Files\Notepad++\notepad++.exe'

Confirm: True

DisplayLog: True
```

ゾーンマッピングファイルにデータを入力する

オンプレミスゾーンは、クラウドのリソースロケーションに相当します。他のサイトコンポーネントとは異なり、オンプレミスゾーンをクラウドに自動的にインポートすることはできません。代わりに、`ZoneMapping.yml`ファイルを使用して手動でマッピングする必要があります。ゾーン名が既存のリソースロケーション名に関連付けられていない場合、インポートエラーが発生する可能性があります。

オンプレミスサイトに1つのゾーンしかなく、クラウドサイトに1つのリソースロケーションしかない場合、自動構成ツールが正しい関連付けを行い、`ZoneMapping.yml`ファイルを手動で管理する必要がなくなります。

ただし、オンプレミスサイトに複数のゾーンがある場合、またはクラウドサイトに複数のリソースロケーションがある場合は、オンプレミスゾーンとクラウドのリソースロケーションの正しいマッピングを反映するように、`ZoneMapping.yml`ファイルを手動で更新してください。

`ZoneMapping.yml`ファイルは`%HOMEPATH%\Documents\Citrix\AutoConfig`にあります。`.yml`ファイルの内容は、ゾーン名をキーとし、リソースロケーション名を値とする辞書です。

例えば、「Zone-1」というプライマリゾーンと「Zone-2」というセカンダリゾーンを持つオンプレミスのCitrix Virtual Apps and Desktopsサイトが、「Cloud-RL-1」と「Cloud-RL-2」という2つの新しく作成されたクラウドのリソースロケーションを持つCitrix DaaS展開に移行されるとします。この場合、ZoneMapping.ymlは次のように構成されます。

```
Zone-1: Cloud-RL-1



Zone-2: Cloud-RL-2
```

注:

コロンとリソースロケーション名の間にスペースを追加します。ゾーン名またはリソースロケーション名にスペースが含まれている場合は、名前を引用符で囲みます。

ホスト接続用のセキュリティファイルを更新する

ホスト接続およびそれらに関連付けられているハイパーバイザーは、ACT を使用してエクスポートおよびインポートできます。

ホスト接続にハイパーバイザーを追加するには、ハイパーバイザーの種類に固有のセキュリティ情報が必要です。この情報は、セキュリティ上の理由からオンプレミスサイトからエクスポートできません。Automated Configuration がホスト接続とハイパーバイザーをクラウドサイトに正常にインポートできるように、情報を手動で指定する必要があります。

エクスポートプロセスにより、`%HOMEPATH%\Documents\Citrix\AutoConfig` に `CvadAcSecurity.yml` ファイルが作成されます。これには、特定のハイパーバイザーの種類に必要な各セキュリティ項目のプレースホルダーが含まれています。クラウドサイトにインポートする前に、`CvadAcSecurity.yml` ファイルを更新する必要があります。管理者による更新は、必要に応じて新しいセキュリティプレースホルダーが追加された複数のエクスポートで保持されます。セ

キュリティ項目が削除されることはありません。詳細については、「CvadAcSecurity.yml ファイルを手動で更新する」を参照してください。

```
HostConn1:

ConnectionType: XenServer®

UserName: root

PasswordKey: rootPassword

HostCon2:

ConnectionType: AWS

ApiKey: 78AB6083-EF60-4D26-B2L5-BZ35X00DA5CH

SecretKey: TwBLaaaaaaaaaaaaaaaaw==

Region: East
```

ハイパーバイザーごとのセキュリティ情報

以下に、各ハイパーバイザーの種類に必要なセキュリティ情報を示します。

- ゼノサーバー、ハイパーブイ、ヴイエムウェア
  - ユーザー名
  - クリアテキストパスワード
- マイクロソフト アジュール
  - サブスクリプションID
  - アプリケーションID
  - アプリケーションシークレット
- AWS
  - サービスアカウントID
  - アプリケーションシークレット
  - 地域

セキュリティに関する特別な考慮事項

すべてのセキュリティ情報はクリアテキストで入力されます。クリアテキストが推奨されない場合は、ホスト接続と関連するハイパーバイザーを**Studio**を使用して手動で作成できます。ホスト接続とハイパーバイザーの名前は、オンプレミスの対応するものと完全に一致している必要があります。そうすることで、ホスト接続を使用するマシンカタログを正常にインポートできます。

Citrix Virtual Apps and Desktopsのオンプレミス構成をエクスポートする

`export` PowerShellコマンドを使用して、既存のオンプレミス構成をエクスポートし、必要な`.yml`ファイルを取得できます。これらのファイルは、目的の構成をCitrix Cloudにインポートするために使用されます。

サポートされている移行オブジェクト

自動構成は、以下のコンポーネントの構成の移動をサポートしています。

- タグ
- 委任管理
  - スコープ
  - ロール
- ホスト接続
  - 単一のリソースプール
  - 管理者スコープ
- マシンカタログ
  - 管理者スコープ
  - マシン
  - リモートPCアクセス、物理、プール、プロビジョニング済み、MCS、割り当て済み
- StoreFront™
- デリバリー グループ
  - アクセスポリシー
  - 管理スコープの関連付け
  - アプリケーションアクセスポリシー
  - 割り当てポリシー

    - エンタイトルメント/デスクトップポリシー
    - 電源スケジュール
    - セッションの残存
    - セッションの事前起動
    - 再起動スケジュール
    - タグ
- アプリケーション グループ
    - 管理スコープの関連付け
    - デリバリー グループ
    - ユーザーとグループ
- アプリケーション
    - アプリケーション フォルダー
    - アイコン
    - アプリケーション
    - ブローカー構成済みFTA
    - タグ
- グループポリシー
- ユーザーゾーンの優先設定

オンプレミス構成のエクスポート

1. **Auto Config**アイコンをダブルクリックします。PowerShellウィンドウが表示されます。
2. 次のコマンドを実行して、すべてのコンポーネントをエクスポートします。オンプレミス構成をエクスポートしても、その構成が変更されることは*ありません*。

```
Export-CvadAcToFile
```

初めてコマンドレットを実行すると、`.yml`構成ファイルとログを含むエクスポートフォルダーが作成されます。フォルダーは`%HOMEPATH%\Documents\Citrix\AutoConfig`にあります。エクスポートが成功するたびにサブフォルダーが作成されます。親フォルダー`%HOMEPATH%\Documents\Citrix\AutoConfig`には、常に最新のエクスポートからのエクスポートファイルが含まれています。

注:

Delivery ControllerにAutomated Configurationがインストールされていない場合は、PowerShellを介してツールを使用する前に`import-module Citrix.AutoConfig.Commands`を実行してください。**Auto Config**アイコンを使用してAutomated Configurationを開く場合は、この手順は不要です。

エラーまたは例外が発生した場合は、ログファイルの **Fixups** セクションを参照してください。

Citrix DaaSへの構成のインポート

重要:

- オンプレミス展開をクラウドに移行する際は、Citrix設定を含むドメインおよびOU GPOがクラウドに移行されていることを確認してください。Citrix Web Studio™はGPMCをサポートしていないため、ドメインおよびOU GPOはWeb Studioに表示されません。Citrixポリシーエンジンは、ドメインおよびOU内のVDAとユーザーに対してドメインおよびOU GPOを適用します。VDAにログインした後、ユーザーはドメインおよびOU GPOからのポリシーがセッションに適用されていることを確認できます。ただし、管理者はこれらのポリシーと設定を確認できないため、混乱を招く可能性があります。

コンポーネントの移行順序

コンポーネントとその依存関係をここに示します。コンポーネントの依存関係は、インポートまたはマージする前に配置されている必要があります。依存関係が欠落していると、インポートまたはマージコマンドが失敗する可能性があります。インポートまたはマージが失敗した場合、ログファイルの**Fixups**セクションに欠落している依存関係が表示されます。

1. タグ
    - 事前依存関係なし
2. 委任管理者
    - 事前依存関係なし
3. ホスト接続

- CvadAcSecurity.yml のセキュリティ情報

4. マシンカタログ
   - Active Directory に存在するマシン
   - ホスト接続
   - タグ
5. StoreFront
6. デリバリーグループ
   - Active Directory に存在するマシン
   - Active Directory に存在するユーザー
   - マシンカタログ
   - タグ
7. アプリケーショングループ
   - デリバリーグループ
   - タグ
8. アプリケーション
   - デリバリーグループ
   - アプリケーショングループ
   - タグ
9. グループポリシー
   - デリバリーグループ
   - タグ
10. ユーザーゾーン設定

インポートを実行する

1. **Auto Config**アイコンをダブルクリックします。PowerShellウィンドウが表示されます。
2. すべてのコンポーネントをインポートするには、次のコマンドを実行します。

```
Merge-CvadAcToSite
```

期待される状態と新しい現在の状態を確認します。さまざまなインポートオプションにより、インポート結果がオンプレミスサイトと同一であるか、そのサブセットであるかが制御されます。

コマンドレットを実行すると、`.yml`構成ファイルとログを含むエクスポートフォルダーが作成されます。フォルダーは`%HOMEPATH%\Documents\Citrix\AutoConfig`にあります。

エラーまたは例外が発生した場合は、ログファイルの**Fixups**セクションを参照してください。

> **注記：**
>
> Delivery Controller に Automated Configuration がインストールされていない場合、PowerShell を介してツールを使用する前に `import-module Citrix.AutoConfig.Commands` を実行します。**Auto Config** アイコンを使用して Automated Configuration を開く場合は、この手順は不要です。
>
> 元の Citrix DaaS 構成に戻すには、Citrix DaaS 構成のバックアップ を参照してください。

インポート操作を理解する

インポートプロセスは、更新を正確に実行し、必要な更新のみを実行し、すべての更新が正しく行われたことを確認するように設計されています。すべてのインポート操作で以下の手順が実行されます。

1. エクスポートされた .yml ファイルを読み取ります (期待される状態)。
2. クラウドを読み取ります (現在の状態)。
3. インポート前のクラウドの状態を .yml ファイルにバックアップします (必要に応じて、事前バックアップを復元できます)。
4. 期待される状態と現在の状態の間の差異を評価します。これにより、実行する更新が決定されます。
5. 更新を実行します。
6. クラウドを再読み込みします (新しい現在の状態)。
7. インポート後のクラウドの状態を .yml ファイルにバックアップします (必要に応じて、事後バックアップを復元できます)。
8. 新しい現在の状態を期待される状態と比較します。
9. 比較結果を報告します。

きめ細かな移行

> **重要:**
>
> コンポーネントの移行順序の詳細については、「」(#component-migration-order)を参照してください。

> コンポーネントのみ、あるいはコンポーネント名のみを選択的に移行できます。

- サポートされているコンポーネントパラメーターには、`MachineCatalogs`、`Tags`などがあります。
- サポートされているコンポーネント名パラメーターには、`IncludeByName`および`ExcludeByName`パラメーターなどがあります。

パラメーターとその使用方法の詳細については、「」(/ja-jp/citrix-virtual-apps-desktops/2503/manage-deployment/auto-config-cmdlets-migration#granular-migration-parameters)を参照してください。

サイトのアクティブ化

オンプレミスサイトとクラウドサイトの両方にあるデリバリーコントローラーは、デスクトップ、アプリケーションの仲介、マシンの再起動などのリソースを制御します。2つ以上のサイトによって共通のリソースセットが制御されると、問題が発生します。このような状況は、オンプレミスサイトからクラウドサイトに移行する際に発生する可能性があります。オンプレミスとクラウドの両方のデリバリーコントローラーが同じリソースセットを管理する可能性があります。このような二重管理は、リソースが利用できなくなり、管理不能になる可能性があり、診断が困難になる場合があります。

サイトのアクティブ化により、アクティブなサイトがどこで制御されるかを管理できます。

サイトのアクティブ化は、デリバリーグループのメンテナンスモードを使用して管理されます。サイトが非アクティブの場合、デリバリーグループはメンテナンスモードになります。アクティブなサイトのデリバリーグループからは、メンテナンスモードが解除されます。

サイトのアクティブ化は、VDA登録やマシンカタログに影響を与えたり、それらを管理したりすることはありません。

- `Set-CvadAcSiteActiveStateCloud`
- `Set-CvadAcSiteActiveStateOnPrem`

すべてのコマンドレットは、`IncludeByName`および`ExcludeByName`フィルタリングをサポートしています。このパラメーターを使用すると、メンテナンスモードを変更できるデリバリーグループを選択できます。デリバリーグループは必要に応じて選択的に変更できます。

インポートとクラウドへの制御の移行

オンプレミスサイトからクラウドサイトへのインポートと制御の移行に関する概要を以下に示します。

1. オンプレミスサイトをエクスポートしてクラウドにインポートします。`-SiteActive`パラメーターがどのインポートコマンドレットにも存在しないことを確認してください。オンプレミスサイトはアクティブになり、クラウドサイトは非アクティブになります。デフォルトでは、クラウドサイトのデリバリーグループはメンテナンスモードになっています。
2. クラウドのコンテンツと構成を確認します。
3. 営業時間外に、オンプレミスサイトを非アクティブに設定します。`-SiteActive`パラメーターは存在しない必要があります。すべてのオンプレミスサイトのデリバリーグループはメンテナンスモードになっています。
    - `Set-CvadAcSiteActiveStateOnPrem`
4. クラウドサイトをアクティブに設定します。`-SiteActive`パラメーターが存在している必要があります。クラウドサイトのデリバリーグループはメンテナンスモードではありません。
    - `Set-CvadAcSiteActiveStateCloud -SiteActive`
5. クラウドサイトがアクティブで、オンプレミスサイトが非アクティブであることを確認します。

オンプレミスサイトに制御を戻す

クラウドサイトからオンプレミスサイトに制御を転送するには：

1. 営業時間外に、クラウドサイトを非アクティブに設定します。すべてのクラウドサイトのデリバリーグループはメンテナンスモードになっています。
    - `Set-CvadAcSiteActiveStateCloud`
2. オンプレミスサイトをアクティブに設定します。オンプレミスサイトのデリバリーグループはメンテナンスモードではありません。
    - `Set-CvadAcSiteActiveStateOnPrem -SiteActive`

その他のサイトアクティベーション情報

- マシンが電源管理されておらず、再起動スケジュールもない場合（通常、ホスト接続もないことを意味します）、すべてのクラウドデリバリーグループをアクティブとしてインポートできます。インポート後に`Merge-CvadAcToSite` / `Import-CvadAcToSite`に`-SiteActive`を追加するか、`Set-CvadAcSiteActiveStateCloud -SiteActive`を実行します。
- マシンが電源管理されているか、再起動スケジュールがある場合は、別のプロセスが必要です。たとえば、この状況でオンプレミスからクラウドに切り替える場合は、`Set-CvadAcSiteActiveStateOnPrem`を使用してオンプレミスサイトを非アクティブに設定します。その後、`Set-CvadAcSiteActiveStateCloud -SiteActive`を使用してクラウドサイトをアクティブに設定します。
- `Set-CvadAcSiteActiveStateCloud`および`Set-CvadAcSiteActiveStateOnPrem`コマンドレットは、プロセスを元に戻すためにも使用されます。たとえば、`-SiteActive`パラメーターなしで`Set-CvadAcSiteActiveStateCloud`を実行し、次に`-SiteActive`パラメーターを指定して`Set-CvadAcSiteActiveStateOnPrem`を実行します。

Machine Creation Servicesでプロビジョニングされたカタログの移行について

> **注:**
>
> この機能はバージョン3.0以降でのみ利用可能です。Automated Configuration内で`Get-CvadAcStatus`を使用してバージョンを確認してください。

> Machine Creation Services (MCS) カタログは、2種類のカタログを作成します。

- マシンに加えられた変更が失われるか元に戻される場合（一般的に、アプリケーションが公開されるサーバーOSの場合） – これはプールされたVDI/マルチセッションのユースケースです
- マシンに加えられた変更が再起動後も保持される場合（一般的に、専用ユーザーを持つクライアントOSの場合） – これは静的VDIのユースケースです

カタログの種類は、Citrix Studioのカタログノードでカタログの「User data:」値を確認することで確認できます。

> **注:**

> Automated Configurationを使用して、クラウドからMCSをバックアップすることはできません。

プールされたVDI / マルチセッションカタログ

「ユーザーデータ: 破棄」のカタログはプールされたVDIカタログであり、メインイメージと構成のみを移行できます。これらのカタログ内の仮想マシンは移行されません。これは、仮想マシンのライフサイクルがインポート元のサイトによって維持されており、マシンが起動されるたびにその状態が変化する可能性があるためです。このため、仮想マシンのインポートデータがすぐに同期されなくなり、インポートが不可能になります。

このツールを使用してこれらのカタログを移行する場合、カタログメタデータが作成され、メインイメージの作成が開始されますが、マシンはインポートされません。

メインイメージのサイズに基づいてこのプロセスの作成には時間がかかる場合があるため、ツール内のインポートコマンドはMCSカタログの作成を開始するだけで、完了を待機しません。インポートが完了したら、クラウド展開のStudioを使用してカタログ作成の進行状況を監視してください。

メインイメージが作成されたら、マシンをプロビジョニングできます。オンプレミスでの使用によって容量が消費されるため、容量に関する考慮事項を検討してください。

そのカタログを使用する他のすべてのオブジェクト（デリバリーグループ、アプリケーション、ポリシーなど）はインポートでき、メインイメージの作成を待つ必要はありません。カタログの作成が完了したら、インポートされたカタログにマシンを追加でき、その後ユーザーはリソースを起動できます。

> **注:**
>
> カタログおよびその他すべてのオブジェクトを移行するには、ツール内で利用可能な同じコマンドを使用します。

静的VDIカタログ

> **注:**
>
> この操作はデータベースに保存されている低レベルの詳細をインポートするため、このプロセスはデータベースアクセス権を持つマシンから実行する必要があります。

> 静的VDIカタログは、メインイメージ、構成、およびすべての仮想マシンを移行します。プールされたVDIのユースケースとは異なり、イメージを作成する必要はありません。

VDAがクラウドに登録されるように、コネクタを指すように設定する必要があります。

クラウドサイトをアクティブにするには、サイトのアクティブ化セクションを参照してください。これにより、再起動スケジュール、電源管理、その他の項目がクラウドによって制御されます。

移行が完了した後、オンプレミスサイトからこのカタログを削除したい場合は、**VMとADアカウントを残す**を選択する必要があります。そうしないと、それらは削除され、クラウドサイトは削除されたVMを指したままになります。

移行後に孤立したリソースを検出するためにMCSタグを更新する

オンプレミス構成からクラウドサイトへ、またはクラウド構成から別のクラウドサイトへ移行した後、永続的なVMの場合、孤立したリソースを正しく検出できるようにMCSサイトIDタグを更新する必要があります。これを行うには、PowerShellコマンド`Set-ProvResourceTags`を使用します。現在、この機能はAzureに適用されます。

詳細な手順は次のとおりです。

1. 新しいCitrixサイトからPowerShellコマンド `Set-ProvResourceTags` を使用して、MCSサイトIDタグを更新します。例:

   ```
   Set-ProvResourceTags -ProvisioningSchemeUid xxxxx  [-VMName <String>]
   [-VMBatchSize XX] [-ResourceType XX]
   ```

   または、,

   ```
   Set-ProvResourceTags -ProvisioningSchemeName xxxxx  [-VMName <String>]
   [-VMBatchSize XX] [-ResourceType XX]
   ```

パラメーターの詳細は次のとおりです。

- `ProvisioningSchemeUid` または `ProvisioningSchemeName` は必須パラメーターです。
- `VMName` はオプションパラメーターです。`VMName` が指定されていない場合、このマシンカタログのすべてのVMのタグが更新されます。

- `VMBatchSize` は、すべてのVMをバッチに分割するためのオプションパラメーターです。`VMBatchSize` が指定されていない場合、デフォルト値 (10) が適用されます。範囲は1から60です。
- `ResourceType` は次のいずれかです。
  - `MachineCatalog`: マシンカタログリソースのタグを更新する場合。
  - `VirtualMachine`: VM関連リソースのタグを更新する場合。
  - `All`: (デフォルトのResourceType): マシンカタログとVM関連リソースの両方のタグを更新する場合。

複数のサイトを単一のサイトに統合する

自動構成のマルチサイトサポートは、複数のオンプレミスサイトを単一のクラウドサイトに統合する方法を提供します。

マルチサイトサポートは、オンプレミスサイトごとにコンポーネント名に一意のプレフィックスとサフィックスを追加し、複数のオンプレミスサイトが単一のクラウドサイトに統合された後も名前の一意性を確保します。

プレフィックスとサフィックスは、オンプレミスサイトごとに次の各コンポーネントに割り当てることができます。

- `AdminScope`
- `AdminRole`
- `ApplicationAdmin`
- `ApplicationFolder`
- `ApplicationGroup`
- `ApplicationUser`
- `DeliveryGroup`
- `GroupPolicy`
- `HostConnection`
- `MachineCatalog`
- `StoreFront`
- `Tag`

アプリケーションフォルダーは、プレフィックス、サフィックス、およびルートの再設定をサポートしています。ルートの再設定により、アプリケーションの既存のフォルダー構造に最上位のフォルダーが追加されます。

プレフィックスとサフィックスの規則

1. プレフィックスとサフィックスには、次の特殊文字を含めることはできません。`\ , / ; : # . * ? = < > | ( ) " ' { } [ ]`
2. プレフィックスとサフィックスには末尾のスペースを含めることができますが、先頭のスペースは含めることができません。
3. 末尾のスペースを含めるには、プレフィックスとサフィックスを二重引用符で囲む必要があります。
4. プレフィックスとサフィックスは、インポート、マージ、追加の際に適用されます。ソースの.ymlファイルが変更されることはありません。
5. プレフィックスとサフィックスの処理では、該当する場合、依存するコンポーネント名に自動的にプレフィックスまたはサフィックスが付けられます。たとえば、マシンカタログ名に「East」というプレフィックスが付いている場合、それらを参照するデリバリーグループにも「East」というプレフィックスが付けられます。
6. コンポーネント名がすでにプレフィックスまたはサフィックスで始まっている場合、プレフィックスまたはサフィックスは追加されません。コンポーネント名に、同じプレフィックスまたはサフィックスが二重に含まれることはありません。
7. プレフィックスとサフィックスは個別に、または組み合わせて使用できます。
8. コンポーネントでのプレフィックスまたはサフィックスの使用はオプションです。

> **注:**
>
> Studioはコンポーネントをアルファベット順に表示します。

コンポーネントをサイト別にグループ化する

プレフィックスを使用して、単一サイトのコンポーネントを視覚的にグループ化します。各サイトは独自のグループにリストされ、プレフィックスによって異なるサイトグループの順序がアルファベット順に制御されます。

コンポーネントを名前でグループ化する

サフィックスを使用して、複数のサイトから同じ名前のコンポーネントを視覚的にグループ化します。異なるサイトの同じ名前のコンポーネントは、視覚的に交互に表示されます。

プレフィックスとサフィックスのマッピングファイル

サイトのプレフィックス付けは、1つ以上のオンプレミスサイトのサイトプレフィックスとサフィックスのマッピングを含むSiteMerging.ymlファイルから始まります。SiteMerging.ymlファイルは、手動で管理することも、複数のオンプレミスサイトをマージするコマンドレットセクションに記載されている利用可能なコマンドレットを使用して管理することもできます。

オンプレミスサイトのエクスポート

オンプレミスサイトをエクスポートするまで、マージを開始できません。オンプレミスサイトをエクスポートするには、「」(/ja-jp/citrix-virtual-apps-desktops/2503/manage-deployment/migrate#export-on-premises-configuration)を参照してください。

中央エクスポートターゲットフォルダー

このセクションで説明する方法では、複数のサイトのエクスポートを中央のファイル共有の場所に配置します。`SiteMerging.yml`ファイル、`CustomerInfo.yml`ファイル、およびすべてのエクスポートファイルは、そのファイル共有の場所に存在するため、オンプレミスサイトとは独立して1つの場所からインポートを実行できます。

クラウドアクセス操作は、オンプレミスサイトやActive Directoryを参照しないため、どこからでもクラウドアクセス操作を実行できます。

これを行うには、2つの方法があります。

- 直接ファイル共有: 直接ファイル共有からインポート、マージ、または追加するには、どのマシンからクラウドアクセス操作を実行するかを決定する必要があります。
- `SiteMerging.yml`を使用したファイル共有参照: この方法では、サイトのプレフィックスセットの`SiteRootFolder`メンバーを使用し、エクスポート、インポート、マージ、または追加の際に誤ったフォルダーをターゲットにする可能性を減らします。

中央ファイル共有方法を使用しない場合は、個々のDelivery Controllerからインポート、マージ、または追加を実行します。クラウドに移行する各Delivery Controllerで`SiteMerging.yml`ファイルを作成してレプリケートします。デフォルトの場所は`%HOMEPATH%\Documents\Citrix\AutoConfig`です。正しいサイトプレフィックスを選択するには、`-SiteName`パラメーターを指定する必要があります。

直接ファイル共有

エクスポート、インポート、マージ、および新規/追加操作では、デフォルトフォルダーである *%HOMEPATH%\Documents\Citrix\AutoConfig* 以外のフォルダーをターゲットまたはソースとするパラメーターが提供されます。次の例では、管理者がすでにアクセス権を持ち、必要に応じて資格情報を提供している`\\share.central.net`にある中央ファイル共有を使用します。

エクスポートをサイト固有のフォルダーにターゲット設定するには、`-TargetFolder` パラメーターを使用します。

東デリバリーコントローラー™ から:

```
mkdir \\share.central.net\AutoConfig\SiteEast
```

```
Export-CvadAcToFile –TargetFolder \\share.central.net\AutoConfig\SiteEast
```

ウェスト デリバリーコントローラー から:

```
mkdir \\share.central.net\AutoConfig\SiteWest
```

```
Export-CvadAcToFile –TargetFolder \\share.central.net\AutoConfig\SiteWest
```

エクスポートが完了したら、`CustomerInfo.yml`と`SiteMerging.yml`ファイルを作成し、`\\share.central.net\AutoConfig`に配置します。

> **注:**
>
> この直接ファイル共有参照方法を使用する場合、`SitePrefixes.yml`を作成する際に`SiteRootFolder`パラメーターを使用しないでください。

> 直接ファイル共有からインポート、マージ、または追加するには、どのマシンからクラウドアクセス操作を実行するかを決定する必要があります。オプションは次のとおりです。

- ツールがすでにインストールされているオンプレミスの Delivery Controller のいずれか。
- ファイル共有をホストしているマシン。
- 別のマシン。

クラウドにアクセスするマシンには、Automated Configurationがインストールされている必要があります。オンプレミスのPowerShell SDK、Delivery Controller、Active Directoryのいずれも使用されないため、クラウドアクセス実行要件はエクスポート要件よりも単純です。

イーストデリバリーコントローラーをクラウドにマージするには:

```
Merge-CvadAcToSite –SiteName East –SourceFolder \
\share.central.net\AutoConfig\SiteEast -CustomerInfoFileSpec \
\share.central.net\AutoConfig\CustomerInfo.yml
```

ウェストデリバリーコントローラーをクラウドにマージするには:

`Merge-CvadAcToSite –SiteName West –SourceFolder \`
`\share.central.net\AutoConfig\SiteWest -CustomerInfoFileSpec \`
`\share.central.net\AutoConfig\CustomerInfo.yml`

以下は、前の例で使用されているサンプル`SitePrefixes.yml`ファイルです。

```
East:

  SiteRootFolder: "" # Important: leave this empty

  AdminScopePrefix: "East_"

  AdminRolePrefix: "East_"

  ApplicationAdminPrefix: "East_"

  ApplicationFolderPrefix: "" # Note that a new parent root folder is used
instead

  ApplicationFolderRoot: "East"

  ApplicationGroupPrefix: "East_"

  ApplicationUserPrefix: "East_"

  DeliveryGroupPrefix: "East_"

  GroupPolicyPrefix: "East_"

  HostConnectionPrefix: "East_"

  MachineCatalogPrefix: "East_"

  StoreFrontPrefix: "East_"

  TagPrefix: "East_"

  AdminScopeSuffix: "_east"

  AdminRoleSuffix: "_east"

  ApplicationAdminSuffix: "_east"
```

```
  ApplicationFolderSuffix: "_east"

  ApplicationGroupSuffix: "_east"

  ApplicationUserSuffix: "_east"

  DeliveryGroupSuffix: "_east"

  GroupPolicySuffix: "_east"

  HostConnectionSuffix: "_east"

  MachineCatalogSuffix: "_east"

  StoreFrontSuffix: "_east"

  TagSuffix: "_east"

West:

  SiteRootFolder: "" # Important: leave this empty

  AdminScopePrefix: "Western "

  AdminRolePrefix: "Western "

  ApplicationAdminPrefix: "Western "

  ApplicationFolderPrefix: "" # Note that a new parent root folder is used
instead

  ApplicationFolderRoot: "Western"

  ApplicationGroupPrefix: "Western "

  ApplicationUserPrefix: "Western "

  DeliveryGroupPrefix: "Western "

  GroupPolicyPrefix: "Western "

  HostConnectionPrefix: "Western "
```

```
MachineCatalogPrefix: "Western "

StoreFrontPrefix: "Western "

TagPrefix: "Western "

AdminScopeSuffix: ""

AdminRoleSuffix: ""

ApplicationAdminSuffix: ""

ApplicationFolderSuffix: ""

ApplicationGroupSuffix: ""

ApplicationUserSuffix: ""

DeliveryGroupSuffix: ""

GroupPolicySuffix: ""

HostConnectionSuffix: ""

MachineCatalogSuffix: ""

StoreFrontSuffix: ""

TagSuffix: ""
```

SITEMERGING.YML を使用したファイル共有参照

この方法では、サイトのプレフィックスセットの`SiteRootFolder`メンバーを使用します。直接ファイル共有方法よりも複雑ですが、この方法により、エクスポート、インポート、マージ、または追加時に誤ったフォルダーをターゲットにする可能性が低減されます。

まず、SiteMerging.yml ファイルで各サイトの`SiteRootFolder`を設定します。これは共有場所で実行する必要があります。

`New-CvadAcSiteMergingInfo –SiteName East –SiteRootFolder \`
`\share.central.net\AutoConfig\SiteEast -SitePrefixesFolder \`
`\share.central.net\AutoConfig`

```
New-CvadAcSiteMergingInfo –SiteName West –SiteRootFolder SiteWest
-SitePrefixesFolder \\share.central.net\AutoConfig
```

この例では、Eastは完全修飾フォルダー指定であり、Westは相対フォルダー指定です。

SiteMerging.yml ファイルを使用してエクスポートをサイト固有のフォルダーにターゲット設定するには:

イーストデリバリーコントローラーから:

```
mkdir \\share.central.net\AutoConfig\SiteEast
```

```
Export-CvadAcToFile -SiteName East -CustomerInfoFileSpec \
\share.central.net\AutoConfig\CustomerInfo.yml
```

ウェスト デリバリーコントローラーから：

```
mkdir \\share.central.net\AutoConfig\SiteWest
```

```
Export-CvadAcToFile -SiteName West -CustomerInfoFileSpec \
\share.central.net\AutoConfig\CustomerInfo.yml
```

エクスポートコマンドレットは、`CustomerInfo.yml` フォルダーの場所を使用して、`SiteMerging.yml` ファイルを見つけます。Eastの場合、`SiteRootFolder` は完全修飾されています。そのまま使用されます。Westの場合、`SiteRootFolder` は完全修飾されていません。これは、`CustomerInfo.yml` フォルダーの場所と組み合わされて、Westの完全修飾フォルダーの場所を取得します。

East Delivery Controller をクラウドにマージするには:

```
Merge-CvadAcToSite –SiteName East -CustomerInfoFileSpec \
\share.central.net\AutoConfig\CustomerInfo.yml
```

West Delivery Controller をクラウドにマージするには:

```
Merge-CvadAcToSite –SiteName West -CustomerInfoFileSpec \
\share.central.net\AutoConfig\CustomerInfo.yml
```

以下は、前の例で使用されたサンプル `SitePrefixes.yml` ファイルです。

```
East:

SiteRootFolder: "\\\\share.central.net\\AutoConfig\\SiteEast"
```

```
  AdminScopePrefix: "East_"

  AdminRolePrefix: "East_"

  ApplicationAdminPrefix: "East_"

  ApplicationFolderPrefix: "" # Note that a new parent root folder is used
instead

  ApplicationFolderRoot: "East"

  ApplicationGroupPrefix: "East_"

  ApplicationUserPrefix: "East_"

  DeliveryGroupPrefix: "East_"

  GroupPolicyPrefix: "East_"

  HostConnectionPrefix: "East_"

  MachineCatalogPrefix: "East_"

  StoreFrontPrefix: "East_"

  TagPrefix: "East_"

  AdminScopeSuffix: "_east"

  AdminRoleSuffix: "_east"

  ApplicationAdminSuffix: "_east"

  ApplicationFolderSuffix: "_east"

  ApplicationGroupSuffix: "_east"

  ApplicationUserSuffix: "_east"

  DeliveryGroupSuffix: "_east"

  GroupPolicySuffix: "_east"
```

```
  HostConnectionSuffix: "_east"

  MachineCatalogSuffix: "_east"

  StoreFrontSuffix: "_east"

  TagSuffix: "_east"

West:

  SiteRootFolder: "\\\\share.central.net\\AutoConfig\\SiteWest"

  AdminScopePrefix: "Western "

  AdminRolePrefix: "Western "

  ApplicationAdminPrefix: "Western "

  ApplicationFolderPrefix: "" # Note that a new parent root folder is used
instead

  ApplicationFolderRoot: "Western"

  ApplicationGroupPrefix: "Western "

  ApplicationUserPrefix: "Western "

  DeliveryGroupPrefix: "Western "

  GroupPolicyPrefix: "Western "

  HostConnectionPrefix: "Western "

  MachineCatalogPrefix: "Western "

  StoreFrontPrefix: "Western "

  TagPrefix: "Western "

  AdminScopeSuffix: ""

  AdminRoleSuffix: ""
```

```
ApplicationAdminSuffix: ""

ApplicationFolderSuffix: ""

ApplicationGroupSuffix: ""

ApplicationUserSuffix: ""

DeliveryGroupSuffix: ""

GroupPolicySuffix: ""

HostConnectionSuffix: ""

MachineCatalogSuffix: ""

StoreFrontSuffix: ""

TagSuffix: ""
```

中央ファイル共有方法が使用されておらず、個々のDelivery Controllerからインポート、マージ、または追加が行われる場合は、クラウドに移行される各Delivery Controllerで `SiteMerging.yml` ファイルを作成して複製します。デフォルトの場所は *%HOMEPATH%\Documents\Citrix\AutoConfig* です。正しいサイトプレフィックスを選択するには、`-SiteName` パラメーターを指定する必要があります。

サイトをマージする

Citrix®は、クラウド操作を段階的に実行し、次のクラウド操作を行う前に各結果を完全にレビューすることを推奨しています。たとえば、3つのサイトを単一のクラウドサイトにマージする場合：

1. 適切な `SiteName` 値を使用して、最初のサイトをクラウドにマージします。
2. Studioで結果を確認します。
3. 結果が正しくない場合は、問題とその原因を特定し、修正してからマージを再実行します。必要に応じて、クラウドコンポーネントを削除し、選択したコンポーネントとメンバーに `Remove-CvadAcFromSite` を使用して最初からやり直します。結果が正しい場合は、続行します。
4. 最初のマージが正しければ、2番目のサイトを単一のクラウドサイトにマージします。

5. 手順2と3を繰り返します。
6. 2番目のマージが正しければ、3番目のサイトを単一のクラウドサイトにマージします。
7. 手順2と3を繰り返します。
8. ユーザーの視点からリソースを確認し、ビューが目的の状態であることを確認します。

サイトプレフィックスを使用してコンポーネントを削除する

`Remove-CvadAcFromSite` コマンドレットの `-IncludeByName` パラメーターにプレフィックスを使用することで、単一サイトのコンポーネントを選択的に削除できます。次の例では、West Delivery Controller のデリバリーグループが正しくありません。West サイトのみのデリバリーグループを削除するには：

```
Remove-CvadAcFromSite -DeliveryGroups -IncludeByName “Western *”
```

すべてのWestコンポーネントを削除するには、次のコマンドレットを順番に実行します。

1. `Remove-CvadAcFromSite -GroupPolicies -IncludeByName “Western *”`
2. `Remove-CvadAcFromSite -Applications -IncludeByName “Western *”`
3. `Remove-CvadAcFromSite - ApplicationGroups -IncludeByName “Western *”`
4. `Remove-CvadAcFromSite -DeliveryGroups -IncludeByName “Western *”`
5. `Remove-CvadAcFromSite -MachineCatalogs -IncludeByName “Western *”`
6. `Remove-CvadAcFromSite -HostConnections -IncludeByName “Western *”`
7. `Remove-CvadAcFromSite -Tags -IncludeByName “Western *”`

東コンポーネントのグループポリシーを削除するには、次のサフィックスを使用します。

```
Remove-CvadAcFromSite -GroupPolicies -IncludeByName “*_east”
```

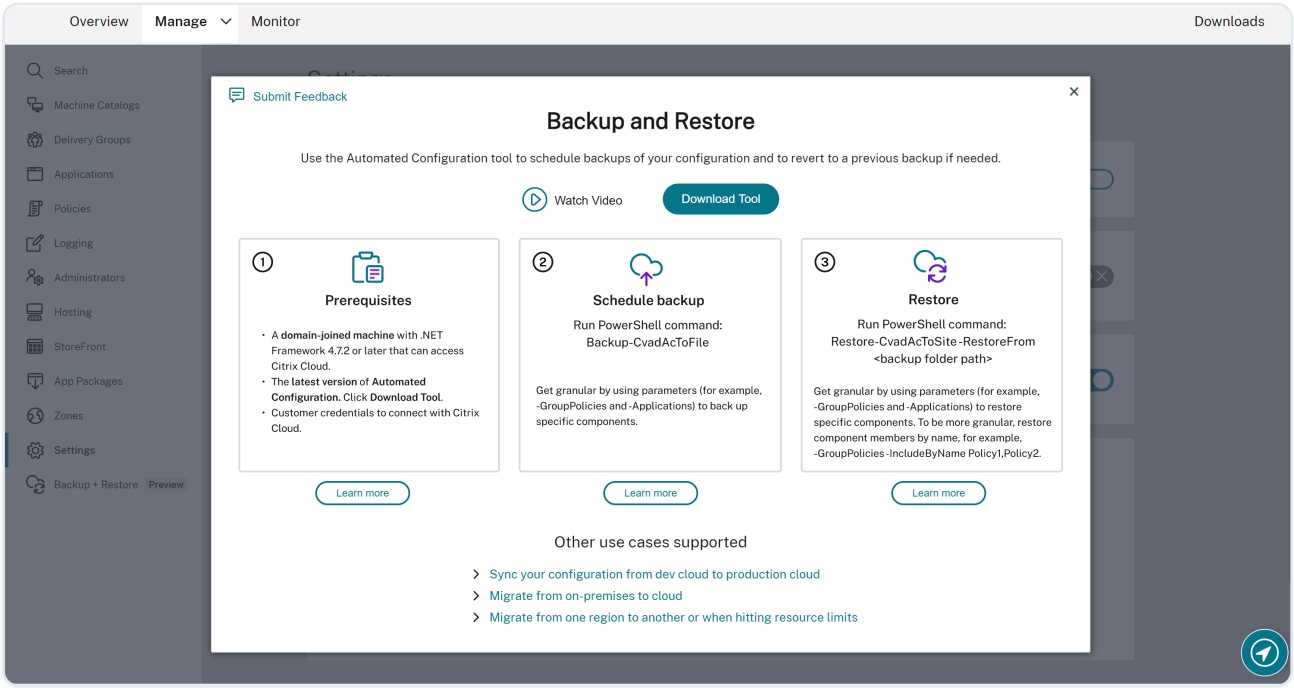
クラウドからクラウドへの移行

自動構成を使用すると、クラウド構成を別のクラウドサイトに移動したり、独自のクラウドサイトを復元したりする作業を自動化できます。

自動構成を使用すると、多くのユースケースを解決できます。

- テストまたはステージングから本番環境へのサイトの同期
- 構成のバックアップと復元
- リソース制限への到達
- あるリージョンから別のリージョンへの移行

Citrix Cloud™ の Studio で、Automated Configuration と、それがクラウドからクラウドへの構成の移行にどのように使用できるかについては、「バックアップと復元」ノードを参照してください。



構成を移行するための前提条件

構成をバックアップおよび復元するには、以下が必要です。

- Citrix DaaS™ がプロビジョニングされていること。
- Connector がインストールされているアクティブなリソースの場所。
- Citrix Cloud にアクセスするサイトへの接続が許可され、利用可能である必要があります。詳細については、「システムおよび接続要件」を参照してください。

> **注:**
>
> MCSは、Automated Configurationを使用してクラウドからバックアップすることはできません。

Citrix DaaS の構成をバックアップする

要件

Citrix DaaS の構成をバックアップする前に、次の操作を実行します。

1. `CustomerInfo.yml` ファイルに、顧客 ID、クライアント ID、および含まれているシークレットキー情報を入力します。顧客 ID、クライアント ID、およびシークレットキーの取得方法の詳細については、「顧客 ID、クライアント ID、およびシークレットキーを生成する」を参照してください。この情報を `CustomerInfo.yml` ファイルに追加する方法については、「顧客情報ファイルに入力する」を参照してください。

バックアップコマンドを実行するときは、`CustomerInfo.yml` にバックアップ元のソースサイト顧客の詳細が含まれている必要があります。

復元コマンドを実行するときは、`CustomerInfo.yml` に構成を復元する先の宛先サイト顧客の詳細が含まれている必要があります。

1. `ZoneMapping.yml` ファイルに、クラウド内のリソースの場所をマッピングする情報を入力します。ゾーンのマッピング方法の詳細については、「ゾーンマッピングファイルに入力する」を参照してください。
2. ホスト接続がある場合は、対応する情報を `CvadAcSecurity.yml` ファイルに入力する必要があります。「ホスト接続のセキュリティファイルを更新する」を参照してください。

Citrix DaaS 構成をバックアップする手順

1. Automated Configuration をインストールする。

> **注：**
>
> クラウドからクラウドへの移行の場合、Automated Configuration は、管理者が直接アクセスできるインターネットにアクセス可能なマシンにインストールできます。

2. **Auto Config** アイコンをダブルクリックします。PowerShell ウィンドウが表示されます。
3. バックアップを実行するには、次のコマンドを実行します。

```
Backup-CvadAcToFile
```

初めて任意のコマンドレットを実行すると、`.yml` 構成ファイルとログを含むエクスポートフォルダーが作成されます。フォルダーは `%HOMEPATH%\Documents\Citrix\AutoConfig` にあります。

エラーまたは例外が発生した場合は、ログファイルの **Fixups** セクションを参照してください。

Citrix DaaS に構成を復元する

1. **Auto Config**アイコンをダブルクリックします。PowerShellウィンドウが表示されます。
2. 復元を実行するには、次のコマンドを実行します。

```
Restore-CvadAcToSite -RestoreFolder <folder path of the backup files>
```

期待される状態と新しい現在の状態を検証します。

コマンドレットを実行すると、`.yml` 構成ファイルとログを含むエクスポートフォルダーが作成されます。フォルダーは *%HOMEPATH%\Documents\Citrix\AutoConfig* にあります。

エラーまたは例外が発生した場合は、ログファイルの **Fixups** セクションを参照してください。

バックアップと復元プロセスは、意図しないクラウドサイト構成の変更や破損から保護します。自動構成は変更が行われるたびにバックアップを作成しますが、このバックアップは変更前のクラウドサイト構成の状態を反映しています。自身を保護するには、クラウドサイト構成を定期的にバックアップし、安全な場所に保存する必要があります。望ましくない変更や破損が発生した場合、バックアップを使用して、きめ細かいレベルまたは完全なサイト構成レベルで変更や破損を修正できます。

きめ細かい移行

> **重要:**

> コンポーネントの移行順序の詳細については、「コンポーネントの移行順序」を参照してください。

すべてのコンポーネントを復元する

1つのコンポーネントを復元するには、1つ以上のコンポーネントパラメーターを選択します。

復元するには:

- 配信グループ全体とマシンカタログコンポーネント
- 完全なクラウドサイト構成

次の例に従ってください。

```
Restore-CvadAcToSite   -RestoreFolder   %HOMEPATH%
\Documents\Citrix\AutoConfig/Backup_yyyy_mm_dd_hh_mm_ss
```

コンポーネントメンバーを復元する

1つ以上のコンポーネントメンバーを復元するには、`IncludeByName` 機能を使用します。`Restore` コマンドレットは、選択した単一のコンポーネントとインクルージョンリストとともに `RestoreFolder` パラメーターを指定して呼び出されます。

バックアップから2つのグループポリシーを復元するには、次の例に従ってください。

```
Restore-CvadAcToSite   -RestoreFolder   %HOMEPATH%
\Documents\Citrix\AutoConfig/Backup_yyyy_mm_dd_hh_mm_ss
```

```
-GroupPolicies -IncludeByName   Policy1,Policy2
```

```
-DeliveryGroups -MachineCatalogs`
```

サイトをアクティブ化する

サイトのアクティブ化により、アクティブなサイトを制御し、リソースを管理できます。詳細については、「サイトをアクティブ化する」を参照してください。

クラウド構成をオンプレミスに移行する

この記事では、クラウド構成をバックアップし、オンプレミスサイトに移行する方法について説明します。

構成を移行するための前提条件

- 少なくとも1つの登録済みVDAを持つCitrix Virtual Apps and Desktops™オンプレミス環境。
- 以下のいずれかのバージョンで実行されているCitrix Virtual Apps and Desktopsオンプレミス環境：
  - 最新のLong-Term Service Release (LTSR) バージョン - 2402。
  - いずれかのCurrent Releases (CR) バージョン - 2308、2311。
- .Net 4.7.2以降のバージョンがインストールされたドメイン参加済みマシンで、Automated Configuration tool (ACT) コマンドを実行します。

- Citrix PowerShell SDKがインストールされたマシン。PowerShell SDKはCitrix Delivery Controller™のインストールファイルに含まれています。

> **注：**
>
> - 別のマシンでACTを実行する場合、そのマシンはドメインに参加している必要があり、Studioには適切なPowerShellスナップインがインストールされている必要があります。インストーラーを入手するには、Citrix Virtual Apps and DesktopsダウンロードWebサイトにアクセスしてください。
> - オンプレミスサイトでは、ACTをDelivery Controllerにインストールすることをお勧めします。ACTはデスクトップアイコンから起動できます。
> - ACTを標準のPowershellウィンドウから使用する場合は、次のコマンドを実行する必要があります。 `Import-Module Citrix.AutoConfig.Commands`

> ACTはシステムPowerShellパスの一部ではないため、明示的にインポートする必要があります

主な手順

クラウド構成をオンプレミスに移行するには、以下の手順に従ってください。

1. クラウド構成のバックアップ
2. YML ファイルの変更
3. 構成をオンプレミスにインポート

クラウド構成のバックアップ

1. **Automated Configuration** をインストールします。
2. **Auto Config** アイコンをダブルクリックします。PowerShell ウィンドウが表示されます。
3. **CustomerInfo.yml** ファイルを作成するには、`New-CvadAcCustomerInfoFile` を実行します。詳細については、「顧客情報ファイルの入力」を参照してください。
4. クラウド構成のバックアップを作成するには、コマンド `Backup-CvadAcToFile` を実行します。

> **注：**

- 任意のコマンドレットを初めて実行すると、.yml 構成ファイルとログを含むエクスポートフォルダーが作成されます。フォルダーは `%HOMEPATH%\Documents\Citrix\AutoConfig` にあります。
- エラーまたは例外が発生した場合は、ログファイルの **Fixups** セクションを参照してください。
- Backup-CvadToFile は、パラメーター `IncludeByName` または `ExcludeByName` をサポートしていません。

重要：

Citrix は、すべてのコンポーネントをまとめてバックアップすることをお勧めします。

YMLファイルの変更

次の表に記載されているオンプレミスの詳細を含めるように、`%HOMEPATH%\Documents\Citrix\AutoConfig` にある `.yml` ファイルを変更します。

YMLファイル	パラメーター	説明	例
CustomerInfo.yml	環境	環境をOnPremに変更します。環境パラメーターの値は大文字と小文字を区別します。	
ZoneMapping.yml	DaaS:CVAD	クラウドのリソースロケーションをオンプレミスゾーンにマッピングします。	old:new zones の形式である必要があります
CvadAcSecurity.yml	ハイパーバイザー: 接続タイプ: ‘ ‘ ユーザー名: ‘ ’ パスワード: ‘ ‘	ハイパーバイザーのユーザー名とパスワードを追加します。	ハイパーバイザーがXenServerの場合、 XenServer: ConnectionType: ‘XenServer’ Username: ‘root’ Password: ‘ ‘

オンプレミスに構成をインポートする

1. 要件に基づいて、オンプレミスサイトで以下のいずれかのコマンドを実行します。

   a. `Merge-CvadAcToSite` - オンプレミスサイトが稼働中で、そこにクラウド構成をマージしたい場合。

   b. `Import-CvadAcToSite -Environment OnPrem` - オンプレミス構成が利用できず、クラウド構成をインポートして新しいものを作成する場合。

> **重要:**
>
> Citrixは、競合を避けるため、一度に1つのコンポーネントをインポートすることを推奨します。

オンプレミス構成をオンプレミスサイトに移行する

この記事では、Automated Configuration Tool (ACT) を使用して、オンプレミス構成をあるオンプレミスサイトから別のオンプレミスサイトに移行する手順について説明します。

要件

- 両方のオンプレミスサイトが同じドメインに参加している必要があります。
- Citrix Virtual Apps and Desktops™ バージョン 2305 以降を使用してください。

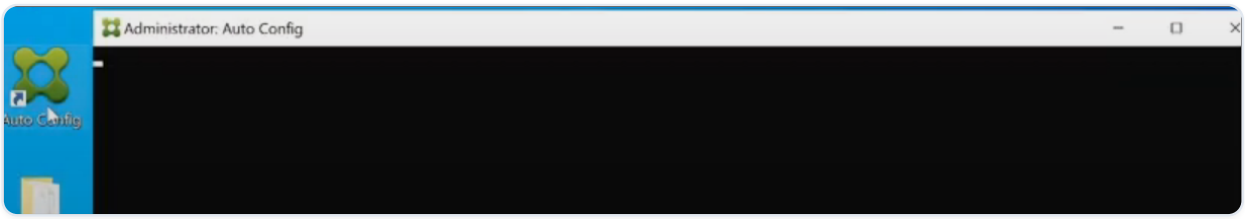
手順

1. Automated Configuration Tool をダウンロードし、システム要件を確認します。Automated Configuration のダウンロード を参照してください。
2. ACT を開き、次のコマンドを使用してオンプレミスサイトをエクスポートします。

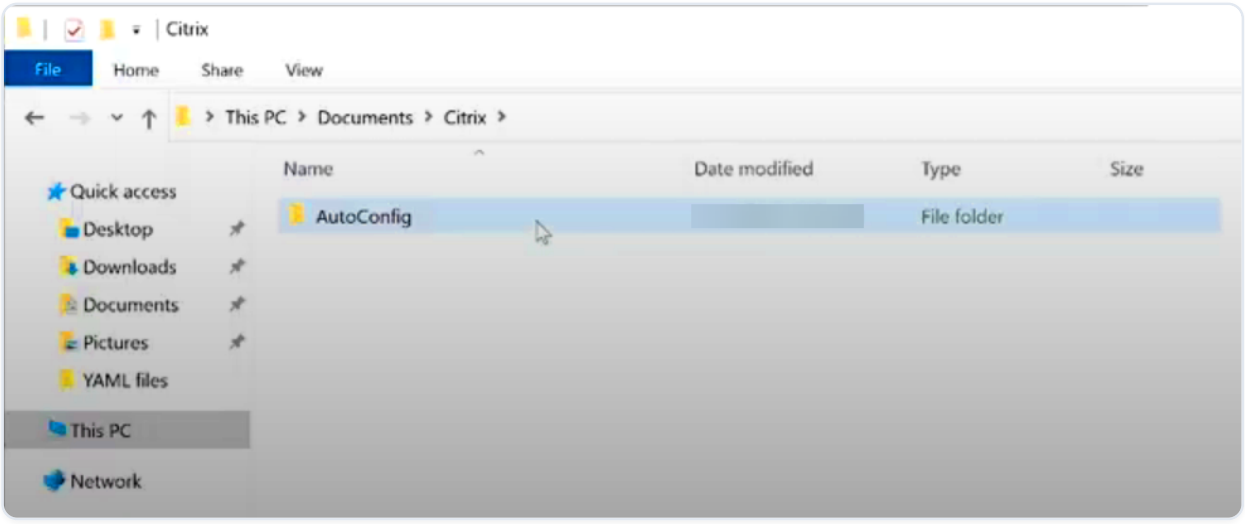
   ```
   Export-CvadAcToFile
   ```

   移行でサポートされているコンポーネントのリストについては、サポートされている移行オブジェクト を参照してください。エクスポートの手順については、オンプレミス構成のエクスポート を参照してください。親フォルダー `%HOMEPATH%\\Documents\\Citrix\\AutoConfig` には、常に最新のエクスポートからのエクスポートされたファイルが含まれています。

3. ターゲットサイトで ACT を起動します。`%HOMEPATH%\\Documents\\Citrix` に `AutoConfig` フォルダーが作成されていることを確認してください。



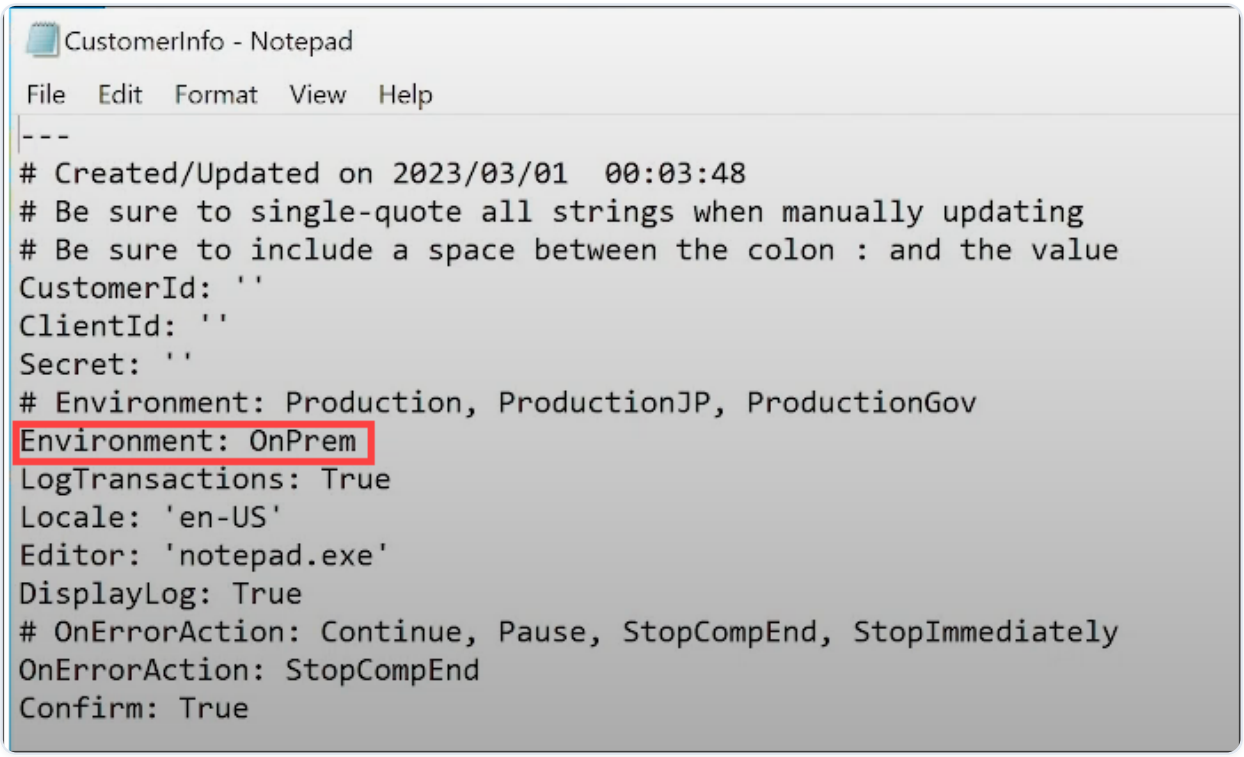
4. ソースサイトの **Export** フォルダーから `.yml` ファイルをターゲットサイトの `%HOMEPATH%\\Documents\\Citrix\\AutoConfig` フォルダーにコピーします。



5. `Set-CvadAcCustomerInfoFile` コマンドを使用して、作業している環境を指定します。例:

```
Set-CvadAcCustomerInfoFile -Environment OnPrem
```

このコマンドは、**CustomerInfo** ファイルを環境で更新します。



6. 次のコマンドを使用して構成ファイルを移行します。

```
Import-CvadAcToFile
```

`AutoConfig` フォルダー以外のフォルダーからインポートする場合は、次を実行します。

```
Import-CvadAcToFile -Sourcefolder PATH
```

注:

ホスト接続を移行する場合は、各ホストタイプの接続情報で `CvadAcSecurity.yml` ファイルを更新してください。「ホスト接続のセキュリティファイルを更新する」を参照してください。

エラーまたは例外が発生した場合は、ログファイルの「Fixups」セクションを参照してください。

7. Web Studioを使用して、構成がターゲットサイトに移行されていることを確認します。

移行用の自動構成ツール コマンドレット

このページには、移行ユースケース向けにツールでサポートされているすべてのコマンドレットとパラメーターが一覧表示されています。

すべてのコマンドレットは、次のいずれかの型のパラメーターを受け取ります。

- 文字列
- 文字列のリスト
- ブール値: `$true` または `$false`
- SwitchParameter: パラメーターが存在する場合は `$true` を意味し、パラメーターが存在しない場合は `$false` を意味します。

注:

SwitchParameter は真偽の選択に推奨される方法ですが、レガシーの問題により、ツールでは引き続きブール値が使用されています。

次の表は、すべてのコマンドレットの概要です。各コマンドレットがサポートするパラメータについては、各セクションを参照してください。

カテゴリ	コマンドレット	説明
オンプレミスからクラウドへの移行	`Export-CvadAcToFile`	オンプレミスファイルをYAMLファイルにエクスポートします。
	`Import-CvadAcToSite`	YAMLファイルをクラウドにインポートします。作成、更新、削除の操作をサポートします。
	`Merge-CvadAcToSite`	YAMLファイルをクラウドにインポートします。作成および更新の操作をサポートします。
	`New-CvadAcToSite`	YAMLファイルをクラウドにインポートします。作成およ

カテゴリ	コマンドレット	説明
		び更新の操作をサポートします。
	`Sync-CvadAcToSite`	1つのステップでエクスポートとインポートを行います。
	きめ細かな移行 コンポーネントの場合は、上記のコマンドでパラメータを使用します。例: `MachineCatalogs`、`Tags`。コンポーネント名の場合は、上記のコマンドでパラメータを使用します。例: `IncludeByName`、`ExcludeByName`。	コンポーネントまたはコンポーネント名のみを選択的に移行する
クラウドからクラウドへのコマンドレット	`Backup-CvadAcToFile`	クラウドサイトからすべての構成をバックアップします。
	`Restore-CvadAcToSite`	バックアップYAMLファイルをクラウドサイトに復元します。このクラウドサイトは、ソースクラウドサイトと同じでも異なっていてもかまいません。
	`Remove-CvadAcFromSite`	クラウドからコンポーネントメンバーを削除します。
	きめ細かな移行 コンポーネントの場合は、上記のコマンドでパラメーターを使用します。例: `MachineCatalogs`、`Tags`。コンポーネント名の場合は、上記のコマンドでパラメーターを使用します。例: `IncludeByName`、`ExcludeByName`。	コンポーネントまたはコンポーネント名のみを選択的に移行する

カテゴリ	コマンドレット	説明
その他の基本コマンドレット	`Compare-CvadAcToSite`	オンプレミスの.ymlファイルをクラウド構成と比較します。
前提条件関連のコマンドレット	`New-CvadAcCustomerInfoFile`	顧客情報ファイルを作成します。
	`Set-CvadAcCustomerInfoFile`	既存の顧客情報ファイルを更新します。
サポートおよびトラブルシューティングのコマンドレット	`New-CvadAcZipInfoForSupport`	すべてのログファイルと.ymlファイルを1つのzipファイルに圧縮し、サポートのためにCitrix®に送信します。
	`Get-CvadAcStatus`	接続をテストし、すべての前提条件が満たされていることを確認するために使用します。バージョン番号、クラウドとの接続、コネクターステータスなど、ツールに関する情報を返します。
	`Test-CvadAcConnectionWithSite`	クラウドサイトとの接続をテストします。
	`Find-CvadAcConnector`	既存のコネクタを特定し、その実行状態を判断します。
	`Get-CvadAcCustomerSites`	すべての顧客サイトのリストを返します。
	`New-CvadAcTemplateToFile`	選択したコンポーネントのテンプレートファイルを作成します。
	`Show-CvadAcDocument`	このドキュメントをデフォルトのブラウザに表示します。
	`Find-CvadAcInFile`	ファイル内検索は、ワイルドカードを含む可能性のある1つ以上の名前に一致するメン

カテゴリ	コマンドレット	説明
		バーを探して、コンポーネントのYAMLファイルを検索します。
サイトアクティベーションコマンドレット(#site-activation-cmdlets)	`Set-CvadAcSiteActiveStateOnPrem`	オンプレミスサイトの状態をアクティブまたは非アクティブのいずれかに設定します。
	`Set-CvadAcSiteActiveStateCloud`	クラウドサイトの状態をアクティブまたは非アクティブのいずれかに設定します。
複数のオンプレミスサイトをマージするコマンドレット(#merging-multiple-on-premises-sites-cmdlets)	`New-CvadAcSiteMergingInfo`	サイトマージのプレフィックス/サフィックス情報セットを作成します。
	`Set-CvadAcSiteMergingInfo`	既存のサイトマージのプレフィックス/サフィックス情報セットを更新します。
	`Remove-CvadAcSiteMergingInfo`	既存のサイトマージのプレフィックス/サフィックス情報セットを削除します。

パラメーターとその使用方法の詳細については、「きめ細かな移行パラメーター」を参照してください。

基本的なコマンドレット

オンプレミスからクラウドへのコマンドレット

- `Export-CvadAcToFile` - オンプレミスファイルをYAMLファイルにエクスポートします。

  オンプレミス設定から構成をエクスポートします。これは、自動構成のデフォルトのエクスポート操作です。オンプレミスサイトの構成には変更は加えられません。エクスポートされたファイルは、一意の名前が付けられた **Export** サブフォルダー内のディレクトリ *%HOMEPATH%\Documents\Citrix\AutoConfig* に配置されます。フォルダー *%HOMEPATH%\Documents\Citrix\AutoConfig* には、常に最新のエクスポートされたオンプレミスサイト構成が含まれています。

  パラメーター:

名前	説明	必須ですか?	タイプ
コンポーネントによる移行	「コンポーネントによる移行」を参照してください。		SwitchParameters
オブジェクト名によるフィルタリング	「オブジェクト名によるフィルタリング」を参照してください(#filtering-by-object-names)		文字列のリスト
`TargetFolder`	エクスポート先のフォルダーを指定します。		文字列
`Locale`	エクスポート可能な人間が判読できるテキストの言語を指定します。		文字列
`Quiet`	コンソールへのログ記録を抑制します。		SwitchParameter
`AdminAddress`	エクスポートがDelivery Controllerで実行されていない場合に、Delivery ControllerのDNSまたはIPアドレスを指定します。		文字列
`CheckUserAndMachines`	ユーザーとマシンがActive Directoryに存在するかどうかを確認します。Active Directoryに存在しないユーザーとマシンは、インポートの失敗につながる可能性があります。		`$true` または `$false`

名前	説明	必須ですか?	タイプ
`ZipResults`	バックアップされたYAMLファイルを単一のzipファイルに圧縮します。このファイルは、バックアップされたYAMLファイルと同じフォルダーにあり、フォルダーと同じ名前になります。		SwitchParameter

戻り値:

- Cmdletの戻り値を参照してください。

データをクラウドにインポートする方法は3つあります。特定のコマンドレットを実行すると、クラウドサイトで次の3つのアクションの組み合わせのいずれかが発生する可能性があります。

- 追加、更新、および削除
- 追加と更新のみ
- 追加のみ

コマンドレット	追加	更新	削除
インポート	X	X	X
マージ	X	X	
新規	X		

- `Import-CvadAcToSite` - YAMLファイルをクラウドにインポートします。作成、更新、削除操作をサポートします。

  すべてのオンプレミスファイルをクラウドにインポートします。このコマンドは、クラウドの最終状態がオンプレミスの状態と同一であることを保証します。このオプションは、クラウドに存在する変更をすべて削除します。インポートされたサイト構成ファイルは、*%HOMEPATH%\Documents\Citrix\AutoConfig* から取得されます。*注意して使用してください。*

パラメーター:

名前	説明	必須ですか？	タイプ
コンポーネントによる移行	コンポーネントによる移行を参照してください。		SwitchParameters
オブジェクト名によるフィルタリング	オブジェクト名によるフィルタリングを参照してください。		文字列のリスト
クラウドアクセスパラメータ	クラウドアクセスパラメーターを参照してください。		SwitchParameters
`SourceFolder`	*%HOMEPATH%\Documents\Citrix\AutoConfig* の代替ルートフォルダーを識別します。		文字列
`Locale`	エクスポート可能な人間が判読できるテキストの言語を指定します。		文字列
`Quiet`	コンソールへのログ記録を抑制します。		SwitchParameter
`DisplayLog`	コマンドレットの完了時にログファイルを表示します。ログ表示を抑制するには、`$false` に設定します。		`$true` または `$false`
`Merge`	`$true` に設定すると、クラウドサイトにコンポーネントのみを追加します。コンポーネントは削除されません。コン		`$true` または `$false`

名前	説明	必須ですか？	タイプ
	ポーネントを削除するには、`$false`に設定します。		
`AddOnly`	`$true`に設定すると、新しいコンポーネントのみを追加し、既存のコンポーネントを更新または削除しません。更新と削除を許可するには、`$false`に設定します。このパラメーターが`$true`の場合、`Merge`は無視されます。		`$true`または`$false`
`MergePolicies`	ポリシー設定とフィルターをマージします。マージは、インポートされるポリシーがクラウドDDCに既に存在する場合にのみ行われます。ポリシーをマージした結果、クラウドDDCポリシーには、既存の設定とフィルターに加えて、インポートされる新しい設定とフィルターが含まれます。設定とフィルターの競合が発生した場合、インポートされた値が優先されることに注意してください。		SwitchParameter
`OnErrorAction`	「OnErrorAction parameter」を参照		文字列

名前	説明	必須ですか？	タイプ
	してください(/ja-jp/citrix-virtual-apps-desktops/2503/upgrade-migrate/auto-config-troubleshoot#onerroraction-parameter)。		

戻り値:

- 「Cmdlet return values」を参照してください(#cmdlet-return-values)

- `Restore-CvadAcToSite` - バックアップされたYAMLファイルをクラウドサイトに復元します。このクラウドサイトは、ソースクラウドサイトと同じでも異なっていてもかまいません。

  オンプレミスファイルをクラウドにマージしますが、クラウドまたはオンプレミスサイトのコンポーネントを削除することは*ありません*。これにより、クラウドで既に行われた変更が保持されます。同じ名前のコンポーネントがCitrix Cloudに存在する場合、このコマンドはそのコンポーネントを変更できます。これは、自動構成のデフォルトのインポート操作です。マージされたサイト構成ファイルは、*%HOMEPATH%\Documents\Citrix\AutoConfig* から取得されます。

  パラメータ:

名前	説明	必須?	タイプ
コンポーネントによる移行	「Migrate by components」を参照してください(#migrate-by-components)。		SwitchParameters
オブジェクト名によるフィルタリング	「オブジェクト名によるフィルタリング」を参照してください(#filtering-by-object-names)。		文字列のリスト

名前	説明	必須?	タイプ
クラウドアクセスパラメーター	「クラウドアクセスパラメーター」を参照してください (#cloud-accessing-parameters)。		SwitchParameters
`SourceFolder`	*%HOMEPATH%\Documents\Citrix\AutoConfig* の代替ルートフォルダーを識別します。		文字列
`Locale`	エクスポート可能な人間が判読できるテキストの言語を指定します。		文字列
`Quiet`	コンソールへのログ記録を抑制します。		スイッチパラメーター
`DisplayLog`	コマンドレットの完了時にログファイルを表示します。ログ表示を抑制するには `$false` に設定します。		`$true` または `$false`
`Merge`	`$true` に設定すると、クラウドサイトにコンポーネントのみを追加します。コンポーネントは削除されません。コンポーネントを削除するには `$false` に設定します。		`$true` または `$false`
`AddOnly`	`$true` に設定すると、新しいコンポーネントのみを追加し、既存のコンポー		`$true` または `$false`

名前	説明	必須?	タイプ
	ネントを更新または削除しません。更新と削除を許可するには `$false` に設定します。このパラメーターが `$true` の場合、 `Merge` は無視されます。		
`MergePolicies`	ポリシー設定とフィルターをマージします。マージは、インポートされるポリシーがクラウドDDCに既に存在する場合にのみ行われます。ポリシーをマージした結果、クラウドDDCポリシーには、既に持っていた設定とフィルターに加えて、インポートされる新しい設定とフィルターが含まれます。設定とフィルターの競合が発生した場合、インポートされた値が優先されることに注意してください。		スイッチパラメーター
`OnErrorAction`	OnErrorAction パラメーターを参照してください。		文字列

戻り値:

- コマンドレットの戻り値を参照してください

- `New-CvadAcToSite` - YAMLファイルをクラウドにインポートします。作成および更新操作をサポートします。

オンプレミスサイト構成をクラウドにインポートしますが、新しいコンポーネントのみを追加します。既存のクラウドサイトコンポーネントは更新も削除もされません。既存のクラウドサイトコンポーネントを変更しないままにする必要がある場合は、このコマンドを使用してください。

パラメーター:

名前	説明	必須?	タイプ
コンポーネントによる移行	コンポーネントによる移行を参照してください。		SwitchParameters
オブジェクト名によるフィルタリング	オブジェクト名によるフィルタリングを参照してください。		文字列のリスト
クラウドアクセスパラメータ	クラウドアクセスパラメータを参照してください。		SwitchParameters
`SourceFolder`	*%HOMEPATH%\Documents\Citrix\AutoConfig* の代替ルートフォルダーを識別します。		文字列
`Locale`	エクスポート可能な人間が判読できるテキストの言語を指定します。		文字列
`Quiet`	コンソールへのログ記録を抑制します。		SwitchParameter
`DisplayLog`	コマンドレットの完了時にログファイルを表示します。ログ表示を抑制するには、`$false`に設定します。		`$true` または `$false`

名前	説明	必須?	タイプ
`OnErrorAction`	を参照してください(/ja-jp/citrix-virtual-apps-desktops/2503/upgrade-migrate/auto-config-troubleshoot#onerroraction-parameter)。		文字列

戻り値:

- を参照してください(#cmdlet-return-values)

- `Sync-CvadAcToSite` - 1つのステップでエクスポートとインポートを実行します。

  同期は、1つのステップでエクスポートとインポートの両方を実行します。`SourceTargetFolder` パラメーターを使用して、エクスポート/インポートの宛先フォルダーを指定します。

  パラメーター:

名前	説明	必須ですか？	種類
コンポーネントごとに移行	を参照してください(#migrate-by-components)		SwitchParameters
オブジェクト名によるフィルタリング	オブジェクト名によるフィルタリングを参照してください。		文字列のリスト
クラウドアクセスパラメータ	クラウドアクセスパラメータを参照してください。		SwitchParameters
`SourceTargetFolder`	エクスポート/インポートの保存先フォルダを指定します。		文字列
`Locale`	エクスポート可能な人間が判読できるテ		文字列

名前	説明	必須ですか？	種類
	キストの言語を指定します。		
`AdminAddress`	エクスポートがデリバリーコントローラで実行されていない場合に、デリバリーコントローラのDNSまたはIPアドレスを指定します。		文字列
`Quiet`	コンソールへのログ記録を抑制します。		SwitchParameter
`DisplayLog`	コマンドレットの完了時にログファイルを表示します。ログ表示を抑制するには、`$false` に設定します。		`$true` または `$false`
`Merge`	`$true` に設定すると、クラウドサイトにコンポーネントを追加するだけです。コンポーネントは削除されません。コンポーネントを削除するには、`$false` に設定します。		`$true` または `$false`
`AddOnly`	`$true` に設定すると、新しいコンポーネントのみを追加し、既存のコンポーネントを更新または削除しません。更新と削除を許可するには、`$false` に設定します。このパラメーターが `$true`		`$true` または `$false`

名前	説明	必須ですか？	種類
	の場合、`Merge` は無視されます。		
`MergePolicies`	ポリシー設定とフィルターをマージします。マージは、インポートされるポリシーがクラウドDDCに既に存在する場合にのみ行われます。ポリシーをマージした結果、クラウドDDCポリシーには、既存の設定とフィルターに加えて、インポートされる新しい設定とフィルターが含まれます。設定とフィルターの競合が発生した場合、インポートされた値が優先されることに注意してください。		SwitchParameter

戻り値:

- 参照: コマンドレットの戻り値

クラウド間コマンドレット

- `Backup-CvadAcToFile` - クラウドサイトからすべての構成をバックアップします。

  クラウド構成を.ymlファイルにエクスポートします。このバックアップは、バックアップおよび復元プロセスで失われたコンポーネントを復元するために使用できます。

  パラメーター:

名前	説明	必須?	種類
コンポーネントによる移行	参照: コンポーネントによる移行		SwitchParameters
クラウドアクセスパラメーター	を参照してください(#cloud-accessing-parameters)		SwitchParameters
`TargetFolder`	エクスポート先のフォルダーを指定します。		文字列
`Locale`	エクスポート可能な人間が判読できるテキストの言語を指定します。		文字列
`Quiet`	コンソールへのログ記録を抑制します。		SwitchParameter
`DisplayLog`	コマンドレットの完了時にログファイルを表示します。ログ表示を抑制するには、`$false` に設定します。		`$true` または `$false`
`ZipResults`	YAMLファイルを単一のzipファイルにバックアップして圧縮します。このファイルは、バックアップされたYAMLファイルと同じフォルダーにあり、フォルダーと同じ名前です。		SwitchParameter

戻り値:

- 「Cmdlet の戻り値」を参照してください(#cmdlet-return-values)

- `Restore-CvadAcToSite` - バックアップされたYAMLファイルをクラウドサイトに復元します。このクラウドサイトは、ソースクラウドサイトと同じでも異なっていてもかまいません。

  クラウドサイトを以前の構成に復元します。インポートされたファイルは、`-RestoreFolder` パラメーターを使用して指定されたフォルダーから取得されます。このパラメーターは、クラウドサイトに復元する.ymlファイルを含むフォルダーを識別します。これは、完全修飾フォルダー指定である必要があります。このコマンドレットは、以前の構成に戻すため、またはクラウドサイトをバックアップおよび復元するために使用できます。このコマンドは、クラウドサイトの追加、削除、更新を行うことができます。

  パラメーター:

名前	説明	必須?	種類
コンポーネントによる移行	「コンポーネントによる移行」を参照してください (#migrate-by-components)。		SwitchParameters
オブジェクト名によるフィルタリング	「オブジェクト名によるフィルタリング」を参照してください。		文字列のリスト
クラウドアクセスパラメーター	「クラウドアクセスパラメーター」を参照してください。		Switchパラメーター
`RestoreFolder`	クラウドサイトに復元する.ymlファイルを含むフォルダーを識別します。これは完全修飾フォルダー指定である必要があります。		文字列
`Locale`	エクスポート可能な人間が判読できるテキストの言語を指定します。		文字列

名前	説明	必須?	種類
`Quiet`	コンソールへのログ記録を抑制します。		Switchパラメーター
`DisplayLog`	コマンドレットの完了時にログファイルを表示します。ログ表示を抑制するには、`$false` に設定します。		`$true` または `$false`
`Merge`	`$true` に設定すると、クラウドサイトにコンポーネントのみを追加します。コンポーネントは削除されません。コンポーネントを削除するには、`$false` に設定します。		`$true` または `$false`
`AddOnly`	`$true` に設定すると、新しいコンポーネントのみを追加し、既存のコンポーネントを更新または削除しません。更新と削除を許可するには、`$false` に設定します。このパラメーターが `$true` の場合、`Merge` は無視されます。		`$true` または `$false`
`MergePolicies`	ポリシー設定とフィルターをマージします。マージは、インポートされるポリシーがクラウドDDCに既に存在する場合にのみ行われます。ポリシーを		SwitchParameter

名前	説明	必須?	種類
	マージした結果、クラウドDDCポリシーには、既存の設定とフィルターに加えて、インポートされる新しい設定とフィルターが含まれます。設定とフィルターの競合が発生した場合、インポートされた値が優先されることに注意してください。		
`OnErrorAction`	OnErrorAction パラメーター を参照してください。		文字列

戻り値:

- Cmdlet の戻り値を参照してください

- `Remove-CvadAcFromSite` – クラウドからコンポーネントメンバーを削除します。

  サイト全体をリセットしたり、コンポーネントからメンバーアイテムを削除したりできます（例：カタログのリストから1つのマシンカタログを削除する）。これは、`IncludeByName` パラメーターと組み合わせて使用すると、特定のメンバーを選択的に削除できます。

  パラメーター:

名前	説明	必須?	種類
コンポーネントによる移行	コンポーネントによる移行を参照してください		SwitchParameters
オブジェクト名によるフィルタリング	オブジェクト名によるフィルタリングを参照してください		文字列のリスト

名前	説明	必須?	種類
クラウドアクセスパラメーター	「クラウドアクセスパラメータ」を参照		スイッチパラメータ
`Quiet`	コンソールへのログ記録を抑制します。		スイッチパラメータ
`DisplayLog`	コマンドレットの完了時にログファイルを表示します。ログ表示を抑制するには、`$false`に設定します。		`$true`または`$false`

戻り値:

- 「コマンドレットの戻り値」を参照

その他の基本コマンドレット

- `Compare-CvadAcToSite` - オンプレミスの.ymlファイルをクラウド構成と比較し、`Import`、`Merge`、または`Restore`コマンドレットによって行われた変更のレポートを作成します。

  パラメータ:

名前	説明	必須ですか？	種類
コンポーネントによる移行	コンポーネントによる移行を参照してください。		SwitchParameters
オブジェクト名によるフィルタリング	オブジェクト名によるフィルタリングを参照してください。		文字列のリスト
クラウドアクセスパラメーター	クラウドアクセスパラメーターを参照してください。		SwitchParameters
`SourceFolder`	*%HOMEPATH%\Documents\Citrix\AutoConfig* の代替		文字列

名前	説明	必須ですか？	種類
	ルートフォルダーを識別します。		
`Locale`	エクスポート可能な人間が判読できるテキストの言語を指定します。		文字列
`Quiet`	コンソールへのログ出力を抑制します。		SwitchParameter
`DisplayLog`	コマンドレットの完了時にログファイルを表示します。ログ表示を抑制するには、`$false` に設定します。		`$true` または `$false`
`Merge`	`$true` に設定すると、クラウドサイトにコンポーネントを追加するだけです。コンポーネントは削除されません。コンポーネントを削除するには、`$false` に設定します。		`$true` または `$false`
`AddOnly`	`$true` に設定すると、新しいコンポーネントのみを追加し、既存のコンポーネントを更新または削除しません。更新と削除を許可するには、`$false` に設定します。このパラメーターが `$true` の場合、`Merge` は無視されます。		`$true` または `$false`

名前	説明	必須ですか？	種類
`OnErrorAction`	OnErrorAction パラメーターを参照してください。		文字列

戻り値:

- コマンドレットの戻り値を参照してください。

詳細な移行パラメーター

コンポーネント別に移行

以下のコンポーネントは、それらをサポートするコマンドレットで指定できます。コンポーネントパラメーターが指定されていない場合、`All`オプションが自動的に選択されます。エラーを回避するために、コンポーネントを以下の順序で移行することをお勧めします。

- `All`
- `Tags`
- `AdminRoles`
- `AdminScopes`
- `HostConnections`
- `MachineCatalogs`
- `StoreFronts`
- `DeliveryGroups`
- `ApplicationGroups`
- `ApplicationFolders`
- `Applications`
- `GroupPolicies`
- `UserZonePreference`

オブジェクト名によるフィルタリング

コンポーネント名による移行

`IncludeByName` および `ExcludeByName` パラメーターを使用すると、名前でコンポーネントメンバーをコマンドレットに含めたり除外したりできます。サポートされているコマンドレットで

は、一度に1つのコンポーネント（たとえば、デリバリーグループ）のみを選択できます。コンポーネントメンバーが両方の領域にある場合、除外は他のすべてのパラメーターを上書きし、除外されたコンポーネントとメンバー名を識別するエントリがログ修正リストに作成されます。

`IncludeByName` および `ExcludeByName` は、コンポーネントメンバー名のリストを受け取ります。任意の名前には、1つ以上のワイルドカードを含めることができます。2種類のワイルドカードがサポートされています。メンバー名に特殊文字が含まれている場合、コンポーネントメンバー名のリストは単一引用符で囲む必要があります。

- * 任意の数の文字に一致します
- ？1つの文字に一致します

`IncludeByName` および `ExcludeByName` は、各メンバーが明示的であるかワイルドカードを含むメンバーのリストを含むファイルを受け取ることもできます。ファイルの各行には1つのメンバーを含めることができます。メンバー名から先頭と末尾のスペースはトリミングされます。ファイル名の前には @ 記号を付け、単一引用符で囲む必要があります（@ が再解釈されないようにするためのPowerShellの要件）。複数のファイルを、メンバー名と混在させてリストすることもできます。

名前が `DgSite1` で始まり、`Home2` を含むすべてのデリバリーグループをマージする例は、次のように記述されます。

```
Merge-CvadAcToSite –DeliveryGroups –IncludeByName DgSite1*,*Home2*
```

デリバリーグループ名別

`ByDeliveryGroupName` は、アプリケーションおよびアプリケーショングループのデリバリーグループ名でフィルタリングします。このパラメータは常に、デリバリーグループの関連付けに基づいて含めるメンバーを識別するインクルージョンリストです。

`ByDeliveryGroupName` は、デリバリーグループ名のリストを受け取ります。任意の名前には、1つ以上のワイルドカードを含めることができます。2種類のワイルドカードがサポートされています。

- * は任意の数の文字に一致します
- ？は単一の文字に一致します

次の例では、`EastDg` で始まるすべてのデリバリーグループ名を参照するすべてのアプリケーションをマージします。

```
Merge-CvadAcToSite –Applications –ByDeliveryGroupName EastDg*
```

無効なものを除外

`ExcludeDisabled` は、無効になっているすべてのアプリケーションおよびアプリケーショングループをインポート操作から除外します。`ExcludeDisabled` の既定値は `false` であり、これはすべてのアプリケーションおよびアプリケーショングループが有効状態に関係なくインポートされることを意味します。

マシン名別

`ByMachineName` は、マシンカタログおよびデリバリーグループのマシン名でフィルタリングします。このパラメータは常に、マシン名の関連付けに基づいて含めるメンバーを識別するインクルージョンリストです。

`ByMachineName` は、任意の名前が1つ以上のワイルドカードを含むことができるマシン名のリストを受け取ります。2種類のワイルドカードがサポートされています。

- * は任意の数の文字に一致します
- ? は単一の文字に一致します

エクスポートまたはインポート時に `ByMachineName` を使用し、マシン名フィルターによってマシンカタログまたはデリバリーグループにマシンが存在しない場合、そのマシンカタログまたはデリバリーグループはエクスポートまたはインポートから除外されます。

> **注:**
>
> 任意のインポート型コマンドレットで `ByMachineName` を使用すると、`MergeMachines` が `$true` に設定されます。

マシンのマージ

`MergeMachines` が `$true` に設定されている場合、インポート操作はマシンをマシンカタログまたはデリバリーグループにのみ追加するように指示します。マシンは削除されないため、増分的な追加操作が可能です。

`MergeMachines` はデフォルトでfalseであり、これはマシンカタログまたはデリバリーグループの.ymlファイルに存在しないマシンは削除されることを意味します。`ByMachineName` が使用される場合、`MergeMachines` は `$true` に設定されますが、`MergeMachines` をfalseに設定することで上書きできます。

前提条件関連のコマンドレット

- `New-CvadAcCustomerInfoFile` - 顧客情報ファイルを作成します。デフォルトでは、顧客情報ファイルは *%HOMEPATH%\Documents\Citrix\AutoConfig* にあります。

  パラメータ:

名前	説明	必須？	タイプ
`CustomerId`	顧客ID。	x	文字列
`ClientId`	Citrix Cloud で作成された顧客のクライアント ID。このパラメーターを使用する場合は、CustomerId と Secret を指定する必要があります。	条件付き	文字列
`Secret`	Citrix Cloud で作成された顧客のシークレットキー。このパラメーターを使用する場合は、CustomerId と ClientId を指定する必要があります。	条件付き	文字列
`Environment`	Production、ProductionGov、またはProductionJP環境。		列挙
`LogFileName`	ログファイルプレフィックスをCitrixLogから別のものに変更します。		文字列
`AltRootUrl`	Citrixの指示の下でのみ使用してください。		文字列

名前	説明	必須？	タイプ
`StopOnError`	最初のエラーで操作を停止します。		`$true` または `$false`
`TargetFolder`	ルートフォルダとして、*%HOMEPATH%\Documents\Citrix\AutoConfig* の代わりに指定されたフォルダを使用します。		文字列
`Locale`	ツールが実行されているシステムから派生したロケールの代わりに、指定されたロケールを使用します。		文字列
`Editor`	各コマンドレットの完了時にログを表示するために、指定されたエディターを使用します。Notepad.exe がデフォルトのエディターです。このパラメーターには、エディターへの完全修飾ファイル指定を含める必要があり、エディターはログファイル指定を唯一のパラメーターとして受け取る必要があります。		文字列
`SecurityCsvFileSpec`	Citrix Identity and Access Managementからダウンロードした SecurityClient.csv		文字列

名前	説明	必須？	タイプ
	ファイルを指す完全修飾ファイル指定。このパラメータを使用する場合、CustomerIdを指定する必要があります。		

戻り値:

- コマンドレットの戻り値を参照

- `Set-CvadAcCustomerInfoFile` - 既存の顧客情報ファイルを更新します。コマンドレットで指定されたパラメータのみが変更されます。CustomerInfo.ymlファイル内の指定されていないすべてのパラメータ値は変更されません。

  パラメータ:

名前	説明	必須?	型
`CustomerId`	顧客ID。		文字列
`ClientId`	Citrix Cloudで作成された顧客のクライアントID。		文字列
`Secret`	Citrix Cloudで作成されたお客様のシークレットキー。		文字列
`Environment`	Production、ProductionGov、またはProductionJP環境。		列挙
`LogFileName`	ログファイルプレフィックスをCitrixLogから別のものに変更します。		文字列

名前	説明	必須?	型
`StopOnError`	最初のエラーで操作を停止します。		`$true` または `$false`
`TargetFolder`	*%HOMEPATH%\Documents\Citrix\AutoConfig* の代わりに、指定されたフォルダーをルートフォルダーとして使用します。		文字列
`Locale`	ツールが実行されているシステムから派生したロケールではなく、指定されたロケールを使用します。		文字列
`Editor`	各コマンドレットの完了時にログを表示するために、指定されたエディターを使用します。Notepad.exeがデフォルトのエディターです。このパラメーターには、エディターへの完全修飾ファイル指定を含める必要があり、エディターはログファイル指定を唯一のパラメーターとして受け取る必要があります。		文字列
`SecurityCsvFileSpec`	Citrix Identity and Access Managementからダウンロードした SecurityClient.csv		文字列

名前	説明	必須?	型
	ファイルを指す完全修飾ファイル指定。このパラメーターを使用する場合は、CustomerIdを指定する必要があります。		

戻り値:

- コマンドレットの戻り値を参照してください

前提条件関連のパラメーター

クラウドアクセスパラメーターとともに、前提条件関連のコマンドレットで以下のパラメーターを使用できます。

- `Environment` – 本番環境または本番Gov環境。
- `LogFileName` – ログファイルプレフィックスをCitrixLogから別のものに変更します。
- `StopOnError` – 最初のエラーで操作を停止します。
- `AlternateRootFolder` – *%HOMEPATH%\Documents\Citrix\AutoConfig* の代わりに、指定されたフォルダーをルートフォルダーとして使用します。
- `Locale` – ツールが実行されているシステムから派生したロケールの代わりに、指定されたロケールを使用します。
- `Editor` – 各コマンドレットの完了時にログを表示するために、指定されたエディターを使用します。Notepad.exe がデフォルトのエディターです。このパラメーターには、エディターへの完全修飾ファイル指定を含める必要があり、エディターはログファイル指定を唯一のパラメーターとして受け取る必要があります。

サポートおよびトラブルシューティングのコマンドレット

- `New-CvadAcZipInfoForSupport` - サポートのためにCitrixに送信するすべてのログファイルと.ymlファイルを1つのzipファイルに圧縮します。お客様の機密情報 (CustomerInfo.yml および CvadAcSecurity.yml) はzipに含まれません。Icon.ymlファイルもサイズが大きいため除外されます。zipファイルは *%HOMEPATH%\Documents\Citrix\AutoConfig* に配置され、日付とタイムスタンプに基づいて *CvadAcSupport_yyyy_mm_dd_hh_mm_ss.zip* という名前が付けられます。このzipファイルはバックアップとしても機能します。

パラメーター:

名前	説明	必須?	タイプ
`TargetFolder`	zipファイルを作成して保存するターゲットフォルダーを指定します。		文字列
`Quiet`	コンソールへのログ出力を抑制します。		SwitchParameter

戻り値:

- コマンドプロンプトに、zipファイル名と場所を含むzipファイルが表示されます。

- `Get-CvadAcStatus` - 接続をテストし、すべての前提条件が満たされていることを確認するために使用します。ツールに関する情報（バージョン番号、クラウドとの接続、コネクターステータスなど）を返します。

  パラメータ:

名前	説明	必須?	タイプ
クラウドアクセスパラメータ	クラウドアクセスパラメータを参照してください。		SwitchParameters
`SiteId`	接続先のサイトを識別します。		文字列
`AdminAddress`	これは、管理者のアクセスレベルを確認するために使用されるオンプレミスのDelivery ControllerのDNSまたはIPアドレスです。ツールがDelivery Controller上で実行されていない場合に必要です。		文字列

戻り値:

- 各項目の結果を表示します。

- `Test-CvadAcConnectionWithSite` – クラウドサイトとの接続をテストし、通信接続が機能していることを確認します。このコマンドレットは、クラウドアクセスパラメータまたはCustomerInfo.ymlファイルを使用して、顧客の接続情報を指定します。

  パラメーター:

名前	説明	必須?	タイプ
クラウドアクセスパラメーター	クラウドアクセスパラメーターを参照してください。		スイッチパラメーター
`Quiet`	コンソールへのログ記録を抑制します。		スイッチパラメーター

  戻り値:

  - テスト結果はコマンドラインに表示されます。

- `Find-CvadAcConnector` - 既存のコネクタを特定し、その実行状態を判断します。このコマンドレットは、CustomerInfo.yml ファイルまたは顧客IDパラメーターからの情報を使用して、顧客のコネクタを特定します。

  パラメーター:

名前	説明	必須?	タイプ
`CustomerInfoFileSpec`	デフォルトの場所と名前を上書きするための顧客情報ファイルを指すファイル指定。このパラメーターは、`CustomerId` パラメーターが指定されている場合は無視されます。		文字列

名前	説明	必須?	タイプ
`CustomerId`	顧客のID。このパラメーターは、CustomerInfo.yml ファイル内の同じ値を上書きします。		文字列

戻り値：

- 結果はコマンドラインに表示されます。

- `Get-CvadAcCustomerSites` - すべての顧客サイトのリストを返します。このコマンドレットは、クラウドアクセスパラメーターまたはCustomerInfo.ymlファイルを使用して、顧客の接続情報を指定します。

  パラメーター：

  - クラウドアクセスパラメーターを参照

  戻り値：

  - 見つかった顧客サイトIDのリストを表示します。

- `New-CvadAcTemplateToFile` – 選択したコンポーネントのテンプレートファイルを作成し、インポートファイルを手動で作成できるようにします。

  パラメーター：

名前	説明	必須？	タイプ
コンポーネントごとに移行	を参照してください (#migrate-by-components)		スイッチパラメーター
`TargetFolder`	エクスポート先のフォルダーを指定します。		文字列

  戻り値:

  - コマンドレットの戻り値を参照

- `Show-CvadAcDocument` - このドキュメントをデフォルトのブラウザーに表示します。

パラメーター:

- なし。

戻り値:

- このWebページをデフォルトのWebブラウザーに表示します。

- `Find-CvadAcInFile` - ファイル内検索は、ワイルドカードを含む1つ以上の名前に一致するメンバーを探して、コンポーネントのYAMLファイルを検索します。結果は、見つかったメンバーのレポートです。ファイル内検索は、一度に1つのコンポーネントしか検索できません。ファイル内検索は、現在のフォルダーおよびすべてのサブフォルダー内のすべてのYAMLファイルを検索します。検索するファイルの数を制限するには、`FindSourceFolder`を使用します。

  パラメーター:

名前	説明	必須?	種類
コンポーネントによる移行	コンポーネントによる移行を参照してください。注: `-All` の値は無効です。		SwitchParameters
`IncludeByName`	サイトのアクティブ状態をアクティブに設定する際に含めるデリバリーグループの名前を指定するリスト。名前に「*」と「?」のワイルドカードがサポートされています。		文字列のリスト
`Unique`	一意に見つかったメンバーのみを報告します。		SwitchParameter
`IncludeYaml`	メンバー固有のYAMLを含めます。		スイッチパラメーター
`FindSourceFolder`	検索を開始するフォルダー。		文字列

名前	説明	必須?	種類
`DisplayLog`	コマンドレットの完了時にログファイルを表示します。ログ表示を抑制するには、`$false` に設定します。		スイッチパラメーター
`Quiet`	コンソールへのログ記録を抑制します。		スイッチパラメーター

戻り値:

- 指定されたコンポーネントについて、検出されたメンバーを含むレポートを作成します。

サイトアクティベーションコマンドレット

サイトのアクティベーションとこれらのコマンドレットの使用方法の詳細については、「サイトのアクティベーション」を参照してください。

- `Set-CvadAcSiteActiveStateOnPrem` - オンプレミスサイトの状態をアクティブまたは非アクティブに設定します。

  パラメータ:

名前	説明	必須ですか？	タイプ
クラウドアクセスパラメータ	クラウドアクセスパラメータを参照してください		SwitchParameters
`SiteActive`	存在する場合、オンプレミスサイトをアクティブに設定し、すべてのデリバリーグループからメンテナンスモードを削除します。このパラメータが存在しない場合、すべてのデリバリーグループにメ		SwitchParameter

名前	説明	必須ですか？	タイプ
	ンテナンスモードが設定されます。		
`IncludeByName`	サイトのアクティブ状態をアクティブに設定する際に含めるデリバリーグループの名前を指定するリスト。名前に「*」と「?」のワイルドカードがサポートされています。		文字列のリスト
`ExcludeByName`	サイトのアクティブ状態をアクティブに設定する際に除外するデリバリーグループの名前を指定するリスト。名前に「*」と「?」のワイルドカードがサポートされています。		文字列のリスト
`Quiet`	コンソールへのログ記録を抑制します。		SwitchParameter
`DisplayLog`	コマンドレットの完了時にログファイルを表示します。ログ表示を抑制するには、`$false` に設定します。		`$true or $false`

戻り値:

- Cmdlet の戻り値 を参照してください。

- `Set-CvadAcSiteActiveStateCloud` - クラウドサイトの状態をアクティブまたは非アクティブのいずれかに設定します。

  パラメーター:

名前	説明	必須ですか？	タイプ
クラウドアクセスパラメーター	を参照してください (#cloud-accessing-parameters)		SwitchParameters
`SiteActive`	存在する場合、クラウドサイトをアクティブに設定し、すべてのデリバリーグループからメンテナンスモードを削除します。このパラメーターが存在しない場合、すべてのデリバリーグループでメンテナンスモードが設定されます。		SwitchParameter
`IncludeByName`	サイトのアクティブ状態をアクティブに設定する際に含めるデリバリーグループの名前を指定するリスト。名前に「*」と「?」のワイルドカードがサポートされています。		文字列のリスト
`ExcludeByName`	サイトのアクティブ状態をアクティブに設定する際に除外するデリバリーグループの名前を指定するリスト。名前に「*」と「?」のワイルドカードがサポートされています。		文字列のリスト
`Quiet`	コンソールへのログ出力を抑制します。		SwitchParameter

名前	説明	必須ですか？	タイプ
`DisplayLog`	コマンドレットの完了時にログファイルを表示します。ログ表示を抑制するには、`$false` に設定します。		`$true or $false`

戻り値:

- コマンドレットの戻り値を参照してください。

複数のオンプレミスサイトをマージするコマンドレット

サイトのマージとこれらのコマンドレットの使用方法の詳細については、複数のサイトを単一のサイトにマージするを参照してください。

- `New-CvadAcSiteMergingInfo` - サイトマージのプレフィックス/サフィックス情報セットを作成します。最初からすべてのプレフィックスまたはサフィックスを知っている必要はありません。これらは`Set-CvadAcSiteMergingInfo`で、またはSiteMerging.ymlファイルを手動で編集することで更新できます。 パラメーター:

名前	説明	必須ですか？	タイプ
`SiteName`	特定のサイトのプレフィックス/サフィックスのセットを識別するために使用される名前。実際のサイト名と一致してもよいし、一致しなくてもよい。	x	文字列
サイト統合パラメーター	サイト統合パラメーターを参照してください		SwitchParameters
`Quiet`	コンソールへのログ記録を抑制します。		SwitchParameter

戻り値:

- なし

- `Set-CvadAcSiteMergingInfo` - 既存のサイト統合プレフィックス/サフィックス情報セットを更新します。

  パラメーター:

名前	説明	必須？	型
`SiteName`	特定のサイトのプレフィックス/サフィックスのセットを識別するために使用される名前。実際のサイト名と一致してもよいが、必須ではない。	x	文字列
サイト統合パラメーター	を参照してください (#site-merging-parameters)		SwitchParameters
`Quiet`	コンソールへのログ記録を抑制します。		SwitchParameter

  戻り値:

  - なし

- `Remove-CvadAcSiteMergingInfo` - 既存のサイト統合プレフィックス/サフィックス情報セットを削除します。

  パラメーター:

  - `SiteName` – サイトのプレフィックスとサフィックスのセットを識別します。これは文字列であり、必須です。

  戻り値:

  - なし

サイト統合パラメーター

サイト統合コマンドレットの実行時に、次のパラメーターを使用できます。リストされているすべてのパラメーターは文字列です。

- `SiteName` – 特定のサイトのプレフィックス/サフィックスのセットを識別するために使用される名前。実際のサイト名と一致してもかまいませんが、一致する必要はありません。SiteName は必須パラメーターです。
- `AdminScopedPrefix` – 管理者スコープに適用するプレフィックス。
- `ApplicationPrefix` - アプリケーションに適用するプレフィックス。
- `ApplicationFolderPrefix` – アプリケーションフォルダーに適用するプレフィックス。`ApplicationFolderPrefix` は `ApplicationFolderRoot` と組み合わせることができます。
- `ApplicationFolderRoot` – アプリケーションフォルダーの新しいルートフォルダー。これにより、追加のフォルダー階層が作成されます。`ApplicationFolderRoot` は `ApplicationFolderPrefix` と組み合わせることができます。
- `ApplicationGroupPrefix` – アプリケーショングループのプレフィックス。
- `ApplicationUserPrefix` – ユーザーに表示されるアプリケーション名に適用するプレフィックス。
- `ApplicationAdminPrefix` – 管理者に表示されるアプリケーション名に適用するプレフィックス。
- `DeliveryGroupPrefix` – デリバリーグループに適用するプレフィックス。
- `GroupPolicyPrefix` – ポリシー名に適用するプレフィックス。
- `HostConnectionPrefix` – ホスト接続に適用するプレフィックス。
- `MachineCatalogPrefix` – マシンカタログに適用するプレフィックス。
- `StoreFrontPrefix` – StoreFront™名に適用するプレフィックス。
- `TagPrefix` – タグに適用するプレフィックス。
- `AdminScopedSuffix` – 管理者スコープに適用するサフィックス。
- `ApplicationSuffix` - アプリケーションに適用するサフィックス。
- `ApplicationFolderSuffix` – アプリケーションフォルダーに適用するサフィックス。`ApplicationFolderSuffix` は `ApplicationFolderRoot` と組み合わせることができます。
- `ApplicationGroupSuffix` – アプリケーショングループのサフィックス。

- `ApplicationUserSuffix` – ユーザーに表示されるアプリケーション名に適用するサフィックス。
- `ApplicationAdminSuffix` – 管理者に表示されるアプリケーション名に適用するサフィックス。
- `DeliveryGroupSuffix` – デリバリーグループに適用するサフィックス。
- `GroupPolicySuffix` – ポリシー名に適用するサフィックス。
- `HostConnectionSuffix` – ホスト接続に適用するサフィックス。
- `MachineCatalogSuffix` – マシンカタログに適用するサフィックス。
- `StoreFrontSuffix` – StoreFront名に適用するサフィックス。
- `TagSuffix` – タグに適用するサフィックス。
- `SiteRootFolder` – エクスポートおよびインポートに使用する完全修飾フォルダー名。ローカルフォルダーまたはファイル共有にすることができます。

汎用パラメーター

クラウドアクセスパラメーター

クラウドにアクセスするすべてのコマンドレットは、以下の追加パラメーターをサポートしています。

> **注:**
>
> CustomerId、ClientId、およびSecretは、CustomerInfo.ymlファイルに配置するか、以下のパラメーターを使用してコマンドレットで指定できます。両方の場所で指定されている場合、コマンドレットパラメーターが優先されます。

- `CustomerId` – Rest APIで使用される顧客IDで、すべてのRest APIにアクセスするために必要です。顧客IDはCitrix Cloudで見つけることができます。
- `ClientId` – Citrix Cloud Identity and Access Management Webサイトで作成されたクライアントID。これは、すべてのRest APIの認証に必要なベアラートークンを取得するために必要です。
- `Secret` – Citrix Cloud Identity and Access Management Webサイトで作成された秘密鍵。これは、すべてのRest APIの認証に必要なベアラートークンを取得するために必要です。
- `CustomerInfoFileSpec` – デフォルトの場所と名前を上書きするための顧客情報ファイルを指すファイル指定。

移行モードパラメーター

クラウドサイト構成を変更するコマンドレット (`Import` 、 `Restore` 、 `Merge` 、 `New` 、および `Sync`) は、さらなる柔軟性を提供するために以下の追加パラメーターをサポートしています。

- `CheckMode` – インポート操作を実行しますが、変更は*行いません*。すべての予期される変更は、インポートが完了する前に報告されます。このコマンドを使用して、インポートが実行される前にテストできます。
- `BackupFirst` – クラウド設定を変更する前に、クラウドコンテンツを.ymlファイルにバックアップします。これはデフォルトで有効になっています。
- `Confirm` – trueの場合、クラウドサイト設定に変更を加えることをユーザーに確認するプロンプトを表示します。 `Remove` コマンドレットは、その破壊的な性質のためプロンプトを表示します。自動スクリプト内で実行する場合など、プロンプトが不要な場合はfalseに設定します。 `Confirm` はデフォルトでtrueです。
- `SecurityFileFolder` – これは、CustomerInfo.ymlファイルを含む完全修飾フォルダーであり、ローカルフォルダーまたは認証制御下にある可能性のあるネットワーク共有フォルダーを指す場合があります。ツールは資格情報を要求しません。ツールを実行する前に、制御されたリソースへのアクセスを取得する必要があります。
- `SiteName` – インポート時に使用するサイトマージのプレフィックスとサフィックスのセットを指定します。
- `SiteActive` – インポートされたサイトがアクティブか非アクティブかを指定します。デフォルトでは、このパラメーターは `$false` に設定されており、インポートされたサイトは非アクティブであることを意味します。

ログ表示パラメーター

The `Export` , `Import` , `Sync` , `Restore` , `Backup` , `Compare` , and `Remove` コマンドレットは、操作が完了するとログファイルを表示します。 `-DisplayLog` パラメーターを `$false` に設定することで、表示を抑制できます。ログファイルの表示には、デフォルトでNotepad.exeが使用されます。CustomerInfo.ymlファイルで別のエディターを指定できます。

```
Editor: C:\Program Files\Notepad++\notepad++.exe
```

コマンドレットの戻り値

ActionResult

すべてのコマンドレットは次の値を返します。

```
public class ActionResult

{

    public bool                         Overall_Success;

    public Dictionary&lt;string, string>   Individual_Success;

    public object                       CustomResult;

}
```

`Overall_Success` は、選択されたすべてのコンポーネントにおけるコマンドレット全体の成功を示す単一のブール値を返します。trueは成功、falseは失敗を意味します。

`Individual_Success` は、各主要コンポーネントに対して1つまたは3つの値を返します。コンポーネントの結果は、Success、Failure、またはSkippedのいずれかになります。Skippedは、そのコンポーネントがコマンドレットによる実行のために選択されなかったことを示します。

`CustomResult` はコマンドレット固有です。

CustomResult

`Import`、`Merge`、`Restore`、`Sync`、`Compare`、`Compare File`、および`Remove`は、`EvaluationResultData`の単一インスタンスに以下のカスタム結果情報を返します。

> **注:**
>
> `Export` および `Template` コマンドレットはカスタム結果を返しません。

```
 public class EvaluationResultData

 {

     public Dictionary&lt;string, Dictionary&lt;string, ActionResultValues
>> EvaluationResults;

     public int                  Added;

     public int                  Updated;
```

```
    public int                  Deleted;
    public int                  NoChange;
    public int                  TotalChanged;
    public EvaluationResults     OverallResult;
    public string               CloudBackupFolder;
    public string               SourceBackupFolder;
}
Where:
public enum ActionResultValues
{
    Add,
    Update,
    Delete,
    Identical,
    DoNothing
}
public enum EvaluationResults
{
    Success,
    Failure,
    Skipped
```

```
}
```

`EvaluationResults`は、選択されたコンポーネントごとに1つのエントリを持つリストを表示します。キーはコンポーネント名で、値は各コンポーネントメンバーのリストと、そのコンポーネントメンバーに対して実行されたアクションです。アクションは`ActionResultValues`の値のいずれかになります。

`Added`、`Updated`、`Deleted`、および`NoChange`は、追加、更新、削除、またはアクションなしのコンポーネントメンバーの合計数をこの順序で示します。

`TotalChanged` は、`Added`、`Updated`、および `Deleted` の合計です。

`OverallResult` は、コマンドレットの結果を示す単一のブール値です。True はすべてのコンポーネントでの完全な成功を示し、False は 1 つ以上のコンポーネントの処理の失敗を示します。

`CloudBackupFolder` は、コマンドレットがクラウド変更アクションを実行する前の、クラウドサイト構成バックアップの完全修飾ファイル指定です。

`SourceBackupFolder` は、コマンドレットの完了後に作成されたソースファイルバックアップの完全修飾ファイル指定です。デフォルトでは、これらのファイルは *%HOMEPATH%\Documents\Citrix\AutoConfig* にあります。

PowerShell ヘルプ

各コマンドレットにはPowerShellヘルプが用意されています。すべてのパラメーターは、コマンドレットの簡単な説明とともに、各コマンドレットに文書化されています。任意のコマンドレットのヘルプにアクセスするには、コマンドレットの前に`Get-Help`と入力します。

`Get-Help Import-CvadAcToSite`

自動構成ツール コマンドレット（バックアップと復元用）

このページには、Web Studioが使用するバックアップおよび復元APIをトリガーするためにツールでサポートされているすべてのコマンドレットとパラメーターがリストされています。

バックアップストレージ コマンドレット

Get-BckRstrStorage

このコマンドレットはオンプレミスのみに適用されます。バックアップが保存されるストレージの詳細を取得します。

パラメーター:

パラメーター	説明
`CustomerId`	ベアラートークンを取得するために必要な顧客ID。
`CientId`	ベアラートークンを取得するために必要なクライアントID。
`Secret`	ベアラートークンを取得するために必要なシークレット。
`CustomerInforFileSpec`	セキュリティおよび環境情報を含む顧客情報ファイルの完全修飾ファイル指定。
`ProfileName`	以前のパラメーターの代わりに使用される既存のセキュリティプロファイルを識別するためのパラメーター。セキュリティプロファイルの設定方法については、「XenApp & XenDesktop: Remote PowerShell SDK v2 for Citrix Cloud」を参照してください。
`Environment`	本番環境のタイプ: Production、ProductionGov、ProductionJP、OnPrem。
`Quiet`	コンソールへの出力を抑制するためのパラメーター。

Set-BckRstrStorage

このコマンドレットはオンプレミスのみに適用されます。バックアップが保存される新しいストレージを設定します。

パラメーター:

パラメーター	説明
`CustomerId`	ベアラートークンを取得するために必要な顧客ID。

パラメーター	説明
`CientId`	ベアラートークンを取得するために必要なクライアントID。
`Secret`	ベアラートークンを取得するために必要なシークレット。
`CustomerInforFileSpec`	セキュリティおよび環境情報を含む顧客情報ファイルの完全修飾ファイル指定。
`ProfileName`	以前のパラメーターの代わりに使用される既存のセキュリティプロファイルを識別するためのパラメーター。セキュリティプロファイルの設定方法については、XenApp & XenDesktop: Remote PowerShell SDK v2 for Citrix Cloudを参照してください。
`Environment`	本番環境のタイプ: Production、ProductionGov、ProductionJP、OnPrem。
`Quiet`	コンソールへの出力を抑制するためのパラメーター。
`MaximumBackups`	新しいバックアップが作成されたときに、バックアップクリーンアッププロセスが最も古いバックアップを削除するまで保持される、ピン留めされていないバックアップの最大数。
`MaximumPinnedBackups`	保持されるピン留めされたバックアップの最大数。これらのバックアップはクリーン

パラメーター	説明
	アッププロセスによって削除されません。
`BlobStorageType`	ストレージの種類: `FileStorage` または `CustomerAzureStorage`。
`FileStoragefolder`	`BlobStorageType` `FileStorage` オプションの完全修飾フォルダー指定。
`Info1`	`FileStorage` の場合、オプションの `UserName` `CustomerAzureStorage` の場合、Azure SAS URL
`Info2`	`FileStorage` の場合、オプションの Password
`Info3` および `Info4`	使用されていません

Test-BckRstrStorage コマンドレット

このコマンドレットはオンプレミスのみに適用されます。定義されたストレージが有効であることを確認するためにテストします。

`FileStorage` の場合、テストはフォルダーが存在し、書き込み可能であることを確認します。

`CustomerAzureStorage` の場合、テストは SAS URL が正しい権限を持ち、現在の日付が URL の開始日と終了日の範囲内であることを検証します。

有効な場合は `true` を、無効な場合は `false` を返します。

パラメーター:

パラメーター	説明
`CustomerId`	ベアラートークンを取得するために必要な顧客 ID。

パラメーター	説明
`CientId`	ベアラートークンを取得するために必要なクライアント ID。
`Secret`	ベアラートークンを取得するために必要なシークレット。
`CustomerInforFileSpec`	セキュリティおよび環境情報を含む顧客情報ファイルの完全修飾ファイル指定。
`ProfileName`	以前のパラメーターの代わりに使用される、既存のセキュリティプロファイルを識別するためのパラメーター。セキュリティプロファイルの設定方法については、XenApp & XenDesktop: Remote PowerShell SDK v2 for Citrix Cloud を参照してください。
`Environment`	本番環境の種類: Production、ProductionGov、ProductionJP、OnPrem。
`Quiet`	コンソールへの出力を抑制するパラメーター。

バックアップコマンドレット

Get-BckRstrBackups

バックアップまたは復元BLOBストレージの場所に保存されているバックアップを列挙します。Citrix Virtual Apps and Desktops™の場合、この場所は管理者がWebStudioを通じて設定します。DaaSの場合、これは既存の顧客Azureストレージです。各バックアップに関する完全な情報については、`Get-BckRstrBackupsWithDetiails`を使用してください。バックアップの詳細は次のとおりです。

- バックアップ名
- 注
- ピン留め済み（trueまたはfalse）
- バックアップの日時
- 履歴UID
- 関連UID (最後の復元履歴レコードのUID)

- 関連日時
- チェックモードで実行された場合に関連付けられる
- 期間（秒）
- 管理者名
- 各コンポーネントと各コンポーネントのメンバー数を列挙した詳細。

パラメーター:

パラメーター	説明
`CustomerId`	ベアラートークンを取得するために必要な顧客ID。
`CientId`	ベアラートークンを取得するために必要なクライアントID。
`Secret`	ベアラートークンを取得するために必要なシークレット。
`CustomerInforFileSpec`	セキュリティおよび環境情報を含む顧客情報ファイルの完全修飾ファイル指定。
`ProfileName`	以前のパラメータの代わりに使用される既存のセキュリティプロファイルを識別するためのパラメータ。セキュリティプロファイルの設定方法については、XenApp & XenDesktop: Remote PowerShell SDK v2 for Citrix Cloudを参照してください。
`Environment`	本番環境のタイプ: Production、ProductionGov、ProductionJP、OnPrem。
`Quiet`	コンソールへの出力を抑制するためのパラメータ。

Get-BckRstrBackupsMembers

選択したバックアップに保存されている単一のコンポーネントのメンバーを列挙します。メンバー名は単純なリストで返されます。

コンポーネントは次のとおりです。

- タグ
- AdminScopes
- AdminRoles
- AdminAdministrators (オンプレミスのみ)
- HostConnections
- アイコン
- AdminFolders
- MachineCatalogs
- StoreFronts
- DeliveryGroups
- ApplicationGroups
- ApplicationFolders
- アプリケーション
- App-Vサーバー
- Appライブラリパッケージ検出
- App-V分離グループ
- グループポリシー
- ユーザーゾーン設定
- サイトデータ
- ゾーン (オンプレミスのみ)

パラメーター:

パラメーター	説明
`CustomerId`	ベアラートークンを取得するために必要な顧客ID。
`CientId`	ベアラートークンを取得するために必要なクライアントID。
`Secret`	ベアラートークンを取得するために必要なシークレット。

パラメーター	説明
`CustomerInforFileSpec`	セキュリティおよび環境情報を含む顧客情報ファイルの完全修飾ファイル指定。
`ProfileName`	以前のパラメーターの代わりに使用される既存のセキュリティプロファイルを識別するためのパラメーター。セキュリティプロファイルの設定方法については、XenApp & XenDesktop: Remote PowerShell SDK v2 for Citrix Cloudを参照してください。
`Environment`	本番環境のタイプ: Production、ProductionGov、ProductionJP、OnPrem。
`Quiet`	コンソールへの出力を抑制するためのパラメーター。
`BackupName`	バックアップの名前。`.zip` 拡張子はオプションです。
`Component`	バックアップに含めるコンポーネント。

New-BckRstrBackup

Delivery Controller で新しいバックアップアクションを開始します。このアクションは、`New-BckRstrBackup` コマンドレットに対して非同期です。

パラメーター:

パラメーター	説明
`CustomerId`	ベアラートークンを取得するために必要な顧客ID。
`CientId`	ベアラートークンを取得するために必要なクライアントID。
`Secret`	ベアラートークンを取得するために必要なシークレット。
`CustomerInforFileSpec`	セキュリティおよび環境情報を含む顧客情報ファイルの完全修飾ファイル指定。

パラメーター	説明
`ProfileName`	以前のパラメーターの代わりに使用される、既存のセキュリティプロファイルを識別するためのパラメーター。セキュリティプロファイルの設定方法については、XenApp & XenDesktop: Remote PowerShell SDK v2 for Citrix Cloud を参照してください。
`Environment`	本番環境のタイプ: Production、ProductionGov、ProductionJP、OnPrem。
`Quiet`	コンソールへの出力を抑制するためのパラメーター。
`Notes`	バックアップに関するメモ。
`PollForCompletion`	アクションが完了するまで、Delivery Controllerで実行中のアクションをポーリングするパラメーター。`Quite`パラメーターが指定されていない限り、ポーリングは進行状況と完了結果をコンソールにログに記録します。

バックアップをピン留めするコマンドレット

Set-BckRstrPinBackups

Delivery Controllerのバックアップクリーンアッププロセスの一部として削除されないように、バックアップをピン留めします。

パラメーター:

パラメーター	説明
`CustomerId`	ベアラートークンを取得するために必要な顧客ID。
`CientId`	ベアラートークンを取得するために必要なクライアントID。
`Secret`	ベアラートークンを取得するために必要なシークレット。

パラメーター	説明
`CustomerInforFileSpec`	セキュリティおよび環境情報を含む顧客情報ファイルの完全修飾ファイル指定。
`ProfileName`	以前のパラメーターの代わりに使用される既存のセキュリティプロファイルを識別するためのパラメーターです。セキュリティプロファイルの設定方法については、XenApp & XenDesktop: Citrix Cloud 用リモート PowerShell SDK v2 を参照してください。
`Environment`	本番環境のタイプ: Production、ProductionGov、ProductionJP、OnPrem。
`Quiet`	コンソールへの出力を抑制するパラメーター。
`BackupName`	バックアップの名前。`.zip` 拡張子はオプションです。

Set-BckRstrUnpinBackups

バックアップのピン留めを解除し、Delivery Controller のバックアップクリーンアッププロセスで削除できるようにします。

パラメーター:

パラメーター	説明
`CustomerId`	ベアラートークンを取得するために必要な顧客ID。
`CientId`	ベアラートークンを取得するために必要なクライアントID。
`Secret`	ベアラートークンを取得するために必要なシークレット。
`CustomerInforFileSpec`	セキュリティおよび環境情報を含む顧客情報ファイルの完全修飾ファイル指定。

パラメーター	説明
`ProfileName`	以前のパラメーターの代わりに使用される既存のセキュリティプロファイルを識別するためのパラメーター。セキュリティプロファイルの設定方法については、XenApp & XenDesktop: Remote PowerShell SDK v2 for Citrix Cloudを参照してください。
`Environment`	本番環境のタイプ: Production、ProductionGov、ProductionJP、OnPrem。
`Quiet`	コンソールへの出力を抑制するためのパラメーター。
`BackupName`	バックアップの名前。`.zip`拡張子はオプションです。

バックアップ削除コマンドレット

Remove-BckRstrBackup コマンドレット

1つ以上のバックアップを削除します。

パラメーター:

パラメーター	説明
`CustomerId`	ベアラートークンを取得するために必要な顧客ID。
`CientId`	ベアラートークンを取得するために必要なクライアントID。
`Secret`	ベアラートークンを取得するために必要なシークレット。
`CustomerInforFileSpec`	セキュリティおよび環境情報を含む顧客情報ファイルの完全修飾ファイル指定。
`ProfileName`	以前のパラメーターの代わりに使用される、既存のセキュリティプロファイルを識別するためのパラメーター。セキュリティプロファイルの設定方法については、XenApp &

パラメーター	説明
	XenDesktop: Remote PowerShell SDK v2 for Citrix Cloudを参照してください。
`Environment`	本番環境のタイプ: Production、ProductionGov、ProductionJP、OnPrem。
`Quiet`	コンソールへの出力を抑制するためのパラメーター。
`IncludeByName`	復元対象とするコンポーネントメンバーを指定するためのフィルター。これは、フィルター値のコンマ区切りリストであり、ワイルドカード文字 `*` および `?` を含めることができます。

スケジュールされたバックアップコマンドレット

Get-BckRstrSchedules

バックアップスケジュールのリストを取得します。

パラメータ:

パラメータ	説明
`CustomerId`	ベアラートークンを取得するために必要な顧客ID。
`CientId`	ベアラートークンを取得するために必要なクライアントID。
`Secret`	ベアラートークンを取得するために必要なシークレット。
`CustomerInforFileSpec`	セキュリティおよび環境情報を含む顧客情報ファイルの完全修飾ファイル指定。
`ProfileName`	以前のパラメーターの代わりに使用される既存のセキュリティプロファイルを識別するためのパラメーター。セキュリティプロファイルの設定方法については、XenApp &

パラメータ	説明
	XenDesktop: Remote PowerShell SDK v2 for Citrix Cloudを参照してください。
`Environment`	本番環境のタイプ: Production、ProductionGov、ProductionJP、OnPrem。
`Quiet`	コンソールへの出力を抑制するためのパラメーター。
`BackupName`	バックアップの名前。`.zip`拡張子はオプションです。
`Notes`	設定または変更するメモ。

New-BckRstrSchedule

新しいバックアップスケジュールを作成します。

パラメーター:

パラメーター	説明
`CustomerId`	ベアラートークンを取得するために必要な顧客ID。
`CientId`	ベアラートークンを取得するために必要なクライアントID。
`Secret`	ベアラートークンを取得するために必要なシークレット。
`CustomerInforFileSpec`	セキュリティおよび環境情報を含む顧客情報ファイルの完全修飾ファイル指定。
`ProfileName`	以前のパラメーターの代わりに使用される既存のセキュリティプロファイルを識別するためのパラメーター。セキュリティプロファイルの設定方法については、XenApp & XenDesktop: Remote PowerShell SDK v2 for Citrix Cloudを参照してください。

パラメーター	説明
`Environment`	本番環境のタイプ: Production、ProductionGov、ProductionJP、OnPrem。
`Quiet`	コンソールへの出力を抑制するためのパラメーター。
`Name`	スケジュール名。
`Uid`	スケジュール名を変更する場合。
`Frequency`	頻度の種類: 毎日、毎週、または毎月。
`Day`	頻度が毎日の場合。
`DaysInWeek`	頻度が毎週の場合。
`DayInMonth`	頻度が毎月の場合。
`WeekInMonth`	頻度が毎月の場合。
`StartDate`	形式は `M/d/yy` です
`StartTime`	24時間形式で指定された開始時刻。
`FrequencyFactor`	毎日 (値 = 1) または隔日 (値 = 2) のように、n 回ごとに実行します。
`Description`	スケジュールされたバックアップの説明。
`Enabled`	このバックアップスケジュールを有効にするパラメーター。有効な場合は `True`、無効な場合は `false`。
`TimeZoneId`	Windows タイムゾーン ID。

Set-BckRstrSchedule

既存のバックアップスケジュールを変更します。変更するスケジュールを選択するには、名前または Uid を指定します。

パラメーター:

パラメーター	説明
`CustomerId`	ベアラートークンを取得するために必要な顧客ID。
`CientId`	ベアラートークンを取得するために必要なクライアントID。
`Secret`	ベアラートークンを取得するために必要なシークレット。
`CustomerInforFileSpec`	セキュリティおよび環境情報を含む顧客情報ファイルの完全修飾ファイル指定。
`ProfileName`	以前のパラメーターの代わりに使用される既存のセキュリティプロファイルを識別するためのパラメーター。セキュリティプロファイルの設定方法については、XenApp & XenDesktop: Remote PowerShell SDK v2 for Citrix Cloud を参照してください。
`Environment`	本番環境のタイプ: Production、ProductionGov、ProductionJP、OnPrem。
`Quiet`	コンソールへの出力を抑制するためのパラメーター。
`Name`	スケジュール名。
`Uid`	スケジュール名を変更する場合。
`Frequency`	頻度の種類: 毎日、毎週、または毎月。
`Day`	頻度が毎日の場合。
`DaysInWeek`	頻度が毎週の場合。
`DayInMonth`	頻度が毎月の場合。
`WeekInMonth`	頻度が毎月の場合。
`StartDate`	形式は `M/d/yy` です

パラメーター	説明
`StartTime`	24時間形式で指定された開始時刻。
`FrequencyFactor`	毎日 (値 = 1) または隔日 (値 = 2) のように、n 回ごとに実行します。
`Description`	スケジュールされたバックアップの説明。
`Enabled`	このバックアップスケジュールを有効にするパラメーター。有効な場合は `True`、無効な場合は `false`。
`TimeZoneId`	Windows タイムゾーン ID。

Set-BckRstrScheduleEnabled

既存のバックアップスケジュールを有効にします。有効にするスケジュールを選択するには、名前または Uid を指定します。

パラメーター:

パラメーター	説明
`CustomerId`	ベアラートークンを取得するために必要な顧客 ID。
`CientId`	ベアラートークンを取得するために必要なクライアント ID。
`Secret`	ベアラートークンを取得するために必要なシークレット。
`CustomerInforFileSpec`	セキュリティおよび環境情報を含む顧客情報ファイルの完全修飾ファイル指定。
`ProfileName`	以前のパラメーターの代わりに使用される既存のセキュリティプロファイルを識別するためのパラメーター。セキュリティプロファイルの設定方法については、XenApp & XenDesktop: Remote PowerShell SDK v2 for Citrix Cloud を参照してください。

パラメーター	説明
`Environment`	本番環境のタイプ: Production、ProductionGov、ProductionJP、OnPrem。
`Quiet`	コンソールへの出力を抑制するパラメーター。
`Name`	スケジュール名。
`Uid`	スケジュール名を変更する場合。

Set-BckRstrScheduleDisabled

既存のバックアップスケジュールを無効にします。無効にするスケジュールを選択するには、名前またはUidを指定します。

パラメーター:

パラメーター	説明
`CustomerId`	ベアラートークンを取得するために必要な顧客ID。
`CientId`	ベアラートークンを取得するために必要なクライアントID。
`Secret`	ベアラートークンを取得するために必要なシークレット。
`CustomerInforFileSpec`	セキュリティおよび環境情報を含む顧客情報ファイルの完全修飾ファイル指定。
`ProfileName`	以前のパラメーターの代わりに使用される、既存のセキュリティプロファイルを識別するためのパラメーター。セキュリティプロファイルの設定方法については、XenApp & XenDesktop: Remote PowerShell SDK v2 for Citrix Cloudを参照してください。
`Environment`	本番環境のタイプ: Production、ProductionGov、ProductionJP、OnPrem。

パラメーター	説明
`Quiet`	コンソールへの出力を抑制するためのパラメーター。
`Name`	スケジュール名。
`Uid`	スケジュール名を変更する場合。

バックアップを制限するコマンドレット

Set-BckRstrOptions

スケジュールされたバックアップを1日1回に制限し、同一のバックアップを回避します。

パラメーター:

パラメーター	説明
`CustomerId`	ベアラートークンを取得するために必要な顧客ID。
`CientId`	ベアラートークンを取得するために必要なクライアントID。
`Secret`	ベアラートークンを取得するために必要なシークレット。
`CustomerInforFileSpec`	セキュリティおよび環境情報を含む顧客情報ファイルの完全修飾ファイル指定。
`ProfileName`	以前のパラメーターの代わりに使用される既存のセキュリティプロファイルを識別するためのパラメーター。セキュリティプロファイルの設定方法については、XenApp & XenDesktop: Remote PowerShell SDK v2 for Citrix Cloudを参照してください。
`Environment`	本番環境のタイプ：Production、ProductionGov、ProductionJP、OnPrem。
`Quiet`	コンソールへの出力を抑制するためのパラメーター。

パラメーター	説明
`OneScheduledBackupPerDay`	同一のバックアップを避けるため、スケジュールされたバックアップを1日1回に制限するパラメーター。

復元コマンドレット

Restore-BckRstrBackups

既存のバックアップから、単一コンポーネントのメンバーを復元します。

パラメーター:

パラメーター	説明
`CustomerId`	ベアラートークンを取得するために必要な顧客ID。
`CientId`	ベアラートークンを取得するために必要なクライアントID。
`Secret`	ベアラートークンを取得するために必要なシークレット。
`CustomerInforFileSpec`	セキュリティおよび環境情報を含む顧客情報ファイルの完全修飾ファイル指定。
`ProfileName`	以前のパラメータの代わりに使用される既存のセキュリティプロファイルを識別するためのパラメータ。セキュリティプロファイルの設定方法については、XenApp & XenDesktop: Remote PowerShell SDK v2 for Citrix Cloudを参照してください。
`Environment`	本番環境のタイプ: Production、ProductionGov、ProductionJP、OnPrem。
`Quiet`	コンソールへの出力を抑制するためのパラメータ。
`BackupName`	バックアップの名前。`.zip`拡張子はオプションです。

パラメーター	説明
`Component`	バックアップに含めるコンポーネント。
`Notes`	バックアップに関するメモ。
`CheckMode`	復元されるコンポーネントメンバーを識別するが、実際の復元は実行しないパラメータ。
`RestoreType`	復元タイプ: MissingOnly または MissingUpdateExisting
`IncludeByName`	復元対象とするコンポーネントメンバーを指定するフィルター。これは、コンマ区切りのフィルター値のリストであり、ワイルドカード文字 `*` および `?` を含めることができます。

履歴コマンドレット

Get-BckRstrHistory

すべてのアクションの履歴詳細リストを取得します。

パラメーター:

パラメーター	説明
`CustomerId`	ベアラートークンを取得するために必要な顧客ID。
`CientId`	ベアラートークンを取得するために必要なクライアントID。
`Secret`	ベアラートークンを取得するために必要なシークレット。
`CustomerInforFileSpec`	セキュリティおよび環境情報を含む顧客情報ファイルの完全修飾ファイル指定。
`ProfileName`	以前のパラメーターの代わりに使用される既存のセキュリティプロファイルを識別するためのパラメーター。セキュリティプロファイルの設定方法については、XenApp &

パラメーター	説明
	XenDesktop: Remote PowerShell SDK v2 for Citrix Cloudを参照してください。
`Environment`	本番環境のタイプ: Production、ProductionGov、ProductionJP、OnPrem。
`Quiet`	コンソールへの出力を抑制するパラメーター。
`Name`	スケジュール名。
`Uid`	スケジュール名を変更する場合。

バックアップの制限コマンドレット

Set-BckRstrOptions

同一のバックアップを避けるため、スケジュールされたバックアップを1日1回に制限します。

パラメーター:

パラメーター	説明
`CustomerId`	ベアラートークンを取得するために必要な顧客ID。
`CientId`	ベアラートークンを取得するために必要なクライアントID。
`Secret`	ベアラートークンを取得するために必要なシークレット。
`CustomerInforFileSpec`	セキュリティおよび環境情報を含む顧客情報ファイルの完全修飾ファイル指定。
`ProfileName`	以前のパラメーターの代わりに使用される既存のセキュリティプロファイルを識別するためのパラメーター。セキュリティプロファイルの設定方法については、XenApp & XenDesktop: Remote PowerShell SDK v2 for Citrix Cloudを参照してください。

パラメーター	説明
`Environment`	本番環境のタイプ: Production、ProductionGov、ProductionJP、OnPrem。
`Quiet`	コンソールへの出力を抑制するためのパラメーター。
`OneScheduledBackupPerDay`	同一のバックアップを避けるため、スケジュールされたバックアップを1日1回に制限するパラメーター。

復元コマンドレット

レストア-バックリストアバックアップス

既存のバックアップから単一コンポーネントのメンバーを復元します。

パラメーター:

パラメーター	説明
`CustomerId`	ベアラートークンを取得するために必要な顧客ID。
`CientId`	ベアラートークンを取得するために必要なクライアントID。
`Secret`	ベアラートークンを取得するために必要なシークレット。
`CustomerInforFileSpec`	セキュリティおよび環境情報を含む顧客情報ファイルの完全修飾ファイル指定。
`ProfileName`	以前のパラメーターの代わりに使用される、既存のセキュリティプロファイルを識別するためのパラメーター。セキュリティプロファイルの設定方法については、XenApp & XenDesktop: Remote PowerShell SDK v2 for Citrix Cloudを参照してください。
`Environment`	本番環境のタイプ: Production、ProductionGov、ProductionJP、OnPrem。

パラメーター	説明
`Quiet`	コンソールへの出力を抑制するためのパラメーター。
`BackupName`	バックアップの名前。`.zip`拡張子はオプションです。
`Component`	バックアップに含めるコンポーネント。
`Notes`	バックアップに関するメモ。
`CheckMode`	復元されるはずのコンポーネントメンバーを識別するためのパラメーターですが、実際の復元は実行しません。
`RestoreType`	復元タイプ: MissingOnly または MissingUpdateExisting
`IncludeByName`	復元対象とするコンポーネントメンバーを指定するためのフィルター。これは、フィルター値のコンマ区切りリストであり、ワイルドカード文字`*`および`?`を含めることができます。

履歴コマンドレット

Get-BckRstrHistory

すべてのアクションの履歴詳細のリストを取得します。

パラメーター:

パラメーター	説明
`CustomerId`	ベアラートークンを取得するために必要な顧客ID。
`CientId`	ベアラートークンを取得するために必要なクライアントID。
`Secret`	ベアラートークンを取得するために必要なシークレット。

パラメーター	説明
`CustomerInforFileSpec`	セキュリティおよび環境情報を含む顧客情報ファイルの完全修飾ファイル指定。
`ProfileName`	以前のパラメーターの代わりに使用される既存のセキュリティプロファイルを識別するためのパラメーター。セキュリティプロファイルの設定方法については、XenApp & XenDesktop: Remote PowerShell SDK v2 for Citrix Cloudを参照してください。
`Environment`	本番環境のタイプ: Production, ProductionGov, ProductionJP, OnPrem。
`Quiet`	コンソールへの出力を抑制するためのパラメーター。

Get-BckRstrSpecificBackupHistory

特定のバックアップの履歴詳細のリストを取得します。

パラメーター:

パラメーター	説明
`CustomerId`	ベアラートークンを取得するために必要な顧客ID。
`CientId`	ベアラートークンを取得するために必要なクライアントID。
`Secret`	ベアラートークンを取得するために必要なシークレット。
`CustomerInforFileSpec`	セキュリティおよび環境情報を含む顧客情報ファイルの完全修飾ファイル指定。
`ProfileName`	以前のパラメーターの代わりに使用される既存のセキュリティプロファイルを識別するためのパラメーター。セキュリティプロファイルの設定方法については、XenApp &

パラメーター	説明
	XenDesktop: Remote PowerShell SDK v2 for Citrix Cloudを参照してください。
`Environment`	本番環境のタイプ: Production、ProductionGov、ProductionJP、OnPrem。
`Quiet`	コンソールへの出力を抑制するためのパラメーター。
`BackupName`	バックアップの名前。`.zip`拡張子はオプションです。

Set-BckRstrNotes

履歴レコード内のメモを設定または変更します。

パラメーター:

パラメーター	説明
`CustomerId`	ベアラートークンを取得するために必要な顧客ID。
`CientId`	ベアラートークンを取得するために必要なクライアントID。
`Secret`	ベアラートークンを取得するために必要なシークレット。
`CustomerInforFileSpec`	セキュリティおよび環境情報を含む顧客情報ファイルの完全修飾ファイル指定。
`ProfileName`	以前のパラメーターの代わりに使用される既存のセキュリティプロファイルを識別するためのパラメーター。セキュリティプロファイルの設定方法については、XenApp & XenDesktop: Remote PowerShell SDK v2 for Citrix Cloudを参照してください。
`Environment`	本番環境のタイプ：Production、ProductionGov、ProductionJP、OnPrem。

パラメーター	説明
`Quiet`	コンソールへの出力を抑制するパラメーター。
`BackupName`	バックアップの名前。`.zip` 拡張子はオプションです。
`Notes`	設定または変更するメモ。

自動構成のトラブルシューティングと追加情報

> **重要:**
>
> 自動構成でよく発生するエラーメッセージと対応する解決策については、Knowledge Center の記事 CTX277730 にある *トラブルシューティングFAQ* を参照してください。

自動構成ツールのエラー

自動構成ツールの操作中にエラーが発生することがあります。このような場合、たとえばマシンカタログ、デリバリーグループ、またはグループポリシーなどのコンポーネントを処理する際に障害が発生する可能性があります。`OnErrorAction` と継続パラメーターを使用すると、処理中にエラーを捕捉し、解決して、中断したところから再開できます。

デフォルトの `OnErrorAction` 値は `StopCompEnd` です。エラーが発生すると、ツールは現在のコンポーネントの処理を終了します。追加のコンポーネントは処理されず、エラーは下流の依存コンポーネントに引き継がれません。エラーを解決した後、継続パラメーターを適用してコマンドレットを再実行できます。

OnErrorAction パラメーター

移行コマンドで `OnErrorAction` パラメーター値を定義して、コンポーネントの処理中に検出されるエラーに対してツールがどのように応答するかを制御できます。

この表は、パラメーター値とその説明を示しています。

値	説明
`Continue`	すべてのコンポーネントを可能な限り多く処理しようとします。

値	説明
`Pause`	処理の最後に一時停止し、続行するか停止するかを尋ねます。
`StopCompEnd`	コンポーネントを可能な限り多く処理しようとします。コンポーネントの完了後に停止します。(デフォルト)
`StopImmediately`	エラーが検出されると処理が停止します。

移行cmdlet

次の移行コマンドに`OnErrorAction`パラメーターを適用できます。

- `Compare-CvadAcToSite`
- `Import-CvadAcToSite`
- `Merge-CvadAcToSite`
- `New-CvadAcToSite`
- `Restore-CvadAcToSite`

例: `Merge-CvadAcToSite -OnErrorAction StopImmediately`

再開パラメーター

これらのパラメーターは、操作がエラーのために一時停止または停止した後にツールがどのように再開するかを定義します。

次の`OnErrorAction`パラメーター値のいずれかを含む移行コマンドレットに、再開パラメーターを適用できます。

- `Pause`
- `StopCompEnd`
- `StopImmediately`

この表は、パラメーター値とその説明を示しています。

値	説明
`-AllRemaining`	開始コンポーネントが必要です。処理は開始コンポーネントから始まり、残りのすべてのコン

値	説明
	ポーネントを処理します。複数のコンポーネントが処理されます。
`-Resume`	`CurrentComponent.txt` のコンポーネントを開始点として使用します。残りのすべてが true に設定されます。複数のコンポーネントが処理されます。
`-Repeat`	`CurrentComponent.txt` のコンポーネントを開始点として使用します。残りのすべてが false に設定されます。1つのコンポーネントのみが処理されます。

最後に処理されたコンポーネントは、AutoConfig フォルダー内の `CurrentComponent.txt` ファイルに保存されます。このファイルの編集は推奨されません。 `-Resume` または `-Repeat` を指定し、`CurrentComponent.txt` が見つからないか無効な場合、処理は停止し、コンポーネントを選択するように求められます。

CustomerInfo.yml ファイルでの OnErrorAction の設定

`CustomerInfo.yml` ファイルで `OnErrorAction` の値を設定することもできます。次のコマンドレットを使用して値を設定します。

- 新しいファイルの場合: `New-CvadAcCustomerInfoFile -OnErrorAction Continue | Pause | StopCompEnd | StopImmediately`
- 既存のファイルの場合: `Set-CvadAcCustomerInfoFile -OnErrorAction Continue | Pause | StopCompEnd | StopImmediately`

ログ

任意のコマンドレットを実行すると、ログファイルが作成され、メインの履歴ログファイルにエントリが追加されます。すべての操作ログファイルはバックアップフォルダーに配置されます。すべてのログファイル名は `CitrixLog` で始まり、その後に自動構成操作とコマンドレット実行の日付とタイムスタンプが表示されます。ログは自動削除されません。

メインの履歴ログは `*%HOMEPATH%\Documents\Citrix\AutoConfig*` にある **History.Log** というファイルにあります。各コマンドレットの実行により、日付、操作、結果、バックアップ、および実行のログファイルの場所を含むメインログエントリが生成されます。

Citrix にサポートのために送信するログを収集するには、`New-CvadAcZipInfoForSupport` コマンドレットを使用することもできます。このコマンドレットは、すべてのログファイルと .yml ファイルを単一の zip ファイルに圧縮します。お客様の機密情報 (CustomerInfo.yml および CvadAcSecurity.yml) は zip に含まれません。Icon.yml ファイルもサイズが大きいため除外されます。zip ファイルは *%HOMEPATH%\Documents\Citrix\AutoConfig* に配置され、日付とタイムスタンプに基づいて *CvadAcSupport_yyyy_mm_dd_hh_mm_ss.zip* という名前が付けられます。この zip ファイルはバックアップとしても機能します。

各ログファイルには、次のものが含まれます:

- 操作の名前と、チェックモードが有効になっているかどうか
- 開始日時と終了日時
- 各コンポーネントのアクションと成功/失敗通知の複数のエントリ
- 実行されたアクションの概要（作成されたオブジェクトのさまざまな数を含む）
- 該当する場合の推奨される修正
- 該当する場合のバックアップフォルダーの場所
- メインログの場所
- 期間

診断ファイル

診断ファイルは、問題の特定と解決に役立ちます。以下のファイルは、操作が実行されるときに作成されます。これらは、*%HOMEPATH%\Documents\Citrix\AutoConfig* の下にあるアクション固有のサブフォルダーにあります。問題解決サポートのために情報を提供する際は、これらのファイルを含めてください。

エクスポート

`PoshSdk_yyyy_mm_dd_hh_mm_ss.ps1`

このファイルは、サイト構成をファイルにエクスポートするために行われたすべてのBroker PowerShell SDK呼び出しをカウントします。

インポート、マージ、復元、同期、バックアップ、比較

`Transaction_yyyy_mm_dd_hh_mm_ss.txt`

このファイルは、各Rest API呼び出しと関連情報を記録します。

`RestApiContent_yyyy_mm_dd_hh_mm_ss.txt`

このファイルには、すべての`Add`、`Update`、および`Delete` Rest APIコンテンツが含まれています。

依存関係に起因する問題

依存関係の欠落により、インポートとマージが失敗する場合があります。一般的な問題は次のとおりです。

1. グループポリシーにデリバリーグループフィルターがありません。通常の原因は、インポートされていないデリバリーグループです。
2. アプリケーションのインポートまたはマージが失敗します。通常の原因は、インポートされていないデリバリーグループまたはアプリケーショングループです。
3. アプリケーショングループにRestrictToTagがありません。通常の原因は、インポートされていないタグです。
4. ホスト接続が失敗します。通常の原因は、CvadAcSecurity.ymlファイルにセキュリティ情報がないことです。
5. マシンカタログが失敗します。通常の原因は、インポートされなかったホスト接続です。
6. マシンカタログとデリバリーグループからマシンが欠落しています。通常の原因は、Active Directoryで見つからなかったマシンです。
7. デリバリーグループからユーザーが欠落しています。通常の原因は、Active Directoryで見つからなかったユーザーです。

推奨事項

- 自動構成の複数のインスタンスを同時に実行しないでください。複数のインスタンスを同時に実行すると、クラウドサイトで予期しない結果が生じます。この場合、自動構成の1つのインスタンスを再実行して、サイトを目的の状態に戻してください。
- 自動構成の実行中にStudioで作業したり、データを変更したりしないでください。
- クラウドサイトが期待どおりであることを確認するために、Studioでマージ、インポート、または復元の結果を常に視覚的に検証してください。

フォルダー

デフォルトのフォルダーのルート場所

すべての自動構成ツール操作は、ルートフォルダー内またはその中のサブフォルダー内で実行されます。ルートフォルダーは、*%HOMEPATH%\Documents\Citrix\AutoConfig* にあります。

エクスポート

エクスポートされたすべてのファイルは、使いやすさとエクスポート履歴を提供するために、2つのフォルダーの場所に配置されます。エクスポートは常にルートフォルダーに配置されます。コピーは、エクスポートの日時とともに **Export** という名前のサブフォルダーに配置されます。

ルートフォルダーには常に、最新のエクスポートされたオンプレミスサイト構成が含まれています。各 **Export** サブフォルダーには、指定された日時に行われたエクスポートが含まれており、エクスポートの履歴が保持されます。任意の **Export** サブフォルダーを使用してクラウドサイトを構成できます。自動構成は、既存のエクスポートサブフォルダーを削除または変更しません。

インポート/マージ/同期/比較

`Import`、`Merge`、および`Compare`操作は、常にルートフォルダーにあるファイルから取得されます。各操作によりサブフォルダーが作成され、ルートフォルダー内のファイルがそこにコピーされ、クラウドサイトの変更履歴ソースファイルが提供されます。

復元

`Restore`操作は、既存のサブフォルダーを使用してクラウドサイトを構成します。ソースフォルダーは、必須の`-RestoreFolder`パラメーターで指定されます。他のコマンドとは異なり、`Restore`操作は既存のサブフォルダーを使用するため、新しいサブフォルダーは作成されません。復元フォルダーはルートフォルダーにすることができますが、それでも`-RestoreFolder`パラメーターで指定する必要があります。

バックアップ

自動構成は、クラウドサイト構成を初期化、更新、およびバックアップします。長期間使用すると、クラウドサイトでさまざまな構成が変更される可能性があります。長期的な使用を容易にし、履歴の変更を保持するために、自動構成は保存スキームを使用してこの変更履歴を保存し、以前の状態を復元する方法を提供します。

クラウドサイト構成のバックアップは、常にバックアップの日時とともに**Backup**という名前のサブフォルダーに作成されます。自動構成は、既存のエクスポートサブフォルダーを削除または変更しません。

バックアップを使用して、特定のコンポーネントまたは構成全体を復元できます。配信グループとマシンカタログコンポーネント全体を復元するには、次のコマンドレットを使用します。

```
Restore-CvadAcToSite -RestoreFolder %HOMEPATH%\Documents\Citrix\AutoConfig/
Backup_yyyy_mm_dd_hh_mm_ss -DeliveryGroups -MachineCatalogs
```

> **注:**

> 上記のコマンドレットのバックアップファイル情報は、独自のバックアップに基づいています。

> クラウドサイト構成全体を復元するには、次のコマンドレットを使用します。

`Restore-CvadAcToSite -RestoreFolder %HOMEPATH%\Documents\Citrix\AutoConfig\Backup_yyyy_mm_dd_hh_mm_ss`

> **注:**
>
> 上記のコマンドレットのバックアップファイル情報は、独自のバックアップに基づいています。

デフォルトのルートフォルダーの変更

The `Export`, `Import`, `Merge`, `Sync`, and `Compare`の各操作は、`–AlternateFolder`パラメーターを使用してデフォルトのルートフォルダーを変更できます。操作ごとのサブフォルダーの作成と管理は、前述のとおりです。

サブフォルダーにコピーされるファイル

以下のファイルを除き、拡張子が「.yml」のすべてのファイルは操作サブフォルダーにコピーされます。

- CustomerInfo.yml
- ZoneMapping.yml
- CvadAcSecurity.yml

自動フェイルセーフクラウドサイトバックアップ

構成を変更する操作を実行する前に、現在のクラウドサイト構成のバックアップが作成されます。これには、`Import`、`Merge`、`Sync`、および`Restore`パラメーターが含まれます。バックアップは常に、操作サブフォルダーの下のサブフォルダーに保存されます。

`Restore`の場合、バックアップフォルダーは`-RestoreFolder`パラメーターで指定されたフォルダーのサブフォルダーです。

自動化

自動構成ツールコマンドレットは、プロンプトとコマンドレット完了時のログ結果の表示を抑制することで、管理者による介入なしに自動化スクリプトで実行できます。CustomerInfo.ymlファイルを使用して、同じことを行うようにパラメーターを設定することもできます。

プロンプトの表示を抑制するには、クラウド変更コマンドレットに次のパラメーターを追加します。

```
-Confirm $false
```

コマンドレットの完了時にログの表示を抑制するには、コマンドレットに次のパラメーターを追加します。

```
-DisplayLog $false
```

PowerShellコマンドウィンドウへのログ記録を抑制するために、cmdletに次のパラメータを追加します。

```
-Quiet
```

別の方法として、次のパラメーターをCustomerInfo.ymlファイルに配置できます。

```
Confirm: False
```

```
DisplayLog: False
```

Delivery Controller™以外のPCからのエクスポート

自動構成ツールは、複数のCitrix PowerShell SDKを使用して、オンプレミスサイトの構成をファイルにエクスポートします。これらのSDKはDelivery Controllerに自動的にインストールされるため、追加の操作なしでツールをDelivery Controllerで実行できます。Delivery Controller以外のマシンで実行する場合は、ツールが必要とするCitrix PowerShell SDKのセットをインストールする必要があります。このSDKセットはCitrix Studioの一部であり、Citrix Virtual Apps and Desktops™インストールメディアからインストールできます。

> **注:**
>
> 自動構成はCloud Connectorでは実行できません。

Citrix Cloud™ GovernmentおよびJapan Control Planeへの移行

Citrix Cloud GovernmentおよびJapan Control Plane環境では、認証およびアクセストークンの割り当てに異なるアクセスポイントを使用します。この固有の要件は、クラウドにアクセスするすべての自動構成ツールに適用されます。これらの環境で自動構成を使用するには、次の手順を実行します。

1. *%HOMEPATH%\Documents\Citrix\AutoConfig*フォルダーで、CustomerInfo.ymlを編集します。
2. 接続する環境に応じて、次のいずれかの行をCustomerInfo.ymlに追加します（または、すでに存在する場合は変更します）。

   ```
   Environment: 'ProductionGov'
   ```

   または

   ```
   Environment: 'ProductionJP'
   ```

これらの環境で自動構成を使用できるようになりました。

Citrix Cloud データ収集

Citrix Cloud が収集する情報については、Citrix Cloud Services の顧客コンテンツとログの処理を参照してください。

その他のリソース

ディスカッションフォーラム

Citrix 自動構成ディスカッションフォーラムにアクセスしてください。

ビデオ

YouTubeでCitrix Virtual Apps and Desktops 用自動構成ツールの内部を視聴する。

トレーニング

Cloud Learning Center には、この記事で説明されているタスクを含む、サービス展開を構築するためのステップバイステップのビデオガイドが用意されています。Citrix Virtual Apps and Desktops を Citrix Cloud に移行する学習パスを参照してください。

オートスケール™

> **注:**

> Citrix Virtual Apps and Desktops™展開は、Web Studio (Webベース) と Citrix Studio (Windowsベース) の2つの管理コンソールを使用して管理できます。この機能はWeb Studioでのみ利用可能です。

> Autoscaleは、マシンをプロアクティブに電力管理するための、一貫性のある高性能なソリューションを提供する機能です。コストとユーザーエクスペリエンスのバランスを取ることを目的としています。

Autoscaleは、デリバリーグループ内の登録されているすべてのシングルセッションおよびマルチセッションOSマシンのプロアクティブな電源管理を可能にします。

Autoscaleの機能は次のとおりです。

- スケジュールベースおよび負荷ベースの設定(/ja-jp/citrix-virtual-apps-desktops/2503/manage-deployment/autoscale/schedule-based-and-load-based-settings.html)
- 動的セッションタイムアウト(/ja-jp/citrix-virtual-apps-desktops/2503/manage-deployment/autoscale/dynamic-session-timeout.html)
- Autoscaleタグ付きマシン (クラウドバースト)(/ja-jp/citrix-virtual-apps-desktops/2503/manage-deployment/autoscale/autoscale-tagged-machines.html)
- ユーザーログオフ通知(/ja-jp/citrix-virtual-apps-desktops/2503/manage-deployment/autoscale/force-user-logoff.html)

一般的なユースケース

以下は、Autoscaleが一般的に使用されるシナリオです。

- 予想されるワークロードを処理するためのスケジュールベースのマシンの電源オン

  Autoscaleを使用すると、管理者は電源オン容量を30分単位で変更でき、異なる日に異なるスケジュールを設定できます。変動の激しいワークロードが予想される場合は、ユーザーがマシンの電源オンを待つ必要がないように、容量バッファを設定することをお勧めします。

- クラウドバーストのユースケース

  Autoscaleは、デリバリーグループ内のマシンの一部のみを電源管理する柔軟性を提供します。これを実現するには、1つ以上のマシンにタグを適用し、その後、Autoscaleを構成してタグ付きマシンのみを電源管理します。

この機能は、クラウドベースのリソースが追加の需要 (つまり、バーストワークロード) に対応する前に、オンプレミスリソース (または予約済みのパブリッククラウドインスタンス) を使用してワークロードを処理したいクラウドバーストのユースケースで役立ちます。

- 徐々に増加するユーザーまたは季節的なユーザー

  組織が徐々にユーザーをオンボーディングしており、事前に全容量をプロビジョニングしたくない場合、動的プロビジョニング機能が役立ちます。この機能は、デリバリーグループの負荷を常に評価し、現在の負荷状況に基づいてデリバリーグループ内のマシンの数を動的にスケールアップまたはスケールダウンします。管理者は、マシンを作成するために、デリバリーグループの負荷の上限と下限のウォーターマークを定義する必要があります。管理者は、オプションでプロビジョニングされるマシンの最大数と、これらのマシンに適用されるタグを定義できます。

サポートされているVDAホスティングプラットフォーム

Autoscaleは、Citrix Virtual Apps and Desktopsがサポートするすべてのプラットフォームをサポートしています。これには、XenServer、Amazon Web Services、Google Cloud Platform、Microsoft Azure Resource Manager、VMware vSphereなど、さまざまなインフラストラクチャプラットフォームが含まれます。サポートされているプラットフォームの完全なリストについては、Citrix Virtual Apps and Desktopsのシステム要件を参照してください。

> **注:**
>
> 展開にパブリッククラウドホスト接続を追加する場合、ハイブリッドライツライセンスが必要です。ハイブリッドライツライセンスの詳細については、ハイブリッドライツによる移行とトレードアップ (TTU)を参照してください。ライセンスの追加については、サイトの作成を参照してください。

サポートされているワークロード

Autoscaleは、マルチセッションOSとシングルセッションOSの両方のデリバリーグループをサポートしています。留意すべきユーザーインターフェイスは3つあります。

- マルチセッションOSデリバリーグループ (旧称RDSデリバリーグループ) 用のAutoscaleユーザーインターフェイス
- シングルセッションOSランダム (プール型) デリバリーグループ (旧称プール型VDIデリバリーグループ) 用のAutoscaleユーザーインターフェイス

- シングルセッションOS静的デリバリーグループ (旧称静的VDIデリバリーグループ) 用のAutoscaleユーザーインターフェイス

さまざまなデリバリーグループのユーザーインターフェイスの詳細については、Autoscaleユーザーインターフェイスを参照してください。

利点

Autoscale機能には、次の利点があります。

- デリバリーグループ内のマシンを電源管理するための、単一で一貫したメカニズムを提供します。
- 負荷ベースまたはスケジュールベースの電源管理、あるいはその両方の組み合わせによってマシンの電源を管理することで、可用性を確保し、コストを制御します。
- コスト削減やキャパシティ使用率などのメトリックを監視し、通知を有効にするには、Directorを使用します。

2分間のビデオを見る

次のビデオでは、Autoscaleの簡単な概要を説明します。

<iframe src="https://www.youtube.com/embed/5yxERrFZQ68" width="720px" height="480px" frameborder="0" title="YouTube video player" allowfullscreen=""> </iframe>

Autoscale™ の使用を開始する

Autoscale は、構成されたスケジュールまたは負荷要求に基づいてデリバリーグループをプロアクティブにスケーリングするための、一貫性のある高性能な電源管理ソリューションを提供する機能です。

Autoscale は、すべての種類のデリバリーグループに適用されます。

- シングルセッション静的OS
- シングルセッションランダムOS
- マルチセッションランダムOS

この記事では、Autoscale に関連する基本的な概念について説明し、デリバリーグループで Autoscale を有効にして構成する方法に関するガイダンスを提供します。

基本的な概念

開始する前に、Autoscale の次の基本的な概念について学習してください。

- 容量とマシンの登録
- 複数のマシンカタログにわたるスケーリング
- マシンのプロビジョニングとセッションの需要
- インスタンスサイズの考慮事項
- スケジュール
- ピーク時とオフピーク時
- 電源オフ遅延
- プールサイズ
- 容量バッファ
- 負荷インデックス
- Autoscaleとメンテナンスモード
- マシンコスト
- デリバリーグループのスケールアップ
- デリバリーグループのスケールダウン
- ドレイン状態

容量とマシンの登録

Autoscaleは、容量を決定する際にサイトに登録されているマシンのみを含めます。登録されていない電源オンのマシンは、セッション要求を受け入れることができません。その結果、それらはデリバリーグループ全体の容量には含まれません。

複数のマシンカタログにわたるスケール

一部のサイトでは、複数のマシンカタログが単一のデリバリーグループに関連付けられている場合があります。Autoscaleは、スケジュールまたはセッションの需要要件を満たすために、各カタログからマシンをランダムに電源オンにします。

たとえば、あるデリバリーグループには2つのマシンカタログがあります。カタログAには3台のマシンが電源オンになっており、カタログBには1台のマシンが電源オンになっています。Autoscaleが追加のマシンを電源オンにする必要がある場合、カタログAまたはカタログBのいずれかのマシンを電源オンにする可能性があります。

マシンのプロビジョニングとセッションの需要

デリバリーグループに関連付けられているマシンカタログには、需要の増減に応じて電源をオン/オフするのに十分なマシンが必要です。セッション需要がデリバリーグループ内の登録済みマシ

ンの総数を超えた場合、Autoscaleはすべての登録済みマシンの電源がオンになっていることを保証します。ただし、**Autoscaleは追加のマシンをプロビジョニングしません。**

> **注:**
>
> デリバリーグループに63台のマシンがあり、営業時間外に10%のバッファ容量が設定されている場合、Autoscaleの計算に従って、営業時間外には6.3台のマシンがオンになっている必要があります。小数値を処理するためのルールは次のとおりです。
>
> - 最も近い値に丸める：たとえば、値が6.4の場合、6台のマシンがオンになります。値が6.7の場合、7台のマシンがオンになります。
> - 1未満のゼロ以外の値はすべて1に丸める：たとえば、値が0.2または0.9の場合、1台のマシンがオンになります。

インスタンスサイズの考慮事項

パブリッククラウドでインスタンスを適切にサイジングすると、コストを最適化できます。ワークロードのパフォーマンスと容量要件に合致する限り、より小さなインスタンスをプロビジョニングすることをお勧めします。

小さいインスタンスは、大きいインスタンスよりも少ないユーザーセッションをホストします。そのため、最後のユーザーセッションがログオフされるまでの時間が短いため、Autoscaleはマシンをより速くドレイン状態にします。結果として、Autoscaleは小さいインスタンスの電源をより早くオフにし、コストを削減します。

スケジュール

Autoscaleは、設定したスケジュールに基づいて、デリバリーグループ内のマシンの電源をオン/オフします。

スケジュールには、各時間帯のアクティブなマシンの数と、ピーク時およびオフピーク時が定義されています。

スケジュールの設定は、デリバリーグループの種類によって異なります。詳細については、以下を参照してください。

- マルチセッションOSデリバリーグループ
- シングルセッションOSランダムデリバリーグループ
- シングルセッションOS静的デリバリーグループ

ピーク時とオフピーク時

ピーク時とオフピーク時は、1日の特定の期間にどの容量バッファ値を使用するかを示すために使用されます。ピーク時間を定義し、残りの未定義の時間をオフピーク時間として残すことができます。

電源オフ遅延

電源オフ遅延とは、Autoscaleがマシンを電源オフにする前に、マシンが電源オンになってから経過しなければならない最小分数です。これにより、セッション需要が不安定なときにマシンがオンとオフを繰り返すのを防ぎます。デフォルトでは、電源オフ遅延は30分です。0〜60分の範囲で設定できます。

プールサイズ

プールサイズとは、1日の特定の期間に電源オンの状態を維持する必要があるマシンの数です。

容量バッファ

容量バッファは、動的な負荷増加に対応するために、現在の需要に予備容量を追加するために使用されます。注意すべき2つのシナリオがあります。

- マルチセッションOSデリバリーグループの場合、キャパシティバッファは、負荷インデックスの観点から、デリバリーグループの総容量のパーセンテージとして定義されます。
- シングルセッションOSデリバリーグループの場合、キャパシティバッファは、デリバリーグループ内のマシンの総数のパーセンテージとして定義されます。

キャパシティバッファはローリングバッファであり、構成されたプールサイズに加えて計算および適用されるのではなく、現在の使用状況に基づいて計算および適用されます。

たとえば、10台のマシンを持つデリバリーグループ、現在の期間のプールサイズが1台のマシン、キャパシティバッファが10%であるとします。スケジュールで定義された1台の電源オンマシンが、10%のキャパシティバッファが満たされなくなるまで負荷がかかったときに、追加のマシンが電源オンになります。2台目のマシンを電源オンにした後で負荷が減少し、10%のキャパシティバッファを満たすのに十分すぎるほどの空き負荷容量がある場合、Autoscaleは1台のマシンの電源オフを準備します。

負荷インデックス

> **重要:**
>
> 負荷インデックスは、マルチセッションデリバリーグループにのみ適用されます。

> ロードインデックスメトリックは、マシンがユーザーログオン要求を受信する可能性を決定します。これは、同時ログオン、セッション、CPU、ディスク、およびメモリ使用のために構成された**Citrix Load Management policy**設定を使用して計算されます。

ロードインデックスは0から10,000の範囲です。デフォルトでは、マシンが250セッションをホストしている場合、完全にロードされていると見なされます。

- 数字の「0」は、アンロードされたマシンを示します。ロードインデックス値が0のマシンは、ベースラインロードの状態です。
- 「10,000」は、これ以上セッションを実行できない完全にロードされたマシンを示します。

Autoscaleとメンテナンスモード

メンテナンスモードのマシンは、その可用性ステータスに関係なく、全体のプールサイズの計算の一部と見なされます。したがって、プール内のすべてのマシンがメンテナンスモードになる可能性があります。ただし、これらのマシンは容量バッファの計算から除外され、即時の可用性が保証されます。ユーザー接続のために特定の割合のマシンがアクセス可能であることを保証するには、プールサイズとバッファ値を適切に調整してください。

マシンコスト

マシンインスタンスの1時間あたりのコストとは、使用されているコンピューティング容量の1時間あたりのコスト（米ドル）のことです。この設定は、Autoscale設定によるコスト削減を計算するために使用されます。削減額を表示するには、「**Director > コスト最適化 > コスト削減**」に移動します。

デリバリーグループのスケールアップ

Autoscaleは、Autoscaleが有効なデリバリーグループで、次の場合に追加のマシンの電源をオンにします。

1. デリバリーグループのAutoscaleスケジュールが、現在の期間により多くのマシンの電源をオンにする必要があることを示している場合。
2. デリバリーグループの現在の負荷が容量バッファを超過した場合。

マシンの電源をオンにする条件：

1. メンテナンスモードではないこと。
2. ハイパーバイザーがメンテナンスモードではないこと。
3. 電源オフで未登録。
4. スケールアップが必要なデリバリーグループに属している

5. 保留中の電源操作がない。

デリバリーグループをスケールダウンする

Autoscale は、Autoscale が有効なデリバリーグループ内のマシンの電源を、次の場合にオフにします。

1. Autoscaleスケジュールが、現在の期間に設定されたマシン数に合わせるためにマシンを電源オフにする必要があると指定している場合。
2. デリバリーグループの現在の負荷が低下し、プールサイズと容量バッファを満たすために必要な数よりも多くの電源オン状態のマシンが存在する場合。

Autoscale は、プールサイズと容量バッファを満たすために必要な数を超える余分なマシンの電源をオフにすることで、デリバリーグループをスケールダウンします。

スケールダウンプロセスには2つのステップがあります。

1. 必要な数のマシンをドレイン状態にする。
2. 電源オフにするために、すべてのドレイン状態のマシンを選択する。

電源オフの対象となるマシンは、次の条件を満たす必要があります。

1. メンテナンスモードではない
2. ハイパーバイザーがメンテナンスモードではない
3. 現在電源オンの状態である
4. 利用可能として登録されているか、起動後に登録を待機している
5. ドレイン状態であり、アクティブなセッションがない
6. 保留中の電源操作がない
7. 電源オフ遅延を満たしている

ドレイン状態

Autoscale は、デリバリーグループ内の電源オン状態のマシンの数を、構成されたプールサイズと容量バッファにまでスケールダウンしようとします。

この目標を達成するために、Autoscale はセッション数が最も少ない余分なマシンを「ドレイン状態」にし、すべてのセッションがログオフされたときに電源をオフにします。この動作は、セッションの需要が減少し、スケジュールで電源オン状態のマシンよりも少ないマシンが必要な場合に発生します。

マシンがドレイン状態になる条件:

1. 電源オン状態である
2. メンテナンスモードではない
3. ハイパーバイザーがメンテナンスモードではない
4. スケールダウンが必要なデリバリーグループに属している
5. 現在のアクティブセッション数が最も少ない

注:

- 電源オフ遅延で指定された時間以上電源がオンになっているマシンは、ドレインの対象として優先されます。
- ドレイン状態のマシンは、新しいセッションの起動をホストしなくなり、既存のセッションがログオフされるのを待ちます。マシンは、すべてのセッションがログオフされた場合にのみシャットダウンされます。ただし、セッション起動にすぐに利用できるマシンがない場合、Autoscaleはマシンの電源を入れるよりも、ドレイン状態のマシンにセッション起動を誘導することを優先します。

Autoscale は、余分なマシンを「ドレイン状態」に1台ずつ移行します。

- 2台以上のマシンが同じ数のアクティブセッションを持っている場合、Autoscale は、指定された電源オフ遅延の間電源がオンになっていたマシンをドレインします。

  そうすることで、最近電源がオンになったマシンがドレイン状態になるのを避けることができます。なぜなら、それらのマシンはセッション数が最も少ない可能性が高いからです。
- 2台以上のマシンが指定された電源オフ遅延の間電源がオンになっていた場合、Autoscale はそれらのマシンをランダムに1台ずつドレインします。

ドレイン状態のマシンは、新しいセッションの起動をホストしなくなり、既存のセッションがログオフされるのを待っています。マシンは、すべてのセッションがログオフされた場合にのみシャットダウンの候補になります。ただし、セッション起動にすぐに利用できるマシンがない場合、Autoscale は、マシンの電源をオンにするよりも、ドレイン状態のマシンにセッション起動を誘導することを優先します。

次のいずれかの条件が満たされると、マシンはドレイン状態から解除されます。

- マシンの電源がオフになります。
- マシンが属するデリバリーグループでAutoscaleが無効になっています。

- Autoscaleは、スケジュールまたは負荷需要の要件を満たすためにマシンを使用します。このケースは、スケジュール（スケジュールベースのスケーリング）または現在の需要（負荷ベースのスケーリング）が、現在電源がオンになっているマシンの数よりも多くのマシンを必要とする場合に発生します。

> **重要:**
>
> セッション起動にすぐに利用できるマシンがない場合、Autoscale は、マシンの電源をオンにするよりも、ドレイン状態のマシンにセッション起動を誘導することを優先します。セッション起動をホストするドレイン状態のマシンは、ドレイン状態のままになります。

どのマシンがドレイン状態にあるかを確認するには、`Get-BrokerMachine` PowerShellコマンドを使用します。例: `Get-BrokerMachine -DrainingUntilShutdown $true`。または、Studioを使用することもできます。「ドレイン状態のマシンを表示する」を参照してください。

ドレイン状態のマシンを表示する

> **注:**
>
> この機能は、マルチセッションマシンにのみ適用されます。

Studioでは、ドレイン状態のマシンを表示して、どのマシンがシャットダウンしようとしているかを知ることができます。次の手順を実行します。

1. **検索**ノードに移動し、**表示する列**をクリックします。
2. **表示する列**ウィンドウで、**ドレイン状態**の横にあるチェックボックスをオンにします。
3. **保存**をクリックして、**表示する列**ウィンドウを終了します。

ドレイン状態列には、次の情報が表示されます。

- **シャットダウンまでドレイン中。** マシンがシャットダウンされるまでドレイン状態にある場合に表示されます。
- **ドレインしていません。** マシンがまだドレイン状態にない場合に表示されます。

ドレイン状態(/en-us/citrix-virtual-apps-desktops/2503/media/drain-state.png)

デリバリーグループのAutoscaleを有効にする

デリバリーグループを作成すると、Autoscaleはデフォルトで無効になります。Web Studioを使用してデリバリーグループのAutoscaleを有効にして構成するには、次の手順に従います。

PowerShellコマンドを使用して、デリバリーグループのAutoscaleを有効にして構成することもできます。詳細については、Broker PowerShell SDKコマンドを参照してください。

1. 左側のペインで**デリバリーグループ**を選択します。
2. 管理するデリバリーグループを選択し、**Autoscaleの管理**をクリックします。

   クラウドUI(/en-us/citrix-virtual-apps-desktops/2503/media/autoscale-cloud.png)
3. 「**Autoscaleの管理**」ページで、「**Autoscaleを有効にする**」チェックボックスをオンにしてAutoscaleを有効にします。Autoscaleを有効にすると、ページ上のオプションが有効になります。

   クラウドUI(/en-us/citrix-virtual-apps-desktops/2503/media/autoscale-general-ss-static.png)
4. 組織のニーズに基づいてデフォルト設定を変更するには、以下の設定を完了します。

   - スケジュールを設定する(/ja-jp/citrix-virtual-apps-desktops/2503/manage-deployment/autoscale/schedule-based-and-load-based-settings.html#single-session-os-static-delivery-groups)
   - 非アクティブなマシンをより効率的に電源オフにするには、動的セッションタイムアウトとユーザーログオフ通知を使用します。
   - デリバリーグループ内のマシンの一部を電源管理するには、タグ付けされたマシンのAutoscaleを使用します。

Autoscaleを無効にするには、「**Autoscale**」チェックボックスをオフにします。ページ上のオプションは灰色表示になり、選択したデリバリーグループでAutoscaleが無効になっていることを示します。

> **重要：**
>
> - Autoscaleを無効にすると、Autoscaleによって管理されていたすべてのマシンは、無効化された時点の状態を維持します。
> - Autoscaleを無効にすると、ドレイン状態のマシンはドレイン状態から解除されます。ドレイン状態の詳細については、ドレイン状態を参照してください。

- 「**負荷ベースの設定**」ページにあるシングルセッションOS静的デリバリーグループおよびシングルセッションOSランダムデリバリーグループの「**電源ポリシー**」アクションは、Autoscaleの設定（有効または無効）とは独立しています。

ユーザーセッションを持つVMのAutoscaleオプション

Autoscaleは、割り当て済みマシンとプールされたマシンの両方を管理し、それらの電源と可用性を最適化できます。以下のコンテンツでは、ピーク時とオフピーク時、および割り当て済みマシンとプールされたマシンのユーザーセッションに基づいて、マシンの電源状態を制御するためのPowerShellコマンドとUI設定について説明します。

割り当てられたマシンは単一ユーザー専用ですが、プールされたマシンは複数のユーザー間で共有されます。

注：

Citrix Studioのセッション制限ポリシー、特に*切断セッションタイマー*と*セッションアイドルタイマー*は、Citrix Autoscaleが有効になっていない場合でも、ユーザーセッションを管理するために非常に重要です。これらのポリシーは、セッションが切断またはアイドル状態のまま終了されるまでの時間を定義し、リソースの利用を確保し、ロックアウトされたセッションを防ぎます。このポリシー設定は、割り当て済みマシンとプールされたマシンの両方、特にマルチセッションVDAを実行しているマシンで使用できます。詳細については、「セッション制限ポリシー設定」を参照してください。

割り当て済みマシンについて

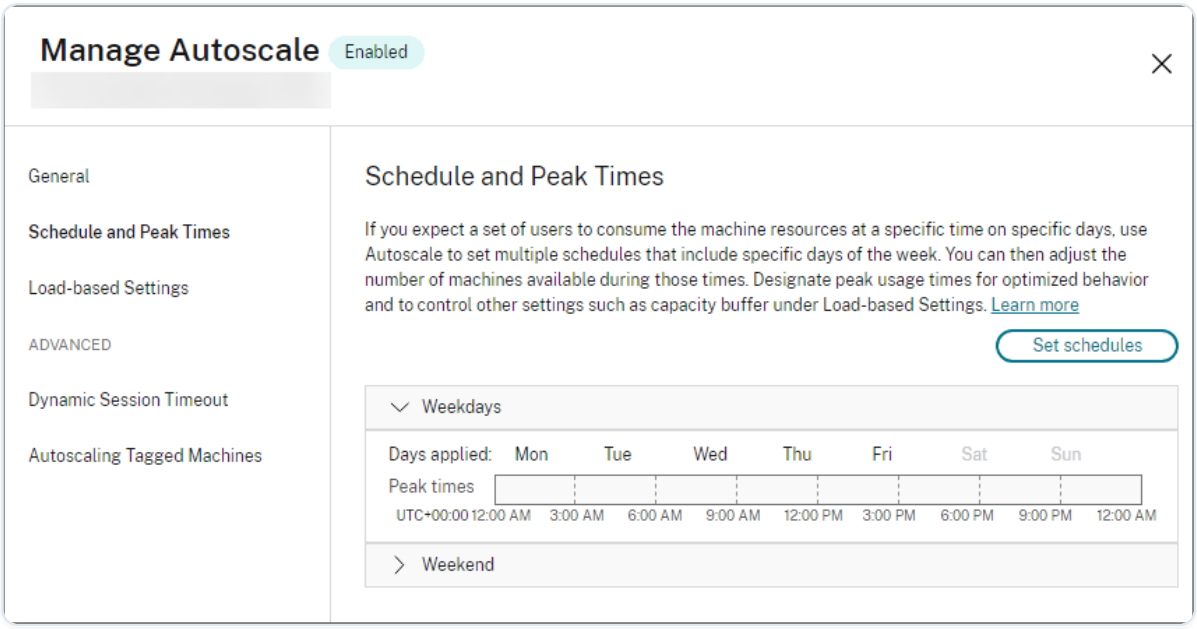
- ピーク時間の開始時に静的デリバリーグループ内の割り当て済みシングルセッションマシンを自動的に電源オンにするには、次のPowerShellコマンドを使用します。

```
Set-BrokerDesktopGroup "Desktop Group Name"
-AutomaticPowerOnForAssigned $True
```

- ピーク時間中に電源がオフになっている割り当て済みマシンが再起動されるようにするには、`AutomaticPowerOnForAssignedDuringPeak`も有効にします。

```
Set-BrokerDesktopGroup "Desktop Group Name"
-AutomaticPowerOnForAssigned $True
-AutomaticPowerOnForAssignedDuringPeak $True
```

- ユーザーがセッションを起動したときにのみVMをオンにしたい場合は、次のいずれかを実行します。
  - `AutomaticPowerOnForAssigned`と`AutomaticPowerOnForAssignedDuringPeak`を`False`に設定します。
  - UIインターフェイスを使用して、すべての時間をピーク時間なしのオフピークとして定義します。「スケジュールベースの設定」を参照してください。オフピーク時間中、Autoscaleで管理されている割り当て済みマシンは、ユーザーセッションがない場合にシャットダウンされます。



- ピーク時にすべてのマシンがAutoscaleによって電源オンにされる場合、UIインターフェイスを使用して、待機時間（分）と、Autoscaleによってマシンが電源オンになった後にユーザーがログオンしない場合の「アクションなし」、「一時停止」、「シャットダウン」などのアクションを設定します。「電源ポリシー」を参照してください。

プールされたマシンについて

セッションログオフ後にプールされたマシンを自動的にシャットダウンするには、デリバリーグループに対してPowerShellコマンド`ShutdownAfterUse`を`True`に設定します。例:

```
Set-BrokerDesktopGroup -Name “DesktopGroupName” -ShutdownDesktopsAfterUse
$true
```

メトリックの監視

デリバリーグループでAutoscaleを有効にすると、DirectorからAutoscaleで管理されているマシンの次のメトリックを監視できます。

- マシンの使用状況
- 推定節約額
- マシンとセッションのアラート通知
- マシンのステータス
- 負荷評価の傾向

> **注:**
>
> デリバリーグループでAutoscaleを最初に有効にすると、そのデリバリーグループの監視データが表示されるまでに数分かかる場合があります。 Autoscaleがデリバリーグループで有効化され、その後無効化された場合でも、監視データは引き続き利用可能です。Autoscaleは5分間隔で監視データを収集します。

> メトリックの詳細については、「Autoscaleで管理されるマシンの監視」を参照してください。

休止状態のVMでのAutoscale

Autoscaleの構成可能な設定を通じてVMを休止状態にできます。PowerShellコマンド `Get-BrokerDesktopGroups`、`New-BrokerDesktopGroups`、または `Set-BrokerDesktopGroups` を使用して、パラメーター `AutoscaleScaleDownActionDuringPeak`（ピーク時）または `AutoscaleScaleDownActionDuringOffPeak`（オフピーク時）に以下の正の値を設定し、電源アクションを定義します。

- 0：スケールダウン時にVMをシャットダウンする
- 1：スケールダウン時に一時停止（VMを休止状態にする）

休止状態にできないVMはシャットダウンされます。

デリバリーグループで休止状態が有効になっている場合、休止状態のVMの再起動スケジュールを構成できます。再起動サイクルでは、VMは再開され、その後シャットダウンされます。再起動スケジュールは、毎週、毎日、毎月、および1回に設定できます。複数のスケジュールを構成できます。ただし、休止状態から再開するVMには数分かかる場合があります。

Autoscaleは、ピーク時にセッションがない休止状態のマルチセッションRemote Desktop Services (RDS) および共有シングルセッションVMの電源をオンにすることもできます。VMはMCSおよび非MCSマシンカタログのいずれでもかまいません。

詳細情報

Autoscaleの詳細については、Tech ZoneのCitrix Autoscaleを参照してください。

スケジュールベースおよび負荷ベースの設定

Autoscale™ がマシンを電源管理する方法

Autoscale は、選択されたスケジュールに基づいてマシンの電源をオン/オフします。Autoscale を使用すると、特定の曜日を含む複数のスケジュールを設定し、それらの時間帯に利用可能なマシンの数を調整できます。特定の曜日の特定の時間に一連のユーザーがマシンリソースを消費すると予想される場合、Autoscale は最適化されたエクスペリエンスを提供するのに役立ちます。これらのマシンは、セッションが実行されているかどうかにかかわらず、スケジュール中に電源がオンになることに注意してください。

> **注:**
>
> Autoscale は、あらゆる電源管理マシンをサポートします。

> スケジュールは、デリバリーグループの**タイムゾーン**に基づいています。タイムゾーンを変更するには、デリバリーグループのユーザー設定を変更できます。詳細については、「デリバリーグループの管理」を参照してください。

Autoscale には、2つのデフォルトスケジュールがあります。*平日*（月曜日から金曜日）と*週末*（土曜日と日曜日）です。デフォルトでは、**平日**スケジュールは、ピーク時には午前7時から午後6時30分まで1台のマシンの電源をオンにし、オフピーク時には電源をオンにしません。デフォルトの容量バッファは、ピーク時とオフピーク時に10%に設定されています。デフォルトでは、**週末**スケジュールはマシンの電源をオンにしません。

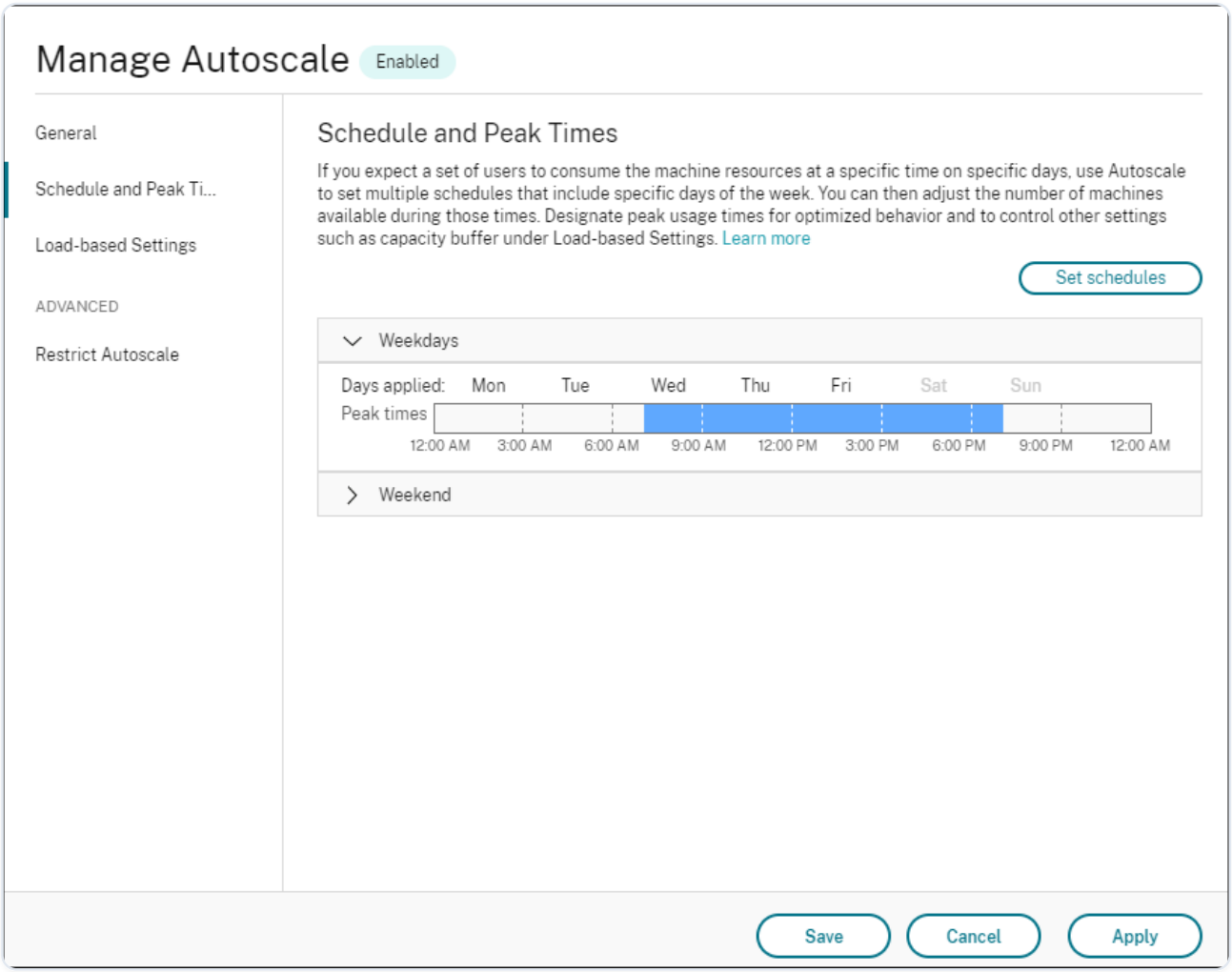
> **注:**
>
> Autoscale は、サイトに登録されているマシンのみを、計算における利用可能な容量の一部として扱います。「登録済み」とは、マシンが使用可能であるか、すでに使用中であること

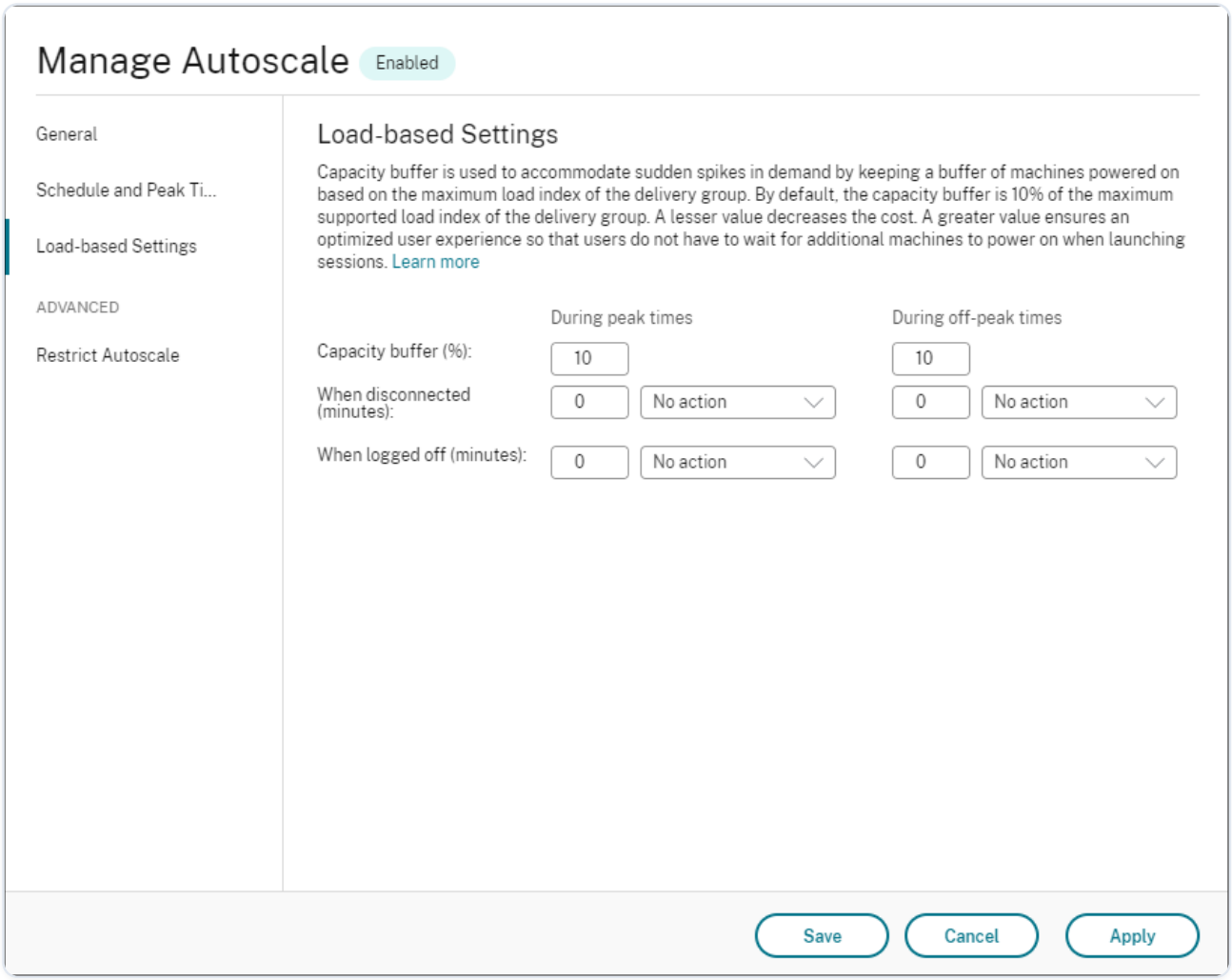
を意味します。これにより、ユーザーセッションを受け入れることができるマシンのみがデリバリーグループの容量に含まれることが保証されます。

ユーザーインターフェイス

留意すべきユーザーインターフェイスは3種類あります。

*シングルセッションOS静的デリバリーグループ*のユーザーインターフェイス:





*シングルセッションOSランダムデリバリーグループ*のAutoscaleユーザーインターフェイス:

Autoscale シングルセッションOS (ランダム) - スケジュール(/en-us/citrix-virtual-apps-desktops/2503/media/autoscale-schedule-ss-random.png)

Autoscale シングルセッションOS (ランダム) - 負荷ベース(/en-us/citrix-virtual-apps-desktops/2503/media/autoscale-load-based-ss-random.png)

Autoscale のユーザーインターフェイス（*マルチセッションOSデリバリーグループ*）：

Autoscale マルチセッションOS - スケジュール(/en-us/citrix-virtual-apps-desktops/2503/media/autoscale-schedule-ms.png)

Autoscale マルチセッションOS - 負荷ベース(/en-us/citrix-virtual-apps-desktops/2503/media/autoscale-load-based-settings-ms.png)

スケジュールベースの設定

Autoscale スケジュール。スケジュールの追加、編集、選択、削除ができます。

適用される曜日。選択したスケジュールに適用した曜日を強調表示します。残りの曜日はグレー表示されます。

編集。1時間ごとまたは30分ごとにマシンを割り当てることができます。マシンは数値またはパーセンテージで割り当てることができます。

注：

- このオプションは、マルチセッションOSおよびシングルセッションOSのランダムデリバリーグループのAutoscaleユーザーインターフェイスでのみ利用可能です。
- **編集**の横にあるヒストグラムは、異なる時間帯で実行されているマシンの数または割合を示します。
- **ピーク時間**の上にある**編集**をクリックして、各時間帯に**マシンを割り当てる**ことができます。**起動するマシン**ウィンドウのメニューから選択したオプションに応じて、マシンを数値またはパーセンテージで割り当てることができます。
- マルチセッションOSデリバリーグループの場合、各日において30分単位で実行中のマシンの最小数を個別に設定できます。シングルセッションOSのランダムデリバリーグループの場合、各日において60分単位で実行中のマシンの最小数を個別に設定できます。

独自のスケジュールを定義するには、次の手順に従います。

1. 「**Manage Autoscale**」ウィンドウの「**Schedule and Peak Times**」ページで、「**Set schedules**」をクリックします。
2. 「**Edit Autoscale Schedules**」ウィンドウで、各スケジュールに適用する日を選択します。必要に応じてスケジュールを削除することもできます。
3. スケジュールを保存して「**Schedule and Peak Times**」ページに戻るには、「**Done**」をクリックします。
4. 該当するスケジュールを選択し、必要に応じて構成します。
5. 「**Manage Autoscale**」ウィンドウを終了するか、他のページで設定を構成するには、「**Apply**」をクリックします。

重要:

- Autoscaleでは、異なるスケジュールで同じ日が重複することはできません。たとえば、schedule1で月曜日を選択した後、schedule2で月曜日を選択すると、schedule1の月曜日は自動的にクリアされます。
- スケジュール名は大文字と小文字を区別しません。
- スケジュール名は空白にしたり、スペースのみを含めたりすることはできません。
- Autoscaleでは、文字間に空白スペースを使用できます。
- スケジュール名には、次の文字を含めることはできません: \ / ; : # . * ? = < > \| ( ) { } " ' `。
- Autoscaleは重複するスケジュール名をサポートしていません。各スケジュールに異なる名前を入力してください。
- Autoscaleは空のスケジュールをサポートしていません。つまり、日が選択されていないスケジュールは保存されません。

注:

選択したスケジュールに含まれる日は強調表示され、含まれない日はグレー表示されます。

負荷ベースの設定

ピーク時間。選択したスケジュールに適用した日のピーク時間を定義できます。これを行うには、横棒グラフを右クリックします。ピーク時間を定義すると、残りの未定義の時間はデフォルトでオフピーク時間になります。**デフォルト**では、午前7時から午後7時までの時間帯が、選択したスケジュールに含まれる日のピーク時間として定義されます。

重要：

- マルチセッションOSデリバリーグループの場合、ピーク時間棒グラフはキャパシティバッファに使用されます。
- シングルセッションOSデリバリーグループの場合、ピーク時間棒グラフはキャパシティバッファに使用され、ログオフ後および/または切断後にトリガーされるアクションを制御します。
- マルチセッションOSおよびシングルセッションOSデリバリーグループの両方で、スケジュールに含まれる日のピーク時間を30分単位で詳細に定義できます。または、代わり

に`New-BrokerPowerTimeScheme PowerShell`コマンドを使用することもできます。詳細については、「Broker PowerShell SDKコマンド」を参照してください。

キャパシティバッファ。電源がオンになっているマシンのバッファを維持できます。値が小さいほどコストが削減されます。値が大きいほど、セッション起動時にユーザーが追加のマシンの電源がオンになるのを待つ必要がないように、最適化されたユーザーエクスペリエンスが保証されます。デフォルトでは、キャパシティバッファはピーク時間とオフピーク時間で10%です。キャパシティバッファを0に設定すると、セッション起動時にユーザーが追加のマシンの電源がオンになるのを待つ必要がある場合があります。Autoscaleでは、ピーク時間とオフピーク時間でキャパシティバッファを個別に決定できます。

その他の設定

ヒント：

- Broker PowerShell SDKを使用してその他の設定を構成することもできます。詳細については、「Broker PowerShell SDKコマンド」を参照してください。
- 切断時およびログオフ時の設定に関連するSDKコマンドを理解するには、`<https://citrix.github.io/delivery-controller-sdk/Broker/about_Broker_PowerManagement/#power-policy>`を参照してください。

切断時。セッション切断後、切断されロックされたマシンがサスペンドまたはシャットダウンされるまで、どのくらいの期間電源がオンのままになるかを指定できます。時間値を指定すると、構成したアクションに応じて、指定された切断時間が経過したときにマシンがサスペンドまたはシャットダウンされます。デフォルトでは、切断されたマシンにはアクションが割り当てられません。ピーク時間とオフピーク時間でアクションを個別に定義できます。そのためには、下矢印をクリックし、メニューから次のいずれかのオプションを選択します。

- **アクションなし**。選択すると、セッション切断後もマシンは電源がオンのままになります。Autoscaleはそれに対してアクションを実行しません。
- **サスペンド**。選択すると、指定された切断時間が経過したときに、Autoscaleはマシンをシャットダウンせずに一時停止します。**サスペンド**を選択すると、次のオプションが使用可能になります。

    - **再接続がない場合（分）**。サスペンドされたマシンは、切断されたユーザーが再接続したときに利用可能ですが、新しいユーザーには利用できません。すべてのワークロードを処理するためにマシンを再度利用可能にするには、シャットダウンします。Autoscaleがそれらをシャットダウンするまでのタイムアウトを分単位で指定します。

- **シャットダウン**。選択した場合、指定された切断時間が経過すると、Autoscale はマシンをシャットダウンします。

> **注:**
>
> このオプションは、シングルセッションOSのランダムおよび静的デリバリーグループ向けのAutoscaleユーザーインターフェイスでのみ利用可能です。

> **ログオフ時**。セッションログオフ後、マシンがサスペンドまたはシャットダウンされるまでに電源がオンのままになる時間を指定できます。時間値を指定した場合、設定したアクションに応じて、指定されたログオフ時間が経過するとマシンはサスペンドまたはシャットダウンされます。デフォルトでは、ログオフされたマシンにはアクションが割り当てられません。ピーク時とオフピーク時でアクションを個別に定義できます。これを行うには、下矢印をクリックし、メニューから次のいずれかのオプションを選択します。

- **アクションなし**。選択した場合、セッションログオフ後もマシンは電源がオンのままになります。Autoscale はそれに対して何も実行しません。
- **サスペンド**。選択した場合、指定されたログオフ時間が経過すると、Autoscale はマシンをシャットダウンせずに一時停止します。
- **シャットダウン**。選択した場合、指定されたログオフ時間が経過すると、Autoscale はマシンをシャットダウンします。

> **注:**
>
> このオプションは、シングルセッションOSの静的デリバリーグループ向けのAutoscaleユーザーインターフェイスでのみ利用可能です。

切断されたセッションを持つシングルセッションOSマシンが異なる時間帯に移行する際の電源管理

重要:

- この機能強化は、切断されたセッションを持つシングルセッションOSマシンにのみ適用されます。ログオフされたセッションを持つシングルセッションOSマシンには適用されません。
- この機能強化を有効にするには、該当するデリバリーグループでAutoscaleを有効にする必要があります。そうしないと、期間移行時に切断電源ポリシーアクションはトリガーされません。

以前のリリースでは、アクション（切断アクション = 「**サスペンド**」または「**シャットダウン**」）が必要な時間帯に移行するシングルセッションOSマシンは、電源がオンのままでした。このシナリオは、アクション（切断アクション = 「**何もしない**」）が不要な時間帯（ピーク時またはオフピーク時）にマシンが切断された場合に発生しました。

このリリースから、Autoscale は、移行先の時間帯に設定された切断アクションに応じて、指定された切断時間が経過するとマシンをサスペンドまたは電源オフにします。

例えば、シングルセッションOSデリバリーグループに対して、以下の電源ポリシーを構成します。

- `PeakDisconnectAction` を「何もしない」に設定します
- `OffPeakDisconnectAction` を「シャットダウン」に設定します
- 'OffPeakDisconnectTimeout' を「10」に設定します

注：

注:

選択したスケジュールに含まれる曜日は強調表示され、含まれない曜日はグレー表示されます。

以前のリリースでは、ピーク時にセッションが切断されたシングルセッションOSマシンは、ピークからオフピークに移行しても電源がオンのままでした。このリリース以降、期間移行時に`OffPeakDisconnectAction`および`OffPeakDisconnectTimeout`ポリシーアク

ションがシングルセッションOSマシンに適用されます。その結果、マシンはオフピークに移行してから10分後に電源がオフになります。

以前の動作（つまり、切断されたセッションを持つマシンがピークからオフピーク、またはオフピークからピークに移行しても何もアクションを実行しない）に戻したい場合は、次のいずれかを実行します。

重要:

- マルチセッションOSデリバリーグループの場合、ピーク時間の棒グラフは容量バッファに使用されます。
- シングルセッションOSデリバリーグループの場合、ピーク時間の棒グラフは容量バッファに使用され、ログオフ後または切断後にトリガーされるアクションを制御します。
- マルチセッションOSおよびシングルセッションOSデリバリーグループの両方で、スケジュールに含まれる日のピーク時間を30分単位で細かく定義できます。または、代わりに`New-BrokerPowerTimeScheme PowerShell`コマンドを使用することもできます。詳細については、「Broker PowerShell SDKコマンド」を参照してください。

キャパシティバッファー。稼働中のマシンのバッファーを維持できます。値が小さいほどコストが削減されます。値が大きいほど、セッション起動時にユーザーが追加のマシンの電源がオンになるのを待つ必要がなくなり、最適化されたユーザーエクスペリエンスが保証されます。デフォルトでは、ピーク時とオフピーク時のキャパシティバッファーは10%です。キャパシティバッファーを0に設定すると、セッション起動時にユーザーが追加のマシンの電源がオンになるのを待つ必要がある場合があります。Autoscaleでは、ピーク時とオフピーク時でキャパシティバッファーを個別に決定できます。

その他の設定

ヒント:

- Broker PowerShell SDKを使用して、その他の設定を構成できます。詳しくは、「Broker PowerShell SDKコマンド」を参照してください。

- 切断時およびログオフ時の設定に関連するSDKコマンドについては、`<https://citrix.github.io/delivery-controller-sdk/Broker/about_Broker_PowerManagement/#power-policy>`を参照してください。

切断時。セッション切断後、切断されロックされたマシンが、中断またはシャットダウンされるまでにどのくらいの時間電源がオンのままになるかを指定できます。時間値を指定すると、構成したアクションに応じて、指定された切断時間が経過したときにマシンが中断またはシャットダウンされます。デフォルトでは、切断されたマシンにはアクションが割り当てられません。ピーク時とオフピーク時でアクションを個別に定義できます。そのためには、下矢印をクリックし、メニューから次のいずれかのオプションを選択します。

- **アクションなし**。選択すると、セッション切断後もマシンは電源がオンのままになります。Autoscaleはそれに対してアクションを実行しません。
- **中断**。選択すると、指定された切断時間が経過したときに、Autoscaleはマシンをシャットダウンせずに一時停止します。**中断**を選択すると、次のオプションが使用可能になります。
  - **再接続なしの場合（分）**。中断されたマシンは、切断されたユーザーが再接続する際には利用可能ですが、新しいユーザーには利用できません。すべてのワークロードを処理するためにマシンを再度利用可能にするには、シャットダウンします。Autoscaleがマシンをシャットダウンするまでのタイムアウトを分単位で指定します。
- **シャットダウン**。選択すると、指定された切断時間が経過したときに、Autoscaleはマシンをシャットダウンします。

注:

このオプションは、シングルセッションOSのランダムおよび静的デリバリーグループ用のAutoscaleユーザーインターフェイスでのみ使用できます。

ログオフ時。セッションログオフ後、マシンが中断またはシャットダウンされるまでにどのくらいの時間電源がオンのままになるかを指定できます。時間値を指定すると、構成したアクションに応じて、指定されたログオフ時間が経過したときにマシンが中断またはシャットダウンされます。デフォルトでは、ログオフされたマシンにはアクションが割り当てられません。ピーク時とオフピーク時でアクションを個別に定義できます。そのためには、下矢印をクリックし、メニューから次のいずれかのオプションを選択します。

- **アクションなし**。選択すると、セッションログオフ後もマシンは電源がオンのままになります。Autoscaleはそれに対してアクションを実行しません。
- **中断**。選択すると、指定されたログオフ時間が経過したときに、Autoscaleはマシンをシャットダウンせずに一時停止します。
- **シャットダウン**。選択すると、指定されたログオフ時間が経過したときに、Autoscaleはマシンをシャットダウンします。

> **注:**
>
> このオプションは、シングルセッションOSの静的デリバリーグループ用のAutoscaleユーザーインターフェイスでのみ使用できます。

切断されたセッションを持つ、異なる時間帯に移行するシングルセッションOSマシンの電源管理

> **重要:**
>
> - この機能強化は、切断されたセッションを持つシングルセッションOSマシンにのみ適用されます。ログオフされたセッションを持つシングルセッションOSマシンには適用されません。
> - この機能強化を有効にするには、該当するデリバリーグループでAutoscaleを有効にする必要があります。そうしないと、期間移行時に切断電源ポリシーアクションはトリガーされません。

> 以前のリリースでは、アクション（切断アクション = 「**一時停止**」または「**シャットダウン**」）が必要な時間帯に移行するシングルセッションOSマシンは、電源が入ったままでした。このシナリオは、マシンがアクション（切断アクション = 「**何もしない**」）が不要な時間帯（ピーク時またはオフピーク時）に切断された場合に発生しました。

このリリース以降、Autoscaleは、指定された切断時間が経過すると、移行先の時間帯に設定されている切断アクションに応じて、マシンを一時停止またはシャットダウンします。

例えば、シングルセッションOSデリバリーグループに対して、以下の電源ポリシーを設定します。

- `PeakDisconnectAction`を「Nothing」に設定します

- `OffPeakDisconnectAction`を「Shutdown」に設定します
- 「OffPeakDisconnectTimeout」を「10」に設定します

> **注:**
>
> 切断アクション電源ポリシーの詳細については、`<https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/about_Broker_PowerManagement/#power-policy>`および`<https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/Get-BrokerDesktopGroup/>`を参照してください。

> 以前のリリースでは、ピーク時にセッションが切断されたシングルセッションOSマシンは、ピークからオフピークに移行しても電源が入ったままでした。このリリース以降、期間移行時に`OffPeakDisconnectAction`および`OffPeakDisconnectTimeout`ポリシーアクションがシングルセッションOSマシンに適用されます。その結果、マシンはオフピークに移行してから10分後に電源がオフになります。

以前の動作（つまり、切断されたセッションを持つマシンがピークからオフピークへ、またはオフピークからピークへ移行しても何もしない）に戻したい場合は、次のいずれかを実行します。

- 「LegacyPeakTransitionDisconnectedBehaviour」レジストリ値を1（true; 以前の動作を有効にする）に設定します。デフォルトでは、値は0（false; 期間移行時に切断電源ポリシーアクションをトリガーする）です。
  - パス: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\DesktopServer
  - 名前: LegacyPeakTransitionDisconnectedBehaviour
  - 種類: REG_DWORD
  - データ: 0x00000001 (1)
- `Set-BrokerServiceConfigurationData` PowerShellコマンドを使用して設定を構成します。例:
  - `PS C:\> Set-BrokerServiceConfigurationData HostingManagement.LegacyPeakTransitionDisconnectedBehaviour -SettingValue $true`

マシンに期間移行時に電源ポリシーアクションを適用する前に、以下の条件を満たしている必要があります。

- 切断されたセッションがあります。
- 保留中の電源操作がない。
- 異なる時間帯に移行するシングルセッションOSデリバリーグループに属している。
- 特定時間帯（ピーク時またはオフピーク時）にセッションが切断され、電源操作が割り当てられている期間に移行する。

容量バッファの仕組み

容量バッファは、動的な負荷増加に対応するために、現在の需要に予備容量を追加するために使用されます。注意すべき2つのシナリオがあります。

- マルチセッションOSデリバリーグループの場合、容量バッファは、ロードインデックスの観点からデリバリーグループの総容量の割合として定義されます。ロードインデックスの詳細については、「ロードインデックス」を参照してください。
- シングルセッションOSデリバリーグループの場合、容量バッファは、マシンの数の観点からデリバリーグループの総容量の割合として定義されます。

> **注：**
>
> Autoscaleをタグ付きマシンに制限するシナリオでは、容量バッファは、ロードインデックスの観点から、デリバリーグループ内のタグ付きマシンの総容量の割合として定義されます。
>
> Autoscaleでは、ピーク時とオフピーク時で容量バッファを個別に設定できます。容量バッファフィールドの値が小さいほど、Autoscaleが起動する予備容量が少なくなるため、コストが削減されます。値が大きいほど、ユーザーはセッション起動時により多くのマシンが起動するのを待つ必要がなくなり、最適化されたユーザーエクスペリエンスが保証されます。デフォルトでは、容量バッファは10%です。

> **重要：**
>
> 容量バッファにより、総予備容量がデリバリーグループの総容量の「X」パーセントを下回ったときにマシンが起動します。これにより、必要な割合の予備容量が確保されます。

マルチセッションOSデリバリーグループ

マシンはいつ起動されますか?

重要:

スケジュールが選択されている場合、Autoscale はスケジュールで電源オンになるように構成されているすべてのマシンの電源をオンにします。Autoscale は、負荷に関係なく、スケジュール中に指定された数のマシンの電源をオンに保ちます。

デリバリーグループ内の電源オン状態のマシンの数が、ロードインデックスの観点からバッファ容量を維持するために必要なバッファを満たせなくなった場合、Autoscale は追加のマシンの電源をオンにします。たとえば、デリバリーグループに 20 台のマシンがあり、スケジュールベースのスケーリングの一部として 3 台のマシンが電源オンになるようにスケジュールされており、容量バッファが 20% であるとします。最終的に、負荷がない場合でも 4 台のマシンが電源オンになります。これは、バッファとして 4 x 10k のロードインデックスが必要なため、少なくとも 4 台のマシンが電源オンになっている必要があるためです。このケースは、ピーク時、マシンの負荷増加、新しいセッションの起動、およびデリバリーグループに新しいマシンを追加する際に発生する可能性があります。Autoscale は、次の条件を満たすマシンのみの電源をオンにすることに注意してください。

- マシンがメンテナンスモードではない。
- マシンが実行されているハイパーバイザーがメンテナンスモードではない。
- マシンが現在電源オフになっている。
- マシンに保留中の電源操作がない。

マシンはいつ電源オフになりますか?

重要:

- スケジュールが選択されている場合、Autoscale はスケジュールに基づいてマシンの電源をオフにします。
- Autoscale は、スケジュール中に電源オンになるようにスケジュールで構成されているマシンの電源をオフにしません。

> デリバリーグループのターゲットとなる電源オン状態のマシン数（バッファを含む）をサポートするのに十分なマシン数を超えている場合、Autoscale は余分なマシンの電源をオフにします。このケースは、オフピーク時、マシンの負荷減少、セッションログオフ、およびデリバリーグループからマシンを削除する際に発生する可能性があります。Autoscale は、次の条件を満たすマシンのみの電源をオフにします。

- マシンと、マシンが実行されているハイパーバイザーがメンテナンスモードではない。
- マシンが現在電源オンになっている。
- マシンは起動後に利用可能として登録されるか、登録待ちの状態です。
- マシンにアクティブなセッションがありません。
- マシンに保留中の電源操作がありません。
- マシンは指定された電源オフ遅延を満たしています。これは、マシンが少なくとも「X」分間電源オンの状態であったことを意味します。「X」はデリバリーグループに指定された電源オフ遅延です。

例のシナリオ

次のシナリオを想定します。

- **デリバリーグループの構成**。Autoscale で電源管理するデリバリーグループには、10台のマシン（M1～M10）が含まれています。
- **Autoscaleの構成**
  - 容量バッファは10%に設定されています。
  - 選択したスケジュールにマシンは含まれていません。

シナリオは次の順序で実行されます。

1. ユーザーはログオンしません。
2. ユーザーセッションが増加します。
3. さらにユーザーセッションが開始されます。
4. セッション終了により、ユーザーセッションの負荷が減少します。
5. ユーザーセッションの負荷は、セッション負荷がオンプレミスリソースのみで処理されるまでさらに減少します。

上記のシナリオでAutoscaleがどのように機能するかの詳細については、以下を参照してください。

- ユーザー負荷なし（初期状態）

    - 1台のマシン（例：M1）が電源オンになります。このマシンは、構成されたキャパシティバッファのために電源オンになります。この場合、10（マシン数）x 10,000（負荷インデックス）x 10%（構成されたキャパシティバッファ）は10,000に等しくなります。したがって、1台のマシンが電源オンになります。
    - 電源オンのマシン（M1）の負荷インデックス値は、ベースライン負荷（負荷インデックスは0に等しい）にあります。

- 最初のユーザーがログオンします
    - セッションはマシンM1でホストされるように指示されます。
    - 電源オンのマシンM1の負荷インデックスが増加し、マシンM1はもはやベースライン負荷ではありません。
    - Autoscaleは、構成されたキャパシティバッファのために需要を満たすために、追加のマシン（M2）の電源をオンにし始めます。
    - マシンM2の負荷インデックス値はベースライン負荷にあります。
- ユーザーが負荷を増加させます
    - セッションはマシンM1とM2の間で負荷分散されます。その結果、電源オンのマシン（M1とM2）の負荷インデックスが増加します。
    - 総予備容量は、負荷インデックスの観点からまだ10,000を超えるレベルにあります。
    - マシンM2の負荷インデックス値はもはやベースライン負荷ではありません。
- より多くのユーザーセッションが開始されます
    - セッションはマシン (M1 および M2) 間で負荷分散されます。その結果、電源がオンになっているマシン (M1 および M2) の負荷インデックスがさらに増加します。
    - 総予備容量が負荷インデックスで10,000を下回ると、構成された容量バッファにより需要を満たすために、Autoscale は追加のマシン (M3) の電源をオンにし始めます。
    - マシン M3 の負荷インデックス値はベースライン負荷です。
- さらに多くのユーザーセッションが開始されます
    - セッションはマシン (M1 から M3) 間で負荷分散されます。その結果、電源がオンになっているマシン (M1 から M3) の負荷インデックスが増加します。
    - 総予備容量は負荷インデックスで10,000を上回っています。
    - マシン M3 の負荷インデックス値はベースライン負荷ではなくなります。
- セッション終了によりユーザーセッションの負荷が減少します

    - ユーザーがセッションからログオフするか、アイドルセッションがタイムアウトすると、マシン M1 から M3 で解放された容量は、他のユーザーが開始したセッションをホストするために再利用されます。
    - 総予備容量が負荷インデックスで10,000を上回ると、Autoscale はマシンの1つ (たとえば M3) をドレイン状態にします。その結果、新たな変更が発生しない限り、他のユーザーが開始したセッションはそのマシンに転送されなくなります。たとえば、エンドユーザーの負荷が再び増加したり、他のマシンの負荷が最も低くなったりした場合です。

- ユーザーセッションの負荷は減少し続けます
    - マシン M3 のすべてのセッションが終了し、指定された電源オフ遅延がタイムアウトすると、Autoscale はマシン M3 の電源をオフにします。
    - さらに多くのユーザーがセッションを終了すると、電源がオンになっているマシン (M1 および M2) で解放された容量は、他のユーザーが開始したセッションをホストするために再利用されます。
    - 総予備容量が負荷インデックスで10,000を上回ると、Autoscale はマシンの1つ (たとえば M2) をドレイン状態にします。その結果、他のユーザーが開始したセッションはそのマシンに転送されなくなります。

- セッションがなくなるまでユーザーセッションの負荷は減少し続けます
    - マシンM2上のすべてのセッションが終了し、指定された電源オフ遅延がタイムアウトすると、Autoscaleはマシン M2の電源をオフにします。
    - 電源オン状態のマシン（M1）の負荷インデックス値はベースライン負荷です。構成されたキャパシティバッファがあるため、AutoscaleはマシンM1をドレイン状態にしません。

> **注:**
>
> マルチセッションOSデリバリーグループの場合、ユーザーがセッションからログオフすると、デスクトップへの変更はすべて失われます。ただし、構成されている場合、ユーザー固有の設定はユーザープロファイルとともにローミングされます。

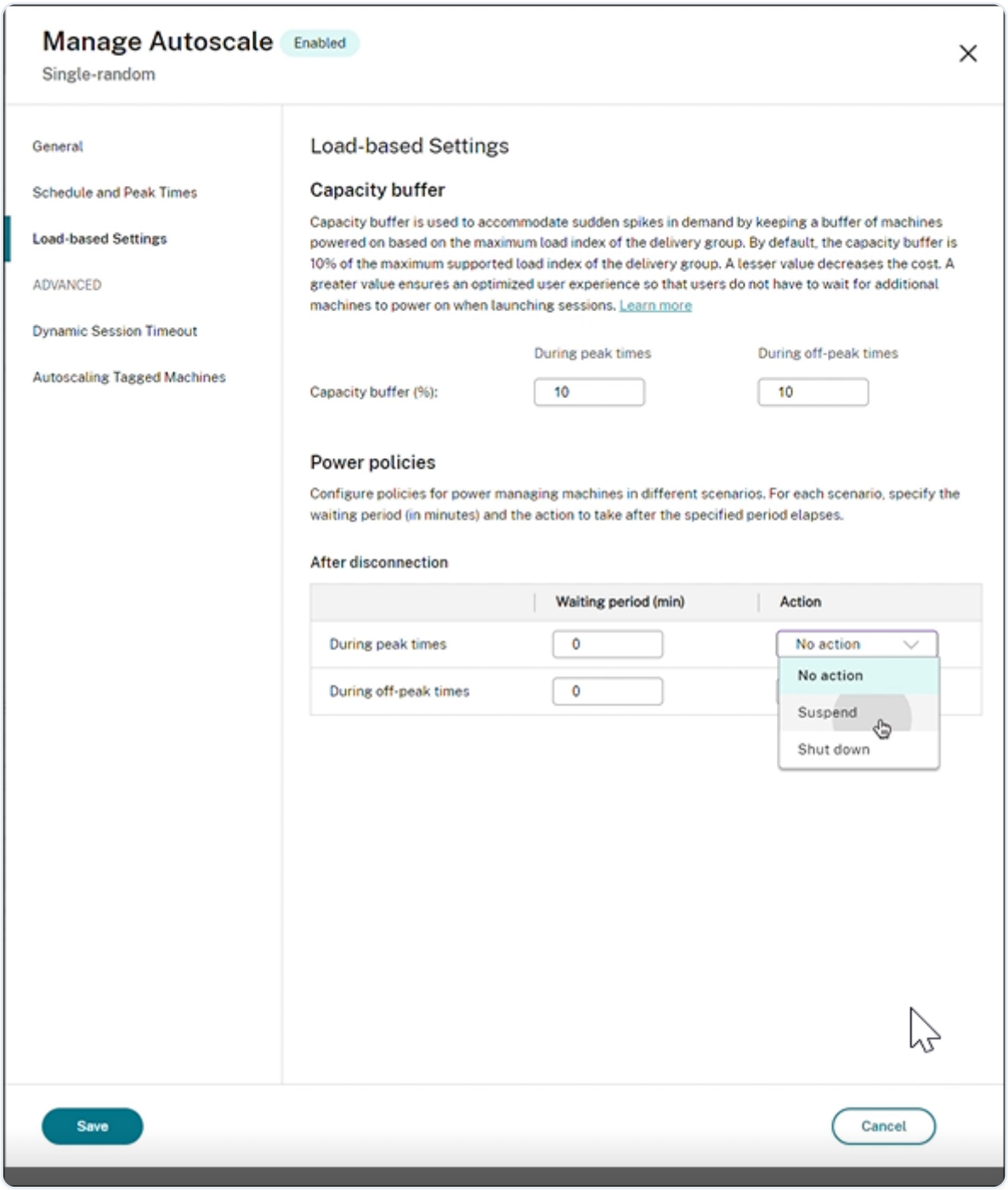
シングルセッションOSランダムデリバリーグループ

キャパシティバッファは、デリバリーグループ内のマシンの総数に基づいて、マシンのバッファを電源オン状態に保つことで、需要の急増に対応するために使用されます。デフォルトでは、キャパシティバッファはデリバリーグループ内のマシンの総数の10%です。

マシンの数（キャパシティバッファを含む）が現在電源オン状態のマシンの総数を超える場合、需要を満たすために追加のマシンが電源オンになります。マシンの数（キャパシティバッファを含む）が現在電源オン状態のマシンの総数より少ない場合、構成したアクションに応じて、余分なマシンはシャットダウンまたは中断されます。

電源ポリシー

さまざまなシナリオでマシンの電源を管理するためのポリシーを構成します。各シナリオについて、待機時間（分）と、指定された時間終了後に実行するアクションを指定できます。電源ポリシーは、シングルセッションOSランダムデリバリーグループとシングルセッションOS静的デリバリーグループに適用されます。

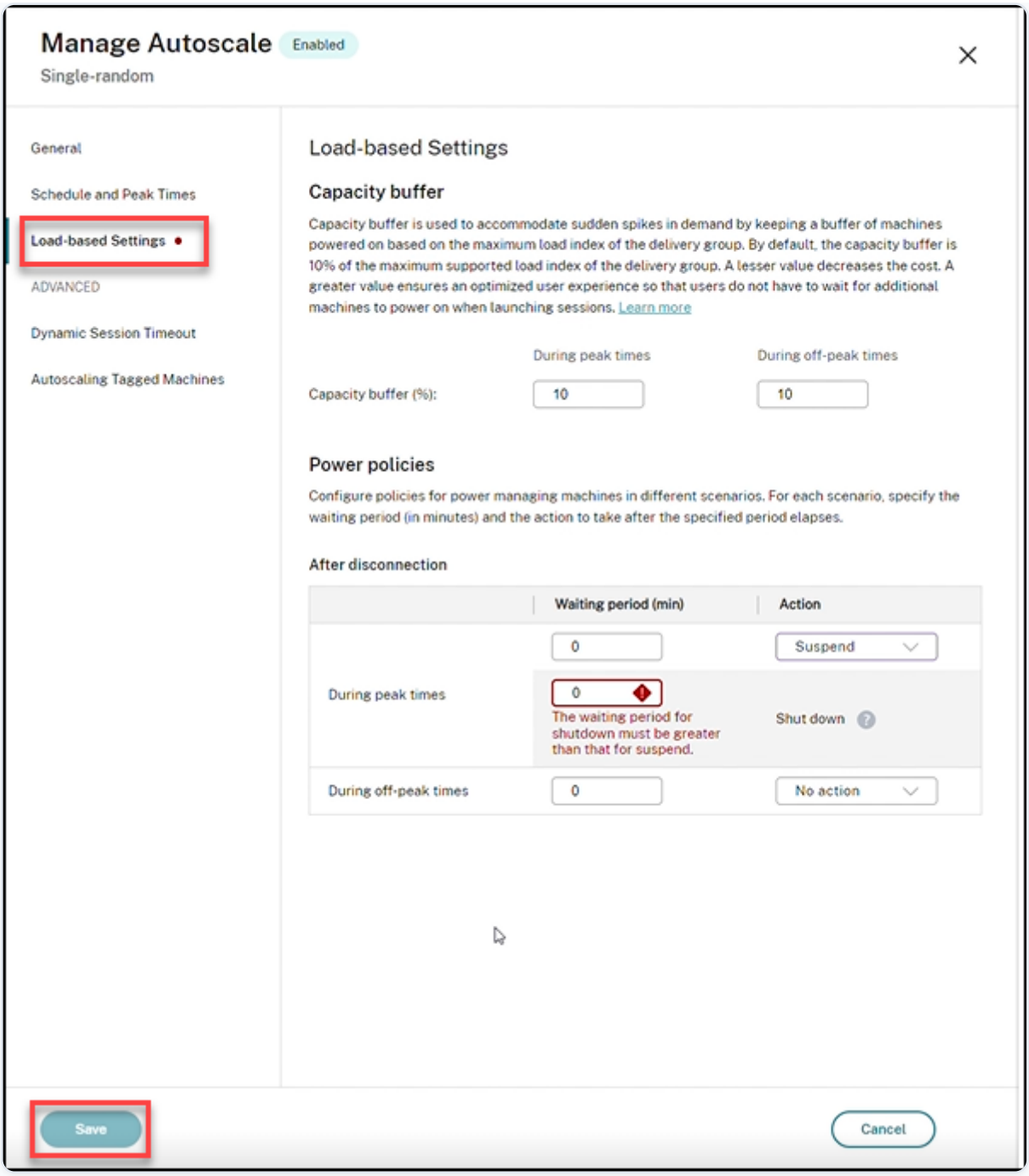


切断後、以下の設定はピーク時とオフピーク時の両方に適用されます。

- ドロップダウンから、待機時間（分）と、アクションなし、中断、またはシャットダウンなどのアクションを設定できます。
- 中断アクションを選択した場合、マシンをシャットダウンするための追加の待機時間を構成します。

注:

- ピーク時およびオフピーク時において、シャットダウンアクションの待機時間は、中断の待機時間よりも長くする必要があります。
- 停止中のマシンは、再接続時に切断されたユーザーのみがアクセスできます。新規ユーザーが停止中のマシンを利用できるようにするには、シャットダウンします。
- サスペンドおよびシャットダウンのフィールドの時刻設定が正しく構成されていない場合、**保存**オプションが無効になり、設定エラーを示す赤い点もナビゲーション項目の横に表示されます。



例

- 待機時間を12分に設定し、最初の操作を「操作なし」に選択した場合、12分経過後もマシンは電源オンの状態を維持します。
- 待機時間を15分に設定し、最初の操作を「サスペンド」に選択し、2番目の待機時間を20分に設定した場合、15分経過後、マシンはサスペンドされます。2番目の待機時間経過後、マシンはシャットダウンされます。
- 待機時間を18分に設定し、最初の操作を「シャットダウン」に選択した場合、18分経過後、マシンはシャットダウンされます。

シナリオ例

次のシナリオを想定します。

- **デリバリーグループの構成**。Autoscaleで電源管理するデリバリーグループには、10台のマシン（M1～M10）が含まれています。
- **Autoscaleの構成**
  - 容量バッファは10%に設定されています。
  - 選択したスケジュールにマシンは含まれていません。

シナリオは次の順序で実行されます。

1. ユーザーはログオンしません。
2. ユーザーセッションが増加します。
3. より多くのユーザーセッションが開始されます。
4. セッション終了により、ユーザーセッションの負荷が減少します。
5. セッション負荷がオンプレミスリソースのみで処理されるまで、ユーザーセッションの負荷はさらに減少します。

上記のシナリオでAutoscaleがどのように機能するかについては、以下を参照してください。

- ユーザー負荷なし（初期状態）
  - 1台のマシン（M1）が電源オンになります。このマシンは、構成されたキャパシティバッファのために電源オンになります。この場合、10（マシン数）x 10%（構成されたキャパシティバッファ）は1になります。したがって、1台のマシンが電源オンになります。
- 最初のユーザーがログオンします
  - ユーザーがデスクトップを使用するために初めてログオンすると、電源オンになっているマシンでホストされているデスクトップのプールからデスクトップが割り当てられます。この場合、ユーザーにはマシンM1からデスクトップが割り当てられます。
  - 構成されたキャパシティバッファのため、Autoscaleは需要を満たすために追加のマシン（M2）の電源をオンにし始めます。
- 2番目のユーザーがログオンします
  - ユーザーにはマシンM2からデスクトップが割り当てられます。
  - 構成されたキャパシティバッファのため、Autoscaleは需要を満たすために追加のマシン（M3）の電源をオンにし始めます。

- 3番目のユーザーがログオンします
  - ユーザーにはマシンM3からデスクトップが割り当てられます。
  - Autoscale は、設定された容量バッファのために、需要を満たすため追加のマシン (M4) の電源を入れ始めます。
- ユーザーがログオフする
  - ユーザーがログオフするか、ユーザーのデスクトップがタイムアウトすると、解放された容量 (例: M3) がバッファとして利用可能になります。その結果、容量バッファが10%に設定されているため、Autoscale はマシン M4 の電源を切り始めます。
- ユーザーがいなくなるまで、さらに多くのユーザーがログオフする
  - さらに多くのユーザーがログオフした後、Autoscale はマシン (例: M2 または M3) の電源を切ります。
  - ユーザーが残っていなくても、Autoscale は残りの1台のマシン (例: M1) の電源を切りません。なぜなら、そのマシンは予備容量として予約されているからです。

> **注：**
>
> シングルセッションOSのランダムデリバリーグループの場合、ユーザーがセッションをログオフすると、デスクトップへのすべての変更は失われます。ただし、設定されている場合、ユーザー固有の設定はユーザープロファイルとともにローミングされます。

シングルセッションOSの静的デリバリーグループ

容量バッファは、デリバリーグループ内の未割り当てマシンの総数に基づいて、未割り当てマシンのバッファの電源をオンに保つことで、急な需要の急増に対応するために使用されます。デフォルトでは、容量バッファはデリバリーグループ内の未割り当てマシンの総数の10%です。

> **重要：**
>
> デリバリーグループ内のすべてのマシンが割り当てられた後、キャパシティバッファはマシンの電源オン/オフには関与しません。

> マシンの数（容量バッファを含む）が現在電源がオンになっているマシンの総数を超える場合、需要を満たすために追加の未割り当てマシンが電源オンになります。マシンの数（容量バッファを含む）が現在電源がオンになっているマシンの総数よりも少ない場合、設定したアクションに応じて、余分なマシンは電源オフまたは一時停止されます。

シングルセッションOS静的デリバリーグループの場合、Autoscaleは次のようになります。

- 該当するシングルセッションOSデリバリーグループの `AutomaticPowerOnForAssigned` プロパティが true に設定されている場合にのみ、ピーク時に割り当てられたマシンの電源をオンにし、オフピーク時に電源をオフにします。
- ピーク時にマシンが電源オフになっていて、そのマシンが属するデリバリーグループの `AutomaticPowerOnForAssignedDuringPeak` プロパティがtrueに設定されている場合、自動的に電源をオンにします。

割り当てられたマシンで容量バッファがどのように機能するかを理解するには、以下を考慮してください。

- 容量バッファは、デリバリーグループに1台以上の未割り当てのマシンがある場合にのみ機能します。
- デリバリーグループに未割り当てのマシンがない場合（デリバリーグループ内のすべてのマシンが割り当てられている場合）、容量バッファはマシンの電源オン/オフには関与しません。
- `AutomaticPowerOnForAssignedDuringPeak` プロパティは、ピーク時に割り当てられたマシンの電源がオンになるかどうかを決定します。trueに設定されている場合、Autoscaleはピーク時にマシンの電源をオンに保ちます。電源がオフになっている場合でも、Autoscaleはそれらの電源をオンにします。

電源ポリシー

さまざまなシナリオでマシンの電源を管理するポリシーを構成します。各シナリオについて、待機時間（分単位）と、指定された時間が終了した後に実行するアクションを指定できます。電源ポリシーは、シングルセッションOSランダムデリバリーグループとシングルセッションOS静的デリバリーグループに適用されます。

シングルセッションOS静的DG電源ポリシー設定(/en-us/citrix-virtual-apps-desktops/2503/media/single-session-os-static-dg-power-policies-settings.png)

切断後および**ログオフ後**の場合、以下の設定はピーク時とオフピーク時の両方に適用されます。ドロップダウンから、待機時間（分単位）と、アクション（アクションなし、一時停止、シャットダウンなど）を設定できます。

Autoscaleによってマシンの電源がオンになった後にユーザーがログオンしない場合、以下の設定はピーク時にのみ適用されます。ピーク時にドロップダウンから、待機時間（分単位）と、アクション（アクションなし、一時停止、シャットダウンなど）を設定できます。

例のシナリオ

以下のシナリオを想定してください。

- **デリバリーグループの構成**。Autoscaleで電源管理したいデリバリーグループには、10台のマシン（M1～M10）が含まれています。
- **Autoscaleの構成**
  - マシンM1～M3は割り当て済みで、マシンM4～M10は未割り当てです。
  - ピーク時とオフピーク時で容量バッファを10%に設定します。
  - 選択されたスケジュールに従って、Autoscaleは午前9時から午後6時の間、マシンの電源を管理します。

上記のシナリオでAutoscaleがどのように機能するかの詳細については、以下を参照してください。

- スケジュールの開始 – 午前9時
  - AutoscaleはマシンM1からM3の電源をオンにします。
  - 設定された容量バッファのため、Autoscaleは追加のマシン（例えばM4）の電源をオンにします。マシンM4は割り当てられていません。
- 最初のユーザーがログオンします
  - ユーザーがデスクトップを使用するために初めてログオンすると、割り当てられていない電源オン状態のマシンでホストされているデスクトップのプールから、ユーザーにデスクトップが割り当てられます。この場合、ユーザーにはマシンM4からデスクトップが割り当てられます。そのユーザーによるその後のログオンは、初回使用時に割り当てられたのと同じデスクトップに接続します。
  - 設定された容量バッファのため、Autoscaleは需要を満たすために追加のマシン（例えばM5）の電源をオンにし始めます。
- 2人目のユーザーがログオンします
  - ユーザーには、割り当てられていない電源オン状態のマシンからデスクトップが割り当てられます。この場合、ユーザーにはマシンM5からデスクトップが割り当てられます。その

ユーザーによるその後のログオンは、初回使用時に割り当てられたのと同じデスクトップに接続します。

- 設定された容量バッファのため、Autoscaleは需要を満たすために追加のマシン（例えばM6）の電源をオンにし始めます。

- ユーザーがログオフします
  - ユーザーがデスクトップからログオフするか、デスクトップがタイムアウトすると、Autoscaleは午前9時から午後6時の間、マシンM1からM5の電源をオンのままにします。それらのユーザーが次回ログオンするときは、初回使用時に割り当てられたのと同じデスクトップに接続します。
  - 割り当てられていないマシンM6は、受信する、割り当てられていないユーザーにデスクトップを提供するのを待機しています。
- スケジュールの終了 – 午後6時
  - 午後6時に、Autoscaleはマシン M1からM5の電源をオフにします。
  - Autoscaleは、設定されたキャパシティバッファのため、割り当てられていないマシンM6の電源をオンのままにします。そのマシンは、入ってくる割り当てられていないユーザーにデスクトップを提供するのを待機しています。
  - デリバリーグループでは、マシンM6からM10は割り当てられていないマシンです。

動的セッションタイムアウト

この機能を使用すると、ピーク時とオフピーク時の使用時間に合わせて、切断されたセッションとアイドル状態のセッションのタイムアウトを構成し、マシンのドレインを高速化してコストを削減できます。この機能は以下に適用されます。

- シングルセッションおよびマルチセッションOSマシン。
- オートスケール用にタグ付けされているかどうかに関わらず、デリバリーグループ内のすべてのマシン。

VDAは、10分以上アイドル状態になっているセッションのアイドル時間を報告するため、動的セッションタイムアウトは、アイドル状態になってから10分以内にアイドルセッションを切断することはできません。より短い値を設定すると、残存するセッションがより早く削除され、コストが削減されます。

Autoscaleマルチセッション OS - 動的セッションタイムアウト(/en-us/citrix-virtual-apps-desktops/2503/media/autoscale-session-timeout-ms.png)

注:

- この機能は、マルチセッションOSデリバリーグループで常に利用できます。
- シングルセッションOSデリバリーグループの場合、この機能はバージョン2206 CR以降、または2203 LTSR CU3以降のVDAに適用されます。これらのVDAがCitrix Cloud™に少なくとも一度登録されていることを確認してください。利用できない場合、次のユーザーインターフェイスが表示されます。

動的セッションタイムアウトは利用できません(/en-us/citrix-virtual-apps-desktops/2503/media/autoscale-session-timeout-unavailable.png)

- Autoscale™の動的タイムアウトはコスト削減を目的としています。セキュリティ目的で使用する場合、構成されたタイムアウトがGPOまたは管理コンソールポリシーと競合する可能性があります。競合が発生した場合、より短いタイムアウトが優先されます。

アイドルセッションタイムアウト。ユーザー入力がない場合に、中断されないユーザー接続が維持される期間を指定するタイマーを有効または無効にします。タイマーが期限切れになると、セッションは切断状態になり、**切断セッションタイムアウト**が適用されます。**切断セッションタイムアウト**が無効になっている場合、セッションはログオフされません。

重要:

- 10分（600秒）以下の値を指定した場合、Autoscaleは、関連するセッションが10分間アイドル状態になった後に切断します。これは、AutoscaleがVDAが報告するセッションのアイドル時間に依存しているためです。VDAは、10分以上アイドル状態になっているセッションのアイドル時間のみを報告します。
- アイドルセッションタイムアウトに達するまでの最後の5分以内にユーザーが操作した場合、アイドル状態のセッションは切断状態に移行する可能性があります。

切断されたセッションのタイムアウト。セッションがログオフされるまでに、切断されたデスクトップがロックされたままになる時間を指定するタイマーを有効または無効にします。有効にすると、タイマーの期限が切れたときに切断されたセッションがログオフされます。

よくある質問

動的セッションタイムアウト機能は、Autoscaling用にタグ付けされたマシンにのみ適用されますか?

動的セッションタイムアウト機能は、Autoscaling用にタグ付けされているかどうかにかかわらず、デリバリーグループ内のすべてのマシンに適用されます。

動的セッションタイムアウトによりセッションがログオフされた場合、タグ付けされていないマシンも、タグ付けされたマシンのAutoscaleターゲットに含まれますか?

動的セッションタイムアウト機能は、Autoscaleタグ付け機能とは関係ありません。動的セッションタイムアウトによってセッションが終了した場合、マシンがシャットダウンされるまでドレイン状態であれば、タグ付けされていないマシンもそのプロセス中にシャットダウンされる可能性があります。

タグ付きマシンの自動スケーリング (クラウドバースト)

> **注:**
>
> この機能は以前、Restrict Autoscaleという名称でした。

はじめに

Autoscaleは、デリバリーグループ内のマシンの一部のみを電源管理する柔軟性を提供します。これを実現するには、1つ以上のマシンにタグを適用し、その後、Autoscaleを構成してタグ付きマシンのみを電源管理します。

この機能は、クラウドベースのリソースが追加の需要（つまり、バーストワークロード）に対応する前に、オンプレミスリソース（または予約済みのパブリッククラウドインスタンス）を使用してワークロードを処理したいクラウドバーストのユースケースで役立ちます。オンプレミスのマシン（または予約済みインスタンス）に最初にワークロードを処理させるには、タグ制限とゾーン優先度を組み合わせて使用する必要があります。

タグ制限は、Autoscaleによって電源管理されるマシンを指定します。ゾーン優先度は、ユーザー起動要求を処理する優先ゾーン内のマシンを指定します。詳細については、タグおよびゾーン優先度を参照してください。

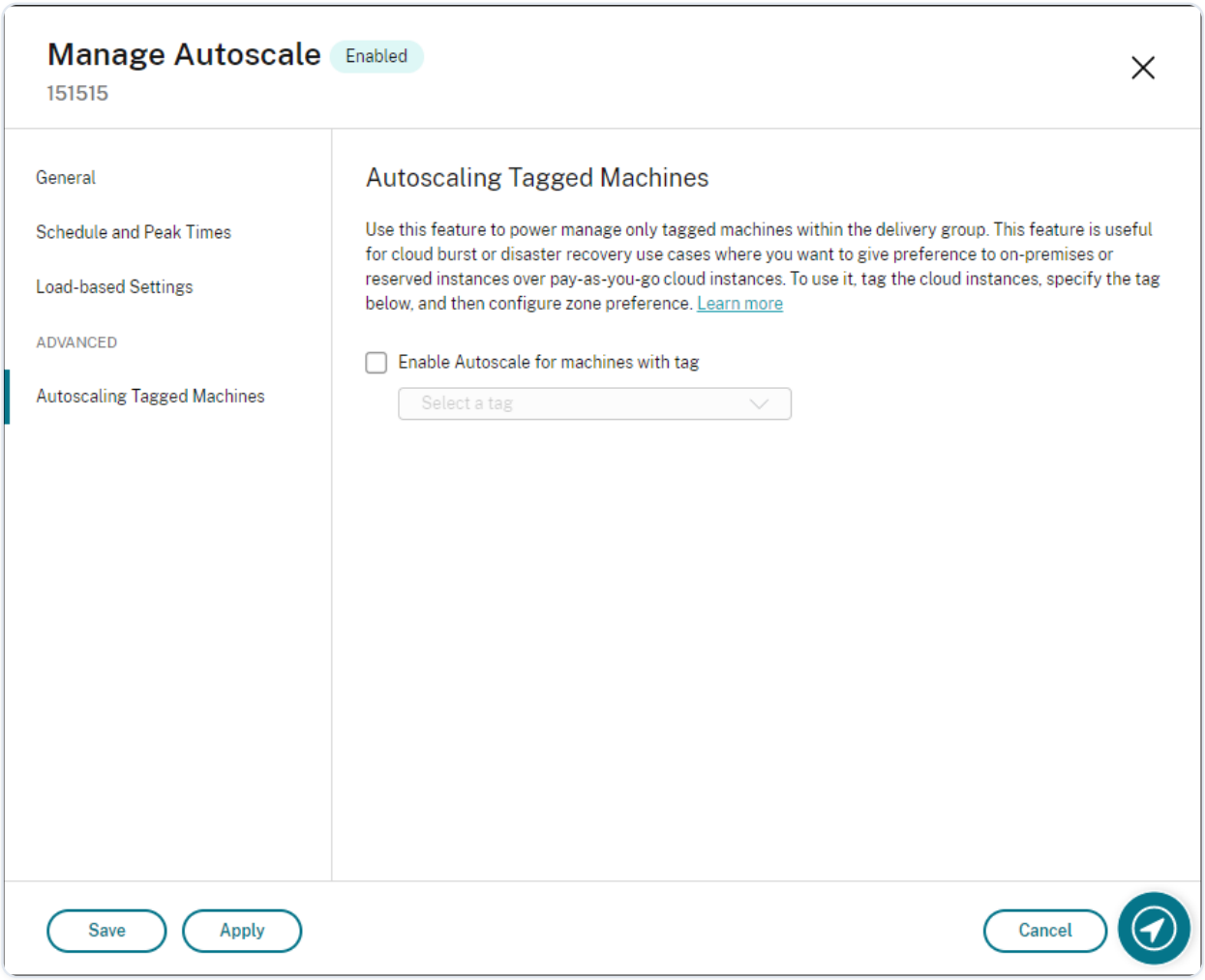
特定のタグ付きマシンを自動スケーリングするには、ManageコンソールまたはPowerShellを使用できます。

Manageコンソールを使用して特定のタグ付きマシンを自動スケーリングする

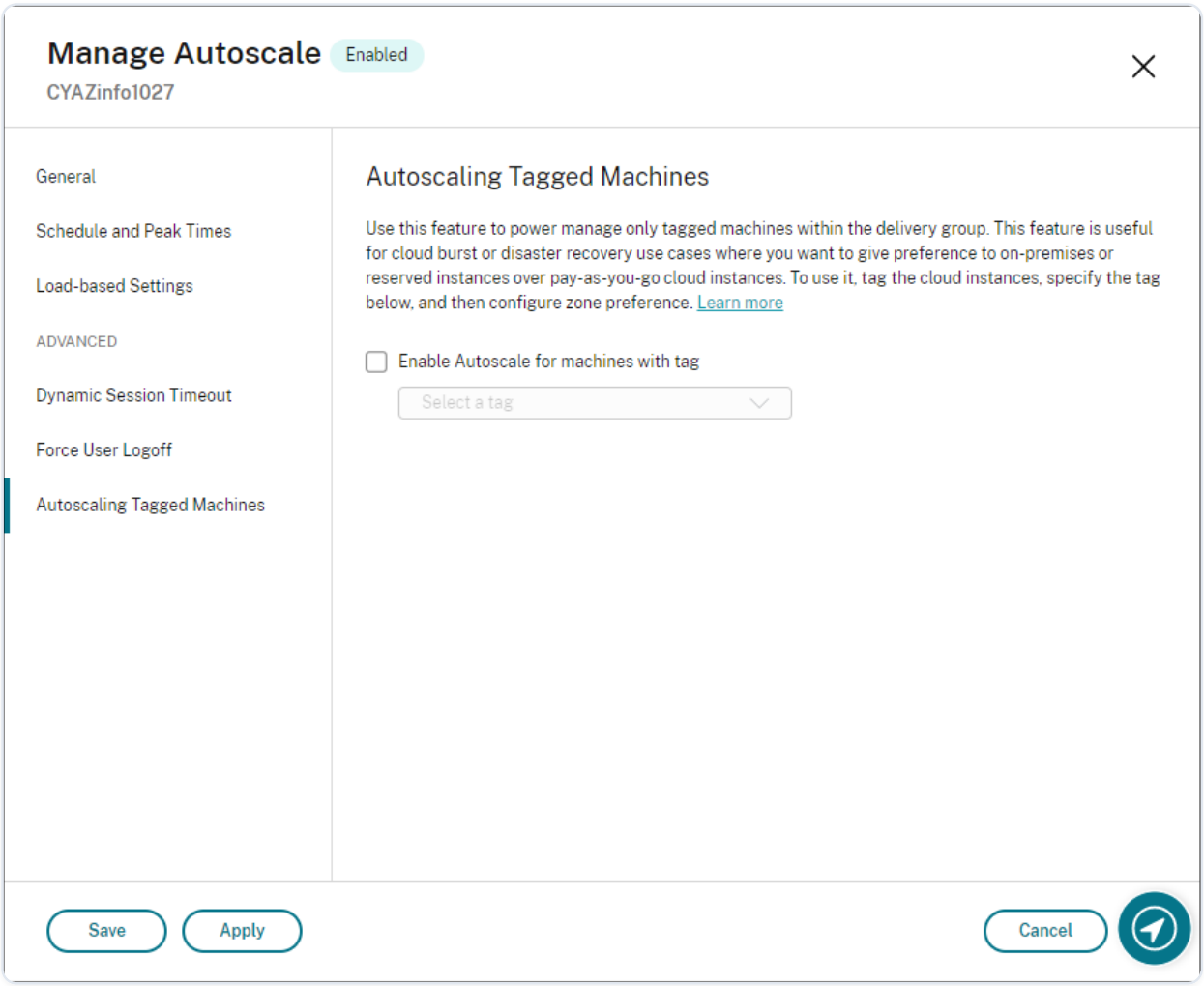
特定のタグ付きマシンを自動スケーリングするには、次の手順を実行します。

1. タグを作成し、そのタグをデリバリーグループ内の該当するマシンに適用します。詳細については、タグとタグ制限の管理を参照してください。
2. デリバリーグループを選択し、**Manage Autoscale**ウィザードを開きます。
3. **タグ付きマシンの自動スケーリング**ページで、**タグ付きマシンのAutoscaleを有効にする**を選択し、リストからタグを選択し、**適用**をクリックして変更を保存します。

   シングルセッションOSの*静的*および*ランダム*デリバリーグループのユーザーインターフェイス:



マルチセッションOSデリバリーグループのユーザーインターフェイス:



警告:

- 特定のタグを持つマシンのAutoscaleは、タグごとのマシンの数を反映するようにヒストグラムを自動的に更新する可能性があります。必要に応じて、**スケジュールとピーク時間**ページで、各時間帯にマシンを手動で割り当てることができます。
- タグ付きマシンで使用されているタグは削除できません。タグを削除するには、まずタグの制限を解除する必要があります。

タグの制限を適用した後、後でデリバリーグループから削除したい場合があります。そのためには、**Autoscaleの管理 > タグ付きマシンのAutoscale**ページに移動し、**タグ付きマシンのAutoscaleを有効にする**のチェックを外します。

警告:

- **タグ付きマシンのAutoscaleを有効にする**のチェックを外さずに、該当するマシンからタグを削除すると、**Autoscaleの管理**ウィザードを開いたときに警告が表示されることがあります。マシンからタグを削除すると、Autoscaleで指定したタグが無効になるため、Autoscaleが管理するマシンがなくなる可能性があります。この警告を解決するには、**タグ付きマシンのAutoscale**ページに移動し、無効なタグを削除してから、**適用**をクリックして変更を保存します。

Autoscaleがリソースの電源をオンにするタイミングを制御する

また、タグなしマシンの使用状況に基づいて、Autoscaleがタグ付きマシンの電源をオンにし始めるタイミングを制御することもできます。これにより、タグ付きまたはパブリッククラウドのワークロードの消費をさらに最適化できます。

これを行うには、次の手順を完了します。

1. **タグ付けされたマシンのAutoscale**ページで、**Autoscaleがタグ付けされたマシンの電源をオンにし始めるタイミングを制御する**を選択します。
2. ピーク時とオフピーク時の両方で到達させたいタグ付けされていないマシンの使用率をパーセンテージで入力し、**適用**をクリックします。サポートされる値: 0〜100。

Autoscaleがタグ付けされたマシンの電源をオンにし始めるタイミングを制御する(/en-us/citrix-virtual-apps-desktops/2503/media/autoscale-powers-on-tagged-machines.png)

ヒント:

このパーセンテージは、Autoscaleがタグ付きマシンの電源をオンにし始めるタイミングを制御します。パーセンテージがしきい値（デフォルト10%）を下回ると、Autoscaleはタグ付きマシンの電源をオンにし始めます。パーセンテージがしきい値を超えると、Autoscaleは電源オフモードになります。パーセンテージを入力する際は、次の2つのシナリオを考慮してください。

- シングルセッションOSデリバリーグループの場合：この値は、アイドル状態のタグなしマシンの総数に対する割合として定義されます。例：タグなしのシングルセッションOSマシンが10台あるとします。セッションがないマシンが1台だけになった場合、Autoscaleはタグ付きマシンの電源をオンにし始めます。

- マルチセッションOSデリバリーグループの場合：この値は、利用可能なタグなしマシンの総容量（ロードインデックスの観点から）に対する割合として定義されます。例：タグなしのマルチセッションOSマシンが10台あるとします。それらが90%ロードされた場合、Autoscaleはタグ付きマシンの電源をオンにし始めます。

PowerShellを使用して特定のタグ付けされたマシンをAutoscaleする

PowerShell SDKを直接使用するには、次の手順を完了します。

1. **タグを作成します。** New-Brokertag PowerShellコマンドを使用してタグを作成します。
   - 例：`$managed = New-BrokerTag Managed`。この場合、タグは「Managed」という名前です。New-Brokertag PowerShellコマンドの詳細については、`<https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/New-BrokerTag/>`を参照してください。
2. **マシンにタグを適用します。** Get-Brokermachine PowerShellコマンドを使用して、Autoscaleに電源管理させたいカタログ内のマシンにタグを適用します。
   - 例：`Get-BrokerMachine -CatalogName "cloud" | Add-BrokerTag $managed.Name`。この場合、カタログは「cloud」という名前です。
   - Get-Brokermachine PowerShellコマンドの詳細については、`<https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/Get-BrokerMachine/>`を参照してください。

   注:

   タグを適用した後で、カタログに新しいマシンを追加する場合があります。その場合、タグは新しいマシンに自動的に適用*されません*。

3. **タグ付きマシンを、Autoscaleに電源管理させたいデリバリーグループに追加します。** Get-BrokerDesktopGroup PowerShellコマンドを使用して、マシンを含むデリバリーグループにタグ制限を追加します（つまり、「タグXを持つマシンへの起動を制限する」）。
   - 例：`Get-BrokerDesktopGroup -Uid 1 | Set-BrokerDesktopGroup -RestrictAutoscaleTagUid $managed.Uid`。この場合、デリバリーグループのUIDは1です。

- Get-BrokerDesktopGroup PowerShellコマンドの詳細については、`<https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/Get-BrokerDesktopGroup/>`を参照してください。

タグ制限を適用した後、後でデリバリーグループから削除したい場合があります。その場合は、Get-BrokerDesktopGroup PowerShellコマンドを使用します。

例: `Get-BrokerDesktopGroup –Uid 1 | Set-BrokerDesktopGroup –RestrictAutoscaleTagUid $null`。この場合、デリバリーグループのUIDは1です。

> **注:**
>
> タグ付けされていないマシンは、ユーザーが電源を切った後に自動的に再起動します。この動作により、ワークロードをより早く処理できるようになります。これは、`Set-BrokerDesktopGroup`の`AutomaticRestartForUntaggedMachines`プロパティを使用して、デスクトップグループごとに有効または無効にできます。詳細については、`<https://citrix.github.io/delivery-controller-sdk/Broker/Set-BrokerDesktopGroup/>`を参照してください。

例のシナリオ

次のシナリオを想定します。

- **マシンカタログ構成**。2つのマシンカタログ（C1とC2）があります。
  - カタログC1には、オンプレミス展開でローカルな5台のマシン（M1～M5）が含まれています。
  - カタログC2には、クラウド展開でリモートな5台のマシン（M6～M10）が含まれています。
- **タグ制限**。「Cloud」という名前のタグが作成され、カタログC2のマシンM6～M10に適用されます。
- **ゾーン構成**。2つのゾーン（Z1とZ2）が作成されます。
  - カタログC1を含むゾーンZ1は、オンプレミス展開に対応します。
  - カタログC2を含むゾーンZ2は、クラウド展開に対応します。
- **デリバリーグループ構成**

  - デリバリーグループには、10台のマシン（M1～M10）が含まれており、そのうち5台はカタログC1（M1～M5）から、5台はカタログC2（M6～M10）からです。
  - M1からM5までのマシンは手動で電源がオンにされ、スケジュール期間中ずっと電源がオンのままになります。

- **Autoscale構成**
  - 容量バッファは10%に設定されています。
  - Autoscaleは、「Cloud」タグが付いたマシンのみを電源管理します。この場合、Autoscaleはクラウドマシン M6からM10を電源管理します。

- **公開アプリケーションまたはデスクトップ構成**。公開デスクトップ（例）にはゾーン設定が構成されており、ユーザー起動要求ではゾーンZ2よりもゾーンZ1が優先されます。
  - ゾーンZ1は、公開デスクトップの優先ゾーン（ホームゾーン）として構成されています。

このシナリオは、次の順序で実行されます。

1. ユーザーはログオンしません。
2. ユーザーセッションが増加します。
3. 利用可能なすべてのオンプレミス・マシンが消費されるまで、ユーザーセッションはさらに増加します。
4. さらに多くのユーザーセッションが開始されます。
5. セッション終了により、ユーザーセッションが減少します。
6. セッション負荷がオンプレミス マシンのみで処理されるまで、ユーザーセッションはさらに減少します。

上記のシナリオでAutoscaleがどのように機能するかについては、以下を参照してください。

- ユーザー負荷なし（初期状態）
  - オンプレミス環境のマシンM1からM5はすべて電源がオンになっています。
  - クラウド内のマシン1台（例: M6）の電源がオンになっています。このマシンは、構成されたキャパシティバッファのために電源がオンになっています。この場合、10（マシン数）x 10,000（ロードインデックス）x 10%（構成されたキャパシティバッファ）は10,000になります。したがって、マシン1台の電源がオンになります。
  - 電源がオンになっているすべてのマシン（M1からM6）のロードインデックス値は、ベースライン負荷（ロードインデックスは0）にあります。
- ユーザーがログオンします

    - セッションは、構成されたゾーン設定を通じてマシンM1からM5でホストされるように指示され、これらのオンプレミス環境のマシン間で負荷分散されます。
    - 電源がオンになっているマシン（M1からM5）のロードインデックス値が増加します。
    - 電源がオンになっているマシンM6のロードインデックス値は、ベースライン負荷にあります。
- ユーザーが負荷を増やし、すべてのオンプレミスリソースを消費します
    - セッションは、構成されたゾーン設定を通じてマシンM1からM5でホストされるように指示され、これらのオンプレミス環境のマシン間で負荷分散されます。
    - 電源がオンになっているすべてのマシン（M1からM5）のロードインデックス値は10,000に達しました。
    - 電源がオンになっているマシンM6のロードインデックス値は、ベースライン負荷のままです。
- もう1人のユーザーがログオンします
    - セッションはゾーン設定を超過し、クラウドマシンM6でホストされるように指示されます。
    - 電源がオンになっているすべてのマシン（M1からM5）のロードインデックス値は10,000に達しました。
    - 電源がオンになっているマシンM6のロードインデックス値が増加し、ベースライン負荷ではなくなります。ロードインデックスの合計予備容量が10,000を下回ると、Autoscaleは構成されたキャパシティバッファのために、需要を満たすため追加のマシン（M7）の電源をオンにし始めます。マシンM7の電源をオンにするには時間がかかる場合があることに注意してください。そのため、マシンM7が準備できるまでに遅延が発生する可能性があります。
- より多くのユーザーがログオンします。
    - セッションはマシンM6でホストされるように指示されます。
    - 起動中のすべてのマシン（M1～M5）のロードインデックス値が10,000に達しました。
    - 起動中のマシンM6のロードインデックス値はさらに増加しますが、ロードインデックスの観点から見ると、総予備容量は10,000を超えるレベルにあります。
    - 起動中のマシンM7のロードインデックス値はベースライン負荷のままです。
- さらに多くのユーザーがログオンします。

    - マシンM7の準備が整うと、セッションはマシンM6とM7でホストされるように指示され、これらのマシン間で負荷分散されます。
    - 起動中のすべてのマシン（M1～M5）のロードインデックス値が10,000に達しました。
    - マシンM7のロードインデックス値は、もはやベースライン負荷ではありません。
    - 起動中のマシン（M6とM7）のロードインデックス値が増加します。
    - ロードインデックスの観点から見ると、総予備容量は依然として10,000を超えるレベルにあります。

- セッション終了によりユーザーセッション負荷が減少します。
    - ユーザーがセッションからログオフしたり、アイドル状態のセッションがタイムアウトしたりすると、マシンM1～M7で解放された容量は、他のユーザーが開始したセッションをホストするために再利用されます。
    - ロードインデックスの観点から総予備容量が10,000を超えるレベルに増加すると、Autoscaleはクラウドマシン（M6～M7）のいずれかをドレイン状態にします。その結果、新しい変更（たとえば、ユーザー負荷が再び増加したり、他のクラウドマシンの負荷が最も低くなったりする場合）が発生しない限り、他のユーザーが開始したセッションはそのマシン（たとえばM7）に転送されなくなります。
- 1つ以上のクラウドマシンが不要になるまで、ユーザーセッション負荷はさらに減少します。
    - M7マシン上のすべてのセッションが終了し、指定された電源オフ遅延時間が経過すると、AutoscaleはM7マシンの電源をオフにします。
    - 電源がオンになっているすべてのマシン（M1からM5）のロードインデックス値が10,000未満のレベルに低下する可能性があります。
    - 電源がオンになっているマシン（M6）のロードインデックス値が減少します。
- クラウドマシンが不要になるまで、ユーザーセッションはさらに減少します。
    - M6マシンにユーザーセッションがない場合でも、Autoscaleは予備容量として予約されているため、電源をオフにしません。
    - Autoscaleは、構成された容量バッファのため、残りのクラウドマシンM6の電源をオンのままにします。そのマシンは、着信するユーザーにデスクトップを提供するのを待機しています。
    - オンプレミス環境のマシンに利用可能な容量がある限り、セッションはM6マシンでホストされるようには指示されません。

ユーザーログオフ通知

重要:

この機能は、マルチセッションアプリベースのデリバリーグループ向けのAutoscale™ユーザーインターフェイスでのみ利用可能です。

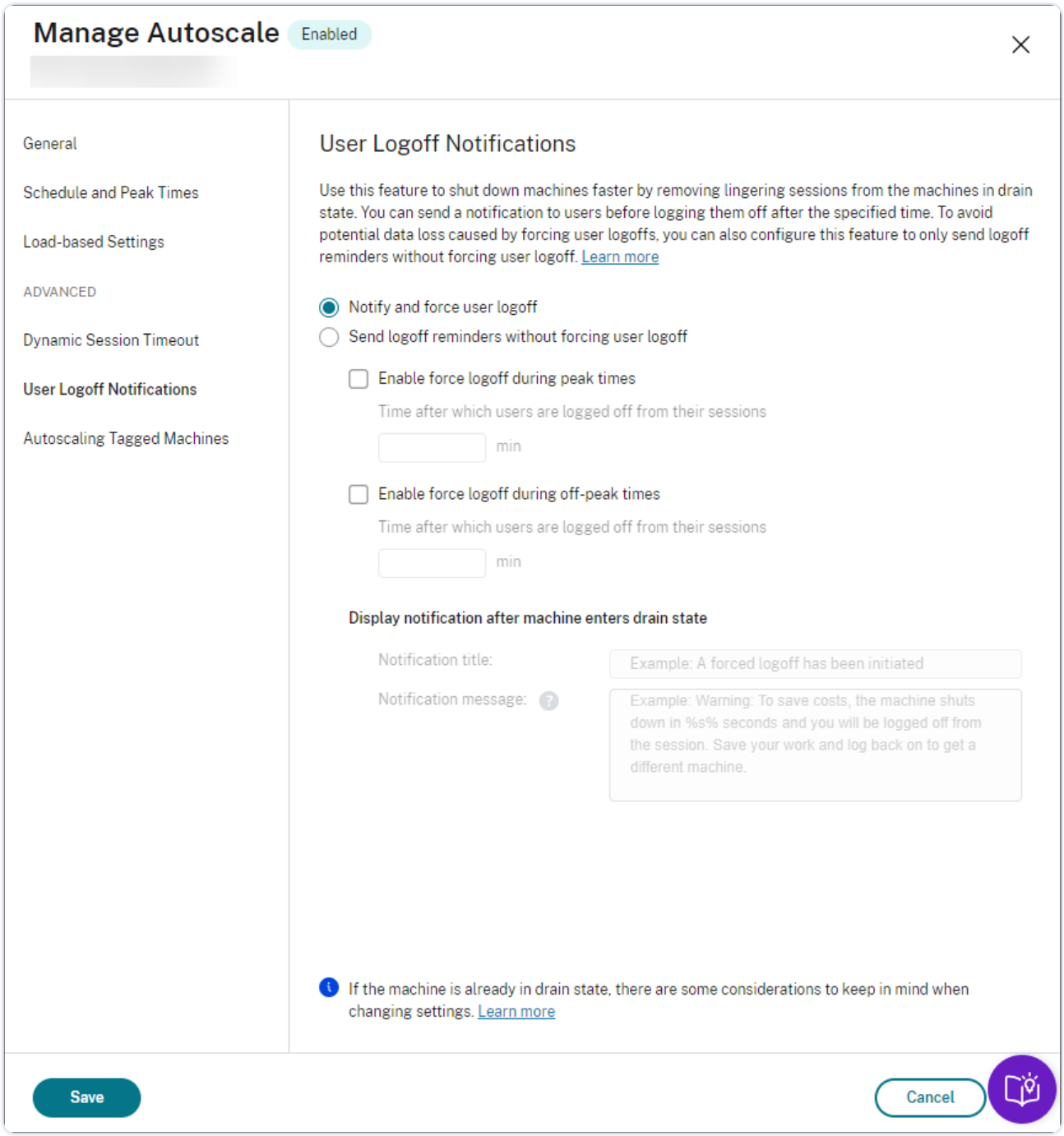
コスト削減をより効果的に実現するため、Autoscaleでは、残存セッションを強制的にログオフできます。これは、ユーザーにカスタム通知を送信し、その猶予期間が経過した後にセッションを強制的にログオフすることで行われます。これは、ドレイン状態の仮想マシンに対してのみ行われ、すべての電源オン状態の仮想マシンに対して行われるわけではありません。ユーザーの強制ログオフによって発生する可能性のあるデータ損失を回避するため、この機能は、ユーザーのログオフを強制することなく、ログオフのリマインダーのみを送信するように構成することもできます。

以下の2つのオプションがあります。

- **ユーザーに通知してログオフを強制する**
- **ユーザーのログオフを強制せずにログオフのリマインダーを送信する**

ユーザーに通知してログオフを強制する

選択すると、Autoscaleは以下で指定された時間が経過した後、ユーザーをセッションからログオフします。



ピーク時の強制ログオフを有効にする。選択すると、指定された時間が経過したピーク時に、Autoscaleはそれらのユーザーをセッションからログオフします。

オフピーク時の強制ログオフを有効にする。選択すると、指定された時間が経過したオフピーク時に、Autoscaleはそれらのユーザーをセッションからログオフします。

仮想マシンがドレイン状態になった後に通知を表示する。仮想マシンがドレイン状態になった後、ユーザーに通知を送信できます。

- **通知のタイトル。**ユーザーに送信される通知のタイトルを指定できます。例: `A forced logoff has been initiated.`.

- **通知メッセージ**。ユーザーに送信される通知の内容を指定できます。メッセージで指定された時間を示す変数として、%s%または%m%を使用できます。時間を秒で表すには、%s%を使用します。時間を分で表すには、%m%を使用します。例: `Warning: To save costs, the machine shuts down in %s% seconds and you will be logged off from the session. Save your work and log back on to get a different machine.`.

ユーザーのログオフを強制せずにログオフリマインダーを送信する

これを選択すると、マシンがドレイン状態になった後、ユーザーはマシンからログオフするようリマインダーを受け取ります。このリマインダーは、以下で指定された間隔で送信されるように構成できます。

AutoscaleマルチセッションOS - ログオフリマインダーを送信(/en-us/citrix-virtual-apps-desktops/2503/media/autoscale-logoff-reminder-ms.png)

ピーク時にユーザーにリマインダーを送信する。これを選択すると、ユーザーはピーク時にX分ごとにセッションからログオフするようリマインダーを受け取ります（Xは指定された時間を表します）。

オフピーク時にユーザーにリマインダーを送信する。これを選択すると、ユーザーはオフピーク時にX分ごとにセッションからログオフするようリマインダーを受け取ります（Xは指定された時間を表します）。

ログオフリマインダー。マシンがドレイン状態になった後、ユーザーに送信されるリマインダーを構成できます。

- **リマインダーのタイトル**。ユーザーに送信するリマインダーのタイトルを指定できます。例: `Please log off from your session`。
- **リマインダーメッセージ**。ユーザーに送信するメッセージを指定できます。例: `Please log off from your session and log back on to save costs`。

考慮事項

マシンがすでにドレイン状態である場合、設定を変更する際には以下を考慮してください。

- 設定を**ユーザーのログオフを強制せずにログオフリマインダーを送信する**から**通知してユーザーのログオフを強制する**に変更した場合、新しい設定はすぐに有効になります。
- 設定を**通知してユーザーのログオフを強制する**から**ユーザーのログオフを強制せずにログオフリマインダーを送信する**に変更した場合、新しい設定はマシンが次にドレイン状態になるまで有効になりません。ユーザーは引き続きログオフを強制されます。

Autoscale™設定の有効性を分析する

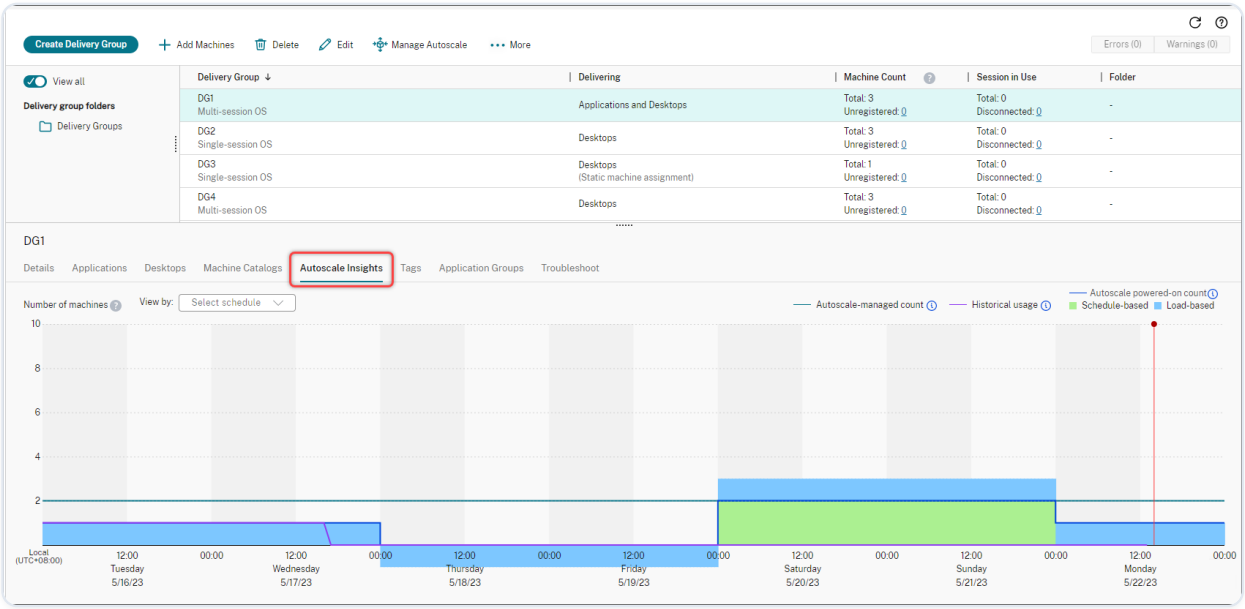
この記事では、前週のマシン使用状況に基づいてAutoscale設定の有効性を分析する方法について説明します。この分析を通じて、Autoscale設定の有効性について次のインサイトを得ることができます。

- 過剰プロビジョニングによる経済的無駄を特定する。
- プロビジョニング不足によりユーザーエクスペリエンスが悪影響を受けているかどうかを判断する。
- プロビジョニングされた容量がマシン使用状況と適切に一致していることを確認する。

この目標を達成するには、次の手順に従います。

1. Autoscaleが有効なデリバリーグループを選択します。
2. 下部ペインで、**Autoscale Insights**タブをクリックします。

   次のグラフが表示され、前週のマシン使用状況データとAutoscale設定に基づいて電源がオンになるマシンの数の比較が示されます。



* 赤い垂直線は現在の時刻を示します。

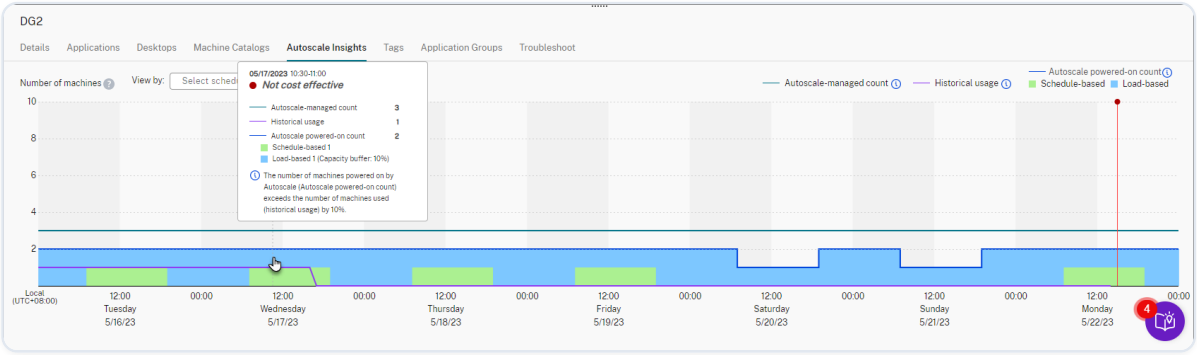
次の表は、このグラフに表示されるメトリックの説明を示しています。

メトリック	説明
Autoscale管理対象数	Autoscale によって管理されているマシンの総数。Autoscale 管理対象数 = デリバリーグループ内のマシンの総数 – メンテナンスモードのマシンの数 – Autoscale 用にタグ付けさ

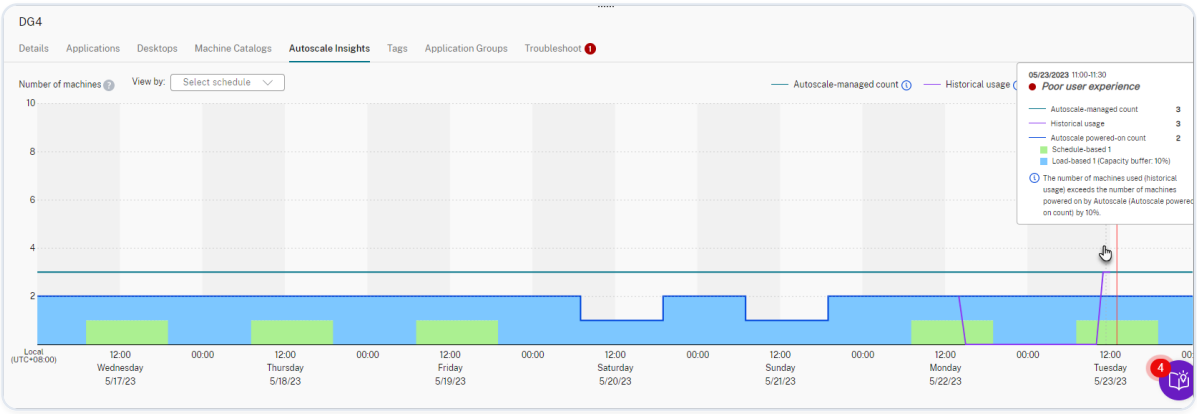
メトリック	説明
	れていないマシンの数 (タグ付けされた Autoscale 機能が有効な場合)。
Autoscale の電源オン数	Autoscale によって電源がオンにされたマシンの総数。Autoscale の電源オン数 = スケジュールベースのマシン数 + 負荷ベースのマシン数。
履歴使用状況	ユーザーに提供されたマシンの数。
スケジュールベース	Autoscale のスケジュールベース設定に基づいて電源がオンになっているマシンの数 (**注:** スケジュールベース設定は、静的シングルセッションOSタイプのデリバリーグループには適用されません)。
負荷ベース	Autoscale の負荷ベース設定に基づいて電源がオンになっているマシンの数。

3. 特定の時間帯における Autoscale 設定の有効性を確認するには、グラフ上のその時間帯にマウスを合わせます。比較結果と詳細なマシン数が表示された情報ボックスが表示されます。

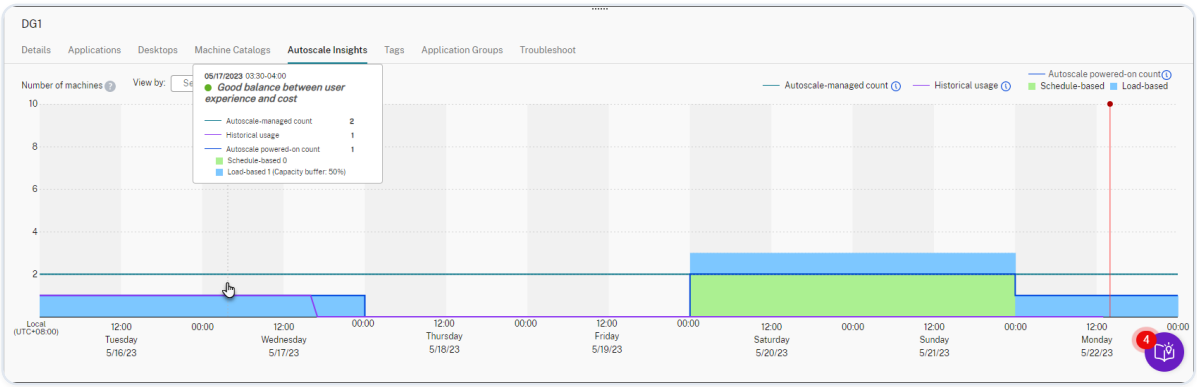
   - **費用対効果が低い**。履歴使用状況が Autoscale 設定 (Autoscale の電源オン数) の 90% 未満です。その結果、無駄な容量が存在する可能性があります。



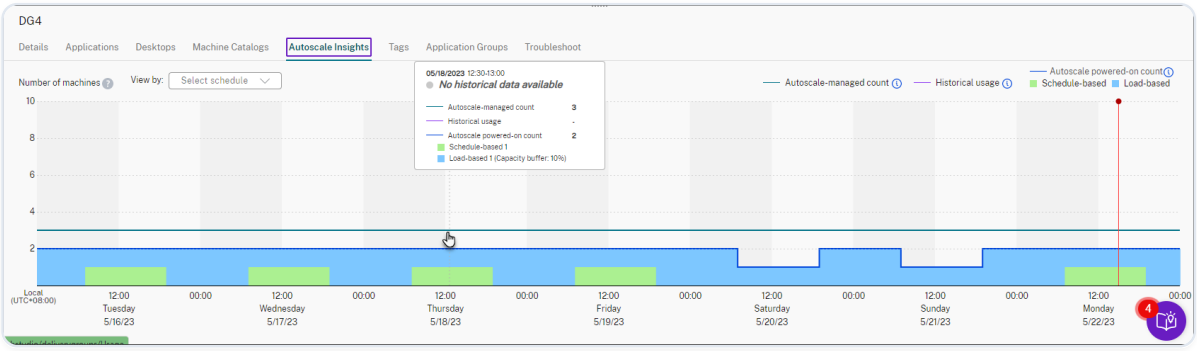
   - **ユーザーエクスペリエンスが悪い**。履歴使用状況が Autoscale 設定 (Autoscale の電源オン数) の 110% を超えています。その結果、ユーザーはマシンの電源がオンになるまで長い待ち時間を経験する可能性があります。



- **ユーザーエクスペリエンスとコストのバランスが良い。**履歴使用状況と Autoscale 設定 (Autoscale の電源オン数) の差が 10% 未満です。Autoscale 設定は履歴使用状況と一致しています。



- **履歴データなし。**履歴データがありません。考えられる原因としては、デリバリーグループでAutoscaleが有効になってから1週間未満であることなどが挙げられます。



4. Autoscaleスケジュールに基づいて日付範囲を強調表示するには、「**表示方法**」フィールドからスケジュールを選択します。
5. 分析に基づいて、Autoscale設定を調整します。詳細については、「スケジュールベースおよび負荷ベースの設定」を参照してください。

Broker PowerShell SDKコマンド

Broker PowerShell SDKを使用して、デリバリーグループのAutoscaleを構成できます。PowerShellコマンドを使用してAutoscaleを構成するには、PowerShell SDKバージョン7.21.0.12以降を使用

する必要があります。PowerShell SDKの詳細については、「SDKとAPI」(/ja-jp/citrix-virtual-apps-desktops/2503/sdk-api.html)を参照してください。

Set-BrokerDesktopGroup

既存の BrokerDesktopGroup を無効または有効にするか、その設定を変更します。このコマンドレットの詳細については、`<https://citrix.github.io/delivery-controller-sdk/Broker/Set-BrokerDesktopGroup/>`を参照してください。

例

PowerShellコマンドレットの使用方法の詳細については、以下の例を参照してください。

Autoscale™を有効にする

- 「MyDesktop」という名前のデリバリーグループに対して Autoscale を有効にしたいとします。`Set-BrokerDesktopGroup` PowerShell コマンドを使用します。例:
  - `PS C:\> Set-BrokerDesktopGroup "MyDesktop" -AutoscalingEnabled $true`

ピーク時とオフピーク時で容量バッファを個別に構成する

- 「MyDesktop」という名前のデリバリーグループに対して、容量バッファをピーク時に 20%、オフピーク時に 10% に設定したいとします。`Set-BrokerDesktopGroup` PowerShell コマンドを使用します。例:
  - `PS C:\> Set-BrokerDesktopGroup "MyDesktop" -PeakBufferSizePercent 20 -OffPeakBufferSizePercent 10`

切断時のタイムアウト設定を構成する

- 「MyDesktop」という名前のデリバリーグループに対して、**切断時のタイムアウト**値をピーク時に 60 分、オフピーク時に 30 分に設定したいとします。`Set-BrokerDesktopGroup` PowerShell コマンドを使用します。例:
  - `PS C:\> Set-BrokerDesktopGroup "MyDesktop" -PeakDisconnectTimeout 60 -OffPeakDisconnectTimeout 30`

「**ログオフ時タイムアウト**」設定を構成する

- 名前が「MyDesktop」であるデリバリーグループに対して、ピーク時には**ログオフ時タイムアウト**値を60分に、オフピーク時には30分に設定したいとします。`Set-BrokerDesktopGroup` PowerShellコマンドを使用します。例：

    - `PS C:\> Set-BrokerDesktopGroup "MyDesktop" -PeakLogOffTimeout 60 -OffPeakLogOffTimeout 30`

「**電源オフ遅延**」設定を構成する

- 名前が「MyDesktop」であるデリバリーグループに対して、電源オフ遅延を15分に設定したいとします。`Set-BrokerDesktopGroup` PowerShellコマンドを使用します。例：
    - `PS C:\> Set-BrokerDesktopGroup "MyDesktop" -PowerOffDelay 15`

電源オフ遅延が適用されない期間を構成する

- 名前が「MyDesktop」であるデリバリーグループに対して、電源オフ遅延が30分経過するまで有効になるようにしたいとします。`Set-BrokerDesktopGroup` PowerShellコマンドを使用します。例：
    - `C:\PS> Set-BrokerDesktopGroup "MyDesktop" -SettlementPeriodBeforeAutoShutdown 30`。

「**マシンインスタンスコスト**」設定を構成する

- 「MyDesktop」という名前のデリバリーグループに対して、1時間あたりのマシンインスタンスコストを0.2ドルに設定したいとします。`Set-BrokerDesktopGroup` PowerShellコマンドを使用します。例:
    - `PS C:\> Set-BrokerDesktopGroup "MyDesktop" -MachineCost 0.2`

New-BrokerPowerTimeScheme

デリバリーグループのBrokerPowerTimeSchemeを作成します。詳細については、`<https://citrix.github.io/delivery-controller-sdk/Broker/New-BrokerPowerTimeScheme/>`を参照してください。

例

UID値が3のデリバリーグループの電源時間スキームを作成するとします。新しいスキームは週末、月曜日、火曜日を対象とします。午前8時から午後6時30分までの時間帯は、スキームに含まれる日のピーク時間として定義されます。ピーク時間の場合、プールサイズ（電源がオンのまま維持されるマシンの数）は20です。オフピーク時間の場合、5です。`Set-BrokerDesktopGroup` PowerShellコマンドを使用できます。例：

- `PS C:\> $ps48=(0..47 | %{ if ($_ -lt 16 -or $_ -gt 37) { 5 } else { 20 } } )`

- `PS C:\> $pt48=(0..47 | %{ if ($_ -lt 16 -or $_ -gt 37) { $false } else { $true } } )`
- `PS C:\> New-BrokerPowerTimeScheme -Name 'First Half Week' -DaysOfWeek Weekend,Monday,Tuesday -DesktopGroupUid 3 -PeakHalfHours $pt48 -PoolSize $ps48`

動的セッションタイムアウトのパラメーター

以下のBroker PowerShell SDKコマンドレットは、複数の新しいパラメーターをサポートすることで、動的セッションタイムアウト用に拡張されました。

- Get-BrokerDesktopGroup
- New-BrokerDesktopGroup
- Set-BrokerDesktopGroup

これらのパラメーターには以下が含まれます。

- **DisconnectPeakIdleSessionAfterSeconds** – ピーク時にアイドル状態のセッションが切断されるまでの時間を秒単位で表します。このプロパティのデフォルト値は0で、ピーク時の関連動作が無効になっていることを示します。0より大きい値は、ピーク時のみデリバリーグループの動作を有効にします。
- **DisconnectOffPeakIdleSessionAfterSeconds** - オフピーク時間中にアイドルセッションが切断されるまでの時間を秒単位で表します。このプロパティのデフォルト値は0で、オフピーク中の関連動作が無効になっていることを示します。0より大きい値は、オフピーク時間中のみデリバリーグループの関連動作を有効にします。
- **LogoffPeakDisconnectedSessionAfterSeconds** - ピーク時に切断されたセッションが終了されるまでの時間を秒単位で表します。このプロパティのデフォルト値は0で、ピーク時の関連動作が無効になっていることを示します。0より大きい値は、ピーク時のみデリバリーグループの関連動作を有効にします。
- **LogoffOffPeakDisconnectedSessionAfterSeconds** - オフピーク時間中に切断されたセッションが終了されるまでの時間を秒単位で表します。このプロパティのデフォルト値は0で、オフピーク中の関連動作が無効になっていることを示します。0より大きい値は、オフピーク時間中のみデリバリーグループの関連動作を有効にします。

例

たとえば、「MyDesktop」という名前のデリバリーグループに対して、ピーク時のアイドルセッションタイムアウトを3,600秒に設定したいとします。`Set-BrokerDesktopGroup` PowerShellコマンドを使用します。例:

- `C:\PS> Set-BrokerDesktopGroup "MyDesktop" -DisconnectOffPeakIdleSessionAfterSeconds 3600`

これにより、「MyDesktop」という名前のデスクトップグループでは、オフピーク時に1時間以上アイドル状態だったセッションが切断されます。

Citrix Insightサービス

Citrix Insightサービス（CIS）は、計測、テレメトリ、ビジネスインサイト生成のためのCitrixプラットフォームです。その計測およびテレメトリ機能により、技術ユーザー（顧客、パートナー、エンジニア）は問題を自己診断して修正し、環境を最適化できます。CISの詳細と最新情報、およびその仕組みについては、`<https://cis.citrix.com>`を参照してください（Citrixアカウントの資格情報が必要です）。

Citrixにアップロードされるすべての情報は、トラブルシューティングと診断の目的、および製品の品質、信頼性、パフォーマンスの向上のために使用されます。ただし、以下に従います。

- `<https://cis.citrix.com/legal>`のCitrix Insightサービスポリシー
- `<https://www.cloud.com/privacy-policy>`のCitrixプライバシーポリシー

このCitrix Virtual Apps and Desktops™リリースは、以下のテクノロジーをサポートしています。

- Citrix Virtual Apps and Desktopsのインストールおよびアップグレード分析
- Citrixカスタマーエクスペリエンス向上プログラム（CEIP）
- シトリックス コールホーム
- シトリックス スカウト

CISおよびCitrix Analyticsとは別に、Studioをインストール（またはアップグレード）すると、Google Analyticsが自動的に収集され（後でアップロードされます）。Studioのインストール後、レジストリキーHKLM\\Software\\Citrix\\DesktopStudio\\GAEnabledを使用してこの設定を変更できます。値が1の場合は収集とアップロードが有効になり、0の場合は収集とアップロードが無効になります。

インストールおよびアップグレード分析

フルプロダクトインストーラーを使用してCitrix Virtual Apps and Desktopsコンポーネントを展開またはアップグレードすると、インストールプロセスに関する匿名情報が、コンポーネントをインストール/アップグレードしているマシンに収集および保存されます。このデータは、Citrixが顧客のインストールエクスペリエンスを向上させるために使用されます。

情報は、%ProgramData%\\Citrix\\CTQsの下にローカルに保存されます。

このデータの自動アップロードは、フルプロダクトインストーラーのグラフィカルインターフェイスとコマンドラインインターフェイスの両方でデフォルトで有効になっています。

- レジストリ設定のデフォルト値を変更できます。インストール/アップグレード前にレジストリ設定を変更すると、フルプロダクトインストーラーを使用する際にその値が使用されます。
- コマンドラインインターフェイスでインストール/アップグレードする場合、コマンドでオプションを指定することで、デフォルト設定を上書きできます。

自動アップロードの制御:

- インストール/アップグレード分析の自動アップロードを制御するレジストリ設定 (デフォルト = 1):
  - 場所: `HKLM:\Software\Citrix\MetaInstall`
  - 名前: SendExperienceMetrics
  - 値: 0 = 無効、1 = 有効
- PowerShell を使用すると、次のコマンドレットでインストール/アップグレード分析の自動アップロードを無効にできます。

```
New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\MetaInstall -Name
SendExperienceMetrics -PropertyType DWORD -Value 0
```

- XenDesktopServerSetup.exe または XenDesktopVDASetup.exe コマンドで自動アップロードを無効にするには、`/disableexperiencemetrics` オプションを含めます。

  XenDesktopServerSetup.exe または XenDesktopVDASetup.exe コマンドで自動アップロードを有効にするには、`/sendexperiencemetrics` オプションを含めます。

Citrix カスタマーエクスペリエンス向上プログラム

Citrixカスタマーエクスペリエンス向上プログラム (CEIP) に参加すると、匿名の統計情報と使用状況情報がCitrixに送信され、Citrix製品の品質とパフォーマンスの向上に役立てられます。詳細については、https://more.citrix.com/XD-CEIP を参照してください。

サイト作成時またはアップグレード時の登録

サイトを作成すると (最初のDelivery Controller™をインストールした後)、CEIPに自動的に登録されます。最初のデータアップロードは、サイト作成後約7日で行われます。

サイト作成後、いつでも参加を停止できます。Web Studioの左ペインで ノードを選択し、 設定をオフにします。

Citrix Virtual Apps and Desktops 展開をアップグレードする場合:

- CEIPをサポートしていなかったバージョンからアップグレードする場合、参加を希望するかどうか尋ねられます。
- CEIPをサポートしていたバージョンからアップグレードし、参加が有効になっていた場合、アップグレードされたサイトでCEIPが有効になります。
- CEIPをサポートしていたバージョンからアップグレードし、参加が無効になっていた場合、アップグレードされたサイトでCEIPが無効になります。
- CEIPをサポートしていたバージョンからアップグレードし、参加状況が不明な場合、参加を希望するかどうか尋ねられます。

収集された情報は匿名であるため、Citrix Insight Servicesにアップロードされた後は閲覧できません。

VDAインストール時の登録

デフォルトでは、Windows VDAをインストールすると、CEIPに自動的に登録されます。このデフォルト設定はレジストリ設定で変更できます。VDAをインストールする前にレジストリ設定を変更すると、その値が使用されます。

CEIPへの自動登録を制御するレジストリ設定（デフォルト = 1）：

場所: HKLM: `\\Software\Citrix\Telemetry\CEIP` 名前: Enabled 値: 0 = 無効, 1 = 有効

デフォルトでは、`Enabled` プロパティはレジストリに隠されています。指定されていない場合、自動アップロード機能は有効になります。

PowerShellを使用すると、次のコマンドレットでCEIPへの登録を無効にできます。

```
New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\Telemetry\CEIP -Name Enabled
-PropertyType DWORD -Value 0
```

収集されたランタイムデータポイントは、定期的にファイルとして出力フォルダー（デフォルト %programdata%/Citrix/VdaCeip）に書き込まれます。

データの初回アップロードは、VDAのインストール後約7日で行われます。

その他の製品およびコンポーネントのインストール時の登録

関連するCitrix製品、コンポーネント、テクノロジー（Citrix Provisioning™、AppDNA、Citrix License Server、Windows向けCitrix Workspace™アプリ、Universal Print Server、Session Recordingなど）をインストールする際にも、CEIPに参加できます。インストールと参加のデフォルト値の詳細については、それぞれのドキュメントを参照してください。

シトリックス コールホーム

Citrix Virtual Apps and Desktopsで特定のコンポーネントと機能をインストールすると、Citrix Call Homeに参加する機会が提供されます。Call Homeは診断データを収集し、そのデータを分析およびトラブルシューティングのために、Citrix Insight Servicesに直接（デフォルトポート443のHTTPS経由で）定期的にテレメトリパッケージをアップロードします。

Citrix Virtual Apps and Desktopsでは、Call HomeはCitrix Telemetry Serviceという名前のバックグラウンドサービスとして実行されます。

Call Homeのスケジュール機能はCitrix Scoutでも利用できます。詳細については、Citrix Scoutを参照してください。

収集される情報

Citrix Diagnostic Facility (CDF) トレースは、トラブルシューティングに役立つ情報をログに記録します。Call Homeは、VDA登録やアプリケーション/デスクトップの起動など、一般的な障害のトラブルシューティングに役立つCDFトレースのサブセットを収集します。このテクノロジーは、常時オンのトレース (AOT) として知られています。AOTログは、C:\ProgramData\Citrix\TelemetryService\CitrixAOTにディスク保存されます。

> **注:**
>
> `ProgramData`フォルダーは非表示になっています。表示するには、**表示** > **表示/非表示** > **隠しファイル** をクリックします。

> Call Homeは、他のEvent Tracing for Windows (ETW) 情報を収集しません。また、そのように構成することもできません。

Call Homeは、次のような他の情報も収集します。

- Citrix Virtual Apps and Desktopsによって`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix`の下に作成されたレジストリ。

- Citrix名前空間の下にあるWindows Management Instrumentation (WMI) 情報。
- 実行中のプロセスの一覧。
- %PROGRAM DATA%\\Citrix\\CDFに保存されているCitrixプロセスのクラッシュダンプ。
- インストールおよびアップグレード情報。これには、製品の完全なメタインストーラーログ、失敗したMSIログ、MSIログアナライザーからの出力、StoreFront™ログ、ライセンス互換性チェックログ、および予備的なサイトアップグレードテストの結果が含まれる場合があります。

トレース情報は収集時に圧縮されます。Citrix Telemetry Serviceは、最大10 MBの圧縮された最新のトレース情報を、最大8日間の時間制限で保持します。

- データを圧縮することで、Call HomeはVDA上で小さなフットプリントを維持できます。
- トレースはメモリに保持され、プロビジョニングされたマシンでのIOPsを回避します。
- トレースバッファは循環メカニズムを使用して、メモリ内のトレースを保持します。

Call Homeは、(/ja-jp/citrix-virtual-apps-desktops/2503/manage-deployment/call-home-datapoints.html)に記載されている主要なデータポイントを収集します。

構成と管理の概要

Call Homeには、製品の完全なインストールウィザードを使用するか、後でPowerShellコマンドレットを使用して登録できます。登録すると、デフォルトで診断情報が毎週日曜日の現地時間午前3時頃に収集され、Citrixにアップロードされます。アップロードは、指定された時刻から2時間の範囲でランダム化されます。これは、デフォルトのスケジュールを使用するアップロードが午前3時から午前5時の間に行われることを意味します。

診断情報をスケジュールに基づいてアップロードしたくない場合（またはスケジュールを変更したい場合）は、PowerShellコマンドレットを使用して、診断情報を手動で収集してアップロードするか、ローカルに保存することができます。

スケジュールされた Call Home アップロードに登録する場合、および診断情報を手動で Citrix にアップロードする場合、Citrix アカウントまたは Citrix Cloud™ の資格情報を提供します。Citrix は、資格情報をアップロードトークンと交換します。このトークンは、顧客を識別し、データをアップロードするために使用されます。資格情報は保存されません。

アップロードが行われると、Citrix アカウントに関連付けられているアドレスに通知メールが送信されます。

コンポーネントをインストールするときにCall Homeを有効にした場合、後で(#disable-call-home)無効にできます。

前提条件

- マシンはPowerShell 3.0以降を実行している必要があります。
- Citrix Telemetry Serviceがマシン上で実行されている必要があります。
- システム変数 `PSModulePath` は、Telemetryのインストールパス（例: C:\\Program Files\\Citrix\\Telemetry Service\\.）に設定する必要があります。

コンポーネントのインストール中に Call Home を有効にする

VDA のインストールまたはアップグレード中: 製品版インストーラーのグラフィカルインターフェイスを使用して Virtual Delivery Agent をインストールまたはアップグレードする際に、Call Home に参加するかどうかを尋ねられます。次の 2 つのオプションがあります。

- Call Home に参加する。
- Call Home に参加しない。

VDAをアップグレードしていて、以前にCall Homeに登録していた場合、そのウィザードページは表示されません。

Controllerのインストールまたはアップグレード中: グラフィカルインターフェイスを使用してDelivery Controllerをインストールまたはアップグレードすると、Call Homeに参加するかどうかを尋ねられます。3つのオプションがあります。

Controllerをインストールする際、そのサーバーに「サービスとしてログオン」ポリシー設定が適用されたActive Directory GPOがある場合、インストールウィザードのCall Homeページで情報を構成することはできません。詳細については、CTX218094を参照してください。

Controllerをアップグレードしていて、以前にCall Homeに登録していた場合、参加について尋ねられることはありません。

PowerShellコマンドレット

PowerShellヘルプには、これらの一般的なユースケースでは使用されないコマンドレットとパラメーターの説明を含む、包括的な構文が記載されています。

アップロードにプロキシサーバーを使用するには、「プロキシサーバーの構成」を参照してください。

- **スケジュールされたアップロードを有効にする:** 診断コレクションはCitrixに自動的にアップロードされます。カスタムスケジュール用の追加のコマンドレットを入力しない場合、デフォルトのスケジュールが使用されます。

```
$cred = Get-Credential

Enable-CitrixCallHome -Credential $cred
```

スケジュールされたアップロードが有効になっていることを確認するには、`Get-CitrixCallHome`と入力します。有効になっている場合、戻り値は`IsEnabled=True`と`IsMasterImage=False`です。

- **マスターイメージから作成されたマシンに対するスケジュールされたアップロードを有効にする:** マスターイメージでスケジュールされたアップロードを有効にすると、マシンカタログで作成される各マシンを構成する必要がなくなります。

  `Enable-CitrixCallHome -Credential $cred -MasterImage`

  スケジュールされたアップロードが有効になっていることを確認するには、**Get-CitrixCallHome** と入力します。有効になっている場合、戻り値は `IsEnabled=True` と `IsMasterImage=True` です。

- **カスタムスケジュールを作成する:** 診断コレクションとアップロードの毎日または毎週のスケジュールを作成します。

```
$timespan = New-TimeSpan –Hours hours -Minutes minutes

Set-CitrixCallHomeSchedule –TimeOfDay $timespan –DayOfWeek day
-UploadFrequency {Daily|Weekly}
```

例:

次のコマンドレットは、毎日夜の10時20分にデータをバンドルしてアップロードするスケジュールを作成します。Hoursパラメーターは24時間形式を使用します。`UploadFrequency` パラメーターの値がDailyの場合、`DayOfWeek` パラメーターは指定されていても無視されます。

```
$timespan – New-TimeSpan –Hours 22 –Minutes 20

Set-CitrixCallHomeSchedule –TimeOfDay $timespan -UploadFrequency Daily
```

スケジュールを確認するには、`Get-CitrixCallHomeSchedule`と入力します。上記の例では、`StartTime=22:20:00, DayOfWeek=Sunday (ignored), Upload Frequency=Daily`が返されます。

次のコマンドレットは、毎週水曜日の夜10時20分にデータをバンドルしてアップロードするスケジュールを作成します。

```
$timespan – New-TimeSpan –Hours 22 –Minutes 20

Set-CitrixCallHomeSchedule –TimeOfDay $timespan –DayOfWeek Wed
-UploadFrequency Weekly
```

スケジュールを確認するには、`Get-CitrixCallHomeSchedule`と入力します。上記の例では、`StartTime=22:20:00, DayOfWeek=Wednesday, Upload Frequency=Weekly`が返されます。

Call Homeを無効にする

PowerShellコマンドレットを使用するか、Citrix Scoutを介してCall Homeを無効にできます。

Call Homeのスケジュールされたアップロードが無効になっている場合でも、AOTログは収集されディスクに保存されます。(スケジュールされたアップロードが無効になっている場合、AOTログはCitrixに自動的にアップロードされません。) AOTログの収集とローカルストレージを無効にすることができます。

PowerShellでCall Homeを無効にする

次のコマンドレットを実行すると、診断データはCitrixに自動的にアップロードされなくなります。(Citrix ScoutまたはテレメトリPowerShellコマンドレットを使用して、診断データをアップロードすることは引き続き可能です。)

`Disable-CitrixCallHome`

Call Homeが無効になっていることを確認するには、`Get-CitrixCallHome`と入力します。無効になっている場合、戻り値は`IsEnabled=False`と`IsMasterImage=False`です。

Citrix Scoutを使用して収集スケジュールを無効にする

Citrix Scout を使用して診断収集スケジュールを無効にするには、コレクションのスケジュール のガイダンスに従ってください。ステップ 3 で、**オフ** をクリックして、選択したマシンのスケジュールをキャンセルします。

AOTログの収集を無効にする

次のコマンドレットを実行すると(`Enabled`フィールドを`false`に設定すると)、AOTログは収集されなくなります。

`Enable-CitrixTrace -Listen'{"trace":{"enabled":false,"persistDirectory":"C:\Users\Public","maxSizeBytes":1000000, "sliceDurationSeconds":300}}'`

`Listen`パラメーターには、JSON形式の引数が含まれています。

Call Homeアップロード用のプロキシサーバーを構成する

Call Home が有効になっているマシンで、次のタスクを完了します。以下の手順の例の図には、サーバーアドレスとポート 10.158.139.37:3128 が含まれています。お使いの情報は異なります。

1. ブラウザにプロキシサーバー情報を追加します。Internet Explorer で、**インターネットオプション \> 接続 \> LAN の設定** を選択します。「**LAN にプロキシサーバーを使用する**」を選択し、プロキシサーバーのアドレスとポート番号を入力します。
2. PowerShell で `netsh winhttp import proxy source=ie` を実行します。

   プロキシサーバーを構成する際に netsh コマンドを実行する例 (/en-us/citrix-virtual-apps-desktops/2503/media/call-home-proxy-ie.png)
3. テキストエディターを使用して、C:\\Program Files\\Citrix\\Telemetry Service にある TelemetryService.exe 設定ファイルを編集します。赤枠内に示されている情報を追加します。

   TelemetryService.exe ファイルにプロキシ情報を追加する (/en-us/citrix-virtual-apps-desktops/2503/media/call-home-proxy-config.png)
4. テレメトリサービスを再起動します。

PowerShell で Call Home コマンドレットを実行します。

診断情報を手動で収集してアップロードする

CIS Webサイトを使用して、診断情報バンドルをCISにアップロードできます。PowerShell コマンドレットを使用して、診断情報を収集し、CISにアップロードすることもできます。

CIS Webサイトを使用してバンドルをアップロードするには：

1. Citrixアカウントの資格情報を使用して、Citrix Insight Servicesにログオンします。
2. を選択します。
3. を選択し、データの場所に移動します。

CISは、データアップロードを管理するいくつかのPowerShellコマンドレットをサポートしています。このドキュメントでは、2つの一般的なケースにおけるコマンドレットについて説明します。

- `Start-CitrixCallHomeUpload` コマンドレットを使用して、診断情報バンドルを手動で収集し、CISにアップロードします。（バンドルはローカルに保存されません。）
- `Start-CitrixCallHomeUpload` コマンドレットを使用して、データを手動で収集し、診断情報バンドルをローカルに保存します。これにより、データをプレビューできます。その後、

`Send-CitrixCallHomeBundle` コマンドレットを使用して、そのバンドルのコピーをCISに手動でアップロードします。(最初に保存したデータはローカルに残ります。)

PowerShellヘルプには、これらの一般的なユースケースでは使用されないコマンドレットとパラメーターの説明を含む、包括的な構文が記載されています。

CISにデータをアップロードするコマンドレットを入力すると、アップロードの確認を求められます。アップロードが完了する前にコマンドレットがタイムアウトした場合は、システムイベントログでアップロードのステータスを確認してください。サービスがすでにアップロードを実行している場合、アップロード要求が拒否されることがあります。

データの収集とバンドルのCISへのアップロード:

```
Start-CitrixCallHomeUpload [-Credential] PSCredential [-InputPath string]
[-Description string] [-IncidentTime string] [-SRNumber string] [-Name
string] [-UploadHeader string] [-AppendHeaders string] [-Collect string]
[<CommonParameters>]
```

データの収集とローカルへの保存:

```
Start-CitrixCallHomeUpload -OutputPath <String> [-InputPath string] [-
Description string] [-IncidentTime string] [-SRNumber string] [-Name
string] [-UploaderHeader string] [-AppendHeaders string] [-Collect
strings] [<CommonParameters>]
```

次のパラメーターが有効です。

- **Credential：** アップロードをCISに指示します。
- **InputPath:** バンドルに含めるzipファイルの場所。これは、Citrixサポートが要求する追加ファイルである可能性があります。.zip拡張子を含めるようにしてください。
- **OutputPath:** 診断情報が保存される場所。このパラメーターは、Call Homeデータをローカルに保存する場合に必要です。
- **Description and Incident Time:** アップロードに関する自由形式の情報。
- **SRNumber:** Citrixテクニカルサポートのインシデント番号。
- **Name:** バンドルを識別する名前。
- **UploadHeader:** CISにアップロードされるアップロードヘッダーを指定するJSON形式の文字列。
- **AppendHeaders:** CISにアップロードされる追加ヘッダーを指定するJSON形式の文字列。

- **Collect:** 収集または省略するデータを指定するJSON形式の文字列で、{'collector': {'enabled':Boolean}} の形式で、Booleanはtrueまたはfalseです。 有効なコレクター値は次のとおりです。

  - 'WMI'
  - 'プロセス'
  - 'レジストリ'
  - 'クラッシュレポート'
  - 'トレース'
  - 'ファイル'
  - 'MSI'
  - 'ローカルデータ'
  - 'サイトデータ'
  - 'SFB'

  デフォルトでは、「sfb」を除くすべてのコレクターが有効になっています。

  「sfb」コレクターは、Skype for Business の問題を診断するためにオンデマンドで使用されるように設計されています。「enabled」パラメーターに加えて、「sfb」コレクターはターゲットユーザーを指定するための「account」および「accounts」パラメーターをサポートしています。次のいずれかの形式を使用します。

  - "-収集 "{'sfb':{'account':'domain\\\user1'}}"
  - 収集 "{'sfb':{'accounts':}}"

- **共通パラメーター:** PowerShell ヘルプを参照してください。

以前ローカルに保存されたデータをアップロードする:

```
Send-CitrixCallHomeBundle -Credential <PSCredentia\> -Path string
[<CommonParameters>]
```

`Path` パラメーターは、以前に保存されたバンドルの場所を指定します。

例:

以下のコマンドレットは、Call Home データ（WMI コレクターからのデータを除く）を CIS にアップロードするよう要求します。このデータは、Citrix Support ケース 123456 について午後 2 時 30 分に記録された Citrix Provisioning VDA の登録失敗に関連しています。Call Home データに

加えて、ファイル「`c:\Diagnostics\ExtraData.zip`」がアップロードされたバンドルに組み込まれます。

```
C:\PS\>Start-CitrixCallHomeUpload -InputPath "c:
\Diagnostics\ExtraData.zip" -Description "Registration failures with
Citrix Provisioning VDAs" -IncidentTime "14:30" -SRNumber 123456 -Name
"RegistrationFailure-021812016" -Collect "{'wmi':{'enabled':false}}"
-UploadHeader "{'key1':'value1'}" -AppendHeaders "{'key2':'value2'}"
```

以下のコマンドレットは、午前 8 時 15 分に記録された Citrix Support ケース 223344 に関連する Call Home データを保存します。データはネットワーク共有上のファイル mydata.zip に保存されます。Call Home データに加えて、ファイル「`c:\Diagnostics\ExtraData.zip`」が保存されたバンドルに組み込まれます。

```
C:\PS\>Start-CitrixCallHomeUpload -OutputPath \
\mynetwork\myshare\mydata.zip -InputPath "c:\Diagnostics\ExtraData.zip"
-Description "Diagnostics for incident number 223344" -IncidentTime "8:15"
-SRNumber 223344
```

以下のコマンドレットは、以前に保存したデータバンドルをアップロードします。

```
$cred=Get-Credential

C:\PS>Send-CitrixCallHomeBundle –Credential $cred -Path \
\mynetwork\myshare\mydata.zip
```

シトリックス スカウト

はじめに

Citrix Scout は診断情報を収集し、ヘルスチェックを実行します。その結果を使用して、Citrix Virtual Apps and Desktops™ の展開を維持できます。Citrix は、Citrix Insight Services を通じて、診断情報収集の包括的で自動化された分析を提供します。また、Scout を使用して、単独で、または Citrix Support のガイダンスを受けて問題をトラブルシューティングすることもできます。

収集ファイルを Citrix にアップロードして、Citrix Support からの分析とガイダンスを受けることができます。または、収集したファイルをローカルに保存して自分で確認し、後でその収集ファイルを Citrix にアップロードして分析することもできます。

Scout には、次の手順があります。

- **収集:** サイトで選択したマシンに対して、一度限りの診断情報収集を実行します。その後、ファイルを Citrix にアップロードするか、ローカルに保存することができます。
- **トレースと再現:** 選択したマシンで手動トレースを開始します。その後、それらのマシンで問題を再現します。問題を再現した後、トレースは停止されます。その後、Scout は他の診断情報を収集し、ファイルを Citrix にアップロードするか、ローカルに保存します。
- **スケジュール:** 選択したマシンで、毎日または毎週指定した時刻に診断情報収集が実行されるようにスケジュールします。ファイルは自動的に Citrix にアップロードされます。
- **ヘルスチェック:** サイトとそのコンポーネントの正常性と可用性を評価するチェックを実行します。Delivery Controller、Virtual Delivery Agent (VDA)、StoreFront™ サーバー、Citrix License Server のヘルスチェックを実行できます。チェック中に問題が見つかった場合、Scout は詳細なレポートを提供します。Scout が起動するたびに、更新されたヘルスチェックスクリプトが確認されます。新しいバージョンが利用可能な場合、Scout はそれらを自動的にダウンロードし、次回のヘルスチェック実行時に使用します。

> **注:**
>
> **トレースと再現、スケジュール、ヘルスチェック**の手順は、現在 Linux VDA では利用できません。

> この記事で説明されているグラフィカルインターフェイスは、Scout を使用する主要な方法です。または、PowerShell を使用して、一度限りの診断情報収集またはスケジュールされた診断情報収集とアップロードを構成することもできます。「Call Home」を参照してください。

Scout の実行場所:

- オンプレミス展開では、Delivery Controller™ から Scout を実行して、1つ以上のVirtual Delivery Agent (VDA)、Delivery Controller、StoreFront サーバー、Federated Authentication Service (FAS) サーバー、および License Server の診断情報を取得したり、チェックを実行したりできます。また、VDA から Scout を実行して、ローカル診断情報を収集することもできます。

  > **注:**
  >
  > 現在、FAS構成の問題を診断するための*Health Check*は、FASサーバー上のScoutではサポートされていません。

- Citrix DaaS (旧Citrix Virtual Apps and Desktops service) を使用するCitrix Cloud環境では、VDAからScoutを実行してローカル診断を収集します。

Scout アプリケーションのログは `C:\ProgramData\Citrix\TelemetryService\ScoutUI.log` に保存されます。このファイルはトラブルシューティングに使用できます。

収集される情報

Scoutによって収集される診断情報には、Citrix Diagnostic Facility (CDF) トレースログファイルが含まれます。Always-on Tracing (AOT) と呼ばれるCDFトレースのサブセットも含まれます。AOT情報は、VDA登録やアプリケーション/デスクトップの起動などの一般的な問題のトラブルシューティングに役立ちます。その他のEvent Tracing for Windows (ETW) 情報は収集されません。

収集される情報には以下が含まれます。

- `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix` の下にCitrix Virtual Apps and Desktopsによって作成されたレジストリエントリ。
- **Citrix 名前空間**の下にあるWindows Management Instrumentation (WMI) 情報。
- 実行中のプロセス。
- `%PROGRAMDATA%\Citrix\CDF` に保存されているCitrixプロセスのクラッシュダンプ。
- Citrixポリシー情報（CSV形式）。
- インストールおよびアップグレード情報。収集される情報には、製品の完全なメタインストーラーログ、失敗したMSIログ、MSIログアナライザーからの出力、StoreFrontログ、ライセンス互換性チェックログ、および予備的なサイトアップグレードテストの結果が含まれる場合があります。

トレース情報について：

- トレース情報は収集時に圧縮されるため、マシン上のフットプリントは小さく保たれます。
- 各マシンでは、Citrix Telemetry Serviceが圧縮された最新のトレース情報を最大8日間保持します。
- Citrix Virtual Apps and Desktops 7 1808以降、AOTトレースはデフォルトでローカルディスクに保存されます。(以前のバージョンでは、トレースはメモリに保持されていました。) デフォルトパス = `C:\Users\CitrixTelemetryService\AppData\Local\CitrixAOT`。
- Citrix Virtual Apps and Desktops 7 1811以降、ネットワーク共有に保存されたAOTトレースは、他の診断情報とともに収集されます。

- `Enable-CitrixTrace` コマンドレットまたは `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Telemetry DefaultListen` レジストリ文字列を使用して、最大サイズ (デフォルト = 10 MB) とスライス期間を変更できます。
- トレースは、ファイルが `MaxSize` の10%に達するまでファイルに追加されます。

Scoutが収集するデータポイントのリストについては、「Call Home key datapoints」を参照してください。

Scoutの構成

ScoutはLinux VDAで動作するように構成できます。Linux VDAとテレメトリの詳細については、「Citrix Telemetry Serviceとの統合」を参照してください。

Linux VDAは、`ctxtelemetry` ソケットポートまたはテレメトリサービス用のポートを自動的に変更する場合があります。その場合、ポートを手動で構成する必要があります。

1. C:\Program Files\Citrix\Telemetry Serviceに移動します。
2. ScoutUI.exe.configファイルを開きます。
3. LinuxVDATelemetryServicePortまたはLinuxVDATelemetryWakeupPortの値を、Linux VDAで構成された値に変更します。

- `<add key="LinuxVDATelemetryServicePort" value="7502"/>`
- `<add key="LinuxVDATelemetryWakeupPort" value="7503"/>`

1. 変更を保存してファイルを閉じます。
2. Scoutを再度開いて、最新の構成が読み込まれていることを確認します。

ヘルスチェックについて

ヘルスチェックデータは、`C:\ProgramData\Citrix\TelemetryService\` の下のフォルダーに保存されます。

サイトのヘルスチェック

サイトヘルスチェックは、FlexCast Management Architecture (FMA) サービスの包括的な評価を提供する環境テストサービスに含まれています。これらのチェックでは、サービスの可用性を確認するだけでなく、データベース接続などの他のヘルスインジケーターも調べます。

サイトヘルスチェックは、Delivery Controller で実行されます。サイトの規模によっては、これらのチェックの完了に最大1時間かかる場合があります。

DELIVERY CONTROLLER の構成チェック

サイトヘルスチェックの一環として、Delivery Controller の構成チェックでは、Citrix の Virtual Apps and Desktops サイトに関する推奨事項に基づいて、以下の問題が存在するかどうかを確認します。

- 1 つ以上の Delivery Controller が失敗状態にある。
- サイトに Delivery Controller が 1 つしかない。
- Delivery Controller のバージョンが異なる。

ヘルスチェックの権限と要件を満たすことに加えて、Delivery Controller の構成チェックには以下が必要です。

- 少なくとも 1 つの Controller の電源がオンになっていること。
- Controller 上で Broker Service が実行されていること。
- Controller からサイトデータベースへの接続が機能していること。

VDA の健全性チェック

VDA の健全性チェックは、一般的な VDA 登録、セッション起動、およびタイムゾーンリダイレクトの問題の考えられる原因を特定します。

VDAでの登録について、Scoutは以下をチェックします。

- VDA ソフトウェアのインストール
- VDA マシンのドメインメンバーシップ
- VDA 通信ポートの可用性
- VDA サービスステータス
- Windows ファイアウォール構成
- Controller との通信
- Controller との時刻同期
- VDA 登録ステータス

VDAでのセッション起動について、Scoutは以下をチェックします。

- セッション起動通信ポートの可用性
- セッション起動サービスのステータス
- セッション起動 Windows ファイアウォール構成
- VDA リモートデスクトップサービス クライアントアクセスライセンス

- VDA アプリケーション起動パス
- セッション起動レジストリ設定

VDA でのタイムゾーンリダイレクトについて、Scout は以下をチェックします。

- Windows ホットフィックスのインストール
- Citrix ホットフィックスのインストール
- Microsoft グループポリシー設定
- Citrix グループポリシー設定

VDA 上の Profile Management について、Scout は以下をチェックします。

- ハイパーバイザーの検出
- プロビジョニングの検出
- シトリックス バーチャル アプリケーションズ アンド デスクトップス
- Personal vDisk の構成
- ユーザー ストア
- Profile Management Service のステータス検出
- Winlogon.exe フッキングテスト

Profile Management のチェックを実行するには、VDA に Profile Management をインストールして有効にする必要があります。Profile Management の構成チェックの詳細については、Knowledge Center の記事 CTX132805 を参照してください。

StoreFront の健全性チェック

StoreFront のチェックでは、以下を確認します。

- Citrix Default Domain サービスが実行されていること
- Citrix Credential Wallet サービスが実行されていること
- StoreFront サーバーから Active Directory ポート 88 への接続
- StoreFront サーバーから Active Directory ポート 389 への接続
- ベース URL が有効な FQDN を持っていること
- ベース URL から正しい IP アドレスを取得できること
- IIS アプリケーションプールが .NET 4.0 を使用していること
- 証明書がホスト URL の SSL ポートにバインドされているかどうか
- 証明書チェーンが完全であるかどうか

- 証明書の有効期限が切れているかどうか
- 証明書がまもなく（30日以内に）期限切れになるかどうか

ライセンスサーバーのチェック

ライセンスサーバーのチェックでは、以下を確認します。

- Delivery Controllerからのライセンスサーバー接続
- ライセンスサーバーのファイアウォールリモートアクセスステータス
- Citrix Licensingサービスのステータス
- ライセンスサーバーのライセンスキャッシュモードの状態
- ライセンスサーバーポートの接続
- Citrix ベンダーデーモン (CITRIX) が実行されているかどうか
- システムクロックが同期されているかどうか
- Citrix Licensingサービスがローカルサービスアカウントで実行されているかどうか
- `CITRIX.opt`ファイルの存在
- Customer Success Servicesの有効期限
- Citrix ライセンスサーバーの更新
- ライセンスサーバー証明書がDelivery Controllerの信頼されたルートストアにあるかどうか

ヘルスチェックの権限と要件を満たすことに加えて、ライセンスサーバーはドメインに参加している必要があります。そうしないと、ライセンスサーバーは検出されません。

ヘルスチェックの実行

ヘルスチェック手順は、マシンの選択、チェックの開始、および結果レポートの確認で構成されます。

1. Scoutを起動します。マシンの**スタート**メニューから、**Citrix > Citrix Scout**を選択します。開いたページで、**Health Check**をクリックします。
2. マシンを選択します。**Find machine**をクリックしてマシンを検出します。**Select machines**ページには、サイトで検出されたすべてのVDA、Delivery Controller、およびLicense Serverが一覧表示されます。マシン名で表示をフィルタリングできます。診断を収集する各マシンの横にあるチェックボックスをオンにして、**Continue**をクリックします。

   その他のコンポーネントタイプ（StoreFrontサーバーやVDAマシンなど）を追加するには、Add machines manuallyおよびImport VDA machinesを参照してください。Citrix Provisioning™ ServerまたはLicense Serverを手動で追加することはできません。

Scoutは、選択された各マシンで検証テストを自動的に起動し、Verification testsに記載されている基準を満たしていることを確認します。検証に失敗した場合、**Status**列にメッセージが表示され、そのマシンのチェックボックスがオフになります。次のいずれかを実行できます。

- 問題を解決し、そのマシンのチェックボックスを再度選択します。これにより、検証テストが再試行されます。
- そのマシンをスキップします（チェックボックスをオフのままにします）。そのマシンではヘルスチェックは実行されません。

検証テストが完了したら、**続行**をクリックします。

3. 選択したマシンでヘルスチェックを実行します。概要には、テストが実行されたマシン（検証テストに合格した選択済みのマシン）が一覧表示されます。**チェック開始**をクリックします。

   チェック中およびチェック後：

   - **Status**列には、マシンの現在のチェック状態が表示されます。
   - 進行中のすべてのチェックを停止するには、ページ右下隅にある**Stop Checking**をクリックします。（個々のマシンのヘルスチェックをキャンセルすることはできず、選択したすべてのマシンのみをキャンセルできます。チェックが完了したマシンからの情報は保持されます。）.
   - 選択したすべてのマシンのチェックが完了すると、右下隅にある**Stop Checking**ボタンが**Done**に変わります。
   - チェックが失敗した場合は、**Action**列の**Retry**をクリックできます。
   - チェックが問題なく完了した場合、**Action**列は空になります。
   - チェックで問題が見つかった場合は、「**View Details**」をクリックして結果を表示します。
   - 選択したすべてのマシンでチェックが完了したら、「**Back**」をクリックしないでください。(クリックすると、チェック結果が失われます。)

4. チェックが完了したら、「**Done**」をクリックしてScoutの開始ページに戻ります。

ヘルスチェックの結果

レポートを生成するCitrixチェックの場合、レポートには以下が含まれます。

- 結果レポートが生成された日時
- チェックされたマシン
- 対象のマシンでチェックによって確認された条件

権限と要件

権限:

- 診断情報を収集するには:
  - 診断情報を収集する各マシンで、ローカル管理者およびドメインユーザーである必要があります。
  - 各マシンでLocalAppDataディレクトリに書き込む権限が必要です。
- ヘルスチェックを実行するには:
  - ドメインユーザーグループのメンバーである必要があります。
  - サイトに対して、フル管理者であるか、読み取り専用および**環境テストの実行**権限を持つカスタムロールを持っている必要があります。
  - スクリプトの実行を許可するには、スクリプト実行ポリシーを少なくとも `RemoteSigned` に設定します。例: `Set-ExecutionPolicy RemoteSigned`。**注:** 他のスクリプト実行権限でも機能する場合があります。
- Scout を起動するときは、**管理者として実行**を使用します。

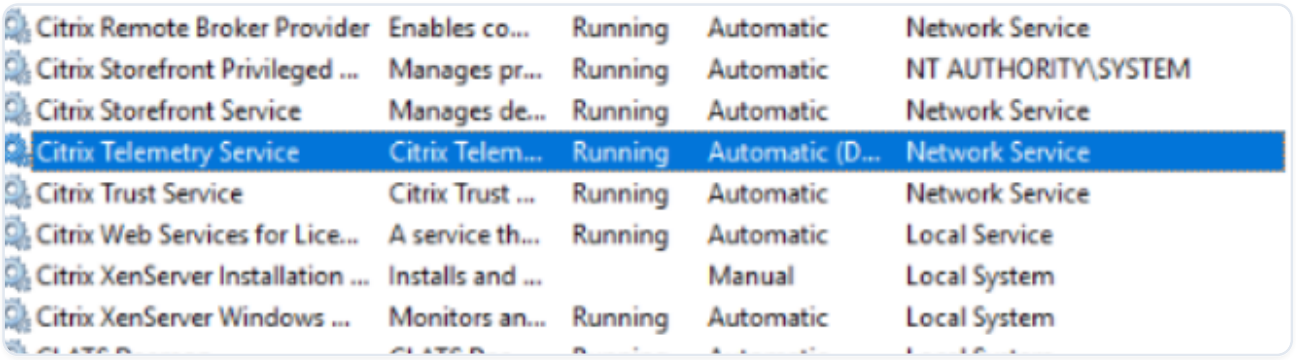
診断情報を収集したり、ヘルスチェックを実行したりする各マシンについて:

- Scout はマシンと通信できる必要があります。
- ファイルとプリンターの共有が有効になっている必要があります。
- PSRemoting と WinRM が有効になっている必要があります。マシンでは PowerShell 3.0 以降が実行されている必要もあります。
- Citrix Telemetry Service がマシンで実行されている必要があります。
- マシンで Windows Management Infrastructure (WMI) アクセスが有効になっている必要があります。
- 診断情報収集のスケジュールを設定するには、マシンで 互換性のあるScoutバージョン が実行されている必要があります。

パス名で指定するユーザー名にドル記号 ($) を使用しないでください。診断情報の収集が妨げられます。

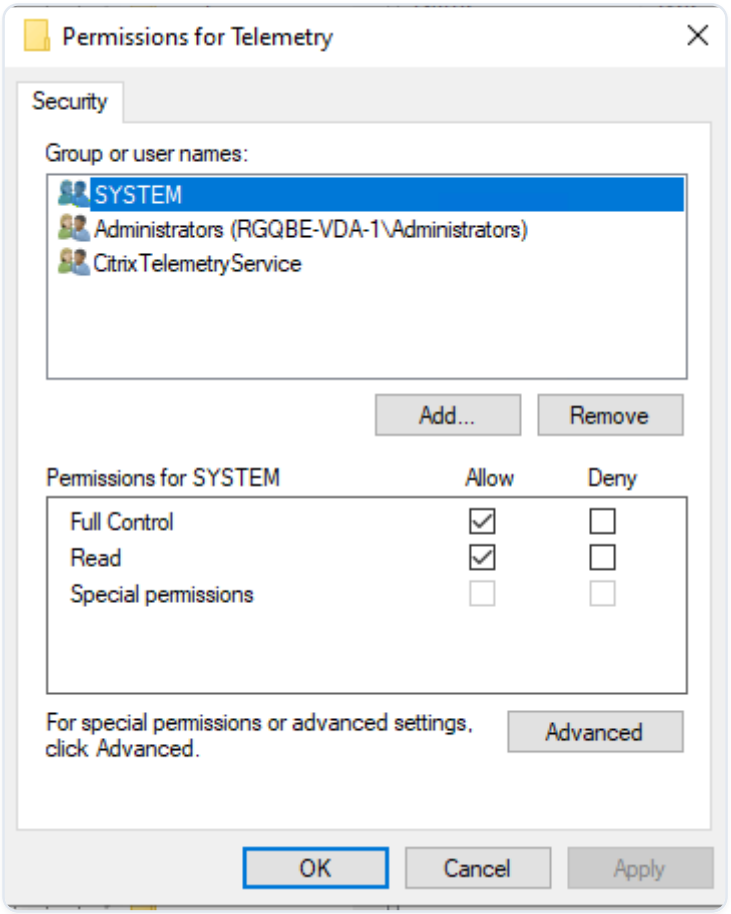
Scout は、選択したマシンで検証テストを実行し、これらの要件が満たされていることを確認します。

Windows 用 Telemetry Service は Network Service で実行されます。

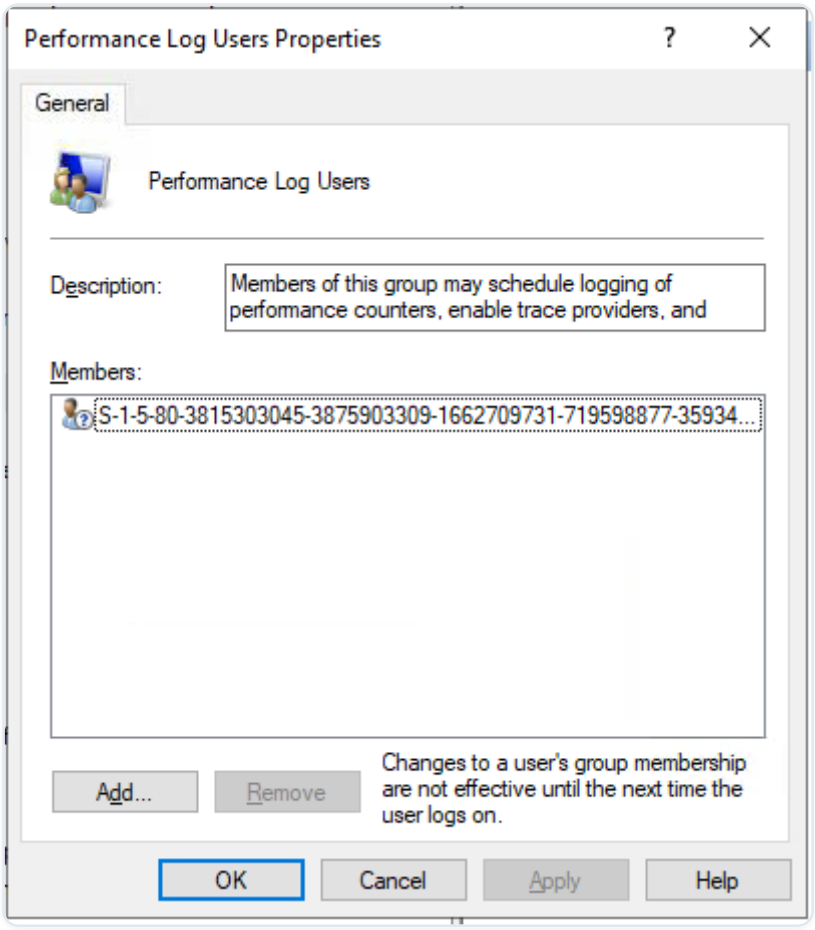


AOT トレースフォルダーは `C:\ProgramData\Citrix\TelemetryService\CitrixAOT` に保存されます。

Administratorグループ、System、およびTelemetry Service SIDのユーザーのみが、`HKEYLOCALMACHINE:SOFTWARE\Citrix\Telemetry` レジストリにアクセスする権限を持っています。



Telemetry Service SIDは、Telemetry Serviceをアンインストールした後もPerformance Log Usersグループに残りますが、手動で削除できます。



検証テスト

診断収集またはヘルスチェックが開始される前に、選択された各マシンに対して検証テストが自動的に実行されます。これらのテストは、要件が満たされていることを確認します。マシンのテストが失敗した場合、Scoutは推奨される是正措置を含むメッセージを表示します。

- **Scoutがこのマシンに到達できません** - 以下を確認してください。
  - マシンが電源オンになっていること。
  - ネットワーク接続が正常に機能していること。(これには、ファイアウォールが適切に構成されていることの確認も含まれます。)
  - ファイルとプリンターの共有がオンになっていること。手順については、Microsoftのドキュメントを参照してください。
- **PSRemotingとWinRMを有効にする** - PowerShellリモート処理とWinRMを同時に有効にできます。**管理者として実行**を使用して、`Enable-PSRemoting`コマンドレットを実行します。詳細については、コマンドレットに関するMicrosoftのヘルプを参照してください。
- **ScoutにはPowerShell 3.0 (最小) が必要です** - マシンにPowerShell 3.0 (またはそれ以降) をインストールし、PowerShellリモート処理を有効にします。

- **このマシン上のLocalAppDataディレクトリにアクセスできません** - アカウントがマシン上のLocalAppDataディレクトリに書き込む権限を持っていることを確認してください。
- **Citrix Telemetry Serviceが見つかりません** - Citrix Telemetry Serviceがマシンにインストールされ、開始されていることを確認してください。
- **スケジュールを取得できません** - マシンを(最小) XenAppおよびXenDesktop 7.14にアップグレードしてください。
- **WMIがマシンで実行されていません** - Windows Management Instrumentation (WMI) アクセスが有効になっていることを確認してください。
- **WMI接続がブロックされています** - Windows FirewallサービスでWMIを有効にしてください。
- **Citrix Telemetry Serviceの新しいバージョンが必要です** - （バージョンはCollectおよびTrace & Reproduceの場合にのみチェックされます。）マシンのTelemetry Serviceバージョンをアップグレードしてください（インストールとアップグレードを参照）。サービスをアップグレードしない場合、そのマシンは**Collect**または**Trace & Reproduce**アクションに含まれません。
- **Scoutがこのマシン上のsystemdソケットに接続できません** - 以下を確認してください。
  - ポート7503が開いていること。`systemd ctxtelemetry.socket`がマシン上のポート7503でリッスンしていることを確認してください。`ctxtelemetry.socket`ポートが変更されている場合、ポートが異なる可能性があります。ポートを調整するには、Scout構成を参照してください。
  - ネットワーク接続が正常に機能していること。（これには、ファイアウォールが適切に構成されていることの確認が含まれる場合があります。）
- **Linux VDA Telemetry Serviceがこのマシンで開始されていません** - 以下を確認してください。
  - ポート7502が開いていること。Linux VDA Telemetry Serviceがマシンにインストールされ、開始されていることを確認してください。テレメトリサービスポートが変更されている場合、ポートが異なる可能性があります。ポートを調整するには、Scout構成を参照してください。
  - ネットワーク接続が正常に機能していること。（これには、ファイアウォールが適切に構成されていることの確認が含まれる場合があります。）

バージョン互換性

このバージョンのScout (3.x) は、Citrix Virtual Apps and Desktops（または最低限XenApp and XenDesktop 7.14）のコントローラーおよびVDAで実行することを目的としています。

| 機能 | スカウト 2.23 | スカウト 3.0 | --- | --- | ---| -- | Citrix Virtual Apps and Desktops（およびXenApp and XenDesktop 7.14〜7.18）をサポート | はい | はい XenDesktop 5.x、7.1〜7.13をサポート | はい | いいえ XenApp 6.x、7.5〜7.13をサポート | はい | いいえ 製品に同梱 | 7.1〜7.13 | 7.14以降 CTX記事からダウンロード可能 | はい | いいえ CDFトレースをキャプチャ | はい | はい 常時トレース (AOT) をキャプチャ | いいえ | はい 診断データの収集を許可 | 一度に最大10台のマシン (デフォルト) | 無制限 (リソースの可用性による) 診断データをCitrixに送信することを許可 | はい | はい 診断データをローカルに保存することを許可 | はい | はい Citrix Cloud™資格情報をサポート | いいえ | はい Citrix資格情報のサポート | はい | はい アップロード用プロキシサーバーのサポート | はい | はい スケジュールを調整 | 該当なし | はい スクリプトのサポート | コマンドライン（ローカルコントローラーのみ） | Call Homeコマンドレットを使用したPowerShell（Telemetry Serviceがインストールされている任意のコンピューター） ヘルスチェック | いいえ | はい データマスキング | いいえ | 3.17以降

インストールとアップグレード

デフォルトでは、VDAまたはControllerをインストールまたはアップグレードすると、Citrix Telemetry Serviceの一部としてScoutが自動的にインストールまたはアップグレードされます。

VDAのインストール時にCitrix Telemetry Serviceを省略した場合、または後でサービスを削除した場合は、Citrix Virtual Apps and Desktopsインストールメディアの`x64\Virtual Desktop Components`または`x86\Virtual Desktop Components`フォルダーから`TelemetryServiceInstaller_xx.msi`を実行します。

Collectまたは**Trace & Reproduce**アクションを選択すると、マシンで古いバージョンのCitrix Telemetry Serviceが実行されている場合に通知されます。Citrixでは、サポートされている最新バージョンを使用することをお勧めします。そのマシンでTelemetry Serviceをアップグレードしない場合、そのマシンは**Collect**または**Trace & Reproduce**アクションに含まれません。Telemetry Serviceをアップグレードするには、インストールと同じ手順を使用します。

アップロードの承認

診断コレクションをCitrixにアップロードする予定がある場合は、CitrixアカウントまたはCitrix Cloudアカウントが必要です。（これらは、Citrixダウンロードにアクセスしたり、Citrix Cloud Control Centerにアクセスしたりするために使用する資格情報です。）アカウントの資格情報が検証されると、トークンが発行されます。

CitrixアカウントまたはCitrix Cloudアカウントで認証する場合、リンクをクリックして、デフォルトのブラウザーでHTTPSを使用してCitrix Cloudにアクセスします。Citrix Cloudの資格情報を入力すると、トークンが表示されます。トークンをコピーしてScoutに貼り付けます。その後、Scoutウィザードを続行できます。

トークンは、Scoutを実行しているマシンにローカルに保存されます。次回**Collect**または**Trace & Reproduce**を実行するときにそのトークンを使用できるようにするには、**Store token and skip this step in the future**チェックボックスをオンにします。

Scoutの開始ページで**Schedule**を選択するたびに、再承認する必要があります。スケジュールを作成または変更する際に、保存されたトークンを使用することはできません。

アップロードにプロキシを使用する

Citrixにコレクションをアップロードするためにプロキシサーバーを使用したい場合、Scoutにブラウザのインターネットプロパティで設定されたプロキシ設定を使用するように指示できます。または、プロキシサーバーのIPアドレスとポート番号を指定することもできます。

マシンの検索

収集、**トレースと再現**、**スケジュール**の手順では、Scoutは自動的に検出したコントローラーとVDAを一覧表示します。

Delivery ControllerからScout Health Checkを実行する場合、**マシンの検索**をクリックして、Delivery Controller、VDA、ライセンスサーバー、StoreFrontサーバーなどのマシンを検出します。

Delivery Controllerではないドメイン参加済みマシンからScout Health Checkを実行する場合、Scoutはマシンを自動的に検出できません。マシンを手動で追加するか、VDAマシンをインポートする必要があります。

マシンを手動で追加

Scout が検出したコントローラーと VDA を一覧表示した後、StoreFront サーバー、ライセンスサーバー、Citrix Provisioning サーバーなど、展開内の他のマシンを手動で追加できます。

ヘルスチェックの実行時：

- ドメイン内の Citrix ライセンスサーバーは自動的に検出されます。ライセンスサーバーを手動で追加することはできません。
- ヘルスチェックは現在、Citrix Provisioning サーバーをサポートしていません。

検出されたマシンを一覧表示するScoutの任意のページで、**+ マシンの追加**をクリックします。追加するマシンのFQDNを入力し、**続行**をクリックします。必要に応じて、他のマシンを追加するために繰り返します。（FQDNの代わりにDNSエイリアスを入力しても有効に見えることがありますが、ヘルスチェックが失敗する可能性があります。）

手動で追加されたマシンは、常に検出されたマシンよりも上の、マシンリストの先頭に表示されます。

手動で追加されたマシンを識別する簡単な方法は、行の右端にある赤い削除ボタンです。そのボタンがあるのは手動で追加されたマシンのみです。検出されたマシンにはありません。

手動で追加されたマシンを削除するには、行の右端にある赤いボタンをクリックします。削除を確認します。他の手動で追加されたマシンを削除するために繰り返します。

Scout は、手動で追加されたマシンを削除するまで記憶しています。Scout を閉じてから再度開くと、手動で追加されたマシンは引き続きリストの先頭に表示されます。

StoreFrontサーバーで**Trace & Reproduce**を使用している場合、CDFトレースは収集されません。ただし、その他のすべてのトレース情報は収集されます。

VDAマシンをインポートする

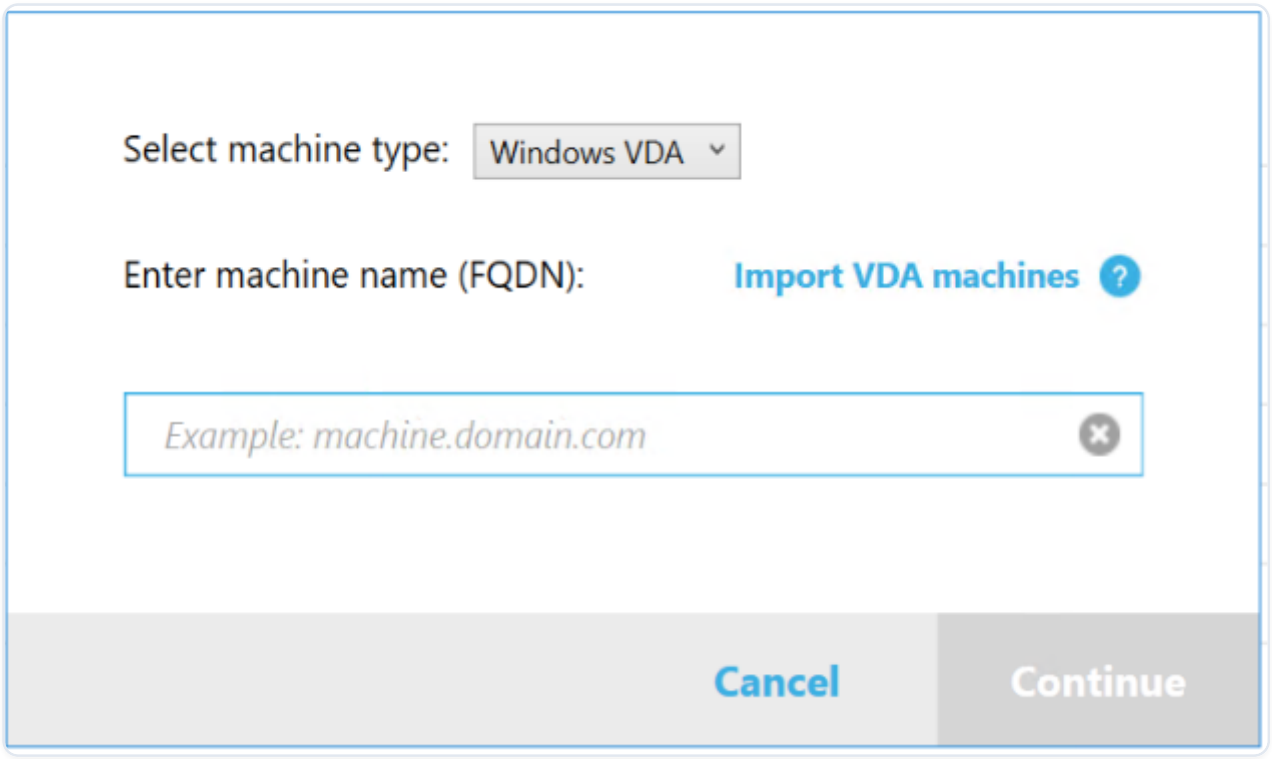
ヘルスチェックの実行時に、展開内のVDAマシンをインポートできます。

1. Delivery ControllerまたはConnectorで、PowerShellコマンドを使用してマシンリストファイルを生成します。Connectorでは、Citrixの資格情報を入力し、ポップアップダイアログで顧客を選択する必要があります。

   ```
   Get-BrokerMachine| foreach { $_.DnsName } | out-file C:\machineList.txt
   ```

2. machineList.txtファイルを、Scout Health Checkを起動するドメイン参加済みマシンにコピーします。
3. Scout Health Checkページで、**Add Machine**をクリックします。
4. **Windows VDA**マシンタイプを選択します。
5. **Import VDA machines**をクリックします。
6. machineList.txtファイルを選択します。
7. **Open**をクリックします。

インポートされたVDAマシンは、Scout Health Checkページに一覧表示されます。



診断を収集する

Collect手順には、マシンの選択、診断収集の開始、および収集を含むファイルのCitrixへのアップロードまたはローカルへの保存が含まれます。

1. Scout を起動します。マシンの メニューから、 **>** を選択します。開いたページで、 をクリックします。
2. マシンを選択します。

   - Controllerでは、**Select machines**ページに、サイト内のすべてのVDAとControllerが一覧表示されます。マシン名で表示をフィルターできます。その他のマシン（StoreFrontやCitrix Provisioningサーバーなど）を手動で追加するには、「Add machines manually」を参照してください。
   - その他のコンポーネント（VDAサーバーなど）では、**Select machines**ページにはローカルマシンのみが表示されます。マシンの手動追加はサポートされていません。

   診断情報を収集する各マシンの横にあるチェックボックスをオンにして、**Continue**をクリックします。

   Scoutは、選択した各マシンで検証テストを自動的に起動し、「Verification tests」に記載されている基準を満たしていることを確認します。検証に失敗すると、**Status**列にメッセージが表示され、そのマシンのチェックボックスはオフになります。次のいずれかを実行できます。

- 問題を解決してから、そのマシンのチェックボックスを再度オンにします。これにより、検証テストが再試行されます。
- そのマシンをスキップします（チェックボックスをオフのままにします）。そのマシンからは診断情報は収集されません。

検証テストが完了したら、**続行**をクリックします。

3. 診断情報を収集します。概要には、診断情報が収集されるすべてのマシン（選択した検証テストに合格したマシン）が一覧表示されます。**Start Collecting**をクリックします。

   収集中:

   - **Status**列には、マシンの現在の収集状態が表示されます。
   - 単一マシンでの進行中の収集を停止するには、そのマシンの**Action**列にある**Cancel**をクリックします。
   - 進行中のすべての収集を停止するには、ページの右下隅にある**Stop Collection**をクリックします。収集が完了したマシンからの診断情報は保持されます。収集を再開するには、各マシンの**Action**列にある**Retry**をクリックします。
   - 選択したすべてのマシンで収集が完了すると、右下隅にある**Stop Collection**ボタンが**Continue**に変わります。
   - 診断情報を再度収集するには、そのマシンの**アクション**列にある**Collect Again**をクリックします。新しい収集が以前のものを上書きします。
   - 収集が失敗した場合は、**アクション**列にある**Retry**をクリックできます。成功した収集のみがアップロードまたは保存されます。
   - 選択したすべてのマシンで収集が完了したら、**戻る**をクリックしないでください。(クリックすると、収集は失われます。)

   収集が完了したら、**続行**をクリックします。

4. コレクションを保存またはアップロードします。ファイルをCitrixにアップロードするか、ローカルマシンに保存するかを選択します。

   今すぐファイルをアップロードする場合は、手順5に進みます。

   ファイルをローカルに保存することを選択した場合:

   - Windowsの**保存**ダイアログボックスが表示されます。目的の場所に移動します。
   - ローカル保存が完了すると、ファイルのパス名が表示され、リンクされます。ファイルを表示できます。後でファイルをCitrixにアップロードできます。CTX136396を参照してください。

完了をクリックしてScoutの開始ページに戻ります。この手順でこれ以上ステップを完了する必要はありません。

5. アップロードの認証を行い、必要に応じてプロキシを指定します。詳細については、(#upload-authorization)を参照してください。

   - Scoutを介して認証していない場合は、この手順に進みます。
   - Scoutを介して認証済みの場合、保存されている認証トークンがデフォルトで使用されます。これを行う場合は、このオプションを選択して**続行**をクリックします。この収集の資格情報は求められません。手順6に進みます。
   - 以前に認証済みで、再認証して新しいトークンを取得したい場合は、**変更/再認証**をクリックしてこの手順に進みます。

   アップロードを認証するためにCitrix資格情報を使用するか、Citrix Cloud資格情報を使用するかを選択します。**続行**をクリックします。資格情報ページは、保存されたトークンを使用していない場合にのみ表示されます。

   資格情報ページで:

   - ファイルアップロードにプロキシサーバーを使用する場合は、**プロキシの構成**をクリックします。Scoutに、ブラウザのインターネットプロパティに設定されているプロキシ設定を使用するように指示できます。または、プロキシサーバーのIPアドレスとポート番号を入力することもできます。プロキシダイアログボックスを閉じます。
   - Citrix Cloudアカウントの場合は、**トークンを生成**をクリックします。デフォルトのブラウザがCitrix Cloudページに起動し、トークンが表示されます。トークンをコピーし、Scoutページに貼り付けます。
   - Citrixアカウントの場合は、資格情報を入力します。

   完了したら、「**続行**」をクリックします。

6. アップロードに関する情報を入力します。

   - 名前フィールドには、収集された診断ファイルのデフォルト名が含まれています。ほとんどのコレクションではこれで十分ですが、名前を変更することもできます。(デフォルト名を削除して名前フィールドを空のままにすると、デフォルト名が使用されます。)
   - 必要に応じて、8桁のCitrixサポートケース番号を指定します。
   - オプションの「**説明**」フィールドに、問題について説明し、該当する場合は問題が発生した時期を示します。

   完了したら、**アップロードを開始**をクリックします。

アップロード中、ページの左下部分にアップロードの完了パーセンテージが表示されます。進行中のアップロードをキャンセルするには、**アップロードを停止**をクリックします。

アップロードが完了すると、その場所のURLが表示され、リンクされます。リンクをたどってCitrixの場所に移動し、アップロードの分析を表示するか、リンクをコピーすることができます。

「**完了**」をクリックして、Scoutの開始ページに戻ります。

トレースと再現

「**トレースと再現**」手順は、マシンの選択、トレースの開始、問題の再現、診断コレクションの完了、そしてファイルをCitrixにアップロードするかローカルに保存することから構成されます。

この手順は、標準の**収集**手順に似ています。ただし、マシン上でトレースを開始し、それらのマシンで問題を再現することができます。すべての診断コレクションにはAOTトレース情報が含まれます。この手順では、トラブルシューティングに役立つCDFトレースを追加します。

1. Scoutを起動します。マシンの**スタート**メニューから、**Citrix > Citrix Scout**を選択します。開いたページで、**Trace & Reproduce**をクリックします。
2. マシンを選択します。**マシンの選択**ページには、サイト内のすべてのVDAとコントローラーが一覧表示されます。マシン名で表示をフィルタリングできます。トレースと診断を収集する各マシンの横にあるチェックボックスを選択します。次に、**続行**をクリックします。

   他のマシン（StoreFrontやCitrix Provisioningサーバーなど）を手動で追加するには、「マシンの手動追加」を参照してください。

   Scoutは、選択された各マシンで検証テストを自動的に起動し、「検証テスト」に記載されている基準を満たしていることを確認します。マシンの検証が失敗した場合、**ステータス**列にメッセージが表示され、そのマシンのチェックボックスは選択解除されます。次のいずれかを実行できます。

   - 問題を解決してから、そのマシンのチェックボックスを再度選択します。これにより、検証テストが再試行されます。
   - そのマシンをスキップします（チェックボックスは選択解除のままにします）。そのマシンからは診断とトレースは収集されません。

   検証テストが完了したら、**Continue** をクリックします。
3. トレースを開始します。概要には、トレースが収集されるすべてのマシンが一覧表示されます。**Start Tracing** をクリックします。

選択した1つ以上のマシンで、発生した問題を再現します。その間もトレースの収集は続行されます。問題の再現が完了したら、Scoutで**続行**をクリックします。これにより、トレースが停止します。

トレースを停止した後、トレース中に問題を再現したかどうかを示します。

4. マシンから診断情報を収集します。**Start Collecting** をクリックします。収集中に：

   - **ステータス**列には、マシンの現在の収集状態が表示されます。
   - 単一マシンでの進行中の収集を停止するには、そのマシンの**アクション**列にある**キャンセル**をクリックします。
   - 進行中のすべての収集を停止するには、ページ右下隅にある**収集の停止**をクリックします。収集が完了したマシンからの診断は保持されます。収集を再開するには、各マシンの**アクション**列にある**再試行**をクリックします。
   - すべての選択されたマシンで収集が完了すると、右下隅の**コレクションを停止**ボタンが**続行**に変わります。
   - マシンから診断を再度収集するには、そのマシンの**アクション**列にある**再収集**をクリックします。新しい収集が以前のものを上書きします。
   - 収集が失敗した場合は、**アクション**列の**再試行**をクリックできます。成功した収集のみがアップロードまたは保存されます。
   - すべての選択されたマシンで収集が完了した後、**戻る**をクリックしないでください。(クリックすると、収集は失われます。)

   収集が完了したら、**続行**をクリックします。

5. 収集を保存またはアップロードします。ファイルをCitrixにアップロードするか、ローカルに保存するかを選択します。

   今すぐファイルをアップロードすることを選択した場合は、手順6に進みます。

   ファイルをローカルに保存する場合:

   - Windowsの保存ダイアログボックスが表示されます。目的の場所を選択します。
   - ローカル保存が完了すると、ファイルのパス名が表示され、リンクされます。ファイルを表示できます。注意: ファイルは後でCitrixからアップロードできます。Citrix Insight Servicesについては、CTX136396を参照してください。

   完了をクリックしてScoutの開始ページに戻ります。この手順でこれ以上完了する必要のある手順はありません。

6. アップロードの認証を行い、必要に応じてプロキシを指定します。このプロセスの詳細については、アップロード認証を確認してください。

   - Scoutを通じて認証していない場合は、この手順に進みます。
   - Scoutを通じて認証した場合、保存されている認証トークンがデフォルトで使用されます。これを実行したい場合は、このオプションを選択して**続行**をクリックします。この収集の資格情報は求められません。手順7に進みます。
   - 以前に認証済みで、再認証して新しいトークンを取得したい場合は、**変更/再認証**をクリックしてこの手順に進みます。

   Citrix資格情報またはCitrix Cloud資格情報のどちらを使用してアップロードを認証するかを選択します。**続行**をクリックします。資格情報ページは、保存されたトークンを使用していない場合にのみ表示されます。

   資格情報ページで、次の操作を行います。

   - ファイルをアップロードするためにプロキシサーバーを使用する場合は、**プロキシの構成**をクリックします。Scoutに、ブラウザのインターネットプロパティ用に構成されたプロキシ設定を使用するように指示できます。または、プロキシサーバーのIPアドレスとポート番号を入力することもできます。プロキシダイアログボックスを閉じます。
   - Citrix Cloudアカウントの場合は、**トークンを生成**をクリックします。デフォルトのブラウザがCitrix Cloudページを起動し、トークンが表示されます。トークンをコピーし、Scoutページに貼り付けます。
   - Citrixアカウントの場合は、資格情報を入力します。

   完了したら、**続行**をクリックします。

7. アップロードに関する情報を提供します。

   アップロードの詳細を入力します。

   - 名前フィールドには、収集された診断ファイルのデフォルト名が含まれています。ほとんどの収集ではこれで十分ですが、名前を変更することもできます。（デフォルト名を削除して名前フィールドを空のままにすると、デフォルト名が使用されます。）
   - 必要に応じて、8桁のCitrixサポートケース番号を指定します。
   - オプションの「説明」フィールドに、問題について説明し、該当する場合は問題が発生した時期を示します。

   完了したら、**アップロードの開始**をクリックします。

アップロード中、ページの左下部分にアップロードの完了率が概算で表示されます。進行中のアップロードをキャンセルするには、**アップロードの停止**をクリックします。

アップロードが完了すると、その場所のURLが表示され、リンクされます。リンクをたどってCitrixの場所に移動し、アップロードの分析を表示したり、リンクをコピーしたりできます。

完了をクリックして、Scoutの開始ページに戻ります。

Scout は TraceLogging プロバイダーをサポートします

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

Citrix Virtual Apps and Desktops バージョン 2411 以降、Scout は TraceLogging プロバイダーをサポートします。このプロバイダーは追加のデコードファイルを必要とせず、同じプロバイダーに対して最大 8 つのトレースセッションからイベントを有効にして受信できます。この機能はデフォルトで有効になっています。

追加のログ収集を有効にする

追加のログ収集を有効にする機能を使用すると、トレースおよび再現機能を perfmon、Netsh、DebugView、Wireshark などのより多くのツールと組み合わせて使用できます。

2407 リリース以降、追加のログ収集を有効にすると、Scout はマシンにインストールされている CDC 関連ツールを自動的に検出し、CDC ツール関連のトレースログを zip パッケージに自動収集します。これらの zip ファイルをカスタマイズして Scout に添付できます。この自動化により、Citrix Scout をより効果的に使用でき、問題の迅速な診断に役立ちます。

> **注:**
>
> これはローカルマシンにのみ適用されます。
>
> 追加のログ収集を有効にするには、次の必要なツールがインストールされており、指定された場所にディレクトリが手動で作成されていることを確認してください。

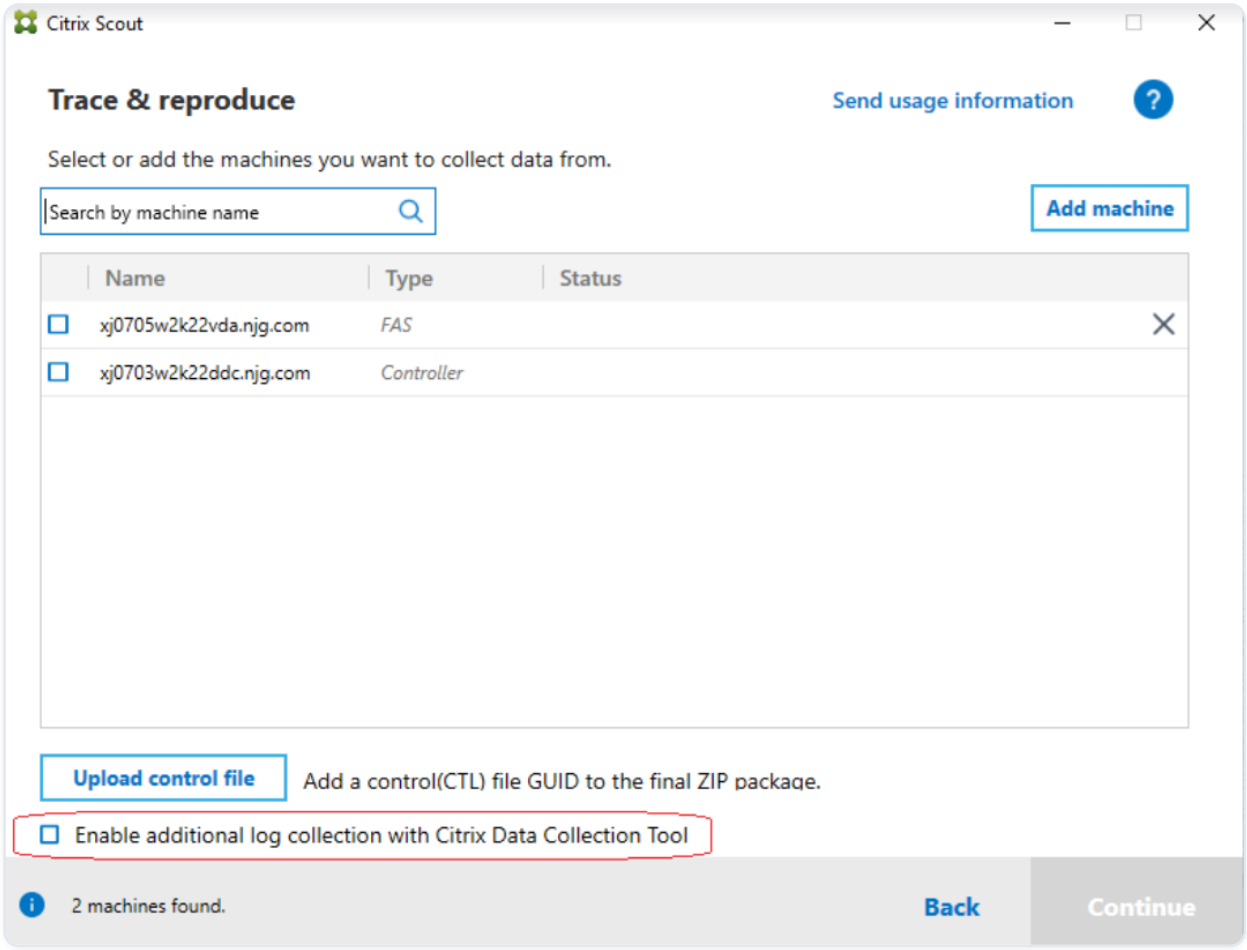
ツールのインストール場所:

- **Procdump** ログ: **Procdump** をダウンロードし、%ProgramData%\Citrix\TelemetryService\CDC\Lib\Resources\Tools\Procdump\procdump.exe に配置します

- **StoreFront** ログ: **DbgView** をダウンロードし、%ProgramData%\Citrix\TelemetryService\CDC\Lib\Resources\Tools\DebugView\Dbgview.exe に配置します
- **Procmon** ログ: **Process Monitor** をダウンロードし、%ProgramData%\Citrix\TelemetryService\CDC\Lib\Resources\Tools\ProcessMonitor\Procmon.exe に配置します
- **Wireshark** ログ: システムに **Wireshark** を手動でインストールします。

追加のログを収集するには:

1. Scoutのホームページで、**Trace & Reproduce**をクリックします。
2. データ収集元の**Select or add machines**ページで、ローカルマシンのチェックボックスをオンにします。ステータスは*Verified*と表示されている必要があります。
3. 追加のログ収集を有効にするには、**Enable additional log collection with Citrix Data Collection Tool**チェックボックスをオンにします。
4. **Upload control file**ボタンをクリックして、1つのCTLファイルをロードします。このボタンを使用すると、ScoutでのAOT収集のために、AOT収集リストに追加のGUIDを追加できます。
5. **Continue**をクリックし、Trace and Reproduceの手順に従います。
6. 完了後、zipファイル内のログを確認します。ログは*CDCLogs*フォルダーにzip圧縮されています。



注:

トレースに Procmon ツールが選択されている場合、Process Monitor のログはすぐに大きくなる可能性があります。必要なツールのみを選択するようにしてください。ログのサイズは *%temp%\Scout-CDC-Log* で監視することもできます。

コレクションのスケジュール

注:

現在、コレクションをスケジュールすることはできますが、ヘルスチェックをスケジュールすることはできません。

スケジュール手順は、マシンを選択し、スケジュールを設定またはキャンセルすることで構成されます。スケジュールされたコレクションは自動的にCitrixにアップロードされます。

> （PowerShellインターフェイスを使用して、スケジュールされたコレクションをローカルに保存できます。Citrix Call Homeを参照してください。）

1. Scoutを起動します。マシンのスタートメニューから、**Citrix > Citrix Scout**を選択します。開いたページで、**Schedule**をクリックします。
2. マシンを選択します。サイト内のすべてのVDAとコントローラーが一覧表示されます。マシン名で表示をフィルターできます。

   グラフィカルインターフェイスを使用してVDAとControllerをインストールしたときに、Call Homeスケジュールを設定した場合（Citrix Call Homeを参照）、Scoutはデフォルトでそれらの設定を表示します。このバージョンのScoutを使用して、スケジュールされたコレクションを初めて開始したり、以前に構成したスケジュールを変更したりできます。

   コンポーネントのインストール中にマシンごとにCall Homeを有効/無効にした場合でも、Scoutで構成されたスケジュールは、選択したすべてのマシンに影響します。

   診断情報を収集する各マシンの横にあるチェックボックスをオンにしてから、**［続行］**をクリックします。

   その他のマシン（StoreFrontサーバーやCitrix Provisioningサーバーなど）を手動で追加するには、「マシンの手動追加」を参照してください。

   Scoutは、選択した各マシンで検証テストを自動的に起動し、検証テストの基準を満たしていることを確認します。マシンの検証が失敗した場合、**［状態］**列にメッセージが表示され、そのマシンのチェックボックスがオフになります。次のいずれかを実行できます。

   - 問題を解決してから、そのマシンのチェックボックスを再度オンにします。これにより、検証テストが再試行されます。
   - そのマシンをスキップします（チェックボックスをオフのままにします）。そのマシンからは診断情報（またはトレース）は収集されません。

   検証テストが完了したら、**［続行］**をクリックします。

   概要ページには、スケジュールが適用されるマシンが一覧表示されます。**［続行］**をクリックします。
3. スケジュールを設定します。診断情報を収集するタイミングを指定します。注意：スケジュールは、選択したすべてのマシンに影響します。

   - 選択したマシンに週次スケジュールを構成するには、**［週次］**をクリックします。曜日を選択します。コレクションを開始する時刻（24時間形式）を入力します。

- 選択したマシンに日次スケジュールを構成するには、**［日次］**をクリックします。コレクションを開始する時刻（24時間形式）を入力します。
- 選択したマシンの既存のスケジュールをキャンセルする（別のスケジュールに置き換えない）には、**［オフ］**をクリックします。これにより、それらのマシンに対して以前に構成されたすべてのスケジュールがキャンセルされます。

［続行］をクリックします。

4. アップロードの認証を行い、必要に応じてプロキシを指定します。このプロセスの詳細については、「アップロードの承認」を参照してください。注意：Scoutスケジュールを使用する場合、保存されたトークンを使用して認証することはできません。

   アップロードの認証に Citrix 資格情報を使用するか、Citrix Cloud 資格情報を使用するかを選択します。 をクリックします。

   資格情報ページで、次の操作を行います。

   - ファイルをアップロードするためにプロキシサーバーを使用する場合は、**プロキシの構成**をクリックします。Scoutに、ブラウザーのインターネットプロパティ用に構成されたプロキシ設定を使用するように指示できます。または、プロキシサーバーのIPアドレスとポート番号を入力することもできます。プロキシダイアログボックスを閉じます。
   - Citrix Cloudアカウントの場合は、**トークンの生成**をクリックします。デフォルトのブラウザーがCitrix Cloudページに起動し、トークンが表示されます。トークンをコピーし、Scoutページに貼り付けます。
   - Citrixアカウントの場合は、資格情報を入力します。

   完了したら、 をクリックします。

   構成されたスケジュールを確認します。 をクリックして Scout の開始ページに戻ります。

   収集中、選択された各マシンのWindowsアプリケーションログには、収集とアップロードに関するエントリが含まれます。

データマスキング

Citrix Scout を使用して収集された診断情報には、セキュリティ上機密性の高い情報が含まれる場合があります。Citrix Scout のデータマスキング機能を使用すると、診断ファイルを Citrix にアップロードする前に、機密データをマスクできます。

Scout のデータマスキングは、IP アドレス、マシン名、ドメイン名、ユーザー名、ハイパーバイザー名、デリバリーグループ名、カタログ名、アプリケーション名、および SID をマスクするように構成されています。

> **注:**
>
> CDF トレースは暗号化されており、マスクできません。
>
> Linux VDA ログは `.tar.gz2` 形式に圧縮されており、マスクできません。

新しい診断を収集し、データマスキングを実行する

Citrix Scout のデータマスキング機能を使用するには、コマンドラインから Scout を起動します。

1. Windows で、コマンドプロンプトを管理者として開きます。
2. Scout がインストールされているディレクトリに移動します: `cd C:\Program Files\Citrix\Telemetry Service`。
3. Scout を起動します: `ScoutUI.exe datamasking`。
4. 診断情報を収集するには、**Collect** または **Trace & Reproduce** をクリックします。
5. 収集が完了したら、**Enable data masking** を選択します。このオプションはデフォルトで有効になっています。
6. データマスクを設定します。デフォルトのルールを使用することも、ルールをカスタマイズすることもできます。
7. 診断情報の収集をアップロードするか、保存するかを選択します。
   - **Upload the diagnostics collection to Citrix** を選択すると、マスクされた診断ファイルが Citrix にアップロードされます。
   - **Save the diagnostics collection on your local machine** を選択すると、元の診断情報とマスクされた診断情報の両方が指定された場所に保存されます。

既存の診断情報に対してデータマスキングを実行する

1. Windows で、コマンドプロンプトを管理者として開きます。
2. Scout がインストールされているディレクトリに移動します: `cd C:\Program Files\Citrix\Telemetry Service`。
3. データマスキングモードで Scout を直接起動します: `ScoutUI.exe datamasking filePath`。
4. 続行するには「Enable data masking」を選択します。このオプションはデフォルトで有効になっています。

5. データマスクを設定します。データマスキングは、デフォルトのルールで実行することも、ルールをカスタマイズすることもできます。
6. 診断コレクションをアップロードするか保存するかを選択します。

    - **診断コレクションをCitrixにアップロード**を選択した場合、マスクされた診断ファイルがCitrixにアップロードされます。
    - **診断コレクションをローカルマシンに保存**を選択した場合、元の診断とマスクされた診断の両方が指定された場所に保存されます。

マスクされたデータファイルとマッピングファイルの場所

診断コレクションをアップロードまたは保存した後、リンクをクリックして元の診断とマスクされた診断を開き、マッピング情報ファイルを開きます。

使用状況データ収集

Scoutを使用すると、CitrixはGoogle Analyticsを使用して匿名の使用状況データを収集し、将来の製品機能と改善に役立てます。データ収集はデフォルトで有効になっています。

使用状況データの収集とアップロードを変更するには、Scout UIの**設定**アイコンをクリックします。その後、**はい**または**いいえ**を選択し、**保存**をクリックして情報を送信するかどうかを選択できます。

Scout使用状況データ収集の画像(/en-us/citrix-virtual-apps-desktops/2503/media/scout-usage.png)

Scout 機能のコマンドラインインターフェイス

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

以下の機能にコマンドが追加されました。

- ヘルプ
- 診断を収集
- トレースを開始する](/ja-jp/citrix-virtual-apps-desktops/2503/manage-deployment/cis/scout#start-trace)
- トレースを停止する](/ja-jp/citrix-virtual-apps-desktops/2503/manage-deployment/cis/scout#stop-trace)

- 進行中のトレースセッションを一覧表示する](/ja-jp/citrix-virtual-apps-desktops/2503/manage-deployment/cis/scout#list-ongoing-trace-sessions)
- CDCを開始および停止する](/ja-jp/citrix-virtual-apps-desktops/2503/manage-deployment/cis/scout#start-and-stop-cdc)

> **注:**
>
> リモートトレースセッションを実行する場合、新しいテレメトリバージョンはVDAとDDCの両方にインストールされている必要があります。ScoutコマンドラインはCitrix Virtual Apps and Desktopsバージョン2411からサポートされており、`TelemetryService`の古いバージョンはこの機能をサポートしていないため、このインストールが必要です。

次の表に、新しく追加されたコマンドを示します。

ヘルプ

コマンドラインインターフェイス	説明	例
`ScoutCLI.exe -h`	コンテキストに応じたヘルプを表示します。	`ScoutCLI.exe -h` `ScoutCLI.exe -help`

診断を収集するためのコマンド

コマンドラインインターフェイス	説明	例
`ScoutCLI.exe Collect -exclude <collector>`	指定されたコレクター（Windows Management Instrumentation (WMI) プロセス、レジストリ、クラッシュレポート、ヘッダー、トレース、`msi`、`vcu`、ツールテレメトリ、ローカルデータ）からの診断を除外します。	`ScoutCLI.exe collect -exclude wmi, localdata -output "C:/Logs/mydata.zip"`
`ScoutCLI.exe Collect -output <filename>`	`.zip`をサフィックスとして出力ログファイルを保存する場所を指定します。	

コマンドラインインターフェイス	説明	例
`ScoutCLI.exe Collect -fqdn <hostname>`	サイト内の指定されたマシンで診断を収集します。	`ScoutCLI.exe collect -fqdn hostname -exclude wmi, localdata -output "C:/Logs/mydata.zip"`

トレースの開始

コマンドラインインターフェイス	説明	例
`ScoutCLI.exe StartTrace -guids <filename (xxx.ctl)>`	指定されたGUIDのターゲットモジュールのログを収集します。	ローカルマシンのトレース開始の例 - `ScoutCLI.exe StartTrace -guids C:\Logs\provider1.ctl -output C:\Logs\xxx.etl -name session1 -level 16 -max 50` ; リモートマシンのトレース開始の例 - `ScoutCLI.exe StartTrace -fqdn hostname -guids C:\Logs\provider1.ctl -output C:\Logs\xxx.etl -name session1 -level 16 -max 50`
`ScoutCLI.exe StartTrace -output <filename>`	出力ログファイルをサフィックスとして.etlで保存する場所を指定します。	
`ScoutCLI.exe StartTrace -name <session name>`	トレースセッションの名前を定義します。	
`ScoutCLI.exe StartTrace -level <value>`	ターゲットの診断詳細をログに記録するログレベルを選択します。デフォルト値は16です。	
`ScoutCLI.exe StartTrace -max <value>`	ログファイルの最大サイズをMB単位で指定します。デフォルト値は50です。	
`ScoutCLI.exe StartTrace -fqdn <hostname>`	サイト内の指定されたマシンでトレースを開始します。	

トレースの停止

コマンドラインインターフェイス	説明	例
`ScoutCLI.exe StopTrace -name <session name>`	指定されたトレースセッションを停止します。	`ScoutCLI.exe StopTrace -name session1`

コマンドラインインターフェイス	説明	例
`ScoutCLI.exe StopTrace -fqdn <hostname>`	サイト内の指定されたマシンでトレースを停止します。リモートの `.etl` がコピーされるローカルパスを割り当てるには、-o オプションが必要です。	`ScoutCLI.exe StopTrace -fqdn hostname -name session1 -output C:\Logs\xxx.etl`
`ScoutCLI.exe StopTrace -output <filename>`	出力ログファイルをサフィックス .etl で保存する場所を指定します。	

進行中のトレースセッションを一覧表示

コマンドラインインターフェイス	説明	例
`ScoutCLI.exe ListSession -name <session name>`	指定されたトレースセッションの詳細を表示します。名前が指定されていない場合は、実行中のすべてのトレースセッションの詳細を表示します。	`ScoutCLI.exe ListSession -name session1`
`ScoutCLI.exe ListSession -fqdn <hostname>`	サイト内の指定されたマシンでトレースの詳細を表示します。	`ScoutCLI.exe ListSession -fqdn hostname -name session1`

CDC の開始と停止

コマンドラインインターフェイス	説明	例
`ScoutCLI.exe StartCDC -config <filename>`	Citrix Diagnostic Collectors (CDC) ツールのパラメーターの JSON 構成ファイルを指定します。	`ScoutCLI.exe StartCDC -config xxx.json -path C:\Logs`
`ScoutCLI.exe StartCDC -path <folder>`	出力ログファイルの保存場所を指定します。	

コマンドラインインターフェイス	説明	例
`ScoutCLI.exe StopCDC`	CDC ツールの収集を停止します。	`ScoutCLI.exe StopCDC`

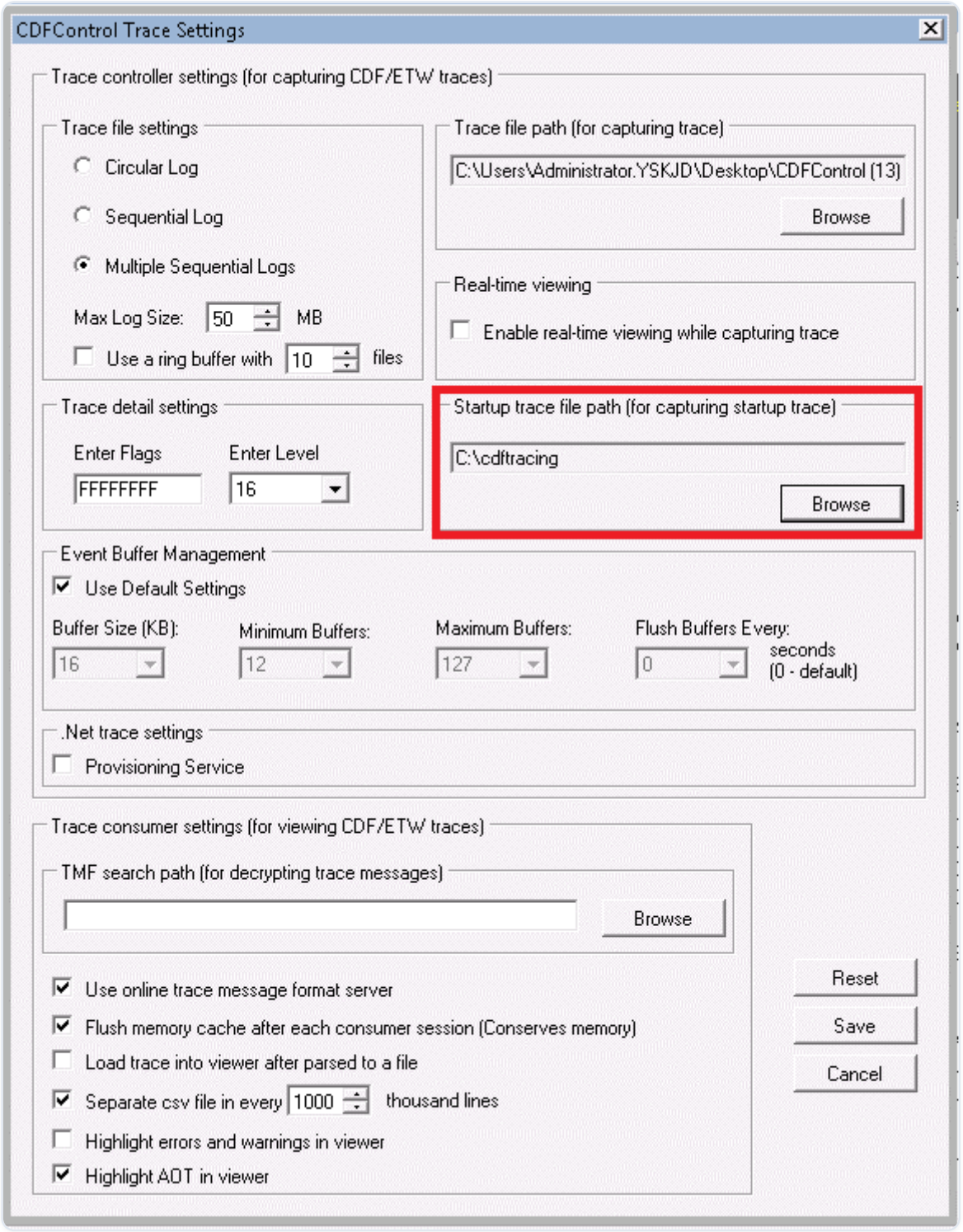
システム起動時にCitrix Diagnostic Facility (CDF) トレースを収集する

CDFControlユーティリティは、さまざまなCitrixトレースプロバイダーから表示されるCitrix Diagnostic Facility (CDF) トレースメッセージをキャプチャするためのイベントトレースコントローラーまたはコンシューマーです。これは、複雑なCitrix関連の問題のトラブルシューティング、フィルターサポートの解析、およびパフォーマンスデータの収集を目的としています。CDFControlユーティリティをダウンロードするには、CTX111961を参照してください。

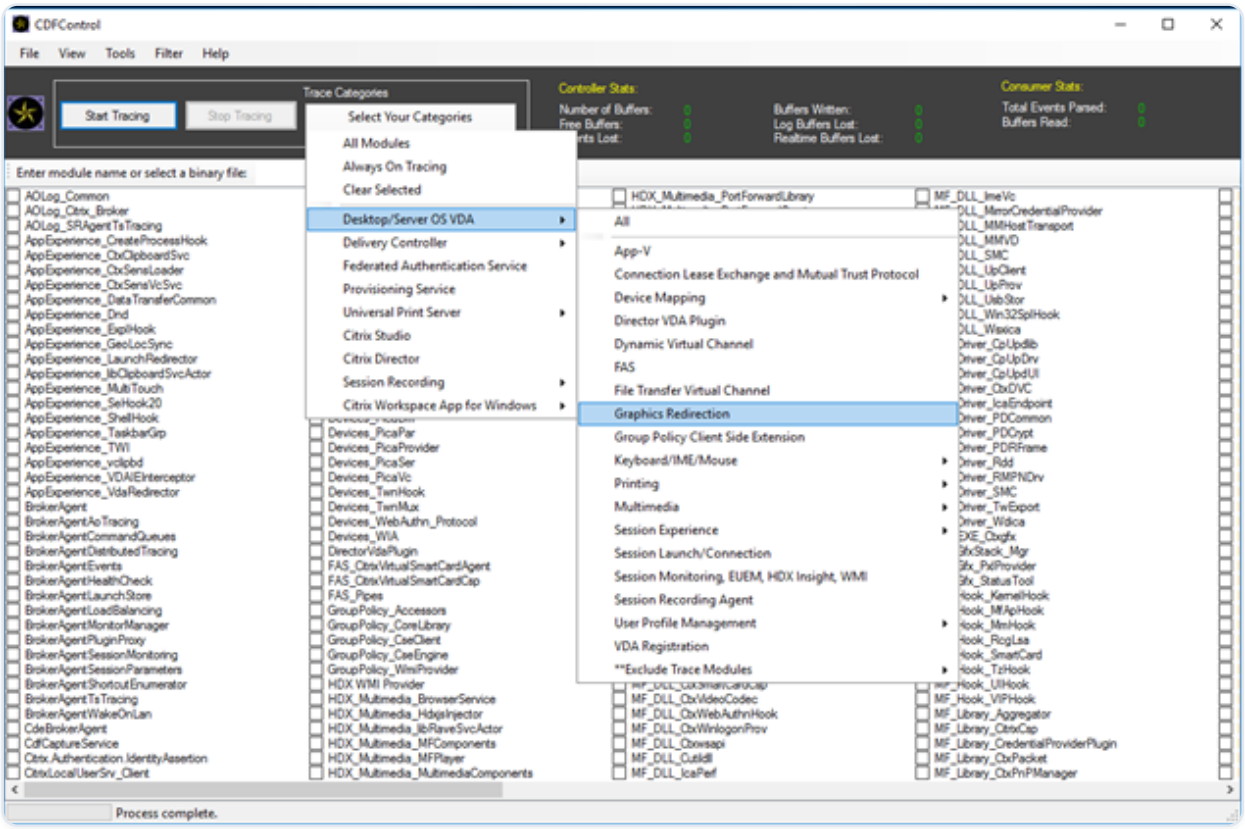
システム起動時にトレースを収集する

システム起動時にCDFトレースを収集するには、次の手順を使用します。管理者権限が必要です。

1. **CDFControl**を起動し、**ツール**メニューから**オプション**を選択します。
2. **起動トレースをキャプチャするための起動トレースファイルパス**セクションでトレースファイルパスを指定します。次に、**保存**をクリックします。



3. Citrix Support が推奨する **Trace Categories** を選択します。（次の例では、**Graphics Redirection** が選択されています。この選択は単なる例です。トラブルシューティングを行う特定の問題に対してプロバイダーを有効にすることをお勧めします。）



4. **起動トレース**を選択し、**ツール**メニューから**有効にする**を選択します。

   有効にするを選択すると、アニメーションバーがスクロールを開始します。このアクティビティは手順に影響しません。次のステップに進みます。

5. **起動トレース**が有効になったら、**CDFControlユーティリティ**を閉じ、システムを再起動します。

6. **CDFControl**ユーティリティを起動します。システムが再起動し、エラーが表示されたら、**ツール**メニューから**起動トレース**を選択し、**無効にする**をクリックして起動トレースを無効にします。

7. 手順2で指定したトレースファイルパスに移動し、分析のためにトレースログファイル（.etl）を収集します。

委任管理

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

委任管理モデルは、役割ベースおよびオブジェクトベースの制御を使用して、組織が管理アクティビティを委任する方法に合わせて柔軟性を提供します。委任管理は、あらゆる規模の展開に対応し、展開の複雑さが増すにつれて、より詳細な権限の粒度を構成できるようにします。委任管理では、管理者、役割、スコープという3つの概念を使用します。

- **管理者:** 管理者は、Active Directoryアカウントによって識別される個人またはグループを表します。各管理者は、1つ以上の役割とスコープのペアに関連付けられています。
- **役割:** 役割は職務を表し、それに関連付けられた定義済みの権限を持ちます。たとえば、デリバリーグループ管理者役割には、「デリバリーグループの作成」や「デリバリーグループからのデスクトップの削除」などの権限があります。管理者はサイトに対して複数の役割を持つことができるため、ある人物がデリバリーグループ管理者とマシンカタログ管理者の両方になることができます。役割は組み込みまたはカスタムにできます。

  組み込みの役割は次のとおりです。

役割	権限
フル管理者	すべてのタスクと操作を実行できます。フル管理者は常に「すべて」スコープと組み合わされます。
読み取り専用管理者	グローバル情報に加えて、指定されたスコープ内のすべてのオブジェクトを表示できますが、何も変更できません。たとえば、Scope=Londonの読み取り専用管理者は、すべてのグローバルオブジェクト（構成ログなど）と、ロンドンにスコープ指定されたオブジェクト（ロンドンデリバリーグループなど）を表示できます。ただし、その管理者はニューヨークスコープ内のオブジェクトを表示できません（ロンドンとニューヨークのスコープが重複しないと仮定した場合）。
ヘルプデスク管理者	デリバリーグループを表示し、それらのグループに関連付けられたセッションとマシンを管理できます。監視対象のデリバリーグループのマシンカタログとホスト情報を表示できます。また、それらのデリバリーグループ内のマシンに対してセッション管理およびマシン電源管理操作を実行できます。

役割	権限
マシンカタログ管理者	マシンカタログを作成および管理し、それらにマシンをプロビジョニングできます。仮想化インフラストラクチャ、Provisioning Services、および物理マシンからマシンカタログを構築できます。この役割は、ベースイメージの管理とソフトウェアのインストールはできますが、アプリケーションやデスクトップをユーザーに割り当てることはできません。
デリバリーグループ管理者	アプリケーション、デスクトップ、およびマシンを配信できます。関連するセッションも管理できます。ポリシーや電源管理設定など、アプリケーションとデスクトップの構成も管理できます。
ホスト管理者	ホスト接続とその関連リソース設定を管理できます。マシン、アプリケーション、またはデスクトップをユーザーに配信することはできません。

特定の製品エディションでは、組織の要件に合わせてカスタムロールを作成し、より詳細な権限を委任できます。カスタムロールを使用して、コンソール内のアクションまたはタスクの粒度で権限を割り当てることができます。

- **スコープ:** スコープはオブジェクトのコレクションを表します。スコープは、組織に関連する方法でオブジェクトをグループ化するために使用されます（たとえば、営業チームが使用するデリバリーグループのセット）。オブジェクトは複数のスコープに属することができます。オブジェクトに1つ以上のスコープがラベル付けされていると考えることができます。組み込みスコープは1つあります。「All」で、すべてのオブジェクトが含まれます。フル管理者ロールは常に**All**スコープとペアになります。

例

XYZ社は、部門（経理、営業、倉庫）とデスクトップオペレーティングシステム（Windows 7またはWindows 8）に基づいてアプリケーションとデスクトップを管理することにしました。管理者は5つのスコープを作成し、各デリバリーグループに2つのスコープをラベル付けしました。1つは使用される部門用、もう1つは使用されるオペレーティングシステム用です。

次の管理者が作成されました。

管理者	ロール	スコープ
domain/fred	フル管理者	すべて (フル管理者ロールには常にすべてのスコープがあります)
domain/rob	読み取り専用管理者	すべて
domain/heidi	読み取り専用管理者、ヘルプデスク管理者	すべての営業
domain/warehouseadmin	ヘルプデスク管理者	倉庫
domain/peter	デリバリーグループ管理者、マシンカタログ管理者	Win7

- Fredはフル管理者であり、システム内のすべてのオブジェクトを表示、編集、削除できます。
- Robはサイト内のすべてのオブジェクトを表示できますが、編集または削除はできません。
- ハイジはすべてのオブジェクトを表示でき、Salesスコープ内のデリバリーグループに対してヘルプデスクタスクを実行できます。これにより、彼女はそれらのグループに関連付けられたセッションとマシンを管理できますが、マシンの追加や削除など、デリバリーグループに変更を加えることはできません。
- warehouseadmin Active Directoryセキュリティグループのメンバーであれば誰でも、Warehouseスコープ内のマシンを表示し、ヘルプデスクタスクを実行できます。
- ピーターはWindows 7のスペシャリストであり、どの部署スコープに属しているかに関わらず、すべてのWindows 7マシンカタログを管理し、Windows 7アプリケーション、デスクトップ、およびマシンを提供できます。管理者はピーターをWin7スコープのフル管理者とすることを検討しました。しかし、フル管理者は「サイト」や「管理者」など、スコープが設定されていないすべてのオブジェクトに対しても完全な権限を持つため、この案は見送られました。

委任管理の使用方法

一般的に、管理者の数とその権限の粒度は、展開の規模と複雑さに依存します。

- 小規模な展開や概念実証の展開では、1人または少数の管理者がすべての作業を行います。委任は行われません。この場合、各管理者を、すべてのスコープを持つ組み込みのフル管理者ロールで作成します。
- より多くのマシン、アプリケーション、デスクトップを伴う大規模な展開では、より多くの委任が必要です。複数の管理者が、より具体的な機能的責任（ロール）を持つ場合があります。

たとえば、2人がフル管理者で、他の管理者がヘルプデスク管理者であるといったケースです。また、管理者はマシンカタログなど、特定のオブジェクトグループ（スコープ）のみを管理する場合もあります。この場合、新しいスコープを作成し、組み込みロールのいずれかと適切なスコープを持つ管理者を作成します。

- さらに大規模な展開では、より多くの（またはより具体的な）スコープ、および型にはまらないロールを持つ異なる管理者が必要になる場合があります。この場合、スコープを編集または追加作成し、カスタムロールを作成し、組み込みロールまたはカスタムロール、および既存のスコープと新しいスコープを持つ各管理者を作成します。

柔軟性と構成の容易さのために、管理者を作成する際にスコープを作成できます。また、マシンカタログや接続を作成または編集する際にもスコープを指定できます。

管理者の作成と管理

ローカル管理者としてサイトを作成すると、ユーザーアカウントは自動的にすべてのオブジェクトに対する完全な権限を持つFull Administratorになります。サイトが作成された後、ローカル管理者には特別な権限はありません。

The Full Administrator role always has the All scope; you cannot change this.

既定では、管理者は有効になっています。管理者を今作成しても、その人が後で管理業務を開始しない場合は、管理者を無効にする必要があるかもしれません。既存の有効な管理者については、オブジェクト/スコープを再編成している間に複数人を無効にし、更新された構成で稼働準備が整ったときに再度有効にしたい場合があります。有効なフル管理者がいなくなる場合、フル管理者を無効にすることはできません。管理者の作成、コピー、または編集時に、有効/無効チェックボックスが利用可能です。

管理者をコピー、編集、または削除する際にロール/スコープのペアを削除すると、その管理者に対するロールとスコープ間の関連付けのみが削除されます。ロールもスコープも削除されません。また、そのロール/スコープのペアで構成されている他の管理者には影響しません。

管理者を作成および管理するには、次の手順に従います。

1. Web Studio にサインインし、左ペインで をクリックし、 タブをクリックします。
2. 実行するタスクの手順に従います。

    - **管理者を作成する:** アクションバーで をクリックします。ユーザーアカウント名を入力または参照し、スコープを選択または作成してから、役割を選択します。新しい管理者はデフォルトで有効になっています。これは変更できます。

- **管理者をコピーする:** 管理者を選択し、アクションバーで をクリックします。ユーザーアカウント名を入力または参照します。役割/スコープのペアを選択して編集または削除したり、新しいペアを追加したりできます。新しい管理者はデフォルトで有効になっています。これは変更できます。
- **管理者を編集する:** 管理者を選択し、アクションバーで をクリックします。役割/スコープのペアを編集または削除したり、新しいペアを追加したりできます。
- **管理者を削除する:** 管理者を選択し、アクションバーで をクリックします。有効なフル管理者がいなくなる場合は、フル管理者を削除できません。

上部のペインには、作成した管理者が表示されます。管理者を選択すると、下部のペインにその詳細が表示されます。 列は、管理者に関連付けられている役割とスコープのペアに、使用できない役割またはスコープが含まれているかどうかを示します。関連付けられている役割とスコープのペアに、使用できない役割またはスコープが含まれている場合、次の警告メッセージが表示されます。

- 関連付けられているロールまたはスコープが使用できません

重要:

警告メッセージは、関連付けられているロールとスコープのペアに、使用できないロール、スコープ、またはその両方が含まれている場合にのみ表示されます。

管理者からロールとスコープのペアを削除するには、次のいずれかの手順を実行します。

- 役割とスコープのペアを削除します。
  a. アクションバーで をクリックします。
  b. ウィンドウで、役割とスコープのペアを選択し、 をクリックします。
  c. 「**保存**」をクリックして終了します。
- 管理者を削除します。
  a. アクションバーで、**管理者削除**をクリックします。
  b. 確認ウィンドウで、**削除**をクリックします。

役割の作成と管理

管理者がロールを作成または編集する場合、自分自身が持っている権限のみを有効にできます。これにより、管理者が現在持っている権限よりも多くの権限を持つロールを作成し、それを自分自身に割り当てたり（または既に割り当てられているロールを編集したり）することを防ぎます。

役割名には最大64個のUnicode文字を含めることができます。ただし、バックスラッシュ、スラッシュ、セミコロン、コロン、ポンド記号、コンマ、アスタリスク、疑問符、等号、左右の矢印、パイプ、左右の角括弧、左右の丸括弧、引用符、アポストロフィは含めることができません。説明には最大256個のUnicode文字を含めることができます。

組み込みロールを編集または削除することはできません。カスタムロールは、いずれかの管理者が使用している場合は削除できません。

> **注:**
>
> 特定の製品エディションのみがカスタム役割をサポートしています。カスタム役割をサポートするエディションのみが、アクションバーに関連エントリを持っています。

役割を作成および管理するには、次の手順に従います。

1. Web Studioにサインインし、左側のペインで「**管理者**」をクリックし、次に「**ロール**」タブをクリックします。
2. 完了したいタスクの手順に従います。

   - **ロールの詳細を表示する：** ロールを選択します。下部のペインに、そのロールのオブジェクトの種類と関連する権限が一覧表示されます。下部のペインで「**管理者**」タブをクリックすると、現在このロールを持つ管理者の一覧が表示されます。
   - **カスタムロールを作成する：** アクションペインで「**ロールの作成**」をクリックします。名前と説明を入力します。オブジェクトの種類と権限を選択します。
   - **役割をコピー:** 役割を選択し、アクションバーの「**役割をコピー**」をクリックします。必要に応じて、名前、説明、オブジェクトの種類、および権限を変更します。
   - **カスタム役割を編集:** 役割を選択し、アクションバーの「**役割を編集**」をクリックします。必要に応じて、名前、説明、オブジェクトの種類、および権限を変更します。
   - **カスタム役割を削除:** 役割を選択し、アクションバーの「**役割を削除**」をクリックします。プロンプトが表示されたら、削除を確定します。

スコープの作成と管理

サイトを作成すると、利用可能なスコープは「すべて」スコープのみであり、これは削除できません。

次の手順でスコープを作成できます。管理者を作成するときにもスコープを作成できます。各管理者は、少なくとも1つのロールとスコープのペアに関連付けられている必要があります。デスクトップ、マシンカタログ、アプリケーション、またはホストを作成または編集するときに、それらを既存のスコープに追加できます。スコープに追加しない場合、それらは「すべて」スコープの一部として残ります。

サイトの作成はスコープ化できず、委任された管理オブジェクト（スコープと役割）もスコープ化できません。ただし、スコープ化できないオブジェクトは「すべて」スコープに含まれます。（フル管理者は常に「すべて」スコープを持っています。）マシン、電源操作、デスクトップ、およびセッションは直接スコープ化されません。管理者は、関連するマシンカタログまたはデリバリーグループを通じて、これらのオブジェクトに対する権限を割り当てることができます。

スコープの作成と管理に関するルール:

- スコープ名には最大64個のUnicode文字を含めることができます。スコープ名には、バックスラッシュ、スラッシュ、セミコロン、コロン、ポンド記号、コンマ、アスタリスク、疑問符、等号、左矢印、右矢印、パイプ、左または右の角括弧、左または右の丸括弧、引用符、またはアポストロフィを含めることはできません。
- スコープの説明には、最大256個のUnicode文字を含めることができます。
- スコープをコピーまたは編集する際は、スコープからオブジェクトを削除すると、それらのオブジェクトが管理者からアクセスできなくなる可能性があることに注意してください。編集されたスコープが1つ以上の役割とペアになっている場合、スコープの更新によって役割/スコープのペアが使用できなくなることがないようにしてください。

スコープを作成および管理するには、次の手順に従います。

1. Web Studioにサインインし、左ペインの「**管理者**」をクリックしてから、「**スコープ**」タブをクリックします。
2. 実行したいタスクの手順に従ってください:

    - **スコープを作成:** アクションバーの「**新しいスコープを作成**」をクリックします。名前と説明を入力します。特定の種類のすべてのオブジェクト（例: Delivery Groups）を含めるには、オブジェクトの種類を選択します。特定のオブジェクトを含めるには、種類を展開してから個々のオブジェクト（例: 営業チームが使用するDelivery Groups）を選択します。

- **スコープをコピー:** スコープを選択し、アクションバーで**スコープのコピー**をクリックします。名前と説明を入力します。必要に応じて、オブジェクトの種類とオブジェクトを変更します。
- **スコープを編集:** スコープを選択し、アクションバーで**スコープの編集**をクリックします。必要に応じて、名前、説明、オブジェクトの種類、およびオブジェクトを変更します。
- **スコープを削除:** スコープを選択し、アクションバーで**スコープの削除**をクリックします。プロンプトが表示されたら、削除を確定します。

テナント管理をセットアップする

単一のCitrix Virtual Apps and Desktopsサイト内で管理パーティションを作成するために、テナント管理をセットアップします。各テナントには、マシンカタログやデリバリーグループなどの分離されたリソースと構成があります。特定のテナントへのアクセス権を持つ管理者は、そのテナントに関連付けられたリソースと構成のみを管理できます。ユースケースの例としては、単一サイト内に異なるビジネスサイロ（独立した部門または個別のIT管理チーム）を持つ企業が挙げられます。

大まかに言うと、テナント管理をセットアップするためのワークフローには以下が含まれます。

1. テナントを作成する
2. テナントの管理者を追加する

テナントを作成する

テナントスコープを作成してテナントを作成します。詳細な手順は次のとおりです。

1. Web Studioにサインインし、左ペインで**管理者**をクリックし、**スコープ**タブをクリックします。
2. *スコープの作成**をクリックして、テナントの作成を開始します。
3. テナントスコープの以下の詳細を入力します。
    a. スコープのわかりやすい名前を入力します。この名前はテナントの識別子としても機能します。
    b. （オプション）簡単な説明を入力します。
    c. **テナントスコープ**を選択します。
    d. 必要に応じて、テナントに関連付けられているオブジェクトを選択します。オブジェクトの作成時または管理時に、テナントスコープにオブジェクトを追加することもできます。
    e. 作成を完了するには、「**OK**」をクリックします。

完了後、以下を確認できます。

- 新しいテナントスコープレコードがスコープリストに表示され、「**種類**」列で「**テナント**」として識別されます。
- スコープ名は、Web Studioの右上隅にある「**すべてのテナント**」ドロップダウンリストに表示されます。

テナントスコープを操作する際は、次の考慮事項に留意してください。

- テナントプロパティは、ホスティング > マシンカタログ > デリバリーグループ > アプリケーションという階層的な割り当て順序に従います。下位レベルのオブジェクトは、上位レベルのオブジェクトからテナントプロパティを継承します。たとえば、テナントスコープのデリバリーグループを選択する場合は、関連するホスティングとマシンカタログも選択していることを確認してください。そうしないと、デリバリーグループはテナントのプロパティを継承できません。
- テナントスコープを作成した後、オブジェクトを変更することでテナントの割り当てを編集できます。テナントの割り当てが変更された場合でも、同じテナントまたはそれらのテナントのサブセットに割り当てられる必要があるという制約が適用されます。ただし、テナントの割り当てが変更されても、下位レベルのオブジェクトは再評価されません。テナントの割り当てを変更する際は、オブジェクトが適切に制限されていることを確認してください。たとえば、マシンカタログが `TenantA` と `TenantB` で利用可能な場合、 `TenantA` 用と `TenantB` 用のデリバリーグループを作成できます。(`TenantA` と `TenantB` は両方ともそのマシンカタログに関連付けられています。)その後、マシンカタログを `TenantA` のみに関連付けられるように変更できます。その結果、 `TenantB` に関連付けられているデリバリーグループは無効になります。

テナントの管理者を追加する

管理者ロールとテナントを持つユーザーアカウントを割り当てることで、テナントの管理者を追加します。

テナントの管理者を追加するには、次の手順に従います。

1. Web Studioにサインインし、左ペインで「**管理者**」をクリックし、次に「**管理者**」タブをクリックします。
2. 「**管理者を追加**」をクリックし、次の手順に従って完了します。
    a. ユーザーアカウント名を入力または参照し、「**次へ**」をクリックします。
    b. 「**カスタムアクセス**」を選択し、必要に応じて1つ以上の役割（例: マシンカタログ管理者）を選択します。

c. 各役割の横にある「**スコープの編集**」をクリックし、スコープを「**すべて**」から目的のテナントスコープに変更して、「**保存**」をクリックします。

3. 「**次へ**」をクリックします。
4. 「**確認と確定**」ページで、「**招待状を送信**」をクリックします。

レポートの作成

委任管理レポートには、次の2種類を作成できます。

- 管理者に関連付けられている役割/スコープのペアを一覧表示するHTMLレポート。各種類のオブジェクト（例: デリバリーグループやマシンカタログ）に対する個別の権限も含まれます。このレポートはWeb Studioから生成します。

  このレポートを作成するには、次の手順に従います。

  a. Web Studioにサインインし、左ペインで「**管理者**」をクリックします

  b. 管理者を選択し、アクションバーで「**レポートの作成**」をクリックします。

  このレポートは、管理者の作成、コピー、または編集時にも要求できます。

- すべての組み込み役割とカスタム役割を権限にマッピングするHTMLまたはCSVレポート。このレポートは、OutputPermissionMapping.ps1という名前のPowerShellスクリプトを実行して生成します。

  このスクリプトを実行するには、完全な管理者、読み取り専用管理者、または役割の読み取り権限を持つカスタム管理者である必要があります。スクリプトは、Program Files\Citrix\DelegatedAdmin\SnapIn\Citrix.DelegatedAdmin.Admin.V1\Scriptsにあります。

  構文：

  `OutputPermissionMapping.ps1 [-Help] [-Csv] [-Path string] [-AdminAddress string] [-Show] [CommonParameters]`

パラメーター	説明
`-Help`	スクリプトのヘルプを表示します。
`-Csv`	CSV出力を指定します。デフォルト = HTML
`-Path string`	出力の書き込み先。デフォルト = stdout

パラメーター	説明
`-AdminAddress string`	接続するDelivery Controller™のIPアドレスまたはホスト名。デフォルト = localhost
`-Show`	(`-Path` パラメーターも指定されている場合にのみ有効) 出力をファイルに書き込むと、`-Show` によって、Webブラウザーなどの適切なプログラムで出力が開かれます。
共通パラメーター	`Verbose`、`Debug`、`ErrorAction`、`ErrorVariable`、`WarningAction`、`WarningVariable`、`OutBuffer`、および `OutVariable`。詳細については、Microsoftのドキュメントを参照してください。

次の例では、HTMLテーブルをRoles.htmlという名前のファイルに書き込み、そのテーブルをWebブラウザーで開きます。

```
& "$env:ProgramFiles\Citrix\DelegatedAdmin\SnapIn\

Citrix.DelegatedAdmin.Admin.V1\Scripts\OutputPermissionMapping.ps1"

-Path Roles.html –Show
```

次の例では、CSVテーブルをRoles.csvという名前のファイルに書き込みます。テーブルは表示されません。

```
& "$env:ProgramFiles\Citrix\DelegatedAdmin\SnapIn\

Citrix.DelegatedAdmin.Admin.V1\Scripts\OutputPermissionMapping.ps1"

–CSV -Path Roles.csv
```

Windowsのコマンドプロンプトから、上記の例のコマンドは次のとおりです。

```
powershell -command "& '%ProgramFiles%\Citrix\DelegatedAdmin\SnapIn\

Citrix.DelegatedAdmin.Admin.V1\Scripts\OutputPermissionMapping.ps1'
```

```
-CSV -Path Roles.csv"
```

デリバリーコントローラー

注:

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

Delivery Controllerは、ユーザーアクセスの管理、接続の仲介と最適化を担当するサーバー側コンポーネントです。コントローラーは、デスクトップおよびサーバーイメージを作成するMachine Creation Services™も提供します。

サイトには少なくとも1つのコントローラーが必要です。最初のコントローラーをインストールした後、サイト作成時または後でコントローラーを追加できます。サイトに複数のコントローラーを配置することには、主に2つの利点があります。

- **冗長性:** ベストプラクティスとして、本番サイトでは、常に異なる物理サーバー上に少なくとも2つのコントローラーを配置してください。1つのコントローラーが故障した場合でも、他のコントローラーが接続を管理し、サイトを管理できます。
- **スケーラビリティ:** サイトのアクティビティが増加すると、コントローラーのCPU使用率とデータベースのアクティビティも増加します。追加のコントローラーにより、より多くのユーザー、アプリケーション、およびデスクトップ要求を処理できるようになり、全体的な応答性を向上させることができます。

各コントローラーはサイトデータベースと直接通信します。複数のゾーンがあるサイトでは、各ゾーンのコントローラーは、プライマリゾーンのサイトデータベースと通信します。

重要:

サイトの構成後、コントローラーのコンピューター名またはドメインメンバーシップを変更しないでください。

VDAがコントローラーに登録する方法

VDAを使用する前に、サイト内のDelivery Controllerに登録（通信を確立）する必要があります。VDA登録の詳細については、「VDA registration with Controllers」を参照してください。

コントローラーの追加、削除、または移動

コントローラーを追加、削除、または移動するには、「Databases」の記事に記載されているサーバーロールとデータベースロールの権限が必要です。

SQLクラスタリングまたはSQLミラーリングインストール内のノードにコントローラーをインストールすることはサポートされていません。

Delivery Controller™をサイトに追加する場合は、高可用性のために使用するレプリカSQL Serverに、そのマシンのログオン資格情報を追加してください。

展開でデータベースミラーリングを使用している場合:

- コントローラーを追加、削除、または移動する前に、プリンシパルデータベースとミラーデータベースの両方が実行中であることを確認してください。さらに、SQL Server Management Studioでスクリプトを使用している場合は、スクリプトを実行する前にSQLCMDモードを有効にしてください。
- コントローラーの追加、削除、または移動後にミラーリングを確認するには、PowerShell `Get-configdbconnection` コマンドレットを実行します。このコマンドレットにより、ミラーへの接続文字列にフェールオーバーパートナーが設定されていることが保証されます。

Controller を追加、削除、または移動した後:

- 自動更新が有効になっている場合、VDA は 90 分以内に更新された Controller のリストを受け取ります。
- 自動更新が有効になっていない場合は、すべての VDA で Controller ポリシー設定または ListOfDDCs レジストリキーが更新されていることを確認してください。Controller を別のサイトに移動した後、両方のサイトでポリシー設定またはレジストリキーを更新してください。

Controllerを追加する

サイトの作成時および後から Controller を追加できます。このソフトウェアの以前のバージョンでインストールされた Controller を、このバージョンで作成されたサイトに追加することはできません。

1. サポートされているオペレーティングシステムを含むサーバーでインストーラーを実行します。Delivery Controller コンポーネントと、必要なその他のコアコンポーネントをインストールします。インストールウィザードを完了します。
2. まだサイトを作成していない場合は、この Controller で Citrix Site Manager を実行してサイトを作成します。この Controller の IP アドレスは、新しいサイトに自動的に追加されます。

   データベースを初期化するスクリプトを生成する予定がある場合は、スクリプトを生成する前に Controller を追加してください。
3. すでにサイトを作成している場合は、次の手順に従います。

   a. このコントローラーでCitrix Site Manager を実行し、**既存のサイトに参加**をクリックして、参加したいサイト内のコントローラーのアドレスを入力します。

   b. Studio構成ツール を実行して、コントローラーをWeb Studioに追加します。

Controller を削除する

サイトから Controller を削除しても、Citrix ソフトウェアやその他のコンポーネントがアンインストールされるわけではありません。この操作は、Controller をデータベースから削除し、接続の仲介やその他のタスクに使用できなくするものです。Controller を削除しても、後で同じサイトまたは別のサイトに再度追加できます。サイトには少なくとも 1 つの Controller が必要であるため、Web Studio に表示されている最後の Controller を削除することはできません。

サイトから Controller を削除しても、データベースサーバーへの Controller のログオンは削除されません。これにより、同じマシン上の他の製品のサービスで使用されているログオンが誤って削除されるのを防ぎます。ログオンが不要になった場合は、手動で削除する必要があります。ログオンを削除するには、`securityadmin` サーバーロールの権限が必要です。

Controllerを削除した後：

- 自動更新を使用しているVDAは、他の利用可能なコントローラーに再登録します。この再登録は、自動更新メカニズムが有効になっており、VDAが他のコントローラー（削除されたコントローラーと同じセカンダリゾーン内、またはオンプレミス展開のプライマリゾーン内）に到達できる場合にのみ発生します。
- Citrix StoreFrontでコントローラー情報を更新します。詳細については、「コントローラーの管理」を参照してください。
- Citrix StoreFrontで、Citrix Gatewayを介したリモートアクセス用のSecure Ticket Authority (STA) URLを更新します。詳細については、「Secure Ticket Authority の管理」を参照してください。

- Citrix Gatewayで、仮想サーバーのSTA URLを更新します。詳細については、「Citrix Gateway」を参照してください。

> **重要：**
>
> サイトからControllerを削除するまで、Active DirectoryからControllerを削除しないでください。

1. Web Studioがロードされ、削除したいControllerが表示されるように、Controllerの電源がオンになっていることを確認してください。
2. Web StudioがControllerを完全にロードした後、Controller上のすべてのサービスが実行されており、Controllerの電源がオンのままであることを確認してください。
3. Web Studioにサインインし、左ペインで**設定**を選択します。
4. **Delivery Controller**タイルを見つけて、**編集**をクリックします。
5. **Delivery Controllerの管理**ページで、削除したいControllerを選択します。
6. 「**Controllerの削除**」を選択します。適切なデータベースロールと権限がない場合は、データベース管理者がControllerを削除できるようにするスクリプトを生成するオプションが提示されます。

   Web Studioは、コントローラーを削除する前に事前チェックを実行します。コントローラーの電源がオフで、以下のサービスステータスではない場合、安全に削除できます。

   - 不明
   - 障害保留中
   - 古いバージョン
   - 新しいバージョン
   - バージョン変更が進行中
   - 必須機能が不足しています

   Controller の電源がオフになっておらず、上記のいずれかのサービスステータスである場合、Web Studio は Controller の電源をオフにするよう求めます。
7. データベースサーバーから Controller のマシンアカウントを削除する必要があります。削除する前に、別サービスがそのアカウントを使用していないことを確認してください。

Web Studioを使用してControllerを削除した後、現在のタスクが適切に完了するように、そのControllerへのトラフィックが短時間残る場合があります。短時間でControllerの削除を強制したい場合は、Citrixは、Controllerがインストールされていたサーバーをシャットダウンするか、そのサーバーをActive Directoryから削除することをお勧めします。その後、サイト上の他のControllerを再起動して、削除されたControllerとの通信がこれ以上行われないようにします。

Controller を別のゾーンに移動する

サイトに複数のゾーンが含まれている場合、Controllerを別のゾーンに移動できます。この移動がVDA登録やその他の操作にどのように影響するかについては、「ゾーン」を参照してください。

1. 左ペインで「**ゾーン**」を選択します。
2. 中央ペインでゾーンを選択し、次にControllerを選択します。
3. アクションバーで**Move Items**を選択します。
4. 表示される**Move Items**ページで、Controllerを移動するゾーンを選択します。
5. **Save**をクリックします。

VDAを別のサイトに移動する

Citrix Provisioning™を使用してプロビジョニングされたVDA、または既存のイメージであるVDAは、アップグレード時、またはテストサイトで作成されたVDAイメージを本番サイトに移動する際に、別のサイト（サイト1からサイト2へ）に移動できます。Machine Creation Services (MCS)を使用してプロビジョニングされたVDAは、あるサイトから別のサイトに移動できません。MCSは、VDAがControllerに登録するためにチェックするListOfDDCsの変更をサポートしていません。MCSを使用してプロビジョニングされたVDAは、常に作成されたサイトに関連付けられているListOfDDCsをチェックします。

VDAを別のサイトに移動する方法は2つあります。インストーラーを使用するか、Citrixポリシーを使用します。

インストーラー

インストーラーを実行し、サイト2のControllerのFQDN（DNSエントリ）を指定してControllerを追加します。

インストーラーでControllerを指定するのは、Controllerポリシー設定が使用されていない場合のみです。

グループポリシーエディター

次の例では、複数のVDAをサイト間で移動します。

1. サイト1で以下の設定を含むポリシーを作成し、そのポリシーをデリバリーグループレベルにフィルターして、サイト間の段階的なVDA移行を開始します。
   - Controller: サイト2の1つ以上のControllerのFQDN（DNSエントリ）を含みます。
   - Controllerの自動更新を有効にする: 無効に設定します。
2. デリバリーグループ内の各VDAは、新しいポリシーが適用されてから90分以内に通知を受け取ります。VDAは受信したControllerのリストを無視し（自動更新が無効になっているため）、ポリシーで指定されたControllerのいずれかを選択します。このポリシーにはサイト2のControllerがリストされています。
3. VDAがサイト2のControllerに正常に登録されると、サイト2のListOfDDCsとポリシー情報を受け取ります。これらはデフォルトで自動更新が有効になっています。サイト1でVDAが登録されていたControllerは、サイト2のControllerから送信されたリストには含まれていません。そのため、VDAはサイト2のリストにあるControllerの中から選択して再登録します。それ以降、VDAはサイト2からの情報で自動的に更新されます。

Group Policy Editor の使用方法については、Citrix policies ドキュメントを参照してください。

Web Studio のホームページ

Web Studio のホームページには、Citrix Virtual Apps and Desktops™ の展開とワークロードの概要、およびサブスクリプションを最大限に活用するのに役立つ情報が表示されます。この記事では、このページで利用できるウィジェットを紹介します。

- サイトの詳細
- リソース
- セッション
- 最近
- エラーと警告
- 開始

ニーズに合わせてウィジェットを追加、削除、または再配置することで、このホームページをカスタマイズできます。

サイトの詳細

このウィジェットは、Citrix Virtual Apps and Desktopsサイトの概要を一目で確認できます。ライセンスの種類、Studioのバージョン、Delivery Controllerのバージョンとステータスなどの主要な情報が表示されます。

リソース

このウィジェットは、Citrix Virtual Apps and Desktops展開の概要を提供します。

- **リソース**。展開されているリソースの数と、カテゴリごとのカウントが表示されます。

リソース	カテゴリ別にカウントを表示するには
マシン	**マシン**をクリックし、状態を選択してから、ドーナツグラフにカーソルを合わせると詳細が表示されます。利用可能なオプション: **可用性状態** (利用可能、使用中、オフ、利用不可)、**登録状態** (登録済み、未登録)、**メンテナンス状態** (メンテナンス中、メンテナンス中ではない)。可用性状態別にマシンのカウントを表示する場合、状態をクリックすると対応するマシンの詳細を表示できます。
アプリケーション	**アプリケーション**をクリックし、ドーナツグラフにカーソルを合わせると詳細が表示されます。
デリバリーグループ	**デリバリーグループ**をクリックし、ドーナツグラフにカーソルを合わせると詳細が表示されます。
マシンカタログ	**マシンカタログ**をクリックし、ドーナツグラフにカーソルを合わせると詳細が表示されます。

- **過去7日間に起動されたセッション**。過去7日間に毎日起動されたデスクトップおよびアプリセッションの数を表示します。詳細を確認するには、Directorに移動をクリックします。

セッション

このウィジェットは、過去7日間のCitrix Virtual Apps and Desktopsワークロードの概要を提供します。過去7日間に毎日起動されたデスクトップおよびアプリセッションの数を表示します。

最近

このウィジェットは、Web Studioで最近アクセスしたオブジェクトの履歴を表示します。オブジェクトのアクセス履歴をすばやく確認するのに役立ちます。リスト内のオブジェクト名をクリックすると、そのオブジェクトがそれぞれのノード内で直接開きます。

以下に留意してください。

- リストはブラウザのキャッシュにローカルに保存されます。キャッシュをクリアしたり、ブラウザを切り替えたり、シークレットモードを使用したりすると、リストはリセットされます。
- このリストは、過去30日間にアクセスした最新の100個のオブジェクトに限定されます。
- このリストには、個々のオブジェクトの表示または操作のみが記録されます。一度に*複数*のオブジェクトを選択した場合、それらはリストに記録*されません*。
- 次のオブジェクトは追跡*されません*。
  - **設定**、**ライセンス**、および**ログ**ノード内のオブジェクト。
  - **ポリシー**ノードの**比較**タブと**モデリング**タブ内のオブジェクト。
  - **バックアップと復元**ノードの**履歴**タブと**設定**タブ内のオブジェクト。

はじめに

このウィジェットは、Citrix Virtual Apps and Desktopsの展開をセットアップするのに役立つ一連の質問に答えることで、展開を迅速に構成できます。

エラーと警告

展開からのエラーと警告を一元的に表示します。

- 以下の構成ノードに存在するエラー数と警告数を一覧表示します: ゾーン、マシン、マシンカタログ、デリバリーグループ、ホスティング、およびイメージ。数字をクリックすると、対応するノードのUIにリンクされます。
- サイト内の優先度の高いエラーを一覧表示し、推奨されるアクションも示します。

ホームページのカスタマイズ

ホームページをカスタマイズするには、次の手順に従います。

1. Web Studioにサインインします。

   ホームページが表示されます。
2. ホームページの右上隅にある**編集**アイコンをクリックします。
3. ウィジェットを再配置するには、目的の位置にドラッグします。
4. ホームページからウィジェットを削除するには、ウィジェットの右上にある**削除**アイコンをクリックします。

5. ウィジェットをホームページに再度追加するには、ホームページの右上隅にある**ウィジェットの追加**アイコンをクリックします。
6. 変更を保存するには、**完了**をクリックします。

IPv4/IPv6 のサポート

このリリースでは、純粋な IPv4、純粋な IPv6、および重複する IPv4 と IPv6 ネットワークを使用するデュアルスタック展開をサポートしています。

以下のコンポーネントはIPv4のみをサポートします。その他のすべてのコンポーネントはIPv4とIPv6をサポートします。

- XenServer®
- Virtual Delivery Agent (VDA) のうち、**Only use IPv6 Controller registration** ポリシー設定によって制御されないもの

IPv6 通信は、VDA 接続に関連する2つの Citrix® ポリシー設定によって制御されます。

- **IPv6の使用を強制する主要な設定:** Only use IPv6 Controller registration.

  このポリシー設定は、VDA が Delivery Controller に登録するために使用するアドレス形式を制御します。

  有効にすると、VDA は次の優先順位で選択された単一の IPv6 アドレスを使用して Controller と登録および通信します: グローバル IP アドレス、ユニークローカルアドレス (ULA)、リンクローカルアドレス (他の IPv6 アドレスが利用できない場合のみ)。

  無効にすると、VDA はマシンの IPv4 アドレスを使用して Controller と登録および通信します。これがデフォルト値です。

  チームが頻繁にIPv6ネットワークを使用する場合、**Only use IPv6 Controller registration** ポリシー設定が有効になっているイメージまたは組織単位 (OU) に基づいて、それらのユーザー向けにデスクトップとアプリケーションを公開します。

  チームが頻繁にIPv4ネットワークを使用する場合、**Only use IPv6 Controller registration** ポリシー設定が無効になっているイメージまたはOUに基づいて、それらのユーザー向けにデスクトップとアプリケーションを公開します。
- **IPv6ネットマスクを定義する依存設定:** Controller registration IPv6 netmask.

  マシンは複数の IPv6 アドレスを持つことができます。このポリシー設定により、管理者は、登録されている場合に、VDA をグローバル IP ではなく、優先サブネットのみに制限できま

す。この設定は、VDA が登録するネットワークを指定します。VDA は、指定されたネットマスクに一致する最初のアドレスにのみ登録します。

この設定は、**Only use IPv6 Controller registration policy** 設定が有効になっている場合にのみ有効です。デフォルト = 空の文字列

展開に関する考慮事項

環境にIPv4とIPv6の両方のネットワークが含まれている場合、IPv4専用クライアントとIPv6ネットワークにアクセスできるクライアント用に、個別のデリバリーグループ構成を作成します。ユーザーを区別するために、命名規則、手動のActive Directoryグループ割り当て、またはSmartAccessフィルターの使用を検討してください。 接続がIPv6ネットワークで開始され、その後IPv4アクセスのみを持つクライアントから再接続しようとすると、セッションの再接続が失敗する可能性があります。

注記 - DNS解決が有効になっている場合は、これらの考慮事項は適用されません。

Web Studio を使用した Citrix Virtual Apps and Desktops™ のライセンス

注記:

- License Activation Service (LAS) は、従来の Citrix® レガシーライセンスに代わる新しいクラウドベースのライセンスソリューションです。LAS はアクティベーション用の新しいモジュールを導入し、ライセンス管理へのシームレスで最新のアプローチを保証します。詳細については、License Activation Service を参照してください。
- Citrix Virtual Apps and Desktops の展開は、Web Studio (Webベース) と Citrix Studio (Windowsベース) の2つの管理コンソールを使用して管理できます。この記事では Web Studio のみを取り上げます。Citrix Studio については、Citrix Virtual Apps and Desktops 7 2212 以前の同等の記事を参照してください。

Web Studio から、ライセンスサーバーが Web Studio と同じドメイン内にあるか、信頼されたドメイン内にある場合、ライセンスを管理および追跡できます。ライセンスタスクの詳細については、ライセンスドキュメント および 複数タイプのライセンス を参照してください。

次の表に、サポートされているエディションとライセンスモデルを示します。

製品	エディション	ライセンスモデル
シトリックス バーチャル アプリ	プレミアム、アドバンスト、スタンダード	同時接続
シトリックス バーチャル デスクトップ	プレミアム、アドバンスト、スタンダード	ユーザー/デバイスおよび同時接続

詳細については、「同時使用ライセンス」および「ユーザー/デバイスライセンス」を参照してください。

サポートされているCurrent Release (CR) およびLong Term Service Release (LTSR) のバージョン

Citrixでは、機能やセキュリティの改善を享受するために、常にCitrix License Serverの最新バージョンを使用することを強くお勧めします。

> **注:**
>
> License Server VPXは非推奨となり、今後のメンテナンスやセキュリティ修正は提供されません。License Server VPXのバージョン11.16.6以前を使用しているお客様は、できるだけ早くWindows向けLicense Serverの最新バージョンに移行することをお勧めします。

> Citrix製品のライフサイクル日付の詳細については、製品マトリックスを参照してください。

レガシー製品および製品バージョンについては、「レガシー製品マトリックス」を参照してください。

以下のタスクを完了するには、完全なライセンス管理者である必要があります。Web Studioでライセンス情報を表示するには、管理者は少なくとも「ライセンスの読み取り」の委任管理権限を持っている必要があります。組み込みの「完全管理者」および「読み取り専用管理者」の役割には、その権限があります。

Web Studioを使用してCitrixからライセンスをダウンロードしてインストールする

1. Web Studioにサインインし、左ペインで**［ライセンス］**を選択します。
2. アクションバーで**［ライセンスの割り当て］**を選択します。

3. ライセンスの購入または更新後にCitrixからメールで受け取ったライセンスアクセスコードを入力します。
4. 製品を選択し、**［ライセンスの割り当て］**を選択します。その製品で利用可能なライセンスが割り当てられ、ダウンロードされます。特定のライセンスアクセスコードのすべてのライセンスを割り当ててダウンロードした後、そのライセンスアクセスコードを再利用することはできません。同じコードで他のトランザクションを行うには、My Accountにログオンしてください。

ローカルコンピューターまたはネットワークに保存されているライセンスを追加する

1. Web Studioにサインインし、左ペインで**［ライセンス］**を選択します。
2. アクションバーで**ライセンスの追加**を選択します。
3. ライセンスファイルを参照して、ライセンスサーバーに追加します。

ライセンスサーバーを変更する

1. Web Studioにサインインし、左側のペインで**ライセンス**を選択します。
2. アクションバーで**ライセンスサーバーの変更**を選択します。
3. *name:port* の形式でライセンスサーバーのアドレスを入力します。ここで、nameはDNS、NetBIOS、またはIPアドレスです。ポート番号を指定しない場合、デフォルトのポート（27000）が使用されます。

使用するライセンスの種類を選択する

- サイトを構成する際、ライセンスサーバーを指定すると、使用するライセンスの種類を選択するよう求められます。サーバーにライセンスがない場合、ライセンスなしで製品を30日間試用するオプションが自動的に選択されます。
- サーバーにライセンスがある場合、その詳細が表示され、いずれかを選択できます。または、ライセンスファイルをサーバーに追加してから、そのライセンスを選択することもできます。

製品エディションとライセンスモデルを変更する

1. Web Studioにサインインし、左側のペインで**ライセンス**を選択します。
2. アクションバーで**製品エディションの編集**を選択します。
3. 適切なオプションを更新します。

License Administration Consoleにアクセスするには、アクションバーで**［License Administration Console］**を選択します。コンソールがすぐに表示されるか、ダッシュボードがパスワードで保護されている場合は、License Administration Consoleの資格情報の入力を求められます。コンソールの使用方法の詳細については、ライセンスドキュメントを参照してください。

> **注：**
>
> Web Studioでライセンスを切り替えると、その変更がCitrix Directorに反映されるまでに最大5分かかります。たとえば、AdvancedとPremiumを切り替える場合などです。

ライセンス管理者を追加する

1. Web Studioにサインインし、左側のペインで**［ライセンス］**を選択します。
2. **［ライセンス管理者］**タブを選択します。
3. アクションバーで**［ライセンス管理者の追加］**を選択します。
4. 管理者として追加するユーザーを参照し、アクセス許可を選択します。

ライセンス管理者のアクセス許可を変更またはライセンス管理者を削除する

1. Web Studioにサインインし、左側のペインで**［ライセンス］**を選択します。
2. **［ライセンス管理者］**タブを選択し、管理者を選択します。
3. アクションバーで**ライセンス管理者編集**または**ライセンス管理者削除**のいずれかを選択します。

ライセンス管理者グループを追加する

1. Web Studioにサインインし、左ペインで**ライセンス**を選択します。
2. **ライセンス管理者**タブを選択します。
3. アクションバーで**ライセンス管理者グループの追加**を選択します。
4. ライセンス管理者として機能させたいグループを参照し、権限を選択します。Active Directoryグループを追加すると、そのグループ内のユーザーにライセンス管理者権限が付与されます。

ライセンス管理者グループの権限を変更または削除する

1. Web Studio にサインインし、左ペインで を選択します。
2. タブを選択し、管理者グループを選択します。

3. アクションバーで または のいずれかを選択します。

ライセンス情報を表示する

Web Studio にサインインし、左ペインで を選択します。サイトのライセンス使用状況と設定の概要が、指定されたライセンスサーバーに現在インストールされているすべてのライセンスのリストとともに表示されます。

製品タイプ、ライセンスエディション、ライセンスモデルを含むサイトのライセンス設定が、構成済みのライセンスサーバーが使用するライセンスと一致していることを確認してください。一致しない場合は、サイトのライセンス設定に合わせて既存のライセンスをダウンロードまたは割り当てる必要がある場合があります。

次のライセンス情報を取得するには、コマンド `Get-Brokersite` を実行します。

- TotalUniqueLicenseUsers
- PeakConcurrentLicenseUsers
- PeakConcurrentLicensedDevice

> **注:**
>
> Citrix DaaS の情報を取得するには、クラウドライセンス API を使用します。クラウドライセンス API の詳細については、「Citrix Cloud ライセンスを管理するための API」を参照してください。

ライセンス有効期限アラートを表示する

Web Studio は、Citrix License Server からライセンスファイルの有効期限を照会します。ライセンスファイルの有効期限が近づいているか、すでに期限切れになっている場合、Web Studio は概要タブで管理者にアラートを表示します。

関連リンク

- 「年間および期間ベースの小売ライセンス向けCitrixオンプレミスサブスクリプション」を参照してください(/ja-jp/licensing/current-release/license-types.html#citrix-on-premises-subscription-for-annual-and-term-based-retail-licenses)。
- 「ハイブリッド権限による移行およびアップグレード（TTU）」を参照してください(/ja-jp/licensing/current-release/hybrid-rights-ttu.html)。

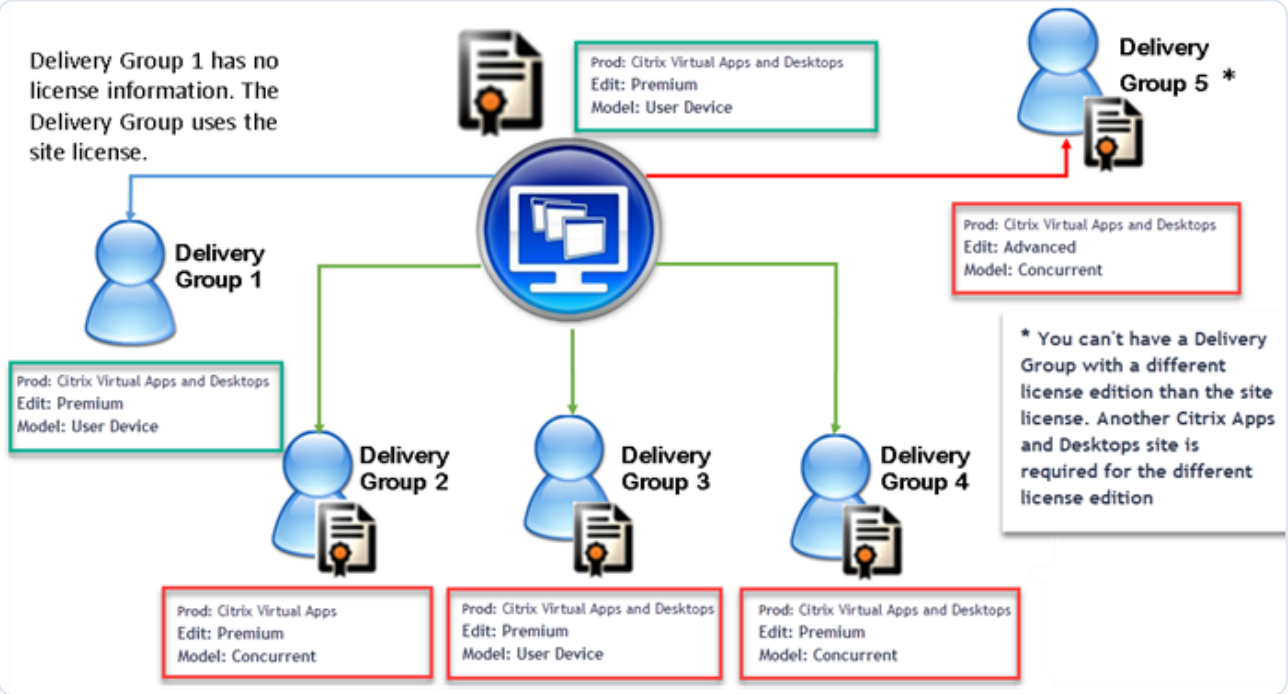
マルチタイプライセンス

注:

ライセンスアクティベーションサービスは、マルチタイプライセンスをサポートしていません。

マルチタイプライセンスは、単一のCitrix Virtual Apps and Desktopsサイト上のデリバリーグループに対して、異なるライセンスタイプの消費をサポートします。**タイプ**は、製品ID（XDTまたはMPS）とモデル（UserDeviceまたはConcurrent）の単一の組み合わせです。デリバリーグループは、サイトレベルで構成されているものと同じ製品エディション（PLT/PremiumまたはENT/Advanced）を使用する必要があります。Citrix Virtual Apps and Desktops展開でマルチタイプライセンスを構成する際は、この記事の最後にある特別な考慮事項に注意してください。

マルチタイプライセンスが構成されていない場合、異なるライセンスタイプは、個別のサイト用に構成されている場合にのみ使用できます。デリバリーグループはサイトライセンスを使用します。マルチタイプライセンスが構成されている場合の重要な通知の制限については、特別な考慮事項を参照してください。



異なる種類のライセンスを消費するデリバリーグループを特定するには、次のBroker PowerShellコマンドレットを使用します。

- New-BrokerDesktopGroup

- Set-BrokerDesktopGroup
- Get-BrokerDesktopGroup

ライセンスをインストールするには、以下を使用します。

- シトリックス スタジオ
- シトリックス ライセンシング マネージャー
- citrix.com

Customer Success Services の日付は、各ライセンスファイル、各製品、およびモデルに固有です。異なる設定のデリバリーグループは、互いに異なる Customer Success Services の日付を持つ場合があります。

特別な考慮事項

マルチタイプライセンスは、通常のCitrix Virtual Apps and Desktops™ライセンスとは異なる機能を持ちます。

サイト構成とは異なるタイプを使用するように構成されたデリバリーグループの場合、DirectorまたはStudioからのアラートや通知はありません。

- ライセンス制限に近づいている場合、またはライセンスバーストモードのトリガーや有効期限が切れた場合の情報はありません。
- 特定のグループに問題が発生した場合の通知はありません。

マルチタイプライセンス用に構成されたデリバリーグループは、そのライセンスタイプのみを消費し、完全に消費された場合でもサイト構成にフォールバックしません。

Citrix Virtual Apps StandardとCitrix Virtual Desktops™ Standardのライセンスエディション名はどちらもStandardであることを示していますが、これらは同じエディションではありません。マルチタイプライセンスは、Citrix Virtual Apps StandardおよびCitrix Virtual Desktop Standardライセンスでは利用できません。

ライセンス互換性マトリックス

この表は、古い製品名、新しい製品名、および関連する機能名を詳述しています。4つの互換性列は、マルチタイプライセンスで互換性のある製品とライセンスモデルの組み合わせを指定します。CCUとCCSは同時接続ライセンスを表し、UDはユーザー/デバイスライセンスを表します。

ライセンス互換性マトリックスと新旧の名称(/en-us/citrix-virtual-apps-desktops/2503/media/multi-type-compatibility-names.png)

ブローカー PowerShell SDK

DesktopGroup オブジェクトには、関連するNew-BrokerDesktopGroupおよびSet-BrokerDesktopGroupコマンドレットを使用して操作できる次の2つのプロパティがあります。

名前	値	制限
LicenseModel	グループのライセンスモデルを指定するパラメーター (Concurrent または UserDevice)。指定されていない場合、サイト全体のライセンスモデルが使用されます。	機能トグルが無効になっている場合、プロパティを設定しようとすると失敗します。
ProductCode	グループのライセンス製品IDを指定するXDT (Citrix Virtual Desktops用) またはMPS (Citrix Virtual Apps™用) のテキスト文字列。指定されていない場合、サイト全体の製品コードが使用されます。	機能トグルが無効になっている場合、プロパティを設定しようとすると失敗します。

LicenseModel および ProductCode の詳細については、about_Broker_Licensing を参照してください。

New-BrokerDesktopGroup

デスクトップグループのブローカリングを管理するためのデスクトップグループを作成します。このコマンドレットの詳細については、`<https://citrix.github.io/delivery-controller-sdk/Broker/New-BrokerDesktopGroup/>` を参照してください。

Set-BrokerDesktopGroup

既存のブローカーデスクトップグループを無効または有効にするか、その設定を変更します。このコマンドレットの詳細については、`<https://citrix.github.io/delivery-controller-sdk/Broker/Set-BrokerDesktopGroup/>` を参照してください。

Get-BrokerDesktopGroup

指定された条件に一致するデスクトップグループを取得します。Get-BrokerDesktopGroup コマンドレットの出力には、グループの **ProductCode** および **LicenseModel** プロパティが含まれます。New-BrokerDesktopGroup または Set-BrokerDesktopGroup を使用してプロパティが設定されていない場合、null 値が返されます。null の場合、サイト全体のライセンスモデルと製品コードが使用

されます。このコマンドレットの詳細については、`<https://citrix.github.io/delivery-controller-sdk/Broker/Get-BrokerDesktopGroup/>` を参照してください。

デリバリーグループごとに異なるライセンス製品とモデルを構成する

> **注:**
>
> 単一のデリバリーグループで、2つ以上の異なる種類の製品、エディション、またはライセンスモデルを構成することはできません。異なる種類の製品、エディション、またはライセンスモデルがある場合は、それらを個別のデリバリーグループで構成してください。

1. 管理者権限でPowerShellを開き、Citrixスナップインを追加します。 (/en-us/citrix-virtual-apps-desktops/2503/media/license-configuration-1.png)
2. コマンド **Get-BrokerDesktopGroup –Name “DeliveryGroupName”** を実行して、現在のライセンス構成を表示します。パラメーター **LicenseModel** と **ProductCode** を見つけてください。これらのパラメーターを以前に構成していない場合、空白になっている可能性があります。

   > **注:**
   >
   > デリバリーグループにライセンス情報が設定されていない場合、デフォルトで**サイトレベルのサイトライセンス**になります。

   > PowerShellコマンド(/en-us/citrix-virtual-apps-desktops/2503/media/license-configuration-2.png)

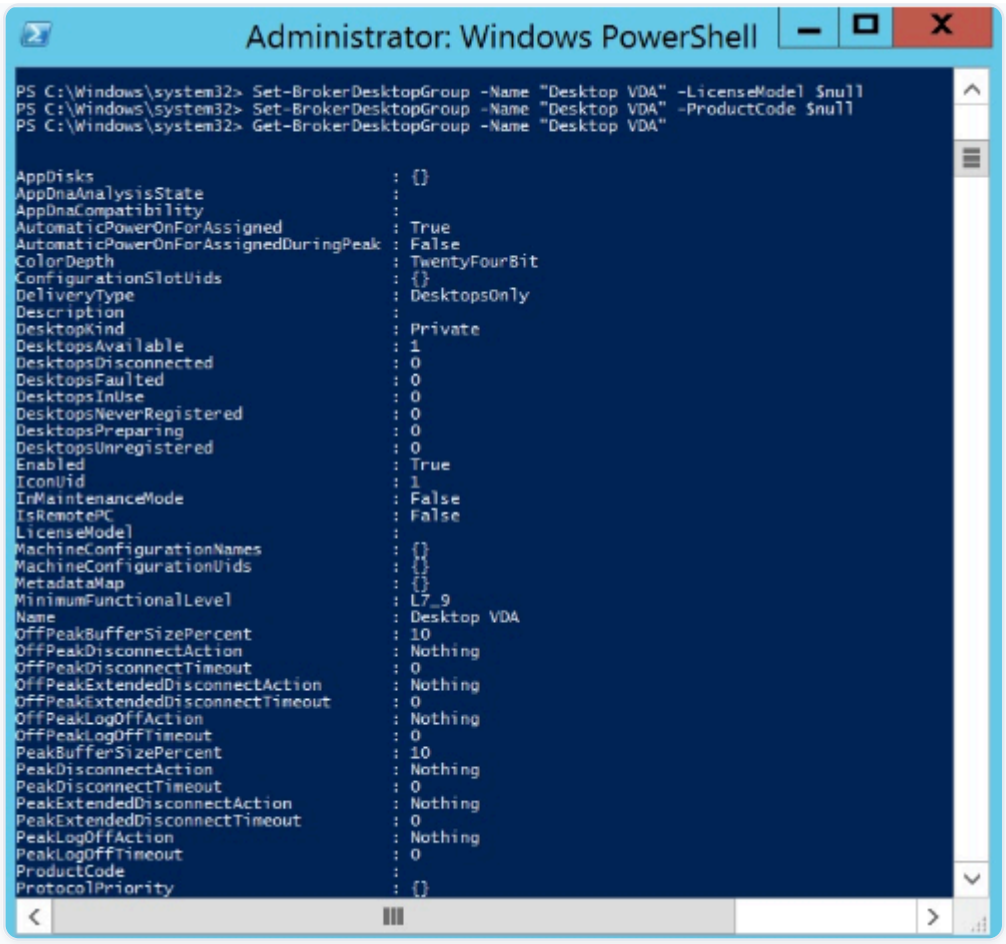
3. コマンド **Set-BrokerDesktopGroup –Name “DeliveryGroupName” –LicenseModel LicenseModel** を実行して、ライセンスモデルを変更します。 (/en-us/citrix-virtual-apps-desktops/2503/media/license-configuration-3.png)
4. コマンド **Set-BrokerDesktopGroup –Name “DeliveryGroupName” –ProductCode ProductCode** を実行して、ライセンス製品を変更します。 (/en-us/citrix-virtual-apps-desktops/2503/media/license-configuration-4.png)
5. コマンド **Get-BrokerDesktopGroup –Name “DeliveryGroupName”** を入力して、変更を検証します。

> **注:**
>
> 同じサイト内でエディションを混在させることはできません。たとえば、Premiumライセンスとライセンスなどです。異なるエディションのライセンスがある場合は、複数のサイトが必要です。

> PowerShellコマンド(/en-us/citrix-virtual-apps-desktops/2503/media/license-configuration-5.png)

6. 前の手順で説明したのと同じ **Set-BrokerDesktopGroup** コマンドを実行し、値を **$null** に設定して、ライセンス構成を削除します。

> **注:**
>
> Studioでは、各デリバリーグループのライセンス構成は表示されません。現在の構成を表示するにはPowerShellを使用してください。



例

このPowerShellコマンドレットの例は、既存の2つのデリバリーグループに対するマルチタイプライセンスの設定方法を示し、3つ目のデリバリーグループを作成して設定します。

デリバリーグループに関連付けられているライセンス製品とライセンスモデルを確認するには、**Get-BrokerDesktopGroup** PowerShellコマンドレットを使用します。

1. 最初のデリバリーグループをXenApp®およびConcurrentに設定しました。

   Set-BrokerDesktopGroup -Name "シトリックス バーチャル アプリケーションズ プレミアム コンカレント 用のデリバリーグループ" -ProductCode MPS -LicenseModel Concurrent

2. 2番目のデリバリーグループをXenDesktop®およびConcurrentに設定しました。

   Set-BrokerDesktopGroup -Name "シトリックス バーチャル デスクトップス プレミアム コンカレント 用デリバリーグループ" -ProductCode XDT -LicenseModel Concurrent

3. 3番目のデリバリーグループをXenDesktopとUserDevice用に作成および設定します。

   New-BrokerDesktopGroup -Name "Citrix Virtual Desktops Premium UserDevice 用のデリバリーグループ" -PublishedName "MyDesktop" -DesktopKind Private -ProductCode XDT -LicenseModel UserDevice

ライセンスアクティベーションサービス

ライセンスアクティベーションサービス (LAS) は、従来のCitrix®レガシーライセンスに代わる、新しいクラウドベースのライセンスソリューションです。LASは、アクティベーション用の新しいモジュールを導入し、ライセンス管理へのシームレスで最新のアプローチを保証します。

LASは、Citrixライセンスのエクスペリエンスを簡素化します。ライセンスサーバーで生成、ダウンロード、またはインストールするライセンスアクセスコードやファイルは不要になりました。ライセンスサーバーをアップグレードし、Citrix Cloudに登録するだけです。互換性のある製品がライセンスサーバーを指すように設定されると、自動的にアクティベートされます。

アクティベーション後、ライセンスサーバーはライセンスアクティベーションサービスと定期的に通信し、アクティベーションを最新の状態に保ちます。LASはクラウドテクノロジーで構築されており、パフォーマンスを向上させ、ダウンタイムがないことを保証します。何らかの理由でライセンスサーバーまたはLASに到達できない場合、システムはライセンスキャッシュモードに入ります。これは、システムがライセンスなしの状態になるのを防ぎ、停止を回避するように設計されています。詳細については、「ライセンスキャッシュモード」を参照してください。

LASの詳細については、ライセンスドキュメントの「ライセンスアクティベーションサービス」を参照してください。

前提条件

- ライセンスサーバーをバージョン11.17.2ビルド51000以降にインストールまたは更新します。
- ライセンスサーバー用の信頼性の高い継続的なインターネット接続。

考慮事項

- Web StudioがアクティベーションをIに、すべてのDelivery ControllerがLASと互換性がある必要があります。1つのサイトでレガシーライセンスまたはLASのいずれかを使用できます。
- 同じCitrix Cloud ID (CCID) またはOrgIDに複数のライセンスサーバーを登録できます。ただし、サイトは1つのライセンスサーバーのみを指すように構成できます。

制限事項

- LASへの移行により、製品エディションは**Premium**に、ライセンスモデルは**Concurrent**に設定されますが、これは将来変更される可能性があります。PowerShellを使用してライセンス構成を変更しないでください。登録とセッション起動に影響を与える可能性があるためです。
- 既存のレガシーライセンスからLASへのCitrix Virtual Apps and Desktops™サイトの移行は、Web Studioのみを使用して実行できます。

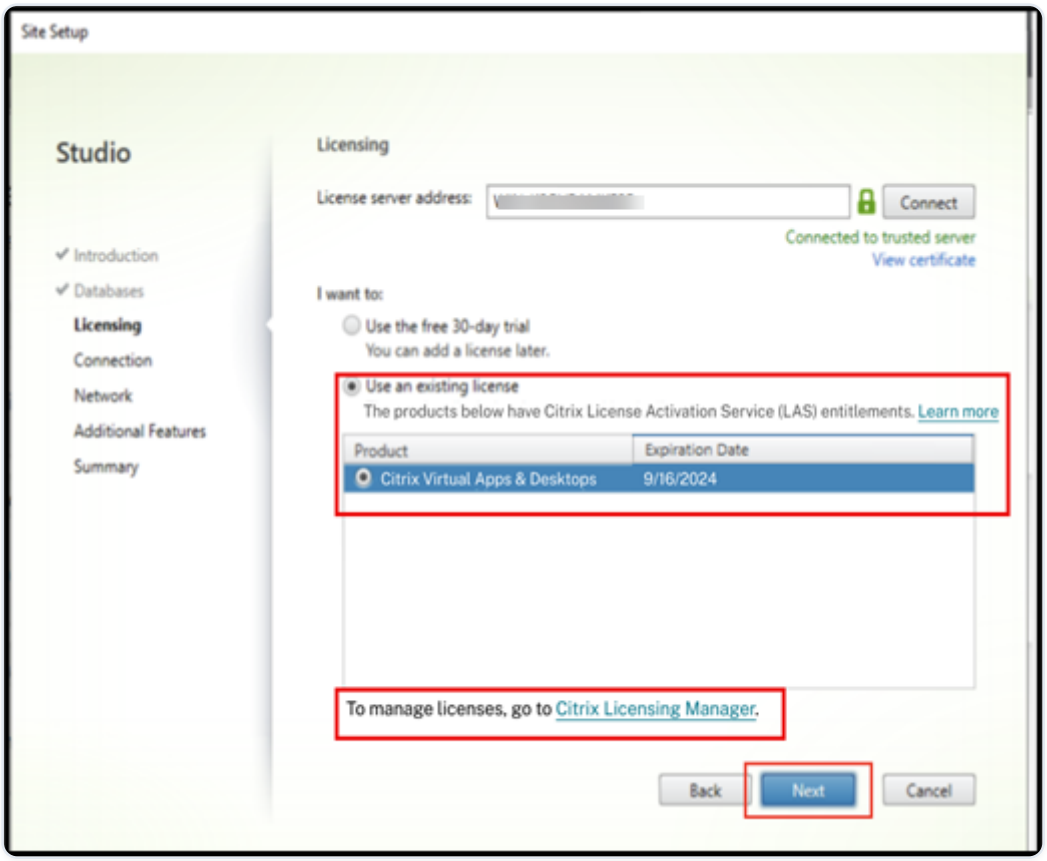
主な手順

1. License Server をバージョン 11.17.2 ビルド 51000 以降にインストールまたはアップグレードし、(/ja-jp/licensing/current-release/license-activation-service#how-to-configure-license-server-for-license-activation-service) に記載されている手順に従って LAS を構成します。
2. Citrix Virtual Apps and Desktops バージョン 2411 以降をインストールします。Citrix Delivery Controller、Citrix Studio、Web Studio、Citrix Director などのコアコンポーネントをインストールします。

   > **注:**
   >
   > Citrix Virtual Apps and Desktopsサイト内のすべてのDelivery Controllerは、LASと互換性がある必要があります。

3. 必要なコンポーネントをインストールしたら、Citrix Site Manager を使用してサイトを作成します。サイトの作成については、(/ja-jp/citrix-virtual-apps-desktops/2503/install-configure/site-create) を参照してください。License Server が LAS を使用するように構成されている場合、

Metainstaller はエンタイトルメントを表示します。エンタイトルメントは、対応するライセンス有効期限とともに提供されます。



注:

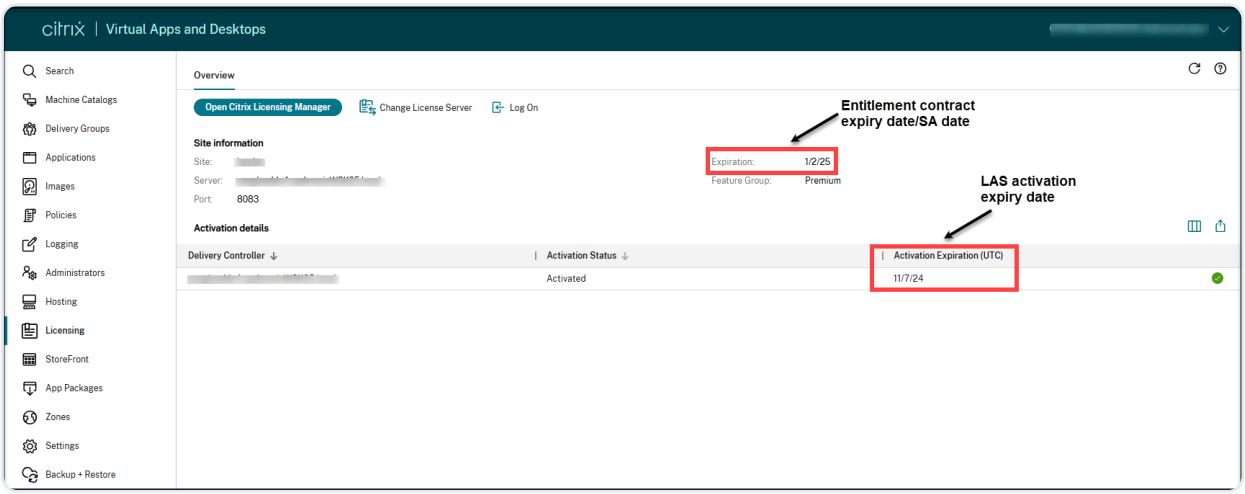
License Serverが最新のLicense Serverバージョンにアップグレードされていない場合、エラーメッセージが表示されます。

4. ライセンスの詳細を確認する。
5. レガシーライセンスをLASに移行する。

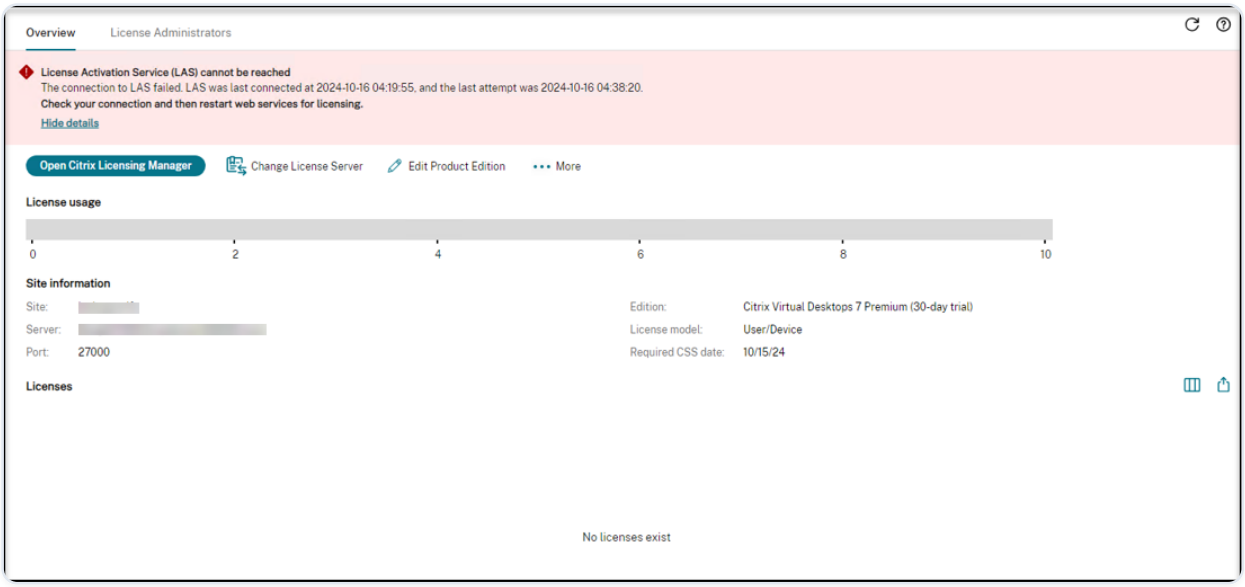
ライセンスの詳細を確認する

サイトを作成したら、Web Studio を使用してライセンスの詳細を確認します。

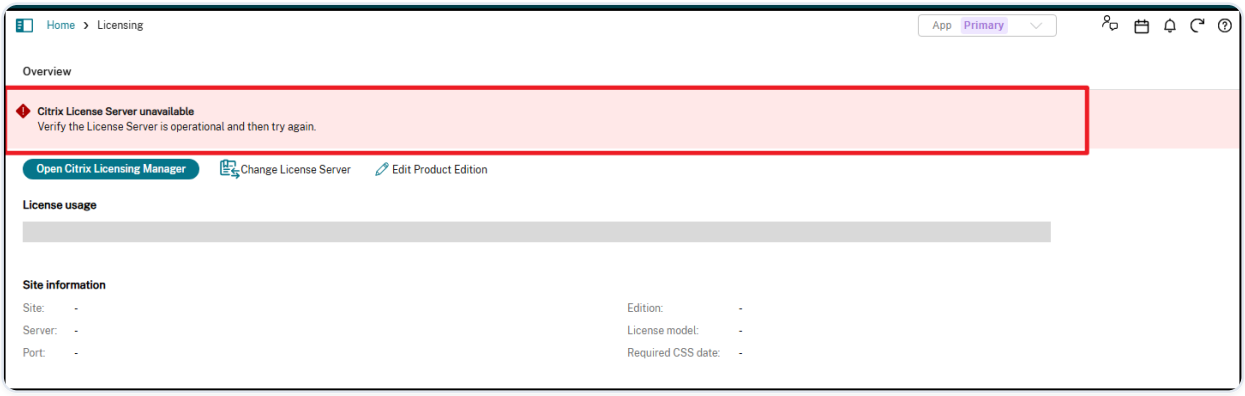
1. Web Studio で、 ノードを選択します。
2. タブで、Citrix Virtual Apps and Desktops サイトに適切なライセンスがあるか、または LAS 機能の使用中にライセンスの有効期限が切れていないかを確認します。



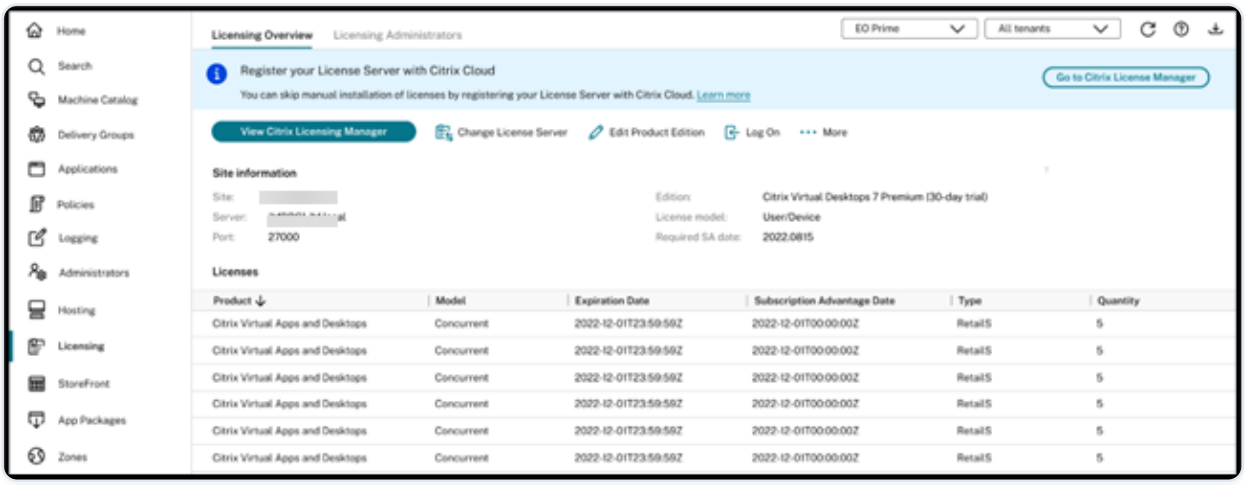
LASに到達できない場合、エラーメッセージが表示されることがあります。



ライセンスサーバーが利用できない場合、エラーメッセージが表示されることがあります。



お使いのライセンスサーバーが古いレガシーライセンスをまだ使用しており、Citrix Virtual Apps and DesktopsサイトがLAS対応である場合、Web StudioはCitrix Cloudにライセンスサーバーを登録するよう促します。



レガシーライセンスをLASに移行する

Citrix Cloudにライセンスサーバーをすでに登録しており、必要なエンタイトルメントがある場合、ユーザーセッションに影響を与えることなく、既存のCitrix Virtual Apps and Desktopsサイトをレガシーライセンスから LASに移行するには、以下の特定の順序に従う必要があります。

1. **ライセンスサーバーのアップグレード:** ライセンスサーバーをサポートされている最小バージョンにアップグレードします。
2. **Delivery Controllerのアップグレード:** サイト内のすべてのDelivery ControllerをLAS対応バージョンにアップグレードします。
3. **デリバリーグループのライセンス割り当てを削除:**
   - **Migrate to LAS**をクリックする前に、サイトレベルより下に設定されているライセンス割り当てを手動で削除します (つまり、デリバリーグループレベルのライセンス割り当てを削除します)。
4. **割り当ての確認:** LASの割り当てが正確であることを確認します。
5. **Migrate to LASをクリックする:**
   - 前の手順が完了したら、**LASに移行**をクリックします。

     レガシーライセンスからLASに移行する(/en-us/citrix-virtual-apps-desktops/2503/media/migrate-to-las.png)
   - LASに移行すると、Citrix Virtual Apps and Desktopsサイトの**ライセンスエディション**は**Citrix Virtual Apps and Desktops Premium**に設定され、**ライセンスモデル**は**同時使用**に構成されます。

LASからレガシーライセンスへのロールバック

LASからレガシーライセンスにロールバックするには、次の手順を実行します。

1. 次のPowerShellコマンドを実行します。

```
Set-ConfigSite -UseLicenseActivationService $false
```

2. Web Studioでレガシーライセンスを構成します。

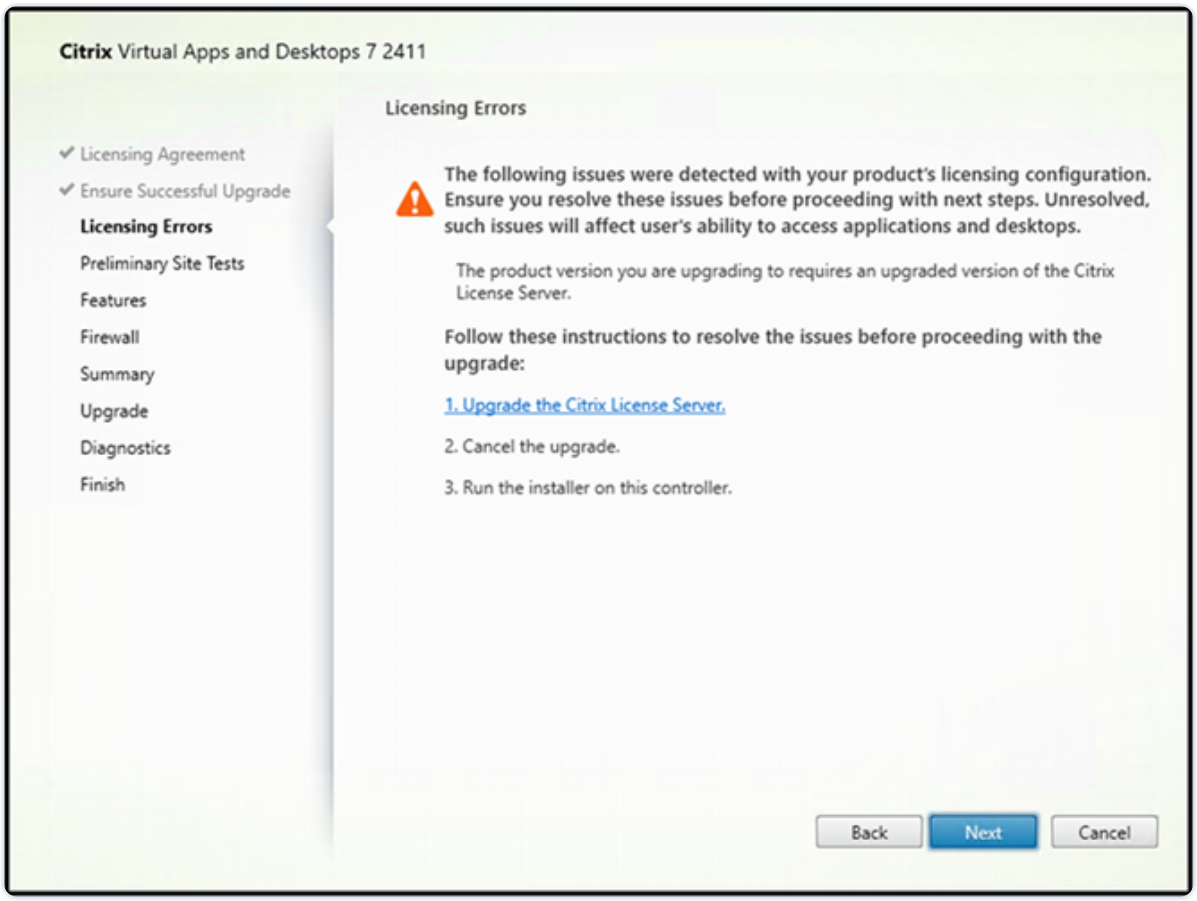
注:

これらの手順は、一時的なトラブルシューティングのみを目的としています。レガシーライセンスファイルはサポート終了（EOL）に近づいており、April 15, 2026以降は機能しません。中断のないサービスを確保するため、License Activation Service (LAS) への移行をお勧めします。詳細については、お知らせを参照してください。

アップグレードに関する重要な考慮事項

以前のCitrix Virtual Apps and Desktopsバージョンから2411以降にアップグレードする場合は、ライセンスサーバーを最新バージョン（バージョン11.2.17ビルド51000以降）にアップグレードしてください。

- メタインストーラーUIを使用してアップグレードする際に、ライセンスエラーページに次のエラーが表示されます。
    - 最新のライセンスサーバーバージョンにアップグレードしない場合：



  - ライセンスサーバーのバージョンが古い、またはライセンスが利用できないなど、互換性の問題がある場合：

    古いライセンスサーバーまたはライセンスの利用不可(/en-us/citrix-virtual-apps-desktops/2503/media/outdated-license-server-error.png)

- コマンドラインを使用してアップグレードする場合は、アップグレードの失敗を避けるために次のコマンドを実行します（マウントされたISOの\x64フォルダー内にいると仮定します）。

1. 次を実行します：

   ```
   \x64\Licensing\CitrixLicensing.exe /quiet
   ```

   ライセンスバイナリをローカルドライブのいずれかにコピーしている場合、次のコマンドを実行します：

   ```
   \x64\Licensing\CitrixLicensing.exe /quiet /l install.log
   ```

2. 次を実行します：

```
\x64\XenDesktop Setup\XenDesktopServerSetup.exe  /components
"CONTROLLER,DESKTOPSTUDIO,DESKTOPDIRECTOR" /CONFIGURE_FIREWALL
```

コアコンポーネントのアンインストール

アップグレード中に、`\x64\Licensing\CitrixLicensing.exe /quiet`または`\x64\Licensing\CitrixLicensing.exe /quiet /l install.log`コマンドを使用して最初にライセンスサーバーをインストールし、次にコアコンポーネントをインストールした場合は、アンインストールも同じ順序で行ってください。

1. コマンドラインを使用してライセンスサーバーをアンインストールします。

```
CitrixLicensing.exe /quiet /uninstall /l uninstall.log
```

2. GUIまたはコマンドラインを使用してコンポーネントをアンインストールします。詳しくは、「コンポーネントの削除」を参照してください。

コマンドライン`XenDesktopServerSetup.exe`または`removeall`を使用してライセンスサーバーとコンポーネントをアンインストールする場合は、レジストリエントリと残りのファイルをクリーンアップします。

レジストリエントリをクリーンアップするには：

1. レジストリキー`Citrix Licensing`を検索し、そのエントリを削除します。ほとんどの場合、エントリは次の場所にあります。

```
"Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\Cur
rentVersion\Uninstall\
```

2. レジストリキーの**Uninstall String**が指すフォルダーを削除します。

トラブルシューティング

Citrix Cloudでライセンスサーバーのステータスが緑色以外で表示されている場合は、問題が発生している可能性のあるアクティベーションの詳細を把握するために、次の手順を実行します。

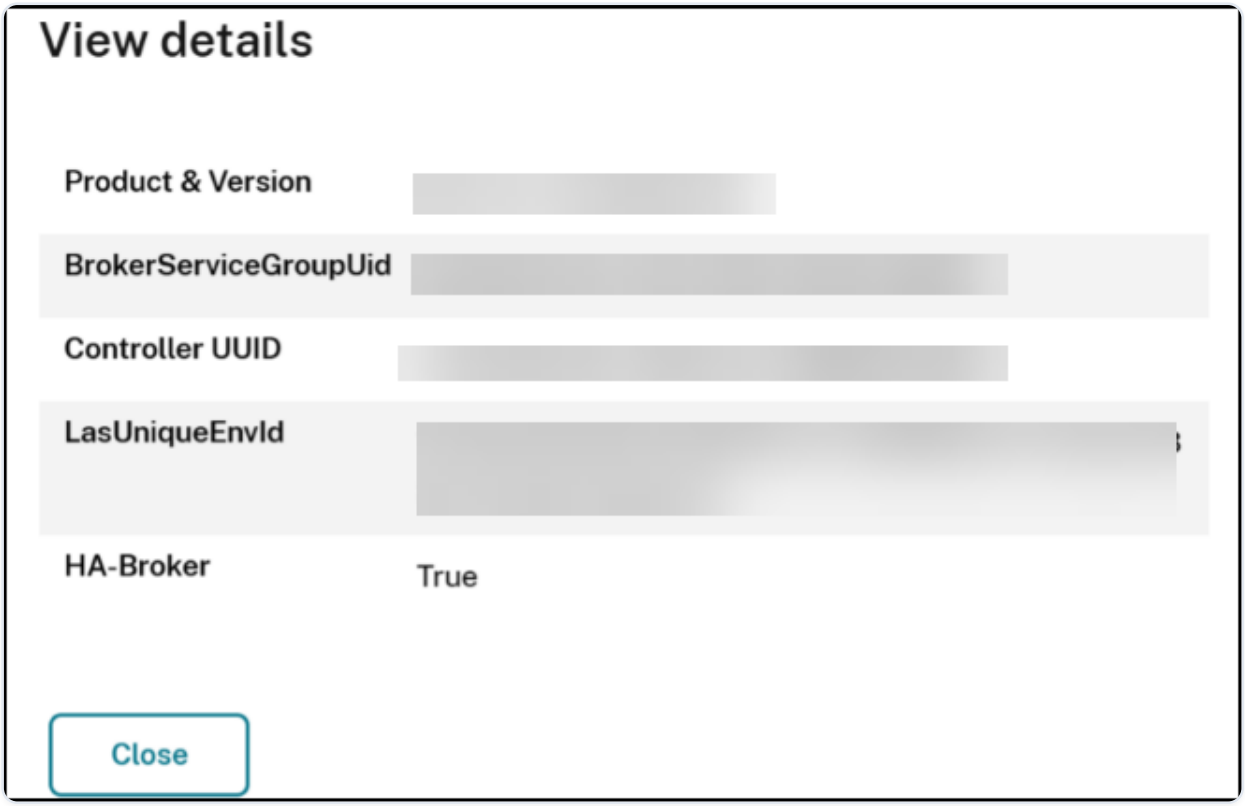
1. Citrix Cloud で、**ライセンス > ライセンス済み展開 > ライセンスサーバー** に移動します。
2. Citrix Virtual Apps and Desktops の横にある展開ボタン **>** をクリックして、アクティブ化された Delivery Controller のリストを表示します。

アクティブ化された Delivery Controller の cvad リスト(/en-us/citrix-virtual-apps-desktops/2503/media/las-product-activation1.png)

3. アクティベーションの横にある **詳細の表示** をクリックして、詳細な情報を表示します。

   IDは、アクティベーションを識別するための一意の識別子です。

   次の詳細が提供されます。



   - **製品とバージョン**: LAS でアクティブ化する際に製品が使用するように構成されている Product_Edition_Model と Burn In Date。BurnInDate は通常、製品のリリース日です。
   - **BrokerServiceGroupUid**: ブローカーサービスグループの UID。
   - **コントローラー UUID**: デリバリーコントローラーの UUID。
   - **LasUniqueEnvId**: アクティベーションのために LAS によって提供されるインスタンスの一意の ID。
   - **HA-Broker**: HA ブローカーかメインブローカーかを示す True または False。

アクティブ化されたホストの詳細を実際のホストにマッピングするには、ホストで次のコマンドを実行します。

- `Get-BrokerSite`: 画面に表示される **BrokerServiceGroupUid** の値を、コマンドの `BrokerServiceGroupId` 出力と比較します。

- `Get-BrokerController`: 画面に表示される **Controller UUID** の値を、コマンドの UUID 出力と比較します。

ライセンスイベントに関連するイベントビューアーログ

イベントID	説明
1112	Citrix Broker Service は、ユーザーからリソースへの接続を仲介できませんでした。このサイトの製品およびエディションのライセンス構成では、このタイプのリソースは許可されていません。このサイトに正しいライセンスが選択されていることを確認してください。
1150	Citrix Broker Service はライセンスサーバーへの接続に成功しました。
1151	Citrix Broker Service はライセンスサーバーに接続できません。ライセンスサーバーが正しく機能していること、およびライセンスサーバーを識別する詳細がXenDesktop構成で正しいことを確認してください。
1152	このXenDesktopサイトには、ライセンスサーバーに必要な製品ライセンスがありません。ライセンス管理コンソールを使用して、関連する製品ライセンスをライセンスサーバーに追加してください。
1153	このXenDesktopサイトのライセンスの有効期限が切れました。Citrix Brokerサービスは、ライセンスサーバーから新しいライセンスを要求します。
1154	このコントローラーは、ライセンスサーバーに接続できなかったため、ライセンスキャッシュモードに入りました。このコントローラーがデスクトップおよびアプリケーションセッションの提供を停止するまで、残り2時間です。
1155	Citrix Broker Service は、デスクトップおよびアプリケーションセッションの提供を停止します。このコントローラーは、ライセンスサー

イベントID	説明
	バーとの通信が継続的に失敗したため、ライセンスキャッシュモードになっていないか、ライセンスキャッシュモードに入ることができませんでした。ライセンスサーバーが機能していることを確認し、必要に応じて、License Administration Console を使用して関連するライセンスをライセンスサーバーに追加してください。
1156	Citrix Broker Service は、ライセンスサーバーと正常に通信しています。このコントローラーは、ライセンスキャッシュモードではなくなりました。
1157	実行中のライセンスサーバーのバージョンは、Citrix Broker Service のバージョンよりも古く、互換性がありません。ライセンスサーバーをアップグレードするか、XenDesktop 構成で正しいバージョンのライセンスサーバーの場所を指定してください。
1158	Citrix Broker Service は、このエディションのライセンスサーバーで、このサイトに利用可能なライセンス数を超過していることを検出しました。ライセンスサーバーは、オーバードラフトライセンスを付与しました。
1159	Citrix Broker Service は、このサイトにインストールされているライセンスの最大数を超過したため、デスクトップ接続を拒否しました。このエディションには3つのライセンスがインストールされていますが、このエディションで許可されているライセンスの最大数は2つです。ライセンス制限に準拠するために、ライセンスサーバーから関連するライセンスを削除してください。
1160	Citrix Broker Service は、ライセンスの管理中に内部エラーを検出しました。ライセンスサーバーが正しく機能していること、および XenDesktop 構成でライセンスサーバーを識別する詳細が正しいことを確認してください。

イベントID	説明
	Citrix Broker Service を再起動すると、問題が解決する場合もあります。この問題が解決しない場合は、Citrix XenDesktop Controller を再インストールしてください。Citrix Knowledge Base の記事 CTX126990 を参照してください。
1161	ライセンスの初期化エラー。ライセンスサーバーの接続を確認してください。
1162	ライセンスの停止エラー。ライセンスサーバーの接続を確認してください。
1163	接続ライセンスがありません。解決するには、不要なセッションを閉じてライセンスを解放するか、ライセンスを追加してください。
1164	接続ライセンスのチェックアウト中にエラーが発生しました。ライセンスサーバーの接続を確認してください。
1165	接続ライセンスのチェックイン中にエラーが発生しました。ライセンスサーバーの接続を確認してください。
1166	ライセンスの可用性確認中にエラーが発生しました。ライセンスサーバーの接続を確認してください。
1167	ライセンスの開始に失敗しました。ライセンスサーバーの接続を確認してください。
1168	ライセンスユーザー通知設定の読み取り中にエラーが発生しました。ライセンスサーバーの接続を確認してください。
1169	ライセンスサーバーで適切なライセンスが見つからなかったため、このコントローラーは初期設定のライセンスキャッシュモードに入りました。このコントローラーがデスクトッ

イベントID	説明
	プおよびアプリケーションセッションの提供を停止するまで、残り2時間です。
1170	Citrix Broker Service は、ライセンスサーバー上で適切なライセンスを正常に検出しました。このコントローラーは、初期設定のライセンスキャッシュモードではなくなりました。
1171	ライセンスサーバーが指定されていません。有効なライセンスサーバーが指定されるまで、Citrix Broker Service はユーザーにデスクトップとアプリケーションを提供できません。Citrix Studio または Citrix PowerShell SDK コマンドレット Set-ConfigSite を使用して、ライセンスサーバーを指定できます。
1172	ライセンスサーバーの適合性チェック中にエラーが発生しました。Citrix Broker Service は、マシンがライセンスサーバーとして使用するのに適しているかどうかを確認する際に、予期しない応答を受信しました。コントローラーからマシンに接続できること、およびマシンのファイアウォールがコントローラーからの接続を許可していることを確認してください。マシンにライセンスサーバーがインストールされている場合は、それが正しく構成され、動作していることを確認してください。
1173	この XenDesktop サイトには、ライセンスサーバーに必要な起動ライセンスがありません。ライセンス管理コンソールを使用して、関連するライセンスをライセンスサーバーに追加してください。
1174	この XenDesktop サイトに構成されている製品エディションはアプリケーションをサポートしていません。アプリケーションリソースは利用できません。

イベントID	説明
1176	構成されている製品エディションは、マルチセッションマシンをサポートしていません。登録は拒否されました。
1177	構成されている製品エディションは、シングルセッションマシンをサポートしていません。登録は拒否されました。
1178	構成されている製品エディションは RemotePC をサポートしていません。登録は拒否されました。
1179	構成された製品エディションは、クラウドシステムにプロビジョニングされたマシンをサポートしていません。登録は拒否されました。
1180	このXenDesktopサイト用に構成された製品エディションは、シングルセッション（ワークステーションOS）マシン上のアプリケーションをサポートしていません。アプリケーションリソースの起動は拒否されました。
1181	このXenDesktopサイト用に構成された製品エディションは、マルチセッション（サーバーOS）マシン上のアプリケーションをサポートしていません。アプリケーションリソースの起動は拒否されました。
1182	このXenDesktopサイト用に構成された製品エディションは、シングルセッション（ワークステーションOS）マシン上のデスクトップをサポートしていません。デスクトップリソースの起動は拒否されました。
1183	このXenDesktopサイト用に構成された製品エディションは、マルチセッション（サーバーOS）マシン上のデスクトップをサポートしていません。デスクトップリソースの起動が拒否されました。

イベントID	説明
1196	このコントローラーは、ライセンスサーバー上の使用可能なすべてのライセンスを使い果たしたため、ライセンスバーストモードに入りました。これを解決するには、さらにライセンスを追加してください。このコントローラーがデスクトップおよびアプリケーションセッションの提供を停止するまで、残り2時間です。
1197	Citrix Broker Serviceは、デスクトップおよびアプリケーションセッションの提供を停止します。このコントローラーは、ライセンスサーバー上のライセンス不足のため、ライセンスバーストモードに入っていないか、入ることができませんでした。ライセンス管理コンソールを使用して、関連するライセンスをライセンスサーバーに追加してください。
1198	Citrix Broker Serviceはライセンスサーバーからライセンスを正常に消費しています。現在の需要を満たすのに十分なライセンスがサーバーにあります。このコントローラーは、ライセンス枯渇によって引き起こされるライセンスバーストモードではなくなりました。
1199	Citrix Broker Serviceは、デスクトップおよびアプリケーションセッションの提供を停止します。ライセンスサーバーにライセンスがインストールされていないため、このコントローラーはライセンスキャッシュモードではなくなったか、ライセンスキャッシュモードに入ることができませんでした。ライセンス管理コンソールを使用して、関連するライセンスをライセンスサーバーに追加してください。
1205	ソフトウェアメンテナンスの有効期限が切れました。Citrix環境は現在サポートされていません。ライセンスサーバーで期限切れのライセンスを確認し、削除してください。ユーザーが警告メッセージを受け取り始める前に、30

イベントID	説明
	日間のライセンスキャッシュモードがあります。
1206	ライセンス証明書のハッシュが無効です。Citrixライセンス証明書のハッシュが無効です。
1300	Citrix Broker Serviceは、デスクトップおよびアプリケーションセッションの提供を停止します。ライセンスサーバーのシステムクロックに問題があります。
1301	ライセンスサーバーのシステムクロックの問題が修正されました。Citrix Broker Serviceは通常の操作を再開します。
1302	このコントローラーは、接続ライセンスのチェックインまたはチェックアウトに再度失敗しました。以前に検出された障害はまだ存在します。過剰なイベントログを避けるため、問題が解決されるまで、サービスは関連メッセージ（イベントID 1163、1164、1165）を抑制しています。ライセンス試行は継続されます。
1303	このコントローラーは、関連メッセージ（イベントID 1163、1164、1165）の抑制を停止しました。
1304	Citrix Broker ServiceはLASに正常に接続しました。
1305	Citrix Broker ServiceはLASに接続できません。LASが正しく機能していること、およびLASを識別する詳細がXenDesktop構成で正しいことを確認してください。

詳細情報

サイトのLAS状態の確認、またはサイトがライセンスキャッシュモードであるかどうかの確認については、以下を参照してください。

- サイトの LAS 状態を確認するにはどうすればよいですか？
- サイトがライセンスキャッシュモードであるかどうかを確認するにはどうすればよいですか？

コマンドの詳細については、以下を参照してください。

- Get-BrokerController
- Get-ConfigSite

Citrix Virtual Apps and Desktops™ テレメトリデータ要素

ブローカー

使用方法

ヘッダー

キー	説明	例
バージョン	テレメトリイベントのバージョンを示します。	1
id	使用状況イベントの一意の識別子を示します。	d4ce7919-5d80-44de-a8fa-102923fe0ead
タイプ	Citrix Analytic Service がクラウド使用状況イベントを識別するために使用するイベントタイプを示します。	SendBrokerTelemetryData
st	Brokerでイベントが生成されたときのタイムスタンプを示します。	2011-08-12T20:17:46.384Z
製品	使用状況イベントの発信元の製品と展開を識別します。	XenDesktop.Broker (クラウド) OnPrem.Broker (OnPrem)

キー	説明	例
prodVer	Citrix DaaS/Citrix Virtual Apps and Desktopsの製品バージョンを示します。	7.25.0.0

ペイロード

フィールド	説明	例
TotalPublishedApps	公開されているアプリケーションの総数を示します。	10
TotalPublishedDesktops	公開されているデスクトップの総数を示します。	10
VDAs.Total	VDAの総数を示します。	10
VDAs.OSTypes	Windows、Linux、MacなどのOSタイプ別のVDAの総数を示します。	10
VDAs.OSVersions	Windows 10、11、2022、2019などのOSバージョン別の総数を示します。	10
VDAs.HostingLocations.Azure	Azure、AWS、GCP、Nutanix、VMWare、XenServer、HyperVなどのサポートされているホスティングロケーションごとのVDAの数を示します。	10
VDAs.HostingLocations.AWS		
VDAs.HostingLocations.Nutanix		
VDAs.HostingLocations.VMWare		
VDAs.HostingLocations.XenServer		
VDAs.HostingLocations.HyperV		

フィールド	説明	例
VDAs.ProvisionedMethod.MCS	Machine Creation Service (MCS) によってプロビジョニングされたマシンの数を示します。	10
VDAs.ProvisionedMethod.ManualOr3P	手動または3Pでプロビジョニングされたマシンの数を示します。	10
VDAs.SessionSupport.StaticSingle	静的に割り当てられたシングルセッションのマシンの数を示します。	10
VDAs.SessionSupport.DynamicSingle	動的にシングルセッションが割り当てられたマシンの数を示します。	10
VDAs.SessionSupport.Multi	マルチセッションマシンの総数を示します。	10
VDAs.RemotePCAccess.Windows	OSタイプ（Win、Mac、Linux）別のRemote PC Accessマシンの数を示します。	10
VDAs.RemotePCAccess.Linux		
VDAs.RemotePCAccess.MacOS		
VDAs.ActiveSessionRecordingAgents	アクティブなセッション記録エージェントを持つVDAの数を示します。	5
VDAs.Subscriptions	VDAのパブリッククラウドサブスクリプションの数を示します。	2
VDAs.LocationTypes	VDAのロケーションタイプの数を示します。	2

フィールド	説明	例
AutoScale.DGWithAutoscaleEnabled	**Autoscale** が有効になっているデリバリーグループの数を示します。	2
AutoScale.TotalMachinesCtrlByAutoscale	オートスケールによって制御されるマシンの数を示します。	5
AutoScale.VerticalAutoscaleEnabledByDGandSite	DGとサイトによって**垂直オートスケール**が有効になっているマシンの数を示します。	2
AutoScale.TaggedBasedAutoscaledDG	タグベースで自動スケーリングされたデリバリーグループの数を示します。	2
DeliveryGroup.TotalRebootSchedulesEnabled	**再起動スケジュール**が有効になっているデリバリーグループの数を示します。	2
DeliveryGroup.Total	デリバリーグループの合計数を示します。	10
Policy.TotalPolicySets	ポリシーセットの数を示します。	3
Policy.TotalPolicies	グループポリシーの数を示します。	2
Policy.TotalPolicySettings	グループ設定の数を示します。	2
PublishedPackageApps.AppVSingleAdmin	AppVシングル管理者モードで公開されているパッケージ化されたアプリの総数を示します。	2
PublishedPackageApps.AppVDualAdmin	AppVデュアル管理者モードで公開されているパッケージ	2

フィールド	説明	例
	化されたアプリの総数を示します。	
PublishedPackageApps.Msix	MSIXモードで公開されているパッケージ化されたアプリの総数を示します。	2
PublishedPackageApps.AppAttach	AppAttachモードで公開されているパッケージ化されたアプリの総数を示します。	2
PublishedPackageApps.FlexApp	FlexAppモードで公開されたパッケージ化されたアプリの総数を示します。	2

セッション

ヘッダー

フィールド	説明	例
バージョン	ライセンス使用状況イベントのバージョンを示します。	1
id	使用状況イベントの一意の識別子を示します。	d4ce7919-5d80-44de-a8fa-102923fe0ead
タイプ	Citrix Analytic Serviceがクラウド使用状況イベントを識別するために使用するイベントタイプを示します。	Cloud.Licensing
st	Brokerでイベントが生成されたときのタイムスタンプを示します。	2011-08-12T20:17:46.384Z

フィールド	説明	例
プロダクト	使用状況イベントの発生元製品と展開を識別します。	XenDesktop.Broker (クラウド) OnPrem.Broker (OnPrem)
prodVer	Citrix DaaSまたはCitrix Virtual Apps and Desktopsの製品バージョンを示します。	7.25.0.0
ユーザー	セッション起動を開始するユーザーを一意に識別するためのユーザーIDを特定します。**値はスクランブル化されています。**	fullName: C648FE671A44B3F7 **(常にスクランブル化されています)** samName:C758LH671A44B3F7 **(常にスクランブル化されています)** upn: C7948FE671A44B3F7 **(常にスクランブル化されています)** userLicenseId:C265FE671A44B3F7 **(常にスクランブル化されています)** userSid: C097FE671A44B3F7 **(常にスクランブル化されます)**
テナント -> ID	Citrix Cloud™アカウントの顧客IDを示します。オンプレミス展開の場合、この	ジョジイチエムゼロゴキュウハチティージェイ

フィールド	説明	例
	フィールドは適用されず、値はありません。	
デバイス -> デバイスID	セッション起動が開始されたデバイスを一意に識別するためのデバイスIDを示します。	AE18C4D5
デバイス -> デバイス名	デバイスのフレンドリ名を示します。**値はスクランブル化されています。**	C758LH671A44B3F7 **(常にスクランブル化されます)**

ペイロード

フィールド	説明	例
appProtectionKeyLoggingRequired	セッションがキーロギング保護を有効にして起動されたかどうかを示します。	偽
appProtectionScreenCaptureRequired	セッションが画面キャプチャ保護を有効にして起動されたかどうかを示します。	偽
cspTenantCustomerId	CSPテナントのCitrix Cloudアカウントの顧客IDを示します。オンプレミス展開の場合、このフィールドは適用されず、値はありません。	ロクシーツーブイティーエックスジーエックスワイエフティーティー
isAnonymousUser	認証されていないセッションが起動さ	偽

フィールド	説明	例
	れたかどうかを示します。	
licenseActivityTimeStamp	ペイロードが生成されたときのタイムスタンプを示します。	2011-08-12T20:17:46.384Z
licenseActivityType	ライセンスイベントの種類を示します。このフィールドは、ライセンスイベントの種類が割り当てアクションか解放アクションかを示します。	接続
licenseModel	展開のライセンスモデルを示します。	UserDevice
productEdition	展開の製品エディションを示します。	プレミアム
productId	展開内の製品の製品IDを示します。	CAVDS
プロトコル	セッションの起動に使用されたプロトコルを示します。	HDX™
sessionKey	セッションの一意の識別子を示します。	uq390c5fc3-86eb-4df3-bd9a-f4a8fed2c9e2
sessionSupport	セッションサポートの種類を示します。	SingleSession
sessionType	セッションの種類を示します。	アプリケーション
バージョン	ペイロードのバージョンを示します。	1.3

フィールド	説明	例
workerSid	セッションに使用されるVDAの一意の識別子を示します。**値はスクランブル化されています。**	1E5LH671A44B3F7 **(常にスクランブル化されています)**
isWindows365	セッションがWindows 365向けに起動されたかどうかを示します。	真
entitlementType	顧客のライセンスエンタイトルメントタイプを示します。	本番
siteId	サイトの一意の識別子を示します。	a35647d0-901c-4477-87e0-dcd781d455f4
desktopGroupId	デスクトップまたはデリバリーグループの一意の識別子を示します。	e9d859dc-1bfc-4b3e-bad3-41806bb4e694
clientType	Citrix Workspace™ アプリの種類を示します。	ウィンドウズ
clientVersion	Citrix Workspaceアプリのバージョンを示します。	23.5.1.83
workerCloudType	VDAプロビジョニングに使用されるパブリッククラウドの種類を示します。	アジュール
enabledFeatures	セッションで有効になっている機能を示します。たとえば、`AppProtectionScr`	66

フィールド	説明	例
	`eenCaptureRequired` と `SessionRecording` が有効になっているセッションでは、このフィールドの値は 66 です。	
launchRequestSource	起動を要求するために使用された製品を記録します。オンプレミスStoreFront™またはCloud StoreFrontのいずれかです。	0 (StoreFront or 3P) 1 (ワークスペース)
isEvents	{{page.lic}}における重大な障害を示します。	STデータベースを作成できません。
heartBeatTime	CISまたはCitrix Analytic Serviceへのライセンスサーバーのハートビート時間を示します。	1689058813
vdaTelemetry	App Layering、User Personalization Layer、User Profile management、Workspace Environment Management™、およびHDX機能のためにキャプチャされるペイロードを示します。	vdaTelemetry SessionTelemetry CPM_機能: 32 HDX1: 66 HDX2: 0 MachineTelemetry AL_productVersion: 23.12.0.1001 UPL_isEnabled: 1

フィールド	説明	例
		CPMバージョン: 22.3.4000 wem_enableMethod: 1 wem_agentVersion: 2402.1

スタジオ

使用方法

ヘッダー

フィールド	説明	例
バージョン	ライセンス使用状況イベントのバージョンを示します。	1
id	使用状況イベントの一意の識別子を示します。	8c2e20a5-ca3f-4401-ad69-d037933c40a0
タイプ	Citrix Analytic Service がクラウド使用状況イベントを識別するために使用するイベントタイプを示します。	Studio.Usage
st	Studio でイベントが生成されたときのタイムスタンプを示します。	2024-03-22T01:32:23.4056195Z
製品	使用状況イベントの発生元となる製品と展開を識別します。	XenDesktop.Studio
prodVer	Citrix DaaS/Citrix Virtual Apps and Desktops の製品バージョンを示します	7.42.0.0

ペイロード

フィールド	説明	例
AdminLoginList	一意の管理者 SamAccountName のリストを示します。**値はスクランブルされています。**	{AdminLoginList: [UFMJ+JvXOTHO9mQDsOweiw= =]}**(常にスクランブルされます)**
TotalApiRequests	オーケストレーションサービスのAPIリクエストを示します。	{TotalApiRequests: 1000}
BackupCount	Studio管理者が操作したバックアップの数を示します。	{BackupCount: 200}
RestoreCount	Studio管理者が操作した復元回数を示します。	{RestoreCount: 20}

ディレクター

使用状況レポート

ヘッダー

フィールド	説明	例
バージョン	ライセンス使用状況イベントのバージョンを示します。	1
id	使用状況イベントの一意の識別子を示します。	8c2e20a5-ca3f-4401-ad69-d037933c40a0
タイプ	Citrix Analytic Service がクラウド使用状況イベントを識別するために使用するイベントタイプを示します。	テレメトリ
st	Studio でイベントが生成されたときのタイムスタンプを示します。	2024-03-22T01:32:23.4056195Z

フィールド	説明	例
製品	使用状況イベントの発生元となる製品と展開を識別します。	XenApp.Monitor
prodVer	Director の製品バージョンを示します。	7.42.0.0
dvcName	サーバー名	C758LH671A44B3F7

ペイロード

フィールド	説明	例
AdminLoginCount	これは、管理者のログイン数を提供するペイロードのセクションです。	タイプ: AdminLogin 統計 0: 1 1: 7
FeatureUsageCount	ペイロードのこのセクションには、Director で使用されている主要機能の数が含まれています。	タイプ: 機能使用状況 統計 0: 15 1: 20 5: 10
OdataUsageCount	ペイロードのこのセクションには、Odata API の使用状況のカウントが含まれています。	タイプ: OData_v3 統計 0: 1 2: 7 5: 9 タイプ: OData_v4 統計

フィールド	説明	例
		0: 1 2: 8 6: 7
AppUsage	公開されたアプリケーションの週次使用状況メトリックを示します。	タイプ: AppUsage ヘッダー: applicationName,processName,totalDurationInMinutes 期間: 01/05/24-07/05/24 値: [Calc_AWTSVDA-1907R,calc.exe,0.13, Notepad_AWTSVDA-1907R,notepad.exe,4]
UniqueAppUsers	公開されたアプリケーションについて、1か月間のユニークユーザー数とアプリケーションの合計起動数を示します。	タイプ: UniqueAppUsers ヘッダー: applicationName,totalLaunches,totalUniqueUsers 期間: 04/24 値: [Calc_AWTSVDA-1907R,100,10,

フィールド	説明	例
		Notepad_AWTSVDA-1907R,200,20]
DesktopUsage	公開されたデスクトップの週ごとの使用状況メトリックを示します。	タイプ: DesktopUsage ヘッダー: desktopGroupName,sessionSupport,totalDurationInMinutes 期間: 01/05/24-07/05/24 値: [RdsDesktopAndAppGroup,1,10]
UniqueDesktopUsers	公開デスクトップについて、1か月間の総起動回数とともにユニークユーザーの数を表します。	タイプ: UniqueDesktopUsers ヘッダー: desktopGroupName,totalLaunches,totalUniqueUsers 期間: 04/24 値: [RdsDesktopAndAppGroup,10,5]
AvgLogonDuration	平均ログオン期間を示します。	タイプ: AvgLogonDuration ヘッダー: totalUserLogons,

フィールド	説明	例
		avgLogonDurationInSeconds 期間: 01/05/24-07/05/24 値: [200,4]
CostSaved	顧客が1か月に節約したコストを示します。	タイプ: CostSaved ヘッダー: ハイパーバイザー,コスト削減,通貨 期間: 04/24 値: [1,221.02,1 2,301.02,2]

Storefront の構成

使用方法

ヘッダー

フィールド	説明	例
バージョン	ライセンス使用状況イベントのバージョンを示します	1.0
id	使用状況イベントの一意の識別子を示します	d4ce7919-5d80-44de-a8fa-102923fe0ead
タイプ	CAS がクラウド使用状況イベントを識別するために使用するイベントタイプを示します	構成

フィールド	説明	例
st	StoreFront でイベントが生成されたときのタイムスタンプを示します	2011-08-12T20:17:46.384Z
製品	使用状況イベントの発生元の製品と展開を識別します	OnPrem.StoreFront
prodVer	StoreFrontのバージョンを示します (内部)	3.30.0.0

ペイロード

フィールド	説明	例
serverName	StoreFrontが稼働しているサービスのホスト名を示します	storefront-01.storefront.local
deploymentId	StoreFrontの展開の一意の識別子を示します	f47ac10b-58cc-4372-a567-0e02b2c3d479
installedWithCVAD	StoreFrontがCVADと並行してインストールされたかどうかを示します	偽
cpuCores	CPUコアの総数を示します	4
cpuModel	StoreFrontを実行しているCPUを示します	第12世代 Intel(R) Core(TM) i7-1255U 1.70 GHz
ramGb	RAMの総容量（GB単位）を示します	16
numServersInGroup	サーバーグループ内のサーバー数を示します	3
ストア	StoreFront Store構成JSONブロブを示します。Storeオブジェクトの配列です。**一部の値はスクランブルされています**	例

フィールド	説明	例
rfWebSites	StoreFront RFWeb構成JSONブロブを示します。RFWeb Configオブジェクトの配列です。	例
ゲートウェイ	ゲートウェイ構成オブジェクトをJSONブロブとして示します。ゲートウェイオブジェクトの配列です。	例
authServices	認証サービス構成オブジェクトをJSONブロブとして示します。認証サービスオブジェクトの配列です。	例
IsPiiScrambled	真	

フィールド STORES の例

```
[{

            "BaseUrl": "baseUrl",

            "StorePath": "/",

            "EnabledFeatures": 21 bit bitmap,

            "ResourceTypeFilteringEnabled": "disabled|
Citrix.MPS.Application;Citrix.MPS.Desktop",

            "DefaultRfWebSite": "/Citrix/StoreWeb",

            "GatewaysUsed": [

                "gatewayId"

            ],

            "VdaLogonDataProvider": "",

            "ResourceFeeds": [
```

```
                {
                    "FeedName": "<resourceFeedName>|scrambled",
                    "Type": "CVAD",
                    "LoadBalancingEnabled": true,
                }
            ],
            "AdvancedAggregation": {
                 "Enabled": true,
                 "GroupingCount": 1,
                 "ControllersPushIdenticalResources": true,
                 "LoadBalanced": true,
                 "AnyPrimaryFarms": true,
                 "AnyBackupFarms": true,
            }
}]
```

ストアが見つからない場合、それは空の配列になります 。

フィールド RFWEBSITES の例

```
[{
    "SiteId": "siteId",
    "BaseUrl": "baseUrl",
    "StorePath": "storePath",
    "UiExperienced": 0,
```

```
    "EnabledFeatures": 9 bit,
    "AuthMethodsEnabled": [
        "ad"
    ],
    "CanUsersDownloadApps": {
        "Enabled": true,
        "Windows": "exe",
        "MacOS": "dmg"
    },
    "WorkspaceControl": {
        "Enabled": true,
        "LogoffAction": 0,
        "AutoReconnectAtLogon": true,
        "ShowReconnectButton": true,
        "ShowDisconnectButton": true
    },
    "MultiClickTimeout": 1,
    "UiViews": [
        "apps",
        "desktops"
    ],
    "DefaultTab": 0,
```

```
}]
```

rfWebSites が見つからない場合、空の配列になります 。

フィールド GATEWAYS の例

```
[{
            "GatewayId": "gatewayId",
            "IsCloudGateway": true,
            "LoadBalancingSTAEnabled": true,
            "SessionReliabilityEnabled": true,
            "RequestTicketsFromTwoSTA": true,
            "Version": "1234",
            "LogonType": "domain",
            "SmartCardFallbackEnabled": true
}]
```

gateways が見つからない場合、空の配列になります 。

フィールド AUTHSERVICES の例

```
[{
    "SiteId": "SiteId",
    "Store": "StoreAuth",
    "AuthMethodsEnabled": [
        "ad"
    ],
    "PasswordChangeWhenExpired": 0,
```

```
    "PasswordRemindersForm": 1,

    "DelegateCredentialValidationToCitrix": true,

    "ValidatePasswordsOnDeliveryControllers": true

}]
```

認証サービスが見つからない場合、空の配列になります 。

ストアフロントログイン

使用方法

ヘッダー

フィールド	説明	例
バージョン	ライセンス使用状況イベントのバージョンを示します	1.0
id	使用状況イベントの一意の識別子を示します	d4ce7919-5d80-44de-a8fa-102923fe0ead
タイプ	CAS がクラウド使用状況イベントを識別するために使用するイベントの種類を示します	ログイン
st	Broker でイベントが生成されたときのタイムスタンプを示します	2011-08-12T20:17:46.384Z
本番	使用状況イベントの発生元の製品と展開を識別します	OnPrem.StoreFront
prodVer	StoreFront バージョン (内部)	3.30.0.0

ペイロード

フィールド	説明	例
ユーザー	起動を開始したユーザー。**値はスクランブル化されています**	fullName: C648FE671A44B3F7 **(常にスクランブル化されています)** samName:C758LH671A44B3F7 **(常にスクランブル化されています)** upn: C7948FE671A44B3F7 **(常にスクランブル化されています)** userLicenseId:C265FE671A44B3F7 **(常にスクランブル化されています)** userSid: C097FE671A44B3F7 **(常にスクランブル化されています)**
サーバー名	StoreFrontが稼働しているサービスのホスト名を示します	storefront-01.storefront.local
loginMethodRfWeb	ユーザーがRFWebからStoreFrontにログインするために使用した方法を示します	0
loginMethodAuth	ユーザーがAuthサービスからStoreFrontにログインするために使用した方法を示します	0

フィールド	説明	例
gatewayURL	ログイン中に使用されたNetscaler Gatewayを示します	netscaler-gateway.com
enabledFeatures	有効な機能のビットマスクを示します	12
userAgent	ログインに使用されたクライアントのUserAgentを示します	シトリックスレシーバー/22.11.0.19 リナックス/5.17.15 X1クラス CWACapable CWA/22.11.0.19
baseUrl	ユーザーがログインするストアを示します	storefront-dev.storefront.dev
storePath	ユーザーがログインするストアを示します	/Citirx/StoreWeb
apiUsed	クライアントがStore APIまたはPNAgent APIを使用しているかどうかを示します	0
deviceId	StoreFrontへのログインに使用されるデバイスを示します。**値はスクランブルされています**	ジョン・ドウ
transactionId	単一のトランザクション中に送信/生成されるトランザクションIDを示します。	773aba9e-5b91-4ef9-8782-c4afb75698e7

委任管理

使用方法

ヘッダー

キー	説明	例
バージョン	ライセンス使用状況イベントのバージョンを示します。	1
id	使用状況イベントの一意の識別子を示します。	8c2e20a5-ca3f-4401-ad69-d037933c40a0
タイプ	Citrix Analytic Service がクラウド使用状況イベントを識別するために使用するイベントタイプを示します。	DelegatedAdmin.Usage
st	イベントが Delegated Admin で生成されたときのタイムスタンプを示します。	2024-03-22T01:32:23.4056195Z
製品	使用状況イベントの発生元の製品と展開を識別します。	XenDesktop.DelegatedAdmin (クラウド)
		OnPrem.DelegatedAdmin (OnPrem)
prodVer	Citrix DaaS または Citrix Virtual Apps and Desktops の製品バージョンを示します。	7.42.0.0

ペイロード

キー	説明	例
TotalCustomScopes	カスタムスコープの総数を示します。	2
TotalCustomRoles	カスタムロールの総数を示します。	4

ライセンス テレメトリ データをスクランブルする

ライセンス テレメトリで送信される情報の機密性を考慮し、Citrix はデータを難読化するオプションを提供します。

次の表に、難読化できるデータを示します。

フィールド	説明	例
ユーザー	セッション起動を開始するユーザーを一意に識別するためのユーザー ID を識別します。	• フルネーム: `C648FE671A44B3F7` • samName: `C758LH671A44B3F7` • UPN: `C7948FE671A44B3F7` • userLicenseId: `C265FE671A44B3F7` • userSid: `C097FE671A44B3F7`
dvc を dvcName に	デバイスのフレンドリ名を示します。	`C758LH671A44B3F7`
workerSid	セッションに使用されるVDAの一意の識別子を示します。	`1E5LH671A44B3F7`
AdminLoginList	一意の管理者SamAccountNameのリストを示します	`{AdminLoginList: [UFMJ+JvXOTHO9mQDsOweiw= =]}`
ストア	StoreFrontストア構成のJSONブロブを示します。ストアオ	例

フィールド	説明	例
	ブジェクトの配列です。**一部の値はスクランブルされています**	
deviceId	StoreFrontへのログインに使用されるデバイスを示します。	ジョン・ドウ

スクランブルを有効または無効にするには、Delivery Controllerで次のPowerShellコマンドを実行します。

注：

Citrix Service Provider™ (CSP) のお客様の場合、スクランブルは常に無効になっています。CSP のお客様は、PowerShell コマンドを使用してスクランブルを有効にすることはできません。

1. Delivery ControllerホストからPowerShellウィンドウを開きます。
2. コマンド `asnp citrix` を実行して、Citrix固有のPowerShellモジュールをロードします。
3. スクランブルを有効または無効にするには、次のコマンドを実行します。

   デフォルトでは、値は`1`または`true`であり、ライセンステレメトリデータのスクランブルを有効にします。

   無効にするには：

   ```
   Set-BrokerServiceConfigurationData Core.ScrambleLicensingData
   -SettingValue $false
   ```

   スクランブルを無効にした後、次のコマンドを使用して有効にできます。

   ```
   Set-BrokerServiceConfigurationData Core.ScrambleLicensingData
   -SettingValue $true
   ```

ライセンスに関するFAQ

注記:

- COVID-19パンデミックに関連する事業継続リソースについては、CTX27055を参照してください。
- 事業継続の維持に関する一般情報については、Business continuity — on demandを参照してください。
- 現在のCitrix License Serverの詳細については、Licensingを参照してください。

Citrix®ライセンス

License Activation Serviceとは何ですか?

License Activation Service (LAS) は、オンプレミスのCitrix License Server向けの最新のクラウドベースのライセンスソリューションです。これは、従来のファイルベースのライセンス方式に代わる合理化された方法を提供します。

ライセンスファイルを手動でアップロードする代わりに、ライセンスサーバーをCitrix Cloud™に接続してオンラインアクティベーションを行うことができます。その後、お客様のエンタイトルメントは自動的にライセンスサーバーに配信され、ライセンスファイルのライフサイクル管理の必要がなくなります。

クラウドに接続できないライセンスサーバーの場合、LASはオフラインアクティベーションオプションも提供し、さまざまなネットワーク環境での柔軟性を確保します。このサービスは、Citrix製品ライセンスを管理するためのシームレスで最新のアプローチを導入します。

詳細については、License Activation Serviceを参照してください。

ライセンスファイルはどのように入手できますか?

ライセンスアクセスコードはメールでお送りします。ライセンスアクセスコードを使用してライセンスファイルを生成する方法は3つあります。

- `citrix.com`のMyAccountページにある**Manage Licenses**。詳細については、Manage licenses on citrix.comを参照してください。
- Web Studioでご購入を割り当てると、ライセンスファイルがCitrix License Serverに自動的にインストールされます。

- Citrix License Server内のCitrix Licensing Managerを使用して、購入を割り当て、ライセンスファイルをインストールします。詳細については、ライセンスのインストールを参照してください。

私のアカウントでライセンスを割り当てる方法?

ライセンスの割り当てを参照してください。

割り当てられたライセンスをライセンスサーバーに追加する方法?

ライセンスの変更を参照してください。

CitrixライセンスはどのTCPポートを使用しますか?

- ライセンスサーバーのポート番号は27000です。
- ベンダーデーモンのポート番号は7279です。
- ライセンス用Webサービスのポートは8083です。

Citrixライセンスサーバーとは何ですか?

Citrix License Serverは、ネットワーク全体でライセンスを共有できるシステムです。詳細については、ライセンス操作の概要を参照してください。

Citrixライセンスサーバーを仮想化またはクラスター化できますか?

はい。Citrix License Serverを仮想化またはクラスター化できます。詳細については、クラスター化されたライセンスサーバーを参照してください。

Citrix License Serverを仮想化した場合、どのような利点がありますか?

Citrix License Serverを仮想化すると、冗長なソリューションが提供されます。このソリューションにより、ダウンタイムなしで複数の物理サーバー間での移動が可能になります。

Citrix License Serverを仮想化する場合、考慮すべき制限はありますか?

いいえ。

Citrixライセンスサーバーは、Citrix Virtual Apps and Desktops™展開のすべてのライセンスを管理しますか?

Citrix License Server は、Citrix Virtual Apps and Desktops 用に受け取るすべてのライセンスを管理します。ただし、Citrix Gateway で使用される Premium Edition のライセンスは除きます。これらのセキュリティ指向のネットワークデバイスに必要なネットワークアプライアンスに組み込まれたライセンスサーバーが、それらのライセンスを管理します。

Citrix Licensing Managerとは何ですか?

Citrix Licensing Managerを使用すると、Citrix Licensing Managerをインストールしたライセンスサーバーからライセンスファイルをダウンロードして割り当てることができます。Citrix Licensing Managerは、推奨されるライセンスサーバー管理方法であり、以下のことが可能になります。

- Citrix Cloudへのライセンスサーバーのショートコード登録と、登録の簡単な削除。
- ユーザーアカウントとグループアカウントの構成。
- ダッシュボードを使用して、インストール済み、使用中、期限切れ、利用可能なライセンス、およびCustomer Success Servicesの期日を表示する。
- レポート作成のためにライセンス使用状況データをエクスポートする。
- 履歴使用状況データの保持期間を構成する。デフォルトのデータ保持期間は180日です。
- ライセンスアクセスコードまたはダウンロードしたファイルを使用して、ライセンスサーバーにライセンスファイルを簡単にインストールする。
- ライセンスバーストモードを有効または無効にする。
- Customer Experience Improvement Program (CEIP) と コールホーム を構成する。
- Customer Success Servicesの更新ライセンスを自動または手動で確認し、見つかった場合は通知するか、ライセンスをインストールする。
- ライセンスサーバーの状態（起動ライセンスの不足、時間に関する問題、アップローダーの障害など）を通知します。
- これらのポートを変更します。
    - ライセンスサーバー (デフォルト 27000)
    - ベンダーデーモン (デフォルト 7279)
    - ライセンス用Webサービス (デフォルト 8083)

詳細については、「Citrix Licensing Manager」を参照してください。

Citrix License Administration Consoleはどこにありますか?

License Administration Consoleはサポートされなくなり、License Serverバージョン11.16.6から削除されました。Citrix Licensing Managerを使用することをお勧めします。

License ServerがStudioと同じドメイン内、または信頼されたドメイン内にある場合、Studioを使用してライセンスを管理および追跡できます。

詳細については、「Citrix Licensing Manager」を参照してください。

ライセンス割り当て期間とは何ですか?

ライセンス割り当て期間とは、Citrix Virtual Apps and Desktopsライセンスがユーザーまたはデバイスに割り当てられる期間のことです。デフォルトのライセンス割り当て期間は90日です。

組織が購入したライセンスの数を確認するにはどうすればよいですか?

購入したすべてのライセンスは、`<https://www.citrix.com>`の**My Account**ページにある安全な**Manage Licenses**ツールボックスから、いつでも（24時間365日）確認およびアクセスできます。

いつでも使用中のライセンス数を確認するにはどうすればよいですか?

Citrix Licensing ManagerとStudioは、リアルタイムのライセンス使用状況に関する詳細情報を提供します。

ライセンスサーバーのディザスターリカバリとメンテナンス

ライセンスサーバーのディザスターリカバリとメンテナンスについては、Citrix Licensingドキュメントの「ディザスターリカバリとメンテナンス」を参照してください。

Citrix Virtual Apps and Desktopsのライセンス

Citrix Virtual Apps and Desktopsはどのようにライセンスされますか?

シトリックス バーチャル アプリケーションズ アンド デスクトップス のライセンスは、ユーザー/デバイスおよび同時使用ライセンスモデルを提供します。

ユーザー/デバイス：

柔軟なユーザー/デバイスモデルは、以下と連携します。

- 企業全体のデスクトップ使用。
- 基盤となるMicrosoftデスクトップ仮想化ライセンス。
- 仮想デスクトップとアプリへのアクセスが時々しか必要ない顧客向けの同時使用ライセンス。

ユーザー/デバイスライセンスにより、ユーザーは無制限の数のデバイスから仮想デスクトップとアプリにアクセスできます。デバイスライセンスにより、無制限の数のユーザーが単一のデバイスから仮想デスクトップとアプリにアクセスできます。このアプローチは、最大限の柔軟性を提供し、Microsoftデスクトップ仮想化ライセンスとの整合性を向上させます。

> **重要：**

> ライセンスをユーザーまたはデバイスに手動で割り当てることはできません。ライセンスサーバーまたはクラウドサービスがライセンスを割り当てます。ユーザー/デバイスライセンスでは、一度割り当てられたライセンスは、90日間非アクティブになるまで別のユーザーに割り当てることはできません。

> **同時使用：**

同時使用ライセンスは、任意のユーザーおよび任意のデバイスに対して、無制限の数の仮想アプリおよびデスクトップへの1つの接続を許可します。ライセンスはアクティブなセッション中にのみ消費されます。セッションが切断または終了した場合、ライセンスはプールに戻されます。

ユーザー/デバイスライセンスの詳細については、ユーザー/デバイスライセンス を参照してください。同時使用ライセンスについては、同時使用ライセンス を参照してください。

ライセンスを購入する前にCitrix Virtual Apps and Desktopsを試用することは可能ですか?

はい。Citrix Virtual Apps and Desktopsソフトウェアをダウンロードし、試用モードで実行できます。試用モードでは、Citrix Virtual Apps and Desktopsをオンプレミスで30日間、10接続まで、ライセンスなしで使用できます。詳細については、評価ライセンスを参照してください。

Citrix Cloud向けのCitrix DaaS™（旧Citrix Virtual Apps and Desktopsサービス）は、承認に基づいて試用サービスとして利用可能です。詳細については、Citrix担当者にお問い合わせください。

CitrixはCitrix Virtual Apps and Desktopsの同時使用をどのように定義していますか?

Citrix Virtual Apps and Desktopsの同時接続モデルでは、任意のユーザーと任意のデバイスに対して、無制限の数の仮想アプリとデスクトップへの1つの接続を許可します。ライセンスはアクティブなセッション中にのみ消費されます。セッションが切断または終了した場合、ライセンスは再発行のためにプールに戻されます。詳細については、「同時接続ライセンス」を参照してください。

共通のライセンスサーバーにCitrix Virtual Apps and Desktopsライセンスの複数のエディションを展開できますか?

はい。ライセンスサーバーは、Citrix Virtual AppsとCitrix Virtual Desktopsの両方のライセンスを同時に管理します。最新のライセンスサーバーバージョンをインストールすることをお勧めします。お使いのライセンスサーバーのバージョンが最新であるか不明な場合は、Citrixダウンロードサイトの番号とご自身のバージョンを比較して確認してください。

単一のサイトでCitrix Virtual AppsとCitrix Virtual Apps and Desktopsの両方のライセンスを使用できます?

バージョンによっては、単一のCitrix Virtual AppsまたはCitrix Virtual Apps and Desktopsサイトで、ユーザー/デバイスまたは同時接続の両方のライセンスモデルをサポートできます。単一のCitrix Virtual AppsまたはCitrix Virtual Apps and Desktopsサイトは、1つのエディションのみをサポートできます。詳細については、「マルチタイプライセンス」を参照してください。

複数タイプライセンスをサポートする最小バージョンは、XenApp and XenDesktop 7.15 Long Term Service Release (LTSR) およびCitrix Virtual Apps and Desktops 7 1808です。

ライセンスサーバーにCitrix Virtual Apps and Desktopsユーザー/デバイスまたはCitrix Virtual Apps and Desktops同時接続ライセンスがインストールされている場合、製品モデルとしてCitrix Virtual Apps同時接続を選択できます?

Citrix Virtual AppsをCitrix Virtual Apps and Desktops AdvancedまたはPremium Editionの機能として使用する場合、Citrix Virtual Appsのライセンスモデルは、Citrix Virtual Apps and DesktopsのAdvancedまたはPremium Editionと同じになります。Citrix Virtual Apps and Desktopsを購入した場合、Citrix Virtual Appsの機能のみを使用する予定であっても、ライセンスをCitrix Virtual Apps and Desktopsとして構成してください。製品モデルとしてCitrix Virtual Appsを選択するのは、ライセンスサーバーにCitrix Virtual Apps同時接続スタンドアロンライセンスがインストールされている場合のみです。

各Citrix Virtual AppsおよびCitrix Virtual Apps and Desktopsエディションには、どのような製品コンポーネントが含まれていますか?

エディションごとの全機能マトリックスについては、Citrix Virtual Apps and Desktops の機能を参照してください。

Citrix Virtual Apps and Desktops EULA に準拠して Citrix Virtual Desktops™ 環境をライセンスするにはどうすればよいですか?

Citrix Virtual Apps and Desktops EULA に準拠して、ユーザー/デバイスまたは同時接続ライセンスモデルで Citrix Virtual Apps and Desktops を展開するには、ライセンスファイルをライセンスサーバーに適用します。ライセンスサーバーは、ライセンスのコンプライアンスを制御および監視します。購入した内容に基づいて製品を構成することをお勧めします。たとえば、Citrix Virtual Apps and Desktops Premium を購入したが、Citrix Virtual Apps 機能のみを使用したい場合は、コンプライアンスを満たすために製品を Citrix Virtual Apps and Desktops に構成します。詳細については、製品ライセンスコンプライアンスセンターを参照してください。

Citrix Virtual Apps EULA に準拠して Citrix Virtual Apps 環境をライセンスするにはどうすればよいですか?

Citrix Virtual Apps EULA に準拠して同時接続ライセンスモデルで Citrix Virtual Apps を展開するには、ライセンスファイルをライセンスサーバーに適用します。ライセンスサーバーは、ライセンスのコンプライアンスを制御および監視します。

Citrix Virtual Apps and Desktops のサービスオプション: Long Term Service Release (LTSR) または Current Release (CR) にライセンス要件はありますか?

Long-Term Service Release などの Citrix Virtual Apps and Desktops のサービスオプションは、Customer Success Services プログラムの特典です。LTSR の特典を受けるには、アクティブな Customer Success Services が必要です。詳細については、[Citrix Virtual Apps、Citrix Virtual Apps and Desktops、および XenServer のサービスオプションを参照してください。

Remote Browser Isolation (RBI) サービスのプールされた時間はどのように機能しますか?

サービスを最低 25 ユーザー購入すると、すべてのユーザーでプールされた 5000 時間のサービス利用権が付与されます。その後のユーザー権限の購入では、プールされた時間の権利は増加しません。サービス時間の権利を増やすには、アドオンパックを購入してください。

CCU ライセンスで Remote PC Access を使用できますか?

はい。

Remote PC Access の詳細については、Remote PC Accessを参照してください。

Citrix 環境のソフトウェアメンテナンスの有効期限が切れるとどうなりますか?

ソフトウェアメンテナンス (SWM) またはサブスクリプションの有効期限が切れると、ソフトウェアアップグレードとテクニカルサポートへのアクセスが一時停止されます。また、ライセンスの種類と製品バージョンによっては、エンドユーザーと管理者に、環境がサポートされていないことを示す特定の警告通知が届きます。

これらの通知は、サーバー上のすべてのライセンスの有効期限が切れた場合にのみトリガーされます。

エンドユーザーエクスペリエンス

ユーザーはセッション起動後に警告メッセージを受け取ります。メッセージには次のように表示されます。

```
Citrix Virtual Apps and Desktops warning: Your corporate Citrix
environment is currently unsupported. Please contact your IT department to
resolve.
```

管理者エクスペリエンス

管理者は、Citrix Studio コンソール内で、間近に迫った、または有効期限切れの警告アラートを受け取ります。

ライセンスの種類による有効期限の動作

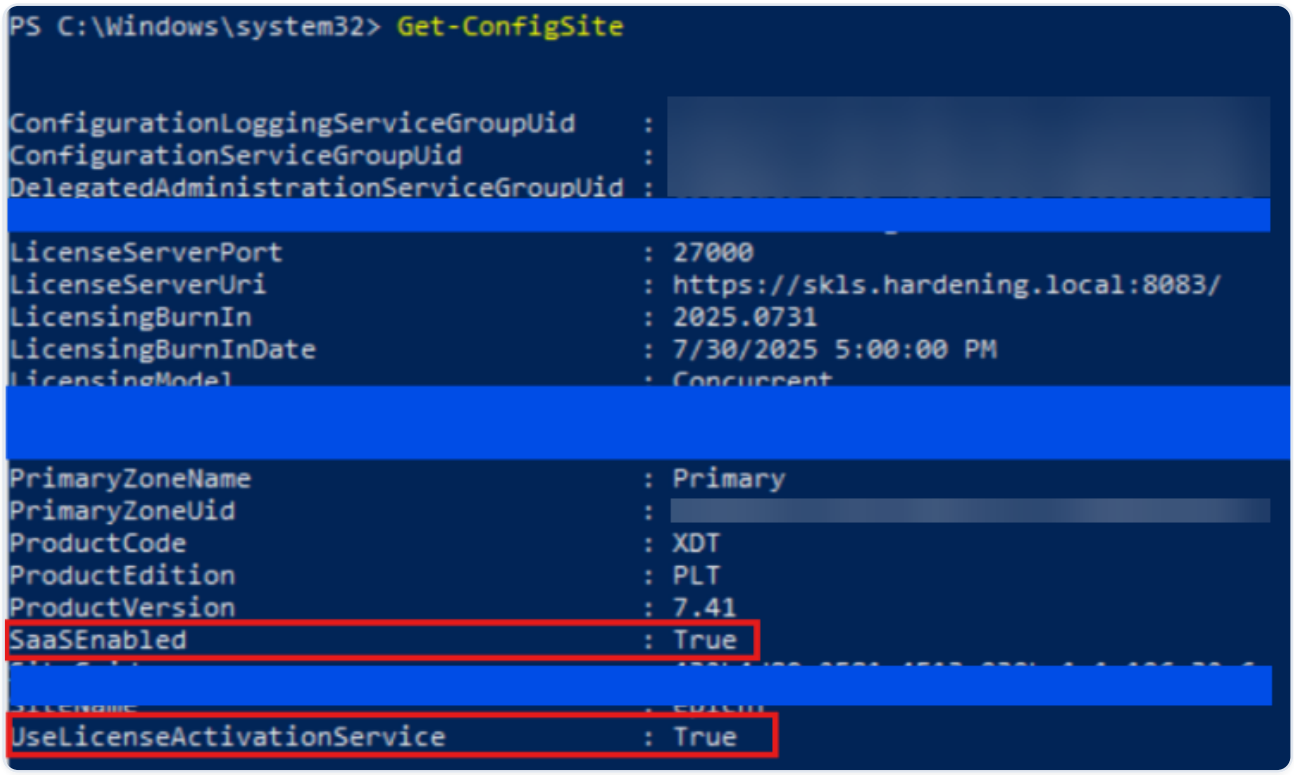
これらのメッセージの表示タイミングは、ライセンスの種類とインストールされているCitrix Virtual Apps and Desktopsのバージョンによって異なります。

オンプレミスサブスクリプションライセンス

- エンドユーザー警告: サブスクリプションの有効期限が切れた後、猶予期間中に表示されます。
- 管理者警告: サブスクリプションの有効期限が切れる30日前にStudioに表示されます。
- サポートされているバージョン:
  - 現在のリリース: Citrix Virtual Apps and Desktops 2411以降。
  - LTSR: 2203 CU6、2402 CU1、およびそれ以降のLTSRリリース

サイトのLAS状態を確認するにはどうすればよいですか?

LASアクティベーション状態とSaaSビットステータスを確認するには、`Get-configsite` を実行します。



サイトがライセンスキャッシュモードになっているか確認するにはどうすればよいですか?

キャッシュモードと残り時間の詳細を取得するには、`Get-Brokercontroller`と`Get-brokersite`を実行します。

- `Get-Brokercontroller`出力：

  Get-Brokercontroller コマンドの画像 (/en-us/citrix-virtual-apps-desktops/2503/media/get-broker-controller-brk-cmnd.png)

- `Get-brokersite`出力：

  Get-brokersite コマンドの画像 (/en-us/citrix-virtual-apps-desktops/2503/media/get-brk-site-brk-cmnd.png)

コマンドの詳細については、以下を参照してください。

- Get-BrokerController
- Get-ConfigSite

ライセンスに関するDelivery Controllerのイベントビューアーログについては、ライセンスイベントに関連するイベントビューアーログ を参照してください。

ユーザー/デバイスライセンス

Citrixは、ユーザー/デバイスライセンスモデルでユーザーにライセンスをどのように割り当てますか?

ユーザー/デバイスライセンスモデルでは、ライセンスサーバーはライセンスを一意のユーザーIDに割り当てます。これにより、その単一ユーザーは無制限のデバイスから無制限の接続を行うことができます。ユーザーがデスクトップまたはデバイスに接続する場合、仮想デスクトップまたはアプリケーションにアクセスするには、そのユーザーに割り当てられた1つのライセンスが必要です。ライセンスサーバーまたはクラウドサービスがライセンスを割り当てます。これらのライセンスを手動で割り当てることはできません。ライセンスは共有デバイスではなく、ユーザーに割り当てられます。一度ライセンスが割り当てられると、90日間非アクティブになるまで、別のユーザーに割り当てることはできません。詳細については、ユーザー/デバイスライセンス を参照してください。

Citrixは、ユーザー/デバイスライセンスモデルにおいて、ライセンスデバイスをどのように定義しますか?

ライセンスデバイスには、一意のエンドポイントデバイスIDが必要です。ユーザー/デバイスモデルでは、デバイスとは、Citrix Virtual Apps and Desktopsのインスタンスにアクセスするために、個人が使用することを許可したあらゆる機器を指します。共有デバイスの場合、単一のCitrix

Virtual Apps and Desktopsユーザー/デバイスライセンスで、そのデバイスを共有する複数のユーザーをサポートできます。たとえば、共有デバイスは、教室のワークステーションや病院の臨床ワークステーションなどです。

シトリックス バーチャル デスクトップス スタンダード エディション の同時使用ライセンスをユーザー/デバイスモデルに変換できますか?

Citrix Virtual Desktops Standard Edition の同時接続ライセンスを Citrix Virtual Desktops Standard Edition のユーザー/デバイスライセンスに変換することはできません。同様に、Citrix Virtual Desktops Standard Edition のユーザー/デバイスライセンスを Citrix Virtual Desktops Standard Edition の同時接続ライセンスに変換することもできません。

Citrix Virtual Desktops Standard Edition の同時接続ライセンスをお持ちで、ユーザー/デバイスライセンスモデルをご希望の場合は、Citrix Virtual Apps and Desktops Advanced または Premium Edition のいずれかにアップグレードしてください。

元	STANDARD 同時接続へ	スタンダード ユーザー/デバイスへ	アドバンスト ユーザー/デバイスへ	プレミアムユーザー/デバイスへ
Citrix Virtual Desktops Standard Edition 同時接続ライセンス	N/A	同時接続からユーザー/デバイスへの変換は許可されていません	ライセンスモデルを変換することはできませんが、Citrix Virtual Apps and Desktops Advanced または Premium Edition にアップグレードすることはできます。	ライセンスモデルを変換することはできませんが、Citrix Virtual Apps and Desktops Advanced または Premium Edition にアップグレードすることはできます。
シトリックス バーチャル デスクトップ スタンダード エディション ユーザー/デバイス ライセンス	ユーザー/デバイスから同時接続への変換は許可されていません	該当なし	該当なし	該当なし

同時使用ライセンスとユーザー/デバイスライセンスの違い?

同時使用ライセンスは、デバイスの同時接続数に基づいています。同時使用ライセンスは、デバイスがアクティブな接続を確立している場合にのみ使用されます。接続が終了すると、同時使用ライセンスはすぐに使用可能なライセンスプールに戻されます。このライセンスモデルは、一時的な使用におすすめです。ユーザー/デバイスライセンスは一定期間リースされ、リース期間が終了するまで他のユーザーは利用できません。

ユーザー/デバイスモデルでは、同じ企業内でユーザーとデバイスの両方にライセンスを割り当てることができます?

はい、両方のタイプを同じ企業内で使用できます。ライセンスサーバーは、使用状況に基づいてユーザーまたはデバイスにライセンスを最適に割り当てます。これらのライセンスを手動で割り当てることはできません。

ライセンスを付与するユーザーまたはデバイスの数をどのように決定すればよいですか?

適切なライセンス数を決定するために、ユースケースの要件を評価してください。ユーザー/デバイスライセンスは、無制限のデバイスから無制限の仮想デスクトップと仮想アプリへの無制限のアクセスを可能にします。同時使用ライセンスは、無制限のユーザーが使用できる単一のデバイスから無制限の仮想デスクトップと仮想アプリへの無制限のアクセスを可能にします。次の式を考慮してください。

```
(Number of total users) – (number of users that only access exclusively

 with shared devices) + (number shared devices) = total number

 of licenses to buy.



For example, there are 1000 total users at the hospital. If 700 of them
access only

Citrix Virtual Desktops from 300 shared devices in the hospital, the
number of

licenses to purchase is 1000 – 700 + 300 = 600 licenses.
```

ユーザー/デバイスモデルでは、ライセンスユーザーが自分の環境に接続するために使用できるデバイスの最大数?

各ライセンスユーザーは、接続されているデバイスまたはオフラインのデバイスを無制限に使用できます。

ユーザー/デバイスモデルでは、ライセンスデバイスにアクセスできるユーザーの最大数?

各ライセンスデバイスは、組織内で無制限のユーザーにサービスを提供できます。

ユーザー/デバイスモデルでは、ライセンスユーザーが一度に利用できる仮想デスクトップまたはRBI Webアプリケーションの最大数?

各ライセンスユーザーは、無制限の仮想デスクトップまたはWebアプリケーションに接続できます。

既存のCitrix Virtual Apps and Desktops環境で、ライセンスユーザー/デバイスの数を増やすためにCitrix Virtual Apps and Desktopsライセンスを購入できますか?

はい。既存のCitrix Virtual Apps and Desktops環境で、ライセンスユーザー/デバイスの数を増やすためにCitrix Virtual Apps and Desktopsライセンスを購入できます。

承認されたユーザー/デバイスライセンスを解放するにはどうすればよいですか?

承認済みユーザー/デバイスの割り当てを解放するには、EULAの条項に従って`udadmin`ユーティリティを使用します。その後、ライセンスサーバーは次の適切なユーザー/デバイスにライセンスを割り当てます。詳細については、「ユーザーまたはデバイスのライセンスの表示または解放」を参照してください。

購入したユーザー/デバイスライセンス数を超過した場合はどうなりますか?

ユーザー/デバイスライセンスには10%の超過分が含まれており、これはライセンス生成時に含まれます。この超過分は、インストール済みのライセンス数にも含まれます。使用量が超過分を含むインストール済みライセンス数を超えた場合、それ以上のユーザーのアクセスは拒否されます。より多くのユーザーのアクセスを有効にするには、新しいライセンスを購入して展開してください。

ライセンスの超過分を含め、すべてのライセンスが使用中の場合、ライセンスバーストモードにより製品への無制限の接続が可能になります。ライセンスバーストモードは、最大ライセンス数を超過した理由を特定し、ユーザーを中断することなく追加のライセンスを購入する時間を与えます。この期間は、15日が経過するか、追加のリテールライセンスをインストールするかのいずれか早い方まで続きます。詳細については、「ライセンスバーストモード」を参照してください。

Directorはライセンスキャッシュモードの状態を表示します。詳細については、「Directorダッシュボードのパネル」を参照してください。

ライセンスユーザーが一度に利用できる仮想アプリケーションの最大数?

各ライセンスユーザーは、無制限の仮想アプリケーションに接続できます。

ライセンスユーザーが組織を離れた場合?

既存のライセンスユーザーが組織を離れる場合、Citrixに通知することなく、そのユーザーのライセンスを解放できます。ライセンスを解放するには、`udadmin`ユーティリティを使用します。ライセンスを解放しない場合、ライセンスサーバーは90日間の非アクティブ状態の後、自動的にライセンスを解放します。この情報はEULAに規定されている条項に従います。

ライセンスユーザーが長期間不在の場合はどうなりますか?

既存のライセンスユーザーが長期間不在の場合、Citrix に通知することなくライセンスを解放し、再割り当てできるようにすることができます。ライセンスを解放するには、`udadmin` ユーティリティを使用します。

組織内でライセンスデバイスを交換した場合はどうなりますか?

既存のライセンスデバイスを交換する場合、Citrixに通知することなくライセンスを解放し、再割り当て可能にすることができます。ライセンスを解放するには、`udadmin`ユーティリティを使用します。

ライセンスデバイスが長期間サービス停止した場合、どうなりますか?

既存のライセンスデバイスが長期間サービス停止した場合、Citrixに通知することなくライセンスを解放し、再割り当て可能にすることができます。ライセンスを解放するには、`udadmin`ユーティリティを使用します。ライセンスを解放しない場合、ライセンスサーバーは90日間アクティビティがないライセンスを自動的に解放します。この情報は、EULAに規定されている条件に従います。

ライセンスをデバイスまたはユーザーに割り当てた後で、ユーザーライセンスをデバイスライセンスに、またはその逆に切り替えることはできますか?

はい、可能です。この変更は自動的に行われます。ライセンスサーバーは、使用パターンに基づいてユーザーまたはデバイスのいずれかにライセンスを割り当てます。使用パターンが変更された場合、ライセンスサーバーは新しい使用状況に基づいて割り当てを切り替えることがあります。ライセンスサーバーは常に、お客様にとって最も経済的な方法でライセンスを割り当てます。また、ライセンスサーバーは、90日間の割り当て期間が経過した後に**未使用**のライセンスを特定するためにライセンスを監視します。90日間の割り当て期間後に未使用と識別されたライセンスは、他のユーザーまたはデバイスに再割り当てできます。

同時使用ライセンス

同時使用モデルでは、Citrix Virtual Apps and Desktops のライセンスユーザーが一度に消費できる仮想デスクトップの最大数はいくつですか?

エンドポイントは多数のユーザーにサービスを提供でき、無制限の接続を許可します。

以前のバージョンの Citrix Virtual Apps and Desktops の同時使用ライセンスと、新しいユーザー/デバイスライセンスまたは同時使用ライセンスを、単一のライセンスサーバーに展開できます?

はい。同じライセンスサーバーを使用して、ユーザー/デバイスまたは同時使用ライセンスの展開をサポートし続けることができます。

単一のライセンスサーバーに、同時使用ライセンスとユーザー/デバイスライセンス、または同時使用ライセンスを展開できます?

はい。同じライセンスサーバーを使用して、同時使用およびユーザー/デバイスまたは同時使用ライセンスの展開をサポートし続けることができます。

Citrix Virtual Apps and Desktops AdvancedおよびPremiumエディションには、Citrix Virtual Appsの同時使用ライセンスが含まれていますか?

Citrix Virtual Apps and Desktops AdvancedおよびPremiumのユーザー/デバイスライセンスには、互換性のためのみにCitrix Virtual Appsの同時使用ライセンスが含まれています。これらの同時使用ライセンスは、ユーザー/デバイスライセンスと互換性のない以前の製品バージョンでのみ使用できます。ユーザー/デバイスライセンスに含まれる同時使用互換ライセンスの使用は、XenApp 6.5より前のバージョンおよびXenDesktop 5.0 Service Pack 1より前のバージョンでのみ許可されます。

購入した同時使用ライセンス数を超過した場合、どうなりますか?

すべてのライセンスが使用中の場合、ライセンスバーストモードにより、製品への無制限の接続が可能になります。ライセンスバーストモードは、最大ライセンス数を超過した理由を特定し、ユーザーに中断を与えることなく追加のライセンスを購入する時間を与えます。この期間は、15日が経過するか、追加の小売ライセンスをインストールするかのいずれか早い方まで続きます。詳細については、「ライセンスバーストモード」を参照してください。(/ja-jp/licensing/current-release/license-types.html#supplemental-grace-period).

Directorは猶予期間の状態を表示します。詳細については、「Directorダッシュボードのパネル」を参照してください。(/ja-jp/citrix-virtual-apps-desktops/2503/director/site-analytics.html#panels-on-the-director-dashboard).

超過ライセンス

超過ライセンスを取得するにはどうすればよいですか?

ユーザー/デバイス、ユーザー、またはデバイスライセンスモデルをサポートする製品（Citrix Cloudを除く）には、アクセス拒否を防ぐために限られた数の追加ライセンスを使用できるライセンス超過機能が含まれています。当社は、超過機能をライセンスの権利としてではなく、便宜のために提供しています。同時接続ライセンスおよびサーバーライセンスには超過機能は含まれていません。使用された超過ライセンスは、初回使用から30日以内に購入する必要がありますが、使用期間は30日に限定されません。Citrixは、新しい製品リリースで超過機能を削除する権利を留保します。詳細については、「ライセンス超過」を参照してください。(/ja-jp/licensing/current-release/license-types.html#license-overdraft).

ライセンス超過をどのように識別できますか?

Citrix Licensing Managerで、超過しているライセンス数を含む使用状況情報を表示できます。Studioにも超過使用状況情報が含まれています。

超過ライセンスが消費されるとどうなりますか?

Citrix Virtual Apps and Desktops環境へのアクセスを有効にするために、インストールされているライセンスからライセンスが割り当てられます。この超過ライセンスは、他のライセンスと同等のアクセスと機能を提供します。

超過ライセンスが消費されたときにアラートを受け取ることはできますか?

現在、オーバードラフトライセンスが消費されたときに提供される特定の警告はありません。

オーバードラフトライセンスはどのくらいの期間消費できます?

最初に使用してから30日以内に使用されたオーバードラフトライセンスを購入してください。

その他の製品固有のライセンス情報

- シトリックス ADC
- シトリックス クラウド
- シトリックス エンドポイント マネジメント
- シトリックス ゲートウェイ
- XenServer
- シトリックス ライセンシング

ローカルホストキャッシュ

Citrix Virtual Apps and Desktopsサイトデータベースが常に利用可能であることを保証するため、Citrixは、Microsoftの可用性の高いベストプラクティスに従い、フォールトトレラントなSQL Server展開から開始することを推奨します。(サポートされているSQL Serverの高可用性機能については、データベースを参照してください。) しかし、ネットワークの問題や中断により、ユーザーがアプリケーションやデスクトップに接続できなくなる可能性があります。

Local Host Cache機能により、障害発生時でもサイトでの接続仲介操作を続行できます。障害は、オンプレミスのCitrix®環境でDelivery Controller™とサイトデータベース間の接続が失敗した場合に発生します。Local Host Cacheは、サイトデータベースに90秒間アクセスできない場合に作動します。

XenAppおよびXenDesktop 7.16以降、接続リース機能（以前のリリースにおける先行の高可用性機能）は製品から削除され、利用できなくなりました。

データコンテンツ

Local Host Cacheには次の情報が含まれます。これはメインデータベースの情報の一部です。

- サイトから公開されたリソースへの権限が割り当てられているユーザーとグループのID。
- サイトから公開されたリソースを現在使用している、または最近使用したユーザーのID。
- サイトで構成されているVDAマシン（Remote PC Accessマシンを含む）のID。
- 公開されたリソースへの接続に積極的に使用されているクライアントCitrix Receiver™マシンのID（名前とIPアドレス）。

また、メインデータベースが利用できなかったときに確立された、現在アクティブな接続に関する情報も含まれます。

- Citrix Receiverによって実行されたクライアントマシンのエンドポイント分析の結果。
- サイトに関与するインフラストラクチャマシン（NetScaler GatewayやStoreFront™サーバーなど）のID。
- ユーザーによる最近のアクティビティの日時と種類。

動作の仕組み

以下の図は、通常の操作におけるローカルホストキャッシュのコンポーネントと通信パスを示しています。

ローカルホストキャッシュの通常の操作における通信パスの図(/en-us/citrix-virtual-apps-desktops/2503/media/lhc-normal1.png)

通常の操作時

- コントローラー上の *プリンシパルブローカー* (Citrix Broker Service) は、StoreFront からの接続要求を受け入れます。ブローカーはサイトデータベースと通信し、コントローラーに登録されている VDA とユーザーを接続します。
- Citrix Config Synchronizer Service (CSS) は、約5分ごとにブローカーに問い合わせて、変更があったかどうかを確認します。これらの変更は、管理者によって開始されたもの（デリバリーグループのプロパティの変更など）である場合もあれば、システムアクション（マシン割り当てなど）である場合もあります。
- 前回のチェック以降に構成変更があった場合、CSS は情報をコントローラー上のセカンダリブローカーに同期（コピー）します。（セカンダリブローカーは高可用性サービスとも呼ばれます。）

  前回のチェック以降に変更された項目だけでなく、すべての構成データがコピーされます。CSS は構成データをコントローラー上の Microsoft SQL Server Express LocalDB データベースにインポートします。このデータベースはローカルホストキャッシュデータベースと呼ばれます。CSS は、ローカルホストキャッシュデータベースの情報がサイトデータベースの情報と一致することを確認します。ローカルホストキャッシュデータベースは、同期が行われるたびに再作成されます。

  Microsoft SQL Server Express LocalDB（ローカルホストキャッシュデータベースで使用）は、コントローラーをインストールするときに自動的にインストールされます。（コマンドラインからコントローラーをインストールする際に、このインストールを禁止できます。）ローカルホストキャッシュデータベースは、複数のコントローラー間で共有することはできません。ローカルホストキャッシュデータベースをバックアップする必要はありません。構成変更が検出されるたびに再作成されます。
- 前回のチェック以降に変更がない場合、データはコピーされません。

以下の図は、プリンシパルブローカーがサイトデータベースとの接続を失った場合（障害が発生した場合）の通信パスの変化を示しています。

障害発生時のローカルホストキャッシュの通信パスの図(/en-us/citrix-virtual-apps-desktops/2503/media/lhc-outage1.png)

障害発生時

障害が発生すると：

- セカンダリブローカーは接続要求のリッスンと処理を開始します。

- 障害が発生すると、セカンダリブローカーは最新の VDA 登録データを持っていませんが、VDA がセカンダリブローカーと通信すると、登録プロセスがトリガーされます。そのプロセス中に、セカンダリブローカーはその VDA に関する現在のセッション情報も取得します。
- セカンダリブローカーが接続を処理している間、ブローカリングプリンシパルは引き続き接続を監視します。接続が復元されると、ブローカリングプリンシパルはセカンダリブローカーに接続情報のリスニングを停止するよう指示し、ブローカリングプリンシパルはブローカリング操作を再開します。次にVDAがブローカリングプリンシパルと通信するときに、登録プロセスがトリガーされます。セカンダリブローカーは、以前の停止から残っているVDA登録をすべて削除します。CSSは、展開で構成変更が発生したことを認識すると、情報の同期を再開します。

同期中に停止が開始されるという万が一の事態が発生した場合、現在のインポートは破棄され、最後に認識された構成が使用されます。

イベントログは、同期と停止に関する情報を提供します。

停止モードでの運用に時間制限はありません。

通常モードと停止モード間の移行は、既存のセッションには影響しません。新しいセッションの起動のみに影響します。

意図的に停止をトリガーすることもできます。その理由と方法の詳細については、「停止の強制」を参照してください。

複数のControllerがあるサイト

その他のタスクの中でも、CSSは、ゾーン内のすべてのコントローラーに関する情報をセカンダリブローカーに定期的に提供します。(展開に複数のゾーンが含まれていない場合、このアクションはサイト内のすべてのコントローラーに影響します。)その情報を持つことで、各セカンダリブローカーは、ゾーン内の他のコントローラーで実行されているすべてのピアセカンダリブローカーについて認識します。

セカンダリブローカーは、別のチャネルで相互に通信します。これらのブローカーは、実行されているマシンのFQDN名のアルファベット順リストを使用して、停止が発生した場合にゾーン内でブローカー操作を行うセカンダリブローカーを決定（選出）します。停止中、すべてのVDAは選出されたセカンダリブローカーに登録します。ゾーン内の選出されていないセカンダリブローカーは、受信接続およびVDA登録要求を積極的に拒否します。

停止中に選出されたセカンダリブローカーが失敗した場合、別のセカンダリブローカーが引き継ぐために選出され、VDAは新しく選出されたセカンダリブローカーに登録します。

停止中にControllerが再起動された場合：

- そのコントローラーが選出されたブローカーでない場合、再起動による影響はありません。
- そのコントローラーが選出されたブローカーである場合、別のコントローラーが選出され、VDAが登録されます。再起動されたコントローラーが起動すると、自動的にブローカリングを引き継ぎ、VDAが再度登録されます。このシナリオでは、登録中にパフォーマンスが影響を受ける可能性があります。

通常の操作中にコントローラーの電源をオフにし、停止中に電源をオンにした場合、そのコントローラーがブローカーとして選出された場合、そのコントローラーではローカルホストキャッシュを使用できません。

イベントログは、選出に関する情報を提供します。

停止中に利用できないもの、およびその他の違い

停止モードでの運用に時間制限はありません。ただし、Citrix は可能な限り迅速に接続を復元することを推奨します。

停止中：

- Studio を使用できません。
- PowerShell SDK へのアクセスが制限されます。
    - まず、次の操作を行う必要があります。
        - 値が1のレジストリキー `EnableCssTestMode` を追加します: `New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer\LHC -Name EnableCssTestMode -PropertyType DWORD -Value 1`
        - ポート89を使用します: `Get-BrokerMachine -AdminAddress localhost:89 | Select MachineName, ControllerDNSName, DesktopGroupName, RegistrationState`
    - これらのコマンドを実行すると、以下にアクセスできます。
        - すべての `Get-Broker*` コマンドレット。
- ハイパーバイザーの資格情報はホストサービスから取得できません。すべてのマシンは不明な電源状態になり、電源操作を発行できません。ただし、電源がオンになっているホスト上の VM は、接続要求に使用できます。
- 割り当てられたマシンは、通常の操作中に割り当てが行われた場合にのみ使用できます。停止中に新しい割り当てを行うことはできません。

- Remote PC Access マシンの自動登録と構成はできません。ただし、通常の操作中に登録および構成されたマシンは使用できます。
- サーバーでホストされているアプリケーションおよびデスクトップのユーザーは、リソースが異なるゾーンにある場合、構成されたセッション制限よりも多くのセッションを使用する可能性があります。
- ユーザーは、現在アクティブ/選出されているセカンダリブローカーを含むゾーン内の登録済みVDA からのみアプリケーションとデスクトップを起動できます。ゾーンをまたぐ起動（あるゾーンのセカンダリブローカーから別のゾーンの VDA への起動）は、停止中はサポートされません。
- 配信グループ内のVDAのスケジュールされた再起動が開始される前にサイトデータベースの停止が発生した場合、停止が終了したときに再起動が開始されます。これは意図しない結果を招く可能性があります。詳細については、「データベース停止により遅延するスケジュールされた再起動」を参照してください。
- ゾーンの優先順位は構成できません。構成されている場合、セッション起動時に優先順位は考慮されません。
- タグがゾーンの指定に使用されるタグ制限は、セッション起動ではサポートされていません。このようなタグ制限が構成されており、StoreFrontストアの高度なヘルスチェックオプションが有効になっている場合、セッションが断続的に起動に失敗する可能性があります。

アプリケーションとデスクトップのサポート

LHCは、次の種類のVDAと配信モデルをサポートしています。

VDAタイプ	配信モデル	LHCイベント中のVDAの可用性
マルチセッションOS	アプリケーションとデスクトップ	常に利用可能。
シングルセッションOS静的（割り当て済み）	デスクトップ	常に利用可能。
電源管理されたシングルセッションOSランダム（プール済み）	デスクトップ	デフォルトでは利用できません。プールされたデリバリーグループ内の電源管理されたVDAへのすべてのセッション起動

VDAタイプ	配信モデル	LHCイベント中のVDAの可用性	
		試行は、デフォルトで失敗します。LHCイベント中に新しい接続でそれらを利用可能にすることができます。詳細については、Web Studioを使用した有効化およびPowerShellを使用した有効化を参照してください。 **重要:** 電源管理されたシングルセッションのプールされたマシンへのアクセスを有効にすると、以前のユーザーセッションからのデータや変更が後続のセッションに存在する可能性があります。	

注:

プールされたデリバリーグループ内の電源管理されたデスクトップVDAへのアクセスを有効にしても、通常の操作中に構成された`ShutdownDesktopsAfterUse`プロパティの動作には影響しません。LHC中にこれらのデスクトップへのアクセスが有効になっている場合、LHCイベントが完了してもVDAは自動的に再起動しません。プールされたデリバリーグループ内の電源管理されたデスクトップVDAは、VDAが再起動するまで以前のセッションからのデータを保持できます。VDAの再起動は、ユーザーが非LHC操作中にVDAからログオフした場合、または管理者がVDAを再起動した場合に発生する可能性があります。

Web Studioを使用して、電源管理されたシングルセッションOSプールVDAのLHCを有効にする

Web Studioを使用して、LHCイベント中にデリバリーグループごとにそれらのマシンを新しい接続で利用可能にすることができます。

- デリバリーグループ作成中にこの機能を有効にするには、デリバリーグループの作成を参照してください。
- 既存のデリバリーグループでこの機能を有効にするには、デリバリーグループの管理を参照してください。

> **注:**
>
> この設定は、電源管理されたVDAを提供するプールされたデスクトップデリバリーグループに対してのみ、Web Studioで利用可能です。

PowerShellを使用して、電源管理されたシングルセッションOSのプールされたVDAに対してLHCを有効にする

特定のデリバリーグループ内のVDAに対してLHCを有効にするには、以下の手順に従います。

1. このコマンドを実行して、サイトレベルでこの機能を有効にします。

   ```
   Set-BrokerSite -ReuseMachinesWithoutShutdownInOutageAllowed $true
   ```

2. デリバリーグループ名を指定してこのコマンドを実行し、デリバリーグループのLHCを有効にします。

   ```
   Set-BrokerDesktopGroup -Name "name" -ReuseMachinesWithoutShutdownInOutage $true
   ```

新しく作成された電源管理VDAを持つプール型デリバリーグループのデフォルトのLHC可用性を変更するには、次のコマンドを実行します。

```
Set-BrokerSite -DefaultReuseMachinesWithoutShutdownInOutage $true
```

RAM サイズに関する考慮事項

LocalDBサービスは、約1.2 GBのRAMを使用できます（データベースキャッシュに最大1 GB、SQL Server Express LocalDBの実行に200 MB）。セカンダリブローカーは、多くのログオンが発生する長時間の停止（たとえば、10,000ユーザーで12時間）が続く場合、最大1 GBのRAMを使用

できます。これらのメモリ要件は、コントローラーの通常のRAM要件に追加されるため、RAM容量の合計を増やす必要がある場合があります。

サイトデータベースにSQL Server Expressインストールを使用している場合、サーバーには2つのsqlserver.exeプロセスがあります。

CPU コアとソケット構成に関する考慮事項

コントローラーのCPU構成、特にSQL Server Express LocalDBで利用可能なコア数は、メモリ割り当てよりもさらに、ローカルホストキャッシュのパフォーマンスに直接影響します。このCPUオーバーヘッドは、データベースに到達できず、セカンダリブローカーがアクティブな停止期間中にのみ観測されます。

LocalDBは複数のコア（最大4つ）を使用できますが、単一のソケットに制限されています。ソケットを追加してもパフォーマンスは向上しません（たとえば、各ソケットに1コアを持つ4ソケットの場合）。代わりに、Citrixは複数のソケットと複数のコアを使用することを推奨しています。Citrixのテストでは、2x3（2ソケット、3コア）構成が4x1および6x1構成よりも優れたパフォーマンスを提供しました。

ストレージに関する考慮事項

ユーザーが障害中にリソースにアクセスすると、LocalDB は増大します。たとえば、1 秒あたり 10 回のログオンで実行されるログオン/ログオフ テスト中に、データベースは 2 ～ 3 分ごとに 1 MB 増加しました。通常の操作が再開されると、ローカル データベースが再作成され、スペースが返されます。ただし、障害中のデータベースの増大を許容するために、LocalDB がインストールされているドライブには十分な空き容量が必要です。ローカル ホスト キャッシュは、障害中にさらに多くの I/O を発生させます。具体的には、1 秒あたり約 3 MB の書き込みと、数十万回の読み取りが発生します。

パフォーマンスに関する考慮事項

障害発生中は、1 つのセカンダリ ブローカーがすべての接続を処理するため、通常の操作中に複数のコントローラー間で負荷分散を行うサイト（またはゾーン）では、選出されたセカンダリ ブローカーが障害中に通常よりもはるかに多くの要求を処理する必要がある場合があります。したがって、CPU の要求は高くなります。障害中に選出されるセカンダリ ブローカーは変更される可能性があるため、サイト（ゾーン）内のすべてのセカンダリ ブローカーは、ローカル ホスト キャッシュ データベースと影響を受けるすべての VDA によって課される追加の負荷を処理できる必要があります。

VDI の制限：

- シングルゾーン VDI 展開では、障害発生時に最大 10,000 台の VDA を効果的に処理できます。
- マルチゾーン VDI 展開では、障害発生時に各ゾーンで最大 10,000 台の VDA を効果的に処理でき、サイト全体では最大 40,000 台の VDA を処理できます。たとえば、以下の各サイトは障害発生時に効果的に処理できます。
  - 4 つのゾーンがあり、それぞれに 10,000 台の VDA が含まれるサイト。
  - 7 つのゾーンがあり、1 つのゾーンに 10,000 台の VDA、残りの 6 つのゾーンにそれぞれ 5,000 台の VDA が含まれるサイト。

障害発生中は、サイト内の負荷管理が影響を受ける可能性があります。負荷評価機能（特にセッション数ルール）が超過する可能性があります。

すべての VDA がセカンダリ ブローカーに登録されるまでの間、そのサービスは現在のセッションに関する完全な情報を持っていない可能性があります。そのため、その期間中のユーザー接続要求は、既存のセッションへの再接続が可能であったとしても、新しいセッションが起動される結果となる可能性があります。この間隔（「新しい」セカンダリ ブローカーが再登録中にすべての VDA からセッション情報を取得する間）は避けられません。障害開始時に接続されているセッションは移行期間中に影響を受けませんが、新しいセッションやセッションの再接続は影響を受ける可能性があります。

この間隔は、VDA が登録する必要がある場合に発生します。

- 障害の開始時：プライマリ ブローカーからセカンダリ ブローカーに移行する場合。
- 障害中のセカンダリ ブローカーの障害：障害が発生したセカンダリ ブローカーから新しく選出されたセカンダリ ブローカーに移行する場合。
- 障害からの復旧時：通常の操作が再開され、プライマリ ブローカーが制御を再開する場合。

Citrix Broker Protocolの`HeartbeatPeriodMs`レジストリ値（デフォルト = 600000 ms、つまり10分）を下げることで、間隔を短縮できます。このハートビート値は、VDAがpingに使用する間隔の2倍であるため、デフォルト値では5分ごとにpingが実行されます。

たとえば、次のコマンドはハートビートを5分（300000ミリ秒）に変更し、2.5分ごとにpingが実行されるようにします。

```
New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer -Name HeartbeatPeriodMs -PropertyType DWORD –Value 300000
```

ハートビート値を変更する際は注意してください。頻度を上げると、通常モードと停止モードの両方でControllerへの負荷が増大します。

VDAがどれだけ迅速に登録されても、この間隔を完全に排除することはできません。

セカンダリブローカー間の同期にかかる時間は、オブジェクト（VDA、アプリケーション、グループなど）の数が増えるにつれて長くなります。例えば、5000のVDAを同期するには10分以上かかる場合があります。

XenApp 6.xリリースとの違い

このローカルホストキャッシュの実装は、XenApp 6.xおよびそれ以前のXenAppリリースにおけるローカルホストキャッシュ機能と同じ名前を共有していますが、大幅な改善が施されています。この実装は、より堅牢で破損の影響を受けません。定期的な`dsmaint`コマンドの必要性を排除するなど、メンテナンス要件が最小限に抑えられています。このローカルホストキャッシュは、技術的には全く異なる実装です。

ローカルホストキャッシュの管理

ローカルホストキャッシュが正しく機能するには、各ControllerのPowerShell実行ポリシーをRemoteSigned、Unrestricted、またはBypassに設定する必要があります。

SQL Server エクスプレス ローカルDB

ローカルホストキャッシュが使用するMicrosoft SQL Server Express LocalDBソフトウェアは、Controllerをインストールするか、バージョン7.9より前のControllerをアップグレードすると自動的にインストールされます。セカンダリブローカーのみがこのデータベースと通信します。PowerShellコマンドレットを使用してこのデータベースに関する何も変更することはできません。LocalDBはController間で共有できません。

SQL Server Express LocalDBデータベースソフトウェアは、ローカルホストキャッシュが有効になっているかどうかに関係なくインストールされます。

そのインストールを防ぐには、`XenDesktopServerSetup.exe`コマンドを使用してControllerをインストールまたはアップグレードし、`/exclude "Local Host Cache Storage (LocalDB)"`オプションを含めます。ただし、ローカルホストキャッシュ機能はデータベースなしでは機能せず、セカンダリブローカーで別のデータベースを使用することはできないことに注意してください。

このLocalDBデータベースのインストールは、サイトデータベースとして使用するためにSQL Server Expressをインストールするかどうかには影響しません。

以前のSQL Server Express LocalDBバージョンを新しいバージョンに置き換える方法については、「Replace SQL Server Express LocalDB」を参照してください。

製品のインストールとアップグレード後のデフォルト設定

Citrix Virtual Apps and Desktops（最小バージョン7.16）の新規インストール中に、ローカルホストキャッシュが有効になります。

アップグレード後（バージョン7.16以降）、展開全体で10,000未満のVDAがある場合、ローカルホストキャッシュが有効になります。

ローカルホストキャッシュの有効化と無効化

- ローカルホストキャッシュを有効にするには、次のように入力します。

  ```
  Set-BrokerSite -LocalHostCacheEnabled $true
  ```

  ローカルホストキャッシュが有効になっているかどうかを確認するには、`Get-BrokerSite`と入力します。`LocalHostCacheEnabled`プロパティが`True`であることを確認します。
- ローカルホストキャッシュを無効にするには、次のように入力します。

  ```
  Set-BrokerSite -LocalHostCacheEnabled $false
  ```

注意：XenAppおよびXenDesktop 7.16以降、接続リース（バージョン7.6以降のローカルホストキャッシュに先行する機能）は製品から削除され、利用できなくなりました。

ローカルホストキャッシュが機能していることを確認する

ローカルホストキャッシュが正しく設定され、機能していることを確認するには：

- 同期インポートが正常に完了していることを確認します。イベントログを確認してください。
- 各Delivery ControllerでSQL Server Express LocalDBデータベースが作成されていることを確認します。これにより、必要に応じてセカンダリブローカーが引き継ぐことができることが確認されます。
  - Delivery Controllerサーバーで、`C:\Windows\ServiceProfiles\NetworkService`に移動します。
  - `HaDatabaseName.mdf`と`HaDatabaseName_log.ldf`が作成されていることを確認します。
- Delivery ControllerでForce an outageを実行します。ローカルホストキャッシュが機能することを確認したら、すべてのControllerを通常モードに戻すことを忘れないでください。これには約15分かかる場合があります。

イベントログ

イベントログは、同期と停止が発生した時期を示します。イベントビューアーログでは、停止モードは *HA モード* と呼ばれます。*

設定同期サービス:

通常の操作中、CSSがLocal Host Cacheブローカーを使用して構成データをLocal Host Cacheデータベースにインポートすると、次のイベントが発生する可能性があります。

- 503: Citrix Config Sync Serviceが更新された構成を受信しました。このイベントは、同期プロセスの開始を示します。
- 504: Citrix Config Sync Serviceが更新された構成をインポートしました。構成のインポートは正常に完了しました。
- 505: Citrix Config Sync Serviceがインポートに失敗しました。構成のインポートは正常に完了しませんでした。以前に成功した構成が利用可能な場合、停止が発生したときにそれが使用されます。ただし、それは現在の構成から古くなります。以前の構成が利用できない場合、サービスは停止中にセッションブローカーに参加できません。この場合、Troubleshootセクションを参照し、Citrixサポートに連絡してください。
- 507: システムが停止モードであり、Local Host Cacheブローカーがブローカー処理に使用されているため、Citrix Config Sync Serviceはインポートを中止しました。サービスは新しい構成を受信しましたが、停止が発生したためインポートは中止されました。これは予期される動作です。
- 510: プライマリConfiguration ServiceからConfiguration Service構成データが受信されませんでした。
- 517: プライマリBrokerとの通信に問題がありました。
- 518: セカンダリBroker (High Availability Service) が実行されていないため、Config Syncスクリプトは中止されました。

高可用性サービス:

このサービスは、ローカルホストキャッシュブローカーとも呼ばれます。

- 3502: 停止が発生し、ローカルホストキャッシュブローカーが仲介操作を実行しています。
- 3503: 停止が解決され、通常の操作が再開されました。
- 3504: どのローカルホストキャッシュブローカーが選出されたか、および選出に関与した他のローカルホストキャッシュブローカーを示します。

- 3507: 2分ごとにローカルホストキャッシュのステータス更新を提供し、選出されたブローカーでローカルホストキャッシュモードがアクティブであることを示します。停止期間、VDA登録、セッション情報を含む停止の概要が含まれます。
- 3508: 選出されたブローカーでローカルホストキャッシュがアクティブでなくなり、通常の操作が復元されたことを通知します。停止期間、ローカルホストキャッシュイベント中に登録されたマシンの数、LHCイベント中の正常な起動の数を含む停止の概要が含まれます。
- 3509: 非選出ブローカーでローカルホストキャッシュがアクティブであることを通知します。2分ごとの停止期間が含まれ、選出されたブローカーを示します。
- 3510: 非選出ブローカーでローカルホストキャッシュがアクティブでなくなったことを通知します。停止期間が含まれ、選出されたブローカーを示します。

停止を強制する

意図的に停止を強制したい場合があります。

- ネットワークが繰り返し停止したり再開したりする場合。ネットワークの問題が解決されるまで停止を強制することで、通常モードと停止モード間の継続的な移行（およびそれに伴う頻繁なVDA登録ストーム）を防ぎます。
- 災害復旧計画をテストするため。
- ローカルホストキャッシュが正しく機能していることを確認するため。
- サイトデータベースサーバーの交換または保守中。

停止を強制するには、Delivery Controllerを含む各サーバーのレジストリを編集します。`HKLM\Software\Citrix\DesktopServer\LHC`で、`OutageModeForced`を`REG_DWORD`として`1`に作成して設定します。この設定により、データベースの状態に関係なく、ローカルホストキャッシュブローカーは停止モードに入ります。値を`0`に設定すると、ローカルホストキャッシュブローカーは停止モードを終了します。

イベントを確認するには、`C:\ProgramData\Citrix\WorkspaceCloud\Logs\Plugins\HighAvailabilityService`にある`Current_HighAvailabilityService`ログファイルを監視します。

トラブルシューティング

ローカルホストキャッシュデータベースへの同期インポートが失敗し、505イベントが投稿された場合、いくつかのトラブルシューティングツールが利用可能です。

CDFトレース: `ConfigSyncServer` および `BrokerLHC` モジュールのオプションが含まれています。これらのオプションは、他のブローカーモジュールとともに、問題を特定するのに役立つでしょう。

レポート: 同期インポートが失敗した場合、レポートを生成できます。このレポートは、エラーの原因となっているオブジェクトで停止します。このレポート機能は同期速度に影響するため、Citrixは使用しないときは無効にすることを推奨します。

CSSトレースレポートを有効にして生成するには、次のコマンドを入力します。

```
New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer\LHC -Name EnableCssTraceMode -PropertyType DWORD -Value 1
```

HTMLレポートは `C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\CitrixBrokerConfigSyncReport.htm` に投稿されます。

レポートが生成されたら、レポート機能を無効にするには次のコマンドを入力します。

```
Set-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer\LHC -Name EnableCssTraceMode -Value 0
```

ブローカー構成のエクスポート: デバッグ目的で正確な構成を提供します。

```
Export-BrokerConfiguration | Out-File <file-pathname>
```

たとえば、`Export-BrokerConfiguration | Out-File C:\\BrokerConfig.xml`。

ローカルホストキャッシュのPowerShellコマンド

PowerShellコマンドを使用して、Delivery Controllerでローカルホストキャッシュ (LHC) を管理できます。

PowerShellモジュールは、Delivery Controllerの次の場所にあります。

```
C:\Program Files\Citrix\Broker\Service\ControlScripts
```

> **重要:**
>
> このモジュールはDelivery Controllerでのみ実行してください。

PowerShell モジュールのインポート

モジュールをインポートするには、Delivery Controllerで次を実行します。

```
cd C:\Program Files\Citrix\Broker\Service\ControlScripts Import-Module .\HighAvailabilityServiceControl.psm1
```

LHC を管理するための PowerShell コマンド

以下のコマンドは、Delivery Controller で LHC モードをアクティブ化および管理するのに役立ちます。

コマンドレット	機能
`Enable-LhcForcedOutageMode`	BrokerをLHCモードにします。`Enable-LhcForcedOutageMode`が適切に機能するには、ConfigSyncサービスによってLHCデータベースファイルが正常に作成されている必要があります。このコマンドレットは、実行されたDelivery ControllerでのみLHCを強制します。LHCをアクティブにするには、このコマンドをゾーン内のすべてのDelivery Controllerで実行する必要があります。
`Disable-LhcForcedOutageMode`	BrokerをLHCモードから外します。このコマンドレットは、実行されたDelivery ControllerでのみLHCモードを無効にします。`Disable-LhcForcedOutageMode`は、ゾーン内のすべてのDelivery Controllerで実行する必要があります。
`Set-LhcConfigSyncIntervalOverride`	Citrix Config Synchronizer Service (CSS) がサイト内の構成変更をチェックする間隔を設定します。時間間隔は 60 秒 (1 分) から 3600 秒 (1 時間) の範囲で指定できます。この設定は、実行された Delivery Controller にのみ適用されます。Delivery Controller 間で一貫性を持たせるには、各 Delivery Controller でこのコマンドレットを実行することを検討してください。例: `Set-LhcConfigSyncIntervalOverride -Seconds 1200`
`Clear-LhcConfigSyncIntervalOverride`	Citrix Config Synchronizer Service (CSS) がサイト内の構成変更をチェックする間隔を、デ

コマンドレット	機能
	フォルト値の 300 秒 (5 分) に設定します。この設定は、実行された Delivery Controller にのみ適用されます。Delivery Controller 間で一貫性を持たせるには、各 Delivery Controller でこのコマンドレットを実行することを検討してください。
`Enable-LhcHighAvailabilitySDK`	実行された Delivery Controller 内のすべての `Get-Broker*` コマンドレットへのアクセスを有効にします。
`Disable-LhcHighAvailabilitySDK`	実行された Delivery Controller 内の Broker コマンドレットへのアクセスを無効にします。

注:

- Delivery Controller で `Get-Broker*` コマンドレットを実行するときは、ポート 89 を使用します。例:
  - `Get-BrokerMachine -AdminAddress localhost:89`
- LHC モードでない場合、Delivery Controller 上の LHC Broker は構成情報のみを保持します。
- LHC モード中、選出された Delivery Controller 上の LHC Broker は次の情報を保持します。
  - リソースの状態
  - セッションの詳細
  - VDA登録
  - 構成情報

検索を使用してマシンとセッションを監視および管理する

注:

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

特定のマシン、セッション、マシンカタログ、アプリケーション、またはデリバリーグループに関する情報を表示するには、検索機能を使用します。Web Studioで**検索**を選択すると、いくつかのオプションが表示されます。

- タブを使用して、マシンを種類（シングルセッションまたはマルチセッションOS）別に一覧表示するか、すべてのセッションを一覧表示します。
- 検索ボックスに名前を入力します。入力すると、クイック検索用のフィルターが提供されます。
- フィルターを使用して検索を絞り込みます。
    - デフォルトでは、次のフィルターがビューに固定されています：**名前**、**セッション状態**、**障害状態**。フィルターを選択して式を作成します。フィルターをカスタマイズするには、省略記号をクリックします。表示されるウィンドウで、次のことができます。
        - フィルターを固定または固定解除します。固定解除されたフィルターは一度限りの使用であり、保存されません。
        - フィルターをクリックしてビューに追加します。
        - フィルターをクリアして、現在のフィルター検索をクリアし、固定解除されたフィルターを削除します。

吹き出し	領域	説明
A	検索バー	クイック検索と、複雑な検索条件を定義できるフィルターベースの検索を提供します。詳細については、「インスタンスの検索」を参照してください。
B	タイプタブ	マシンを種類別に一覧表示したり、すべてのセッションを一

吹き出し	領域	説明
		覧表示したりするためのタブが表示されます。インスタンス数はタブ名に表示されます。
C	インスタンスレベルのアクション	*選択したインスタンス*（マシンまたはセッション）に対して実行できるアクションが表示されます。詳細については、マシンアクションおよびセッションアクションを参照してください。
D	リストレベルのアクション	現在の*リスト*に対して実行できるアクションが表示されます。 • **エクスポート**アイコン: メインビューに表示されているインスタンスのリストをCSVファイルにエクスポートします。 • **表示する列**アイコン: リストのメインビューをカスタマイズします。 • **エラー** ラベル: このラベルを有

吹き出し	領域	説明	
		効にすると、メインビューにエラーのある未登録のマシンのみが表示されます。問題の詳細を表示するには、「**詳細**」ペインの「**トラブルシューティング**」タブに移動します。 • **警告** ラベル: このラベルを有効にすると、メインビューに警告のある未登録のマシンのみが表示されます。問題の詳細を表示するには、「**詳細**」ペインの「**トラブルシューティング**」タブに移動します。	
E	メインビュー	インスタンスとそのプロパティを表示します。「**表示する列**」アイコンを選択して、メインビューをカスタマイズできます。利用可能な列の詳細については、マシン列およびセッ	

吹き出し	領域	説明
		ション列を参照してください。
F	詳細ペイン	次の詳細が表示されます: • 選択したインスタンス（マシンまたはセッション）の詳細 • 選択したマシンに適用されているタグ • 選択したマシンに関するエラーまたは警告の詳細。問題、考えられる原因、推奨される解決策が含まれます。

フィルターセットを管理(/en-us/citrix-virtual-apps-desktops/2503/media/manage-filter-sets.png)

フィルターなしで検索

- フィルターを使用した検索
- クイック検索のために現在のフィルターセットを保存する
- 検索バーにフィルターフィールドをピン留めする
- クイック検索ボックスを使用した検索
- 検索を強化するためのヒント
- VM01 名前。名前で検索します。
- VM01 マシンカタログ。名前で検索します。
- VM01デリバリーグループ。デリバリーグループ名で検索します。

たとえば、*静的でユーザーに割り当てられている*すべてのシングルセッションOSマシンを検索するには、次の手順に従います。

1. On the **シングルセッションOSマシン**タブで、**フィルター**アイコンをクリックします。フィルターパネルが表示されます。

ユーザー、デスクトップグループ、カタログ、マシンなどの特定の項目を検索する場合、一般的な検索は必要な情報を見つける便利な方法を提供します。

マシンカタログまたはデリバリーグループの検索

1. 検索で、すべてのフィルター条件に一致する結果を返すようにしたい場合は、「**すべて一致**」(AND演算子)を選択します。検索で、いずれかのフィルター条件に一致する結果を返すようにしたい場合は、「**いずれか一致**」(OR演算子)を選択します。
2. 「**適用**」をクリックします。

- **カタログ名**。マシンカタログの名前で検索します。
- **割り当ての種類**。静的（専用）またはランダム（プール）割り当て、あるいはその両方でフィルターします。
- **プロビジョニングの種類**。手動またはMCSプロビジョニング方法、あるいはその両方でフィルタリングします。
- **セッションサポート**。シングルセッションまたはマルチセッションマシン、あるいはその両方でフィルタリングします。
- **割り当て済み数**。割り当て済みマシンの数でフィルタリングします。
- **永続性**。非永続的（破棄）または永続的（ローカルディスク上）なマシン変更、あるいはその両方でフィルタリングします。
- **マシンの種類**。物理マシンまたは仮想マシンの種類、あるいはその両方でフィルタリングします。

デリバリーグループでは、次のフィルターが利用可能です。

- **グループ名**。デリバリーグループの名前で検索します。
- **説明**。デリバリーグループ作成時に指定されたデリバリーグループの説明でフィルタリングします。
- **セッションサポート**。シングルセッションまたはマルチセッションマシン、あるいはその両方でフィルタリングします。
- **マシンID**。マシンのIDでフィルタリングします。
- **リモートPCアクセス**。リモートPCアクセス マシンでフィルタリングします。

- **メンテナンスモード**。メンテナンスモードのマシン（オン、オフ、またはその両方）でフィルタリングします。
- **グループの状態**。グループの状態によってフィルタリングします。（> の オプションは、アプリケーションとデスクトップの配信を停止するかどうかを制御します。）
- **割り当ての種類**。静的（専用）またはランダム（プール）の種類、あるいはその両方でフィルタリングします。

1. フィルターベースの検索を実行した後、前の図に示すように、検索バーの「**星**」アイコンをクリックします。
2. 表示されるページで、このフィルターセットの名前を入力します (例: *静的および割り当て済みマシン*)。
3. 「**保存**」をクリックします。

   検索ボックスをクリックすると、保存されたフィルターセットが検索履歴リストに表示されます。

   - 名前: フォルダーパスを含む名前でマシンカタログを検索します。
   - マシンカタログ: 名前でマシンカタログを検索します。
   - 説明。カタログ作成時に指定されたマシンカタログの説明で検索します。

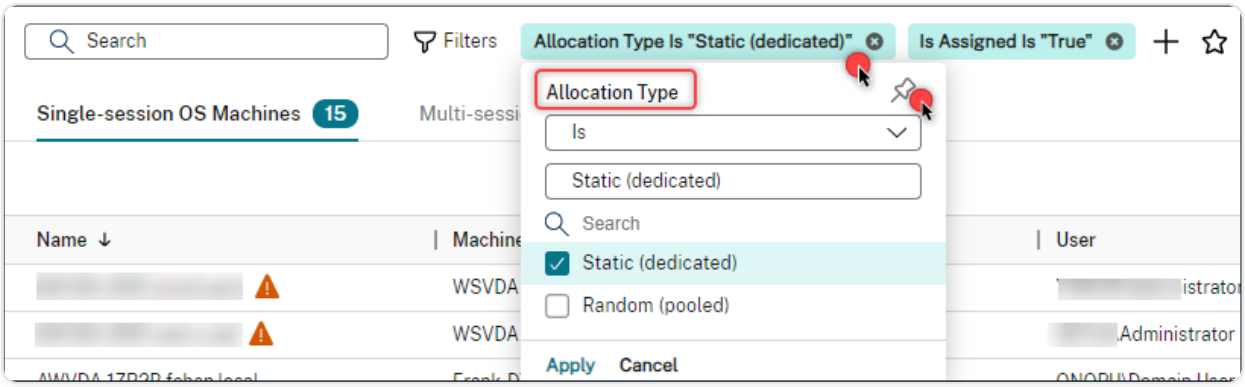
> **注:**
>
> フィルターセットはユーザーアカウントごとに保存されます。保存されたフィルターセットを管理するには、「**管理**」を選択します。

検索バーにフィルターフィールドをピン留めする

頻繁に使用するフィルター *フィールド*を検索バーにピン留めすると、簡単にアクセスできます。たとえば、フィルターベースの検索を実行した後、「**割り当ての種類**」を検索バーにピン留めしたいとします。次の手順に従います。

アプリケーショングループに対して、一般的な検索とフィルターベースの検索を実行できます。アプリケーショングループでは、次のフィルターが利用可能です:

1. 表示されるパネルで、**ピン**アイコンをクリックして、フィルターフィールド（この例では*割り当ての種類*）を検索バーにピン留めします。



表示する列をカスタマイズする

クイック検索ボックスを使用すると、名前関連のプロパティまたは保存されたフィルターセットに基づいてインスタンスを検索するのに便利です。詳細な手順は次のとおりです。

カスタマイズにパフォーマンスを低下させる列が含まれている場合、それらを保持するかどうかを決定するよう求められます。このプロンプトは、ブラウザウィンドウを更新するか、コンソールからサインアウトして再度サインインした後に表示されます。列を保持することを決定した場合は、以下の考慮事項に注意してください。

1. 新しい検索を開始するには、次のオプションから完全な名前または部分的な名前を入力します。

検索結果をCSVファイルにエクスポートする

検索結果（最大10,000項目）をCSVファイルにエクスポートできます。ファイルはブラウザのデフォルトのダウンロード場所に保存されます。

この機能は、マシンとセッションの両方で利用できます。検索結果をエクスポートするには、右上隅のエクスポートアイコンをクリックします。エクスポートの完了には最大1分かかる場合があります。

検索ノードの各タブで、エクスポートが進行中の間は、別のエクスポートを実行できません。

検索を強化するためのヒント

検索機能を使用する際は、次のヒントを考慮してください。

- 「**検索**」ノードで、項目を並べ替えるには、任意の列を選択します。

- 検索および並べ替えが可能な表示に含める特性をさらに表示するには、「**表示する列**」を選択するか、任意の列をクリックして「**表示する列**」を選択します。「**表示する列**」ウィンドウで、表示する項目の横にあるチェックボックスをオンにし、「**保存**」を選択して終了します。

  > **注:**
  >
  > 性能を低下させる項目には、**性能を低下させる**というラベルが付けられています。

- マシンに接続されているユーザーデバイスを見つけるには、「**クライアント (IP)**」と「**は**」を使用し、デバイスのIPアドレスを入力します。
- アクティブなセッションを見つけるには、「**セッション状態**」、「**は**」、および「**接続済み**」を使用します。
- デリバリーグループ内のすべてのマシンを一覧表示するには、左ペインで「**デリバリーグループ**」を選択します。グループを選択し、アクションバーまたはコンテキストメニューから「**マシンの表示**」を選択します。

並べ替え操作を実行する際は、以下の考慮事項を念頭に置いてください。

- 項目の数が5,000を超えない限り、任意の列をクリックして項目を並べ替えることができます。数が5,000を超えると、名前または現在のユーザー（現在表示しているタブによって異なります）でのみ並べ替えることができます。並べ替えを有効にするには、フィルターを使用して項目の数を5,000以下に減らします。
- アイテム数が500より多く、5,000以下の場合:
  - 並べ替えのパフォーマンスを向上させるために、すべてのデータをローカルにキャッシュします。「**シングルセッションOSマシン**」タブと「**マルチセッションOSマシン**」タブでは、列（「**名前**」列を除く任意の列）をクリックして並べ替える最初のときにデータをキャッシュします。「**セッション**」タブでは、列（「**現在のユーザー**」列を除く任意の列）をクリックして並べ替える最初のときにデータをキャッシュします。その結果、並べ替えの完了に時間がかかります。パフォーマンスを高速化するには、名前または現在のユーザーで並べ替えるか、フィルターを使用して項目の数を減らします。
  - テーブルの下に表示される次のメッセージは、データがキャッシュされていることを示します: 最終更新: `<the time when you refreshed the table>`。この場合、並べ替え操作は以前に読み込まれた項目に基づいています。これらの項目は最新ではない可能性があります。最新の状態にするには、更新アイコンをクリックします。

表示する列をカスタマイズする

日常業務に不可欠なプロパティとステータスを表示するパーソナライズされたメインビューを作成します。詳細な手順は次のとおりです。

1. 「**検索**」ノードで、必要に応じて「**マルチセッションOSマシン**」、「**シングルセッションOSマシン**」、または「**セッション**」タブを選択します。
2. アクションバーの**表示する列**アイコンをクリックし、列を選択します。

   利用可能な列とその説明の詳細については、「マシン列」および「セッション列」を参照してください。

列を選択する際、**パフォーマンスが低下します**というラベルが付いた列が表示されることがあります。これらの列を選択すると、コンソールのパフォーマンスが低下する可能性があります。以下の点を考慮してください。

- カスタマイズが完了すると、選択した列を表示するためにテーブルが更新されます。これらの列が存在すると、テーブルの更新時に遅延が発生する可能性があります。
- ブラウザを更新するか、コンソールからサインアウトして再度サインインすると、それらの列を保持するかどうかを尋ねるメッセージが表示されます。保持することを選択した場合、最適なコンソールパフォーマンスを維持するために、テーブルの更新は1分間に1回までに制限されます。より頻繁に更新するには、パフォーマンスを低下させる列を削除してください。

マシンとセッションの管理

検索ノードのアクションを使用して、マシンとセッションの問題をトラブルシューティングしたり、ユーザー要求を処理したりします。

知っておくと便利な情報

マシンはさまざまなレベルで管理できます。

- 個々のマシンレベル。**検索**ノードを使用して、ターゲットマシンを特定し、アクションを実行します。
- マシンカタログレベル。カタログのマスターイメージの変更、カタログからのマシンの削除、カタログへのマシンの追加などです。詳細については、「マシンカタログの管理」を参照してください。
- デリバリーグループレベル。グループ内のマシンのメンテナンスモードのオン/オフなどです。詳細については、「デリバリーグループの管理」を参照してください。

個々のセッションレベルに加えて、デリバリーグループレベルでもセッションを管理できます。たとえば、デリバリーグループのセッションの事前起動と維持を設定するなどです。詳細については、「デリバリーグループの管理」を参照してください。

マシンまたはセッションに対するアクションの実行

個々のインスタンスレベルでマシンまたはセッションを管理するには、次の手順に従います。

1. 「**検索**」ノードで、「**マルチセッションOSマシン**」、「**シングルセッションOSマシン**」、または「**セッション**」タブを選択します。
2. 必要に応じて、1つまたは複数のインスタンスを選択します。
3. アクションバーまたは右クリックメニューから、それらのインスタンスまたはユーザー要求で発生した問題に基づいてアクションを選択します。

   利用可能なアクションとその説明について詳しくは、「マシンアクション」および「セッションアクション」を参照してください。

> **注：**
>
> 2つ以上のインスタンスを選択した場合、それらすべてに適用されるアクションのみが利用可能です。

マシンまたはセッションデータをCSVファイルにエクスポートする

タブに表示されているインスタンス（マシンまたはセッション）のリスト（最大30,000項目）をCSVファイルにエクスポートします。詳細な手順は次のとおりです。

1. 「**検索**」ノードで、必要に応じて「**マルチセッションOSマシン**」、「**シングルセッションOSマシン**」、または「**セッション**」タブを選択します。
2. 右上隅にある「**エクスポート**」アイコンをクリックします。
3. 表示されるダイアログボックスで、「**続行**」をクリックします。

   エクスポートが完了するまでに数分かかる場合があります。ファイルはブラウザーのデフォルトのダウンロードフォルダーにあります。

> **注：**

> 「**検索**」ノードの各タブでは、エクスポートの進行中に別のエクスポートを実行することはできません。

マシンのアクションと列

この記事では、参照用にマシンのアクションと列を説明とともに示します。

アクション

マシンで実行できるアクションとその説明を表示します。

アクション	説明	適用対象
デリバリーグループから削除	デリバリーグループからマシンを削除します。	シングルセッションおよびマルチセッション
デリバリーグループに追加	マシンをデリバリーグループに追加します。	シングルセッションおよびマルチセッション
セッションの表示	マシンで実行中のセッションを表示します	シングルセッションおよびマルチセッション
タグの管理	マシンにタグを追加して管理します。タグの一般的な使用例について詳しくは、「タグ」を参照してください。	シングルセッションおよびマルチセッション
メンテナンスモードをオンにする	パッチを適用する前、またはトラブルシューティングのために、マシンをメンテナンスモードにします。 このモードでは、そのマシンへの新しい接続が防止されます。ユーザーはそのマシン上の既存のセッションに接続できますが、そのマシン上で新しいセッションを開始することはできません。	シングルセッションおよびマルチセッション
メンテナンスモードをオフにする	マシンのメンテナンスモードをオフにします。	シングルセッションおよびマルチセッション

アクション	説明	適用対象
VDAのアップグレード	マシンのVDAをアップグレードします。	特定の要件を満たすシングルセッションまたはマルチセッションOSマシン: 詳細はこちら。
ログオフ	マシンを強制的にログオフする	シングルセッションおよびマルチセッション
削除	ハイパーバイザーまたはクラウドサービス上でVMをそのまま残したまま、マシンカタログからVMを削除します。	シングルセッションおよびマルチセッション
ユーザーの変更	特定のユーザーにマシンを割り当てる。	シングルセッションの*静的*マシン。
起動	マシンを起動する。	シングルセッションおよびマルチセッション
シャットダウン	マシンをシャットダウンする。	シングルセッションおよびマルチセッション
再起動	マシンを再起動する	シングルセッションおよびマルチセッション
サスペンド	マシンを休止状態またはサスペンド状態にする。マシンをサスペンドすると、Delivery Controller はマシンのメモリ内容をファイルに保存し、マシンをシャットダウンします。	シングルセッションOSマシン
再開	サスペンドされたマシンを再開する。サスペンドされたマシンを再開すると、Delivery Controller はマシンを起動し、以前の状態に復元します。	シングルセッションOSマシン

アクション	説明	適用対象
強制再起動	マシンを強制的に再起動する。	シングルセッションOSマシン
強制シャットダウン	マシンを強制的にシャットダウンする。	シングルセッションOSマシン

列

すべてのマシン列とその説明を種類別に表示します。

- マシン
- マシンの詳細
- アプリケーション
- ホスティング
- 接続
- 登録
- セッションの詳細
- セッション

マシン

マシンカテゴリの列。

列	説明	適用対象
名前	マシンのDNSホスト名。	シングルセッションおよびマルチセッション
マシンカタログ	マシンが属するカタログの名前。	シングルセッションおよびマルチセッション
デリバリーグループ	マシンが属するデリバリーグループの名前。	シングルセッションおよびマルチセッション

列	説明	適用対象
ユーザー表示名	マシンに関連付けられているユーザーのフルネーム (通常、`Firstname Lastname`の形式)。関連付けられているユーザーとは、共有マシンの現在のユーザーと、専用マシンの割り当て済みユーザーです。	シングルセッションおよびマルチセッション
ユーザー	マシンに関連付けられているユーザーのユーザー名 (「domain\user」の形式)。関連付けられているユーザーとは、共有マシンの現在のユーザーと、専用マシンの割り当て済みユーザーです。	シングルセッションおよびマルチセッション
ユーザープリンシパル名	マシンに関連付けられているユーザーのユーザープリンシパル名（「user@domain」の形式）。関連付けられているユーザーとは、共有マシンの現在のユーザーと、専用マシンに割り当てられているユーザーです。	シングルセッションおよびマルチセッション
デスクトップ表示名	セッションの起動に元々使用されたマシンの公開名。Citrix Workspace™アプリまたはStoreFrontに	シングルセッションのみ

列	説明	適用対象
	表示される名前です。	
	注： デスクトップの表示を変更するには、**Perform Machine Update** 権限が必要です。表示名の変更には、マシンプロパティの更新が含まれるためです。	
デスクトップの状態	マシンに関する未解決のデスクトップ状態のリスト。可能な値：Unknown、CPU、ICALatency、UPMLogonTime。	シングルセッションおよびマルチセッション
割り当ての種類	マシンの割り当ての種類：ユーザーに永続的に割り当てられる場合は **Permanent**。ランダムに割り当てられる場合は **Random**。	シングルセッションおよびマルチセッション
メンテナンスモード	マシンがメンテナンスモードであるかどうかを示します。	シングルセッションおよびマルチセッション
Windows接続設定	Windowsによって報告されたログオンモード。	マルチセッションのみ
	指定可能な値: LogonEnabled、Draining、DrainingUntilRestart、LogonDisabled。	

列	説明	適用対象
割り当て済み	専用デスクトップがユーザーまたはクライアント（名前/アドレス）に割り当てられているかどうかを示します。ユーザーは明示的に割り当てるか、マシンを初めて使用する際に割り当てることができます。	シングルセッションおよびマルチセッション
物理	マシンが物理であるかどうかを示します。`True` はマシンが物理であることを示し、Delivery Controllerによって電源管理されていないことを意味します。`False` はその逆を示します。	シングルセッションおよびマルチセッション
プロビジョニングの種類	マシンがプロビジョニングされた方法。考えられる値 • 手動: PVSまたはMCSを使用してプロビジョニングされていません。 • PVS: PVSを使用してプロビジョニング済み(物理マシン、ブ	シングルセッションおよびマルチセッション

列	説明	適用対象	
	レードマシン、仮想マシン) • MCS: MCSを使用してプロビジョニング済み(VMのみ)		
スケジュールされた再起動	マシンに対してスケジュールされた再起動操作の状態。指定可能な値 • なし: 再起動はスケジュールされていません。 • 保留中: 再起動を待機中ですが、使用可能です。 • ドレイン中: 再起動を待機しており、新しいセッションには利用できません。ただし、既存の接続への再接続は引き続き許可されます。 • 進行中: スケジュールされた再起動がアクティブに進行中です。	シングルセッションおよびマルチセッション	

列	説明	適用対象
	• 自然: 自然な再起動が進行中です。マシンは再起動を待機しています。	
ゾーン	マシンが配置されているゾーンの名前。	シングルセッションおよびマルチセッション
状態	マシンに関連付けられているデスクトップの全体的な状態。これは、セッション状態、登録状態、電源状態など、さまざまな特定の状態から派生しています。	シングルセッションおよびマルチセッション
	可能な状態: オフ、未登録、利用可能、切断済み、使用中、準備中。	
タグ	マシンに関連付けられているタグのリスト。	シングルセッションおよびマルチセッション
VDAアップグレード	VDAパッケージアップグレードアクションのマシン状態。	シングルセッションおよびマルチセッション
	指定可能な値: MissingUpgradeType、UpgradeScheduled、UpgradeAvailable、UpToDate、および Unknown。	

列	説明	適用対象
サスペンド可能	マシンが電源操作（サスペンドと再開）をサポートしているかどうかを示します。	シングルセッションおよびマルチセッション
ロード評価インデックス	マシンの全体的な実効負荷インデックス（パーセンテージ）。詳細については、「CTX202150」を参照してください。	マルチセッションのみ
ロードインデックス	現在のロードインデックス。詳細については、「詳細はこちら」を参照してください。	マルチセッションのみ
ドレイン状態	マシンがドレイン中で、マシン上のすべてのセッションが終了した後にシャットダウンするかどうかを示します。True は、電源管理されたマルチセッションマシンにのみ表示されます。	マルチセッションのみ
	注: マシンがメンテナンスモードの場合、シャットダウンしません。シャットダウンするのは、メンテナンスモードが解除された後のみです。	

マシン詳細

マシン詳細カテゴリの列。

列	説明	適用対象
エージェントバージョン	マシンにインストールされているCitrix Virtual Delivery Agent (VDA) のバージョン。	シングルセッションおよびマルチセッション
IPアドレス	マシンのIPアドレスです。	シングルセッションおよびマルチセッション
割り当て済み	専用デスクトップがユーザーまたはクライアント（名前/アドレス）に割り当てられているかどうかを示します。ユーザーは明示的に割り当てることも、マシンの初回使用時に割り当てることもできます。	シングルセッションおよびマルチセッション
OSの種類	マシンで実行されているオペレーティングシステムの種類です。	シングルセッションのみ

アプリケーション

アプリケーションカテゴリの列。

列	説明	適用対象
使用中のアプリケーション	マシンで使用中のアプリケーションのリスト（ブラウザ名として表示されます）。	シングルセッションおよびマルチセッション
公開アプリケーション	マシンによって公開されたアプリケーションのリスト（ブラウザ名として表示されます）。	シングルセッションおよびマルチセッション

接続

接続カテゴリの列。

列	説明	適用対象
クライアント (IP)	マシンに接続されているクライアントのIPアドレス。	シングルセッションのみ
クライアント	マシンに接続されているクライアントのホスト名。	シングルセッションのみ
プラグインバージョン	接続されているクライアント上のCitrix Workspaceアプリのバージョン。	シングルセッションのみ
接続元	受信接続のホスト名。通常はゲートウェイ、ルーター、またはクライアントです。	シングルセッションのみ
接続元 (IP)	受信接続のIPアドレス。通常はゲートウェイ、ルーター、またはクライアントです。	シングルセッションのみ
接続の種類	セッションに使用されるプロトコル。可能な値：HDX、RDP、およびConsole。注：XenDesktop® 5 VDA上のコンソールセッションの場合、このフィールドは空白になります。	シングルセッションのみ
最終接続時刻 (UTC)	失敗または成功した、最後に検出された接続試行の時刻。	シングルセッションおよびマルチセッション
最終接続ユーザー	そのマシンへの接続を最後に試行したユーザーのSAM名（「DOMAIN\user」形式）。SAM名が利用できない場合は、SIDが使用されます。	シングルセッションおよびマルチセッション
Secure ICA® アクティブ	SecureICA が現在のセッションでアクティブであるかどうかを示します。マルチセッションマシンでは常に null です。	シングルセッションおよびマルチセッション

ホスティング

ホスティングカテゴリの列。

列	説明	適用対象
VM	セッションを実行しているホストされたマシンの、ハイパーバイザーで使用されるフレンドリ名。マシンの DNS 名または AD 名と必ずしも一致するとは限りません。	シングルセッションおよびマルチセッション
ホスティングサーバー名	管理対象の場合、マシンをホストしているハイパーバイザーの DNS 名。	シングルセッションおよびマルチセッション
接続	セッションをホストしているマシンに割り当てられているホスト接続の名前。	シングルセッションおよびマルチセッション
更新保留中	ホストされているマシンのVMイメージが古いかどうか、およびマシンの次回の再起動時に新しいイメージに更新される予定があるかどうかを示します。	シングルセッションおよびマルチセッション
ユーザー変更の永続性	ユーザーの変更がどのように処理されるかを示し、変更が永続的であるかどうかを示します。	シングルセッションおよびマルチセッション

列	説明	適用対象	
	• OnLocal: 永続的。ユーザーの変更はローカルに保存されます。 • Discard: 非永続的。ユーザーの変更は破棄されます。		
保留中の電源操作	マシンに保留中の電源操作があるかどうかを示します。	シングルセッションおよびマルチセッション	
電源状態	マシンの電源状態。可能な値: Unmanaged、Unknown、Unavailable、Off、On、Suspended、TurningOn、TurningOff、Suspending、Resuming。	シングルセッションおよびマルチセッション	
使用後にシャットダウン	電源管理されたシングルセッションマシンにのみ適用されます。マシンが汚染されており、すべてのセッションが終了した後にシャットダウンするかどうかを示します。	シングルセッションのみ	
	注: マシンがメンテナンスモードの場合、シャットダウンしません。メンテナ		

列	説明	適用対象
	ンスモードから解除された後にのみシャットダウンします。	

登録

登録カテゴリの列。

列	説明	適用対象
最終登録失敗	ブローカーへのマシンの最終登録解除の理由。	シングルセッションおよびマルチセッション
	考えられる値は次のとおりです: AgentShutdown, AgentSuspended, AgentRequested, IncompatibleVersion, AgentAddressResolutionFailed, AgentNotContactable, AgentWrongActiveDirectoryOU, EmptyRegistrationRequest, MissingRegistrationCapabilities, MissingAgentVersion, InconsistentRegistrationCapabilities, NotLicensedForFeature, UnsupportedCredentialSecurityVersion, InvalidRegistrationRequest,	

列	説明	適用対象
	SingleMultiSessionMismatch, FunctionalLevelTooLowForCatalog, FunctionalLevelTooLowForDesktopGroup, PowerOff, DesktopRestart, DesktopRemoved, AgentRejectedSettingsUpdate, SendSettingsFailure, SessionAuditFailure, SessionPrepareFailure, ContactLost, SettingsCreationFailure, UnknownError, および BrokerRegistrationLimitReached です。	
最終登録失敗時刻 (UTC)	マシンの最終登録解除時刻。	シングルセッションおよびマルチセッション
登録状態	マシンの登録状態。考えられる値: Unregistered, Initializing, Registered, および AgentError。	シングルセッションおよびマルチセッション
障害状態	マシンの現在の障害状態の概要。考えられる値 • なし: 障害なし。マシンは正常です。	シングルセッションおよびマルチセッション

列	説明	適用対象	
	• FailedToStart: マシンの最後の電源投入操作が失敗しました。 • StuckOnBoot: 電源投入後、マシンが起動に失敗しました。 • 未登録。マシンが予期された期間内に登録に失敗したか、登録が拒否されました。 • MaxCapacity。マシンが最大容量に達していることを報告しています。		

セッションの詳細

セッションの詳細カテゴリの列。

列	説明	適用対象
起動元	現在のブローカーセッションの起動に使用されたStoreFrontサーバーのホスト名。マルチセッションマシンでは常にnullです。	シングルセッションおよびマルチセッション
起動元 (IP)	現在のブローカーセッションの起動に使用されたStoreFrontサーバーのIPアドレス。マルチセッションマシンでは常にnullです。	シングルセッションおよびマルチセッション

列	説明	適用対象
セッション変更時刻 (UTC)	現在のセッションの最後の状態変更時刻。	シングルセッションのみ
SmartAccessフィルター	現在のセッションのSmart Accessタグ。マルチセッションマシンでは常にヌルです。	シングルセッションおよびマルチセッション

セッション

セッションカテゴリの列。

列	説明	適用対象
セッション状態	現在のセッションの状態。可能な値: Other、PreparingSession、Connected、Active、Disconnected、Reconnecting、NonBrokeredSession、Unknown。	シングルセッションのみ
現在のユーザー	現在のセッションのユーザー名（「DOMAIN\user」の形式）。	シングルセッションのみ
開始時刻 (UTC)	現在のセッションの開始時刻。	シングルセッションのみ
セッション数	マシン上のセッション数。	マルチセッションのみ

セッションのアクションと列

この記事では、参照用にマシンのアクションと列を説明とともに示します。

アクション

セッションで実行できるアクションとその説明を表示します。

アクション	説明	適用対象セッション
ログオフ	セッションからユーザーをログオフします。	シングルセッションOSマシンまたはマルチセッションOSマシン
メッセージを送信	セッションのユーザーにメッセージを送信します。	シングルセッションOSマシンまたはマルチセッションOSマシン
マシンの表示	セッションのホストマシンを表示します。	シングルセッションOSマシンまたはマルチセッションOSマシン
切断	セッションを切断します。セッションが切断されても、セッションはアクティブなままでアプリケーションは実行され続けますが、ユーザーデバイスはDelivery Controllerと通信しなくなります。	シングルセッションOSマシンまたはマルチセッションOSマシン
マシンのシャットダウン	セッションに関連付けられているマシンをシャットダウンします。	シングルセッションOSマシン
マシンの再起動	セッションに関連付けられているマシンを再起動します。	シングルセッションOSマシン

列

セッションの列とその説明を表示します。

列	説明
現在のユーザー	ユーザーの名前。ユーザーのユーザープリンシパル名 (UPN)。
名前	セッションをホストしているマシンのDNSホスト名。

列	説明
デリバリーグループ	セッションのホストマシンを含むデリバリーグループの名前。
マシンカタログ	セッションのホストマシンを含むマシンカタログの名前。
エージェントバージョン	セッションをホストしているマシンにインストールされているCitrix Virtual Delivery Agent (VDA) のバージョン。
使用中のアプリケーション	セッションで使用されているアプリケーションのリスト。管理名で識別されます。
自律的に仲介済み	これは、仲介されずに直接接続によって確立されたHDX™セッションであるかどうか。
仲介時間 (UTC)	セッションが仲介された時刻。
ブローカリングユーザー名	ブローカリングユーザーの名前。
クライアント (IP)	セッションに接続されているクライアントのIPアドレス。
クライアント	セッションに接続されているクライアントのホスト名。
プラグインバージョン	セッションに接続されているクライアントで実行されているCitrix Workspace™アプリのバージョン。
接続元	受信接続のホスト名。通常はゲートウェイ、ルーター、またはクライアントです。

列	説明
接続元 (IP)	受信接続のIPアドレス。通常、ゲートウェイ、ルーター、またはクライアントです。
割り当ての種類	セッションが共有か専用かを示します。
非表示	セッションがユーザーから隠されているか、再接続されないように設定されているか。
VM	セッションをホストしているVMの、ハイパーバイザーで使用されるフレンドリ名。これは、マシンのDNS名またはAD名のいずれとも必ずしも一致しません。
ホスティングサーバー名	セッションのホスティングマシンをホストしているハイパーバイザーのDNS名。
接続	セッションをホストしているマシンに割り当てられているホスト接続の名前。
保留中の更新	ホストされているマシンのVMイメージが古く、次回の再起動時に新しいイメージに更新される予定であるかどうか。
メンテナンスモード	セッションをホストしているマシンがメンテナンスモードであるかどうか。
IPアドレス	セッションをホストしているマシンのIPアドレス。

列	説明
物理であるか	セッションをホストしているマシンが物理であるかどうか。`True` はマシンが物理であることを示し、これはDelivery Controllersによって電源管理されていないことを意味します。`False` はそうでないことを示します。
起動元	セッションの起動に使用されたStoreFront™サーバーのホスト名。セッションがWorkspace経由で起動された場合は空白です。
起動元 (IP)	セッションの起動に使用されたStoreFrontサーバーのIPアドレス。セッションがWorkspace経由で起動された場合は空白です。
OSの種類	セッションをホストしているオペレーティングシステムの識別文字列。
ユーザー変更の永続性	ユーザーの変更がどのように処理されるかを示し、変更が永続的であるかどうかを示します。 • OnLocal: 永続的。ユーザーの変更はローカルに保存されます。 • Discard: 非永続的。ユーザーの変更は破棄されます。

列	説明
接続の種類	HDX、RDP、Consoleなど、セッションに使用されるプロトコル。 **注:** XenDesktop® 5 VDA上のコンソールセッションの場合、このフィールドは空白です。
プロビジョニングの種類	セッションをホストしているマシンがどのようにプロビジョニングされたか • 手動: PVSまたはMCSを使用してプロビジョニングされていません。 • PVS: PVSによってプロビジョニングされました（物理マシン、ブレードマシン、仮想マシン）。 • MCS: MCSによってプロビジョニングされました（VMのみ）。
Secure ICA® アクティブ	セッションでSecureICAがアクティブであるかどうか。
セッションの状態	セッションの状態。可能な値: 接続済み、アクティブ、または切断済み。L7より前の機能レベルのマシン上のセッションでは、PreparingSession、Reconnecting、NonBrokeredSession、Other、Unknownなどの他の状態が発生する場合があります。

列	説明
セッション変更時刻	セッションの最新の状態変更時刻。
アプリケーションの状態	セッション内のアプリケーションの状態。可能な値: PreLogon、PreLaunched、Active、Desktop、Lingering、NoApps。
セッションサポート	セッションをホストしているマシンが複数セッションをサポートするか、単一セッションをサポートするか。
ゾーン	セッションをホストしているマシンが配置されているゾーンの名前。
SmartAccessフィルター	セッションのSmart Accessタグ。
開始時刻 (UTC)	セッションが開始された日時。
状態	マシンの概要状態。可能な値: Unregistered、Disconnected、または InUse。
状態時間 (UTC)	セッションが現在の状態になってからの時間。
デリバリーコントローラー™	セッションのホストマシンが登録されているコントローラーのDNSホスト名。
ユーザー表示名	ユーザーのフルネーム。
デスクトップ表示名	セッションの起動に元々使用されたマシンの公開名。Citrix Workspaceアプリまたはストアフロントに表示される名

列	説明
	前です。アプリケーションセッションの場合、そのアプリケーションが終了していても、セッションで最初に起動されたアプリケーションの名前です。リソースが後で名前変更または削除されても、名前は変更されません。

セキュリティキー

重要:

- この機能は、StoreFront™ 1912 LTSR CU2以降と組み合わせて使用する必要があります。
- Secure XML機能は、Citrix ADCおよびCitrix Gatewayリリース12.1以降でのみサポートされています。

注:

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

この機能を使用すると、承認されたStoreFrontおよびCitrix Gatewayマシンのみがデリバリーコントローラーと通信できるようになります。この機能を有効にすると、キーを含まないすべての要求はブロックされます。この機能を使用して、内部ネットワークから発生する攻撃から保護するためのセキュリティ層を追加します。

この機能を使用するための一般的なワークフローは次のとおりです。

1. Web Studioを有効にして、機能設定を表示します。
2. サイトの設定を構成します。

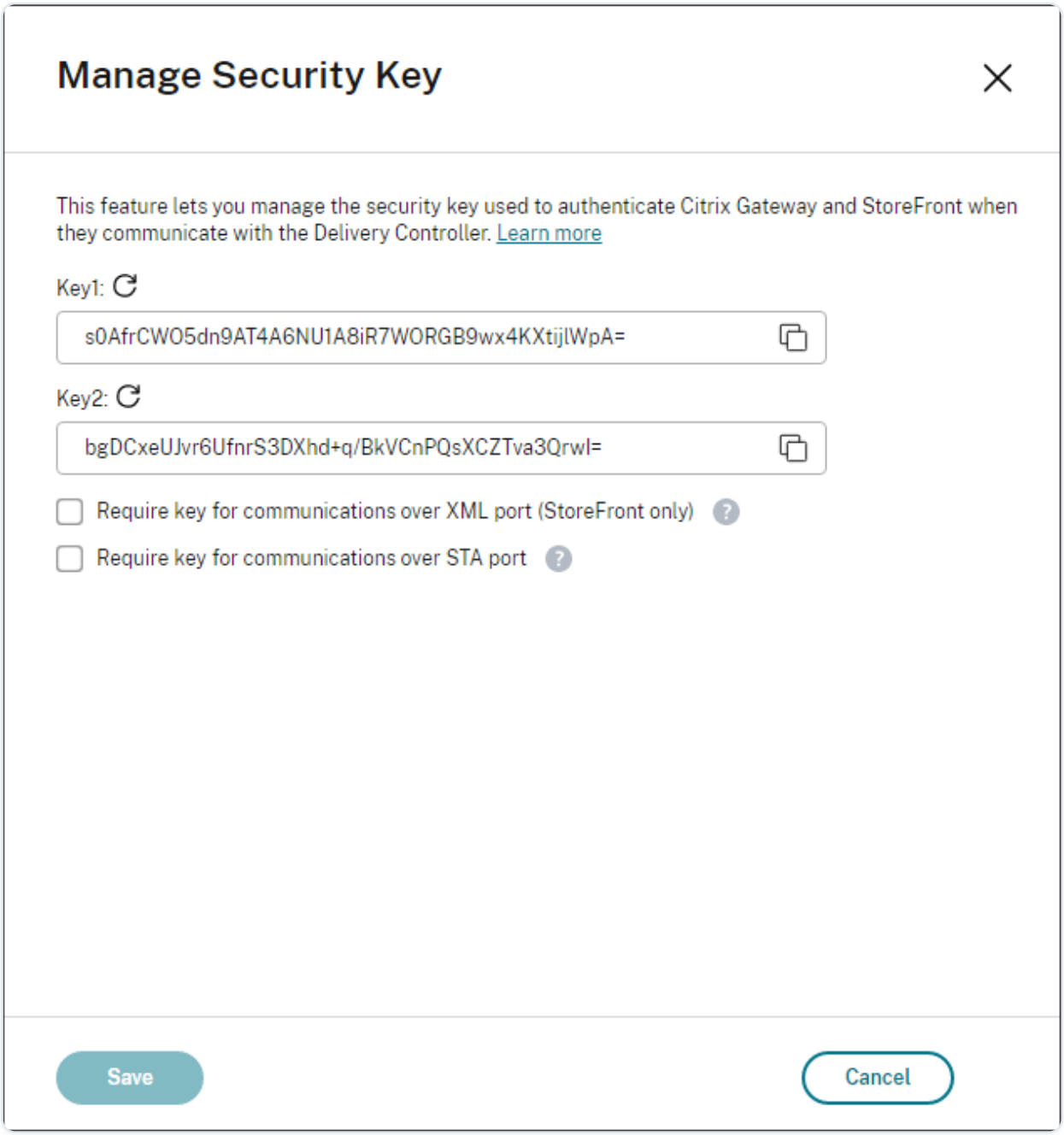
3. StoreFrontの設定を構成します。
4. Citrix ADCの設定を構成します。

サイトの設定を構成する

Web StudioまたはPowerShellを使用して、サイトのセキュリティキー設定を構成できます。

Web Studioを使用する

1. Web Studio にサインインし、左側のペインで **設定** を選択します。
2. **セキュリティキーの管理** タイルを見つけて、**編集** をクリックします。**セキュリティキーの管理** ページが表示されます。



3. 更新アイコンをクリックしてキーを生成します。

> **重要:**
>
> - 使用可能なキーは2つあります。XMLポートおよびSTAポートを介した通信には、同じキーまたは異なるキーを使用できます。一度に1つのキーのみを使用することをお勧めします。未使用のキーはキーローテーションにのみ使用されます。
> - 既に使用中のキーを更新するために更新アイコンをクリックしないでください。クリックすると、サービスが中断されます。

4. 通信にキーが必要な場所を選択します。

   - **XMLポートを介した通信にキーを要求する（StoreFrontのみ）**。選択した場合、XMLポートを介した通信を認証するためにキーが必要になります。StoreFrontはこのポートを介してCitrix Cloudと通信します。XMLポートの変更については、Knowledge Centerの記事CTX127945を参照してください。
   - **STAポートを介した通信にキーを要求する**。選択した場合、STAポートを介した通信を認証するためにキーが必要になります。Citrix GatewayとStoreFrontはこのポートを介してCitrix Cloudと通信します。STAポートの変更については、Knowledge Centerの記事CTX101988を参照してください。

5. 変更を適用してウィンドウを閉じるには、**保存** をクリックします。

PowerShell を使用する

以下は、Web Studioの操作に相当するPowerShellの手順です。

1. Citrix Virtual Apps and Desktops Remote PowerShell SDK を実行します。
2. コマンドウィンドウで、次のコマンドを実行します。

   - `Add-PSSnapIn Citrix*`

3. 次のコマンドを実行して、キーを生成し、Key1 を設定します。

   - `New-BrokerXmlServiceKey`
   - `Set-BrokerSite -XmlServiceKey1 <the key you generated>`

4. 次のコマンドを実行して、キーを生成し、Key2 を設定します。

- `New-BrokerXmlServiceKey`
- `Set-BrokerSite -XmlServiceKey2 <the key you generated>`

5. 次のコマンドのいずれか、または両方を実行して、キーの使用を有効にし、通信を認証します。
   - XML ポート経由で通信を認証するには:
     - `Set-BrokerSite -RequireXmlServiceKeyForNFuse $true`
   - STAポート経由の通信を認証するには:
     - `Set-BrokerSite -RequireXmlServiceKeyForSta $true`

ガイダンスと構文については、PowerShellコマンドのヘルプを参照してください。

StoreFrontの設定を構成する

サイトの構成が完了したら、PowerShellを使用してStoreFrontの関連設定を構成する必要があります。

StoreFront サーバーで、以下の PowerShell コマンドを実行します。

XMLポートを介した通信用のキーを構成するには、コマンドを使用します。例:

```
$store = Get-STFStoreService -VirtualPath [Path to store]

$farm = Get-STFStoreFarm -StoreService $store -FarmName [Resource feed
name]

Set-STFStoreFarm -Farm $farm -XMLValidationEnabled $true
-XMLValidationSecret [secret]
```

次のパラメータに適切な値を入力します。

- `Path to store`
- `Resource feed name`
- `secret`

STAポート経由の通信用にキーを構成するには、`New-STFSecureTicketAuthority`および`Set-STFRoamingGateway`コマンドを使用します。例:

```
$gateway = Get-STFRoamingGateway -Name [Gateway name]

$sta1 = New-STFSecureTicketAuthority -StaUrl [STA1 URL]
-StaValidationEnabled $true -StaValidationSecret [secret]

$sta2 = New-STFSecureTicketAuthority -StaUrl [STA2 URL]
-StaValidationEnabled $true -StaValidationSecret [secret]

Set-STFRoamingGateway -Gateway $gateway -SecureTicketAuthorityObjs
$sta1,$sta2
```

次のパラメータに適切な値を入力します。

- `Gateway name`
- `STA URL`
- `Secret`

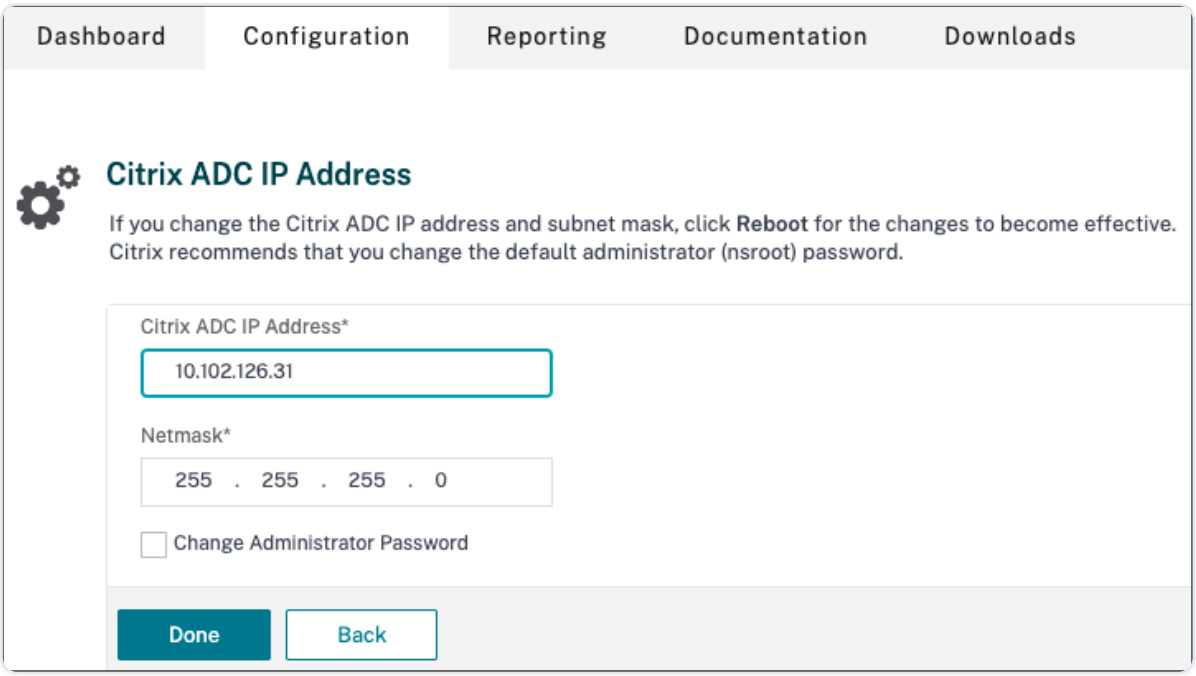
ガイダンスと構文については、PowerShellコマンドのヘルプを参照してください。

Citrix ADCの設定を構成する

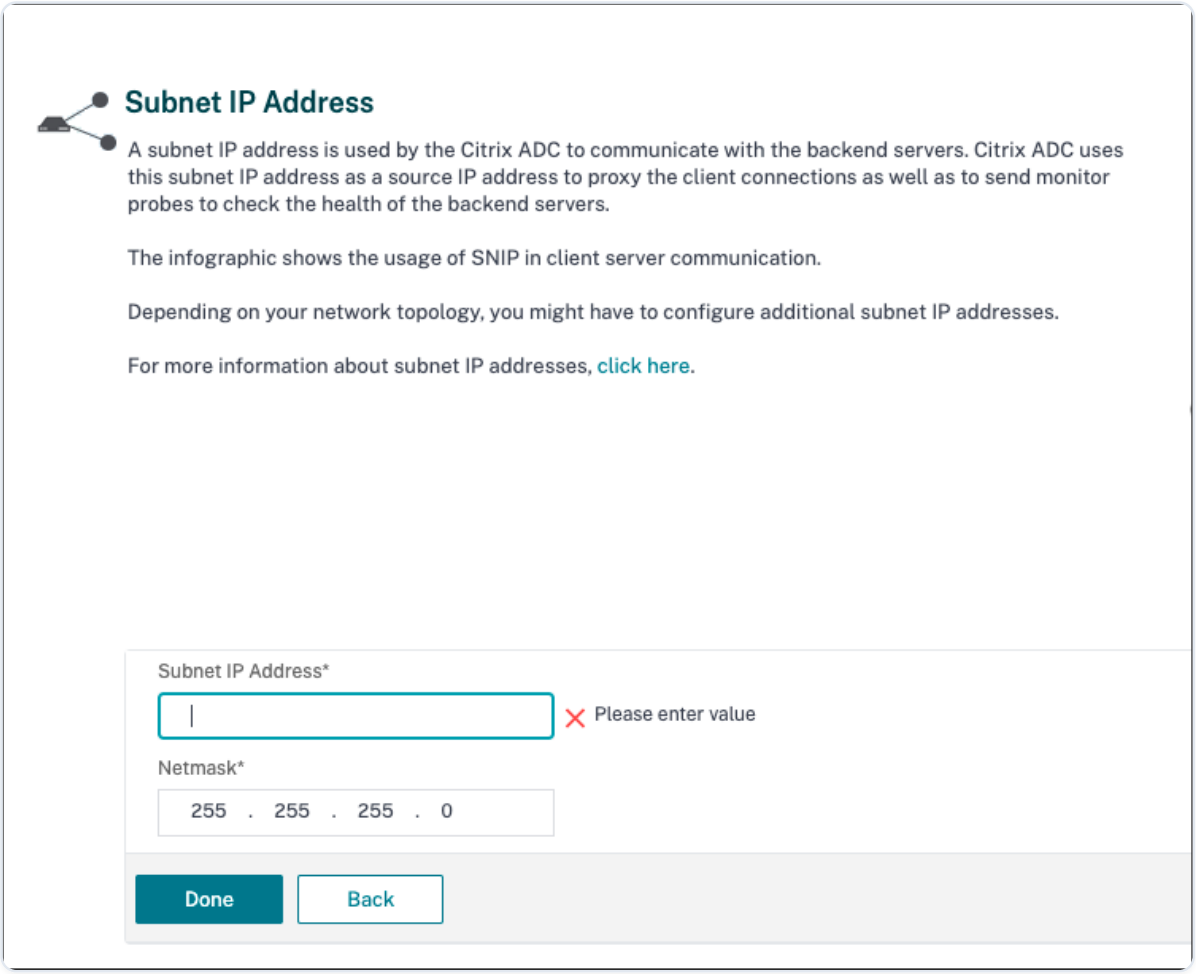
注:

Citrix ADCをゲートウェイとして使用しない限り、Citrix ADCでこの機能を構成する必要はありません。Citrix ADCを使用する場合は、次の手順に従ってください。

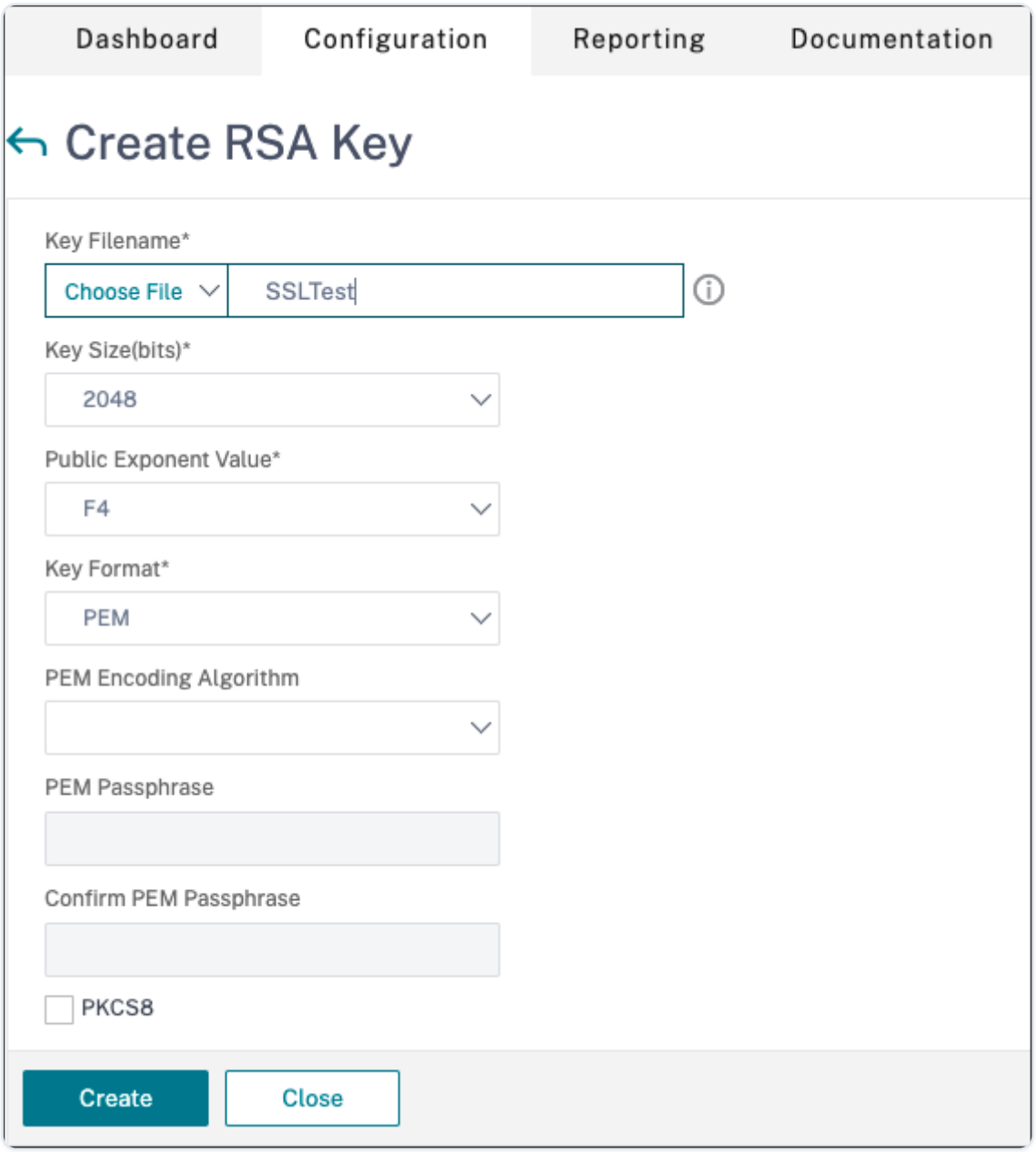
1. 次の前提条件となる構成がすでに設定されていることを確認してください。
    - 次のCitrix ADC関連のIPアドレスが構成されています。
        - Citrix ADCコンソールにアクセスするための Citrix ADC管理IP (NSIP) アドレス。詳細については、「NSIPアドレスの構成」を参照してください。



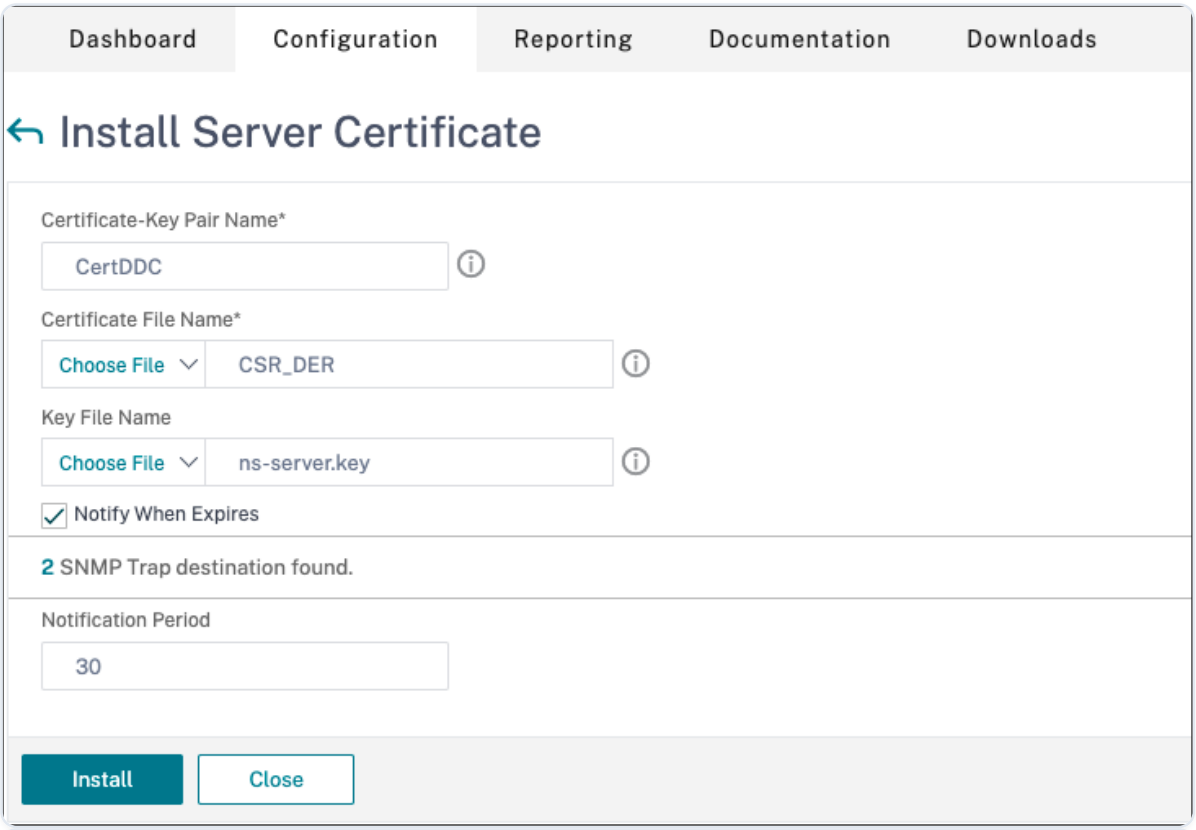
- Citrix ADCアプライアンスとバックエンドサーバー間の通信を有効にするためのサブネットIP（SNIP）アドレス。詳細については、「サブネットIPアドレスの構成」を参照してください。
- セッション起動のためにADCアプライアンスにログインするためのCitrix Gateway仮想IPアドレスとロードバランサー仮想IPアドレス。詳細については、「仮想サーバーの作成」を参照してください。

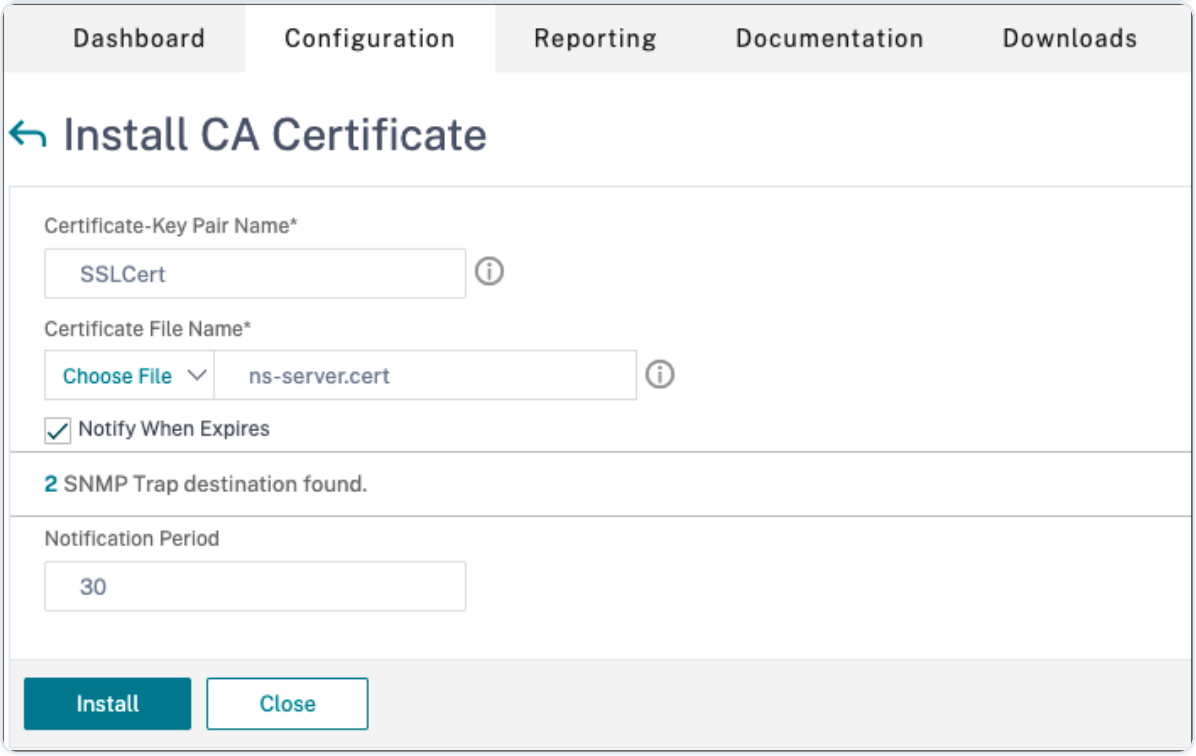


- Citrix ADCアプライアンスで必要なモードと機能が有効になっています。
  - モードを有効にするには、Citrix ADC GUIで **System > Settings > Configure Mode** に移動します。
  - 機能を有効にするには、Citrix ADC GUIで **System > Settings > Configure Basic Features** に移動します。
- 証明書関連の構成が完了しています。
  - 証明書署名要求（CSR）が作成されます。詳細については、「証明書の作成」を参照してください。

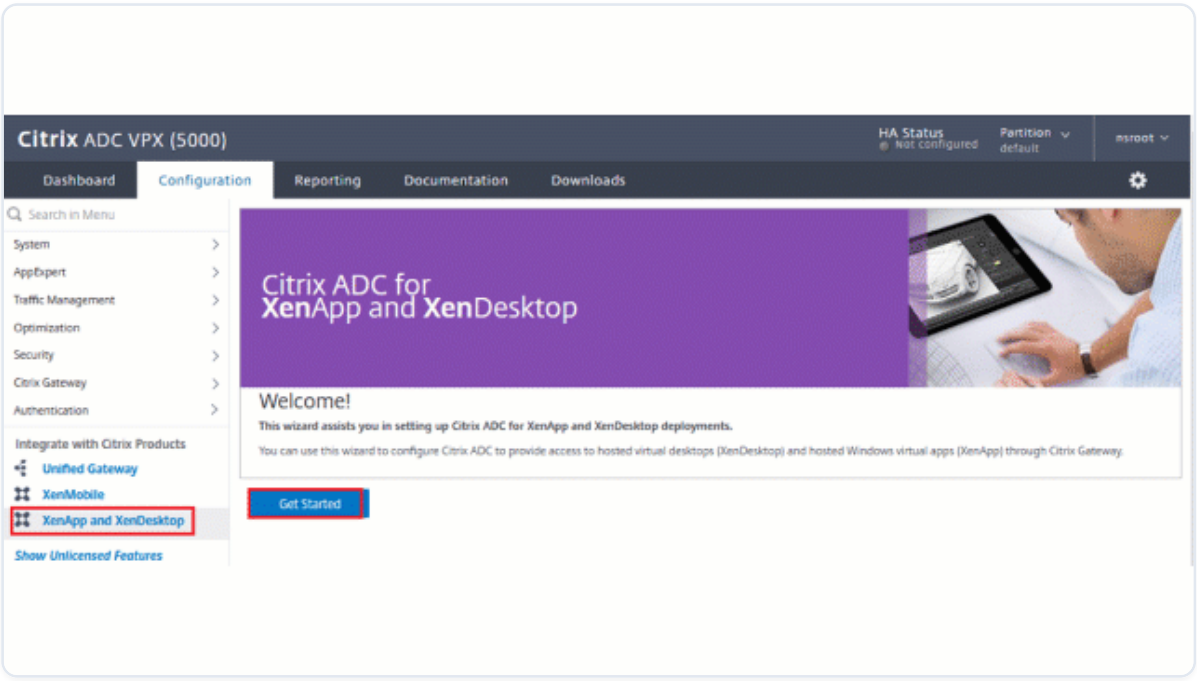


- サーバー証明書、CA証明書、およびルート証明書がインストールされます。詳細については、「インストール、リンク、および更新」を参照してください。





- Citrix Virtual Desktops用にCitrix Gatewayが作成されました。仮想サーバーがオンラインであることを確認するには、**Test STA Connectivity**ボタンをクリックして接続をテストします。詳細については、「Citrix Virtual Apps and Desktops向けCitrix ADCのセットアップ」(/ja-jp/citrix-adc/current-release/solutions/deploy-xa-xd.html)を参照してください。



2. リライトアクションを追加します。詳細については、「リライトアクションの構成」(/ja-jp/citrix-adc/current-release/appexpert/rewrite.html#configuring-a-rewrite-action)を参照してください。

   a. 「**AppExpert > Rewrite > Actions**」に移動します。

   b. 新しい書き換えアクションを追加するには、**追加**をクリックします。アクションの名前は「set Type to INSERT_HTTP_HEADER」にすることができます。

   書き換えアクションの追加(/en-us/citrix-virtual-apps-desktops/2503/media/adc-appexpert-rewrite-action.png)

   a. **タイプ**で、**INSERT_HTTP_HEADER**を選択します。

   b. **ヘッダー名**に、X-Citrix-XmlServiceKeyと入力します。

   c. **式**に、引用符付きで`<XmlServiceKey1 value>`を追加します。Desktop Delivery Controller™の構成からXmlServiceKey1の値をコピーできます。

   XMLサービスキーの値(/en-us/citrix-virtual-apps-desktops/2503/media/xml-service-key-values.png)

3. リライトポリシーを追加します。詳細については、「リライトポリシーの構成」(/ja-jp/citrix-adc/current-release/appexpert/rewrite.html#configure-rewrite-policy)を参照してください。

   a. **AppExpert > Rewrite > Policies**に移動します。

   b. 新しいポリシーを追加するには、**追加**をクリックします。

書き換えポリシーの追加(/en-us/citrix-virtual-apps-desktops/2503/media/adc-appexpert-rewrite-policy.png)

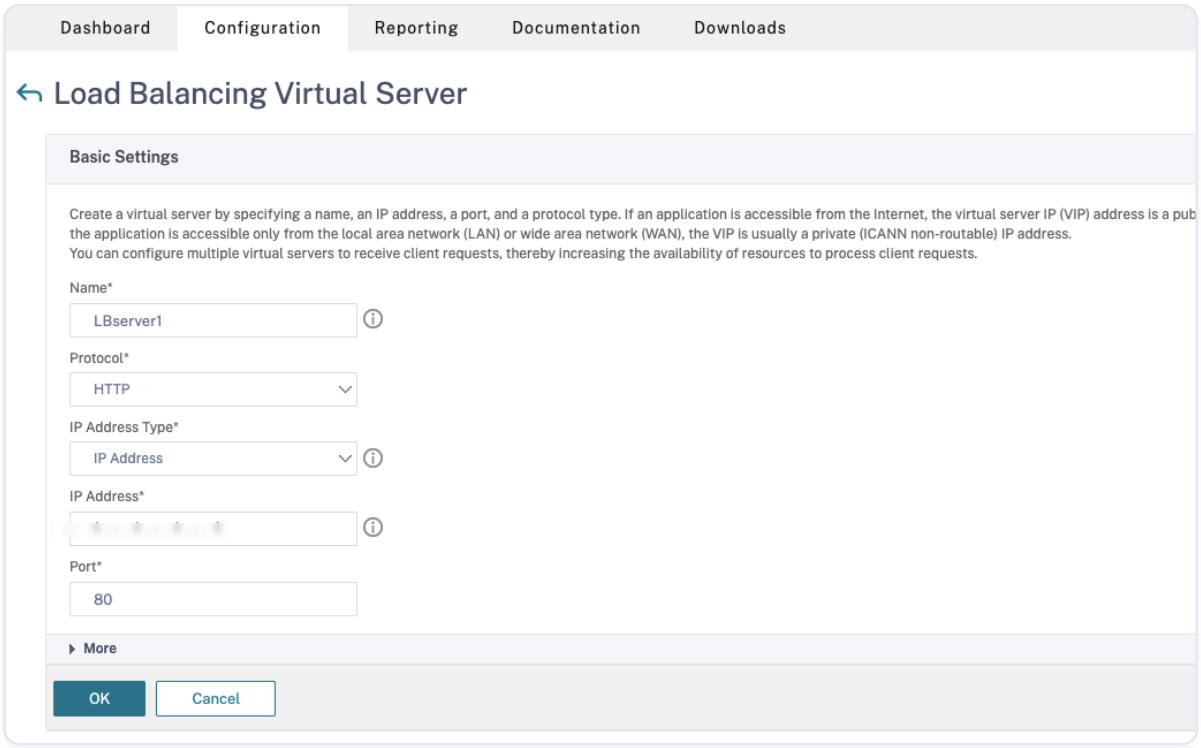
a. **アクション**で、前の手順で作成したアクションを選択します。
b. **式**に「HTTP.REQ.IS_VALID」を追加します。
c. **OK**をクリックします。

4. 負荷分散を設定します。STAサーバーごとに1つの負荷分散仮想サーバーを構成する必要があります。構成しない場合、セッションの起動に失敗します。

詳細については、基本的な負荷分散のセットアップを参照してください。

a. 負荷分散仮想サーバーを作成します。

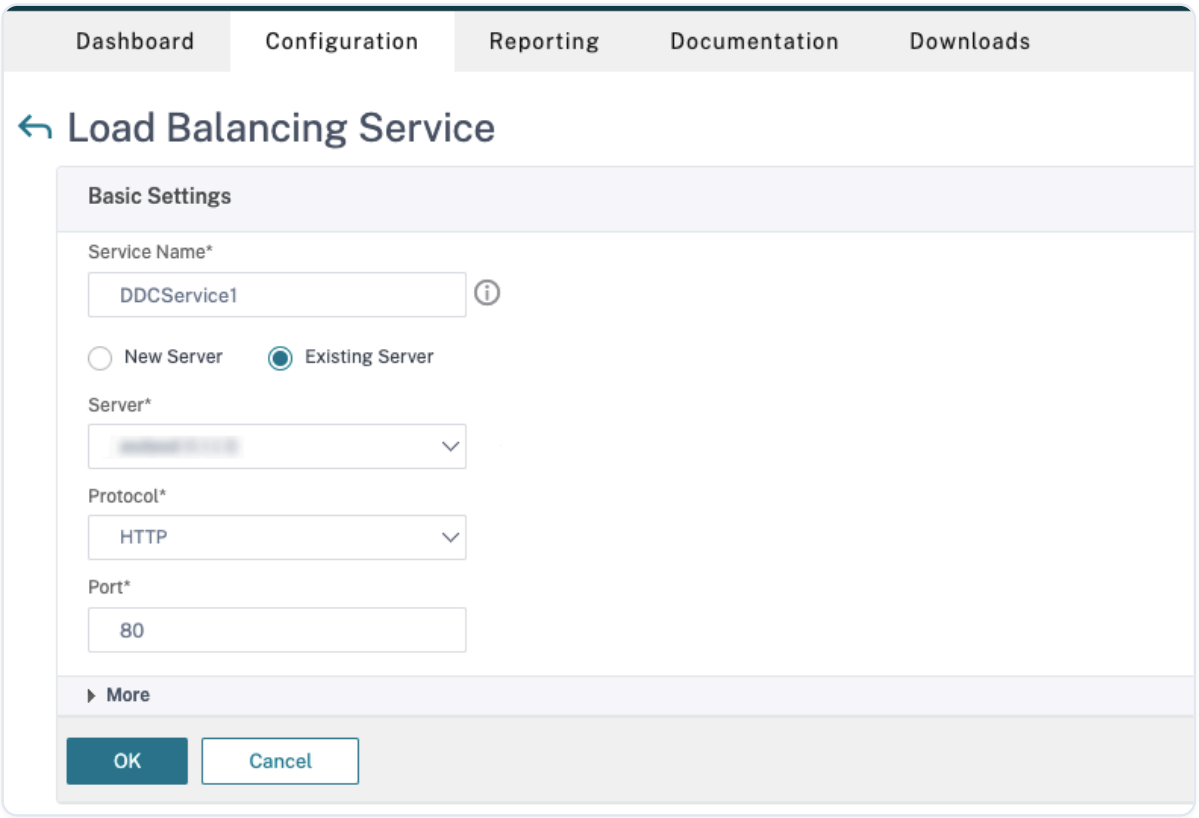
- **トラフィック管理 > ロードバランシング > サーバー** に移動します。
- **仮想サーバー**ページで、**追加**をクリックします。



- **Protocol**で、**HTTP**を選択します。
- 負荷分散仮想IPアドレスを追加し、**Port**で**80**を選択します。
- **OK**をクリックします。

b. 負荷分散サービスを作成します。

- **トラフィック管理 > ロードバランシング > サービス** に移動します。



- **Existing Server**で、前のステップで作成した仮想サーバーを選択します。
- **Protocol**で**HTTP**を選択し、**Port**で**80**を選択します。
- **OK**をクリックし、その後**Done**をクリックします。

c. サービスを仮想サーバーにバインドします。

- 以前に作成した仮想サーバーを選択し、「**Edit**」をクリックします。
- 「**サービスとサービスグループ**」で、「**ロードバランシングなし仮想サーバーサービスバインディング**」をクリックします。

仮想サーバーにサービスをバインドする(/en-us/citrix-virtual-apps-desktops/2503/media/adc-bind-service-to-lbvserver.png)

- **Service Binding**で、以前に作成したサービスを選択します。
- **バインド**をクリックします。

d. 以前に作成した書き換えポリシーを仮想サーバーにバインドします。

- 以前に作成した仮想サーバーを選択し、**編集**をクリックします。
- **詳細設定**で、**ポリシー**をクリックし、次に**ポリシー**セクションで**+**をクリックします。

リライトポリシーをバインドする(/en-us/citrix-virtual-apps-desktops/2503/media/adc-bind-rewrite-policy.png)

- 「**Choose Policy**」で「**Rewrite**」を選択し、「**Choose Type**」で「**Request**」を選択します。
- 「**Continue**」をクリックします。
- 「**ポリシーの選択**」で、以前に作成した書き換えポリシーを選択します。
- 「**バインド**」をクリックします。
- 「**完了**」をクリックします。

e. 必要に応じて、仮想サーバーの永続性を設定します。

- 以前に作成した仮想サーバーを選択し、「**編集**」をクリックします。
- 「**詳細設定**」で、「**永続性**」をクリックします。

永続性の設定(/en-us/citrix-virtual-apps-desktops/2503/media/adc-lb-vserver-persistence.png)

- 永続性の種類として「**その他**」を選択します。
- 仮想サーバーによって選択されたサービスのIPアドレス (宛先IPアドレス) に基づいて永続セッションを作成するには、「**DESTIP**」を選択します。
- 「**IPv4ネットマスク**」で、DDCと同じネットワークマスクを追加します。
- 「**OK**」をクリックします。

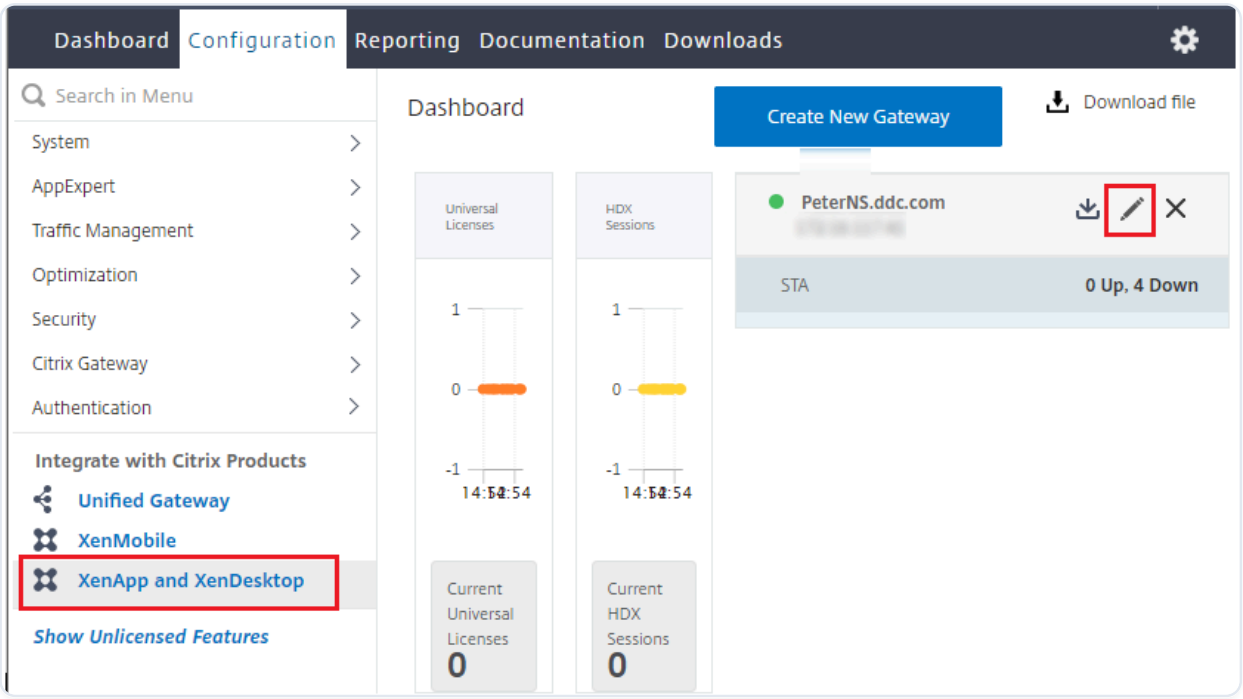
f. 他の仮想サーバーについても、これらの手順を繰り返します。

Citrix ADCアプライアンスがCitrix Virtual Desktops™で既に構成されている場合の構成の変更点

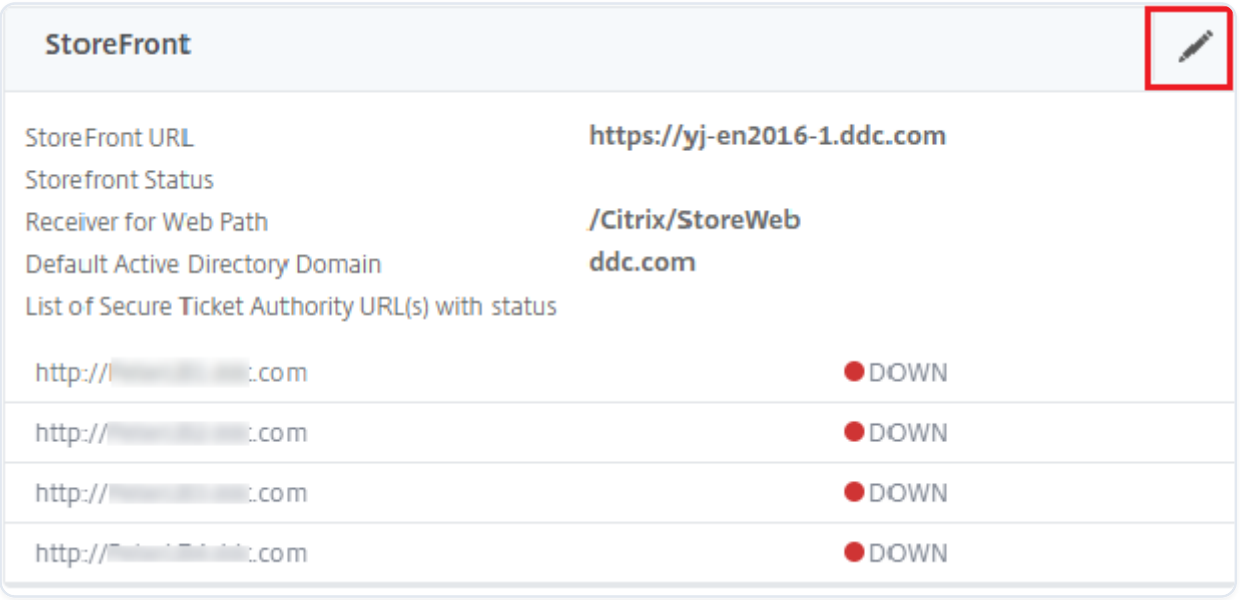
Citrix ADCアプライアンスをCitrix Virtual Desktopsで既に構成している場合、Secure XML機能を使用するには、以下の構成変更を行う必要があります。

- セッション起動前に、ゲートウェイの「**セキュリティチケット機関URL**」を変更して、負荷分散仮想サーバーのFQDNを使用するようにします。
- `TrustRequestsSentToTheXmlServicePort` パラメーターが False に設定されていることを確認します。デフォルトでは、`TrustRequestsSentToTheXmlServicePort` パラメーターは False に設定されています。ただし、お客様が Citrix Virtual Desktops 用に Citrix ADC をすでに構成している場合、`TrustRequestsSentToTheXmlServicePort` は True に設定されます。

1. Citrix ADC GUIで、**構成 > Citrix製品との統合**に移動し、**XenApp and XenDesktop®**をクリックします。
2. ゲートウェイインスタンスを選択し、編集アイコンをクリックします。

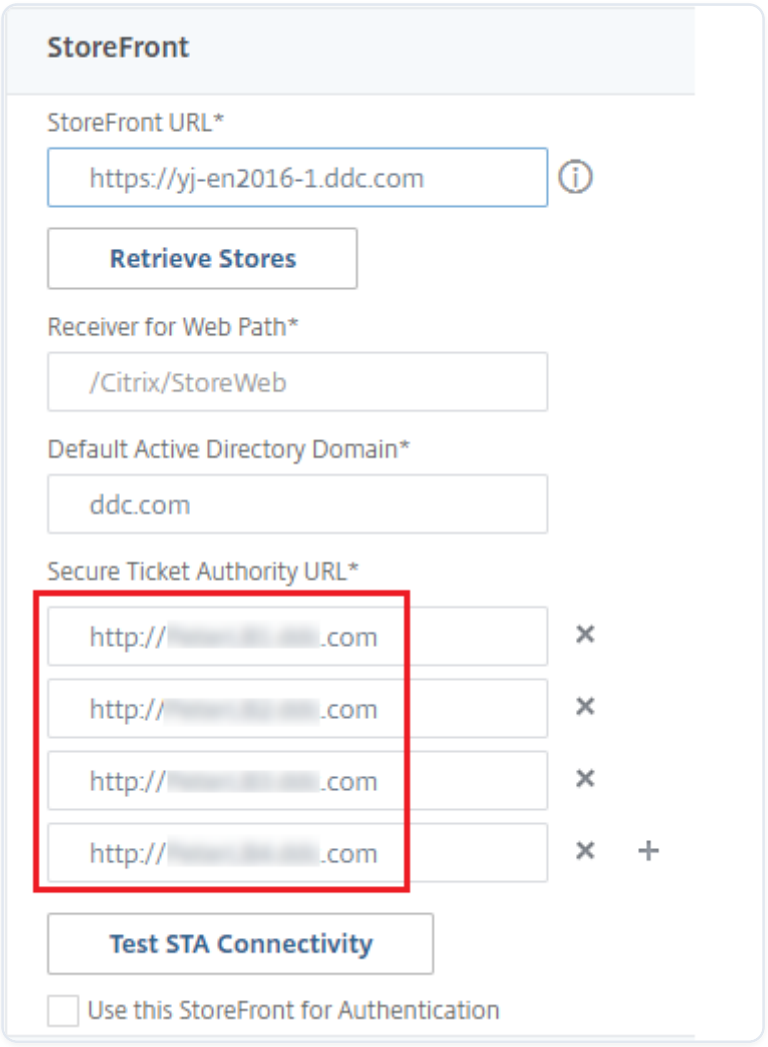


3. StoreFrontペインで、編集アイコンをクリックします。



4. **Secure Ticket Authority URL** を追加します。
   - Secure XML 機能が有効になっている場合、STA URL は負荷分散サービスの URL である必要があります。

- Secure XML 機能が無効になっている場合、STA URL は STA の URL (DDC のアドレス) である必要があり、DDC の `TrustRequestsSentToTheXmlServicePort` パラメーターは True に設定されている必要があります。



セッションの回復性設定

セッションアクティビティを維持することは、最高のユーザーエクスペリエンスを提供するために不可欠です。信頼性の低いネットワーク、変動の大きいネットワーク遅延、ワイヤレスデバイスの範囲制限による接続の喪失は、ユーザーの不満につながる可能性があります。デバイス間を素早く移動し、ログオンするたびに同じアプリケーションにアクセスすることは、医療従事者などの多くのモバイルワーカーにとって優先事項です。

この記事で説明する機能は、セッションの信頼性を最適化し、不便さ、ダウンタイム、生産性の損失を軽減します。これらの機能を使用することで、モバイルユーザーはデバイス間を迅速かつ簡単にローミングできます。

セッションの信頼性

セッションの信頼性により、ネットワーク接続が中断されてもセッションはアクティブな状態を保ち、ユーザーの画面に表示され続けます。ユーザーは、ネットワーク接続が再開されるまで、使用しているアプリケーションを引き続き見ることができます。

この機能は、ワイヤレス接続を使用するモバイルユーザーにとって特に便利です。たとえば、ワイヤレス接続を使用しているユーザーが鉄道トンネルに入り、一時的に接続が失われたとします。通常、セッションは切断されてユーザーの画面から消え、ユーザーは切断されたセッションに再接続する必要があります。セッションの信頼性を使用すると、セッションはマシン上でアクティブなままになります。接続が失われたことを示すために、ユーザーのディスプレイはフリーズし、カーソルは砂時計のアイコンに変わり、トンネルの反対側で接続が再開されるまでその状態が続きます。ユーザーは中断中もディスプレイにアクセスし続け、ネットワーク接続が復元されるとアプリケーションとの対話を再開できます。セッションの信頼性により、再認証のプロンプトなしでユーザーが再接続されます。

Citrix Workspace™アプリのユーザーは、Controllerの設定を上書きできません。

セッションの信頼性は、Transport Layer Security (TLS) とともに使用できます。TLSは、ユーザーデバイスとCitrix Gateway間で送信されるデータのみを暗号化します。

次のポリシー設定でセッションの信頼性を有効にして構成します。

- セッションの信頼性接続ポリシー設定は、セッションの信頼性を許可または禁止します。
- セッションの信頼性タイムアウトポリシー設定のデフォルトは180秒、つまり3分です。セッションの信頼性がセッションを開いたままにする時間を延長することはできますが、この機能はユーザーの利便性のために設計されています。したがって、ユーザーに再認証を促すことはありません。セッションを開いたままにする時間を延長すると、ユーザーが注意をそらされてユーザーデバイスから離れる可能性が高まります。これらの行動により、セッションが不正なユーザーにアクセスされる可能性があります。
- セッションの信頼性ポート番号ポリシー設定でポート番号を変更しない限り、受信セッションの信頼性接続はポート2598を使用します。
- ユーザーが再認証なしで中断されたセッションに再接続するのを防ぐには、自動クライアント再接続機能を使用します。自動クライアント再接続認証ポリシー設定を構成して、中断されたセッションに再接続する際にユーザーに再認証を促すことができます。

セッションの信頼性と自動クライアント再接続の両方を使用する場合、これら2つの機能は順次動作します。セッションの信頼性は、セッションの信頼性タイムアウトポリシー設定で指定した時間の経過後、ユーザーセッションを閉じるか、切断します。その後、自動クライアント再接続ポリシー設定が有効になり、切断されたセッションにユーザーを再接続しようとします。

クライアントの自動再接続

「自動クライアント再接続」機能を使用すると、Citrix WorkspaceアプリはICA®セッションの意図しない切断を検出し、影響を受けるセッションにユーザーを自動的に再接続できます。この機能がサーバーで有効になっている場合、ユーザーは手動で再接続することなく作業を続行できます。

アプリケーションセッションの場合、Citrix Workspaceアプリは、再接続が成功するか、ユーザーが再接続の試行をキャンセルするまで、セッションへの再接続を試行します。

デスクトップセッションの場合、Citrix Workspaceアプリは、再接続が成功するか、ユーザーが再接続の試行をキャンセルしない限り、指定された期間、セッションへの再接続を試行します。デフォルトでは、この期間は5分です。この期間を変更するには、ユーザーデバイスで次のレジストリ設定を編集します (`seconds` は、セッションの再接続がそれ以上試行されなくなるまでの秒数です)。

`HKLM\Software\Citrix\ICA Client\TransportReconnectRetryMaxTimeSeconds; DWORD;<seconds>`

自動クライアント再接続を有効にして構成するには、次のポリシー設定を使用します。

- **自動クライアント再接続:** 接続が中断された後にCitrix Workspaceアプリによる自動再接続を有効または無効にします。
- **自動クライアント再接続認証:** 自動再接続後のユーザー認証の要件を有効または無効にします。
- **自動クライアント再接続ログ:** イベントログでの再接続イベントのログ記録を有効または無効にします。ログ記録はデフォルトで無効になっています。有効にすると、サーバーのシステムログに、成功および失敗した自動再接続イベントに関する情報が記録されます。各サーバーは、再接続イベントに関する情報を独自のシステムログに保存します。サイトは、すべてのサーバーの再接続イベントの結合ログを提供しません。

> **注：**
>
> 再認証なしの自動クライアント再接続はパスワード認証でのみサポートされます。フェデレーション認証サービスまたはスマートカード認証を使用している場合、再認証なしの自動クライアント再接続はサポートされません。そのような場合、ユーザーはログオン画面にリダイレクトされます。

> 自動クライアント再接続は、暗号化されたユーザー資格情報に基づく認証メカニズムを組み込んでいます。ユーザーが最初にログオンすると、サーバーはユーザー資格情報を暗号化してメモリに保存します。サーバーはまた、暗号化キーを含むCookieを作成し、Citrix Workspaceアプリに送信します。Citrix Workspaceアプリは、再接続のためにキーをサーバーに送信します。サーバーは資格情報を復号化し、認証のためにWindowsログオンに送信します。Cookieの有効期限が切れると、ユーザーはセッションに再接続するために再認証する必要があります。

自動クライアント再接続認証設定を有効にすると、Cookieは使用されません。代わりに、Citrix Workspaceアプリが自動的に再接続を試行する際に、資格情報を要求するダイアログボックスがユーザーに表示されます。

ユーザー資格情報とセッションを最大限に保護するために、クライアントとサイト間のすべての通信に暗号化を使用してください。

icaclient.admファイルを使用して、Windows版Citrix WorkspaceアプリでAuto Client Reconnectを無効にします。詳細については、お使いのWindows版Citrix Workspaceアプリのバージョンのドキュメントを参照してください。

接続の設定もAuto Client Reconnectに影響します。

- デフォルトでは、Auto Client Reconnect は、前述のとおり、サイトレベルのポリシー設定によって有効になっています。ユーザーの再認証は不要です。ただし、サーバーの ICA TCP 接続が、切断された通信リンクでセッションをリセットするように構成されている場合、自動再接続は行われません。Auto Client Reconnect は、切断された接続またはタイムアウトした接続がある場合にサーバーがセッションを切断する場合にのみ機能します。このコンテキストでは、ICA TCP 接続とは、TCP/IP ネットワーク上のセッションに使用されるサーバーの仮想ポート (実際のネットワーク接続ではなく) を指します。
- デフォルトでは、サーバー上の ICA TCP 接続は、切断された接続またはタイムアウトした接続でセッションを切断するように設定されています。切断されたセッションはシステムメモリにそのまま残り、Citrix Workspace アプリによる再接続が可能です。
- 接続は、切断された接続またはタイムアウトした接続でセッションをリセットまたはログオフするように構成できます。セッションがリセットされると、再接続を試みると新しいセッションが開始されます。使用中のアプリケーションでユーザーを同じ場所に戻すのではなく、アプリケーションが再起動されます。
- サーバーがセッションをリセットするように構成されている場合、Auto Client Reconnect は新しいセッションを作成します。このプロセスでは、ユーザーはサーバーにログオンするために資格情報を入力する必要があります。

- Citrix Workspace アプリまたはプラグインが誤った認証情報を送信した場合 (攻撃中に発生する可能性や、サーバーが切断された接続を検出してから時間が経ちすぎたと判断した場合など) は、自動再接続が失敗することがあります。

ICA キープアライブ

ICA Keep-Alive 機能を有効にすると、切断された接続が切断されるのを防ぎます。有効にすると、サーバーがアクティビティを検出しない場合、この機能はリモートデスクトップサービスがそのセッションを切断するのを防ぎます。アクティビティがない例としては、時計の変更がない、マウスの動きがない、画面の更新がないなどがあります。サーバーは数秒ごとにキープアライブパケットを送信して、セッションがアクティブであるかどうかを検出します。セッションがアクティブでなくなった場合、サーバーはそのセッションを切断済みとしてマークします。

重要:

ICA Keep-Alive works only if you are not using Session Reliability. Session Reliability has its own mechanisms to prevent broken connections from being disconnected. Configure ICA Keep-Alive only for connections that do not use Session Reliability.

ICA Keep-Alive 設定は、Windows グループポリシーで構成されているキープアライブ設定を上書きします。

次のポリシー設定を使用して、ICA Keep-Alive を有効にして構成します。

- **ICA キープアライブタイムアウト:** ICA キープアライブメッセージの送信に使用される間隔 (1～3600秒) を指定します。切断された接続が非常にまれで、ユーザーがセッションに再接続することを許可しても問題ない環境で、ネットワーク監視ソフトウェアに非アクティブな接続を閉じさせたい場合は、このオプションを構成しないでください。

  デフォルトの間隔は60秒です。ICA Keep-Alive パケットは60秒ごとにユーザーデバイスに送信されます。ユーザーデバイスが60秒以内に応答しない場合、ICA セッションのステータスは切断済みに変わります。

- **ICA キープアライブ:** ICA キープアライブメッセージを送信するか、送信を防止します。

ワークスペースコントロール

ワークスペースコントロールにより、デスクトップとアプリケーションはユーザーに追従し、デバイス間を移動できます。このローミング機能により、ユーザーはログオンするだけで、各デバイスでデスクトップやアプリケーションを再起動することなく、どこからでもすべてのデスクトップや

開いているアプリケーションにアクセスできます。たとえば、ワークスペースコントロールは、病院で異なるワークステーション間を素早く移動し、ログオンするたびに同じアプリケーションセットにアクセスする必要がある医療従事者を支援できます。ワークスペースコントロールオプションを許可するように構成すると、これらの医療従事者は1つのクライアントデバイスで複数のアプリケーションから切断し、別のクライアントデバイスで同じアプリケーションを開くために再接続できます。

ワークスペースコントロールは、次のアクティビティに影響します。

- **ログオン:** デフォルトでは、ワークスペースコントロールにより、ユーザーはログオン時に実行中のすべてのデスクトップとアプリケーションに自動的に再接続でき、手動で再開する必要がありません。ワークスペースコントロールを通じて、ユーザーは切断されたデスクトップやアプリケーション、および別のクライアントデバイスでアクティブになっているものを開くことができます。デスクトップまたはアプリケーションから切断しても、それはサーバー上で実行されたままになります。一部のデスクトップまたはアプリケーションを1つのクライアントデバイスで実行したままにし、別のクライアントデバイスでデスクトップまたはアプリケーションのサブセットに再接続する必要があるローミングユーザーがいる場合、以前にユーザーが切断したデスクトップまたはアプリケーションのみを開くようにログオン再接続動作を構成できます。
- **再接続:** サーバーにログオンした後、ユーザーは「再接続」をクリックすることで、いつでもすべてのデスクトップまたはアプリケーションに再接続できます。デフォルトでは、「再接続」は切断されたデスクトップまたはアプリケーション、および現在別のクライアントデバイスで実行されているものを開きます。以前にユーザーが切断したデスクトップまたはアプリケーションのみを開くように「再接続」を構成できます。
- **ログオフ:** StoreFront™ を介してデスクトップまたはアプリケーションを開くユーザーの場合、**ログオフ**コマンドを構成して、StoreFrontとすべてのアクティブなセッションからユーザーをログオフするか、StoreFrontのみからログオフすることができます。
- **切断:** ユーザーは、実行中のすべてのデスクトップとアプリケーションから一度に切断でき、個別に切断する必要はありません。

ワークスペースコントロールは、Citrix StoreFront接続を介してデスクトップおよびアプリケーションにアクセスするCitrix Workspaceアプリユーザーのみが利用できます。デフォルトでは、ワークスペースコントロールは仮想デスクトップセッションでは無効になっていますが、ホスト型アプリケーションでは有効になっています。公開されたデスクトップと、それらのデスクトップ内で実行されている公開されたアプリケーションの間では、デフォルトでセッション共有は行われません。

ユーザーが新しいクライアントデバイスに移動すると、ユーザーポリシー、クライアントドライブマッピング、およびプリンター構成が適切に変更されます。ポリシーとマッピングは、ユーザーがセッションにログオンしているクライアントデバイスに応じて適用されます。たとえば、医療従事者が救急治療室のデバイスからログオフし、X線検査室のワークステーションにログオンする場合、X線検査室でのセッションに適したポリシー、プリンターマッピング、およびクライアントドライブマッピングがセッション開始時に有効になります。

ユーザーが場所を変更したときに表示されるプリンターをカスタマイズできます。また、ユーザーがローカルプリンターに印刷できるかどうか、ユーザーがリモートで接続したときに消費される帯域幅の量、およびその他の印刷エクスペリエンスの側面を制御することもできます。

ユーザー向けにワークスペースコントロールを有効にして構成する方法については、StoreFrontのドキュメントを参照してください。

セッションローミング

注:

以下の情報は、PowerShellを使用してセッションローミングを構成するためのガイドです。代わりにWeb Studioを使用することもできます。詳細については、「デリバリーグループの管理」を参照してください。

デフォルトでは、セッションはユーザーとともにクライアントデバイス間をローミングします。ユーザーがセッションを起動し、別のデバイスに移動すると、同じセッションが使用され、両方のデバイスでアプリケーションが利用可能になります。アプリケーションは、デバイスや現在のセッションの有無にかかわらず追従します。多くの場合、アプリケーションに割り当てられたプリンターやその他のリソースも追従します。

このデフォルトの動作には多くの利点がありますが、すべての場合に理想的であるとは限りません。PowerShell SDKを使用してセッションローミングを防止できます。

例1：医療従事者が2台のデバイスを使用しており、デスクトップPCで保険フォームを完成させ、タブレットで患者情報を閲覧しています。

- セッションローミングが有効になっている場合、両方のアプリケーションが両方のデバイスに表示されます（1つのデバイスで起動されたアプリケーションは、使用中のすべてのデバイスで表示されます）。これはセキュリティ要件を満たさない可能性があります。

- セッションローミングが無効になっている場合、患者記録はデスクトップPCに表示されず、保険フォームはタブレットに表示されません。

例2：生産マネージャーがオフィスにあるPCでアプリケーションを起動します。デバイス名と場所によって、そのセッションで利用できるプリンターやその他のリソースが決まります。その日の後半、彼はプリンターの使用が必要な会議のため、隣の建物のオフィスに行きます。

- セッションローミングが有効になっている場合、生産マネージャーは会議室近くのプリンターにアクセスできない可能性があります。なぜなら、彼がオフィスで以前に起動したアプリケーションによって、その場所近くのプリンターやその他のリソースが割り当てられたためです。
- セッションローミングが無効になっている場合、彼が別のマシンに（同じ資格情報を使用して）ログオンすると、新しいセッションが開始され、近くのプリンターとリソースが利用可能になります。

セッションローミングの構成

セッションローミングを構成するには、「SessionReconnection」プロパティを持つ以下のエンタイトルメントポリシー規則コマンドレットを使用します。オプションで、「LeasingBehavior」プロパティも指定できます。

デスクトップセッションの場合：

```
Set-BrokerEntitlementPolicyRule <Delivery-Group-name> -SessionReconnection <value> -LeasingBehavior Allowed|Disallowed
```

アプリケーションセッションの場合：

```
Set-BrokerAppEntitlementPolicyRule <Delivery-Group-name> -SessionReconnection <value> -LeasingBehavior Allowed|Disallowed
```

`value` は次のいずれかになります。

- **Always:** セッションは、クライアントデバイスやセッションが接続されているか切断されているかに関係なく、常にローミングします。これがデフォルト値です。
- **DisconnectedOnly:** 既に切断されているセッションにのみ再接続します。それ以外の場合は、新しいセッションを起動します。（セッションは、最初に切断するか、Workspace Control を使用して明示的にローミングすることで、クライアントデバイス間をローミングできます。）別のクライアントデバイスからのアクティブな接続済みセッションは使用されません。代わりに、新しいセッションが起動されます。

- **SameEndpointOnly:** ユーザーは、使用するクライアントデバイスごとに一意のセッションを取得します。これにより、ローミングが完全に無効になります。ユーザーは、以前セッションで使用したのと同じデバイスにのみ再接続できます。

「LeasingBehavior」プロパティについては、以下で説明します。

他の設定からの影響:

セッションローミングの無効化は、デリバリーグループ内のアプリケーションのプロパティにあるアプリケーション制限 **ユーザーごとにアプリケーションのインスタンスを1つのみ許可** の影響を受けます。

- セッションローミングを無効にする場合は、「Allow only one instance ...」アプリケーション制限も無効にします。
- 「Allow only one instance ...」アプリケーション制限を有効にする場合は、新しいデバイスでの新しいセッションを許可する2つの値のいずれも構成しないでください。

ログオン間隔

デスクトップVDAを含む仮想マシンがログオンプロセス完了前に閉じられた場合、そのプロセスにより多くの時間を割り当てることができます。バージョン7.6以降のデフォルトは180秒です（7.0〜7.5のデフォルトは90秒です）。

マシン（またはマシンカタログで使用されるマスターイメージ）で、次のレジストリキーを設定します。

キー: `HKLM\SOFTWARE\Citrix\PortICA`

- 値: `AutoLogonTimeout`
- 種類: `DWORD`
- 0〜3600の範囲で、秒単位の10進数を指定します。

マスターイメージを変更した場合は、カタログを更新します。

この設定は、デスクトップVDAを持つVMにのみ適用されます。Microsoftは、サーバーVDAを持つマシンでのログオンタイムアウトを制御します。

設定

> **注:**

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

> Web Studioを使用して、以下の設定を管理できます。

- 認証の管理
- Studioログインページのデフォルトドメイン名を設定する
- Citrixカスタマーエクスペリエンス向上プログラム
- デリバリーコントローラーの削除
- データベースの場所を変更する
- 日付と時刻の設定
- サイト管理の一元化
- リモートPCアクセスで複数のユーザーの自動割り当てを有効にする
- DNS解決の有効化
- XML信頼の有効化
- セキュリティキーの管理
- Studioコンソールの非アクティブタイムアウトを設定する(#set-the-inactivity-timeout-for-the-studio-console)

認証の管理

デフォルトでは、ユーザーはドメインのユーザー名とパスワードを使用してWeb Studioにログオンします。スマートカード認証や統合Windows認証など、ユーザーに対して別の認証方法を選択することもできます。

Studio を使用して管理

ユーザーの認証方法を選択するには、次の手順に従います。

1. Web Studioにサインインし、左側のペインで「**設定**」を選択します。
2. 「**認証**」タイルを見つけて「**編集**」をクリックし、オプションを選択します。
    - 「**ドメイン資格情報**」
    - 「**ドメイン資格情報または統合Windows認証**」

統合 Windows 認証が有効になっている場合、ユーザーは Windows 資格情報 (Kerberos/NTLM) またはクライアント証明書を使用して Web Studio にアクセスできます。

Web StudioとDelivery Controller™が異なるマシンにインストールされている場合、統合Windows認証を機能させるには、「クロスオリジンアクセスを許可」を有効にし、Web StudioサーバーのURLを許可リストに追加します。

> 「**重要**」
>
> Web Studio が Delivery Controller のプロキシとして構成されている場合、統合 Windows 認証は機能しません。

- 「**スマートカード認証**」
- 「**ドメイン資格情報またはスマートカード認証**」

スマートカード認証を有効にするには、追加の構成が必要です。詳細については、Web Studio 用スマートカード認証のセットアップを参照してください。

PowerShell スクリプトを使用して管理

認証方法は、Delivery Controllerデータベースで構成されます。認証方法を設定するには、以下のPowerShellスクリプトを使用できます。

1. Delivery Controller で次のコマンドを実行して、現在のサイト ID を取得します。

   `Get-ConfigSite | Select SiteGuid`

2. 次のスクリプトを実行して認証方法を設定します。

```
# Generate a new bearer token

$bearerData = New-TrustBearerToken

# Define the Delivery Controller DNS name and Site ID

$ddc = "ddc.dc.com" # replace this with the Delivery Controller's DNS
name

$siteid = "c68a8f89-42af-4bea-a6e9-c8c936353f49" # replace this with
the site ID you get from step #1
```

```
# Define the URL and headers

$url = "https://$ddc/citrix/orchestration/api/CitrixOnPremises/Sites/
$siteid/Settings"

$headers = @{

"Content-Type" = "application/json"

"Authorization" = "Bearer $($bearerData.Token)"

}

# Define the JSON body

$body = @{

SupportedAuthenticators = "BasicAndSmartCard" # replace this with a
required authentication method: "Basic" for "Domain credentials";
"BasicAndIntegratedWindowsAuthentication" for "Domain credentials or
integrated Windows authentication"; "BasicAndSmartCard" for "Domain
credentials or smart card authentication"; "SmartCard" for "Smart card
authentication"

} | ConvertTo-Json -Depth 10

# Send the PATCH request

Invoke-RestMethod -Uri $url -Method Patch -Headers $headers -Body $body
```

統合Windows認証用にブラウザーを構成する

ドメイン資格情報または統合Windows認証を使用して*統合Windows認証*を有効にすると、次回ユーザーがサインインするときに、自動的にサインインされます。ユーザーとして自動的にサインインできない場合は、以下の手順に従ってWebブラウザーを構成し、統合Windows認証を許可してください。

Google Chromeの場合：

1. コントロールパネルから、**インターネットオプション**を選択します。
2. **詳細設定**タブを選択します。

3. **統合Windows認証を有効にする**を選択します。
4. **セキュリティ**タブを選択します。
5. **ローカルイントラネット > サイト > 詳細設定**を選択します。
6. **このWebサイトをゾーンに追加する**ボックスで：
    - Web Studio と Delivery Controller が同じサーバー上にある場合、Web Studio を実行しているホストの URL を入力します。
    - そうでない場合は、ワイルドカードドメインを入力します。例: Delivery Controller が `ddc.domain.com` にある場合、`*.domain.com` と入力します。
7. **追加 > 閉じる** をクリックします。

Mozilla Firefox の場合:

1. ブラウザーから、URL ボックスに `about:config` と入力します。
2. **検索** ボックスに `network negotiate` と入力します。
3. **network.negotiate-auth.trusted-uris** を右クリックし、**変更** を選択します。
4. **文字列値を入力** ボックスで:
    - Web Studio と Delivery Controller が同じサーバー上にある場合、Web Studio をホストしているサーバー名を参照する URL および/またはエイリアスのコンマ区切りリストを追加します。
    - そうでない場合は、次のように URL を追加します。例: Delivery Controller が `ddc.domain.com` にある場合、`*.domain.com` と入力します。

ブラウザーを設定したら、サインインページで **Windows 統合サインイン** をクリックして再試行できます。

Web Studio と Delivery Controller が異なるマシンにインストールされている場合、統合 Windows 認証を機能させるには、**クロスオリジンアクセスを許可** を有効にする必要があります。

クロスオリジンアクセスを許可 を有効にするには、次の手順に従います。

1. **クロスオリジンアクセスを許可** チェックボックスをオンにします。
2. Web Studio サーバーの URL を許可リストに追加します。
3. 「**URLの入力**」フィールドにURLを入力します。必要に応じて「**追加**」をクリックしてさらに追加します。

> **注**
>
> - URL は正しい形式 `<scheme>://<hostname>` に従う必要があります。パスや末尾のスラッシュを含まないようにしてください。
> - IP アドレスと FQDN がサポートされています。URL を追加するときは、Web Studio へのアクセス方法と一致していることを確認してください。たとえば、IP アドレスを使用して Web Studio にアクセスする場合は、IP アドレスベースの URL をリストに追加します。
> - デフォルト以外のポートを使用する場合は、ポート番号を含めるようにしてください。

4. 必要に応じて、「**追加**」をクリックしてさらに追加します。
5. 完了したら、「**完了**」をクリックして保存し、終了します。

Studioログインページのデフォルトドメイン名を設定する

Studioログインページの**ドメイン**フィールドにドメイン名を自動入力するには、次の手順に従います。

1. Web Studioにサインインし、左ペインで設定を選択します。
2. **ドメイン名の構成**タイルで、必要に応じてドメイン名を入力します。
3. **適用**をクリックします。

   管理者がStudioログインページにアクセスすると、設定したドメイン名が*ドメイン*フィールドに自動的に入力されます。

タイムゾーンを設定する

DaaSサイトのデフォルトのタイムゾーン、日付形式、時刻形式を構成します。Studioは、これらの設定を時刻表示や、スケジュールされた再起動や自動スケーリングなどのスケジューリングに使用します。

必要に応じて、個々のデリバリーグループのタイムゾーンを変更できます。詳細については、「デリバリーグループのユーザー設定を変更する」を参照してください。

> **注:**

> この設定は、Citrixユーザーアカウントごとに異なります。

> デフォルトのタイムゾーンを設定するには、次の手順に従います。

1. Web Studioから、**「設定」>「日付と時刻」**に移動します。
2. **「編集」**をクリックします。
3. 次の設定を構成します。

   - **日付形式**: 日付の表示方法を選択します（例: yyyy/MM/dd）。

     > **注:**
     >
     > Studioで選択した言語に関連付けられた日付形式を使用するには、**「ローカルを使用」**を選択します。

   - **時刻形式:** 12時間形式（例：午後09:00）または24時間形式（例：21:00）で時刻を表示するように選択します。

     > **注:**
     >
     > Studioで選択した言語に関連付けられた時刻形式を使用するには、**「ローカルを使用」**を選択します。

   - **タイムゾーン:** タイムゾーンを選択します。

     > **注:**
     >
     > コンピューターのタイムゾーン設定を使用するには、「**Use local**」を選択します。

4. 「**保存**」をクリックします。

   > **注:**

> Web Studio全体で、表示されている時刻にカーソルを合わせると、ローカルタイムゾーンでの同等の時刻を確認できます。

DNS解決を有効にする

ICA®ファイルでIPアドレスの代わりにDNS名を表示するには、次の手順に従います。

1. Web Studioにサインインし、左ペインで「**設定**」を選択します。
2. 「**DNS解決を有効にする**」設定をオンにします。

Studioコンソールの非アクティビティタイムアウトを設定する

管理者がStudioコンソールから自動的にサインアウトされるまでの非アクティビティ期間を設定できます。

1. Web Studioにサインインし、左ペインで「**設定**」を選択します。
2. 10分から24時間の範囲で期間を入力します。
3. この設定を適用するには、ページを更新するか、サインアウトしてから再度サインインします。

サイト管理の一元化

この機能を使用すると、1つのWeb Studioコンソールで複数のCitrix Virtual Apps and Desktopsサイトを管理できます。詳細については、「複数のサイト管理を有効にする」を参照してください。

タグ

> **注:**

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

はじめに

タグは、マシン、アプリケーション、デスクトップ、デリバリーグループ、アプリケーショングループ、ポリシーなどの項目を識別する文字列です。タグを作成して項目に追加すると、特定のタグを持つ項目にのみ適用されるように特定の操作を調整できます。

- Web Studioでの検索表示を調整します。

  たとえば、テスター向けに最適化されたアプリケーションのみを表示するには、「test」という名前のタグを作成し、それらのアプリケーションに追加（適用）します。これで、Web Studioの検索を「test」タグでフィルタリングできます。
- 選択したデリバリーグループ内のマシンの一部のみを考慮して、アプリケーショングループからアプリケーションを公開したり、デリバリーグループから特定のデスクトップを公開したりします。これは*タグ制限*と呼ばれます。

  タグ制限を使用すると、既存のマシンを複数の公開タスクに使用できるため、より多くのマシンを展開および管理するコストを節約できます。タグ制限は、デリバリーグループ内のマシンを細分化（またはパーティション分割）するものと考えることができます。その機能は、XenApp 7.xより前のリリースにおけるワーカーグループと似ていますが、同一ではありません。

  タグ制限付きのアプリケーショングループまたはデスクトップを使用すると、デリバリーグループ内のマシンの一部を分離してトラブルシューティングする際に役立ちます。
- デリバリーグループ内のマシンの一部に対して定期的な再起動をスケジュールします。

  マシンにタグ制限を使用すると、新しいPowerShellコマンドレットを使用して、デリバリーグループ内のマシンの一部に対して複数の再起動スケジュールを構成できます。例と詳細については、「デリバリーグループの管理」を参照してください。
- 指定されたタグを持つ（または持たない）デリバリーグループ、デリバリーグループの種類、またはOU内のマシンの一部に対して、Citrixポリシーの適用（割り当て）を調整します。

  たとえば、より高性能なワークステーションにのみCitrixポリシーを適用したい場合は、それらのマシンに「high power」という名前のタグを追加します。次に、ポリシー作成ウィザードの**ポリシーの割り当て**ページで、そのタグと**有効にする**チェックボックスを選択します。デリバリーグループにタグを追加し、そのグループにCitrixポリシーを適用することもできます。詳細については、「ポリシーの作成」を参照してください。

タグは以下に適用できます。

- マシン

- アプリケーション
- マシンカタログ (PowerShellのみ。「マシンカタログのタグ」を参照)
- デリバリーグループ
- アプリケーショングループ

Web Studioで以下を作成または編集する際に、タグ制限を構成できます。

- 共有デリバリーグループ内のデスクトップ
- アプリケーショングループ

> **重要:**
>
> タグは、マシンに明示的に適用することも、マシンカタログまたはデリバリーグループレベルで明示的に適用することもできます。タグがマシンカタログまたはデリバリーグループレベルで適用されると、そのカタログまたはデリバリーグループ内のすべてのマシンが暗黙的にそのタグを継承します。これらの継承されたタグは、マシンレベルで削除することはできません。タグの効果を削除するには、マシンカタログまたはデリバリーグループレベルからタグを削除する必要があります。

デスクトップまたはアプリケーショングループのタグ制限

タグ制限にはいくつかの手順があります。

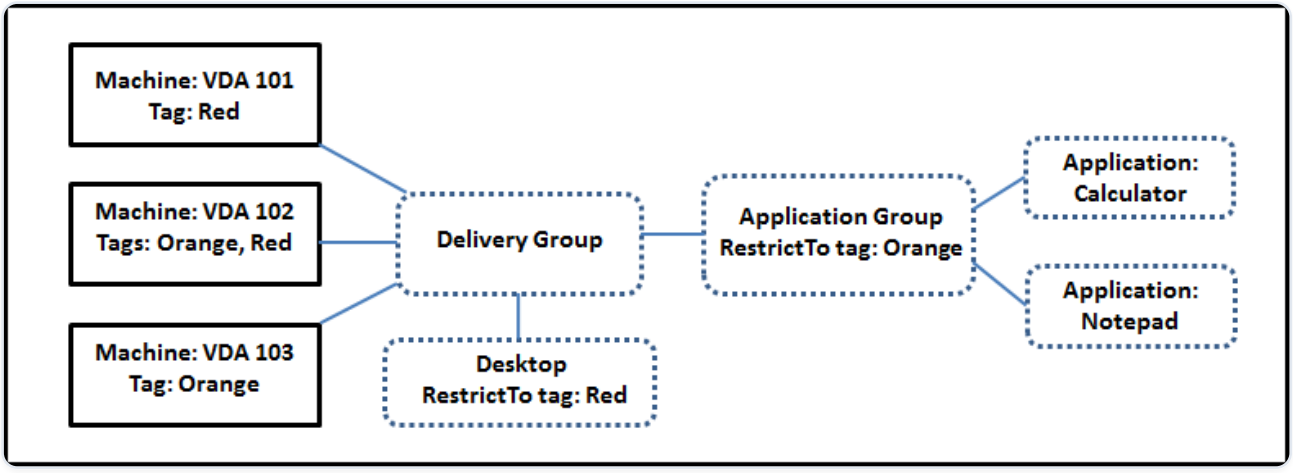
- タグを作成し、マシンに追加（適用）します。
- タグ制限付きのグループを作成または編集します（つまり、「タグxを持つマシンへの起動を制限する」）。

タグ制限は、ブローカーのマシン選択プロセスを拡張します。ブローカーは、関連付けられたデリバリーグループから、アクセスポリシー、構成されたユーザーリスト、ゾーン設定、起動準備、およびタグ制限（存在する場合）に従ってマシンを選択します。アプリケーションの場合、ブローカーは優先順位に従って他のデリバリーグループにフォールバックし、検討対象の各デリバリーグループに同じマシン選択ルールを適用します。

例1：シンプルなレイアウト

この例では、タグ制限を使用して、特定のデスクトップおよびアプリケーションの起動に考慮されるマシンを制限するシンプルなレイアウトを紹介します。サイトには、共有デリバリーグループ

が1つ、公開デスクトップが1つ、2つのアプリケーションで構成されたアプリケーショングループが1つあります。



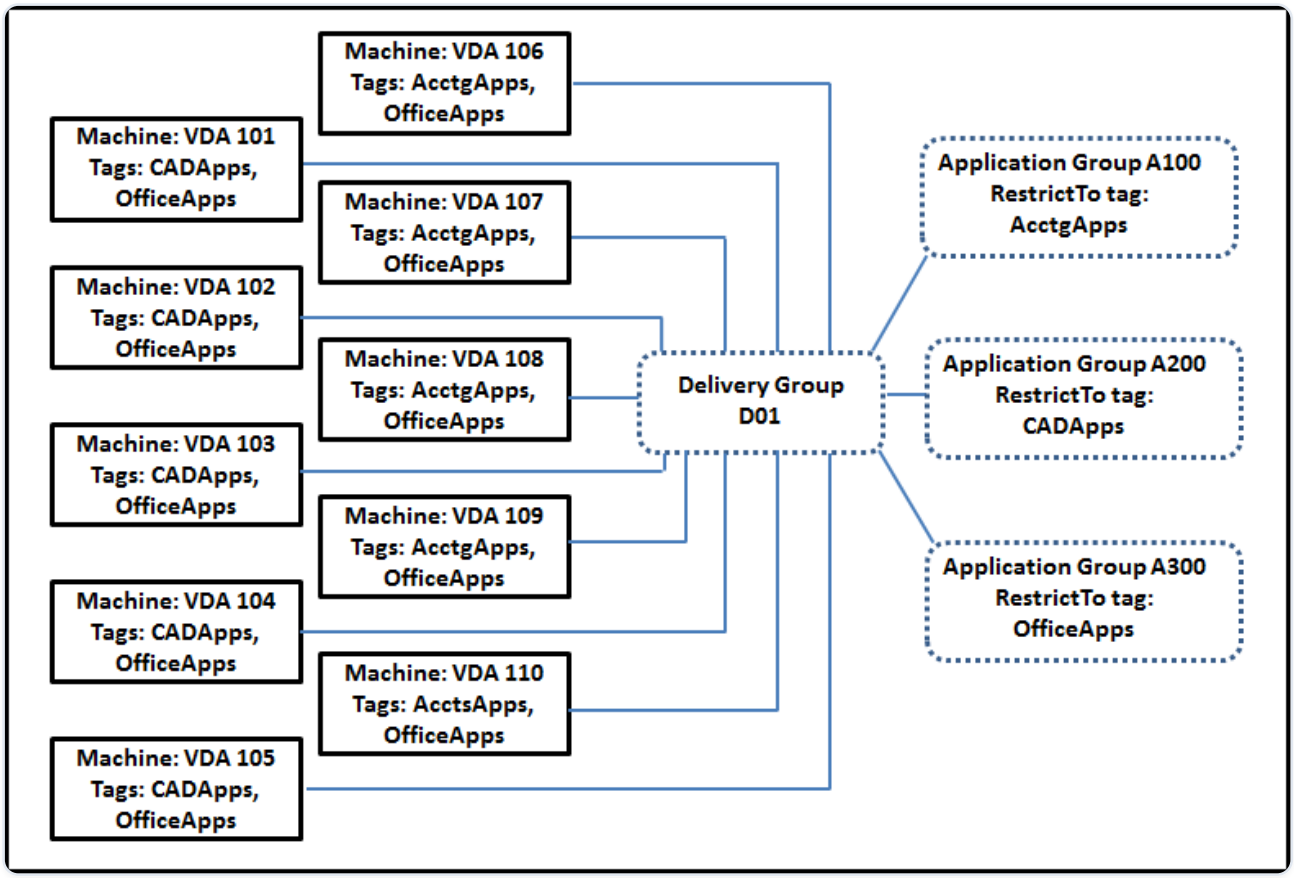
- 3台のマシン（VDA 101～103）のそれぞれにタグが追加されています。
- 共有デリバリーグループ内のデスクトップは、「Red」という名前のタグ制限で作成されました。デスクトップは、そのデリバリーグループ内で「Red」タグを持つマシン（VDA 101および102）でのみ起動できます。
- アプリケーショングループは「Orange」タグ制限で作成されたため、そのアプリケーション（CalculatorとNotepad）はそれぞれ、そのデリバリーグループ内で「Orange」タグを持つマシン（VDA 102および103）でのみ起動できます。

マシンVDA 102は両方のタグ（RedとOrange）を持っているため、アプリケーションとデスクトップの起動に考慮されます。

例2：より複雑なレイアウト

この例には、タグ制限で作成された複数のアプリケーショングループが含まれています。これにより、デリバリーグループのみを使用した場合に必要となるよりも少ないマシンで、より多くのアプリケーションを提供できるようになります。

(#how-to-configure-example-2)は、この例でタグを作成して適用し、タグ制限を構成する手順を示しています。



この例では、10台のマシン（VDA 101～110）、1つのデリバリーグループ（D01）、および3つのアプリケーショングループ（A100、A200、A300）を使用しています。各マシンにタグを適用し、各アプリケーショングループの作成時にタグ制限を指定することで、次のことが可能になります。

- グループ内の経理ユーザーは、5台のマシン（VDA 101～105）で必要なアプリにアクセスできます
- グループ内のCAD設計者は、5台のマシン（VDA 106-110）で必要なアプリにアクセスできます
- グループ内でOfficeアプリケーションを必要とするユーザーは、10台のマシン（VDA 101～110）でOfficeアプリにアクセスできます

使用されるマシンは10台のみで、デリバリーグループは1つだけです。デリバリーグループのみを使用する場合（アプリケーショングループなし）は、マシンが1つのデリバリーグループにしか属せないため、2倍の数のマシンが必要になります。

タグとタグ制限の管理

タグは、Web Studioの**［タグの管理］**アクションを通じて、選択したアイテムに対して作成、追加（適用）、編集、削除されます。

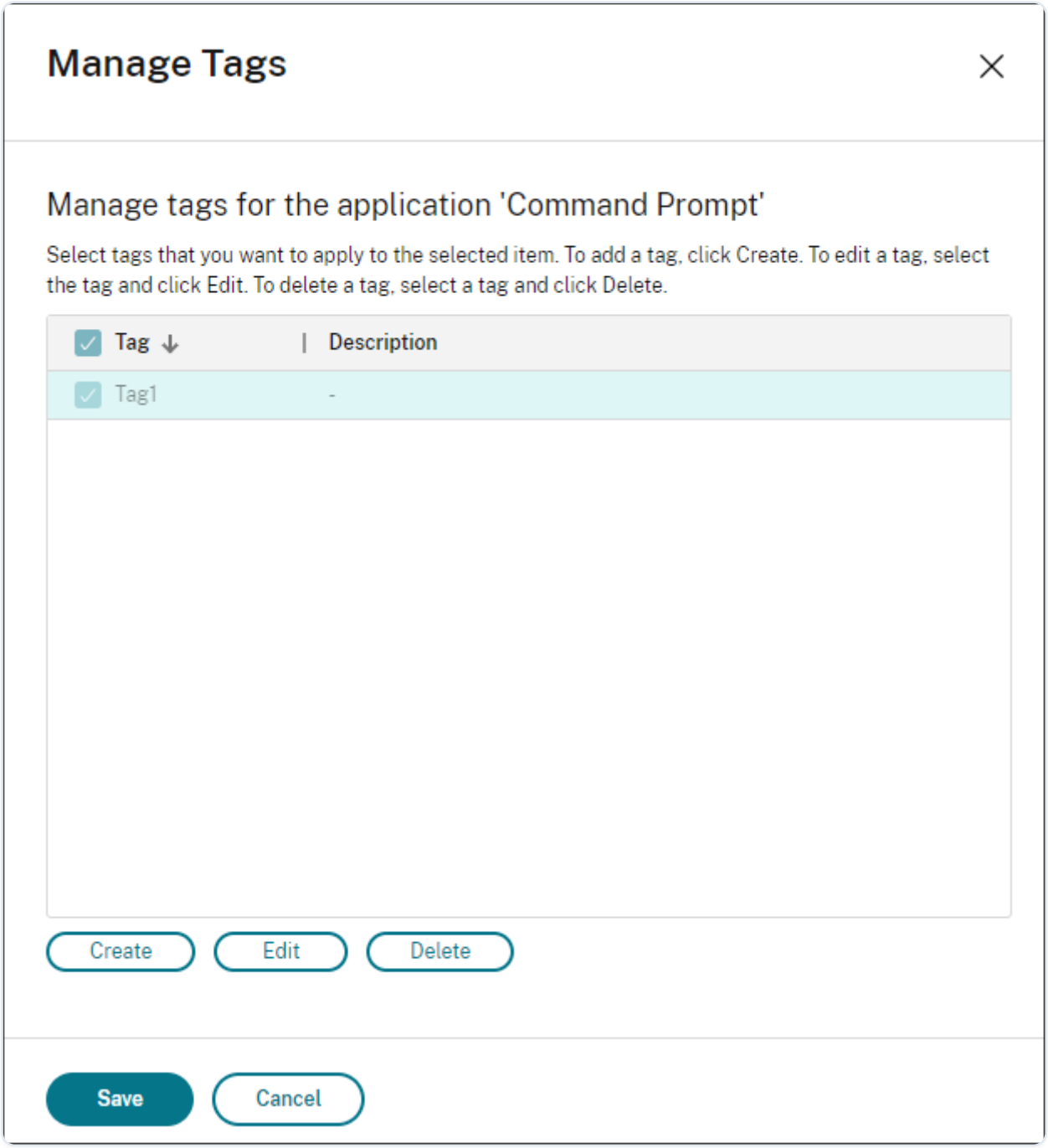
（例外：ポリシー割り当てに使用されるタグは、Web Studioの**［タグの管理］**アクションを通じて作成、編集、削除されます。ただし、タグはポリシーの作成時に適用（割り当て）されます。詳細については、「ポリシーの作成」を参照してください。）

タグ制限は、デリバリーグループでデスクトップを作成または編集するとき、およびアプリケーショングループを作成および編集するときに構成されます。

Web Studioで［タグの管理］ダイアログを使用する

Web Studioで、タグを適用するアイテム（1つまたは複数のマシン、アプリケーション、デスクトップ、デリバリーグループ、またはアプリケーショングループ）を選択し、アクションバーで**［タグの管理］**を選択します。ダイアログボックスには、選択したアイテムだけでなく、サイトで作成されたすべてのタグが一覧表示されます。

- チェックマークが付いたチェックボックスは、そのタグが選択したアイテムに既に追加されていることを示します。（以下のスクリーンショットでは、選択したマシンに「Tag1」という名前のタグが適用されています。）
- 複数のアイテムを選択した場合、ハイフンが付いたチェックボックスは、選択したアイテムの一部にのみそのタグが追加されていることを示します。



タグの管理ダイアログボックスから、次のアクションが利用できます。タグを使用する際の注意点を必ず確認してください。

- **タグを作成するには:**

  作成をクリックします。名前と説明を入力します。タグ名は一意である必要があり、大文字と小文字は区別されません。次に**OK**をクリックします。（タグを作成しても、選択した項目に自動的に適用されるわけではありません。チェックボックスを使用してタグを適用してください。）

- **1つ以上のタグを追加（適用）するには:**

タグ名の横にあるチェックボックスを有効にします。複数の項目を選択していて、タグの横にあるチェックボックスにハイフンが含まれている場合（選択した項目の一部にのみタグがすでに適用されていることを示す）、それをチェックマークに変更すると、選択したすべてのマシンに影響します。

1つ以上のマシンにタグを追加しようとしたときに、そのタグがアプリケーショングループで制限として使用されている場合、その操作によってそれらのマシンが起動可能になる可能性があるという警告が表示されます。それが意図した動作であれば、続行してください。

- **1つ以上のタグを削除するには:**

  タグ名の横にあるチェックボックスをオフにします。複数の項目を選択していて、タグの横にあるチェックボックスにハイフンが含まれている場合（選択した項目の一部にのみタグが適用されていることを示す）、チェックボックスをオフにすると、選択したすべてのマシンからタグが削除されます。

  制限としてタグを使用しているマシンからタグを削除しようとすると、その操作が起動対象となるマシンに影響を与える可能性があるという警告が表示されます。それが意図した動作であれば、続行してください。

- **タグを編集するには:**

  タグを選択し、**編集**をクリックします。新しい名前、説明、またはその両方を入力します。一度に編集できるタグは1つだけです。

- **1つ以上のタグを削除するには:**

  タグを選択し、**削除**をクリックします。「タグの削除」ダイアログボックスには、現在選択されているタグを使用している項目の数（例：「2台のマシン」）が表示されます。項目をクリックすると、詳細情報が表示されます。たとえば、「2台のマシン」項目をクリックすると、そのタグが適用されている2台のマシン名が表示されます。タグを削除するかどうかを確認します。

  制限として使用されているタグをWeb Studioで削除することはできません。まず、アプリケーショングループを編集し、タグの制限を削除するか、別のタグを選択してください。

タグの管理ダイアログボックスでの作業が完了したら、**保存**をクリックします。

マシンにタグが適用されているかどうかを確認するには、左ペインで**デリバリーグループ**を選択します。中央ペインでデリバリーグループを選択し、アクションバーで**マシンの表示**を選択します。中央ペインでマシンを選択し、**詳細**ペインで**タグ**タブを選択します。

タグの制限を管理する

タグの制限を構成するには、複数の手順が必要です。まずタグを作成し、それをマシンに追加/適用します。次に、アプリケーショングループまたはデスクトップに制限を追加します。

- **タグを作成して適用する：**

  タグを作成し、前述の**タグの管理**アクションを使用して、タグの制限の影響を受けるマシンにタグを追加（適用）します。

- **アプリケーショングループにタグ制限を追加するには：**

  アプリケーショングループを作成または編集します。**デリバリーグループ**ページで、**タグを持つマシンへの起動を制限する**を選択し、リストからタグを選択します。

- **アプリケーショングループのタグ制限を変更または削除するには：**

  グループを編集します。**デリバリーグループ**ページで、リストから別のタグを選択するか、**タグを持つマシンへの起動を制限する**のチェックを外してタグ制限を完全に削除します。

- **デスクトップにタグ制限を追加するには：**

  デリバリーグループを作成または編集します。**デスクトップ**ページで、**追加**または**編集**をクリックします。「デスクトップの追加」ダイアログボックスで、**タグを持つマシンへの起動を制限する**を選択し、メニューからタグを選択します。

- **デリバリーグループのタグ制限を変更または削除するには：**

  グループを編集します。デスクトップページで、**編集**をクリックします。ダイアログボックスで、リストから別のタグを選択するか、**タグを持つマシンへの起動を制限する**のチェックを外してタグ制限を完全に削除します。

タグを使用する際の注意点

アイテムに適用されたタグはさまざまな目的に使用できるため、タグの追加、削除、および削除が意図しない影響を与える可能性があることに注意してください。Web Studioの検索フィールドでマシンの表示を並べ替えるためにタグを使用できます。アプリケーショングループまたはデスクトップを構成する際に、同じタグを制限として使用できます。このタグは、起動の考慮事項を、そのタグを持つ指定されたデリバリーグループ内のマシンのみに制限します。

デスクトップまたはアプリケーショングループのタグ制限としてタグが構成された後で、そのタグをマシンに追加しようとすると、警告が表示されます。そのタグを追加すると、マシンが追加のアプリケーションまたはデスクトップの起動に利用可能になる可能性があります。それが意図したとおりであれば、続行してください。そうでない場合は、操作をキャンセルできます。

たとえば、「Red」タグ制限を持つアプリケーショングループを作成したとします。その後、そのアプリケーショングループで使用されているのと同じデリバリーグループに他のマシンをいくつか追加します。そのマシンに「Red」タグを追加しようとすると、Web Studioは次のようなメッセージを表示します。「タグ「Red」は、以下のアプリケーショングループの制限として使用されています。このタグを追加すると、選択したマシンがこのアプリケーショングループ内のアプリケーションを起動できるようになる可能性があります。」その後、それらの追加のマシンにそのタグを追加することを確認またはキャンセルできます。

同様に、アプリケーショングループがタグを使用して起動を制限している場合、Web Studioは、制限として削除するためにグループを編集するまでタグを削除できないことを警告します。（アプリケーショングループで制限として使用されているタグを削除することが許可された場合、そのアプリケーショングループに関連付けられたデリバリーグループ内のすべてのマシンでアプリケーションが起動できるようになる可能性があります。）タグがデスクトップ起動の制限として使用されている場合も、タグの削除に対する同じ禁止事項が適用されます。そのタグ制限を削除するためにアプリケーショングループまたはデリバリーグループ内のデスクトップを編集した後、タグを削除できます。

すべてのマシンが同じアプリケーションセットを持っているとは限りません。ユーザーは複数のアプリケーショングループに属することができ、それぞれが異なるタグ制限と、デリバリーグループからの異なるまたは重複するマシンセットを持っています。次の表は、マシンの考慮事項がどのように決定されるかを示します。

アプリケーションが追加された場合	選択されたデリバリーグループ内のこれらのマシンが起動対象と見なされます
タグ制限のないアプリケーショングループが1つ	任意のマシン。
タグ制限Aのあるアプリケーショングループが1つ	タグAが適用されているマシン。
タグ制限Aのあるアプリケーショングループと、タグ制限Bのあるアプリケーショングループの2つ	タグAとタグBの両方を持つマシン。利用可能なマシンがない場合は、タグAまたはタグBを持つマシン。
タグ制限Aのあるアプリケーショングループと、タグ制限のないアプリケーショングループの2つ	タグAを持つマシン。利用可能なマシンがない場合は、任意のマシン。

マシン再起動スケジュールでタグ制限を使用した場合、タグの適用または制限に影響を与える変更は、次のマシン再起動サイクルに影響します。変更が行われている間に進行中の再起動サイクルには影響しません。

例2の構成方法

以下の手順では、タグを作成して適用し、2番目の例で示されているアプリケーショングループのタグ制限を構成する手順を示します。

VDAとアプリケーションはすでにマシンにインストールされており、デリバリーグループも作成されています。

マシンにタグを作成して適用します。

1. Web Studioで、デリバリーグループD01を選択し、アクションバーで**マシンを表示**を選択します。
2. マシン VDA 101～105 を選択し、アクションバーで**タグの管理**を選択します。
3. ダイアログボックスで、**作成**をクリックし、`CADApps`という名前のタグを作成します。**OK**をクリックします。
4. もう一度**作成**をクリックし、OfficeAppsという名前のタグを作成します。**OK**をクリックします。
5. **タグの管理**ダイアログボックスを開いたまま、各タグの名前（`CADApps`と`OfficeApps`）の横にあるチェックボックスをオンにして、新しく作成したタグを選択したマシンに追加（適用）します。完了したら、ダイアログボックスを閉じます。
6. デリバリーグループD01を選択し、アクションバーで**マシンの表示**を選択します。
7. マシン VDA 106～110 を選択し、アクションバーで**タグの管理**を選択します。
8. **タグの管理**ダイアログボックスで、**作成**をクリックします。`AcctgApps`という名前のタグを作成します。**OK**をクリックします。
9. 各タグ名の横にあるチェックボックスをクリックして、新しく作成した`AcctgApps`タグと`OfficeApps`タグを選択したマシンに適用し、ダイアログボックスを閉じます。

タグ制限付きのアプリケーショングループを作成します。

1. Web Studioで、左側のペインで**アプリケーション**を選択し、**アプリケーショングループ**タブを選択し、アクションバーで**アプリケーショングループの作成**を選択します。アプリケーショングループの作成ウィザードが起動します。
2. ウィザードの**デリバリーグループ**ページで、デリバリーグループD01を選択します。**タグ付きマシンへの起動を制限**を選択し、リストから`AcctgApps`タグを選択します。

3. ウィザードを完了し、経理ユーザーと経理アプリケーションを指定します。（アプリケーションを追加するときは、`AcctgApps`タグを持つマシンでアプリケーションを検索する**スタートメニューから**ソースを選択します。）**概要**ページで、グループに`A100`という名前を付けます。
4. 前述の手順を繰り返して、アプリケーショングループ`A200`を作成し、`CADApps`タグを持つマシンと、適切なユーザーおよびアプリケーションを指定します。
5. 手順を繰り返して、アプリケーショングループ`A300`を作成し、`OfficeApps`タグを持つマシンと、適切なユーザーおよびアプリケーションを指定します。

マシンカタログのタグ

マシンカタログでタグを使用できます。タグを作成し、それをカタログに適用する全体的な手順は、以前に説明したとおりです。ただし、カタログへのタグの適用はPowerShellインターフェイスを介してのみサポートされています。Web Studioを使用してカタログにタグを適用したり、カタログからタグを削除したりすることはできません。Web Studioのカタログ表示では、タグが適用されているかどうかは示されません。

概要: Web StudioまたはPowerShellを使用して、カタログで使用するタグを作成または削除できます。タグをカタログに適用するにはPowerShellを使用します。

カタログでタグを使用する例をいくつか示します。

- デリバリーグループには複数のカタログからのマシンが含まれていますが、操作（再起動スケジュールなど）を特定のカタログ内のマシンのみに影響させたい場合。そのカタログにタグを適用することで、それが実現できます。
- アプリケーショングループで、アプリケーションセッションを特定のカタログ内のマシンに制限したい場合。そのカタログにタグを適用することで、それが実現できます。

影響を受けるPowerShellコマンドレット:

- `Add-BrokerTag`や`Remove-BrokerTag`などのコマンドレットにカタログオブジェクトを渡すことができます。
- `Get-BrokerTagUsage`は、タグを含むカタログの数を示します。
- `Get-BrokerCatalog`には`Tags`という名前のプロパティがあります。

例えば、次のコマンドレットは、`acctg`という名前のカタログに`fy2018`という名前のタグを追加します。`Get-BrokerCatalog -Name acctg | Add-BrokerTag fy2018`。（このタグは、以前にWeb StudioまたはPowerShellを使用して作成されています。）

詳細なガイダンスと構文については、PowerShellコマンドレットのヘルプを参照してください。

自動タグ

自動タグを使用すると、マシン、アプリケーショングループ、アプリケーション、デスクトップグループ、またはデスクトップへのタグの自動追加および削除のルールを定義できます。定義されたルールを満たさない場合、タグも自動的に削除されます。この機能強化により、環境最適化のために定期的に実行されるさまざまなスクリプトを維持する必要がなくなります。

ユースケース

自動タグ付けを使用すると、コスト削減、インフラストラクチャの最適化、消費の促進など、ビジネスドライバーに関連するルールを実装できます。以下にいくつかのユースケースを示します。

- **未使用のVDIを再利用** - 事前設定された日数以上使用されていない専用ワークロードを、利用可能なプールに解放するため。
- **アプリの煩雑さを解消** - 事前設定された日数以上使用されていないアプリケーションを特定することで、アプリケーションの煩雑さを軽減するため。
- **X未満の機能レベルを持つDG** - 特定の機能レベル未満のデリバリーグループを見つけるため。
- **非アクティブユーザー** - 事前設定された日数以上ログオンしていないユーザーのリソースを再利用するため。

> **注:**
>
> 30日以上使用されていないマシンに付与されたタグは、30日後にユーザーがそのマシンにログオンして次回実行されたときに、そのマシンから削除されます。

PowerShellコマンド

PowerShellコマンドを使用して自動タグを作成できます。自動タグルールが作成されると、3600秒の頻度で評価されます。詳細については、New-BrokerAutoTagRuleを参照してください。

`New-BrokerAutoTagRule` のパラメーターは次のとおりです。

- 名前: ルールの汎用名
- オブジェクトタイプ: マシン
- ルールテキスト: ルールを定義するフィルター。
- タグUid: 関連付けたいタグID。

例

1. 30日以上使用されていない専用VDIにタグを付けるには:

```
New-BrokerAutoTagRule -Name ‘UnusedVdi’ -ObjectType ‘Machine’ -RuleText
“-AllocationType Static -IsAssigned $true -Filter { SummaryState -ne
`”InUse`” -and ( LastConnectionTime -lt ‘-30’ -or LastConnectionTime
-eq `$null ) }” -TagUid 123
```

ルールが構成された後、タグ **unused-VDI** が付いたマシンは解放されます。

2. X未満の機能レベルを持つデリバリーグループにタグを付けるには (**L7_20** をしきい値機能レベルとして使用):

```
New-BrokerAutoTagRule -Name 'LowFL' -ObjectType 'DesktopGroup'
-RuleText " -Filter { MinimumFunctionalLevel -lt 'L7_20' } " -TagUid
143
```

3. フォルダーなしで公開された、ユーザーに表示されるアプリにタグを付けるには:

```
New-BrokerAutoTagRule -Name 'NoFolder' -ObjectType 'Application'
-RuleText "-Enabled $true -Filter { ClientFolder -eq $null } " -TagUid
153`
```

詳細情報

ブログ投稿: 特定のサーバーにデスクトップを割り当てる方法。

ユーザープロファイル

デフォルトでは、Virtual Delivery Agentをインストールすると、Citrix Profile Managementはマスターイメージにサイレントインストールされますが、プロファイルソリューションとしてProfile Managementを使用する必要はありません。

ユーザーのさまざまなニーズに合わせて、Citrix Virtual Apps and Desktops™ポリシーを使用して、各デリバリーグループのマシンに異なるプロファイル動作を適用できます。たとえば、あるデリバリーグループでは、テンプレートが1つのネットワークロケーションに保存されているCitrix強制プロファイルが必要な場合があり、別のデリバリーグループでは、複数のリダイレクトされたフォルダーを持つ別のロケーションに保存されているCitrixローミングプロファイルが必要な場合があります。

- 組織内の他の管理者がCitrix Virtual Apps and Desktopsのポリシーを担当している場合は、彼らと協力して、Delivery Group全体でプロファイル関連のポリシーが設定されていることを確認してください。

- Profile Managementポリシーは、グループポリシー、Profile Management .iniファイル、および個々の仮想マシン上でローカルに設定することもできます。プロファイル動作を定義するこれらの複数の方法は、次の順序で読み取られます。

  a. グループポリシー（.admまたは.admxファイル）

  b. ポリシーノード内のCitrix Virtual Apps and Desktopsポリシー

  c. ユーザーが接続する仮想マシン上のローカルポリシー

  d. Profile Management .iniファイル

  たとえば、グループポリシーとポリシーノードの両方で同じポリシーを構成した場合、システムはグループポリシーのポリシー設定を読み取り、Citrix Virtual Apps and Desktopsポリシー設定を無視します。

どのプロファイルソリューションを選択しても、Director管理者は診断情報にアクセスし、ユーザープロファイルのトラブルシューティングを行うことができます。詳細については、Directorのドキュメントを参照してください。

自動構成

デスクトップタイプは、Virtual Delivery Agentのインストールに基づいて自動的に検出され、Studioで行う構成の選択に加えて、それに応じてProfile Managementのデフォルトが設定されます。

Profile Managementが調整するポリシーを次の表に示します。デフォルト以外のポリシー設定はすべて保持され、この機能によって上書きされることはありません。各ポリシーの詳細については、Profile Managementのドキュメントを参照してください。プロファイルを作成するマシンの種類は、調整されるポリシーに影響します。主な要因は、マシンが永続的かプロビジョニング済みか、および複数のユーザーで共有されるか、1人のユーザー専用であるかです。

永続システムには何らかのローカルストレージがあり、その内容はシステムがオフになっても永続することが期待されます。永続システムは、SANなどのストレージテクノロジーを使用してローカルディスクを模倣する場合があります。対照的に、プロビジョニング済みシステムは、ベースディスクと何らかのIDディスクから「オンザフライ」で作成されます。ローカルストレージは通常、RAMディスクまたはネットワークディスクによって模倣され、後者は高速リンクを備えたSANによって提供されることがよくあります。プロビジョニングテクノロジーは通常、Citrix ProvisioningまたはMachine Creation Services™（またはサードパーティの同等品）です。プロビジョニング済みシステムが永続的なローカルストレージを持つ場合もあります。これらは永続的として分類されます。

これら2つの要素を合わせると、以下のマシンタイプが定義されます。

- **永続的かつ専用**。例としては、Machine Creation Servicesで作成された静的割り当てと永続的なローカルストレージを持つシングルセッションOSマシン、物理ワークステーション、ラップトップなどがあります。
- **永続的かつ共有**。例としては、Machine Creation Servicesで作成されたマルチセッションOSマシン、およびCitrix Virtual Appsサーバーなどがあります。
- **プロビジョニング済みかつ専用**。例としては、静的割り当てを持つが永続ストレージを持たないシングルセッションOSマシンで、Citrix Provisioning Service (Citrix Virtual Desktops™内) で作成されたものなどがあります。
- **プロビジョニング済みかつ共有**。例としては、ランダム割り当てを持つシングルセッションOSマシンで、Citrix Provisioning™ Service (Citrix Virtual Desktops内) で作成されたもの、およびCitrix Virtual Appsサーバーなどがあります。

以下のProfile Managementポリシー設定は、異なるマシンタイプに対する推奨ガイドラインです。ほとんどの場合にうまく機能しますが、展開の要件に応じてこれらから逸脱することもできます。

> **重要:**
>
> **ログオフ時にローカルにキャッシュされたプロファイルを削除**、**プロファイルストリーミング**、および**常にキャッシュ**は、自動構成機能によって適用されます。その他のポリシーは手動で調整してください。

永続マシン

ポリシー	永続的かつ専用	永続的かつ共有
ログオフ時にローカルにキャッシュされたプロファイルを削除する	無効	有効
プロファイルストリーミング	無効	有効
常にキャッシュ	有効 (注1)	無効 (注2)
アクティブライトバック	無効	無効 (注3)
ローカル管理者のログオンを処理	有効	無効 (注4)

プロビジョニング済みマシン

ポリシー	プロビジョニング済みと専用の両方	プロビジョニング済みと共有の両方
ログオフ時にローカルにキャッシュされたプロファイルを削除する	無効 (注5)	有効
プロファイルストリーミング	有効	有効
常にキャッシュ	無効 (注6)	無効
アクティブライトバック	有効	有効
ローカル管理者のログオンを処理する	有効	有効 (注 7)

1. このマシンタイプでは**プロファイルストリーミング**が無効になっているため、**常にキャッシュ**設定は常に無視されます。
2. **常にキャッシュ**を無効にします。ただし、このポリシーを有効にし、ファイルサイズ制限 (MB単位) を定義することで、ログオン後できるだけ早く大きなファイルがプロファイルにロードされるようにすることができます。このサイズ以上のファイルは、できるだけ早くローカルにキャッシュされます。
3. Citrix Virtual Appsサーバー間をローミングするユーザーのプロファイルへの変更を保存する場合を除き、**アクティブなライトバック**を無効にします。この場合は、このポリシーを有効にします。
4. ホスト型共有デスクトップの場合を除き、**ローカル管理者によるログオンの処理**を無効にします。この場合は、このポリシーを有効にします。
5. **ログオフ時にローカルにキャッシュされたプロファイルを削除**を無効にします。この設定により、ローカルにキャッシュされたプロファイルが保持されます。マシンはログオフ時にリセットされますが、個々のユーザーに割り当てられるため、プロファイルがキャッシュされている場合はログオンが高速になります。
6. **常にキャッシュ**を無効にします。ただし、このポリシーを有効にし、ファイルサイズ制限 (MB単位) を定義することで、ログオン後できるだけ早く大きなファイルがプロファイルにロードされるようにすることができます。このサイズ以上のファイルは、できるだけ早くローカルにキャッシュされます。

7. Citrix Virtual Apps and Desktopsサーバー間をローミングするユーザーのプロファイルの場合を除き、**ローカル管理者によるログオンの処理**を有効にします。この場合は、このポリシーを無効にします。

フォルダーリダイレクト

フォルダーリダイレクトを使用すると、プロファイルが保存されている場所とは異なるネットワーク共有にユーザーデータを保存できます。フォルダーリダイレクトはプロファイルサイズとロード時間を削減しますが、ネットワーク帯域幅に影響を与える可能性があります。フォルダーリダイレクトは、Citrixユーザープロファイルが使用されていることを必要としません。独自のユーザープロファイルを管理することを選択し、それでもフォルダーをリダイレクトできます。

StudioのCitrixポリシーを使用してフォルダーリダイレクトを構成します。

- リダイレクトされたフォルダーのコンテンツを保存するために使用されるネットワークの場所が利用可能であり、正しい権限を持っていることを確認してください。場所のプロパティは検証されます。
- リダイレクトされたフォルダーはネットワーク上に設定され、そのコンテンツはログオン時にユーザーの仮想デスクトップから入力されます。

フォルダーリダイレクトは、CitrixポリシーまたはActive Directoryグループポリシーオブジェクトのいずれかのみを使用して構成し、両方を使用しないでください。両方のポリシーエンジンを使用してフォルダーリダイレクトを構成すると、予期しない動作が発生する可能性があります。

高度なフォルダーリダイレクト

複数のオペレーティングシステム (OS) を使用する展開では、ユーザープロファイルの一部を各OSで共有したい場合があります。プロファイルの残りの部分は共有されず、1つのOSでのみ使用されます。OS間で一貫したユーザーエクスペリエンスを確保するには、各OSで異なる構成、つまり高度なフォルダーリダイレクトが必要です。たとえば、2つのOSで実行されているアプリケーションの異なるバージョンが共有ファイルを読み取ったり編集したりする必要がある場合、両方のバージョンがアクセスできる単一のネットワークロケーションにリダイレクトすることを決定します。あるいは、2つのOSで**スタートメニュー**フォルダーの内容の構造が異なるため、両方ではなく一方のフォルダーのみをリダイレクトすることに決定します。このアプローチにより、各OSで**スタートメニュー**フォルダーとその内容が分離され、ユーザーに一貫したエクスペリエンスが保証されます。

展開で高度なフォルダーリダイレクトが必要な場合は、ユーザーのプロファイルデータの構造を理解し、そのどの部分をOS間で共有できるかを判断する必要があります。フォルダーリダイレクトが正しく使用されないと、予期しない動作が発生する可能性があります。

高度な展開でフォルダーをリダイレクトするには:

- 各OSに個別のDelivery Groupを使用します。
- 仮想デスクトップ上のものを含む仮想アプリケーションがユーザーデータと設定をどこに保存するかを理解し、データの構造を理解します。
- 安全にローミングできる共有プロファイルデータ（各OSで同じ構造であるため）については、各Delivery Groupでそのデータを含むフォルダーをリダイレクトします。
- ローミングできない非共有プロファイルデータについては、デスクトップグループのいずれか1つ（通常は最も使用されているOSまたはデータが最も関連性の高いOS）で、そのデータを含むフォルダーをリダイレクトします。あるいは、OS間でローミングできない非共有データについては、両方のシステムでそのデータを含むフォルダーを別々のネットワークロケーションにリダイレクトします。

高度な展開の例

この展開では、Windows 10デスクトップで実行されるMicrosoft OutlookおよびInternet Explorerのバージョンを含むアプリケーションと、Windows Server 2019によって配信されるOutlookおよびInternet Explorerの他のバージョンを含むアプリケーションがあります。2つのOS用に2つのDelivery Groupをすでに設定しています。ユーザーは、2つのアプリケーションのどちらのバージョンでも同じ**連絡先**と**お気に入り**のセットにアクセスしたいと考えています。

重要: 以下の決定とアドバイスは、説明されているOSと展開に有効です。組織では、リダイレクトするフォルダーとそれらを共有するかどうかの決定は、特定の展開に固有のさまざまな要因によって異なります。

- Delivery Groupに適用されるポリシーを使用して、以下のフォルダーをリダイレクトするように選択します。

フォルダー	WINDOWS 10でリダイレクトされますか？	WINDOWS SERVER 2019でリダイレクトされますか？
マイドキュメント	はい	はい
アプリケーションデータ	いいえ	いいえ
連絡先	はい	はい
デスクトップ	はい	いいえ
ダウンロード	いいえ	いいえ

フォルダー	WINDOWS 10でリダイレクトされますか？	WINDOWS SERVER 2019でリダイレクトされますか？
お気に入り	はい	はい
リンク	はい	いいえ
マイミュージック	はい	はい
マイピクチャ	はい	はい
マイビデオ	はい	はい
検索	はい	いいえ
保存されたゲーム	いいえ	いいえ
スタートメニュー	はい	いいえ

- 共有され、リダイレクトされるフォルダーの場合：
  - OutlookとInternet Explorerの異なるバージョンによって保存されたデータの構造を分析した結果、**連絡先**フォルダーと**お気に入り**フォルダーを共有しても安全であると判断しました。
  - **マイドキュメント**、**マイミュージック**、**マイピクチャ**、**マイビデオ**フォルダーの構造はOS間で標準的であることがわかっています。そのため、これらのフォルダーを各デリバリーグループで同じネットワークロケーションに保存しても安全です。
- 共有されない、リダイレクトされるフォルダーの場合：
  - Windows Serverデリバリーグループでは、デスクトップ、リンク、検索、または**スタートメニュー**フォルダーをリダイレクトしません。これらのフォルダー内のデータは2つのOSで異なる方法で整理されているためです。したがって、共有することはできません。
  - この共有されないデータの予測可能な動作を保証するために、Windows 10デリバリーグループでのみリダイレクトします。Windows 10は、ユーザーが日常業務でより頻繁に使用します。ユーザーはWindows Serverによって提供されるアプリケーションにたまにしかアクセスしません。また、この場合、共有されないデータはアプリケーション環境よりもデスクトップ環境により関連性が高くなります。たとえば、デスクトップショートカットは**デスクトップ**フォルダーに保存され、Windows 10マシンから作成されたものであれば役立つ可能性がありますが、Windows Serverマシンから作成されたものではありません。

- リダイレクトされないフォルダーの場合:
  - ユーザーのダウンロードファイルでサーバーを散らかしたくないため、ダウンロードフォルダーをリダイレクトしないことを選択します
  - 個々のアプリケーションからのデータは互換性やパフォーマンスの問題を引き起こす可能性があるため、アプリケーションデータフォルダーをリダイレクトしないことを決定します

フォルダーリダイレクトの詳細については、「フォルダーリダイレクト、オフラインファイル、および移動ユーザープロファイルの概要」を参照してください。

フォルダーリダイレクトと除外

Citrix Profile Management（Studioではない）では、パフォーマンス強化機能により、除外を使用してフォルダーが処理されないようにすることができます。この機能を使用する場合は、リダイレクトされたフォルダーを除外しないでください。フォルダーリダイレクト機能と除外機能は連携して動作します。リダイレクトされたフォルダーが除外されないようにすることで、後でリダイレクトしないと決定した場合でも、Profile Managementがそれらをプロファイルフォルダー構造に戻し、データ整合性を維持できます。除外の詳細については、「項目の含める/除外」を参照してください。

VDA登録

はじめに

> **注:**
>
> オンプレミス環境では、VDAはDelivery Controllerに登録されます。Citrix Cloudサービス環境では、VDAはCloud Connectorに登録されます。ハイブリッド環境では、一部のVDAはDelivery Controllerに登録され、他のVDAはCloud Connectorに登録されます。

> VDAを使用する前に、サイト上の1つ以上のControllerまたはCloud Connectorに登録（通信を確立）する必要があります。VDAは、`ListofDDCs`と呼ばれるリストを確認してControllerまたはConnectorを見つけます。VDA上の`ListOfDDCs`には、そのVDAをサイト上のControllerまたはCloud Connectorに指し示すDNSエントリが含まれています。負荷分散のため、VDAはリスト内のすべてのControllerまたはCloud Connectorに接続を自動的に分散します。

VDA登録がそれほど重要であるのはなぜですか？

- セキュリティの観点から見ると、登録は機密性の高い操作です。ControllerまたはCloud ConnectorとVDA間の接続を確立しています。このような機密性の高い操作では、すべてが完璧な状態でない場合は接続を拒否するのが期待される動作です。VDAからControllerまたはCloud Connectorへ、およびControllerまたはCloud ConnectorからVDAへの2つの別々の通信チャネルを実質的に確立しています。接続にはKerberosが使用されるため、時刻同期やドメインメンバーシップの問題は容赦されません。Kerberosはサービスプリンシパル名（SPN）を使用するため、負荷分散されたIP\\ホスト名は使用できません。
- Controller（またはCloud Connector）を追加および削除する際に、VDAが正確で最新のControllerまたはCloud Connector情報を持っていない場合、VDAはリストにないControllerまたはCloud Connectorによって仲介されるセッション起動を拒否する可能性があります。無効なエントリは、仮想デスクトップシステムソフトウェアの起動を遅らせる可能性があります。VDAは、不明で信頼できないControllerまたはCloud Connectorからの接続を受け入れません。

`ListofDDCs`に加えて、`ListOfSIDs`（セキュリティID）は、`ListofDDCs`内のどのマシンが信頼されているかを示します。`ListofSIDs`は、Active Directoryの負荷を軽減したり、侵害されたDNSサーバーからの潜在的なセキュリティ脅威を回避したりするために使用できます。詳細については、「ListOfSIDs」を参照してください。

`ListofDDCs`が複数のControllerまたはCloud Connectorを指定している場合、VDAはランダムな順序でそれらに接続しようとします。オンプレミス展開では、`ListofDDCs`にControllerグループを含めることもできます。VDAは、`ListofDDCs`内の他のエントリに移動する前に、グループ内の各Controllerに接続しようとします。

Citrix Virtual Apps and Desktops™は、VDAのインストール中に、構成されたControllerまたはCloud Connectorへの接続性を自動的にテストします。ControllerまたはCloud Connectorに到達できない場合、エラーが表示されます。ControllerまたはCloud Connectorに接続できないという警告を無視した場合（またはVDAのインストール中にControllerまたはCloud Connectorのアドレスを指定しなかった場合）、メッセージが表示されます。

ControllerまたはCloud Connectorアドレスを構成する方法

管理者は、VDAが初めて登録する際（初回登録）に使用する構成方法を選択します。初回登録中に、VDA上に永続的なキャッシュが作成されます。その後の登録では、構成の変更が検出されない限り、VDAはこのローカルキャッシュからControllerまたはCloud Connectorのリストを取得します。

その後の登録時にそのリストを取得する最も簡単な方法は、自動更新機能を使用することです。自動更新はデフォルトで有効になっています。詳細については、「自動更新」を参照してください。

VDA上でControllerまたはCloud Connectorアドレスを構成する方法はいくつかあります。

- ポリシーベース (LGPO または GPO)
- レジストリベース (手動、グループポリシー基本設定 (GPP)、VDA インストール時に指定)
- Active Directory OU ベース (レガシー OU 検出)
- MCS ベース (personality.ini)

VDA をインストールするときに、初期登録方法を指定します。(自動更新を無効にすると、VDA のインストール時に選択した方法が以降の登録に使用されます。)

次の図は、VDA インストールウィザードの ページを示しています。

VDA インストールウィザードの Delivery Controller ページ(/en-us/citrix-virtual-apps-desktops/2503/media/vda-install-controllers-all.png)

ポリシーベース (LGPO\\GPO)

Citrix® は、初期 VDA 登録に GPO を使用することを推奨しています。これは最も優先度が高いです。(自動更新が最も優先度が高いとされていますが、自動更新は初期登録後にのみ使用されます。) ポリシーベースの登録は、構成にグループポリシーを使用する集中管理の利点を提供します。

この方法を指定するには、以下の両方の手順を完了します。

- VDA インストールウィザードの ページで、 を選択します。VDA のインストール中にコントローラーアドレスを指定しない場合でも、ウィザードはコントローラーアドレスを指定するよう何度か通知します。(VDA 登録はそれほど重要です。)
- Citrix ポリシーを使用して、`Virtual Delivery Agent Settings > Controllers` 設定でポリシーベースの VDA 登録を有効または無効にします。(セキュリティが最優先事項の場合は、`Virtual Delivery Agent Settings > Controller SIDs` 設定を使用します。)

この設定は `HKLM\Software\Policies\Citrix\VirtualDesktopAgent (ListOfDDCs)` に保存されます。

レジストリベース

この方法を指定するには、以下のいずれかの手順を完了します。

- VDAインストールウィザードの**Delivery Controller**ページで、**手動で実行**を選択します。次に、インストールされているControllerのFQDNを入力し、**追加**をクリックします。複数のControllerをインストールしている場合は、それらのアドレスを追加します。
- コマンドラインVDAインストールの場合、/controllersオプションを使用して、インストールされているControllerまたはCloud ConnectorのFQDNを指定します。

この情報は、レジストリキー`HKLM\Software\Citrix\VirtualDesktopAgent`または`HKLM\Software\Wow6432Node\Citrix\VirtualDesktopAgent`の下のレジストリ値`ListOfDDCs`に保存されます。

このレジストリキーは、手動で構成することも、グループポリシー設定（GPP）を使用することもできます。この方法は、ポリシーベースの方法よりも推奨される場合があります（たとえば、異なるControllerまたはCloud Connectorの条件付き処理が必要な場合。例：XDW-001-で始まるコンピューター名にはXDC-001を使用する）。

`ListOfDDCs`レジストリキーを更新します。このキーには、サイト内のすべてのControllerまたはCloud ConnectorのFQDNが一覧表示されます。(このキーはActive DirectoryサイトOUに相当します。)

`HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent\ListOfDDCs (REG_SZ)`

`HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent`レジストリの場所に`ListOfDDCs`と`FarmGUID`の両方のキーが含まれている場合、ControllerまたはCloud Connectorの検出には`ListOfDDCs`が使用されます。VDAインストール中にサイトOUが指定された場合、`FarmGUID`が存在します。（これはレガシー展開で使用される場合があります。）

必要に応じて、`ListOfSIDs`レジストリキーを更新します（詳細については、ListOfSIDsを参照してください）。

`HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent\ListOfSIDs (REG_SZ)`

注意：VDAインストール中に指定した設定を上書きするCitrixポリシーを通じてポリシーベースのVDA登録も有効にする場合、それは優先度の高い方法であるためです。

Active Directory OUベース (レガシー)

この方法は主に下位互換性のためにサポートされており、推奨されません。まだ使用している場合は、別の方法に変更することをCitrixは推奨します。

この方法を指定するには、以下の両方の手順を完了します。

- VDAインストールウィザードの**Delivery Controller**ページで、**Active Directoryから場所を選択**を選択します。
- `Set-ADControllerDiscovery.ps1`スクリプト（すべてのControllerで利用可能）を使用します。また、各VDAで`FarmGuid`レジストリエントリを構成して、正しいOUを指すようにします。この設定はグループポリシーを使用して構成できます。

MCSベース

MCSを使用してVMをプロビジョニングする場合、MCSはControllerまたはCloud Connectorのリストを設定します。この機能は自動更新と連携します。カタログの作成時、MCSは初期プロビジョニング中にControllerまたはCloud Connectorのリストを `Personality.ini` ファイルに挿入します。自動更新により、リストは最新の状態に保たれます。

この方法を指定するには、VDAインストールウィザードの **Delivery Controller** ページで、**Machine Creation Services™に任せる** を選択します。

レビューと推奨事項

ベストプラクティスとして:

- 初期登録にはグループポリシー登録方法を使用します。
- Controllerのリストを最新の状態に保つには、自動更新（デフォルトで有効）を使用します。
- マルチゾーン展開では、初期構成にグループポリシーを使用します（少なくとも2つのControllerまたはCloud Connectorを使用）。VDAを、そのゾーン内のローカルなControllerまたはCloud Connectorにポイントします。自動更新を使用して、それらを最新の状態に保ちます。自動更新は、サテライトゾーンのVDAの`ListofDDCs`を自動的に最適化します。
- Controllerが利用できない場合の登録の問題を防ぐため、`ListOfDDCs`レジストリキーに複数のControllerをスペースで区切ってリストします。例:

```
DDC7x.xd.local DDC7xHA.xd.local



32-bit: HKEY_LOCAL_MACHINE
\Software\Citrix\VirtualDesktopAgent\ListOfDDCs
```

```
HKEY_LOCAL_MACHINE \Software\Citrix\VirtualDesktopAgent\ListOfDDCs
(REG_SZ)
```

- 起動時の登録遅延を防ぐため、`ListofDDCs`の下にリストされているすべての値が有効な完全修飾ドメイン名にマップされていることを確認します。

自動更新

自動更新（XenAppおよびXenDesktop 7.6で導入）はデフォルトで有効になっています。これは、VDA登録を最新の状態に保つための最も効率的な方法です。初期登録には使用されませんが、初期登録時に、自動更新ソフトウェアは`ListofDDCs`をダウンロードし、VDA上の永続キャッシュに保存します。このプロセスは各VDAに対して実行されます。キャッシュにはマシンポリシー情報も保持され、ポリシー設定が再起動後も保持されることを保証します。

自動更新は、MCSまたはCitrix Provisioning™を使用してマシンをプロビジョニングする場合にサポートされますが、Citrix Provisioningのサーバー側キャッシュは除きます。自動更新キャッシュ用の永続ストレージがないため、サーバー側キャッシュは一般的なシナリオではありません。

この方法を指定するには:

- 設定`Virtual Delivery Agent Settings > Enable auto update of Controllers`を含むCitrixポリシーを介して、自動更新を有効または無効にします。この設定はデフォルトで有効になっています。

仕組み:

- VDAが再登録するたび（たとえば、マシンの再起動後）に、キャッシュが更新されます。各ControllerまたはCloud Connectorも90分ごとにサイトデータベースをチェックします。前回のチェック以降にControllerまたはCloud Connectorが追加または削除された場合、あるいはVDA登録に影響するポリシー変更があった場合、ControllerまたはCloud Connectorは登録済みのVDAに更新されたリストを送信し、キャッシュが更新されます。VDAは、最新のキャッシュリストにあるすべてのControllerまたはCloud Connectorからの接続を受け入れます。
- VDAが、登録されているControllerまたはCloud Connectorが含まれていないリスト（つまり、そのControllerまたはCloud Connectorがサイトから削除された場合）を受信すると、VDAは`ListofDDCs`内のControllerまたはCloud Connectorの中から選択して再登録します。

例:

- 展開には3つのController（A、B、C）があります。VDAはController Bに登録されます（これはVDAのインストール時に指定されました）。

- その後、2つのController（DとE）がサイトに追加されます。90分以内に、VDAは更新されたリストを受信し、Controller A、B、C、D、Eからの接続を受け入れます。（VDAが再起動されるまで、負荷はすべてのControllerに均等に分散されません。）
- さらにその後、Controller Bが別のサイトに移動されます。90分以内に、元のサイトのVDAは、前回のチェック以降にControllerの変更があったため、更新されたリストを受信します。元々Controller Bに登録されていたVDA（リストにはもうありません）は、現在のリスト（A、C、D、E）のControllerの中から選択して再登録します。

マルチゾーン展開では、サテライトゾーンの自動更新は、まずすべてのローカル Controller を自動的にキャッシュします。プライマリゾーンのすべての Controller は、バックアップグループにキャッシュされます。サテライトゾーンにローカル Controller が利用できない場合、プライマリゾーンの Controller で登録が試行されます。

次の例に示すように、キャッシュファイルにはホスト名とセキュリティIDのリスト（`ListofSIDs`）が含まれています。VDAはSIDをクエリしないため、Active Directoryの負荷が軽減されます。

```
<?xml version="1.0"?>
<ListOfDDcsListIfSids xmlns="http://schemas.datacontract.org/2004/07/Citrix.Cds.BrokerAgent" xmlns:i="http://www.w3.org/2001/XMLSchema-instance">
 - <_x003C_GroupsOfDDCs_x003E_k__BackingField xmlns:d2p1="http://schemas.microsoft.com/2003/10/Serialization/Arrays">
    - <d2p1:ArrayOfstring>
        <d2p1:string>CTX-XDC-002.zugec.lan</d2p1:string>
        <d2p1:string>CTX-XDC-001.zugec.lan</d2p1:string>
      </d2p1:ArrayOfstring>
   </_x003C_GroupsOfDDCs_x003E_k__BackingField>
 - <_x003C_ListOfDDCs_x003E_k__BackingField xmlns:d2p1="http://schemas.microsoft.com/2003/10/Serialization/Arrays">
      <d2p1:string>CTX-XDC-002.zugec.lan</d2p1:string>
      <d2p1:string>CTX-XDC-001.zugec.lan</d2p1:string>
   </_x003C_ListOfDDCs_x003E_k__BackingField>
 - <_x003C_ListOfSids_x003E_k__BackingField xmlns:d2p1="http://schemas.microsoft.com/2003/10/Serialization/Arrays">
      <d2p1:string>S-1-5-21-726903571-3621260514-849154371-1119</d2p1:string>
      <d2p1:string>S-1-5-21-726903571-3621260514-849154371-1126</d2p1:string>
   </_x003C_ListOfSids_x003E_k__BackingField>
   <_x003C_NonAutoListOfDDCsMethod_x003E_k__BackingField>RegistryBasedFarm</_x003C_NonAutoListOfDDCsMethod_x003E_k__BackingField>
   <_x003C_NonAutoListOfDDCsOrOu_x003E_k__BackingField>CTX-XDC-002.zugec.lan</_x003C_NonAutoListOfDDCsOrOu_x003E_k__BackingField>
</ListOfDDcsListIfSids>
```

キャッシュファイルはWMI呼び出しで取得できます。ただし、SYSTEMアカウントのみが読み取り可能な場所に保存されています。

> **重要:**
>
> この情報は情報提供のみを目的としています。このファイルを変更しないでください。このファイルまたはフォルダーへの変更は、サポートされていない構成になります。

```
Get-WmiObject -Namespace "Root\Citrix\DesktopInformation" -Class "Citrix_VirtualDesktopInfo" -Property "PersistentDataLocation"
```

セキュリティ上の理由から (Active Directoryの負荷軽減とは別に) `ListofSIDs` を手動で構成する必要がある場合、自動更新機能は使用できません。詳細については、ListOfSIDs を参照してください。

自動更新の優先順位の例外

通常、自動更新はすべてのVDA登録方法の中で最も高い優先順位を持ち、他の方法の設定を上書きしますが、例外があります。キャッシュ内の`NonAutoListOfDDCs`要素は、初期VDA構成方法を指定します。自動更新はこの情報を監視します。初期登録方法が変更された場合、登録プロセスは自動更新をスキップし、次に優先順位の高い構成済み方法を使用します。このプロセスは、VDAを別のサイトに移動する場合（たとえば、災害復旧中）に役立ちます。

構成に関する考慮事項

一般的なVDA登録構成を表示します。

<iframe src="https://www.youtube.com/embed/MgGMZp4SnZgEq9ieibQc9j" width="720px" height="480px" frameborder="0" title="YouTube video player" allowfullscreen=""> </iframe>
VDA登録手順を表示します。

<iframe src="https://www.youtube.com/embed/iwsbajSVY5QvoUTh6m7AjG" width="720px" height="480px" frameborder="0" title="YouTube video player" allowfullscreen=""> </iframe>
VDA登録に影響を与える可能性のある項目を構成する際は、以下の点を考慮してください。

ControllerまたはCloud Connectorのアドレス

ControllerまたはCloud Connectorを指定するためにどの方法を使用する場合でも、CitrixはFQDNアドレスを使用することを推奨します。IPアドレスは、DNSレコードよりも侵害されやすいため、信頼できる構成とは見なされません。`ListofSIDs`を手動で入力する場合、`ListofDDCs`でIPを使用できます。ただし、FQDNが引き続き推奨されます。

負荷分散

前述のとおり、VDAは`ListofDDCs`内のすべてのControllerまたはCloud Connectorに接続を自動的に分散します。フェイルオーバーと負荷分散機能は、Citrix Brokering Protocol（CBP）に組み込まれています。構成で複数のControllerまたはCloud Connectorを指定した場合、必要に応じて登録はそれらの間で自動的にフェイルオーバーします。自動更新では、すべてのVDAで自動フェイルオーバーが自動的に発生します。

セキュリティ上の理由から、Citrix ADCなどのネットワークロードバランサーを使用することはできません。VDA登録ではKerberos相互認証が使用され、クライアント（VDA）はサービス（Controller）に自身のIDを証明する必要があります。ただし、ControllerまたはCloud Connector

もVDAに自身のIDを証明する必要があります。これは、VDAとControllerまたはCloud Connectorが同時にサーバーとクライアントとして機能することを意味します。この記事の冒頭で述べたように、VDAからController/Cloud Connectorへの通信チャネルと、Controller/Cloud ConnectorからVDAへの通信チャネルの2つがあります。

このプロセスにおけるコンポーネントの1つは、サービスプリンシパル名（SPN）と呼ばれ、Active Directoryコンピューターオブジェクトのプロパティとして保存されます。VDAがControllerまたはCloud Connectorに接続するとき、通信したい相手を指定する必要があります。このアドレスがSPNです。負荷分散されたIPを使用すると、相互Kerberos認証は、そのIPが予期されたControllerまたはCloud Connectorに属していないことを正しく認識します。

詳細については、以下を参照してください。

- Kerberos の概要
- Kerberos を使用した相互認証(https://docs.microsoft.com/ja-jp/windows-server/security/kerberos/kerberos-authentication-overview)

自動更新によるCNAMEの置き換え

自動更新機能は、XenAppおよびXenDesktopの7.xより前のバージョンにおけるCNAME（DNSエイリアス）機能を置き換えます。XenAppおよびXenDesktop 7以降、CNAME機能は無効になっています。CNAMEの代わりに自動更新を使用してください。（CNAMEを使用する必要がある場合は、CTX137960を参照してください。DNSエイリアスが常に機能するように、自動更新とCNAMEを同時に使用しないでください。）

Controller/Cloud Connectorグループ

特定のシナリオでは、ControllerまたはCloud Connectorをグループで処理し、一方のグループを優先し、すべてのController/Cloud Connectorが失敗した場合に他方のグループをフェイルオーバーに使用したい場合があります。ControllerまたはCloud Connectorはリストからランダムに選択されるため、グループ化によって優先的な使用を強制できることを覚えておいてください。

これらのグループは、単一のサイト内での使用を目的としています（複数のサイトではありません）。

Controller/Cloud Connectorのグループを指定するには、括弧を使用します。たとえば、4つのController（プライマリ2つとバックアップ2つ）がある場合、グループ化は次のようになります。

```
(XDC-001.cdz.lan XDC-002.cdz.lan) (XDC-003.cdz.lan XDC-004.cdz.lan)
```

この例では、最初のグループ（001と002）のControllerが最初に処理されます。両方が失敗した場合、2番目のグループ（003と004）のControllerが処理されます。

XenDesktop 7.0以降の場合、**登録グループ**機能を使用するには、追加の手順を実行する必要があります。Studioから**Controllerの自動更新を有効にする**ポリシーを**禁止**する必要があります。

ListOfSIDs

VDAが登録のために連絡できるControllerのリストは`ListofDDCs`です。VDAは、`ListofDDCs`内のControllerを自動的に信頼しないため、どのControllerを信頼すべきかも知っている必要があります。`ListofSIDs`（セキュリティID）は、信頼できるControllerを識別します。VDAは、信頼できるControllerにのみ登録を試みます。

ほとんどの環境では、`ListofSIDs`は`ListofDDCs`から自動的に生成されます。CDFトレースを使用して`ListofSIDs`を読み取ることができます。

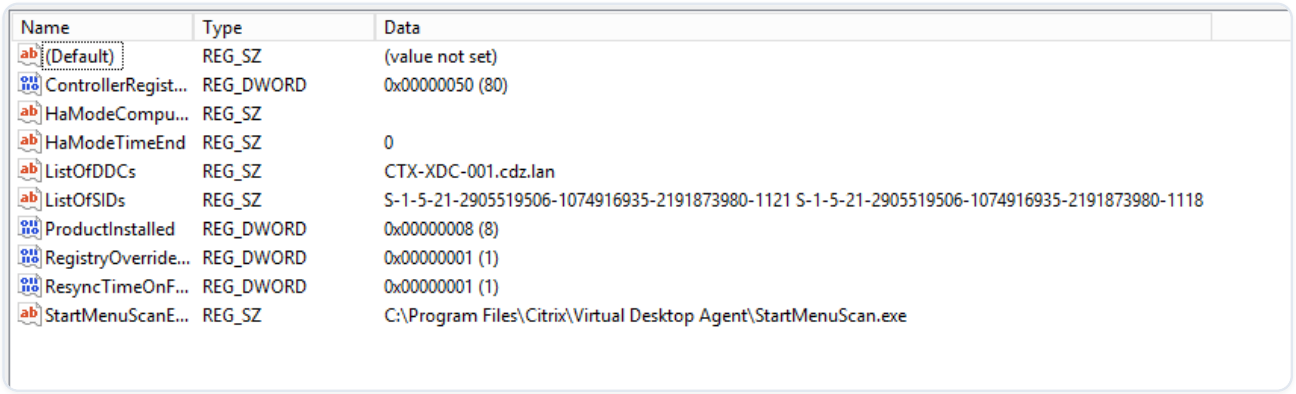
一般的に、`ListofSIDs`を手動で変更する必要はありません。いくつかの例外があります。最初の2つの例外は、新しいテクノロジーが利用可能になったため、もはや有効ではありません。

- **コントローラーの役割を分離:** XenAppおよびXenDesktop 7.7でゾーンが導入される前は、登録にコントローラーのサブセットのみが使用されていた場合、`ListofSIDs`は手動で構成されていました。たとえば、XDC-001とXDC-002をXMLブローカーとして、XDC-003とXDC-004をVDA登録に使用していた場合、すべてのコントローラーを`ListofSIDs`に、XDC-003とXDC-004を`ListofDDCs`に指定しました。これは一般的な構成でも推奨される構成でもありません。新しい環境では使用しないでください。代わりにゾーンを使用してください。
- **Active Directoryの負荷軽減:** XenAppおよびXenDesktop 7.6で自動更新機能が導入される前は、ドメインコントローラーの負荷を軽減するために`ListofSIDs`が使用されていました。`ListofSIDs`を事前に入力することで、DNS名からSIDへの解決をスキップできます。しかし、この永続キャッシュにはSIDが含まれているため、自動更新機能によりこの作業は不要になります。Citrixは自動更新機能を有効にしておくことを推奨します。
- **セキュリティ:** 一部の高度に保護された環境では、侵害されたDNSサーバーからの潜在的なセキュリティ脅威を回避するために、信頼されたコントローラーのSIDが手動で構成されていました。ただし、これを行う場合は、自動更新機能も無効にする必要があります。そうしないと、永続キャッシュからの構成が使用されます。

したがって、特別な理由がない限り、`ListofSIDs`を変更しないでください。

`ListofSIDs`を変更する必要がある場合は、`HKLM\Software\Citrix\VirtualDesktopAgent`の下に`ListOfSIDs (REG_SZ)`という名前のレジストリキーを作成します。値は信頼されたSIDのリストであり、複数ある場合はスペースで区切ります。

次の例では、VDA登録には1つのコントローラー (`ListofDDCs`) が使用されますが、ブローカー処理には2つのコントローラー (List OfSIDs) が使用されます。



Name	Type	Data
(Default)	REG_SZ	(value not set)
ControllerRegist...	REG_DWORD	0x00000050 (80)
HaModeCompu...	REG_SZ	
HaModeTimeEnd	REG_SZ	0
ListOfDDCs	REG_SZ	CTX-XDC-001.cdz.lan
ListOfSIDs	REG_SZ	S-1-5-21-2905519506-1074916935-2191873980-1121 S-1-5-21-2905519506-1074916935-2191873980-1118
ProductInstalled	REG_DWORD	0x00000008 (8)
RegistryOverride...	REG_DWORD	0x00000001 (1)
ResyncTimeOnF...	REG_DWORD	0x00000001 (1)
StartMenuScanE...	REG_SZ	C:\Program Files\Citrix\Virtual Desktop Agent\StartMenuScan.exe

VDA登録中のコントローラー検索

VDAが登録を試行すると、Broker Agentはまずローカルドメインで DNSルックアップを実行し、指定されたコントローラーに到達できることを確認します。

その最初のルックアップでコントローラーが見つからない場合、Broker AgentはADでフォールバックのトップダウンクエリを開始できます。そのクエリはすべてのドメインを検索し、頻繁に繰り返されます。コントローラーアドレスが無効な場合（たとえば、管理者がVDAのインストール時に誤ったFQDNを入力した場合）、そのクエリのアクティビティは、ドメインコントローラー上で分散型サービス拒否（DDoS）状態を引き起こす可能性があります。

最初の検索中にコントローラーを見つけられない場合に、Broker Agentがフォールバックのトップダウンクエリを使用するかどうかは、次のレジストリキーによって制御されます。

`HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent`

- 名前: `DisableDdcWildcardNameLookup`
- 種類: `DWORD`
- 値: `0` (デフォルト) または任意のゼロ以外の値

`0` に設定すると、フォールバック検索が有効になります。コントローラーの初期検索が失敗した場合、フォールバックのトップダウン検索が開始されます。これはデフォルトの動作です。ただし、ゼロ以外の値に設定すると、フォールバック検索は無効になります。コントローラーの初期検索が失敗した場合、ブローカーエージェントは検索を停止します。

読み取り専用ドメインコントローラーを使用した VDA 登録中の LDAP バインディングシーケンス

VDAが読み取り専用ドメインコントローラー (RODC) に登録する場合、ブローカーエージェントは無視するLight Directory Access Protocol (LDAP) バインディングを選択する必要があります。この選択を行うには、ブローカーエージェントに適切なレジストリキーが必要です。

レジストリキーが提供されていない場合、またはレジストリキーフィールドが空の場合、RODCへのVDA登録は、元のLDAPバインディングシーケンスを経由する必要があるため、時間がかかります。

LDAPバインディングシーケンスを変更するために、レジストリキー`ListofIgnoredBindings`が`HKEY_LOCAL_MACHINE\Software\Policies\Citrix\VirtualDesktopAgent`に追加されました。`ListofIgnoredBindings`を使用すると、必要に応じてLDAPバインディングシーケンスを変更でき、RODCへのVDA登録を高速化できます。

- 名前: `ListofIgnoredBindings`
- 種類: `REG_SZ`
- 値: `DefaultPath`, `DomainPath`, `PDCPath`

値は、コンマで区切られたバインディングパスオプションのリストです。レジストリキーは、有効と認識しない値を無視します。

VDA登録の問題のトラブルシューティング

前述のとおり、VDAは、仲介されたセッションを起動する際に考慮されるために、Delivery ControllerまたはCloud Connectorに登録されている必要があります。未登録のVDAは、利用可能なリソースの利用率低下につながる可能性があります。VDAが登録されない理由はさまざまであり、その多くは管理者がトラブルシューティングできます。Studioは、カタログ作成ウィザードおよびデリバリーグループ作成後にトラブルシューティング情報を提供します。

- **マシンカタログ作成中の問題の特定:** カタログ作成ウィザードで、既存のマシンを追加した後、コンピューターアカウント名の一覧は、各マシンがカタログに追加するのに適しているかどうかを示します。各マシンの横にあるアイコンにカーソルを合わせると、そのマシンに関する情報メッセージが表示されます。

  メッセージで問題のあるマシンが特定された場合、そのマシンを削除する（**Remove**ボタンを使用）か、マシンを追加することができます。たとえば、マシンに関する情報が取得されなかった（おそらく一度も登録されなかったため）というメッセージが表示された場合でも、そのマシンを追加することを選択できます。

カタログの機能レベルは、カタログ内のマシンで利用できる製品機能を制御します。新しい製品バージョンで導入された機能を使用するには、新しいVDAが必要になる場合があります。機能レベルを設定すると、そのバージョンで導入されたすべての機能（および機能レベルが変更されない場合はそれ以降のバージョン）がカタログ内のマシンで利用可能になります。ただし、以前のVDAバージョンを持つカタログ内のマシンは登録できません。

- **デリバリーグループ作成後の問題の特定:** デリバリーグループを作成すると、Studioはそのグループに関連付けられたマシンに関する詳細を表示します。

  デリバリーグループの詳細ペインには、登録が必要だが登録されていないマシンの数が表示されます。つまり、電源が入っていてメンテナンスモードではないが、現在コントローラーに登録されていないマシンが1台以上存在する可能性があります。「登録されていないが、登録が必要な」マシンを表示している場合は、詳細ペインの**トラブルシューティング**タブで、考えられる原因と推奨される是正措置を確認してください。

VDA登録のトラブルシューティングに関する詳細情報

- 機能レベルの詳細については、「VDAのバージョンと機能レベル」を参照してください。
- VDA登録のトラブルシューティングについて詳しくは、「CTX136668」を参照してください。
- VDA登録とセッション起動のトラブルシューティングには、Citrix Scoutのヘルスチェックも使用できます。詳細については、「ヘルスチェックについて」を参照してください。

仮想IPおよび仮想ループバック

重要:

- Windows 10 Enterprise multi-session および Windows 11 Enterprise multi-session は、リモートデスクトップIP仮想化 (仮想IP) をサポートしていません。
- リモートデスクトップIP仮想化 (仮想IP) は、クラウドホスト型マシンではサポートされていません。 詳細については、Microsoft のドキュメントを参照してください。

Remote Desktop IP Virtualization および仮想ループバック機能は、Windows Server 2016、Windows Server 2019、および Windows Server 2022 マシンでサポートされています。これらの機能は、Windows デスクトップ OS マシンには適用されません。

Microsoft リモートデスクトップIP仮想化アドレス機能は、公開されたアプリケーションにセッションごとに一意の動的に割り当てられたIPアドレスを提供します。Citrix 仮想ループバック機能を使用すると、localhost (デフォルトでは 127.0.0.1) との通信に依存するアプリケーションを、localhost 範囲 (127.*) 内の一意の仮想ループバックアドレスを使用するように構成できます。

CRM やコンピュータテレフォニー統合 (CTI) などの特定のアプリケーションは、アドレス指定、ライセンス、識別、または一意のIPアドレスやループバックアドレスを必要とするその他の目的のためにIPアドレスを使用します。他のアプリケーションは静的ポートにバインドする可能性があり、その場合、マルチユーザー環境でアプリケーションの追加インスタンスを起動しようとすると、ポートが使用中であるため失敗します。Citrix Virtual Apps™ 環境でこのようなアプリケーションが正しく機能するには、デバイスごとに一意のIPアドレスが必要です。

Remote Desktop IP Virtualization と仮想ループバックは、互いに独立した機能です。どちらか一方、または両方を使用できます。

管理者アクションの概要:

- Microsoft リモートデスクトップIP仮想化を使用するには、Windows サーバーでそれを有効にして構成します。(Citrix® ポリシー設定は不要です。)
- Citrix 仮想ループバックを使用するには、Citrix ポリシーで2つの設定を構成します。

リモートデスクトップIP仮想化 (仮想IP)

Windows サーバーで Remote Desktop IP Virtualization が有効になり構成されると、セッションで実行されている構成済みの各アプリケーションは、一意のアドレスを持っているように見えます。ユーザーは、Citrix Virtual Apps サーバー上のこれらのアプリケーションに、他の公開アプリケーションと同じ方法でアクセスします。プロセスが Remote Desktop IP Virtualization を必要とするのは、次のいずれかのケースです。

- プロセスがハードコードされたTCPポート番号を使用している
- プロセスがWindowsソケットを使用しており、一意のIPアドレスまたは指定されたTCPポート番号を必要としている

アプリケーションがRemote Desktop IP Virtualizationアドレスを使用する必要があるかどうかを判断するには：

1. Microsoftから**TCPView**ツールを入手します。このツールは、特定のIPアドレスとポートをバインドするすべてのアプリケーションを一覧表示します。TCPViewの詳細については、Microsoftドキュメントを参照してください。
2. ホスト名ではなくアドレスが表示されるように、**IPアドレスの解決**機能を無効にします。

3. アプリケーションを起動し、**TCPView**を使用して、アプリケーションが開くIPアドレスとポート、およびこれらのポートを開いているプロセス名を確認します。
4. サーバーのIPアドレス、0.0.0.0、または127.0.0.1を開くプロセスを構成します。
5. アプリケーションが異なるポートで同じIPアドレスを開かないようにするには、アプリケーションの別のインスタンスを起動します。

Microsoft Remote Desktop (RD) IP仮想化の仕組み

- Microsoftサーバーで仮想IPアドレス指定を有効にする必要があります。

  たとえば、Windows Server 2016環境では、サーバーマネージャーから**リモートデスクトップサービス > RDセッションホスト接続**を展開して、RD IP仮想化機能を有効にし、セッションごとまたはプログラムごとに動的ホスト構成プロトコル (DHCP) サーバーを使用してIPアドレスを動的に割り当てる設定を構成します。Remote Desktop IP Virtualizationの構成の詳細については、Microsoftドキュメントを参照してください。
- この機能を有効にすると、セッションの起動時に、サーバーはDHCPサーバーから動的に割り当てられたIPアドレスを要求します。
- **RD IP仮想化**機能は、リモートデスクトップ接続にセッションごとまたはプログラムごとにIPアドレスを割り当てます。複数のプログラムにIPアドレスを割り当てる場合、それらはセッションごとのIPアドレスを共有します。
- アドレスがセッションに割り当てられると、以下の呼び出しが行われるたびに、セッションはシステムのプライマリIPアドレスではなく仮想アドレスを使用します:
  `bind`, `closesocket`, `connect`, `WSAConnect`, `WSAAccept`, `getpeername`, `getsockname`, `sendto`, `WSASendTo`, `WSASocketW`, `gethostbyaddr`, `getnameinfo`, `getaddrinfo`。

リモートデスクトップセッションホスティング構成内でMicrosoft IP仮想化機能を使用する場合、アプリケーションとWinsock関数呼び出しの間に「フィルター」コンポーネントを挿入することで、アプリケーションは特定のIPアドレスにバインドされます。これにより、アプリケーションは使用すべき正しいIPアドレスのみを認識します。アプリケーションがTCPまたはUDP通信をリッスンしようとすると、自動的に割り当てられた仮想IPアドレス（またはループバックアドレス）にバインドされます。アプリケーションによって開かれた発信接続はすべて、アプリケーションにバインドされたIPアドレスから発信されます。

アドレスを返す関数（Windowsポリシーが制御する`GetAddrInfo()`など）で、ローカルホストのIPアドレスが要求された場合、Remote Desktop IP Virtualizationは返されたIPアドレスを調べ、それをセッションのRemote Desktop IP Virtualizationアドレスに変更します。このような名前関数を介してローカルサーバーのIPアドレスを取得しようとするアプリケーションは、そのセッションに割り当てられた一意のRemote Desktop IP Virtualizationアドレスのみを認識します。このIPア

ドレスは、bindやconnectなどの後続のソケット呼び出しでよく使用されます。Windowsポリシーの詳細については、Windows ServerでのRDS IP仮想化を参照してください。

多くの場合、アプリケーションはアドレス0.0.0.0でリッスンするためにポートへのバインドを要求します。アプリケーションがこれを行い、静的ポートを使用する場合、アプリケーションの複数のインスタンスを起動することはできません。Remote Desktop IP Virtualizationアドレス機能は、これらの呼び出しタイプでも0.0.0.0を探します。特定のRemote Desktop IP Virtualizationアドレスでリッスンするように呼び出しを変更し、これにより、複数のアプリケーションが同じコンピューター上の同じポートでリッスンできるようになります。これは、すべて異なるアドレスでリッスンしているためです。呼び出しは、ICAセッション内であり、Remote Desktop IP Virtualizationアドレス機能が有効になっている場合にのみ変更されます。たとえば、異なるセッションで実行されているアプリケーションの2つのインスタンスが、両方ともすべてのインターフェイス（0.0.0.0）と特定のポート（9000など）にバインドしようとした場合、それらはVIPAddress1:9000とVIPAddress2:9000にバインドされ、競合は発生しません。

仮想ループバック

Citrix Remote Desktop IP Virtualization loopback policy設定を有効にすると、各セッションが通信用に独自のループバックアドレスを持つことができます。アプリケーションがWinsock呼び出しでローカルホストアドレス（デフォルト = 127.0.0.1）を使用すると、仮想ループバック機能は127.0.0.1を127.X.X.Xに置き換えます。ここで、X.X.Xはセッション ID + 1を表します。たとえば、セッションIDが7の場合、アドレスは127.0.0.8になります。セッションIDが第4オクテット（255を超える）を超過する可能性は低いですが、その場合はアドレスは次のオクテット（127.0.1.0）に繰り上がり、最大で127.255.255.255までとなります。

プロセスが仮想ループバックを必要とするのは、次のいずれかのケースです。

- プロセスがWindowsソケットループバック（ローカルホスト）アドレス（127.0.0.1）を使用している場合
- プロセスがハードコードされたTCPポート番号を使用している場合

プロセス間通信にループバックアドレスを使用するアプリケーションには、仮想ループバックポリシー設定を使用します。追加の構成は不要です。仮想ループバックは仮想IPに依存しないため、Microsoftサーバーを構成する必要はありません。

- 仮想IPループバックサポート。有効にすると、このポリシー設定により、各セッションが独自の仮想ループバックアドレスを持つことができます。この設定はデフォルトで無効です。この機能は、仮想IP仮想ループバックプログラムリストポリシー設定で指定されたアプリケーションにのみ適用されます。

- 仮想IP仮想ループバックプログラムリスト。このポリシー設定は、仮想IPループバック機能を使用するアプリケーションを指定します。この設定は、仮想IPループバックサポートポリシー設定が有効になっている場合にのみ適用されます。
- 仮想IPループバックポート除外。アプリケーションがこの設定で指定されたポートでループバックアドレスを呼び出す場合、仮想ループバックは呼び出しをセッション固有のループバックアドレスに変更しません。

関連機能

仮想ループバックが仮想IPよりも優先されるように、次のレジストリ設定を使用できます。この機能は優先ループバックと呼ばれます。ただし、注意して進めてください。

- 優先ループバックは、仮想IPと仮想ループバックの両方が有効になっている場合にのみ使用してください。そうしないと、意図しない結果が生じる可能性があります。
- レジストリを誤って編集すると、オペレーティングシステムの再インストールが必要になるような重大な問題が発生する可能性があります。Citrixは、レジストリエディターの誤った使用によって生じる問題が解決できることを保証できません。レジストリエディターの使用は自己責任でお願いします。編集する前に必ずレジストリをバックアップしてください。

アプリケーションが配置されているサーバーでregeditを実行します。

- `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\VIP`
- 名前: PreferLoopback, 種類: REG_DWORD, データ: 1
- 名前: PreferLoopbackProcesses, 種類: REG_MULTI_SZ, データ: \<プロセスの一覧\>

ゾーン

> **注:**

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

> WANで接続された広範囲に分散した場所にまたがる展開では、ネットワークの遅延と信頼性により課題に直面する可能性があります。これらの課題を軽減する2つのオプションがあります。

- 複数のサイトを展開し、それぞれに独自のSQL Serverサイトデータベースを持つ。

  このオプションは、大規模なエンタープライズ展開に推奨されます。複数のサイトは個別に管理され、それぞれ独自のSQL Serverサイトデータベースが必要です。各サイトは個別のCitrix Virtual Apps™展開です。

- 単一のサイト内に複数のゾーンを構成する。

  ゾーンを構成することで、遠隔地のユーザーが、接続がWANの大部分を通過することを必ずしも強制することなく、リソースに接続できるようになります。ゾーンを使用すると、単一のWeb Studioコンソール、Citrix Director、およびサイトデータベースから効果的なサイト管理が可能になります。これにより、遠隔地に個別のデータベースを含むより多くのサイトを展開、人員配置、ライセンス供与、および運用するコストを節約できます。

  ゾーンはあらゆる規模の展開で役立ちます。ゾーンを使用すると、アプリケーションとデスクトップをエンドユーザーに近づけることができ、パフォーマンスが向上します。ゾーンには、冗長性と回復性のために1つ以上のControllerをローカルにインストールできますが、必須ではありません。

  サイトに構成されているControllerの数は、サイト自体に新しいControllerを追加するなどの一部の操作のパフォーマンスに影響を与える可能性があります。これを避けるため、Citrix Virtual AppsまたはCitrix Virtual Desktops™サイトのゾーン数を50以下に制限することをお勧めします。

  ゾーンのネットワーク遅延が250ミリ秒RTTを超える場合、ゾーンではなく複数のサイトを展開することをお勧めします。

この記事全体を通して、「ローカル」という用語は議論されているゾーンを指します。たとえば、「VDAがローカルControllerに登録する」とは、VDAが配置されているゾーン内のControllerにVDAが登録することを意味します。

このリリースでのゾーンは、XenAppバージョン6.5以前のゾーンと似ていますが、同一ではありません。たとえば、このゾーンの実装では、データコレクターはありません。サイト内のすべてのControllerは、プライマリゾーンの1つのサイトデータベースと通信します。また、このリリースではフェールオーバーゾーンと優先ゾーンの動作が異なります。

ゾーンの種類

サイトには常に1つのプライマリゾーンがあります。オプションで1つ以上のサテライトゾーンを持つこともできます。サテライトゾーンは、災害復旧、地理的に離れたデータセンター、支社、クラウド、またはクラウド内のアベイラビリティゾーンに使用できます。

プライマリゾーン:

プライマリゾーンのデフォルト名は「Primary」です。このゾーンには、SQL Serverサイトデータベース（および使用されている場合は高可用性SQLサーバー）、Web Studio、Director、Citrix StoreFront™、Citrix License Server、Citrix Gatewayが含まれます。サイトデータベースは常にプライマリゾーンに保持してください。

プライマリゾーンには、冗長性のために少なくとも2つのControllerが必要です。プライマリゾーンには、データベースおよびインフラストラクチャと密接に連携するアプリケーションを持つVDAを配置できます。

サテライトゾーン:

サテライトゾーンには、1つ以上のVDA、Controller、StoreFrontサーバー、およびCitrix Gatewayサーバーが含まれます。通常の運用では、サテライトゾーンのControllerはプライマリゾーンのデータベースと直接通信します。

サテライトゾーン、特に大規模なゾーンには、そのゾーンのマシンをプロビジョニングおよび保存するために使用されるハイパーバイザーが含まれる場合もあります。サテライトゾーンを構成する際、ハイパーバイザーまたはその他のサービス接続を関連付けることができます。（その接続を使用するカタログがすべて同じゾーンにあることを確認してください。）

サイトには、独自のニーズと環境に基づいて、さまざまな構成のサテライトゾーンを含めることができます。次の図は、プライマリゾーンとサテライトゾーンの例を示しています。

プライマリゾーンとサテライトゾーンの図(/en-us/citrix-virtual-apps-desktops/2503/media/zones1.png)

図では、次のようになります。

- **プライマリゾーン:** 2つのController、Web Studio、Director、StoreFront、License Server、およびサイトデータベース（高可用性SQL Server展開を含む）が含まれます。プライマリゾーンには、複数のVDAとCitrix Gatewayも含まれます。
- **サテライトゾーン1：Controllerを持つVDA：** サテライトゾーン1には、Controller、VDA、およびStoreFrontサーバーが含まれます。このサテライトゾーンのVDAは、ローカルのControllerに登録されます。ローカルのControllerは、プライマリゾーンのサイトデータベースおよびライセンスサーバーと通信します。

  WANが失敗した場合、ローカルホストキャッシュ機能により、サテライトゾーンのControllerは、そのゾーンのVDAへの接続の仲介を続行できます。このような展開は、従業員がローカル

のStoreFrontサイトとローカルのControllerを使用してローカルリソースにアクセスするオフィスで効果的です。

- **サテライトゾーン2: 冗長Controllerを持つVDA:** サテライトゾーン2には、2つのController、VDA、およびStoreFrontサーバーが含まれます。これは最も回復力のあるゾーンタイプであり、WANとローカルControllerの1つが同時に障害を起こした場合でも保護を提供します。

VDAの登録先とControllerのフェールオーバー先

プライマリゾーンとサテライトゾーンを含むサイトで、VDAの最小バージョンが7.7の場合:

- プライマリゾーンのVDAは、プライマリゾーンのControllerに登録します。プライマリゾーンのVDAがサテライトゾーンのControllerに登録を試みることはありません。
- サテライトゾーンのVDAは、可能であればローカルのControllerに登録します。(これは優先Controllerと見なされます。)ローカルのControllerが利用できない場合(たとえば、これ以上VDA登録を受け入れられない、または失敗した場合)、VDAはプライマリゾーンのControllerに登録を試みます。この場合、サテライトゾーンのControllerが再び利用可能になったとしても、VDAはプライマリゾーンに登録されたままになります。サテライトゾーンのVDAが、別のサテライトゾーンのControllerに登録を試みることはありません。
- ControllerのVDA検出で自動更新が有効になっており、VDAのインストール中にControllerアドレスのリストを指定した場合、初期登録のためにそのリストからControllerがランダムに選択されます（Controllerがどのゾーンにあるかに関わらず）。そのVDAがインストールされているマシンが再起動された後、VDAはローカルゾーンのControllerへの登録を優先し始めます。
- サテライトゾーンのControllerが失敗した場合、可能であれば別のローカルControllerにフェイルオーバーします。ローカルControllerが利用できない場合は、プライマリゾーンのControllerにフェイルオーバーします。
- Controllerをゾーンに出し入れし、自動更新が有効になっている場合、両方のゾーンのVDAは、どのControllerがローカルで、どのControllerがプライマリゾーンにあるかを示す更新されたリストを受け取ります。これにより、VDAは登録できる相手と接続を受け入れる相手を認識します。
- カタログを別のゾーンに移動すると、そのカタログ内のVDAは、カタログを移動したゾーンのControllerに再登録します。(カタログを別のゾーンに移動するときは、このゾーンと関連するホスト接続があるゾーンが適切に接続されていることを確認してください。帯域幅が制限されているか、高遅延の場合は、ホスト接続を関連するマシンカタログを含む同じゾーンに移動してください。)

プライマリゾーン内のすべてのControllerが失敗した場合：

- Web Studioはサイトに接続できません。

- プライマリゾーン内のVDAへの接続はできません。
- プライマリゾーン内のControllerが利用可能になるまで、サイトのパフォーマンスが低下します。

VDAバージョン7.7より前のサイトの場合：

- サテライトゾーンのVDAは、そのローカルゾーンとプライマリゾーンのControllerからの要求を受け入れます。(最小バージョン7.7のVDAは、他のサテライトゾーンからのController要求を受け入れることができます。)
- サテライトゾーンのVDAは、プライマリゾーンまたはローカルゾーンのControllerにランダムに登録します。(最小バージョン7.7のVDAはローカルゾーンを優先します。)

ゾーンの優先順位

ゾーン優先機能を使用するには、最小限StoreFront 3.7およびCitrix Gateway 11.0-65.xを使用している必要があります。

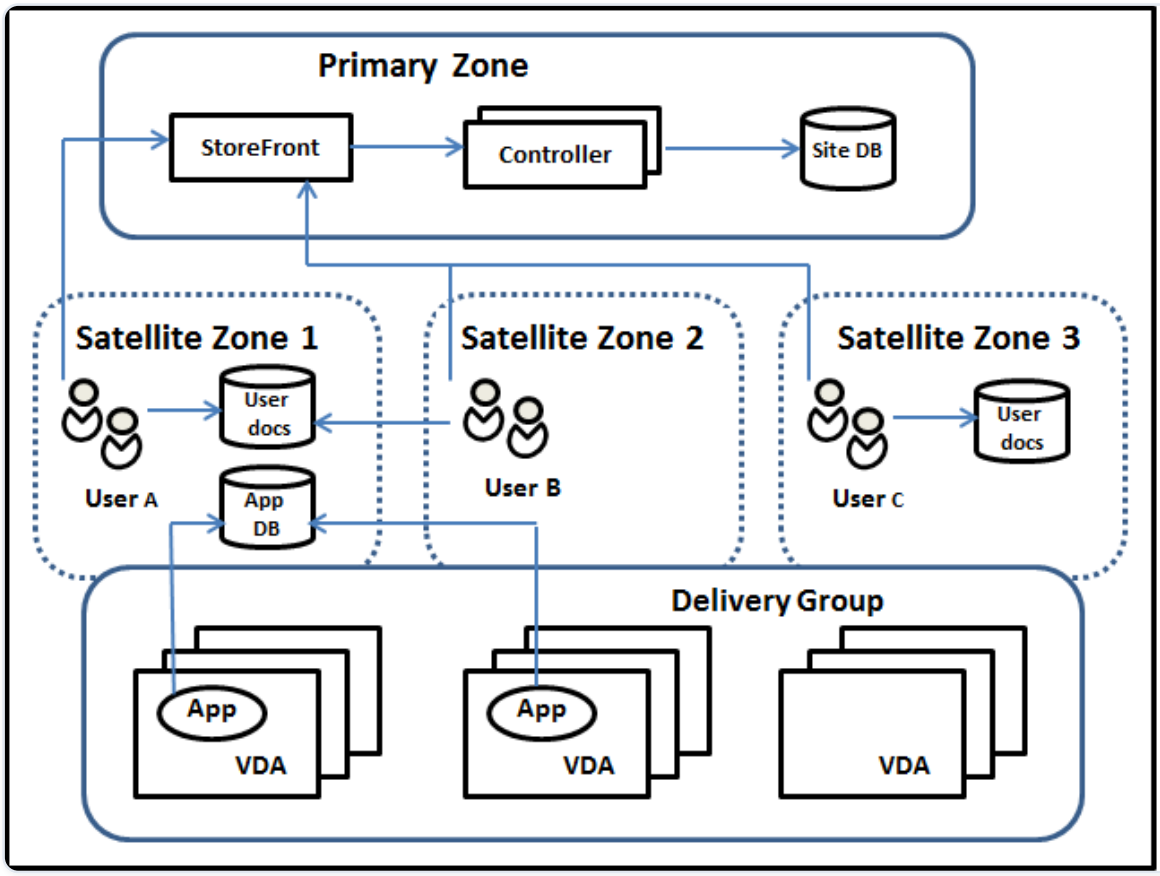
マルチゾーンサイトでは、ゾーン優先機能により、管理者はアプリケーションまたはデスクトップの起動に使用されるVDAをより柔軟に制御できます。

ゾーンの優先順位の仕組み

ゾーンの優先順位には3つの形式があります。特定のゾーンのVDAを使用することを優先する場合があります。その理由は次のとおりです。

- アプリケーションのデータが保存されている場所。これはアプリケーションホームと呼ばれます。
- ユーザーのホームデータ（プロファイルやホーム共有など）の場所。これはユーザーホームと呼ばれます。
- ユーザーの現在の場所（Citrix Workspace™アプリが実行されている場所）。これはユーザーの場所と呼ばれます。

次の図は、マルチゾーン構成の例を示しています。



この例では、VDAは3つのサテライトゾーンに分散していますが、すべて同じデリバリーグループに属しています。そのため、ブローカーはユーザーの起動要求に対してどのVDAを使用するかを選択できます。この例は、ユーザーがCitrix Workspaceアプリのエンドポイントを実行できる場所がいくつかあることを示しています。

- ユーザーAは、サテライトゾーン1でCitrix Workspaceアプリがインストールされたデバイスを使用しています。
- ユーザーBは、サテライトゾーン2でデバイスを使用しています。
- ユーザーのドキュメントはさまざまな場所に保存できます。
  - ユーザーAとBは、サテライトゾーン1にある共有を使用します。
  - ユーザーCは、サテライトゾーンCの共有を使用します。
  - 公開されているアプリケーションの1つは、サテライトゾーン1にあるデータベースを使用します。

ユーザーまたはアプリケーションにホームゾーンを構成することで、ユーザーまたはアプリケーションをゾーンに関連付けます。Delivery Controller™ のブローカーは、リソースが利用可能な場合、これらの関連付けを使用してセッションが起動されるゾーンの選択を支援します。次のことができます。

- ユーザーをゾーンに追加して、ユーザーのホームゾーンを構成します。

- アプリケーションのプロパティを編集して、アプリケーションのホームゾーンを構成します。

ユーザーまたはアプリケーションは、一度に1つのホームゾーンしか持つことができません。（ユーザーグループのメンバーシップにより複数のゾーンメンバーシップが発生する場合、ユーザーには例外が発生する可能性があります。「その他の考慮事項」セクションを参照してください。ただし、この場合でも、ブローカーは1つのホームゾーンのみを使用します。）

ユーザーおよびアプリケーションのゾーン設定を構成できますが、ブローカーは起動時に優先ゾーンを1つだけ選択します。優先ゾーンを選択するためのデフォルトの優先順位は、アプリケーションホーム \> ユーザーホーム \> ユーザーロケーションです。この順序を制限できます。ゾーン設定の調整を参照してください。ユーザーがアプリケーションを起動すると、次のようになります。

- そのアプリケーションに構成済みのゾーン関連付け（アプリケーションホーム）がある場合、優先ゾーンはそのアプリケーションのホームゾーンになります。
- アプリケーションに構成済みのゾーン関連付けがないが、ユーザーに構成済みのゾーン関連付け（ユーザーホーム）がある場合、優先ゾーンはそのユーザーのホームゾーンになります。
- アプリケーションとユーザーのどちらにも構成済みのゾーン関連付けがない場合、優先ゾーンはユーザーがCitrix Workspaceアプリインスタンスを実行しているゾーン（ユーザーロケーション）になります。そのゾーンが定義されていない場合、ランダムなVDAとゾーンの選択が使用されます。優先ゾーン内のすべてのVDAに負荷分散が適用されます。優先ゾーンがない場合、Delivery Group内のすべてのVDAに負荷分散が適用されます。

ゾーンの優先順位の調整

ユーザーまたはアプリケーションのホームゾーンを構成（または削除）する際、ゾーン設定の使用方法をさらに制限することもできます。

- **必須のユーザーホームゾーンの使用:** Delivery Groupでは、セッションがユーザーのホームゾーン（構成されている場合）で起動するように指定できます。ホームゾーンに利用可能なリソースがない場合でも、他のゾーンへのフェイルオーバーは行われません。この制限は、ゾーン間で大きなプロファイルやデータファイルをコピーするリスクを回避する必要がある場合に役立ちます。つまり、別のゾーンでセッションを起動するよりも、セッションの起動を拒否する方が望ましいということです。
- **必須のアプリケーションホームゾーンの使用:** 同様に、アプリケーションのホームゾーンを構成する際、アプリケーションがそのゾーンでのみ起動され、アプリケーションのホームゾーンでリソースが利用できない場合でも別のゾーンへのフェイルオーバーは行われないように指定できます。

- **アプリケーションホームゾーンなし、および構成済みユーザーホームゾーンを無視:** アプリケーションのホームゾーンを指定しない場合、そのアプリケーションを起動する際に、構成済みのユーザーゾーンを考慮しないように指定することもできます。たとえば、一部のユーザーが異なるホームゾーンを持っていても、ユーザーロケーションゾーン設定を使用して、ユーザーがデバイスに近いVDAでアプリケーションを実行することを優先する場合があります。

優先ゾーンがセッションの使用に与える影響

ユーザーがアプリケーションまたはデスクトップを起動すると、ブローカーは既存のセッションを使用するよりも優先ゾーンを使用することを優先します。

アプリケーションまたはデスクトップを起動するユーザーが、起動されるリソースに適したセッション（たとえば、アプリケーションのセッション共有を使用できるセッション、または起動されるリソースがすでに実行されているセッション）をすでに持っているが、そのセッションがユーザー/アプリケーションの優先ゾーン以外のゾーンにあるVDAで実行されている場合、システムは新しいセッションを作成する可能性があります。これにより、そのユーザーのセッション要件にとって優先度の低いゾーンのセッションに再接続するよりも前に、正しいゾーンでの起動（利用可能な容量がある場合）が満たされます。

到達できなくなった孤立セッションを防ぐため、既存の切断されたセッションへの再接続は、優先されないゾーンにある場合でも許可されます。

起動を満たすためのセッションの望ましさの順序は次のとおりです。

1. 優先ゾーン内の既存のセッションに再接続します。
2. 優先ゾーン以外のゾーンにある既存の切断されたセッションに再接続します。
3. 優先ゾーンで新しいセッションを開始します。
4. 優先ゾーン以外のゾーンにある接続済みの既存セッションに再接続します。
5. 優先ゾーン以外のゾーンで新しいセッションを開始します。

その他のゾーン優先度に関する考慮事項

- ユーザーグループ（セキュリティグループなど）にホームゾーンを構成すると、そのグループのユーザー（直接的または間接的なメンバーシップを通じて）は指定されたゾーンに関連付けられます。ただし、ユーザーは複数のセキュリティグループのメンバーである可能性があり、そのため、他のグループメンバーシップを通じて異なるホームゾーンが構成されている場合があります。このような場合、そのユーザーのホームゾーンの決定は曖昧になる可能性があります。

ユーザーがグループメンバーシップを通じて取得したものではない構成済みのホームゾーンを持っている場合、そのゾーンがゾーン優先度に使用されます。グループメンバーシップを通じて取得されたゾーン関連付けはすべて無視されます。

ユーザーがグループメンバーシップのみを通じて取得した複数の異なるゾーン関連付けを持っている場合、ブローカーはゾーンの中からランダムに選択します。ブローカーがこの選択を行うと、そのゾーンはユーザーのグループメンバーシップが変更されるまで、以降のセッション起動に使用されます。

- ユーザーロケーションゾーンの優先度では、エンドポイントデバイス上のCitrix Workspaceアプリが、そのデバイスが接続しているCitrix Gatewayによって検出される必要があります。Citrix Gatewayは、IPアドレスの範囲を特定のゾーンに関連付けるように構成する必要があり、検出されたゾーンIDはStoreFrontを介してControllerに渡される必要があります。

ゾーン優先度について詳しくは、「ゾーン優先度の内部」を参照してください。

考慮事項、要件、およびベストプラクティス

- ゾーンには、コントローラー、マシンカタログ、ホスト接続、ユーザー、アプリケーションを配置できます。カタログがホスト接続を使用する場合、カタログと接続が同じゾーンにあることを確認してください。(ただし、低遅延で高帯域幅の接続が利用可能な場合は、異なるゾーンに配置できます。)
- アイテムをサテライトゾーンに配置すると、サイトがそれらや関連する他のオブジェクトとどのようにやり取りするかに影響します。
    - コントローラーがサテライトゾーンに配置されると、それらのマシンは同じゾーン内のハイパーバイザーおよびVDAと良好な（ローカル）接続性を持つと想定されます。そのサテライトゾーンのコントローラーは、それらのハイパーバイザーおよびVDAマシンの処理において、プライマリゾーンのコントローラーよりも優先的に使用されます。
    - ハイパーバイザー接続がサテライトゾーンに配置されると、そのハイパーバイザー接続を介して管理されるすべてのハイパーバイザーもそのサテライトゾーンに存在すると想定されます。そのサテライトゾーンのコントローラーは、そのハイパーバイザー接続と通信する際に、プライマリゾーンのコントローラーよりも優先的に使用されます。
    - マシンカタログがサテライトゾーンに配置されると、そのカタログ内のすべてのVDAマシンがサテライトゾーンにあると想定されます。各VDAの初回登録後にコントローラーリストの自動更新メカニズムがアクティブになった後、サイトへの登録を試みる際には、プライマリゾーンのコントローラーよりもローカルコントローラーが優先的に使用されます。
    - Citrix Gatewayインスタンスもゾーンに関連付けることができます。これは、ここで説明する他の要素のようにサイト構成の一部としてではなく、StoreFrontのOptimal HDX™ルー

ティング構成の一部として行われます。Citrix Gatewayがゾーンに関連付けられている場合、そのゾーン内のVDAマシンへのHDX接続が使用される際に、優先的に使用されます。

- 運用サイトを作成し、最初のカタログとデリバリーグループを作成すると、すべてのアイテムはプライマリゾーンに配置されます。この初期設定が完了するまで、サテライトゾーンを作成することはできません。(空のサイトを作成した場合、プライマリゾーンには最初にコントローラーのみが含まれます。カタログとデリバリーグループを作成する前または後にサテライトゾーンを作成できます。)
- 1つ以上のアイテムを含む最初のサテライトゾーンを作成すると、サイト内の他のすべてのアイテムはプライマリゾーンに残ります。
- プライマリゾーンはデフォルトで「Primary」という名前ですが、この名前は変更できます。Web Studioはどのゾーンがプライマリゾーンであるかを示しますが、プライマリゾーンには識別しやすい名前を使用することがベストプラクティスです。プライマリゾーンを再割り当て（つまり、別のゾーンをプライマリゾーンにする）できますが、常にサイトデータベースと高可用性サーバーが含まれている必要があります。
- サイトデータベースは常にプライマリゾーンに保持してください。
- ゾーンを作成した後、後でアイテムをあるゾーンから別のゾーンに移動できます。この柔軟性により、近接して動作するのが最適なアイテムを分離できる可能性があります。たとえば、カタログを、そのカタログ内のマシンを作成する接続（ホスト）とは異なるゾーンに移動すると、パフォーマンスに影響を与える可能性があります。ゾーン間でアイテムを移動する前に、予期しない影響の可能性を考慮してください。カタログとそれが使用するホスト接続は同じゾーンに、または良好に接続されたゾーン（たとえば、低遅延で高帯域幅のネットワーク経由）に保持してください。
- 最適なパフォーマンスを得るには、Web StudioとDirectorはプライマリゾーンにのみインストールしてください。Web StudioとDirectorはWebアプリケーションであるため、サテライトゾーン（たとえば、プライマリゾーンがアクセス不能になった場合のフェイルオーバーとして使用するコントローラーを含むサテライトゾーン）からアクセスできます。
- 理想的には、サテライトゾーンのCitrix Gatewayは、他のゾーンまたは外部の場所からそのゾーンに入ってくるユーザー接続に使用されますが、ゾーン内の接続にも使用できます。
- 注意：ゾーン優先機能を使用するには、StoreFront 3.7以降およびCitrix Gateway 11.0-65.x以降を使用している必要があります。

接続品質の制限

サテライトゾーンのControllerは、サイトデータベースと直接SQL対話を行います。これにより、サテライトゾーンとサイトデータベースを含むプライマリゾーン間のリンクの品質にいくつかの制限が課されます。具体的な制限は、サテライトゾーンに展開されているVDAの数と、それらの

VDA上のユーザーセッションの数に比例します。したがって、VDAとセッションが少ないサテライトゾーンは、VDAとセッションが多いサテライトゾーンよりも、データベースへの接続品質が低い状態でも機能できます。

詳しくは、「待機時間とSQLブロッククエリの改善」を参照してください。

ブローカー処理のパフォーマンスに対する待機時間の影響

ゾーンによってユーザーは待機時間の長いリンク上に配置できますが、ローカルブローカーが存在する場合でも、追加の待機時間はエンドユーザーエクスペリエンスに必然的に影響を与えます。ユーザーが行うほとんどの作業において、サテライトゾーンのControllerとサイトデータベース間のラウンドトリップによって引き起こされる遅延が発生します。

アプリケーションの起動では、セッションブローカー処理がセッション起動要求を送信するのに適したVDAを特定する際に、追加の遅延が発生します。

ゾーンの作成と管理

フル管理者であれば、すべてのゾーン作成および管理タスクを実行できます。ただし、ゾーンの作成、編集、削除を許可するカスタムロールを作成することもできます。ゾーン間でアイテムを移動する場合、ゾーン関連の権限（ゾーンの読み取り権限を除く）は必要ありませんが、移動するアイテムに対する編集権限が必要です。たとえば、カタログをあるゾーンから別のゾーンに移動するには、そのカタログに対する編集権限が必要です。詳しくは、「委任管理」を参照してください。

Citrix Provisioning™を使用している場合： Citrix Provisioningコンソールはゾーンを認識しないため、サテライトゾーンのカタログを作成するにはWeb Studioを使用することをお勧めします。Web Studioでカタログを作成し、正しいサテライトゾーンを指定します。その後、Citrix Provisioningコンソールを使用して、そのカタログ内のマシンをプロビジョニングします。（Citrix Provisioningウィザードを使用してカタログを作成した場合、カタログはプライマリゾーンに配置されます。後でWeb Studioを使用してサテライトゾーンに移動する必要があります。）

ゾーンの作成

1. Web Studioにサインインします。
2. 左側のペインで を選択します。
3. アクションバーで を選択します。
4. ゾーンの名前と説明（オプション）を入力します。名前はサイト内で一意である必要があります。

5. 新しいゾーンに配置するアイテムを選択します。選択可能なアイテムのリストをフィルター処理または検索できます。空のゾーンを作成することもできます。その場合は、どのアイテムも選択しないでください。
6. **［保存］**をクリックします。

この方法の代わりに、Web Studioで1つ以上のアイテムを選択し、アクションバーで を選択することもできます。

ゾーン名または説明の変更

1. Web Studioにサインインします。
2. 左側のペインで を選択します。
3. 中央のペインでゾーンを選択し、アクションバーで**ゾーンの編集**を選択します。
4. ゾーン名、説明、またはその両方を変更します。プライマリゾーンの名前を変更する場合は、そのゾーンがプライマリゾーンとして容易に識別できることを確認してください。
5. または をクリックします。

項目をあるゾーンから別のゾーンに移動する

1. Web Studioにサインインします。
2. 左側のペインで を選択します。
3. 中央ペインでゾーンを選択し、1つ以上の項目を選択します。
4. 項目を移動先のゾーンにドラッグするか、アクションバーで**項目の移動**を選択し、移動先のゾーンを指定します。

確認メッセージには、選択したアイテムが一覧表示され、それらすべてを移動してもよろしいかどうかが尋ねられます。

注意: カタログがハイパーバイザーまたはその他のサービスへのホスト接続を使用する場合、カタログと接続の両方を同じゾーンに配置してください。そうしないと、パフォーマンスに影響が出る可能性があります。一方を移動する場合は、もう一方も移動してください。

ゾーンを削除する

ゾーンを削除するには、ゾーンが空である必要があります。プライマリゾーンは削除できません。

1. Web Studioにサインインします。
2. 左ペインで**ゾーン**を選択します。
3. 中央ペインでゾーンを選択します。

4. アクションバーから**ゾーンの削除**を選択します。ゾーンが空でない場合（項目が含まれている場合）、それらの項目を移動するゾーンを選択するよう求められます。
5. 削除を確定します。

ユーザーのホームゾーンを追加する

ユーザーのホームゾーンを構成することは、*ユーザーをゾーンに追加する*とも呼ばれます。

1. Web Studioにサインインします。
2. 左ペインで**ゾーン**を選択し、中央ペインでゾーンを選択します。
3. アクションバーで**ゾーンにユーザーを追加**を選択します。
4. **ゾーンにユーザーを追加**ダイアログボックスで、**追加**をクリックし、ゾーンに追加するユーザーとユーザーグループを選択します。すでにホームゾーンを持つユーザーを指定した場合、メッセージに2つの選択肢が表示されます:**はい** = ホームゾーンを持たない指定したユーザーのみを追加します。**いいえ** = ユーザー選択ダイアログに戻ります。
5. **OK**をクリックします。

ホームゾーンが構成されているユーザーの場合、セッションをそのホームゾーンからのみ起動するように要求できます。

1. デリバリーグループを作成または編集します。
2. **ユーザー**ページで、**セッションをユーザーのホームゾーンで起動することを要求する（構成されている場合）**チェックボックスをオンにします。

そのデリバリーグループのユーザーが起動するすべてのセッションは、そのユーザーのホームゾーン内のマシンから起動する必要があります。デリバリーグループ内のユーザーにホームゾーンが構成されていない場合、この設定は無効です。

ユーザーのホームゾーンを削除する

この手順は、ゾーンからユーザーを削除することとも呼ばれます。

1. Web Studioにサインインします。
2. 左側のペインで**ゾーン**を選択し、中央のペインでゾーンを選択します。
3. アクションバーで**ゾーンからユーザーを削除**を選択します。
4. 「**ゾーンにユーザーを追加**」ダイアログボックスで、**削除**をクリックし、ゾーンから削除するユーザーとグループを選択します。この操作では、ユーザーはゾーンからのみ削除されます。これらのユーザーは、所属するデリバリーグループおよびアプリケーショングループに残ります。

5. プロンプトが表示されたら、削除を確認します。

アプリケーションのホームゾーンを管理する

アプリケーションのホームゾーンを構成することは、アプリケーションをゾーンに追加することとも呼ばれます。デフォルトでは、マルチゾーン環境では、アプリケーションにホームゾーンはありません。

アプリケーションのホームゾーンは、アプリケーションのプロパティで指定されます。アプリケーションのプロパティは、アプリケーションをグループに追加するとき、または後で構成できます。

- デリバリーグループを作成する、アプリケーショングループを作成する、または既存のグループにアプリケーションを追加するときに、ウィザードの**アプリケーション**ページで**プロパティ**を選択します。
- アプリケーションの追加後にアプリケーションのプロパティを変更するには、左側のペインで**アプリケーション**を選択します。アプリケーションを選択し、アクションバーで**アプリケーションプロパティの編集**を選択します。

アプリケーションのプロパティ/設定の ページで、次の操作を行います。

- アプリケーションにホームゾーンを設定したい場合：
  - **選択したゾーンを使用して決定する**ラジオボタンを選択し、ゾーンを選択します。
  - アプリケーションを、選択したゾーンからのみ（他のゾーンからは起動しない）起動したい場合は、ゾーン選択の下にあるチェックボックスを選択します。
- アプリケーションにホームゾーンを設定したくない場合：
  - **ホームゾーンを構成しない**ラジオボタンを選択します。
  - このアプリケーションを起動する際に、ブローカーが構成済みのユーザーゾーンを考慮しないようにしたい場合は、ラジオボタンの下にあるチェックボックスを選択します。この場合、アプリケーションまたはユーザーのホームゾーンのいずれも、このアプリケーションを起動する場所を決定するために使用されません。

ゾーンの指定を含むその他のアクション

少なくとも1つのサテライトゾーンを作成した後、ホスト接続を追加するか、カタログを作成する際にゾーンを指定できます。

通常、プライマリゾーンがデフォルトです。Machine Creation Services™を使用してカタログを作成する場合、ホスト接続用に構成されたゾーンが自動的に選択されます。

サイトにサテライトゾーンが含まれていない場合、プライマリゾーンが想定され、ゾーン選択ボックスは表示されません。

キャッシュからブローカーユーザーを削除する

管理者がキャッシュからブローカーユーザーを削除できない場合や、`Get-BrokerUser` の実行時にユーザーが AD から誤った SID を表示する場合があります。

これは、ユーザーが AD から削除されて再作成されたにもかかわらず、ブローカーキャッシュに以前のユーザー SID が残っている場合に発生します。

これを解決するには、次の手順を実行します。

1. Active Directory からユーザーを削除します。
2. 削除された各アカウントに対して `Get-BrokerUser` を実行します。どこからも参照されていないアカウントは、結果を返しません。参照されているユーザーの場合、`Get-BrokerUser` を実行すると値が取得されます。次に、ユーザーが割り当てられているリソースを特定し、それらのリソースからユーザーを手動で削除する必要があります。

   例:

   - ユーザーがアプリケーションに割り当てられているかを確認します: `Get-BrokerApplication`
   - ユーザーがアプリケーショングループに割り当てられているかを確認します: `Get-BrokerApplicationGroup`
   - ユーザーがアクセスポリシーに割り当てられているかを確認します: `Get-BrokerAccessPolicyRule`
   - ユーザーがアプリケーションエンタイトルメントポリシーに割り当てられているかを確認します: `Get-BrokerAppEntitlementPolicyRule`
   - ユーザーがデスクトップエンタイトルメントポリシーに割り当てられているかを確認します: `Get-BrokerEntitlementPolicyRule`
   - ユーザーがデスクトップグループセッションの残存に割り当てられているかを確認します: `Get-BrokerSessionLinger`
   - ユーザーが VDA 上でセッションを実行しているかを確認します: `Get-BrokerSession`
   - ユーザーがマージされたグループのリソースに割り当てられているかを確認します: `Get-BrokerMergedResource`

- ユーザーがリソースグループに割り当てられているかを確認します: `Get-BrokerMergeGroup`
- ユーザーに対してコマンドがキューに入っているか確認します: `Get-BrokerMachineCommand`
- ユーザーがプライベートデスクトップに割り当てられているか確認します: `Get-BrokerMachine`
- ユーザーがゾーン設定に割り当てられているか確認します: `Get-BrokerUserZonePreference`

3. リソースからユーザーを手動で削除します。
4. `Get-BrokerUser` コマンドを実行して、ユーザーがすべてのリソースから削除されたことを確認します。
5. ユーザーがすべてのリソースから削除されたら、キャッシュからユーザーを削除するために、以下を実行します。

```
Update-BrokerNameCache -Users -Purge -UnusedFor 0
```

モニター

管理者とヘルプデスク担当者は、さまざまな機能とツールを使用してCitrix Virtual Apps and Desktops™サイトを監視できます。これらのツールを使用して、以下を監視できます。

- ユーザーセッションおよびセッションの使用状況
- ログオンパフォーマンス
- 接続とマシン（障害を含む）
- 負荷評価
- 履歴トレンド
- インフラストラクチャ

Citrix Director (シトリックス ディレクター)

Directorは、監視とトラブルシューティング、およびエンドユーザーのサポートタスクの実行に使用できるリアルタイムのWebツールです。

詳細については、Director の記事を参照してください。

構成ログ

構成ログを使用すると、管理者はサイトへの管理上の変更を追跡できます。構成ログは、構成変更が行われた後の問題の診断とトラブルシューティングに役立ち、変更管理と構成の追跡を支援し、管理アクティビティを報告できます。

Studioからログに記録された情報のレポートを表示および生成できます。また、Directorのトレンドビューでログに記録された項目を表示して、構成変更の通知を提供することもできます。この機能は、Studioにアクセスできない管理者にとって役立ちます。

トレンドビューは、一定期間にわたる構成変更の履歴データを提供します。これにより、管理者はサイトに対してどのような変更がいつ誰によって行われたかを評価し、問題の原因を特定できます。このビューは、構成情報を3つのカテゴリに分類します。

- 接続障害
- 失敗したシングルセッションマシン

- 失敗したマルチセッションマシン

構成ログの有効化と構成方法の詳細については、「構成ログ」を参照してください。Directorの記事では、そのツールからログ情報を表示する方法について説明しています。

イベントログ

Citrix Virtual Apps and Desktops 内のサービスは、発生したイベントをログに記録します。イベントログは、操作の監視とトラブルシューティングに使用されます。

詳細については、イベントログを参照してください。個々の機能の記事にもイベント情報が含まれている場合があります。

構成ログ

構成ログは、サイト構成の変更と管理アクティビティをデータベースに記録する機能です。この機能はデフォルトで有効になっています。ログに記録されたコンテンツを使用して、次のことができます。

- 構成変更が行われた後の問題の診断とトラブルシューティング。ログはブレッドクラムトレイルを提供します。
- 変更管理を支援し、構成を追跡する。
- 管理アクティビティを報告する。

Citrix Studioから、構成ログ設定を設定し、構成ログを表示し、HTMLおよびCSVレポートを生成します。構成ログの表示は、日付範囲と全文検索結果でフィルタリングできます。強制ログが有効になっている場合、ログに記録できない限り、構成変更は行われません。適切な権限があれば、構成ログからエントリを削除できます。構成ログ機能を使用してログコンテンツを編集することはできません。

構成ログは、PowerShell SDKと構成ログサービスを使用します。構成ログサービスは、サイト内のすべてのコントローラーで実行されます。いずれかのコントローラーで障害が発生した場合、別のコントローラーのサービスがログ要求を自動的に処理します。

デフォルトでは、構成ログ機能は有効になっており、サイト作成時に作成されるデータベース（サイト構成データベース）を使用します。データベースの別の場所を指定できます。構成ログデータベースは、サイト構成データベースと同じ高可用性機能をサポートします。

構成ログへのアクセスは、委任管理によって制御され、「ログ設定の編集」および「構成ログの表示」権限が付与されます。

構成ログは、作成時にローカライズされます。たとえば、英語で作成されたログは、リーダーのロケールに関係なく、英語で読み取られます。

ログに記録される内容

Studio、Director、およびPowerShellスクリプトから開始された構成変更と管理アクティビティはログに記録されます。ログに記録される構成変更の例には、次のものとの連携（作成、編集、削除、割り当て）が含まれます。

- マシンカタログ
- デリバリーグループ（電源管理設定の変更を含む）
- 管理者ロールとスコープ
- ホストリソースと接続
- Studioを介したCitrixポリシー

ログに記録される管理変更の例には、以下が含まれます。

- 仮想マシンまたはユーザーデスクトップの電源管理
- StudioまたはDirectorがユーザーにメッセージを送信する

次の操作はログに記録されません。

- プール管理による仮想マシンの電源投入などの自律的な操作。
- グループポリシー管理コンソール (GPMC) を介して実装されたポリシーアクション。これらのアクションのログを表示するには、Microsoft ツールを使用します。
- レジストリ、データベースへの直接アクセス、または Studio、Director、PowerShell 以外のソースを介して行われた変更。
- 展開が初期化されると、最初の構成ログサービスインスタンスが構成サービスに登録されたときに、構成ログが利用可能になります。したがって、構成の初期段階はログに記録されません (たとえば、データベーススキーマが取得および適用されたとき、ハイパーバイザーが初期化されたときなど)。

構成ログの管理

デフォルトでは、構成ログはサイトの作成時に作成されるデータベース (サイト構成データベースとも呼ばれます) を使用します。Citrix は、次の理由から、構成ログデータベース (および監視データベース) には別の場所を使用することをお勧めします。

- 構成ログデータベースのバックアップ戦略は、サイト構成データベースのバックアップ戦略とは異なる可能性があります。
- 構成ログ (および監視サービス) のために収集されるデータ量によって、サイト構成データベースで利用可能な領域に悪影響が及ぶ可能性があります。
- 3つのデータベースの単一障害点を分割します。

構成ログをサポートしない製品エディションには、Studioにログノードがありません。

構成ログと強制ログの有効化と無効化

デフォルトでは、構成ログは有効になっており、強制ログは無効になっています。

1. Web Studioにサインインし、左ペインで**ログ**を選択します。
2. アクションバーで**設定**を選択します。構成ログダイアログボックスには、データベース情報が含まれており、構成ログと強制ログが有効か無効かを示します。
3. 目的のアクションを選択します。

   構成ログを有効にするには、**有効にする**を選択します。これはデフォルト設定です。データベースに書き込めない場合、ログ情報は破棄されますが、操作は続行されます。

   構成ログを無効にするには、**Disable** を選択します。以前にログが有効になっていた場合、既存のログはPowerShell SDKで読み取り可能です。

   強制ログを有効にするには、**Prevent changes to the site configuration when the database is not available** を選択します。通常ログに記録される構成変更や管理アクティビティは、構成ログデータベースに書き込みが可能な場合にのみ許可されます。強制ログは、構成ログが有効になっている場合（**Enable** が選択されている場合）にのみ有効にできます。構成ログサービスが失敗し、高可用性が使用されていない場合、強制ログが有効であると見なされます。そのような場合、通常ログに記録される操作は実行されません。

   強制ログを無効にするには、**データベースが利用できない場合にサイト構成の変更を許可する**を選択します。構成ログデータベースにアクセスできない場合でも、構成変更および管理アクティビティは許可されます。これはデフォルト設定です。

構成ログデータベースの場所を変更する

強制ログが有効になっている場合、データベースの場所を変更することはできません。これは、場所の変更にはログに記録できない短い切断期間が含まれるためです。

1. サポートされているSQL Serverバージョンを使用して、データベースサーバーを作成します。
2. Web Studioにサインインし、左ペインで**ログ**を選択します。

3. アクションバーで**設定**を選択します。
4. 「ログ設定」ダイアログボックスで、「**ログデータベースの変更**」を選択します。
5. 「ログデータベースの変更」ダイアログボックスで、新しいデータベースサーバーを含むサーバーの場所を指定します。有効な形式については、「データベースアドレス形式」を参照してください。
6. Studioでデータベースを作成するには、「**OK**」をクリックします。プロンプトが表示されたら「**OK**」をクリックすると、データベースが自動的に作成されます。Studioは、現在のStudioユーザーの資格情報を使用してデータベースへのアクセスを試行します。失敗した場合は、データベースユーザーの資格情報の入力を求められます。その後、Studioはデータベーススキーマをデータベースにアップロードします。（資格情報はデータベース作成中のみ保持されます。）
7. データベースを手動で作成するには、「**データベーススクリプトの生成**」をクリックします。生成されたスクリプトには、データベースを手動で作成するための手順が含まれています。スキーマをアップロードする前に、データベースが空であり、少なくとも1人のユーザーがデータベースにアクセスして変更する権限を持っていることを確認してください。

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

構成ログコンテンツの表示

構成ログコンテンツを表示するには、左ペインで「**ログ**」を選択し、「**イベント**」タブを選択します。

デフォルトでは、イベントログは管理者名で一覧表示されます。必要に応じて、次のタスクを実行できます。

- **ログの詳細を表示します。** 高レベルの操作は、1つ以上のサービスおよびSDK呼び出し（低レベルの操作）をもたらします。上部のペインで高レベルの操作を選択すると、下部のペインに低レベルの操作が表示されます。
- **表示を並べ替えます。** 列ヘッダーをクリックして表示を並べ替えます。
- **ログをフィルターします。** 日間隔やカスタム期間などのフィルター条件を設定するか、検索ボックスにメインタスクの完全または部分的な名前を入力して表示を絞り込みます。検索を使用した後に標準表示に戻るには、検索ボックスのテキストをクリアします。
- **ログをエクスポートします。** 選択したログまたはすべてのログをCSVファイルにエクスポートして、アーカイブまたは詳細な分析を行います。

- **列をカスタマイズします。** クライアントIPやラベルなどのデフォルト以外の列を追加して、表示をニーズに合わせて調整します。
- **ラベルを管理します。** イベントログのラベルを追加、編集、削除して、ログの整理と追跡を強化します。

表示特性:

- 操作が完了する前に失敗した場合、ログ操作がデータベースで完了しない可能性があります。たとえば、開始レコードに対応する停止レコードがない場合などです。このような場合、ログには情報が不足していることが示されます。時間範囲に基づいてログを表示すると、データが条件に一致する場合、不完全なログが表示されます。

  たとえば、過去5日間のログを要求し、過去5日間に開始時刻があるログに終了時刻がない場合、そのログは含まれます。
- PowerShellコマンドレットを呼び出すスクリプトを使用する場合、親の高レベル操作を指定せずに低レベル操作を作成すると、構成ログは代理の高レベル操作を作成します。

レポートを生成する

構成ログデータを含むCSVおよびHTMLレポートを生成できます。

- CSVレポートには、指定された時間間隔のすべてのログデータが含まれます。データベース内の階層データは、単一のCSVテーブルにフラット化されます。データのどの側面もファイル内で優先されません。書式設定は使用されず、人間が読めることは想定されていません。ファイル（MyReportという名前）には、普遍的に利用可能な形式でデータが含まれています。CSVファイルは、データのアーカイブや、Microsoft Excelなどのレポート作成ツールやデータ操作ツールのデータソースとしてよく使用されます。
- HTMLレポートは、指定された時間間隔のログデータを人間が読める形式で提供します。変更を確認するための構造化されたナビゲート可能なビューを提供します。HTMLレポートは、SummaryとDetailsという名前の2つのファイルで構成されます。Summaryには、各操作がいつ、誰によって行われたか、およびその結果といった高レベルの操作が一覧表示されます。各操作の横にある**Details**リンクをクリックすると、Detailsファイル内の低レベル操作に移動し、追加情報が表示されます。

構成ログレポートを生成するには、Studioナビゲーションペインで**Logging**を選択し、アクションバーで**Create custom report**を選択します。

- レポートの日付範囲を選択します。
- レポート形式（CSV、HTML、またはその両方）を選択します。

- レポートを保存する場所を参照します。

構成ログコンテンツを削除する

構成ログを削除するには、特定の委任管理権限とSQL Serverデータベース権限が必要です。

- **委任管理:** 展開構成を読み取ることができる委任管理ロールが必要です。完全管理者ロールにはこの権限があります。カスタムロールには、その他の権限カテゴリで「読み取り専用」または「管理」が選択されている必要があります。

  構成ログデータを削除する前にバックアップを作成するには、カスタムロールにログ権限カテゴリで「読み取り専用」または「管理」が選択されている必要もあります。

- **SQL Serverデータベース:** データベースからレコードを削除する権限を持つSQL Serverログインが必要です。これには2つの方法があります。

  - データベースサーバー上のあらゆるアクティビティを実行できるsysadminサーバーロールを持つSQL Serverデータベースログインを使用します。または、`serveradmin`または`setupadmin`サーバーロールを使用すると、削除操作を実行できます。
  - 展開でより高いセキュリティが必要な場合は、データベースからレコードを削除する権限を持つデータベースユーザーにマッピングされた非sysadminデータベースログインを使用します。

    a. SQL Server Management Studioで、「sysadmin」以外のサーバーロールを持つSQL Serverログインを作成します。

    b. ログインをデータベース内のユーザーにマッピングします。SQL Serverは、ログインと同じ名前のユーザーをデータベース内に自動的に作成します。

    c. データベースロールメンバーシップで、データベースユーザーのロールメンバーの少なくとも1つを指定します: `ConfigurationLoggingSchema_ROLE`または`dbowner`。

  詳細については、SQL Server Management Studioのドキュメントを参照してください。

構成ログを削除するには:

1. Web Studioにサインインし、左ペインで**ログ**を選択します。
2. アクションバーで**ログの削除**を選択します。
3. ログを削除する前にバックアップを作成するかどうかを尋ねられます。バックアップを作成することを選択した場合は、バックアップアーカイブが保存される場所を参照します。バックアップはCSVファイルとして作成されます。

構成ログがクリアされると、ログの削除が空のログに投稿される最初のアクティビティになります。そのエントリには、誰がいつログを削除したかに関する詳細が記載されています。

APIおよびPowerShellログを表示する

現在のセッション中に実行されたAPIリクエストを監視するには、**API**タブをクリックします。APIログは、Web Studioからサインアウトするとクリアされます。

その日に実行したUIアクションに対応するPowerShellコマンドを表示するには、**PowerShell**タブをクリックします。

構成ログにメタデータを関連付ける

ログレコードに`MetadataMap`と呼ばれる`name-value`ペアを関連付けることで、構成ログにメタデータを添付できます。

> **注:**
>
> - メタデータは、高レベルの操作オブジェクトにのみ添付できます。
> - メタデータは、実行時に既存のレコードに関連付けられます。

メタデータを設定する

ログレコードを`MetadataMap`に関連付けるには、PowerShellコマンド`Set-LogHighLevelOperationMetadata`を実行します。 `Set-LogHighLevelOperationMetadata`は次のパラメーターを受け取ります。

- **Id**: 高レベル操作のID。
- **InputObject**: メタデータを追加する高レベル操作。これは、高レベル操作オブジェクトまたはオブジェクトのリストがPowerShellコマンドに渡される`Id`パラメーターの代替です。
- **Name**: 追加するメタデータのプロパティ名。指定された高レベル操作に対して、プロパティは一意である必要があります。プロパティには、次の文字を含めることはできません ()\/;:#.*?=<>|'"。
- **Value**: プロパティの値。
- **Map**: プロパティの(名前、値)ペアの辞書。これは、`-Name`および`-Value`パラメーターを使用してメタデータを設定する代替手段です。

たとえば、Id 40を持つすべての高レベルログレコードにメタデータを添付するには、次のPowerShellコマンドを実行します。

```
Get-LogHighLevelOperation – Id 40 | Set-LogHighLevelOperationMetadata -Name A -Value B
```

ユーザー`abc@example.com`を持つ上位レベルのレコードにメタデータを添付するには、次のPowerShellコマンドを実行します。

```
Get-LogHighLevelOperation – User `abc@example.com` | Set-LogHighLevelOperationMetadata -Name C -Value D
```

メタデータを使用して取得する

関連付けられたメタデータを使用してログレコードを取得するには、次のPowerShellコマンドを実行します。

- キーと値で検索:

  ```
  Get-LogHighLevelOperation -Metadata "Key:Value"
  ```

- 値で任意のキーを検索:

  ```
  Get-LogHighLevelOperation -Metadata "*:Value"
  ```

- キーと任意の値で検索:

  ```
  Get-LogHighLevelOperation -Metadata "Key:*"
  ```

メタデータを削除

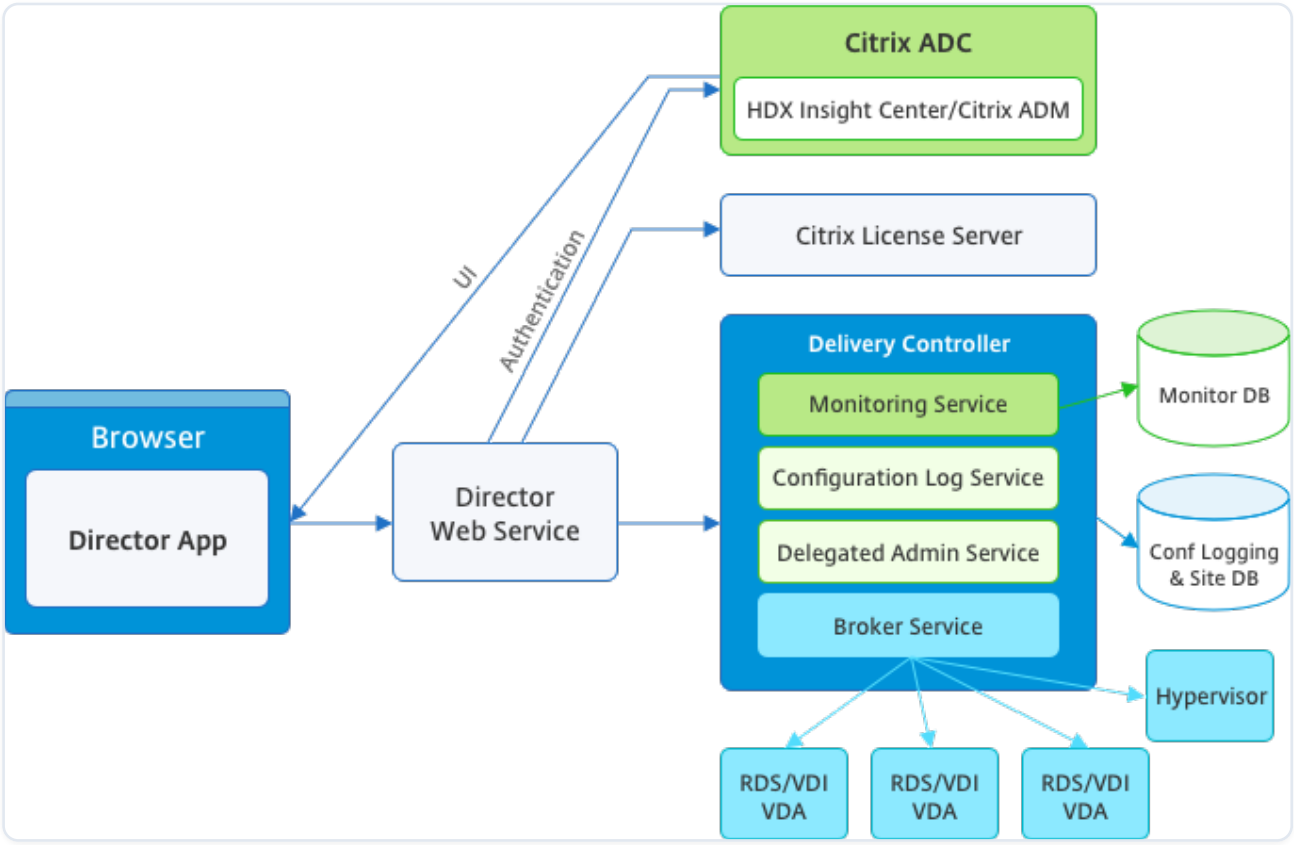
関連付けられたメタデータを削除するには、PowerShellコマンド`Remove-LogHighLevelOperationMetadata`を実行します。`Remove-LogHighLevelOperationMetadata`は次のパラメーターを受け取ります:

- **Id**: 高レベル操作のID。
- **InputObject**: メタデータを追加する上位レベルの操作。これは、`Id``パラメーターの代替であり、上位レベルの操作オブジェクトまたはオブジェクトのリストがPowerShell コマンドに渡されます。
- **Name**: 削除するメタデータのプロパティ名。指定されたオブジェクトのすべてのメタデータを削除するには、$nullに設定します。
- **Map**: プロパティの(名前、値)ペアの辞書。これは、ハッシュテーブル (@{"name1" = "val1"; "name2" = "val2"} で作成) または文字列辞書 (new-object

"System.Collections.Generic.Dictionary" で作成) のいずれかです。マップ内のキーと名前が一致するプロパティは削除されます。

ディレクター

ディレクターは、Citrix Virtual Apps and Desktops 用の監視およびトラブルシューティングコンソールです。



ディレクターは以下にアクセスできます:

- Analytics、Performance Manager、およびNetwork Inspectorと統合された統合コンソールを使用して、Broker Agentからのリアルタイムデータにアクセスします。Citrix ADMは、Citrix Virtual Apps™またはDesktops環境におけるネットワークに起因するボトルネックを特定するために、以下の分析を提供します。
  - 健全性と容量保証のためのパフォーマンス管理
  - 履歴傾向とネットワーク分析
- Monitorデータベースに保存されている履歴データにアクセスして、Configuration Loggingデータベースにアクセスします。
- Citrix ADMを使用してCitrix GatewayからのICA®データにアクセスします。

- Citrix Virtual AppsまたはDesktopsの仮想アプリケーション、デスクトップ、およびユーザーのエンドユーザーエクスペリエンスを可視化します。
- 効果的なトラブルシューティングのために、ネットワークデータとアプリケーションデータおよびリアルタイムメトリックを関連付けます。
- Citrix Virtual Desktop 7 Director監視ツールと統合します。

ディレクターは、Citrix Virtual Apps または Desktops Site のリアルタイムおよび履歴の健全性監視を提供するトラブルシューティングダッシュボードを使用します。この機能により、リアルタイムで障害を確認でき、エンドユーザーが何を経験しているかをよりよく把握できます。

Director機能とDelivery Controller (DC)、VDA、およびその他の依存コンポーネントとの互換性については、「機能互換性マトリックス」を参照してください。

> **注:**

> MeltdownおよびSpectreの投機的実行サイドチャネル脆弱性が開示されたことを受け、Citrixは関連する緩和パッチをインストールすることを推奨します。これらのパッチはSQL Serverのパフォーマンスに影響を与える可能性があります。詳細については、Microsoftサポート記事「Protect SQL Server from attacks on Spectre and Meltdown side-channel vulnerabilities」を参照してください。Citrixは、実稼働環境にパッチを展開する前に、規模をテストし、ワークロードを計画することを推奨します。

> Director は、デフォルトで Delivery Controller 上の Web サイトとしてインストールされます。前提条件およびその他の詳細については、このリリースの システム要件 ドキュメントを参照してください。Director のインストールと構成に関する具体的な情報については、Director のインストールと構成 を参照してください。

Director へのログオン

Director Webサイトはhttpsまたは`http://<Server FQDN>/Director`にあります。

マルチサイト展開でいずれかのサイトがダウンしている場合、ダウンしているサイトへの接続を試行している間、ログオンに少し時間がかかります。

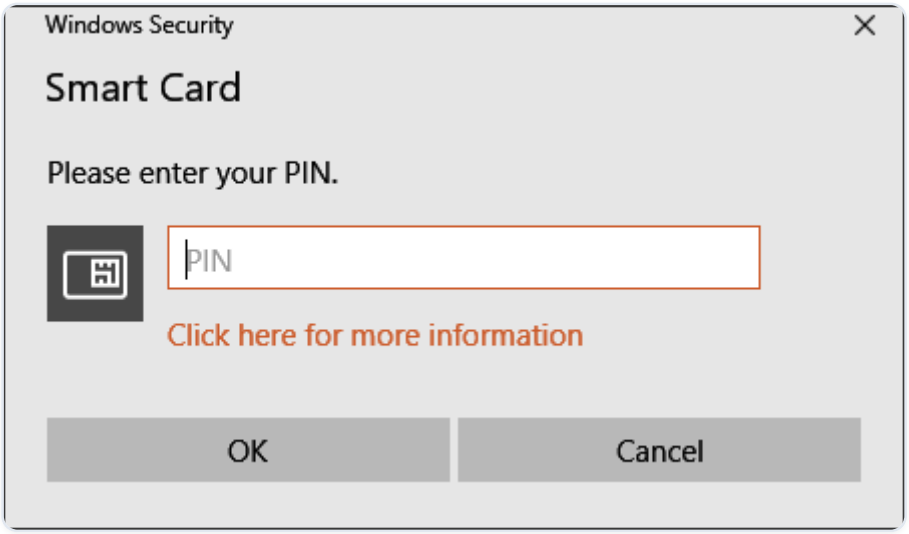
PIV スマートカード認証での Director の使用

Directorは、Personal Identity Verification（PIV）ベースのスマートカード認証によるログオンをサポートするようになりました。この機能は、アクセス制御にスマートカードベースの認証を使用する組織や政府機関にとって役立ちます。 スマートカード認証には、Directorサーバーおよび Active Directoryでの特定の構成が必要です。構成手順の詳細については、「PIVスマートカード認証の構成」を参照してください。

> **注:**
>
> スマートカード認証は、同じ Active Directory ドメインのユーザーのみがサポートされます。

必要な構成を実行した後、スマートカードを使用して Director にログオンできます。

1. スマートカードをスマートカードリーダーに挿入します。
2. ブラウザーを開き、Director の URL `https://<directorfqdn>/Director` にアクセスします。
3. 表示されたリストから有効なユーザー証明書を選択します。
4. スマートカードトークンを入力します。



5. 認証後、Directorログオンページで追加の資格情報を入力することなく、Directorにアクセスできます。

統合 Windows 認証での Director の使用

統合Windows認証 (IWA) を使用すると、ドメイン参加ユーザーはDirectorログオンページで資格情報を再入力することなく、Directorに直接アクセスできます。統合Windows認証とDirectorを使用するための前提条件は次のとおりです。

- DirectorをホストするIIS Webサイトで統合Windows認証を有効にします。Directorをインストールすると、匿名認証とフォーム認証が有効になります。統合Windows認証とDirectorをサポートするには、匿名認証を無効にし、Windows認証を有効にします。ドメイン外のユーザーの認証のために、フォーム認証は有効のままにしておく必要があります。

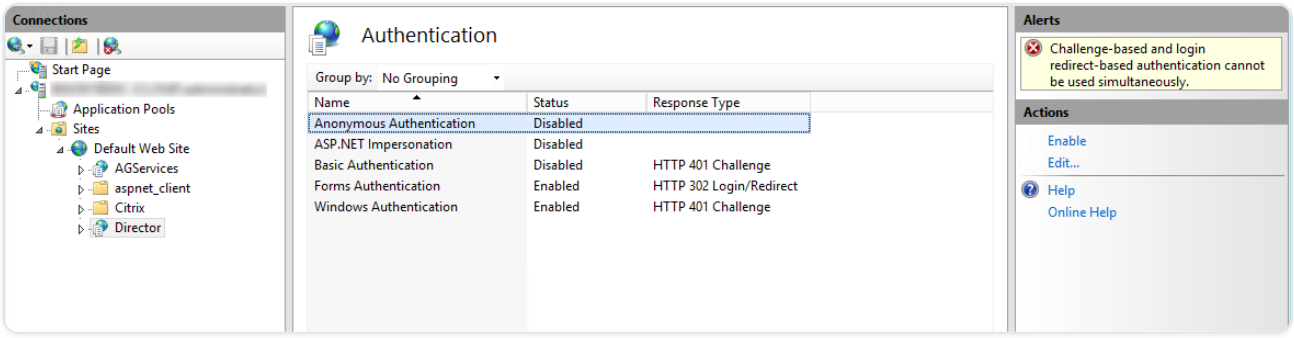
  a. IISマネージャーを起動します。

  b. **サイト** > **既定のWebサイト** > **Director** に移動します。

  c. **認証** を選択します。

  d. **匿名認証** を右クリックし、**無効** を選択します。

  e. **Windows認証** を右クリックし、**有効** を選択します。



- Directorマシンに対してActive Directoryの委任権限を構成します。構成が必要となるのは、DirectorとDelivery Controller™が別々のマシンにインストールされている場合のみです。

  a. Active Directoryマシンで、Active Directory管理コンソールを開きます。

  b. Active Directory管理コンソールで、**ドメイン名** \> **コンピューター** に移動します。Directorマシンを選択します。

  c. 右クリックして **プロパティ** を選択します。

  d. プロパティで、**委任** タブを選択します。

  e. 「**このコンピューターを任意のサービスへの委任に信頼する (Kerberos のみ)**」オプションを選択します。

- Director へのアクセスに使用するブラウザーは、統合 Windows 認証をサポートしている必要があります。Firefox および Chrome では、追加の構成手順が必要になる場合があります。詳しくは、ブラウザーのドキュメントを参照してください。

- Monitoring Service は、Microsoft .NET Framework 4.5.1 以降の、Director のシステム要件に記載されているサポート対象バージョンを実行している必要があります。詳しくは、「システム要件」を参照してください。

ユーザーが Director からログオフするか、セッションがタイムアウトすると、ログオンページが表示されます。ログオンページから、ユーザーは認証の種類を「**自動ログオン**」または「**ユーザー資格情報**」に設定できます。

インターフェイスビュー

Directorは、特定の管理者向けに調整されたさまざまなインターフェイスビューを提供します。製品の権限によって、表示される内容と利用可能なコマンドが決まります。

たとえば、ヘルプデスク管理者は、ヘルプデスクタスクに合わせたインターフェイスを表示します。Director を使用すると、ヘルプデスク管理者は、問題を報告しているユーザーを検索し、そのユーザーに関連するアクティビティを表示できます。たとえば、ユーザーのアプリケーションとプロセスのステータスなどです。応答しないアプリケーションやプロセスを終了する、ユーザーのマシンで操作をシャドウする、マシンを再起動する、ユーザープロファイルをリセットするなどのアクションを実行することで、問題を迅速に解決できます。

対照的に、完全な管理者はサイト全体を表示および管理し、複数のユーザーとマシンに対してコマンドを実行できます。ダッシュボードには、セッションのステータス、ユーザーログオン、サイトインフラストラクチャなど、展開の主要な側面に関する概要が表示されます。情報は毎分更新されます。問題が発生した場合、発生した障害の数と種類に関する詳細が自動的に表示されます。

Director におけるさまざまな役割とその権限について詳しくは、「委任管理とDirector」を参照してください。

Pendoによる使用状況データ収集

Director のインストール後、Director Service は Pendo を使用して使用状況データの収集を開始します。トレンドページの利用状況や OData API 呼び出し分析に関する統計が収集されます。分析データの収集は、Citrix プライバシーポリシーに準拠しています。Director をインストールすると、データ収集はデフォルトで有効になります。

Pendo のデータ収集をオプトアウトするには、Director がインストールされているマシンでレジストリキーを編集します。レジストリキーが存在しない場合は、作成して目的の値に設定します。レジストリキーの値を変更した後、Director インスタンスを更新してください。

注意: レジストリエディターを誤って使用すると、オペレーティングシステムの再インストールが必要になるような深刻な問題が発生する可能性があります。Citrix は、レジストリエディターの誤った使用によって生じる問題が解決されることを保証できません。レジストリエディターの使用は自己責任で行ってください。Citrix は、変更を行う前に Windows レジストリをバックアップすることをお勧めします。

場所：HKEY_LOCAL_MACHINE\Software\Citrix\Director

名前：DisableGoogleAnalytics

> **注:**
>
> 以前は、Director Service は Google Analytics を使用してデータを収集していました。現在、同じレジストリキーが Pendo で使用されています。

値: 0 = 有効 (デフォルト), 1 = 無効

次の PowerShell コマンドレットを使用して、Pendo によるデータ収集を無効にできます。

```
New-Item HKLM:\SOFTWARE\Citrix -Name Director



New-ItemProperty HKLM:\SOFTWARE\Citrix\Director -Name
DisableGoogleAnalytics -PropertyType DWORD -Value 1
```

新機能ガイド

Director には、Pendo を使用した製品内ガイドがあり、Director の現在のバージョンでリリースされた新機能についての洞察を提供します。概要と適切な製品内メッセージを組み合わせることで、製品の新機能を理解するのに役立ちます。

この機能をオプトアウトするには、Director がインストールされているマシンで、以下に説明するようにレジストリキーを編集します。レジストリキーが存在しない場合は、作成して目的の値に設定します。レジストリキーの値を変更した後、Director インスタンスを更新します。

> **注意:**

> レジストリエディターを誤って使用すると、オペレーティングシステムの再インストールが必要になるような深刻な問題が発生する可能性があります。Citrix は、レジストリエディターの誤った使用によって発生した問題が解決できることを保証できません。レジストリエディターの使用は、お客様ご自身の責任で行ってください。Citrix は、Windows レジストリを変更する前にバックアップすることをお勧めします。

> 場所: HKEY_LOCAL_MACHINE\Software\Citrix\Director

名前: DisableGuidedHelp

値: 0 = 有効 (デフォルト), 1 = 無効

次の PowerShell コマンドレットを使用して、製品内ガイドを無効にできます。

```
New-Item HKLM:\SOFTWARE\Citrix -Name Director



New-ItemProperty HKLM:\SOFTWARE\Citrix\Director -Name DisableGuidedHelp
-PropertyType DWORD -Value 1
```

参照記事

- Citrix Director からの MTTR の削減
- Citrix Director - PowerShell を使用したアラートと通知の管理および構成
- Citrix Virtual Apps and Desktops 開発者向けドキュメント

関連製品の新機能

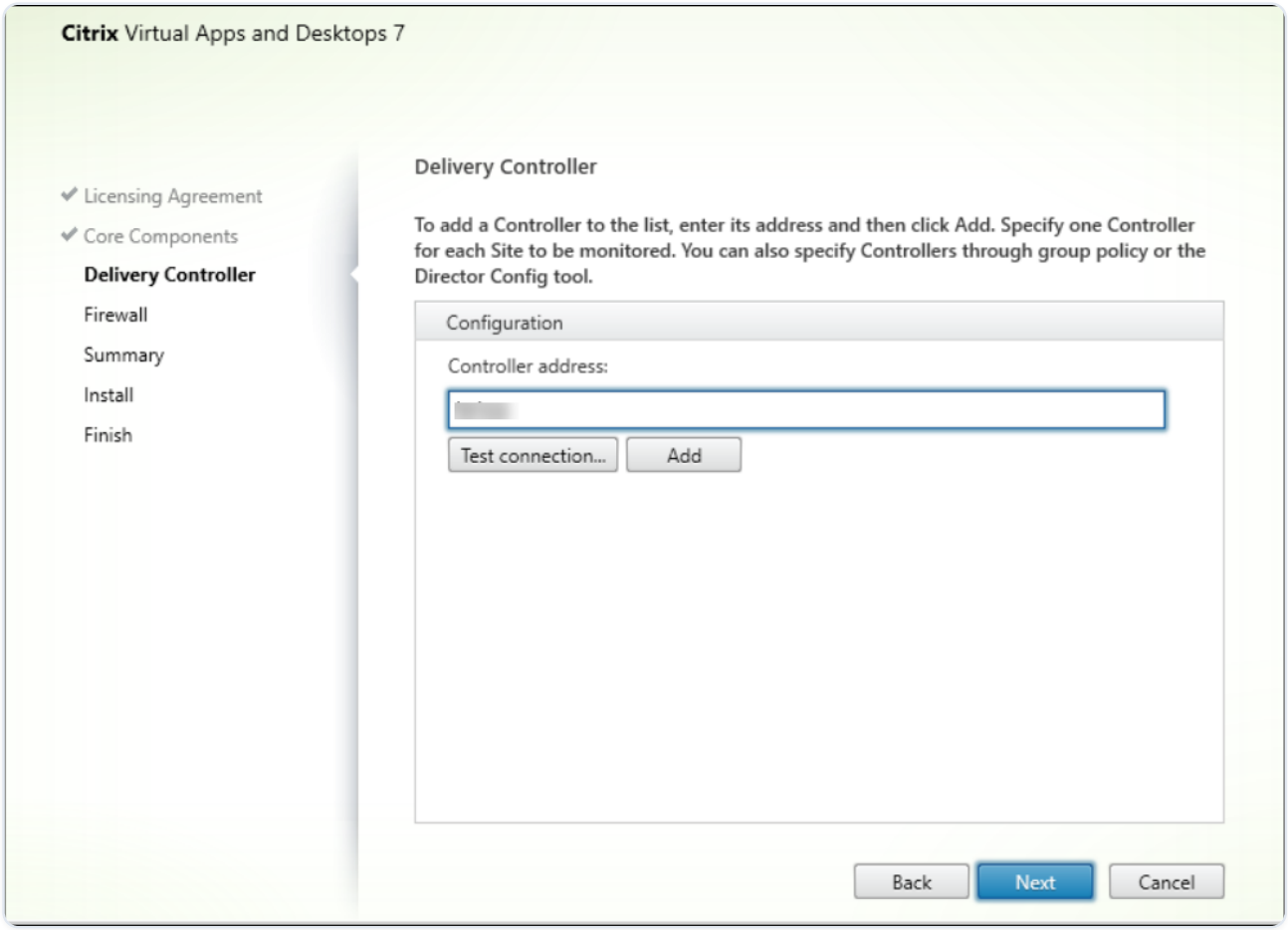
- シトリックス DaaS
- StoreFront
- セキュアプライベートアクセス
- シトリックス エンタープライズ ブラウザ
- Citrix Workspace (シトリックス ワークスペース)
- プロビジョニング

インストールと構成

Director のインストール

Citrix Virtual Apps and Desktops の製品版 ISO インストーラーを使用して Director をインストールします。これにより、前提条件の確認、不足しているコンポーネントのインストール、Director Webサイトのセットアップ、および基本的な構成が実行されます。前提条件およびその他の詳細については、このリリースのシステム要件ドキュメントを参照してください。このリリースのDirectorは、Virtual Apps 6.5以前の展開、またはVirtual Desktops 7以前の展開とは互換性がありません。 ISOインストーラーによって提供されるデフォルト構成は、一般的な展開に対応します。インストール時にDirectorが含まれていなかった場合は、ISOインストーラーを使用してDirectorを追加します。追加のコンポーネントを追加するには、ISOインストーラーを再実行し、インストールするコンポーネントを選択します。ISOインストーラーの使用方法については、インストールドキュメントのコアコンポーネントのインストールを参照してください。Citrixでは、.MSIファイルではなく、製品版ISOインストーラーのみを使用してインストールすることをお勧めします。

DirectorがControllerにインストールされている場合、サーバーアドレスとしてlocalhostが自動的に構成され、Directorはデフォルトでローカルの Controllerと通信します。Controllerから離れた専用サーバーにDirectorをインストールする場合は、ControllerのFQDNまたはIPアドレスの入力を求められます。



注:

「**追加**」をクリックして、監視するControllerを追加します。

Directorは、デフォルトで指定されたControllerと通信します。監視するサイトごとにControllerアドレスを1つだけ指定してください。指定したControllerが失敗した場合、Directorは同じサイト内の他のすべてのControllerを自動的に検出し、それらのControllerにフォールバックします。

注:

DirectorはController間で負荷分散を行いません。

ブラウザーとWebサーバー間の通信を保護するために、Citrix®はDirectorをホストするIIS WebサイトでTLSを実装することをお勧めします。手順については、Microsoft IISのドキュメントを参照してください。TLSを有効にするためにDirectorの構成は必要ありません。

Director の展開および構成

Directorが複数のサイトを含む環境で使用される場合、Controller、Director、およびその他のコアコンポーネントがインストールされているすべてのサーバーでシステムクロックを同期してください。そうしないと、Directorでサイトが正しく表示されない可能性があります。

重要:

ネットワーク経由でプレーンテキストで送信されるユーザー名とパスワードのセキュリティを保護するため、Director接続にはHTTPではなくHTTPSのみを使用してください。特定のツールは、HTTP（暗号化されていない）ネットワークパケット内のプレーンテキストのユーザー名とパスワードを読み取ることができ、ユーザーにとって潜在的なセキュリティリスクを生じさせる可能性があります。

権限の構成

Directorにログオンするには、Directorの権限を持つ管理者はActive Directoryドメインユーザーであり、以下の権限を持っている必要があります。

- 検索対象となるすべてのActive Directoryフォレストに対する読み取り権限（高度な構成を参照）。
- 構成済みの委任管理者ロール（委任管理とDirectorを参照）。
- ユーザーをシャドウするには、管理者はWindowsリモートアシスタンス用のMicrosoftグループポリシーを使用して構成する必要があります。さらに：
  - VDAをインストールする際は、すべてのユーザーデバイスでWindowsリモートアシスタンス機能が有効になっていることを確認してください（デフォルトで選択されています）。
  - サーバーにDirectorをインストールする際は、Windowsリモートアシスタンスがインストールされていることを確認してください（デフォルトで選択されています）。ただし、サーバーではデフォルトで無効になっています。Directorがエンドユーザーにアシスタンスを提供するために、この機能を有効にする必要はありません。Citrixは、サーバーのセキュリティを向上させるために、この機能を無効のままにしておくことを推奨します。
  - 管理者がWindowsリモートアシスタンスを開始できるようにするには、リモートアシスタンス用の適切なMicrosoftグループポリシー設定を使用して、必要な権限を付与します。詳細については、CTX127388: How to Enable Remote Assistance for Desktop Directorを参照してください。

DirectorとのCitrix uberAgent®統合

Citrix uberAgentは、Citrix Virtual Apps and Desktops™のインストールにデフォルトで含まれるようになり、強化された監視機能とCitrix Directorとのシームレスな統合を提供します。管理者は、Virtual Delivery Agentのセットアップ中に**オプションソフトウェア**画面で選択を解除することで、インストールから除外できます。

Citrix Virtual Apps and Desktopsのインストールの一部としてuberAgentをインストールする方法の詳細については、uberAgentドキュメントを参照してください。

主な機能：

ローカルアプリケーション使用状況の監視: Citrix uberAgentを使用すると、仮想デスクトップセッション内で起動されたアプリケーション（ローカルアプリケーションとも呼ばれます）の使用状況を監視でき、Director統合を通じて、データはDirectorダッシュボードで直接利用できます（Platinumライセンスで利用可能）。

DirectorとのCitrix uberAgent統合の構成

Citrix uberAgentをインストールした後、DirectorとuberAgentを完全に統合して使用するには、Citrix Web Studio™で以下のポリシーを構成します。

- **uberAgentデータ収集ポリシーを有効にする**: 有効にすると、uberAgentはアプリケーションの使用状況とパフォーマンス、システムヘルス、ネットワークメトリック、およびセキュリティ分析に関するインサイトを提供します。このポリシーはデフォルトで無効になっています。
- **uberAgentデータポリシーでDirectorを強化する**: このポリシーは、DirectorとuberAgentの統合を有効にします。これにより、DirectorはuberAgentが提供するデータを処理して、ローカルアプリケーションの使用状況の監視を含む監視機能を強化できます。このポリシーはデフォルトで有効になっています。

設定が完了すると、データはCitrix Directorのアプリケーション使用状況の監視セクションで利用可能になります。

> **注:**
>
> ローカルアプリケーションの使用状況に関するuberAgentデータがDirectorに集計され、表示されるまで、少なくとも1日かかります。

高度な構成

Director は、ユーザー、Delivery Controller (DC)、VDA、および Director が異なるフォレストに配置されているフォレスト構成にまたがるマルチフォレスト環境をサポートできます。これには、フォレスト間の信頼関係と構成設定の適切なセットアップが必要です。

マルチフォレスト環境での推奨構成

推奨される構成では、ドメイン全体の認証を使用して、フォレスト間で送信および受信フォレスト信頼関係を作成する必要があります。

マルチフォレストサイト構成(/en-us/citrix-virtual-apps-desktops/2503/media/multiforest-config.png)

Director からの信頼関係により、異なるフォレストにあるユーザーセッション、VDA、および Delivery Controller の問題をトラブルシューティングできます。

Director が複数のフォレストをサポートするために必要な高度な構成は、インターネットインフォメーションサービス (IIS) マネージャーで定義された設定によって制御されます。

> **重要:**

> IIS で設定を変更すると、Director サービスは自動的に再起動し、ユーザーをログオフします。

> IIS を使用して高度な設定を構成するには:

1. インターネットインフォメーションサービス (IIS) マネージャーコンソールを開きます。
2. デフォルトの Web サイトの下にある Director Web サイトに移動します。
3. をダブルクリックします。
4. 設定をダブルクリックして編集します。
5. をクリックして新しい設定を追加します。

Director は Active Directory を使用してユーザーを検索し、ユーザーとマシンの詳細情報を参照します。デフォルトでは、Director は次のドメインまたはフォレストを検索します。

- 管理者アカウントがメンバーである。
- Director Web サーバーがメンバーである (異なる場合)。

Director は、Active Directory グローバルカタログを使用してフォレストレベルで検索を実行しようとします。フォレストレベルで検索する権限がない場合は、ドメインのみが検索されます。

別のActive Directoryドメインまたはフォレストからデータを検索または参照するには、検索するドメインまたはフォレストを明示的に設定する必要があります。IISマネージャーで、Director Web サイトに次のアプリケーション設定を構成します。

```
Connector.ActiveDirectory.Domains = (user),(server)
```

値属性 user と server は、それぞれ Director ユーザー (管理者) と Director サーバーのドメインを表します。

追加のドメインまたはフォレストからの検索を有効にするには、この例に示すように、ドメインの名前をリストに追加します。

```
Connector.ActiveDirectory.Domains = (user),(server),\&lt;domain1\>,
\&lt;domain2\>
```

リスト内の各ドメインについて、Director はフォレストレベルで検索を実行しようとします。フォレストレベルで検索する権限がない場合は、ドメインのみが検索されます。

ドメインローカルグループの構成

ほとんどのCitrix Service Provider（CSP）は、インフラストラクチャフォレストにVDA、DC、およびDirectorで構成される同様の環境設定を持っています。ユーザーまたはユーザーグループのレコードはカスタマーフォレストに属します。インフラストラクチャフォレストからカスタマーフォレストへの一方向の送信信頼が存在します。

CSP管理者は通常、インフラストラクチャフォレストにドメインローカルグループを作成し、カスタマーフォレストのユーザーまたはユーザーグループをこのドメインローカルグループに追加します。

推奨されるマルチフォレストサイト構成(/en-us/citrix-virtual-apps-desktops/2503/media/domainlocalgroup-config.png)

Directorはこのようなマルチフォレスト設定をサポートし、ドメインローカルグループを使用して構成されたユーザーのセッションを監視できます。

1. IISマネージャーで、Director Webサイトに次のアプリケーション設定を追加します。

   ```
   Connector.ActiveDirectory.DomainLocalGroupSearch= true



   DomainLocalGroupSearchDomains= \&lt;domain1\>,\&lt;domain2\>
   ```

   \<domain1\>\<domain2\> は、ドメインローカルグループが存在するフォレストの名前です。
2. Web Studioでドメインローカルグループをデリバリーグループに割り当てます。
3. 変更を有効にするには、IISを再起動し、Directorに再度ログオンします。これで、Directorはこれらのユーザーのセッションを監視および表示できます。

Directorにサイトを追加する

Directorがすでにインストールされている場合は、複数のサイトで動作するように構成します。構成するには、各DirectorサーバーのIISマネージャーコンソールを使用して、アプリケーション設定のサーバーアドレスのリストを更新します。

各サイトのControllerのアドレスを次の設定に追加します。

```
Service.AutoDiscoveryAddresses = SiteAController,SiteBController
```

SiteAControllerとSiteBControllerは、2つの異なるサイトのDelivery Controllerのアドレスです。

アクティビティマネージャーで実行中のアプリケーションの可視性を無効にする

デフォルトでは、Directorのアクティビティマネージャーには、ユーザーセッションのすべての実行中アプリケーションのリストが表示されます。この情報は、Directorのアクティビティマネージャー機能にアクセスできるすべての管理者が表示できます。委任された管理者ロールの場合、これにはフル管理者、デリバリーグループ管理者、およびヘルプデスク管理者が含まれます。

ユーザーのプライバシーと実行中のアプリケーションを保護するために、**アプリケーション**タブを無効にして、実行中のアプリケーションを一覧表示しないようにすることができます。

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

1. VDAで、HKEY_LOCAL_MACHINE\\Software\\Citrix\\Director\\TaskManagerDataDisplayed のレジストリキーを変更します。デフォルトでは、このキーは1に設定されています。値を0に変更すると、VDAから情報が収集されなくなり、アクティビティマネージャーに表示されなくなります。
2. Directorがインストールされているサーバーで、実行中のアプリケーションの表示を制御する設定を変更します。デフォルトでは、値は「true」であり、アプリケーションタブで実行中のアプリケーションの表示が許可されます。値を「false」に変更すると、表示が無効になります。このオプションは、Directorのアクティビティマネージャーのみに影響し、VDAには影響しません。 次の設定の値を変更します。 UI.TaskManager.EnableApplications = false

> **重要：**
>
> 実行中のアプリケーションの表示を無効にするには、アクティビティマネージャーにデータが表示されないように、両方の変更を行います。

PIVスマートカード認証を構成する

この記事では、スマートカード認証機能を有効にするためにDirectorサーバーとActive Directoryで必要な構成を一覧表示します。

> **注:**
>
> スマートカード認証は、同じActive Directoryドメインのユーザーのみがサポートされます。

Directorサーバーの構成

Directorサーバーで以下の構成手順を実行します。

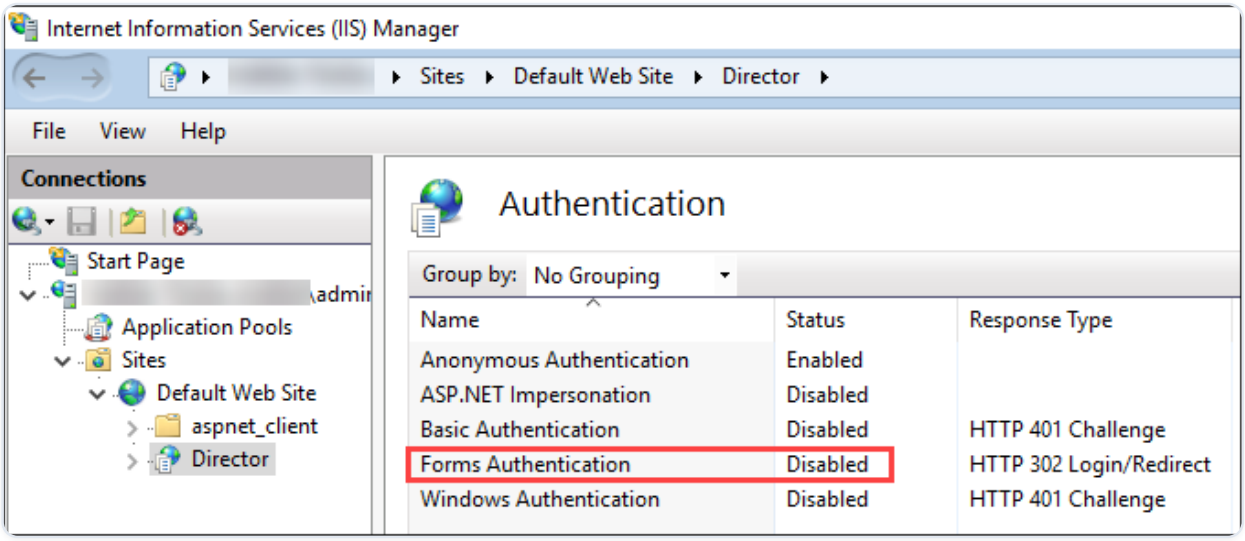
1. クライアント証明書マッピング認証をインストールして有効にします。Microsoftドキュメントの「クライアント証明書マッピング認証」にある**Active Directoryを使用したクライアント証明書マッピング認証**の手順に従ってください。
2. Directorサイトでフォーム認証を無効にします。

   IISマネージャーを起動します。

   サイト \> **既定のWebサイト** \> **Director** に移動します。

   認証 を選択します。

   フォーム認証を右クリックし、**無効にする**を選択します。



3. クライアント証明書認証のために、DirectorのURLをより安全なhttpsプロトコル (HTTPではなく) に構成します。

   a. IISマネージャーを起動します。

b. **サイト** \> **既定のWebサイト** \> **Director** に移動します。

c. 「**SSL Settings**」を選択します。

d. 「**SSL を要求**」と「**クライアント証明書**」 \> 「**要求**」を選択します。

SSL設定(/en-us/citrix-virtual-apps-desktops/2503/media/dir-smartcard-config2.png)

4. web.config を更新します。web.config ファイル（c:\\inetpub\\wwwroot\\Director にあります）をテキストエディターで開きます。

`<system.webServer>` 親要素の下に、次のスニペットを最初の子要素として追加します。

```
&lt;defaultDocument>

   &lt;files>

       &lt;add value="LogOn.aspx"/>

   &lt;/files>

&lt;/defaultDocument>
```

Active Directory の構成

デフォルトでは、Director アプリケーションは「**アプリケーションプール**」ID プロパティで実行されます。スマートカード認証には委任が必要であり、Director アプリケーションIDはサービスホスト上でTrusted Computing Base (TCB) 権限を持っている必要があります。

Citrixでは、アプリケーションプールID用に個別のサービスアカウントを作成することをお勧めします。Microsoft MSDNの記事「Protocol Transition with Constrained Delegation Technical Supplement」の指示に従って、サービスアカウントを作成し、TCB権限を割り当ててください。

新しく作成したサービスアカウントを Director アプリケーションプールに割り当てます。次の図は、サンプルサービスアカウント「Domain Pool」のプロパティダイアログを示しています。

サンプルサービスアカウント(/en-us/citrix-virtual-apps-desktops/2503/media/dir-smartcard-config3.png)

このアカウントに対して、次のサービスを構成します:

- Delivery Controller™：ホストとHTTP
- Director：ホスト、HTTP
- アクティブディレクトリ: GC, LDAP

構成するには、,

1. 「ユーザーアカウントのプロパティ」ダイアログで、「**追加**」をクリックします。
2. **サービスの追加**ダイアログで、ユーザーまたはコンピューターをクリックします。
3. Delivery Controllerのホスト名を選択します。
4. **利用可能なサービス**の一覧から、HOSTとHTTPの**サービスの種類**を選択します。

サービスを構成する(/en-us/citrix-virtual-apps-desktops/2503/media/dir-smartcard-config4.png)

同様に、**Director**および**Active Directory**ホストのサービスの種類を追加します。

サービスプリンシパル名レコードを作成する

各Directorサーバーと、Directorサーバーのプールへのアクセスに使用される負荷分散された仮想IP（VIP）ごとにサービスアカウントを作成する必要があります。新しく作成されたサービスアカウントへの委任を構成するには、サービスプリンシパル名（SPN）レコードを作成する必要があります。

- DirectorサーバーのSPNレコードを作成するには、次のコマンドを使用します。

```
  setspn -a http/<directorServer>.<domain_fqdn>
<domain>\<DirectorAppPoolServiceAcct>
```

- 負荷分散されたVIPのSPNレコードを作成するには、次のコマンドを使用します。

```
  setspn -S http/<DirectorFQDN> <domain>\<DirectorAppPoolServiceAcct>
```

- 作成されたSPNを表示またはテストするには、次のコマンドを使用します。

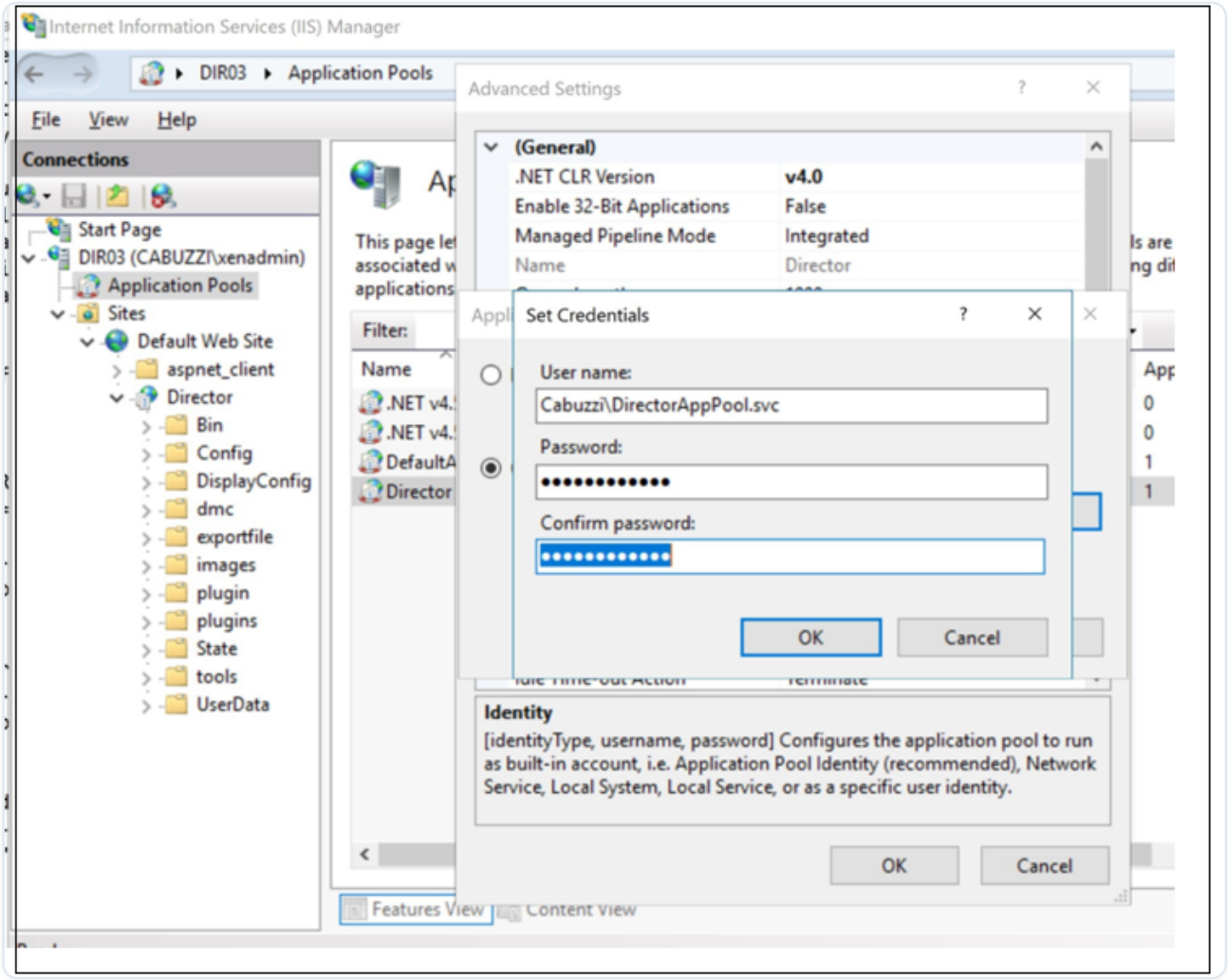
```
 setspn –l <DirectorAppPoolServiceAcct>
```

スマートカード(/en-us/citrix-virtual-apps-desktops/2503/media/dir-smart-card-auth-2.png)

- 左ペインでDirector仮想ディレクトリを選択し、 をダブルクリックします。 ウィンドウで をクリックし、**AllowKerberosConstrainedDelegation** が1に設定されていることを確認します。

ケルベロス(/en-us/citrix-virtual-apps-desktops/2503/media/dir-smart-card-auth-3.png)

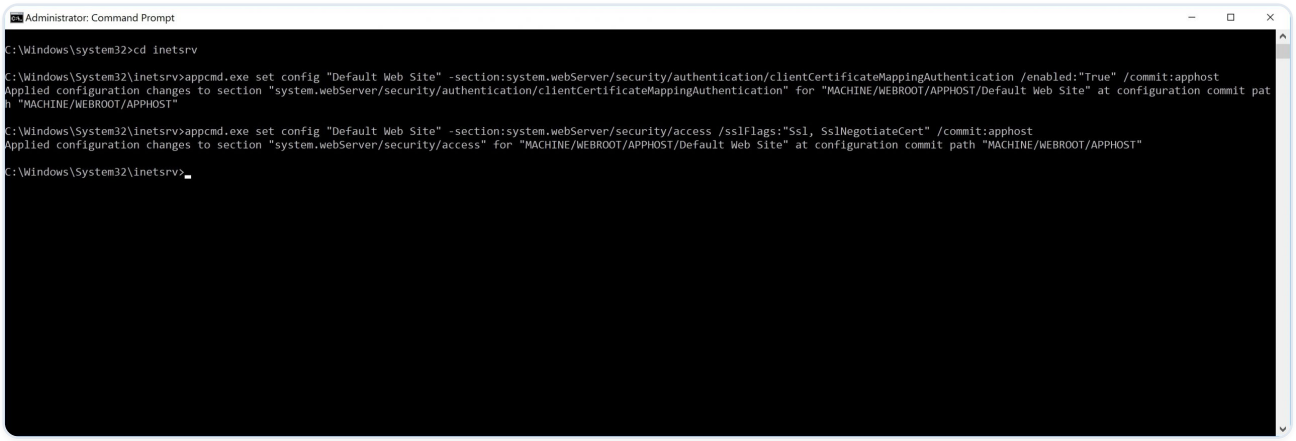
- 左側のペインで**アプリケーションプール**を選択し、Directorアプリケーションプールを右クリックして**詳細設定**を選択します。
- **ID**を選択し、省略記号（「...」）をクリックしてサービスアカウントのドメイン\ログオンとパスワードの資格情報を入力します。IISコンソールを閉じます。



- 管理者として実行したコマンドプロンプトから、ディレクトリをC:\Windows\System32\inetsrvに変更し、以下のコマンドを入力します。

```
   appcmd.exe set config “Default Web Site” -section:system.webServer/
security/authentication/clientCertificateMappingAuthentication /
enabled:”True” /commit:apphost
```

```
appcmd.exe set config “Default Web Site” -section:system.webServer/
security/access /sslFlags:”Ssl, SslNegotiateCert” /commit:apphost
```



Firefoxブラウザの設定

Firefoxブラウザを使用するには、OpenSC 0.17.0で入手できるPIVドライバーをインストールします。インストールと構成の手順については、Installing OpenSC PKCS#11 Module in Firefox, Step by Stepを参照してください。 Directorでのスマートカード認証機能の使用方法については、Directorの記事のUse Director with PIV based smart card authenticationセクションを参照してください。

ネットワーク分析を構成する

> **注:**
>
> この機能の利用可否は、組織のライセンスと管理者権限によって異なります。

DirectorはCitrix ADMと統合され、ネットワーク分析とパフォーマンス管理を提供します。

- ネットワーク分析は、Citrix ADMのHDX™ Insightレポートを使用して、ネットワークのアプリケーションおよびデスクトップのコンテキストビューを提供します。この機能により、Directorは展開環境におけるICAトラフィックの高度な分析を提供します。
- パフォーマンス管理は、履歴保持と傾向レポートを提供します。リアルタイム評価と比較してデータの履歴保持を行うことで、容量や健全性の傾向を含むトレンドレポートを作成できます。

Directorでこの機能を有効にすると、HDX InsightレポートはDirectorに追加情報を提供します。

- トレンドページのネットワークタブには、展開環境全体のアプリケーション、デスクトップ、およびユーザーに対する遅延と帯域幅の影響が表示されます。
- ユーザー詳細ページには、特定のユーザーセッションに固有の遅延と帯域幅の情報が表示されます。

制限事項:

- トレンドビューでは、バージョン7より前のVDAのHDX接続ログオンデータは収集されません。それより前のVDAの場合、グラフデータは0として表示されます。

ネットワーク分析を有効にするには、DirectorにCitrix ADMをインストールして構成する必要があります。Directorには、Citrix ADMバージョン11.1ビルド49.16以降が必要です。MASはXenServer上で動作する仮想アプライアンスです。ネットワーク分析を使用すると、Directorは展開環境に関連する情報を通信および収集します。

詳細については、Citrix ADMドキュメントを参照してください。

> **注:**
>
> Citrix NetScaler Insight Centerは、15 May 2018をもってメンテナンス終了日を迎えました。Citrix製品マトリックス を参照してください。ネットワーク分析のためにDirectorをCitrix ADMと統合してください。NetScaler Insight CenterをCitrix ADMに移行するには、「NetScaler Insight CenterからCitrix ADMへの移行」を参照してください。

1. Director がインストールされているサーバーで、C:\inetpub\wwwroot\Director\tools にある DirectorConfig コマンドラインツールを見つけ、コマンドプロンプトからパラメーター /configgetscaler を指定して実行します。
2. プロンプトが表示されたら、Citrix ADM マシン名（FQDN または IP アドレス）、ユーザー名、パスワード、HTTPS 接続タイプ（HTTP よりも推奨）、および Citrix ADM 統合を選択します。
3. 変更を確認するには、ログオフしてから再度ログオンします。

> **注:**
>
> セキュリティ上の理由から、HDX Insight のみにアクセスするのに十分な権限を持つ、Director との ADM 統合用のカスタムロールを作成することをお勧めします。

詳細については、「アクセスポリシーの構成」を参照してください。

委任管理とDirector

委任管理では、管理者、役割、スコープという3つの概念を使用します。権限は、管理者の役割と、その役割のスコープに基づいています。たとえば、管理者は、スコープが1つのサイトのエンドユーザーに対する責任を含むヘルプデスク管理者ロールを割り当てられる場合があります。

委任管理者の作成については、メインの委任管理の記事を参照してください。

管理権限によって、管理者に表示されるDirectorインターフェイスと、実行できるタスクが決まります。権限によって以下が決定されます。

- 管理者がアクセスできるビュー（総称してビューと呼ばれます）。
- 管理者が表示および操作できるデスクトップ、マシン、セッション。
- 管理者が実行できるコマンド（ユーザーセッションのシャドウイングやメンテナンスモードの有効化など）。

組み込みの役割と権限は、管理者がDirectorをどのように使用するかを決定します。

管理者ロール	DIRECTORでの権限
フル管理者	すべてのビューへのフルアクセスと、ユーザーセッションのシャドウイング、メンテナンスモードの有効化、トレンドデータのエクスポートを含むすべてのコマンドを実行できます。
デリバリーグループ管理者	すべてのビューへのフルアクセスと、ユーザーセッションのシャドウイング、電源管理とセッション管理、メンテナンスモードの有効化、トレンドデータのエクスポートを含むすべてのコマンドを実行できます。
読み取り専用管理者	指定されたスコープ内のすべてのビューにアクセスし、すべてのオブジェクトとグローバル情報を表示できます。HDX™チャネルからレポートをダウンロードし、トレンドビューの「エクスポート」オプションを使用してトレンドデータをエクスポートできます。その他の

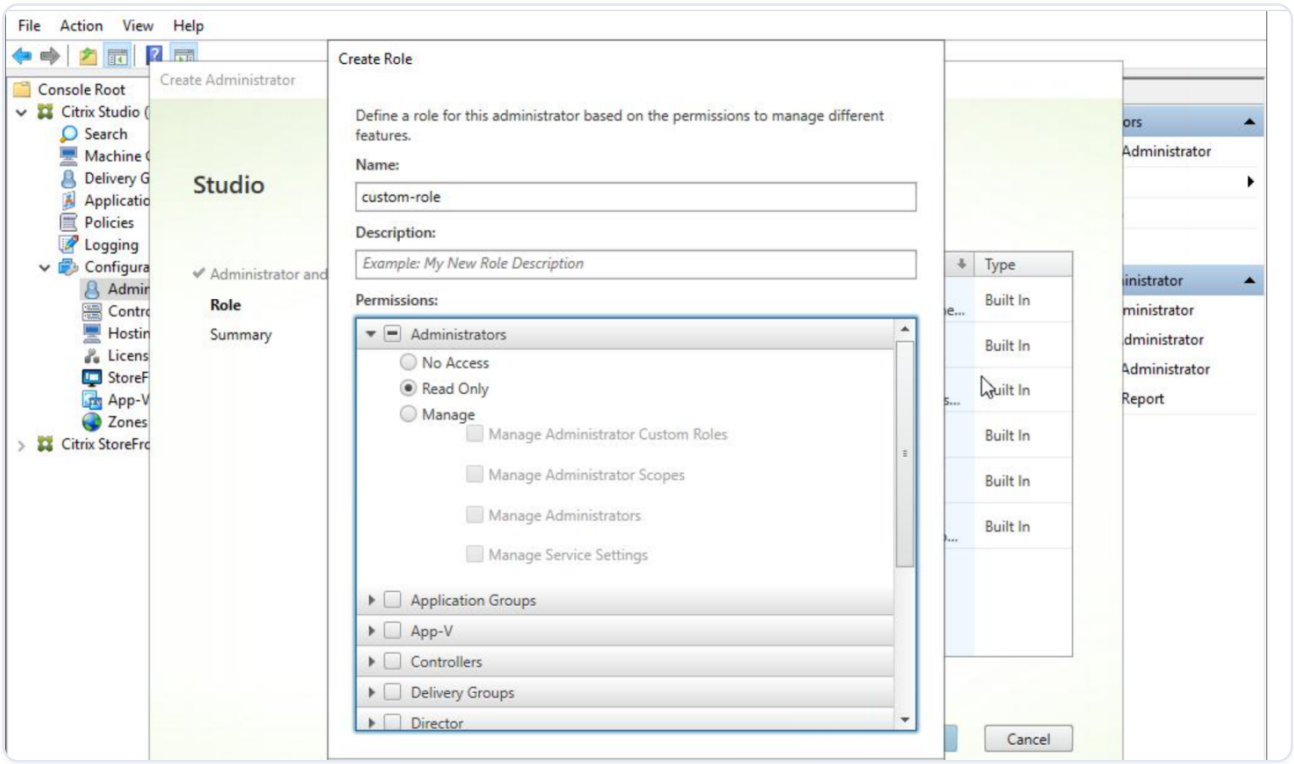
管理者ロール	DIRECTORでの権限
	コマンドを実行したり、ビュー内の何かを変更したりすることはできません。
ヘルプデスク管理者	ヘルプデスクビューとユーザー詳細ビューにのみアクセスでき、管理者が管理を委任されているオブジェクトのみを表示できます。ユーザーのセッションをシャドウし、そのユーザーのコマンドを実行できます。メンテナンスモード操作を実行できます。シングルセッションOSマシンに対して電源制御オプションを使用できます。ダッシュボード、トレンド、アラート、またはフィルタービューにはアクセスできません。マルチセッションOSマシンに対して電源制御オプションを使用することはできません。
マシンカタログ管理者	マシンの詳細ページ（マシンベースの検索）にのみアクセスできます。
ホスト管理者	アクセス不可。この管理者はDirectorではサポートされておらず、データを表示できません。

Director管理者用のカスタム役割を構成する

Studioでは、組織の要件により厳密に一致させ、権限をより柔軟に委任するために、Director固有のカスタム役割を構成することもできます。たとえば、組み込みのヘルプデスク管理者役割を制限して、この管理者がセッションをログオフできないようにすることができます。

Director権限を持つカスタム役割を作成する場合、その役割に他の一般的な権限も付与する必要があります。

- DirectorにログオンするためのDelivery Controller™権限 - 管理者ノードでの読み取り専用アクセス以上
- Directorでそれらのデリバリーグループに関連するデータを表示するためのデリバリーグループへの権限 - 読み取り専用アクセス以上

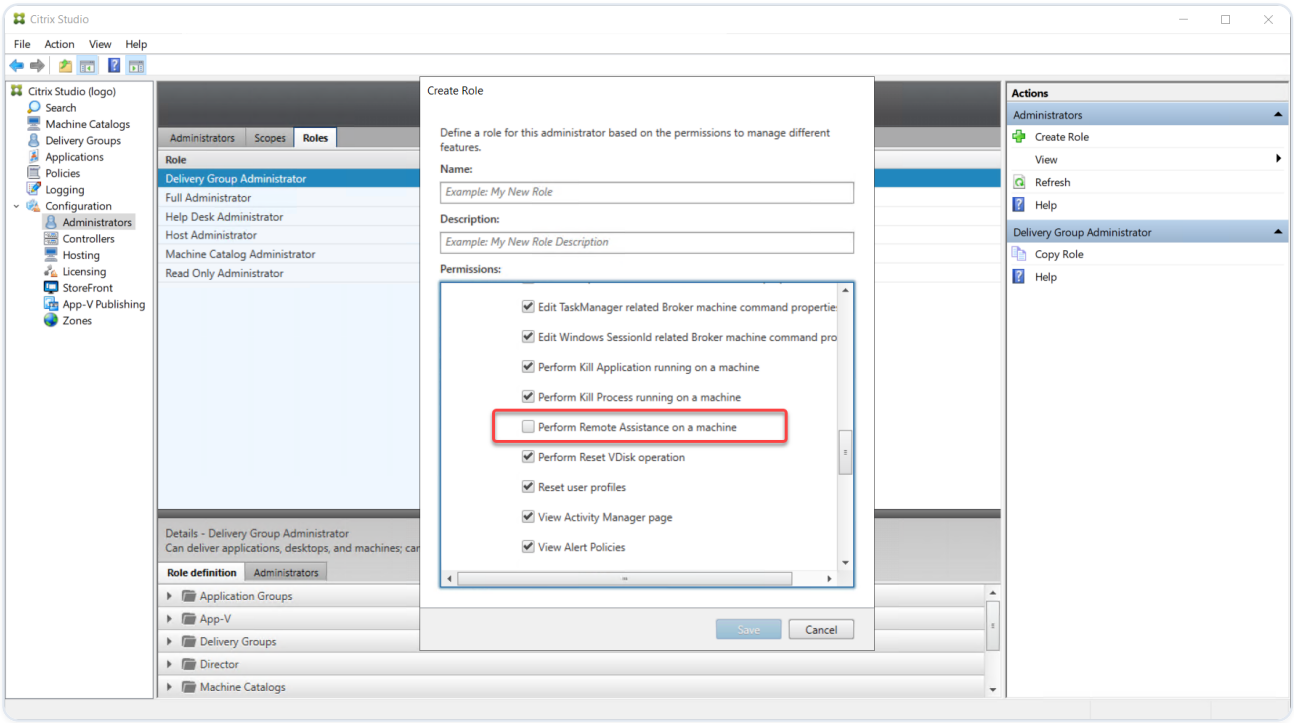


あるいは、既存のロールをコピーして、異なるビューに対する追加の権限を含めることで、カスタムロールを作成できます。たとえば、ヘルプデスクロールをコピーして、ダッシュボードまたはフィルターページを表示する権限を含めることができます。

カスタムロールのDirector権限を選択します。これには以下が含まれます。

- マシン上で実行中のアプリケーションの強制終了を実行する
- マシン上で実行中のプロセスの強制終了を実行する
- マシン上でリモートアシスタンスを実行する
- ユーザープロファイルをリセットする
- クライアント詳細ページを表示
- ダッシュボードページの表示
- フィルターページを表示する
- マシン詳細ページを表示
- トレンドページの表示
- ユーザー詳細ページを表示

この例では、シャドウイング（マシン上でリモートアシスタンスを実行する）が無効になっています。



権限は、UIで適用可能になるために他の権限に依存する場合があります。たとえば、**マシン上で実行中のアプリケーションの強制終了を実行する**権限を選択すると、ロールに権限があるパネルでのみ**アプリケーションの終了**機能が有効になります。次のパネル権限を選択できます。

- フィルターページを表示する
- ユーザー詳細ページを表示
- マシン詳細ページを表示
- クライアント詳細ページを表示

さらに、他のコンポーネントの権限リストから、デリバリーグループの以下の権限を検討してください。

- デリバリーグループのメンバーシップを使用して、マシンのメンテナンスモードを有効/無効にする。
- デリバリーグループのメンバーシップを使用して、Windowsデスクトップマシンで電源操作を実行する。
- デリバリーグループのメンバーシップを使用して、マシンでセッション管理を実行する。

Directorの展開を保護する

この記事では、Directorの展開と構成時にシステムセキュリティに影響を与える可能性のある領域について説明します。

Directorの通信

実稼働環境では、Directorとサーバー間でやり取りされるデータを保護するためにHTTPSプロトコルを使用します。HTTPSは、強力なデータ暗号化を提供するためにトランスポート層セキュリティ（TLS）プロトコルを使用します。

注:

- Citrix®は、イントラネットネットワーク内でのDirectorコンソールへのアクセスを制限することを強くお勧めします。
- Citrixは、実稼働環境でDirectorへのセキュリティで保護されていない接続を有効にしないことを強くお勧めします。
- TLS 1.2以降を使用してください。レガシーTLSまたはSSLは使用しないでください。

ユーザーのWebブラウザーとDirector間の通信を保護するには、「Web StudioおよびDirectorでTLSを有効にする」を参照してください。

DirectorとCitrix Virtual Apps and Desktopsサーバー間の通信（監視およびレポート用）を保護するには、「オンプレミスMonitor OData APIアクセスを保護する」を参照してください。

DirectorとCitrix ADC間の通信（Citrix Insight用）を保護するには、「ネットワーク分析を構成する」ときに、接続の種類としてHTTPSを選択します。

マイクロソフト インターネット インフォメーション サービス (IIS) の構成

制限されたIIS構成でDirectorを構成できます。

アプリケーションプールのリサイクル制限

Directorは、**Director**という名前のアプリケーションプールを使用します。アプリケーションプールで次のアプリケーションプールのリサイクル制限を設定できます。

- 仮想メモリ制限: 4,294,967,295
- プライベートメモリ制限: StoreFront™サーバーの物理メモリのサイズ
- 要求制限: 4,000,000,000

ファイル名拡張子

インストール中、Directorは要求フィルタリングを構成して、以下の拡張子のみを許可します。

- .

- .aspx
- .css。
- .eot。
- .html ファイル
- .ico。
- .js
- .png。
- .svc。
- .svg。
- ． gif
- .json ファイル
- .woff
- .woff2
- ． ttf

HTTP動詞

インストール中に、Directorは以下の動詞のみを許可するように要求フィルタリングを構成します。

- GET
- POST
- HEAD

IIS機能

Directorは以下のIISコンポーネントを必要としません。

- ISAPI拡張機能
- CGIプログラム
- FastCGIプログラム

これらのコンポーネントは削除できます。

.NET信頼レベル

Directorでは、**.NET信頼レベル**を**完全信頼**に設定する必要があります。.NET信頼レベルを他の値に設定しないでください。

ユーザー権限の構成

Directorがインストールされると、そのアプリケーションプールには次のものが付与されます。

- 「**サービスとしてログオン**」ログオン権限
- 「**プロセスのメモリクォータの調整**」、「**セキュリティ監査の生成**」、および「**プロセスレベルトークンの置き換え**」特権

言及されている権限と特権は、アプリケーションプールが作成される際の通常のインストール動作です。

これらのユーザー権限を変更する必要はありません。これらの特権は Director では使用されず、自動的に無効になります。

Director のセキュリティ分離

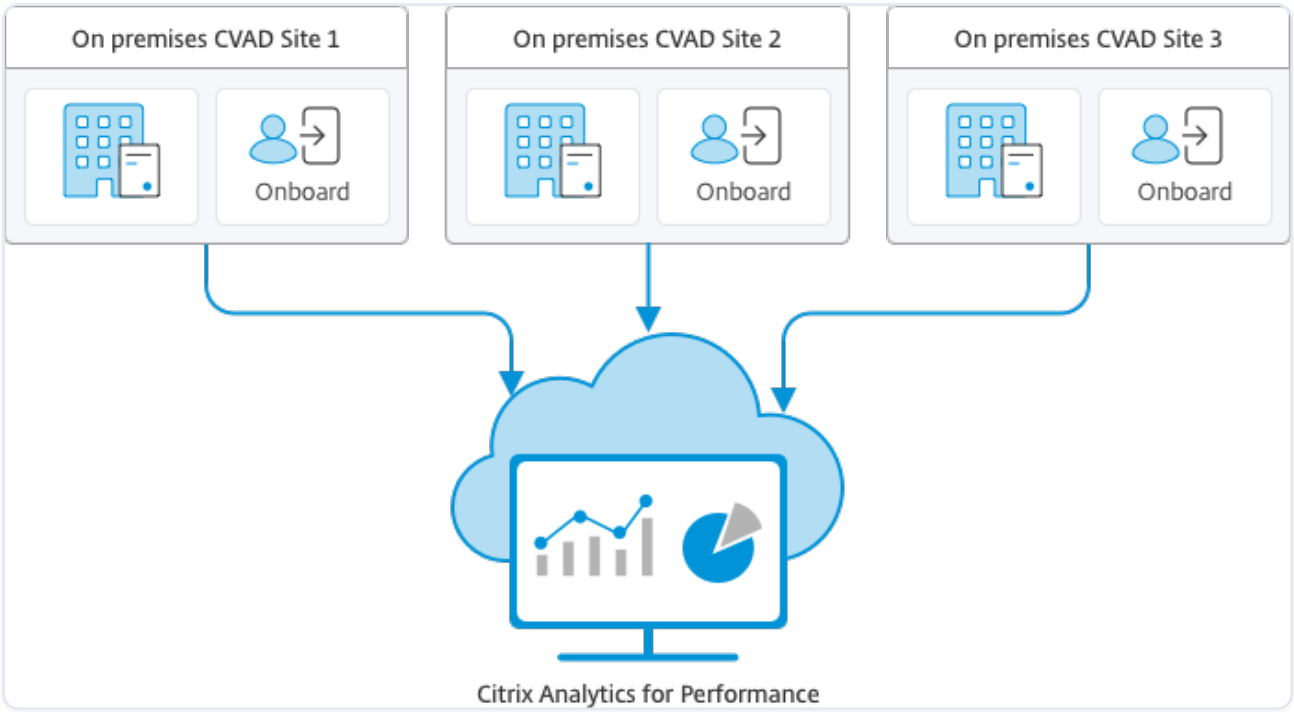
Director と同じ Web ドメイン（ドメイン名とポート）に任意の Web アプリケーションを展開できます。ただし、それらの Web アプリケーションのセキュリティリスクは、Director 展開のセキュリティを低下させる可能性があります。より高度なセキュリティ分離が必要な場合は、Citrix では Director を別の Web ドメインに展開することをお勧めします。

Citrix Analytics for Performance™ を使用したオンプレミスサイトの構成

Citrix Analytics for Performance (Performance Analytics) は、Citrix Analytics Cloud Service の包括的なパフォーマンス監視ソリューションです。Performance Analytics は、パフォーマンスメトリックに基づいて構築された高度なインサイトと分析を提供します。Performance Analytics を使用すると、組織内の1つ以上のCitrix Virtual Apps and Desktops™サイトの使用状況とパフォーマンスメトリックを監視および表示できます。

Performance Analytics の詳細については、Performance Analytics の記事を参照してください。

サイトからCitrix Cloud™上のCitrix Analytics for Performanceにパフォーマンスデータを送信して、その高度なパフォーマンス分析機能を活用できます。Performance Analytics を表示および使用するには、まず **Director** の **Analytics** タブから、オンプレミスサイトを Citrix Analytics for Performance で構成する必要があります。



Performance Analytics は安全な方法でデータにアクセスし、Citrix Cloud からオンプレミス環境にデータが転送されることはありません。

前提条件

Director から Citrix Analytics for Performance を構成するために、新しいコンポーネントをインストールする必要はありません。次の要件が満たされていることを確認してください。

- Delivery Controller と Director はバージョン 1912 CU2 以降である必要があります。詳細については、機能互換性マトリックスを参照してください。

注:

- Delivery Controller が Microsoft .NET Framework バージョン 4.8 より前のバージョンを実行している場合、Director からオンプレミスサイトを Citrix Analytics for Performance で構成できないことがあります。回避策として、Delivery Controller の .NET Framework をバージョン 4.8 にアップグレードしてください。LCM-9255。
- Director から Citrix Virtual Apps and Desktops バージョン 2012 を実行しているオンプレミスサイトを Citrix Analytics for Performance で構成すると、数時間後または Delivery Controller で Citrix Monitor Service を再起動した後に構成が失敗する場合があります。この場合、Analytics タブには「未接続」ステータスが表示されます。回避策として、Delivery Controller のレジストリに Encryption フォルダーを作成します。場所: HKEY_LOCAL_MACHINE\Software\Citrix\XDservices\Monitor、フォルダー名:

> Encryption。CitrixMonitor アカウントが Encryption フォルダーに対してフルコントロールアクセス権を持っていることを確認してください。Citrix Monitor Service を再起動します。DIR-14324。

- この構成を実行するための **Analytics** タブへのアクセスは、フル管理者のみが利用できます。
- Performance Analytics がパフォーマンスメトリックにアクセスできるようにするには、すべての Delivery Controller および Director がインストールされているマシンで、アウトバウンドインターネットアクセスが利用可能である必要があります。具体的には、次の URL へのアクセス可能性を確認してください。
  - シトリックス キー登録: `https://*.citrixnetworkapi.net/`
  - シトリックス クラウド：`https://*.citrixworkspacesapi.net/`
  - シトリックス アナリティクス：`https://*.cloud.com/`
  - Microsoft Azure: `https://*.windows.net/` Delivery ControllerとDirectorマシンがイントラネット内にあり、アウトバウンドインターネットアクセスがプロキシサーバー経由である場合は、以下を確認してください。
- プロキシサーバーは、前述のURLリストを許可する必要があります。
- Directorのweb.configファイルとcitrix.monitor.exe.configファイルに以下の構成を追加します。この構成は**configuration**タグ内に必ず追加してください。

```
&lt;system.net>

    &lt;defaultProxy>

        &lt;proxy  usesystemdefault = "false"  proxyaddress = "http://
&lt;your_proxyserver_address>:80" bypassonlocal = "true"  />

    &lt;/defaultProxy>

&lt;/system.net>
```

  - Director web.config は、Director がインストールされているマシンの `C:\inetpub\wwwroot\Director\web.config` にあります。
  - citrix.monitor.exe.config は、Delivery Controller がインストールされているマシンの `C:\Program Files\Citrix\Monitor\Service\Citrix.Monitor.exe.Config` にあります。

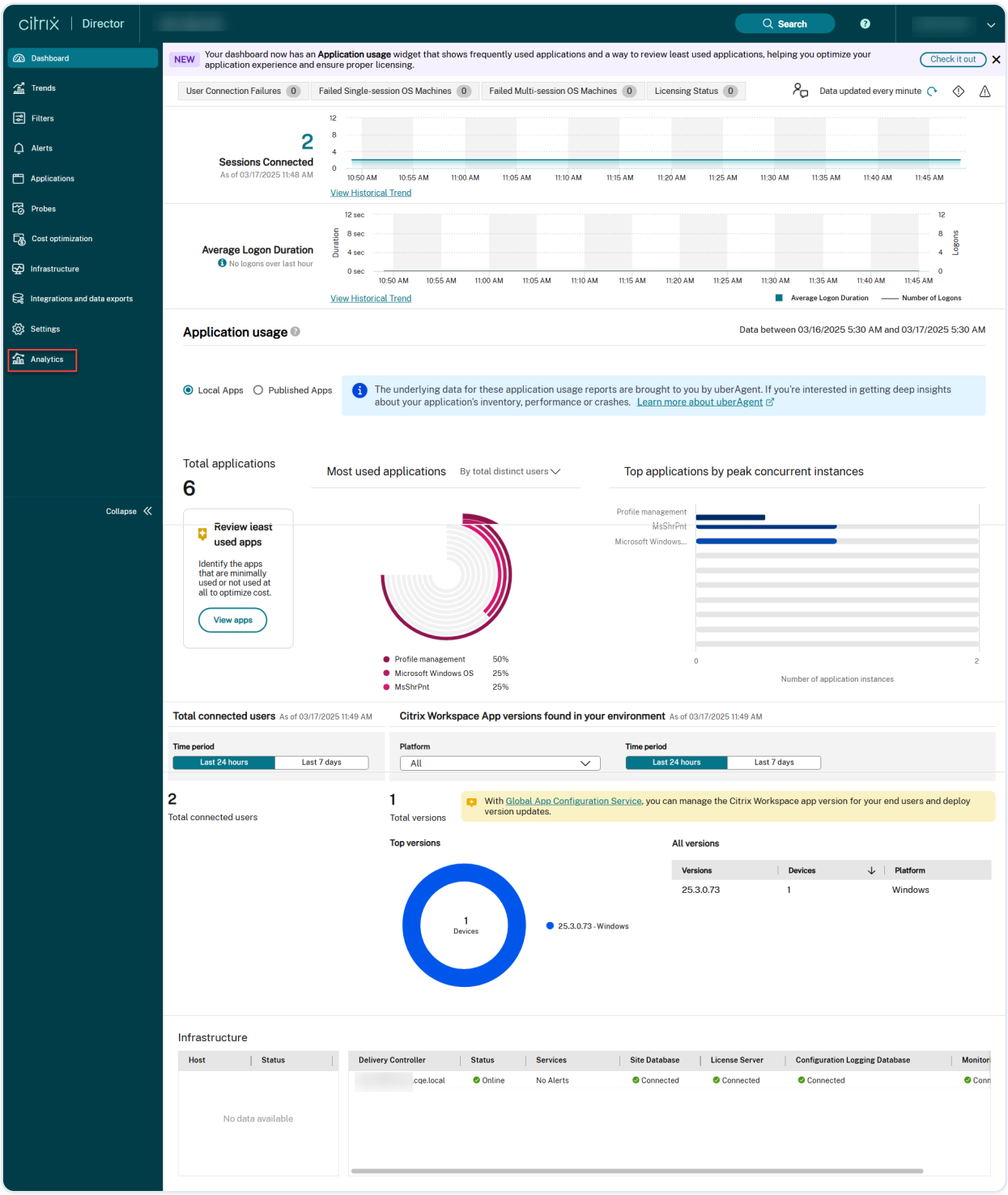
この設定は、MicrosoftによってIISで提供されています。詳細については、`https://docs.microsoft.com/ja-jp/dotnet/framework/network-programming/proxy-configuration`を参照してください。 構成ファイルの**defaultproxy**フィールドは、DirectorおよびMonitor Serviceのアウトバウンドアクセスを制御します。Performance Analyticsとの構成および通信には、**defaultproxy**フィールドを**true**に設定する必要があります。有効なポリシーによってこのフィールドがfalseに設定されている可能性があります。この場合、フィールドを手動でtrueに設定する必要があります。変更を行う前に、構成ファイルのバックアップを取ってください。変更を有効にするには、Delivery Controller™で監視サービスを再起動してください。

- Citrix Analytics for PerformanceのCitrix Cloudエンタイトルメントがアクティブであること。
- Citrix Cloudアカウントが、製品登録エクスペリエンスに対する権限を持つ管理者アカウントであること。管理者権限の詳細については、「」(/ja-jp/citrix-cloud/citrix-cloud-management/identity-access-management/add-admins.html#modify-administrator-permissions)を参照してください。

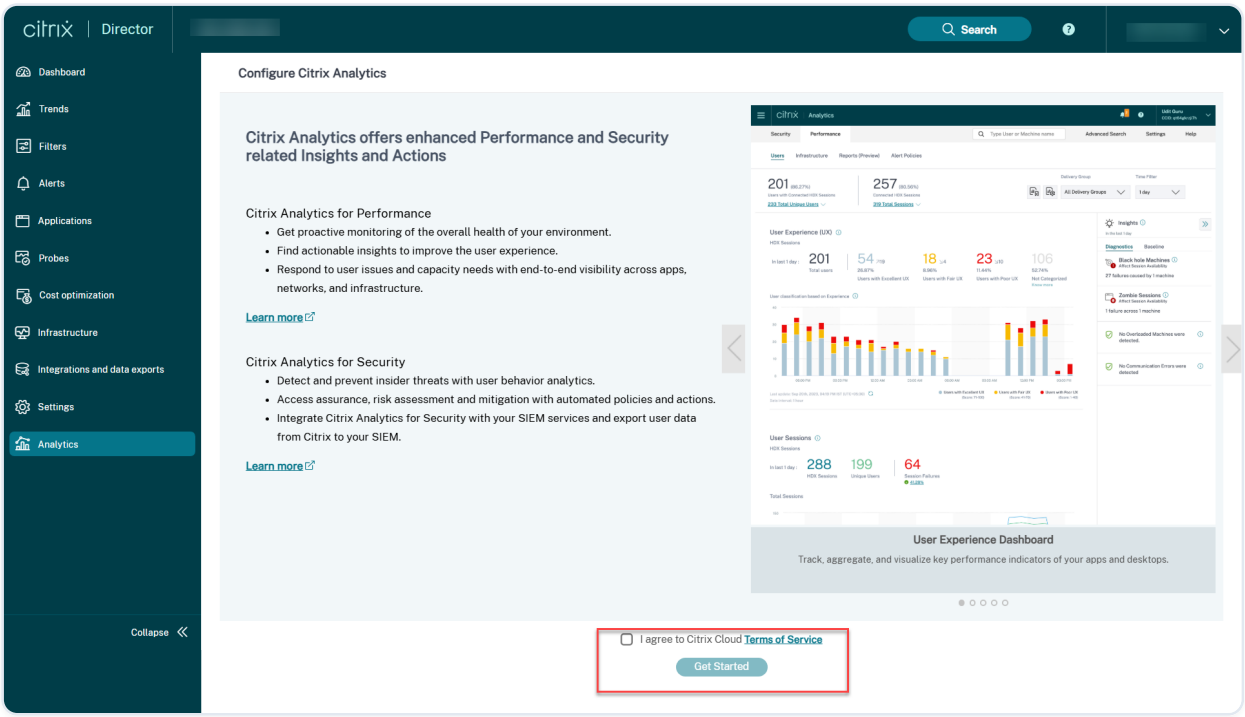
構成手順

前提条件を確認したら、次の手順を実行します。

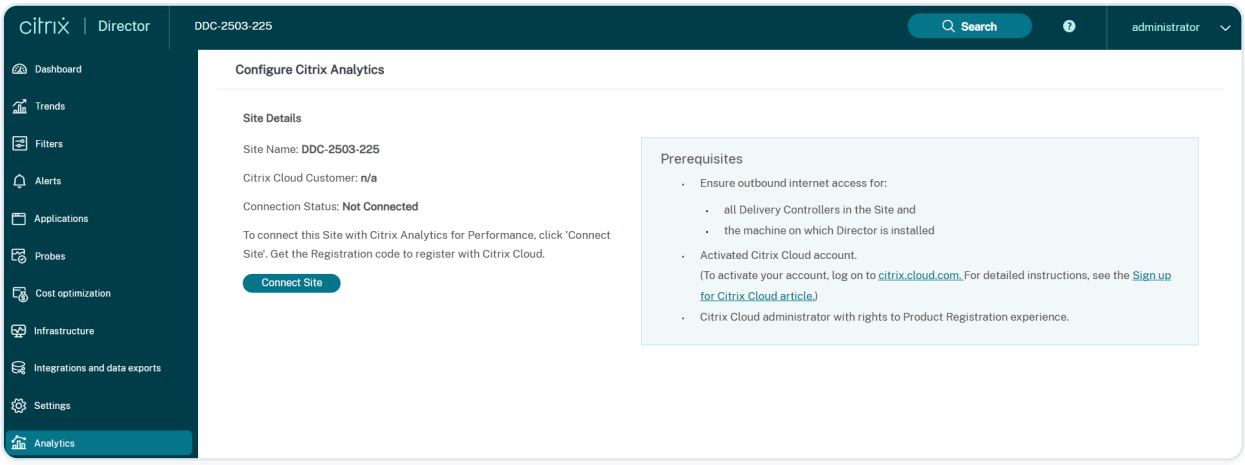
1. Director にフル管理者としてサインインし、Performance Analytics で構成するサイトを選択します。Director ダッシュボードページが表示されます。



2. **Analytics**タブをクリックします。**Citrix Analyticsの構成**ページが表示されます。

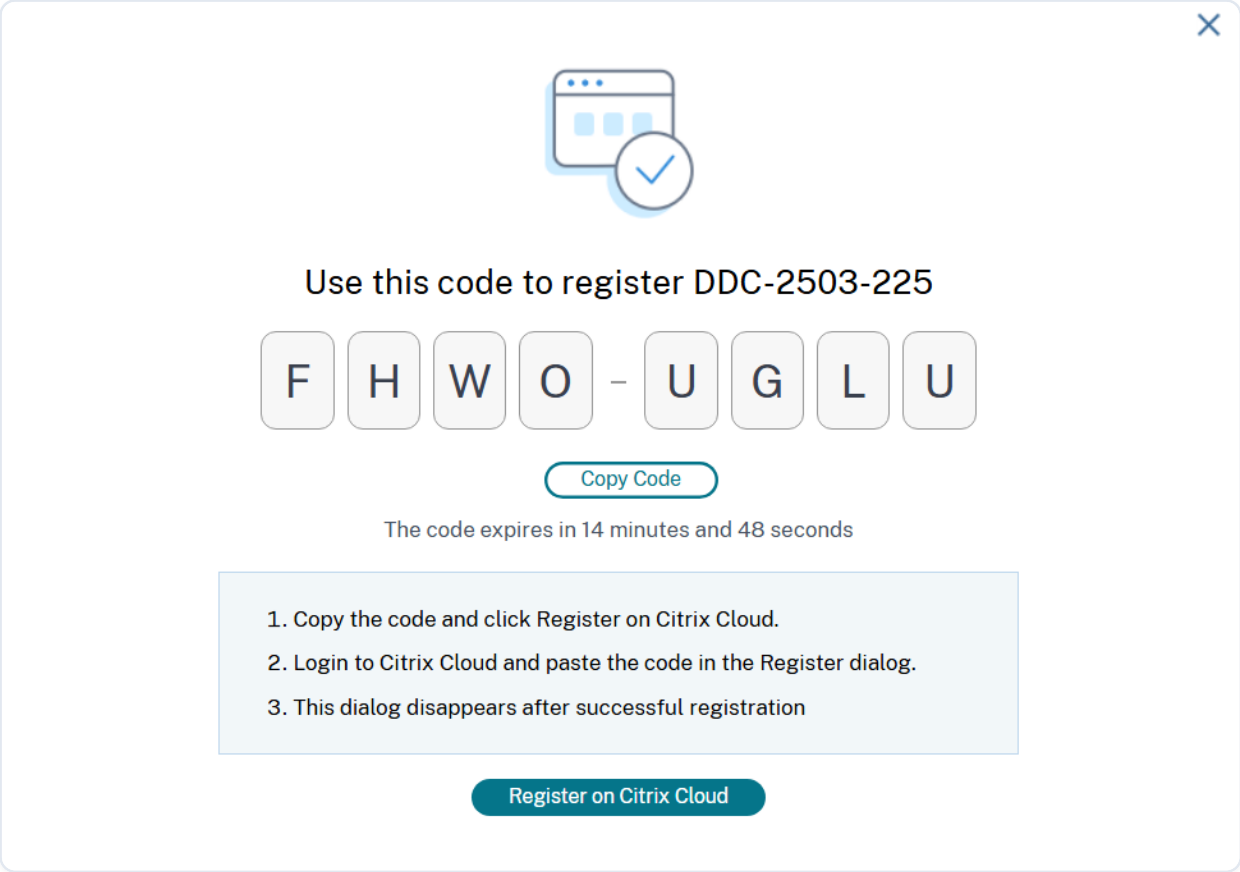


3. 手順を確認し、サービス規約を選択してから、**「開始する」をクリックします。**「サイトの詳細」**ページが表示されます。



4. 前提条件を確認し、満たされていることを確認します。サイトの詳細を確認します。
5. 構成プロセスを開始するには、**「サイトを接続」**をクリックします。

   このサイトを Citrix Cloud に登録するために使用する、一意の8桁の登録コードが生成されます。



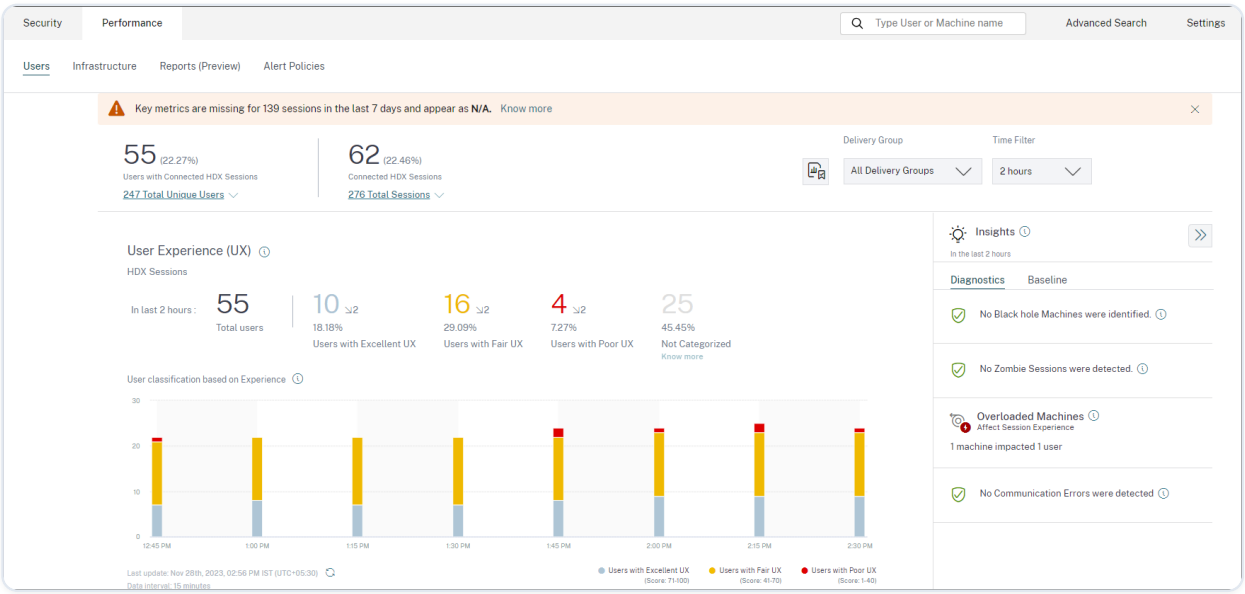
6. コードをコピーするには**「コードをコピー」**をクリックし、次に**「Citrix Cloudで登録」**をクリックします。Citrix Cloudの登録URLにリダイレクトされます。
7. Citrix Cloudの資格情報でサインインし、顧客を選択します。
8. コピーした登録コードをCitrix Cloudの製品登録ページに貼り付けます。**「続行」**をクリックして登録します。登録の詳細を確認し、**「登録」**をクリックします。

   Citrix Cloudでの登録(/en-us/citrix-virtual-apps-desktops/2503/media/dir-onboarding6.png)

   オンプレミスサイトがCitrix Cloudに登録されます。
9. **Director**から、**「Analytics」**タブの**「Analyticsに移動」**をクリックします。

   Analyticsに移動(/en-us/citrix-virtual-apps-desktops/2503/media/dir-onboarding7.png)

Performance Analyticsがブラウザーの新しいタブで開きます。



Citrix Cloudセッションの有効期限が切れている場合、Citrix.comまたはMy Citrixアカウントのログオンページにリダイレクトされることがあります。

10. 複数のサイトをPerformance Analyticsに登録するには、Directorから各サイトについて前述の設定手順を繰り返します。設定されたすべてのサイトのメトリックは、Performance Analyticsダッシュボードに表示されます。

    サイトごとに複数のDirectorインスタンスが実行されている場合は、いずれか1つのDirectorインスタンスから構成します。サイトに接続されている他のすべてのDirectorインスタンスは、構成プロセスの後の次回の更新時に更新されます。

11. サイトをCitrix Cloudから切断するには、 をクリックします。このオプションは、既存の構成を削除します。

> **注:**
>
> サイトを初めて構成する場合、サイトからのイベントが処理されるまでに時間がかかる（約1時間）ことがあり、Performance Analyticsダッシュボードにメトリックが表示されるまでに遅延が生じます。その後、イベントは定期的に更新されます。
>
> 切断後、新しいアカウントからのイベントが送信されるまで、古いアカウントからのデータ送信はしばらく継続されます。データ送信が停止してから約1時間、古いアカウントに関連する分析はPerformance Analyticsダッシュボードに表示されたままになります。

> Citrix Analyticsサービスへのエンタイトルメントの有効期限が切れると、サイトメトリックがPerformance Analyticsに送信されなくなるまでに最大1日かかります。

LTSR展開向けDirectorの独立リリース

LTSR展開向けDirectorの独立リリースは、互換性のあるLTSR環境において、Citrix®環境でのトラブルシューティングと監視を強化するための最新のDirector機能にアクセスするオプションを提供するようになりました。この機能により、2402 LTSR展開で最新のDirectorバージョンを使用できます。また、アプリケーション配信インフラストラクチャに影響を与えることなく、LTSR発表後にリリースされた機能へのアクセスも提供します。

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

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

- シトリックス バーチャル アプリケーションズ アンド デスクトップス 2407 リリース
- シトリックス バーチャル アプリケーションズ アンド デスクトップス 2411 リリース

VDAの最小バージョンでのDirectorの特定の機能について詳しくは、Directorバージョンマトリックスを参照してください。

メリット

- **新機能へのアクセス**: 2402 LTSR発表後にリリースされたDirector機能（Citrix Virtual Apps and Desktops™ 2407および2411累積リリース（CR）の機能を含む）にアクセスできます。
- **ターゲットを絞ったアップグレード**: LTSRインフラストラクチャの残りの部分に影響を与えることなく、Directorおよび監視サービスコンポーネントのみをアップグレードします。
- **LTSR互換性**: 最新のDirector機能強化の恩恵を受けながら、LTSR環境を維持します。
- **ロールバックオプション**: 必要に応じて、以前のDirectorバージョンにロールバックする柔軟性があります。

主な考慮事項

アップグレードされたDirectorコンポーネントはLTSR互換ですが、LTSRコアコンポーネントのサポート対象ではありません。ただし、LTSRインフラストラクチャの残りの部分は既存のサポートを維持します。

前提条件

1. Citrix downloadsページから`Director2411.zip`ファイルをダウンロードします。
2. インストーラーファイルを解凍すると、次のインストーラーが見つかります。
   - DesktopDirector.msi
   - Monitor_PowerShellSnapIn.msi
   - Monitor_Service_x64.msi
3. Citrix Virtual Apps and Desktops 2402 LTSRまたは2402 LTSR CU1サイトを使用していることを確認してください。

概要

Citrix Virtual Apps and Desktops 2402 LTSR CU1サイトをCurrent Releaseの最新機能でアップグレードするには、次の手順に従います。

1. **データベースのバックアップ**: アップグレードする前に、監視データベースをバックアップしてください。アップグレードプロセスではデータベースも更新されるため、この手順は非常に重要です。
2. **サイトのアップグレード**: サイトをアップグレードして、現在のリリースの新機能を取り込みます。
3. **ロールバックオプション**: アップグレードされたサイトの使用を継続しないと判断した場合、ロールバック手順を使用して以前のサイトに戻すことができます。

アップグレード手順

1. 監視データベースのバックアップを取ります。
2. Citrix downloadsページから`Director2411.zip`ファイルをダウンロードします。
3. インストーラーファイルを解凍すると、次のインストーラーが見つかります。
   - DesktopDirector.msi
   - Monitor_PowerShellSnapIn.msi
   - Monitor_Service_x64.msi
4. .msi ファイルの場所に移動します。
5. コマンドラインを使用してモニターサービスをインストールします。

```
msiexec /i Monitor_service_x64 REINSTALLMODE=amus /l*v <logfile path
and name>
```

6. 画面の指示に従い、ウィザードを完了します。
7. コマンドラインを使用して Director サービスをインストールします。

```
msiexec /i DesktopDirector /l*v <logfile path and name>
```

8. 画面の指示に従い、ウィザードを完了します。
9. コマンドラインを使用して次のコマンドを実行します。

```
DirectorConfig.exe /UPGRADE
```

10. コマンドラインを使用して Monitor スナップインをインストールします。

```
msiexec /i Monitor_PowershellSnapin_x64.msi
```

11. すべての .msi インストールが完了したら、Program Files の Monitor サービスに移動し、次のコマンドを実行します。

```
Citrix.Monitor.exe /upgrade /enablefeatures
```

12. Citrix Site Managerを開き、**自動サイトアップグレード**オプションを選択して、アップグレードワークフローを完了します。
13. Directorにサインインして、新機能が利用可能であることを確認します。

ロールバック手順

1. 監視データベースのバックアップを必ず取得してください。
2. 「dbollback.zip」という名前のデータベースロールバックスクリプト(/ja-jp/citrix-virtual-apps-desktops/2503/downloads/dbrollback.zip)をダウンロードして実行します。
3. コントロールパネルから以下をアンインストールします。
   - **Citrix Monitor Service PowerShell Snap-in- x64** を選択し、**アンインストール**をクリックします。
   - **Citrix Monitor Service - x64** を選択し、**アンインストール**をクリックします。

- **Citrix Director** を選択し、**アンインストール**をクリックします。

4. 既に取得したバックアップから監視データベースを復元します。詳細については、ナレッジ共有記事 CTX135207 を参照してください。
5. Citrix Virtual Apps and Desktopsインストーラーを使用して、Delivery ControllerとDirectorを再インストールします。詳細については、コアコンポーネントのインストールを参照してください。

   または、,

次のコマンドを使用してコンポーネントを再インストールすることもできます。

```
XenDesktopServerSetup.exe /components controller,director /
configure_firewall /quiet
```

1. インストールが完了したら、**Citrix Site Managerを開く**チェックボックスを選択します。
2. Citrix Site Managerで推奨される場合は、サイトのアップグレードを実行します。

サポートとコンプライアンス

サポート

- Directorの累積リリース（CR）バージョンはLTSR互換ですが、LTSR準拠ではありません。
- アップグレード後、必要なすべてのサポートチケットとバグ修正は、Directorの次の累積リリース（CR）に追加されます。
- 変更または修正を含むCRは、以下の累積更新プログラム（CU）で利用可能になります。

508/WCAG 2.1

- 508/WCAG 2.1 準拠の義務があるお客様には、すべてのコアコンポーネントの LTSR バージョンを継続して使用することをお勧めします。

サイト分析

Directorを使用して、展開の健全性を監視できます。オンボードされているすべてのサイトでユーザー、エンドポイント、またはマシンを検索することで、パフォーマンスの問題をトラブルシューティングできます。

Directorダッシュボード(/en-us/citrix-virtual-apps-desktops/2503/media/dir-login.png)

完全な管理者権限があれば、Directorを開くと、ダッシュボードはサイトの健全性と使用状況を監視するための一元的な場所を提供します。

Directorダッシュボード(/en-us/citrix-virtual-apps-desktops/2503/media/dir-dashboard.png)

現在障害がなく、過去60分間に障害が発生していない場合、パネルは折りたたまれたままになります。障害が発生すると、特定の障害パネルが自動的に表示されます。

> **注:**
>
> 組織のライセンスと管理者権限によっては、一部のオプションまたは機能が利用できない場合があります。

Directorダッシュボードのパネル

ユーザー接続障害

過去60分間の接続障害。合計数の横にあるカテゴリをクリックすると、その種類の障害のメトリックが表示されます。隣接するテーブルでは、その数がデリバリーグループ別に分類されています。接続障害には、アプリケーション制限に達したことによる障害が含まれます。アプリケーション制限の詳細については、「アプリケーション」を参照してください。

失敗したシングルセッションOSマシンまたは失敗したマルチセッションOSマシン

過去60分間のデリバリーグループ別の合計障害。障害は、起動失敗、ブート中に停止、未登録などの種類別に分類されます。マルチセッションOSマシンの場合、障害には最大負荷に達したマシンも含まれます。

ライセンスステータス

ライセンスサーバーアラートは、ライセンスサーバーによって送信されたアラートと、アラートを解決するために必要なアクションを表示します。License Serverバージョン11.12.1以降が必要です。Delivery Controllerアラートは、Controllerによって認識されるライセンス状態の詳細を表示し、Controllerによって送信されます。XenApp 7.6またはXenDesktop 7.6以降のControllerが必要です。Studioでアラートのしきい値を設定できます。**Delivery Controllers** > **Details** > **Product Editions** > **PLT** に表示されるライセンスステータスは、**Premium** を示し、**Platinum** ではありません。

猶予状態

Director は、次のいずれかのグレース状態を表示します。この情報は Delivery Controller から取得されます。

1. **非アクティブ:** いずれの種類のライセンスキャッシュモードでもありません。通常のライセンス制限が適用されます。
2. **緊急グレース:** ライセンスサーバーに到達できない場合、または接続の仲介中にライセンス情報を取得できない場合に有効になります。ユーザーには影響ありません。Director に表示されるエラーは、ライセンスサーバーに到達可能になるまで閉じることができません。
3. **猶予期間の期限切れ:** 緊急ライセンスキャッシュモードの有効期限が切れました。

詳細については、ライセンスの超過 および ライセンスバーストモード を参照してください。

接続されているセッション

過去 60 分間のすべてのデリバリーグループにおける接続済みセッション。

平均ログオン時間

過去 60 分間のログオンデータ。左側の大きな数字は、1 時間あたりの平均ログオン時間です。XenDesktop 7.0 より前の VDA のログオンデータは、この平均には含まれません。詳細については、「ユーザーログオンの問題の診断」を参照してください。

インフラストラクチャ

サイトのインフラストラクチャ（ホストとコントローラー）を一覧表示します。XenServer または VMware のインフラストラクチャの場合、パフォーマンスアラートを表示できます。たとえば、XenCenter を構成して、管理対象サーバーまたは仮想マシンで CPU、ネットワーク I/O、またはディスク I/O の使用率が指定されたしきい値を超えたときにパフォーマンスアラートを生成できます。デフォルトでは、アラートの繰り返し間隔は 60 分ですが、これも構成できます。詳細については、「XenServer 製品ドキュメント」の XenCenter パフォーマンスアラートのセクションを参照してください。

> **注:**
>
> 特定のメトリックにアイコンが表示されない場合、そのメトリックは使用しているホストの種類でサポートされていないことを示します。たとえば、System Center Virtual Machine Manager (SCVMM) ホスト、AWS、CloudStack では、正常性情報は利用できません。

> 次のオプション（以下のセクションで説明）を使用して、問題のトラブルシューティングを続行します。

- ユーザーマシンの電源を制御する
- マシンへの接続を防止する

接続ユーザーの合計数

過去24時間または過去7日間に少なくとも1つの接続があったユーザーの数を表示します。このパネルは、管理者が導入傾向を経営陣に示すのに役立ちます。

環境内で検出されたCitrix Workspace™アプリのバージョン

組織全体で使用されているCitrix Workspaceアプリのバージョン概要を提供します。これにより、異なるバージョンを使用しているデバイスの数を示すことで、バージョンを統一するのに役立ちます。デフォルトでは、すべてのOSプラットフォームのCitrix Workspaceアプリのバージョンデータが表示されます。特定のOSプラットフォームのバージョンデータは、**Platformドロップダウン**リストから対応するOSを選択することで表示できます。

セッションの監視

セッションが切断されても、そのセッションはアクティブであり、アプリケーションは引き続き実行されますが、ユーザーデバイスはサーバーと通信しなくなります。

アクション	説明
ユーザーの現在接続されているマシンまたはセッションを表示する	アクティビティマネージャーとユーザー詳細ビューから、ユーザーの現在接続されているマシンまたはセッション、およびこのユーザーがアクセスできるすべてのマシンとセッションのリストを表示します。このリストにアクセスするには、ユーザータイトルバーのセッションスイッチャーアイコンをクリックします。詳細については、「セッションの復元」を参照してください。
すべてのデリバリーグループにわたる接続セッションの合計数を表示する	ダッシュボードの**接続セッション**ペインで、過去60分間のすべてのデリバリーグループにわたる接続セッションの合計数を表示します。次に、大きな合計数をクリックすると、フィルタービューが開き、選択したデリバリーグループと範囲、およびデリバリーグループ全体

アクション	説明
	の使用状況に基づいてグラフィカルなセッションデータを表示できます。
アイドルセッションを終了する	セッションフィルタービューには、すべてのアクティブなセッションに関連するデータが表示されます。関連ユーザー、デリバリーグループ、セッション状態、およびしきい値時間より長いアイドル時間に基づいてセッションをフィルター処理します。フィルター処理されたリストから、ログオフまたは切断するセッションを選択します。詳しくは、「アプリケーションのトラブルシューティング」を参照してください。
より長期間のデータを表示する	トレンドビューで、**［セッション］**タブを選択すると、より長期間にわたる接続済みセッションと切断済みセッションのより具体的な使用状況データ（つまり、過去60分より前のセッションの合計）をドリルダウンできます。この情報を表示するには、**［履歴トレンドの表示］**をクリックします。

注:

ユーザーデバイスがバージョン7より前のVDAやLinux VDAなどのレガシーVirtual Delivery Agent（VDA）を実行している場合、Directorはセッションに関する完全な情報を表示できません。代わりに、情報が利用できないことを示すメッセージが表示されます。

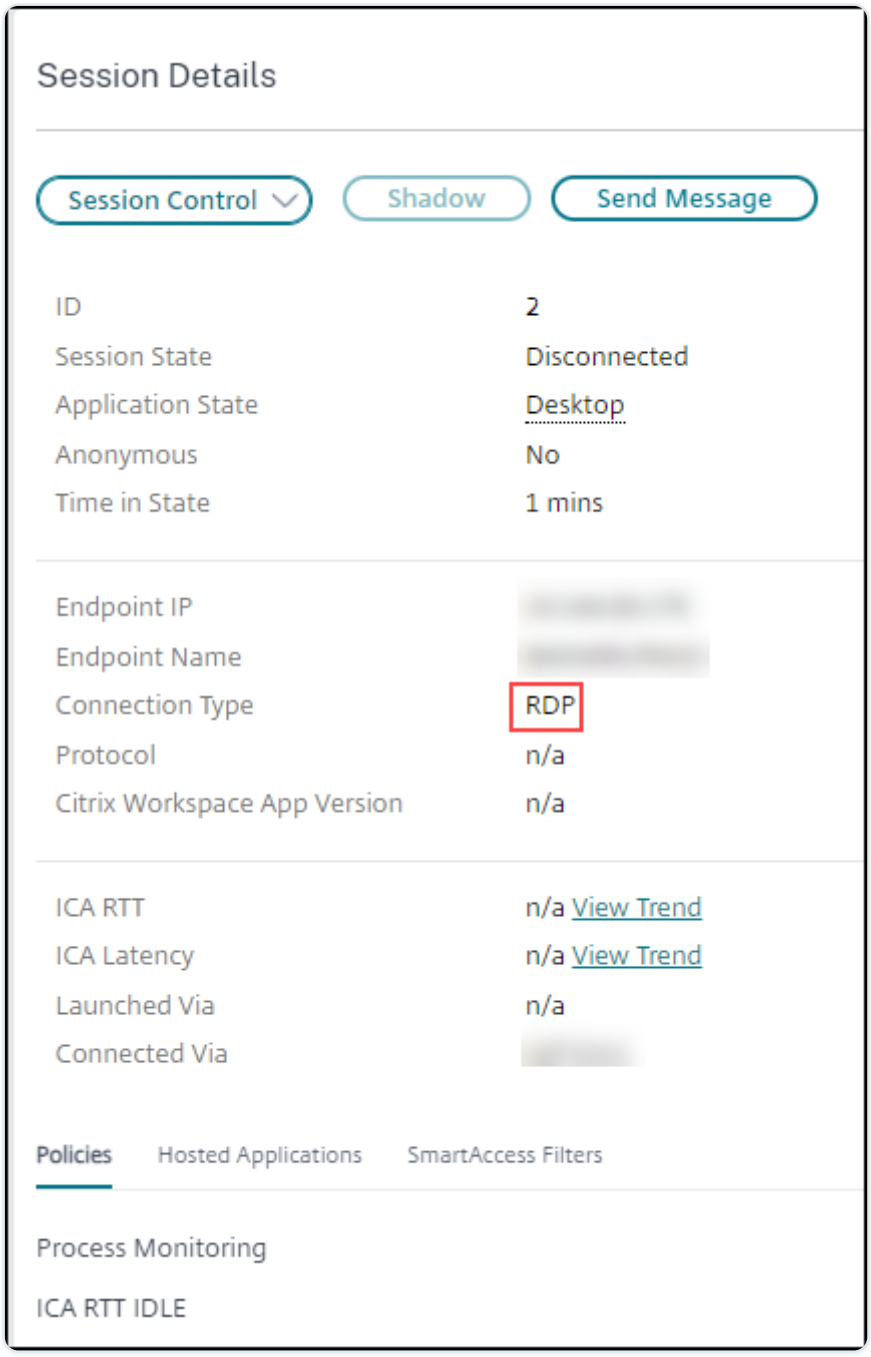
デスクトップ割り当て規則の制限： Web Studioでは、異なるユーザーまたはユーザーグループに対して複数のデスクトップ割り当て規則（DAR）を、デリバリーグループ内の単一のVDAに割り当てることができます。StoreFront™は、ログインしたユーザーのDARに従って、対応する**表示名**とともに割り当てられたデスクトップを表示します。ただし、DirectorはDARをサポートしておらず、ログインしたユーザーに関係なく、デリバリーグループ名を使用して割り当てられたデスクトップを表示します。結果として、Directorで特定のデスクトップをマシンにマッピングすることはできません。 StoreFrontに表示される割り当てられ

> たデスクトップを、Directorに表示されるデリバリーグループ名にマッピングするには、次のPowerShellコマンドを使用します。

```
Get-BrokerDesktopGroup | Where-Object { $\_.Uid -eq (Get-
BrokerAssignmentPolicyRule | Where-Object { $\_.PublishedName -eq
"\&lt;Name on StoreFront\>" }).DesktopGroupUid } | Select-Object -Property
Name, Uid
```

セッション転送プロトコル

［セッションの詳細］パネルで、現在のセッションのHDX接続タイプに使用されている転送プロトコルを表示します。この情報は、VDAバージョン7.13以降で起動されたセッションで利用できます。



- **HDX™**接続タイプの場合、,
  - HDX接続にEDTが使用されている場合、プロトコルは**UDP**と表示されます。
  - HDX接続にTCPが使用されている場合、プロトコルは**TCP**と表示されます。
- **RDP**接続タイプの場合、プロトコルは**n/a**と表示されます。

アダプティブトランスポートが構成されている場合、セッション転送プロトコルはネットワークの状態に基づいてEDT（UDP経由）とTCPの間で動的に切り替わります。HDXセッションがEDTを使用して確立できない場合、TCPプロトコルにフォールバックします。

アダプティブトランスポートの構成について詳しくは、「アダプティブトランスポート」を参照してください。

レポートのエクスポート

定期的な使用状況および容量管理レポートを生成するために、トレンドデータをエクスポートできます。エクスポートは、PDF、Excel、CSVのレポート形式をサポートしています。PDFおよびExcel形式のレポートには、グラフと表で表されたトレンドが含まれます。CSV形式のレポートには、ビューを生成するために処理できる、またはアーカイブできる表形式のデータが含まれます。

レポートをエクスポートするには：

1. **トレンド**タブに移動します。
2. フィルター条件と期間を設定し、**適用**をクリックします。トレンドグラフと表にデータが入力されます。
3. **エクスポート**をクリックし、レポートの名前と形式を入力します。

Directorは、選択したフィルター条件に基づいてレポートを生成します。フィルター条件を変更した場合は、**エクスポート**をクリックする前に**適用**をクリックしてください。

> **注:**
>
> 大量のデータをエクスポートすると、Directorサーバー、Delivery Controller、およびSQLサーバーのメモリとCPUの使用量が大幅に増加します。最適なエクスポートパフォーマンスを実現するために、サポートされる同時エクスポート操作の数とエクスポートできるデータ量は、デフォルトの制限に設定されています。

サポートされるエクスポート制限

エクスポートされたPDFおよびExcelレポートには、選択されたフィルター条件に対する完全なグラフが含まれます。ただし、すべてのレポート形式の表形式データは、テーブル内の行数またはレコード数のデフォルト制限を超えると切り捨てられます。サポートされるレコードのデフォルト数は、レポート形式に基づいて定義されます。

Internet Information Services (IIS) のDirectorアプリケーション設定を構成することで、デフォルトの制限を変更できます。

レポート形式	サポートされるレコードのデフォルト数	DIRECTORアプリケーション設定のフィールド	サポートされるレコードの最大数
PDF	500	UI.ExportPdfDrilldownLimit	5000
エクセル	100,000	UI.ExportExcelDrilldownLimit	100,000
CSV	100,000 (「**セッション**」タブでは10,000,000)	UI.ExportCsvDrilldownLimit	100,000

エクスポートできるレコード数の制限を変更するには：

1. IISマネージャーコンソールを開きます。
2. デフォルトのWebサイトの下にあるDirector Webサイトに移動します。
3. **アプリケーション設定**をダブルクリックします。
4. 必要に応じて、UI.ExportPdfDrilldownLimit、UI.ExportExcelDrilldownLimit、またはUI.ExportCsvDrilldownLimitフィールドの設定を編集または追加します。

アプリケーション設定でこれらのフィールド値を追加すると、デフォルト値が上書きされます。

> **警告:**
>
> サポートされている最大レコード数を超えるフィールド値を設定すると、エクスポートのパフォーマンスに影響を与える可能性があり、サポートされていません。

エラー処理

このセクションでは、エクスポート操作中に発生する可能性のあるエラーの対処方法について説明します。

- **Directorがタイムアウトしました**

このエラーは、ネットワークの問題、DirectorサーバーまたはMonitor Serviceでのリソース使用率の高さが原因で発生する可能性があります。

デフォルトのタイムアウト期間は100秒です。Director Serviceのタイムアウト期間を長くするには、Internet Information Services (IIS) のDirectorアプリケーション設定で**Connector.DataServiceContext.Timeoutフィールド**の値を設定します。

1. IISマネージャーコンソールを開きます。
2. デフォルトのWebサイトの下にあるDirector Webサイトに移動します。
3. **アプリケーション設定**をダブルクリックします。
4. **Connector.DataServiceContext.Timeout**の値を編集します。

- **モニターがタイムアウトしました**

このエラーは、ネットワークの問題、またはモニターサービスやSQLサーバーでのリソース使用率が高いことが原因で発生する可能性があります。

モニターサービスのタイムアウト期間を延長するには、Delivery Controllerで次のPowerShellコマンドを実行します。

```
asnp Citrix.*

Get-MonitorConfiguration

Set-MonitorConfiguration -MonitorQueryTimeoutSeconds &lt;timeout value>
```

- **最大同時エクスポートまたはプレビュー操作が進行中**

Directorは、エクスポートまたはプレビューの1つのインスタンスをサポートします。**最大同時エクスポートまたはプレビュー操作が進行中**というエラーが表示された場合は、次のエクスポート操作を後でもう一度試してください。

同時エクスポートまたはプレビュー操作の数を増やすことは可能ですが、これはDirectorのパフォーマンスに影響を与える可能性があり、サポートされていません。

1. IISマネージャーコンソールを開きます。
2. デフォルトのWebサイトの下にあるDirector Webサイトに移動します。
3. **アプリケーション設定**をダブルクリックします。
4. 値**UI.ConcurrentExportLimit**を編集します。

- **Directorのディスク容量不足**

各エクスポート操作には、Windows Tempフォルダーに最大2 GBのハードディスク容量が必要です。空き容量を確保するか、Directorサーバーにハードディスク容量を追加してから、エクスポートを再試行してください。

Monitorのホットフィックス

特定のVDAマシン（物理またはVM）にインストールされているホットフィックスを表示するには、**マシン詳細**ビューを選択します。

ユーザーマシンの電源状態を制御する

Directorで選択したマシンの状態を制御するには、電源制御オプションを使用します。これらのオプションは、シングルセッションOSマシンで利用できますが、マルチセッションOSマシンでは利用できない場合があります。

注：

この機能は、物理マシンまたはリモートPCアクセスを使用するマシンでは利用できません。

コマンド	機能
再起動	VMの正常な（ソフト）シャットダウンを実行し、VMを再起動する前にすべての実行中のプロセスが個別に停止されます。たとえば、Directorで「起動に失敗しました」と表示されるマシンを選択し、このコマンドを使用して再起動します。
強制再起動	シャットダウン手順を最初に実行せずにVMを再起動します。このコマンドは、物理サーバーのプラグを抜き、再度差し込んで電源を入れるのと同じように機能します。
シャットダウン	VMの正常な（ソフト）シャットダウンを実行します。すべての実行中のプロセスが個別に停止されます。

コマンド	機能
強制シャットダウン	シャットダウン手順を最初に実行せずにVMをシャットダウンします。このコマンドは、物理サーバーのプラグを抜くのと同じように機能します。すべての実行中のプロセスが常にシャットダウンされるとは限らず、この方法でVMをシャットダウンすると、データが失われるリスクがあります。
一時停止	実行中のVMを現在の状態で一時停止し、その状態をデフォルトのストレージリポジトリのファイルに保存します。このオプションを使用すると、VMのホストサーバーをシャットダウンし、後で再起動した後、VMを再開して元の実行状態に戻すことができます。
再開	停止中のVMを再開し、元の実行状態に戻します。
開始	VMがオフのときに起動します（コールドスタートとも呼ばれます）。

電源制御アクションが失敗した場合、アラートにマウスを重ねると、失敗の詳細を示すポップアップメッセージが表示されます。

マシンへの接続を防止する

適切な管理者がイメージのメンテナンス作業を実行している間、メンテナンスモードを使用して新しい接続を一時的に防止します。

マシンでメンテナンスモードを有効にすると、無効にするまで新しい接続は許可されません。ユーザーが現在ログオンしている場合、すべてのユーザーがログオフするとすぐにメンテナンスモードが有効になります。ログオフしないユーザーには、マシンが特定の時間にシャットダウンされることを通知するメッセージを送信し、電源制御を使用してマシンを強制的にシャットダウンします。

1. ユーザー詳細ビューから、またはフィルタービューでマシンのグループから、マシンを選択します。
2. **メンテナンスモード**を選択し、オプションをオンにします。

ユーザーが割り当てられたデスクトップにメンテナンスモード中に接続しようとすると、デスクトップが利用できないことを示すメッセージが表示されます。メンテナンスモードを無効にするまで、新しい接続はできません。

アプリケーション分析

「**アプリケーション**」タブには、アプリケーションベースの分析が単一の統合ビューで表示され、アプリケーションのパフォーマンスを効率的に分析および管理するのに役立ちます。サイトで公開されているすべてのアプリケーションの健全性および使用状況に関する貴重な情報を得ることができます。プローブ結果、アプリケーションごとのインスタンス数、公開されたアプリケーションに関連する障害やエラーなどのメトリックが表示されます。詳細については、**アプリケーションのトラブルシューティング**のアプリケーション分析セクションを参照してください。

アラートと通知

アラートは、Directorのダッシュボードやその他の上位レベルのビューに、警告および重大なアラートシンボルとともに表示されます。アラートは、**Premium**ライセンスサイトで利用できます。アラートは1分ごとに自動的に更新されます。また、オンデマンドでアラートを更新することもできます。

「Directorのアラート」(/en-us/citrix-virtual-apps-desktops/2503/media/dir-alerts.png)

警告アラート（琥珀色の三角形）は、条件の警告しきい値に達したか、それを超えたことを示します。

重大アラート（赤い円）は、条件の重大なしきい値に達したか、それを超えたことを示します。

サイドバーからアラートを選択するか、サイドバーの下部にある**アラートに移動**リンクをクリックするか、Directorページの上部から**アラート**を選択することで、アラートに関する詳細情報を表示できます。

アラートビューでは、アラートをフィルタリングしてエクスポートできます。たとえば、過去1か月間の特定のデリバリーグループの失敗したマルチセッションOSマシン、または特定のユーザーのすべてのアラートなどです。詳細については、「レポートのエクスポート」を参照してください。

「アラートのフィルター」(/en-us/citrix-virtual-apps-desktops/2503/media/director_filteralerts.png)

Citrix®アラート

Citrixアラートは、Citrixコンポーネントから発生し、Directorで監視されるアラートです。Directorの**アラート** \> **Citrixアラートポリシー**でCitrixアラートを構成できます。構成の一部として、ア

ラートが設定したしきい値を超えたときに、個人やグループに電子メールで通知を送信するように設定できます。Citrixアラートの設定の詳細については、「アラートポリシーの作成」を参照してください。

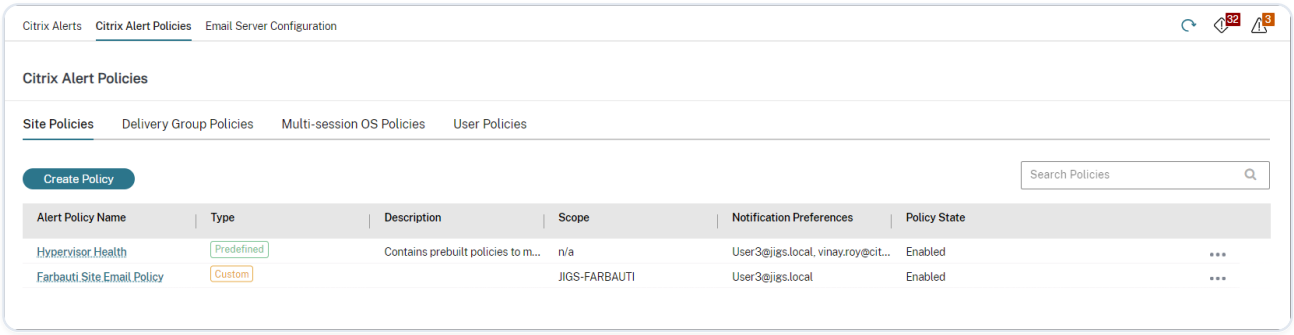
> **注:**
>
> ファイアウォール、プロキシ、またはMicrosoft Exchange Serverがメールアラートをブロックしないようにしてください。

スマートアラートポリシー

事前定義されたしきい値を持つ一連の組み込みアラートポリシーは、デリバリーグループおよびマルチセッションOS VDAのスコープで利用できます。この機能には、Delivery Controllerバージョン7.18以降が必要です。組み込みアラートポリシーのしきい値パラメーターは、**アラート** \> **Citrixアラートポリシー**で変更できます。 これらのポリシーは、サイトに少なくとも1つのアラートターゲット（デリバリーグループまたはマルチセッションOS VDA）が定義されている場合に作成されます。さらに、これらの組み込みアラートは、新しいデリバリーグループまたはマルチセッションOS VDAに自動的に追加されます。

Directorとサイトをアップグレードする場合、以前のDirectorインスタンスのアラートポリシーが引き継がれます。組み込みアラートポリシーは、Monitorデータベースに対応するアラートルールが存在しない場合にのみ作成されます。

組み込みのアラートポリシーのしきい値については、(#alerts-policies-conditions)セクションを参照してください。



高度なアラートポリシー

Directorのプロアクティブ通知およびアラート機能が強化され、**高度なアラートポリシー**という新しいアラートフレームワークが追加されました。この機能を使用すると、各要素または条件にきめ細かい詳細を含めてアラートを作成できるため、アラートの範囲に対する制御が強化されま

す。現在、これらのポリシーには、コスト削減とインフラストラクチャに関するアラートが含まれています。

データソース駆動型アラートである高度なアラートポリシーの導入により、複数条件のスコープフィルタリングを使用できます。

この機能は、過剰なアラートを減らすのに役立ちます。過剰なアラートは、重要な問題への対応の迅速性や有効性を低下させる可能性があります。このポリシーは、アラートポリシーの有効性と管理者からのエンゲージメントを測定するのに役立ちます。

アラート > **高度なアラートポリシー** > **ポリシーの作成**セクションから、高度なアラートポリシーを作成できます。

次のデータソースのいずれかを選択できます。

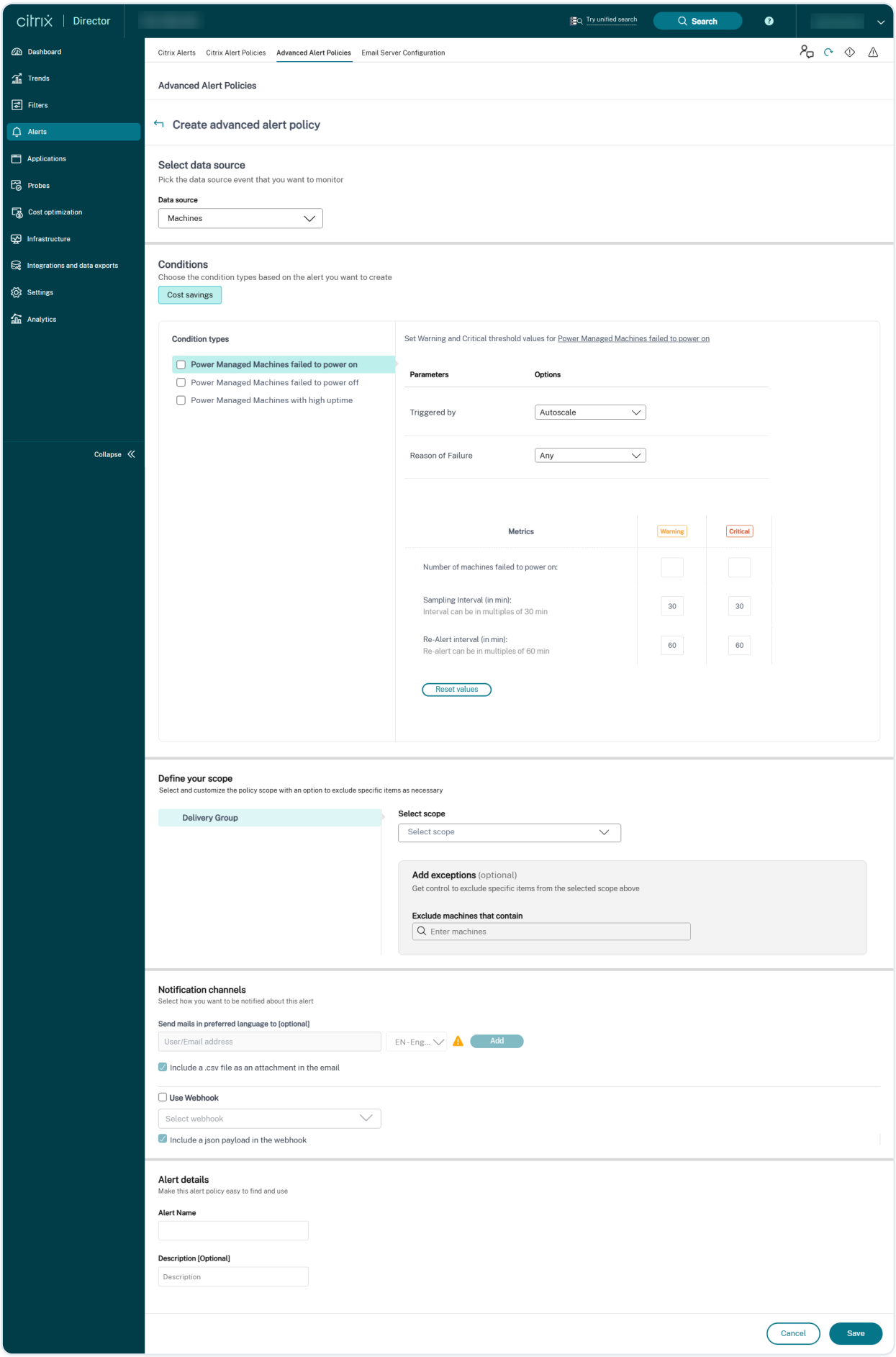
- マシン
- プロビジョニングサービス
- StoreFront™
- デリバリー コントローラー™

コスト削減に関するアラート

コストを最適化するのに役立つコスト削減のためのアラートを作成できます。現在、マシン用のアラートを作成できます。

マシンに関するアラートを作成するには、次の手順を実行します。

1. 「**アラート**」タブ > 「**高度なアラートポリシー**」をクリックします。「**高度なアラートポリシー**」ページが表示されます。
2. 「**ポリシーの作成**」をクリックします。「**高度なアラートポリシーの作成**」セクションが表示されます。
3. データソースドロップダウンリストから「**マシン**」を選択します。コスト削減条件とそれに対応する条件タイプが表示されます。


citrix | Director
Try unified search
Search
Dashboard
Trends
Filters
Alerts
Applications
Probes
Cost optimization
Infrastructure
Integrations and data exports
Settings
Analytics
Collapse
Citrix Alerts
Citrix Alert Policies
Advanced Alert Policies
Email Server Configuration
Advanced Alert Policies
Create advanced alert policy
Select data source
Pick the data source event that you want to monitor
Data source
Machines
Conditions
Choose the condition types based on the alert you want to create
Cost savings
Condition types
Power Managed Machines failed to power on
Power Managed Machines failed to power off
Power Managed Machines with high uptime
Set Warning and Critical threshold values for Power Managed Machines failed to power on
Parameters
Options
Triggered by
Autoscale
Reason of Failure
Any
Metrics
Warning
Critical
Number of machines failed to power on:
Sampling Interval (in min):
Interval can be in multiples of 30 min
30
30
Re-Alert interval (in min):
Re-alert can be in multiples of 60 min
60
60
Reset values
Define your scope
Select and customize the policy scope with an option to exclude specific items as necessary
Delivery Group
Select scope
Select scope
Add exceptions (optional)
Get control to exclude specific items from the selected scope above
Exclude machines that contain
Enter machines
Notification channels
Select how you want to be notified about this alert
Send mails in preferred language to [optional]
User/Email address
EN - Eng...
Add
Include a .csv file as an attachment in the email
Use Webhook
Select webhook
Include a json payload in the webhook
Alert details
Make this alert policy easy to find and use
Alert Name
Description [Optional]
Description
Cancel
Save

4. 必要な条件タイプを以下から選択します。
    - 電源管理されたマシンの電源オンに失敗しました
    - 電源管理されたマシンの電源オフに失敗しました
    - 稼働時間の長い電源管理されたマシン
5. 選択した各条件について、特定のパラメーターとそれに対応するオプションを選択します。
6. 選択した条件タイプについて、警告およびクリティカルのメトリックを設定します。
    - 稼働時間の長い電源管理されたマシンについて：
        - 稼働時間しきい値を超えているマシンの数
        - 再アラート間隔（分）。間隔は最低60分です。
    - 電源管理されたマシンの電源オンに失敗した場合、および電源管理されたマシンの電源オフに失敗した場合：
        - 稼働時間しきい値を超えているマシンの数
        - サンプリング間隔（分単位）間隔は30分の倍数にできます
        - 再アラート間隔（分単位）再アラートは60分の倍数にできます
7. 必要に応じて、選択したアラートの再アラート間隔をスケジュールします。
8. アラートのスコープを定義します。
9. 通知チャネルを設定します。これはメールまたはWebhookにすることができます。
    a. 次のチェックボックスを選択できます。
        - WebhookにJSONペイロードを添付として含める
        - メールにCSVファイルを添付として含める

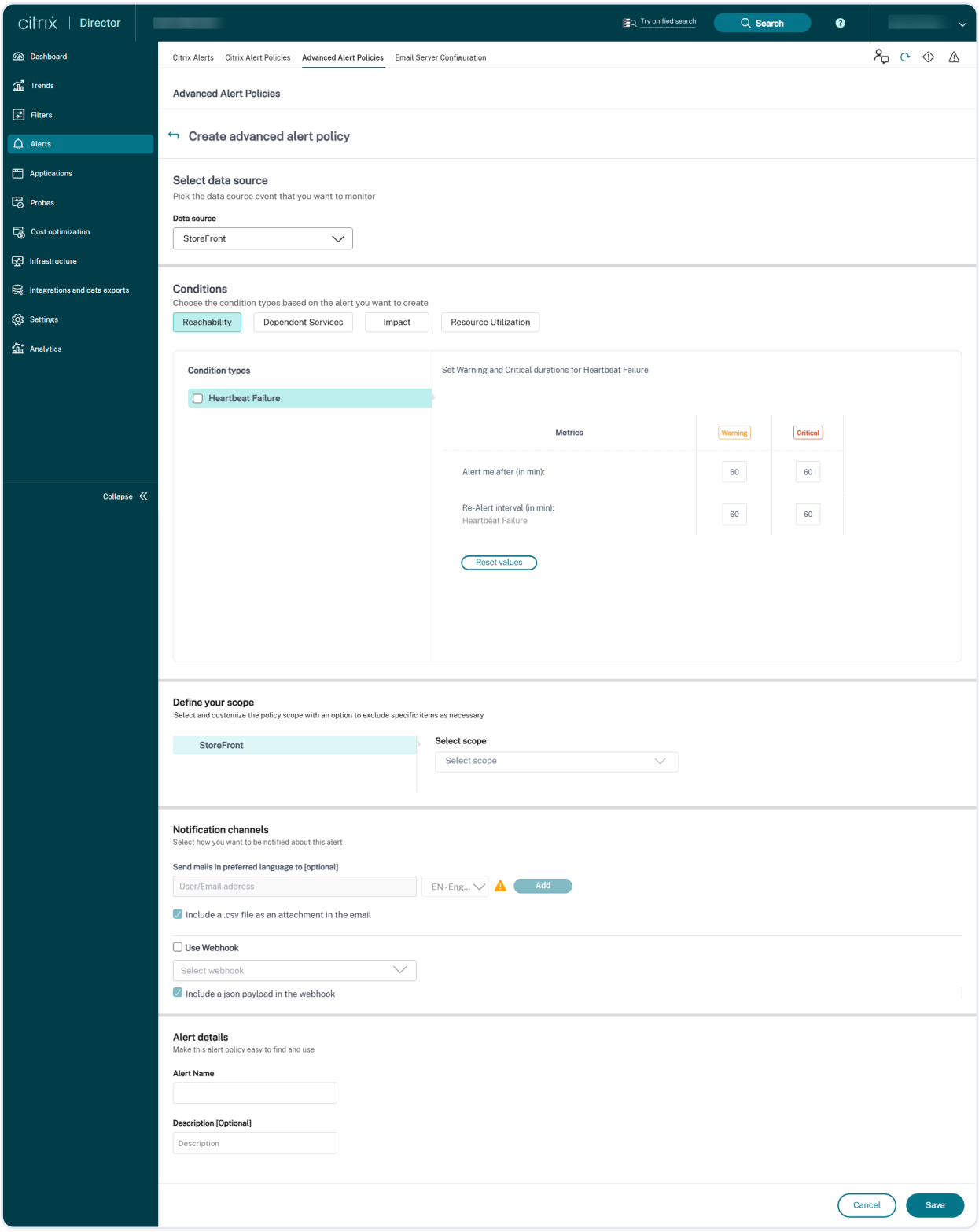
    詳細については、アラートコンテンツの機能強化を参照してください。
10. **アラート名**や**説明**（オプション）などの**アラートの詳細**を入力します。
11. **保存**をクリックします。アラートが作成されます。

インフラストラクチャ監視のアラート

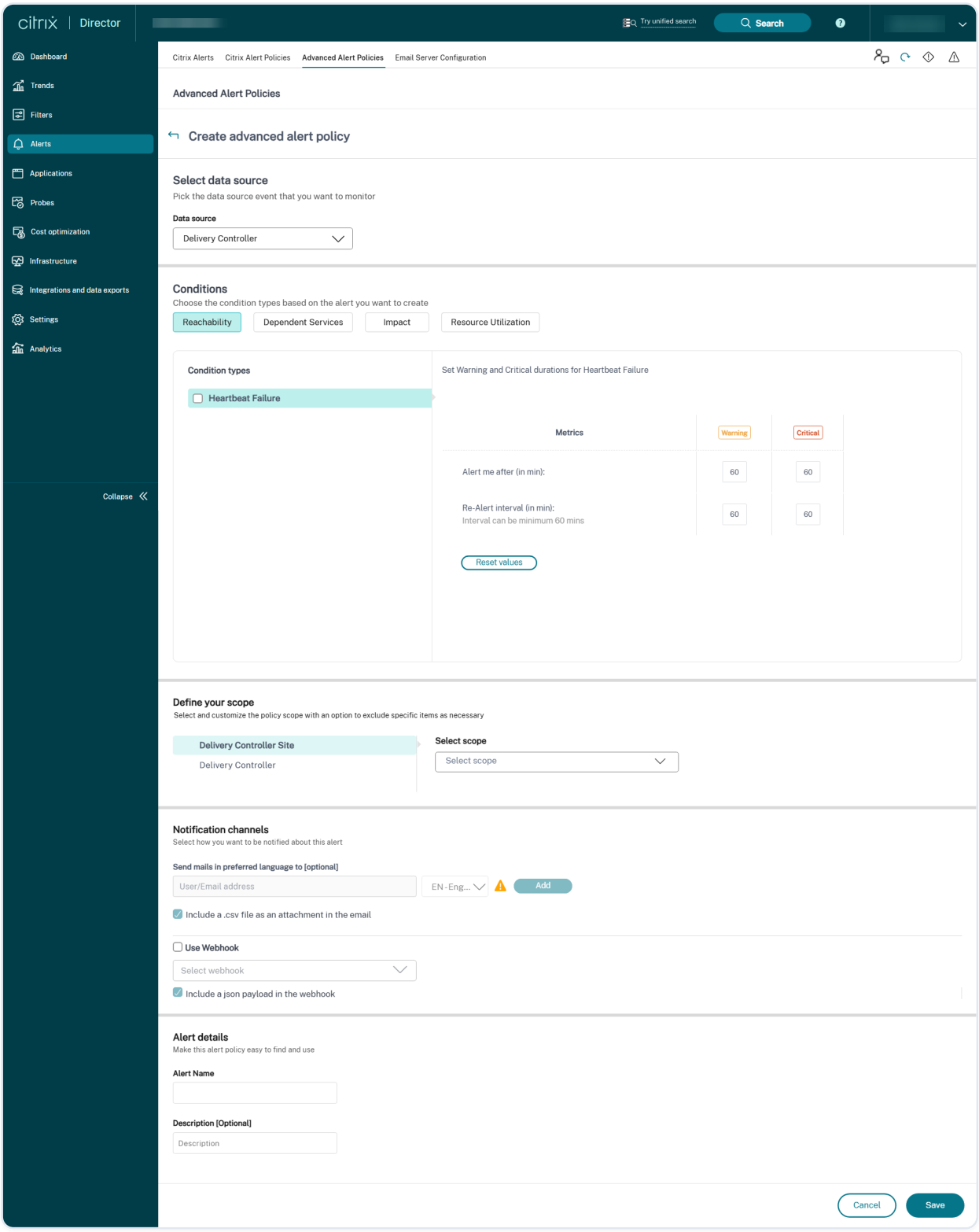
次のサポートされているCitrix Virtual Apps and Desktops™コンポーネントの健全性を監視するためにアラートを作成できます。

- プロビジョニングサービス

- StoreFront



- デリバリーコントローラー



インフラストラクチャ監視のセットアップが完了すると、Directorで利用可能な健全性データを使用して、必要なコンポーネントのアラートを設定できます。管理者は、条件、スコープ、通知媒体を設定して、メールまたはWebhook経由のJSONペイロードで重要なアラートを受信できます。Provisioning ServiceおよびDelivery Controllerの場合、アラートのスコープをサイトレベルまたは個々のサーバーレベルとして選択できます。たとえば、Provisioning Serviceの場合、「すべてのProvisioning Service」を選択すると、サイトに2台のサーバーがある場合でも、サイト全体に対し

て1つのアラートのみを受信します。これはサイトレベルのアラートと見なされます。発生したアラートは、分析と管理のために**Citrix Alerts**セクションでも利用できます。

新しく導入されたインフラストラクチャポリシーの一部として、アラート条件は次の4つのセクションに分類されます。

- 到達可能性
- 依存サービス
- 影響
- リソース使用率

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

アラート > **Citrixアラートポリシー**セクションからインフラストラクチャポリシーを作成できます。必要なカテゴリを選択し、ポリシーに必要な条件を選択できます。ポリシーの作成方法の詳細については、「アラートポリシーの作成」を参照してください。ポリシーが作成された後、Citrix Alertsページでポリシーを編集、削除、または無効にできます。

各カテゴリとコンポーネントでサポートされている条件の詳細については、以下を参照してください。

- Provisioning Serviceの健全性メトリック
- StoreFrontの健全性メトリック
- 「デリバリーコントローラーの健全性メトリック」(/ja-jp/citrix-virtual-apps-desktops/2503/director/infrastructure-monitoring/infrastructure-dashboard#delivery-controller-health-metrics)

次のデータは、メールまたはCitrixアラートページでアラートとして受信されます。

フィールド	説明
顧客ID	サイトの顧客ID。
アラートレベル	指定できる値は、致命的 (Critical) と警告 (Warning) です。
ターゲット	アラートがトリガーされたマシンの名前。
時間	アラートがトリガーされた時刻。
スコープ	ポリシーのスコープ。

フィールド	説明
ポリシー	ポリシーの名前。
説明	アラートがトリガーされる問題の説明。

ポリシーのスコープを定義する

アラートのスコープを定義し、例外を追加できます。アラートは選択したスコープに対してのみ生成され、例外の追加を使用して除外されたサブスコープはアラート生成に含まれません。この機能は、詳細なレベルでアラートを作成するのに役立ちます。

メールまたはWebhook URLを介して通知を作成できます。アラートを受信する優先言語を選択することもできます。また、メールの場合は.CSVファイル添付として、Webhook URLを介してはJSONペイロードとしてアラートパラメータを受信するオプションを選択することもできます。添付ファイルには、必要なパラメータの詳細が含まれています。詳細については、「アラートコンテンツの機能強化」を参照してください。

次のデータは、メールまたは**Citrix Alerts**ページでアラートとして受信されます。

フィールド	説明
顧客ID	サイトの顧客ID。
アラートレベル	この値は、各アラート条件に設定された事前定義値です。可能な値は「Critical」と「Warning」です。
条件	この値は、ポリシー作成時に設定された条件です。たとえば、未登録のマシンの数が20以上である場合などです。
ターゲット	アラートがトリガーされるデリバリーグループまたはサイトの名前。
サイト	サイトの名前。
スコープ	ポリシーのスコープ。この値にはサブスコープも含まれます。
ポリシー	ポリシーの名前。
説明	アラートがトリガーされる問題の説明。

PowerShellスクリプトを使用して高度なアラートポリシーを作成する方法?

アラートポリシーを作成するためのPowerShellスクリプト:

```
asnp Citrix.Monitor.*

# Add Parameters

$timeSpan = New-TimeSpan -Seconds 30

$alertThreshold = 1

$alarmThreshold = 2

# Add Target UID's

$targetIds = @()

$targetIds += "e9a211b4-a1f3-4f74-b6c7-85225902e997"

# Add email addresses

$emailaddress = @()

$emailaddress += "loki@abc.com"

# Create new policy

$policy = New-MonitorNotificationPolicy -Name
"FailedMachinePercentageAlertCreationViaPowershell" -Description "Policy
created to test urm" -Enabled $true
```

次の行をFAILEDMACHINEPERCENTAGEの正しい条件に置き換えます

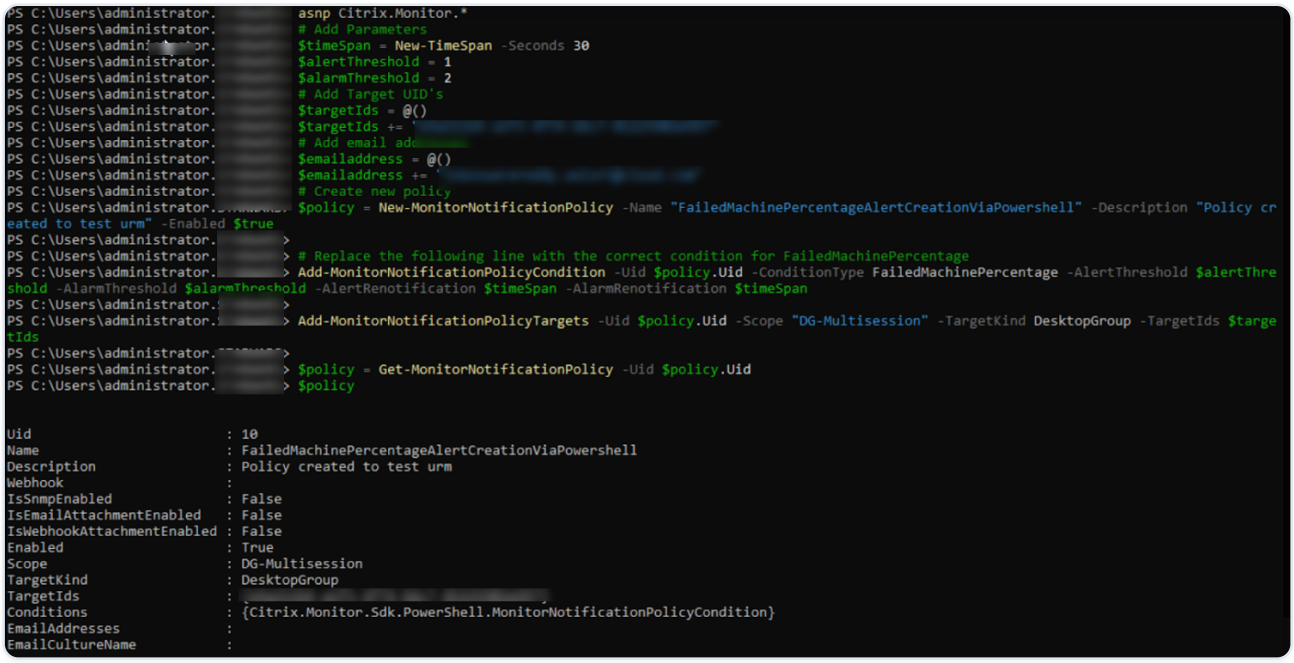
```
Add-MonitorNotificationPolicyCondition -Uid $policy.Uid -ConditionType
FailedMachinePercentage -AlertThreshold $alertThreshold -AlarmThreshold
$alarmThreshold -AlertRenotification $timeSpan -AlarmRenotification
$timeSpan



Add-MonitorNotificationPolicyTargets -Uid $policy.Uid -Scope "DG-
Multisession" -TargetKind DesktopGroup -TargetIds $targetIds
```

```
$policy = Get-MonitorNotificationPolicy -Uid $policy.Uid

$policy
```



上記の画像から、ポリシーが作成され、Uidが10であることがわかります。

構成にメールを追加するには

```
Set-MonitorNotificationEmailServerConfiguration -ProtocolType SMTP
-ServerName NameOfTheSMTPServerOrIPAddress -PortNumber 80
-SenderEmailAddress loki@abc.com -RequiresAuthentication 0
```

ポリシーにメールを追加するには

```
Add-MonitorNotificationPolicyEmailAddresses -Uid $policy.Uid
-EmailAddresses $emailaddress -EmailCultureName "en-US"
```

メールを追加するためのサンプルスクリプト:

```
Add-MonitorNotificationPolicyEmailAddresses -Uid 10 -EmailAddresses
$emailaddress -EmailCultureName "en-US"
```

PSメール追加(/en-us/citrix-virtual-apps-desktops/2503/media/powershell-email.png)

ポリシーにWEBHOOK URLを追加するには

```
Set-MonitorNotificationPolicy –Uid $polcy.Uid –Webhook 'URL'
```

PS Webhook追加(/en-us/citrix-virtual-apps-desktops/2503/media/powershell-add-wehook.png)

Webhook URLを追加するためのサンプルスクリプト:

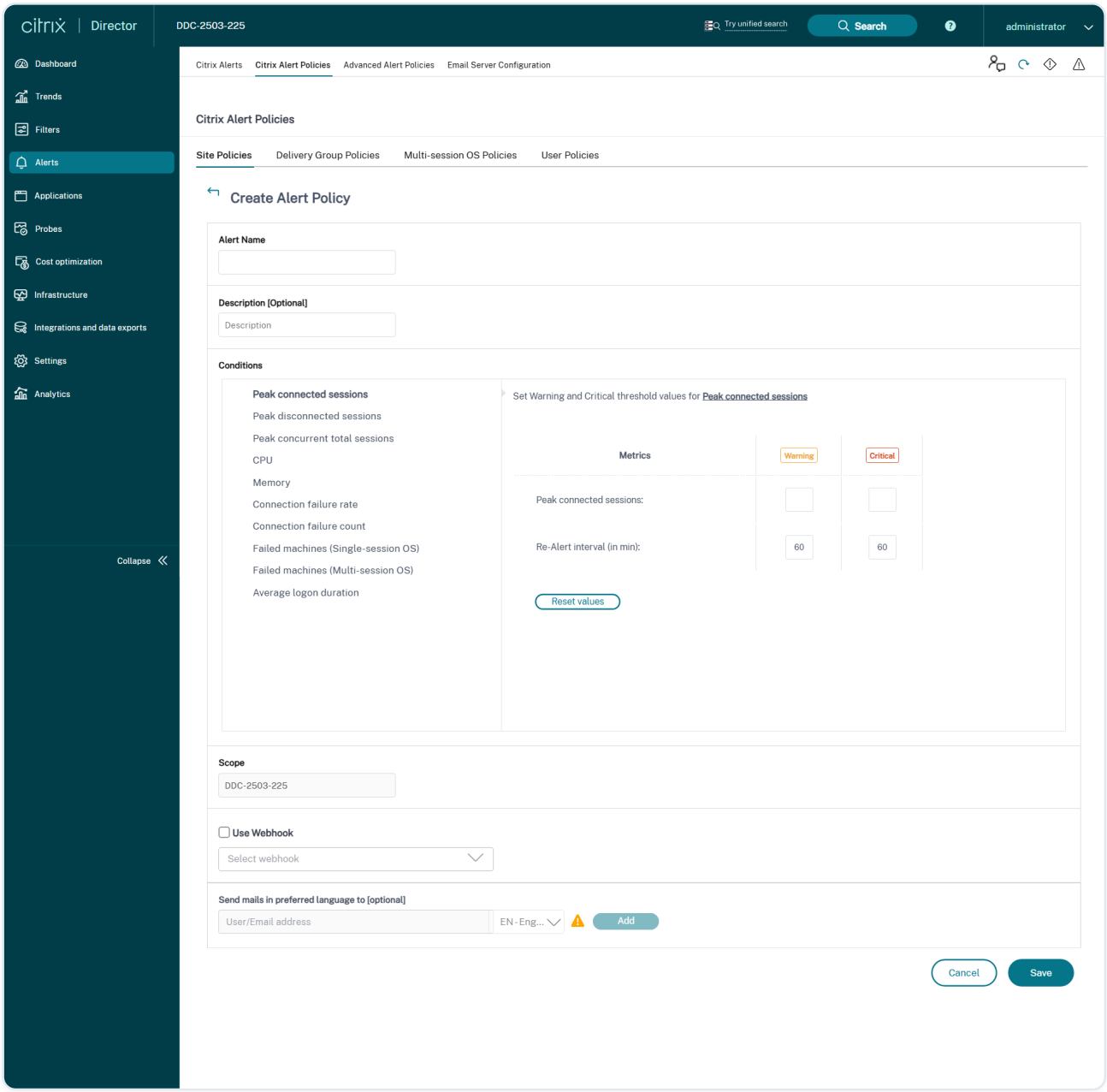
```
Set-MonitorNotificationPolicy –Uid 10  –Webhook  'https://hooks.slack.com/
triggers/E030QBY6FHU/6405020258726/8b6471a3e4827a5f834e7679022a1f1c'
```

作成されたポリシーの詳細を取得

```
Get-MonitorNotificationPolicy -Uid 10
```

PSポリシー作成(/en-us/citrix-virtual-apps-desktops/2503/media/powershell-create-policy.png)

アラートポリシーを作成する



アラートポリシーを作成するには、たとえば、特定のセッション数基準が満たされたときにアラートを生成するには、次の手順を実行します。

1. **アラート** > **Citrixアラートポリシー** に移動し、たとえば「マルチセッションOSポリシー」を選択します。
2. **作成** をクリックします。
3. ポリシーに名前を付けて説明し、アラートがトリガーされる条件を設定します。たとえば、ピーク接続セッション、ピーク切断セッション、ピーク同時合計セッションの警告値と重大値を指定します。警告値は重大値より大きくしてはいけません。詳細については、アラートポリシーの条件を参照してください。

4. 再アラート間隔を設定します。アラートの条件が引き続き満たされている場合、この時間間隔でアラートが再度トリガーされ、アラートポリシーで設定されている場合は、メール通知が生成されます。却下されたアラートは、再アラート間隔でメール通知を生成しません。
5. スコープを設定します。たとえば、特定のデリバリーグループに設定します。
6. 通知設定で、アラートがトリガーされたときにメールで通知する必要があるユーザーを指定します。アラートポリシーでメール通知設定を行うには、**メールサーバー構成**タブでメールサーバーを指定する必要があります。

    a. .CSV添付ファイルまたはJSONペイロードを介してアラートコンテンツを受信することもできます。これには、次のチェックボックスをオンにします。

    - **Webhookにjsonペイロードを添付として含める**
    - **メールにcsvファイルを添付として含める**

> **注:**
>
> .CSV添付ファイルおよびJSONペイロードオプションを介してアラートコンテンツを受信できるのは、現在、一部のアラートのみです。詳細については、「アラートコンテンツの機能強化」を参照してください。

7. 「**保存**」をクリックします。

スコープで20以上のデリバリーグループが定義されたポリシーを作成すると、構成の完了に約30秒かかる場合があります。この間、スピナーが表示されます。

最大20の固有のデリバリーグループ（合計1000のデリバリーグループターゲット）に対して50を超えるポリシーを作成すると、応答時間が増加する（5秒を超える）可能性があります。

アクティブなセッションを含むマシンをあるデリバリーグループから別のデリバリーグループに移動すると、マシンパラメーターを使用して定義された誤ったデリバリーグループアラートがトリガーされる可能性があります。

> **注:**
>
> アラートポリシーを削除した後、そのポリシーによって生成されたアラート通知が停止するまでに最大30分かかる場合があります。

アラートコンテンツの機能強化

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

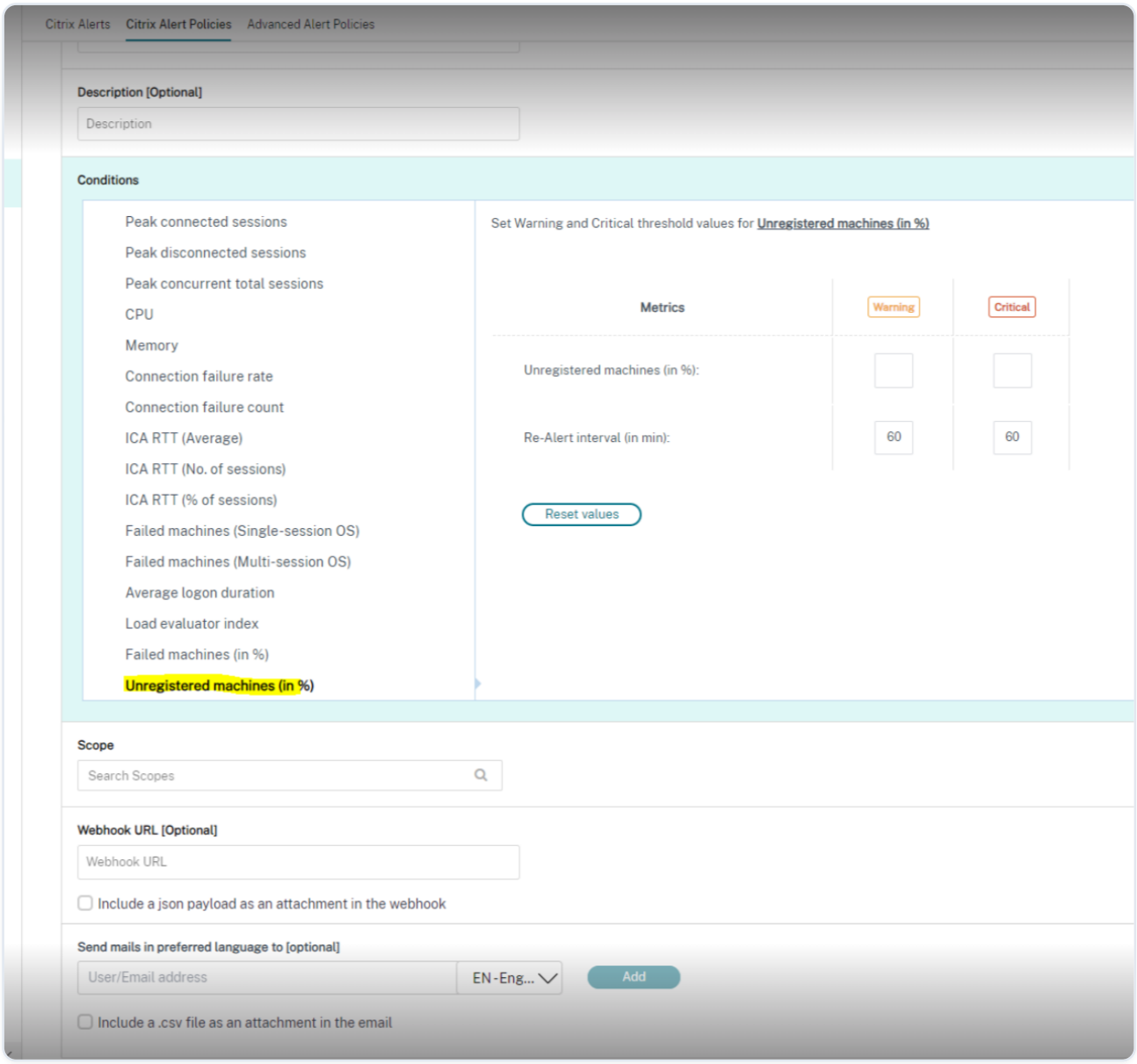
現在、この機能強化は次のアラートでのみ利用可能です。

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

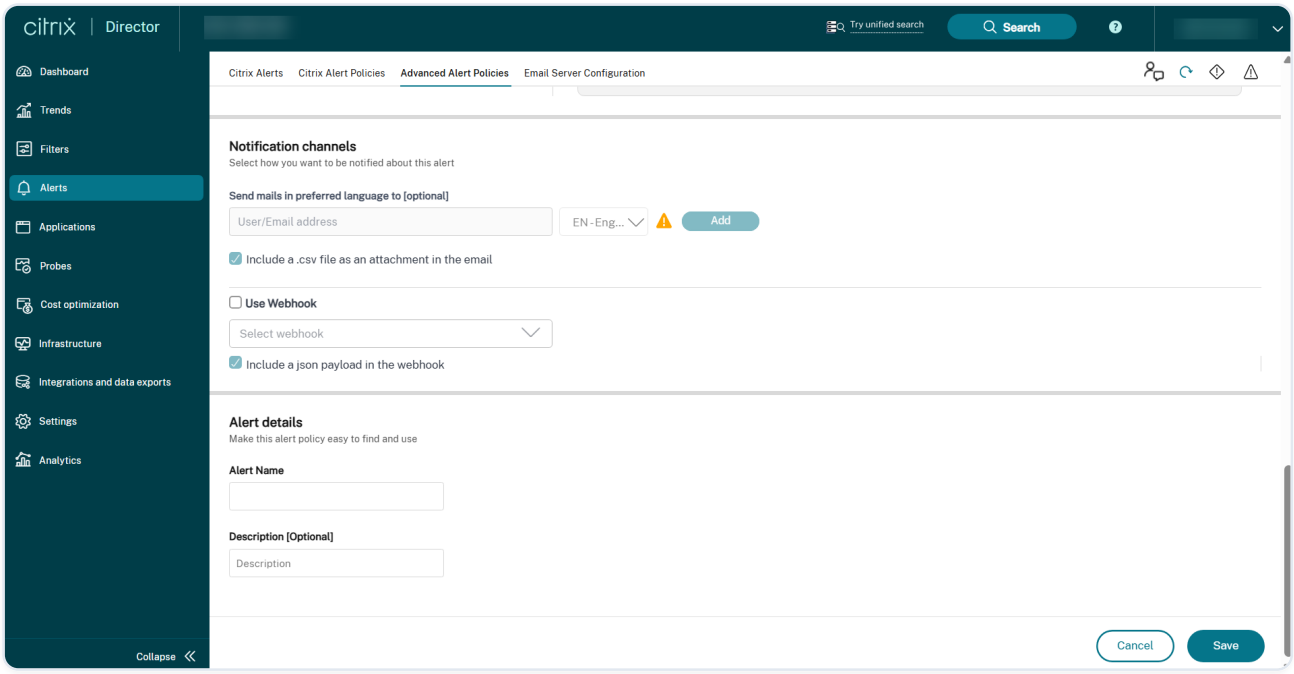
この機能を使用するには、アラートに移動し、次のチェックボックスを選択します。

- **Webhookにjsonペイロードを添付として含める**
- **メールにcsvファイルを添付として含める**

以下は、**Citrixアラートポリシー**セクションのスクリーンショットです。



以下は、**高度なアラートポリシー**セクションのスクリーンショットです。



CSV添付ファイル

次の表は、サポートされているすべてのアラートの.CSV添付ファイルの列を示しています。

列	適用されるアラート
マシン名、IPアドレス、およびデリバリーグループ名	マシンの稼働時間、電源オフ失敗アクションと電源オン失敗アクション、および未登録マシン（%）
現在の登録状態、失敗日、障害状態、およびライフサイクル状態	未登録マシン（%）
最終電源アクション失敗理由、最終電源アクショントリガー元、最終電源アクションタイプ、および最終電源アクション完了日	電源オフ失敗アクションと電源オン失敗アクション
電源状態、電源オン日時、総稼働時間（分）	マシンの稼働時間

WEBHOOKペイロード

未登録マシンの割合アラート

```
{

  "text": "{\"Address\":\"<Webhook URL>\",\"NotificationId\":
\"<NotificationGUID>\",\"NotificationState\":\"NotificationActive\",
\"Priority\":\"<Critical/Warning>\",\"Target\":\"<DeliveryGroupName>\",
\"Condition\":\"Unregistered machines (in %)\",\"Value\":\"<Value Set as
```

```
Threshold>\",\"Timestamp\":\"<Timestamp string Eg: April 25, 2024 9:33 PM
(UTC +5)>\",\"PolicyName\":\"<Alert Policy Name>\",\"Description\":
\"<Alert Policy Description>\",\"Scope\":\"DeliveryGroup\",\"Site\":
\"<Name of the Site>\",\"AttachmentData\":[{\"MachineName\":\"<Name of the
Machine>\",\"IPAddress\":\"<IP Address>\",\"DeliveryGroupName\":\"<Name of
the DeliveryGroup>\",\"CurrentRegistrationState\":\"Unregistered\",
\"FailureDate\":\"<Date of Failure>\",\"FaultState\":\"<Fault State of the
Machine>\",\"LifecycleState\":\"<Lifecycle state of the Machine>\"},
{\"MachineName\":\"<Name of the Machine>\",\"IPAddress\":\"<IP Address>\",
\"DeliveryGroupName\":\"<Name of the DeliveryGroup>\",
\"CurrentRegistrationState\":\"Unregistered\",\"FailureDate\":\"<Date of
Failure>\",\"FaultState\":\"<Fault State of the Machine>\",
\"LifecycleState\":\"<Lifecycle state of the Machine>\"}]}"

}
```

電源オン失敗アクションアラート

```
{

  "text": "{\"Address\":\"<Webhook URL>\",\"NotificationId\":
\"<NotificationGUID>\",\"NotificationState\":\"NotificationActive\",
\"Priority\":\"<Critical/Warning>\",\"Target\":\"<DeliveryGroupName>\",
\"Condition\":\"Failure To PowerOn Action\",\"Value\":\"<Value Set as
Threshold>\",\"Timestamp\":\"<Timestamp string Eg: April 25, 2024 9:33 PM
(UTC +5)>\",\"PolicyName\":\"<Alert Policy Name>\",\"Description\":
\"<Alert Policy Description>\",\"Scope\":\"DeliveryGroup\",\"Site\":
\"<Name of the Site>\",\"AttachmentData\":[{\"MachineName\":\"<Name of the
Machine>\",\"IPAddress\":\"<IP Address>\",\"DeliveryGroupName\":\"<Name of
the DeliveryGroup>\",\"LastPowerActionFailureReason\":
\"<HypervisorReportedFailure, HypervisorRateLimitExceeded, UnknownError,
Power Action Type>\",\"LastPowerActionTriggeredBy\":\"<End-User,
Administrator, Auto-Scale, Schedule>\",\"LastPowerActionType\":\"<PowerOn/
PowerOff>\",\"LastPowerActionCompletedDate\":\"<Time string Eg:
2024-05-15T15:04:27.723>\"},{\"MachineName\":\"<Name of the Machine>\",
\"IPAddress\":\"<IP Address>\",\"DeliveryGroupName\":\"<Name of the
DeliveryGroup>\",\"LastPowerActionFailureReason\":
\"<HypervisorReportedFailure, HypervisorRateLimitExceeded, UnknownError,
Power Action Type>\",\"LastPowerActionTriggeredBy\":\"<End-User,
Administrator, Auto-Scale, Schedule>\",\"LastPowerActionType\":\"<PowerOn/
PowerOff>\",\"LastPowerActionCompletedDate\":\"<Time string Eg:
2024-05-15T15:04:27.723>\"}]}"
```

```
}
```

電源オフ失敗アクションアラート

```
{

  "text": "{\"Address\":\"<Webhook URL>\",\"NotificationId\":
\"<NotificationGUID>\",\"NotificationState\":\"NotificationActive\",
\"Priority\":\"<Critical/Warning>\",\"Target\":\"<DeliveryGroupName>\",
\"Condition\":\"Failure To PowerOff Action\",\"Value\":\"<Value Set as
Threshold>\",\"Timestamp\":\"<Timestamp string Eg: April 25, 2024 9:33 PM
(UTC +5)>\",\"PolicyName\":\"<Alert Policy Name>\",\"Description\":
\"<Alert Policy Description>\",\"Scope\":\"DeliveryGroup\",\"Site\":
\"<Name of the Site>\",\"AttachmentData\":[{\"MachineName\":\"<Name of the
Machine>\",\"IPAddress\":\"<IPV4 Address of the Machine>\",
\"DeliveryGroupName\":\"<Name of the DeliveryGroup>\",
\"LastPowerActionFailureReason\":
\"<HypervisorReportedFailure,HypervisorRateLimitExceeded,UnknownError,Powe
r Action Type>\",\"LastPowerActionTriggeredBy\":\"<End-
User,Administrator,Auto-Scale,Schedule>\",\"LastPowerActionType\":
\"<PowerOn/PowerOff>\",\"LastPowerActionCompletedDate\":\"<Time string Eg:
2024-05-15T15:04:27.723>\"},{\"MachineName\":\"<Name of the Machine>\",
\"IPAddress\":\"<IPV4 Address of the Machine>\",\"DeliveryGroupName\":
\"<Name of the DeliveryGroup>\",\"LastPowerActionFailureReason\":
\"<HypervisorReportedFailure,HypervisorRateLimitExceeded,UnknownError,Powe
r Action Type>\",\"LastPowerActionTriggeredBy\":\"<End-
User,Administrator,Auto-Scale,Schedule>\",\"LastPowerActionType\":
\"<PowerOn/PowerOff>\",\"LastPowerActionCompletedDate\":\"<Time string Eg:
2024-05-15T15:04:27.723>\"}]}"

}
```

マシンの稼働時間アラート

```
{

  "text": "{\"Address\":\"<Webhook URL>\",\"NotificationId\":
\"<NotificationGUID>\",\"NotificationState\":\"NotificationActive\",
\"Priority\":\"<Critical/Warning>\",\"Target\":\"<DeliveryGroupName>\",
\"Condition\":\"Machine Uptime Alert\",\"Value\":\"<Value Set as
Threshold>\",\"Timestamp\":\"<Timestamp string Eg: April 25, 2024 9:33 PM
```

```
(UTC +5)>\",\"PolicyName\":\"<Alert Policy Name>\",\"Description\":
\"<Alert Policy Description>\",\"Scope\":\"DeliveryGroup\",\"Site\":
\"<Name of the Site>\",\"AttachmentData\":[{\"MachineName\":\"<Name of the
Machine>\",\"IPAddress\":\"<IP Address>\",\"DeliveryGroupName\":\"<Name of
the DeliveryGroup>\",\"PowerState\":\"<On/Off>\",\"PoweredOnDate\":
\"2024-05-15T15:04:27.723\",\"TotalUptimeInMinutes\":180},
{\"MachineName\":\"<Name of the Machine>\",\"IPAddress\":\"<IP Address>\",
\"DeliveryGroupName\":\"<Name of the DeliveryGroup>\",\"PowerState\":
\"<ON/OFF>\",\"PoweredOnDate\":\"2024-05-15T15:04:27.723\",
\"TotalUptimeInMinutes\":\"<Uptime Duration>\"}]}"

}
```

アラートポリシーの条件

以下に、アラートカテゴリ、アラートを軽減するための推奨されるアクション、および定義されている場合は組み込みポリシー条件を示します。組み込みアラートポリシーは、アラートおよび再アラートの間隔が60分に設定されています。

ピーク接続セッション

- Directorのセッショントレンドビューで、接続済みセッションのピークを確認します。
- セッション負荷に対応する十分な容量があることを確認してください。
- 必要に応じて新しいマシンを追加する

ピーク切断セッション

- Directorのセッショントレンドビューで、切断済みセッションのピークを確認します。
- セッション負荷に対応できる十分な容量があることを確認します。
- 必要に応じて新しいマシンを追加します

ピーク時の同時合計セッション数

- Directorのセッショントレンドビューで、同時セッションのピークを確認します。
- セッション負荷に対応できる十分な容量があることを確認します。
- 必要に応じて新しいマシンを追加します。
- 必要に応じて切断されたセッションをログオフします

ピーク時の同時合計セッション

- Directorのセッション傾向ビューで、ピーク時の同時セッションを確認します。

- セッション負荷に対応できる十分な容量があることを確認します。
- 必要に応じて新しいマシンを追加します。
- 必要に応じて、切断されたセッションをログオフします。

CPU

CPU 使用率の割合は、プロセスを含む VDA 上の全体的な CPU 消費量を示します。個々のプロセスによる CPU 使用率の詳細については、対応する VDA の ページで確認できます。

- **> >** に移動し、CPU を消費しているプロセスを特定します。プロセスレベルのリソース使用状況統計の収集を開始するには、プロセス監視ポリシーが有効になっていることを確認してください。
- 必要に応じてプロセスを終了します。
- プロセスを終了すると、保存されていないデータが失われます。
- すべてが期待どおりに機能している場合は、将来的に追加のCPUリソースを追加します。

> **注：**
>
> **リソース監視を有効にする**ポリシー設定は、VDAがインストールされているマシンでのCPUおよびメモリのパフォーマンスカウンターの監視に対して、デフォルトで許可されています。このポリシー設定が無効になっている場合、CPUおよびメモリの状態に関するアラートはトリガーされません。詳細については、「監視ポリシー設定」を参照してください。
>
> **スマートポリシー条件：**
>
> - **スコープ：**デリバリーグループ、マルチセッションOSスコープ
> - **しきい値：**警告 - 80%、重大 - 90%

メモリ

メモリ使用率の割合は、プロセスを含むVDA全体のメモリ消費量を示します。個々のプロセスによるメモリ使用量の詳細については、対応するVDAの**マシン詳細**ページで確認できます。

- **マシン詳細 > 履歴使用率の表示 > 上位10プロセス**に移動し、メモリを消費しているプロセスを特定します。プロセスレベルのリソース使用状況統計の収集を開始するには、プロセス監視ポリシーが有効になっていることを確認してください。
- 必要に応じてプロセスを終了します。

- プロセスを終了すると、保存されていないデータが失われます。
- すべてが期待どおりに機能している場合は、今後、追加のメモリを追加します。

> **注:**
>
> **リソース監視を有効にする**ポリシー設定は、VDAがインストールされたマシン上のCPUおよびメモリのパフォーマンスカウンターを監視するために、デフォルトで許可されています。このポリシー設定が無効になっている場合、CPUおよびメモリの状態に関するアラートはトリガーされません。詳細については、監視ポリシー設定を参照してください。

> **スマートポリシー条件:**

- **スコープ:** デリバリーグループ、マルチセッションOSスコープ
- **しきい値:** 警告 - 80%、クリティカル - 90%

メモリ

メモリ使用率は、VDA上の全体的なメモリ消費量（プロセスによるものを含む）を示します。個々のプロセスによるメモリ使用量に関する詳細な情報は、対応するVDAの**マシン詳細**ページから取得できます。

- **［マシン詳細］>［履歴使用率の表示］>［上位10プロセス］** に移動し、メモリを消費しているプロセスを特定します。プロセスレベルのリソース使用状況統計の収集を開始するには、プロセス監視ポリシーが有効になっていることを確認してください。
- 必要に応じてプロセスを終了します。
- プロセスを終了すると、保存されていないデータが失われます。
- すべてが期待どおりに機能している場合は、将来的に追加のメモリを追加します。

> **注:**
>
> **リソース監視を有効にする**ポリシー設定は、VDAがインストールされているマシンでのCPUおよびメモリのパフォーマンスカウンターの監視に対して、デフォルトで許可されています。このポリシー設定が無効になっている場合、CPUおよびメモリの状態に関するアラートはトリガーされません。詳しくは、「監視ポリシー設定」を参照してください。

> **スマートポリシー条件:**

- **スコープ：** デリバリーグループ、マルチセッションOSスコープ
- **閾値:** 警告 - 80%、危機的 - 90%

接続失敗率

過去1時間の接続失敗の割合。

- 試行された総接続数に対する総失敗数に基づいて計算されます。
- 構成ログから記録されたイベントについては、Directorの接続失敗傾向ビューを確認してください。
- アプリケーションまたはデスクトップに到達可能かどうかを判断します。

接続失敗数

過去1時間の接続失敗数。

- Director接続障害トレンドビューで、構成ログから記録されたイベントを確認します。
- アプリケーションまたはデスクトップに到達可能かどうかを判断します。

ICA® RTT (平均)

平均ICAラウンドトリップ時間。

- ICA RTTの内訳についてCitrix ADMを確認し、根本原因を特定します。詳細については、Citrix ADMドキュメントを参照してください。
- Citrix ADMが利用できない場合は、DirectorのユーザーDetailビューでICA RTTと遅延を確認し、ネットワークの問題か、アプリケーションまたはデスクトップの問題かを判断します。

ICA RTT (セッション数)

しきい値のICAラウンドトリップ時間を超えるセッションの数。

- ICA RTTが高いセッションの数についてCitrix ADMを確認します。詳細については、Citrix ADMドキュメントを参照してください。
- Citrix ADMが利用できない場合は、ネットワークチームと協力して根本原因を特定します。

  スマートポリシーの条件:

  - **スコープ:** デリバリーグループ、マルチセッションOSスコープ
  - **しきい値:** 警告 - 5セッション以上で300ミリ秒、重大 - 10セッション以上で400ミリ秒

ICA RTT (セッションの割合)

平均ICAラウンドトリップ時間を超えるセッションの割合。

- ICA RTTが高いセッションの数についてCitrix ADMを確認します。詳細については、Citrix ADMドキュメントを参照してください。
- Citrix ADMが利用できない場合は、ネットワークチームと協力して根本原因を特定してください。

ICA RTT (ユーザー)

指定されたユーザーによって起動されたセッションに適用されるICAラウンドトリップ時間。少なくとも1つのセッションでICA RTTがしきい値を超えると、アラートがトリガーされます。

失敗したマシン（シングルセッションOS）

失敗したシングルセッションOSマシンの数。失敗は、Directorのダッシュボードビューおよびフィルタービューに示されているように、さまざまな理由で発生する可能性があります。

- Citrix Scout診断を実行して、根本原因を特定します。

  スマートポリシーの条件:

  - **スコープ:** デリバリーグループ、マルチセッションOSスコープ
  - **しきい値:** 警告 - 1、重大 - 2

失敗したマシン (マルチセッションOS)

失敗したマルチセッションOSマシンの数。失敗は、Directorのダッシュボードビューおよびフィルタービューに示されているように、さまざまな理由で発生する可能性があります。

- Citrix Scout診断を実行して、根本原因を特定します。

  スマートポリシーの条件:

  - **スコープ:** デリバリーグループ、マルチセッションOSスコープ
  - **しきい値:** 警告 - 1、危険 - 2

失敗したマシン (単位: %)

デリバリーグループ内の失敗したシングルセッションおよびマルチセッションOSマシンの割合で、失敗したマシンの数に基づいて計算されます。このアラート条件を使用すると、デリバリーグループ内の失敗したマシンの割合としてアラートしきい値を構成でき、30秒ごとに計算されます。Directorダッシュボードおよびフィルタービューに示されているように、さまざまな理由で障害が

発生する可能性があります。Citrix Scout診断を実行して、根本原因を特定してください。詳細については、「ユーザーの問題のトラブルシューティング」を参照してください。

電源オンアクションの失敗と電源オフアクションの失敗

デリバリーグループ内の電源オンアクションの失敗数と電源オフアクションの失敗数で、電源オンまたはオフに失敗した**電源管理対象マシン**の数に基づいて計算されます。このアラート条件を使用すると、デリバリーグループ内で電源オンまたはオフに失敗した**電源管理対象マシン**の数としてアラートしきい値を構成でき、30分ごとに計算されます。

管理者は、高度なアラートポリシーでこれらのアラートに対して次のパラメーターを構成できます。

- トリガー元: 電源アクションをトリガーしたもの
- 失敗の理由: アクションが失敗した理由
- しきい値: ポリシーをトリガーするために電源アクションに失敗したマシンのしきい値の数
- サンプリング間隔: 失敗した電源アクションを確認する間隔
- 再アラート間隔: アラートを再送信するまでの時間

Directorダッシュボードおよびフィルタービューに示されているように、さまざまな理由で障害が発生する可能性があります。Citrix Scout診断を実行して、根本原因を特定してください。詳細については、「ユーザーの問題のトラブルシューティング」を参照してください。

未登録のマシン (単位: %)

マシンが再起動によって不安定になった場合、またはデリバリーコントローラーと仮想マシンの間で通信の問題が発生した場合、マシンは未登録と見なされます。**未登録のマシン (単位: %)** は、デリバリーグループ内の未登録のシングルセッションおよびマルチセッションOSマシンの割合で、未登録のマシンの数に基づいて計算されます。このアラート条件を使用すると、デリバリーグループ内の未登録のマシンの割合として警告および危険のしきい値を構成できます。再アラートの間隔を設定できます。また、**未登録のマシン (単位: %)** の条件が満たされたときに通知を受け取るためにメールを追加することもできます。危険または警告のしきい値を超えると、アラートとメールが生成されます。アラートは**Citrix Alerts**で確認できます。**未登録のマシン (単位: %)** カテゴリで、必要な状態と時間でフィルターできます。

メールがある場合はCSV添付ファイルで、Webhookがある場合はJSONペイロードを通じてアラートの詳細を受け取ることもできます。

> **注:**

> 致命的な値は警告値よりも大きくなければなりません。

> **ポリシー条件:**

- **範囲**: シングルセッションOS、およびマルチセッションOSデリバリーグループ
- **しきい値**: 警告と致命的

マシン稼働時間アラート

デリバリーグループ内のマシンの稼働時間は、デリバリーグループ内で電源がオンになっているマシンについて、1日あたりの時間数、1週間あたりの時間数、または1か月あたりの時間数に基づいて計算されます。このアラート条件を使用すると、デリバリーグループ内でマシンがオンになっている時間としてアラートしきい値を構成できます。マシンの稼働時間アラートは、次の場合に次のように機能します。

- 1日あたりの時間数 - マシンが1日あたりにオンになっている時間数を指定でき、30分ごとに計算されます。設定できる1日あたりの最大時間数は24時間です。
- 1週間あたりの時間数 - マシンが1週間あたりにオンになっている時間数を指定でき、6時間ごとに計算されます。設定できる1週間あたりの最大時間数は168時間です。
- 1か月あたりの時間数 - マシンが1か月あたりにオンになっている時間数を指定でき、毎日1回計算されます。1か月あたりの最大時間数は720時間です。 設定できる再アラート間隔の最小値は60分です。警告および致命的アラートセクションで、マシンの稼働時間のしきい値を超過するマシンの数を入力できます。また、任意のマシンに対して例外を追加することもできます。

たとえば、このアラートに5つのデリバリーグループが追加されており、最初のデリバリーグループと4番目のデリバリーグループで、マシンの数が警告または致命的なしきい値を超過した場合、アラートは最初のデリバリーグループと4番目のデリバリーグループに対して個別にトリガーされます。

このアラートは、管理者がマシンの稼働時間を分析するのに役立ち、この分析に基づいて、管理者はコストの最適化に役立てることができます。メールがある場合はCSV添付ファイルでアラートの詳細を受け取ることも、Webhookがある場合はJSONペイロードを介して受け取ることもできます。

平均ログオン時間

過去1時間に発生したログオンの平均ログオン時間。

- ログオン時間に関する最新のメトリックを取得するには、Directorダッシュボードを確認してください。短期間に多くのユーザーがログインすると、ログオン時間が増加する可能性があります。

- ログオンのベースラインと内訳を確認して、原因を絞り込みます。詳細については、「ユーザーログオンの問題の診断」を参照してください。

  スマートポリシー条件:

  - **スコープ:** デリバリーグループ、マルチセッションOSスコープ
  - **しきい値:** 警告 - 45秒、重大 - 60秒

ログオン期間 (ユーザー)

過去1時間に発生した、指定されたユーザーのログオンのログオン時間。

ロード評価インデックス

過去5分間のロード評価インデックスの値。

- ピーク負荷 (最大負荷) が発生している可能性のあるマルチセッションOSマシンについてDirectorを確認します。ダッシュボード (障害) とトレンドのロード評価インデックスレポートの両方を表示します。

  スマートポリシーの条件:

  - **スコープ:** デリバリーグループ、マルチセッションOSスコープ
  - **しきい値:** 警告 - 80%、重大 - 90%

Webhookでアラートポリシーを構成する

メール通知とは別に、Webhookでアラートポリシーを構成できます。

注: この機能には、Delivery Controller バージョン 7.11 以降が必要です。

PowerShell コマンドレットを使用して、HTTP コールバックまたは HTTP POST でアラートポリシーを構成できます。これらは Webhook をサポートするように拡張されています。

新しいOctobluワークフローの作成と、対応するWebhook URLの取得については、Octoblu Developer Hubを参照してください。

新しいアラートポリシーまたは既存のポリシーの Webhook URL を構成するには、次の PowerShell コマンドレットを使用します。

Webhook URLを使用して新しいアラートポリシーを作成します:

```
$policy = New-MonitorNotificationPolicy -Name <Policy name> -Description
<Policy description> -Enabled $true -Webhook <Webhook URL>
```

既存のアラートポリシーに Webhook URL を追加する:

```
Set-MonitorNotificationPolicy - Uid <Policy id> -Webhook <Webhook URL>
```

PowerShellコマンドのヘルプについては、PowerShellヘルプを使用してください。例:

```
Get-Help  <Set-MonitorNotificationPolicy>
```

アラートポリシーから生成された通知は、Webhook URL への POST 呼び出しで Webhook をトリガーします。POST メッセージには、JSON 形式の通知情報が含まれています。

```
{"NotificationId" : \<Notification Id\>,


"Target" : \<Notification Target Id\>,


"Condition" : \<Condition that was violated\>,


"Value" : \<Threshold value for the Condition\>,


"Timestamp": \<Time in UTC when notification was generated\>,


"PolicyName": \<Name of the Alert policy\>,


"Description": \<Description of the Alert policy\>,


"Scope" : \<Scope of the Alert policy\>,
```

```
"NotificationState": \<Notification state critical, warning, healthy or
dismissed\>,



"Site" : \<Site name\>}
```

アラートの一括解除

この機能は、管理者向けのアラート管理プロセスを最適化し、柔軟性を提供し、アラート疲労を軽減します。管理者は、時間、種類、またはカテゴリに基づいてアラートを一括で解除でき、メンテナンス中やハイパーバイザーおよびその他の環境を扱う際のアラート管理を簡素化します。

アラートの一括解除は、管理者がワークロードを効率的に管理し、大量のアラートに圧倒されるのを防ぐのに役立ちます。

アラートを一括解除する手順

1. **アラート** > **Citrixアラート**タブに移動します。アラートが表示されます。

   「一括アラート」(/en-us/citrix-virtual-apps-desktops/2503/media/bulk-alert.png)
2. **ソース**、**カテゴリ**、**状態**、または**期間**からオプションを選択して、解除したいアラートをフィルタリングします。特定のアラートが表示されます。
3. 特定のアラートの横にあるチェックボックスを選択するか、上部にあるチェックボックスを選択してすべてのアラートを選択します。
4. **解除**をクリックします。アラートの解除を確認する通知が表示されます。
5. **はい**をクリックします。選択されたアラートは*解除済み*としてマークされ、アラートのステータスがそれに応じて更新されます。

PowerShell SDK を使用した Webhook の構成

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

注：

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

> 最新のペイロード形式は次のとおりです。

```
{"text": "This is a message from a Webex incoming webhook."}
```

Webhookを作成する

Webhook プロファイルを作成するには、次のサンプル PowerShell コマンドを使用できます。

承認ヘッダーなしで Webhook を作成するには：

```
$headers = [System.Collections.Generic.Dictionary[string,string]]::new()


$headers.Add("Content-Type", "application/json")


$payloads = '{ "text": "$PAYLOAD" }'


$url = "<Fill this field with the required URL>"


Add-MonitorWebhookProfile -Name "profile_slack" -Description "webhook
profile for slack" -Url $url -Headers $headers -PayloadFormat $payloads
```

承認ヘッダー付きで Webhook を作成するには：

```
$headers = [System.Collections.Generic.Dictionary[string,string]]::new()


$headers.Add("Content-Type", "application/json")
```

```
$headers.Add("Authorization", "Basic <Fill this field with the
authorization token>")



$payloads = '{ "text": "$PAYLOAD" }'



$url = "<Fill this field with the required URL>"



Add-MonitorWebhookProfile -Name "profile_azure" -Description "webhook
profile for azure function with Authentication" -Url $url -Headers
$headers -PayloadFormat $payloads
```

プロファイルが作成されたら、データベースで確認できます。また、新しく作成されたWebhookプロファイルは、**Citrix Alerts**ページで見つけることができます。

Webhook プロファイル(/en-us/citrix-virtual-apps-desktops/2503/media/webhook-profile.png)

Webhookプロファイルを更新する

Webhook プロファイルを更新するには、次のサンプル PowerShell コマンドを使用できます。

```
$headers = [System.Collections.Generic.Dictionary[string,string]]::new()



$headers.Add("Content-Type", "application/json")



$payloads = '{ "text": "$PAYLOAD" }'



$url =  "<Fill this field with the required URL>"



Set-MonitorWebhookProfile -Uid 1  -Name "profile_slack_citrix"
```

```
-Description "webhook profile for citrix slack" -Url $url -Headers
$headers -PayloadFormat $payloads
```

すべてのWebhookプロファイルの一覧を取得する

利用可能なすべてのWebhookプロファイルの一覧を取得するには、以下のPowerShellコマンドのサンプルを使用できます。

```
Get-MonitorWebhookProfile



Get-MonitorWebhookProfile -Name 'profile_msteams'



Get-MonitorWebhookProfile -Uid 1
```

Webhookプロファイルを削除する

Webhookプロファイルを削除するには、以下のPowerShellコマンドのサンプルを使用できます。

```
Remove-MonitorWebhookProfile -Uid 1
```

注:

Webhookプロファイルがいずれかのポリシーにマッピングされている場合、削除できません。回避策として、まずポリシーからWebhookマッピングを削除する必要があります。

Webhookプロファイルを含むポリシーを作成する

Webhookプロファイルを含むポリシーを作成するには、以下のPowerShellコマンドのサンプルを使用できます。

```
New-MonitorNotificationPolicy -Name "Policy1" -Description "Policy
Description" -Enabled $true -WebhookProfileId 1
```

Webhookプロファイルを含むポリシーを更新する

Webhookプロファイルを含むポリシーを更新するには、以下のPowerShellコマンドのサンプルを使用できます。

```
$Policy = Set-MonitorNotificationPolicy -Uid 1 -WebhookProfileId 1
```

ポリシーからWebhookマッピングを削除する

ポリシーからWebhookプロファイルを削除するには、以下のPowerShellコマンドのサンプルを使用できます。

```
$Policy = Set-MonitorNotificationPolicy -Uid 1 -WebhookProfileId 0
```

Webhookプロファイルをテストする

Webhookプロファイルをテストするには、以下のPowerShellコマンドのサンプルを使用できます。

```
$headers = [System.Collections.Generic.Dictionary[string,string]]::new()



$headers.Add("Content-Type", "application/json")



$headers.Add("Authorization", "Basic <Fill this with authorization
token>")



$payloads = '{ "text": "$PAYLOAD" }'



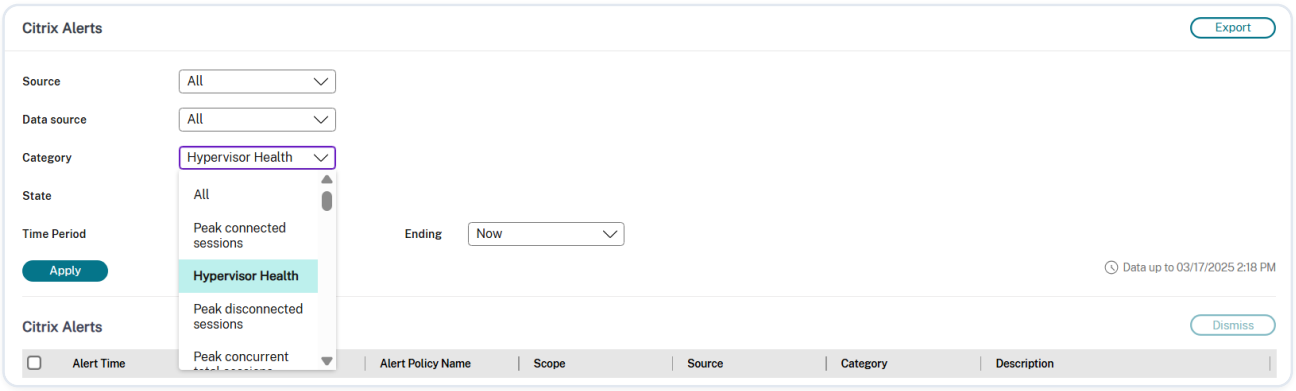
$url ="<Fill this field with the required URL>"



Test-MonitorWebhookProfile -Url $url -Headers $headers -PayloadFormat
$payloads
```

ハイパーバイザーアラートの監視

Directorは、ハイパーバイザーの健全性を監視するためのアラートを表示します。XenServer®およびVMware vSphereからのアラートは、ハイパーバイザーのパラメーターと状態の監視に役立ちます。ハイパーバイザーへの接続ステータスも監視され、ホストのクラスターまたはプールが再起動されたり、利用できなくなったりした場合にアラートが提供されます。



ハイパーバイザーアラートを受信するには、Web Studioでホスティング接続が作成されていることを確認してください。詳細については、「接続とリソース」を参照してください。ハイパーバイザーアラートについては、これらの接続のみが監視されます。

これらのアラートは、しきい値に達するか超えると表示されます。ハイパーバイザーアラートは次のいずれかです。

- 致命的 — ハイパーバイザーアラームポリシーの致命的なしきい値に達したか、超えた場合
- 警告 — ハイパーバイザーアラームポリシーの警告しきい値に達したか、超えた場合
- 却下済み — アラートがアクティブなアラートとして表示されなくなった場合

ハイパーバイザーアラートの表示(/en-us/citrix-virtual-apps-desktops/2503/media/hypervisor_alerts_display.png)

この機能には、Delivery Controllerバージョン7 1811以降が必要です。サイト7 1811以降で古いバージョンのDirectorを使用している場合、ハイパーバイザーアラートの数のみが表示されます。アラートを表示するには、Directorをアップグレードする必要があります。

次の表は、ハイパーバイザーアラートのさまざまなパラメーターと状態について説明しています。

アラート	サポートされているハイパーバイザー	トリガー元	条件	構成
CPU使用率	ゼノサーバー、ヴイエムウェア ブイスフィア	ハイパーバイザー	CPU使用率アラートのしきい	アラートのしきい値はハイパーバイザーで構成

アラート	サポートされているハイパーバイザー	トリガー元	条件	構成
			値に達したか、超えました	する必要があります。
メモリ使用率	ゼノサーバー、ヴイエムウェア ブイスフィア	ハイパーバイザー	メモリ使用率アラートのしきい値に達したか、超えました	アラートのしきい値はハイパーバイザーで構成する必要があります。
ネットワーク使用率	ゼノサーバー、ヴイエムウェア ブイスフィア	ハイパーバイザー	ネットワーク使用率アラートのしきい値に達したか、超えました	アラートのしきい値はハイパーバイザーで構成する必要があります。
ディスク使用量	ヴイエムウェア vSphere	ハイパーバイザー	ディスク使用量アラートのしきい値に達したか、超過しました	アラートのしきい値はハイパーバイザーで構成する必要があります。
ホスト接続または電源状態	ヴイエムウェア vSphere	ハイパーバイザー	ハイパーバイザーホストが再起動されたか、利用できません	アラートは VMware vSphereに組み込まれています。追加の構成は不要です。
ハイパーバイザー接続が利用できません	ゼンサーバー、ヴイエムウェア vSphere	デリバリーコントローラー	ハイパーバイザー（プールまたはクラスター）への接続が失われたか、電源がオフになったか、再起動されました。このアラートは、接続が利用できない間、1	アラートはデリバリーコントローラーに組み込まれています。追加の構成は不要です。

アラート	サポートされているハイパーバイザー	トリガー元	条件	構成
			時間ごとに生成されます。	

注:

アラートの設定に関する詳細については、Citrix XenCenter Alerts を参照するか、VMware vCenter Alerts のドキュメントを確認してください。

メール通知設定は、**Citrix Alerts Policy > Site Policy > Hypervisor Health** で構成できます。ハイパーバイザーアラートポリシーのしきい値条件は、Director からではなく、ハイパーバイザーからのみ構成、編集、無効化、または削除できます。ただし、メール設定の変更やアラートの解除は Director で行うことができます。役割にインフラストラクチャの監視が含まれていない場合は、アラートを無効にできます。

重要:

- ハイパーバイザーによってトリガーされたアラートは、Director で取得および表示されます。ただし、ハイパーバイザーアラートのライフサイクル/状態の変更は Director には反映されません。
- ハイパーバイザーコンソールで正常、解除、または無効化されたアラートは、Director に表示され続け、明示的に解除する必要があります。
- Director で解除されたアラートは、ハイパーバイザーコンソールでは自動的に解除されません。

アプリケーション使用状況の監視

Citrix Directorは、以下の使用状況を監視するのに役立ちます。

- 仮想デスクトップセッション内で起動されたアプリケーション（ローカルアプリケーションとも呼ばれます）

- Citrix Workspace™アプリセッションから直接起動されたアプリケーション（公開アプリケーションとも呼ばれます）

アプリケーション使用状況レポートは、最も使用されているアプリケーション、ほとんど使用されていないアプリケーション、および使用されていないアプリケーションを可視化します。最も使用されているアプリケーションはダッシュボードに表示され、厳選されたグラフが含まれています。これらのグラフは、IT管理者またはアプリケーション管理者が、どのアプリケーションが頻繁に使用されているか、およびその使用状況の程度を把握するのに役立ちます。

注:

- この機能は、プラチナライセンスサイトでのみ利用できます。
- ローカルアプリケーションの使用状況を監視するには、uberAgentをDirectorと統合する必要があります。詳細については、「Citrix uberAgentとDirectorの統合」を参照してください。
- 環境で同じアプリケーションが公開アプリとデスクトップ内にインストールされたアプリ（ローカルアプリ）の両方として提供されている場合、そのアプリが公開アプリレポートとローカルアプリレポートの両方に表示されることがあります。

この機能を使用すると、管理者はどのローカルアプリケーションと公開アプリケーションが最も使用されているかを確認できます。このデータを使用して、管理者は使用状況の程度をさらに深く掘り下げることができます。管理者は、過去24時間の人気アプリの詳細を次のデータポイントで分析できます。

- アプリケーションの総数 - 企業のサイトのすべてのユーザーが使用しているアプリケーションの総数を特定します。
- 個別ユーザー数による最も使用されているアプリケーション - ユニークユーザーの総数による上位10アプリを特定します。
- アプリケーション起動総数による最も使用されているアプリケーション - アプリケーション起動総数に基づいた上位10アプリを特定します。
- ピーク時の同時実行アプリインスタンス数 - 各アプリケーションの使用状況における同時インスタンスの最大数に基づいた上位10アプリを特定します。この情報は、リストされているアプリケーションの最大需要を示します。

このグラフはダッシュボードページの下部に表示されます。ただし、画面上部の をクリックすると、グラフに直接アクセスできます。

アプリケーション監視(/en-us/citrix-virtual-apps-desktops/2503/media/application-monitoring.png)

単一のアプリの詳細を表示するには、**すべてのアプリの使用状況を表示**をクリックすることもできます。このリンクをクリックすると、**トレンド** > **キャパシティ管理** > **ホストされているアプリケーションの使用状況**ページが開きます。

このグラフは、アプリの使用状況を視覚的に表現したものです。また、グラフにカーソルを合わせると、選択したデータポイントの絶対数が表示されます。グラフ上の任意のデータポイントをクリックすると、特定のアプリ名が選択された状態で**トレンド** > **キャパシティ管理** > **ホストされているアプリケーションの使用状況**ページが開きます。このデータは、企業のシステムに存在するすべてのアプリに対する比較値を示すものです。データポイントの絶対値も、同じホバーで個別に表示されます。

使用頻度の低いアプリと未使用アプリのレポート

大規模なCitrix Virtual Apps and Desktops™環境では、利用率の低いアプリケーションが多数存在することがよくあります。環境を最適化するために、**アプリケーション**ページでは、組織内のアプリケーション使用パターンを理解し、データに基づいた意思決定を行ってリソース割り当てとコスト削減を改善するのに役立つ追加のメトリックが提供されるようになりました。

主な機能

- **詳細な使用状況情報:** 各アプリケーションの個別ユーザー数（過去30日間）、合計起動回数、同時実行インスタンスのピーク数、および経時的な個別ユーザー数の傾向グラフを表示します。
- **データの焦点:** 過去7日間、30日間、または90日間のアプリケーション使用パターンを分析して、アプリケーションの必要性を評価します。90日間のデータを表示することをお勧めします。これにより、四半期分のデータが提供され、アプリケーションの使用状況が変動するか、一貫しているかを観察できます。X軸の日付は、組織のイベントと使用状況の傾向を関連付け、低下が予想されたものかどうかを判断するのに役立ちます。このデータにより、管理者は不要なアプリケーションを排除して効率的な環境を維持できます。
- **最適化:** 公開されているアプリの総数、使用頻度の低いアプリ、未使用のアプリを特定して、Citrix展開を最適化します。
- **実用的なデータ:** アプリケーション管理を支援するデータに基づいた意思決定を行い、リソース割り当てとライセンス管理を最適化します。
- **データのエクスポート:** 詳細な分析のために、データをPDFまたはCSV形式でエクスポートします。アプリケーションの使用状況を使用して、Power BI統合またはODATAクエリを使用してデータをエクスポートすることもできます。

要件

- Delivery Controller バージョン 7.16 以降
- VDA バージョン 7.15 以降

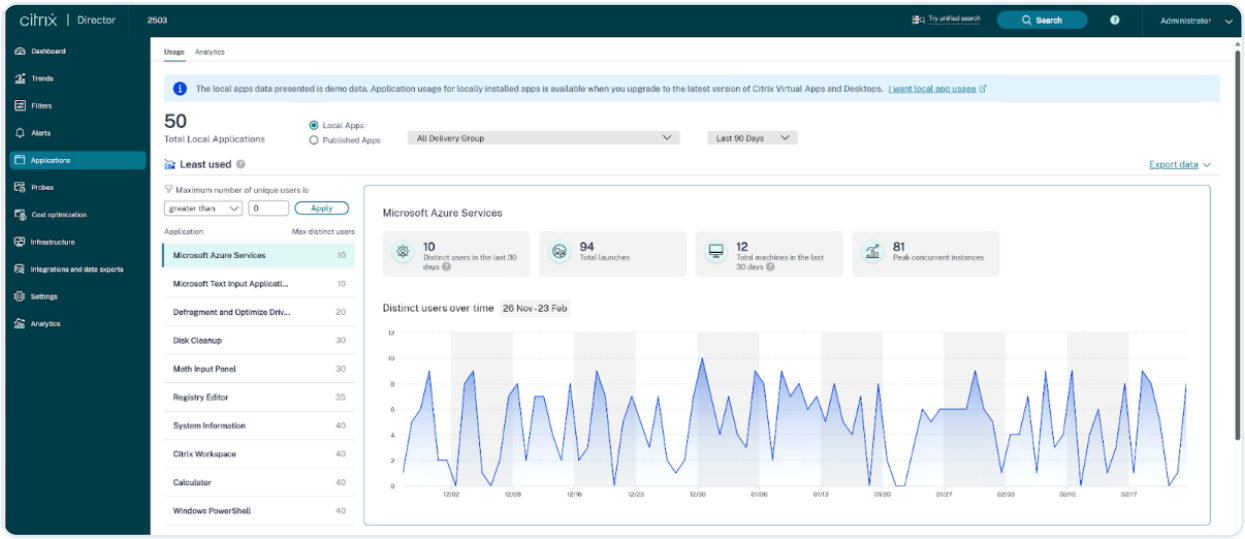
アプリケーション使用状況の詳細の表示

1. ダッシュボードの**使用頻度の低いアプリのレビュー**セクションにある**アプリの表示**リンクをクリックします。

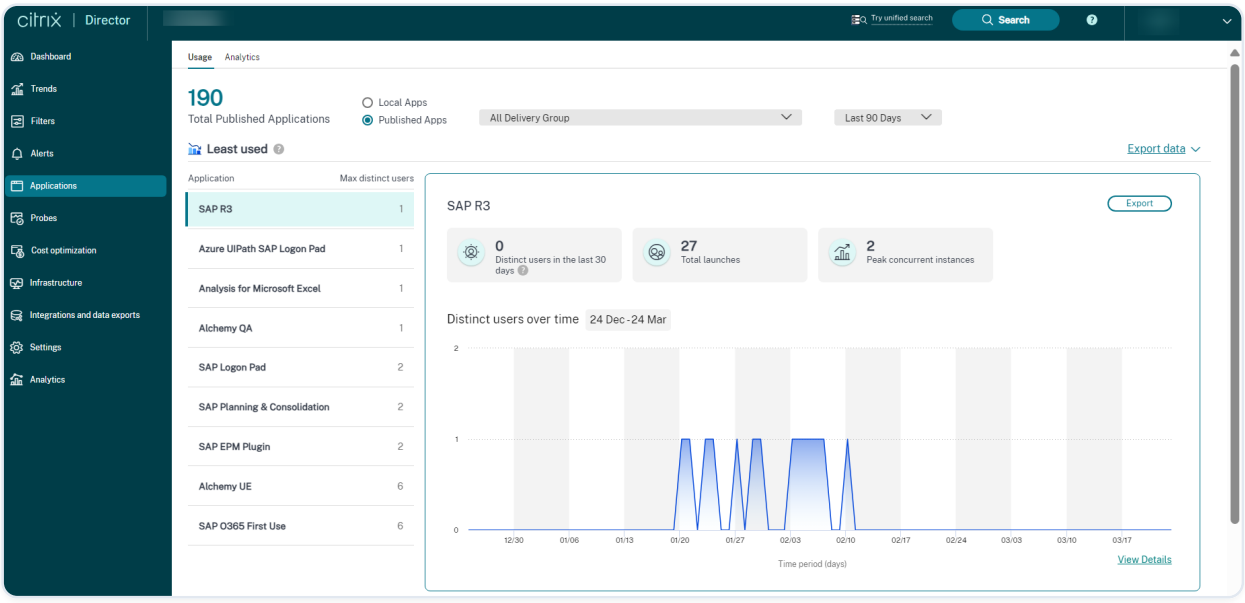
   または、,

   アプリケーションタブをクリックします。次のページが表示されます。

   ローカルアプリオプションが選択されている場合:



   公開アプリオプションが選択されている場合:



2. 目的のデリバリーグループを選択します。

3. 必要な期間を選択します。(注: 最適な分析のため、デフォルトは過去90日間です。)

   次の情報が表示されます。

   - **ローカルおよび公開アプリケーションの合計:** ローカルおよび公開アプリケーションの合計数を表示します。
   - **使用頻度の低いもの:** 選択した期間で、一意のユーザーが最も少ないアプリを表示します。計算は次のように行われます。

     a. **1日のユーザー数:** 各アプリの一意のユーザー数が毎日カウントされます。

     b. **1日のピーク使用量:** 各アプリの1日のユーザー数の最高値が特定されます。

     c. **全体で最も高い使用量:** 選択した期間における各アプリのユーザー数の最高値が決定されます。

     d. **昇順:** アプリは、最も低いユーザー数のアプリから始まり、最も高い全体ユーザー数に基づいて昇順でリストされます。

     > **注:**
     >
     > 分析期間として過去90日間を選択することをお勧めします。この期間は四半期分のデータを提供し、アプリの使用パターンを包括的に把握できます。ただし、7日間および1か月でフィルタリングするオプションも利用できます。

   - **未使用:** 過去90日間に一度も起動されていないアプリケーションが一覧表示されます。それらが配信されたデリバリーグループ、アプリのバージョン、および最終使用の正確なタイムスタンプが提供されます。この情報は、管理者が仮想デスクトップからアプリケーションを削除する前に、情報に基づいた意思決定を行うのに役立ちます。

     「アプリケーション」タブ - 未使用(/en-us/citrix-virtual-apps-desktops/2503/media/dir-app-analytics-not-used.png)

4. **最も使用頻度の低い**カテゴリからアプリを選択して、次のような詳細な使用状況情報を表示します。

   - **過去30日間のユニークユーザー数:** 過去30日間にアプリにアクセスしたユニークユーザーの数を表示します。7日間でフィルタリングした場合、このメトリックは、選択したアプリのその7日間のユニークユーザー数を表示します。

   > **注:**

> 90日を選択した場合でも、このメトリックは過去30日間のデータのみを表示します。

- **合計起動回数:** アプリが起動された回数を表示します。
- **過去30日間の合計マシン数:** 過去30日間にインストールされたマシンの数を表示します。このメトリックは、ローカルアプリの詳細を表示する場合にのみ表示されます。
- **ピーク同時実行インスタンス数:** 同時に実行されているインスタンスの最大数を表示します。
- **トレンドチャート:** 選択したアプリの経時的なユニークユーザー数を示すトレンドチャートを表示します。**詳細を表示**をクリックすると、**キャパシティ管理 > ホストされたアプリケーションの使用状況**セクションで詳細情報が表示されます。

トレンドチャートの使用方法

トレンドチャートは使用パターンを示し、選択した期間における傾向や使用量の低い期間または高い期間を特定するのに役立ちます。X軸は日数を表し、Y軸は経時的なユニークユーザー数を表します。これらのメトリックと使用パターングラフを分析することで、管理者はCitrix Virtual Apps and Desktops環境を自信を持って最適化できます。

トレンドチャートは以下の方法で使用できます。

- **データポイントにカーソルを合わせる:** 選択した期間の個別のユーザー数を表示します。
- **トレンドを表示する:** 使用パターンを特定し、アプリの使用状況が一貫しているか、一時的な急増に過ぎないかを判断します。このチャートは、管理者が従業員の活動を監視し、潜在的な問題や改善領域を特定するのに役立ちます。たとえば、従業員が休暇を取ると、その期間はアプリケーションの使用がない場合があります。従業員が戻ると、アプリケーションの使用が増加します。期間のデフォルトフィルターは90日間であり、管理者がこれらの計算を行うのに役立ちます。
- **詳細を表示する:** 日付と対応する個別のユーザー数を表示します。
- **フィルターオプション:** 異なる「期間」フィルターオプションを選択して、対応するデータを表示します。

サイト全体の履歴トレンドを監視する

トレンドビューでは、各サイトの履歴トレンド情報に以下のパラメーターでアクセスできます。

- セッション
- 接続障害

- マシン障害
- ログオンパフォーマンス
- 負荷評価
- キャパシティ管理
- マシン使用状況
- リソース使用率
- 各サイトのネットワーク分析。

この情報を見つけるには、**トレンド**メニューをクリックします。

ズームインしてドリルダウンする機能を使用すると、期間をズームイン（グラフのデータポイントをクリック）し、トレンドに関連する詳細をドリルダウンして表示することで、トレンドチャートをナビゲートできます。この機能により、誰が、または何が影響を受けているかの詳細をよりよく理解できます。

各グラフのデフォルトのスコープを変更するには、データに別のフィルターを適用します。

履歴トレンド情報が必要な期間を選択します。期間の利用可能性は、Directorの展開によって次のように異なります。

- 過去1年間（365日間）のトレンドレポートは、Premiumライセンスサイトで利用できます。
- 過去1か月間（31日間）のトレンドレポートは、Advancedライセンスサイトで利用できます。
- PremiumおよびAdvanced以外のライセンスサイトでは、過去7日間のトレンドレポートが利用できます。

> **注：**
>
> - すべてのDirector展開において、期間が「過去1か月間」（**現在まで**）またはそれより短い期間に設定されている場合、セッション、障害、ログオンパフォーマンスのトレンド情報はグラフおよびテーブルとして利用できます。終了日をカスタム設定した「過去1か月間」または「過去1年間」の期間を選択した場合、トレンド情報はグラフとして利用でき、テーブルとしては利用できません。
> - Monitor Serviceのグルーミング保持値は、トレンドデータの可用性を制御します。デフォルト値は、データ粒度と保持で確認できます。Premiumライセンスサイトのお客様は、グルーミング保持を希望する保持日数に変更できます。

- IIS Managerの以下のパラメーターは、選択可能なカスタム終了日の範囲を制御します。ただし、選択された日付のデータ可用性は、測定対象の特定のメトリックに対するグルーミング保持設定によって異なります。

パラメーター	デフォルト値
UI.TrendsLast2HoursRange	3
UI.TrendsLast24HoursRange	32
UI.TrendsLast7DaysRange	32
UI.TrendsLastMonthRange	365

利用可能な傾向

セッションの傾向を表示: セッションタブから、デリバリーグループと期間を選択して、同時セッション数に関する詳細情報を表示します。

セッションの自動再接続列には、セッション内の自動再接続の数が表示されます。セッションの信頼性ポリシーまたは自動クライアント再接続ポリシーが有効な場合、自動再接続が有効になります。エンドポイントでネットワークの中断が発生すると、次のポリシーが有効になります。

- セッションの信頼性が有効になり（デフォルトで3分間）、Citrix Receiver™またはCitrix Workspace™アプリがVDAへの接続を試行します。
- 自動クライアント再接続が3分から5分の間に有効になり、クライアントがVDAへの接続を試行します。

両方の再接続がキャプチャされ、ユーザーに表示されます。この情報は、再接続が発生してからDirector UIに表示されるまでに最大5分かかる場合があります。

自動再接続情報は、中断のあるネットワーク接続の表示とトラブルシューティングに役立ちます。また、シームレスなエクスペリエンスを持つネットワークも分析します。フィルターで選択した特定のデリバリーグループまたは期間の再接続数を表示できます。ドリルダウンでは、セッションの信頼性または自動クライアント再接続、タイムスタンプ、エンドポイントIP、およびWorkspaceアプリがインストールされているマシンのエンドポイント名などの追加情報が提供されます。

デフォルトでは、ログはイベントのタイムスタンプの降順でソートされます。この機能は、Windows向けCitrix Workspaceアプリ、Mac向けCitrix Workspaceアプリ、Windows向けCitrix Receiver、およびMac向けCitrix Receiverで利用できます。この機能には、Delivery Controller™ バージョン7 1906以降、およびVDA 1906以降が必要です。

セッションの再接続の詳細については、「セッション」を参照してください。

ポリシーの詳細については、「クライアント自動再接続ポリシー設定」および「セッションの信頼性ポリシー設定」を参照してください。

自動再接続データがDirectorに表示されない場合があります。その理由は次のとおりです。

- WorkspaceアプリがVDAに自動再接続データを送信していません。
- VDAがモニターサービスにデータを送信していません。
- Delivery Controllerは、対応するセッションがない可能性があるため、VDAペイロードを破棄します。

> **注:**
>
> 場合によっては、特定のCitrix Gatewayポリシーが設定されていると、クライアントIPアドレスが正しく取得されないことがあります。

> **接続障害の傾向を表示:** 「障害」タブから、接続、マシンタイプ、障害タイプ、デリバリーグループ、および期間を選択して、サイト全体のユーザー接続障害に関する詳細情報を含むグラフを表示します。

マシン障害の傾向を表示: Single-session OS Machine FailuresタブまたはMulti-session OS Machinesタブから、障害タイプ、デリバリーグループ、および期間を選択すると、サイト全体のマシン障害に関する詳細情報を含むグラフが表示されます。

ログオンパフォーマンスの傾向を表示: ログオンパフォーマンスタブから、デリバリーグループと期間を選択して、サイト全体のユーザーログオン時間とVDAログオン時間の期間、およびログオン数がパフォーマンスに影響するかどうかに関する詳細情報を含むグラフを表示します。このビューには、ブローカリング期間やVM起動時間など、ログオンフェーズとVDA期間フェーズの平均期間も表示されます。このデータは、ユーザーログオンとVDAログオンに特化したものであり、切断されたセッションから再接続しようとしているユーザーは含まれません。 グラフの下の表には、ユーザーセッションごとのログオン期間が表示されます。表示する列を選択し、任意の列でレポートを並べ替えることができます。これらのレポートを.CSVファイルまたはPDFにエク

スポートすることもできます。グラフもこれらのレポートにエクスポートされます。詳細については、ユーザーログオンの問題の診断を参照してください。

負荷評価の傾向を表示: Load Evaluator Indexタブから、Multi-session OSマシン間で分散される負荷に関する詳細情報を含むグラフを表示します。このグラフのフィルターオプションには、デリバリーグループまたはデリバリーグループ内のMulti-session OSマシン、Multi-session OSマシン（デリバリーグループ内のMulti-session OSマシンが選択されている場合にのみ利用可能）、および範囲が含まれます。

ホストされたアプリケーションの使用状況を表示: この機能の利用可能性は、組織のライセンスによって異なります。 **Capacity Management**タブから、**Hosted Applications Usage**タブを選択します。デリバリーグループと期間を選択すると、ピーク時の同時使用状況を示すグラフと、アプリケーションベースの使用状況を示す表が表示されます。Application Based Usage表から、特定のアプリケーションを選択して詳細と、そのアプリケーションを使用している、または使用したユーザーのリストを確認できます。

シングルセッションおよびマルチセッションOSの使用状況を表示: 「傾向」ビューには、サイト別およびデリバリーグループ別のシングルセッションOSの使用状況が表示されます。「**サイト**」を選択すると、デリバリーグループごとの使用状況が表示されます。デリバリーグループを選択すると、ユーザーごとの使用状況が表示されます。 「傾向」ビューには、サイト別、デリバリーグループ別、およびマシン別のマルチセッションOSの使用状況も表示されます。「**サイト**」を選択すると、デリバリーグループごとの使用状況が表示されます。デリバリーグループを選択すると、マシンごとおよびユーザーごとの使用状況が表示されます。マシンが選択されている場合、ユーザーごとの使用状況が表示されます。

仮想マシンの使用状況を表示: 「**マシン使用状況**」タブから、「**シングルセッションOSマシンまたはマルチセッションOSマシン**」を選択して、VM使用状況のリアルタイムビューを取得し、サイトのキャパシティニーズを迅速に評価できるようにします。 シングルセッションOSの可用性 - サイト全体または特定のデリバリーグループの可用性別に、シングルセッションOSマシン（VDI）の現在の状態を表示します。 マルチセッションOSの可用性 - サイト全体または特定のデリバリーグループの可用性別に、マルチセッションOSマシンの現在の状態を表示します。

表示されるバナーの次のリンクをクリックすると、**コスト最適化**によるマシン使用状況の可視性を高めることができます。

- 推定節約額 - このリンクをクリックすると、**コスト最適化**ページの**推定節約額**セクションに移動し、すべてのデリバリーグループの詳細が表示されます。
- 節約レポート - このリンクをクリックすると、**コスト最適化**ページの**節約レポート**セクションに移動し、すべてのデリバリーグループの詳細が表示されます。

注:

「利用可能なカウンター」に表示されるマシンの数には、メンテナンスモードのマシンが含まれます。

「**リソース使用率の表示: リソース使用率**タブから、**シングルセッションOSマシンまたはマルチセッションOSマシン**を選択して、CPUとメモリ使用量、IOPSとディスク待機時間に関する履歴トレンドデータを各VDIマシンについて取得し、より適切なキャパシティプランニングに役立てます。 この機能には、Delivery ControllersおよびVDAs **バージョン7.11**以降が必要です。 グラフには、平均CPU、平均メモリ、平均IOPS、ディスク待機時間、およびピーク時の同時セッションのデータが表示されます。マシンにドリルダウンして、CPUを消費している上位10個のプロセスのデータとグラフを表示できます。」

「デリバリーグループと期間でフィルターします。CPU、メモリ使用量、およびピーク時の同時セッションのグラフは、過去2時間、24時間、7日間、1か月、1年間で利用できます。平均IOPSとディスク待機時間のグラフは、過去24時間、1か月、1年間で利用できます。バナーの**Check out**リンクをクリックすると、コスト最適化によりマシンの使用状況をより詳細に把握できます。このリンクをクリックすると、**コスト最適化**ページの**ワークロードの適正化**タブに移動し、**リソース使用率**タブから選択したデリバリーグループの詳細が表示されます。」.

「**注:**」:

- 「履歴マシン使用率ページの「上位10プロセス」テーブルでデータを収集して表示するには、監視ポリシー設定の**プロセス監視を有効にする**を**許可**に設定する必要があります。このポリシーは、デフォルトで**禁止**に設定されています。すべてのリソース使用率データはデフォルトで収集されます。これは、**リソース監視を有効にする**ポリシー設定を使用して無効にできます。グラフの下のテーブルには、マシンごとのリソース使用率データが表示されます。詳しくは、「監視ポリシー設定」を参照してください。」.
- 「平均IOPSは日次平均を示します。ピークIOPSは、選択した期間のIOPS平均の最高値として計算されます。（IOPS平均とは、VDAで1時間中に収集されたIOPSの時間平均です）。」.
- 「マシンのドリルダウンでは、平均CPUまたは平均メモリ使用量が1%を超えるプロセスが一覧表示されます。これは、場合によっては10個未満のプロセスしか表示されない可能性があることを意味します。」.

> 「**ネットワーク分析データの表示:** この機能の可用性は、組織のライセンスと管理者権限によって異なります。この機能には、Delivery Controllers **バージョン7.11**以降が必要です。」.

「**ネットワーク**タブから、ネットワーク分析を監視します。これにより、ネットワークのユーザー、アプリケーション、およびデスクトップのコンテキストビューが提供されます。この機能により、DirectorはCitrix ADMからのHDX Insightレポートを通じて、展開におけるICAトラフィックの高度な分析を提供します。詳しくは、「ネットワーク分析の構成」を参照してください。」

アプリケーション障害の表示: アプリケーション障害タブには、VDA上の公開アプリケーションに関連する障害が表示されます。

「この機能には、Delivery ControllersおよびVDAs **バージョン7.15**以降が必要です。Windows Vista以降を実行するシングルセッションOS VDA、およびWindows Server 2008以降を実行するマルチセッションOS VDAがサポートされています。 詳しくは、「履歴アプリケーション障害監視」を参照してください。」

デフォルトでは、マルチセッションOS VDAからのアプリケーション障害のみが表示されます。監視ポリシーを使用して、アプリケーション障害の監視を設定できます。詳細については、「監視ポリシー設定」を参照してください。

プローブ結果の表示: プローブ結果タブには、構成ページでプローブ用に構成されたアプリケーションおよびデスクトップのプローブ結果が表示されます。ここでは、障害が発生した起動の段階が記録されます。

詳しくは、「アプリケーションおよびデスクトップのプローブ」を参照してください。

カスタマイズされたレポートの作成: カスタムレポートタブは、監視データベースからリアルタイムおよび履歴データを表形式で含むカスタムレポートを生成するためのユーザーインターフェイスを提供します。

「この機能には、Delivery Controllers **バージョン7.12**以降が必要です。」.

以前に保存したカスタムレポートクエリのリストから、「**実行してダウンロード**」をクリックしてレポートをCSV形式でエクスポートしたり、「**ODataをコピー**」をクリックして対応するODataクエリをコピーして共有したり、「**編集**」をクリックしてクエリを編集したりできます。 マシン、接続、セッション、またはアプリケーションインスタンスに基づいてカスタムレポートクエリを作成できます。マシン、デリバリーグループ、または期間などのフィールドに基づいてフィルター条件を指定します。カスタムレポートに必要な追加の列を指定します。プレビューにはレポートデータのサンプルが表示されます。カスタムレポートクエリを保存すると、保存済みクエリのリストに追加されます。

コピーしたODataクエリに基づいてカスタムレポートクエリを作成できます。これを行うには、「ODataクエリ」オプションを選択し、コピーしたODataクエリを貼り付けます。結果のクエリは後で実行するために保存できます。

> **注:**
>
> ODataクエリを使用して生成されたプレビューおよびエクスポートレポートの列名はローカライズされておらず、英語で表示されます。

> グラフ上のフラグアイコンは、特定の期間における重要なイベントまたはアクションを示します。フラグにマウスを重ねてクリックすると、イベントまたはアクションが一覧表示されます。

> **注:**
>
> - HDX™接続ログオンデータは、7より前のVDAでは収集されません。それより前のVDAの場合、グラフデータは0として表示されます。
> - Citrix Studioで削除されたデリバリーグループは、関連データが整理されるまで、Directorトレンドフィルターで選択できます。削除されたデリバリーグループを選択すると、保持期間までの利用可能なデータのグラフが表示されます。ただし、テーブルにはデータが表示されません。
> - アクティブなセッションを含むマシンをあるデリバリーグループから別のデリバリーグループに移動すると、新しいデリバリーグループの「**リソース使用率と負荷評価インデックス**」テーブルに、古いデリバリーグループと新しいデリバリーグループから統合されたメトリックが表示されます。

Autoscale管理マシンの監視

Autoscaleは、デリバリーグループ内の登録済みすべてのマルチセッションおよびシングルセッションOSマシンのプロアクティブな電源管理を可能にする電源管理機能です。Web Studioで、選択したデリバリーグループのAutoscaleを構成できます。詳しくは、Autoscaleを参照してください。 Directorを使用して、Autoscaleが有効なマシンの主要なメトリックを監視できます。

マシン使用状況

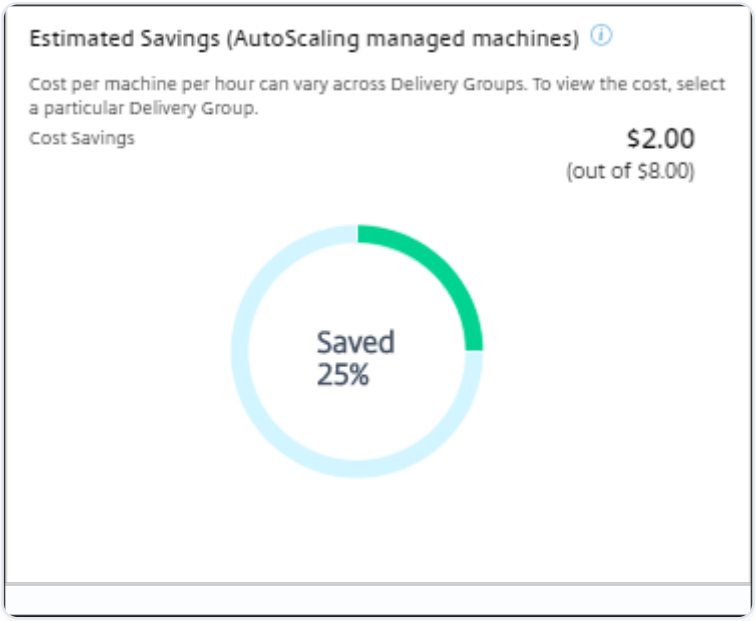
マシン使用状況ページには、選択したデリバリーグループと期間で電源がオンになっているAutoscaleが有効なマルチセッションおよびシングルセッションOSマシンの合計数が表示されます。このメトリックは、デリバリーグループ内のマシンの実際の使用状況を示します。 **シングルセッションOSマシン**タブまたは**マルチセッションOSマシン**タブから、デリバリーグループと期間を選択します。

グラフには次のメトリックが表示されます。

- **電源オンのマシン** - 電源がオンになっているAutoscaleが有効なマシンの数
- **登録済みマシン** - 登録済みのマルチセッションまたはシングルセッションOSマシンの数
- **メンテナンス中のマシン** - メンテナンスモードがオンになっているマルチセッションまたはシングルセッションOSマシンの数

推定節約額

マシン使用状況ページには、選択したデリバリーグループでAutoscaleを有効にすることによって達成された推定コスト削減額も表示されます。



推定節約額は、**デリバリーグループの編集** > **Autoscale**で構成されている、マシンあたりの1時間あたりの節約額（米ドル）の割合として計算されます。マシンあたりの節約額の構成について詳しくは、Autoscaleを参照してください。

すべてのデリバリーグループを選択すると、すべてのデリバリーグループにおける推定節約額の平均値が表示されます。

推定節約額は、管理者が既存のインフラストラクチャを統合し、最大限の節約と利用率を達成するためのキャパシティを計画するのに役立ちます。

マシンとセッションのアラート通知

Directorダッシュボードには、アラート通知が表示されます。これらの通知はさらにドリルダウンできます。アラートの詳細は、**アラート**ページに表示されます。

- デリバリーグループでアラートポリシーを作成するには、**アラート** > **Citrixアラートポリシー** > **デリバリーグループポリシー**に移動します。
- ここで、次の警告および重大なしきい値を設定できます。
  - 失敗したマシン（シングルセッションOS）および失敗したマシン（マルチセッションOS）、,
  - デリバリーグループ内のピーク接続セッション、ピーク切断セッション、およびピーク同時合計セッション。
- デリバリーグループ内の対応するメトリックがしきい値に達すると、アラートが生成されます。

アラートポリシーの条件と新しいアラートポリシーの作成に関する詳細については、「アラートと通知」を参照してください。

マシンのステータス

- **フィルター** > **マシン**には、すべてのマシンの電源状態が表形式で表示されます。特定のデリバリーグループでフィルターできます。
- **フィルター** > **セッション**では、マシン名でフィルターして、関連するセッションとそのリアルタイムステータスを表示します。
- **トレンド** > **セッション**で、デリバリーグループと期間を選択して、セッションとその関連メトリックの傾向を確認します。

詳細については、「障害のトラブルシューティングのためにデータをフィルターする」を参照してください。

負荷評価のトレンド

トレンド > **負荷評価インデックス**ページには、マルチセッションOSマシン間で分散されている負荷に関する詳細情報を含むグラフが表示されます。このグラフのフィルターオプションには、デリバリーグループまたはデリバリーグループ内のマルチセッションOSマシン、マルチセッションOSマシン（デリバリーグループ内のマルチセッションOSマシンが選択されている場合にのみ利用可能）、および範囲が含まれます。負荷評価インデックスは、合計CPU、メモリ、ディスク、またはセッションの割合として表示され、最後の間隔での接続ユーザー数と比較して示されます。

展開のトラブルシューティング

アプリケーションのトラブルシューティング

リアルタイムアプリケーション監視

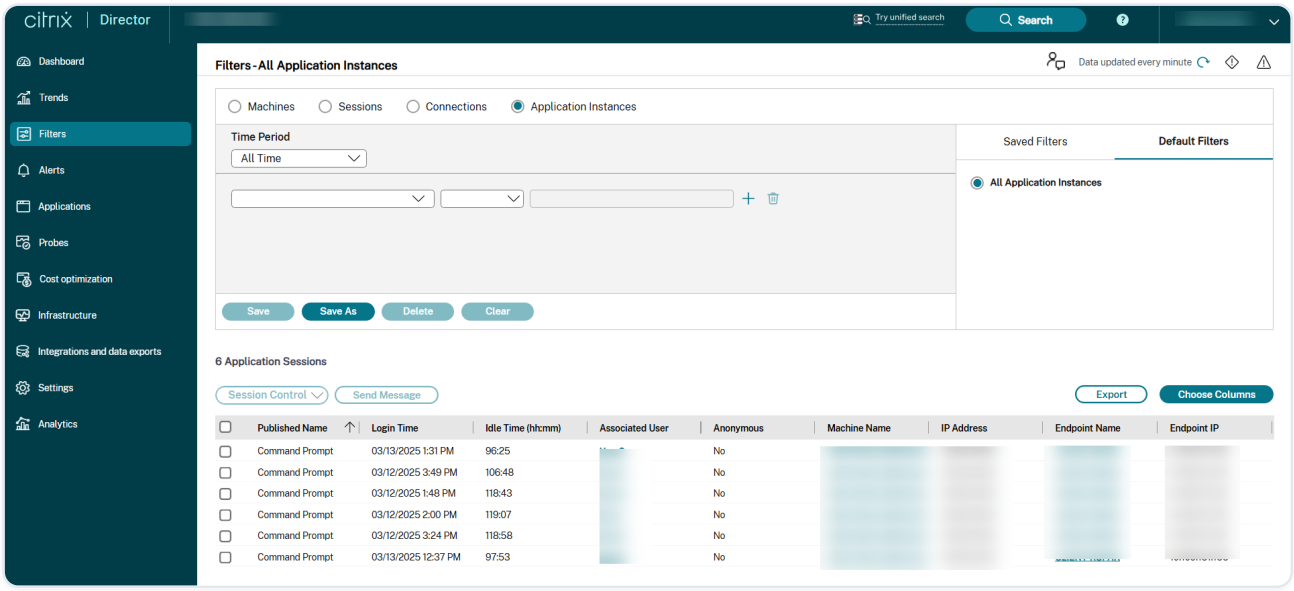
アイドル時間メトリックを使用すると、特定の時間制限を超えてアイドル状態になっているアプリケーションとセッションのインスタンスを特定してトラブルシューティングできます。

アプリケーションベースのトラブルシューティングの典型的なユースケースは、従業員がアプリケーションライセンスを共有する医療分野にあります。そこでは、Citrix Virtual Apps and Desktops™環境をパージしたり、パフォーマンスの低いサーバーを再構成したり、アプリケーションを保守およびアップグレードしたりするために、アイドル状態のセッションとアプリケーションインスタンスを終了する必要があります。

アプリケーションインスタンスフィルターページには、サーバーおよびシングルセッションOSのVDA上のすべてのアプリケーションインスタンスが一覧表示されます。関連するアイドル時間測定値は、少なくとも10分間アイドル状態であったマルチセッションOSのVDA上のアプリケーションインスタンスに対して表示されます。

> **注:**
>
> アプリケーションインスタンスのメトリックは、すべてのライセンスエディションのサイトで利用できます。

この情報を使用して、特定の期間を超えてアイドル状態になっているアプリケーションインスタンスを特定し、必要に応じてログオフまたは切断します。これを行うには、**フィルター\> アプリケーションインスタンス**を選択し、事前に保存されたフィルターを選択するか、**すべてのアプリケーションインスタンス**を選択して独自のフィルターを作成します。

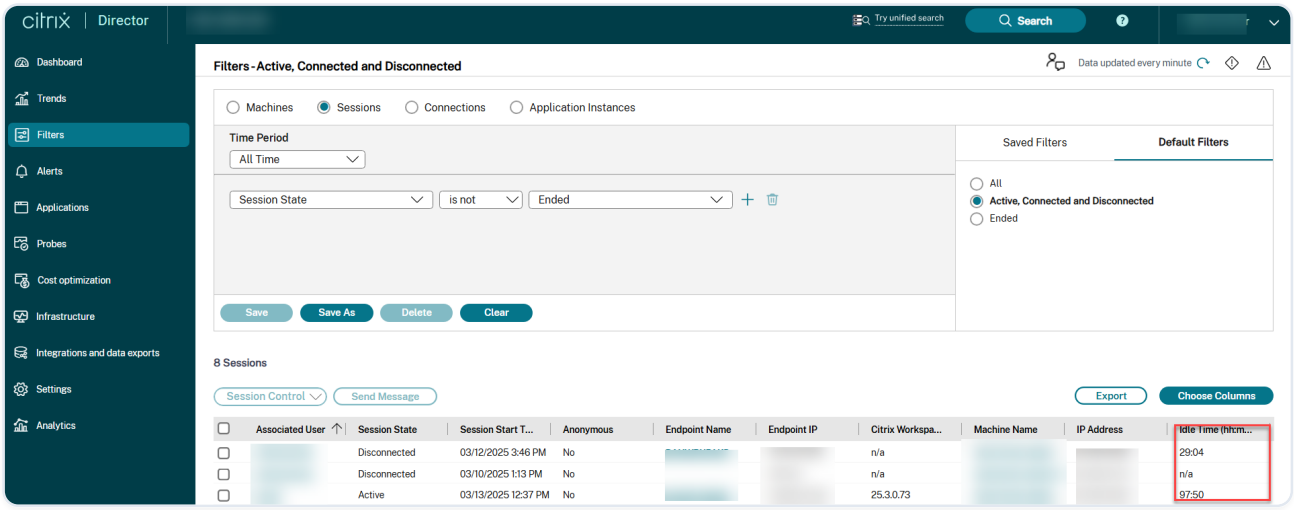


フィルターの例は次のとおりです。**フィルター条件**として、**公開名**（アプリケーションの）と**アイドル時間**を選択します。次に、**アイドル時間**を特定の時間制限**以上**に設定し、再利用のためにフィルターを保存します。フィルターされたリストから、アプリケーションインスタンスを選択します。メッセージを送信するオプションを選択するか、**セッション制御**ドロップダウンから**ログオフ**または**切断**を選択してインスタンスを終了します。

注:

アプリケーションインスタンスをログオフまたは切断すると、現在のセッションがログオフまたは切断され、それにより同じセッションに属するすべてのアプリケーションインスタンスが終了します。

セッションの状態とセッションアイドル時間メトリックを使用して、**セッション**フィルターページからアイドル状態のセッションを特定できます。**アイドル時間**列で並べ替えるか、特定の時間制限を超えてアイドル状態になっているセッションを特定するためのフィルターを定義します。アイドル時間は、少なくとも10分間アイドル状態であったマルチセッションOSのVDA上のセッションに対して一覧表示されます。



セッションまたはアプリケーションインスタンスが次の場合は、**アイドル時間**は**N/A**と表示されます

- 10分以上アイドル状態になっていない場合、,
- シングルセッションOSのVDAで起動されている場合、または
- バージョン7.12以前のVDAで起動されている場合。

アプリケーション障害の履歴監視

トレンド -\> **アプリケーション障害**タブには、VDA上の公開アプリケーションに関連する障害が表示されます。

アプリケーション障害の傾向は、PremiumおよびAdvancedライセンスサイトの場合、過去2時間、24時間、7日間、および1か月間利用できます。その他のライセンスタイプの場合、過去2時間、24時間、7日間利用できます。「Application Errors」をソースとしてイベントビューアーに記録されたアプリケーション障害が監視されます。**エクスポート**をクリックすると、CSV、Excel、またはPDF形式でレポートを生成できます。

アプリケーション障害監視のグルーミング保持設定であるGroomApplicationErrorsRetentionDaysとGroomApplicationFaultsRetentionDaysは、Premiumおよび非Premiumライセンスサイトの両方で、デフォルトで1日に設定されています。この設定は、PowerShellコマンドを使用して変更できます。

```
Set-MonitorConfiguration -\<setting name\> \<value\>
```

アプリケーション障害の傾向(/en-us/citrix-virtual-apps-desktops/2503/media/dir_application_faults.png)

障害は、その重大度に基づいて**アプリケーションフォールト**または**アプリケーションエラー**として表示されます。アプリケーションフォールトタブには、機能またはデータの損失に関連する障害が表示されます。アプリケーションエラーは、すぐには関連しない問題を示します。これらは将来問題を引き起こす可能性のある状態を示します。

公開アプリケーション名、**プロセス名**、**デリバリーグループ**、および**期間**に基づいて障害をフィルターできます。テーブルには、フォールトまたはエラーコードと障害の簡単な説明が表示されます。詳細な障害の説明はツールチップとして表示されます。

> **注:**
>
> 対応するアプリケーション名を特定できない場合、公開アプリケーション名は「不明」と表示されます。これは通常、起動されたアプリケーションがデスクトップセッションで失敗した場合、または依存する実行可能ファイルによって引き起こされた未処理の例外が原因で失敗した場合に発生します。
>
> デフォルトでは、マルチセッションOS VDAでホストされているアプリケーションの障害のみが監視されます。監視グループポリシー（アプリケーション障害の監視を有効にする、シングルセッションOS VDAでのアプリケーション障害の監視を有効にする、障害監視から除外されるアプリケーションのリスト）を通じて監視設定を変更できます。詳細については、監視ポリシー設定のアプリケーション障害監視のポリシーを参照してください。

トレンド \> アプリケーションプローブ結果ページには、過去24時間および7日間にサイトで実行されたアプリケーションプローブの結果が表示されます。アプリケーションプローブの設定方法の詳細については、アプリケーションプロービングを参照してください。

マシンのトラブルシューティング

> **注：**
>
> **Citrix Health Assistant**は、未登録VDAの構成に関する問題をトラブルシューティングするためのツールです。このツールは、VDA登録の失敗、セッション起動、タイムゾーンリダイレクト構成に関する問題の根本原因を特定するために、いくつかのヘルスチェックを自動化します。Knowledge Centerの記事「Citrix Health Assistant - Troubleshoot VDA Registration and Session Launch」には、**Citrix Health Assistant**ツールのダウンロードと使用方法が記載されています。

> Directorコンソールの**フィルター > マシン**ビューには、サイトで構成されているマシンが表示されます。マルチセッションOSマシンタブには、ロード評価インデックスが含まれており、これはパフォーマンスカウンターの分布と、リンクにカーソルを合わせると表示されるセッション数のツールヒントを示します。

失敗したマシンの**失敗理由**列をクリックすると、失敗の詳細な説明と、その失敗をトラブルシューティングするために推奨されるアクションが表示されます。マシンおよび接続の失敗の理由と推奨されるアクションについては、「Citrix Director failure reasons and troubleshooting」を参照してください。

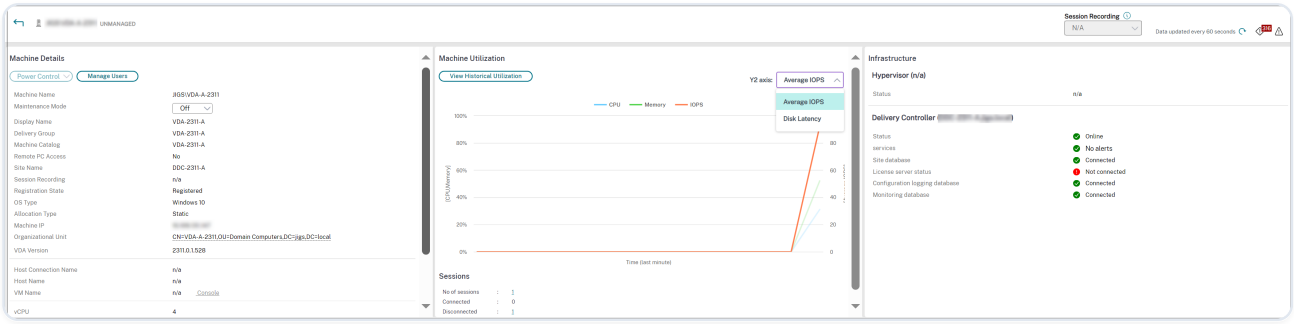
マシン名のリンクをクリックすると、**マシン詳細** ページに移動します。

マシン詳細ページには、マシンの詳細、インフラストラクチャの詳細、およびマシンに適用されたホットフィックスの詳細が一覧表示されます。

マシンベースのリアルタイムリソース使用率

マシン使用率パネルには、CPUとメモリのリアルタイム使用率を示すグラフが表示されます。さらに、Delivery ControllerとVDAのバージョンが**7.14**以降のサイトでは、ディスクおよびGPU監視グラフが利用できます。

ディスク監視グラフ、平均IOPS、ディスク遅延は、VDAディスクに関連する問題を監視およびトラブルシューティングするのに役立つ重要なパフォーマンス測定値です。平均IOPSグラフは、ディスクへの読み取りおよび書き込みの平均数を表示します。**ディスク遅延**を選択すると、データの要求からディスクからの応答までの遅延をミリ秒単位で測定したグラフが表示されます。



GPU使用率

GPU使用率を選択すると、GPU、GPUメモリ、エンコーダー、およびデコーダーのパーセンテージ使用率が表示され、マルチセッションおよびシングルセッションOS VDAでのGPU関連の問題をトラブルシューティングできます。

サポートされているGPUバージョン：

- Display Driverバージョン369.17以降を実行しているNVIDIA Tesla M60 GPU。詳細については、「NVIDIA vGPU Software」を参照してください。
- AMD Radeon Instinct MI25 GPUおよびAMD EPYC 7V12 (Rome) CPU。詳細については、「AMD Drivers and Support」を参照してください。

ドライバー:

適切なドライバーまたは拡張機能をVDAにインストールする必要があります。

- NVIDIA GPUの場合は、GRIDドライバーを手動で、または拡張機能経由でインストールします。詳細については、「NVIDIA vGPU Software」を参照してください。
  - NVIDIAの場合、GRIDドライバーのみがサポートされています。CUDAドライバーはNVadsA10 v5シリーズでは動作せず、サポートされていません。
  - Azureベースのマシンに拡張機能経由でNVIDIA Grid GPUドライバーをインストールするプロセス例については、「NVIDIA GRID drivers. NVIDIA GPU Driver Extension - Azure Windows VMs - Azure Virtual Machines」を参照してください。
  - NVIDIA Grid GPUドライバーを手動でインストールするプロセス例については、「Azure N-series NVIDIA GPU driver setup for Windows - Azure Virtual Machines」を参照してください。
- AMD GPUの場合は、AMDグラフィックドライバーを手動で、または拡張機能経由でインストールします。詳細については、「AMD Drivers and Support」を参照してください。
  - Azureベースのマシンに拡張機能経由でAMD GPUドライバーをインストールするプロセス例については、「AMD GPU Driver Extension - Azure Windows VMs - Azure Virtual Machines」を参照してください。
  - AzureマシンにAMD GPUドライバーを手動でインストールするプロセス例については、「Install AMD GPU drivers on N-series VMs running Windows」を参照してください。

使用上の注意:

- GPU使用率グラフは、64ビットWindowsを実行しているVDAでのみ利用可能です。
- GPUアクセラレーションを提供するには、VDAでHDX 3D Proを有効にする必要があります。詳細については、「GPU acceleration for Windows Single-session OS」および「GPU acceleration for Windows Multi-session OS」を参照してください。
- VDAが複数のGPUにアクセスする場合、使用率グラフには、個々のGPUから収集されたGPUメトリックの平均が表示されます。GPUメトリックは、個々のプロセスではなく、VDA全体に対して収集されます。

- AMDの場合、エンコーダーとデコーダーの使用状況は個別にサポートされていません。GPUを使用するエンコード/デコードワークロードは、GPU使用率の一般的な3D負荷として報告されます。
- NVIDIA WMI をインストール時にインストールしてください。このウィンドウは手動インストール時のみ利用可能です。
- ドライバーがインストールされているのに Director が GPU を検出しない場合
  - タスクマネージャーを確認してください。ドライバーが適切にインストールされていれば、GPU はタスクマネージャーに表示されるはずです。
  - マシンが登録されているか確認してください。マシンがオンラインとして検出されるまでに時間がかかる場合があります。
- Director で GPU 使用率にアクティビティが表示されない場合は、実行しているワークロードが GPU を使用していることを確認してください。グラフィックワークロードの場合、これは「設定 > システム > ディスプレイ > グラフィック設定 > 設定するアプリを選択」から有効にできます。「高パフォーマンス」をオンにしてください。他の設定によっては、これがシステムデフォルトまたは省電力に設定されている場合、Windows はグラフィックワークロードに CPU を使用することがあります。
- データは毎分更新され、**GPU 使用率**を選択してから1分以内にデータの視覚化が開始されます。

マシンベースの履歴リソース使用率

「**マシン使用率**」パネルで、「**履歴使用率の表示**」をクリックすると、選択したマシンにおけるリソースの履歴使用状況が表示されます。 使用率グラフには、CPU、メモリ、同時セッションのピーク、平均 IOPS、およびディスク遅延の重要なパフォーマンスカウンターが含まれます。

> **注:**

> 監視ポリシー設定の**プロセス監視を有効にする**は、履歴マシン使用率ページの「上位10プロセス」テーブルでデータを収集および表示するために「許可」に設定する必要があります。この収集はデフォルトで禁止されています。

> CPU とメモリの使用率、平均 IOPS、およびディスク遅延データはデフォルトで収集されます。**リソース監視を有効にする**ポリシー設定を使用して、この収集を無効にできます。



1. **マシン詳細**ビューの**マシン使用率**パネルから、**履歴使用率の表示**を選択します。
2. **履歴マシン使用率**ページで、**期間**を「過去2時間」、「24時間」、「7日間」、「月」、または「年」に設定して使用状況を表示します。

> **注:**
>
> 平均IOPSとディスク遅延の使用状況データは、現在までの過去24時間、月、年についてのみ利用可能です。カスタム終了時刻はサポートされていません。

3. **適用**をクリックし、必要なグラフを選択します。
4. グラフの異なるセクションにカーソルを合わせると、選択した期間の詳細情報が表示されます。

IOPSとディスク遅延を含む過去のマシンの利用状況(/en-us/citrix-virtual-apps-desktops/2503/media/dir-machine-util-iops-latency.png)

たとえば、**過去2時間**を選択した場合、ベースライン期間は選択した時間範囲の2時間前になります。過去2時間とベースライン時間のCPU、メモリ、セッションの傾向を表示します。**先月**を選択した場合、ベースライン期間は前月になります。先月とベースライン時間の平均IOPSとディスク遅延を表示するように選択します。

1. **エクスポート**をクリックして、選択した期間のリソース使用状況データをエクスポートします。詳細については、Monitor Deploymentsのレポートのエクスポートセクションを参照してください。

2. グラフの下の表には、CPUまたはメモリ使用率に基づいた上位10のプロセスが一覧表示されます。選択した時間範囲におけるアプリケーション名、ユーザー名、セッションID、平均CPU、ピークCPU、平均メモリ、ピークメモリを示す任意の列で並べ替えることができます。IOPSとディスク遅延の列は並べ替えることができません。

   > **注:**
   >
   > システムプロセスのセッションIDは「0000」と表示されます。

3. 特定のプロセスのリソース消費の履歴傾向を表示するには、上位10のプロセスのいずれかをドリルダウンします。

マシンコンソールアクセス

XenServerバージョン7.3以降でホストされているシングルセッションおよびマルチセッションOSマシンのコンソールに、Directorから直接アクセスできます。これにより、XenServerでホストされているVDAの問題をトラブルシューティングするためにXenCenterは不要になります。この機能を利用するには：

- バージョン7.16以降のDelivery Controllerが必要です。
- マシンをホストしているXenServerはバージョン7.3以降である必要があり、Director UIからアクセスできる必要があります。

マシンコンソールアクセス(/en-us/citrix-virtual-apps-desktops/2503/media/director_machine_console_716.png)

マシンのトラブルシューティングを行うには、対応するマシン詳細パネルの**コンソール**リンクをクリックします。提供されたホスト資格情報が認証されると、WebベースのVNCクライアントであるnoVNCを使用して、マシンコンソールが別のタブで開きます。これで、コンソールにキーボードとマウスでアクセスできるようになります。

> **注:**
>
> - この機能はInternet Explorer 11ではサポートされていません。
> - マシンコンソール上のマウスポインターがずれている場合は、問題を解決する手順についてCTX230727を参照してください。

- Directorは新しいタブでコンソールアクセスを起動します。ブラウザの設定でポップアップが許可されていることを確認してください。
- セキュリティ上の理由から、Citrix®はブラウザにSSL証明書をインストールすることを推奨しています。

最近の電源操作があるマシンを検査する

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

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

注:

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

マシンの電源操作ステータスは、次の方法で表示できます。

フィルター -> **マシン**タブから。この場合、デフォルトでは**電源操作時刻**と**電源操作結果**の列が表示されます。表示したい列を選択することもできます。

コスト最適化タブから。この場合、デフォルトのフィルターは**電源操作のトリガー元**が*Autoscale*™に設定され、**電源操作結果**が*失敗*に設定されています。

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

電源操作ステータスを表示するために、以下のフィルターが追加されました。

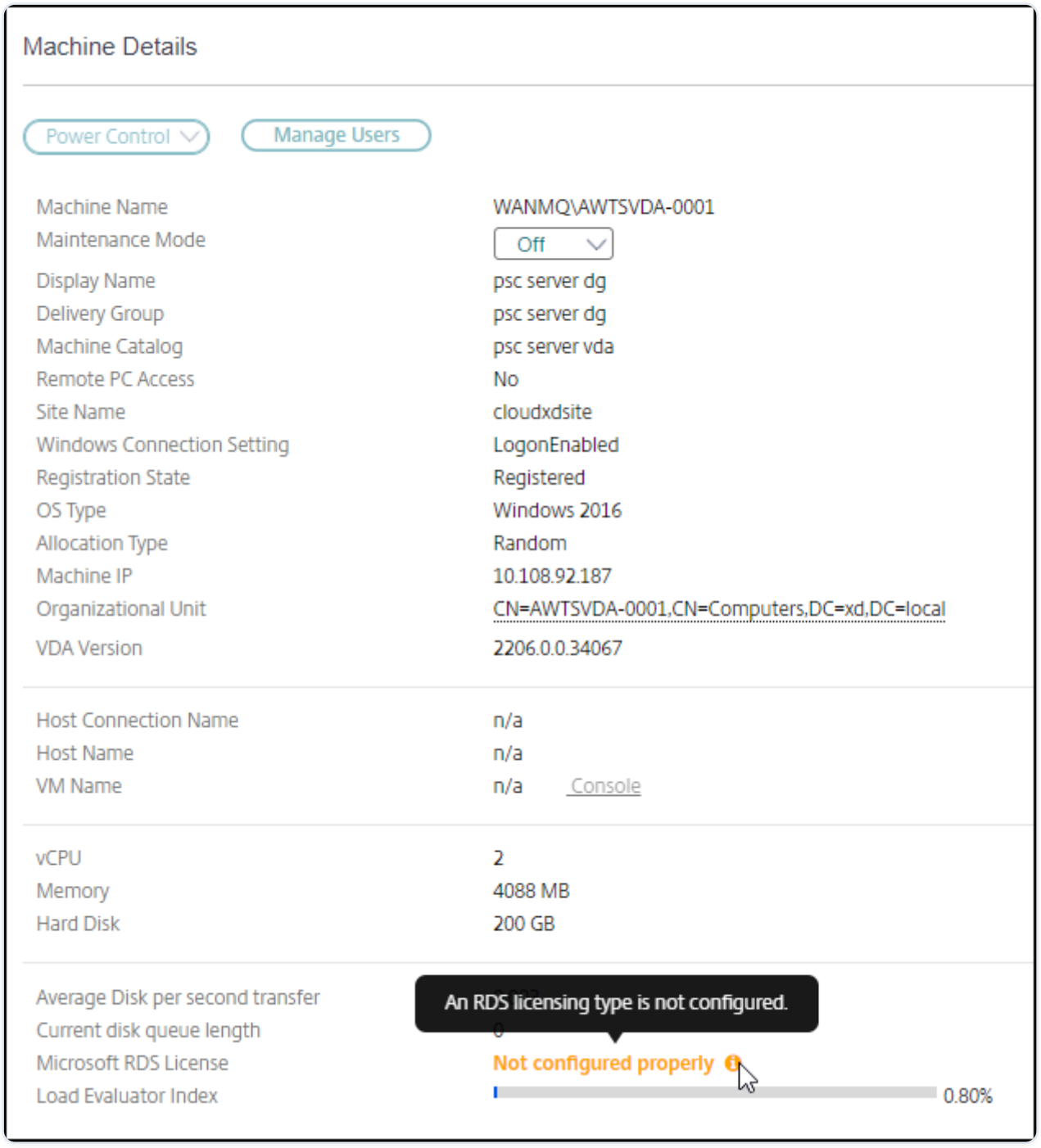
フィルター	説明
電源操作の結果	電源操作の結果を表示します。可能なフィルター値は「成功」と「失敗」です。

フィルター	説明
電源操作のトリガー元	電源操作をトリガーした人物または内容を表示します。可能なフィルター値は以下のとおりです。
	• オートスケール - この値は、電源操作が以下によってトリガーされた場合に表示されます。
	• 管理者がVMのOSディスクを初期状態に戻すためにVMをシャットダウンした場合
	• 設定されたポリシーに基づいてVMがシャットダウンまたは一時停止された場合
	• プールサイズまたはバッファサイズの構成に基づいてVMが利用可能になった場合
	• 管理者 - この値は、管理者によって電源操作がトリガーされたときに表示されます。考えられる例としては、管理者がVMのシャットダウン、起動、一時停止、再開、再起動、またはリブートを要求した場合などがあります。
	• ユーザー - この値は、ユーザーによって電源操作がトリガーされたときに表示されます。例としては、ユーザーがVMを

フィルター	説明
	リセット、起動、または作業を再開した場合などがあります。
	• その他 - この値は、電源操作がスケジュールされた理由または不明な理由によってトリガーされたときに表示されます。
最終電源操作	マシンで発生した正確な電源操作（電源オン、電源オフ、シャットダウン、再起動、リセット、再開など）を表示します。
電源操作時刻	電源操作が完了した時刻。可能なフィルター値は、過去1分、過去5分、過去30分、過去1時間、今日、過去24時間、昨日です。
電源操作失敗理由	失敗の理由を表示します。可能なフィルター値は、ハイパーバイザー報告の失敗、ハイパーバイザーのレート制限超過、不明なエラー、なしです。操作が成功した場合は「なし」と表示されます。

Microsoft RDSライセンスの健全性

マルチセッションOSマシンの**マシン詳細**ページおよび**ユーザー詳細**ページの**マシン詳細**パネルで、Microsoft RDSライセンスのステータスを表示できます。



次のいずれかのメッセージが表示されます。

- ライセンス利用可能
- 適切に構成されていません（警告）
- ライセンスエラー（エラー）
- 互換性のないVDAバージョン（エラー）

> **注:**

有効なライセンスを持つ猶予期間中のマシンのMicrosoft RDSライセンスの健全性ステータスは、緑色で**ライセンス利用可能**メッセージを表示します。ライセンスの有効期限が切れる前に更新してください。

警告メッセージとエラーメッセージについては、情報アイコンにカーソルを合わせると、次の表に示す追加情報が表示されます。

メッセージの種類	DIRECTOR内のメッセージ
エラー	VDAバージョン7.16以降で利用可能です。
エラー	新しいRDS接続は許可されていません。
エラー	Microsoft RDSライセンスの猶予期間が過ぎました。
エラー	必要なOSレベルに対して、デバイスごとのクライアントアクセスライセンスの種類でライセンスサーバーが構成されていません。
エラー	構成されているライセンスサーバーは、デバイスごとのクライアントアクセスライセンスの種類でRDSホストOSレベルと互換性がありません。
警告	Personal Terminal Serverは、Citrix Virtual Apps and Desktops™展開において有効なRDSライセンスの種類ではありません。
警告	管理用リモートデスクトップは、Citrix Virtual Apps and Desktops展開において有効なライセンスの種類ではありません。
警告	RDSライセンスの種類が構成されていません。
警告	ユーザーごとのクライアントアクセスRDSライセンスの種類では、ドメインコントローラーまたはライセンスサーバーに到達できません。

メッセージの種類	DIRECTOR内のメッセージ
警告	「デバイスごとのクライアントアクセス」ライセンスタイプでは、必要なOSレベルのライセンスサーバーに到達できないため、クライアントデバイスライセンスを判別できません。

> **注:**
>
> この機能は、Microsoft RDS CAL (クライアントアクセスライセンス) にのみ適用されます。

ユーザーの問題のトラブルシューティング

Directorの**ヘルプデスク**ビュー（**アクティビティマネージャー**ページ）を使用して、ユーザーまたはセッションに関する情報を表示します。

ユーザーの詳細(/en-us/citrix-virtual-apps-desktops/2503/media/dir-user-details-summary.png)

アクティビティマネージャーからユーザーに対して**詳細の表示**をクリックすると、**ユーザーの詳細**ページが開きます。 アクティビティマネージャーからエンドポイントに対して**詳細の表示**をクリックすると、**エンドポイントの詳細**ページが開きます。

ユーザーの詳細のドリルダウン(/en-us/citrix-virtual-apps-desktops/2503/media/dir-user-details-drilldown1.png)

セッションセレクター

ユーザーが複数のセッションを開始している場合、セッションセレクターはセッションの選択に役立ちます。

セッションセレクター(/en-us/citrix-virtual-apps-desktops/2503/media/dir-session-selector.png)

セッションを選択して詳細を表示します。

- セッション、ユーザーのサインインエクスペリエンス、セッションの起動、接続、およびアプリケーションに関する詳細を確認します。
- ユーザーのマシンをシャドウできます。
- ICA®セッションを記録します。

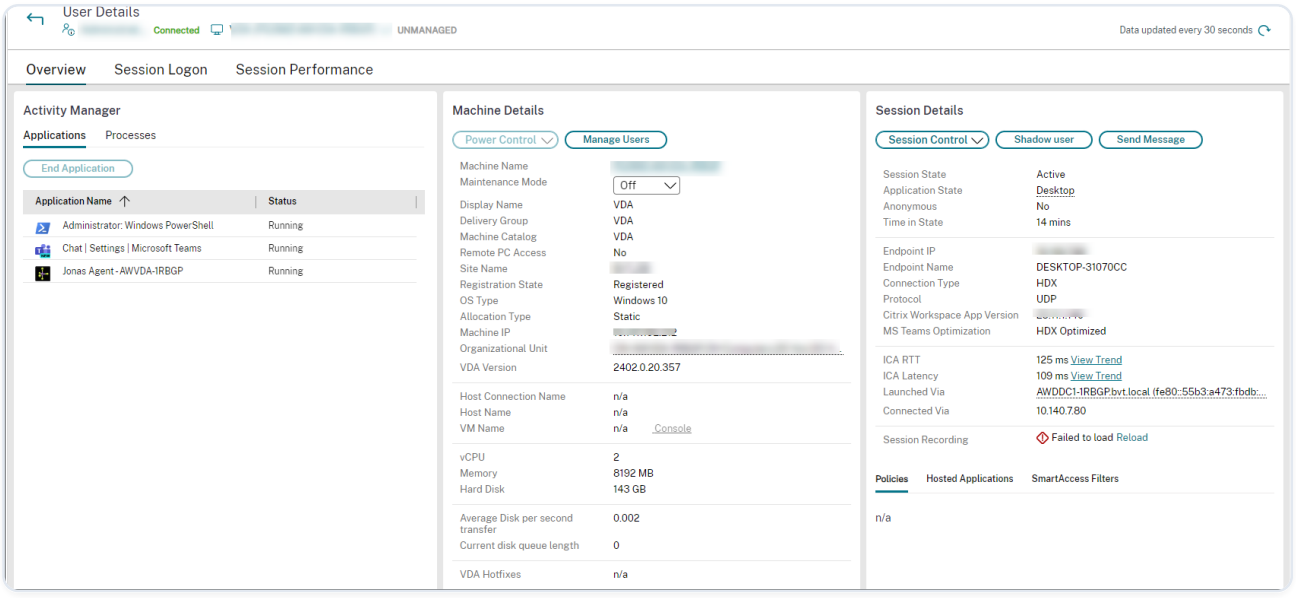
Microsoft Teamsの最適化ステータス

Directorは、HDX™セッションのMicrosoft Teamsの最適化ステータスを、**ユーザーの詳細**ページ > **セッションの詳細**パネル > **MS Teamsの最適化**フィールドに表示します。Microsoft Teamsが最適化されていることは、クリアなオーディオとビデオなど、より良いユーザーエクスペリエンスにとって重要です。Microsoft Teamsの最適化ステータスの可視性は、チケット解決にかかる時間を短縮し、トラブルシューティング中に管理者が重要なメトリックを特定するのに役立ちます。

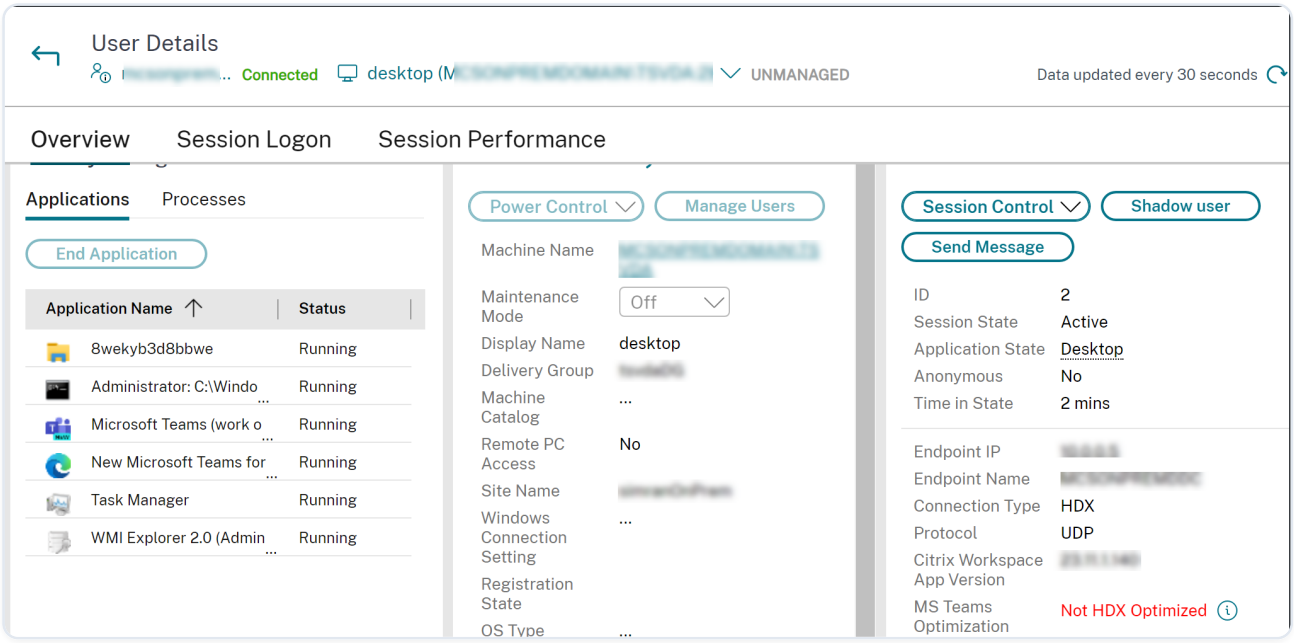
> **注:**
>
> Citrix Directorは、Microsoft Teamsバージョン2.1以前をサポートしています。

前提条件:

- VDA はバージョン 2311 以降で実行されています。
- サポートされている Citrix Workspace アプリのバージョンは、Microsoft Teams の最適化 に記載されています。
- Microsoft Teams は、公開アプリケーションとして、または公開デスクトップ内で実行されます。
- Citrix HDX HTML5 Video Redirection Service などの重要なサービスが実行されています。



Microsoft Teams が最適化されていない場合、ツールチップには、Microsoft Teams を最適化するためのヒントを含む HDX の外部トラブルシューティングライブ記事へのリンクが表示されます。HDX の最適化のトラブルシューティング。



トラブルシューティングのヒント

次の表の推奨されるアクションで問題をトラブルシューティングし、必要に応じて、適切な管理者に問題をエスカレートしてください。

ユーザーの問題	提案
ログオンに時間がかかる、または断続的または繰り返し失敗する	ユーザーログオンの問題を診断する
セッションの起動に時間がかかる、または断続的または繰り返し失敗する	セッション起動の問題を診断する
セッションの応答が遅い、または応答しない	セッションパフォーマンスの問題を診断する
アプリケーションが遅い、または応答しない	アプリケーション障害の解決
接続に失敗しました	デスクトップ接続の復元
セッションが遅い、または応答しない	セッションの復元
セッションを記録する	セッションの記録
ビデオが遅い、または品質が悪い	HDXチャネルシステムレポートの実行

注:

> マシンがメンテナンスモードになっていないことを確認するには、ユーザー詳細ビューからマシン詳細パネルを確認します。

セッションログオン

「**ユーザー詳細**」ビュー > 「**セッションログオン**」タブには、セッションログオンプロセスの包括的なビューが表示されます。このタブには、合計ログオン時間、クライアントとコントローラーのログオン時間、およびVDAのログオン時間が表示されます。「**セッションログオン**」タブには、さまざまなログオンフェーズがプロットされたログオン時間フェーズチャートが含まれています。このデータを使用して、ユーザーログオンの問題をトラブルシューティングします。詳細については、「ユーザーログオンの問題の診断」を参照してください。

セッションパフォーマンス

「**セッションパフォーマンス**」タブには、ユーザーセッション内の問題を特定するためにリアルタイムメトリックを関連付ける機能から始まる、強化されたトラブルシューティングワークフローがあります。「**セッショントポロジ**」パネルは、接続されたHDXセッションのセッション内パスを視覚的に表現します。「**パフォーマンスメトリック**」パネルは、ICARTT、ICA Latency、Frames Per Second、Output Bandwidth Available、Output Bandwidth Consumedなどのセッションメトリックの傾向を提供し、これらのメトリックが時間の経過とともにどのようにパフォーマンスしたかを示します。詳細については、「セッションパフォーマンスの問題の診断」を参照してください。

検索のヒント

検索フィールドにユーザー名を入力すると、Director は Director をサポートするように構成されているすべてのサイトのユーザーについて、Active Directory でユーザーを検索します。

検索フィールドにマルチユーザーマシンの名前を入力すると、Director は指定されたマシンのマシン詳細を表示します。

検索フィールドにエンドポイント名を入力すると、Directorは特定のEndpointに接続されている認証されていない（匿名）セッションと認証されたセッションを使用します。この検索により、認証されていないセッションのトラブルシューティングが可能になります。認証されていないセッションのトラブルシューティングを可能にするには、エンドポイント名が一意であることを確認してください。

検索結果には、現在マシンを使用していない、またはマシンに割り当てられていないユーザーも含まれます。

- 検索では大文字と小文字は区別されません。

- 部分的な入力でも、一致する可能性のあるリストが生成されます。
- スペースで区切られた2つの部分からなる名前の数文字を入力すると、両方の文字列に一致する結果が表示されます。2つの部分からなる名前の例としては、ユーザー名、姓と名、または表示名です。たとえば、「jo rob」と入力すると、「John Robertson」や「Robert Jones」などの文字列が結果に含まれる場合があります。

ランディングページに戻るには、「**Directorロゴ**」をクリックします。

Citrix Insight Servicesへのアクセス

Directorの**ユーザー**ドロップダウンリストからCitrix Insight Services (CIS) にアクセスして、追加の診断情報を取得できます。CISで利用できるデータは、Call HomeやCitrix Scoutなどのソースから取得されます。

シトリックス インサイト サービス(/en-us/citrix-virtual-apps-desktops/2503/media/director-cis.png)

Citrixテクニカルサポートへのトラブルシューティング情報のアップロード

選択したコンピューターのトラブルシューティングを行うには、単一のDelivery Controller™またはVDAからCitrix Scoutを実行して、主要なデータポイントとCitrix Diagnostics Facility (CDF) トレースをキャプチャします。Scoutは、データをCISプラットフォームに安全にアップロードする機能を提供し、Citrixテクニカルサポートのトラブルシューティングを支援します。Citrixテクニカルサポートは、CISプラットフォームを使用して、顧客から報告された問題の解決にかかる時間を短縮します。

Scoutは、Citrix Virtual Apps and Desktops™コンポーネントとともにインストールされます。Windowsのバージョンによっては、Citrix Virtual Apps and Desktopsをインストールまたはアップグレードすると、Scoutが**Windowsのスタート**メニューまたはスタート画面に表示されます。

Scoutを起動するには、スタートメニューまたはスタート画面から、**Citrix \> Citrix Scout**を選択します。

Scoutの使用方法と構成、およびFAQについては、CTX130147を参照してください。

セッション起動の問題を診断する

ユーザーログオンの問題の診断セクションで述べられているログオンプロセスフェーズに加えて、Directorはセッション起動時間を表示します。これは、**ユーザー詳細**ページと**マシン詳細**ページで、Workspace Appセッション起動時間とVDAセッション起動時間に分けられます。これらの2つの期間は、さらに個々のフェーズを含み、その起動時間も表示されます。このデータは、セッション起動時間の長さの理解とトラブルシューティングに役立ちます。さらに、セッション起動に関わる各フェーズの時間も、個々のフェーズに関連する問題のトラブルシューティングに役立ちま

す。たとえば、ドライブマッピングの時間が長い場合、GPOまたはスクリプトですべての有効なドライブが正しくマッピングされているかどうかを確認できます。この機能は、Delivery Controllerバージョン7 1906以降およびVDA 1903以降で利用可能です。

前提条件

セッション起動時間のデータが表示されるには、以下の前提条件が満たされていることを確認してください。

- デリバリーコントローラー™ 7 1906 以降。
- VDA 1903以降。
- Citrix End User Experience Monitoring (EUEM)サービスがVDA上で実行されている必要があります。

制限事項

Directorがセッション起動時間のデータを表示する際には、以下の制限事項が適用されます。

- セッション起動時間は、HDX™セッションでのみ利用可能です。
- iOSおよびAndroid OSからのセッション起動の場合、VDA起動時間のみが利用可能です。
- ICA®ファイルダウンロード時間 (IFDCD) は、ブラウザから起動する際にWorkspace Appが検出された場合にのみ利用可能です。
- Mac OSからのセッション起動の場合、IFDCDはWorkspace App 1902以降でのみ利用可能です。
- Windows OSからのセッション起動の場合、IFDCDはWorkspace app 1902以降で利用可能です。それ以前のバージョンでは、IFDCDはWorkspace appが検出されたブラウザからのアプリ起動の場合にのみ表示されます。

注:

- 前提条件が満たされた後もセッション起動時間の表示に問題がある場合、CTX130320に記載されているように、DirectorサーバーとVDAのログを確認してください。 共有セッション（同じセッションで複数のアプリケーションが起動されている場合）の場合、Workspace Appの起動メトリックは、最新の接続または最新のアプリケーション起動に対して表示されます。
- VDAセッション起動の一部のメトリックは、再接続時には適用されません。そのような場合、メッセージが表示されます。

> セッション起動(/en-us/citrix-virtual-apps-desktops/2503/media/session_startup.png)

Workspace App セッション起動フェーズ

セッション起動クライアント期間 (SSCD)

このメトリックが高い場合、起動時間が長くなる原因となっているクライアント側の問題を示しています。問題の根本原因を特定するために、後続のメトリックを確認してください。SSCDは、要求（マウスクリック）の時刻にできるだけ近い時点から開始されます。クライアントデバイスとVDA間のICA接続が確立されたときに終了します。共有セッションの場合、新しいサーバー接続の作成に関連するセットアップコストの多くが発生しないため、この期間ははるかに短くなります。次のレベルでは、いくつかの詳細なメトリックが利用可能です。

ICA ファイルダウンロード期間

これは、クライアントがサーバーからICAファイルをダウンロードするのにかかる時間です。全体のプロセスは次のとおりです。

1. ユーザーがWorkspace Applicationでリソース（アプリケーションまたはデスクトップ）をクリックします。
2. ユーザーからの要求は、Citrix Gateway（構成されている場合）を介してStoreFront™に送信され、StoreFront™は要求をDelivery Controllerに送信します。
3. Delivery Controllerは要求に対して利用可能なマシンを見つけ、マシン情報とその他の詳細をStoreFrontに送信します。また、StoreFrontはSecure Ticket Authorityからワンタイムチケットを要求し、受け取ります。
4. StoreFrontはICAファイルを生成し、Citrix Gateway（構成されている場合）を介してユーザーに送信します。

IFDCDは、完全なプロセス（ステップ1〜4）にかかる時間を表します。クライアントがICAファイルを受信したときに、IFDCDのカウントは停止します。

LPWD は、プロセスの StoreFront コンポーネントです。

IFDCD が高い (ただし LPWD が正常である) 場合、起動のサーバー側処理は成功しましたが、クライアントデバイスと StoreFront の間に通信の問題がありました。これは、2つのマシン間のネットワークの問題に起因します。したがって、まず潜在的なネットワークの問題をトラブルシューティングできます。

起動ページ WEB サーバー期間 (LPWD)

これは、StoreFrontで起動ページ (launch.aspx) を処理するのにかかった時間です。LPWDが高い場合、StoreFrontにボトルネックがある可能性があります。

考えられる原因は次のとおりです。

- StoreFrontの負荷が高い。Internet Information Services (IIS) のログと監視ツール、タスクマネージャー、パフォーマンスモニターなどを確認して、速度低下の原因を特定してみてください。
- StoreFrontがDelivery Controllerなどの他のコンポーネントと通信する際に問題が発生している。StoreFrontとDelivery Controller間のネットワーク接続が遅いか、一部のDelivery Controllerがダウンしているか、過負荷になっていないかを確認してください。

名前解決WEBサーバー期間 (NRWD)

これは、Delivery Controllerが公開アプリケーション/デスクトップの名前をVDAマシンIPアドレスに解決するのにかかる時間です。

このメトリックが高い場合、Delivery Controllerが公開アプリケーションの名前をIPアドレスに解決するのに時間がかかっていることを示します。

考えられる原因としては、クライアント側の問題、Delivery Controllerの過負荷などのDelivery Controllerの問題、またはそれらの間のネットワークリンクの問題が挙げられます。

チケット応答WEBサーバー期間 (TRWD)

この期間は、Secure Ticket Authority (STA) サーバーまたはDelivery Controllerからチケットを取得するのにかかる時間を示します (必要な場合)。この期間が高い場合、STAサーバーまたはDelivery Controllerが過負荷になっていることを示します。

セッション検索クライアント期間 (SLCD)

この期間は、要求された公開アプリケーションをホストするためにすべてのセッションを照会するのにかかる時間を表します。既存のセッションがアプリケーション起動要求を処理できるかどうかを判断するために、クライアントでチェックが実行されます。使用される方法は、セッションが新規か共有かによって異なります。

セッション作成クライアント期間 (SCCD)

この期間は、wfica32.exe (または同様の同等ファイル) が起動されてから接続が確立されるまでの、セッション作成にかかる時間を表します。

VDAセッション起動フェーズ

セッション起動VDA期間 (SSVD)

この期間は、VDAが起動操作全体を実行するのにかかる時間を含む、高レベルのサーバー側接続起動メトリックです。このメトリックが高い場合、セッション起動時間を増加させるVDAの問題があることを示します。これには、VDAで起動操作全体を実行するのに費やされた時間が含まれます。

資格情報取得VDA期間 (COVD)

VDAがユーザー資格情報を取得するのにかかった時間。

この期間は、ユーザーがタイムリーに資格情報を提供できない場合、人為的に増加する可能性があります。そのため、VDA起動期間には含まれません。この時間は、手動ログインが使用され、サーバー側の資格情報ダイアログが表示される場合（またはログイン開始前に法的通知が表示される場合）にのみ重要となる可能性があります。

資格情報認証VDA期間 (CAVD)

これは、VDAが認証プロバイダーに対してユーザーの資格情報を認証するのにかかる時間です。認証プロバイダーは、Kerberos、Active Directory、またはセキュリティサポートプロバイダーインターフェース (SSPI) のいずれかです。

グループポリシーVDA期間 (GPVD)

この期間は、ログオン中にグループポリシーオブジェクトを適用するのにかかる時間です。

ログオンスクリプト実行VDA期間 (LSVD)

これは、VDAがユーザーのログオンスクリプトを実行するのにかかる時間です。

ユーザーまたはグループのログオンスクリプトを非同期にすることを検討してください。アプリケーション互換性スクリプトを最適化するか、代わりに環境変数を使用することを検討してください。

プロファイルロードVDA期間 (PLVD)

これは、VDAがユーザープロファイルをロードするのにかかる時間です。

この期間が長い場合は、ユーザープロファイルの設定を検討してください。ローミングプロファイルのサイズと場所は、セッションの起動が遅くなる原因となります。ユーザーがターミナルサービスローミングプロファイルとホームフォルダーが有効になっているセッションにログオンすると、ログオン中にローミングプロファイルの内容とそのフォルダーへのアクセスがマップされます。これには追加のリソースが必要です。場合によっては、CPU使用率の大部分を消費することがあります。この問題を軽減するには、リダイレクトされた個人フォルダーとともに**ターミナルサービスホーム**フォルダーを使用することを検討してください。一般に、Citrix環境でユーザープロファイルを管理するには、Citrix Profile Managementの使用を検討してください。Citrix Profile Managementを使用しており、ログオン時間が遅い場合は、アンチウイルスソフトウェアがCitrix Profile Managementツールをブロックしていないか確認してください。

プリンター作成VDA期間 (PCVD)

これは、VDAがユーザーのクライアントプリンターを同期的にマップするのにかかる時間です。プリンター作成が非同期で実行されるように設定されている場合、セッション起動の完了に影響しないため、PCVDの値は記録されません。

プリンターのマッピングに過剰な時間がかかるのは、多くの場合、プリンターの自動作成ポリシー設定が原因です。ユーザーのクライアントデバイスにローカルで追加されたプリンターの数と、印刷設定は、セッションの起動時間に直接影響する可能性があります。セッションが開始されると、Citrix Virtual Apps and Desktops™は、クライアントデバイス上のローカルにマップされたすべてのプリンターを作成する必要があります。特にユーザーが多数のローカルプリンターを持っている場合は、作成されるプリンターの数を減らすように印刷ポリシーを再構成することを検討してください。これを行うには、Delivery ControllerおよびCitrix Virtual Apps and Desktopsでプリンター自動作成ポリシーを編集します。

ドライブマッピングVDA期間 (DMVD)

これは、VDAがユーザーのクライアントドライブ、デバイス、ポートをマップするのにかかる時間です。

ベースポリシーに、未使用の仮想チャネルを無効にする設定が含まれていることを確認してください。たとえば、ICAプロトコルを最適化し、セッション全体のパフォーマンスを向上させるために、オーディオまたはCOMポートのマッピングを無効にします。

アプリケーション/デスクトップ起動VDA期間 (ALVD/DLVD)

このフェーズは、UserinitとShellの期間の組み合わせです。ユーザーがWindowsマシンにログオンすると、winlogonがuserinit.exeを実行します。Userinit.exeはログオンスクリプトを実行し、ネットワーク接続を再確立してから、Explorer.exeを起動します。Userinitは、userinit.exeの開始から仮想デスクトップまたはアプリケーションのユーザーインターフェイスの開始までの期間を表します。Shell期間は、ユーザーインターフェイスの初期化からユーザーがキーボードとマウスの制御を受け取るまでの時間です。

セッション作成VDA期間 (SCVD)

この時間には、VDAでのセッション作成時間のあらゆる雑多な遅延が含まれます。

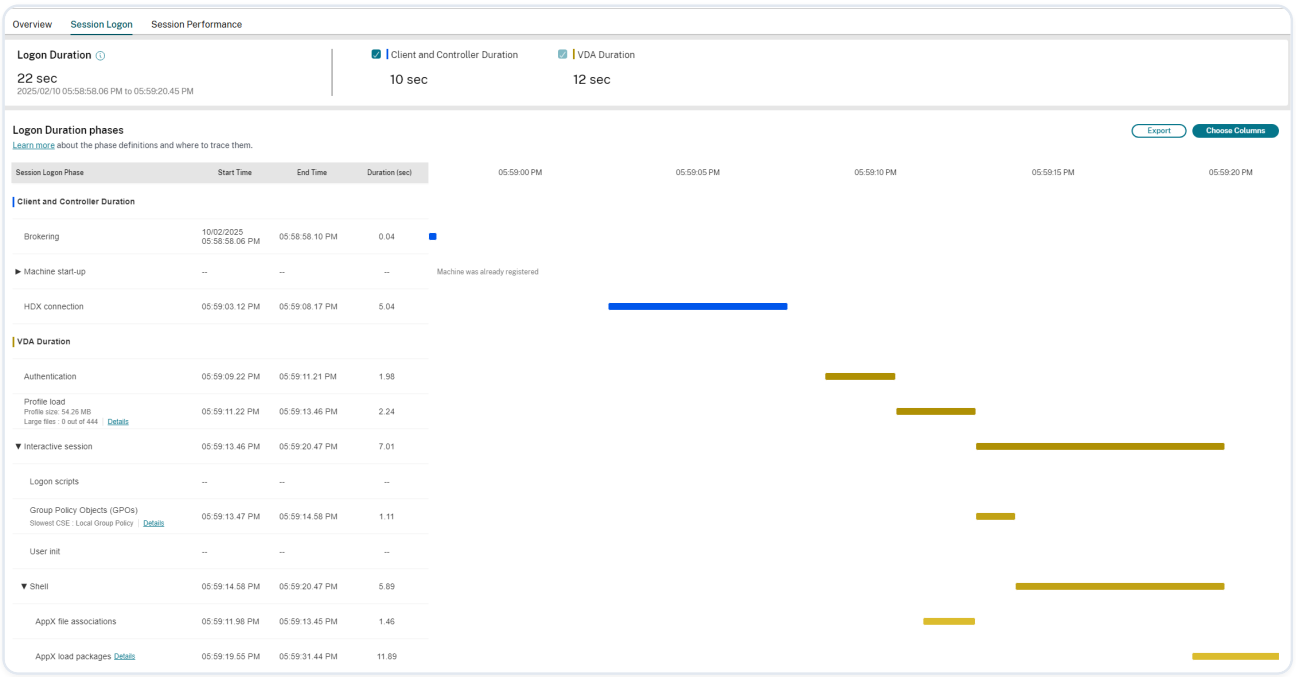
ユーザーログオンの問題を診断する

ビュー > タブには、セッションログオンプロセスの包括的なビューが表示されます。このタブには、総ログオン時間、クライアントとコントローラーの所要時間、およびVDAの所要時間が表示されます。このデータを使用して、ユーザーログオンの問題をトラブルシューティングします。

ログオン時間は、HDXを使用したデスクトップまたはアプリへの初回接続に対してのみ測定されます。このデータには、リモートデスクトッププロトコルで接続しようとしているユーザーや、切断されたセッションから再接続するユーザーは含まれません。具体的には、ユーザーが最初に非HDXプロトコルを使用して接続し、HDXを使用して再接続する場合、ログオン時間は測定されません。

ユーザーがCitrix Virtual Apps and Desktops™にログオンすると、Monitor Serviceはログオンプロセスのフェーズを追跡します。これらのフェーズは、ユーザーがCitrix Workspace™アプリから接続した時点から、アプリまたはデスクトップが使用可能になるまでの時間です。

タブには、さまざまなログオンフェーズがプロットされたログオン時間フェーズチャートが含まれています。ログオン時間は、Delivery Controller™から接続を確立してアプリまたはデスクトップを取得するのに費やされた時間と、仮想アプリまたはデスクトップに認証してログオンするのに費やされた時間を表します。所要時間情報は秒（または秒の端数）で表示されます。



ログオン時間フェーズチャートは、さまざまなログオンフェーズとその開始時刻および終了時刻を明確に示します。このチャートは、個々のログオンフェーズの重なりを示しています。総ログオン時間は、個々のログオンフェーズの所要時間の合計ではない場合があります。これは、個々のフェーズが重複している可能性があり、すべてのログオンフェーズがこの表現の一部ではないためです。また、特定のフェーズは、ユーザーが仮想アプリまたはデスクトップとの対話を開始した後も延長される可能性があり、この所要時間は全体的なログオン時間の一部としては測定されません。

このビューを使用して、セッション起動の遅延を引き起こしている特定のログオンフェーズを特定します。各ログオンフェーズの定義と、情報を追跡できるイベントソースは、さらなるトラブルシューティングに役立ちます。チャートにカーソルを合わせると、現在のセッションのフェーズ所要時間、ユーザーの7日間平均、およびデリバリーグループの7日間平均を含むツールチップが表示されます。この情報は、現在のセッションのログオン時間を7日間平均値と比較するのに役立ちます。GPOおよびプロファイルの詳細の場合、サブフェーズの測定値にさらにドリルダウンできます。この視覚化は、ログオン時間に関連する問題を簡単に理解し、トラブルシューティングするのに役立ちます。

前提条件

ログオン期間データとドリルダウンが表示されるように、次の前提条件が満たされていることを確認してください。

1. VDAに**Citrix User Profile Manager**と**Citrix User Profile Manager WMI Plugin**をインストールします。
2. Citrix Profile Management Serviceが実行されていることを確認してください。
3. XenAppおよびXenDesktopサイト7.15以前の場合、GPO設定の**** を無効にします。
4. 対話型セッションのドリルダウンには、監査プロセス追跡を有効にする必要があります。
5. GPOドリルダウンの場合、グループポリシーの運用ログのサイズを増やします。

注：

- ログオン時間は、デフォルトのWindowsシェル (explorer.exe) でのみサポートされ、カスタムシェルではサポートされません。
- Remote PC Accessのログオン期間は、Remote PC Accessのインストール中に**Citrix User Profile Manager**と**Citrix User Profile Manager WMI Plugin**が追加コンポーネントとしてインストールされている場合にのみ利用可能です。詳細については、Remote PC Accessの構成とシーケンスに関する考慮事項のステップ4を参照してください。

ユーザーログオンの問題をトラブルシューティングする手順

1. **ユーザー詳細**ビュー > **セッションログオン**タブから、ログオン期間グラフを使用してログオン状態をトラブルシューティングします。
   - ユーザーがログオン中の場合、ビューにはログオンのプロセスが反映されます。
   - ユーザーがログオンしている場合、ログオン時間パネルには、ユーザーが現在のセッションにログオンするまでにかかった時間が表示されます。
2. ログオンプロセスのフェーズを検査します。

ログオンプロセスのフェーズ

クライアントとコントローラーの時間

ユーザーがアプリまたはデスクトップアイコンをクリックしてから、キーボードとマウスの制御がエンドユーザーに渡され、セッションと対話できるようになるまでの時間。
ブローカリング

ユーザーに割り当てるデスクトップを決定するまでにかかった時間。
マシンの起動
セッションでマシンの起動が必要な場合、これは仮想マシンを起動するのにかかった時間です。次のサブセクションでは、異なるフェーズで仮想マシンを起動するのにかかった時間の内訳を示します。

- **電源投入** - 仮想マシンの電源投入にかかった時間を表示します
- **起動と登録** - 仮想マシンの起動と登録にかかった時間を表示します

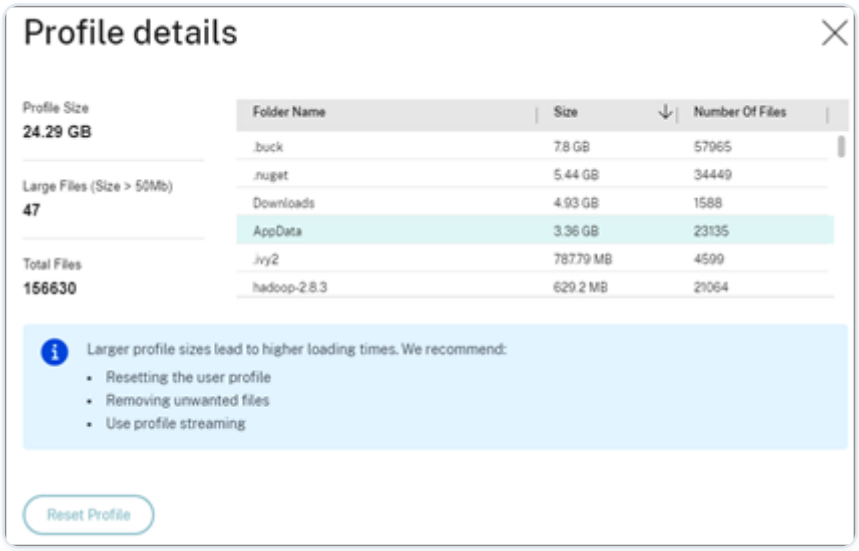
折りたたみボタンを使用して、**マシンの起動**の下にあるオプションを折りたたんだり展開したりできます。
HDX接続
クライアントから仮想マシンへのHDX接続のセットアップに必要な手順を完了するのにかかった時間。

VDAの時間

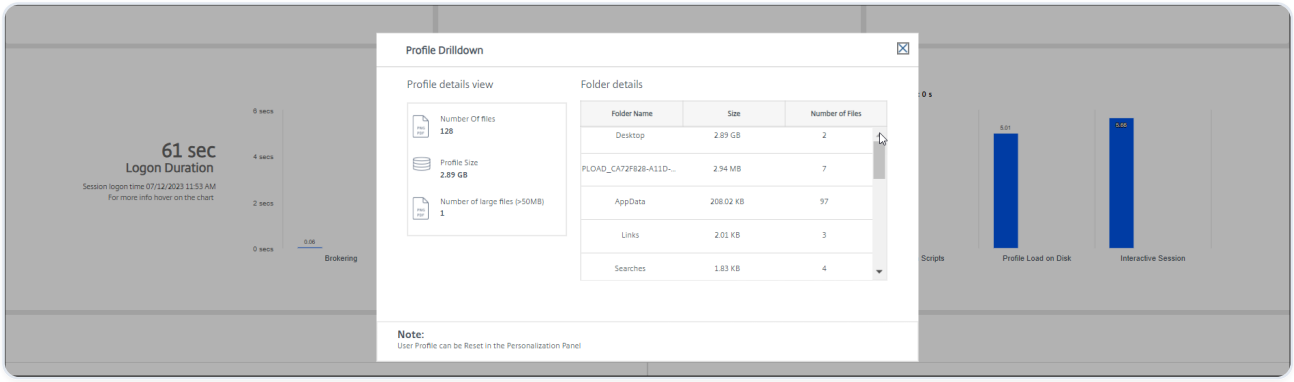
VDAでセッションを作成するのにかかった時間。
認証
リモートセッションへの認証を完了するのにかかった時間。
プロファイル読み込み
ユーザーまたは仮想マシンにプロファイル設定が構成されている場合、これはプロファイルの読み込みにかかる時間です。

Citrix Profile ManagementとFSLogixが構成されている場合、プロファイル読み込みバーには、Citrix Profile ManagementとFSLogixがユーザープロファイルを処理するのにかかった時間が含まれます。この情報は、管理者がプロファイル処理時間の長さに関する問題をトラブルシューティングするのに役立ちます。Profile ManagementとFSLogixが構成されている場合、プロファイル読み込みバーには増加した期間が表示されます。この増加はこの機能強化によって引き起こされるものであり、パフォーマンスの低下を反映するものではありません。この機能強化は、VDAバージョン2407以降で利用できます。

プロファイル読み込みバーにカーソルを合わせると、現在のセッションのユーザープロファイルの詳細を示すツールヒントが表示されます。



詳細をクリックして、プロファイルルートフォルダー（例：C:/Users/username）内の個々のフォルダー、そのサイズ、およびファイル数（ネストされたフォルダー内のファイルを含む）をさらにドリルダウンします。



プロファイルのドリルダウンは、Delivery Controllerバージョン7 1811以降およびVDA 1811以降で利用できます。プロファイルのドリルダウン情報を使用して、高いプロファイルロード時間に関連する問題を解決できます。次のことができます。

- ユーザープロファイルをリセットする
- 不要な大きなファイルを削除してプロファイルを最適化する
- ネットワーク負荷を軽減するためにファイル数を減らす
- プロファイルストリーミングを使用する

デフォルトでは、プロファイルルート内のすべてのフォルダーがドリルダウンに表示されます。フォルダーの表示を非表示にするには、VDAマシンで次のレジストリ値を編集します。

> **警告:**

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

1. VDAで、HKEY_LOCAL_MACHINE\Software\Citrix\Director\ に新しいレジストリ値 **ProfileFoldersNameHidden** を追加します。
2. 値を1に設定します。この値はDWORD（32ビット）値である必要があります。これでフォルダー名の表示が無効になります。
3. フォルダー名を再度表示するには、値を0に設定します。

> **注:**
>
> GPOまたはPowerShellコマンドを使用して、複数のマシンにレジストリ値の変更を適用できます。GPOを使用してレジストリの変更を展開する方法の詳細については、ブログを参照してください。

追加情報

- プロファイルドリルダウンは、リダイレクトされたフォルダーを考慮しません。
- ルートフォルダー内のNTUser.datファイルは、エンドユーザーには表示されない場合があります。ただし、プロファイルドリルダウンに含まれ、**ルートフォルダー**のファイルリストに表示されます。
- AppDataフォルダー内の一部の隠しファイルは、プロファイルドリルダウンに含まれません。
- ファイル数とプロファイルサイズデータは、特定のWindowsの制限により、パーソナライゼーションパネルのデータと一致しない場合があります。

対話型セッション

対話型セッションとは、ユーザープロファイルがロードされた後、キーボードとマウスの制御をユーザーに「引き渡す」のにかかる時間です。通常、ログオンプロセスのすべてのフェーズの中で最も長い期間であり、**対話型セッション期間 = デスクトップ準備完了イベントタイムスタンプ (VDA上のEventId 1000) - ユーザープロファイルロード済みイベントタイムスタンプ (VDA上のEventId 2)** として計算されます。対話型セッションには、Pre-userinit、Userinit、Shellの3つのサブフェーズがあります。対話型セッションにカーソルを合わせると、次のツールヒントが表示されます。

- サブフェーズ
- 各サブフェーズにかかった時間
- これらのサブフェーズ間の合計累積時間遅延

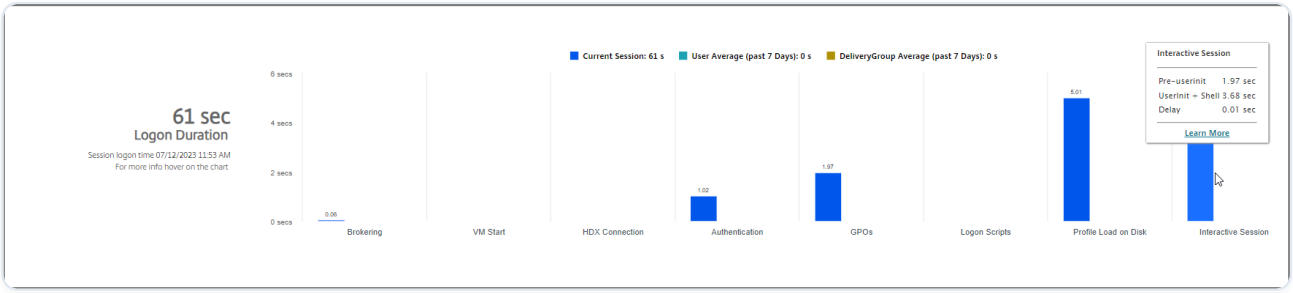
折りたたみ可能なボタンを使用して、**インタラクティブセッション**の下のオプションを折りたたんだり展開したりできます。

> **注:**
>
> この機能はVDA 1811以降で利用できます。7.18より前のサイトでセッションを起動し、その後7.18以降にアップグレードした場合、「サーバーエラーのためドリルダウンを利用できません」というメッセージが表示されます。ただし、アップグレード後にセッションを起動した場合は、エラーメッセージは表示されません。

各サブフェーズの期間を表示するには、VM (VDA) で監査プロセス追跡を有効にします。監査プロセス追跡が無効になっている場合 (デフォルト)、Pre-userinitの期間と、UserinitおよびShellの合計期間が表示されます。グループポリシーオブジェクト (GPO) を使用して監査プロセス追跡を有効にするには、次の手順を実行します。

1. GPOを作成し、GPOエディターを使用して編集します。
2. **コンピューターの構成 > Windowsの設定 > セキュリティの設定 > ローカルポリシー > 監査ポリシー**に移動します。
3. 右側のペインで、**監査プロセス追跡**をダブルクリックします。
4. **成功**を選択し、OKをクリックします。
5. このGPOを必要なVDAまたはグループに適用します。

監査プロセス追跡とその有効化または無効化の詳細については、Microsoftドキュメントの監査プロセス追跡を参照してください。



ユーザー詳細ビューのログオン期間パネル。

- **対話型セッション – Pre-userinit:** これは、グループポリシーオブジェクトとスクリプトと重複する対話型セッションのセグメントです。このサブフェーズは、GPOとスクリプトを最適化することで短縮できます。
- **対話型セッション – Userinit:** ユーザーがWindowsマシンにログオンすると、Winlogonはuserinit.exeを実行します。Userinit.exeはログオンスクリプトを実行し、ネットワーク接続を再確立してから、WindowsユーザーインターフェイスであるExplorer.exeを起動します。対話型セッションのこのサブフェーズは、Userinit.exeの開始から仮想デスクトップまたはアプリケーションのユーザーインターフェイスの開始までの期間を表します。
- **対話型セッション – Shell:** 前のフェーズでは、UserinitがWindowsユーザーインターフェイスの初期化を開始します。Shellサブフェーズは、ユーザーインターフェイスの初期化から、ユーザーがキーボードとマウスの制御を受け取るまでの期間を捕捉します。
- **遅延:** これは、**Pre-userinitとUserinit**サブフェーズ間、および**UserinitとShell**サブフェーズ間の累積時間遅延です。

合計ログオン時間は、これらのフェーズの正確な合計ではありません。たとえば、一部のフェーズは並行して発生し、一部のフェーズでは、合計よりも長いログオン期間につながる可能性のあるより多くの処理が発生します。 合計ログオン時間には、ICAファイルのダウンロードとアプリケーションのICAファイル起動の間の時間であるICA®アイドル時間は含まれません。 アプリケーション起動時にICAファイルを自動的に開くには、ICAファイルのダウンロード時にICAファイルを自動的に起動するようにブラウザを設定します。詳細については、CTX804493を参照してください。

> **注:**
>
> ログオン期間グラフは、ログオンフェーズを秒単位で表示します。1秒未満の期間値は、サブ秒値として表示されます。1秒を超える値は、最も近い0.5秒に丸められます。グラフは、Y軸の最大値が200秒になるように設計されています。200秒を超える値は、バーの上に実際の値が表示されます。

ログオンスクリプト
セッションにログオンスクリプトが構成されている場合、これはログオンスクリプトの実行にかかる時間です。
GPO
仮想マシンでグループポリシー設定が有効になっている場合、これはログオン中にグループポリシーオブジェクトを適用するのにかかる時間です。CSE（クライアント側拡張）に従って各ポリ

シーを適用するのにかかる時間のドリルダウンは、GPOバーにカーソルを合わせるとツールチップとして表示されます。



詳細をクリックすると、ポリシーのステータスと対応するGPO名が記載された表が表示されます。ドリルダウンの期間はCSEの処理時間のみを表しており、GPOの合計時間には加算されません。ドリルダウンテーブルは、さらなるトラブルシューティングやレポートでの使用のためにコピーできます。ポリシーのGPO時間は、イベントビューアーのログから取得されます。ログは、運用ログに割り当てられたメモリ（デフォルトサイズは4MB）によって上書きされる可能性があります。運用ログのログサイズを増やす方法の詳細については、Microsoft TechNetの記事「イベントログの構成」を参照してください。

ユーザー初期化

ユーザーがWindowsマシンにログオンすると、Winlogonはuserinit.exeを実行します。Userinit.exeはログオンスクリプトを実行し、ネットワーク接続を再確立してから、Windowsユーザーインターフェイスであるexplorer.exeを起動します。この対話型セッションのサブフェーズは、Userinit.exeの開始から仮想デスクトップまたはアプリケーションのユーザーインターフェイスの開始までの期間を表します。

シェル

シェルサブフェーズは、ユーザーインターフェイスの初期化から、ユーザーがキーボードとマウスの制御を受け取るまでの期間を捕捉します。

AppXファイル関連付け

新しいVDAセッション中にAppXファイルを関連付けるのにかかった時間。

AppXパッケージの読み込み

新しいVDAセッション中にAppXパッケージを読み込むのにかかった時間。

> **注:**

> 新しいVDAセッション中にAppXパッケージの読み込み期間を収集するには、uberAgentをDirectorと統合する必要があります。詳細については、「Citrix uberAgentとDirectorの統合」を参照してください。

データのエクスポート

デフォルトのログオン期間フェーズテーブルオプション（セッションログオンフェーズと期間）に加えて、セッションログオンページで次の列を選択することもできます。

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

以前のデータを.CSVファイルにエクスポートすることもできます。

トラブルシューティングのヒント

グラフ内の異常な値や予期しない値を特定するには、現在のセッションの各フェーズにかかった時間と、このユーザーの過去7日間の平均所要時間、およびこのデリバリーグループ内の全ユーザーの過去7日間の平均所要時間を比較します。

必要に応じてエスカレートします。たとえば、**マシンの起動**が遅い場合、問題はハイパーバイザーにある可能性があるため、ハイパーバイザー管理者にエスカレートできます。

以下を含む異常な相違点を調べます。

- 不足している（現在の）ログオンバー
- 現在の所要時間とこのユーザーの平均所要時間との間の大きな不一致。原因は次のとおりです。
  - 新しいアプリケーションがインストールされた。
  - オペレーティングシステムのアップデートが行われた。
  - 構成変更が行われた。
  - ユーザーのプロファイルサイズが大きい。この場合、プロファイルロードが高くなります。
- ユーザーのログオン数（現在の所要時間と平均所要時間）とデリバリーグループの平均所要時間との間の大きな不一致。

必要に応じて、**再起動**をクリックしてユーザーのログオンプロセスを監視し、**マシンの起動**や**ブローカリング**などの問題をトラブルシューティングします。

セッションパフォーマンスの問題を診断する

ユーザー詳細ページの**セッションパフォーマンス**タブには、HDX™ユーザーセッション内の問題を特定するのに役立つ、強化されたトラブルシューティングワークフローが用意されています。**セッショントポロジとパフォーマンスメトリック**パネルは、セッションのコンポーネントビューと複数のパフォーマンスメトリックを単一のビューで関連付け、セッションエクスペリエンスの問題解決にかかる平均時間を短縮します。

セッションパフォーマンスビュー(/en-us/citrix-virtual-apps-desktops/2503/media/dir-session-performance.png)

エンドツーエンドネットワークホップビュー

エンドツーエンドネットワークホップビューは、セッションパス全体の視覚的な表現を提供することで、トラブルシューティングを強化します。エンドツーエンドネットワークホップビューを見つけるには、**ユーザー詳細** > **セッションパフォーマンス** > **セッショントポロジ**をクリックします。このビューには、接続されたHDXセッションのコンポーネント、メタデータ、リンク、および公開アプリケーションが表示されます。

このビューは管理者が次のことを行うのに役立ちます。

- セッションデータフローを理解する。
- 特定のホップでのパフォーマンスのボトルネックを特定する。

> **注:**
>
> パフォーマンスメトリックは、接続されているHDXセッションでのみ利用可能です。

セッションパフォーマンスメトリック

以下のメトリックは、管理者が特定のセッションのパフォーマンスを理解するのに役立つように、コンテキストに応じて利用できます。エンドツーエンドネットワークホップビューに表示されるメトリックは、ほぼリアルタイムで利用可能であり、UIに表示される間隔に基づいて定期的に更新されます。
エンドポイントメトリック
エンドポイントメトリックは、Citrix®セッションパフォーマンスのトラブルシューティングに不可欠です。これは、ユーザーエクスペリエンスの「ラストマイル」に関する洞察を提供し、ユーザーの即時環境に関する詳細を明らかにするためです。これらのメトリックは、低速なWi-Fi、低

いネットワークスループット、エンドポイントデバイスの制限などのローカルのボトルネックを特定し、サーバー側とクライアント側の問題を区別するのに役立ちます。セッショントポロジのメトリックと組み合わせることで全体的なビューを提供し、エンドポイントデータは、パフォーマンス問題のより迅速な根本原因特定と解決を可能にし、ユーザーエクスペリエンスを向上させます。

Citrix Studioのポリシーを使用して、要件に基づいてリストされたエンドポイントメトリックの収集を有効または無効にします。これらのポリシーは、Citrix管理者がコンプライアンス要件に準拠してメトリックを報告するためのきめ細かな制御を提供します。

ポリシー名	ポリシーの説明	UIメトリック	デフォルト値	値のオプション	VIRTUAL DELIVERY AGENTのバージョン
エンドポイント統計間隔	ユーザーエンドポイントからのエンドポイントネットワーク詳細の収集を許可します。このポリシーを有効にすることは、他のエンドポイント関連ポリシーが有効になるための前提条件です。	Wi-Fi信号強度、ネットワークインターフェースタイプ、送受信スループット、リンク速度、ワークスペースタイプ、エンドポイントCPU、エンドポイントメモリ、エンドポイントGPU	有効	有効または無効。頻度を60秒～3600秒の間で変更するオプション。60秒が推奨値です。	2407以降
エンドポイント位置情報データ収集	Locusサービス - `<https://locus.analytics.cloud.com>` を使用して、ユーザーエ	パブリックIPアドレス、国、都市、インターネットサービスプロバイダー。	無効	有効または無効	2411以降

ポリシー名	ポリシーの説明	UIメトリック	デフォルト値	値のオプション	VIRTUAL DELIVERY AGENTのバージョン
	ンドポイントからエンドポイントの位置情報とISPの詳細を収集することを許可します。				
エンドポイントネットワーク遅延測定間隔	エンドポイントとビーコンホスト間のネットワーク遅延の測定と収集を許可します - `<https://downloadplugins.citrix.com>`	ネットワーク遅延（エンドポイントネットワーク詳細内）	無効	有効または無効。頻度を60秒～3600秒の間で変更するオプション。60秒が推奨値です。	2411以降

注:

Citrix Virtual Apps and Desktops™ 2507以降では、**エンドポイントの場所データ収集**ポリシーと**エンドポイントネットワーク遅延測定間隔**ポリシーはデフォルトで無効になっています。そのため、これらのポリシーがStudioで手動で有効にされない限り、関連データはDirectorで利用できません。

すぐに利用できるエンドポイントメトリックは以下のとおりです。

- エンドポイント名
- エンドポイントIP
- エンドポイントOS

- Citrix Workspace™アプリのバージョン

次の表に、サポートされている製品バージョンに依存するメトリックを示します。

機能名	UIパラメーター	VDA WINDOWS バージョン	VDA MAC バージョン	VDA LINUX バージョン	WINDOWS 向け CITRIX WORKSPACE アプリのバージョン	MAC 向け CITRIX WORKSPACE アプリのバージョン	LINUX向け CITRIX WORKSPACE アプリのバージョン	HTML5向け CITRIX WORKSPACE アプリのバージョン	CHROME OS向け CITRIX WORKSPACE アプリのバージョン
エンドポイントネットワークの詳細	ネットワークインターフェイスの種類	2407 以降	該当なし	該当なし	2405.10 以降	2409 以降	2408 以降	2411 以降	2411 以降
	信号強度	2407 以降	該当なし	該当なし	2405.10 以降	2409 以降	2408 以降	該当なし	該当なし
	エンドポイントスループット (受信、送信)	2407 以降	該当なし	該当なし	2405.10以降	2409 以降	2408 以降	該当なし	該当なし

機能名	UIパラメーター	VDA WINDOWSバージョン	VDA MACバージョン	VDA LINUXバージョン	WINDOWS向けCITRIX WORKSPACEアプリのバージョン	MAC向けCITRIX WORKSPACEアプリのバージョン	LINUX向けCITRIX WORKSPACEアプリのバージョン	HTML5向けCITRIX WORKSPACEアプリのバージョン	CHROME OS向けCITRIX WORKSPACEアプリのバージョン
	リンク速度	2407以降	該当なし	該当なし	2405.10以降	2409以降	2408以降	2411以降	2411以降
	エンドポイントのパブリックIPアドレス	2411以降	該当なし	該当なし	2409以降	2409以降	2408以降	2411以降	2411以降
	エンドポイントの都市、エンドポイントの国	2411以降	N/A	N/A	2409以降	2409以降	2408以降	2411以降	2411以降
	インターネッ	2411以降	N/A	N/A	2409以降	2409以降	2408以降	2411以降	2411以降

機能名	UIパラメーター	VDA WINDOWSバージョン	VDA MACバージョン	VDA LINUXバージョン	WINDOWS向けCITRIX WORKSPACEアプリのバージョン	MAC向けCITRIX WORKSPACEアプリのバージョン	LINUX向けCITRIX WORKSPACEアプリのバージョン	HTML5向けCITRIX WORKSPACEアプリのバージョン	CHROME OS向けCITRIX WORKSPACEアプリのバージョン
	トサービスプロバイダー								
	ワークスペースの種類	2411以降	該当なし	該当なし	2409以降	2409以降	2408以降	2411以降	2411以降
	アクセスタイプ(Workspace / StoreFront経由)	2411以降	該当なし	該当なし	2409以降	2409以降	2408以降	2411以降	2411以降
	エンドポイントCPU	2411以降	該当なし	該当なし	2409以降	2409以降	2408以降	該当なし	2411以降

機能名	UIパラメーター	VDA WINDOWSバージョン	VDA MACバージョン	VDA LINUXバージョン	WINDOWS向けCITRIX WORKSPACEアプリのバージョン	MAC向けCITRIX WORKSPACEアプリのバージョン	LINUX向けCITRIX WORKSPACEアプリのバージョン	HTML5向けCITRIX WORKSPACEアプリのバージョン	CHROMEOS向けCITRIX WORKSPACEアプリのバージョン
	エンドポイントメモリ	2411以降	該当なし	該当なし	2409以降	2409以降	2408以降	該当なし	2411以降
	エンドポイントGPU	2411以降	該当なし	該当なし	2409以降	2409以降	2408以降	該当なし	該当なし
	ネットワーク遅延	2411以降	NA	NA	2409以降	2409以降	2408以降	2411以降	2411以降

データ定義:

UIパラメーター	説明
エンドポイント名	セッションに使用されるユーザーのエンドポイントデバイスの名前。
エンドポイントIP	Virtual Delivery Agent (VDA) で利用可能なエンドポイントのIPアドレス。エンドポイントデ

UIパラメーター	説明
	バイスのプライベートIPアドレスまたはパブリックIPアドレスが含まれる場合があります。
エンドポイントOS	エンドポイントデバイスのオペレーティングシステム
Citrix Workspaceアプリのバージョン	インストールされているCitrix Workspaceアプリのバージョン
信号強度	ワイヤレス信号の品質と強度を表示します。
エンドポイントスループット (受信、送信)	ネットワークインターフェイスへのデータ転送速度と、ネットワークインターフェイスからのデータ転送速度を示します。エンドポイントで観測されるアップロードおよびダウンロードのインターネット速度に類似しています。
リンク速度	イーサネット、Wi-Fi、セルラーなどのネットワーク接続の種類を指定します。
ネットワークインターフェイスの種類	ネットワーク接続の最大データ転送速度を表します。
エンドポイントのパブリックIPアドレス	インターネットサービスプロバイダーによってデバイスに割り当てられた外部IPアドレス。
エンドポイントの都市、エンドポイントの国	デバイスの地理的な場所（国と都市を含む）。
インターネットサービスプロバイダー	エンドユーザーデバイスにインターネットアクセスを提供する会社の名前。
ワークスペースの種類	使用されているワークスペースの種類（Citrix WorkspaceアプリまたはWebブラウザのいずれか）。
アクセスタイプ (Workspace / StoreFront経由)	リソースにアクセスする方法（Citrix WorkspaceまたはStoreFrontのいずれかを通じて）。
エンドポイントCPU	現在使用されているCPUリソースの割合。

UIパラメーター	説明
エンドポイントメモリ	現在使用されているメモリリソースの割合。
エンドポイントGPU	現在使用されているGPUリソースの割合。
ネットワーク遅延テスト	ネットワークで発生する時間遅延（ミリ秒単位で測定）。

ネットワークメトリック

ネットワークメトリックは、Citrixセッションのトラブルシューティングにとって重要です。なぜなら、Citrixセッションのパフォーマンスと安定性は、基盤となるネットワークの状態に大きく依存しているからです。ローカルアプリケーションとは異なり、Citrixセッションはネットワーク経由でインタラクティブなデスクトップまたはアプリケーションエクスペリエンスをストリーミングするため、ネットワークの不安定性やボトルネックはユーザーのパフォーマンス認識に直接影響します。

Citrix Studioのポリシーを使用して、要件に基づいてリストされているネットワークメトリックの収集を有効または無効にします。これらのポリシーにより、Citrix管理者は、コンプライアンス要件に準拠してメトリックを報告するための詳細な制御が可能になります。

ポリシー名	ポリシーの説明	UIメトリック	デフォルト値	値のオプション	VIRTUAL DELIVERY AGENTバージョン
ネットワークテレメトリ	ユーザーエンドポイントとバックエンドコンポーネント間のネットワーク詳細の収集を許可します。	Citrix GatewayおよびCitrix Gatewayサービスに関するすべてのHDX Insightsメトリック	無効	有効または無効。頻度を60秒～3600秒の間で変更するオプション。60秒が推奨値です。	Gatewayサービスの場合は2411以降。Citrix Gatewayの場合は2503以降。

Citrix Gatewayサービス

次の表に、サポートされている製品バージョンに依存するメトリックを示します。

機能名	UIパラメーター	WINDOWS VDA バージョン	MAC VDA バージョン	LINUX VDA バージョン	WINDOWS 向け CITRIX WORKSPACE アプリのバージョン	MAC向け CITRIX WORKSPACE アプリのバージョン	LINUX向け CITRIX WORKSPACE アプリのバージョン	HTML5向け CITRIX WORKSPACE アプリのバージョン	CHROME OS向け CITRIX WORKSPACE アプリのバージョン
ネットワークメトリック	L7 サーバー遅延	2411 以降	2507 以降	2507 以降	2409 以降	2505 以降	2505 以降	該当なし	該当なし
	L7 クライアント遅延	2411 以降	2507 以降	2507 以降	2409 以降	2505 以降	2505 以降	NA	NA
	クライアント側の再送信 注: TCP セッションでのみ利用可能	2411 以降	2507 以降	2507 以降	2409 以降	2505 以降	2505 以降	NA	NA
	スループット	2411 以降	該当なし	該当なし	2409 以降	2505 以降	2505 以降	該当なし	該当なし

Citrix ゲートウェイ

次の表に、サポートされている製品バージョンに依存するメトリックを示します。

機能名	UIパラメーター	CITRIX GATEWAY のバージョン	WINDOWS VDA のバージョン	MAC のバージョン	LINUX のバージョン	CITRIX WORKSPACE APP FOR WINDOWS のバージョン	CITRIX WORKSPACE APP FOR MAC のバージョン	CITRIX WORKSPACE APP LINUX 版バージョン	CITRIX WORKSPACE APP FOR HTML5 バージョン	CITRIX WORKSPACE APP FOR CHROMEOS バージョン
ネットワークメトリック	WAN 遅延	Netscaler 14.1-47.46 以降	2503 以降	2507 以降	2507 以降	2503 以降	2505 以降	2505 以降	NA	NA
	DC 遅延	Netscaler 14.1-47.46 以降	2503 以降	2507 以降	2507 以降	2503 以降	2505 以降	2505 以降	NA	NA
	サーバー側再送信	Netscaler 14.1-47.46 以降	2503 以降	2507 以降	2507 以降	2503 以降	2505 以降	2505 以降	NA	NA

機能名	UIパラメーター	CITRIX GATEWAYのバージョン	WINDOWS VDAのバージョン	MACのバージョン	LINUXのバージョン	CITRIX WORKSPACE APP FOR WINDOWSのバージョン	CITRIX WORKSPACE APP FOR MACのバージョン	CITRIX WORKSPACE APP LINUX版バージョン	CITRIX WORKSPACE APP FOR HTML5バージョン	CITRIX WORKSPACE APP FOR CHROME OSバージョン
	クライアント側再送信	Netscaler 14.1-47.46以降	2503以降	2507以降	2507以降	2503以降	2505以降	2505以降	該当なし	該当なし
	L7サーバー遅延	Netscaler 14.1-47.46以降	2503以降	2507以降	2507以降	2503以降	2505以降	2505以降	該当なし	該当なし
	L7クライアント遅延	Netscaler 14.1-47.46以降	2503以降	2507以降	2507以降	2503以降	2505以降	2505以降	該当なし	該当なし
	クライアント側の	Netscaler 14.1	2503以降	2507以降	2507以降	2503以降	2505以降	2505以降	該当なし	該当なし

機能名	UIパラメーター	CITRIX GATEWAYのバージョン	WINDOWS VDAのバージョン	MACのバージョン	LINUXのバージョン	CITRIX WORKSPACE APP FOR WINDOWSのバージョン	CITRIX WORKSPACE APP FOR MACのバージョン	CITRIX WORKSPACE APP LINUX版バージョン	CITRIX WORKSPACE APP FOR HTML5バージョン	CITRIX WORKSPACE APP FOR CHROME OSバージョン
	ゼロウィンドウサイズイベント	-47.46以降								
	クライアント側高速RTO	Netscaler 14.1-47.46以降	2503以降	2507以降	2507以降	2503以降	2505以降	2505以降	該当なし	該当なし
	サーバー側ゼロウィンドウサイズイベント	Netscaler 14.1-47.46以降	2503以降	2507以降	2507以降	2503以降	2505以降	2505以降	該当なし	N/A

機能名	UIパラメーター	CITRIX GATEWAYのバージョン	WINDOWS VDAのバージョン	MACのバージョン	LINUXのバージョン	CITRIX WORKSPACE APP FOR WINDOWSのバージョン	CITRIX WORKSPACE APP FOR MACのバージョン	CITRIX WORKSPACE APP LINUX版バージョン	CITRIX WORKSPACE APP FOR HTML5バージョン	CITRIX WORKSPACE APP FOR CHROME OSバージョン
	サーバー側高速RTO	Netscaler 14.1-47.46以降	2503以降	2507以降	2507以降	2503以降	2505以降	2505以降	N/A	N/A

データ定義:

UI パラメーター	説明
WAN遅延	NetScaler®からエンドユーザーまでの、ネットワークのクライアント側によって引き起こされる遅延。
DC遅延	NetScalerからバックエンドサーバーまでの、ネットワークのサーバー側によって引き起こされる遅延。
L7クライアント遅延	ICA®クライアントとNetScalerインスタンス間で観測される平均L7遅延。このメトリックは、配信パスに存在するCitrix以外のデバイスで役立ちます。
L7サーバー遅延	NetScalerデバイスとCitrix Virtual App間で観測される平均L7遅延。このメトリックは、配信

UI パラメーター	説明
	パスにCitrix以外のデバイスが存在する場合に役立ちます。
クライアント再送信	NetScalerとエンドユーザー間の接続で再送信されたパケットの数。このメトリックの値が高い場合、再送信による高い帯域幅使用率を示しますが、必ずしもユーザーエクスペリエンスが悪いことを意味するわけではありません。注: Gateway serviceを使用するセッションの場合、クライアント再送信はTCPセッションでのみ利用可能です。
サーバー側再送信	NetScalerとバックエンドサーバー間の接続で再送信されたパケットの数。
クライアント側ゼロウィンドウ数	クライアントがゼロTCPウィンドウをアドバタイズした回数。
サーバー側ゼロウィンドウ数	サーバーがゼロTCPウィンドウをアドバタイズした回数。

HDXメトリック

HDXメトリックは、ユーザーの仮想エクスペリエンスの品質を理解し、トラブルシューティングを行う上で不可欠です。これらのメトリックは、仮想セッションを提供するICA/HDXプロトコルのパフォーマンスを直接測定します。

注:

ICAメトリックは、Citrix Workspaceアプリ for Windowsバージョン2405.10以降、およびCitrix Virtual Apps and Desktops 2407以降で利用可能です。ただし、データの更新と修正は最新バージョンで利用できます。各データポイントの推奨バージョンについては、次の表を参照してください。

機能名	UIパラメーター	WINDOWS VDA バージョン	MAC VDA バージョン	LINUX VDA バージョン	CITRIX WORKSPACE アプリ FOR WINDOWS バージョン	CITRIX WORKSPACE アプリ FOR MAC バージョン	CITRIX WORKSPACE アプリ FOR LINUX バージョン	CITRIX WORKSPACE アプリ FOR HTML5バージョン
ICAメトリック	ICA RTT	2507以降	NA	NA	2503以降	2503以降	2503以降	2503以降
	ネットワーク遅延	2507以降	NA	NA	2503以降	2503以降	2503以降	2503以降
	HDX接続タイプ	2411以降	NA	NA	2411以降	2411以降	2411以降	2411以降
	プロトコル	2411以降	NA	NA	2411以降	2411以降	2411以降	2411以降
	EDT MTU	2411以降	NA	NA	2411以降	2411以降	2411以降	2411以降

データ定義:

UIパラメーター	説明
ICA RTT	ユーザー操作から画面応答までの時間を測定します。Thinwire RTTカウンターは、Citrix Virtual Apps and Desktopsバージョン2507以降、このメトリックを表します。以前のバージョンでは引き続きEUEM RTTを使用します。

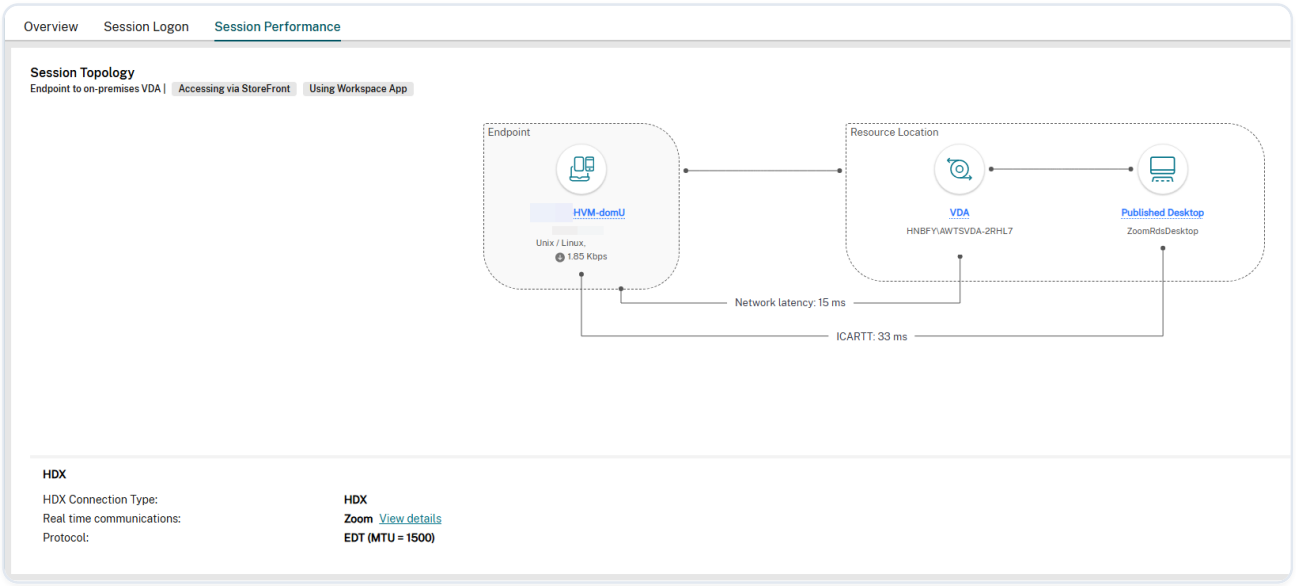
UIパラメーター	説明
ネットワーク遅延	ネットワーク遅延と潜在的な速度低下を示します。Citrix Virtual Apps and Desktopsバージョン2503以降、クライアント側とサーバー側の遅延の合計として定義されます。以前のバージョンでは、VDAで報告されるHDX遅延を引き続き使用します。
HDX接続タイプ	ユーザーセッションのHDX接続タイプ。
プロトコル	ユーザーセッションに使用される基盤となるプロトコル。値は*TCP*または*EDT*です。
EDT MTU	MTU（Maximum Transmission Unit）は、ネットワークインターフェイスがフラグメント化することなく送信できるパケットの最大サイズ（バイト単位）です。EDT MTUは、ユーザーのEDTセッション用に確立されたMTUを表します。

リアルタイム通信の最適化の可視性
セッショントポロジは、Citrixセッション内のMicrosoft Teams、Zoom、WebExなどのリアルタイム通信（RTC）アプリケーションの最適化ステータスに関する包括的な可視性を提供します。これにより、アプリケーションが最適化されているかどうかを特定し、最適なパフォーマンスを妨げる不足しているコンポーネント（必要なプラグイン、プラグイン管理、プラットフォーム固有の制限など）を識別します。

利点:

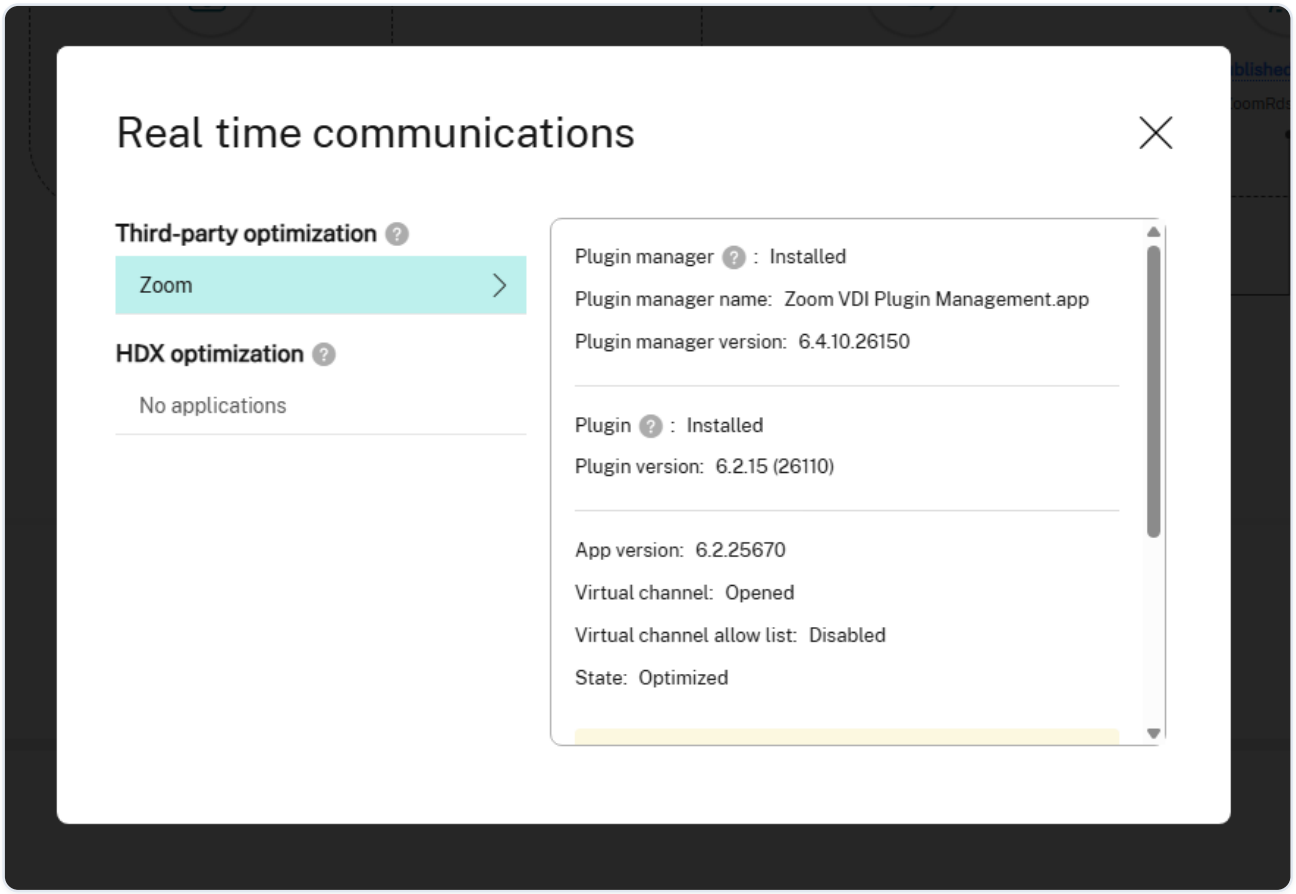
- 顧客はRTCアプリケーションの最適化に関して明確な保証を得られ、セッションが本当に最適化されているかどうかを推測する必要がなくなります。
- 不足しているコンポーネントを直接把握することで、問題をプロアクティブに対処し、完全な最適化を実現できます。
- トラブルシューティングの高速化により、重要なコミュニケーションツールのユーザーエクスペリエンスが向上します。

各アプリケーションの最適化の詳細を表示するには、**Session Topology** の **Real time communications** フィールドを使用します。



サードパーティ製の最適化されたアプリケーションは、Citrixテクノロジーを使用して仮想チャネルを作成しますが、その他の構成と設定はアプリケーションベンダーが管理します。最適化はベンダーが所有するソリューションに依存します。

Session Topology 画面の **Real time communications** フィールドの横にある **View details** リンクをクリックします。次の画面が表示されます。



HDX最適化アプリケーションはCitrix仮想チャネルを使用し、Citrixの構成と設定によって直接影響を受けます。

Real time communications 画面の **HDX optimization** セクションをクリックします。次の画像が表示されます。

MS Teamsリアルタイム通信(/en-us/citrix-daas/media/msteams-real-time-opt.png)

リアルタイム通信の詳細は5分ごとに更新されます。次の表は、サードパーティの最適化に依存するアプリケーションで利用可能な詳細を示します。完全な可視性を得るには、サポートされている製品バージョンを使用していることを確認してください。

注：

- Microsoft Teams Slimcore Optimizationは、公開デスクトップおよびベンダーサポートに従ったNew Teamsでのみ利用可能です。
- Zoomの場合、プラグインの詳細と最適化の状態を取得するためのベンダーの変更はバージョン6.3.10以降で利用可能です。詳細については、Zoomドキュメントを参照してください。

次の表に、Citrix HDX最適化に依存するアプリケーションで利用可能な詳細を示します。完全な可視性を得るには、サポートされている製品バージョンを使用していることを確認してください。

機能名	UIパラメーター	VIRTUAL DELIVERY AGENTバージョン	CITRIX WORKSPACE APP FOR WINDOWS のバージョン	CITRIX WORKSPACE APP FOR MAC のバージョン	CITRIX WORKSPACE APP LINUX版 バージョン
Microsoft Teams スリムコア	プラグインマネージャー、プラグインマネージャー名、プラグインマネージャーバージョン	2503	2503	ベンダーによってサポートされていません	ベンダーによってサポートされていません
	アプリバージョン、仮想チャネ	2503	2402	ベンダーではサポート	ベンダーではサポート

機能名	UIパラメーター	VIRTUAL DELIVERY AGENTバージョン	CITRIX WORKSPACE APP FOR WINDOWS のバージョン	CITRIX WORKSPACE APP FOR MAC のバージョン	CITRIX WORKSPACE APP LINUX版 バージョン
	ル、仮想チャネル許可リスト			されていません	されていません
	プラグイン、プラグインバージョン、状態	2507	2503	ベンダーではサポートされていません	ベンダーではサポートされていません
ズーム	プラグインマネージャー、プラグインマネージャー名、プラグインマネージャーバージョン	2507	2503	2505	プラグインが利用できません
	アプリバージョン、仮想チャネル、仮想チャネル許可リスト	2507	2402	2402	2402
	プラグイン、プラグインバージョン、状態	2507	2503	2505	プラグインが利用できません
ウェブエックス	プラグインマネージャー、プラグインマネージャー	2507	2503	プラグインは利用できません	プラグインは利用できません

機能名	UIパラメーター	VIRTUAL DELIVERY AGENTバージョン	CITRIX WORKSPACE APP FOR WINDOWS のバージョン	CITRIX WORKSPACE APP FOR MAC のバージョン	CITRIX WORKSPACE APP LINUX版 バージョン
	名、プラグインマネージャーバージョン				
	アプリのバージョン、仮想チャネル、仮想チャネル許可リスト	2507	2402	2402	2402

次の表に、Citrix HDX最適化に依存するアプリケーションで利用可能な詳細を示します。完全な可視性を得るには、サポートされている製品バージョンを使用していることを確認してください。

機能名	UIパラメーター	VIRTUAL DELIVERY AGENTバージョン	CITRIX WORKSPACE APP FOR WINDOWS のバージョン	CITRIX WORKSPACE APP FOR MAC のバージョン	CITRIX WORKSPACE APP LINUX版 バージョン
マイクロソフト チームズ	状態	1906.2	2112	2203	2203

データ定義:

UIパラメーター	説明
プラグインマネージャー	プラグインマネージャーがインストールされているかどうかを示します。プラグインマネージャーは、仮想チャネルを開き、最適化に必要なメディアエンジン（プラグイン）をダウンロードする小さな管理コンポーネントです。

UIパラメーター	説明
	注：機能はベンダーによって異なる場合があります。
プラグインマネージャー名	インストールされているプラグインマネージャーの名前。
プラグインマネージャーのバージョン	インストールされているプラグインマネージャーのバージョン。
プラグイン	プラグインがインストールされているかどうかを示します。プラグインは最適化に必要なメディアエンジンです。注：機能はベンダーによって異なる場合があります。
プラグインのバージョン	エンドポイントにインストールされているプラグインのバージョン。
アプリケーションのバージョン	仮想配信エージェント (VDA) 上のアプリケーションのバージョンを表します。
仮想チャネル	リアルタイム通信アプリの仮想チャネルが開いているか閉じているかを表します。
仮想チャネル許可リスト	仮想チャネルのステータスを示します。値は *有効* または *無効* です。
状態	特定のユーザーセッションにおけるアプリケーションの最適化状態を示します。

セッショントポロジのシナリオ

サイトの展開シナリオに応じて、セッションに関与するコンポーネントは次のすべてまたは一部です。

- エンドポイント上のCitrix Workspaceアプリ
- Gatewayサービス/オンプレミスGateway
- Cloud Connector – ハイブリッド接続の場合、GatewayはCloud Connectorを介してDaaSに接続されます。
- VDA

したがって、可能なネットワークトポロジは次のとおりです。

- エンドポイント上のCitrix Workspaceアプリは、Citrix WorkspaceおよびGateway Serviceを介してオンプレミスのVDAに接続します。VDAへの接続にCloud Connectorは使用されません。

セッショントポロジビュー(/en-us/citrix-virtual-apps-desktops/2503/media/dir-session-topology1.png)

- エンドポイント上のCitrix Workspaceアプリは、Citrix WorkspaceおよびGateway Serviceを介して、Cloud Connector経由でオンプレミスのVDAに接続します。

セッショントポロジビュー(/en-us/citrix-virtual-apps-desktops/2503/media/dir-session-topology2.png)

- エンドポイント上のCitrix Workspaceアプリは、StoreFront™およびオンプレミスGatewayを介してオンプレミスVDAに接続します。

セッショントポロジビュー(/en-us/citrix-virtual-apps-desktops/2503/media/dir-session-topology3.png)

- エンドポイント上のCitrix Workspaceアプリは、StoreFrontを介してオンプレミスVDAに接続します。

セッショントポロジビュー(/en-us/citrix-virtual-apps-desktops/2503/media/dir-session-topology4.png)

パフォーマンスメトリック

パフォーマンスメトリックパネルでは、ユーザーセッション内の問題を特定するためにリアルタイムメトリックを関連付けることができます。セッションメトリックの傾向は、これらのメトリックが時間の経過とともにどのようにパフォーマンスを発揮したかを示すのに役立ちます。**セッションパフォーマンス**タブをクリックすると、リアルタイムデータとともに、過去15分間および48時間分のデータを表示できます。プロットは、複数のコンポーネントのパフォーマンスメトリックを単一のビューで関連付けるのに役立ちます。

セッションパフォーマンスメトリック(/en-us/citrix-virtual-apps-desktops/2503/media/dir-session-performance-trends.png)

> **注:**
>
> - 過去15分間のメトリックサポートにより、セッションが接続および切断された期間のグラフがプロットされます。切断されたセッションのメトリックはゼロ値で表示されます。

- 過去48時間のメトリックサポートにより、ICARTT、ICA待機時間、およびセッション再接続のプロットが履歴データメトリックで更新されます。セッション再接続情報は、中断のあるネットワーク接続を表示およびトラブルシューティングするのに役立ちます。また、シームレスなエクスペリエンスを持つネットワークも分析します。セッション再接続数、合計セッション再接続数、自動クライアント再接続、およびセッション信頼性再接続の数を確認するためのグラフ。

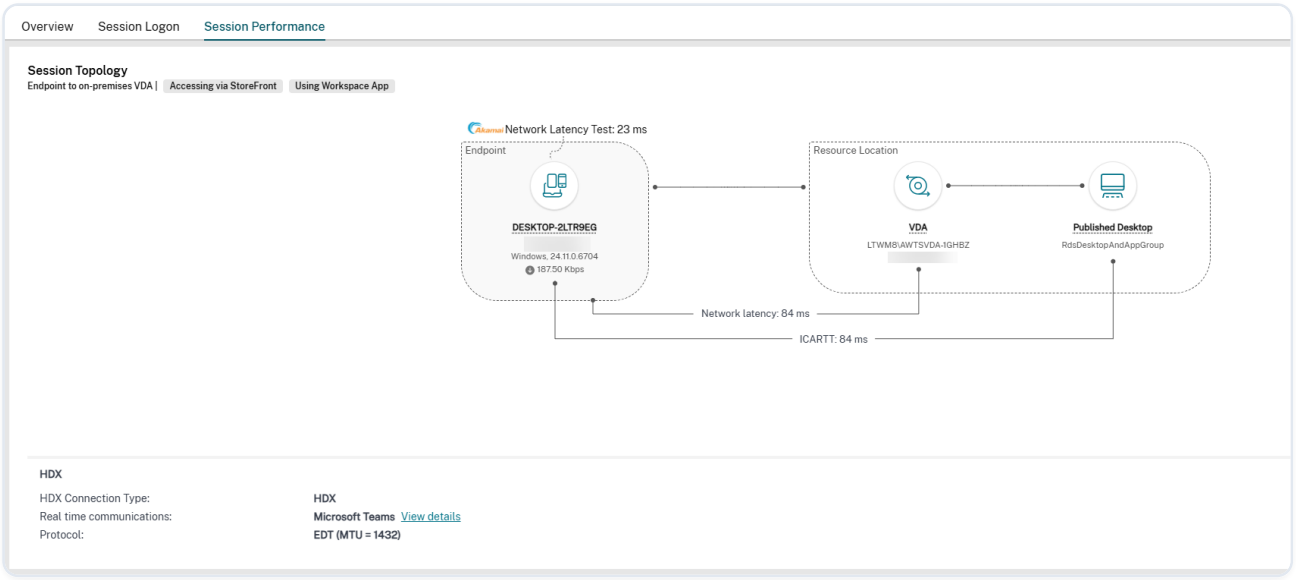
ICARTTとICA Latencyの他に、リアルタイムおよび過去15分間のメトリックとして以下のメトリックが利用可能です。

- 1秒あたりのフレーム数 - 1秒あたりのフレーム数は、セッションの応答性を示す重要なメトリックです。
- 利用可能な出力帯域幅 - 利用可能な出力帯域幅は、VDAからエンドポイントにデータを送信するために利用可能な総帯域幅の尺度です。
- 消費された出力帯域幅 - 消費された出力帯域幅は、ユーザーにセッションを表示するためにVDAからエンドポイントに送信された実際のデータ量を示します。
- WAN待機時間 - NetScalerからエンドユーザーへのネットワークのクライアント側によって引き起こされる待機時間。
- DC待機時間 - ネットワークのサーバー側によって引き起こされる待機時間。つまり、NetScalerからバックエンドサーバーまで。
- L7クライアント待機時間 - ICAクライアントとNetScalerインスタンス間で観測された平均L7待機時間。このメトリックは、配信パスに存在する非Citrixデバイスで役立ちます。
- L7サーバー待機時間 - NetScalerデバイスとCitrix Virtual App間で観測された平均L7待機時間。このメトリックは、配信パスに存在する非Citrixデバイスで役立ちます。
- クライアント再送信 - NetScalerとエンドユーザー間の接続で再送信されたパケットの数。このメトリックの値が高い場合、再送信による高い帯域幅使用率を示しますが、必ずしもユーザーエクスペリエンスが悪いことを意味するわけではありません。
- サーバー再送信 - NetScalerとバックエンドサーバー間の接続で再送信されたパケットの数。

利用可能な出力帯域幅と消費された出力帯域幅を分析することで、セッションを提供するために十分な帯域幅が利用可能であるか、またセッションが帯域幅不足の影響を受けているかどうかを確認できます。

HDX最適化の詳細

セッショントポロジ画面でHDX最適化の詳細を表示できます。



以下の詳細が表示されます。

- **HDX接続タイプ**: HDXまたは非HDX
- 「**リアルタイム通信**」：現在のところ、Microsoft Teamsのみがサポートされています。「**詳細を表示**」をクリックできます。
- 「**プロトコル**」：使用されているプロトコルを表示します。

新機能を使用するには、次の前提条件を満たすことをお勧めします。

前提条件:

- Windows向けCitrix Workspaceアプリバージョン2503
- VDA 2503
- SlimCoreの場合：
  - SlimCore用プラグインマネージャーがエンドポイントにインストールされていること
  - 仮想チャネルの許可リスト構成
  - 仮想チャネルが開いていること

> **注:**
>
> この機能はHDXセッション専用です。

リアルタイム通信の詳細を表示

リアルタイム通信の一部としてアプリケーションを監視できます。ただし、現在のところ、HDX最適化されているかどうかにかかわらず、Microsoft Teamsのみが監視されます。この機能により、Microsoft Teams以外の監視対象ソフトウェアを追加できる可能性があります。また、アプリケーションの横にある「**詳細を表示**」をクリックすると、追加の詳細を表示できます。

セッションパフォーマンスの詳細を表示(/en-us/citrix-virtual-apps-desktops/2503/media/session-performance-details.png)

上の画像では、アプリケーションはサードパーティ最適化とHDX最適化に分類されています。Microsoft Teams SlimCoreの場合、サードパーティ最適化の一部です。そうでない場合は、HDX最適化されています。

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

以前は、EUEMサービスまたはプロファイル管理サービスが実行に失敗した場合、ICA RTTまたはセッションログオン期間に関連するデータ取得の失敗理由が表示されませんでした。この新機能により、失敗の理由とその失敗に対する対応する解決策を得ることができます。**詳細**リンクには、次の表に示すように、ICA RTTおよびセッションログオン期間のエラー、失敗の理由、および解決策が記載されています。

エラーの種類	エラー	エラーメッセージ	解決策
ICA RTTエラー	ICA RTT値が表示されません。	**Citrix End User Experience Monitoringが実行されていません。**	1. サービスコンソールを開きます。このコンソールを開くには、**スタート**をクリックし、**サービス**と入力します。
			2. Citrix End User Experience Monitoring Serviceが実行されていることを確認します。
			3. デスクトップセッションを再度開き、試してください。ICA RTT値が表示されるはずです。

エラーの種類	エラー	エラーメッセージ	解決策
			4. 問題が解決しない場合は、Citrix管理者に連絡してください。
ICA RTTエラー	ICA RTT値が表示されません。	**Citrix End User Experience Monitoring がインストールされていません。**	1. VDAを再インストールしてください。
			2. サービスコンソールを開きます。このコンソールを開くには、**スタート**をクリックし、「サービス」と入力します。
			3. Citrix End User Experience Monitoring Service が実行されていることを確認します。
			4. デスクトップセッションを再度開き、試してください。ICA RTT の値が表示されるはずです。
			5. 問題が解決しない場合は、Citrix 管理者に連絡してください。
ICA RTT エラー	ICA RTT の値が表示されません。	**データの取得エラー。**	1. サービスコンソールを開きます。このコンソールを開くには、**スタート**をクリックし、「サー

エラーの種類	エラー	エラーメッセージ	解決策
			ビス」と入力します。
			`2.` **Windows Management Instrumentation Service** が実行されていることを確認してください。
			`3.` また、WfShell.exe/PicaShell.exe プロセスが**アクティビティマネージャー** > **プロセス** タブで実行されていることを確認してください。実行されていない場合は、デスクトップセッションを再開してください。
			`4.` 前述の手順で解決しない場合は、Citrix_Euem_RoundTrip インスタンスが存在することを確認するために、次のコマンドを実行してください。`Get-CimInstance -Namespace 'ROOT\Citrix\Euem' -Query "select * from Citrix_Euem_RoundTrip"`
			`5.` Citrix_Euem_Round

エラーの種類	エラー	エラーメッセージ	解決策
			Trip インスタンスが存在する場合は、デスクトップセッションを再開してください。
			6. 問題が解決しない場合は、Citrix 管理者に連絡してください。
セッションログオン期間エラー	グラフが読み込まれていません。	**Citrix Profile Management が実行されていません**	1. サービスコンソールを開きます。このコンソールを開くには、**スタート**をクリックし、「サービス」と入力します。
			2. **Citrix Profile Management Service**が実行されていることを確認します。
			3. デスクトップセッションを再度開き、試してください。グラフが表示されるはずです。
			4. 問題が解決しない場合は、Citrix 管理者に問い合わせてください。
セッションログオン期間エラー	グラフが読み込まれていません。	**Citrix Profile Managementがインストールされていません。**	1. Citrix Profile Managementサービスをインストールします。

エラーの種類	エラー	エラーメッセージ	解決策
			2. サービスコンソールを開きます。このコンソールを開くには、**スタート**をクリックし、「サービス」と入力します。
			3. **Citrix Profile Management**サービスが実行されていることを確認します。
			4. デスクトップセッションを再度開き、試してください。グラフが表示されるはずです。
			5. 問題が解決しない場合は、Citrix 管理者に連絡してください。
セッションログオン期間エラー	グラフが読み込まれません。	**データの取得中にエラーが発生しました。**	1. **サービス**コンソールを開きます。このコンソールを開くには、**スタート**をクリックし、「サービス」と入力します。
			2. **Windows Management Instrumentation Service**が実行されていることを確認してください。
			3. 前述のサービスがすでに実行されて

エラーの種類	エラー	エラーメッセージ	解決策
			いる場合は、次のコマンドを実行して、`LogonTimings instance is present` を確認します: `Get-CimInstance -Namespace 'ROOT\Citrix\Profile\Metrics' -Query "select * from LogonTimings"`
			`4.` 問題が解決しない場合は、Citrix管理者に問い合わせてください。
ICA RTTエラー	ICA RTT値が表示されません。	コンソールはサポートされていません。	HDXを使用してセッションを開始します。
ICA RTTエラー	ICA RTT値が表示されません。	リモートデスクトッププロトコル (RDP) はサポートされていません。	HDXを使用してセッションを開始します。
ICA RTTエラー	ICA RTT値が表示されません。	詳細なエラー検出とすべての機能へのアクセスを得るには、VDAをバージョン2402以降にアップグレードしてください。	VDAを2402以降にアップグレードしてください。
セッションログオン期間エラー	グラフが読み込まれていません。	Citrix Profile Management WMIプラグインがインストールされていません。	Citrix Profile Management WMIプラグインをインストールしてください。

終了したユーザーセッションの診断

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

- マシンの詳細パネル - 選択したセッションが起動されたマシンの利用可能な詳細を表示します
- セッションの詳細パネル - 選択したセッションの利用可能な詳細を表示します。
- セッションログオン期間 - 選択したセッションにかかったログオン期間に関する情報を表示します。以下の時間にかかったチャートを表示できます。
    - ブローカリング
    - マシンの起動
    - HDX™ 接続
    - 認証
    - GPO
    - ログオンスクリプト
    - ディスクへのプロファイル読み込み
    - 対話型セッション

過去のユーザーセッションを表示するには、次の手順を実行します。

1. **フィルター** > **セッション** ビューをクリックします。
2. 「**関連ユーザー**」をクリックして、ユーザーのアクティビティマネージャーを開きます。

    履歴ユーザーセッションのアクティビティマネージャー(/en-us/citrix-virtual-apps-desktops/2503/media/dir-his-user-sessions-am.png)
3. 「**終了したセッション**」セクションから、必要なセッションを選択します。
4. 「**マシン詳細**」パネルと「**セッション詳細**」パネルを表示します。

    履歴ユーザーセッションの詳細(/en-us/citrix-virtual-apps-desktops/2503/media/dir-his-user-sessions-details.png)
5. 下にスクロールして、終了したセッションの「**セッションログオン期間**」を表示します。

    履歴ユーザーセッションの期間(/en-us/citrix-virtual-apps-desktops/2503/media/dir-his-user-sessions-duration.png)

6. 「**セッションログオン**」タブをクリックして、詳細を表示します。

   終了したユーザーセッションのログオン期間(/en-us/citrix-virtual-apps-desktops/2503/media/session-logon-ended.png)

7. 「**セッションパフォーマンス**」タブをクリックして、詳細を表示します。

   終了したユーザーセッションのパフォーマンス(/en-us/citrix-virtual-apps-desktops/2503/media/session-performance-ended.png)

ユーザーのシャドウ

Directorから、シャドウユーザー機能を使用して、ユーザーの仮想マシンまたはセッションを直接表示したり操作したりできます。Windows VDAとLinux VDAの両方をシャドウできます。ユーザーは、シャドウするマシンに接続している必要があります。これは、ユーザーのタイトルバーに表示されているマシン名を確認することで検証できます。

Directorは新しいタブでシャドウイングを起動します。DirectorのURLからのポップアップを許可するようにブラウザ設定を更新してください。

シャドウイング機能は、**ユーザーの詳細**ビューからアクセスします。ユーザーセッションを選択し、アクティビティマネージャービューまたはセッションの詳細パネルで**シャドウ**をクリックします。

Linux VDAのシャドウ

シャドウイングは、RHEL7.3またはUbuntuバージョン16.04のLinuxディストリビューションを実行している、バージョン7.16以降のLinux VDAで利用できます。

> **注:**
>
> - シャドウイングが機能するには、VDAがDirector UIからアクセス可能である必要があります。したがって、シャドウイングはDirectorクライアントと同じイントラネット内のLinux VDAでのみ可能です。
> - DirectorはFQDNを使用してターゲットLinux VDAに接続します。Directorクライアントが Linux VDAのFQDNを解決できることを確認してください。
> - VDAには、python websockifyおよびx11vncパッケージがインストールされている必要があります。
> - VDAへのnoVNC接続はWebSocketプロトコルを使用します。デフォルトでは、**ws://** WebSocketプロトコルが使用されます。セキュリティ上の理由から、Citrixは安全な

> **wss://** プロトコルを使用することを推奨します。各DirectorクライアントとLinux VDAにSSL証明書をインストールしてください。

> セッションシャドウイングの指示に従って、シャドウイング用にVDAを構成してください。

1. **シャドウ**をクリックすると、シャドウイング接続が初期化され、ユーザーデバイスに確認プロンプトが表示されます。
2. ユーザーに**はい**をクリックするよう指示して、マシンまたはセッションの共有を開始します。
3. 管理者はシャドウされたセッションを表示することのみ可能です。

Windows VDA のシャドウイング

Windows VDA セッションのシャドウイングには、Windows リモートアシスタンスを使用します。VDA のインストール時に、**User Windows Remote Assistance** 機能を有効にします。詳しくは、機能の有効化または無効化を参照してください。

1. **シャドウ**をクリックするとシャドウイング接続が初期化され、.msrc インシデントファイルを開くか保存するかを確認するダイアログボックスが表示されます。
2. 既定で選択されていない場合は、リモートアシスタンスビューアーでインシデントファイルを開きます。ユーザーデバイスに確認のプロンプトが表示されます。
3. ユーザーに**はい**をクリックして、マシンまたはセッションの共有を開始するよう案内します。
4. さらに操作するには、キーボードとマウスの制御を共有するようユーザーに依頼します。

シャドウイング用に MICROSOFT INTERNET EXPLORER ブラウザーを効率化する

ダウンロードした Microsoft リモートアシスタンス（.msra）ファイルをリモートアシスタンスクライアントで自動的に開くように、Microsoft Internet Explorer ブラウザーを構成します。

これを行うには、グループポリシーエディターで「ファイルのダウンロード時に自動的にダイアログを表示」設定を有効にする必要があります：

コンピューターの構成 \> 管理用テンプレート \> Windows コンポーネント \> Internet Explorer \> インターネットコントロールパネル \> セキュリティページ \> インターネットゾーン \> ファイルのダウンロード時に自動的にダイアログを表示。

既定では、このオプションはローカルイントラネットゾーンのサイトで有効になっています。Director サイトがローカルイントラネットゾーンにない場合は、そのサイトをこのゾーンに手動で追加することを検討してください。

デスクトップ接続を復元する

Directorから、ユーザーのタイトルバーで現在のマシンに対するユーザーの接続ステータスを確認します。

デスクトップ接続に失敗した場合、失敗の原因となったエラーが表示され、トラブルシューティングの方法を決定するのに役立ちます。

アクション	説明
マシンがメンテナンスモードでないことを確認する	［ユーザーの詳細］ページで、メンテナンスモードがオフになっていることを確認します。
ユーザーのマシンを再起動する	マシンを選択し、**［再起動］**をクリックします。ユーザーのマシンが応答しない、または接続できない場合にこのオプションを使用します。たとえば、マシンが異常に高いCPUリソースを使用しており、CPUが使用不能になっている場合などです。

HDX™ チャネルシステムレポートを実行する

ユーザーの詳細ビューで、**HDX**パネルにあるユーザーのマシン上のHDXチャネルのステータスを確認します。このパネルは、ユーザーのマシンがHDXを使用して接続されている場合にのみ利用可能です。

情報が現在利用できないことを示すメッセージが表示された場合は、ページが更新されるまで1分間待つか、「**更新**」ボタンを選択してください。HDXデータは、他のデータよりも更新に時間がかかります。

詳細については、エラーまたは警告アイコンをクリックしてください。

> ヒント：
>
> タイトルバーの左隅にある左右の矢印をクリックすると、同じダイアログボックスで他のチャネルに関する情報を表示できます。
>
> HDXチャネルシステムレポートは、主にCitrixサポートがさらなるトラブルシューティングのために使用します。

1. HDXパネルで、をクリックします。

2. .xmlレポートファイルを表示または保存できます。

   - .xmlファイルを表示するには、をクリックします。.xmlファイルは、Directorアプリケーションと同じウィンドウに表示されます。
   - .xmlファイルを保存するには、をクリックします。ウィンドウが表示され、Directorマシン上のファイルのダウンロード先を尋ねられます。

ユーザープロファイルをリセットする

> **注意:**
>
> プロファイルがリセットされると、ユーザーのフォルダーとファイルは保存され、新しいプロファイルにコピーされます。ただし、ほとんどのユーザープロファイルデータは失われます（たとえば、レジストリがリセットされ、アプリケーション設定が削除される可能性があります）。
>
> リセット機能は、ファイルベースとコンテナベースの両方のプロファイルソリューションに適用されます。

リセットされたプロファイルの処理方法

Citrix®ユーザープロファイルまたはMicrosoftローミングプロファイルのいずれもリセットできます。ユーザーがログオフし、リセットコマンド（DirectorまたはPowerShell SDKを使用して）を選択すると、Directorはまず使用中のユーザープロファイルを識別し、適切なリセットコマンドを発行します。Directorは、プロファイルサイズ、種類、ログオン時間などの情報を含むProfile Managementを介して情報を受け取ります。

この図は、ユーザープロファイルがリセットされた場合の、ユーザーログオン後のプロセスを示しています。

ユーザープロファイルのリセットフロー図(/en-us/citrix-virtual-apps-desktops/2503/media/userprofile.png)

Directorによって発行されたリセットコマンドは、プロファイルの種類を指定します。その後、Profile Managementサービスはその種類のプロファイルをリセットしようとし、適切なネットワーク共有（ユーザー格納場所）を探します。ユーザーがProfile Managementによって処理されているにもかかわらず、ローミングプロファイルコマンドを受け取った場合、それは拒否されます（またはその逆も同様です）。

1. ローカルプロファイルが存在する場合、それは削除されます。

2. ネットワークプロファイルの名前が変更されます。
3. 次のアクションは、リセットされるプロファイルがCitrixユーザープロファイルであるか、Microsoftローミングプロファイルであるかによって異なります。

   Citrixユーザープロファイルの場合、新しいプロファイルはProfile Managementのインポートルールを使用して作成されます。フォルダーはネットワークプロファイルにコピーされ、ユーザーは通常どおりログオンできます。リセットにローミングプロファイルが使用される場合、ローミングプロファイル内のレジストリ設定はリセットされたプロファイルに保持されます。必要に応じて、テンプレートプロファイルがローミングプロファイルを上書きするようにProfile Managementを構成できます。

   Microsoftローミングプロファイルの場合、Windowsはプロファイルを作成し、ユーザーがログオンすると、フォルダーはユーザーデバイスにコピーされます。ユーザーが再度ログオフすると、新しいプロファイルはネットワークストアにコピーされます。

Directorでユーザープロファイルをリセットするには

Citrix Virtual Desktops™ (Desktop VDA) を使用している場合は、次の操作を行います。

1. **Director** で、プロファイルをリセットするユーザーを検索し、そのユーザーのセッションを選択します。
2. をクリックします。
3. ユーザーにすべてのセッションからログオフするよう指示します。
4. ユーザーに再度ログオンするよう指示します。 ユーザーのプロファイルから保存されたフォルダーとファイルは、新しいプロファイルにコピーされます。

Citrix Virtual Desktops (Server VDA) を使用している場合は、プロファイルのリセットを実行するためにログオンしている必要があります。その後、ユーザーはログオフして再度ログオンし、プロファイルのリセットを完了する必要があります。

> **重要:**
>
> ユーザーが複数のプラットフォーム（Windows 8やWindows 7など）にプロファイルを持っている場合は、ユーザーが問題として報告したのと同じデスクトップまたはアプリに最初に再度ログオンするよう指示します。このログオン操作により、正しいプロファイルがリセットされます。プロファイルがCitrixユーザープロファイルの場合、ユーザーのデスクトップが表示されるまでにプロファイルはすでにリセットされています。プロファイルがMicrosoftローミングプロファイルの場合、フォルダーの復元が短時間進行中の可能性があります。ユーザーは復元が完了するまでログオンしたままにする必要があります。

> プロファイルが正常にリセットされない場合（たとえば、ユーザーがマシンに正常にログオンし直せない、または一部のファイルが欠落している場合）は、必要があります。

次の点に注意してください。

- ユーザープロファイルソリューションとしてユーザーストアが有効になっている場合、新しいプロファイルには元のユーザープロファイルから次の個人用フォルダーが含まれます。
  - デスクトップ
  - クッキー
  - お気に入り
  - ドキュメント
  - 画像
  - 音楽
  - ビデオ
- Citrix Profile Managementバージョン2407以降では、プロファイルコンテナがユーザープロファイルソリューション全体として有効になっている場合、新しいプロファイルは上記の個人用フォルダーを保持します。
- Windows 8以降では、プロファイルがリセットされてもCookieは新しいプロファイルにコピーされません。

リセットに失敗した後にプロファイルを手動で復元するには

1. ユーザーにすべてのセッションからログオフするよう指示します。
2. ローカルプロファイルが存在する場合は削除します。
3. フォルダー名に日付と時刻が追加されたアーカイブフォルダー（.upm_datestamp拡張子を持つフォルダー）をネットワーク共有上で見つけます。
4. 現在のプロファイル名（つまり、upm_datestamp拡張子のないもの）を削除します。
5. アーカイブされたフォルダーを元のプロファイル名にリネームします。つまり、日付と時刻の拡張子を削除します。これにより、プロファイルはリセット前の元の状態に戻ります。

PowerShell SDKを使用してプロファイルをリセットするには

Broker PowerShell SDKを使用してプロファイルをリセットできます。

NEW-BROKERMACHINECOMMAND

特定のユーザー、セッション、またはマシンに配信するためにキューに入れられたコマンドを作成します。このコマンドレットの詳細については、`<https://citrix.github.io/delivery-controller-sdk/Broker/New-BrokerMachineCommand/>`を参照してください。

例

PowerShell コマンドレットを使用してプロファイルをリセットする方法の詳細については、以下の例を参照してください。

Profile Management プロファイルをリセットする

- user1 のプロファイルをリセットしたいとします。New-BrokerMachineCommand PowerShell コマンドを使用します。例:
  - `New-BrokerMachineCommand -Category UserProfileManager -CommandName "ResetUpmProfile" -DesktopGroups 1 -CommandData $byteArray -SendTrigger logon -user domain1\user1`

> **重要:**
>
> `CommandData $byteArray` は次の形式である必要があります: `<SID>[,<backup path>]`。バックアップパスを指定しない場合、Profile Management は現在の日時で名前が付けられたバックアップフォルダーを生成します。

Windows ローミングプロファイルをリセットする

- user1 のローミングプロファイルをリセットしたいとします。New-BrokerMachineCommand PowerShell コマンドを使用します。例:
  - `New-BrokerMachineCommand -Category UserProfileManager -CommandName "ResetRoamingProfile" -DesktopGroups 1 -CommandData $byteArray -SendTrigger logon -user domain1\user1`

セッションを記録する

Directorの**ユーザー詳細**画面および**マシン詳細**画面から、セッション記録コントロールを使用してICA®セッションを記録できます。この機能は、**Premium**サイトのお客様にご利用いただけます。

動的セッション記録

ユーザー詳細画面のセッション記録コントロールを使用して、現在アクティブなセッションを記録できます。動的セッション記録の詳細については、セッション記録サービスの記事を参照してください。

ポリシーベースのセッション記録

DirectorConfigツールを使用してDirectorでポリシーベースのセッション記録を構成するには、セッション記録ポリシーの構成の「**Directorでセッション記録サーバーを使用するように構成する**」セクションを参照してください。 セッション記録コントロールは、ログインしているユーザーがセッション記録ポリシーを変更する権限を持っている場合にのみDirectorで利用できます。この権限は、ユーザーの承認で説明されているように、セッション記録承認コンソールで設定できます。

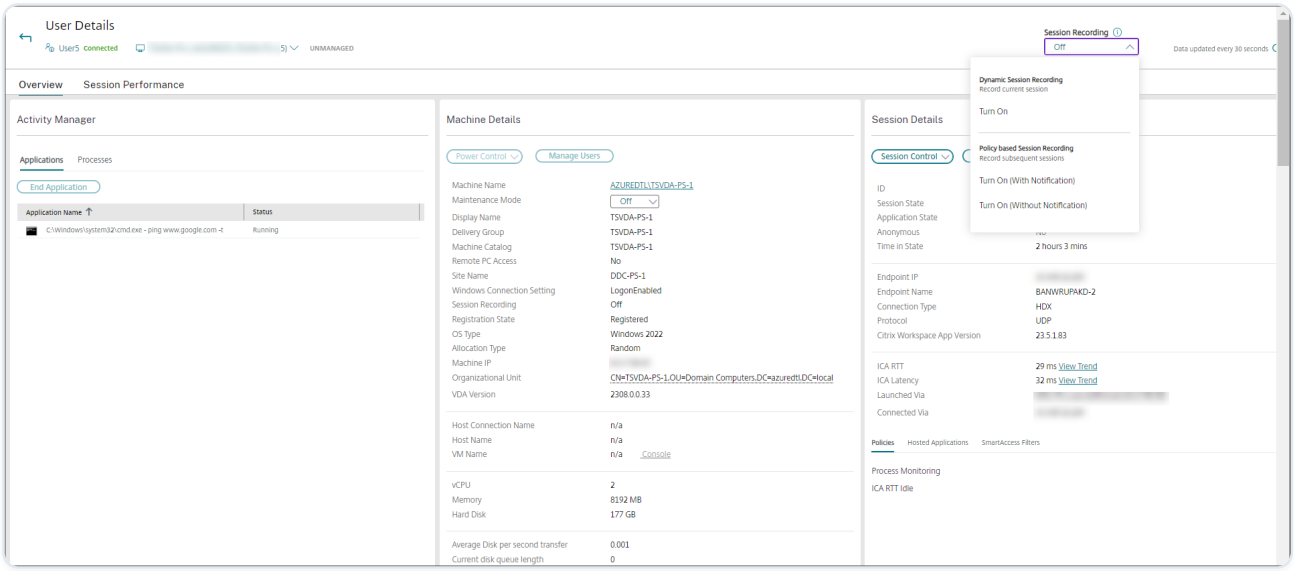
> **注:**
>
> Directorまたはセッション記録ポリシーコンソールを介してセッション記録設定に加えられた変更は、その後のICAセッションから有効になります。

Directorのセッション記録コントロール

ユーザー詳細 > **セッション記録**アクションを使用して、現在のセッションまたはその後のセッションを記録できます。

- 動的セッション記録をオンにする - 現在のセッションが記録されます。
- オンにする（通知あり） - その後のセッションが記録され、ICAセッションにログオンする際に、セッションが記録されていることがユーザーに通知されます。
- オンにする（通知なし） - その後のセッションが記録され、ユーザーに通知することなく、セッションがサイレントに記録されます。
- オフにする - ユーザーのセッション記録を無効にします。

ポリシーパネルには、アクティブなセッション記録ポリシーの名前が表示されます。



「**マシン詳細**」パネルには、マシンのセッション記録ポリシーのステータスが表示されます。

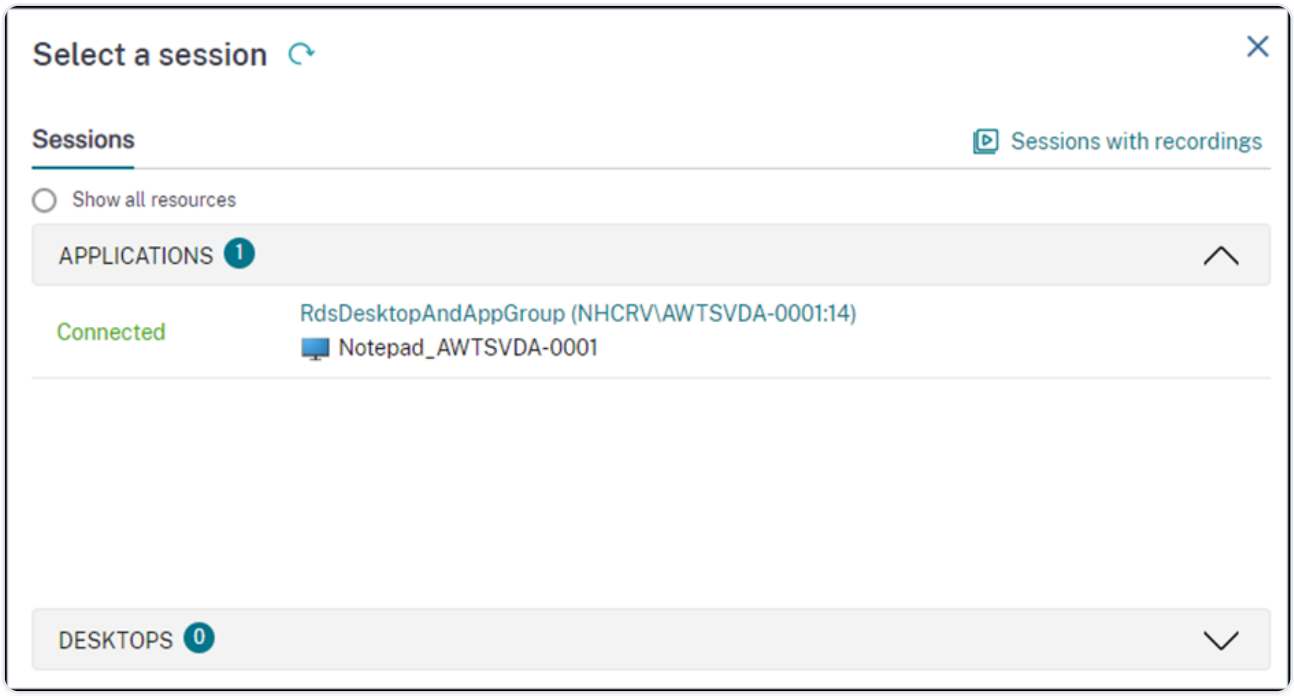
ライブセッションと記録されたセッションの再生

記録されたユーザーセッションとライブユーザーセッションを再生して、ユーザーが遭遇した問題を理解できます。Directorコンソール内で記録とセッション関連のメトリックにすぐにアクセスできるため、複数のセッション記録サーバーで記録を検索したり、記録を表示するためにサードパーティ製アプリを探したりする必要がなくなります。これにより、記録で発見された問題とパフォーマンスメトリックを関連付けることができます。

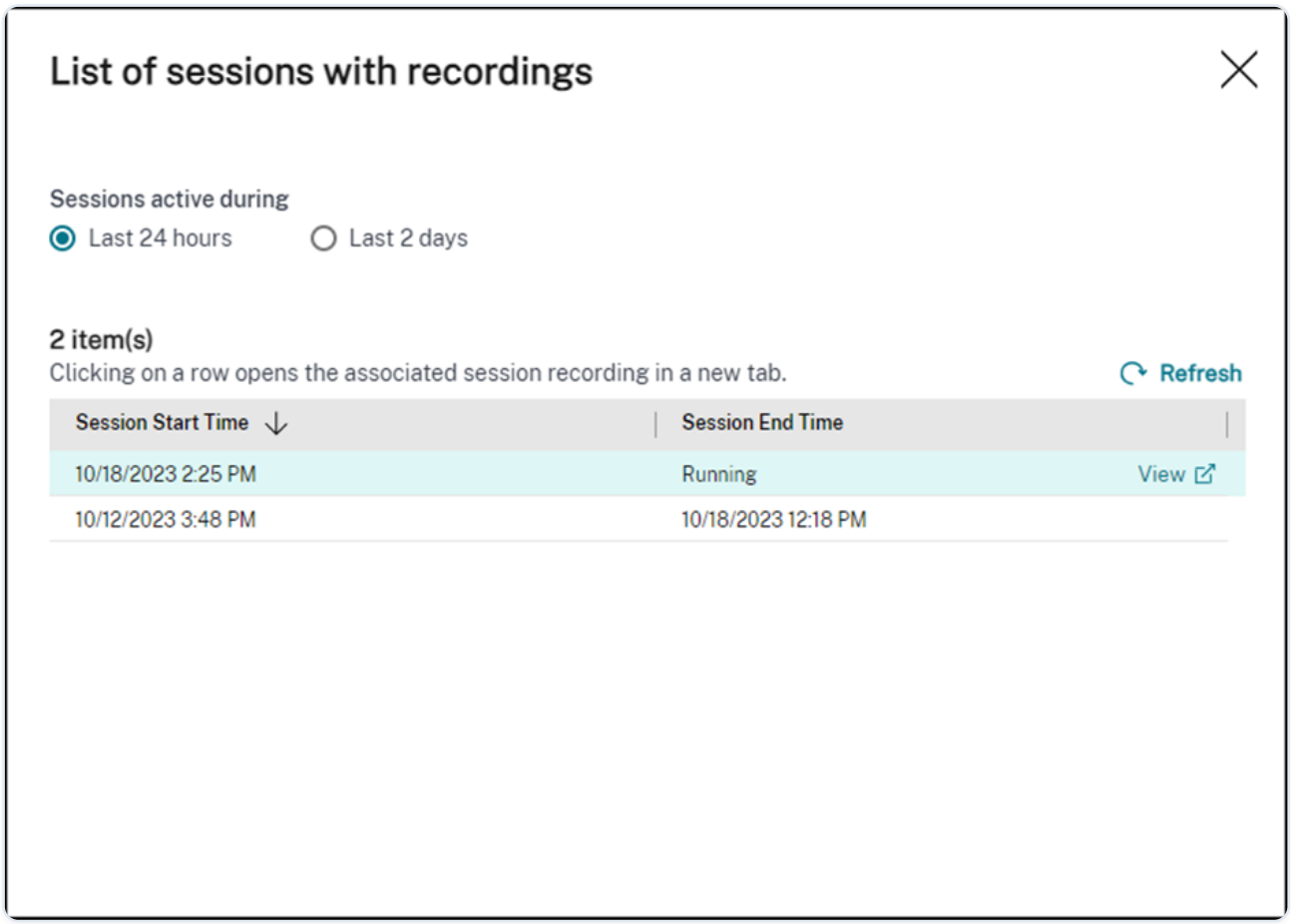
この機能には、以下が必要です。

- VDAおよびセッション記録サーバーはバージョン2308以降であること。
- Delivery Controller™およびDirectorはバージョン2311以降であること。

Directorはセッション記録を一元的なリポジトリに保存します。ユーザーに属する記録のリストは、**セッションセレクター**モーダル > **記録のあるセッション**リンクをクリックすると表示されます。



過去24時間または過去2日間にアクティブだったセッションの録画を表示することを選択できます。現在アクティブなセッションのライブ録画は、「**Session End Time**」が「**Running**」と表示されます。



表示リンクをクリックすると、Citrix Session Recording再生サーバーを使用して新しいタブで記録を再生できます。

ハイブリッドマルチクラウド展開向けの統合検索

以前は、Director でユーザーを検索してトリアージを行う際、ユーザーがオンプレミスサイトのユーザーである場合にのみユーザーの詳細が表示されていました。ユーザーがクラウドサイトのユーザーである場合は、Monitor に移動して再度検索する必要がありました。

この強化された検索機能を使用すると、Director の オプションを使用して、クラウドサイトまたはオンプレミスサイトのユーザーを検索できます。この機能は、ハイブリッド展開（クラウドサイトとオンプレミスサイトの両方）を使用している場合や、トリアージ目的で Director を使用している場合に利用できます。オンプレミスサイトかクラウドサイトかに関係なく、ユーザーの詳細を取得できます。サイトが Director に存在する場合は、選択したセッションの Activity Manager に Director で直接移動できます。サイトが Director に存在しない場合は、選択したセッションの Activity Manager に Monitor で直接移動できます。その後、トリアージを続行できます。

> **注：**
>
> Citrix Director を介して統合検索コンソールを使用できます。
>
> この機能により、問題解決までの平均時間が短縮され、クラウドユーザーとオンプレミスユーザーの両方に単一のコンソールでシームレスなエクスペリエンスが提供されます。追加の利点として、クラウドサイトの詳細のみが Director に追加されるため、データベースのサイズが急増することはありません。ユーザーの詳細はクラウド自体に保存されます。

> **注：**
>
> 6つ以下のクラウドサイトの場合、3秒以内に検索結果を取得できます。
>
> この機能を有効にするには、クラウドサイトを Director に接続する必要があります。

クラウドサイトを Director に接続する

前提条件

Citrix Director で統合検索を構成するために、新しいコンポーネントをインストールする必要はありません。次の要件が満たされていることを確認してください。

- 統合検索の場合、すべての Delivery Controller および Director がインストールされているマシンで、アウトバウンドインターネットアクセスが利用可能である必要があります。具体的には、次の URL へのアクセスが可能であることを確認してください。
  - Citrix キー登録: `<https://*.citrixnetworkapi.net/>`
  - Citrixクラウド: `<https://*.citrixworkspacesapi.net/>`
  - シトリックス DaaS: `<https://*.cloud.com/>`
  - マイクロソフト Azure: `<https://*.windows.net/>`
- Delivery ControllerとDirectorマシンがイントラネット内にあり、外部インターネットアクセスがプロキシサーバー経由である場合は、以下を確認してください。
  - プロキシサーバーは、前述のURLリストを許可する必要があります。
  - Directorの **web.config** および **citrix.monitor.exe.config** ファイルに次の構成を追加します。この構成を **configuration** タグ内に必ず追加してください。

```
<system.net>

    <defaultProxy>

        <proxy usesystemdefault="false" proxyaddress="http://
<your_proxyserver_address>:80" bypassonlocal="true" />

    </defaultProxy>

</system.net>
```

  - Directorの **web.config** は、Directorがインストールされているマシン上の `C:\inetpub\wwwroot\Director\web.config` にあります。
  - **citrix.monitor.exe.config** は、Delivery Controllerがインストールされているマシン上の `C:\Program Files\Citrix\Monitor\Service\Citrix.Monitor.exe.Config` にあります。

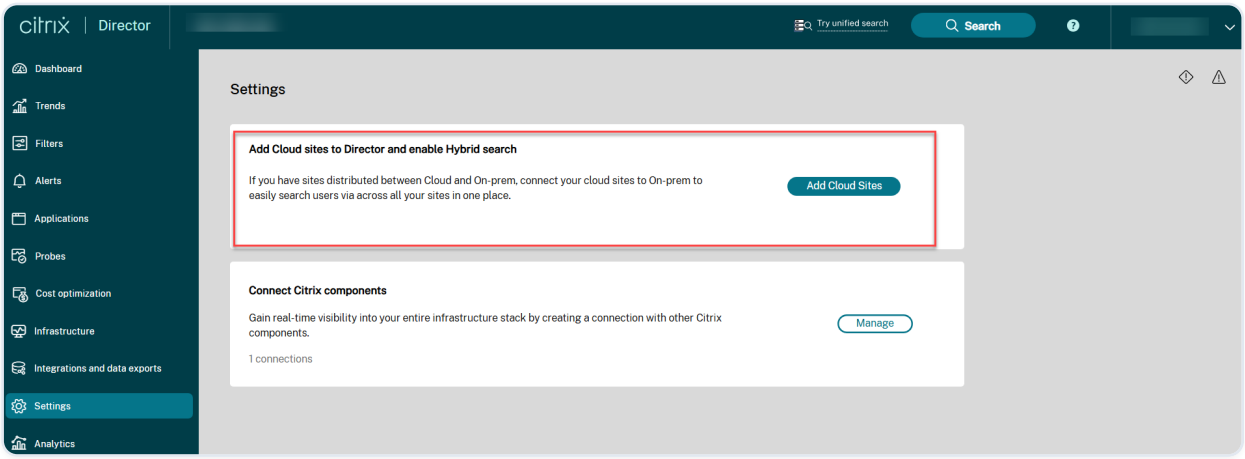
この設定は、IIS上のMicrosoftによって提供されます。詳細については、「プロキシ構成」を参照してください。構成ファイルの **defaultproxy** フィールドは、DirectorおよびMonitor Serviceの外部アクセスを制御します。Citrix DaaSとの構成および通信には、**defaultproxy** フィールドをtrueに設定する必要があります。適用されているポリシーによって、このフィールドがfalseに設定されている可能性があります。この場合、手動でフィールドをtrueに設定する必要があ

ります。変更を行う前に、構成ファイルのバックアップを取ってください。変更を有効にするには、Delivery Controllerで監視サービスを再起動してください。

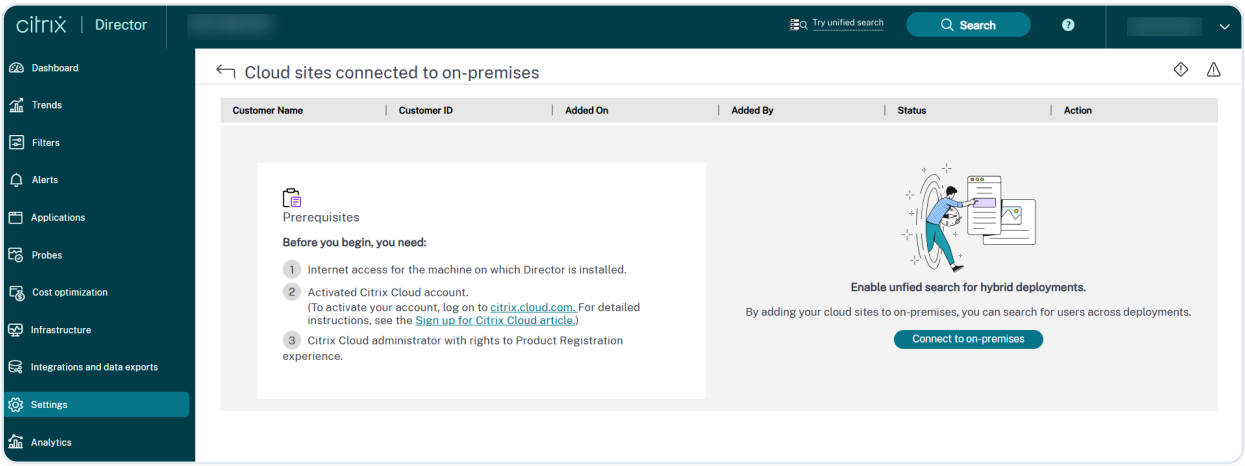
- DaaSのアクティブなCitrix Cloud™エンタイトルメントが必要です。
- Citrix Cloudアカウントは、製品登録エクスペリエンスへの権限を持つ管理者アカウントである必要があります。管理者権限の詳細については、「管理者権限の変更」を参照してください。
- Citrix Directorがインストールされているマシンにインターネットアクセスがあることを確認してください。
- Citrix Cloudサービスを使用するには、HTTPSポート443経由で必要なCitrixアドレスに接続できる必要があります。詳細については、「インターネット接続要件」を参照してください。
- 製品登録を実行するための完全な管理者アクセス権があることを確認してください。

構成手順

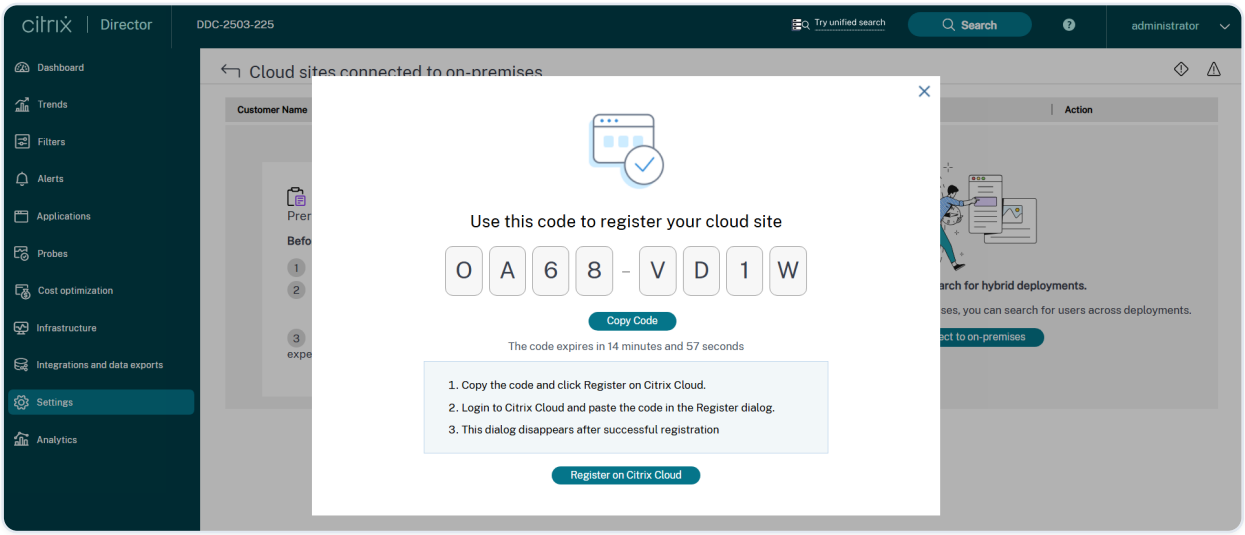
1. 完全な管理者としてDirectorにサインインします。Directorダッシュボードページが表示されます。
2. **設定**タブをクリックします。**設定**ページが表示されます。



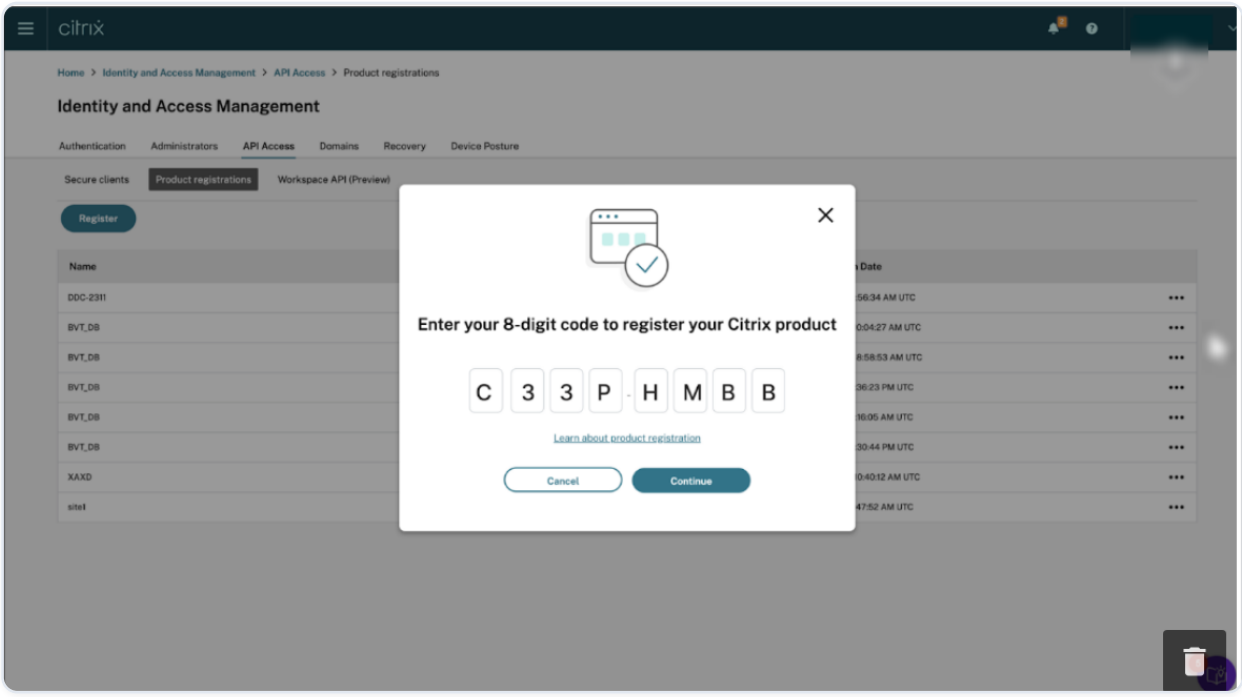
3. **クラウドサイトの追加**をクリックします。次のページが表示されます。



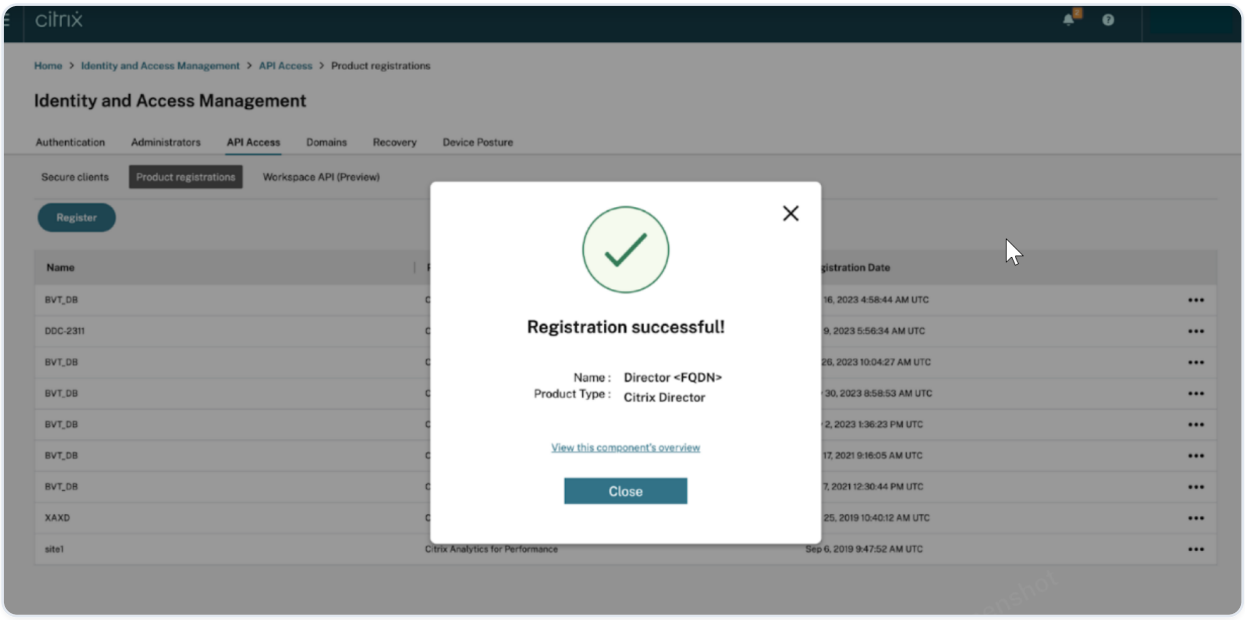
4. 前提条件を確認し、次に、**クラウドサイトの接続**をクリックして構成プロセスを開始します。このサイトをCitrix Cloudに登録するために使用する、一意の8桁の登録コードが生成されます。



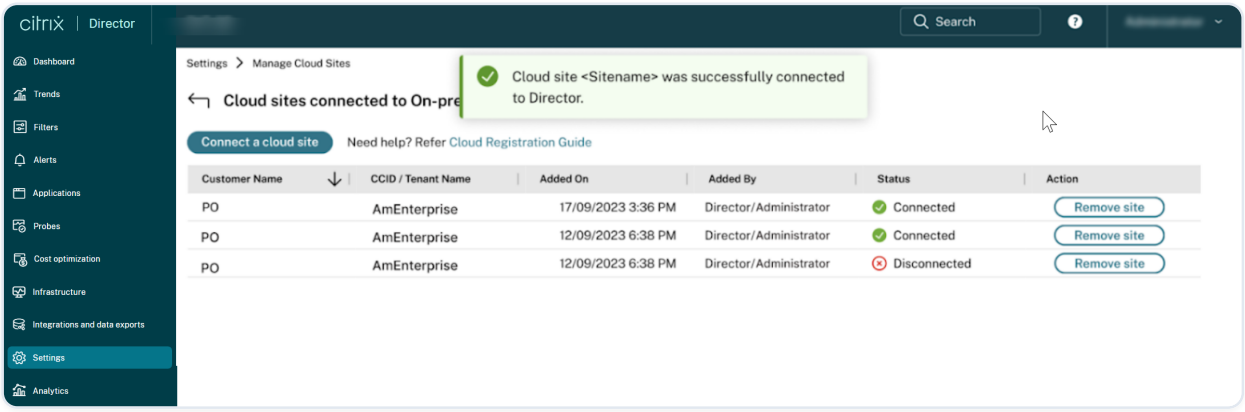
5. コードをコピーするには、**コードのコピー**をクリックし、次に、**Citrix Cloudで登録**をクリックします。Citrix Cloudの登録URLにリダイレクトされます。
6. Citrix Cloudの資格情報でサインインし、顧客を選択します。
7. コピーした登録コードをCitrix Cloudの**製品登録**ページに貼り付けます。サイトを登録するには、**続行**をクリックします。



8. **続行**をクリックします。クラウドサイトがCitrix Directorに登録され、次のメッセージが表示されます。



9. **閉じる**をクリックします。次の画面が表示されます。



10. Directorで複数のクラウドサイトを構成するには、Directorから各サイトについて上記の構成手順を繰り返します。

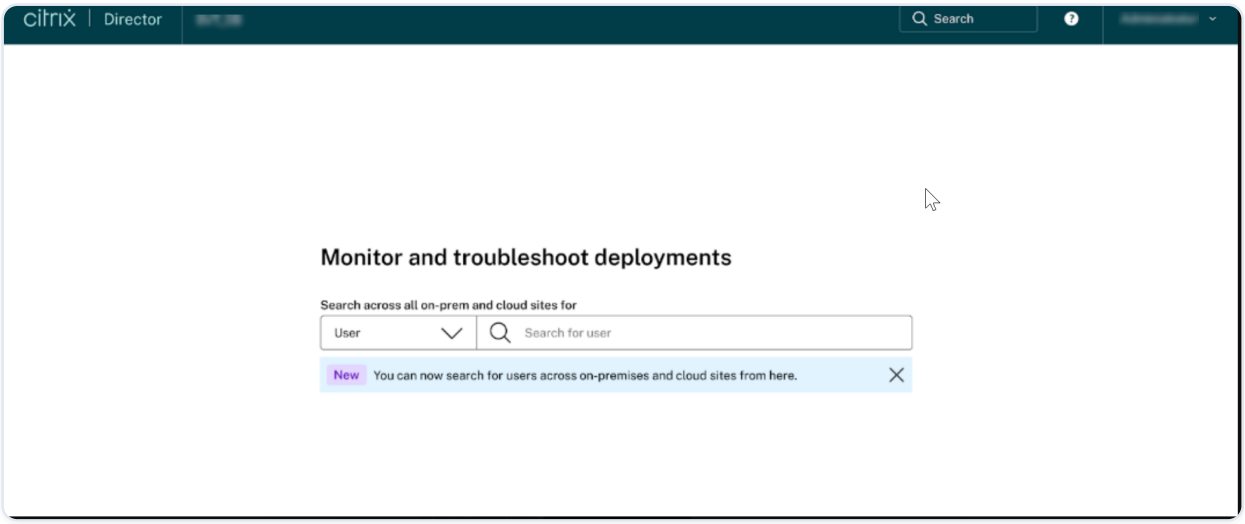
    サイトごとに複数のDirectorインスタンスが実行されている場合は、いずれか1つのDirectorインスタンスから構成します。サイトに接続されている他のすべてのDirectorインスタンスは、構成プロセス後の次回の更新時に更新されます。

> **注:**
>
> サイトをCitrix Directorから切断するには、**Remove site** をクリックします。このオプションは既存の構成を削除します。

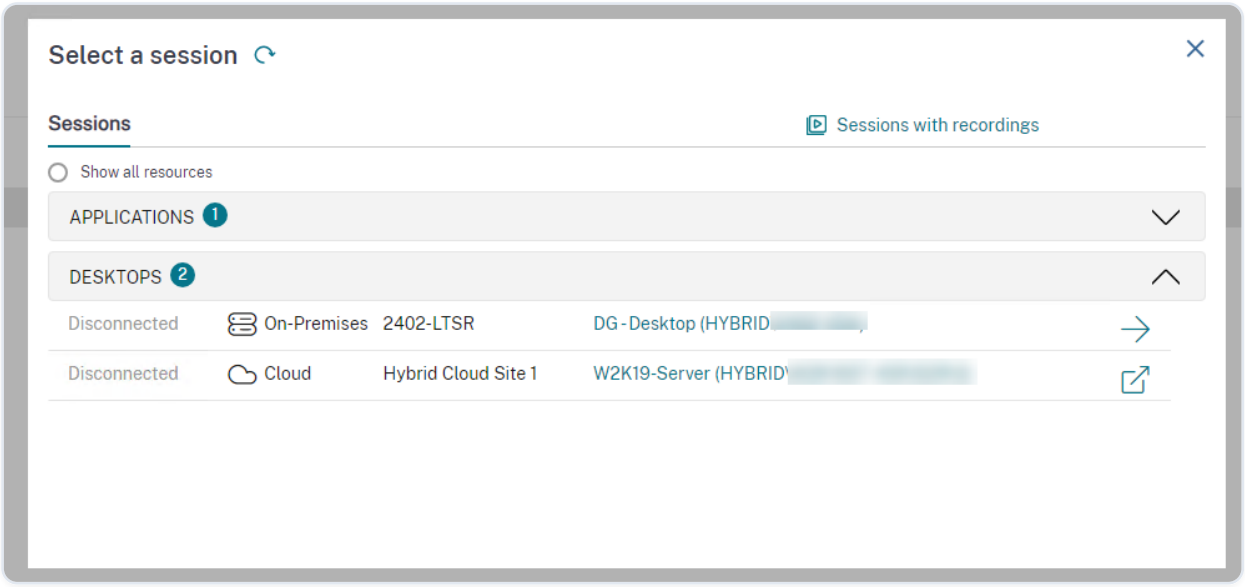
ハイブリッド展開からのユーザー検索

ユーザーを検索するには、次の手順を実行します。

1. 上部のナビゲーションバーで「**検索**」をクリックします。「**展開の監視とトラブルシューティング**」ページが表示されます。



2. ドロップダウンリストから**ユーザー**を選択し、ユーザー名を入力します。オンプレミスおよびクラウド展開からのアクティブおよび失敗したセッションのリストが表示されます。



3. 検査するセッションを選択します。

- クラウド展開を使用しているセッションの場合、ユーザーコンテキストを含む関連するDaaS Monitor URLが「**アクティビティマネージャー**」ページに開き、すばやくトラブルシューティングを開始できます。
- オンプレミス展開を使用しているセッションの場合、アクティビティマネージャーページがすぐに開き、トラブルシューティングを開始できます。

インフラストラクチャ監視

Directorは、Citrix Virtual Apps and Desktops™コンポーネントの運用状況を可視化する機能を提供するようになりました。この機能は、インフラストラクチャに関連する問題を簡単に特定、トラブルシューティング、解決するのに役立ちます。現在、以下のコンポーネントの健全性が監視されています。

- デリバリーコントローラー™
- シトリックス プロビジョニング™ サービス
- StoreFront™

この機能をサポートするため、Citrixコンポーネント向けに`citrixinframonitor.msi`という新しいWindows実行可能ファイルが導入されました。これは、Provisioning ServiceまたはStoreFrontサーバーからDirectorへの関連する健全性メトリックの収集と送信に役立ちます。ただし、Delivery Controllerの監視には`CitrixInfraMonitor.msi`は必要ありません。Delivery Controllerコンポーネントは、Citrix Virtual Apps and Desktopsサイトに接続されると、監視のために自動的にオンボーディングされます。

この機能は、Directorの単一ダッシュボードで、Delivery Controller、Provisioning Service、およびStoreFrontサーバーに関する重要な監視データセットとプロアクティブなアラートを取得するのに役立ちます。最新の情報を確保するため、監視対象コンポーネントから5分ごとにデータが収集されます。

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

主な機能

リアルタイム監視:

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

詳細な分析:

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

自動アラートと通知:

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

ユースケース

運用効率:

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

チケット解決の迅速化:

サーバーの健全性とパフォーマンスに関する主要なメトリックを監視し、仮想アプリケーションとデスクトップのユーザーへの最適な配信を評価します。これらのメトリックを使用して、関連コンポーネントを分析することで、パフォーマンスに関連するユーザーの苦情を診断し、解決します。

前提条件

- Citrix Virtual Apps and Desktops バージョン 2407 以降
- Provisioning Serviceの前提条件またはStoreFrontの前提条件が満たされていることを確認してください。
- Citrix Provisioningを監視する場合:
  - **DB Connectivity** および **License Server Reachability** を監視するために必要な最小バージョンはCitrix Provisioning 2407です。
  - **PXE Service**、**TFTP Service**、および **Total Reconnect Count** を監視するために必要な最小バージョンはCitrix Infra Monitor 2411です。
- Citrix Infrastructure Monitorを実行するために必要なユーザーアカウントまたは権限:
  - エンドポイントマシンにCitrix Infrastructure MonitorをインストールするためのWindows管理者権限を持つユーザーアカウント。
  - 次のDirector権限を持つフル管理者ユーザーアカウントまたはカスタムロール:
    - アラートポリシーの作成\編集\有効化\削除
    - アラートメールサーバー構成の作成\編集\削除

- Citrix コンポーネントへの接続の作成\編集\管理 (インフラ監視)
- アラートの無視
- アラートポリシーの表示
- アラートの表示
- ダッシュボードページの表示
- インフラストラクチャモニターページの表示

注:

- 前述の前提条件は、Provisioning ServiceおよびStoreFrontコンポーネントの監視にのみ有効です。
- **アラート**ページにアクセスする権限がない場合、**インフラストラクチャ監視**ページで**アラートの管理**オプションが無効になります。

詳細については、以下を参照してください。

- インフラストラクチャ監視の概要
- 接続の管理
- インフラストラクチャダッシュボード
- 高度なアラートポリシー
- インフラストラクチャポリシー

インフラストラクチャ監視の開始

Citrix Infrastructure Monitorには、次の方法で接続できます。

- 手動接続 - Citrix Infrastructure Monitorサービスを手動でダウンロードしてインストールします。
- 自動接続 - UIがダウンロードとインストールを自動的に処理します。

手動接続と自動接続の両方の後で、Citrix Infrastructure MonitorのHTTPSをオプションで構成できます。

詳細については、以下を参照してください。

- 手動接続

- 自動接続
- Citrix Infrastructure MonitorのHTTPSを構成する

接続の管理

Citrixコンポーネントの接続ページで、接続の表示、削除、または編集ができます。

接続の表示

このビューで利用可能な、接続済みおよび未接続のすべてのコンポーネントの詳細を表示できます。次の表は、**接続の作成**ページのさまざまな列について説明しています。

列	説明
ホスト名	サーバーの名前。
種類	接続の種類。Delivery Controller™、Provisioning Service、StoreFront のいずれかです。
バージョン	コンポーネントにインストールされている `CitrixInfraMonitor.msi` のバージョン。このフィールドはDelivery Controllerには適用されません。
作成者	接続を作成したユーザーの名前。
作成日	接続が確立された日付。
最終更新日時	接続が最後に更新された日付。
状態	状態には、接続中、接続済み、切断済みがあります。
	接続中: この状態は、新しいコンポーネントのデータが表示されるまでに約5分、リソース使用率データが利用可能になるまでに約10分かかることを示します。
	接続済み: この状態は、コンポーネントとサイト間の接続が稼働中であることを示します。

列	説明
	切断済み: この状態は、コンポーネントとサイト間の接続が切断されていることを示します。切断状態の考えられる理由としては、サーバーのダウンタイムや、サイトがCitrix Infrastructure Monitorに接続できないことなどが挙げられます。

> **注:**
>
> オンプレミスのCitrix Virtual Apps and Desktops™サイトに接続されている場合、このビューにDelivery Controller接続が自動的に入力されます。

接続の編集

Provisioning ServiceまたはStoreFront™接続を確立するために使用される管理者資格情報を更新するには、接続の編集が必要になる場合があります。

既存の接続を編集するには、次の手順を実行します。

1. 「**Settings**」または「**Infrastructure**」タブから「**Connect Citrix Components**」ページに移動します。
2. 接続リストテーブルで、目的のコンポーネントの行の末尾にある3つの点をクリックします。
3. 「**Edit**」をクリックし、必要に応じて詳細を更新します。

コンポーネントを削除する

Director UIまたはPowerShellコマンドを使用して、コンポーネントを削除できます。

Director UIの使用

コンポーネントの削除とは、DirectorからProvisioning ServiceまたはStoreFront接続を登録解除するプロセスです。登録解除プロセスが完了すると、選択したコンポーネントの新しいデータ収集は停止します。既存の接続を削除するには：

1. 「**Settings**」または「**Infrastructure**」タブから「**Connect Citrix Components**」ページに移動します。
2. 接続リストテーブルで、目的のコンポーネントの行の末尾にある3つの点をクリックします。
3. 「**Remove**」をクリックします。接続は登録解除され、Directorから削除されます。

PowerShell SDK の使用

特定のコンポーネントの登録を解除する必要がある場合は、Delivery Controller で次の PowerShell コマンドを実行します。

```
Remove-MonitorDirectorAgent -Fqdn <FQDN of component> -Component
<component>
```

Citrix Infrastructure Monitorの登録を解除するコマンドの例は次のとおりです。

```
Remove-MonitorDirectorAgent -Component PVS -Fqdn [redacted]
```

注:

コンポーネントの登録解除は、特定のコンポーネントからDirectorへのデータフローを停止するだけです。Citrix Infrastructure Monitor をアンインストールする必要がある場合は、「**コントロールパネル**」からアンインストールしてください。

インフラストラクチャダッシュボード

コンポーネントの健全性値は、**インフラストラクチャ監視**ページで確認できます。これらの結果は、インフラストラクチャに関する問題をプロアクティブに分析し、トラブルシューティングするのに役立ちます。

「**インフラストラクチャ監視**」ページは、以下でフィルタリングできます。

- ホスト名 - ホスト名を選択します
- 到達可能性 - **Up** (サーバーに到達可能) または **Down** (サーバーに到達不可) チェックボックスを選択します
- エラー - 「エラーのある行のみ表示」チェックボックスを選択します。

「**列の管理**」オプションを使用して、ダッシュボードに表示するデータを選択します。

Provisioning Service の健全性メトリック

インフラストラクチャタブをクリックし、**Provisioning Service**を選択します。Provisioning Service のインフラストラクチャダッシュボードが表示されます。

プロビジョニングサービス ダッシュボード(/en-us/citrix-virtual-apps-desktops/2503/media/sm-pvs-dashboard.png)

Provisioning Service サーバーについては、以下の詳細が監視されます。

カテゴリ	メトリック	説明
到達可能性	ホスト名	Citrix Infrastructure Monitorがインストールされている Provisioning Serviceマシンの名前。このメトリックは文字列値です。
	Provisioning Serviceサイト名	Provisioning Serviceサイトの名前。このメトリックは文字列値です。
	Provisioning Serviceファーム名	Provisioning Serviceファームの名前。このメトリックは文字列値です。
	プロビジョニングサービス サイトID	Provisioning Serviceサーバーのサイトを表示します。このメトリックは文字列値です。
	プロビジョニングサービス ファームID	Provisioning Serviceサーバーのファームを表示します。このメトリックは文字列値です。
	サーバーの状態	指定されたサーバーの到達可能性の状態を表示します。可能な値は、*Up*、*Down*、*Unknown* です。
	最終起動時刻	Provisioning Service サーバーが最後に起動された時刻を表示します。
	最終更新	Provisioning Service サーバーからデータが収集された時刻を表示します。
依存サービス	ストリーミングサービス	ストリーミングサービスのステータスを表示します。このメトリックは、Windows

カテゴリ	メトリック	説明
		サービスのステータスを示します。可能な値は、*Not running*、*Running*、*Not Installed*、*n/a* (ヘルプアイコン付き) です。
	SOAP サービス	Simple Object Access Protocol (SOAP) サービスのステータスを表示します。このメトリックは、Windows サービスのステータスを示します。可能な値は、*Not running*、*Running*、*Not Installed*、*n/a* (ヘルプアイコン付き) です。
	DB接続	データベース接続のステータスを表示します。Citrix Provisioningサーバーバージョン2402以前を使用している場合、不明なエラーが発生する可能性があります。可能な値は、*未接続*、*接続済み*、*不明*、および*該当なし*（ヘルプアイコン付き）です。
	ライセンスサーバーの到達可能性	ライセンスサーバーに到達可能かどうかを表示します。Citrix Provisioningサーバーバージョン2402以前を使用している場合、不明なエラーが発生する可能性があります。可能な値は、*未接続*、*接続済み*、*不明*、および*該当なし*（ヘルプアイコン付き）です。
	再接続の合計回数	セッションが再接続された回数を表示します。

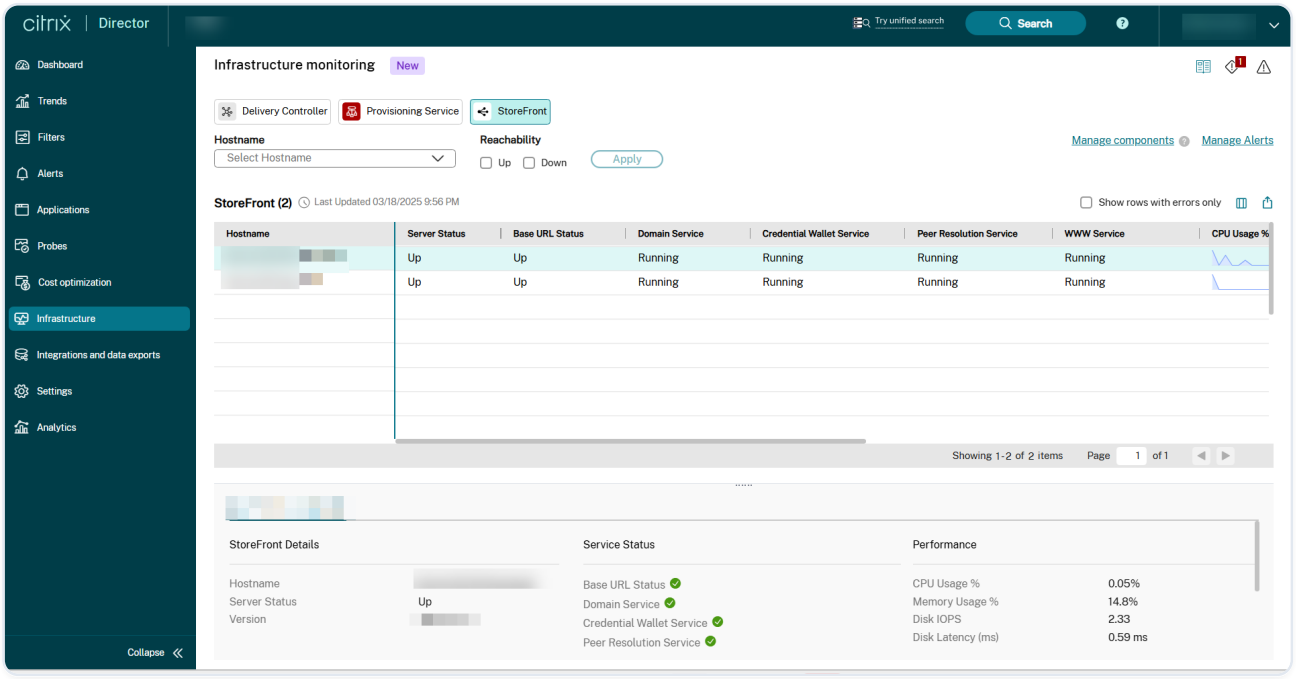
カテゴリ	メトリック	説明
	PXEサービス	Preboot Execution Environmentサービスのステータスを表示します。このメトリックは、Windowsサービスのステータスを示します。可能な値は、*実行中ではない*、*実行中*、*インストールされていない*、および*該当なし*（ヘルプアイコン付き）です。
	TFTPサービス	Trivial File Transfer Protocolサービスのステータスを表示します。このメトリックは、Windowsサービスのステータスを示します。可能な値は、*実行中ではない*、*実行中*、*インストールされていない*、および*該当なし*（ヘルプアイコン付き）です。
リソース使用率	CPU使用率 %	CPUの使用率を折れ線グラフで表示します。表示される値は、過去5分間の終わりの最新の値です。
	平均CPU %	過去10分間に集計されたProvisioning Serviceサーバーの平均CPU使用率を表示します。
	ピークCPU %	過去5分間のProvisioning Serviceサーバーのピーク CPU使用率を表示します。
	メモリ使用率 %	メモリの使用率を積み上げグラフで表示します。表示される値は、過去5分間の終わりの最新の値です。

カテゴリ	メトリック	説明
	平均メモリ %	過去10分間に集計されたProvisioning Serviceサーバーの平均メモリ使用率を表示します。
	ピークメモリ%	過去5分間のProvisioning Serviceサーバーのピークメモリ使用率を表示します。
	ディスクIOPS	折れ線グラフを使用して、ディスクの入出力値を表示します。
	平均ディスクIOPS%	過去10分間に集計されたProvisioning Serviceサーバーの平均ディスクIOPSを表示します。
	ピークディスクIOPS%	過去10分間のProvisioning Serviceサーバーのピークディスク IOPS使用率を表示します。
	ディスク待機時間 (ms)	折れ線グラフを使用して、ディスクの待機時間値を表示します。
	平均ディスク待機時間 %	過去10分間に集計されたProvisioning Serviceサーバーの平均ディスク待機時間を表示します。
	ピークディスク待機時間 %	過去5分間のProvisioning Serviceサーバーのピークディスク待機時間の割合を表示します。
影響	拒否されたログインの合計	ログイン試行の合計数で割った、失敗したログインの合計数。

カテゴリ	メトリック	説明
	アクティブなデバイス数	Provisioning Serviceサーバー内のアクティブなデバイスの総数を表示します。このメトリックは整数値です。

StoreFront™ の正常性メトリック

インフラストラクチャタブをクリックし、**StoreFront**を選択します。StoreFrontのインフラストラクチャダッシュボードが表示されます。



StoreFrontサーバーでは、以下の詳細が監視されます。

カテゴリ	メトリック	説明
到達可能性	ホスト名	StoreFrontサーバーの名前を表示します。このメトリックは文字列値です。
	サーバーの状態	StoreFrontサーバーの状態を表示します。このメトリックはWindowsサービスのステータスを示します。可能な値は、*実行中ではない*、*実行中*、*インストールされていない*

カテゴリ	メトリック	説明
		、および*該当なし*（ヘルプアイコン付き）です。
	ベースURLの状態	ベースURLの健全性を表示します。HTTPステータスコードが200の場合、ステータスはUPです。それ以外の場合、値はDownです。
	最終起動時刻	StoreFrontサーバーが最後に起動された時刻を表示します。
	最終更新	StoreFrontサーバーからデータが収集された時刻を表示します。
依存サービス	ドメインサービス	ドメインサービスという名前のWindowsサービスの正常性。このメトリックは、Windowsサービスのステータスを示します。可能な値は、*実行中ではない*、*実行中*、*インストールされていない*、および*n/a*（ヘルプアイコン付き）です。
	資格情報ウォレットサービス	このサービスは、暗号化されたパスワードを保存するために使用されるWindowsサービスです。可能な値は、*実行中ではない*、*実行中*、*インストールされていない*、および*n/a*（ヘルプアイコン付き）です。
	ピア解決サービス	このサービスは、StoreFrontサーバーのピアメッシュを形成するサーバー間グループネットワーク通信を担当するWindowsサービスです。可能な値は、*実行中ではない*、*実*

カテゴリ	メトリック	説明
		行中、*インストールされていない*、および*n/a*（ヘルプアイコン付き）です。
	WWWサービス	このメトリックは、StoreFrontサーバーのWebサービスです。このメトリックは、Windowsサービスのステータスを示します。可能な値は、*実行中ではない*、*実行中*、*インストールされていない*、および*n/a*（ヘルプアイコン付き）です。
リソース使用率	CPU使用率 %	CPUの使用率を折れ線グラフで表示します。表示される値は、過去5分間の終わり時点での最新の値です。
	平均CPU使用率 %	過去10分間にわたって集計されたStoreFrontサーバーの平均CPU使用率を表示します。
	ピークCPU使用率 %	過去5分間のStoreFrontサーバーのピークCPU使用率を表示します。この値は、CPUに必要な最大容量を決定するのに役立ちます。
	メモリ使用率 %	メモリの使用率を積み上げグラフで表示します。表示される値は、過去5分間の終わり時点での最新の値です。
	平均メモリ使用率 %	過去10分間にわたって集計されたStoreFrontサーバーの平均メモリ使用率を表示します。

カテゴリ	メトリック	説明
	ピークメモリ %	StoreFrontサーバーの過去5分間のピークメモリ使用率を表示します。
	ディスク IOPS	ディスクの入出力値を折れ線グラフで表示します。
	平均ディスク IOPS %	StoreFrontサーバーの平均ディスクIOPSを浮動小数点数で表示します。
	ピークディスク IOPS %	StoreFrontサーバーの過去10分間のピークディスクIOPS使用率を集計して表示します。
	ディスク遅延 (ミリ秒)	ディスクの遅延値を折れ線グラフで表示します。
	平均ディスク待機時間 %	過去10分間に集計されたStoreFrontサーバーの平均ディスク待機時間を表示します。
	ピークディスク待機時間 %	過去5分間のStoreFrontサーバーのピークディスク待機時間の割合を表示します。
影響	ICA®証明書の有効性	ICA証明書の有効性を表示します。可能な値は、*期限切れ*、*期限切れ間近*、*有効*、*見つかりません*です。
	ICA証明書チェーンの有効性	StoreFront ICA証明書チェーンが有効かどうかを表示します。可能な値は、*Yes*または*No*です。
	IIS証明書の有効性	IIS証明書の有効性を表示します。可能な値は、*Expired*、

カテゴリ	メトリック	説明
		Expiring、*Valid*、*Not Found*です。
	IIS証明書チェーンの有効性	StoreFront IIS証明書チェーンが有効かどうかを表示します。可能な値は、*Yes*または*No*です。

Delivery Controller™の健全性メトリック

Delivery Controllerコンポーネントは、インフラストラクチャ監視の一部としてデフォルトで追加されます。Citrix Virtual Apps and Desktops™サイトに接続されているDelivery Controllerコンポーネントは、監視のために自動的にオンボードされます。

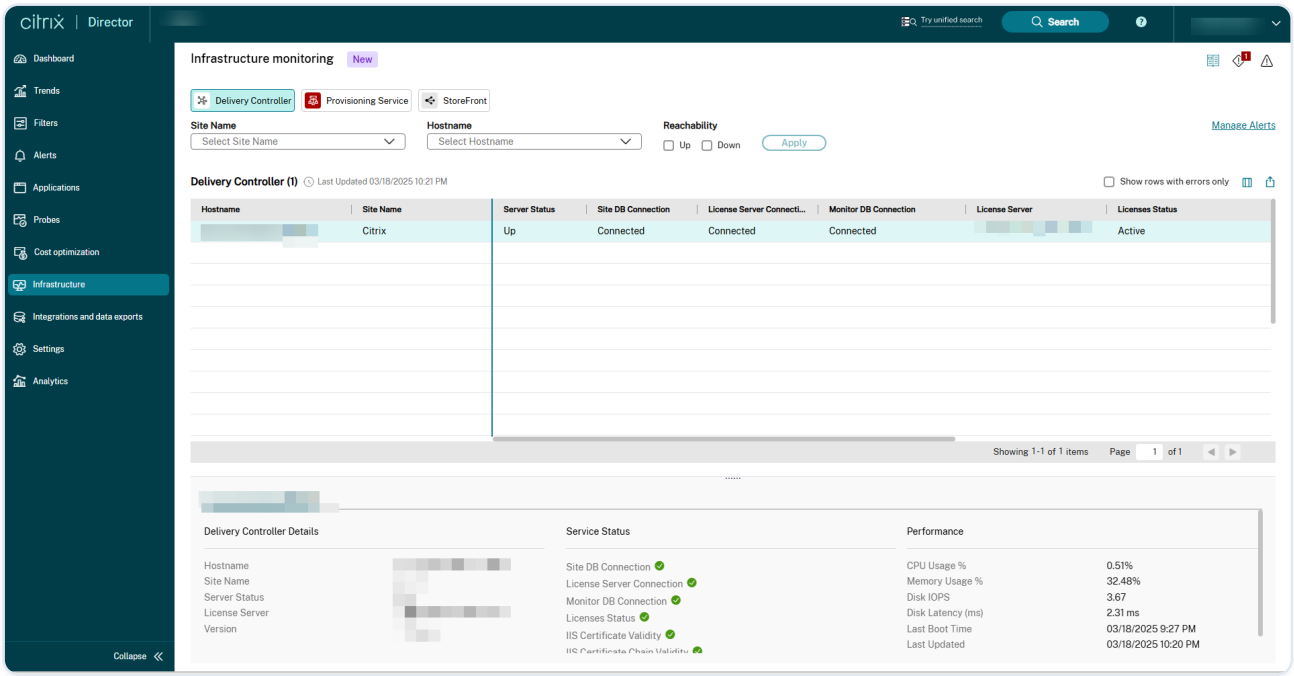
この機能により、お客様はインフラストラクチャ監視ダッシュボードでコントローラーの健全性を監視し、アラートを設定できます。アラート機能により、デリバリーコントローラー用に作成されたポリシーのいずれかがクリティカルまたは警告ステージにある場合、顧客管理者にアラートが通知されます。

必要なサイト名を選択すると、選択したサイト名に応じて詳細が表示されます。また、*Up* または *Down* などの**到達可能性ステータス**を選択することもできます。

注: Delivery Controllerの監視には、`CitrixInfraMonitor.msi`ファイルは必要ありません。

インフラストラクチャの詳細について、シングルサイトとマルチサイトの両方の詳細を監視できます。

インフラストラクチャタブをクリックし、**Delivery Controller**を選択します。Delivery Controllerのインフラストラクチャダッシュボードが表示されます。



Delivery Controllerでは、以下の詳細が監視されます。

カテゴリ	メトリック	説明
到達可能性	サーバーの状態	指定されたDelivery Controllerの到達可能性の状態を示します。可能な値は*Up*と*Down*です。
	バージョン	Delivery Controllerのバージョン。
	最終起動時刻	Delivery Controllerが最後に起動された時刻を表示します。
	最終更新	Delivery Controllerからデータが収集された時刻を表示します。
依存サービス	サイトDB接続	サイトデータベース接続のステータスを表示します。可能な値は、*Not Connected*、*Connected*、*Unknown*、および*n/a*（ヘルプアイコン付き）です。**Unknown:** この値は、メトリックが収集されていないか、利用できない場合に表示されます。**n/a:** 該当な

カテゴリ	メトリック	説明
		し。この値は、サーバーのステータスがダウンしている場合に表示されます。
	ライセンスサーバー接続	ライセンスサーバー接続のステータスを表示します。指定可能な値は、*未接続*、*接続済み*、*不明*、および *n/a* (ヘルプアイコン付き) です。
	監視DB接続	監視データベース接続のステータスを表示します。指定可能な値は、*未接続*、*接続済み*、*不明*、および *n/a* (ヘルプアイコン付き) です。
	ライセンスサーバー	ライセンスサーバーに到達可能かどうかを表示します。
	ライセンスステータス	ライセンスのステータスを表示します。
リソース使用率	CPU使用率 %	CPUの使用率を折れ線グラフでパーセンテージ表示します。表示される値は、過去5分間の終わり時点での最新の値です。
	平均CPU使用率 (%)	過去10分間のデリバリーコントローラーサーバーの平均CPU使用率を表示します。
	ピークCPU使用率 (%)	過去5分間のデリバリーコントローラーサーバーのピークCPU使用率を表示します。
	メモリ使用率 (%)	スタックチャートを使用してメモリ使用率をパーセンテージで表示します。表示される値は、過去5分間の終わりにおける最新の値です。

カテゴリ	メトリック	説明
	平均メモリ使用率 (%)	過去10分間のデリバリーコントローラーサーバーの平均メモリ使用率を表示します。
	ピークメモリ使用率 (%)	過去5分間のデリバリーコントローラーサーバーのピークメモリ使用率を表示します。
	ディスク IOPS	ディスクの入出力値を折れ線グラフで表示します。
	平均ディスク IOPS %	過去10分間のDelivery Controllerサーバーの平均ディスクIOPSを集計して表示します。
	ピークディスク IOPS %	過去10分間のDelivery Controllerサーバーのピークディスク IOPSパーセンテージを表示します。
	ディスク遅延 (ミリ秒)	ディスクの遅延値を折れ線グラフで表示します。
	平均ディスク遅延 %	過去10分間のDelivery Controllerサーバーの平均ディスク遅延を集計して表示します。
	ピークディスク遅延率	過去5分間のDelivery Controllerサーバーのピークディスク遅延率を表示します。
影響	IIS証明書の有効性	IIS証明書の有効性を表示します。可能な値は、*期限切れ*、*期限切れ間近*、*有効*、*見つかりません*です。
	IIS証明書チェーンの有効性	StoreFront IIS証明書チェーンが有効であるかどうかを表示

カテゴリ	メトリック	説明
		します。可能な値は、*はい*または*いいえ*です。

アラートの作成と管理

関心のある条件や範囲をプロアクティブに監視し、アラート疲れを軽減するためにアラートを設定できます。アラートは、重大度、再アラート間隔、通知媒体を設定でき、製品でサポートされているアラートライフサイクルに従います。インフラストラクチャに関連するアラートは、**高度なアラートポリシー**セクションから作成できます。

詳細については、高度なアラートポリシーページを参照してください。

アプリケーションおよびデスクトップのプロービング

アプリケーションおよびデスクトップのプローブは、StoreFrontを使用してサイトで公開されているアプリとデスクトップを順次テスト起動することで、それらの健全性をチェックするプロセスを自動化します。プローブの結果はDirectorで利用できます。

要件

- Delivery Controllerが、アプリケーションプローブの場合はバージョン7.18以降、デスクトッププローブの場合はバージョン1906以降を実行していること。
- プローブエージェントを実行するエンドポイントマシンは、アプリケーションプローブの場合はCitrix Workspace™アプリ for Windowsバージョン1808以降、デスクトッププローブの場合はバージョン1906以降がインストールされたWindowsマシンであること。Unified Windows Platform (UWP) 用のWorkspaceアプリはサポートされていません。
- Citrix Probe Agentは、Active Directory資格情報を使用したStoreFrontおよびCitrix Workspace経由の認証をサポートしています。エンドポイントデバイスがCitrix Gateway経由でStoreFront / Workspaceに接続されている場合、Citrix Gatewayドメイン資格情報または多要素認証 (MFA) を使用して認証できます。Citrix Probe Agentは、シングルサインオン (SSO) などの他の認証方法をサポートしていません。

> **注記：**

    - ユーザーがCitrix Cloud™でサインインポリシーまたは条件付き認証を有効にしている場合、プローブエージェントはStoreFrontまたはCitrix Workspaceアプリにサインインできません。
    - Probe Agentは、Citrix Workspaceアプリへの認証にはActive Directory認証のみをサポートしています。

- Citrix Probe Agentは、Citrix GatewayやCitrix ADCのようなプロキシサーバーまたはロードバランサーが展開されていない場合にのみ機能します。
- Probe Agentをインストールするエンドポイントマシンに、Microsoft .NET Frameworkバージョン4.7.2以降がインストールされていることを確認してください。

プローブの実行に必要なユーザーアカウントまたは権限:

- 各エンドポイントマシンでプローブを実行するための固有のStoreFrontユーザー。StoreFrontユーザーは管理者である必要はありません。プローブは非管理者コンテキストで実行できます。
- エンドポイントマシンにCitrix Probe Agentをインストールおよび構成するためのWindows管理者権限を持つユーザーアカウント。
- ユーザーは、アプリケーションまたはデスクトップの起動に使用されるVDAと同じドメインのメンバーである必要があります。Probe Agentは現在、複数のドメインをサポートしていません。
- 既存のユーザーアカウントをプロービングに再利用すると、ユーザーのアクティブなセッションからログオフする可能性があります。フル管理者ユーザーアカウント、または以下の権限を持つカスタムロールが必要です。
    - デリバリーグループの権限:
        - 読み取り専用
    - Directorの権限:
        - アラートメールサーバー構成の作成\\編集\\削除 - メールサーバーがまだ構成されていない場合
        - プローブ構成の作成\\編集\\削除
        - 構成ページの表示
        - トレンドページの表示

構成

複数の地域で、ピーク時間外にプローブを実行するようにスケジュールできます。包括的なプローブ結果は、ユーザーが問題に遭遇する前に、アプリケーション、ホストマシン、または接続に関連する問題をトラブルシューティングするのに役立ちます。

Citrix Probe Agent バージョン 2103 以降は、サイト集約をサポートしています。Citrix Probe Agent を構成するときは、集約されたサイトからのアプリケーションとデスクトップの列挙を有効にするために、Workspace (StoreFront) Site Aggregation Enabled オプションを選択します。以下のサイトの組み合わせがサポートされています。

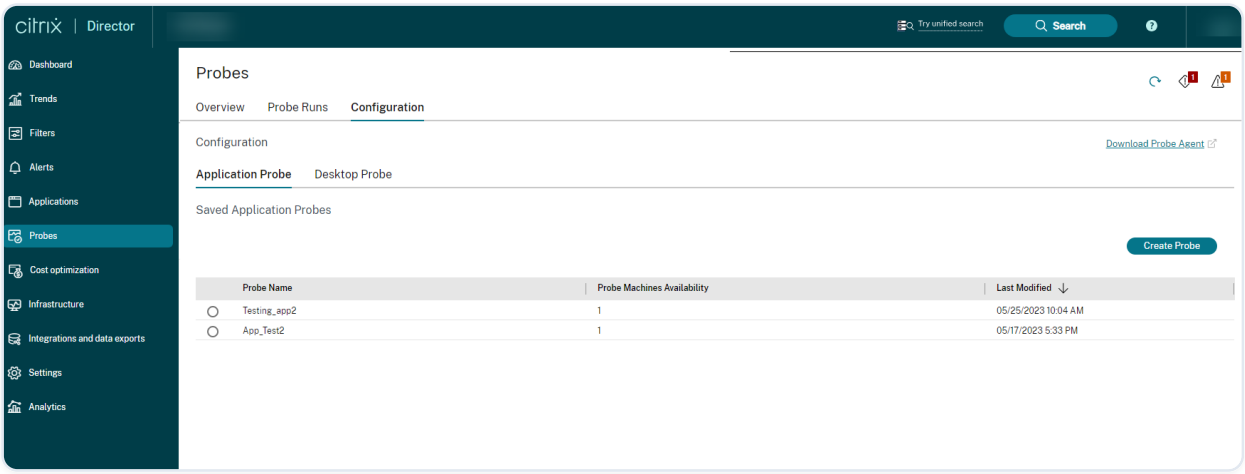
- 1つの StoreFront URL を持つ複数のオンプレミスサイト。
- StoreFront または Workspace URL のいずれかを持つオンプレミスサイトとクラウドサイト。
- 1つの Workspace URL を持つ複数のクラウドサイト。
- Citrix Gateway 経由で StoreFront または Workspace に接続されているオンプレミスサイト。

> **注:**
>
> 1つのサイトにのみアクセスできるプローブを構成するには、個別の管理者またはユーザーを作成する必要があります。

ステップ1：Citrix Probe Agentをインストールして構成する

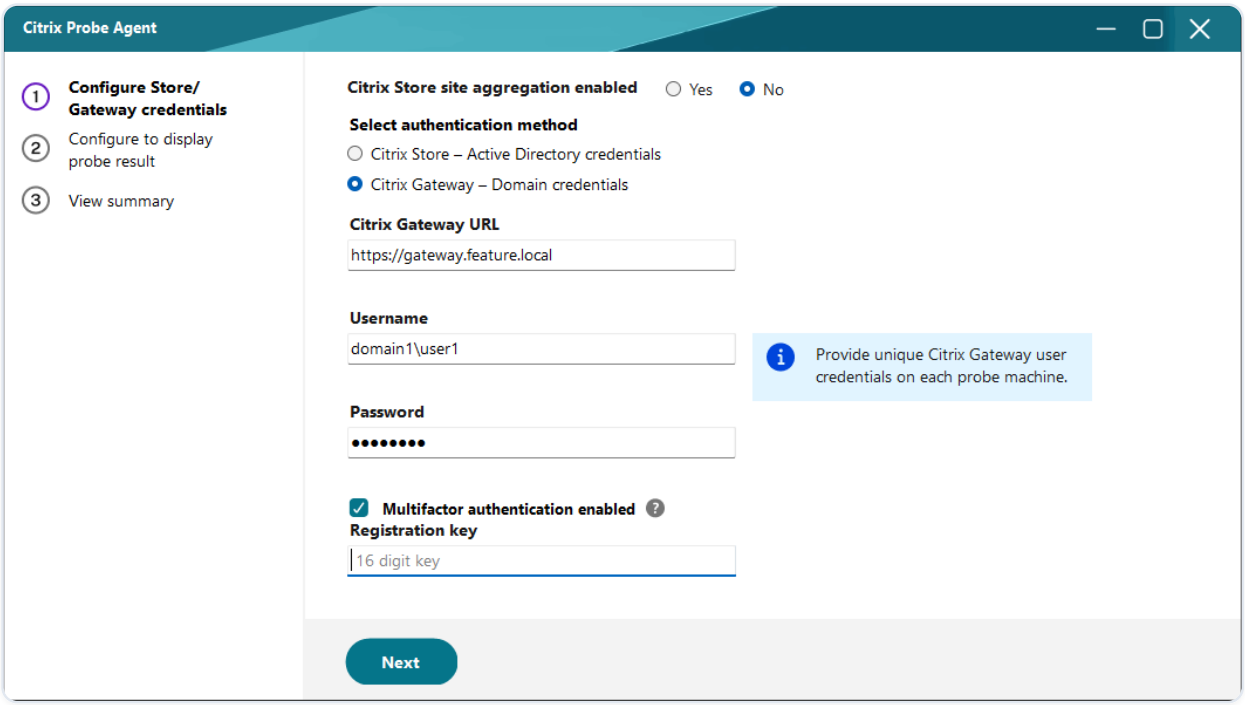
Citrix Probe Agent は、ユーザーが StoreFront を介して実際のアプリケーションまたはデスクトップを起動するのをシミュレートする Windows 実行可能ファイルです。Director で構成された起動をテストし、その結果を Director に報告します。

1. プロービングを実行するエンドポイントマシンを特定します。
2. 管理者権限を持つユーザーは、エンドポイントマシンにCitrix Probe Agentをインストールして構成できます。Citrix downloadsページで入手可能なCitrix Probe Agent実行可能ファイルをダウンロードしてください。ダウンロードリンクは、Directorの**プローブ**タブでも入手できます。



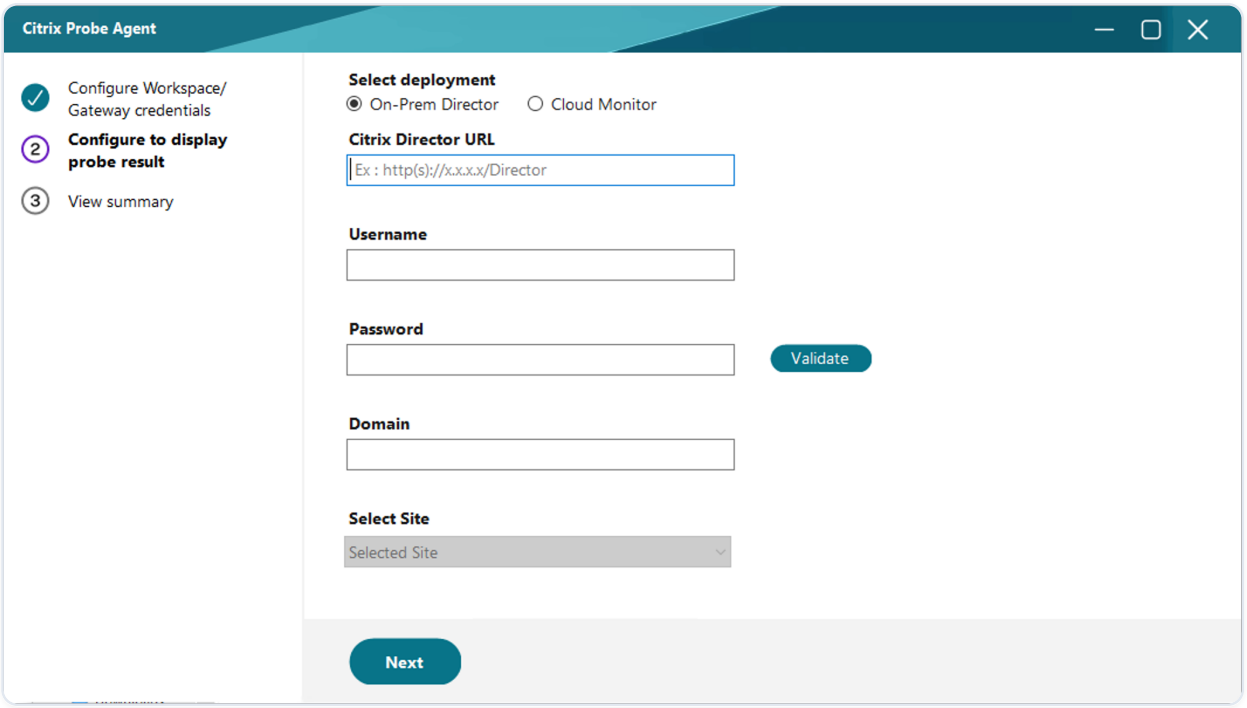
。

3. 集約されたサイトがある場合は、集約されたサイトからのアプリケーションとデスクトップの列挙を有効にするために、Workspace (StoreFront) Site Aggregation Enabledオプションを選択します。
4. 認証方法を選択し、関連する資格情報を入力します。資格情報は暗号化され、安全に保存されます。
5. StoreFront Active Directoryの資格情報で構成します。各エンドポイントマシンで一意のWorkspace (StoreFront) ユーザーを構成します。
6. エンドポイントがCitrix Gatewayを介してStoreFrontに接続されている場合は、Citrix Gatewayオプションを選択し、Citrix Gatewayドメインの資格情報で構成します。



7. ゲートウェイが多要素認証をサポートしている場合は、多要素認証オプションを選択し、16桁の認証キーを入力します。これは、シングルログインスキーマを使用してLDAPおよびネイティブOTPで構成されたCitrix Gatewayでのみ利用可能です。

8. **プローブ結果の表示を構成**タブで、Directorの資格情報を入力し、**検証**をクリックします。



9. サイトを選択し、**次へ**をクリックします。
10. 「**概要の表示**」タブで、構成された詳細が正確であることを確認します。変更が必要な場合は、該当するタブに移動して更新します。

> **注:**
>
> Citrix Probe Agentのインストールと構成の自動化に記載されているPowerShellスクリプトを使用して、Citrix Probe Agentのインストールと構成を自動化できます。

手順2：Directorでのプローブの構成

> **制限：**
>
> 対話型ログオンメッセージバナーが有効になっているWindows VDAからアプリケーションまたはデスクトップがテスト起動されると、プローブは失敗します。これは、対話型ログオンメッセージの承認を待機している間にタイムアウトが発生するためです。 サーバーVDAでログオンメッセージを無効にするには、「コンピューターの構成」>「Windowsの設定」>「セキュリティの設定」>「ローカルポリシー」>「セキュリティオプション」に移動します。

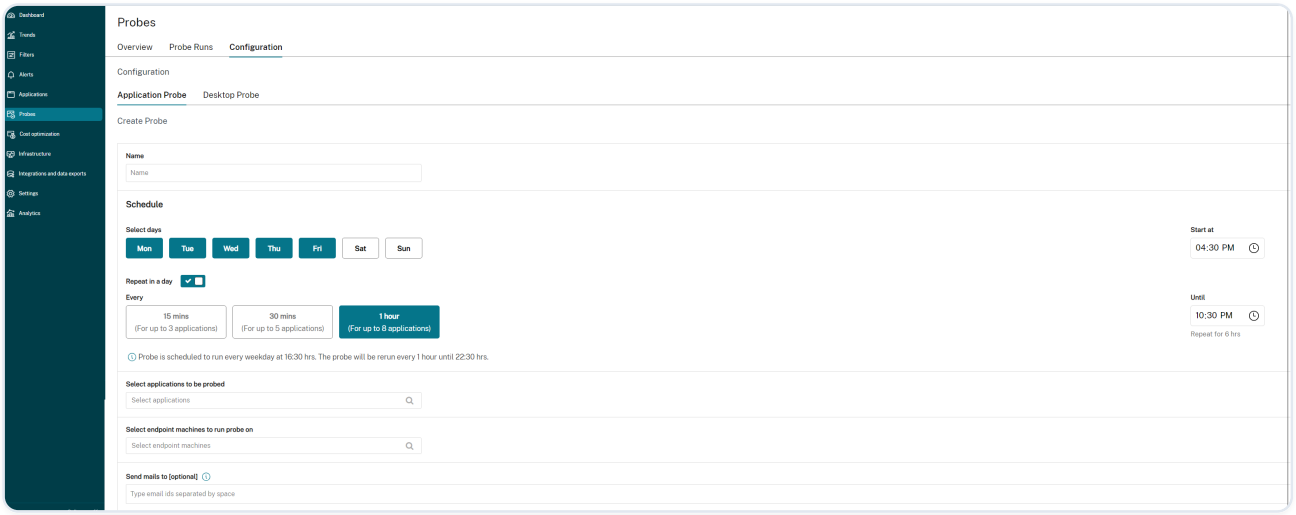
次のフィールドのテキストを削除し、Microsoftポリシーを更新します。

- 対話型ログオン：ログオンしようとしているユーザーへのメッセージテキスト
- 対話型ログオン：ログオンしようとしているユーザーへのメッセージタイトル

プローブユーザーを、対話型ログオンメッセージバナーが無効になっているこの特定のサーバーVDAに割り当てて、プローブがアプリケーションまたはデスクトップの起動状態を通過できるようにします。

詳細については、`<https://learn.microsoft.com/ja-jp/windows/security/threat-protection/security-policy-settings/interactive-logon-message-text-for-users-attempting-to-log-on>`を参照してください。

1. **プローブ** \> **アプリケーションプローブ**または**デスクトッププローブ**に移動し、**プローブの作成**をクリックします。
2. 「**プローブの作成**」ページで、プローブの名前を入力します。
3. スケジュールを選択します。
    a. プローブを実行する曜日を選択します。
    b. プローブを実行する開始時刻を入力します。
    c. さらに、**Repeat in a day** オプションを選択できます。プローブを1日の中で繰り返す終了時刻と間隔を入力します。たとえば、以下の構成では、毎週月曜日、水曜日、木曜日、日曜日に、12時08分から16時34分まで30分ごとにアプリケーションプローブを実行します。
4. 間隔に応じて、プローブするアプリケーションまたはデスクトップの推奨数を選択します。
5. プローブを実行する必要があるエンドポイントマシンを選択します。
6. 失敗したプローブの結果を送信する管理者のメールアドレスを入力します。メールサーバーは、**アラート** > **メールサーバーの構成** で構成します。



この構成では、アプリケーションセッションは毎週月曜日、水曜日、木曜日、日曜日に、12時08分、12時38分、13時08分といった具合に、16時08分まで起動します。

注：

- 構成後、エージェントは次の時間から構成されたプローブを実行します。
- **Repeat in a day** オプションが導入される前に設定されたプローブは、スケジュールされた時間に引き続き実行されます。これらのプローブでは、**Repeat in a day** オプションはデフォルトで無効になっています。
- 重複を防ぐため、各実行に5分の期間が設けられるようにプローブを構成することをお勧めします。

ステップ3：プローブの実行

エージェントは、Directorから定期的に取得するプローブ構成に従ってプロービングを実行します。

StoreFrontを使用して、選択されたアプリケーションを順次起動します。エージェントは、Monitorデータベースを介して結果をDirectorに報告します。障害は5つの特定の段階で報告されます。

- **StoreFront Reachability** - 設定されたStoreFront URLに到達できません。
- **StoreFront Authentication** - 設定されたStoreFrontの資格情報が無効です。
- **StoreFront Enumeration** - StoreFrontのアプリケーション列挙リストに、プローブ対象のアプリケーションまたはデスクトップが含まれていません。
- **ICA® download** - ICAファイルが利用できません。

- **Application / Desktop launch** – アプリケーションまたはデスクトップを起動できませんでした。

ステップ4：プローブ結果の表示

プローブでプローブ結果を確認できます。プローブビューでは、プローブ結果の包括的な概要が表示されます。これらの結果は、問題を事前に分析およびトラブルシューティングするのに役立ち、ユーザーのセッション起動エクスペリエンスをよりスムーズにします。

概要タブには、構成されているすべてのプローブの概要が1つのビューに表示されます。

Directorプローブの実行(/en-us/citrix-virtual-apps-desktops/2503/media/dir-probe-metrics-chart.png)

プローブは、期間、プローブの種類、エンドポイント名、アプリケーション名、デスクトップ名、およびプローブ結果の種類に基づいてフィルタリングできます。フィルタ条件に一致するプローブは、プローブ、アプリケーション/デスクトップ、およびエンドポイントごとに以下の詳細とともに表示されます。

プローブメトリックには、スケジュール済み、計画済み、スキップ済み、成功、失敗した実行の数が表示されます。

- Completed Runs – 完了したプローブ実行の数。
- Failed Runs – 失敗したプローブ実行の数。
- Skipped Runs – エンドポイントが非アクティブであるか、サービスが利用できないために完了しなかった実行の数。
- 成功した実行 – アプリ/デスクトップの起動中に、いずれの段階でも失敗することなく正常に完了したプローブの数。

エンドポイントマシンの総数も、アクティブなマシンと非アクティブなマシンの数とともに表示されます。

プローブ失敗ステージには、各失敗グループの失敗分布が視覚的に表示されます。ほとんどの失敗が発生したステージを分析することで、プローブ結果の解釈と問題のトラブルシューティングが容易になります。グラフィカル表示では、アプリケーション/デスクトップの起動、ICAファイルのダウンロード、Storefront/Workspaceの列挙、Storefront/Workspaceの到達可能性、およびStorefront/Workspaceの認証における失敗したプローブ実行の数が示されます。

これにより、ほとんどの失敗が発生したステージを分析するのに役立ちます。この情報は、プローブ結果を迅速に理解し、トラブルシューティングを行うのに役立ちます。

エンドポイントが非アクティブであるか、サービスが利用できないために、一部のプローブ実行が完了しない場合があります。

プローブ実行タブには、完了したプローブ実行の結果が詳細に表示されます。選択したプローブの個々の実行の詳細を確認するためにドリルダウンできます。重要なピボットポイントに基づいて、さらにフィルタリングおよび分析できます。

Directorプローブ実行(/en-us/citrix-virtual-apps-desktops/2503/media/dir-probe-runs.png)

プローブ実行は、期間、プローブの種類、エンドポイント名、アプリケーション名、デスクトップ名、およびプローブ失敗ステージに基づいてフィルタリングできます。プローブ失敗ステージには、プローブが失敗したステージが表示されます。プローブ名、スケジュールされた実行、失敗した実行、アプリケーション/デスクトップ名のリンクをクリックすると、フィルター条件に一致するプローブ実行のリストが表示されたプローブ実行ページに移動します。

コスト最適化

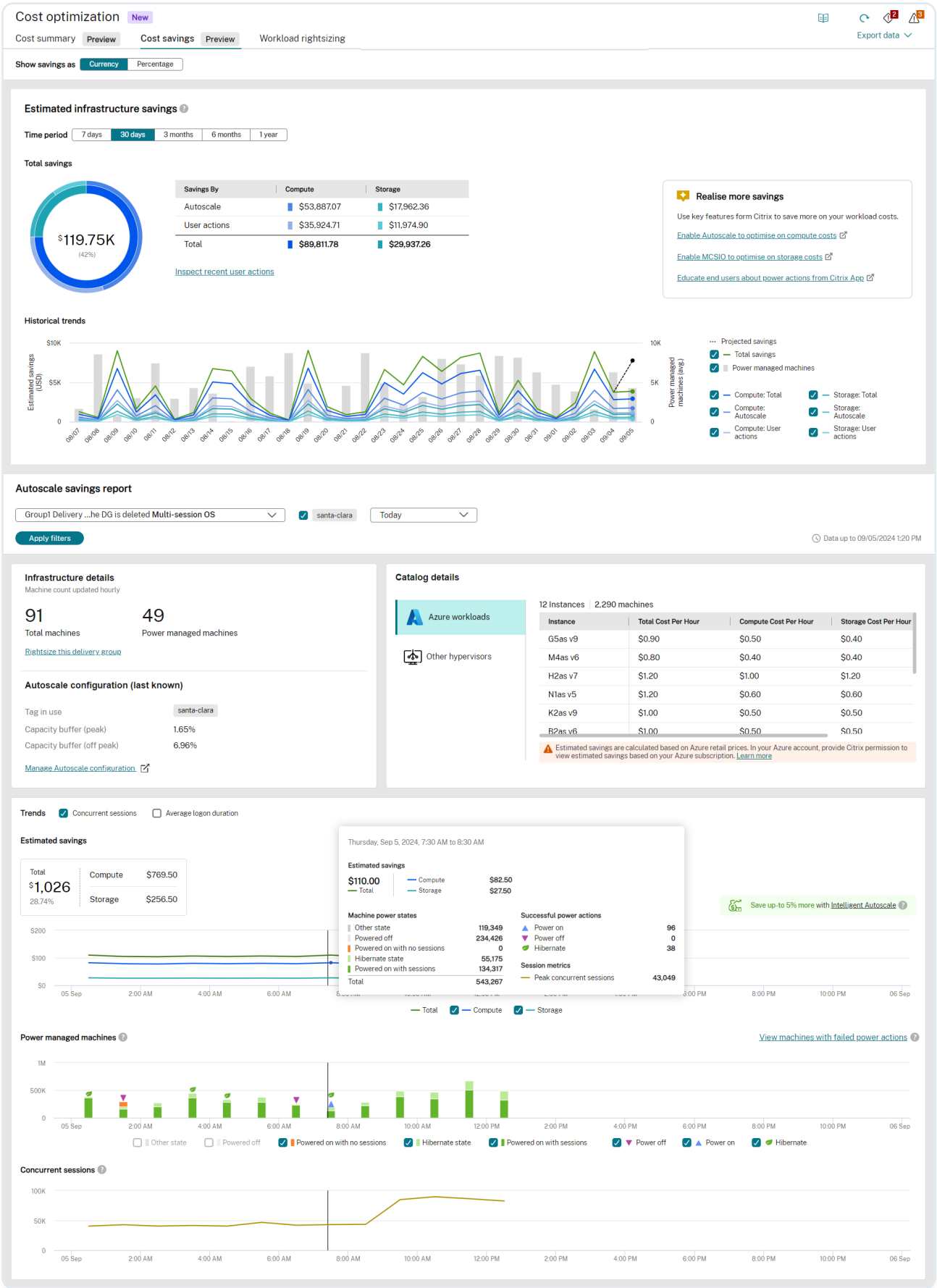
Citrix Director には、仮想マシンとセッションの使用状況を効果的に分析するのに役立つ、コスト最適化と呼ばれる新機能が導入されました。この機能は、コストを最適化する方法について洞察に満ちた視覚的な表現を提供します。また、不要なマシンを排除し、それによってコストを削減するのにも役立ちます。

コスト最適化をサポートするために、次のアラートも導入されました。

- 電源オン失敗アクションと電源オフ失敗アクション
- マシンの稼働時間アラート

最近の電源操作を行ったマシンを検査して、ユーザーの問題を引き起こす電源オンの失敗や、コストを増加させる電源オフの失敗を分析することもできます。詳細については、「最近の電源操作を行ったマシンの検査」セクションを参照してください。

ホームページの左メニューから**コスト最適化**タブをクリックして、**コスト最適化**ページにアクセスします。



コスト最適化ホームページでは、次のことができます。

- 開始リンク - このリンクにアクセスして、コスト最適化機能の詳細を確認してください。

- コスト最適化ページを確認する - **コスト最適化**ページに関するフィードバックを提供できます
- データを更新します。
- 警告を表示する - 重大アラートと警告アラートの両方を表示できます。

コスト最適化ページには、次の機能が含まれています。

- コスト削減
- インフラストラクチャの適正化

コスト最適化のコストはどのように計算されますか?

マシンあたりの時間コストは、ハイパーバイザーがサポートする通貨で表示されます。このセクションでは、Azure マシンとその他のマシンのコストがどのように計算されるかについて説明します。

Azureマシンのコスト

コスト計算の優先順位は次のとおりです:

1. 'Microsoft.Consumption/pricesheets/read 権限が利用可能な場合、有効価格は、Azure サブスクリプションで構成されている通貨で表示されます。
2. 権限が利用できない場合、Azure の小売価格が表示されます。詳細については、「Azure Retail Prices overview」を参照してください。
3. 有効価格または小売価格が利用できない場合、コストは管理者が Web Studio で入力したコストに基づいて表示されます。詳細については、ドキュメントの「Machine cost」セクションを参照してください。
4. Web Studio にコストが記載されていない場合、デフォルトのコストとして 1 ドルが考慮されます。

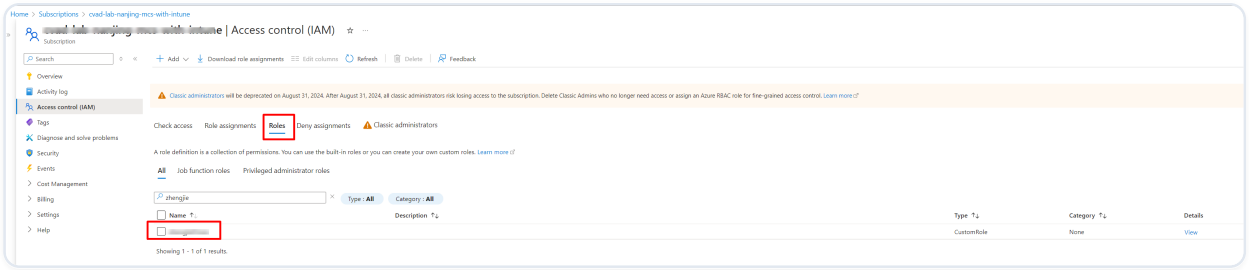
Azure のアカウント詳細を確認し、有効価格を見つけるために必要な権限を追加するには、次の手順を実行します。

1. Citrix DaaS に移動します。
2. **ホスティング**タブをクリックして、ホスティング接続アカウントを見つけます。
3. **ホスティング**タブに記載されている**アプリケーション ID**を探します。

   ホスティングタブ(/en-us/citrix-virtual-apps-desktops/2503/media/daas-azure-hosting.png)
4. Azure AD に移動し、手順 3 でメモした**アプリケーション ID**を探します。

5. **サブスクリプション** > **アクセス制御 (IAM)** に移動し、ホスティング接続 SPN 用に構成されたカスタムロールを選択します。

   Azure ポータル(/en-us/citrix-virtual-apps-desktops/2503/media/azure-portal.png)



6. ロールに *Microsoft.Consumption/pricesheets/read* 権限を追加します。

Azureの小売価格を確認する方法?

`Microsoft.Consumption/pricesheets/read` が利用できない場合、Azure の小売価格が表示されます。現在、Retail Rates Prices API を使用して、すべての Azure サービスの小売価格を取得できます。以前は、Azure サービスの価格を取得する唯一の方法は、Azure Pricing Calculator を使用するか、Azure ポータルを使用することでした。詳細については、Azure Retail Prices の概要 を参照してください。

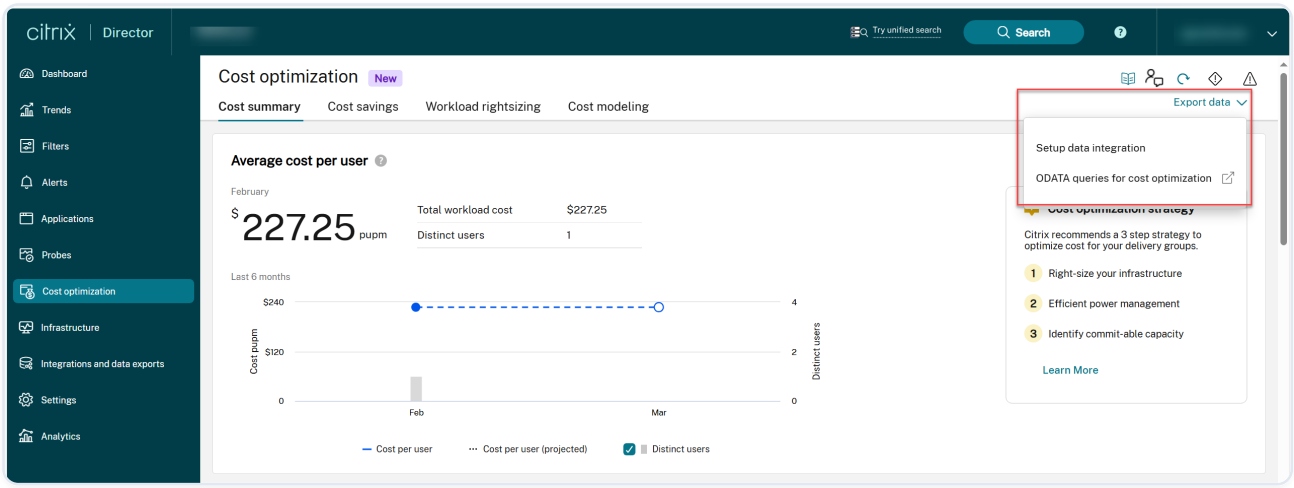
Azure 以外のマシンのコスト計算

その他のマシンについては、Web Studio で管理者が入力したコストに基づいてコストが表示されます。Web Studio でコストが指定されていない場合、デフォルトのコスト $1 が考慮されます。

データのエクスポート

コスト最適化ページで、データ統合と ODATA クエリを使用してデータをエクスポートできます。データをエクスポートするには、**コスト最適化**ページで**データのエクスポート**をクリックすると、次のオプションが表示されます。

- データ統合のセットアップ
- コスト最適化のための ODATA クエリ



データ統合のセットアップ

コスト最適化データを Monitor Service API と統合することで、トラブルシューティングや問題のトリアージのためのデータを収集できます。詳細については、統合とデータのエクスポート ページを参照してください。

コスト最適化のためのODATAクエリ

コスト最適化ページで利用可能なサンプルODATAクエリを使用して、データをエクスポートできます。

ODATAの利用を開始する

以下のリンクは、ODATAの利用を開始するのに役立ちます。

- ODATAの概要
- Citrix CloudのOData v4エンドポイントを使用してCitrix Monitor Serviceデータにアクセスするさまざまな方法
- Citrix Monitor ServiceデータでOData V4集計クエリを使用する
- ODataとAPIクライアントを使用してPowerBIをDaaS Monitorに接続する方法
- Postmanを使用してログオン時間が長いユーザーの詳細を取得する
- Monitor Serviceデータにアクセスする方法
- データアクセスプロトコル
- モニターモデル
- モニター通知

サンプルODATAクエリ

未使用のVDAを特定する

未使用のVDAを特定するには、デスクトップグループID、開始日、およびVDAの終了日を指定する必要があります。

未使用のリソースへの支出を削減するための詳細については、ワークロードの適正化を参照してください。

クエリの例:

```
https://<DDC URL>/monitorodata/ResourceUtilizationSummary?
$apply=filter(DesktopGroupId eq desktop-group-id and granularity eq 1440
and SummaryDate ge startdate and SummaryDate lt enddate)/
groupby((MachineId), aggregate(cast(TotalSessionCount, Edm.Int32) with
average as AvgTotalSessionCount))/filter(AvgTotalSessionCount eq 0.0)/
aggregate($count as UnusedVDACount)
```

1日の平均稼働時間を分単位で確認する

1日の平均稼働時間を分単位で確認するには、以下を指定する必要があります。

- デスクトップグループID
- 開始日
- 終了日
- 終了日と開始日の間の日数差。

未使用のリソースへの支出を削減するための詳細については、ワークロードの適正化を参照してください。

クエリの例:

```
https://[<DDC URL>|https://api-us.cloud.com/monitorodata/
ResourceUtilizationSummary?$apply=filter(DesktopGroupId] /monitorodata/
ResourceUtilizationSummary?$apply=filter(desktopGroupId eq desktop-group-
id and granularity eq 1440 and SummaryDate ge startdate and SummaryDate lt
enddate)/groupby((MachineId), aggregate(cast(UptimeInMinutes, Edm.Int32)
div day-difference with sum as TotalUptimeInMinutes))/
aggregate(TotalUptimeInMinutes with average as
DailyAverageUptimeInMinutes)
```

失敗したマシンの電源アクションを特定する

失敗したマシンの電源アクションの詳細については、電源オンアクションの失敗と電源オフアクションの失敗を参照してください。

クエリの例:

```
https:// <DDC URL> /monitorodata/Machines?$filter=LifecycleState eq 0 and
DesktopGroup/SessionSupport eq 1 and
(cast(LastPowerActionReason,'Edm.Int32') eq 6 or
cast(LastPowerActionReason,'Edm.Int32') eq 7 or
cast(LastPowerActionReason,'Edm.Int32') eq 8) and
(cast(LastPowerActionFailureReason,'Edm.Int32') eq 300 or
cast(LastPowerActionFailureReason,'Edm.Int32') eq 402 or
cast(LastPowerActionFailureReason,'Edm.Int32') eq 401) and MachineRole eq
0&$orderby=Name&$skip=0&$top=50&$expand=DesktopGroup($select=Name)&$select
=Sid,Id,Name,IsAssigned,IPAddress,FaultState,LastDeregisteredCode,FailureD
ate,CurrentPowerState,CurrentSessionCount,IsInMaintenanceMode,LastPowerAct
ionFailureReason,LastPowerActionCompletedDate
```

合計節約額を特定する

コスト削減の詳細については、コスト削減ページを参照してください。

サンプルクエリ:

```
https://[<DDC URL>|https://api-us.cloud.com/monitorodata/
ResourceUtilizationSummary?$apply=filter(DesktopGroupId] /monitorodata/
MachineCostSavingsSummaries?$apply=aggregate(TotalAmountSaved with sum as
TotalAmountSavedSum)
```

マシンの状態を確認する

コスト削減の詳細については、コスト削減ページを参照してください。

サンプルクエリ:

```
https:// <DDC URL> /monitorodata/MachineCostSavingsSummaries?
$filter=SummaryDate eq
2024-08-09T06:00:00Z&$select=TotalMachinesCount,PowerManagedMachinesOff,Po
werManagedMachinesInHibernate,PowerManagedMachinesOnWithSessions,PowerMana
gedMachinesOnWithoutSessions
```

コスト削減

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

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

マシンの使用量は通常、ピーク時に増加し、より多くのリソースを必要とします。Autoscale™機能は、需要の低い期間に未使用のマシンを自動的に電源オフにすることで、コストを削減するのに役立ちます。予測される削減額は、この使用パターンに依存します。ただし、未使用のマシンが存在する場合や、Autoscaleの電源アクションに障害が発生した場合など、特定の状況下ではコストが予想を超える可能性があります。これらの発生の背後にある理由を特定することは、以前は困難でした。

コスト最適化ページでは、予想コストを超える可能性のあるさまざまなシナリオに関する詳細情報を提供します。同様に、たとえば、セッションのないマシンがある場合、さらなるコスト削減の機会が表示されます。

ホームページの左メニューから**コスト最適化**タブをクリックすると、**コスト最適化**ページにアクセスできます。

コスト最適化ページ(/en-us/citrix-virtual-apps-desktops/2503/media/dir-costoptimization.png)

上部のドロップダウンリストから、サイトにクラウドプロバイダーとオンプレミスプロバイダーの両方がある場合、すべてのクラウドプロバイダー、すべてのオンプレミスプロバイダー、または個々のプロバイダーでフィルタリングできるようになりました。

注:

> フィルターは、適用ボタンなしで選択するとすぐに適用されます。

> **コスト最適化**ページには、**推定削減額**と**Autoscale削減レポート**が含まれています。コスト削減額は、ハイパーバイザーの通貨または発生したコストの割合として表示できます。

推定削減額: このグラフ表示は、インフラストラクチャリソースの効率的な利用を評価するのに役立ちます。コスト削減額は、ハイパーバイザーの通貨または発生したコストの割合として表示されます。このグラフは、コンピューティング関連の削減額とストレージの削減額から達成された削減額を示します。

注:

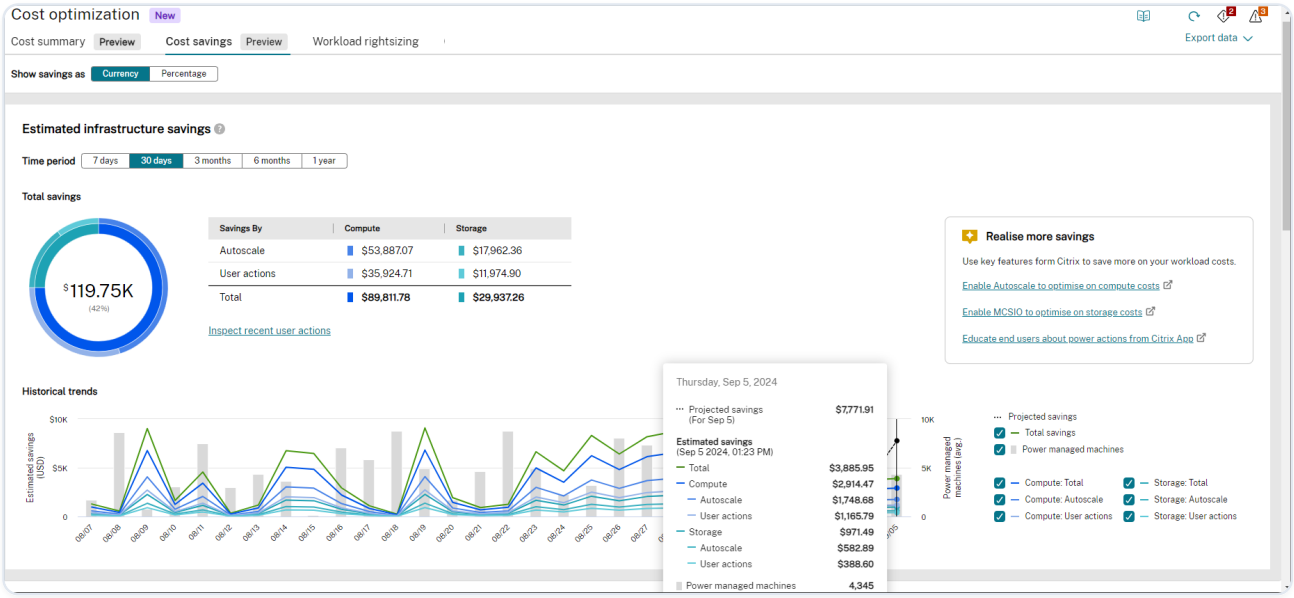
ストレージによる節約を表示するには:

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

以下の期間の結果を表示できます。

- 7日間
- 30日間
- 3か月
- 6か月
- 12か月

次の図は、「推定インフラストラクチャの節約」セクションを示しています:



次の表に、「推定インフラストラクチャの節約」グラフの要素を示します:

要素	説明
合計節約額	選択した期間にインフラストラクチャで達成された合計節約額を表示します。節約額はさらにストレージとコンピューティングコストに分類され、表形式で利用できます。
推定節約額	選択した期間にインフラストラクチャで達成された節約額を表示します。
電源管理されたマシン	電源管理されたマシンの総数を表示します。
予測節約額	残りの期間でどれだけのインフラストラクチャの節約が可能かを表示します。
コンピューティング - 合計	コンピューティング関連の節約から達成された合計節約額を表示します。
コンピューティング - Autoscale	Autoscale機能を使用しているコンピューティング関連の節約から達成された合計節約額を表示します。
コンピューティング - ユーザーアクション	ユーザーアクションによるコンピューティング関連の節約から達成された合計節約額を表示します。
ストレージ - 合計	ストレージの節約によって達成された合計節約額を表示します。

要素	説明
ストレージ - Autoscale	Autoscale機能を使用しているストレージの節約によって達成された合計節約額を表示します。
ストレージ - ユーザーアクション	ユーザーアクションによるストレージの節約によって達成された合計節約額を表示します。

Autoscale節約レポート: このグラフィカルな表示は、Autoscale機能が構成および有効化されているデリバリーグループの節約レポートを提供します。このレポートは、電源管理されているマシンにのみ適用されます。デリバリーグループを選択し、今日、昨日、先週、来週、今月、または来月のデータを選択できます。グラフにカーソルを合わせると、特定のグラフ値を取得できます。

> **注:**
>
> デリバリーグループが削除された場合、Autoscale節約レポートでデータを取得することはできません。

> デリバリーグループのドロップダウンリストから、以下のオプションにドリルダウンできます。

- **すべてのデリバリーグループ**: インフラストラクチャの詳細には、すべてのデリバリーグループ情報が表示されます。
- **すべてのシングルセッション**: シングルセッションマシンであるすべてのデリバリーグループのインフラストラクチャの詳細と、グラフにカーソルを合わせたときに表示されるマシンの電源状態、成功したAutoscale電源アクション、およびセッションのグラフィカルな表示。
- **すべてのマルチセッション**: マルチセッションマシンであるすべてのデリバリーグループのインフラストラクチャの詳細と、グラフィカルな表示。
- **最大15個を選択** - インフラストラクチャの詳細には、選択されたすべてのデリバリーグループ（最大15個）とグラフィカルな表示が表示されます。
- **最大15個を除外** - インフラストラクチャの詳細には、選択されたデリバリーグループ（最大15個）を除外したすべてのデリバリーグループとグラフィカルな表示が表示されます。

選択した期間のデータが表示されます。**推定節約額**のグラフィック表示は、ドロップダウンメニューから選択された実際の節約額です。ピークポイントにカーソルを合わせると、マシンの電源状態、Autoscaleの成功した電源アクション、およびセッションに関する情報が表示されます。

選択したデリバリーグループに基づいて、以下の詳細を表示できます。

- **インフラストラクチャの詳細**
  - 合計マシン数と電源管理されているマシン数 - マシンの総数と、そのうち電源管理されているマシンの数が表示されます。このデータは、残りの電源管理されていないマシンを電源管理されているマシンに変換し、Autoscale機能を有効にしてより包括的なカバレッジを実現する機会を提供します。インフラストラクチャの詳細セクションのデータは、1時間ごとに更新される最新の情報を示します。
- **カタログの詳細**

  ハイパーバイザー（サービスプロバイダー）の名前が表示されます。詳細については、「サポートされているVDAホスティングプラットフォーム」を参照してください。カタログの詳細のデータは、現在の時点で利用可能な最新のデータ（ライブデータ）を示します。

  以下の詳細を取得できます。

  - **ハイパーバイザー名** - サイトが接続されているハイパーバイザーの名前を表示します。複数のハイパーバイザーが存在する場合は、利用可能なすべてのハイパーバイザーを表示します。
  - **インスタンス** - インスタンスの名前を表示します。
  - **1時間あたりの総コスト** - ハイパーバイザーがサポートする通貨で、マシンごとの1時間あたりのコストが表示されます。Azureマシンでは、Microsoft.Consumption/pricesheets/read権限が利用可能な場合、Azureサブスクリプションで構成されている通貨で実効価格が表示されます。権限が利用できない場合は、Azureの小売価格が表示されます。詳細については、「Azure小売価格の概要」を参照してください。その他のマシンについては、Web Studioで管理者が入力したコストに基づいてコストが表示されます。Web Studioでコストが指定されていない場合、デフォルトのコストは1ドルです。詳細については、「」を参照してください。
  - **1時間あたりのコンピューティングコスト** - コンピューティング関連の節約によるコスト削減が表示されます。
  - **1時間あたりのストレージコスト** - ストレージの節約によるコスト削減が表示されます。
  - **マシン** - 選択したインスタンスのマシン数が表示されます。
- **Autoscale構成（最終既知）**

  使用中のタグ - WebStudioのAutoscale設定で構成されているマシンのタグを表示します。タグ付けされたマシンに基づいてデータをフィルタリングすることもできます。この場合、タグ付けされたマシンの概要のみが表示されます。

容量バッファ（ピーク時）および容量バッファ（オフピーク時）

ピーク時およびオフピーク時のデリバリーグループの最大要件に基づいて、電源がオンになっているマシンのバッファの割合を表示します。

- **推定節約額**

  選択した期間にインフラストラクチャで達成された節約額を表示します。Autoscale機能が有効になっているAzureマシンについて、コンピューティング関連の節約とストレージ関連の節約から得られる節約額を表示できます。

- **電源管理対象マシン**

  Autoscaleが有効になっている場合、電源管理対象マシンは、コストを最適化するために使用されていないときに電源がオフになります。以下の詳細情報を取得できます。

  - 電源がオフになったマシンの数 - このデータは、電源がオフになり、コスト削減に貢献したマシンの数を分析するのに役立ちます。
  - 休止状態 - このデータは、休止状態にあるマシンの数を分析するのに役立ちます。
  - セッションなしで電源がオンになっているマシン - このデータは、セッションなしでマシンがアクティブであった理由を分析する機会を提供します。このデータは、より効果的なインフラストラクチャ節約戦略を計画する機会を提供します。
  - セッションありで電源がオンになっているマシン - このデータは、電源がオンになっていてアクティブなセッションがあるマシンの数を分析するのに役立ちます。
  - 電源オフ - このデータは、電源がオフまたは中断されたマシンの数と、このアクションがいつ実行されたかを分析するのに役立ちます。このデータを確認し、さらに変更を加えることで、コスト削減に貢献できます。
  - 電源オン - このデータは、電源がオンになったマシンの数と、このアクションがいつ実行されたかを分析するのに役立ちます。このデータを確認し、さらに変更を加えることで、コスト削減に役立てることができます。
  - セッションなしの失敗状態: このフィールドには、失敗状態にあり、アクティブなセッションがないマシンの数が表示されます。
  - セッションありの未登録状態: このフィールドには、未登録状態にあるがセッションを提供しているマシンの数が表示されます。

> **注:**

> セッションなしの失敗状態のマシンと、電源操作が失敗した状態のマシンの数を確認し、失敗の理由、時間、デリバリーグループに基づいてアクションを実行できます。これらの数はクリック可能なリンクであり、さらなるアクションのためにフィルターページに移動します。この数には、シングルセッションマシンとマルチセッションマシンの両方が含まれます。

- **同時セッション**

  選択した時点でのセッションの合計数を表示します。このデータは、コスト最適化のためにマシンをいつ電源オフにするかを決定するのに役立ちます。

- **平均ログオン時間**

  選択した期間におけるユーザーの平均ログオン時間を表示します。

ワークロードの適正化

「ワークロードの適正化」（以前は**「インフラストラクチャの適正化」**）ページは、リソース使用率に基づいて、デリバリーグループのプロビジョニングとサイジングの側面を分析するのに役立ちます。この分析に基づいて、次のことができます。

- 未使用のリソースへの支出を削減する
- 平均マシン稼働時間と正味の無駄な時間に基づいて計算される、マシンの正味アクティブ使用量を識別する。
- 特定のデリバリーグループの消費に対するマシンが、過剰、不足、または適正なサイズであるかどうかを識別する
- 使用率が主にパワーユーザーによって推進されているかどうかを識別する（グループの残りのマシンと比較して、上位5パーセンタイルのマシンによる使用率が高いことで示されます）

次の項目を使用して、ワークロードの適正化をフィルタリングできます。

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

ワークロードの適正化ページでは、次の機能が提供されます。

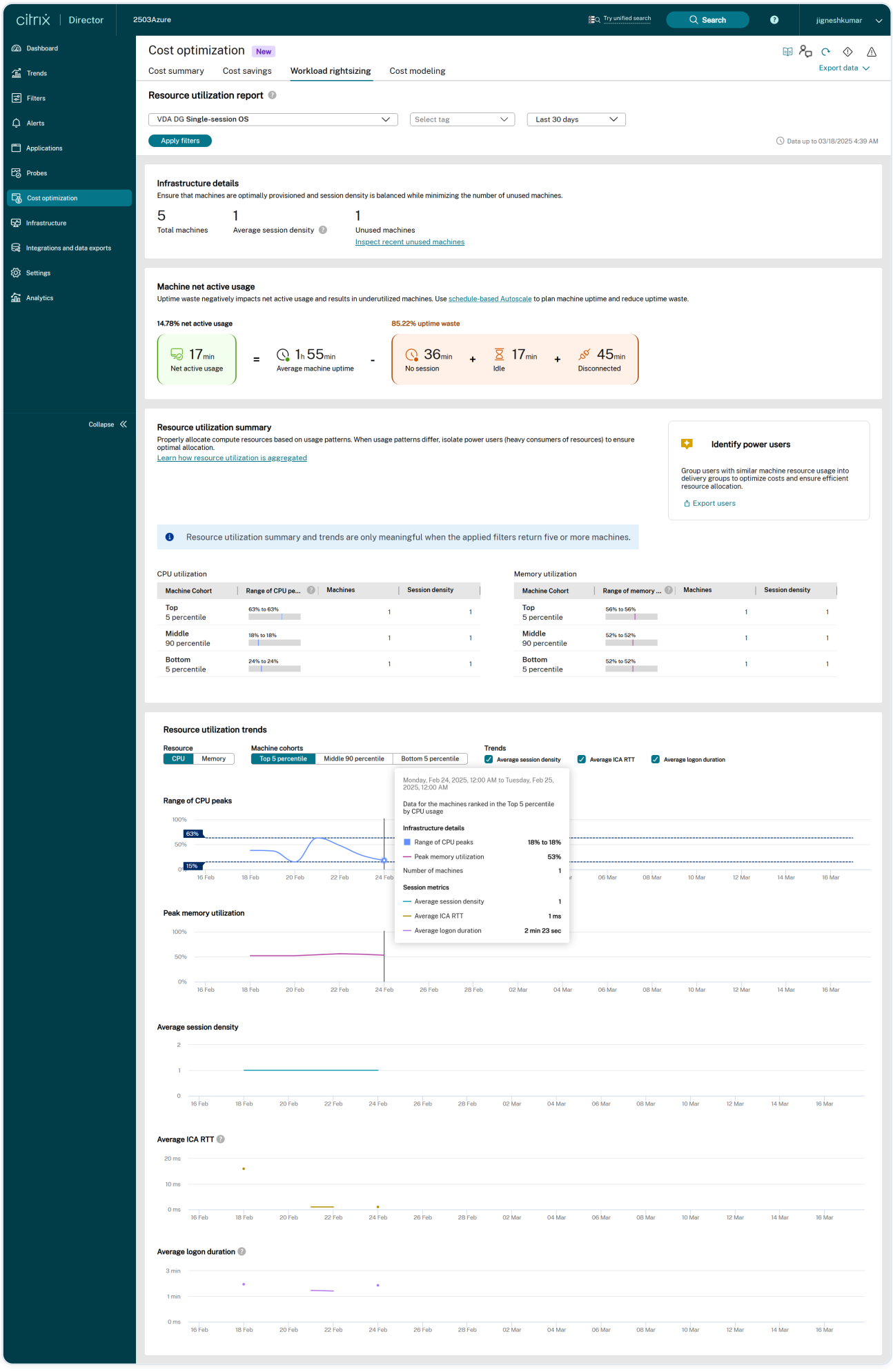
- マシンの正味アクティブ使用量に関するインサイト
- 使用率の詳細に関するインサイト
- パワーユーザーの詳細に関する洞察と、これらのデータのエクスポート
- リソース使用率の概要
- リソース使用率の傾向

このページに表示される集計データは、次のように更新されます。

- 過去24時間および過去7日間のフィルターでは1時間ごと
- 過去30日間のフィルターでは1日ごと

ホームページの左メニューから「**コスト最適化**」タブをクリックします。次に、「**ワークロードの適正化**」タブをクリックして、「**ワークロードの適正化**」ページにアクセスします。

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


citrix | Director
2503Azure
Try unified search
Search
jigneshkumar
Dashboard
Trends
Filters
Alerts
Applications
Probes
Cost optimization
Infrastructure
Integrations and data exports
Settings
Analytics
Collapse
Cost optimization
New
Cost summary
Cost savings
Workload rightsizing
Cost modeling
Export data
Resource utilization report
VDA DG Single-session OS
Select tag
Last 30 days
Apply filters
Data up to 03/18/2025 4:39 AM
Infrastructure details
Ensure that machines are optimally provisioned and session density is balanced while minimizing the number of unused machines.
5
Total machines
1
Average session density
1
Unused machines
Inspect recent unused machines
Machine net active usage
Uptime waste negatively impacts net active usage and results in underutilized machines. Use schedule-based Autoscale to plan machine uptime and reduce uptime waste.
14.78% net active usage
85.22% uptime waste
17 min
Net active usage
=
1h 55min
Average machine uptime
-
36min
No session
+
17 min
Idle
+
45min
Disconnected
Resource utilization summary
Properly allocate compute resources based on usage patterns. When usage patterns differ, isolate power users (heavy consumers of resources) to ensure optimal allocation.
Learn how resource utilization is aggregated
Identify power users
Group users with similar machine resource usage into delivery groups to optimize costs and ensure efficient resource allocation.
Export users
Resource utilization summary and trends are only meaningful when the applied filters return five or more machines.
CPU utilization
Machine Cohort
Range of CPU pe...
Machines
Session density
Top 5 percentile
63% to 63%
1
1
Middle 90 percentile
18% to 18%
1
1
Bottom 5 percentile
24% to 24%
1
1
Memory utilization
Machine Cohort
Range of memory ...
Machines
Session density
Top 5 percentile
56% to 56%
1
1
Middle 90 percentile
52% to 52%
1
1
Bottom 5 percentile
52% to 52%
1
1
Resource utilization trends
Resource
CPU
Memory
Machine cohorts
Top 5 percentile
Middle 90 percentile
Bottom 5 percentile
Trends
Average session density
Average ICA RTT
Average logon duration
Monday, Feb 24, 2025, 12:00 AM to Tuesday, Feb 25, 2025, 12:00 AM
Data for the machines ranked in the Top 5 percentile by CPU usage
Infrastructure details
Range of CPU peaks
18% to 18%
Peak memory utilization
53%
Number of machines
1
Session metrics
Average session density
1
Average ICA RTT
1 ms
Average logon duration
2 min 23 sec
Range of CPU peaks
Peak memory utilization
Average session density
Average ICA RTT
Average logon duration

「**ワークロードの適切なサイジング**」ページには、次のものが含まれます。

- マシンの正味アクティブ使用量
- 使用率の詳細
- リソース使用率の概要
- リソース使用率の傾向

マシンの正味アクティブ使用量:

このセクションには、コストを最適化できる詳細なマシン使用状況情報が表示されます。デリバリーグループ内のマシンの平均正味アクティブ使用時間を理解することで、管理者は最大の節約を実現するための最適な電源管理および課金戦略を決定できます。正味アクティブ使用量は、平均マシン稼働時間から合計稼働時間の無駄を差し引くことによって計算されます。すべての時間は分単位です。

「**マシンの正味アクティブ使用量**」セクションには、次の情報が表示されます。

- **正味アクティブ使用率:** ユーザーがマシンをアクティブに使用した実際の時間。これは、マシンが電源オンの状態で、少なくとも1つのセッションがアクティブであった期間です。
- **平均マシン稼働時間:** マシンが電源オンであった合計時間。
- **セッションなし:** アクティブなセッションがないことによる無駄な稼働時間。
- **アイドル時間:** アイドルセッションによる無駄な稼働時間。これは、マシン上のすべてのセッションがアイドル状態である時間です。
- **切断時間:** 切断されたセッションによる無駄な稼働時間。これは、マシン上のすべてのセッションが切断されている時間です。

使用率の詳細:

このセクションでは、選択したデリバリーグループおよび選択したタグの利用状況に関する詳細を提供します。過去24時間、7日間、30日間の詳細を表示できます。**利用状況の詳細**セクションでは、選択した時間フィルターの全期間に関する詳細を提供します。たとえば、7日間が選択されている場合、合計マシン数は、7日間の任意の時点で電源オンになっていたマシンの総数です。**利用状況の詳細**セクションでは、以下を提供します。

- **合計マシン数** - マシンの総数を表示します。このデータには、選択した期間中に電源オンになっていたすべてのマシンが含まれます。たとえば、7日間が選択されている場合、合計マシン数は、7日間の任意の時点で電源オンになっていたマシンの総数です。
- **平均セッション密度** - このデータは、マシンの数と選択した期間にわたる平均です。セッションに利用可能なリソースに影響を与える、マシン上のセッション負荷の量を指します。

- **平均マシン稼働時間** - これは、電源管理されたマシンの総稼働時間と選択された期間の比率です。1日あたりのマシンごとの稼働時間。1つのデリバリーグループまたは選択されたタグに2台のマシンがあり、1台のマシンが24時間使用され、もう1台のマシンが1時間使用されたとします。平均マシン稼働時間は12時間30分です。この例では、選択されたフィルター値は「過去24時間」です。
- **未使用のマシン** - 選択した期間中にセッションがなかったにもかかわらず、電源オンのままだったマシンの数を表示します。**未使用のマシン**リンクをクリックすると、**フィルター**タブが開き、現在電源オンでセッションがない、同じデリバリーグループ内のすべてのマシンを表示できます。

リソース使用状況の概要:

このセクションでは、選択したデリバリーグループおよび選択したタグのリソースがどのように使用されたかについての概要を提供します。最大5つのタグを選択できます。過去24時間、7日間、30日間の詳細を表示できます。マシンは利用状況に基づいてランク付けされます。**リソース利用状況の概要**セクションでは、アクティブセッションを持つマシンのCPU利用率とメモリ利用率に関する詳細を提供します。このセクションでは、パワーユーザーを特定するオプションも提供し、パワーユーザーデータをエクスポートするのに役立ちます。

- **CPU使用率**:
  - マシンコホート - CPU利用率に基づいて、上位、中間、下位に分類されたマシングループに関する情報を提供します。最も使用頻度の高いマシンの5%は**上位5パーセンタイル**に、最も使用頻度の低いマシンの5%は**下位5パーセンタイル**に、残りの90%は**中間90パーセンタイル**に分類されます。
  - CPUピークの範囲 - マシンコホートに対応する使用率に基づいて、CPUピークの範囲を表示します。
  - マシン - マシンコホートに対応するマシンの数を表示します。
  - セッション密度 - マシンコホートに対応するセッション密度を表示します。
- **メモリ使用率**:
  - マシンコホート - メモリ使用率に基づいて、上位、中間、下位に分類されたマシングループに関する情報を提供します。最も使用されているマシンの5%は**上位5パーセンタイル**に、最も使用されていないマシンの5%は**下位5パーセンタイル**に、残りの90%は**中間90パーセンタイル**に分類されます。
  - メモリピークの範囲 - マシンコホートに対応する使用率に基づいて、メモリピークの範囲を表示します。

- マシン - マシンコホートに対応するマシンの数を表示します。
- セッション密度 - マシンコホートに対応するセッション密度を表示します。
- パワーユーザーの特定 - このオプションを使用すると、パワーユーザーの詳細をエクスポートできます。

> **注**:
>
> この機能は、シングルセッションOSデリバリーグループでのみ利用可能です。

エクスポートデータには、**ユーザー名**、**合計セッション数**、**平均セッション期間 (分)**、**CPUピーク使用率 (%)**、および**メモリピーク使用率 (%)**が含まれます。

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

次の表は、**リソース使用率の概要**セクションに表示される値に基づいて実行可能なアクション項目に関する情報を提供します。

シナリオ	アクション項目
CPU使用率が高い	デリバリーグループのCPU仕様を増やします。または、使用率の高いユーザーを特定し、より良い仕様の別のデリバリーグループに移動します。
CPU使用率が低い	デリバリーグループのCPU仕様を減らします。
メモリ使用率が高い	デリバリーグループのメモリ仕様を増やします。
メモリ使用率が低い	デリバリーグループのメモリ仕様を減らします。

「リソース使用率の概要」セクションのデータはどのように入力されるか?

リソース使用率の概要セクションのデータは、**リソース使用率の傾向**のデータに基づいて入力されます。この概要には、アクティブなセッションを持つマシンのみの詳細が表示されます。5台以上のマシンがある場合、概要はより良い結果を提供します。

選択したデリバリーグループ内のマシンの数に基づいて、最大および最小使用率が計算されます。

たとえば、期間として「過去7日間」を選択し、選択したデリバリーグループに20台のマシンがあるとします。これらの20台のマシンは、さらに**上位5パーセンタイル**、**中間90パーセンタイル**、**下位5パーセンタイル**に分類されます。CPUとメモリの使用率は、アクティブなセッションがある場合に計算されます。たとえば、このケースでは、最初と最後のマシンが上位5パーセンタイルと下位5パーセンタイルに入ります。残りの18台のマシンは中間90パーセンタイルに分類されます。このケースでは、**上位5パーセンタイル**にマシンが1台しかないため、最大値と最小値は同じになります。コホートに複数のマシンがある場合、コホートの最高値と最低値は、そのグループ内で最もランクの高いマシンの最大値と、最もランクの低いマシンの最大値にそれぞれ基づきます。

リソースタイプとして**CPU**を選択すると、選択したマシンの**CPUピーク範囲**と**ピークメモリ使用率**が表示されます。

リソースタイプとしてメモリを選択すると、選択したマシンのメモリピーク範囲とピークCPU使用率が表示されます。

リソース使用率の傾向: このセクションでは、CPUピークの範囲、ピークメモリ使用率、平均セッション密度、平均ICA® RTT、および平均ログオン期間のグラフ表示を提供します。

以下の詳細をフィルターできます。

- リソース - CPUとメモリ
- マシンコホート - 上位5パーセンタイル、中間90パーセンタイル、下位5パーセンタイル
- 傾向 - 平均セッション、平均ICA RTT、平均ログオン期間。

次のグラフを表示できます。

- **CPUピークの範囲** - CPUピークの範囲を帯状に表示します。帯の任意のポイントにカーソルを合わせると、帯の上限値と下限値が表示されます。
- **メモリ使用率のピーク** - 選択したマシンと選択した期間のメモリ使用率の最高値をグラフで表示します。
- **平均セッション密度** - 選択したマシンと選択した期間の平均セッション密度をグラフで表示します。
- **平均ICA RTT** - セッションの平均ラウンドトリップタイムを表示します。このグラフは、アクティブなセッションがない場合やセッションが切断されている場合に中断を示します。
- **平均ログオン期間** - 選択したマシンおよび選択した期間の平均ログオン期間をグラフで表示します。このグラフは、選択した期間中に新しいログオンが開始された場合にデータを表示します。

コスト概要

コストの概要ページには、Citrix®環境の実行に関連する費用の包括的な概要が表示されます。この機能強化により、以下を可視化できます。

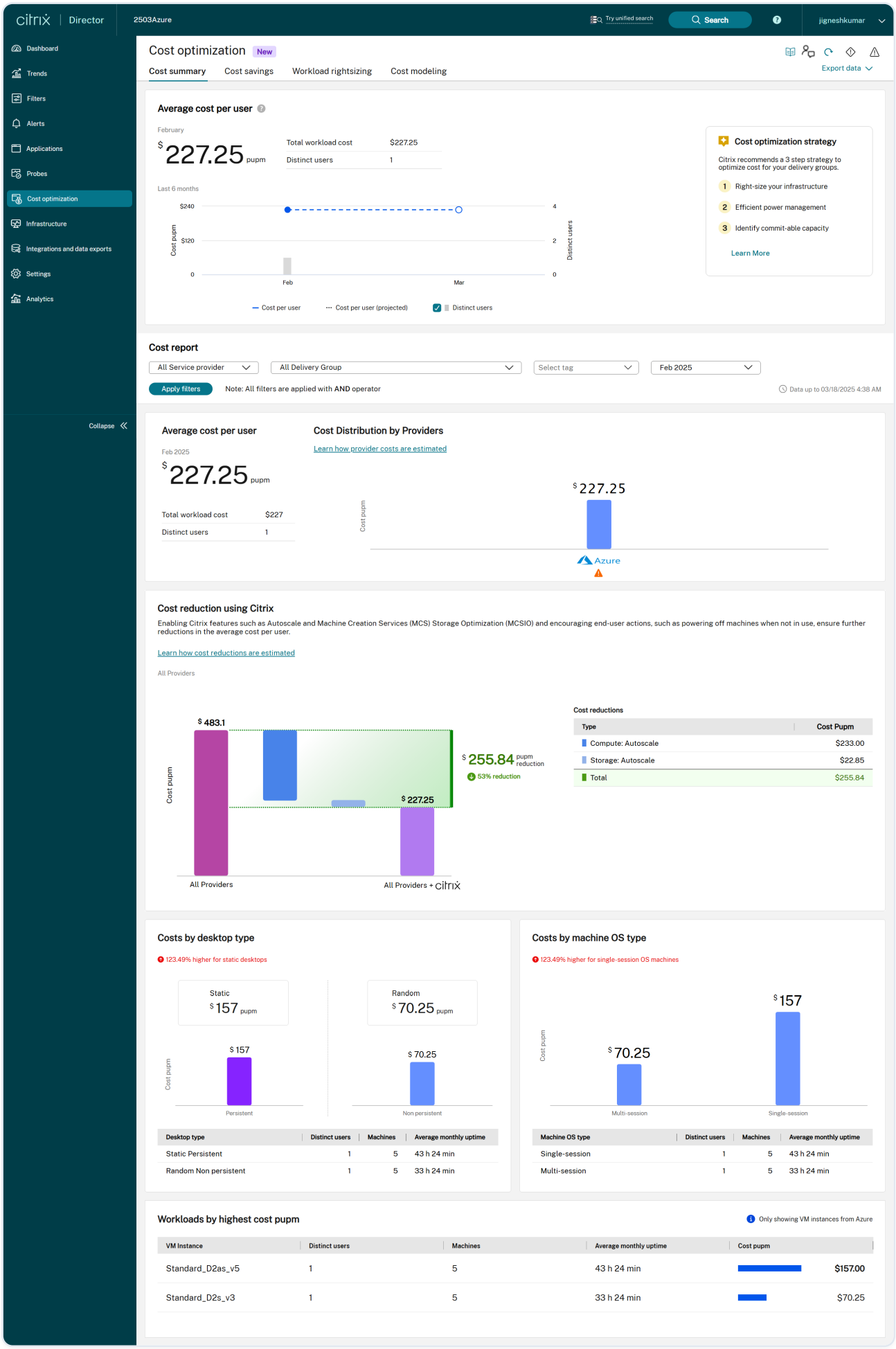
- ユーザーあたりの総コスト
- 選択されたワークロードプロバイダー、デスクトップタイプ、およびVMシリーズセットによる仮想化提供のコスト

このページでは、以下を提供します。

- 仮想化されたアプリまたはデスクトップをユーザーに提供するコストに関する洞察
- 節約された金額
- コストと節約に関する情報（カテゴリ別）：
  - プラットフォームプロバイダー
  - OSの種類
  - デスクトップの種類
  - VMシリーズ

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

> 「**コスト概要**」ページにアクセスするには、「**Director**」>「**コスト最適化**」>「**コスト概要**」をクリックします。「**コスト概要**」ページが表示されます。


citrix | Director
2503Azure
Try unified search
Search
jigneshkumar
Dashboard
Trends
Filters
Alerts
Applications
Probes
Cost optimization
Infrastructure
Integrations and data exports
Settings
Analytics
Collapse
Cost optimization
New
Cost summary
Cost savings
Workload rightsizing
Cost modeling
Export data
Average cost per user
February
$ 227.25 pupm
Total workload cost $227.25
Distinct users 1
Last 6 months
$240
$120
0
Cost pupm
4
2
0
Distinct users
Feb
Mar
Cost per user
Cost per user (projected)
Distinct users
Cost optimization strategy
Citrix recommends a 3 step strategy to optimize cost for your delivery groups.
1 Right-size your infrastructure
2 Efficient power management
3 Identify commit-able capacity
Learn More
Cost report
All Service provider
All Delivery Group
Select tag
Feb 2025
Apply filters
Note: All filters are applied with AND operator
Data up to 03/18/2025 4:38 AM
Average cost per user
Feb 2025
$ 227.25 pupm
Total workload cost $227
Distinct users 1
Cost Distribution by Providers
Learn how provider costs are estimated
$ 227.25
Cost pupm
Azure
Cost reduction using Citrix
Enabling Citrix features such as Autoscale and Machine Creation Services (MCS) Storage Optimization (MCSIO) and encouraging end-user actions, such as powering off machines when not in use, ensure further reductions in the average cost per user.
Learn how cost reductions are estimated
All Providers
$ 483.1
$ 255.84 pupm reduction
53% reduction
$ 227.25
Cost pupm
All Providers
All Providers + citrix
Cost reductions
Type
Cost Pupm
Compute: Autoscale $233.00
Storage: Autoscale $22.85
Total $255.84
Costs by desktop type
123.49% higher for static desktops
Static
$ 157 pupm
Random
$ 70.25 pupm
$ 157
$ 70.25
Cost pupm
Persistent
Non persistent
Desktop type
Distinct users
Machines
Average monthly uptime
Static Persistent 1 5 43 h 24 min
Random Non persistent 1 5 33 h 24 min
Costs by machine OS type
123.49% higher for single-session OS machines
$ 157
$ 70.25
Cost pupm
Multi-session
Single-session
Machine OS type
Distinct users
Machines
Average monthly uptime
Single-session 1 5 43 h 24 min
Multi-session 1 5 33 h 24 min
Workloads by highest cost pupm
Only showing VM instances from Azure
VM Instance
Distinct users
Machines
Average monthly uptime
Cost pupm
Standard_D2as_v5 1 5 43 h 24 min $157.00
Standard_D2s_v3 1 5 33 h 24 min $70.25

「**コスト概要**」ページには以下が含まれます。

- **ユーザーあたりの平均コスト**

  過去6か月間の月間ユーザーあたりの実際のコストと、今月の予測コストを表示できます。さらに、ワークロードの総コストとサイト上のユニークユーザー数を確認できます。複数の通貨が関係している場合、USDが含まれていればコストはUSDで表示されます。そうでない場合は、リストからランダムに選択された通貨でコストが表示されます。先月および先々月と比較したコスト削減額がパーセンテージで表示されます。また、ユニークユーザー数の変化も表示されます。グラフ表示では、毎月の傾向が示されます。

  ユーザーあたりの平均コストを使用して、使用状況を最適化できます。

- **コストレポート**

  選択したサービスプロバイダー、選択したデリバリーグループ、および選択したタグのコストレポートを表示できます。過去3か月間のレポートを個別に表示するか、過去3か月間のデータを統合して表示できます。

- **Citrix を使用したコスト削減**

  AutoscaleやMachine Creation Services™ (MCS)、Storage Optimization (MCSIO) などのCitrix機能を有効にすることで、ユーザーあたりの平均コストをさらに削減できます。また、使用していないときにマシンをシャットダウンするなど、エンドユーザーの行動を促すこともできます。

  このデータは、Citrix機能を適用した場合の合計削減額を表示します。また、エンドユーザーの行動による削減額も表示されます。

- **デスクトップタイプ別のコスト**

  次の種類のデスクトップのコストを表示できます。

  - **静的永続:** ユーザーは毎回同じ仮想デスクトップにサインオンし、デスクトップに加えられた変更は保存されます。
  - **静的非永続:** ユーザーは毎回同じ仮想デスクトップにサインオンしますが、デスクトップに加えられた変更は保存されません。
  - **ランダム永続:** ユーザーはデスクトッププールから仮想デスクトップを割り当てられ、デスクトップに加えられた変更は保存されます。
  - **ランダム非永続:** ユーザーにはデスクトップのプールから仮想デスクトップが割り当てられ、デスクトップに加えられた変更は保存されません。

各マシンタイプについて、個別のユーザー数、マシン数、および月間平均稼働時間を表示できます。

このデータを使用して、ユーザーを異なる種類のデスクトップに移動することでコストを節約する計画を立てることができます。たとえば、静的永続デスクトップタイプは、ランダム非永続デスクトップと比較して、より多くのリソース使用量を必要とします。したがって、一部のユーザーを静的永続デスクトップタイプからランダム非永続デスクトップタイプに移動する計画を立てることができます。

- **OSタイプ別のコスト**

  シングルセッションおよびマルチセッションOSタイプのコストを表示できます。マシンのOSタイプ、個別のユーザー数、マシン数、および月間平均稼働時間を表示できます。このデータを使用して、ユーザーを異なる種類のOSに移動することでコストを節約する計画を立てることができます。

- **ユーザーあたりの月間最高コストによるワークロード**

  仮想マシンインスタンス、個別のユーザー数、マシンの平均稼働時間など、ユーザーあたりの月間最高コストの詳細を表示できます。また、マシン数とユーザーあたりのコストも確認できます。

  このデータを使用して、各VM構成タイプのコストを表示し、どの構成をユーザーに割り当てるかを決定します。

機能互換性マトリックス

Citrix Director 7 2503 は以下と互換性があります。

- Citrix Virtual Apps and Desktops™ 7 2112 およびそれ以降のバージョン
- シトリックス バーチャルアプリおよびデスクトップ 7 1912 LTSR

各サイト内で、Directorを以前のバージョンのDelivery Controller™と併用できますが、Directorの最新バージョンのすべての機能が利用できない場合があります。Citrixは、Director、Delivery Controller、およびVDAを同じバージョンにすることをお勧めします。

> **注:**
>
> Delivery Controllerをアップグレードした後、Studioを開くと、サイトをアップグレードするように求められます。詳細については、展開のアップグレード の「**アップグレードシーケンス**」セクションを参照してください。

Directorのアップグレード後に初めてログインすると、構成済みのサイトでバージョンチェックが実行されます。いずれかのサイトがDirectorよりも古いバージョンのControllerを実行している場合、Directorコンソールにサイトのアップグレードを推奨するメッセージが表示されます。さらに、サイトのバージョンがDirectorよりも古い間は、この不一致を示すメモがDirectorダッシュボードに表示され続けます。

注:

以前のバージョンのCitrix Directorでは、最近のVDAバージョンで実行されているユーザーセッションに適用されたポリシーは表示されません。Citrix Director 1912以前のバージョンでは、VDAバージョン2003以降で実行されているユーザーセッションに適用されたポリシーは表示されません。これらのポリシーを表示するには、Citrix Directorバージョン2003以降を使用してください。

デリバリーコントローラー (DC)、VDA、およびその他の必要な依存コンポーネントの最小バージョンと、ライセンスエディションを伴う特定のDirector機能は、以下に示します。

DIRECTOR バージョン	機能	依存関係 - 必要な最小バージョン	エディション
2503	Azureワークロードのコストモデリング (/ja-jp/citrix-virtual-apps-desktops/2503/director/cost-optimization/cost-modeling.html)	なし	すべて
2503	コスト削減ページへの機能強化(/ja-jp/citrix-virtual-apps-desktops/2503/director/cost-optimization/cost-savings.html)	なし	すべて

DIRECTOR バージョン	機能	依存関係 - 必要な最小バージョン	エディション
2503	uberAgentとのDirector統合(/ja-jp/citrix-virtual-apps-desktops/2503/director/install-and-configure#citrix-uberagent-integration-with-director)	VDA 2503 (uberAgentがインストール済み)	すべて
2503	ローカルアプリケーション使用状況レポート(/ja-jp/citrix-virtual-apps-desktops/2503/director/site-analytics/application-usage-monitoring)	VDA 2503	プラチナライセンスサイト
2503	VDAログオン期間の詳細の監視(/ja-jp/citrix-virtual-apps-desktops/2503/director/troubleshoot-deployments/user-issues/user-logon#logon-process-phases)	VDA 2503	すべて
2503	Provisioning Serviceの追加メトリック収集(/ja-jp/citrix-virtual-apps-desktops/2503/director/infrastructure-monitoring/infrastructure-dashboard#provisioning-service-health-metrics)	VDA 2503	すべて

DIRECTOR バージョン	機能	依存関係 - 必要な最小バージョン	エディション
2503	Microsoft Teams以外のHDX最適化の監視を拡張するオプション(/ja-jp/citrix-virtual-apps-desktops/2503/director/troubleshoot-deployments/user-issues/session-performance#hdx-optimization-details)	VDA 2503	すべて
2503	フィルタービューとセッションパフォーマンスタブでのセッション自動再接続の詳細(/ja-jp/citrix-virtual-apps-desktops/2503/director/site-analytics/trends)	VDA 2503	すべて
2503	Citrix Director 向け統合プラットフォームエクスペリエンス	なし	すべて
2503	ユーザーアクションの一括操作オプションを制限するカスタムロール(/ja-jp/citrix-virtual-apps-desktops/2503/director/troubleshoot-deployments/user-issues/custom-role-to-limit-bulk-action)	なし	すべて
2503	Provisioning Service および Delivery Controller のサイトレベルアラートを設	VDA 2503	すべて

DIRECTOR バージョン	機能	依存関係 - 必要な最小バージョン	エディション
	定するプロビジョン(/ja-jp/citrix-virtual-apps-desktops/2503/director/site-analytics/alerts-notifications#alerts-for-infrastructure-monitoring)		
2503	Webhookとの統合(/ja-jp/citrix-virtual-apps-desktops/2503/director/integrations-and-data-exports#integrations-with-alerting-and-itsm-tools)	なし	すべて
2411	アプリケーションページでの、使用頻度の低い公開アプリと未使用の公開アプリのレポート(/ja-jp/citrix-virtual-apps-desktops/2503/director/site-analytics/application-usage-monitoring#least-used-and-unused-published-apps-report)	ディーディーシー 7.16、ブイディーエー 7.15	Platinumライセンスサイト
2411	アクティビティマネージャーでのTCPまたはUDPアプリの列挙されたアプリケーションの詳細(/ja-jp/citrix-virtual-apps-desktops/2503/	VDA 2411およびDDC 2411	すべて

DIRECTOR バージョン	機能	依存関係 - 必要な最小バージョン	エディション
	director/spa-integration-with-director#session-topology-view-for-secure-private-access-apps.)		
2411	PowerShell SDKを使用したWebhook構成 (/ja-jp/citrix-virtual-apps-desktops/2503/director/site-analytics/alerts-notifications#webhook-configuration-using-powershell-sdk)	VDA 2411およびDDC 2411	すべて
2411	一括アラート解除	VDA 2411およびDDC 2411	すべて
2411	ワークロードの適正化ページでのマシンの純アクティブ使用量	なし	すべて
2411	ストレージ使用量の最適化によるコスト削減 (プレビュー)	なし	すべて
2411	コスト概要 (プレビュー)	なし	すべて
2411	「Delivery Controllerの監視 (プレビュー)」(/ja-jp/citrix-virtual-apps-desktops/2503/director/infrastructure-monitoring/	VDA 2411	すべて

DIRECTOR バージョン	機能	依存関係 - 必要な最小バージョン	エディション
	infrastructure-dashboard#delivery-controller-health-metrics)		
2411	「UI から Citrix コンポーネントを接続する (プレビュー)」(/ja-jp/citrix-virtual-apps-desktops/2503/director/infrastructure-monitoring/manage-connections)	VDA 2411	すべて
2407	「コスト最適化」(/ja-jp/citrix-virtual-apps-desktops/2503/director/cost-optimization#cost-savings)	なし	すべて
2407	「統合とデータエクスポート」(/ja-jp/citrix-virtual-apps-desktops/2503/director/integrations-and-data-exports)	VDA 2407	すべて
2407	過去のユーザーセッションを診断する (プレビュー)	VDA 2407	すべて
2407	Secure Private Accessセッション用アクティビティマネージャー (プレビュー)	VDA 2407	すべて

DIRECTOR バージョン	機能	依存関係 - 必要な最小バージョン	エディション
2407	DirectorによるTCPおよびUDPアプリのSecure Private Access統合 (プレビュー)	VDA 2407	すべて
2407	「インフラストラクチャ監視 (プレビュー)」(/ja-jp/citrix-virtual-apps-desktops/2503/director/infrastructure-monitoring)	VDA 2407	すべて
2407	「未登録マシンアラート」(/ja-jp/citrix-virtual-apps-desktops/2503/director/site-analytics/alerts-notifications#unregistered-machines-in-)	VDA 2407 および DDC 2407	すべて
2407	「マシン稼働時間アラート」(/ja-jp/citrix-virtual-apps-desktops/2503/director/site-analytics/alerts-notifications#machine-uptime-alert-1)	VDA 2407 および DDC 2407	すべて
2407	「電源オンアクション失敗および電源オフアクション失敗アラート」(/ja-jp/citrix-virtual-apps-desktops/2503/director/site-	VDA 2407 および DDC 2407	すべて

DIRECTOR バージョン	機能	依存関係 - 必要な最小バージョン	エディション
	analytics/alerts-notifications#failed-power-on-action-and-failed-power-off-action)		
2407	アラートメールにCSV添付ファイルを含め、アラートWebhookにJSONペイロードを含める機能(/ja-jp/citrix-virtual-apps-desktops/2503/director/site-analytics/alerts-notifications#enhancements-on-alert-content)	VDA 2407およびDDC 2407	すべて
2407	最近の電源操作があるマシンを検査する(/ja-jp/citrix-virtual-apps-desktops/2503/director/troubleshoot-deployments/machines#inspect-machines-with-recent-power-actions)	VDA 2407	すべて
2407	高度なアラートポリシー(/ja-jp/citrix-virtual-apps-desktops/2503/director/site-analytics/alerts-notifications#advanced-alert-policies)	VDA 2407およびDDC 2407	すべて

DIRECTOR バージョン	機能	依存関係 - 必要な最小バージョン	エディション
2407	クラウドおよびオンプレミスユーザー向け統合検索(/ja-jp/citrix-virtual-apps-desktops/2503/director/unified-search)	DDC 2407	すべて
2407	ダッシュボード上の公開アプリケーション使用状況監視チャート(/ja-jp/citrix-virtual-apps-desktops/2503/director/site-analytics/application-usage-monitoring)	VDA 2407およびDDC 2407	Platinumライセンスサイト
2402 LTSR	DirectorによるWebおよびSaaSアプリのSecure Private Access統合（プレビュー）(/ja-jp/citrix-virtual-apps-desktops/2503/2402-ltsr/director/spa-integration-with-director)	VDA 2402 LTSR	すべて
2402 LTSR	Microsoft Teamsバージョン2.1以前のサポート(/ja-jp/citrix-virtual-apps-desktops/2503/2402-ltsr/director/troubleshoot-deployments/user-issues#microsoft-teams-optimization-status)	VDA 2402 LTSR	すべて

DIRECTOR バージョン	機能	依存関係 - 必要な最小バージョン	エディション
2311	ライブセッションと録画セッションの再生(/ja-jp/citrix-virtual-apps-desktops/2503/director/troubleshoot-deployments/user-issues/record-sessions#play-back-live-and-recorded-sessions)	VDA 2308 および DDC 2311	すべて
2311	セッショントポロジとパフォーマンスメトリック	複数のバージョン - リンク	すべて
2311	最適な画面解像度	なし	すべて
2311	MS Teams の最適化	VDA 2311 および DDC 最新	すべて
2311	プローブの概要の機能強化(/ja-jp/citrix-virtual-apps-desktops/2503/director/probes#step-4-view-probe-results)	なし	すべて
2311	改良されたセッションログオン期間ビュー(/ja-jp/citrix-virtual-apps-desktops/2503/director/troubleshoot-deployments/user-issues/user-logon)	なし	すべて
2308	プローブの概要とドリルダウン(/ja-jp/citrix-virtual-apps-	なし	すべて

DIRECTOR バージョン	機能	依存関係 - 必要な最小バージョン	エディション
	desktops/2503/director/probes#step-4-view-probe-results)		
2308	Citrix Gateway多要素認証のCitrix Probe Agentサポート(/ja-jp/citrix-virtual-apps-desktops/2503/director/probes/#step-1-install-and-configure-the-citrix-probe-agent)	シトリックス ゲートウェイ	すべて
2308	ハイパーバイザーアラートの無効化	なし	すべて
2308	セッションエクスペリエンスメトリックの傾向	なし	すべて
2305	Citrix Gateway を介した認証のサポート	なし	すべて
2305	Director での Autoscale 管理	なし	すべて
2303	失敗したマシンのアラート	DC 7 2303	プレミアム
2203	TLS 1.3のサポート	-	すべて
2212	AMD GPUで利用可能なリアルタイムGPU使用率	64ビットWindowsおよびHDX 3D Proが有効なDC 7.14およびVDA 7.14	すべて
2212	高度なプローブスケジューリング	DC 7 1906 と Citrix Probe Agent 2209 の組み合わせ	プレミアム

DIRECTOR バージョン	機能	依存関係 - 必要な最小バージョン	エディション
1909	Citrix Analytics for Performance を使用してオンプレミスサイトを構成する	DC 7 1906 および VDA 1906	すべて
1906	セッションの自動再接続	DC 7 1906 および VDA 1906	すべて
1906	セッションの起動時間	DC 7 1906 および VDA 1903	すべて
1906	デスクトッププロービング(/ja-jp/citrix-virtual-apps-desktops/2503/director/probes.html)	DC 7 1906 と Citrix Probe Agent 1903 の組み合わせ	プレミアム
7.9以降	Citrix Profile Managementのプロファイル読み込み時間(/ja-jp/citrix-virtual-apps-desktops/2503/director/troubleshoot-deployments/user-issues/user-logon.html#profile-load)	VDA 1903	すべて
1811	プロファイルドリルダウン(/ja-jp/citrix-virtual-apps-desktops/2503/director/troubleshoot-deployments/user-issues/user-logon.html#profile-load)	DC 7 1811およびVDA 1811	すべて
1811	ハイパーバイザーアラート監視(/ja-jp/	DC 7 1811	プレミアム

DIRECTOR バージョン	機能	依存関係 - 必要な最小バージョン	エディション
	citrix-virtual-apps-desktops/2503/director/site-analytics/alerts-notifications.html#hypervisor-alerts-monitoring)		
1811	アプリケーションプロービング(/ja-jp/citrix-virtual-apps-desktops/2503/director/probes.html)	DC 7 1811 と シトリックス アプリケーション プローブ エージェント 1811	プレミアム
1811	Microsoft RDS ライセンスの健全性(/ja-jp/citrix-virtual-apps-desktops/2503/director/troubleshoot-deployments/machines.html#microsoft-rds-license-health)	DC 7 1811 および VDA 7.16	すべて
1811	主要なRTOPデータの表示(/ja-jp/citrix-virtual-apps-desktops/2503/)	DC 7 1811 および VDA 1808	プレミアム
1808	フィルターデータのエクスポート(/ja-jp/citrix-virtual-apps-desktops/2503/director/site-analytics/filters-data.html)	DC 7 1808	すべて
1808	インタラクティブセッションのドリルダウン	DC 7 1808および VDA 1808	すべて

DIRECTOR バージョン	機能	依存関係 - 必要な最小バージョン	エディション
1808	GPOのドリルダウン	DC 7 1808およびVDA 1808	すべて
1808	OData APIを使用したマシンの履歴データ	DC 7 1808	すべて
7.18	アプリケーションプロービング	DC 7.18	プレミアム（旧 プラチナ）
7.18	スマートアラートポリシー	DC 7.18	プレミアム（旧 プラチナ）
7.18	Health Assistant リンク	なし	すべて
7.18	インタラクティブセッションのドリルダウン	なし	すべて
7.17	PIVスマートカード認証(/ja-jp/citrix-virtual-apps-desktops/2503/director.html#use-director-with-piv-smart-card-authentication)	なし	すべて
7.16	アプリケーション分析(/ja-jp/citrix-virtual-apps-desktops/2503/director/troubleshoot-deployments/applications.html)	DC 7.16およびVDA 7.15	すべて
7.16	OData エーピーアイ バージョン4	DC 7.16	すべて

DIRECTOR バージョン	機能	依存関係 - 必要な最小バージョン	エディション
7.16	Linux VDAユーザーのシャドウ(/ja-jp/citrix-virtual-apps-desktops/2503/director/troubleshoot-deployments/user-issues/shadow-users.html)	VDA 7.16	すべて
7.16	ドメインローカルグループのサポート	なし	すべて
7.16	マシンのコンソールアクセス	DC 7.16	すべて
7.15	アプリケーション障害監視	DC 7.15およびVDA 7.15	すべて
7.14	アプリケーション中心のトラブルシューティング	DC 7.13およびVDA 7.13	すべて
7.14	ディスク監視	DC 7.14およびVDA 7.14	すべて
7.14	GPU監視	DC 7.14およびVDA 7.14	すべて
7.13	セッション詳細パネルのトランスポートプロトコル	DC 7.xおよびVDA 7.13	すべて
7.12	ユーザーフレンドリーな接続およびマシンの障害の説明	DC 7.12 と VDA 7.x	すべて
7.12	Enterpriseエディションでの履歴データ可用性の向上	DC 7.12 と VDA 7.x	エンタープライズ

DIRECTOR バージョン	機能	依存関係 - 必要な最小バージョン	エディション
7.12	カスタムレポート	DC 7.12 と VDA 7.x	プレミアム（旧 Platinum）
7.11	リソース使用率レポート	DC 7.11 と VDA 7.11	すべて
7.11	CPU、メモリ、ICA RTTの状況に対するアラート機能の拡張(/ja-jp/citrix-virtual-apps-desktops/2503/director/site-analytics/alerts-notifications.html)	DC 7.11およびVDA 7.11	プレミアム（旧プラチナ）
7.11	レポートのエクスポート機能の改善(/ja-jp/citrix-virtual-apps-desktops/2503/director/site-analytics.html#export-reports)	DC 7.11およびVDA 7.x	すべて
7.11	Citrix ADMとの統合(/ja-jp/citrix-virtual-apps-desktops/2503/director/install-and-configure/hdx-insight.html)	DC 7.11、VDA 7.x、およびMASバージョン11.1 Build 49.16	プレミアム（旧プラチナ）
7.9	ログオン期間の内訳(/ja-jp/citrix-virtual-apps-desktops/2503/director/troubleshoot-deployments/user-issues/user-logon.html)	DC 7.9およびVDA 7.x	すべて
7.7	プロアクティブな監視とアラート	DC 7.7およびVDA 7.x	プレミアム (旧称 プラチナ)

DIRECTOR バージョン	機能	依存関係 - 必要な最小バージョン	エディション
7.7	Windows認証統合	DC 7.xおよびVDA 7.x	すべて
7.7	シングルセッションおよびマルチセッションOSの使用状況	DC 7.7およびVDA 7.x	プレミアム (旧称 プラチナ)
7.6.300	Framehawk仮想チャネルのサポート	DC 7.6およびVDA 7.6	すべて
7.6.200	セッション記録の統合	DC 7.6およびVDA 7.x	プレミアム (旧 プラチナ)
7	HDX Insightの統合	DC 7.6、VDA 7.x、およびCitrix ADM	プレミアム (旧 プラチナ)

データの粒度と保持

データ値の集計

Monitor Serviceは、ユーザーセッションの使用状況、ユーザーログオンパフォーマンスの詳細、セッション負荷分散の詳細、接続およびマシン障害情報など、さまざまなデータを収集します。データはカテゴリに応じて異なる方法で集計されます。ODataメソッドAPIを使用して提示されるデータ値の集計を理解することは、データを解釈するために不可欠です。例：

- 接続されたセッションとマシン障害は一定期間に発生します。したがって、それらは一定期間の最大値として公開されます。
- ログオン期間は時間の長さを測定するものであるため、一定期間の平均として公開されます。
- ログオン数と接続障害は一定期間の発生回数であるため、一定期間の合計として公開されます。

同時データ評価

セッションは、同時であると見なされるためには重複している必要があります。ただし、時間間隔が1分の場合、その1分間のすべてのセッション（重複しているかどうかに関わらず）は同時であると見なされます。間隔のサイズが非常に小さいため、精度を計算するのに伴うパフォーマンスオーバーヘッドは、追加される価値に見合いません。セッションが同じ時間内に発生しても、同じ分内で発生しない場合、それらは重複しているとは見なされません。

サマリーテーブルと生データの相関

データモデルは、メトリックを2つの異なる方法で表します。

- サマリーテーブルは、メトリックの集計ビューを分単位、時間単位、日単位の粒度で表します。
- 生データは、セッション、接続、アプリケーション、およびその他のオブジェクトで追跡される個々のイベントまたは現在の状態を表します。

API呼び出し間またはデータモデル自体内でデータを関連付けようとする場合、以下の概念と制限を理解することが重要です。

- **部分的な間隔のサマリーデータはありません。** メトリックのサマリーは、長期間にわたる履歴トレンドのニーズを満たすように設計されています。これらのメトリックは、完全な間隔についてサマリーテーブルに集計されます。データ収集の開始時（利用可能な最も古いデータ）または終了時の部分的な間隔に対するサマリーデータはありません。1日（Interval=1440）の集計を表示する場合、これは最初と最新の不完全な日にはデータがないことを意味します。これらの部分的な間隔には生データが存在する可能性がありますが、集計されることはありません。特定のデータ粒度に対する最も早い集計間隔と最も遅い集計間隔は、特定のサマリーテーブルから最小および最大のSummaryDateを抽出することで判断できます。SummaryDate列は間隔の開始を表します。Granularity列は集計データの期間の長さを表します。
- **時間による相関。** メトリックは、前述のセクションで説明されているように、完全な間隔についてサマリーテーブルに集計されます。これらは履歴トレンドに使用できますが、生イベントはトレンド分析のために集計されたものよりも現在の状態に近い場合があります。サマリーデータと生データの時間ベースの比較では、発生する可能性のある部分的な間隔や期間の開始と終了に対するサマリーデータがないことを考慮する必要があります。
- **見逃されたイベントと潜在的なイベント。** 集計期間に見逃されたイベントや潜在的なイベントがある場合、サマリーテーブルに集計されるメトリックはわずかに不正確になる可能性があります。Monitor Serviceは正確な現在の状態を維持しようとしますが、見逃されたイベントや潜在的なイベントのために、サマリーテーブルの集計を再計算するために過去に戻ることはありません。
- **接続の高可用性。** 接続の高可用性中、現在の接続のサマリーデータカウントにギャップが生じますが、セッションインスタンスは引き続き生データで実行されます。
- **データ保持期間。** サマリーテーブルのデータは、生イベントデータのスケジュールとは異なるグルーミングスケジュールで保持されます。サマリーテーブルまたは生データテーブルからグルーミングによって削除されたため、データが欠落している可能性があります。保持期間は、サマリーデータの粒度によって異なる場合もあります。粒度の低いデータ（分単位）は、粒度の高いデータ（日単位）よりも早くグルーミングされます。グルーミングによってある粒度か

らデータが欠落している場合でも、より高い粒度で見つかる可能性があります。API呼び出しは要求された特定の粒度のみを返すため、ある粒度でデータが受信されないからといって、同じ期間のより高い粒度でデータが存在しないという意味ではありません。

- **タイムゾーン。** メトリックはUTCタイムスタンプで保存されます。サマリーテーブルは、時間単位のタイムゾーン境界で集計されます。時間単位の境界に該当しないタイムゾーンの場合、データが集計される場所に関して多少の不一致が生じる可能性があります。

粒度と保持

Directorによって取得される集計データの粒度は、要求された時間 (T) スパンの関数です。ルールは次のとおりです。

- 0 \< T \<= 1時間 - 分単位の粒度を使用
- 0 \< T \<= 30日 - 時間単位の粒度を使用
- T \> 31日 - 日単位の粒度を使用

集計データから取得されない要求データは、生のセッションおよび接続情報から取得されます。このデータは急速に増加する傾向があるため、独自のグルーミング設定があります。グルーミングにより、関連データのみが長期的に保持されます。グルーミングにより、レポートに必要な粒度を維持しながら、パフォーマンスが向上します。Premiumライセンスサイトのお客様は、グルーミング保持期間を希望する保持日数に変更できます。変更しない場合はデフォルトが使用されます。サイトデータベースとの接続が失われた場合、Monitor Serviceは以下の表で指定されているPremiumエンタイトルメントのデフォルト保持日数を使用します。

設定にアクセスするには、Delivery Controller™ で次のPowerShellコマンドを実行します。

```
asnp Citrix.*

 Get-MonitorConfiguration

 Set-MonitorConfiguration -<setting name> <value>
```

#	設定名	影響を受けるスキーマテーブル	MONITOR ページで影響を受けるテーブルとグラフ	PREMIUM の保持日数	ADVANCED の保持日数
1	GroomSessionsRetentionDays	MonitorData.Session および	この設定は、セッションの詳	90	31

#	設定名	影響を受けるスキーマテーブル	MONITOR ページで影響を受けるテーブルとグラフ	PREMIUM の保持日数	ADVANCED の保持日数
		Monitordata.Connection テーブル	細、ユーザーセッションごとのログオン時間、トレンドページのアプリケーションベースの使用状況テーブルに影響します。		
2	GroomFailuresRetentionDays	MonitorData.MachineFailureLog および MonitorData.ConnectionFailureLog	トレンドページ: この設定は、障害タブのグラフとテーブルに影響します。	90	31
3	GroomLoadIndexesRetentionDays	MonitorData.LoadIndex	この設定は、トレンドページの「ロードエバリュエーターインデックス」タブに表示されるデータに影響します。	3	3
4	GroomDeletedRetentionDays	LifecycleStateが「Deleted」である MonitorData.Machine、	LifecycleStateが「Deleted」である Machine、Catalog、	90	31

#	設定名	影響を受けるスキーマテーブル	MONITORページで影響を受けるテーブルとグラフ	PREMIUMの保持日数	ADVANCEDの保持日数
		MonitorData.Catalog、MonitorData.DesktopGroup、およびMonitorData.Hypervisorエンティティ。この設定は、関連するSession、SessionDetail、Summary、Failure、またはLoadIndexレコードも削除します。	DesktopGroup、およびHypervisorエンティティ。この設定は、関連するSession、SessionDetail、Summary、Failure、またはLoadIndexレコードも削除します。		
5	GroomSummariesRetentionDays	MonitorData.DesktopGroupSummary、MonitorData.FailureLogSummary、およびMonitorData.LoadIndexSummary	この設定は、トレンドページのすべてのグラフデータに影響します。	365	31
6	GroomMachineHotfixLogRetentionDays	MonitorData.Hotfix	この設定は、マシン詳細ページに表示されるVDAホッ	90	31

#	設定名	影響を受けるスキーマテーブル	MONITORページで影響を受けるテーブルとグラフ	PREMIUMの保持日数	ADVANCEDの保持日数
			トフィックスデータに影響します。		
7	GroomMinuteRetentionDays	すべての概要テーブル	この設定は、トレンドページに表示される「過去2時間」の時間期間のグラフに影響します。	3	3
8	GroomHourlyRetentionDays	すべての概要テーブル	これは、トレンドページに表示される週次グラフに影響します。	32	31
9	GroomApplicationInstanceRetentionDays	MonitorData.ApplicationInstance	この設定は、キャパシティ管理タブのグラフとテーブル、およびトレンドページのアプリケーション使用状況テーブルに影響します。	90	該当なし

#	設定名	影響を受けるスキーマテーブル	MONITORページで影響を受けるテーブルとグラフ	PREMIUMの保持日数	ADVANCEDの保持日数
10	GroomNotificationLogRetentionDays	MonitorData.NotificationLog	この設定は、Monitorに表示されるアラートに影響します。	90	該当なし
11	GroomResourceUsageRawDataRetentionDays	MonitorData.Resourceutilization	この設定は、「履歴マシン使用率」のマシン詳細ページに表示されるCPUおよびメモリのグラフと、コスト最適化領域の「ワークロードの適正化」タブでのデータ計算に影響します。	3	3
12	GroomResourceUsageMinuteDataRetentionDays	MonitorData.ResourceUtilizationSummary	この設定は、「履歴マシン使用率」のマシン詳細ページに表示される「過去2時間」の時間範囲のCPUおよびメモリのグラフと、コスト最適化	7	7

#	設定名	影響を受けるスキーマテーブル	MONITORページで影響を受けるテーブルとグラフ	PREMIUMの保持日数	ADVANCEDの保持日数
			領域の「ワークロードの適正化」タブでのデータ計算に影響します。		
13	GroomResourceUsageHourDataRetentionDays	MonitorData.Resourceutilizationsummary	この設定は、「履歴マシン使用率」のマシン詳細ページに表示されるCPUおよびメモリチャートと、コスト最適化領域の「ワークロードの適正化タブ」でのデータ計算に影響します。	30	30
14	GroomResourceUsageDayDataRetentionDays	MonitorData.Resourceutilizationsummary	この設定は、トレンドページの「リソース使用率」のマシンに表示されるCPUおよびメモリチャートと、特定の「マシン使用率」ペー		

#	設定名	影響を受けるスキーマテーブル	MONITORページで影響を受けるテーブルとグラフ	PREMIUMの保持日数	ADVANCEDの保持日数
			ジに影響します。		
15	GroomProcessUsageRawDataRetentionDays	MonitorData.ProcessUtilization	この設定は、マシンの履歴使用状況ページに表示されるプロセスごとのリソーストレンド情報に影響します。	1	1
16	GroomProcessUsageMinuteDataRetentionDays	MonitorData.ProcessUtilizationMinuteSummary	この設定は、履歴マシン使用率ページに表示される「過去2時間」のプロセスごとのCPUおよびメモリ使用量チャートに影響します。	3	3
17	GroomProcessUsageHourDataRetentionDays	MonitorData.ProcessUtilizationHourSummary	この設定は、マシンの履歴使用状況ページに表示されるプロセスごとのCPUおよびメモリ使用量の	7	7

#	設定名	影響を受けるスキーマテーブル	MONITORページで影響を受けるテーブルとグラフ	PREMIUMの保持日数	ADVANCEDの保持日数
			傾向に影響します。		
18	GroomProcessUsageDayDataRetentionDays	MonitorData.ProcessUtilizationDaySummary	この設定は、マシンの履歴使用状況ページに表示されるプロセスごとのCPUおよびメモリ使用量の傾向に影響します。	30	30
19	GroomSessionMetricsDataRetentionDays	MonitorData.Sessionmetrics	この設定は、ユーザー詳細ページの「セッションパフォーマンス」タブに表示されるすべてのグラフに影響します。	1	1
20	GroomMachineMetricDataRetentionDays	MonitorData.Machinemetrics	この設定は、トレンドページの「リソース使用率」タブにあるグラフとテーブルに影響します。	3	3

#	設定名	影響を受けるスキーマテーブル	MONITOR ページで影響を受けるテーブルとグラフ	PREMIUM の保持日数	ADVANCED の保持日数
21	GroomMachineMetricDaySummaryDataRetentionDays	MonitorData.MachineMetricDaySummary	この設定は、「トレンド」ページの「リソース使用率」タブにあるチャートとテーブルに影響します。	365	31
22	GroomApplicationErrorsRetentionDays	MonitorData.ApplicationError	この設定は、「アプリケーション」ページの「アプリケーションエラー」列に表示されるエラーの詳細に影響します。	1	1
23	GroomApplicationFaultsRetentionDays	MonitorData.Applicationfailure	この設定は、アプリケーションページ上の「アプリケーション障害」列に影響します。	1	1

注意：

> Monitor Serviceデータベースの値を変更した場合、新しい値を有効にするにはサービスを再起動する必要があります。Monitor Serviceデータベースへの変更は、Citrixサポートの指示の下でのみ行うことをお勧めします。

> 設定GroomProcessUsageRawDataRetentionDays、GroomResourceUsageRawDataRetentionDays、およびGroomSessionMetricsDataRetentionDaysは、デフォルト値の1に制限されています。一方、GroomProcessUsageMinuteDataRetentionDaysはデフォルト値の3に制限されています。プロセス使用状況データは急速に増加する傾向があるため、これらの値を設定するPowerShellコマンドは無効になっています。 また、ライセンスベースの保持設定は次のとおりです。

- **Premiumライセンスサイト -** すべての設定のグルーミング保持期間は1000日に制限されています（Citrixは365日を推奨しています）。
- **Advancedライセンスサイト -** すべての設定のグルーミング保持期間は31日に制限されています。
- **その他のすべてのサイト -** すべての設定のグルーミング保持期間は7日に制限されています。

例外：

- GroomApplicationInstanceRetentionDaysは、Premiumライセンスサイトでのみ設定できます。
- GroomApplicationErrorsRetentionDaysおよびGroomApplicationFaultsRetentionDaysは、Premiumライセンスサイトでは31日に制限されています。

長期間データを保持すると、テーブルサイズに以下の影響があります:

- **時間単位のデータ。** 時間単位のデータがデータベースに最大2年間保持される場合、1000のデリバリーグループを持つサイトでは、データベースが次のように増大する可能性があります。

  1000のデリバリーグループ x 24時間/日 x 365日/年 x 2年 = 17,520,000行のデータ。集計テーブル内のこれほど大量のデータがパフォーマンスに与える影響は甚大です。ダッシュボードのデータはこのテーブルから取得されるため、データベースサーバーへの要件は大きくなる可能性があります。過度に大量のデータは、パフォーマンスに劇的な影響を与える可能性があります。

- **セッションおよびイベントデータ。** セッションが開始され、接続/再接続が行われるたびに収集されるデータです。大規模なサイト（10万ユーザー）の場合、このデータは急速に増加します。たとえば、これらのテーブルの2年分のデータは1TBを超える量になり、ハイエンドのエンタープライズレベルのデータベースが必要になります。

Citrix Directorの障害理由とトラブルシューティング

以下の表は、さまざまな障害カテゴリ、その理由、および問題を解決するために必要なアクションについて説明しています。詳細については、「列挙型、エラーコード、および説明」を参照してください。

接続障害エラー

カテゴリ	理由	問題	アクション
該当なし	[0] 不明。このエラーコードはマッピングされていません。	監視サービスは、ブローカリングサービスから共有された情報から、報告された起動または接続障害の理由を判断できません。	コントローラでCDFログを収集し、Citrixサポートに連絡してください。
[0] なし	[1] なし	なし	該当なし
[2] MachineFailure	[2] SessionPreparation	デリバリーコントローラーからVDAへのセッション準備要求が失敗しました。考えられる原因：コントローラーとVDA間の通信の問題、Broker Serviceが準備要求を作成する際に発生した問題、またはVDAが要求を受け入れない原因となるネットワークの問題です。	コントローラーとVDA間の通信の問題を引き起こす一般的な問題については、ナレッジセンターの記事「Citrix Virtual Apps and Desktopsにおけるデリバリーコントローラーへの Virtual Delivery Agent登録のトラブルシューティング」に記載されているトラブルシューティング手順を参照してください。
[2] MachineFailure	[3] RegistrationTimeout	VDAは電源が入っていましたが、デリバリーコントローラーへの登録を試行中にタイムアウトが発生しました。	デリバリーコントローラーでCitrix Broker Serviceが実行されていること、およびVDAでDesktop Serviceが実

カテゴリ	理由	問題	アクション
			行されていることを確認してください。停止している場合は、それぞれを開始してください。
[1] ClientConnectionFailure	[4] ConnectionTimeout	セッション起動のためにVDAが準備された後、クライアントはVDAに接続しませんでした。セッションは正常に仲介されましたが、クライアントがVDAに接続するのを待っている間にタイムアウトが発生しました。考えられる原因：ファイアウォールの設定、ネットワークの中断、またはリモート接続を妨げる設定です。	Directorコンソールで、クライアントが現在アクティブな接続を持っているかどうかを確認してください。これは、ユーザーに影響がないことを意味します。セッションが存在しない場合は、クライアントとVDAのイベントログでエラーがないか確認してください。クライアントとVDA間のネットワーク接続に関する問題を解決してください。
[4] NoLicensesAvailable	[5] ライセンス	ライセンス要求が失敗しました。考えられる原因：ライセンス数が不足しているか、ライセンスサーバーが30日以上ダウンしていることです。	ライセンスサーバーがオンラインで到達可能であることを確認します。ライセンスサーバーへのネットワーク接続の問題を解決するか、ライセンスサーバーが誤動作しているように見える場合は再起動します。環境内に十分なライセンスがあることを確認し、必要に応じて追加で割り当てます。

カテゴリ	理由	問題	アクション
[1] ClientConnectionFailure	[6] チケッティング	チケッティング中にエラーが発生しました。これは、VDAへのクライアント接続が仲介された要求と一致しないことを示しています。起動要求チケットはブローカーによって準備され、ICA®ファイルで配信されます。ユーザーがセッションを起動しようとすると、VDAはICAファイル内の起動チケットをブローカーと照合して検証します。考えられる原因：ICAファイルが破損しているか、ユーザーが不正な接続を試みている。	デリバリーグループで定義されたユーザーグループに基づいて、ユーザーがアプリケーションまたはデスクトップにアクセスできることを確認します。ユーザーにアプリケーションまたはデスクトップを再起動するよう指示し、これが一時的な問題であるかどうかを判断します。問題が再発する場合は、クライアントデバイスのイベントログでエラーを確認します。ユーザーが接続しようとしているVDAが登録されていることを確認します。登録されていない場合は、VDAのイベントログを確認し、登録に関する問題を解決します。
[1] ClientConnectionFailure	[7] その他	クライアントが最初にVDAに接続した後、接続シーケンスが完了する前に、セッションがVDAから終了したと報告されました。	起動前にユーザーによってセッションが終了されなかったことを確認します。セッションを再起動してみてください。問題が解決しない場合は、CDFログを収集し、Citrixサポートに連絡してください。

カテゴリ	理由	問題	アクション
[1] ClientConnectionFailure	[8] GeneralFail	セッションの起動に失敗しました。考えられる原因：ブローカーがまだ起動中または初期化中に仲介された起動が要求された、または起動の仲介フェーズ中に内部エラーが発生した。	Citrix Broker Serviceが実行中であることを確認し、セッションの起動を再試行します。
[5] 構成	[9] MaintenanceMode	VDA、またはVDAが属するデリバリーグループがメンテナンスモードに設定されています。	メンテナンスモードが必要かどうかを判断します。不要な場合は、該当するデリバリーグループまたはマシンでメンテナンスモードを無効にし、ユーザーに再接続を試みるよう指示します。
[5] 構成	[10] アプリケーション無効	アプリケーションは管理者によって無効にされているため、エンドユーザーはアクセスできません。	アプリケーションが本番環境で使用されることを意図している場合は、アプリケーションを有効にし、ユーザーに再接続するよう指示します。
[4] ライセンスなし	[11] ライセンス機能拒否	使用されている機能は、既存のライセンスではカバーされていません。	既存のCitrix Virtual Apps and Desktops™ライセンスのエディションとタイプでカバーされている機能を確認するには、Citrixの営業担当者にお問い合わせください。

カテゴリ	理由	問題	アクション
[3] 容量なし	[13] セッション制限に到達	すべてのVDAが使用中であり、これ以上セッションをホストする容量がありません。考えられる原因：すべてのVDAが使用中である（シングルセッションOS VDAの場合）、またはすべてのVDAが設定された最大同時セッション数に達している（マルチセッションOS VDAの場合）。	メンテナンスモードのVDAがないか確認します。容量を増やすために不要な場合は、メンテナンスモードを無効にします。Citrixポリシー設定の**最大セッション数**の値を増やして、サーバーVDAあたりのセッション数を増やすことを検討してください。マルチセッションOS VDAを追加することを検討してください。シングルセッションOS VDAを追加することを検討してください。
[5] 構成	[14] 許可されていないプロトコル	ICAプロトコルとRDPプロトコルは許可されていません。	デリバリーコントローラーで**Get-BrokerAccessPolicyRule** PowerShellコマンドを実行し、**AllowedProtocols**の値に目的のプロトコルがすべてリストされていることを確認します。この問題は、構成が誤っている場合にのみ発生します。
[5] 構成	[15] リソースが利用できません	ユーザーが接続しようとしているアプリケーションまたはデスクトップは利用できません。このアプリケーションまたは	アプリケーションまたはデスクトップがまだ公開されており、VDAがメンテナンスモードになっていないことを確認し

カテゴリ	理由	問題	アクション
		デスクトップが存在しないか、それを実行できるVDAがありません。考えられる原因：アプリケーションまたはデスクトップが非公開になっているか、アプリケーションまたはデスクトップをホストしているVDAが最大負荷に達しているか、アプリケーションまたはデスクトップがメンテナンスモードに設定されています。	ます。マルチセッションOS VDAが最大負荷に達しているかどうかを判断します。その場合は、さらにマルチセッションOS VDAをプロビジョニングします。接続に利用できるシングルセッションOS VDAがあることを確認します。必要に応じて、さらにシングルセッションOS VDAをプロビジョニングします。
[5] 構成	[16] アクティブセッションの再接続が無効	ICAセッションはアクティブで、別のエンドポイントに接続されています。ただし、**アクティブセッションの再接続**が無効になっているため、クライアントはアクティブセッションに接続できません。	デリバリーコントローラーで、**アクティブセッションの再接続**が有効になっていることを確認します。レジストリの**HKEY_LOCAL_MACHINE\Software\Citrix\Desktop\Server**にある**DisableActiveSessionReconnect**の値が0に設定されていることを確認します。
[2] マシンの障害	[17] 再接続するセッションがありません	クライアントは特定のセッションに再接続しようとしましたが、セッションは終了しました。	ワークスペースコントロールの再接続を再試行してください。
[2] MachineFailure	[18] SpinUpFailed	VDAをセッション起動のために電源オン	マシンがまだ電源オフの状態である場合

カテゴリ	理由	問題	アクション
		にできません。これはハイパーバイザーが報告した問題です。	は、Citrix Studioからマシンの起動を試行してください。これが失敗した場合は、ハイパーバイザーの接続と権限を確認してください。VDAがPVSプロビジョニングされたマシンの場合は、PVSコンソールでマシンが実行中であることを確認してください。そうでない場合は、マシンにPersonal vDiskが割り当てられていることを確認し、ハイパーバイザーにログインしてVMをリセットしてください。
[2] MachineFailure	[19] 拒否	デリバリーコントローラーは、エンドユーザーからの接続に備えるようVDAに要求を送信しますが、VDAはこの要求を積極的に拒否します。	pingを使用して、デリバリーコントローラーとVDAが正常に通信できることを確認してください。通信できない場合は、ファイアウォールまたはネットワークルーティングの問題を解決してください。
[2] MachineFailure	[20] 構成セットの失敗	デリバリーコントローラーは、セッション起動中にポリシー設定やセッション情報などの必要な構成データをVDAに送信しませんでし	-

カテゴリ	理由	問題	アクション
		た。考えられる原因：コントローラーとVDA間の通信の問題、構成セット要求の作成中にブローカーサービスで発生した問題、またはVDAが要求を受け入れない原因となるネットワークの問題。	
[3] NoCapacityAvailable	[21] MaxTotalInstancesExceeded	アプリケーションのインスタンスの最大数に達しました。VDA上でアプリケーションの追加インスタンスを開くことはできません。この問題は、アプリケーション制限機能に関連しています。	ライセンスが許す範囲で、アプリケーション設定の「**同時に実行するインスタンスの数を制限する**」をより高い値に増やすことを検討してください。
[3] NoCapacityAvailable	[22] MaxPerUserInstancesExceeded	ユーザーがアプリケーションの複数のインスタンスを開こうとしていますが、アプリケーションはユーザーごとに1つのインスタンスのみを許可するように構成されています。この問題は、アプリケーション制限機能に関連しています。	デフォルトでは、ユーザーごとにアプリケーションのインスタンスは1つのみ許可されています。ユーザーごとに複数のインスタンスが必要な場合は、アプリケーション設定で「**ユーザーごとに1つのインスタンスに制限する**」設定をクリアすることを検討してください。
[1] ClientConnectionFailure	[23] 通信エラー	デリバリーコントローラーは、接続の準備を要求するなど	既に開始されている場合は、VDA上のデスクトップサービス

カテゴリ	理由	問題	アクション
		の情報をVDAに送信しようとしましたが、通信中にエラーが発生しました。これはネットワーク障害が原因である可能性があります。	を再起動して登録プロセスを再開し、VDAが正常に登録されることを確認します。アプリケーションイベントログの詳細を通じて、VDA用に構成されたデリバリーコントローラーが正確であることを確認します。
[3] NoCapacityAvailable	[100] NoMachineAvailable 監視サービスは [12] NoDesktopAvailable をこのエラーコードに変換します。	セッションの起動に割り当てられたVDAが無効な状態であるか、利用できません。考えられる原因：VDAの電源状態が不明または利用できない、VDAが前回のユーザーセッション以降に再起動されていない、現在のセッションで有効にする必要があるにもかかわらずセッション共有が無効になっている、またはVDAがデリバリーグループまたはサイトから削除された。	VDAがデリバリーグループに含まれていることを確認します。含まれていない場合は、適切なデリバリーグループに追加します。ユーザーが要求した公開共有デスクトップまたはアプリケーションを起動できるように、十分なVDAが登録され、準備状態にあることを確認します。VDAをホストしているハイパーバイザーがメンテナンスモードではないことを確認します。
[2] MachineFailure	[101] MachineNotFunctional. 監視サービスは [12] NoDesktopAvailable をこのエラーコードに変換します。	VDA は稼働していません。考えられる原因: VDA がデリバリーグループから削除された、VDA が登録解除されている、VDA の電源状態が利用できない、または	VDA がデリバリーグループ内にあることを確認します。そうでない場合は、適切なデリバリーグループに追加します。Citrix Studio で VDA が電源オンとして表示されていることを

カテゴリ	理由	問題	アクション
		VDA が内部的な問題を抱えている。	確認します。複数のマシンの電源状態が不明な場合は、ハイパーバイザーへの接続またはホスト障害に関する問題を解決します。VDA をホストしているハイパーバイザーがメンテナンスモードではないことを確認します。これらの問題が解決されたら、VDA を再起動します。

マシン障害の種類

エラーコード	エラーコードID	問題	アクション
不明	-	-	-
未登録	3	-	-
MaxCapacity (Director上では最大負荷として表示されます)	4	マシンは、最大容量に達している、つまり最大負荷インデックスに達していると報告しています。	すべてのハイパーバイザーが電源オンになっていることを確認してください。ハイパーバイザーの容量を増やすか、またはハイパーバイザーを追加することによって、影響を受けるデリバリーグループにマシンを追加してください。
StuckOnBoot	2	VMが起動シーケンスを完了せず、ハイパーバイザーと通信していません。	VMがハイパーバイザー上で正常に起動したことを確認してください。OSの問題など、VM上の他の

エラーコード	エラーコードID	問題	アクション
			メッセージを確認してください。ハイパーバイザーツールがVMにインストールされていることを確認してください。VDAがVMにインストールされていることを確認してください。
FailedToStart	1	ハイパーバイザー上で起動しようとしたときに、VMで問題が発生しました。	ハイパーバイザーのログを確認してください。
なし	0	-	-

マシンの登録解除理由 (障害の種類が「未登録」または「不明」の場合に適用)

エラーコード	エラーコードID	問題	処置
AgentShutdown	0	VDAで正常なシャットダウンが発生しました。	既存の電源管理ポリシーに基づいてVDAがオフになっていることが想定されない場合は、VDAの電源をオンにします。イベントログでエラーを確認します。
AgentSuspended	1	VDAは休止状態またはスリープモードです。	VDAを休止状態から復帰させます。電源設定を介してCitrix Virtual Apps and Desktops VDAの休止状態を無効にすることを検討してください。

エラーコード	エラーコードID	問題	処置
IncompatibleVersion	100	Citrixプロトコルバージョンの不一致により、VDAがデリバリーコントローラーと通信できません。	VDAとデリバリーコントローラーのバージョンを合わせます。
AgentAddressResolutionFailed	101	デリバリーコントローラーがVDAのIPアドレスを解決できませんでした。	VDAマシンアカウントがADに存在することを確認します。存在しない場合は作成します。DNS内のVDAの名前とIPアドレスが正確であることを確認します。正確でない場合は修正します。広範囲にわたる場合は、デリバリーコントローラーのDNS設定を検証します。コントローラーから`nslookup`コマンドを実行してDNS解決を確認します。
[Cloud]:AgentAddressResolutionFailed	101	デリバリーコントローラーがVDAのIPアドレスを解決できませんでした。	VDAマシンアカウントがADに存在することを確認します。存在しない場合は作成します。DNS内のVDAの名前とIPアドレスが正確であることを確認します。正確でない場合は修正します。
AgentNotContactable	102	デリバリーコントローラーとVDA間で通信の問題が発生しました。	pingを使用して、デリバリーコントローラーとVDAが正常に通信できることを確認します。通信でき

エラーコード	エラーコードID	問題	処置
			ない場合は、ファイアウォールまたはネットワークの問題を解決します。コントローラーとVDA間の通信問題を引き起こす一般的な問題については、Knowledge Centerの記事「Troubleshooting Virtual Delivery Agent Registration with delivery controllers in Citrix Virtual Apps and Desktops (CTX136668)」に記載されているトラブルシューティング手順を参照してください。
[Cloud]: AgentNotContactable	102	デリバリーコントローラーとVDA間で通信の問題が発生しました。	コントローラーとVDA間の通信問題を引き起こす一般的な問題については、知識センターの記事「Troubleshooting Virtual Delivery Agent Registration with delivery controllers in Citrix Virtual Apps and Desktops (CTX136668)」に記載されているトラブルシューティング手順を参照してください。Citrixサポートに

エラーコード	エラーコードID	問題	処置
			お問い合わせください。
AgentWrongActiveDirectoryOU	103	Active Directoryの検出設定が誤っています。VDAレジストリに構成されているサイト固有のOU (サイトコントローラー情報がADに保存されている場所) が、別のサイト用です。	Active Directoryの構成が正しいことを確認するか、レジストリ設定を確認してください。
EmptyRegistrationRequest	104	VDAからデリバリーコントローラーに送信された登録要求が空でした。これは、VDAソフトウェアのインストールが破損していることが原因である可能性があります。	VDA上のDesktopサービスを再起動して登録プロセスを再開し、アプリケーションイベントログを介してVDAが正しく登録されていることを確認してください。
MissingRegistrationCapabilities	105	VDAのバージョンがデリバリーコントローラーと互換性がありません。	VDAをアップグレードするか、VDAを削除してから再インストールします。
MissingAgentVersion	106	VDAのバージョンがデリバリーコントローラーと互換性がありません。	問題がすべてのマシンに影響している場合は、VDAソフトウェアを再インストールします。
InconsistentRegistrationCapabilities	107	VDAは、その機能をブローカーに通信できません。これは、VDAとデリバリーコントローラーのバージョン間の非互換性が原因である可能性があります。バー	VDAとデリバリーコントローラーのバージョンを合わせます。

エラーコード	エラーコードID	問題	処置
		ジョンごとに変更される登録機能は、登録要求と一致しない形式で表現されています。	
NotLicensedForFeature	108	使用しようとしている機能はライセンスされていません。	Citrixライセンスエディションを確認するか、VDAを削除してから再インストールします。
[Cloud]: NotLicensedForFeature	108	使用しようとしている機能はライセンスされていません。	Citrixサポートにお問い合わせください。
サポートされていないCredentialSecurityバージョン	109	VDAとデリバリーコントローラーが同じ暗号化メカニズムを使用していません。	VDAとデリバリーコントローラーのバージョンを合わせてください。
無効な登録要求	110	VDAがBrokerに登録要求を行いましたが、要求の内容が破損しているか無効です。	コントローラーとVDA間の通信問題を引き起こす一般的な問題については、Knowledge Centerの記事「Troubleshooting Virtual Delivery Agent Registration with delivery controllers in Citrix Virtual Apps and Desktops (CTX136668)」に記載されているトラブルシューティング手順を参照してください。

エラーコード	エラーコードID	問題	処置
シングル/マルチセッションの不一致	111	VDAのオペレーティングシステムタイプは、マシンカタログまたはデリバリーグループと互換性がありません。	VDAを、同じオペレーティングシステムを持つマシンを含む正しいマシンカタログタイプまたはデリバリーグループに追加してください。
カタログに対して機能レベルが低すぎます	112	マシンカタログが、インストールされているVDAバージョンよりも高いVDA機能レベルに設定されています。	VDAのマシンカタログ機能レベルがVDAの機能レベルと一致していることを確認します。VDAの機能レベルと一致するようにマシンカタログをアップグレードまたはダウングレードします。
FunctionalLevelTooLowForDesktopGroup	113	デリバリーグループが、インストールされているVDAバージョンよりも高いVDA機能レベルに設定されています。	VDAのデリバリーグループ機能レベルがVDAの機能レベルと一致していることを確認します。VDAの機能レベルと一致するようにマシンカタログをアップグレードまたはダウングレードします。
PowerOff	200	VDAが正常にシャットダウンされませんでした。	VDAが電源オン状態であるべき場合は、Citrix StudioからVDAの起動を試み、正しく起動して登録されることを確認します。起動または登録に関する問題をトラブルシューティングします。VDAが再び稼働したら、イベン

エラーコード	エラーコードID	問題	処置
			トログを確認してシャットダウンの根本原因を特定するのに役立てます。
AgentRejectedSettingsUpdate	203	Citrixポリシーなどの設定が変更または更新されましたが、VDAへの更新の送信中にエラーが発生しました。これは、更新がインストールされているVDAバージョンと互換性がない場合に発生する可能性があります。	必要に応じてVDAをアップグレードします。適用された更新がVDAバージョンでサポートされているかどうかを確認します。
SessionPrepareFailure	206	ブローカーがVDAで実行されているセッションの監査を完了しませんでした。	広範囲にわたる場合は、デリバリーコントローラーでCitrix Broker Serviceを再起動してください。
[Cloud]: SessionPrepareFailure	206	ブローカーがVDAで実行されているセッションの監査を完了しませんでした。	Citrixサポートにお問い合わせください。
ContactLost	207	デリバリーコントローラーがVDAとの接続を失いました。これはネットワーク障害が原因である可能性があります。	デリバリーコントローラーでCitrix Broker Serviceが実行されており、VDAでDesktop Serviceが実行されていることを確認します。停止している場合はそれぞれを起動します。すでに起動している場合は、VDAでDesktop Serviceを再起動して登録プロセ

エラーコード	エラーコードID	問題	処置
			スを再開し、VDAが正常に登録されることを確認します。アプリケーションイベントログの詳細を通じて、VDA用に構成されているデリバリーコントローラーが正確であることを確認します。pingを使用して、デリバリーコントローラーとVDAが正常に通信できることを確認します。通信できない場合は、ファイアウォールまたはネットワークの問題を解決してください。
[Cloud]: ContactLost	207	デリバリーコントローラーがVDAとの接続を失いました。これはネットワーク障害が原因である可能性があります。	VDA上でDesktopサービスが実行されていることを確認します。停止している場合は開始します。
BrokerRegistrationLimitReached	301	デリバリーコントローラーは、同時に登録できるVDAの構成済み最大数に達しました。デフォルトでは、デリバリーコントローラーは10,000の同時VDA登録を許可します。	サイトにデリバリーコントローラーを追加するか、サイトを作成することを検討してください。また、**HKEY_LOCAL_MACHINE\Software\Citrix\DesktopServer\MaxWorkers** レジストリキーを介して、デリバリーコントローラーに同時に登録できるVDAの数を

エラーコード	エラーコードID	問題	処置
			増やすこともできます。詳細については、ナレッジセンターの記事「Registry Key Entries Used by Citrix Virtual Apps and Desktops (CTX117446)」を参照してください。この数を増やすと、コントローラーにより多くのCPUおよびメモリリソースが必要になる場合があります。
SettingsCreationFailure	208	ブローカーは、VDAに送信する設定と構成のセットを構築しませんでした。ブローカーがデータを収集できない場合、登録は失敗し、VDAは登録解除されます。	デリバリーコントローラーのイベントログでエラーがないか確認してください。ログに特定の問題が明らかでない場合は、Broker Serviceを再起動してください。Broker Serviceが再起動されたら、影響を受けるVDAでDesktopサービスを再起動し、正常に登録されることを確認してください。
[Cloud]: SettingsCreationFailure	208	ブローカーは、VDAに送信する設定と構成のセットを構築しませんでした。ブローカーがデータを収集できない場合、登録は失敗し、VDA	影響を受けるVDAでDesktopサービスを再起動し、正常に登録されることを確認してください。Citrixサポートに連絡してください。

エラーコード	エラーコードID	問題	処置
		は登録解除されます。	
SendSettingsFailure	204	BrokerがVDAに設定と構成データを送信しませんでした。Brokerがデータを収集できても送信できない場合、登録は失敗します。	単一のVDAに限定される場合は、VDA上のDesktopサービスを再起動して再登録を強制し、アプリケーションイベントログを介してVDAが正常に登録されることを確認します。表示されたエラーをトラブルシューティングします。コントローラーとVDA間の通信問題を引き起こす一般的な問題については、ナレッジセンターの記事「Citrix Virtual Apps and Desktopsにおけるデリバリーコントローラーとの Virtual Delivery Agent登録のトラブルシューティング (CTX136668)」に記載されているトラブルシューティング手順を参照してください。
AgentRequested	2	不明なエラーが発生しました。	Citrixサポートにお問い合わせください。
DesktopRestart	201	不明なエラーが発生しました。	Citrixサポートにお問い合わせください。
DesktopRemoved	202	不明なエラーが発生しました。	Citrixサポートにお問い合わせください。

エラーコード	エラーコードID	問題	処置
SessionAuditFailure	205	不明なエラーが発生しました。	Citrixサポートにお問い合わせください。
UnknownError	300	不明なエラーが発生しました。	Citrixサポートにお問い合わせください。
RegistrationStateMismatch	302	不明なエラーが発生しました。	Citrixサポートにお問い合わせください。
不明	-	不明なエラーが発生しました。	Citrixサポートにお問い合わせください。

Secure Private AccessとDirectorの統合（プレビュー）

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

利用可能なアクションには、以下の詳細の表示が含まれます。

- **セッションの選択**ポップアップ > **セッション**タブ > **Web SaaSおよびクライアント/サーバーアプリ**の下にあるユーザーのSecure Private Accessアクティブセッション
- **セッションの選択**ポップアップ > **アクセス拒否**タブの下にあるSecure Private Accessの失敗またはブロックされた列挙、および失敗したアプリ起動
- アクティブおよび失敗したアプリ起動のセッションとアプリケーションの詳細表示
- 失敗およびブロックされた列挙のセッションとアプリケーションの詳細表示

> **注：**
>
> Secure Private AccessとDirectorの統合は、Directorのフォームベース認証のみがサポートされており、統合Windows認証またはスマートカードベース認証はサポートされていません。

前提条件

1. この機能をサポートするには、以下を使用する必要があります。

- Director 2402以降のバージョン
- Secure Private Access 2402以降のバージョン
- Citrix Workspace app 2402以降のバージョン

2. 少なくとも1つのCitrix Virtual Apps and Desktops™サイトがDirectorに構成されていることを確認してください。
3. Secure Private Access を設定する。
4. Director サーバーが Secure Private Access サーバーへのネットワーク接続を持っていることを確認してください。

> **注:**
>
> Citrix Director への接続を正常に確立するには、信頼された証明書が Secure Private Access サーバーにインストールされている必要があります。

5. Director 管理者ユーザーが次の権限を持っていることを確認します。
   a. Secure Private Access 管理コンソールで Secure Private Access のフル管理者または読み取り専用管理者。
   b. Citrix Studio コンソールで Citrix Virtual Apps™ または Desktops のヘルプデスク、フル管理者、または読み取り専用管理者。

Director を Secure Private Access で構成する

1. Director がインストールされているマシンで、管理者としてコマンドプロンプトを開きます。
2. 次のコマンドを実行して、`DirectorConfig` ツールのパスに移動します。

```
cd c:\inetpub\wwwroot\Director\tools
```

3. Secure Private Access を構成するには、次のコマンドを実行します。

```
DirectorConfig.exe /configspa
```

4. Secure Private Access がインストールされているマシンの FQDN とポート番号を入力します。

5. Secure Private Access (サーバーまたはロードバランサー) への接続が安全であり、信頼された証明書が適用されていることを確認してください。

```
PS C:\inetpub\wwwroot\Director\tools> .\DirectorConfig.exe /configspa

 Make sure the SPA server or load balancer is reachable from this Director machine
 Enter SPA server or load balancer FQDN including port [https://spa-server.mydomain.com:4[redacted]3] : https://[redacted]

 Checking connectivity to https://spa1.gwonprem.corp[redacted]

 Spa Server or load balancer: https://[redacted] is reachable.

 Checking Spa Server or load balancer is valid

 Retry with correct Spa Server FQDN which is reachable

 Director configuration encountered an error


=====================================================
Spa Server or load balancer FQDN https://[redacted] is either invalid or Spa server/load balancer is down
=====================================================
```

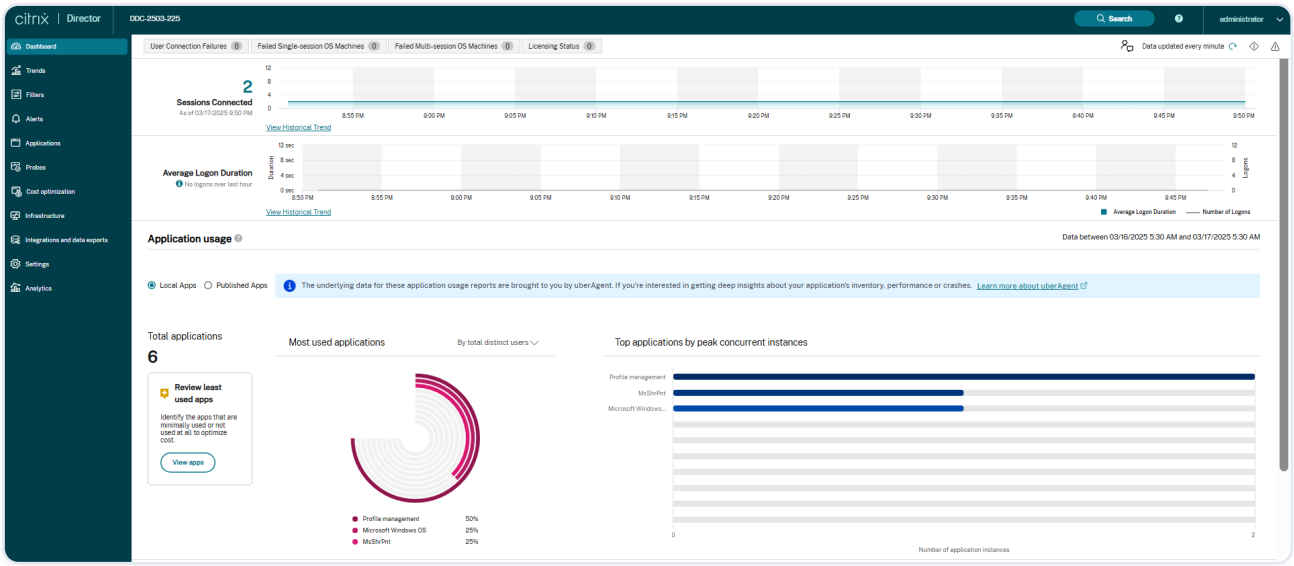
注:

DirectorでSecure Private Accessセッションの詳細を表示するには、管理者をSecure Private Accessコンソールに追加する必要があります。詳細については、「管理者の管理」を参照してください。

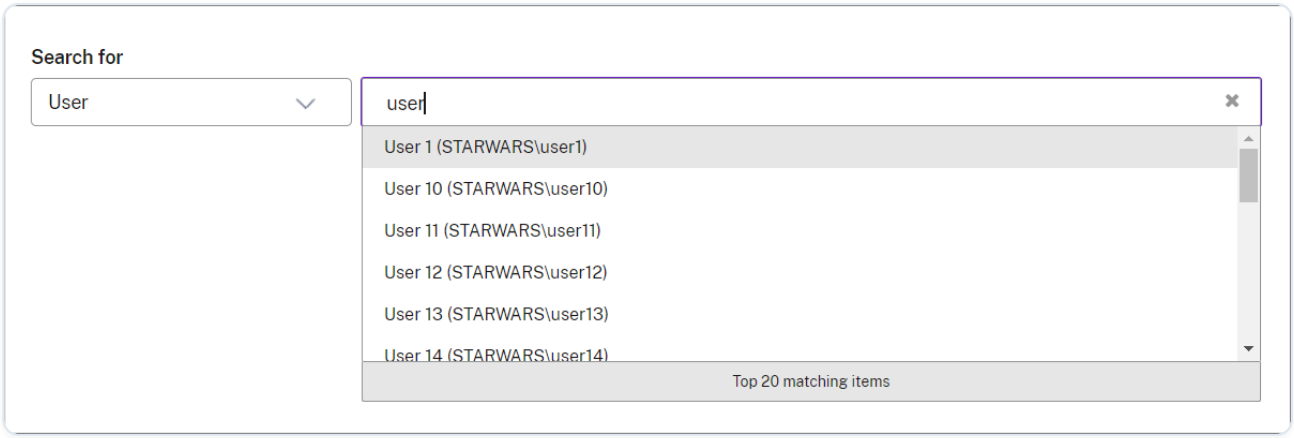
ユーザー別のSecure Private Accessセッションの表示

Directorダッシュボードで、**［検索］をクリックし、ユーザー名を入力します。**［セッションの選択］**画面が表示されます。

フル管理者：



ヘルプデスク管理者：



Secure Private AccessセッションのActivity Managerを表示する

Citrix Directorは、Secure Private AccessセッションのActivity Managerビューを提供し、セッションアクティビティの全体像を把握できます。Activity Managerは、正常に開かれた、開かれなかったすべてのアプリとデスクトップ、およびSecure Private Accessアプリで設定されたポリシーの結果を包括的に表示します。この機能は、Citrix Virtual Apps and Desktopsバージョン2407以降で利用できます。

前提条件：

- Director 2407以降のバージョン
- Secure Private Access 2407以降のバージョン

Activity Managerには、**［利用可能なアプリ］と［起動されたアプリ］**の詳細が表示されます。次のセッションの詳細を確認できます。

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

Activity Managerを表示するには、次の手順を実行します。

1. Director ダッシュボードで、**「検索」をクリックし、ユーザー名を入力します。**「セッションの選択」**画面が表示されます。

2. Secure Private Accessセッションを使用して開かれたセッションを選択します。選択したセッションのアクティビティマネージャーが表示されます。

   アクティビティマネージャー(/en-us/citrix-virtual-apps-desktops/2503/media/spa-activity-manager.png)
3. Citrix Workspaceアプリで利用可能なアプリを表示するには、**利用可能なアプリ**をクリックします。

または、,

Citrix Workspaceアプリで開かれているアプリを表示するには、**起動されたアプリ（セッション）**をクリックします。

Secure Private Accessアプリで設定されたリソースのステータスでリソースをフィルタリングできます。

- Allow - ユーザーがアクセスを許可されているリソース。このステータスは、Secure Private Accessアプリのポリシーを使用して設定されます。このリソースは、Citrix Workspaceアプリでユーザーに表示されます。
- Deny - ユーザーがアクセスを拒否されているリソース。このステータスは、Secure Private Accessアプリのポリシーを使用して設定されます。このリソースは、Citrix Workspaceアプリでユーザーに表示されます。
- Error - Secure Private Accessアプリでユーザーがアクセスを許可されているリソース。ただし、何らかのエラーにより、リソースがCitrix Workspaceアプリで利用できません。列挙エラーとセッションエラーの2種類のエラーがあります。

利用可能なアプリを表示

Citrix Workspaceアプリで利用可能なWebおよびSaaSアプリは、「**利用可能なアプリ**」セクションに表示されます。このセクションには、アプリの最後の列挙試行と、その列挙試行のステータスが表示されます。

次の詳細を表示できます。

- リソース名
- ステータス
- トランザクションID

「**許可**」、「**拒否**」、「**エラー**」などのアプリケーションステータスで、上記の詳細をフィルタリングすることもできます。上下矢印を使用して詳細を並べ替えることもできます。

> **注:**
>
> TCP/UDPアプリは、「**利用可能なアプリ**」セクションには表示されません。

起動されたアプリを表示

Citrix Workspaceアプリで開かれたアプリは、「**起動されたアプリ（セッション）**」セクションに表示されます。次の詳細を表示できます。

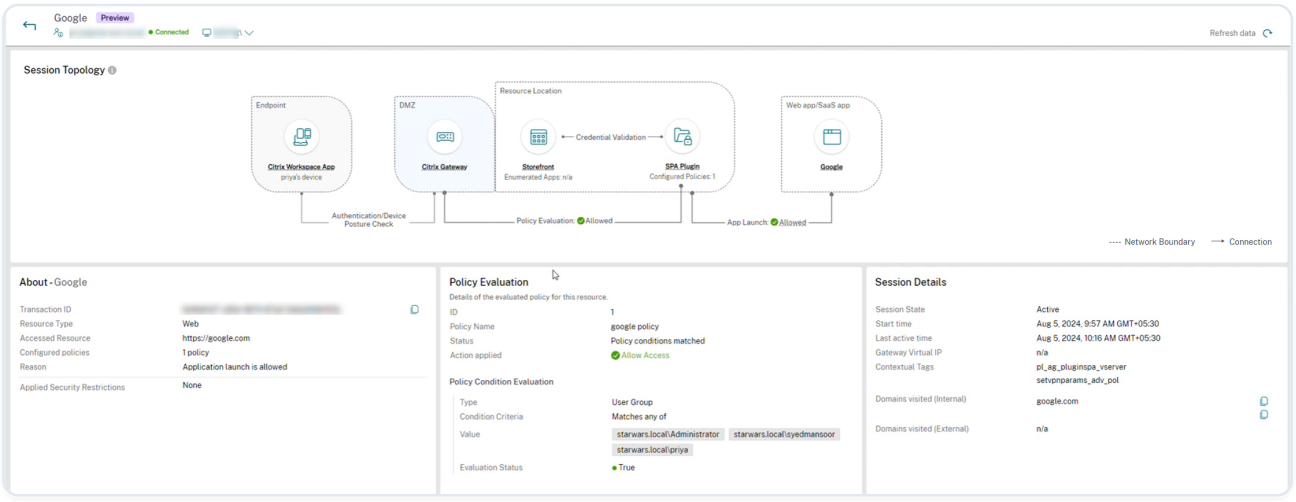
- 起動時間
- リソース名
- リソースの種類
- アクセスされたリソース
- ステータス
- トランザクションID

上記の詳細は、**許可**、**拒否**、**エラー**などのアプリケーションステータスでフィルタリングすることもできます。上下の矢印を使用して詳細を並べ替えることもできます。

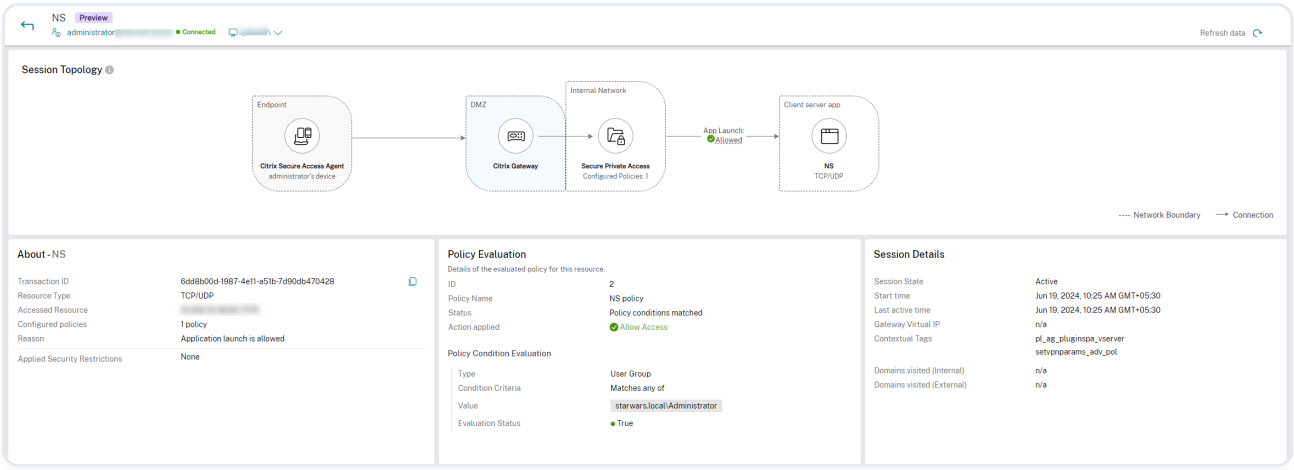
Secure Private Access アプリのセッショントポロジビュー

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

Web/SaaS アプリ:



TCP/UDP アプリ:



セッショントポロジビューは、アプリ起動プロセスのフローを提供します。エンドポイントは Citrix Gateway に接続し、Citrix Gateway は Secure Private Access プラグインに接続します。Secure Private Access プラグインからの情報を使用して、アプリが起動されます。この機能は、Citrix Virtual Apps and Desktops バージョン 2407 以降で利用できます。

前提条件:

- Director 2407 以降のバージョン
- Secure Private Access 2407 以降のバージョン
- Citrix Secure Access 24.8.1.x 以降のバージョン

以下を表示できます。

- エンドポイント - アプリが開かれたエンドポイントを表示します。可能なオプションは Citrix Workspace アプリと Citrix Secure Agent です。デバイス ID が表示されます。
- 内部ネットワーク - 列挙されたアプリの数と構成されたポリシーの数を表示します。
- ポリシー評価 - Secure Private Accessアプリに設定されているポリシーの結果を表示します。値は、**許可**、**拒否**、**制限付きアクセス許可**、**エラー**です。これはWebアプリまたはSaaSアプリにのみ適用されます。
- アプリ起動 - アプリの種類とアプリ起動のステータスを表示します。アプリの種類として考えられる値は、Web/SaaSアプリまたはTCP/UDPアプリです。同様に、アプリ起動ステータスとして考えられる値は、**許可**、**拒否**、**制限付きアクセス許可**、**エラー**です。

セキュアプライベートアクセスアプリの**セッショントポロジ**ビューで、以下の追加の詳細を表示できるようになりました。この変更は、TCP/UDPアプリに加えて、WebアプリとSaaSアプリの両方に適用されます。

セッショントポロジSPA(/en-us/citrix-virtual-apps-desktops/2503/media/session-topology-spa-tcp.png)

エンドポイント:

エンドポイント内のリンクをクリックすると、以下が表示されます。

- **エンドポイントの種類:** これはSecure Access AgentまたはCitrix Workspaceアプリのいずれかです。
- **アクセス詳細:** エンドポイントがStoreFront™またはCitrix Workspaceアプリのどちらを介してアクセスされるかを表示します。
- **エンドポイントOS:** 例: Windows。
- **場所の種類:** 場所が内部か外部かを示します。

リソースの場所:

リソースの場所内のリンクをクリックすると、以下が表示されます。

> **注:** これは、Web アプリと SaaS アプリにのみ適用されます。

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

セキュア プライベート アクセス:

- **構成済みポリシー:** 構成済みポリシーの数を表示します。
- **FQDNプラグイン:** 要求を処理したエージェントのFQDNを表示します。

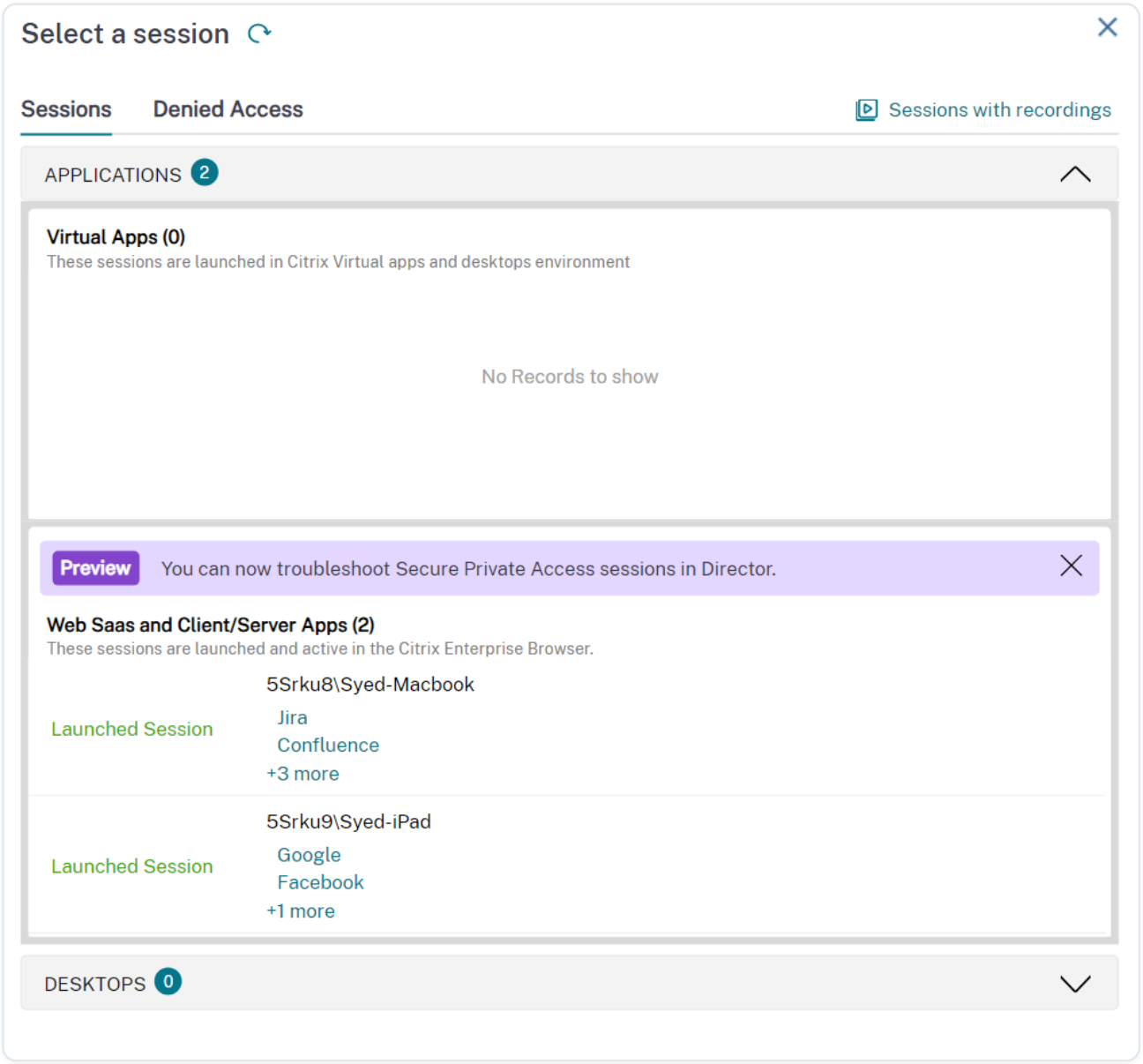
WebおよびSaaSアプリ / クライアントサーバーアプリ (TCP/UDP):

WebおよびSaaSアプリ / クライアントサーバーアプリ内のリンクをクリックして、以下を表示します。

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

正常に起動されたWebアプリとSaaSアプリを表示する

正常に起動されたアプリは、「**Web SaaSおよびクライアント/サーバーアプリ**」セクションに表示されます。



Web SaaSおよびクライアント/サーバーアプリセクションからアプリをクリックして詳細を表示します。

「Director SPAの起動に成功しました」(/en-us/citrix-virtual-apps-desktops/2503/media/director-spa-successful-app.png)

成功コードの詳細については、(/ja-jp/citrix-secure-private-access/current-release/spa-onprem-director-info-codes)を参照してください。

アクセスが拒否されたアプリの詳細を表示する

セッションの選択画面で**アクセス詳細の確認**をクリックします。

「Director SPAのアクセス詳細を確認」(/en-us/citrix-virtual-apps-desktops/2503/media/director-check-access-details.png)

> **注：**
>
> **アクセス詳細の確認**ボタンは、アクティブなセッションがない場合に表示されます。
>
> または、,

アクセスが拒否されたアプリを表示するには、**アクセス拒否**タブをクリックします。

アクセス拒否タブが開きます。

「Director SPAのアクセス拒否の詳細」(/en-us/citrix-virtual-apps-desktops/2503/media/director-spa-denied-access.png)

時間、リソース、エンドポイント名、失敗の理由などのセッション詳細が表示されます。エラーコードの詳細については、(/ja-jp/citrix-secure-private-access/current-release/spa-onprem-director-info-codes)を参照してください。

現在、以下の問題が確認されています。

- ポリシー条件により列挙が拒否されました
- アプリの起動エラー
- 列挙エラー
- ポリシー条件によりアプリの起動が拒否されました

詳細を表示するには、**Denied Access** タブ > **Resource** 列からアプリを選択します。

Director SPA が詳細へのアクセスに失敗しました(/en-us/citrix-virtual-apps-desktops/2503/media/director-spa-failed-app.png)

成功または失敗したセッションについて、以下の詳細が表示されます。

- アプリについて
- ポリシー評価
- セッションの詳細

アプリについて

成功、失敗、または拒否されたアプリの名前が表示されます。それに加えて、成功または失敗したアプリの以下の詳細が表示されます。

フィールド	説明
トランザクションID	セッションまたは列挙中のCitrixトランザクションID。
リソースの種類	リソースの種類を表示します。指定可能な値は、Web、SaaS、TCP/UDP (サーバーからクライアント)、および TCP/UDP (クライアントからサーバー) です。
アクセスされたリソース	セッションまたは列挙中にアクセスされたリソースの URL。TCP または UDP アプリの場合、アクセスされたリソースの種類が TCP か UDP かを示します。
構成済みポリシー	セッションまたは列挙内で使用されるポリシーの数。
理由	セッションまたは列挙アクティビティの分析。
適用されたセキュリティ制限	Secure Private Access アプリで適用されるセキュリティ制限を表示します。

ポリシー評価

成功したセッションの評価中に問題が検出されなかったことを示します。失敗したセッションまたは列挙の場合、評価されたポリシーの次の詳細が表示されます。

フィールド	説明
ID	Citrix トランザクション ID。
ポリシー名	ポリシーの名前。複数のポリシーがある場合、設定された条件に一致する最初のポリシーが表示されます。
ステータス	ポリシーのステータス。

フィールド	説明
適用されたアクション	ポリシーに適用されたアクション。たとえば、アクセス拒否など。
ポリシー条件の評価	
種類	ポリシー条件の種類。
条件の基準	失敗したセッションまたは列挙に適用されたポリシーの条件基準。
値	ポリシーの値。
評価ステータス	ポリシーの評価ステータス。異なる値は、**許可**、**拒否**、**制限付きアクセス許可**、**エラー**です。

セッションの詳細

失敗したセッションの場合、セッション失敗の理由が表示されます。成功したセッションの場合、次の詳細が表示されます。

フィールド	説明
セッションの状態	セッションがアクティブか非アクティブか、その状態を表示します。
開始時刻	セッションの開始時刻を表示します。
最終アクティブ時刻	成功したセッションの最終アクティブ時刻を表示します。
ゲートウェイ仮想IP	正常に接続されたセッションが接続されているゲートウェイの仮想IPアドレスを表示します。
コンテキストタグ	コンテキストタグを表示します。Secure Private Accessプラグインのコンテキストタグは、認証済みユーザーのセッションに適用されるNetScaler® Gatewayポリシー（セッション、事前認証、EPA）の名前です。

フィールド	説明
アクセス済みドメイン (内部)	成功したセッションを使用してアクセスされた内部ドメインを表示します。
アクセス済みドメイン (外部)	成功したセッションを使用してアクセスされた外部ドメインを表示します。

Citrix VDA Upgrade Service (VUS) - テクニカルプレビュー

テクニカルプレビューの機能

テクニカルプレビューの機能は、非本番環境または限定的な本番環境で使用でき、お客様がフィードバックを共有する機会を提供します。Citrixは、テクニカルプレビューの機能に関するサポートケースを受け付けていませんが、改善のためのフィードバックを歓迎します。Citrixは、フィードバックの重大度、重要性、および重要度に基づいて対応する場合があります。

これは、いかなる資料、コード、または機能を提供するというコミットメント、約束、または法的義務ではなく、Citrix 製品の購入決定を行う際に依拠すべきではありません。機能の開発、リリース、およびタイミングは、当社の単独の裁量に委ねられており、通知や協議なしに変更される場合があります。

シトリックス VDA アップグレードサービス (VUS)

Citrix VDA Upgrade Service (VUS) は、Citrix Virtual Apps and Desktops™ (CVAD) のコンポーネントであり、Citrix環境内の永続的なVirtual Delivery Agent (VDA) のアップグレードプロセスを効率化します。このサービスは、環境を最新のVDAバージョンに保ち、パフォーマンスとセキュリティを向上させ、新しいCitrix DaaS機能を有効にするのに役立ちます。

管理者はVUSを活用して、アップデートの確認、アップグレードのスケジュール設定、アップグレードの進行状況の監視を行うことができます。アップグレードはすぐに開始することも、特定の日時にスケジュールすることもでき、アップグレードに最適な時間を選択できます。

VDAのアップグレードがこれまでになく簡単になりました。VDAまたはイメージにVDA Upgrade Agentをインストールし、Web Studioでマシンまたはマシンカタログを右クリックして「Upgrade VDAs」を選択し、環境に最適なオプションを選択します。

アップグレードする前に、アップグレードサイクルオプションを確認してください。VDAには、Long-Term Service Release (LTSR) とCurrent Release (CR) の2つのアップグレードトラックがあります。LTSRはサポートライフサイクルが長く、安定性が高く、アップグレードの頻度が低くなります。CRバージョンはより頻繁にリリースされ、最新かつ最高の機能を提供します。詳細については、 ライフサイクルマイルストーンを参照してください。

VUS を使用した VDA アップグレードの前提条件

VUS を使用して VDA アップグレードを実行するには、次の前提条件を満たす必要があります。

サイトの VDA アップグレードサービスを有効にする

2503 サイトで VUS を有効にするには、次の PowerShell コマンドレットを実行します。

```
Set-VusSite -Enabled $true
```

有効にしたら、次の PowerShell コマンドレットを実行して、最新の VDA バージョンを CVAD サイトにインポートします。

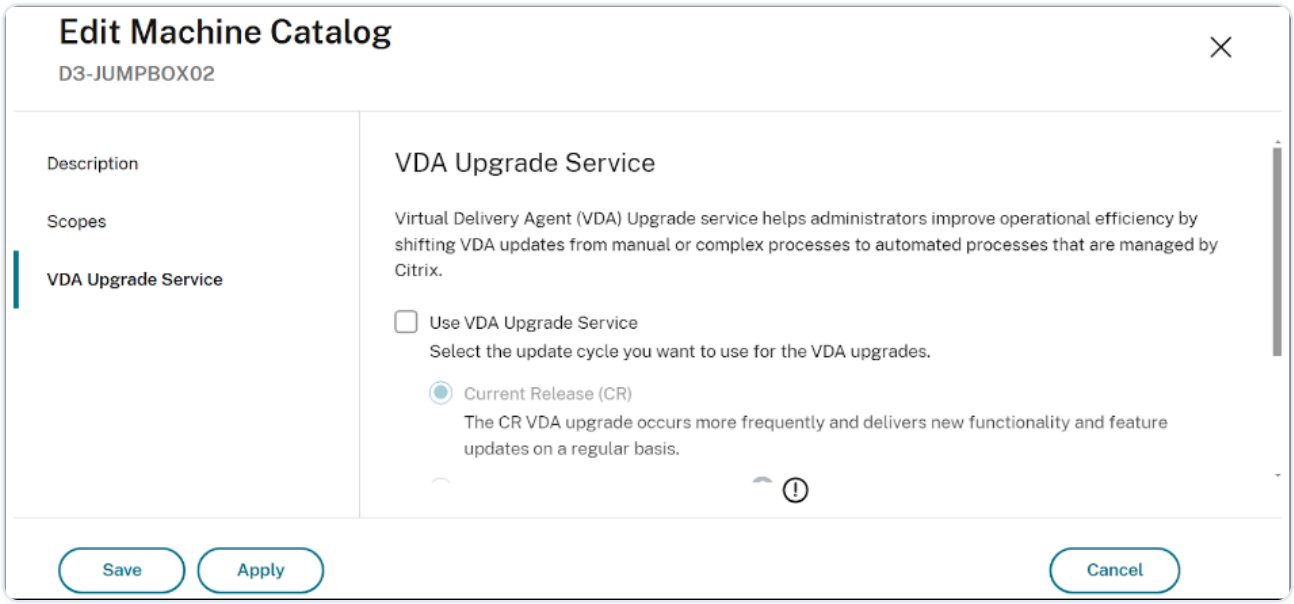
```
Import-VusVdaReleasesMetadata -Path '[<CVAD-2503-ISO>\Support\VdaUpdateServiceMetadata\vda_releases.xml]'
```

VDA アップグレードサービスを有効にする

VDA アップグレードサービス機能を有効にするには、マシンカタログの作成または編集時に VDA アップグレードオプションを使用します。管理者は、VUS を有効にする際に、次のアップグレードサイクルから選択する必要があります。

- LTSR
- CR
- LTSR 早期アクセスリリース (EAR)
- CR EAR

Web Studio からマシンカタログの VDA アップグレードサービスを有効にするには、カタログを右クリックし、 をクリックし、 タブを選択し、 チェックボックスをオンにして、アップグレードトラックを選択します。



PowerShell を使用してマシンカタログの VDA アップグレードサービスを有効にするには、`Set-VusCatalogUpgradeType` コマンドレットを使用します。

アップグレードの種類は、「LTSR」、「CR」、「EAR_CR」、または「EAR_LTSR」に設定できます。

例: `Set-VusCatalogUpgradeType -CatalogName "Workstation catalog" -UpgradeType LTSR`

> **注:**
>
> VDA アップグレードオプションを有効にしても、VDA の自動アップグレードは行われません。VUS を介したすべての VDA アップグレードは、管理者によって明示的に実行される個別のタスクとして開始する必要があります。

VDAの要件

VDA バージョン

- MCS を使用して作成されたマシンの場合:
  - 2311 以降
- Websocket VDA Enrollment を使用して追加されたマシンの場合
  - 2311 以降
- 手動でプロビジョニングされたマシンの場合

- 2411 以降

プロビジョニングタイプ

- Citrix 以外のプロビジョニング™サービスまたは を使用してプロビジョニングされた、シングルまたはマルチセッションの永続マシン。
- シングルセッションのMCSプロビジョニングされた永続マシン（AD参加済み、Azure AD参加済み、およびドメイン非参加）。
- リモートPCアクセス マシン。

VDAアップグレードエージェント

- VDAアップグレードエージェント バージョン7.44以降がVDAにインストールされ、アクティブである必要があります。エージェントは以下のようにインストールできます。
  - VDAをアップグレードするとき、またはVDAのインストールを変更するときに、追加コンポーネントとして。
  - Citrix Virtual Apps and Desktops™ ISOで利用可能なスタンドアロンMSIを使用して。
    - MSI名: CitrixUpgradeAgent_x64.msi
    - パス: x64\仮想デスクトップコンポーネント

権限

CVADでフル管理者またはマシンカタログ管理者ロールを持っている必要があります。

VDAの状態

VUSを介してスケジュールされたアップグレードが意図したとおりに進行するためには、アップグレード対象のVDAは以下の前提条件を満たす必要があります。

- VDAは手動でメンテナンスモードに設定されていてはなりません。
- VDAのアップグレードが正常に実行されるためには、ユーザーがログオンしていない必要があります。
  - アップグレードプロセスがアップグレード期間中にユーザーセッションのドレインを開始すると、VDAはメンテナンスモードに設定されます。アップグレードが正常に完了すると、メンテナンスモードから解除されます。
  - アップグレードウィンドウの期間中、ユーザーがアクティブまたは切断されたセッションを持っている場合、アップグレードはアップグレードウィンドウの終了時にキャンセルされます。

> **注:**
>
> アクティブおよび切断されたセッションは、VUSの強制ログオフオプションを使用して終了できます。

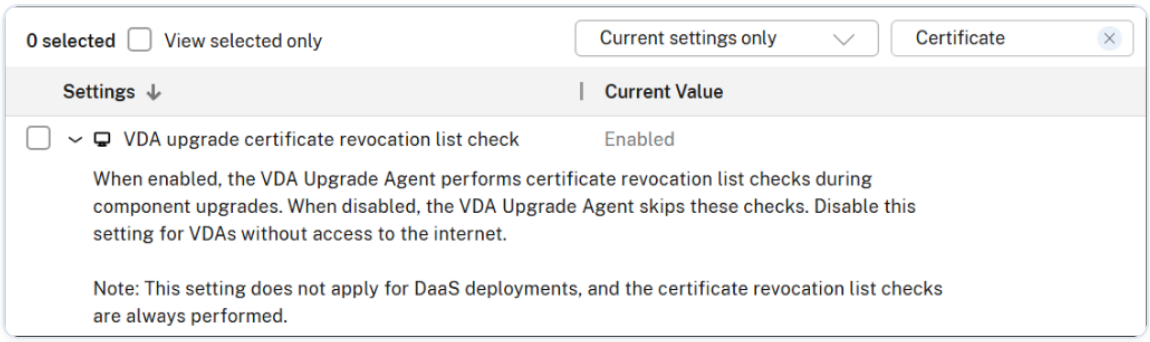
- MCSを介してプロビジョニングされていないVDA（手動でプロビジョニングされたVDA）は、VUSを介してアップグレードを実行する前にデリバリーグループに追加する必要があります。
- VDAは電源が入っている必要があります。

> **注:**
>
> VDAアップグレードがスケジュールされている場合でも、AutoScale™はマシンの電源管理を停止しません。アップグレードの進行中は、デリバリーグループのAutoScaleスケジュールを無効にすることを検討してください。

接続

- VDAアップグレードの場合、VDAはHTTPS経由でデリバリーコントローラーと通信できる必要があります。
  - VDAインストーラーが有効な証明書によって署名されていることを確認するには、VDAは次のURLと通信する必要があります。
    - `<http://crl3.digicert.com/>` *
    - `<http://crl4.digicert.com/>` *
    - `<http://ocsp.digicert.com/>` *
    - `<http://cacerts.digicert.com/>` *
- VDAがインターネットにアクセスできない場合は、証明書失効リスト（CRL）をバイパスするようにVDAを構成します。
  - 「VDAアップグレード証明書失効リストチェック」Citrix®ポリシー設定を無効にし、デリバリーグループに割り当てます。
    - ポリシーの説明:

- 有効にすると、VDAアップグレードエージェントはコンポーネントのアップグレード中に証明書失効リストチェックを実行します。
- 無効にすると、VDAアップグレードエージェントはこれらのチェックをスキップします。インターネットにアクセスできないVDAでは、この設定を無効にしてください。



プロキシ構成を持つVDA

- ホスト名:ポート (IP:ポート) およびPACファイルの形式のプロキシのみがサポートされています。SOCKS5プロキシはサポートされていません。
- VDAアップグレードエージェントは、Web Studioまたはレジストリを使用してプロキシを使用するように構成する必要があります。
  - Web Studioを使用したVDAアップグレードエージェントのプロキシ構成。
    - プロキシを使用するVDAに対して、VDAアップグレードプロキシ構成のCitrixポリシー設定を有効にします。
    - 設定でプロキシアドレスまたはPACファイルへのパスを入力します。
  - レジストリを使用したVDAアップグレードエージェントのプロキシ構成
    - **キー:** `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\VirtualDesktopAgent`
      - **値の型:** `String`
      - **値の名前:** `ProxySettings`
      - **値のデータ:** プロキシアドレスまたはPACファイルへのパス。
        - 例:
          - **プロキシアドレス:** `http://<URL or IP>:\<port>`
          - **PACファイル:** `http://<URL or IP>/\<path/\<filename>.pac`

VDAWorkstationCoreSetup.exe を使用してインストールされた VDA

VDA が VDAWorkstationCoreSetup.exe を使用して最初にインストールされた場合でも、`VDAWorkstationSetup.exe` を利用する VUS を使用してアップグレードできます。

`VDAWorkstationCoreSetup.exe` を使用してインストールされた VDA を VUS でアップグレードする場合は、特に最小限のコアインストールから移行する場合、目的の機能のみが有効になっていることを確認するために、インストールオプションを確認する必要があります。

VDAアップグレードサービスを使用したVDAのアップグレード

ターゲットマシンカタログ、個々のマシン、またはマシンのグループを選択し、その後「VDAのアップグレード」を選択することで、VDAアップグレードサービスを介してVDAアップグレードを開始できます。

> **注:**
>
> Citrix® は、可能な場合はアップグレードを実行する前に VDA をバックアップすることを推奨します。

アップグレードのスケジュール設定

CitrixにおけるVDAアップグレードプロセスは、要件に応じて、カタログレベル、マシンのグループレベル、または個々のマシンレベルで実行できます。アップグレードはすぐに開始するように設定することも、最大7日前までに日時を指定してスケジュールすることもできます。

考慮事項

- **カタログ vs. マシンのグループ vs. マシンのスコープ:** カタログアップグレードは一括更新に最適ですが、個別に、またはグループでマシンをアップグレードすると、よりきめ細かな制御が可能になります。
- **スケジュール設定:** アップグレードは最大7日前までにスケジュールできます。マシンカタログレベルのアップグレードを使用している場合、アップグレードがスケジュールされた後にカタログに追加されたマシンは、既存のスケジュールされたアップグレードの一部として含まれません。

主な違い

機能	カタログごとのアップグレード	マシンごとのアップグレード	マシンのグループ
アップグレードの範囲	カタログ全体	個々のマシン	マシンカタログ内のマシンのグループ
スケジュール制御	単一のスケジュールがマシンカタログ内のすべてのVDAに適用され、大規模なアップグレード操作に最適です	VDAは個別にスケジュールされ、主にテストや1回限りのアップグレードに使用されます	VDAはグループでスケジュールされ、異なるVDAグループを異なる時間にアップグレードする柔軟性を提供します
管理	Web Studioの「マシンカタログ」ノードまたは `New-VusCatalogSchedule` コマンドレットを介して管理されます	Web Studioの「検索」ノードまたは `New-VusMachineUpgrade` コマンドレットを介して管理されます	Web Studioの「検索」ノード、またはマシンのリストを `New-VusMachineUpgrade` コマンドレットに渡すことで管理されます
ユースケース	マシンカタログ全体のバルクアップグレード	ターゲットを絞ったアップグレードとテストシナリオのためのきめ細かい制御	VDAのサブセットを対象とした制御。カタログ内のアップグレードを段階的に実行するために使用できます
利用可能な VDA バージョン	CR および現在サポートされているすべての LTSR VDA バージョンでは、最新バージョンと 2 つ前の (N-2) バージョンにアップグレードできます。詳細については、利用可能な VDA バージョン を参照してください。	CR および現在サポートされているすべての LTSR VDA バージョンでは、最新バージョンと 2 つ前の (N-2) バージョンにアップグレードできます。詳細については、利用可能な VDA バージョン を参照してください。	最新の LTSR または CR VDA バージョンのみがアップグレード可能です

機能	カタログごとのアップグレード	マシンごとのアップグレード	マシンのグループ
追加コンポーネント	各 VDA に VDA コンポーネントをインストールまたはアップグレードします。コンポーネントのチェックを外しても機能はアンインストールされませんが、コンポーネントはアップグレードされません	VDA 上の VDA コンポーネントをインストールまたはアップグレードします。コンポーネントのチェックを外しても機能はアンインストールされませんが、コンポーネントはアップグレードされません	マシンのグループをアップグレードする場合、追加コンポーネントは VDA アップグレードサービスによって管理できません。注: 「復元クリーンアップを有効にする」などの追加機能は、マシンのグループのアップグレードで利用できます
追加機能	追加機能を有効またはアップグレードできます	追加機能を有効またはアップグレードできます	追加機能を有効またはアップグレードできます
同時実行	アップグレードのスケジュール設定時に設定として制御されます。詳細については、同時実行 を参照してください	単一の VDA がアップグレードされます	アップグレードスケジュールの一部として選択されたVDAの数に基づいて自動的に負荷分散されます
失敗しきい値	指定された数のVDAのアップグレードが失敗した場合に、それ以降のアップグレードを防止するために失敗しきい値を設定できます。詳細については、「失敗しきい値」を参照してください。	失敗しきい値は、マシンごとのアップグレードには適用されません。	失敗しきい値は、マシンのグループのアップグレードには使用できません。アップグレードするマシンのグループのサイズを、許容できる失敗数となるVDAの最大数に設定することを検討してください。

スケジュールされたアップグレードの仕組み

VDA上のVDAアップグレードエージェントは、VDAをアップグレードする必要があるかどうかを判断するために、定期的にDelivery Controllerと通信します。 VDAは、すぐにアップグレードするように、または最大7日前にアップグレードするようにスケジュールできます。事前にアップグレードをスケジュールする場合、アップグレードが開始される日付と時刻（UTC）を設定できます。

アップグレード期間は、スケジュールされたアップグレード開始時刻からアップグレードが実行されるまでの時間を設定します。デフォルトでは、マシンカタログおよびマシンのグループのアップグレードの場合、Citrixはパフォーマンスを向上させ、ボトルネックを回避するために、アップグレード期間全体にわたってVDAアップグレードの負荷分散を行います。

アップグレードが開始されると、VDAはアップグレードが完了するまでメンテナンスモードになります。VDAでセッションが実行されている場合、セッションがなくなるまでVDAはアップグレードされません。メンテナンスモードの間は、新しいセッションをVDAに仲介することはできません。アップグレード期間中にユーザーがセッションから切断した場合、アップグレードが完了するまで再接続できません。

VDAは、スケジュールされたアップグレード期間が完了するまでアップグレードを試行し続けます。アップグレード期間全体にわたってセッションが存在する場合、アップグレードはキャンセルされ、VDAのメンテナンスモードはオフになります。VDAアップグレードの成功率を向上させるために、より長いアップグレード期間を検討してください。

> **注:**
>
> スケジュールされたアップグレードの前に手動でメンテナンスモードに設定されたVDAは、アップグレードに失敗します。

利用可能なVDAバージョン

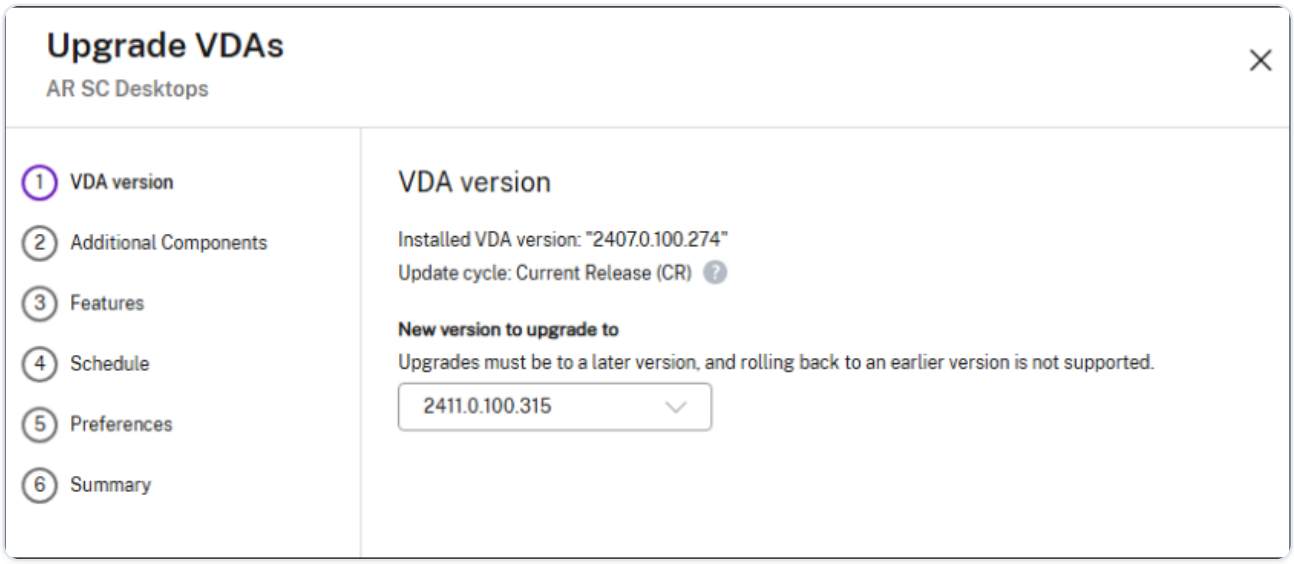
VDAアップグレードサービスは、CRバージョンではVDAのN-2バージョンを、現在サポートされているすべてのLTSRバージョンではN-2 CUバージョンを維持します。

新しいCVADバージョンがリリースされた場合、サイト全体を更新することなく、VUSを更新してより新しいVDAバージョンを含めることができます。VUSは**vda_releases.xml**ファイルを使用して、利用可能なVDAバージョンを投入します。**vda_releases.xmld**ファイルは、CVADメタインストーラーの次の場所にあります。

<CVAD-ISO\>\Support\VdaUpdateServiceMetadata\vda_releases.xml

新しいvda_releases.xmlファイルをVUSにインポートするには、次のコマンドレットを実行します。 `Import-VusVdaReleasesMetadata -Path '[Path to vda_releases.xml]'`

Web Studioで、カタログまたは個々のマシンをアップグレードする際、UIはVDAをアップグレードするバージョンを尋ねます。



PowerShell を使用して利用可能なVDAバージョンを特定するには、`Get-VusAvailableVdaVersion` コマンドレットを使用します。

コマンドレットにマシンまたはカタログを渡さない場合、コマンドレットはすべてのアップグレードトラックで利用可能な最新バージョンを返します。

リソースで利用可能な特定のバージョンを取得するには、`Get-VusAvailableVdaVersion`コマンドレットでVDA（-MachineName、-MachineUid、または-MachineUuid）またはカタログ（-CatalogName、-CatalogUid、または-CatalogUuid）を渡します。

例: `Get-VusAvailableVdaVersion -CatalogName '[Name of your Machine Catalog]'`

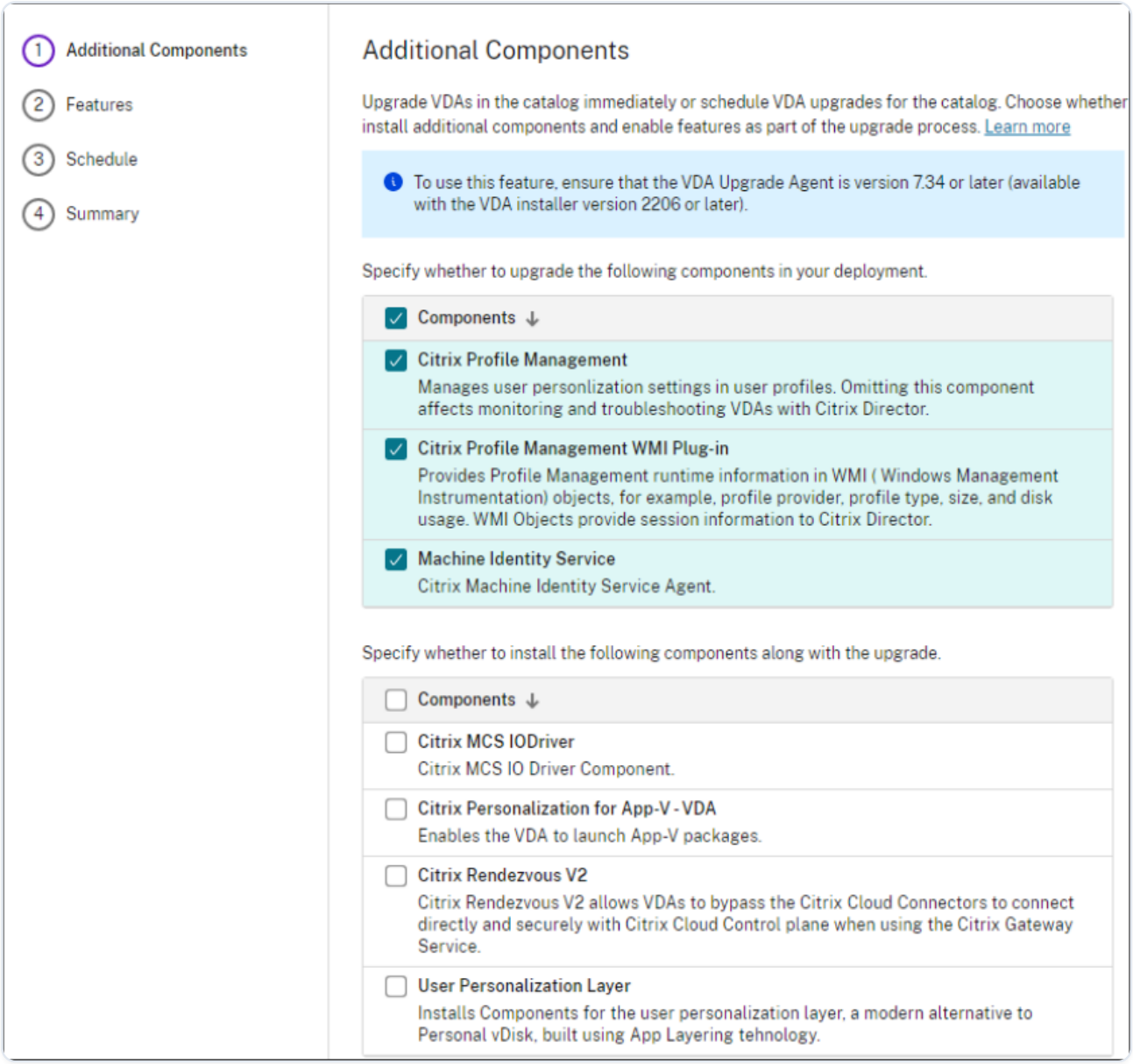
```
PS V:\> Get-VusAvailableVdaVersion -CatalogName 'CR-2303'

UpgradeType Version
----------- -------
         CR 2411.0.100.315
         CR 2407.0.100.274
         CR 2402.0.100.629
```

追加コンポーネント

追加コンポーネントは、マシンカタログまたは個々のマシンによってVDAをアップグレードする際にインストールまたはアップグレードできます。コンポーネントをチェックしない場合、その

コンポーネントはアンインストールされませんが、VDA全体のアップグレードの一部としてアップグレードされません。

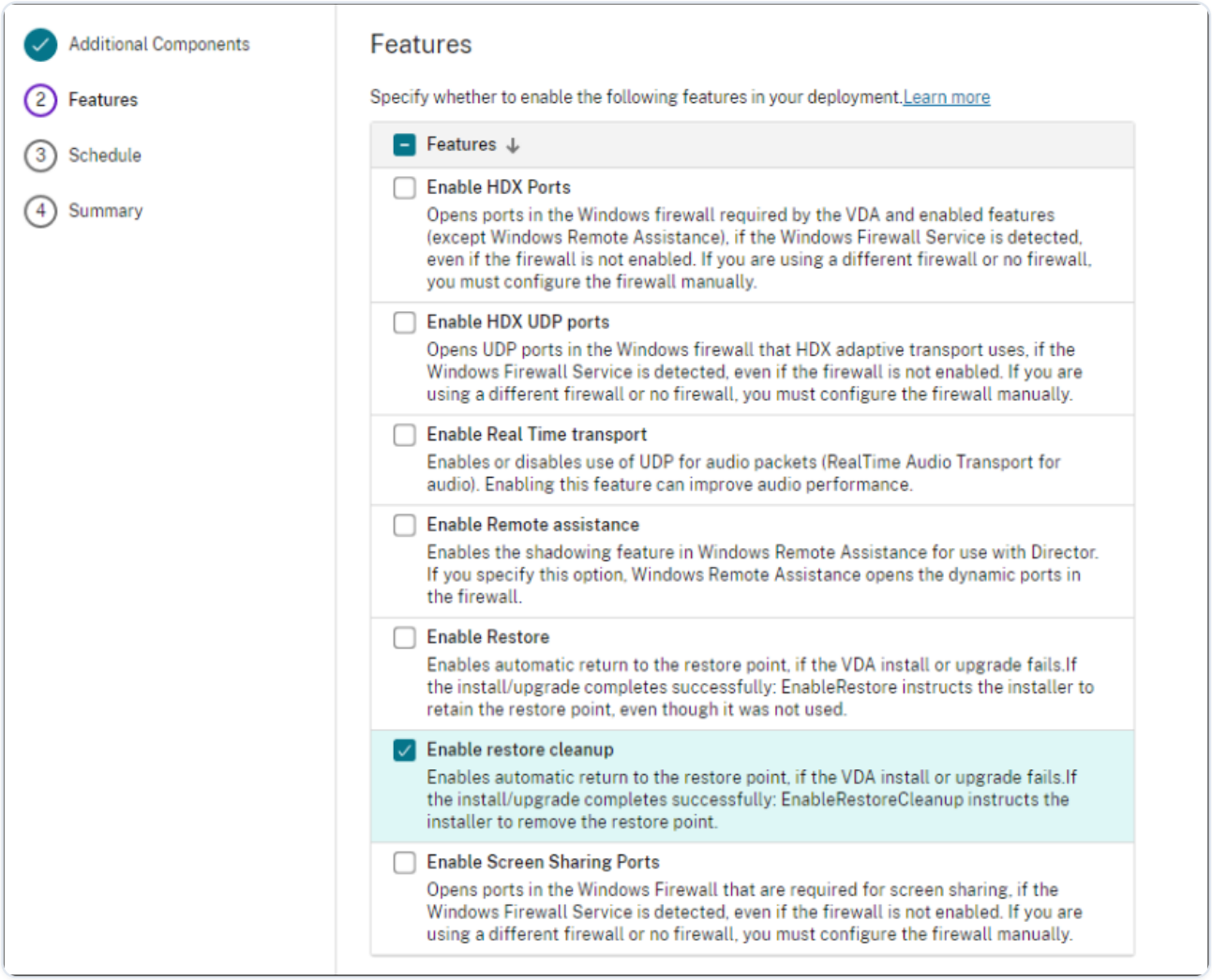


機能

機能は、VDAアップグレードサービスを通じてVDAで有効化またはアップグレードできます。機能をチェックしない場合、その機能は無効になりませんが、VDA全体のアップグレードの一部としてアップグレードされません。

デフォルトでは、**Enable restore cleanup**チェックボックスが選択されています。Citrixは、管理を容易にし、失敗したアップグレードの回復を改善するために、復元クリーンアップ機能を有効にすることをお勧めします。この機能を有効にすると、アップグレードが開始される前にシステム復元ポイントが作成されます。アップグレードが失敗した場合、VDAはシステム復元ポイント

に復元されます。復元ポイントは、VDAのインストールが成功した後に削除されます。詳細については、「インストールまたはアップグレードの失敗時の復元」を参照してください。



注:

Windows システムの復元は、シングルセッションオペレーティングシステム (例: Windows 10 および 11) でのみサポートされています。「復元のクリーンアップを有効にする」機能が動作するためには、VDA で Windows システムの復元機能が有効になっている必要があります。「復元を有効にする」または「復元のクリーンアップを有効にする」が選択されていても、VDA で Windows システムの復元が構成されていない場合、アップグレードが失敗する可能性があります。

同時実行数

マシンカタログをアップグレードする際、VUSを使用すると、同時にアップグレードするVDAの最大数を定義できます。これにより、インターネット接続やファイルサーバーへの負荷を軽減で

き、障害しきい値と組み合わせて使用することで、多数のVDAのアップグレードが失敗した場合にアップグレードを停止できます。

スケジュールされたアップグレードが開始されるとすぐに、カタログ内のすべてのVDAはメンテナンスモードになります。定義された最大同時実行設定に一致する数のVDAでアップグレードが開始されます。VDAのアップグレードが完了するとすぐに、同時にアップグレードしているVDAの数を維持するために、別のVDAがアップグレードを開始します。

マシンカタログのスケジュールされたアップグレードで同時実行性が指定されていない場合、Citrixはカタログ内のVDAの総数とアップグレード期間に基づいてデフォルトの同時実行値を使用します。

アップグレードの完了には平均約30分かかりますが、これは環境条件によって大きく異なります。指定されたアップグレード期間内にすべてのVDAがアップグレードできるような同時実行数を設定することを検討してください。たとえば、4時間で20台のVDAをアップグレードするように設定されている場合、1時間あたり5台のVDAをアップグレードする必要があります。平均アップグレード期間が30分であるとすると、1時間あたり5台のVDAアップグレードという要件を満たすために、同時実行値を3に設定できます（30分あたり3回のアップグレードは、1時間あたり6回の更新になります）。

失敗しきい値

マシンカタログをアップグレードする際、障害しきい値を使用して、特定の数のVDAが失敗した場合にそれ以上のVDAがアップグレードされるのを防ぎます。障害しきい値は、アップグレードの失敗を引き起こす問題の影響範囲を縮小し、管理者のトラブルシューティング作業を軽減できます。

障害しきい値は、将来のVDAがアップグレードを開始するのを防ぎますが、すでにアップグレードを開始しているVDAを停止することはありません。たとえば、マシンカタログに100台のVDAがあり、同時実行が10台のVDAに設定され、障害しきい値が3に設定されている場合、すべてのVDAアップグレードが失敗すると、少なくとも13台のVDAがアップグレードを試行し、残りの87台は開始されず、アップグレードはキャンセルされます。

スケジュールされたアップグレードの開始時に10台の同時実行VDAがアップグレードを開始し、最初のアップグレードが失敗した場合、10台の同時実行アップグレードを維持するために別のVDAがアップグレードを開始します。2番目のアップグレードが失敗した場合、別のVDAがアップグレードを開始します。3番目のアップグレードが失敗した場合、現在アップグレードプロセス中のすべてのVDAは続行され、アップグレードスケジュール内の残りのVDAのアップグレードはキャンセルされます。

VDAインストーラーの場所

VDAインストーラーは、環境内のローカルファイル共有でホストされている必要があります。ファイル共有とVDAインストーラーの要件は以下のとおりです。

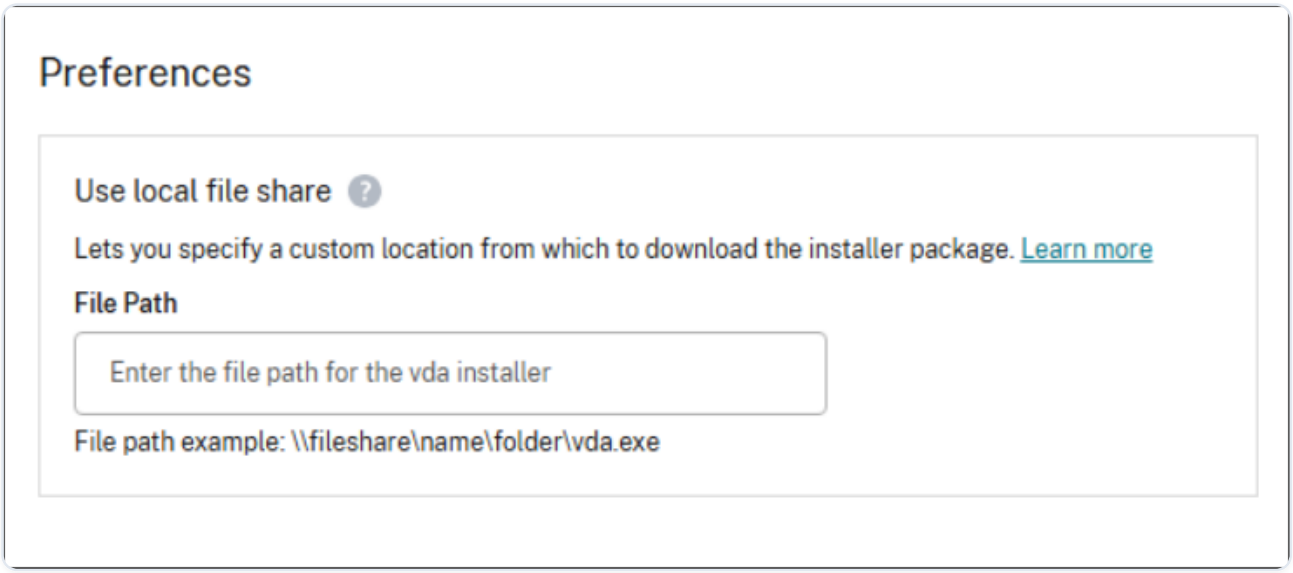
ファイル共有には、次の前提条件が必要です。

- ファイル共有のアクセス許可
  - VDAインストーラーパッケージを含むネットワーク共有には、ローカルシステム (NT AUTHORITY\SYSTEMプリンシパル) として実行されるVDAアップグレードエージェントサービスに対する読み取りアクセス権が必要です。
  - ドメイン参加済みVDA:
    - ローカルシステムアカウント (VUAはローカルシステムとして実行されます) は、ネットワーク共有にアクセスする際にコンピューターの資格情報を使用します。
    - ファイル共有には、ドメインコンピューターに対する読み取りアクセス権を付与する必要があります。
    - 共有の詳細設定で、**ファイルとプリンターの共有**を有効にする必要があります。
  - ドメイン非参加VDA:
    - ローカルシステムアカウント (VUAはローカルシステムとして実行されます) は、ネットワーク共有にアクセスする際に**ANONYMOUS LOGON**を使用します。
    - **ネットワークと共有センター、パスワード保護共有**は無効にする必要があります。
    - フォルダーのアクセス許可の**セキュリティ**タブで、**ANONYMOUS LOGON**に読み取りアクセス許可を付与する必要があります。
    - 詳細共有設定で、**ファイルとプリンターの共有**を有効にする必要があります。
    - 共有フォルダー名は、**ネットワークアクセスセキュリティポリシー**に追加する必要があります。
- VDAインストーラー
  - VDAインストーラーは、Citrix Downloads Webサイトからダウンロードし、ファイル共有に配置する必要があります。
  - マシンカタログに関連するVDAインストーラーをダウンロードする必要があります。
    - カタログタイプがマルチセッションの場合は、**Multi-session OS VDA installer**を使用します。

- カタログタイプがシングルセッションの場合は、**Single-session OS VDA installer**を使用します。

- 特定のアップグレードの場合、ファイル共有上のインストーラーのバージョンは、VUSによって公開されているバージョンと完全に一致している必要があります。利用可能なバージョンを確認するには、`Get-VusAvailableVersion` PowerShellコマンドレットを使用します。

インストーラーへのパスは、実行可能ファイルを含むファイルパスである必要があります。例: `\\hostname\VDA-Packages\VDAWorkstationSetup_2308.exe`。



PowerShellを介してVUSを使用する場合、アップグレードをスケジュールするときに、`-VdaWorkstationPackageUri` (シングルセッションOS) または `-VdaServerPackageUri` (マルチセッションOS) パラメーターを使用します。

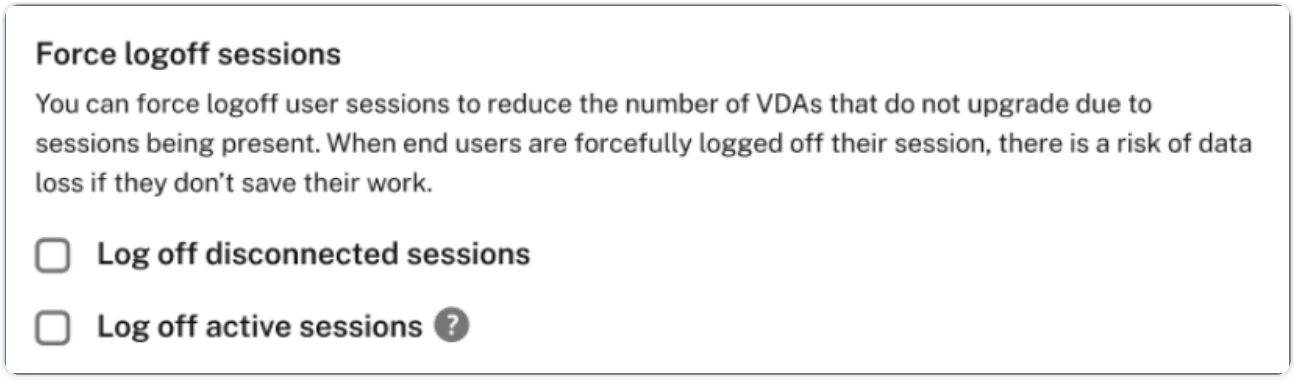
セッションの強制ログオフ

スケジュールされたアップグレード中にアップグレード可能なVDAの数を増やすには、アップグレード中にユーザーセッションを強制的にログオフすることを検討してください。強制ログオフは、個々のVDAのアップグレードが開始されるときに発生し、全体のスケジュールされたアップグレード期間の開始時ではありません。

スケジュールされた期間内で異なるVDAが異なる時間にアップグレードを開始するため、ユーザーは自身の特定のVDAのアップグレードが開始されたときにのみログオフされます。

Web Studioを使用してスケジュールされたアップグレード中に切断されたセッションを強制的にログオフするには、 オプションを選択します。

Web Studioを使用してスケジュールされたアップグレード中にアクティブなセッションを強制的にログオフするには、「**アクティブなセッションをログオフする**」オプションを選択します。アクティブなセッションをログオフする場合、ユーザーはアップグレード開始の10分前にセッション内で通知を受け取り、自動的にログオフされる前に作業を保存するよう促されます。



PowerShellを使用してスケジュールされたアップグレード中に切断されたセッションを強制的にログオフするには、アップグレードをスケジュールするときに`-LogoffOption`パラメーターを使用します。`-LogoffOption`で利用可能なオプションは以下のとおりです。

- **ActiveSessionsOnly:** スケジュールされたアップグレード期間中にVDAでアクティブなセッションがある場合、ユーザーはログオフされます。ユーザーがログオフされる10分前に警告としてバナーが表示されます。切断されたセッションがあるVDAは、アップグレード期間中にログオフされません。切断されたセッションがアップグレード期間中ずっと残っている場合、そのVDAのアップグレードはキャンセルされます。
- **DisconnectedSessionsOnly:** スケジュールされたアップグレード期間中にVDAで切断されたセッションがある場合、ユーザーはログオフされます。ユーザーには、切断されたセッションがログオフされることは通知されません。アクティブなセッションがあるVDAは、アップグレード期間中にログオフされません。アクティブなセッションがアップグレード期間中ずっと残っている場合、そのVDAのアップグレードはキャンセルされます。
- **ActiveAndDisconnectedSessions:** スケジュールされたアップグレード期間中に VDA で切断されたセッションまたはアクティブなセッションがある場合、ユーザーはログオフされます。アクティブなセッションの場合、ユーザーがログオフされる 10 分前に警告としてバナーが表示されます。
- **DoNotLogoff:** アクティブなセッションと切断されたセッションはログオフされません。アップグレードスケジュールの期間中ずっと VDA にセッションが存在する場合、スケジュールされたアップグレード期間の終了時にアップグレードはキャンセルされます。

可能な場合、Citrix は、アップグレードが正常に完了する VDA の数を増やすために、セッションを強制的にログオフすることを推奨します。

> **重要:**
>
> セッションを強制的にログオフすると、ユーザーがセッションから保存していない作業を失う可能性があります。

VDA ワークフローの編集またはキャンセル

カタログのアップグレードをスケジュールした後、アップグレードの開始時刻と期間を編集したり、アップグレードを完全にキャンセルしたりできます。

UI を使用してマシンカタログレベルでアップグレードを編集またはキャンセルするには、既存のスケジュールされたアップグレードがあるマシンカタログを右クリックし、「**スケジュールされた VDA アップグレードの編集**」をクリックします。PowerShell を使用して既存のマシンカタログレベルのアップグレードを編集するには、`Set-VusCatalogUpgrade` および `Remove-VusCatalogUpgrade` コマンドレットを使用します。

マシンレベルでアップグレードを編集またはキャンセルするには、検索ノードで、既存のスケジュールされたアップグレードがあるマシンを右クリックし、「**スケジュールされた VDA アップグレードの編集**」をクリックします。複数のマシンのスケジュールされた VDA アップグレードを同時に編集することはできません。PowerShell を使用して既存のマシンレベルのアップグレードを編集するには、`Set-VusMachineUpgrade` および `Remove-VusMachineUpgrade` コマンドレットを使用します。

VUS の監視とトラブルシューティング

スケジュールされたVDAアップグレードの監視

VDAとマシンカタログには、VDAアップグレードの準備状況と現在のステータスを監視するのに役立つ2つの属性があります。これらは、Studioでフィルタリングしたり、VDAまたはカタログの詳細ペインで表示したりできる列として表示されます。

- VDAアップグレード
- VDAアップグレードの状態

VDAアップグレード

VDAアップグレードは、VDAまたはマシンカタログにVDAアップグレードエージェントが構成されているかどうか、およびVDAが最新であるか、またはアップグレードが利用可能であるかに関する情報を提供します。利用可能なステータスは次のとおりです。

VDAアップグレード (STUDIO)	VDAアップグレード (POWERSHELL)	説明
カタログレベル		
未構成	MissingUpgradeType	マシンカタログのアップグレードトラック (CR、LTSR、CR EAR、またはLTSR EAR) が選択されていません。
スケジュール済み	アップグレードがスケジュール済み	マシンカタログのアップグレードがスケジュールされています。
利用可能	アップグレードが利用可能	カタログ内のVDAは、アップグレードトラックの最新バージョンではありません。アップグレードが推奨されます。
最新	最新	カタログ内のVDAは、アップグレードトラックの最新バージョンです。アクションは不要です。
不明	不明	最新のVDAアップグレード状態を取得しています。
マシンレベル		
未構成	アップグレードタイプがありません	VDAのマシンカタログにアップグレードトラック（CR、LTSR、CR EAR、またはLTSR EAR）が選択されていません。
スケジュール済み	UpgradeScheduled	VDA のアップグレードがスケジュールされています。
利用可能	UpgradeAvailable	VDA はアップグレードトラックの最新バージョンではありません。アップグレードが推奨されます。

VDAアップグレード (STUDIO)	VDAアップグレード (POWERSHELL)	説明
最新	UpToDate	VDA はアップグレードトラックの最新バージョンです。アクションは不要です。
状態を確認中	不明	最新の VDA アップグレード状態を取得しています。

注:

LTSR トラックを使用している VDA の場合、カタログは、VDA が最新の長期サービス (LTSR) バージョンの最新の累積更新プログラム (CU) にある場合にのみ「最新」と表示されます。VDA が以前の LTSR バージョンの最新の CU にある場合でも、VDA アップグレードは「**利用可能**」と表示されます。

VDA アップグレードの状態

VDAアップグレードの状態は、スケジュールされたアップグレードのステータスに関する情報を提供します。VDAアップグレードの状態のステータスは次のとおりです。

VDAアップグレードの状態 (STUDIO)	VDAアップグレードの状態 (POWERSHELL)	説明
カタログレベル		
スケジュールされていません	NotScheduled	カタログに対してアップグレードはスケジュールされていません。
スケジュール済み	UpgradeScheduled	カタログに対してアップグレードがスケジュールされています。
進行中	UpgradeInProgress	カタログに対してアップグレードが進行中です。
キャンセル済み	アップグレードキャンセル済み	カタログのアップグレードがキャンセルされました。これは、手動によるキャンセル、

VDAアップグレードの状態 (STUDIO)	VDAアップグレードの状態 (POWERSHELL)	説明
		または失敗しきい値に達したことが原因である可能性があります。
失敗	アップグレード失敗	カタログのスケジュールされたアップグレードが失敗しました。
成功	アップグレード成功	カタログのスケジュールされたアップグレードが正常に完了しました。注：アップグレードが成功したからといって、カタログ内のすべてのVDAが正常にアップグレードされたわけではありません。
-	空	カタログのアップグレードはスケジュールされていません。
マシンレベル		
スケジュール済み	アップグレードスケジュール済み	VDAのアップグレードがスケジュールされています。
アップグレード待機中	UpgradeInUpgradeWindow	スケジュールされたアップグレードはアクティブですが、VDAはまだアップグレードを開始していません。VDAアップグレードがどのように負荷分散されるかについては、「同時実行」を参照してください。
進行中	UpgradeInProgress	VDAは現在アップグレード中です。
キャンセル済み	UpgradeCancelled	アップグレードが開始される前に、VDAのスケジュールさ

VDAアップグレードの状態 (STUDIO)	VDAアップグレードの状態 (POWERSHELL)	説明
		れたアップグレードがキャンセルされました。
アップグレード失敗	UpgradeFailed	VDAはアップグレードを開始しましたが、アップグレードは正常に完了しませんでした。詳細については、「トラブルシューティング」を参照してください。
成功	UpgradeSuccess	VDAは正常にアップグレードされました。
検証に失敗しました	UpgradeValidationFailed	VDAインストーラーのメタデータをダウンロード中に、証明書の検証に失敗しました。
-	空	VDAのアップグレードはスケジュールされていません。

スケジュールされたVDAアップグレードのトラブルシューティング

アップグレードの失敗が発生した場合、以下のログは問題の特定とトラブルシューティングに役立ちます。これらのログをCitrixテクニカルサポートと共有することで、サポートプロセスを迅速化することもできます。

VDAインストールログ

アップグレードの失敗をトラブルシューティングする際は、VDAの初期インストールと失敗したアップグレードの両方のログを収集して確認してください。インストールおよびアップグレードのログは、以下の場所にあります。

- VDAインストールのインストールログは、次の場所にあります。
  - %temp%/Citrix/XenDesktop インストーラー
- VDAインストールのアップグレードログは、次のいずれかの場所にあります。
  - C:\Windows\Temp\Citrix\XenDesktop Installer **または**
  - C:\Windows\SystemTemp\Citrix\XenDesktop インストーラー

VDA アップグレードエージェントのバージョン

VUSを介してアップグレードの失敗をトラブルシューティングするためのデータを収集する際、VDA上のアップグレードエージェントのバージョンを知ることが重要です。VDAアップグレードエージェントのバージョンを確認するには、次のコマンドレットを使用します: `Get-VusComponentVersion -ComponentType VUS`。これにより、すべてのVDAとそのVDAアップグレードエージェントのバージョンが一覧表示されます。

カタログレベルで VDA アップグレードエージェントのバージョンを確認するには、次のスクリプトを使用できます。

> **注:**

> このスクリプトは例として提供されており、特定の環境に合わせて調整する必要がある場合があります。本番環境で使用する前に、スクリプトを十分にテストすることをお勧めします。

```
Param( [Parameter (Mandatory=$true)] [string] $CatalogName ) try { $Uuids = Get-BrokerMachine -CatalogName $CatalogName | Select-Object -Property UUID
```

```
if($Uuids -eq $null) { throw "Cannot find CatalogName " +$CatalogName } Write-Output("Catalog Name passed is "+$CatalogName)
```

```
foreach($Uuid in $Uuids) { $compVersion = Get-VusComponentVersion -MachineId $machine.UUID -ComponentType VUS $Machine = Get-BrokerMachine -UUID $compVersion.MachineId Write-Output(“MachineName: “+ $Machine.MachineName+”, Machine UUID:”+$machine.MachineId+”, VUA Version:”+ $compVersion.Version) } } catch { Write-Output(“Exception Occured”) Write-Host $_ }
```

VDA アップグレードエージェントに関連するログ

VDAアップグレードエージェント（VUA）ログは、アップグレードの失敗やVUAとVDAアップグレードサービス間の通信に関する問題のトラブルシューティングに不可欠な情報を提供できます。収集できるログには次のものがあります。

- Citrix Diagnostic Facility (CDF) トレース。CDFモジュール名は`VdaUpgradeAgent`です。
- Windowsイベントログ。ログは、**イベントビューアー > Windowsログ > アプリケーション > Citrix VDA Upgrade Agent Service** で表示します。

管理者が、トラブルシューティングに不可欠な情報をキャプチャしつつ、ログファイルが大きくなりすぎるのを防ぐローテーションログファイルを有効にできるレジストリ設定があります。ログファイルの合計サイズは20 MBに制限されています。ファイルへのログ記録を有効にするには、次のレジストリキーを作成します。

- **キー:** `HKLM:\SOFTWARE\Citrix\UpdateServices\UpdateAgent\LogToFile`
- **値の名前:** `LogToFile`
- **値の型:** `REG_DWORD`
- **値のデータ:**
  - `0` - ファイルトレース無効
  - `1` - ファイルトレース有効

PowerShell を使用して VDA に LogToFile レジストリキーを作成するには、次のコマンドレットを使用します。

```
New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\UpdateServices\UpdateAgent\LogToFile -Name LogToFile -Value 1 -PropertyType DWord -Force
```

大規模なマシングループに対して LogToFile を有効にするには、グループポリシー設定を使用してすべての VDA 組織単位 (OU) に LogToFile レジストリを作成することを検討してください。

> **注:**
>
> - `LogToFile=1` が設定されている場合、ログはファイルにのみ書き込まれます。CDF トレースには表示されません。
> - レジストリの変更を有効にするには、VDA Upgrade Agent サービスの再起動が必要です
> - ログファイルは C:\ProgramData\Citrix\Update Services\Logs フォルダーに作成されます

VDAアップグレードのダウンロード失敗のトラブルシューティング

VDAアップグレード機能に関連するダウンロードの失敗をトラブルシューティングし、解決するには、以下の手順に従ってください。

1. URL フィルタリングが設定されている場合は、関連する URL が許可リストに追加されていることを確認してください。接続を参照してください。
2. 必要なURLを許可リストに追加した後、VDAアップグレードの再スケジュールを試してください。

CDFトレースを有効にするか、`LogToFile`を`1`に設定して、分析用に詳細なログをキャプチャできます。ダウンロード失敗の問題が解決しない場合は、エラーを確認してください。「Download Failed: This access control list is not in canonical form and therefore cannot be modified」というエラーメッセージが表示された場合、それはフォルダー`C:\ProgramData\Citrix\UpgradeServices\Downloads\VDA`のアクセス許可が正しくないことを示しています。

この問題に対処するには、次のいずれかを実行します。

- **オプション1：** 次のコマンドを使用して、フォルダーのアクセス制御リスト（ACL）をリセットします。（このコマンドは、一致するすべてのファイルのACLをデフォルトの継承されたACLでリセットします。）
    - icacls.exe "C:\ProgramData\Citrix\UpgradeServices\Downloads\VDA" /reset /T /C /L /Q
- **オプション2：** Downloadsの下にあるVDAフォルダーを削除し、VDAアップグレードをスケジュールします。

VDAアップグレード検証の失敗のトラブルシューティング

VDAアップグレード機能に関連するダウンロードの失敗をトラブルシューティングし、解決するには、以下の手順に従ってください。

1. URLフィルタリングが有効になっている場合は、関連するURL、特に失効チェックに必要な証明書失効リスト（CRL）またはオンライン証明書ステータスプロトコル（OCSP）のURLが許可リストに追加されていることを確認してください。VDAアップグレード要件を参照してください。
2. 必要なURLを許可リストに追加した後、VDAアップグレードの再スケジュールを試してください。

分析のために詳細なログをキャプチャするには、CDFトレースを有効にするか、`LogToFile`を`1`に設定することをお勧めします。ログには次のエラーが含まれる場合があります。

- RevocationStatusUnknown
- 失効機能は、証明書の失効ステータスを確認できませんでした。
- 失効サーバーがオフラインだったため、失効機能は失効を確認できませんでした。

VDAアップグレードエージェントは、証明書を検証し、失効チェックを実行するためにWindowsシステムコールに依存しています。上記のエラーは、エージェントがCRLまたはOCSPのURLへの接続を確立できないことを示しています。

Windows CryptoAPIは現在、プロキシ設定をサポートしていません。アウトバウンドCRL呼び出しを容易にするためにVDAプロキシを構成する方法については、プロキシ構成を持つVDAセクションを確認してください。

SDKおよびAPI

このリリースでは、いくつかのSDKとAPIが利用可能です。SDKとAPIにアクセスするには、Build anything with Citrixにアクセスしてください。そこから、**Citrix Workspace**を選択して、Citrix Virtual Apps and Desktopsおよびその関連コンポーネントのプログラミング情報にアクセスします。

> **注:**
>
> Citrix Virtual Apps and Desktops™ SDKおよびCitrix Group Policy SDKは、モジュールまたはスナップインとしてインストールできます。いくつかのコンポーネントSDK（Citrix Licensing、Citrix Provisioning、StoreFrontなど）は、スナップインのみを使用してインストールされます。

> この製品はPowerShellバージョン3から5をサポートしています。

シトリックス バーチャルアプリおよびデスクトップ SDK

このSDKは、Delivery Controller™またはStudioをインストールすると、PowerShellモジュールとして自動的にインストールされます。これにより、スナップインを追加することなく、このSDKのコマンドレットを使用できます。（このSDKをスナップインとしてインストールすることを選択した場合の指示は以下に記載されています。）

権限

Citrix管理権限を持つIDを使用して、シェルまたはスクリプトを実行する必要があります。Controller上のローカル管理者グループのメンバーは、Citrix Virtual AppsまたはCitrix Virtual Desktops™をインストールするための完全な管理権限を自動的に持ちますが、Citrixは、通常の運用では、ローカル管理者アカウントを使用するのではなく、適切な権限を持つCitrix管理者を作成することを推奨します。

コマンドレットにアクセスして実行する

1. PowerShellでシェルを起動します: Studioを開き、**PowerShell**タブを選択し、**Launch PowerShell**をクリックします。
2. スクリプト内でSDKコマンドレットを使用するには、PowerShellで実行ポリシーを設定します。PowerShellの実行ポリシーについては、Microsoftのドキュメントを参照してください。
3. (モジュールではなく) スナップインを使用する場合は、`Add-PSSnapin` (または`asnp`) コマンドレットを使用してスナップインを追加します。

   V1とV2はスナップインのバージョンを示します。XenDesktop 5のスナップインはバージョン1です。Citrix Virtual Apps and Desktops、およびそれ以前のXenDesktop 7バージョンのスナップインはバージョン2です。たとえば、Citrix Virtual Apps and Desktopsスナップインをインストールするには、`Add-PSSnapin Citrix.ADIdentity.Admin.V2`と入力します。すべてのコマンドレットをインポートするには、次のように入力します: `Add-PSSnapin Citrix.*.Admin.V*`

これで、コマンドレットとヘルプファイルを使用できます。

- このSDKのヘルプファイルにアクセスするには、Categoriesリストで製品またはコンポーネントを選択し、次に**Citrix Virtual Apps and Desktops SDK**を選択します。
- PowerShellのガイダンスについては、Windows PowerShell Integrated Scripting Environment (ISE)を参照してください。

グループポリシーSDK

Citrixグループポリシー SDKを使用すると、グループポリシーの設定とフィルターを表示および構成できます。このSDKは、PowerShellプロバイダーを使用して、マシンとユーザーの設定およびフィルターに対応する仮想ドライブを作成します。このプロバイダーは、`New-PSDrive`の拡張機能として表示されます。

Group Policy SDKを使用するには、StudioまたはCitrix Virtual Apps and Desktops SDKのいずれかがインストールされている必要があります。

Citrix Group Policy PowerShell プロバイダーは、モジュールまたはスナップインとして利用できます。

- モジュールを使用する場合、追加の作業は不要です。
- スナップインを追加するには、`Add-PSSnapin citrix.common.grouppolicy` と入力します。

ヘルプにアクセスするには、`help New-PSDrive -path localgpo:/` と入力します。

仮想ドライブを作成し、設定をロードするには、`New-PSDrive <Standard Parameters> [-PSProvider] CitrixGroupPolicy -Controller <string>` と入力します。ここで、Controller 文字列は、接続して設定をロードしたいサイト内の Controller の完全修飾ドメイン名です。

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

Citrix Virtual Apps and Desktops REST APIを使用すると、Citrix Virtual Apps and Desktops展開内のリソースの管理を自動化できます。

Citrix Virtual Apps and Desktops REST APIは`<https://developer.cloud.com/citrixworkspace/citrix-daas-rest-apis/docs/citrix-virtual-apps-and-desktops-apis>`で利用できます。Citrix Virtual Apps and Desktopsに適用されないAPIは、その旨が示されています。そこにあるガイダンスに従って、APIサービスへのアクセスを構成し、APIを使用してリソースを管理および最適化してください。

モニターサービス OData

Monitor APIを使用すると、OData APIのバージョン3または4を使用してMonitor Serviceデータにアクセスできます。Monitor Serviceデータからクエリされたデータに基づいて、カスタマイズされた監視およびレポートダッシュボードを作成できます。OData V.4はASP.NET Web APIに基づいており、集計クエリをサポートしています。

詳細については、Monitor Service OData API を参照してください。

__index__

サイト全体の履歴トレンドを監視する

トレンドビューでは、各サイトの履歴トレンド情報に以下のパラメーターでアクセスできます。

- セッション
- 接続障害
- マシン障害
- ログオンパフォーマンス
- 負荷評価
- キャパシティ管理
- マシン使用状況
- リソース使用率
- 各サイトのネットワーク分析。

この情報を見つけるには、**トレンド**メニューをクリックします。

ズームインしてドリルダウンする機能を使用すると、期間をズームイン（グラフのデータポイントをクリック）し、トレンドに関連する詳細をドリルダウンして表示することで、トレンドチャートをナビゲートできます。この機能により、誰が、または何が影響を受けているかの詳細をよりよく理解できます。

各グラフのデフォルトのスコープを変更するには、データに別のフィルターを適用します。

履歴トレンド情報が必要な期間を選択します。期間の利用可能性は、Directorの展開によって次のように異なります。

- 過去1年間（365日間）のトレンドレポートは、Premiumライセンスサイトで利用できます。
- 過去1か月間（31日間）のトレンドレポートは、Advancedライセンスサイトで利用できます。
- PremiumおよびAdvanced以外のライセンスサイトでは、過去7日間のトレンドレポートが利用できます。

> **注：**

- すべてのDirector展開において、期間が「過去1か月間」（**現在まで**）またはそれより短い期間に設定されている場合、セッション、障害、ログオンパフォーマンスのトレンド情報はグラフおよびテーブルとして利用できます。終了日をカスタム設定した「過去1か月間」または「過去1年間」の期間を選択した場合、トレンド情報はグラフとして利用でき、テーブルとしては利用できません。
- Monitor Serviceのグルーミング保持値は、トレンドデータの可用性を制御します。デフォルト値は、データ粒度と保持で確認できます。Premiumライセンスサイトのお客様は、グルーミング保持を希望する保持日数に変更できます。
- IIS Managerの以下のパラメーターは、選択可能なカスタム終了日の範囲を制御します。ただし、選択された日付のデータ可用性は、測定対象の特定のメトリックに対するグルーミング保持設定によって異なります。

パラメーター	デフォルト値
UI.TrendsLast2HoursRange	3
UI.TrendsLast24HoursRange	32
UI.TrendsLast7DaysRange	32
UI.TrendsLastMonthRange	365

利用可能な傾向

セッションの傾向を表示: セッションタブから、デリバリーグループと期間を選択して、同時セッション数に関する詳細情報を表示します。

セッションの自動再接続列には、セッション内の自動再接続の数が表示されます。セッションの信頼性ポリシーまたは自動クライアント再接続ポリシーが有効な場合、自動再接続が有効になります。エンドポイントでネットワークの中断が発生すると、次のポリシーが有効になります。

- セッションの信頼性が有効になり（デフォルトで3分間）、Citrix Receiver™またはCitrix Workspace™アプリがVDAへの接続を試行します。
- 自動クライアント再接続が3分から5分の間に有効になり、クライアントがVDAへの接続を試行します。

両方の再接続がキャプチャされ、ユーザーに表示されます。この情報は、再接続が発生してからDirector UIに表示されるまでに最大5分かかる場合があります。

自動再接続情報は、中断のあるネットワーク接続の表示とトラブルシューティングに役立ちます。また、シームレスなエクスペリエンスを持つネットワークも分析します。フィルターで選択した特定のデリバリーグループまたは期間の再接続数を表示できます。ドリルダウンでは、セッションの信頼性または自動クライアント再接続、タイムスタンプ、エンドポイントIP、およびWorkspaceアプリがインストールされているマシンのエンドポイント名などの追加情報が提供されます。

デフォルトでは、ログはイベントのタイムスタンプの降順でソートされます。この機能は、Windows向けCitrix Workspaceアプリ、Mac向けCitrix Workspaceアプリ、Windows向けCitrix Receiver、およびMac向けCitrix Receiverで利用できます。この機能には、Delivery Controller™ バージョン7 1906以降、およびVDA 1906以降が必要です。

セッションの再接続の詳細については、「セッション」を参照してください。

ポリシーの詳細については、「クライアント自動再接続ポリシー設定」および「セッションの信頼性ポリシー設定」を参照してください。

自動再接続データがDirectorに表示されない場合があります。その理由は次のとおりです。

- WorkspaceアプリがVDAに自動再接続データを送信していません。
- VDAがモニターサービスにデータを送信していません。
- Delivery Controllerは、対応するセッションがない可能性があるため、VDAペイロードを破棄します。

> **注:**
>
> 場合によっては、特定のCitrix Gatewayポリシーが設定されていると、クライアントIPアドレスが正しく取得されないことがあります。

> **接続障害の傾向を表示:** 「障害」タブから、接続、マシンタイプ、障害タイプ、デリバリーグループ、および期間を選択して、サイト全体のユーザー接続障害に関する詳細情報を含むグラフを表示します。

マシン障害の傾向を表示: Single-session OS Machine FailuresタブまたはMulti-session OS Machinesタブから、障害タイプ、デリバリーグループ、および期間を選択すると、サイト全体のマシン障害に関する詳細情報を含むグラフが表示されます。

ログオンパフォーマンスの傾向を表示: ログオンパフォーマンスタブから、デリバリーグループと期間を選択して、サイト全体のユーザーログオン時間とVDAログオン時間の期間、およびログオン数がパフォーマンスに影響するかどうかに関する詳細情報を含むグラフを表示します。このビューには、ブローカリング期間やVM起動時間など、ログオンフェーズとVDA期間フェーズの平均期間も表示されます。このデータは、ユーザーログオンとVDAログオンに特化したものであり、切断されたセッションから再接続しようとしているユーザーは含まれません。 グラフの下の表には、ユーザーセッションごとのログオン期間が表示されます。表示する列を選択し、任意の列でレポートを並べ替えることができます。これらのレポートを.CSVファイルまたはPDFにエクスポートすることもできます。グラフもこれらのレポートにエクスポートされます。詳細については、ユーザーログオンの問題の診断を参照してください。

負荷評価の傾向を表示: Load Evaluator Indexタブから、Multi-session OSマシン間で分散される負荷に関する詳細情報を含むグラフを表示します。このグラフのフィルターオプションには、デリバリーグループまたはデリバリーグループ内のMulti-session OSマシン、Multi-session OSマシン（デリバリーグループ内のMulti-session OSマシンが選択されている場合にのみ利用可能）、および範囲が含まれます。

ホストされたアプリケーションの使用状況を表示: この機能の利用可能性は、組織のライセンスによって異なります。 **Capacity Management**タブから、**Hosted Applications Usage**タブを選択します。デリバリーグループと期間を選択すると、ピーク時の同時使用状況を示すグラフと、アプリケーションベースの使用状況を示す表が表示されます。Application Based Usage表から、特定のアプリケーションを選択して詳細と、そのアプリケーションを使用している、または使用したユーザーのリストを確認できます。

シングルセッションおよびマルチセッションOSの使用状況を表示: 「傾向」ビューには、サイト別およびデリバリーグループ別のシングルセッションOSの使用状況が表示されます。**「サイト」**を選択すると、デリバリーグループごとの使用状況が表示されます。デリバリーグループを選択すると、ユーザーごとの使用状況が表示されます。 「傾向」ビューには、サイト別、デリバリーグループ別、およびマシン別のマルチセッションOSの使用状況も表示されます。**「サイト」**を選択すると、デリバリーグループごとの使用状況が表示されます。デリバリーグループを選択すると、マシンごとおよびユーザーごとの使用状況が表示されます。マシンが選択されている場合、ユーザーごとの使用状況が表示されます。

仮想マシンの使用状況を表示: **「マシン使用状況」**タブから、**「シングルセッションOSマシンまたはマルチセッションOSマシン」**を選択して、VM使用状況のリアルタイムビューを取得し、サイトのキャパシティニーズを迅速に評価できるようにします。 シングルセッションOSの可用性 - サイト全体または特定のデリバリーグループの可用性別に、シングルセッションOSマシン（VDI）

の現在の状態を表示します。 マルチセッションOSの可用性 - サイト全体または特定のデリバリーグループの可用性別に、マルチセッションOSマシンの現在の状態を表示します。

表示されるバナーの次のリンクをクリックすると、**コスト最適化**によるマシン使用状況の可視性を高めることができます。

- 推定節約額 - このリンクをクリックすると、**コスト最適化**ページの**推定節約額**セクションに移動し、すべてのデリバリーグループの詳細が表示されます。
- 節約レポート - このリンクをクリックすると、**コスト最適化**ページの**節約レポート**セクションに移動し、すべてのデリバリーグループの詳細が表示されます。

> **注:**
>
> 「利用可能なカウンター」に表示されるマシンの数には、メンテナンスモードのマシンが含まれます。

> 「**リソース使用率の表示: リソース使用率**タブから、**シングルセッションOSマシンまたはマルチセッションOSマシン**を選択して、CPUとメモリ使用量、IOPSとディスク待機時間に関する履歴トレンドデータを各VDIマシンについて取得し、より適切なキャパシティプランニングに役立てます。 この機能には、Delivery ControllersおよびVDAs **バージョン7.11**以降が必要です。 グラフには、平均CPU、平均メモリ、平均IOPS、ディスク待機時間、およびピーク時の同時セッションのデータが表示されます。マシンにドリルダウンして、CPUを消費している上位10個のプロセスのデータとグラフを表示できます。」

「デリバリーグループと期間でフィルターします。CPU、メモリ使用量、およびピーク時の同時セッションのグラフは、過去2時間、24時間、7日間、1か月、1年間で利用できます。平均IOPSとディスク待機時間のグラフは、過去24時間、1か月、1年間で利用できます。バナーの**Check out**リンクをクリックすると、コスト最適化によりマシンの使用状況をより詳細に把握できます。このリンクをクリックすると、**コスト最適化**ページの**ワークロードの適正化**タブに移動し、**リソース使用率**タブから選択したデリバリーグループの詳細が表示されます。」.

> 「**注:**」:

> - 「履歴マシン使用率ページの「上位10プロセス」テーブルでデータを収集して表示するには、監視ポリシー設定の**プロセス監視を有効にする**を**許可**に設定する必要があります。このポリシーは、デフォルトで**禁止**に設定されています。すべてのリソース使用率

データはデフォルトで収集されます。これは、**リソース監視を有効にする**ポリシー設定を使用して無効にできます。グラフの下のテーブルには、マシンごとのリソース使用率データが表示されます。詳しくは、「監視ポリシー設定」を参照してください。」.

- 「平均IOPSは日次平均を示します。ピークIOPSは、選択した期間のIOPS平均の最高値として計算されます。（IOPS平均とは、VDAで1時間中に収集されたIOPSの時間平均です）。」.
- 「マシンのドリルダウンでは、平均CPUまたは平均メモリ使用量が1%を超えるプロセスが一覧表示されます。これは、場合によっては10個未満のプロセスしか表示されない可能性があることを意味します。」.

「**ネットワーク分析データの表示:** この機能の可用性は、組織のライセンスと管理者権限によって異なります。この機能には、Delivery Controllers **バージョン7.11**以降が必要です。」.

「**ネットワーク**タブから、ネットワーク分析を監視します。これにより、ネットワークのユーザー、アプリケーション、およびデスクトップのコンテキストビューが提供されます。この機能により、DirectorはCitrix ADMからのHDX Insightレポートを通じて、展開におけるICAトラフィックの高度な分析を提供します。詳しくは、「ネットワーク分析の構成」を参照してください。」

アプリケーション障害の表示: アプリケーション障害タブには、VDA上の公開アプリケーションに関連する障害が表示されます。

「この機能には、Delivery ControllersおよびVDAs **バージョン7.15**以降が必要です。Windows Vista以降を実行するシングルセッションOS VDA、およびWindows Server 2008以降を実行するマルチセッションOS VDAがサポートされています。 詳しくは、「履歴アプリケーション障害監視」を参照してください。」

デフォルトでは、マルチセッションOS VDAからのアプリケーション障害のみが表示されます。監視ポリシーを使用して、アプリケーション障害の監視を設定できます。詳細については、「監視ポリシー設定」を参照してください。

プローブ結果の表示: プローブ結果タブには、構成ページでプローブ用に構成されたアプリケーションおよびデスクトップのプローブ結果が表示されます。ここでは、障害が発生した起動の段階が記録されます。

詳しくは、「アプリケーションおよびデスクトップのプローブ」を参照してください。

カスタマイズされたレポートの作成: カスタムレポートタブは、監視データベースからリアルタイムおよび履歴データを表形式で含むカスタムレポートを生成するためのユーザーインターフェイスを提供します。

「この機能には、Delivery Controllers **バージョン7.12**以降が必要です。」.

以前に保存したカスタムレポートクエリのリストから、「**実行してダウンロード**」をクリックしてレポートをCSV形式でエクスポートしたり、「**ODataをコピー**」をクリックして対応するODataクエリをコピーして共有したり、「**編集**」をクリックしてクエリを編集したりできます。 マシン、接続、セッション、またはアプリケーションインスタンスに基づいてカスタムレポートクエリを作成できます。マシン、デリバリーグループ、または期間などのフィールドに基づいてフィルター条件を指定します。カスタムレポートに必要な追加の列を指定します。プレビューにはレポートデータのサンプルが表示されます。カスタムレポートクエリを保存すると、保存済みクエリのリストに追加されます。

コピーしたODataクエリに基づいてカスタムレポートクエリを作成できます。これを行うには、「ODataクエリ」オプションを選択し、コピーしたODataクエリを貼り付けます。結果のクエリは後で実行するために保存できます。

注:

ODataクエリを使用して生成されたプレビューおよびエクスポートレポートの列名はローカライズされておらず、英語で表示されます。

グラフ上のフラグアイコンは、特定の期間における重要なイベントまたはアクションを示します。フラグにマウスを重ねてクリックすると、イベントまたはアクションが一覧表示されます。

注:

- HDX™接続ログオンデータは、7より前のVDAでは収集されません。それより前のVDAの場合、グラフデータは0として表示されます。
- Citrix Studioで削除されたデリバリーグループは、関連データが整理されるまで、Directorトレンドフィルターで選択できます。削除されたデリバリーグループを選択すると、保持期間までの利用可能なデータのグラフが表示されます。ただし、テーブルにはデータが表示されません。
- アクティブなセッションを含むマシンをあるデリバリーグループから別のデリバリーグループに移動すると、新しいデリバリーグループの「**リソース使用率と負荷評価イン**

> **デックス**」テーブルに、古いデリバリーグループと新しいデリバリーグループから統合されたメトリックが表示されます。

Azureワークロードのコストモデリング

新しいコストモデリング機能はAzureワークロードをサポートし、使用パターンに基づいて推奨事項を提供します。顧客は、Azure ReservationsまたはSavings Planのどちらが最大のコスト削減に最も適しているかについて推奨事項を受け取ります。Azure Reservationsの顧客は、割引された定額料金で特定の数のマシンを事前に予約しますが、Savings Planでは、割引料金のためにドル額をコミットできます。この機能は、過去28日間のデータを分析して推定推奨事項を提供します。これにより、顧客はリソース割り当てについて情報に基づいた決定を下すことでコストを節約できます。

> **注:**
>
> 最適な推定値を得るには、過去28日間の安定した環境からのデータを使用することをお勧めします。休暇や急激な使用量の増加など、異常なアクティビティ期間のデータは使用しないでください。使用量がベースラインレベルに戻るまで待ってから、これらの推奨事項を適用してください。

> **利点:**

- カスタマイズされたコスト削減の推奨事項を提供します。
- 予約プランとSavings Planの両方をサポートします。
- 正確な洞察のために、最近の使用データを分析します。
- リソース割り当てを最適化し、費用を削減するのに役立ちます。
- デリバリーグループ、タグ、VMシリーズ、およびリージョンの選択において柔軟性を提供します。

> **注:**
>
> コストモデリングはAzureワークロードのみでサポートされています。

プランの種類

Azureには、コストを節約するための2種類のプランがあります。

- **Azure Reservations**: 顧客は、事前に予約するマシンの数を決定します。予約は、従量課金制のコストと比較して、割引料金で異なる定額コストがかかります。
- **Savings Plan**: お客様は、マシンの数ではなく、特定の金額をコミットします。その金額が消費されるまで、割引料金が請求されます。その後は、従量課金制の料金を支払います。

コストモデリングページには、各プランの推奨事項が個別に表示され、潜在的な節約額が示されます。

コスト最適化 > コストモデリングをクリックします。**コストモデルとクラウドワークロード**ページが表示されます。

citrix | DaaS Premium | 0 - Production

DaaS > Monitor > Cost optimization

Try unified search | Search | 1 - Production

Cost optimization New

Cost summary | Cost savings | Workload rightsizing | Cost modeling

Export data

Cost model cloud workloads

We recommend that you filter only by long-term-use machines and production workloads. Delivery groups and machines used for testing or short-term use may skew the cost model results.

All delivery groups | Select tag | All VM series | All regions

Apply filters | Note: All filters are applied with **AND** operator

Data up to 04/03/2025 9:56 AM | Download report

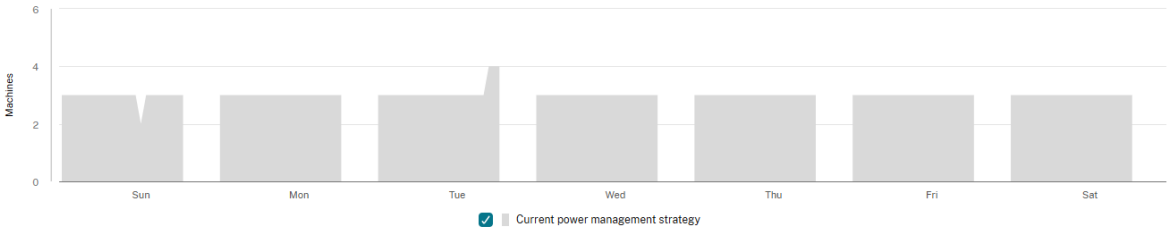
Cost model based on power management strategy

Choose from various Autoscale power management strategies to visualize concurrent machine consumption and savings opportunities.

No changes to Autoscale	Potential changes to Autoscale	
Current power management strategy Analyze potential savings opportunities by utilizing the existing Autoscale configuration.	**Deallocate machines at session end** Analyze potential savings opportunities if Autoscale is configured to deallocate machines at the end of a user's session. **95.45% reduced machine consumption**	**Deallocate machines for inactive session** Analyze potential savings opportunities if Autoscale is configured to deallocate machines when a session is inactive. **99.01% reduced machine consumption**

Concurrent machine consumption

Concurrent machine consumption is analyzed based on the last 28 days of historical consumption.



Savings opportunity

Determine the best commitment strategy and term length based on the selected power management strategy. View cost analysis

	Reserved instances		Savings plan	
	1 year	3 year	1 year	3 year
Potential savings opportunity	**40 %** Save up to $2,717.07 / yr	**61 %** Save up to $4,142.95 / yr	**31 %** Save up to $2,074.39 / yr	**53 %** Save up to $3,570.76 / yr
Commitment	$3,978.07 / yr	$2,552.20 / yr	$4,620.75 / yr	$3,124.39 / yr
Pay as you go	$72.58 / yr	$72.58 / yr	$72.58 / yr	$72.58 / yr
Total	**$4,050.65 / yr**	**$2,624.78 / yr**	**$4,693.33 / yr**	**$3,196.97 / yr**

Recommendations

Review the recommended changes to your commitment strategy based on the term length.

			Machines to be reserved		Savings plan hourly commitment (USD)	
Virtual machine series	Region	Current machines	1 year	3 year	1 year	3 year
Standard_D4s_v3	eastus	727	2	2	$0.26 / hr	$0.18 / hr
Standard_D8as_v4	eastus	21	1	1	$0.26 / hr	$0.18 / hr

Analyze per virtual machine series

Validate the optimum number of machines required per series by correlating with respective cost per user.

Virtual machine series

Standard_D4s_v3 in eastus

Export analysis



必要に応じて、すべてのデリバリーグループ、最大15個（または実際の数）のデリバリーグループを選択したり、最大15個（または実際の数）のデリバリーグループを除外したりできます。ドロップダウンリストから**すべてのシングルセッション**または**すべてのマルチセッション**を選択できます。また、**タグ**、**VMシリーズ**、**リージョン**でフィルタリングすることもできます。オプションを何も選択しない場合、分析はデフォルトで、過去28日間のデータを考慮して、適用可能なデータセット全体に対して実行されます。

> **注:**
>
> コストモデリングの推奨事項は、過去28日間のデータに基づいており、この期間中の動作が一貫していることを前提としています。

電源管理戦略

データ分析は、選択した電源管理戦略によって異なります。同時実行マシンの消費量と節約の機会を視覚化するために、次のAutoscale™電源管理戦略のいずれかを選択できます。

- **現在の電源管理戦略**: 既存のAutoscale構成を使用して潜在的な節約を分析するには、この戦略を選択します。Autoscale構成に変更はありません。推奨されるコストモデリングは、現在のAutoscale設定に基づいて生成され、稼働中のすべてのマシンのコストを計算します。
- **セッション終了時にマシンを割り当て解除する**: ユーザーセッションの終了時にマシンを割り当て解除するようにAutoscale構成を変更して潜在的な節約を分析する場合は、この戦略を選択します。推奨されるコストモデリングは、更新されたAutoscale構成に基づいて生成され、アクティブなセッション時間のみのコストを計算し、切断時間は無視します。
- **非アクティブなセッションのマシンを割り当て解除する**: セッションが非アクティブなときにマシンを割り当て解除するようにAutoscale構成を変更して潜在的な節約を分析する場合は、この戦略を選択します。推奨されるコストモデリングは、更新されたAutoscale構成に基づいて生成され、セッションがアクティブでアイドル状態ではない時間のみのコストを計算します。

たとえば、マシンが60分間稼働し、セッションが20分間切断された場合、残りの40分がアクティブなセッション時間です。アクティブなセッション中にユーザーが10分間アイドル状態だった場合、正味使用時間は30分のみです。

- **現在の電源管理戦略**では、正味使用時間は60分です。
- **セッション終了時にマシンを割り当て解除する戦略**では、切断時間を除いた正味使用時間は40分です。

- 「**非アクティブセッション戦略のマシンの割り当て解除**」では、アイドル時間を含め、正味使用時間は30分です。

これらの基準は分析のベースラインとして機能します。これらの戦略は、マシンの正味使用量をより正確に判断するのに役立ちます。

マシンの消費量と推奨事項

コストモデリングページには、マシンの消費量と推奨事項に関する次の詳細が記載されています。

- **同時マシン消費グラフ**: このグラフは、過去28日間のベースライン使用状況を表示し、各バーは曜日を表します。ベースラインは、平均や中央値と同様の集計メトリックである使用量の75パーセンタイル (p75) を使用して計算されます。たとえば、火曜日の午前10時など、各曜日と時間について、ベースラインは過去4回の火曜日の午前10時のデータのp75を分析することによって決定されます。このプロセスは、週のすべての時間と曜日について繰り返されます。グラフにカーソルを合わせると、現在の電源管理戦略と、Autoscaleへの潜在的な変更が適用された場合の選択された戦略の下で消費されたマシンの数が表示されます。
- **節約の機会**: Azure ReservationsとSavings Plansの両方について、1年間および3年間の潜在的な節約の機会を表示します。「**コミットメント**」と「**従量課金制**」オプションの節約の機会が表示されます。
- **推奨事項**: Azure ReservationsとSavings Plansの両方に対する推奨される変更を表示します。推奨事項には、仮想マシンシリーズ、タイプ、リージョンのすべての該当する組み合わせについて、各プランのコミットメントが含まれます。データは1年間および3年間の期間で利用できます。

仮想マシンシリーズごとの分析

ドロップダウンリストから仮想マシンシリーズを選択して、ユーザーあたりのコストに関して最適なマシン数を検証します。月あたりのユーザーあたりのコストは、予測される月あたりのユーザーあたりのコストの見積もりです。この見積もりは、お客様がAzure Reservationsで特定数のマシンを予約した場合、または**Savings Plan**で特定の時間あたりのドル額をコミットした場合の、予測される月あたりのユーザーあたりのコストを理解するのに役立ちます。Azure Reserved InstancesおよびSavings Planの時間あたりのコミットメントのユーザーあたりのコストを表示します。グラフには、さまざまな予約レベル（**予約なし**から**完全予約**まで、**最適な予約**を含む）および時間あたりのコストコミットメントレベル（**コミットメントなし**から**最大コミットメント**まで、**最適なコミットメント**を含む）のデータポイントが表示されます。

コストモデリングページは、お客様がAzureワークロードを最適化し、コストを節約するのに役立つ貴重な洞察と推奨事項を提供します。使用パターンを分析し、適切なプランを選択することで、お客様は大幅な節約を実現できます。

Citrix Infrastructure Monitor の自動接続

新しい自動接続機能は、以下の手順を自動的に実行することで、オンボーディングプロセスを簡素化します。

- Citrix Infrastructure Monitor のダウンロードとインストール
- 接続の検証

自動接続では、コンポーネントの詳細を手動で追加するだけで済みます。手動接続プロセスは変更されておらず、ユーザーはエージェントをダウンロードし、ターゲットマシンにインストールして、必要な詳細情報を提供する必要があります。

この変更に対応するため、UI には以下の2つのタブが追加されました。

- 自動接続
- 手動接続

自動接続プロセスには、資格情報を入力する前にすべての前提条件が満たされていることを確認するためのチェックボックスが含まれています。

自動接続の目的は、ユーザーにとってオンボーディングプロセスを可能な限りシームレスにすることです。

前提条件

Director UI からマシンに Citrix Infrastructure Monitor サービスをリモートでインストールできます。Director UI からのリモートインストールには、Provisioning Service および StoreFront™ マシンに対して以下が必要です。

- Citrix Infrastructure Monitor がインストールされるターゲットマシンで、ローカル管理者権限が必要です。
- ターゲットマシンで WMI が利用可能である必要があります。ファイアウォールで WMI が許可されていることを確認してください。詳細については、「Setting up a Remote WMI Connection」を参照してください。
- ターゲットマシンで RPC が利用可能である必要があります。管理共有 (Admin$ および C$) は、Delivery Controller™ マシンからアクセスできる必要があります。

- ターゲットマシンには、解決可能なDNSホスト名が必要です。

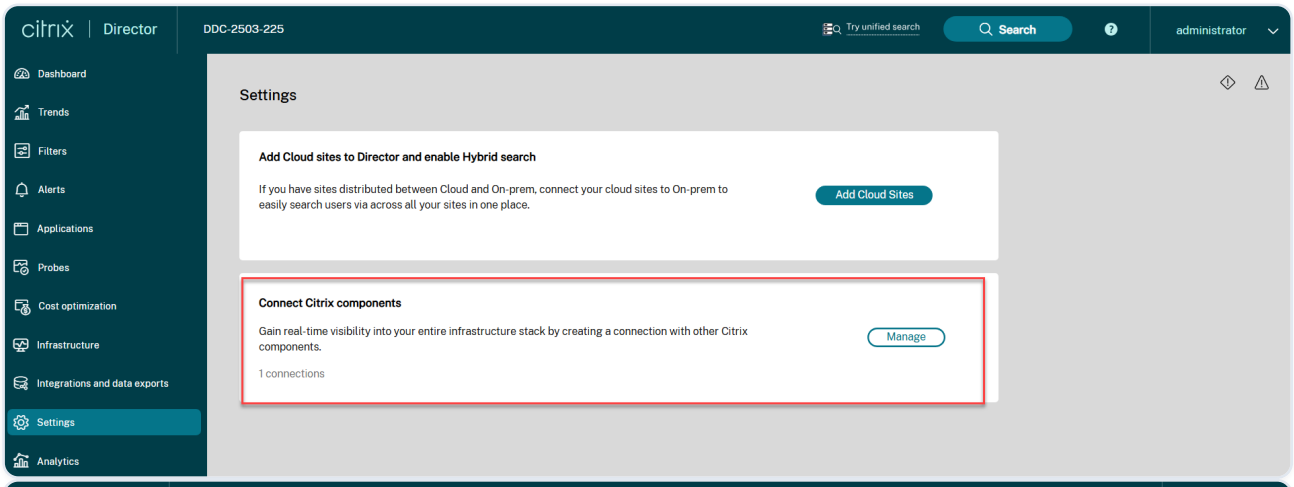
これらの要件が環境で満たせない場合は、「Citrix Infrastructure Monitor の手動オンボーディング」を参照してください。

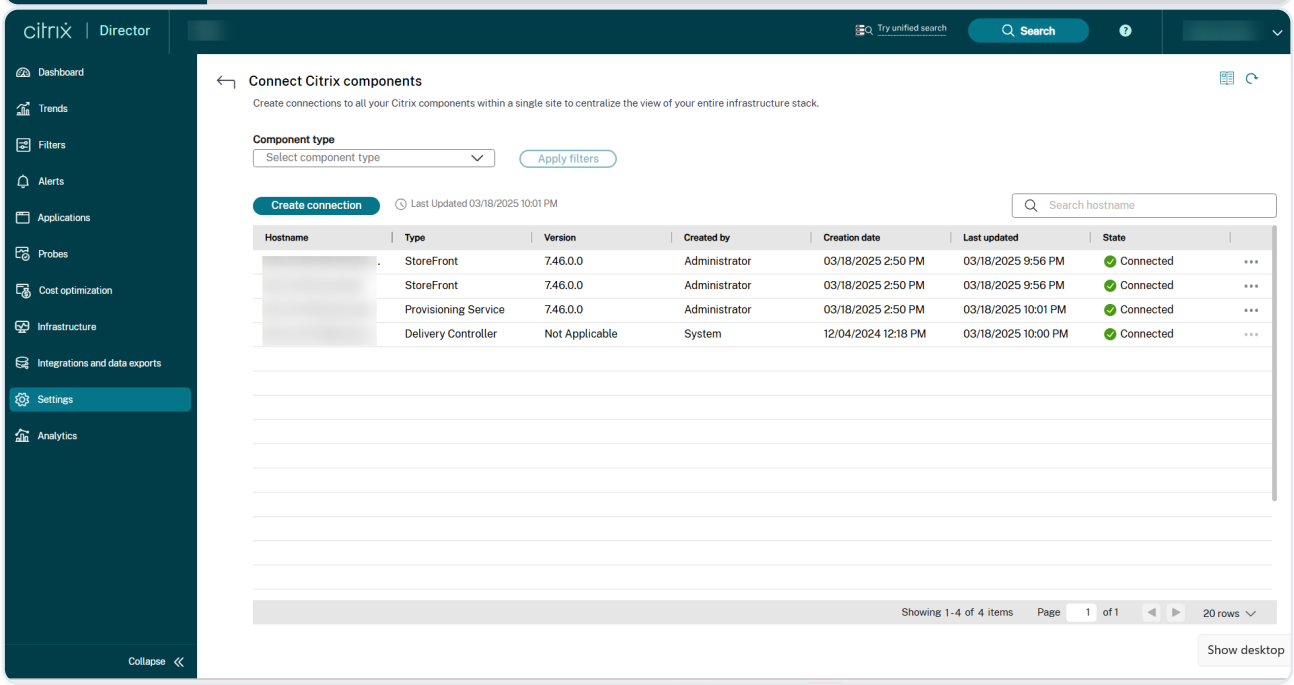
Citrix Infrastructure Monitor を自動的に登録する

Director UI を使用して Citrix Infrastructure Monitor を登録できます。次の手順で Director UI で登録を完了します。

ステップ 1: Citrix コンポーネントの接続ページに移動する

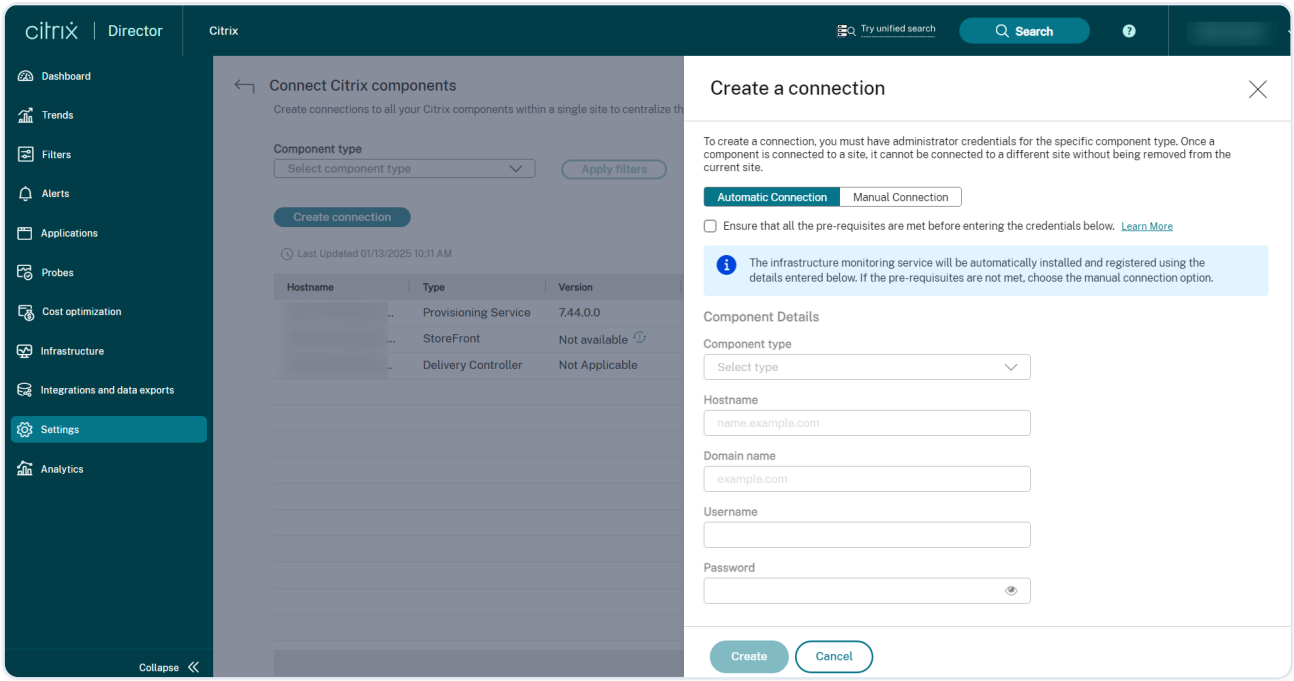
［設定］ > ［Citrix コンポーネントの接続］ > ［管理］ をクリックします。





ステップ 2: コンポーネントの詳細を入力する

［Citrix コンポーネントの接続］画面で、**［接続の作成］** をクリックします。**［接続の作成］** ウィンドウが表示されます。デフォルトでは、**［自動接続］** タブが強調表示されています。



セキュリティで保護された接続を確立するために必要なコンポーネントの詳細を入力します。

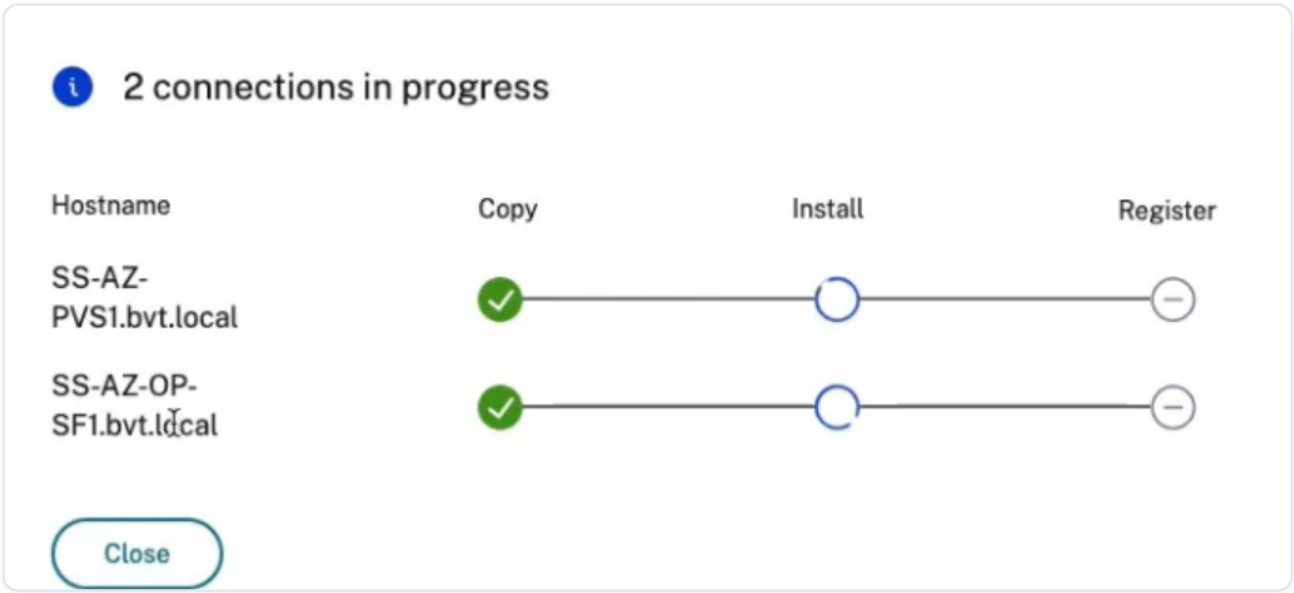
- ドロップダウンリストからコンポーネントの種類を選択します。コンポーネントは Provisioning Service または StoreFront です。
- ホスト名を入力します。
- ドメイン名を入力します。
- Provisioning Service または StoreFront マシンのユーザー名を入力します。
- Provisioning Service または StoreFront マシンのパスワードを入力します。

インフラストラクチャ監視サービスは、上記の詳細情報を使用して自動的にインストールおよび登録されます。

ステップ 3: 接続を作成する

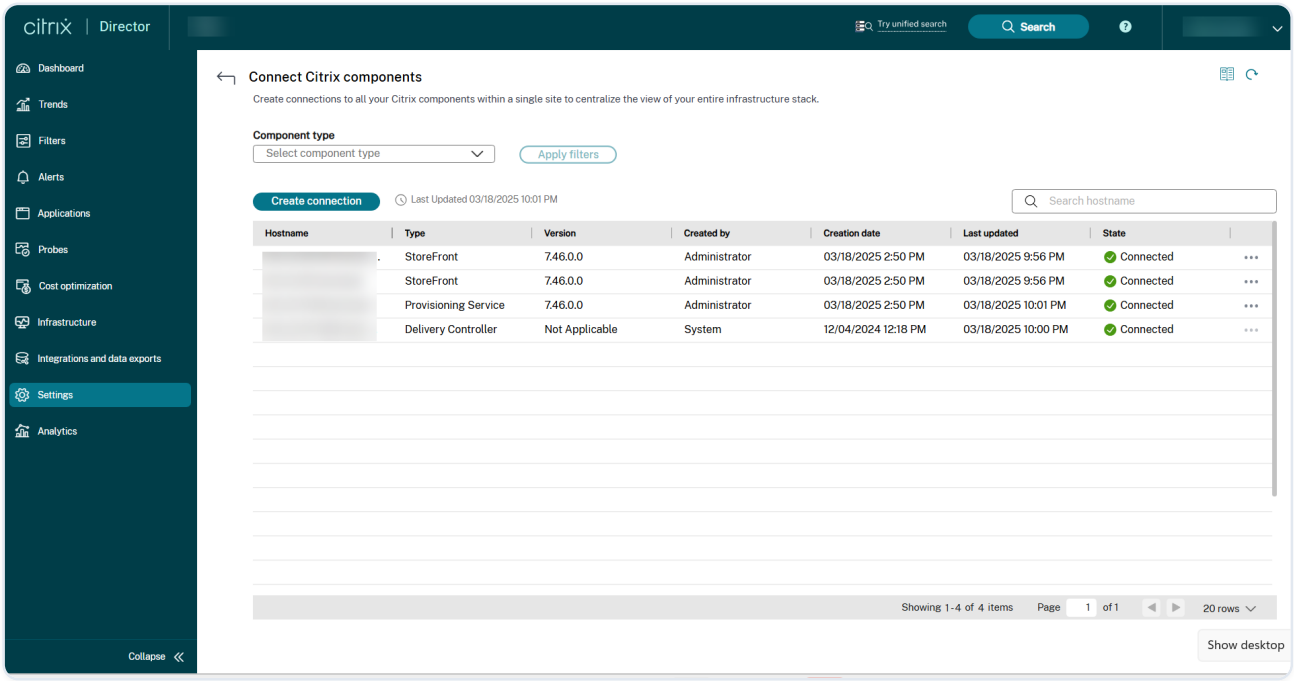
詳細が入力されたら、**作成**をクリックします。リクエストが承認される前に、特定の事前チェックが実行されます。これらのチェックは、続行する前に前提条件が満たされていることを検証します。前提条件が満たされると、自動接続プロセスは、コピー、インストール、登録の各ステップを示すプログレスバーを表示します。いずれかのステップが失敗した場合、ユーザーには再試行オプションが表示されます。

自動接続プロセスの詳細を表示するには、**詳細を表示**をクリックします。



MSIファイルはダウンロードされ、インストール場所にコピーされた後、インストールおよび登録されます。完了すると、作成された接続は「Citrixコンポーネントの接続」ページの接続リストで利用可能になります。

接続が失敗した場合は、接続を再試行できます。再試行するには、管理者資格情報を提供する必要があります。



エラー処理

システムは前提条件の事前チェックを実行し、いずれかのチェックが失敗した場合はエラーメッセージを表示します。

> **注:**

事前チェックは特定の順序で実行されます。たとえば、WMI エラーをチェックするには、資格情報が正しい必要があります。

次の表に、エラーメッセージと対応する解決策を示します。

エラーシナリオ	説明
無効な FQDN 形式	FQDN形式が無効です。この問題を解決するには、FQDN形式を修正してください。
到達不能なFQDN	FQDNマシンに到達できません。
無効な資格情報	ユーザー名またはパスワードが無効です。
リモートマシンでHTTPSが設定されていません。	モニター構成でHTTPSが有効になっているにもかかわらず、リモートマシンでHTTPSを有効にするための環境変数が設定されていません。この問題を解決するには、**System Properties** > **Advanced** > **Environment Variables** > **Edit system variable** で値を設定してください。
リモートマシンでHTTPSが誤って設定されています	モニター構成でHTTPSが無効になっているにもかかわらず、リモートマシンでHTTPSを有効にするための環境変数が設定されています。この問題を解決するには、**System Properties** > **Advanced** > **Environment Variables** > **Edit system variable** の値を削除してください。
リモートマシンでWindows Management Instrumentation (WMI) がブロックされています。	Windowsファイアウォールディフェンダーの WMIに対する**Allowed apps and features**セクションのチェックボックスが選択されていません。この問題を解決するには、WMIがファイアウォールを介してアクセスできることを確認してください。
リモートマシンでSMBポートがブロックされています。	ポート445は、Delivery Controllerからのインバウンドtcp接続に対して有効にする必要があります。

エラーシナリオ	説明
リモートマシンでAdmin Shareが無効になっています	自動接続の前提条件が満たされていません。

アップグレードプロセス

Citrix Infrastructure Monitor の以前のバージョンを使用している場合、アップグレードするオプションがあります。これは、Provisioning Service と StoreFront にのみ適用されます。自動アップグレードでは、進行状況バーが表示され、管理者資格情報が必要です。

アップグレードプロセス(/en-us/citrix-virtual-apps-desktops/2503/media/upgrade-auto.png)

自動または手動でアップグレードを選択できます。

アップグレードのプロンプトは、新しいバージョンが利用可能な場合にのみ表示されます。アップグレードに登録は不要です。アップグレード後、最新バージョンが反映されるまで約5分かかります。

Citrix Infrastructure MonitorのHTTPSを構成する手順

> **注記：**
>
> Citrix Infrastructure Monitor サービスは HTTP モードでも動作し、この場合、以下の構成は不要です。ただし、HTTPS モードでの使用をお勧めします。Citrix Infrastructure Monitor の HTTPS を構成する必要がある場合にのみ、以下の手順を実行してください。

ステップ1：証明書をマシンにアップロードする

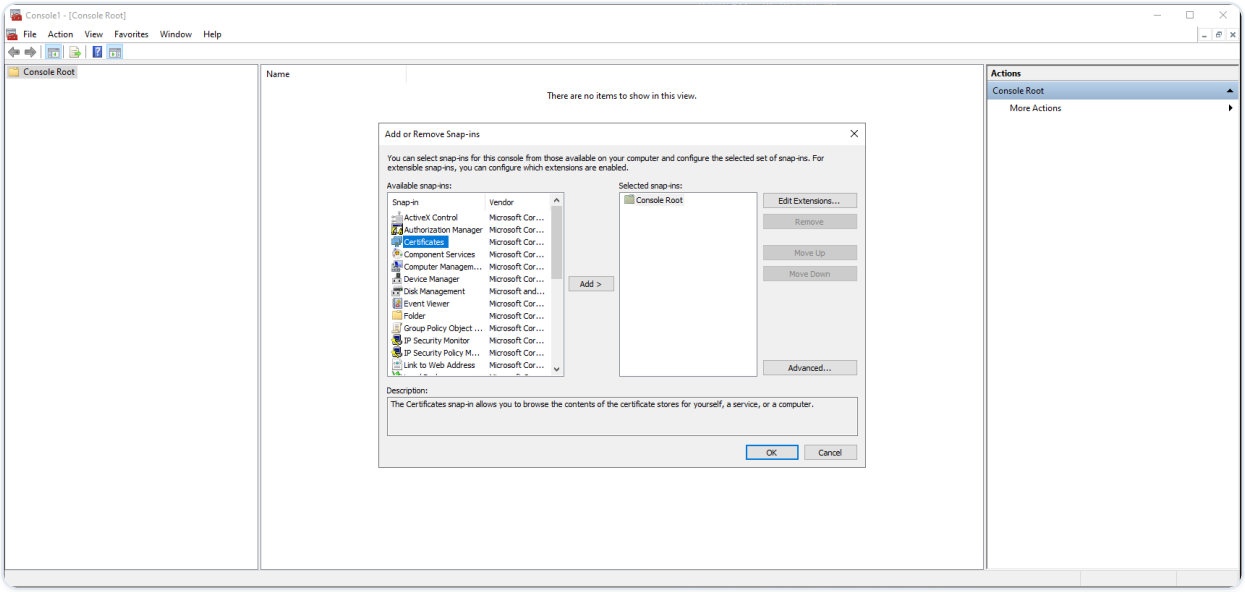
1. Citrix Infrastructure Monitor がインストールされているマシン用の `PFX` 証明書を取得します。PFX ファイルの生成の詳細については、「PFX ファイルを作成する方法」を参照してください。

   > **注記：**
   >
   > パスワードで保護されたPFXファイルも使用できます。

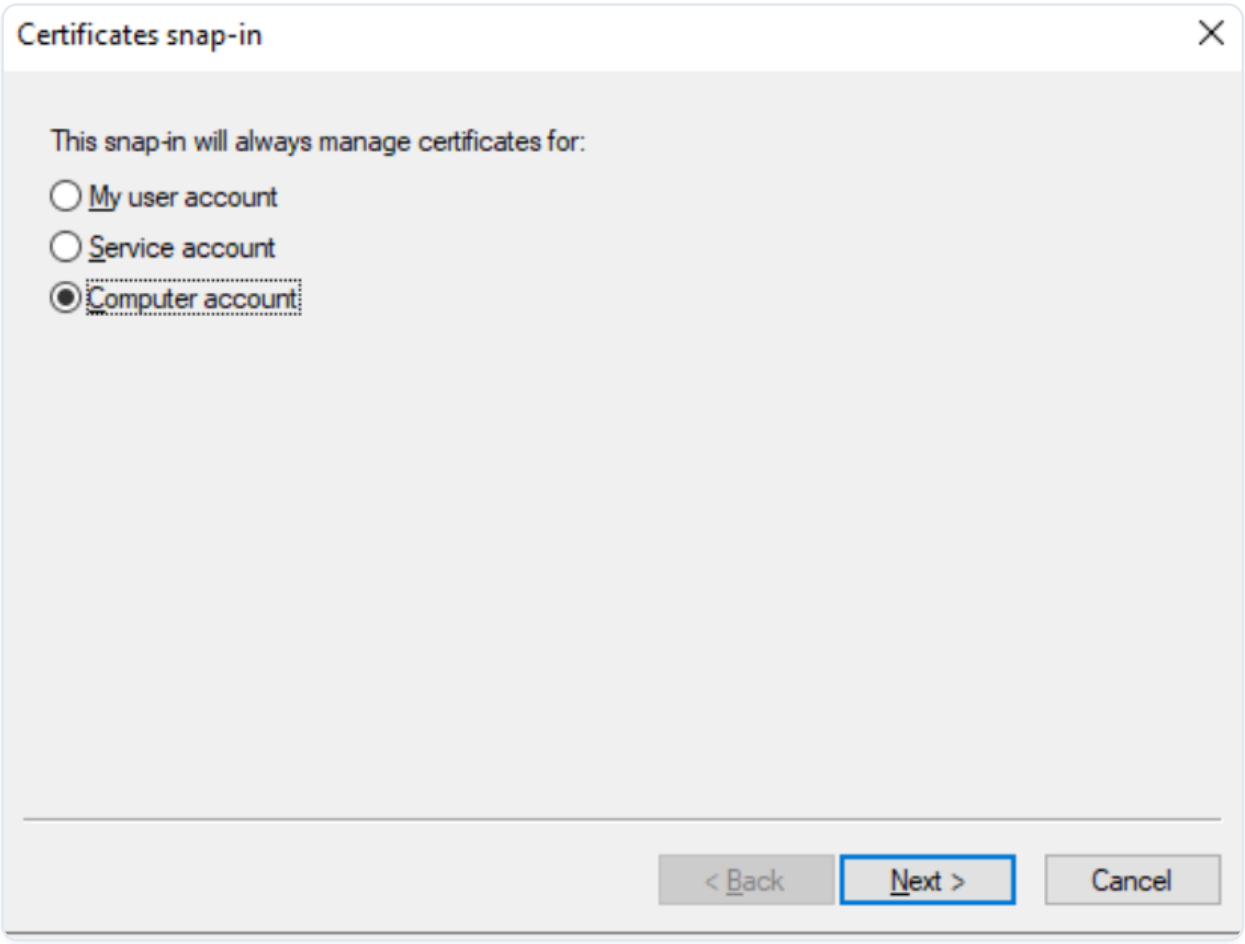
2. 証明書をマシンの任意の場所にアップロードします。

ステップ2：証明書をコンピューター証明書にインポートする

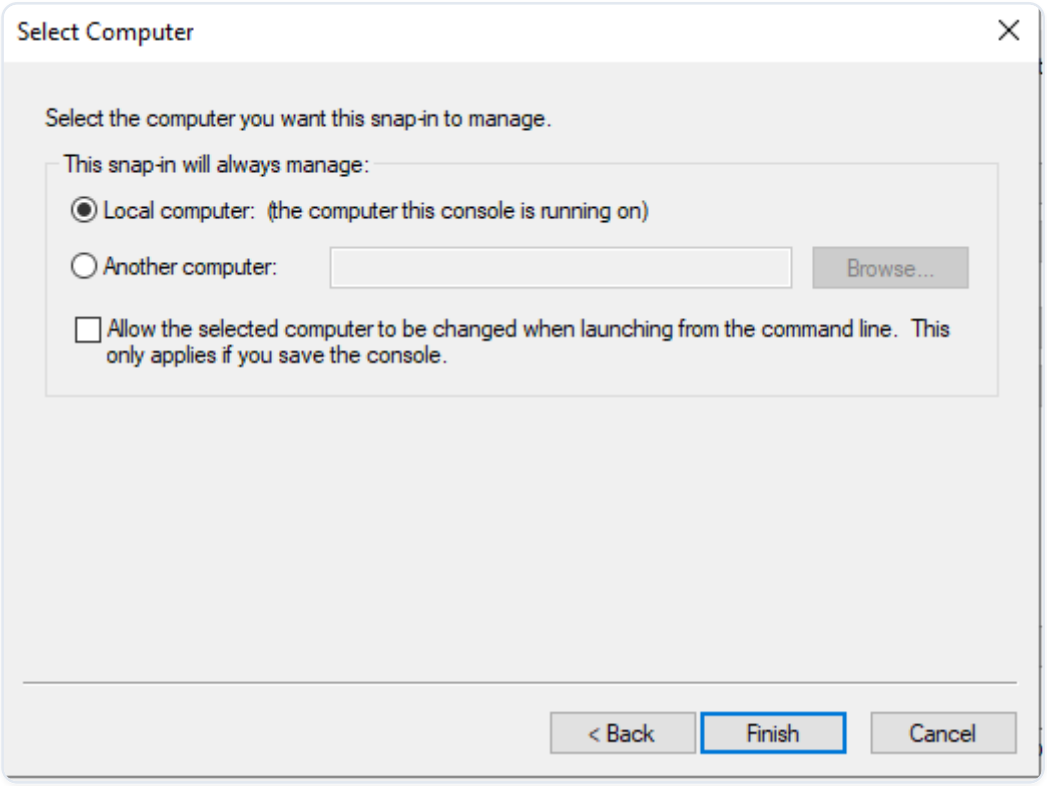
1. **スタート** > **ファイル名を指定して実行**をクリックし、`mmc`と入力して**OK**をクリックします。**コンソール1 - **ウィンドウが表示されます。
2. **ファイル**メニューで、**スナップインの追加と削除**をクリックします。**スナップインの追加と削除**ウィンドウが表示されます。



3. 「**スナップイン**」の下で、「**証明書**」をダブルクリックします。「**証明書スナップイン**」ウィンドウが表示されます。

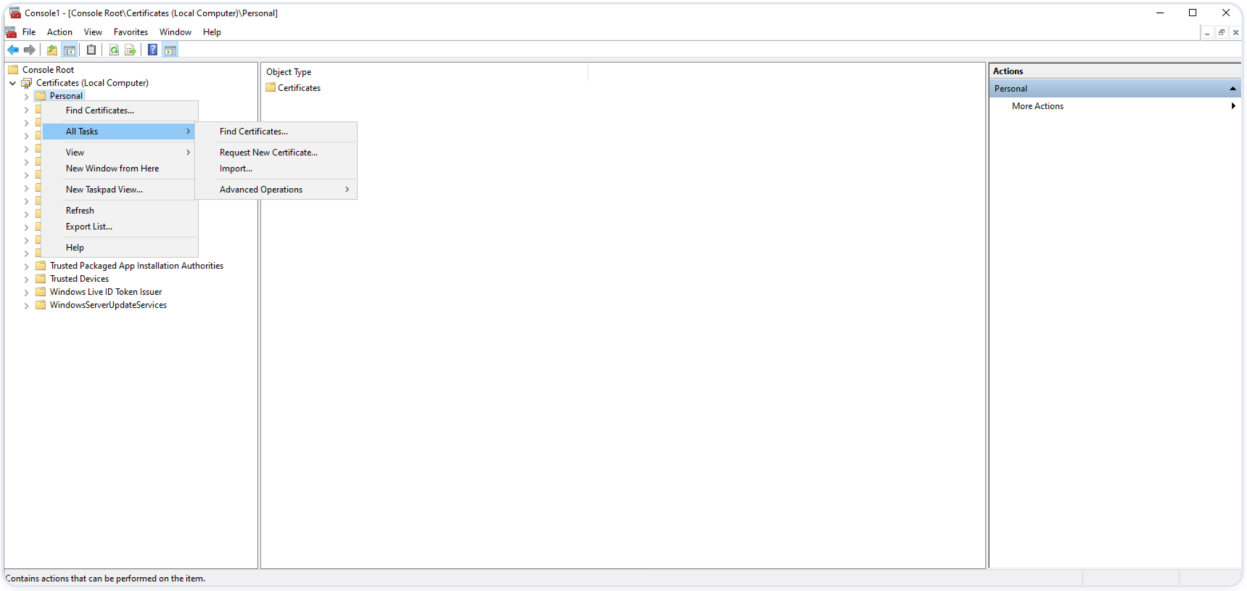


4. 「**コンピューターアカウント**」を選択し、「**次へ**」をクリックします。「**コンピューターの選択**」ウィンドウが表示されます。

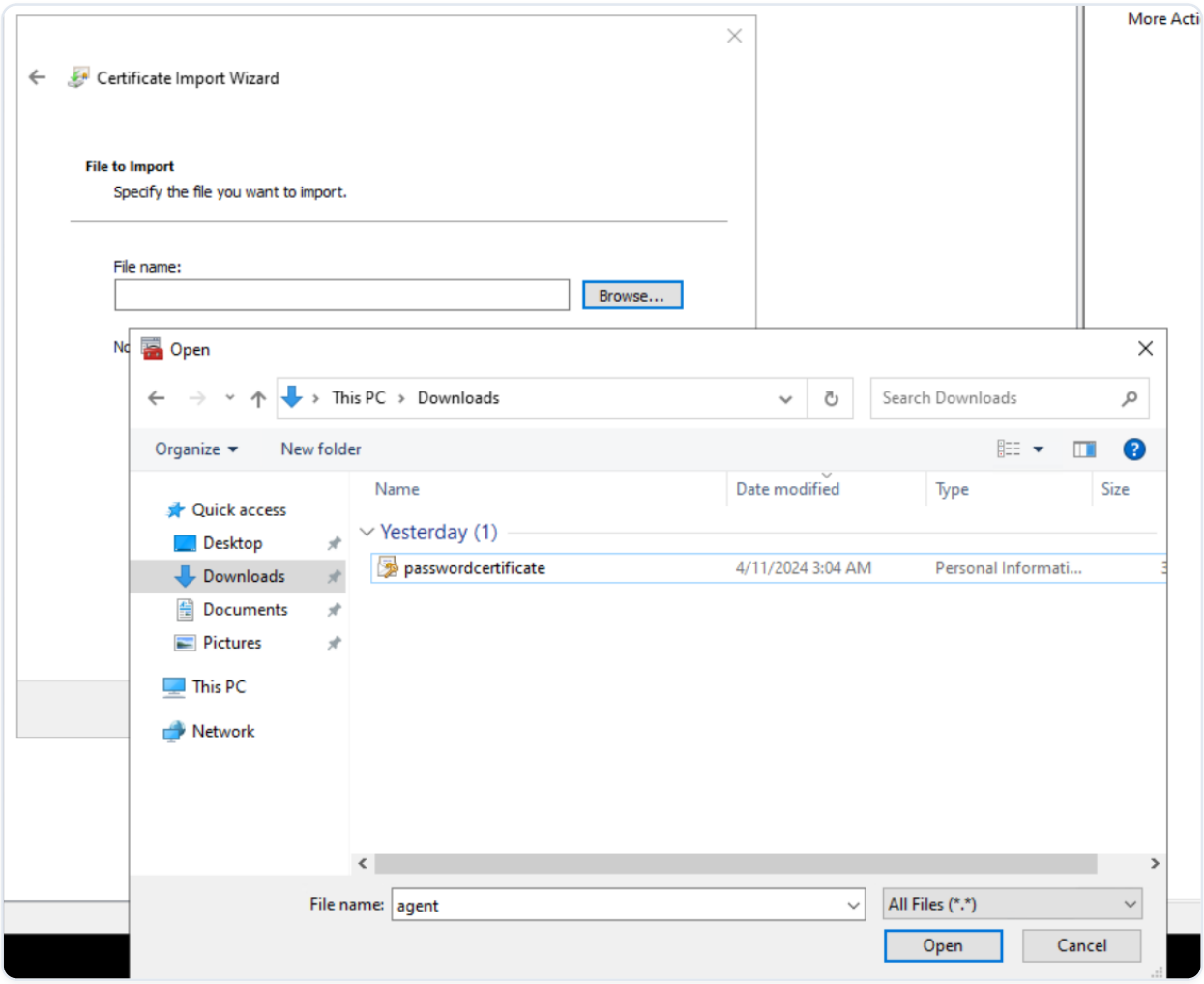


5. 「**ローカルコンピューター**」を選択します。

6. 「**完了**」をクリックします。新しいコンソールの選択されたスナップインのリストに「**証明書(ローカルコンピューター)**」セクションが表示されます。
7. 「**OK**」をクリックします。
8. 「**証明書**」を展開し、「**個人**」を右クリックして、「**すべてのタスク**」 > 「**インポート**」を選択します。「**証明書のインポートウィザードへようこそ**」が表示されます。



9. 「**次へ**」 > 「**ファイルの参照**」を選択します。PFXファイルをアップロードした場所に移動し、ファイルの種類を「**すべてのファイル**」に変更してから、該当するPFX証明書を選択します。



10. PFXパスワードを入力します。パスワードがない場合は空白のままにできます。
11. **Next**をクリックします。
12. 証明書ストアについては、「**証明書をすべて次のストアに配置する**」オプションが選択されており、「**証明書ストア**」が「**個人**」として選択されていることを確認します。

    証明書ストア(/en-us/citrix-virtual-apps-desktops/2503/media/sm-certificate-store.png)
13. **Next**をクリックします。
14. 詳細を確認し、**完了**をクリックします。
15. 確認を待ちます。「*インポートは正常に完了しました*」というメッセージが表示されます。
16. **証明書** > **個人.**
17. マシンからPFX証明書ファイルを削除します。

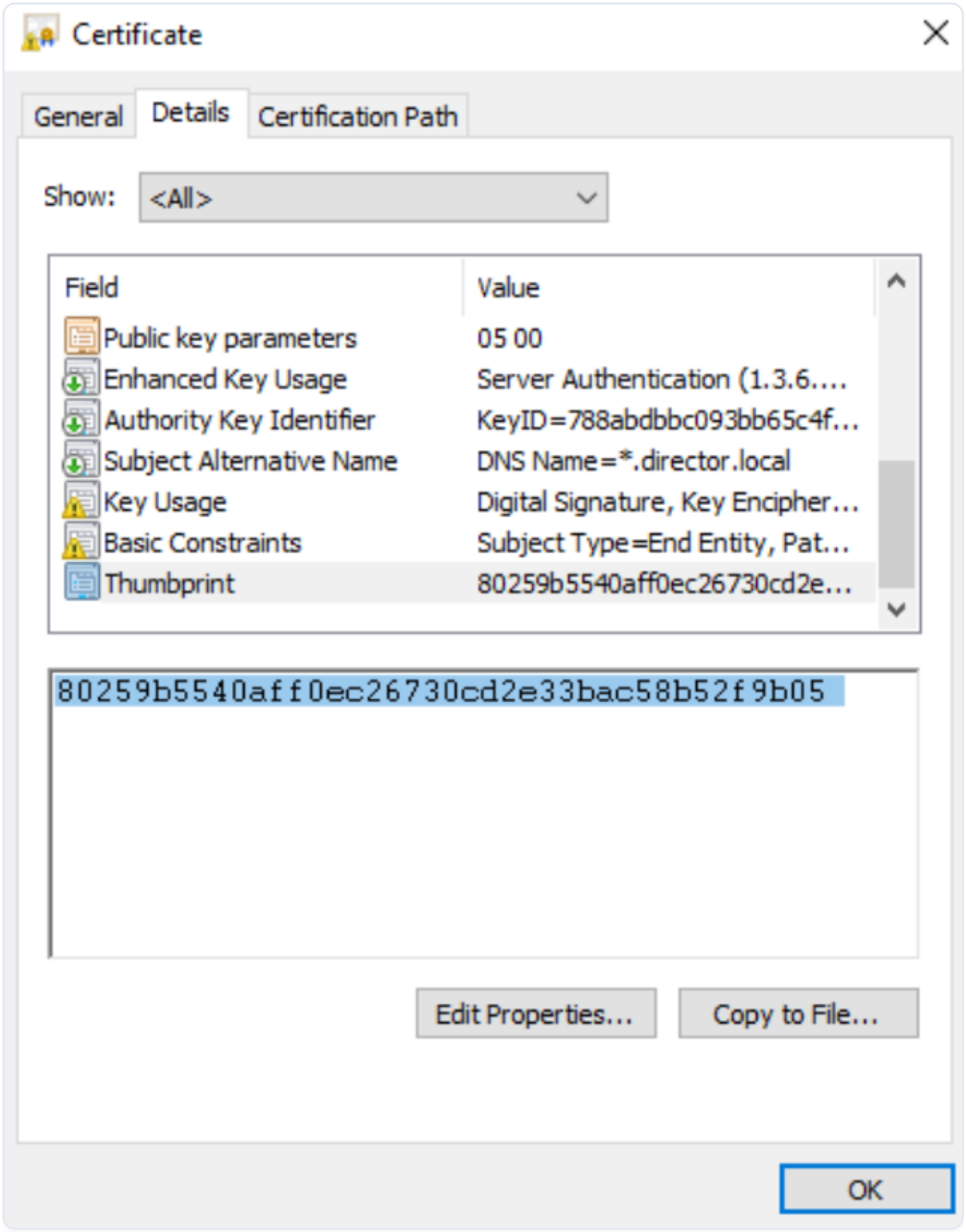
ステップ3：証明書への読み取りアクセス権を付与する

1. インポートした証明書を右クリックし、「**すべてのタスク** > **秘密キーの管理**」を選択します。

2. 開いたダイアログで「**追加**」を選択し、「**Network Service**」を検索します。 「**OK**」をクリックします。
3. 「**グループ**」または「**ユーザー名**」の下にある「**NETWORK SERVICE**」を選択します。
4. 「**NETWORK SERVICE のアクセス許可**」の下で「*読み取り*」アクセスを許可します。
5. 「**OK**」をクリックします。

ステップ4：サムプリントを取得する

1. インポートした証明書をダブルクリックします。
2. 開いたダイアログで、**詳細**タブに移動し、一番下までスクロールします。
3. **Thumbprint**をクリックします。

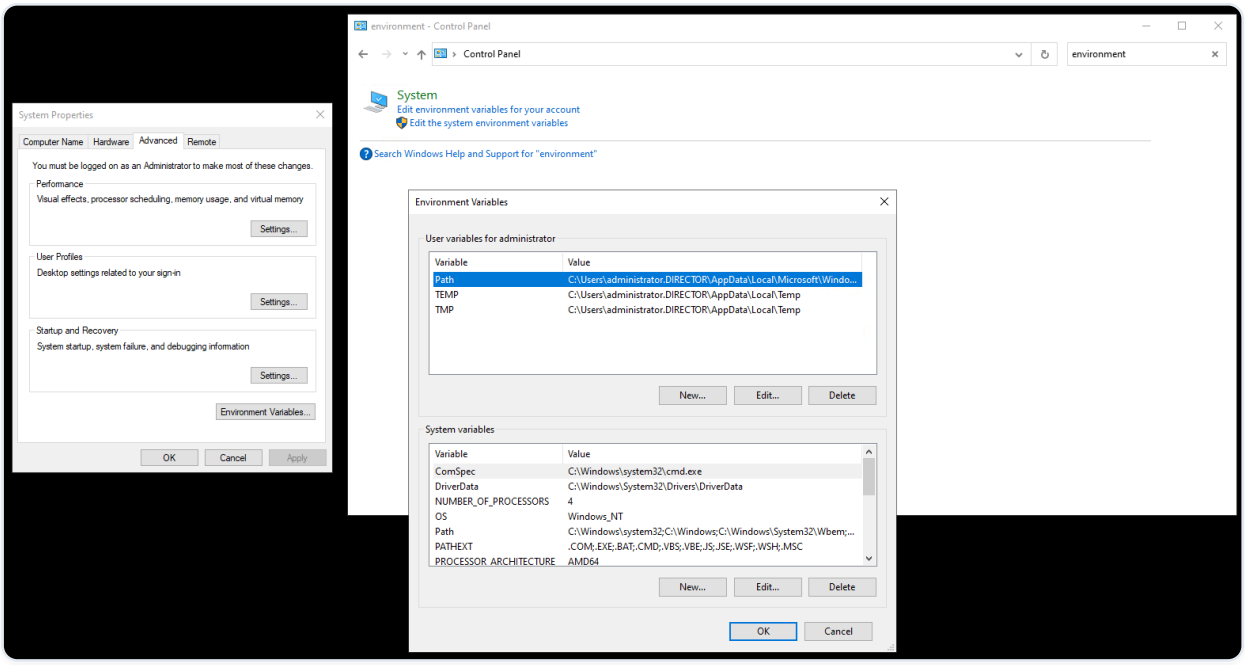


4. 値をコピーし、次のステップのために準備しておきます。

ステップ5：環境変数の設定

1. コントロールパネルを開きます。
2. 「環境」を検索し、「**システム環境変数の編集**」を選択します。

3. 「**システム環境変数 (すべてのユーザー)**」の下にある「**新規**」をクリックします。



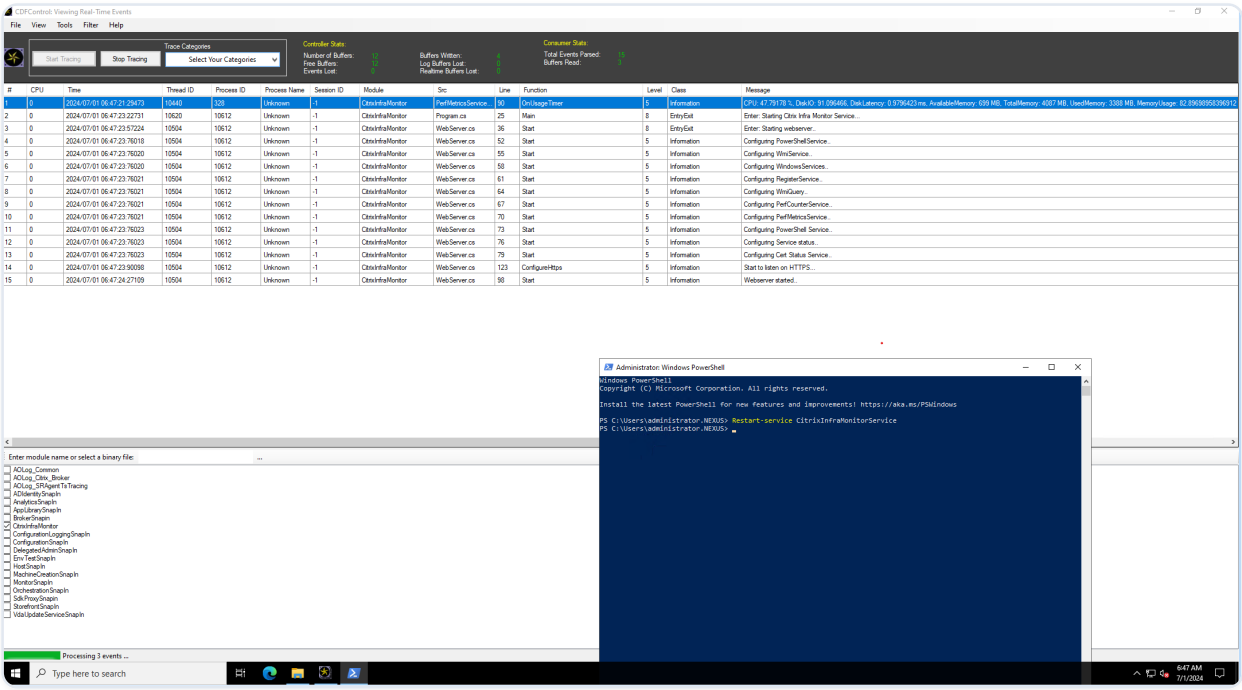
4. 「**変数**」名を「*DIRECTOR_AGENT_HTTPS_CERTIFICATE_THUMBPRINT*」と指定します。
5. 前のステップで取得したサムプリントを「**変数値**」に指定します。
6. 「**OK**」をクリックします。

ステップ6：CitrixInfraMonitorServiceの再起動

1. PowerShellを開き、次のコマンドを実行します。

```
Restart-Service CitrixInfraMonitorService
```

2. **CitrixInfraMonitorService**モジュールをキャプチャし、ログ行**Start to listen on HTTPS...**を探して、HTTPSが有効になっていることを確認します。



ステップ 7: モニター構成で HTTPS を有効にする

Delivery Controller™マシンで次のコマンドを実行します。

```
Set-MonitorConfiguration -DirectorAgentEnableHttps $true
```

Citrix Infrastructure Monitor の手動接続

注:

以下の2つの手順は、Provisioning ServiceおよびStoreFront™コンポーネントの監視にのみ有効です。

ステップ1：Citrix Infrastructure Monitorのインストール

安全なデータ収集のための接続を確立するには、ターゲットコンポーネントにインストールを完了するために以下の手順を実行します。

注:

Citrix Infrastructure Monitor をインストールするマシンには、Provisioning Service または StoreFront のいずれかがすでにインストールされている必要があります。

ステップ1.1：ターゲットコンポーネントの特定

監視する必要がある Provisioning Service または StoreFront サーバーなどのターゲットコンポーネントを特定します。

ステップ1.2：Citrix Infrastructure Monitorのダウンロード

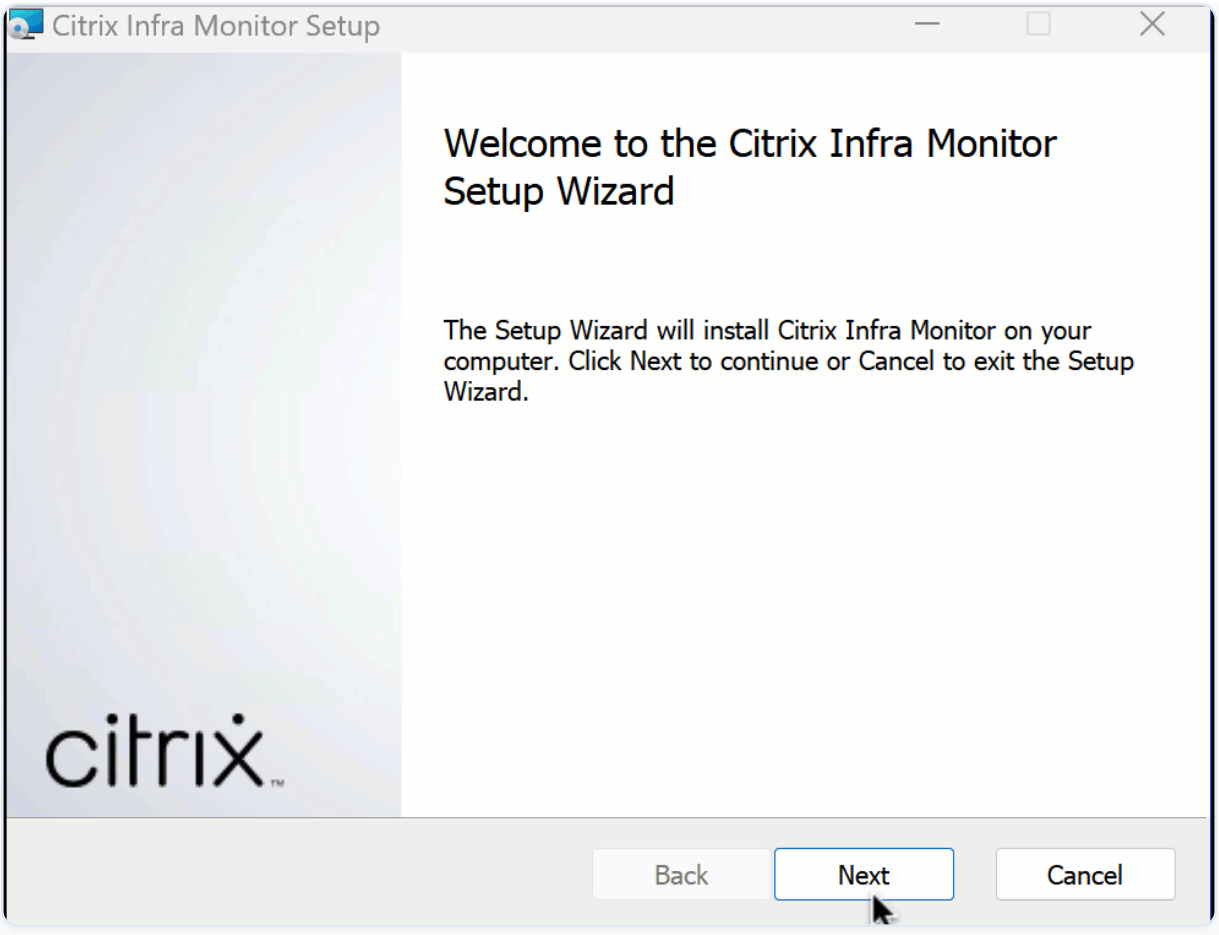
ステップ 1.1 で特定されたターゲットサーバーの Citrix downloads ページから `CitrixInfraMonitor.msi` をダウンロードできます。

ステップ 1.3: Citrix Infrastructure Monitor を実行する

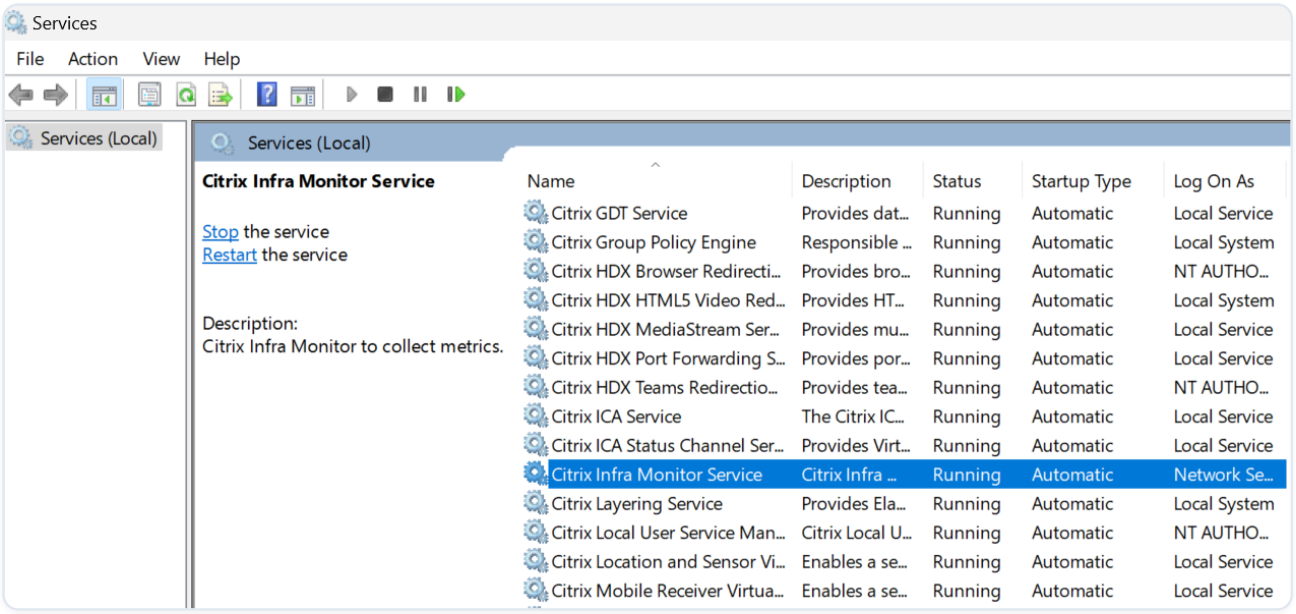
インストールウィザードの指示に従って、ターゲットコンポーネントで `CitrixInfraMonitor.msi` インストーラーを実行します。

注:

管理者権限を持つユーザーは、ターゲットコンポーネントにCitrix Infrastructure Monitorをインストールおよび構成できます。



インストールが正常に完了すると、「**サービス**」セクションでCitrix Infrastructure Monitorサービスを表示できます。



ステップ 1.4: 登録トークンを取得する

Citrix Infrastructure Monitorがインストールされているシステムで、`C:\ProgramData\Citrix\InfraMonitor\RegistrationToken.txt`にある`RegistrationToken.txt`ファイルで提供されているトークンを取得し、ステップ 2: Citrix Infrastructure Monitorを登録するで使用できるように準備しておきます。

ポート要件

`CitrixInfraMonitor.msi`のインストールが正常に完了すると、インストーラーはポート9595の例外を作成します。サードパーティ製のファイアウォールを使用している場合、Citrix Infrastructure Monitoringサービスを使用するには、このポートのTCP通信を手動で許可する必要がある場合があります。

次の表に、Provisioning ServiceおよびStoreFrontマシンに関するインバウンドポート要件の詳細を示します。

送信元	ターゲット	タイプ	ポート	プロトコル	目的
DDC	Provisioning Serviceまたは StoreFront マシン	TCP	9595	HTTPまたは HTTPS	Provisioning Serviceまたは StoreFront マシンから メトリックを収集する

送信元	ターゲット	タイプ	ポート	プロトコル	目的
					ための呼び出し。

> **注：**
>
> Provisioning ServiceおよびStoreFrontマシンは、Infrastructure Monitoringサービスに対してアウトバウンド呼び出しを行いません。

手順2：Citrix Infrastructure Monitorを登録する

Citrix Infrastructure Monitorは、以下を使用して登録できます。

- ディレクターユーザーインターフェース
- PowerShell SDK

Director UIから

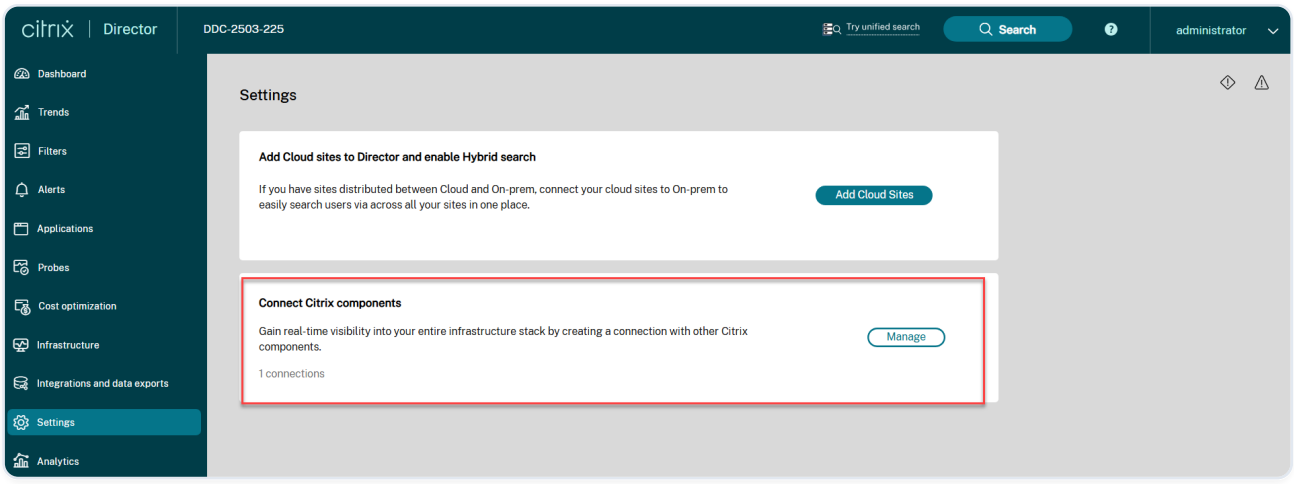
次の手順でDirector UIでの登録を完了します。

手順2.1：Citrixコンポーネントの接続ページに移動する

［設定］ > ［Citrixコンポーネントの接続］ > ［管理］ の順にクリックします。

または、,

インフラストラクチャ > **管理**をクリックします。



](/en-us/citrix-virtual-apps-desktops/2503/media/connect-citrix-components.png)

手順2.2：コンポーネントの詳細を入力する

［Citrix コンポーネントの接続］ 画面で、**［接続の作成］** をクリックします。**［接続の作成］ウィンドウ**が表示されます。

](/en-us/citrix-virtual-apps-desktops/2503/media/create-a-connectiOn.png)

`CitrixInfraMonitor.msi`がターゲットにダウンロードされ、インストールされていることを確認してください。詳細については、このドキュメントの手順1を参照してください。画面の指示に従い、セキュアな接続を確立するために必要なコンポーネントの詳細を入力します。

- ドロップダウンリストからコンポーネントの種類を選択します。コンポーネントはProvisioning ServiceまたはStoreFrontです。
- ホスト名を入力します。
- ドメイン名を入力します。
- Provisioning Service または StoreFront マシンのユーザー名を入力します。
- Provisioning Service または StoreFront マシンのパスワードを入力します。

手順2.3：接続を承認する

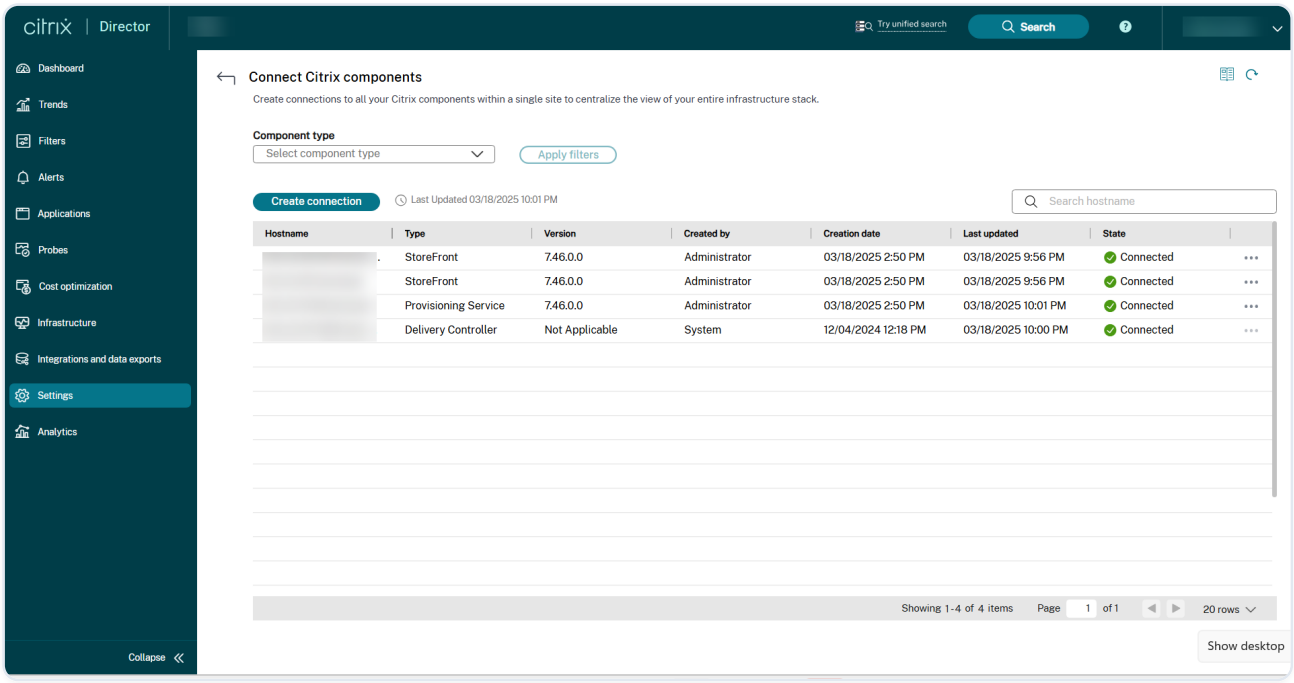
Citrix Infrastructure Monitorがインストールされているシステムで、`C:\ProgramData\Citrix\InfraMonitor\RegistrationToken.txt`にある`RegistrationToken.txt`ファイルからCitrix Infrastructure Monitorトークンを取得します。

取得したトークンの詳細を Director UI に入力します。このトークンは、サイトとコンポーネント間の接続を認証します。

`RegistrationToken.txt`ファイルに存在するトークンテキストは、Citrix Infrastructure Monitorサービスを再起動すると再生成されます。登録が成功すると、トークンファイルはマシンから削除されます。何らかの理由で新しいトークンファイルを再作成する必要がある場合は、Citrix Infrastructure Monitorサービスを再起動してください。セキュリティ上の理由から、無効なトークンによる登録試行が3回失敗すると、トークンファイルは削除されます。

ステップ2.4: 接続を作成する

詳細が入力されたら、**作成**をクリックします。作成された接続は、**Citrixコンポーネントの接続**ページの接続リストに表示されます。



リモート PowerShell SDK の使用

前提条件：

- Citrix Infrastructure Monitor が StoreFront または PVS マシンにインストールされていることを確認します。

PVS または StoreFront マシンと通信するために、Citrix Infrastructure Monitor を DDC に登録します。この登録は、PVS または StoreFront マシンで収集されたインフラストラクチャの健全性メトリックを DDC に送信するためのものです。

Citrix Infrastructure Monitor に登録するには、Delivery Controller™ で次の PowerShell コマンドを実行します。

```
Add-MonitorDirectorAgent -Fqdn <FQDN of component> -Component <component>
-Domain <domain> -Username <username> -Password <password> -Token <token>
```

注:

ユーザー名とパスワードはオプションのパラメーターです。ただし、これらのパラメーターを指定しない場合、一部のメトリックは利用できません。

上記のコマンドのパラメーターは次のとおりです。

パラメーター	説明
`Fqdn`	PVS または StoreFront サーバーの FQDN。
`Component`	オンボーディングするコンポーネント。例: PVS または SF。PVS は Citrix Provisioning™ を表し、SF は StoreFront を表します。
`Domain`	すべてのコンポーネントが属するドメイン。
`Username`	管理ユーザーのユーザー名。
`Password`	管理ユーザーのパスワード。
`Token`	Citrix Infrastructure Monitorがインストールされているシステムの `C:\ProgramData\Citrix\InfraMonitor\RegistrationToken.txt` にある `RegistrationToken.txt` ファイルから、Citrix Infrastructure Monitorトークンを取得します。

注:

- Citrix Infrastructure Monitorサービスを再起動すると、`RegistrationToken.txt` ファイルに存在するトークンテキストが再生成されます。登録が成功すると、トークンファイルはマシンから削除されます。再登録する必要がある場合は、Citrix Infrastructure Monitorサービスを再起動してください。
- セキュリティ上の理由から、無効なトークンによる登録試行が3回失敗すると、トークンファイルは削除されます。

PVSまたはStoreFrontマシンを正常に登録すると、マシン名の詳細が**Director** > **インフラストラクチャ** タブに表示されます。

Citrix Infrastructure Monitorに登録するためのコマンドの例は次のとおりです。

```
Add-MonitorDirectorAgent -Component PVS -Fqdn NX-PVS-
-Domain  -Username  -Password  -Token
```

統合とデータのエクスポート

Citrix Director は、統合とデータエクスポートのための新しいUIを提供するようになりました。この機能は、Citrix Directorで利用可能なさまざまなインターフェイスとサードパーティ統合の認識を高めるのに役立ちます。新しく導入された**統合とデータエクスポート**ページには、以下がリストされています。

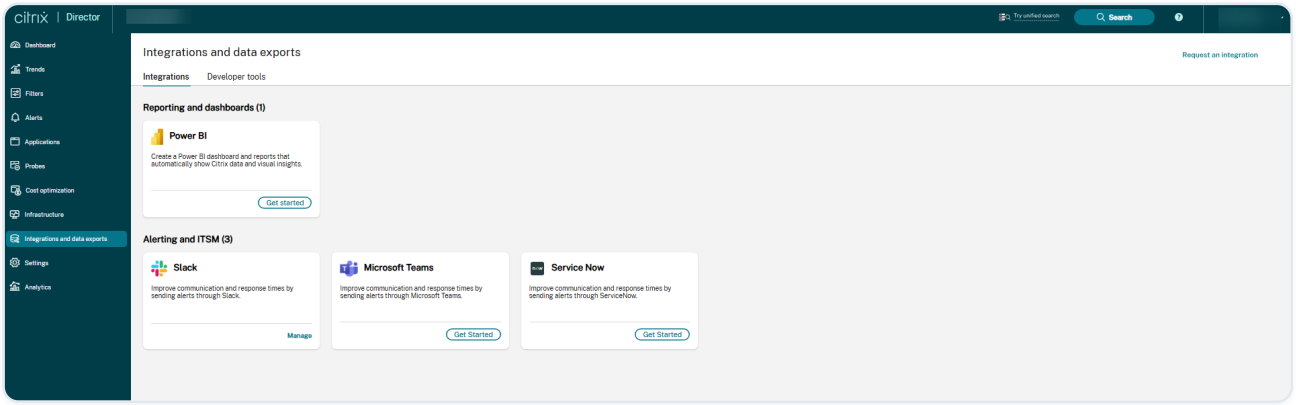
- 利用可能な統合
- サポートされている開発者ツール

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

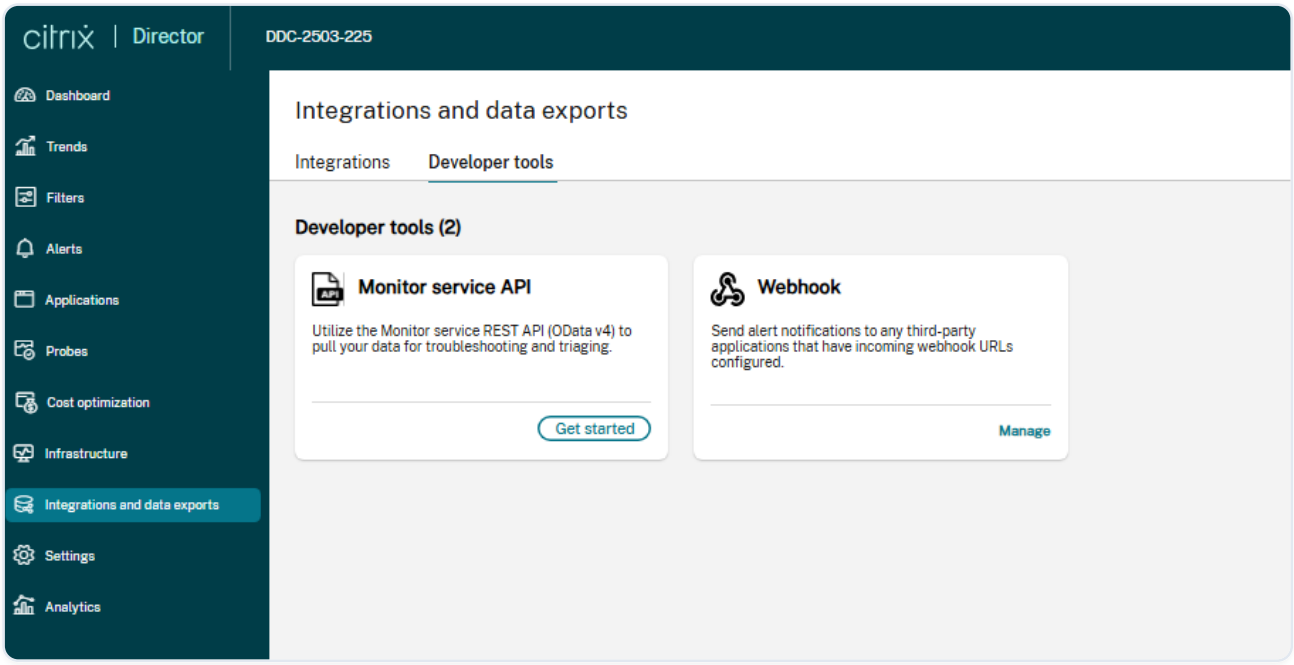
Citrix 監視メトリックを収集するために、次の統合オプションが提供されています。

- Citrix Monitor Service API - Citrix Monitor サービス API を使用して、Citrix Monitor からパフォーマンスデータとイベントを収集し、Power BI にエクスポートできます。
- アラートと ITSM - 受信 Webhook URL が構成されている次のサードパーティアプリケーションにアラート通知を送信できます。
  - スラック
  - マイクロソフト Teams
  - ServiceNow

左側のナビゲーションメニューから をクリックします。 ページが表示されます。



開発者ツール:



利用可能な統合を表示

統合タブには、Citrix Directorで利用可能な統合が表示されます。利用可能な統合は、以下のように分類されます。

- レポートとダッシュボード
- アラートとITSM

レポートとダッシュボード

Power BIは、Citrix Director APIを通じて収集されたメトリックを視覚化するために使用できます。**開始**をクリックします。**REST API**開発者ツール詳細ページが表示されます。

モニターサービスAPIをクリックすると、PowerBIとの統合に関するリソースやブログへの参照リンクが表示されます。

このページには、リソースやブログへの参照リンクが記載されています。

アラートおよびITSMツールとの統合

アラートおよびITSMツールには、次のものが含まれます。

- スラック
- マイクロソフト チームズ
- ServiceNow

アラートおよびITSMツールをWebhookと統合するには、ツールの横にある**開始する**リンクをクリックします。このリンクをクリックすると、特定の警告およびITSMツールの統合ページが開き、前提条件とアラートを送信するための具体的な手順の詳細が表示されます。ツールとWebhook URLを設定できます。たとえば、Slackを統合するには、Slackのドキュメントに従ってチャネルとWebhook URLを作成する必要があります。

完了したら、2番目のステップに進み、Webhookプロファイルを作成します。

参照リソースを確認することもできます。例えば、Slackとの統合の前提条件と手順は次のとおりです。

Slack統合(/en-us/citrix-virtual-apps-desktops/2503/media/slack-integration.png)

Webhookとの統合

1. **統合**タブ > **アラートとITSM**セクション > 選択したツールの横にある**開始**をクリックします。そのツールの**統合**ページが開きます。
2. リソースやブログへの参照リンクにアクセスできます。
3. ステップ1に従います。
4. ステップ2の一部として、**Webhookプロファイルの作成**をクリックします。`<name of the tool>` **Webhookプロファイルの作成**ページが表示されます。
5. Webhookプロファイルの**名前**を入力します。
6. Webhookプロファイルの**説明**を入力します。
7. **Webhook構成**セクションで、目的の**メソッド**を選択します。
8. 前のステップで選択したメソッドに従って、**API/Webhook** URLを入力します。
9. **メッセージ**形式を表示します。
10. **ヘッダー**セクションにキーと値を追加します。
11. 作成したWebhookを検証するには、**テスト**をクリックします。
12. Webhookが正常に検証されたら、**Webhookの作成**をクリックします。Webhookが作成されます。
13. 作成されたWebhookプロファイルを**Developer tools** > **Webhook** > **Manage**で表示します。**Webhook profiles developer tool details**ページが開きます。

Developer tools > **Webhook** > **Create webhook profiles**でWebhookプロファイルを作成することもできます。

WebhookプロファイルをCitrixアラートと統合する

作成されたWebhookプロファイルは、**Alerts** > **Advanced Alert Policies** > **Create Policy**セクションで表示し、Citrixアラートの一部として使用できます。

Webhookプロファイルを新しいCitrixアラートポリシーと統合するには、次の手順を実行します。

1. **アラート** > **高度なアラートポリシー** > **ポリシーの作成**をクリックします。**高度なアラートポリシーの作成**ページが表示されます。
2. **通知チャネル** > **Webhookの使用**セクションに移動します。
3. Webhookプロファイルを選択します。
4. アラートポリシーを保存します。

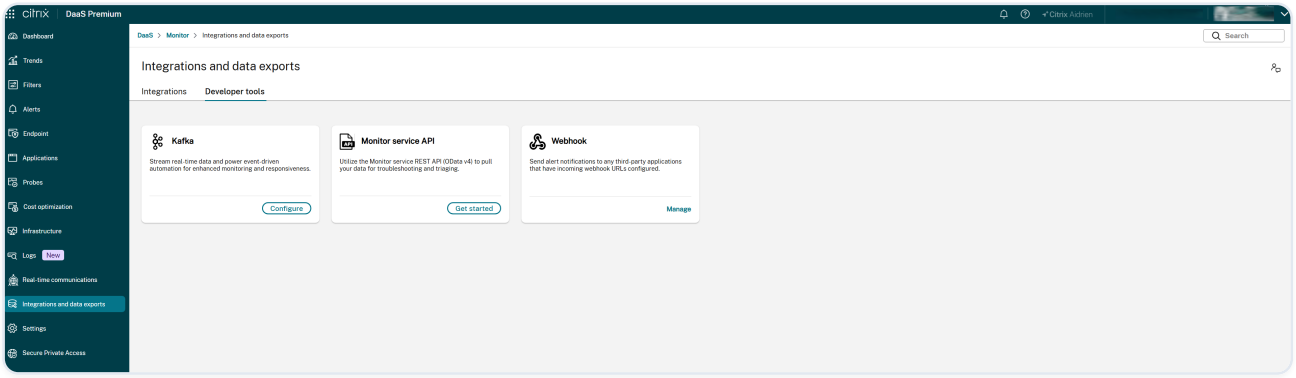
Webhookプロファイルを既存のアラートポリシーと統合するには、次の手順を実行します。

1. **アラート** > **高度なアラートポリシー** > **ポリシーの編集**をクリックします。**高度なアラートポリシーの編集**ページが表示されます。
2. **通知チャネル** > **Webhookの使用**セクションに移動します。
3. Webhookプロファイルを選択または変更します。
4. アラートポリシーを更新して保存します。

サポートされている開発者ツールを表示する

利用可能な開発者ツールを表示するには、**Developer tools**タブをクリックします。

利用可能な開発者ツールは、Monitor service APIとWebhookです。



モニターサービス API

「**開始**」をクリックします。**Monitor Service API** 開発者ツールの詳細ページが開きます。リソースやブログへの参照リンクにアクセスできます。

ウェブフック

Webhookプロファイルは、「**開発者ツール**」>「**Webhook**」>「**Webhookプロファイルの作成**」で表示および作成できます。

ユーザーアクションの一括アクションオプションを制限するカスタムロール

この機能により、管理者が表示および制御できる範囲を制限するためにカスタムロールを追加できます。新しいカスタムロールは、ログオフ、切断、メッセージなどの一括アクションを選択する機能を制限します。この制御は、ユーザーに対する意図しない、または悪意のある大量のアクションを防ぐために必要です。

次の手順で、一括操作の権限を制限するように役割を編集できるようになりました。

1. Citrix Cloudにサインインします。
2. **役割**に移動し、「**一括操作は有効になっていません**」の役割を選択します。
3. 3つの点をクリックし、**編集**を選択します。
4. **Director > 管理**に移動し、「**マシンの電源操作、メンテナンスモード操作、およびセッション管理の一括操作を実行する**」チェックボックスをオンにします。
5. 以下の役割も選択されていることを確認してください。
    - **マシンカタログメンバーシップを介してマシンのメンテナンスモードを有効/無効にする**
    - **マシンカタログメンバーシップを介してデスクトップのメンテナンスモードを有効/無効にする**
    - **マシンカタログメンバーシップを介してWindowsデスクトップマシンで電源操作を実行する**
    - **マシンカタログメンバーシップを介してWindowsサーバーマシンで電源操作を実行する**

ステップ5のオプションが選択されている場合、ユーザーは単一のアクションを実行できます。一括操作を実行するには、ステップ4のオプションとステップ5のオプションが選択されている必要があります。

Web Studio展開のセキュリティ保護

この記事では、Web Studioを展開する際にシステムセキュリティに影響を与える可能性のある構成領域について説明します。

> **注：**
>
> ユーザーのWebブラウザーとWeb Studio間の通信を保護するには、Web StudioおよびDirectorでTLSを有効にするを参照してください。

IIS設定の構成

セキュリティのベストプラクティスとして、Web Studioを制限されたIIS構成で構成します。

1. 要求フィルタリングを制限する：
   - Web StudioをDirectorとともにインストールする場合、IISは以下のフィルタリングルールで自動的に構成されます。
   - Web Studioをスタンドアロンコンポーネントとしてインストールする場合、IISを手動で次のように構成します。
     - 以下のファイル名拡張子のみを許可する：

       `.`, `.aspx`, `.css`, `.eot`, `.html`, `.ico`, `.js`, `.png`, `.svc`, `.svg`, `.jpg`, `.gif`, `.j`

       詳細については、こちらのMicrosoft記事を参照してください。
     - 以下のHTTP動詞のみを許可する：

       `GET`, `POST`, `HEAD`

       詳細については、こちらのMicrosoft記事を参照してください。
2. 不要なハンドラーマッピングを削除します。

   Web Studioには`StaticFile`ハンドラーマッピングのみが必要です。その他はすべて削除してください。詳しくは、こちらのMicrosoft記事を参照してください。
3. 未使用のISAPIフィルターを削除します。

   Web StudioはISAPIフィルターを必要としません。すべて削除できます。詳しくは、こちらのMicrosoft記事を参照してください。

> **注：**
>
> ASP.NETにはISAPI Windows機能が必要です。

4. `C:\inetpub\wwwroot`から以下のデフォルトのIISランディングページファイルを削除します。
   - `iisstart.htm`
   - `welcome.png`
5. **.NET Trust Level**が**Full Trust**に設定されたままであることを確認してください。この設定はインストール中に自動的に構成され、Web Studioが正しく機能するために必要です。変更しないでください。

未使用のアプリケーションプール権限を削除する

インストール中、Web Studioアプリケーションプールには以下のユーザー権限が付与されます。

- **サービスとしてログオン**
- **プロセスのメモリクォータを調整**
- **セキュリティ監査を生成**
- **プロセスレベルトークンを置き換える**

これらの権限はIISアプリケーションプールにとって標準的なものです。Web Studioはこれらを使用しないため、削除できます。

Web Studioの展開を分離する

Web Studioと同じWebドメイン（ドメイン名とポート）に任意のWebアプリケーションを展開できます。ただし、それらのWebアプリケーションにおけるセキュリティリスクは、Web Studio展開のセキュリティを低下させる可能性があります。より高度なセキュリティ分離が必要な場合は、Web Studioを他の*サードパーティ*アプリケーションとは別のWebドメインに展開することをお勧めします。

Ansible を使用した VDA のインストール

概要

この記事では、Ansible を使用して VDA を展開する方法について説明します。詳細については、Ansible ドキュメントを参照してください。

> **注:**

> この記事は、Citrix® が環境をテストした方法に基づいた推奨事項のみを説明しています。これらの手順は、お客様のニーズに合わせてカスタマイズできます。Citrix は、お客様のニーズに合わせて必要な更新や調整について責任を負いません。

Ansible を使用して VDA を展開するための主要な手順

1. 仮想マシン環境を構成する。
2. Ansible をインストールする
3. Kerberos の構成
    a. Kerberos をインストールする
    b. Kerberos を構成する
4. Ansible を構成する

ステップ 1: 仮想マシン環境を構成する

Windows サーバーで次のコマンドを実行します。

1. PS RemoteSigned を設定します。 `Set-ExecutionPolicy RemoteSigned`
2. WinRMを暗号化なしで使用するように設定します。 `winrm set winrm/config/service '@{AllowUnencrypted="true"}'`

    > **注：**
    >
    > このステップでエラーが発生した場合は、次のコマンドを使用してください。
    > `Enable-PSRemoting -Force`

3. ファイアウォールポート5985を開きます。 `New-NetFirewallRule -DisplayName "Allow WinRm port 5985" -Direction Inbound -Profile Any -Action Allow -LocalPort 5985 -Protocol tcp`

ステップ2：Ansibleをインストールする

Ubuntu 20.4以降でAnsibleをインストールするには、次のコマンドを実行します。

- `sudo apt update`
- `sudo apt install software-properties-common`

- `sudo add-apt-repository --yes --update ppa:ansible/ansible`
- `sudo apt install ansible`
- `sudo apt install python3-pip`

ステップ2i：Kerberosをインストールする

Kerberosをインストールするには、次のコマンドを実行します。

`sudo apt install python3-dev libkrb5-dev krb5-user`

ステップ2ii：Kerberosを構成する

Kerberosを構成するには、次のコマンドを実行します。

`Edit /etc/krb5.conf`

```
[libdefaults]
        default_realm = [redacted]

# The following krb5.conf variables are only for MIT Kerberos.
        kdc_timesync = 1
        ccache_type = 4
        forwardable = true
        proxiable = true

# The following encryption type specification will be used by MIT Kerberos
# if uncommented.  In general, the defaults in the MIT Kerberos code are
# correct and overriding these specifications only serves to disable new
# encryption types as they are added, creating interoperability problems.
#
# The only time when you might need to uncomment these lines and change
# the enctypes is if you have local software that will break on ticket
# caches containing ticket encryption types it doesn't know about (such as
# old versions of Sun Java).

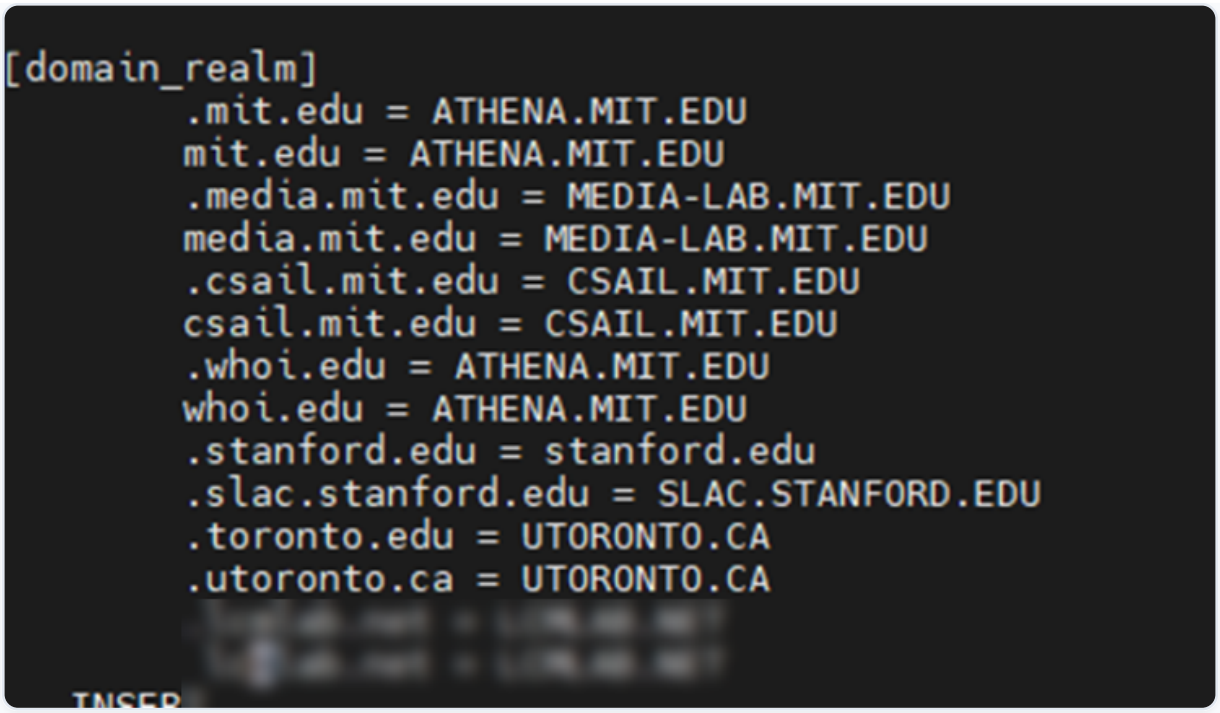
#       default_tgs_enctypes = des3-hmac-sha1
#       default_tkt_enctypes = des3-hmac-sha1
#       permitted_enctypes = des3-hmac-sha1

# The following libdefaults parameters are only for Heimdal Kerberos.
        fcc-mit-ticketflags = true

[realms]
        LTSRLAB.NET = {
                kdc = [redacted]
                admin_server = [redacted]
        }
        ATHENA.MIT.EDU = {
                kdc = [redacted]
```

> **注:**

Kerberosレルム名には大文字を使用します。



ステップ 3: Ansible を構成する

Ansibleホストを構成するには、次の手順を実行します。

1. 次のコマンドを実行します。

   `Edit /etc/ansible/hosts`

2. Delivery Controller `Install.yaml` ファイルを構成します

   `/QUIET /NOREBOOT /NORESUME /OPTIMIZE /VERBOSELOG /COMPONENTS VDA /CONTROLLERS 'MyDDC.xd.local' /ENABLE_HDX_PORTS /ENABLE_REAL_TIME_TRANSPORT`

   「デリバリーコントローラー」(/en-us/citrix-virtual-apps-desktops/2503/media/delivery-controller-yaml-1.png)

   「デリバリーコントローラー」(/en-us/citrix-virtual-apps-desktops/2503/media/delivery-controller-yaml-2.png)

   「デリバリーコントローラー」(/en-us/citrix-virtual-apps-desktops/2503/media/delivery-controller-yaml-3.png)

   デリバリーコントローラー(/en-us/citrix-virtual-apps-desktops/2503/media/delivery-controller-yaml-4.png)

3. 以下のコマンドでyamlファイルを実行します。 `sudo ansible-playbook install.yml -vvv` (詳細モード)
4. 設定ファイルで、他の追加設定とともに複数のホストを構成できます。

   `Edit /etc/ansible/hosts` Ansibleホスト (/en-us/citrix-virtual-apps-desktops/2503/media/ansible-hosts.png)

Call Home の主要データポイント

Call Home は以下の主要なデータポイントを収集します。

(M) = 手動収集時のみ取得 (PowerShell コマンドレット `Start-CitrixCallHomeUpload`)

ファイル名	カテゴリ	データグループ
		マシン
		エックスディーサイト
		サイト情報
		Broker DB 情報 (M)
		インストールされている DB バージョン (M)
		Broker サービスステータス (M)
		登録済みサービスインスタンス (M)
		ブローカーライセンス テスト (M)
		アクティブな HDX™ セッション (M)
		ブローカー管理者
		ブローカー管理者権限

		RDS構成 (LicensingSettings、SessionSettings、SpecifiedLicenseServers、および RegisteredLicenseServersを含む)
		監視サービス (M) (MonitorConfiguration、MonitorDataStore、MonitorDBConnection、MonitorDBSchemaVersion、MonitorService、MonitorServiceAddedCapability、MonitorServiceInstance、MonitorServiceStatus、およびMonitorInstalledDBVersionを含む)
		構成ログ
		接続ログ
		ハイパーバイザー接続 (M)
		ブローカーハイパーバイザー接続
		ハイパーバイザーアラート
		カタログ
		マルチセッションOSエージェント (M)
		シングルセッションOSエージェント (M)
		公開アプリケーション
		デリバリー グループ

		構成済みデリバリーエージェント

		Citrixインストール済みコンポーネント
		Citrix Brokerサービス情報
		ブローカーサービス構成ファイル
		Machine Creation Services™ 構成ファイル
		ホストサービス構成ファイル
		AD IDサービス構成ファイル
		構成サービス構成ファイル
		構成ログサービス構成ファイル
		委任管理サービス構成ファイル
		環境テストサービス構成ファイル
		監視サービス構成ファイル
		Storefront™ サービス構成ファイル
		ワークステーションエージェント構成ファイル
		Citrix VDA情報
		Citrix XD ホットフィックス
		Citrix_VirtualChannel_Graphics_Enum

		Citrix_VirtualChannel_Flash_Enum
		Citrix_VirtualChannel_Printer_Enum

		コンピューター
		BIOS
		メモリ情報
		プロセッサ
		PNP デバイス
		デバイス
		ディスクドライブ
		論理ドライブ
		ページファイル使用状況
		ネットワークアダプター
		ネットワークアダプター構成
		ipConfig
		ビデオコントローラー
		IDE コントローラー
		SCSI コントローラー

		HKLM:\Software\Wow6432Node\Citrix

		HKLM:\System\CurrentControlSet\Control\Citrix
		HKLM:\SOFTWARE\Policies\Citrix
		HKLM:\Software\Microsoft\Cryptography
		HKLM:\Software\Wow6432Node\Microsoft\Cryptography
		HKLM:\Software\Microsoft\Windows NT\CurrentVersion\Windows
		HKLM:\Software\Microsoft\Windows NT\CurrentVersion\Winlogon
		HKLM:\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
		HKLM:\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Policies\Explorer
		HKLM:\SYSTEM\CurrentControlSet\Control\Print\Environments
		HKLM:\システム\カレントコントロールセット\コントロール\セッションマネージャー

		HKLM:\システム\カレントコントロールセット\コントロール\ターミナルサーバー
		HKCU:\Control Panel\Desktop
		HKLM:\SOFTWARE\Classes\ShockwaveFlash.ShockwaveFlash\CurVer
		HKLM:\SYSTEM\CurrentControlSet\Control\SystemInformation
		HKLM:\SYSTEM\CurrentControlSet\Control\FileSystem
		HKLM:\SYSTEM\CurrentControlSet\Control\Windows
		HKLM:\SYSTEM\CurrentControlSet\Control\TimeZoneInformation

		ドライバー
		EnvVariables
		OS
		プロセス
		サービス
		サービスパック
		ジーピーリザルト
		Microsoft ホットフィックス

		ネットスタット
		PNP ドライバー

		システムイベントログ
		AOT (常時オンのトレース)
		クラッシュダンプ

		アップタイム
		メモリ
		コンピューターシステム
		プロセッサ
		ビデオコントローラー
		ディスクドライブ
		ブラウザ情報
		再起動回数
		メモリ使用量
		ディスク使用量
		ICAセッション解像度
		ICAカラー深度
		メタインストーラーCEIPマシンID

		ストア数
		サーバーグループ内のサーバー数

		ストアあたりのDelivery Controller™数
		HTTPS有効
		Citrix Receiver™のクラシックエクスペリエンスが有効
		Citrix レシーバー 用の HTML5 レシーバー設定
		Citrix Receiver向けワークスペースコントロールの有効化
		ストア向けリモートアクセスの有効化
		ゲートウェイ数
		統合されたNetScaler®認証用の明示的なJSONサービス

プロファイルコンテナのポリシー設定

プロファイルコンテナ

ユーザープロファイルに関連付けられた大きなフォルダーは、ログオンを遅くします。Citrix Profile Managementは、プロファイルディスク（VHDXファイル）に含めるフォルダーを指定できるVHDXベースのプロファイルソリューションを提供します。このソリューションは、指定されたフォルダーをネットワークに保存されているプロファイルディスクにマッピングすることで、ログオン時間を短縮します。プロファイルコンテナは、ログオン時にこれらのフォルダーを含むプロファイルディスクをアタッチするため、フォルダーのコピーをローカルプロファイルに保存する必要がなくなります。これにより、ログオン時間が短縮されます。

プロファイルコンテナのローカルキャッシュを有効にする

このポリシーは、Citrix Profile Managementプロファイルコンテナのローカルキャッシュサポートを有効にします。ポリシーが**有効**に設定されている場合、各ローカルプロファイルは、そのCitrix Profile Managementプロファイルコンテナのローカルキャッシュとして機能します。プロファイルストリーミングが使用されている場合、ローカルにキャッシュされたファイルはオンデマンドで作成されます。それ以外の場合は、ユーザーログオン時に作成されます。ローカルキャッシュ機能

を使用するには、ユーザープロファイル全体をCitrix Profile Managementプロファイルコンテナに配置します。

プロファイルコンテナから除外するフォルダー

Citrix Profile Managementプロファイルコンテナから除外するフォルダーのリスト。

プロファイルコンテナに含めるフォルダー

親フォルダーが除外されている場合に、Citrix Profile Managementプロファイルコンテナに保持するフォルダーのリスト。

このリストのフォルダーは、除外されたフォルダーのサブフォルダーである必要があります。そうでない場合、この設定は機能しません。

プロファイルコンテナに含めるファイル

Citrix Profile Managementプロファイルコンテナに含めるファイルのリスト。

このリストのファイルは、除外されたフォルダー内にある必要があります。そうでない場合、この設定は機能しません。

プロファイルコンテナから除外するファイル

Citrix Profile Managementプロファイルコンテナから除外するファイルのリスト。

VHDディスクの圧縮を有効にする

Profile ManagementのVHDディスク圧縮を有効にします。有効にすると、特定の条件が満たされたときに、ユーザーのログオフ時にVHDディスクが自動的に圧縮されます。このポリシーにより、プロファイルコンテナ、OneDriveコンテナ、およびミラーフォルダコンテナによって消費されるストレージスペースを節約できます。

必要に応じて、利用可能なリソースに基づいて、詳細設定にある「**VHDディスク圧縮をトリガーする空き領域の比率**」、「**VHDディスク圧縮をトリガーするログオフ回数**」、および「**VHDディスク圧縮のデフラグを無効にする**」ポリシーを使用して、デフォルトのVHD圧縮設定と動作を調整できます。

プロファイルコンテナのVHD自動拡張を有効にする

プロファイルコンテナのVHD自動拡張を有効にするかどうかを指定できます。有効にすると、すべてのVHD自動拡張設定がプロファイルコンテナに適用されます。

構成の優先順位:

- このポリシーがここで構成されていない場合、.iniファイルの値が使用されます。
- このポリシーがここでも.iniファイルでも構成されていない場合、無効になります。

VHDコンテナへの排他的アクセスを有効にする

デフォルトでは、VHDコンテナは同時アクセスを許可します。この設定を有効にすると、一度に1つのアクセスのみが許可されます。この機能は、プロファイルコンテナとOneDriveコンテナに適用されます。

> **注:**
>
> コンテナベースのプロファイルソリューションでプロファイルコンテナに対してこの設定を有効にすると、「*プロファイルコンテナのマルチセッションライトバックを有効にする*」設定が自動的に無効になります。

構成の優先順位:

1. このポリシーがここで構成されていない場合、.iniファイルの値が使用されます。
2. このポリシーがここでも.iniファイルでも構成されていない場合、設定は無効になります。

ログオン時にプロファイルコンテナが利用できない場合、ユーザーをログオフする

ユーザーログオン時にプロファイルコンテナが利用できない場合、ユーザーを強制的にログオフさせ、(オプションで)ユーザーに表示されるエラーメッセージをカスタマイズできます。

構成の優先順位:

1. ここでこのポリシーが構成されていない場合、.iniファイルの値が使用されます。
2. ここでも.iniファイルでもこのポリシーが構成されていない場合、設定は無効になります。

プロファイルコンテナにアクセスするユーザーとグループ

プロファイルコンテナに対する`Read & Execute`権限を持つADドメインユーザーとグループを指定できます。デフォルトでは、プロファイルコンテナはその所有者のみがアクセスできます。

構成の優先順位:

1. このポリシーがここで構成されていない場合、.iniファイルの設定が使用されます。

2. このポリシーがここでも.iniファイルでも構成されていない場合、プロファイルコンテナはその所有者のみがアクセスできます。